Cisco TelePresence Network Systems 1.1 Design Guide

Cisco Validated Design

March 7, 2008

Cisco Validated Designs for deploying point-to-point Cisco TelePresence 1000 and 3000 systems in enterprise campus and branch, WAN, and VPN networks.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number: OL-14133-01

Cisco Validated Design

The Cisco Validated Design Program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit www.cisco.com/go/validateddesigns.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Cisco TelePresence Network Systems 1.1 Design Guide

CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 8

CHAPTER 9

CHAPTER 1

Cisco TelePresence Solution Overview

The Cisco TelePresence suite of virtual meeting solutions consists of the products and capabilities described in the following sections.

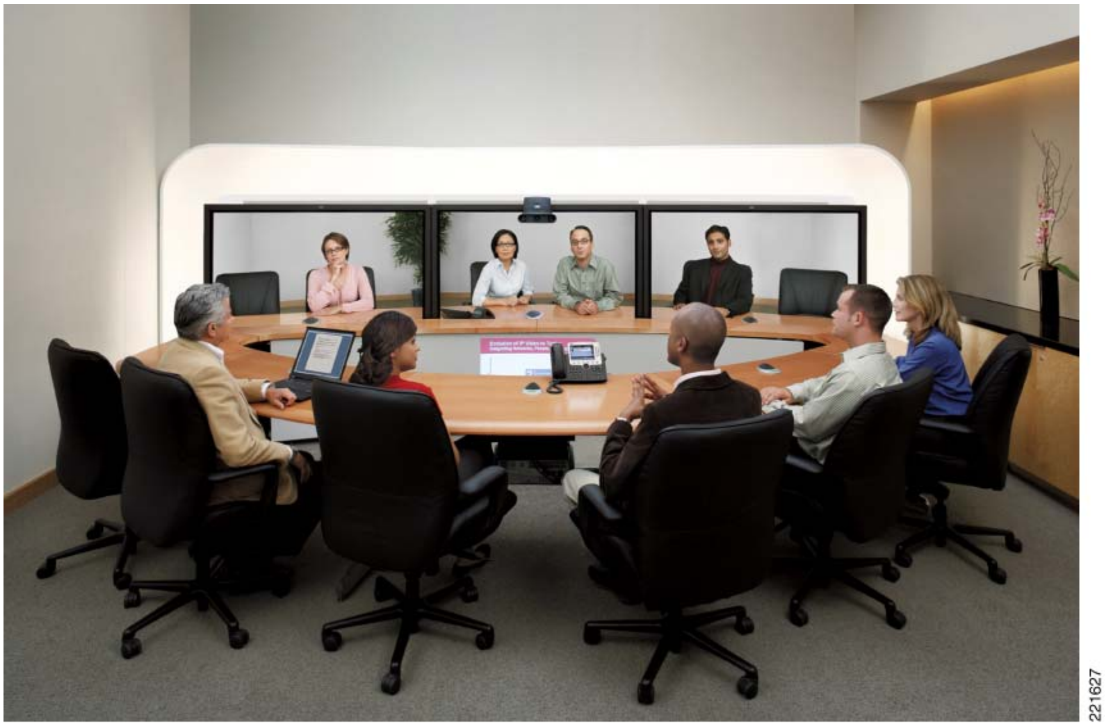
Cisco TelePresence System 3000

The Cisco TelePresence System 3000 (CTS-3000) is designed for large group meetings, seating up to 12 participants around a virtual table. It consists of:

- Three 65" high definition plasma displays
- Three high definition cameras
- Three wide band microphones and speakers
- A lighting shroud integrated around a purpose built meeting room table

Customers must furnish their own chairs. A Cisco 7970G IP phone is used to launch, control, and end the meeting.

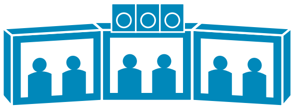
Figure 1-1 Cisco TelePresence System 3000



Participants are displayed life size with two participants per screen/table segment and multi-channel, discrete, full-duplex audio with echo cancellation per channel that appears to emanate from the person speaking. The unique table design also provides power and Ethernet ports in each table leg, so users do not have to hunt for power and network connections during the meeting. A projector is integrated under the middle section of the table for convenient viewing of PC graphics on the panel below the plasma displays. An optional WolfVision® document camera (not shown) may be installed in the ceiling so that objects and documents placed on the table surface may be viewed as well.

The CTS-3000 is represented by the icon in Figure 1-2.

Figure 1-2 CTS-3000 Icon



Cisco TelePresence System 1000

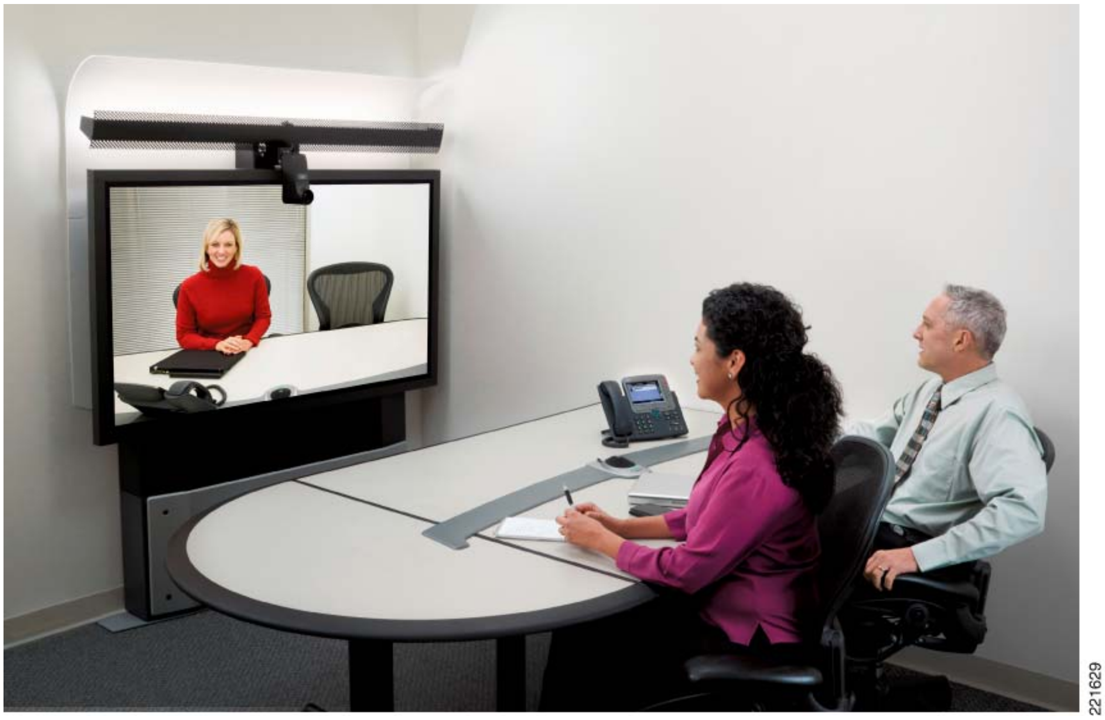
The Cisco TelePresence System 1000 (CTS-1000) is designed for smaller executive meeting room environments and one-on-one conversations, seating up to four participants at a virtual table. It consists of:

- One 65” high definition plasma display
- One high definition camera
- One wide band microphone and speaker

- A lighting shroud integrated over the display

The customer must furnish their own meeting room table and chairs. A Cisco 7970G IP phone is used to launch, control, and end the meeting.

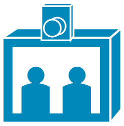
Figure 1-3 Cisco TelePresence System 1000



Participants are displayed life size with two participants per screen/table segment and full-duplex audio with echo cancellation that appears to emanate from the person speaking. An optional NEC® LCD display (not shown) may be installed on the table or on the wall for convenient viewing of PC graphics. An optional WolfVision® document camera (not shown) may be installed on the table so that objects and documents placed on the table surface may be viewed as well.

The CTS-1000 is represented by the icon in Figure 1-4.

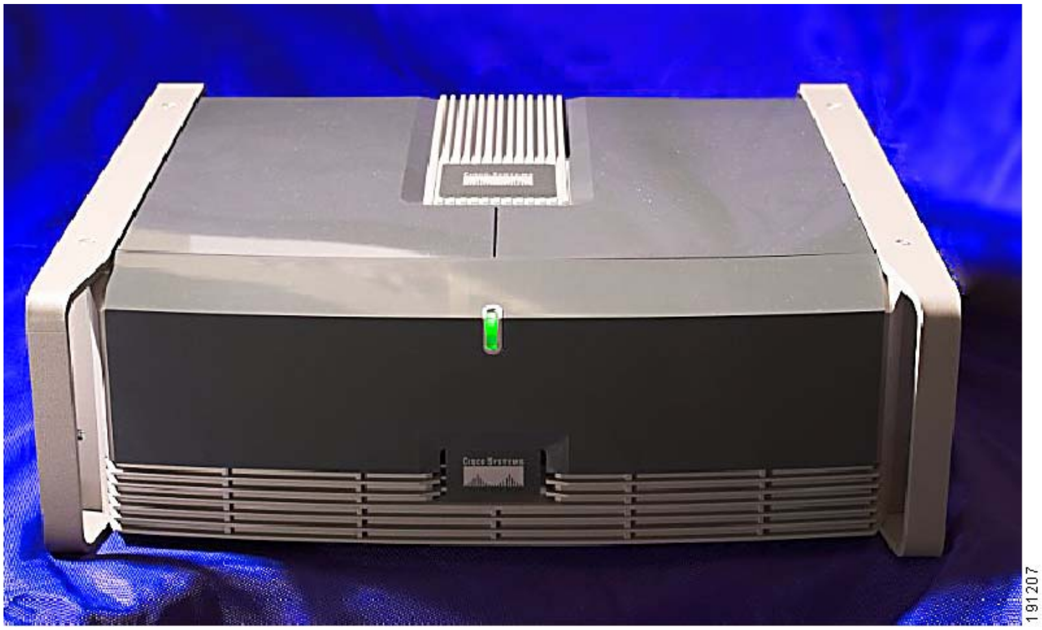
Figure 1-4 CTS-1000 Icon



Cisco TelePresence Codecs

One of the goals of Cisco TelePresence is to hide the technology from the user so that participants experience the meeting, not the technology. Hidden underneath the plasma displays in both the CTS-3000 and CTS-1000 solutions are the Cisco TelePresence Codecs. The CTS-3000 consists of one primary Codec and two secondary Codecs. The CTS-1000 consists of a single primary Codec.

Figure 1-5 Cisco TelePresence Codec



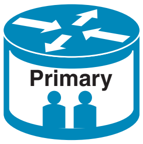
The Codec is the engine which drives the entire Cisco TelePresence solution. All displays, cameras, microphones, and speakers connect to it and it communicates with the network and handles all audio and video processing. The Codec runs a highly-integrated version of the Linux operating system on an embedded Compact Flash module and is managed via Secure Shell (SSH), Hyper-Text Transfer Protocol over Secure Sockets Layer (HTTPs) and Simple Network Management Protocol (SNMP). These Codecs make the Cisco TelePresence solutions an integrated part of Cisco Unified Communications by leveraging established techniques for network automation and Quality of Service (QoS), such as:

- Cisco Discovery Protocol (CDP) and 802.1Q for discovery and assignment to the appropriate Virtual LAN (VLAN).
- 802.1p and Differentiated Services Code Point (DSCP) for QoS.
- Automated provisioning of configuration and firmware from Cisco Unified Communications Manager.
- Session Initiation Protocol (SIP) for all call signaling communications.

From an administrator’s perspective, the entire Cisco TelePresence virtual meeting room appears as a single SIP endpoint on Cisco Unified Communications Manager. It is managed using tools and methodologies that are similar to those used for Cisco Unified IP Phones.

The Cisco TelePresence Codec is represented by the icon in Figure 1-6.

Figure 1-6 Cisco TelePresence Codec Icon



Industry-Leading Audio and Video Support

Cisco TelePresence utilizes industry-leading 1080p high-definition video resolution and 48kHz wide-band spatial audio. 720p high-definition is also supported for sites with restricted bandwidth availability.

Video Resolutions and Compression Formats

The Cisco TelePresence 65" displays and cameras natively support 1080p resolution and utilize digital media interfaces to connect to the Cisco TelePresence Codecs. This ensures the integrity of the video signal from end to end by eliminating the need for any digital/analog conversion.

Inside the Cisco TelePresence Codecs an onboard array of Digital Signal Processors (DSPs) encode the digital video signal from the cameras into Real-Time Transport Protocol (RTP) packets using the H.264 encoding and compression standard. The Cisco TelePresence Codecs can encode the video from the cameras at 1080p or 720p.

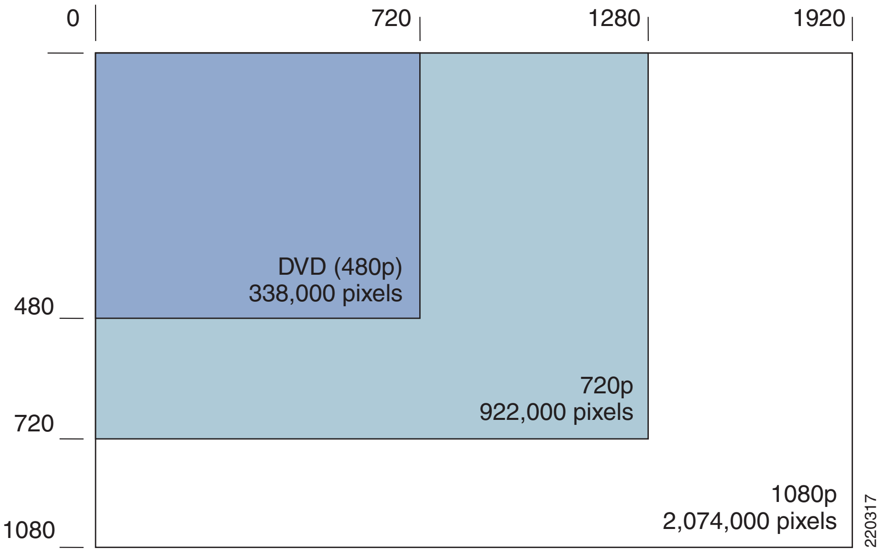
The quality of the video enjoyed by the meeting participants is a function of three variables:

- Resolution (i.e., number of pixels within the image)
- Frame rate (how often those pixels are re-drawn on the display)
- Degree of compression applied to the original video signal

Resolution

1080p provides the highest quality video image currently available on the market, supplying a resolution of 1920 x 1080 and 2,074,000 pixels per frame. 720p provides a resolution of 1280 x 720 and 922,000 pixels per frame. Compared with today's DVD standard video (480p) with a resolution of 720 x 480 and 338,000 pixels per frame, you can see the dramatic increase in resolution and pixel count. Figure 1-7 illustrates the difference between these three resolutions.

Figure 1-7 Video Resolutions



Frame Rate

The frame rate of the displayed video directly corresponds to how motion within the video is perceived by the participants. To maintain excellent motion handling, the Cisco TelePresence System encodes video at from the cameras at 30 frames per second (30fps or 30Hz). In addition, the codec video output signal to the 65” plasma displays utilizes progressive-scan technology to refresh the pixels at 60 fields per second (60Hz). This is twice as fast as traditional television and video conferencing equipment which utilize an interlaced refresh format.

Compression

Note that 1080p video uncompressed is approximately 1.5 Gbps. The Cisco TelePresence Codecs must take this native video received from the cameras and compress it to a more feasible bandwidth value in as little time as possible. As mentioned above, they achieve this by utilizing an array of DSPs to compress the original 1.5 Gbps video from each camera down to under 4 Mbps (per camera), representing a compression ratio of over 99%, and they achieve this in under 90ms. To provide maximum flexibility, the customer is provided with some amount of control over how much compression is applied. For each of the two resolution formats supported (1080p and 720p), the Cisco TelePresence System supports three quality levels. Each quality level is really a function of the degree of compression applied, and has a corresponding bandwidth value. For simplicity, these three levels are referred to as “good,” “better,” and “best.” The “best” quality level has the least amount of compression applied and therefore requires the most bandwidth, while the “good” quality level has the most amount of compression applied and requires the least amount of bandwidth.

Taking the three variables described above—resolution, frame rate, and the degree of compression applied—Table 1-1 illustrates the different quality settings supported by the Cisco TelePresence System and the requisite bandwidth required for each quality setting.

Table 1-1 Resolution, Quality, and Bandwidth Settings Supported (Video Only)

Resolution	**1080p**			**720p**		
Quality Level	Best	Better	Good	Best	Better	Good
Frame Rate	30	30	30	30	30	30
Bandwidth Required	4Mbps	3.5Mpbs	3Mpbs	3Mpbs	2Mpbs	1Mpbs

These bandwidth values apply per camera. Therefore, a CTS-3000 which has three cameras and three displays, running at 1080p resolution at the “best” quality level, requires 12Mbps of video bandwidth, whereas a CTS-1000 requires 4Mbps of video bandwidth. These bandwidth values do not include the audio channels or the auxiliary video channel for displaying PC graphics and document camera images. Therefore, a more complete bandwidth table is Table 4-1.

Audio Resolution and Compression Formats

The Cisco TelePresence System utilizes advanced microphone, speaker, and audio encoding technologies to preserve the quality and directionality of the audio so that it appears to emanate from the location of the person speaking at the same volume as it would be heard if that person were actually sitting across the table from you. Specifically, wideband spatial audio and multi-channel, full-duplex sound provides excellent voice projection and helps enable multiple simultaneous conversations, just like what typically occurs during an in-person meeting. Specially designed microphones eliminate sound interference.

The quality of the audio enjoyed by the meeting participants is a function of three variables:

- Frequency spectrum and decibel levels captured by the microphones
- Spatiality (i.e., directionality) of the audio
- Degree of compression applied to the original audio signal

Frequency Spectrum

The Cisco TelePresence microphones are designed to capture a 48kHz frequency spectrum of audio in a directional pattern that focuses on the people sitting directly in front of it and are geared to the decibel levels of human speech. Filters are designed into the microphones to eliminate interference from GSM and GPRS cellular signals and to eliminate certain frequencies generated by machinery such as the fans found in laptop computers and Heating, Ventilation, and Air Conditioning (HVAC) systems. Echo cancellation technology is built into the Cisco TelePresence Codec to eliminate cross-talk and double-talk.

The Cisco TelePresence speakers are designed to reproduce the same rich frequency spectrum and decibel level of human speech.

Spatiality

To preserve the spatiality (i.e., directional perception) of the audio, the CTS-3000 employs three individual microphones placed at specific locations of the virtual table, along with three individual speakers located under each display.

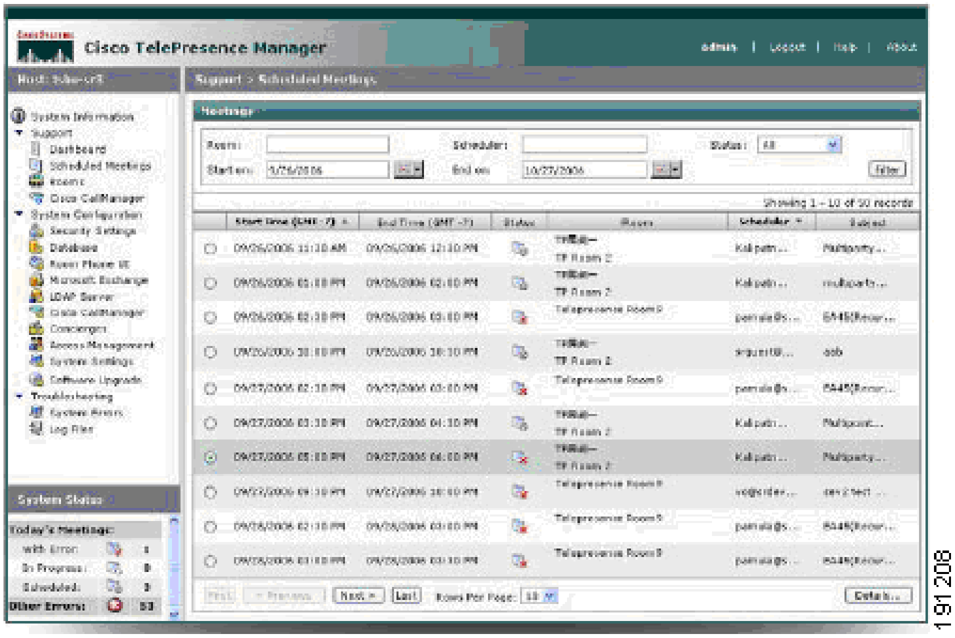
Compression

Inside the Cisco TelePresence Codecs an onboard array of DSPs encode the audio signal from the microphones into RTP packets using the Advanced Audio Coding-Low Delay (AAC-LD) encoding and compression standard. The resulting bandwidth required to transport the audio signals between the systems is 64kbps per microphone. Therefore, a CTS-3000 which has three microphones and speakers requires 192kbps of audio bandwidth, whereas the CTS-1000 requires 64kbps of audio bandwidth. Note that the Cisco TelePresence System also supports a fourth auxiliary audio channel which is used to transmit audio from a PC (used in conjunction with the projector when displaying PC graphics) or from an audio-only participant which is conferenced into the meeting using the Conference/Join softkey on the Cisco 7970G IP Phone (also known as the Audio Add-In feature). Therefore, a CTS-3000 can transmit and receive up to 256kbps of audio, as detailed in Table 4-1. The CTS-1000 transmits up to 128kbps of audio, but can receive up to 256kbps when participating in a meeting with a CTS-3000 (in such a configuration, the CTS-1000 receives three separate [64 kbps] primary audio streams from the CTS-3000, as well as a potentially additional [64 kbps] auxiliary audio stream).

Cisco TelePresence Manager

Cisco TelePresence Manager (CTSMGR) simplifies the scheduling and management of Cisco TelePresence virtual meeting room solutions. CTSMGR is a Linux-based appliance running on a Cisco 7800 Series Media Convergence Server platform. It is the middleware glue between Cisco Unified Communications Manager, the Cisco TelePresence meeting rooms, and the customer’s groupware calendaring and scheduling application (e.g., Microsoft Exchange/Outlook).

Figure 1-8 Cisco TelePresence Manager



Today's Meetings:

With Error:		1
In Progress:		0
Scheduled:		3
Other Errors:		53

Room:
Scheduler:
Status: All
Start on: 9/26/2006
End on: 10/27/2006
Rows Per Page: 10

Showing 1 - 10 of 50 records

	Start Time (GMT -7)	End Time (GMT -7)	Status	Room	Scheduler	Subject
○	09/26/2006 11:10 AM	09/26/2006 12:10 PM		[illegible] TP Room 2	Kalpath...	Multiparty...
○	09/26/2006 01:10 PM	09/26/2006 02:10 PM		[illegible] TP Room 2	Kalpath...	multiparty...
○	09/26/2006 02:10 PM	09/26/2006 03:10 PM		Telepresence Room 9	pamala@s...	6A45(Recur...
○	09/26/2006 10:10 PM	09/26/2006 10:10 PM		[illegible] TP Room 2	srgunt@...	asb
○	09/27/2006 02:10 PM	09/27/2006 03:10 PM		Telepresence Room 9	pamala@s...	6A45(Recur...
○	09/27/2006 03:10 PM	09/27/2006 04:10 PM		[illegible] TP Room 2	Kalpath...	Multipoint...
●	09/27/2006 05:10 PM	09/27/2006 06:10 PM		[illegible] TP Room 2	Kalpath...	Multiparty...
○	09/27/2006 09:10 PM	09/27/2006 10:10 PM		Telepresence Room 9	vo@srider...	dev 2 test ...
○	09/28/2006 02:10 PM	09/28/2006 03:10 PM		Telepresence Room 5	pamala@s...	6A45(Recur...
○	09/28/2006 03:10 PM	09/28/2006 03:10 PM		Telepresence Room 9	pamala@s...	6A45(Recur...

CTSMGR collects information about Cisco TelePresence systems from Cisco Unified Communications Manager and associates those systems to their physical location or conference room as defined in the customer's Microsoft Active Directory and Microsoft Exchange.[1] This allows users to schedule Cisco TelePresence meetings using their Microsoft Outlook group calendar and have that schedule automatically sent to the Cisco TelePresence systems involved in the call. Hence users can launch the Cisco TelePresence call with the push of one button, by simply selecting their meeting from the list of meetings shown on the Cisco Unified 7970G IP phone in the meeting room.

CTSMGR is managed via SSH, HTTPs, and SNMP. From an administrator’s perspective, CTSMGR is managed using tools and methodologies that are similar to those used with a Cisco Unified Communications Manager server.

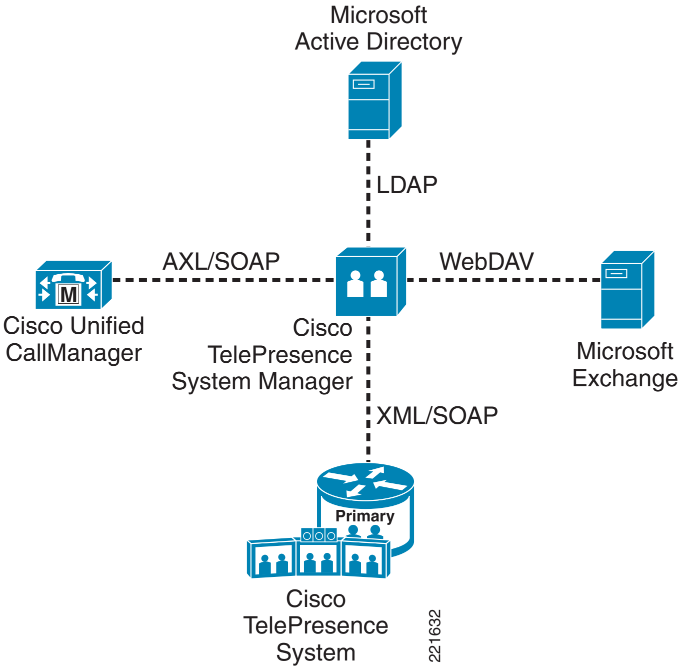
CTSMGR communicates with Cisco Unified Communications Manager using Application XML Layer/Simple Object Access Protocol (AXL/SOAP) and Computer Telephony Integration/Quick Buffer Encoding (CTI/QBE).

CTSMGR communicates with Microsoft Active Directory and Microsoft Exchange using Light-Weight Directory Access Protocol (LDAP) and Web-Based Distributed Authoring and Versioning (WebDAV) standards.

[1] In its first release, Cisco TelePresence Manager supports Microsoft Active Directory 2000 or 2003 and Microsoft Exchange 2003. Other directory services and groupware applications are planned for a future release.

CTSMGR communicates with the Cisco TelePresence Systems using eXtensible Markup Language/Simple Object Access Protocol (XML/SOAP).

Figure 1-9 Cisco TelePresence Manager Connectivity

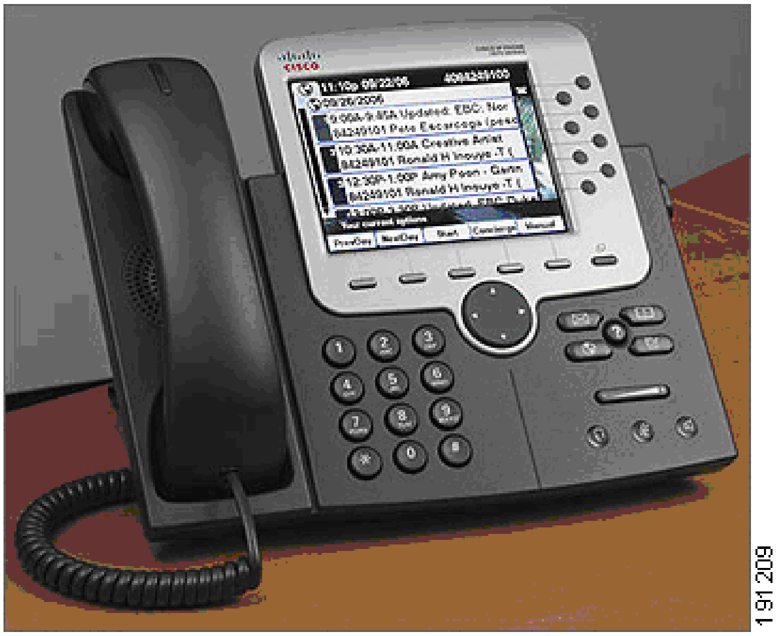


Cisco Unified 7970G IP Phone

To further enhance the meeting participants' experience of the meeting, cumbersome hand-held remote controls are eliminated, the cameras are fixed in their positions (no panning, tilting, or zooming controls), and the microphones are fixed in their positions on the table. There are virtually no moving parts or user interfaces that users must master to use a Cisco TelePresence meeting room.

Rather, the Cisco TelePresence meeting room solutions use a Cisco Unified 7970G IP phone, conveniently located on the table, to launch, control, and conclude meetings. This makes Cisco TelePresence as easy to use as a telephone. Using the high-resolution touch-screen display of the Cisco Unified 7970G IP phone, the user simply dials the telephone number of the Cisco TelePresence room with which they wish to have a meeting and the call is connected. Softkey menu buttons on the phone allow the user to place the call on hold or conference in an audio-only participant. When used in conjunction with Cisco TelePresence Manager, the schedule of meetings for the day are displayed on the phone and the user simply touches the appropriate location on the screen to launch that scheduled meeting.

Figure 1-10 Cisco Unified 7970G IP Phone

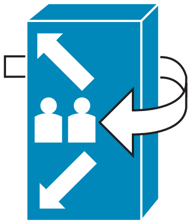


Cisco TelePresence Multipoint Solutions

To enable Cisco TelePresence meetings between more than two rooms, a Cisco TelePresence Multipoint Switch (CTMS) is required. The Cisco TelePresence Multipoint Switch is a purpose-built Linux-based appliance running on a Cisco 7800 Series Media Convergence Server platform. It provides high-capacity, low-latency multipoint switching for Cisco TelePresence only.

The CTMS is represented by the icon in Figure 1-11.

Figure 1-11 CTMS Icon



Cisco TelePresence Virtual Agent

The Cisco TelePresence Virtual Agent solution combines a Cisco TelePresence System 1000 (CTS-1000) with Cisco Unified Contact Center Express, a fully integrated contact center application supporting skills-based routing, built-in interactive voice response (IVR), queuing, and screen pops of customer data to agent desktops. The life-size, high-definition video, CD-quality audio, and interactive elements of the TelePresence solution give customers the feeling of being “in person” with a specialist agent, while the agent maintains all of the contact center functions they would expect.

The Cisco TelePresence Virtual Agent solution enables organizations to provide high-touch customer interactions and is well-suited to applications in the area of banking, retail, health care, administration, and reception.

CHAPTER 2

Connecting the Endpoints

Overview

As discussed in Chapter 1, "TelePresence Overview", there are many elements to Cisco TelePresence endpoint systems, including:

- TelePresence codecs (primary and secondary)
- Cisco Unified 7970G IP phone
- 65" plasma displays
- Cameras
- Microphones
- Speakers
- Auxiliary audio devices
- Auxiliary video devices

There are other elements, such as mounting brackets, furniture, cables, and power cords; the full assembly and connectivity instructions are covered in detail in the documentation.

The focus of this chapter is to provide an overview of how these main system elements are interconnected within CTS-1000 and CTS-3000 systems, as well as how these interact with the network infrastructure. Such an overview helps lay a foundational context for the design chapters that follow.

Connecting a CTS-1000 System

The CTS-1000 includes:

- One Cisco TelePresence codec (a primary codec)
- One Cisco Unified 7970G IP phone
- One 65" plasma display
- One high-definition camera
- One microphone
- One speaker
- One input for auxiliary audio
- One input for auxiliary video

The Cisco TelePresence primary codec is the center of the CTS-1000 and CTS-3000 systems. Essentially, all components connect to it and it, in turn, connects to the network infrastructure.

Specifically, the Cisco Unified 7970G IP phone connects to the TelePresence primary codec via an RJ-45 cable that provides it network connectivity and 802.3af Power-over-Ethernet (PoE).

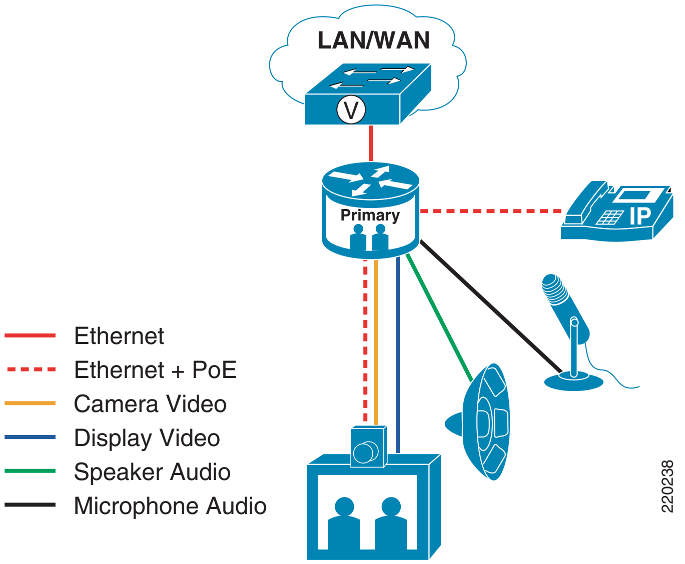
Another RJ-45 cable connects from the TelePresence primary codec to the camera, providing the camera with 802.3af PoE. A second cable from the primary codec to the camera provides video connectivity.

A video cable also connects the primary codec to the 65” plasma display. This cable is essentially an High Definition Multimedia Interface (HDMI) cable, but with a proprietary element for carrying management information instead of audio signals (as the audio signals are processed independently by the master codec).

Additionally, a speaker cable and a microphone cable connect the speaker and microphone to the primary codec, respectively. The primary codec also has inputs for auxiliary audio and auxiliary video.

Finally, an RJ-45 cable provides 10/100/1000 Ethernet connectivity from the primary codec to the network infrastructure. These interconnections for a CTS-1000 system are illustrated in Figure 2-1.

Figure 2-1 Connectivity Schematic for a CTS-1000 System



Connecting a CTS-3000 System

The CTS-3000 system includes:

- One Cisco TelePresence primary codec
- Two Cisco TelePresence secondary codecs
- One Cisco Unified 7970G IP phone
- Three 65” plasma displays
- Three high-definition cameras
- Three microphones
- Three speakers

- One input for auxiliary audio
- One input for auxiliary video

As with the CTS-1000 system, the primary codec is the central part of the CTS-3000 system to which all other components interconnect.

Specifically, the Cisco Unified 7970G IP phone connects to the TelePresence primary codec via an RJ-45 cable that provides it network connectivity and 802.3af Power-over-Ethernet (PoE).

A video cable connects the primary codec to the center 65” plasma display; another of these cables connects the right display to the (right) secondary codec, and a third connects the left display to the (left) secondary codec. As with the CTS-1000 system, this cable is essentially an HDMI cable, but with a proprietary element for carrying management information instead of audio signals (as the audio signals are processed independently by the master codec). Each of these secondary codecs, in turn, are connected to the primary codec via a RJ-45 cable; however, no 802.3af PoE is required over these Ethernet links as the secondary codecs have independent power supplies.

Three cameras are mounted on the central display and each camera is connected to its respective codec:

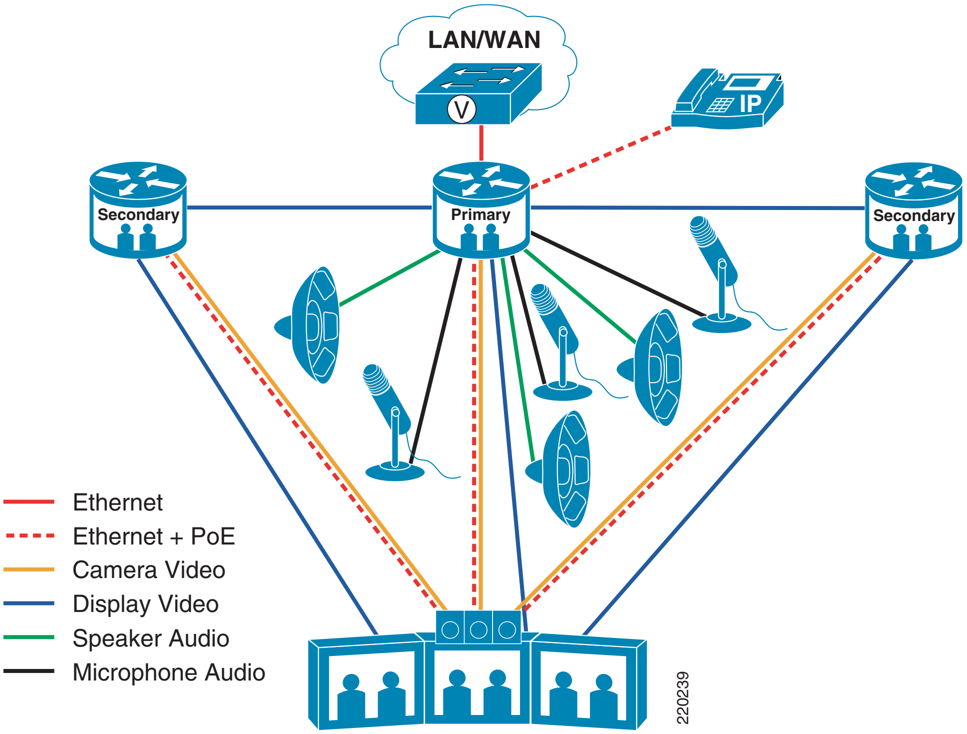
- The left camera is connected to the (left) secondary codec.
- The center camera is connected to the primary codec.
- The right camera is connected to the (right) secondary codec.

Each camera connects to its respective codec via two cables: a RJ-45 cable, which provides 802.3af PoE and network connectivity to the camera and a video cable to carry the video signals to the codec.

Additionally, three speaker cables and three microphone cables connect the (left, center, and right) speakers and (left, center, and right) microphones to the primary codec, respectively. The primary codec also has inputs for auxiliary audio and auxiliary video.

Finally, an RJ-45 cable provides 10/100/1000 Ethernet connectivity from the primary codec to the network infrastructure. These interconnections for a CTS-3000 system are illustrated in Figure 2-2.

Figure 2-2 Connectivity Schematic for a CTS-3000 System

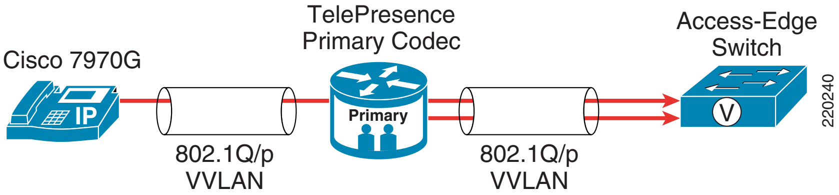


Cisco TelePresence Network Interaction

The primary codec is the interface between the CTS endpoint system and the network infrastructure. The primary codec connects to the network access edge switch via a RJ-45 10/100/1000 port. The access edge Catalyst switch that it connects to provides IP services, 802.1Q/p VLAN services, QoS services, and security services to the TelePresence endpoint.

Additionally, the primary codec provides a RJ-45 connection to the Cisco Unified 7970G IP phone, to which it supplies 802.3af PoE. When the IP phone boots up, it sends a Cisco Discovery Protocol (CDP) message to the primary codec. The codec receives this CDP message and passes it on to the access edge switch, supplementing it with its own CDP advertisement. The access edge switch and Codec exchange CDP messages and the switch (if configured according to best practice recommendations for IP telephony deployments) places the primary codec and the 7970G IP phone in a 802.1Q Voice VLAN (VVLAN), wherein 802.1Q/p Class of Service (CoS) markings are trusted. The primary Codec passes 802.1Q tags between the 7970G IP phone and the network access edge switch, extending the VVLAN all the way to the IP phone. This 802.1Q/p VVLAN assignment is illustrated in Figure 2-3.

Figure 2-3 Voice VLAN Extension Through Cisco TelePresence Primary Codec

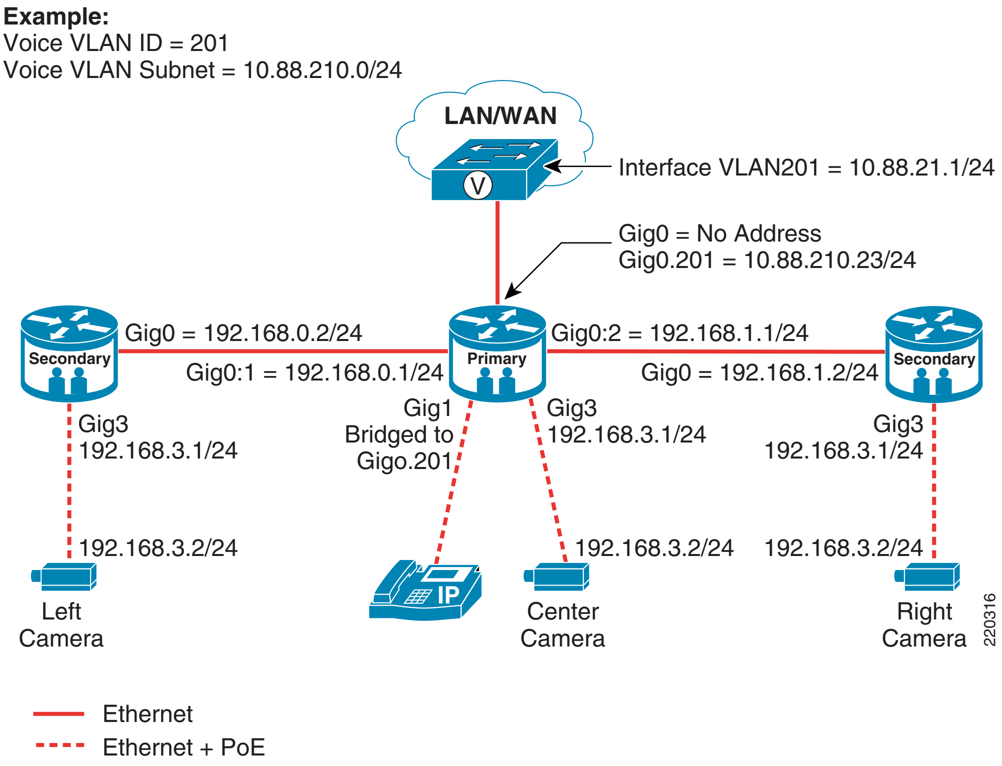


Note The above network interaction assumes that CDP is enabled and Voice VLANs are configured. If this is not the case, then then the network interaction begins with the DHCP requests described next.

The 7970G IP phone and the primary Codec each generate a Dynamic Host Configuration Protocol (DHCP) request to the network and are supplied with IP addresses (one for the IP phone and another for the primary codec). The DHCP server may also provide the IP phone and primary codec with the option 150 IP address of the Cisco Unified Communications Manager (CUCM) TFTP server, from which they download their configuration files and firmware loads. Alternatively, either or both of the devices may be configured with a static IP address and TFTP server address.

Additionally, it is important to note that the TelePresence systems utilize a private network for internal communications between the primary and secondary codecs, as well as between codecs and cameras. By default the internal address range used is 192.168.0.0/24 through 192.168.4.0/24; however, if the TelePresence codec receives a 192.168.x.x address from the network, then the internal private network will switch to 10.0.0.0/24 through 10.0.4.0/24. A default internal network IP address assignment is illustrated in Figure 2-4.

Figure 2-4 Default TelePresence Internal IP Addressing Scheme



Note Even though only 192.168.0.0/24 through 192.168.3.0/24 are illustrated in Figure 2-4, 192.168.4.0/24 is reserved within the system for future (internal) use.

Similarly, if the TelePresence system is using 10.0.0.0/24 through 10.0.3.0/24 for its internal networking address range, then 10.0.4.0/24 is reserved within the system for future (internal) use.

It is important to note three key points regarding the internal networking of TelePresence systems:

- From the network's perspective, the TelePresence primary codec appears as a single endpoint device with a single IP address (but remember, the 7970G IP Phone also appears as a separate endpoint device with its own IP address).
- The internal components (such as secondary codecs and cameras) do not receive a default gateway. Therefore, they cannot route beyond the primary codec.
- If the primary codec is using 192.168.0.0/24 through 192.168.4.0/24 as its internal networking addresses (which is the default), then it is not able to connect to external servers or endpoints that are using these same addresses (as it will attempt to reach such addresses via its internal network, not its external default gateway). Conversely, if the primary codec has been assigned an IP address from the network in the 192.168.x.x range, then it uses internal networking addresses in the range of 10.0.0.0/24 through 10.0.4.0/24, and similarly, is not able to connect to external servers or endpoints that may be using these same addresses. Table 2-1 summarizes the IP addressing best practices for networks supporting TelePresence.

Table 2-1 TelePresence Network IP Addressing Best Practices

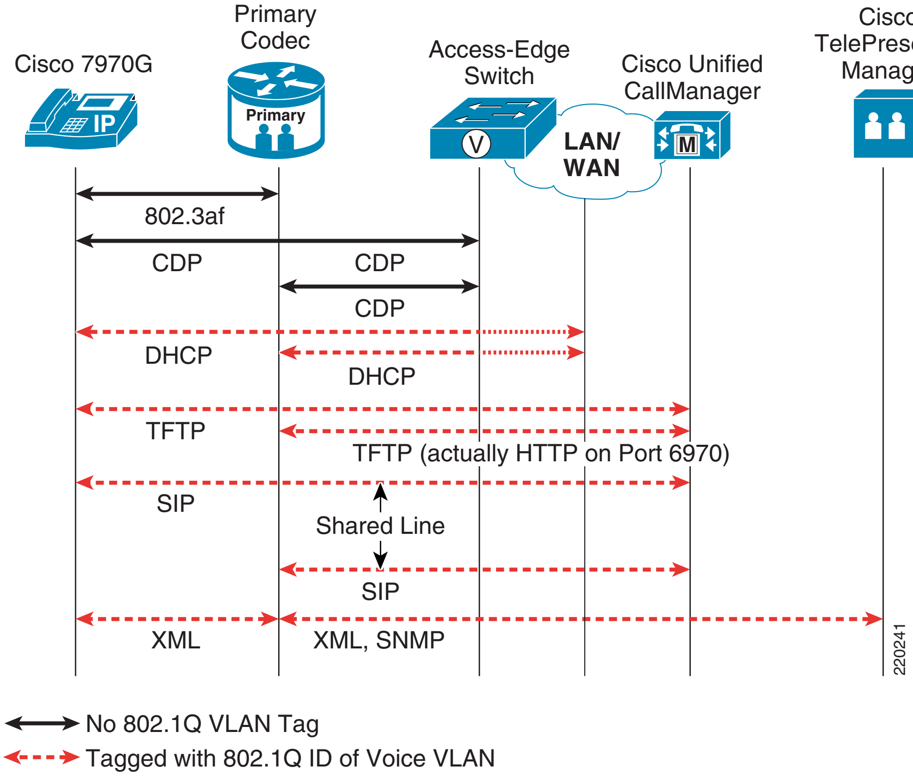
For Environments Where the CTS Uses 192.168.x.x for its Internal Communications. Avoid Using the Following Subnets:	For Environments Where the CTS Uses 10.x.x.x for its Internal Communications. Avoid Using the Following Subnets:
192.168.0.0/24	10.0.0.0/24
192.168.1.0.24	10.0.1.0/24
192.168.2.0.24	10.0.2.0/24
192.168.3.0.24	10.0.3.0/24
192.168.4.0.24	10.0.4.0/24

Provided there are no IP addressing issues, as described above, the IP phone and primary codec then initiate a Trivial File Transfer Protocol (TFTP) session with the Cisco Unified Communications Manager (CUCM) to download their configuration and firmware files.

Note While the Cisco 7970G IP phone uses TFTP for downloading its configuration and software, the Cisco TelePresence primary codec actually uses HTTP over port 6970 to achieve similar functionality.

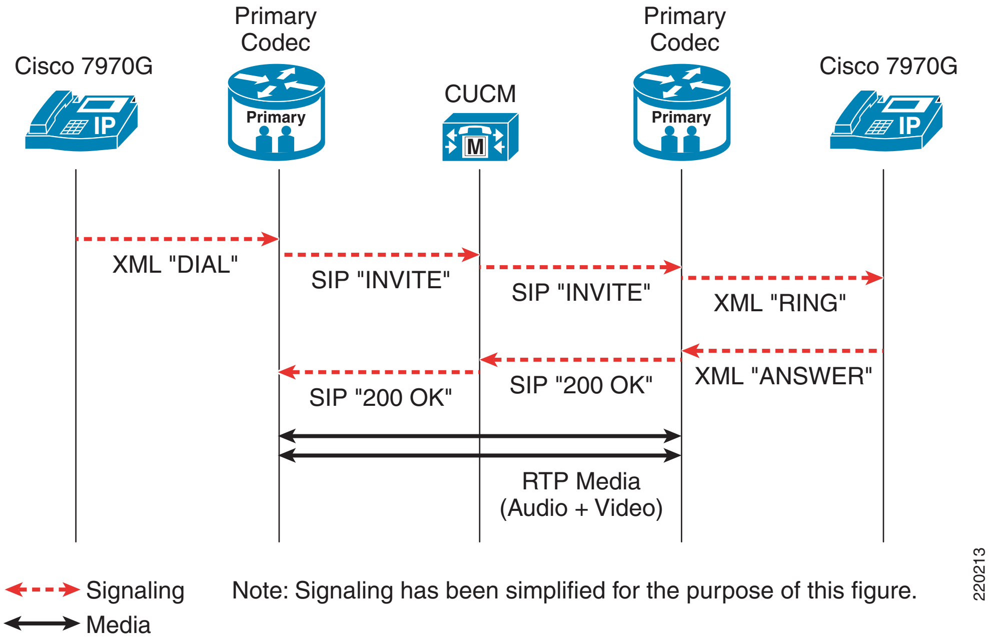
The primary codec then communicates with CUCM via Session Initiation Protocol (SIP). The Cisco 7970G IP Phone also communicates with CUCM via SIP, identifying itself as a shared line with the primary codec. Additional messaging occurs between the 7970G IP phone, the TelePresence primary codec, and the Cisco TelePresence Manager via Extensible Markup Language (XML), as well as Simple Network Management Protocol (SNMP). These network protocol interactions are illustrated in Figure 2-5.

Figure 2-5 Cisco TelePresence Network Control, Management, and Signaling Protocols



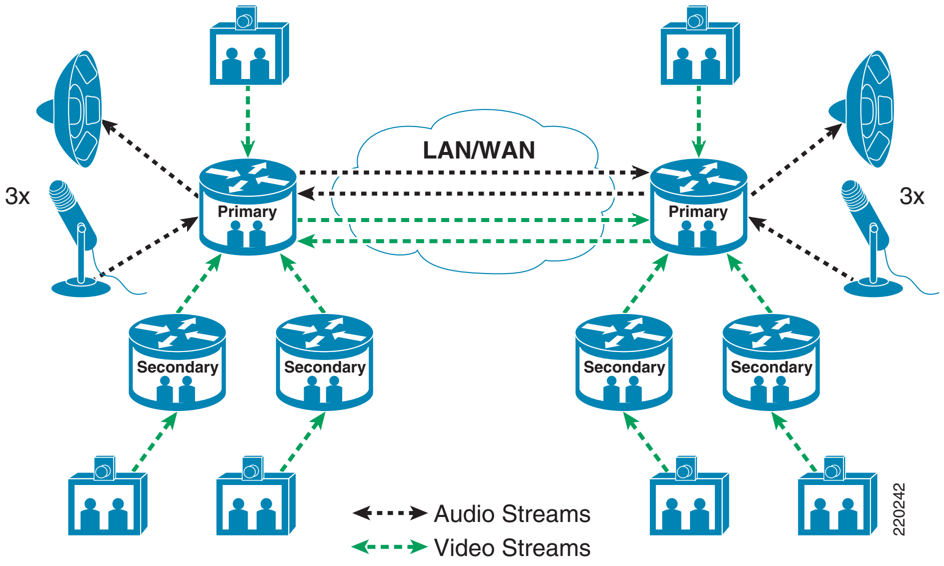
Once the TelePresence system has completed these protocol interactions, it is ready to place and receive calls. When a call is initiated, the Cisco 7970G IP phone sends an XML Dial message to its primary Codec, which forwards the request as a SIP Invite message to the Cisco Unified CallManager. The CallManager, in turn, forwards the SIP Invite message to the destination TelePresence Codec, which forwards the message as an XML Ring message to its 7970G IP phone. The TelePresence primary codec can be set to automatically answer the incoming call or can be set to send an incoming call alert to the 7970G IP phone. If set to auto-answer, the codec answers the call immediately and sends a SIP OK message to CallManager. If auto-answer is not enabled, when the user presses the Answer softkey on the 7970G IP phone, the 7970G IP phone replies with a XML Answer message to the receiving TelePresence primary codec, and the codec in turn sends a SIP 200 OK message to CallManager. The CallManager relays this SIP 200 OK message to the originating TelePresence primary Codec and the call is established. Real-time media, both audio and video, is then passed between the TelePresence primary Codecs over Real Time Protocol (RTP). The signaling and media paths for Cisco TelePresence are illustrated in Figure 2-6.

Figure 2-6 Cisco TelePresence Signaling and Media Paths



CTS-1000 systems send only one audio and one video stream (excluding auxiliary audio and video inputs for the moment). On the other hand, CTS-3000 primary Codecs process three separate audio and three separate video streams. However, these Codecs do not send three separate audio streams and three separate video streams over the network. Rather, CTS-3000 primary Codecs multiplex the three audio streams into one and three video streams into one, and hence send only a single audio and a single video stream over the network. These streams, in turn, are de-multiplexed by the receiving Codec. The multiplexing of audio and video streams performed by the CTS-3000 primary Codecs is illustrated in Figure 2-7. Auxiliary audio and video inputs are also multiplexed into the same audio and video streams. Therefore, in the case of the CTS-1000, the primary video and auxiliary video are multiplexed into one outgoing video stream; likewise the primary audio and auxiliary audio are multiplexed into one outgoing audio stream. In the case of the CTS-3000, the auxiliary video is treated as the 4th video channel and multiplexed in with the rest of the video; likewise the auxiliary audio is treated as the 4th audio channel and multiplexed in with the rest of the audio.

Figure 2-7 CTS-3000 Multiplexing of Audio and Video Streams



CHAPTER 3

TelePresence Network Deployment Models

Introduction

TelePresence systems—CTS-1000 or CTS-3000 systems—can be deployed over enterprise networks in one of four principle ways:

- Intra-Campus Deployment Model
- Intra-Enterprise Deployment Model
- MultiPoint Deployment Model (see Point-to-Point versus Multipoint)
- Inter-Enterprise/Business-to-Business Deployment Model

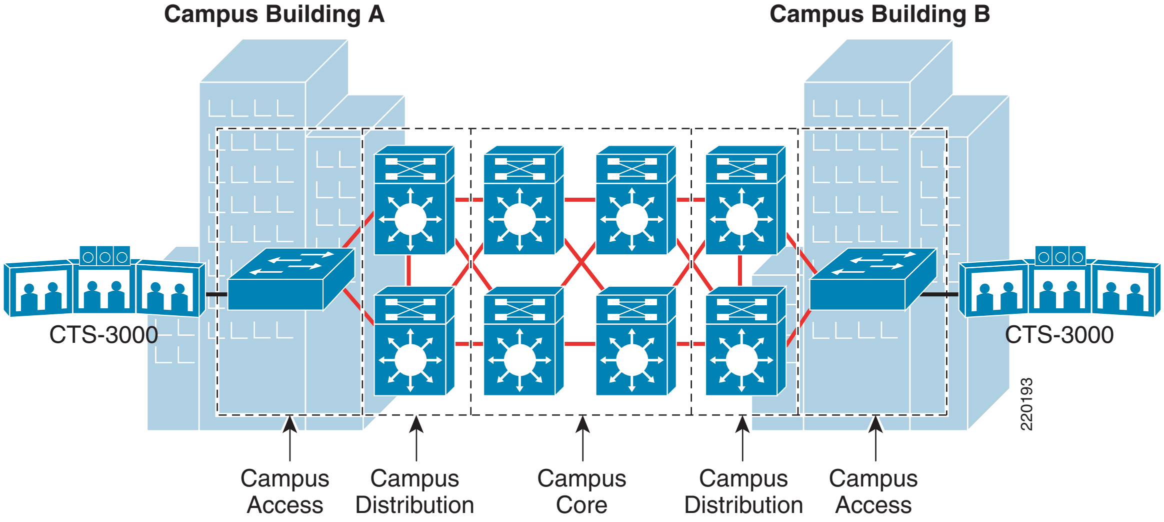
The following sections provide an overview of these TelePresence network deployment models, as well as logical phases of TelePresence deployments. In comparison, CUCM deployment models are discussed in detail in Chapter 9, "Call Processing Deployment Models."

Intra-Campus Deployment Model

The intra-campus network deployment model has TelePresence systems limited to a single enterprise campus or between sites interconnected via a high-speed (1 Gigabit or higher) Metropolitan Area Network (MAN). This deployment model is applicable for enterprises that have a large number of buildings within a given campus and employees who are often required to drive to several different buildings during the course of the day to attend meetings. Deploying multiple TelePresence systems intra-campus can reduce time lost by employees driving between buildings to attend meetings, without sacrificing meeting effectiveness, and thus improve overall productivity. The intra-campus deployment model is also commonly used in conjunction with the other two: where customers deploy multiple CTS rooms within their headquarters campus to meet demand for room availability as part of a global intra-enterprise or inter-enterprise deployment.

The network infrastructure of an intra-campus deployment model is predominantly Cisco Catalyst switches connecting via GigE or 10GigE links. The intra-campus TelePresence deployment model is illustrated in Figure 3-1.

Figure 3-1 TelePresence Intra-Campus Network Deployment Model



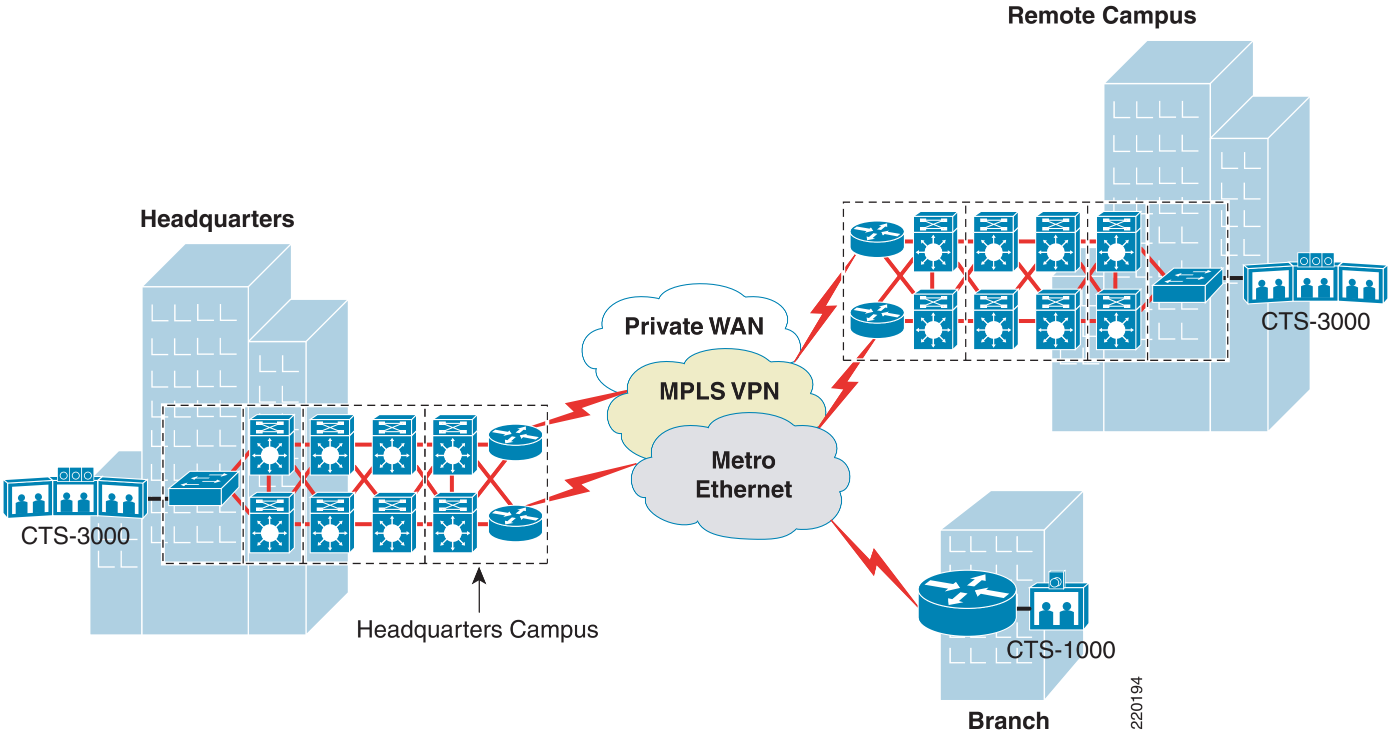
Intra-Enterprise Deployment Model

The intra-enterprise network deployment model for TelePresence systems connects not only buildings within a campus, but also geographically-separated campus sites and branch offices. The intra-enterprise model expands on the intra-campus model to include sites connected via a Wide Area Network (< 1 Gigabit).

The intra-enterprise deployment model is suitable for businesses that often require employees to travel extensively for internal meetings. Deploying TelePresence systems within the enterprise not only improves productivity—by saving travel time—but also reduces travel expenses. Furthermore, the overall quality of work/life is often improved when employees have to travel less.

The network infrastructure of an intra-enterprise deployment model is a combination of Cisco Catalyst switches within the campus and Cisco routers over the WAN, which may include private WANs, MPLS VPNs, or Metro Ethernet networks. WAN speeds may range from 45-Mbps DS3 circuits to 1 Gbps OC-192 circuits. The intra-enterprise TelePresence deployment model is illustrated in Figure 3-2.

Figure 3-2 TelePresence Intra-Enterprise Network Deployment Model



Cisco Powered Networks

A valuable consideration when selecting WAN/VPN service providers is to identify those that have achieved Cisco Powered Network designation. These providers have earned the Cisco Powered designation by maintaining high levels of network quality and by basing their WAN/VPN services end-to-end on Cisco equipment.

In addition, an increasing number of Cisco Powered providers have earned the QoS Certification for WAN/VPN services. This means that they have been assessed by a third party for the ability of their SLAs to support real-time voice and video traffic, and for their use of Cisco best practices for QoS. For a list of recommended service providers, see the following URL: http://www.cisco.com/cpn.

The use of Cisco Powered networks is recommended—but not mandatory—for Cisco TelePresence intra-enterprise deployments. The key is meeting the service levels required by TelePresence, which are detailed in Chapter 4, "Quality of Service Design for TelePresence."

Point-to-Point versus Multipoint

In both the intra-campus and inter-enterprise deployment models, customers may also deploy multipoint TelePresence resources to facilitate multi-site meetings (meetings with three or more TelePresence rooms). These resources may be located at any one of the campus locations or may be located within the service provider cloud as either a co-located resource or a managed/hosted resource.

Multipoint platforms and network design recommendations, such as additional bandwidth and latency considerations, Cisco TelePresence Multipoint switch considerations, scaling considerations, etc., will be discussed in further detail in a future revision of this guide.

Inter-Enterprise/Business-to-Business Deployment Model

The inter-enterprise network deployment model connects not only TelePresence systems within an enterprise, but also allows for TelePresence systems within one enterprise to call systems within another enterprise. The inter-enterprise model expands on the intra-campus and intra-enterprise models to include connectivity between different enterprises. This is also referred to as the business-to-business (B2B) TelePresence deployment model.

The inter-enterprise model offers the most flexibility and is suitable for businesses that often require employees to travel extensively for both internal and external meetings. In addition to the business advantages of the intra-enterprise model, the B2B TelePresence deployment model lets employees maintain high-quality customer relations, without the associated costs of travel time and expense.

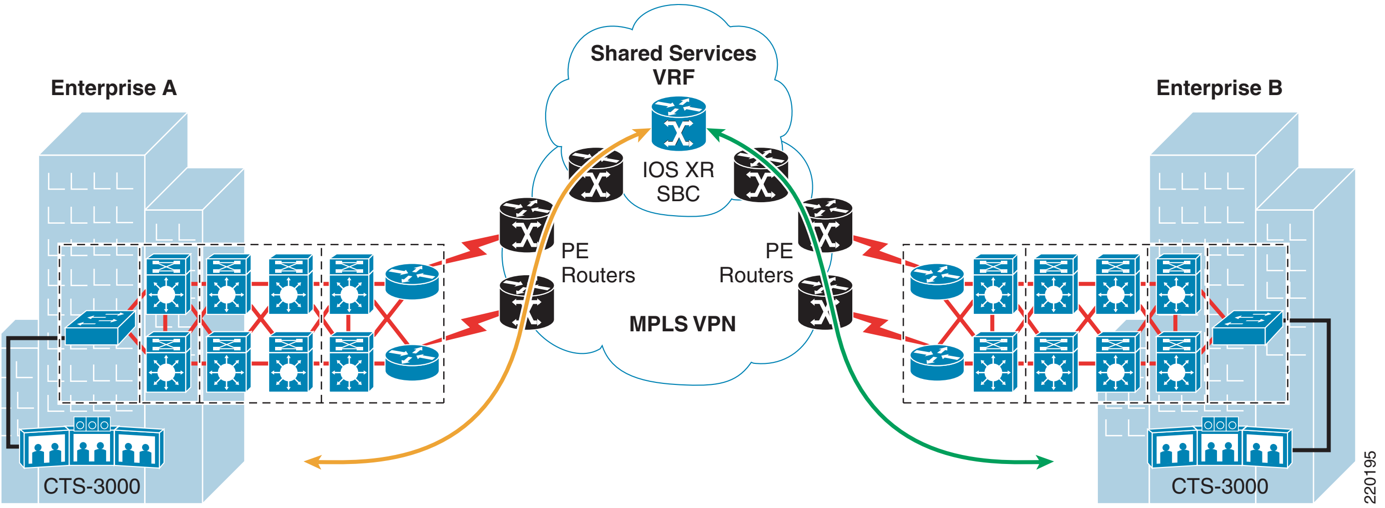
The network infrastructure of the inter-enterprise/B2B deployment model builds on the intra-enterprise model and requires the enterprises to share a common MPLS VPN service provider (SP). Additionally, the MPLS VPN SP must have a "shared services" Virtual Routing and Forwarding (VRF) instance provisioned with a Cisco IOS XR Session/Border Controller (SBC).

The Cisco SBC bridges a connection between two separate MPLS VPNs to perform secure inter-VPN communication between enterprises. Additionally, the SBC provides topology and address hiding services, NAT and firewall traversal, fraud and theft of service prevention, DDoS detection and prevention, call admission control policy enforcement and guaranteed QoS.

Note For more information about Cisco IOS XR SBC functionality and deployment models, refer to: http://www.cisco.com/univercd/cc/td/doc/product/ioxsoft/iox34/cgcr34/sbc_c34/sbc34abt.htm

The inter-enterprise/B2B TelePresence deployment model is illustrated in Figure 3-3.

Figure 3-3 TelePresence Inter-Enterprise Network Deployment Model



The initial release of the B2B solution requires a single SP to provide the shared services to enterprise customers, which includes the secure bridging of customer MPLS VPNs. However, as this solution evolves, multiple providers will be able to peer and provide B2B services between them, which will no longer require that both enterprise customers share the same SP.

Hosting and Management Options

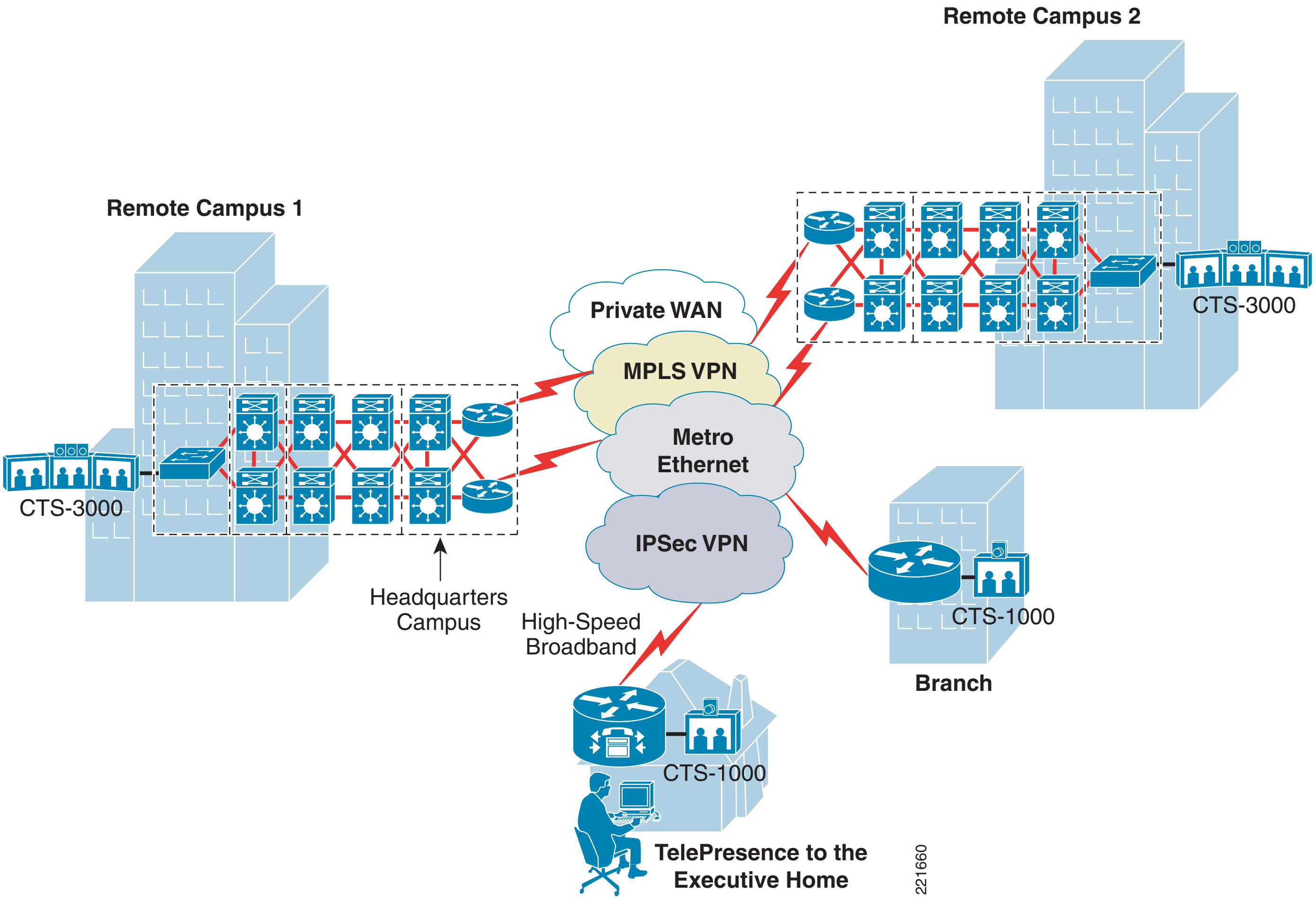
While the focus of this paper is TelePresence deployments within the enterprise, several of these options could be hosted or managed by SPs. For example, the Cisco Unified Communications Manager (CUCM) and Cisco TelePresence Manager (CTSMGR) servers and multipoint resources may be located on-premise at one of the customer campus locations, co-located within the SP network (managed by the enterprise) or hosted within the SP network (managed by the SP). However, with the exception of inter-VPN elements required by providers offering B2B TelePresence services, the TelePresence solution components and network designs remain fundamentally the same whether the TelePresence systems are hosted/managed by the enterprise or the SP.

TelePresence Phases of Deployment

As TelePresence technologies evolve, so too will the complexity of deployment solutions. Therefore, enterprise customers will likely approach their TelePresence deployments in phases, with the main phases of deployment being:

- Phase 1. Intra-Campus/Intra-Enterprise Deployments—Most enterprise customers will likely begin their TelePresence rollouts by provisioning (Point-to-Point) Intra-Enterprise TelePresence deployments. This model could be viewed as the basic TelePresence building block, on which more complex models may be added.
- Phase 2. Intra-Enterprise MultiPoint Deployments—As collaboration requirements may not always be facilitated with Point-to-Point models, the next logical phase of TelePresence deployment would be to introduce multipoint resources to the Intra-Enterprise deployment model. Phases 1 and 2 may often be undertaken simultaneously.
- Phase 3. Business-to-Business Deployments—To expand the application and business benefits of TelePresence meetings to include external (customer- or partner-facing) meetings, a Business-to-Business deployment model can be subsequently overlaid on top of either a Point-to-Point or a MultiPoint Intra-Enterprise deployment.
- Phase 4. TelePresence to the Executive Home—Due to the high executive-perk appeal of TelePresence and the availability of high-speed residential bandwidth options (such as fiber to the home), some executives may benefit greatly from deploying TelePresence units to their residences. Technically, this is simply an extension of the Intra-Enterprise model, but for the purposes of this document it is viewed as a separate phase due to the unique provisioning and security requirements posed by such residential TelePresence deployments.

Figure 3-4 TelePresence to the Executive Home (an Extension of the Intra-Enterprise Deployment Model)



CHAPTER 4

Quality of Service Design for TelePresence

Overview

A major benefit of Cisco's TelePresence solution over competitive offerings is that the realtime, high-definition video and audio are transported over a converged IP network rather than a dedicated network (although dedicated networks are also supported). The key enabling technology to accomplish this convergence is Quality of Service (QoS).

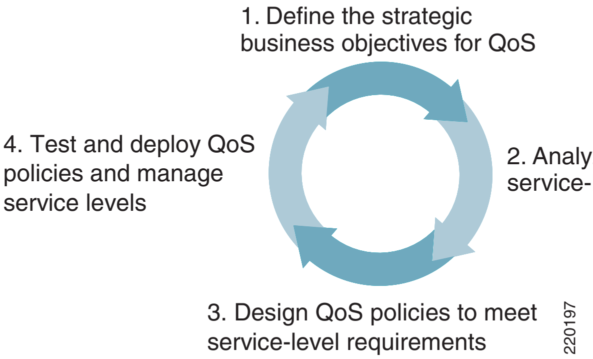
QoS technologies refer to the set of tools and techniques to manage network resources, such as bandwidth, latency, jitter, and loss. QoS technologies allow different types of traffic to intelligently contend for network resources. For example, voice and realtime video—such as TelePresence—may be granted strict priority service, while some critical data applications may receive (non-priority) preferential services and some undesired applications may be assigned deferential levels of service. Therefore, QoS is a critical, intrinsic element for the successful network convergence of voice, video, and data.

There are four principal phases to a successful QoS deployment:

- Clearly define the strategic business objectives of the QoS deployment.
- Analyze application service-level requirements.
- Design (and test) QoS policies to accommodate service level requirements.
- Roll out the QoS policies and monitor service levels.

These phases are sequential and the success of each subsequent phase directly depends on how well the previous phase has been addressed. Furthermore, the entire process is generally cyclical, as business applications and objectives evolve over time and their related QoS policies periodically need to be adjusted to accommodate (see Figure 4-1).

Figure 4-1 The Four Phases of Successful QoS Deployments


1. Define the strategic business objectives for QoS
2. Analyze application service-level requirements
3. Design QoS policies to meet service-level requirements
4. Test and deploy QoS policies and manage service levels
220197

The following sections examine how each of these phases relate to a successful deployment of QoS for TelePresence.

Defining the Strategic Business Objective for QoS for TelePresence

QoS technologies are the enablers for business/organizational objectives. Therefore, the way to begin a QoS deployment is not to activate QoS features simply because they exist, but to start by clearly defining the QoS-related business objectives of the organization.

For example, among the first questions that arise during a QoS deployment are: How many traffic classes should be provisioned for? And what should they be? To help answer these fundamental questions, QoS-related organizational objectives need to be defined, such as:

- Is the business objective to enable TelePresence only? Or is VoIP also required to run over the converged network?
- Are there any non-realtime applications that are considered critical to the core business objectives? If so, what are they?
- Are there applications which should be squelched (i.e., deferential treatment)? If so, what are they?

The answers to these questions define the applications that require QoS policies, either preferential QoS or deferential QoS. Each application that has a unique service level requirement—whether preferential or deferential—requires a dedicated service class to deliver and guarantee the requisite service levels.

Additionally, Cisco offers a non-technical recommendation for this first phase of a successful QoS deployment, namely to always seek executive endorsement of the QoS business objectives prior to design and deployment. This is because QoS is a system of managed application preference and as such often includes political and organizational repercussions when implemented. To minimize the effects of these non-technical obstacles to deployment, it is recommended to address these political and organizational issues as early as possible, garnishing executive endorsement whenever possible.

Analyzing the Service Level Requirements of TelePresence

Once the applications requiring QoS have been defined by the organization business objectives, then the network administrators must carefully analyze the specifics of the service levels required by each application to be able to define the QoS policies to meet them. The service level requirements of realtime applications, such as TelePresence, are defined by the following four parameters:

- Bandwidth
- Latency (delay)
- Jitter (variations in delay)
- Packet loss

TelePresence Bandwidth Requirements

Cisco TelePresence systems are currently available in one screen (CTS-1000) and three screen (CTS-3000) configurations. A CTS-3000 obviously has greater bandwidth requirements than a CTS-1000, but not necessarily by a full-factor of three, as will be shown. Furthermore, the resolution of each CTS-1000 or CTS-3000 system can be set to 720p or 1080p (full HDTV); the resolution setting also significantly impacts the bandwidth requirements of the deployed TelePresence solution.

As discussed in Chapter 1, "Cisco TelePresence Solution Overview," Cisco TelePresence has even more levels of granularity in overall image quality within a given resolution setting, as the motion handling quality can also be selected. Therefore, TelePresence supports three levels of motion handling quality within a given resolution, specifically 720p-Good, 720p-Better, and 720p-Best, as well as 1080p-Good, 1080p-Better, and 1080p-Best. Each of these levels of resolution and motion handling quality results in slightly different bandwidth requirements, as detailed in Table 4-1.

To keep the following sections and examples simple to understand, only two cases will be broken down for detailed analysis: 720p-Good and 1080p-Best.

Let's break down the bandwidth requirements of the maximum bandwidth required by a CTS-1000 system running at 720p-Good, with an auxiliary video stream (for sharing Microsoft PowerPoint or other collateral via the data-projector) and an auxiliary audio stream (for at least one additional person conferenced in by an audio-only bridge). The bandwidth requirements by component are:

1 primary video streams @ 1 Mbps:	1,000 Mbps (1 Mbps)
1 primary audio streams @ 64 Kbps:	64 Kbps
1 auxiliary video stream:	500 Kbps
1 auxiliary audio stream:	64 Kbps
Total audio and video bandwidth (not including burst and network overhead):	1,628 Kbps (1.628 Mbps)

The total bandwidth requirements—without network overhead—of such a scenario would be 1.628 Mbps. However a 10% burst factor on the video channel, along with the IP/UDP/RTP overhead (which combined amounts to 40 bytes per packet) must also be taken into account and provisioned for, as must media-specific Layer 2 overhead. In general, video—unlike voice—does not have clean formulas for calculating network overhead because video packet sizes and rates vary proportionally to the degree of motion within the video image itself. From a network administrator's point of view, bandwidth is always provisioned at Layer 2, but the variability in the packet sizes and the variety of Layer 2 mediums the packets may traverse from end-to-end make it difficult to calculate the real bandwidth that should be provisioned at Layer 2. Cisco TelePresence video packets average 1,100 bytes per packet. However, the conservative rule of thumb that has been thoroughly tested and widely deployed is to overprovision video bandwidth by 20%. This accommodates the 10% burst and the Layer 2-Layer 4 network overhead.

With this 20% overprovisioning rule applied, the requisite bandwidth for a CTS-1000 running at 720p-Good becomes 2 Mbps (rounded).

Now, let's break down the maximum bandwidth required by a CTS-3000 system running at full 1080p-Best, with an auxiliary video stream and an auxiliary audio stream.

The detailed bandwidth requirements are:

3 primary video streams @ 4 Mbps each:	12,000 Kbps (12 Mbps)
3 primary audio streams @ 64 Kbps each:	192 Kbps
1 auxiliary video stream:	500 Kbps
1 auxiliary audio stream:	64 Kbps
Total audio and video bandwidth (not including burst and network overhead):	12,756 Kbps (12.756 Mbps)

With the 20% overprovisioning rule applied, the requisite bandwidth for a CTS-3000 running at 1080p-Best becomes 15 Mbps (rounded).

Table 4-1 shows the bandwidth requirements, with and without network overhead, of CTS-1000 and CTS-3000 systems running at 720p and 1080p with all grades of motion handling quality (Good, Better, and Best).

Table 4-1 Bandwidth Requirements (Including Audio, Video, and Packet Overhead)

Resolution	1080p	1080p	1080p	720p	720p	720p
Motion Handling	Best	Better	Good	Best	Better	Good
Video per Screen (kbps)	4000	3500	3000	3000	2000	1000
Audio per Microphone (kbps)	64	64	64	64	64	64
Auto Collaborate video channel (kbps)	500	500	500	500	500	500
Audio Add-In channel (kbps)	64	64	64	64	64	64
CTS-1000 Total Audio and Video (kbps)	4,628[1]	4,128[1]	3,628[1]	3,628[1]	2,628[1]	1,628[1]
CTS-3000 Total Audio and Video (kbps)	12,756	11,256	9,756	9,756	6,756	3,756
CTS-1000 total bandwidth (Including Layer 2-Layer 4 overhead)	5.5 Mbps[1]	4.9 Mbps[1]	4.3 Mbps[1]	4.3 Mbps[1]	3.2 Mbps[1]	2 Mbps[1]
CTS-3000 total bandwidth (Including Layer 2–Layer 4 overhead)	15.3 Mbps	13.5 Mbps	11.7 Mbps	11.7 Mbps	8.1 Mbps	4.5 Mbps

[1] The CTS-1000 transmits up to 128kbps of audio, but can receive up to 256kbps when participating in a meeting with a CTS-3000.

Note that these bandwidth numbers represent the worst-case scenarios (i.e., peak bandwidth transmitted during periods of maximum motion within the encoded video). Normal use (i.e., average bandwidth), with users sitting and talking and gesturing naturally, typically generates only about 60-80% of these maximum bandwidth rates. This means that a CTS-3000 running at 1080-Best averages only 10-12 Mbps and a CTS-1000 running at 720-Good averages only 1.2-1.6 Mbps.

Burst Requirements

So far, we have discussed bandwidth in terms of bits per second (i.e., how much traffic is sent over a one second interval). However, when provisioning bandwidth and configuring queuing, shaping, and policing commands on routers and switches, burst must also be taken into account. Burst is defined as the amount of traffic (generally measured in bytes) transmitted per millisecond which exceeds the per-second average. For example, a CTS-3000 running at 1080p-Best at approximately 15 Mbps divides evenly into approximately 1,966 bytes per millisecond (15 Mbps ÷ 1,000 milliseconds).

Cisco TelePresence operates at 30 frames per second. This means that every 33ms a video frame is transmitted; we refer to this as a frame interval. Each frame consists of several thousand bytes of video payload, and therefore each frame interval consists of several dozen packets, with an average packet size of 1,100 bytes per packet. However, because video is variable in size (due to the variability of motion in the encoded video), the packets transmitted by the codec are not spaced evenly over each 33ms frame interval, but rather are transmitted in bursts measured in shorter intervals. Therefore, while the overall bandwidth (maximum) averages out to 15 Mbps over one second, when measured on a per millisecond basis the packet transmission rate is highly variable, and the number of bytes transmitted per millisecond for a 15 Mbps per second call bursts well above the 1,966 bytes per millisecond average. Therefore, adequate burst tolerance must be accommodated by all switch and router interfaces in the path (platform-specific recommendations are detailed in the subsequent design chapters).

TelePresence Latency Requirements

Cisco TelePresence has a network latency target of 150 ms; this target does not include codec processing time, but purely network flight time.

There may be scenarios, however, where this latency target may not always be possible to achieve, simply due to the laws of physics and the geographical distances involved. Therefore, TelePresence codecs have been designed to sustain high levels of call quality even up to 200 ms of latency. Beyond this threshold (which we refer to as ‘Latency Threshold 1’) a warning message appears on the screen indicating that network conditions may be affecting call quality. Nonetheless, the call continues. If network latency exceeds 400 ms (which we refer to as ‘Latency Threshold 2’) another warning message appears on the screen and the call quality steadily degrades as latency increases. Visually, the call quality is the same, but aurally the lagtime between one party speaking and the other party responding becomes unnaturally excessive. In the original release of the TelePresence codec, calls were self-terminated by the codec if network latency increased beyond 400 ms. However, due to some unique customer requirements, such as some customers looking at provisioning TelePresence calls over satellite circuits, this behavior changed for release 1.1 of the codec, in which the calls were no longer terminated if Latency Threshold 2 was exceeded. Nonetheless, should customers choose to provision TelePresence over such circuits, user expectations need to be adjusted accordingly.

Network latency time can be broken down further into fixed and variable components:

- Serialization (fixed)
- Propagation (fixed)
- Queuing (variable)

Serialization refers to the time it takes to convert a Layer 2 frame into Layer 1 electrical or optical pulses onto the transmission media. Therefore, serialization delay is fixed and is a function of the line rate (i.e., the clock speed of the link). For example, a 45 Mbps DS3 circuit would require 266 µs to serialize a 1500 byte Ethernet frame onto the wire. At the circuit speeds required for TelePresence (generally speaking DS3 or higher), serialization delay is not a significant factor in the overall latency budget.

The most significant network factor in meeting the latency targets for TelePresence is propagation delay, which can account for over 90% of the network latency time budget. Propagation delay is also a fixed component and is a function of the physical distance that the signals have to travel between the originating endpoint and the receiving endpoint. The gating factor for propagation delay is the speed of light: 300,000 km/s or 186,000 miles per second. Roughly speaking, the speed of light in an optical fiber is slightly less than one third the speed of light in a vacuum. Thus, the propagation delay works out to be approximately 6.3 µs per km or 8.2 µs per mile.

Another point to keep in mind when calculating propagation delay is that optical fibers are not always physically placed over the shortest path between two geographic points, especially over transoceanic links. Due to installation convenience, circuits may be hundreds or thousands of kilometers longer than theoretically necessary.

Nonetheless, the network flight-time budget of 150 ms allows for nearly 24,000 km or 15,000 miles worth of propagation delay (which is approximately 60% of the earth's circumference); the theoretical worst-case scenario (exactly half of the earth's circumference) would require only 126 ms. Therefore, this latency target should be achievable for virtually any two locations on the planet, given relatively direct transmission paths. However, for some of the more extreme scenarios, user expectations may have to be set accordingly, as there is little a network administrator can do about increasing the speed of light.

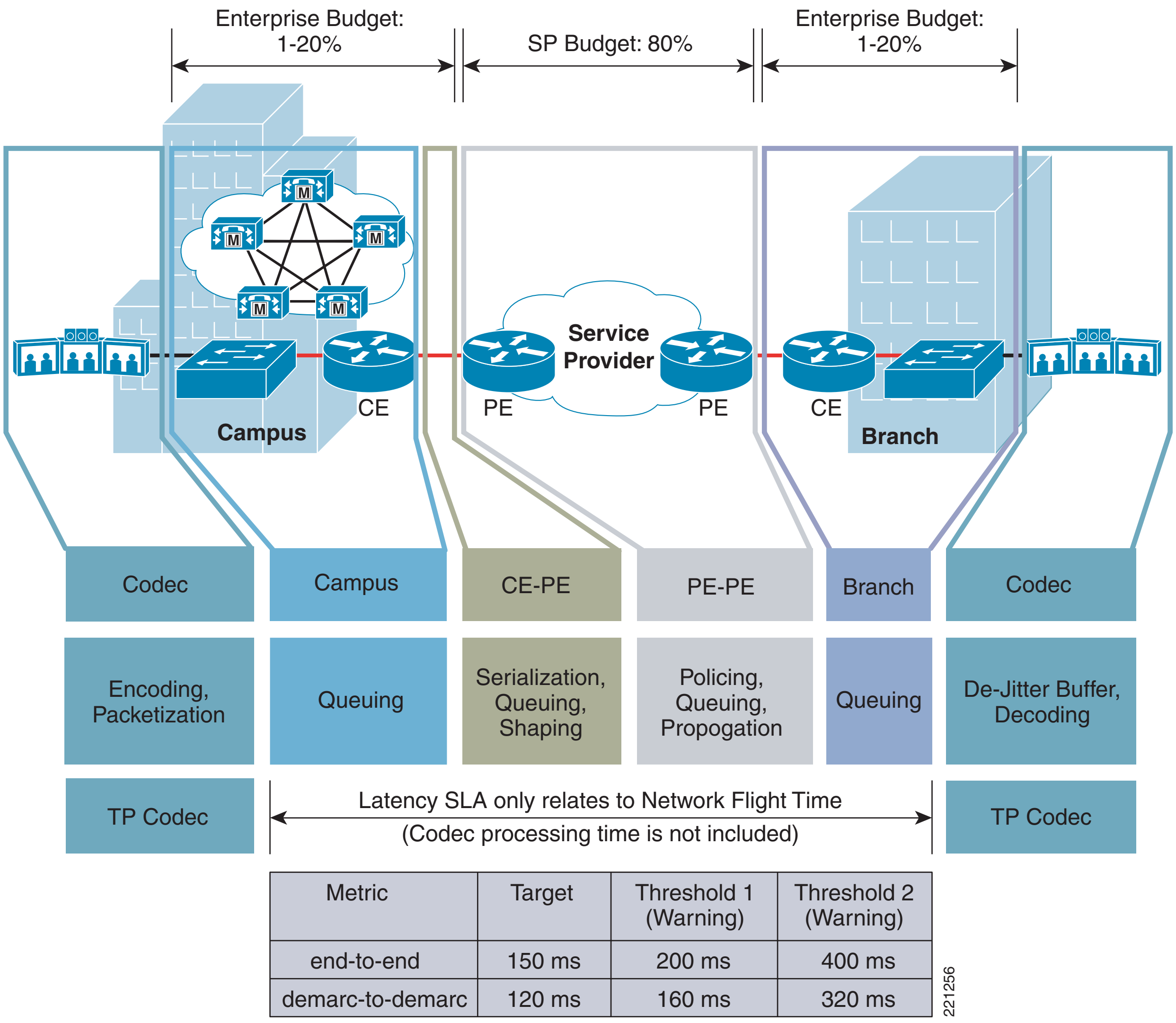
Given the end-to-end latency targets and thresholds for TelePresence, the network administrator also must know how much of this budget is to be allocated to the service provider and how much to the enterprise. The general recommendation for this split is 80:20, with 80% of the latency budget allocated to the service provider (demarc-to-demarc) and 20% to the enterprise (codec-to-demarc on one side and demarc-to-codec on the other). However, some enterprise networks may not require a full 20% of the latency budget and thus may reallocate their allowance to a 90:10 service provider-to-enterprise split, or whatever the case may be. The main point is that a fixed budget needs to be clearly apportioned to both the service provider and to the enterprise, such that the network administrators can design their networks accordingly. Given the target (150ms), threshold1 (200ms), and the service provider-enterprise split of 80:20 or 90:10, it is recommended that SPs engineer their network to meet the target, but base their SLA on threshold1. Threshold1 provides global coverage between any two sites on the planet and allows the SP to offer a 100% guarantee that their network (demarc-to-demarc) will never exceed 160ms (80% of threshold1).

Another point to bear in mind here is the additional latency introduced by multipoint resources. Latency is always measured from end-to-end (i.e., from codec1 to codec2). However, in a multipoint call the media between the two codecs traverses a Multipoint Switch. The multipoint switch itself introduces approximately 20ms of latency, and the path from codec1 to the MS and from the MS to codec2 may be greater than the path between codec1 and codec2 directly, depending on the physical location of the MS. Therefore, when engineering the network with respect to latency, one must calculate both scenarios for every TelePresence System deployed: one for the path between each system and every other system for point-to-point call, and a second for the path between each system, through the MS, to every other system.

The final TelePresence latency component to be considered is queuing delay, which is variable. Queuing delay is a function of whether a network node is congested and what the scheduling QoS policies are to resolve congestion events. Given that the latency target for TelePresence is very tight and, as has been shown, the majority of factors contributing to the latency budget are fixed, careful attention has to be given to queuing delay, as this is the only latency factor that is directly under the network administrator's control via QoS policies.

The latency targets, thresholds and service provider-to-enterprise splits are illustrated in Figure 4-2.

Figure 4-2 Network Latency Target and Thresholds for Cisco TelePresence



Metric	Target	Threshold 1 (Warning)	Threshold 2 (Warning)
end-to-end	150 ms	200 ms	400 ms
demarc-to-demarc	120 ms	160 ms	320 ms

TelePresence Jitter Requirements

Cisco TelePresence has a peak-to-peak jitter target of 10 ms. Jitter is defined as the variance in network latency. Thus, if the average latency is 100 ms and packets are arriving between 95 ms and 105 ms, the peak-to-peak jitter is defined as 10 ms. Measurements within the Cisco TelePresence codecs use peak-to-peak jitter.

Similar to the latency service level requirement, Cisco TelePresence codecs have built in thresholds for jitter to ensure a high quality user experience. Specifically, if peak-to-peak jitter exceeds 20 ms (which we call Jitter Threshold 1) for several seconds, then two things occur:

- A warning message appears at the bottom of the 65” plasma display indicating that the network is experiencing congestion and that call quality may be affected.

- The TelePresence codecs downgrade to a lower level of motion handing quality within the given resolution.

As previously mentioned, Cisco TelePresence codecs have three levels of motion handling quality within a given resolution, specifically 720p-Good, 720p-Better, and 720p-Best and 1080p-Good, 1080p-Better, and 1080p-Best. Therefore, for example, if a call at 1080p-Best would exceed Jitter Threshold 1 (20 ms) for several seconds, the codec would display the warning message in and would downgrade the motion handling quality to 1080p-Good. Similarly a call at 720p-Best would downgrade to 720-Good. Incidentally, downgraded calls do not automatically upgrade should network conditions improve, because this could cause a "flapping" effect where the call upgrades and then downgrades again, over and over.

A second jitter threshold (Jitter Threshold 2) is also programmed into the TelePresence codecs, such that if peak-to-peak jitter exceeds 40 ms for several seconds, then two things occur. The TelePresence codecs:

- Self-terminate the call.
- Display an error message on the 7970G IP Phone indicating that the call was terminated due to excessive network congestion.

Finally, as with latency, the jitter budget is proportioned between the service provider and enterprise networks. Unfortunately, unlike latency or packet loss, peak-to-peak jitter is not necessarily cumulative. Nonetheless, simply for the sake of setting a jitter target for each party, the recommended peak-to-peak jitter split is 50/50 between the service provider and enterprise, such that each group of network administrators can design their networks to a clear set of jitter targets and thresholds. Also like latency, this split may be negotiated differently between the service provider and enterprise to meet certain unique scenarios, such as satellite connections. Again, the main point is that a fixed jitter budget needs to be clearly apportioned to both the service provider and to the enterprise, such that the end-to-end target and thresholds are not exceeded.

It is recommended that SPs engineer their network to meet the target, but base their SLA on threshold1. Threshold1 provides global coverage between any two sites on the planet and allows the SP to offer a 100% guarantee that their network (demarc-to-demarc) will never exceed 10ms of jitter (50% of threshold1).

The TelePresence Jitter targets and thresholds are summarized in Table 4-2.

Table 4-2 TelePresence Jitter Targets, Thresholds, and Service Provide/Enterpriser Splits

Metric	Target	Threshold 1 (Warning and Downgrade)	Threshold 2 (Call Drop)
End-to-end	10 ms	20 ms	40 ms
Service Provider	5 ms	10 ms[1]	20 ms

[1] SP SLA should be based on Threshold 1.

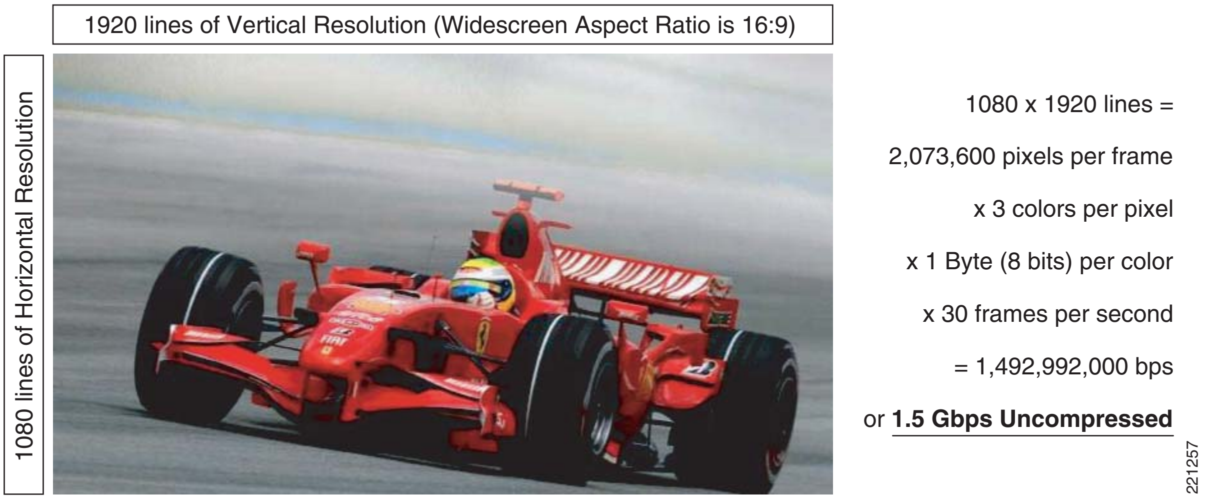
TelePresence Loss Requirements

Cisco TelePresence is highly sensitive to packet loss, and as such has an end-to-end packet loss target of 0.05%.

It may be helpful to review a bit of background information to better understand why TelePresence is so extremely sensitive to packet loss. Specifically, let's review how much information is actually needed to transmit a 1080p30 HD video image, which is the highest video transmission format used by Cisco TelePresence codecs. The first parameter (1080) refers to 1080 lines of horizontal resolution, which are matrixed with 1920 lines of vertical resolution (as per the 16:9 Widescreen Aspect Ratio used in High

Definition video formatting), resulting in 2,073,600 pixels per screen. The second parameter, p, indicates a progressive scan, which means that every line of resolution is refreshed with each frame (as opposed to an interlaced scan, which would be indicated with an i and would mean that every other line is refreshed with each frame). The third parameter 30 refers to the transmission rate of 30 frames per second. While video sampling techniques may vary, each pixel has approximately 3 Bytes of color and/or luminance information. When all of this information is factored together (2,073,600 pixels x 3 Bytes x 8 bits per Byte x 30 frames per second), it results in approximately 1.5 Gbps of information. This is illustrated in Figure 4-3.

Figure 4-3 1080p30 Information Breakdown


1920 lines of Vertical Resolution (Widescreen Aspect Ratio is 16:9)
1080 lines of Horizontal Resolution
1080 x 1920 lines =
2,073,600 pixels per frame
x 3 colors per pixel
x 1 Byte (8 bits) per color
x 30 frames per second
= 1,492,992,000 bps
or **1.5 Gbps Uncompressed**
221257

As shown earlier in this chapter, Cisco TelePresence codecs transmit at approximately 5 Mbps (max) per 1080p display, which translates to over 99% compression. Therefore, the overall effect of packet loss is proportionally magnified and dropping even one packet in 2000 (0.05% packet loss) becomes readily noticeable to end users.

Similar to the latency and jitter service level requirement, Cisco TelePresence codecs have built in thresholds for packet loss to ensure a high-quality user experience. Specifically, if packet loss exceeds 0.10% (or 1 in 1000 packets, which we call Loss Threshold 1) for several seconds, then two things occur:

- A warning message appears at the bottom of the on the 65” plasma display indicating that the network is experiencing congestion and that call quality may be affected.
- The TelePresence codecs downgrade to a lower level of motion handing quality within the given resolution.

As previously mentioned, Cisco TelePresence codecs have three levels of motion handling quality within a given resolution, specifically 720p-Good, 720p-Better, and 720p-Best and 1080p-Good, 1080p-Better, and 1080p-Best. Therefore, for example, if a call at 1080p-Best would exceed Loss Threshold 1 (0.10%) for several seconds, the codec would display the warning message and would downgrade the motion handling quality to 1080p-Good. Similarly a call at 720p-Best would downgrade to 720-Good in the same scenario. Incidentally, downgraded calls do not automatically upgrade should network conditions improve, because this could cause a “flapping” effect where the call upgrades and then downgrades again, over and over.

A second packet loss threshold (Loss Threshold 2) is also programmed into the TelePresence codecs, such that if packet loss exceeds 0.20% (or 1 in 500 packets) for several seconds, then two things occur. The TelePresence codecs:

- Self-terminate the call.

- Display an error message on the 7970G IP Phone indicating that the call was terminated due to excessive network congestion.

Finally, as with previously defined service level requirements, the loss budget is proportioned between the service provider and enterprise networks. The recommend split is 50/50 between the service provider and enterprise, such that each group of network administrators can design their networks to a clear set of packet loss targets and thresholds. Of course, This split may be negotiated differently between the service provider and enterprise to meet certain unique scenarios, such as satellite connections. Again, the main point is that a fixed packet loss budget needs to be clearly apportioned to both the service provider and to the enterprise, such that the end-to-end target and thresholds are not exceeded.

It is recommended that SPs engineer their network to meet the target, but base their SLA on threshold1. Threshold1 provides global coverage between any two sites on the planet and allows the SP to offer a 100% guarantee that their network (demarc-to-demarc) will never exceed .05% loss (50% of threshold1).

The TelePresence packet loss targets and thresholds are summarized in Table 4-3.

Table 4-3 TelePresence Jitter Targets, Thresholds, and Service Provider/Enterprise Splits

Metric	Target	Threshold 1 Warning and Downgrade)	Threshold 2 (Call Drop)
End-to-end	0.05% (1 in 2000)	0.10% (1 in 1000)	0.20 (1 in 500)
Service Provider	.025%	.05%[1]	.10%

[1] SP SLA should be based on Threshold 1.

Tactical QoS Design Best Practices for TelePresence

Once the service level requirements of TelePresence are defined, then the network administrator can proceed to the next step of the QoS deployment cycle (illustrated in Figure 4-1) of designing the actual policies.

A couple of tactical QoS best practices design principles bear mentioning at this point, as these serve to improve the efficiency and scope of your QoS designs. The first principle is to always deploy QoS in hardware, rather than software, whenever a choice exists. Cisco Catalyst switches perform QoS operations in hardware Application Specific Integrated Circuits (ASICS) and as such have zero CPU impact; Cisco IOS routers, on the other hand, perform QoS operations in software, resulting in a marginal CPU impact, the degree of which depends on the platform, the policies, the link speeds, and the traffic flows involved. So, whenever supported, QoS policies like classification, marking/remarking, and/or policing can all be performed at line rates with zero CPU impact in Catalyst switches (as opposed to IOS routers), which makes the overall QoS design more efficient. A practical example of how this principle is applied is as follows: while all nodes in the network path must implement queuing policies, classification policies should be implemented in Cisco Catalyst hardware as close to the source of the traffic as possible (e.g., on the access edge switch to which the TelePresence System is attached), rather than waiting until the traffic hits the WAN router to be classified.

Another best practice principle to keep in mind is to follow industry standards whenever possible, as this extends the effectiveness of your QoS policies beyond your direct administrative control. For example, if you mark a realtime application, such as VoIP, to the industry standard recommendation as defined in RFC 3246 (An Expedited Forwarding Per-Hop Behavior), then you will no doubt provision it with strict priority servicing at every node within your enterprise network. Additionally, if you handoff to a service provider following this same industry standard, they will similarly provision traffic marked Expedited Forwarding (EF - or DSCP 46) in a strict priority manner. Therefore, even though you do not have direct administrative control of the QoS policies within the service provider's cloud, you have extended the influence of your QoS design to include your service provider's cloud, simply by following the industry standard recommendations. Therefore, in line with this principle, it would be beneficial to briefly consider some of the relevant industry standards to QoS design, particularly as these relate to TelePresence.

Relevant Industry Standards and Recommendations

Let's briefly review some of the relevant DiffServ standards and recommendations and see how these relate to TelePresence QoS design.

Note Although Cisco TelePresence requires Cisco CallManager (CCM) 5.1 (or higher) for call processing, and CCM 5.x supports Resource Reservation Protocol (RSVP) for Call Admission Control, the initial phase of the TelePresence solution does not require leveraging RSVP functionality (RSVP remains optional during this phase); therefore, the discussion in this paper focuses on DiffServ QoS designs and standards for Cisco TelePresence (not IntServ/RSVP).

RFC 2474 Class Selector Code Points

This standard defines the use of 6 bits in the IPv4 and IPv4 Type of Service (ToS) byte, termed Differentiated Services Code Points (DSCP). Additionally, this standard introduces Class Selector codepoints to provide backwards compatibility for legacy (RFC 791) IP Precedence bits.

RFC 2597 Assured Forwarding Per-Hop Behavior Group

This standard defines the Per-Hop Behavior of the Assured Forwarding (AF) classes. Four AF classes are defined: AF1, AF2, AF3, and AF4. Additionally, each class has three states of increasing Drop Preference assigned within it, corresponding to three traffic states: conforming (analogous to a green traffic light signal), exceeding (analogous to a yellow traffic light signal), and violating (analogous to a red traffic light signal). For example, conforming AF1 traffic would be marked to AF11 (the second 1 representing the lowest Drop Preference setting), exceeding traffic would have its Drop Preference increased to AF12, and violating traffic would have its Drop Preference increased further to AF13. When such traffic enters a node experiencing congestion, AF13 traffic is more aggressively dropped than AF12 traffic, which in turn is more aggressively dropped than AF11 traffic.

RFC 3246 An Expedited Forwarding Per-Hop Behavior

This standard defines an Expedited Forwarding (EF) Per-Hop Behavior for realtime applications. When traffic marked EF enters a node experiencing congestion, it receives strict priority behavior.

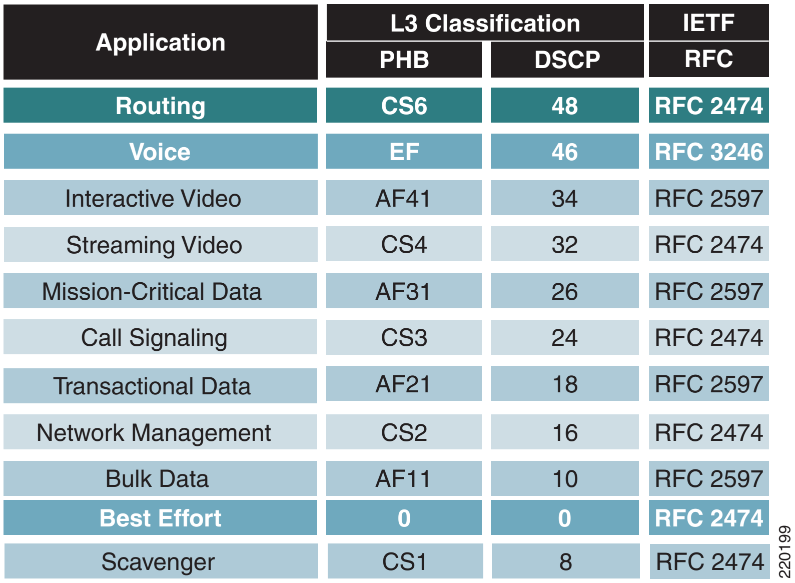
RFC 3662 A Lower Effort Per-Domain Behavior for Differentiated Services

This informational RFC defines a less than Best Effort service for undesired applications and specifies that such applications should be marked to Class Selector 1 (CS1).

Cisco's QoS Baseline

While the IETF RFC standards provided a consistent set of per-hop behaviors for applications marked to specific DSCP values, they never specified which application should be marked to which DiffServ Codepoint value. Much confusion and disagreements over matching applications with standards-defined codepoints led Cisco in 2002 to put forward a standards-based marking recommendation in their strategic architectural QoS Baseline document. Eleven different application classes that could exist within the enterprise were examined and extensively profiled, and then matched to their optimal RFC-defined Per-Hop Behaviors (PHBs). The application-specific marking recommendations from Cisco's QoS Baseline of 2002 are summarized in Figure 4-4.

Figure 4-4 Cisco's QoS Baseline Marking Recommendations



Application	L3 Classification		IETF
	PHB	DSCP	RFC
Routing	CS6	48	RFC 2474
Voice	EF	46	RFC 3246
Interactive Video	AF41	34	RFC 2597
Streaming Video	CS4	32	RFC 2474
Mission-Critical Data	AF31	26	RFC 2597
Call Signaling	CS3	24	RFC 2474
Transactional Data	AF21	18	RFC 2597
Network Management	CS2	16	RFC 2474
Bulk Data	AF11	10	RFC 2597
Best Effort	0	0	RFC 2474
Scavenger	CS1	8	RFC 2474

The adoption of Cisco's QoS Baseline was a great step forward in QoS consistency, not only within Cisco, but also within the industry in general.

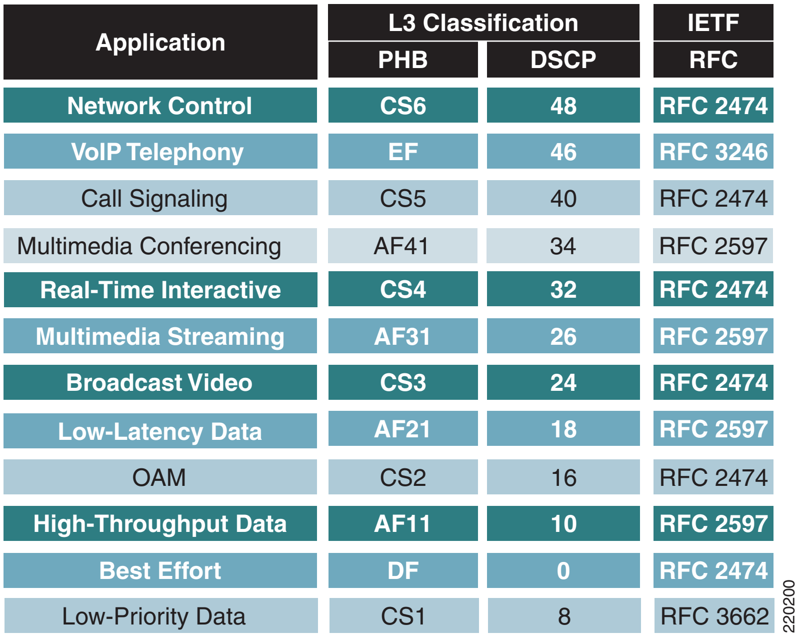
RFC 4594 Configuration Guidelines for DiffServ Classes

More than four years after Cisco put forward its QoS Baseline document, RFC 4594 was formally accepted as an informational RFC (in August 2006).

Before getting into the specifics of RFC 4594, it is important to comment on the difference between the IETF RFC categories of informational and standard. An informational RFC is an industry recommended best practice, while a standard RFC is an industry requirement. Therefore RFC 4594 is a set of formal DiffServ QoS configuration best practices, not a requisite standard.

RFC 4594 puts forward twelve application classes and matches these to RFC-defined Per-Hop Behaviors (PHBs). These application classes and recommended PHBs are summarized in Figure 4-5.

Figure 4-5 RFC 4594 Marking Recommendations



Application	L3 Classification		IETF
	PHB	DSCP	RFC
Network Control	CS6	48	RFC 2474
VoIP Telephony	EF	46	RFC 3246
Call Signaling	CS5	40	RFC 2474
Multimedia Conferencing	AF41	34	RFC 2597
Real-Time Interactive	CS4	32	RFC 2474
Multimedia Streaming	AF31	26	RFC 2597
Broadcast Video	CS3	24	RFC 2474
Low-Latency Data	AF21	18	RFC 2597
OAM	CS2	16	RFC 2474
High-Throughput Data	AF11	10	RFC 2597
Best Effort	DF	0	RFC 2474
Low-Priority Data	CS1	8	RFC 3662

It is fairly obvious that there are more than a few similarities between Cisco's QoS Baseline and RFC 4594, as there should be, since RFC 4594 is essentially an industry-accepted evolution of Cisco's QoS Baseline. However, there are some differences that merit attention.

The first set of differences are minor, as they involve mainly nomenclature. Some of the application classes from the QoS Baseline have had their names changed in RFC 4594. These changes in nomenclature are summarized in Table 4-4.

Table 4-4 Nomenclature Changes from Cisco QoS Baseline to RFC 4594

Cisco QoS Baseline Class Names	RFC 4594 Class Names
Routing	Network Control
Voice	VoIP Telephony
Interactive Video	Multimedia Conferencing
Streaming Video	Multimedia Streaming
Transactional Data	Low-Latency Data
Network Management	Operations/Administration/Management (OAM)
Bulk Data	High-Throughput Data
Scavenger	Low-Priority Data

The remaining changes are more significant. These include one application class deletion, two marking changes, and two new application class additions. Specifically:

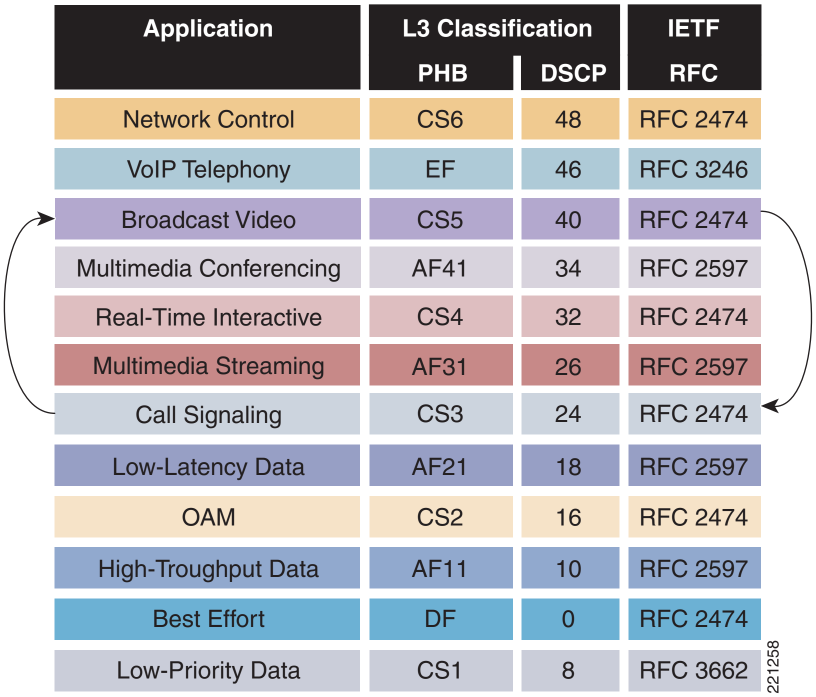
- The QoS Baseline Locally-Defined Mission-Critical Data class has been deleted from RFC 4594.
- The QoS Baseline marking recommendation of CS4 for Streaming Video has been changed in RFC 4594 to mark Multimedia Streaming to AF31.

- The QoS Baseline marking recommendation of CS3 for Call Signaling has been changed in RFC 4594 to mark Call Signaling to CS5.
- A new video class has been added to RFC 4594: Real-Time Interactive, which is to be marked CS4. This was done to differentiate between lower-grade desktop video telephony (referred to as Multimedia Conferencing) and higher-grade videoconferencing and TelePresence. Multimedia Conferencing uses the AF4 class and is subject to markdown policies, while TelePresence uses the CS4 class and is not subject to markdown.
- A second new video class has been added to RFC 4594: Broadcast video, which is to be marked CS3. This was done to differentiate between lower-grade desktop video streaming (referred to as Multimedia Streaming) and higher-grade Broadcast Video applications. Multimedia Streaming uses the AF3 class and is subject to markdown policies, while Broadcast Video uses the CS3 class and is not subject to markdown.

The most significant of the differences between Cisco's QoS Baseline and RFC 4594 is the RFC 4594 recommendation to mark Call Signaling to CS5. Cisco has just completed a lengthy and expensive marking migration for Call Signaling from AF31 to CS3 (as per the original QoS Baseline of 2002), and as such, there are no plans to embark on another marking migration in the near future. It is important to remember that RFC 4594 is an informational RFC (i.e., an industry best-practice) and not a standard. Therefore, lacking a compelling business case at the time of writing, Cisco plans to continue marking Call Signaling as CS3 until future business requirements arise that necessitate another marking migration.

Therefore, for the remainder of this document, RFC 4594 marking values are used throughout, with the one exception of swapping Call-Signaling marking (to CS3) and Broadcast Video (to CS5). These marking values are summarized in Figure 4-6.

Figure 4-6 Cisco-Modified RFC4594 Marking Values (Call-Signaling is Swapped with Broadcast Video)



Application	L3 Classification		IETF
	PHB	DSCP	RFC
Network Control	CS6	48	RFC 2474
VoIP Telephony	EF	46	RFC 3246
Broadcast Video	CS5	40	RFC 2474
Multimedia Conferencing	AF41	34	RFC 2597
Real-Time Interactive	CS4	32	RFC 2474
Multimedia Streaming	AF31	26	RFC 2597
Call Signaling	CS3	24	RFC 2474
Low-Latency Data	AF21	18	RFC 2597
OAM	CS2	16	RFC 2474
High-Troughput Data	AF11	10	RFC 2597
Best Effort	DF	0	RFC 2474
Low-Priority Data	CS1	8	RFC 3662

Classifying TelePresence

One of the first questions to be answered relating to TelePresence QoS design is: should TelePresence be assigned to a dedicated class or should it be assigned to the same class as existing Videoconferencing/Video Telephony? The answer to this question directly relates to whether TelePresence has the same service-level requirements as these other two interactive video applications or whether it has unique service level requirements. Table 4-5 summarizes the service level requirements of both generic Videoconferencing applications and TelePresence.

Table 4-5 Service Level Requirements of Generic Video-Conferencing and TelePresence

Service Level Parameter (Target Values)	(Generic) Videoconferencing/Video Telephony	Cisco TelePresence
Bandwidth	384 kbps or 768 kbps + network overhead	1.5 Mbps to 12.6 Mbps + network overhead
Latency	400-450 ms latency	150 ms latency
Jitter	30-50 ms peak-to-peak jitter	10 ms peak-to-peak jitter
Loss	1% random packet loss	0.05% random packet loss

From Table 4-5 it becomes apparent that TelePresence has unique (and higher/tighter) service level requirements than do generic Videoconferencing/Video Telephony applications; therefore, TelePresence requires a dedicated class along with a dedicated classification marking value.

Videoconferencing/Video Telephony applications have traditionally been marked to (RFC 2597) Assured Forwarding Class 4, which is the recommendation from both the Cisco QoS Baseline as well as RFC 4594. However, the Assured Forwarding (AF) Per-Hop Behavior (PHB) includes policing (to conforming, exceeding, and violating traffic rates), as well as correspondingly increasing the Drop Preferences (to Drop Preference 1, 2, and 3 respectively), and ultimately dropping traffic according to the Drop Preference markings. TelePresence traffic has a very low tolerance to drops (0.05%) and therefore would not be appropriately serviced by an AF PHB.

Because of the low-latency and jitter service-level requirements of TelePresence, it may seem attractive to assign it an (RFC 3246) Expedite Forwarding (EF) Per-Hop Behavior; after all, there is nothing in RFC 3246 that dictates that only VoIP can be assigned to this PHB. However, it is important to recognize that VoIP behaves considerably differently than video. As previously mentioned, VoIP has constant packet sizes and packet rates, whereas video packet sizes vary and video packet rates also vary in a random and bursty manner. Thus, if both video and voice were assigned to the same marking value and class, (bursty) video could easily interfere with (well-behaved) voice. Therefore, for both operational and capacity planning purposes, it is recommended not to mark both voice and video to EF. This recommendation is reflected in both the Cisco QoS Baseline as well as RFC 4594.

What then should TelePresence be marked to? The best formal guidance is provided in RFC 4594, where a distinction is made between a Multimedia Conferencing (i.e., generic Videoconferencing/Video Telephony) service class and a Real-Time Interactive service class. The Real-Time Interactive service class is intended for inelastic video flows, such as TelePresence. The recommended marking for this Real-Time Interactive service class, and thus **the recommended marking for TelePresence is Class Selector 4 (CS4)**.

Policing TelePresence

In general, policing TelePresence traffic should be avoided whenever possible, although some exceptions exist.

As previously mentioned, TelePresence is highly sensitive to drops (with a 0.05% packet loss target); therefore policing TelePresence traffic rates with either a Single Rate Three Color Marker (as defined in RFC 2697) or a Two Rate Three Color Marker (as defined in RFC 2698) could be extremely detrimental to TelePresence flows and ultimately ruin the high-level of user experience that this application is intended to deliver.

However, there are three places where TelePresence traffic may be legitimately policed over the network.

The first automatically occurs if TelePresence is assigned to a Low-Latency Queue (LLQ) within Cisco IOS routers at the WAN or VPN edge. This is because any traffic assigned to a LLQ is automatically policed by an implicit policer set to the exact value as the LLQ rate. For example, if TelePresence is assigned a LLQ of 15 Mbps, it is also implicitly policed by the LLQ algorithm to exactly 15 Mbps; any excess TelePresence traffic is dropped.

Note The implicit policer within the LLQ feature is only active when LLQ is active. In other words, since queuing only engages when there is congestion, LLQ never engages unless the link is physically congested or a (hierarchical QoS) shaper forces LLQ to engage prior to physical link congestion. Similarly, the implicit policer of LLQ never engages unless there is physical congestion on the link or a (hierarchical QoS) shaper forces it to engage prior to physical link congestion. Put another way, when the physical link is un-congested and/or a hierarchical QoS shaper is inactive, neither LLQ nor the implicit policer of LLQ is active.

The second most common place that TelePresence is likely to be policed in the network is at the service provider's provider edge (PE) routers, in the ingress direction. Service providers need to police traffic classes, especially realtime traffic classes, to enforce service contracts and prevent possible oversubscription on their networks and thus ensure service level agreements.

The third place (and optional) place, where policing TelePresence may prove beneficial in the network is at the campus access edge. Administrators can deploy access-edge policers for security purposes to mitigate the damage caused by the potential abuse of trusted switch ports. Since TelePresence endpoints can mark TelePresence flows to the recommended 802.1Q/p CoS value (CoS 4) and DSCP codepoint value (CS4), the network administrator may choose to trust the CoS or DSCP values received from these ports. However, if a disgruntled employee gains physical access to the TelePresence switch ports, they may send whatever traffic they choose to over these ports and their flows are trusted over the network. Such rogue traffic flows may hijack voice or video queues and easily ruin call or video quality over the QoS-provisioned network infrastructure. Therefore, the administrator may choose to limit the scope of damage that such network abuse may present by configuring access-edge policers on TelePresence switch ports to remark (to Scavenger: DSCP CS1) or drop out-of-profile traffic originating on these ports (e.g., CS4 traffic exceeding 15 Mbps). Supporting this approach, RFC 4594 recommends edge policing the Real-Time Interactive service class via a single-rate policer.

Queuing TelePresence

To achieve the high-levels of service required by the Cisco TelePresence Experience, queuing must be enabled on every node along the path to provide service guarantees, regardless of how infrequently congestion may occur on certain nodes (i.e., congestion can and does occur even on very high-bandwidth mediums). If queuing is not properly configured on every node, the Cisco TelePresence eXperience (CTX) cannot be guaranteed.

RFC 4594 specifies the minimum queuing requirement of the Real-Time Interactive service class to be a rate-based queue (i.e., a queue that has a guaranteed minimum bandwidth rate). However, RFC 4594 makes an allowance that while **the PHB for Real-Time Interactive service class** should be configured to provide high bandwidth assurance, it **may be configured as a second EF PHB** that uses relaxed performance parameters, a rate scheduler, and a CS4 DSCP value.

This means that, for example, TelePresence, which has been assigned to this Real-Time Interactive service class, can be queued with either a guaranteed rate non-priority queue (such as a Cisco IOS Class-Based Weighted Fair Queue-CBWFQ) or a guaranteed-rate strict priority queue (such as a Cisco IOS Low-Latency Queue-LLQ); in either case, TelePresence is to be marked as Class Selector 4 (and not EF).

Therefore, since RFC 4594 allows for the Real-Time Interactive service-class to be given a second EF PHB and because of the low latency, low jitter, and low loss requirements of TelePresence, **it is recommended to place TelePresence in a strict-priority queue**, such as a Cisco IOS LLQ or a Cisco Catalyst hardware priority queue whenever possible.

However, an additional provisioning consideration must taken into account when provisioning TelePresence with a second EF PHB, which relates to the amount of bandwidth of a given link that should be assigned for strict priority queuing. The well-established and widely-deployed Cisco best-practice recommendation is to limit the amount of strict priority queuing configured on an interface to no more than one-third of the link's capacity. This has commonly been referred to as the 33% LLQ Rule.

The rationale behind this rule is that if you assign too much traffic for strict priority queuing, then the overall effect is a dampening of QoS functionality for non-realtime applications. Remember, the goal of convergence is to enable voice, video, and data to transparently co-exist on a single network. When realtime applications such as voice and/or TelePresence dominate a link (especially a WAN/VPN link), then data applications fluctuate significantly in their response times when TelePresence calls are present versus when they are absent, thus destroying the transparency of the converged network.

For example, consider a (45 Mbps) DS3 link configured to support 2 separate CTS-3000 calls, both configured to transmit at full 1080p-Best resolution. Each such call requires 15 Mbps of realtime traffic. Prior to TelePresence calls being placed, data applications have access to 100% of the bandwidth (to simplify the example, we are assuming there are no other realtime applications, such as VoIP, on this link). However, once these TelePresence calls are established, all data applications would suddenly be contending for less than 33% of the link. TCP windowing would take effect and many data applications will hang, time-out, or become stuck in a non-responsive state, which usually translates into users calling the IT help desk complaining about the network (which happens to be functioning properly, albeit in a poorly-configured manner).

To obviate such scenarios, Cisco Technical Marketing has done extensive testing and has found that a significant decrease in data application response times occurs when realtime traffic exceeds one-third of link bandwidth capacity. Extensive testing and customer deployments have shown that a general best queuing practice is to limit the amount of strict priority queuing to 33% of link bandwidth capacity. This strict priority queuing rule is a conservative and safe design ratio for merging realtime applications with data applications.

Note As Cisco IOS software allows the abstraction (and thus configuration) of multiple strict priority LLQs, in such a multiple LLQ context, this design principle would apply to the sum of all LLQs to be within one-third of link capacity.

It is vitally important, however, to understand that this strict priority queuing rule is simply a best practice design recommendation and is not a mandate. There may be cases where specific business objectives cannot be met while holding to this recommendation. In such cases, enterprises must provision according to their detailed requirements and constraints. However, it is important to recognize the tradeoffs involved with over-provisioning strict priority traffic and its negative performance impact on non-realtime-application response times. It is also worth noting that the 33% rule only applies for converged networks. In cases where customers choose to deploy dedicated WAN circuits for their TelePresence traffic, the 33% rule does not apply since TelePresence (and perhaps some nominal amount of management and signaling traffic) is the only traffic on the circuit. In these cases, customers are free to use up to 98% of the link capacity for TelePresence (reserving 2% for routing protocols, network management traffic such as SSH and SNMP, and signaling).

Shaping TelePresence?

It is recommended to avoid shaping TelePresence flows unless absolutely necessary. This is because of the QoS objective of shapers themselves. Specifically, the role of shapers is to delay traffic bursts above a certain rate and to smooth out flows to fall within contracted rates. Sometimes this is done to ensure traffic rates are within a carriers Committed Information Rate (CIR); other times shaping is performed to protect other data classes from a bursty class.

Shapers temporarily buffer traffic bursts above a given rate and as such introduce variable delay (jitter) as well as absolute delay. Since TelePresence is so sensitive to delay (150 ms) and especially jitter (10 ms), it is recommended not to shape TelePresence flows.

If the objective of the shaper was to meet a carrier’s CIRs, this can be achieved by properly provisioning the adequate bandwidth and burst allowances on the circuit.

If the objective of the shaper was to protect other traffic classes from TelePresence bursts, then a better approach would be to explicitly protect each class with a guaranteed minimum bandwidth rate (such as a Cisco IOS CBWFQ).

In either case, a shaper would be a sub-optimal tool to meet the desired objective and would cause quality issues on the TelePresence flows and therefore would not be recommended.

The TelePresence traffic queue (whether you choose to place it in a CBWFQ or a second strict priority LLQ) must be provisioned with the proper mean rate (bits per second) and burst allowance (burst bytes exceeding the mean).

Compressed RTP (cRTP) with TelePresence

It is recommended to not enable cRTP for TelePresence. This is because of the large CPU impact of IP RTP Header Compression and the negligible returns in bandwidth savings it entails at TelePresence circuit speeds.

TelePresence, like VoIP, is encapsulated by IP, UDP, and RTP headers and these headers, when combined, account for 40 bytes per packet (at Layer 3). To enhance bandwidth efficiency, compression tools, like IP RTP Header Compression (cRTP) can reduce this overhead from 40 bytes to 2-5 bytes per packet.

However, it is important to recognize that cRTP is the most computationally-intensive QoS operation in the Cisco IOS toolset. Furthermore, it is only recommended on slow-speed links, usually 768 kbps or less, as it is at these speeds that the bandwidth gain offsets the increased CPU cost of the operation and is only useful for RTP-based applications that have a small amount of payload per packet. On high-speeds links and applications like TelePresence in which the payload of each packet averages 1100 bytes, cRTP offers no benefit and only results in sending the routers CPU through the ceiling. **Therefore, it is recommended to not enable cRTP on links carrying TelePresence.**

Link Fragmentation and Interleaving (LFI) with TelePresence

Like cRTP, LFI is only useful on slow-speed links (usually 768 kbps or less) and is used to fragment larger data packets into smaller chunks and interleave voice in between them to reduce the serialization and queuing delays for VoIP applications. Since TelePresence packets average 1100 bytes payload per packet, LFI would want to fragment them. This introduces unwanted jitter and out-of-order and late packets into the TelePresence stream. On high-speed links the serialization delay for large packets is inconsequential to VoIP and thus LFI offers no benefit and only results in sending the routers CPU through the ceiling. **Therefore, it is recommended to not implement LFI on links carrying TelePresence**.

GRE/IPSec Tunnels with TelePresence

Tunneling TelePresence traffic over GRE/IPSec tunnels is supported. The Cisco TelePresence codecs are designed to limit their packets to a maximum of 1200 bytes to leave enough room for GRE/IPSec encapsulation overhead to avoid having the TelePresence traffic fragmented for exceeding the Maximum Transmission Unit (MTU) of any link in the path.

Place in the Network TelePresence QoS Design

At this point, the strategic QoS business objectives for TelePresence have been defined, the service level-requirements of TelePresence have been specified, and the tactical QoS design approach has been sketched via the best practice principles and recommendations reviewed in the previous section. What remains is to flesh out these sketches into detailed Place-in-the-Network (PIN) platform-specific designs.

As the Cisco TelePresence solution evolves, it will become more complex and touch more Places-in-the-Network. The first deployment model to receive Cisco Verified Design (CVD) certification is the Intra-Enterprise, Point-to-Point Deployment Model (as described in Chapter 3, "TelePresence Network Deployment Models"). Such deployments will directly impact enterprise campus, branch, and WAN/MAN PINs, as well as service provider edge and core networks.

An addition to the Intra-Enterprise Deployment Model came with the release of the Cisco TelePresence Multipoint Solution, based on the Cisco TelePresence Multipoint Switch (CTMS) product offering. This addition may require an additional PIN, namely the enterprise and/or service provider data center, as these are often the locations where multipoint resources are hosted. However, note that while many customers are beginning to deploy multipoint resources, the addition of multipoint resources within the Intra-Enterprise Deployment Model has not yet received CVD certification.

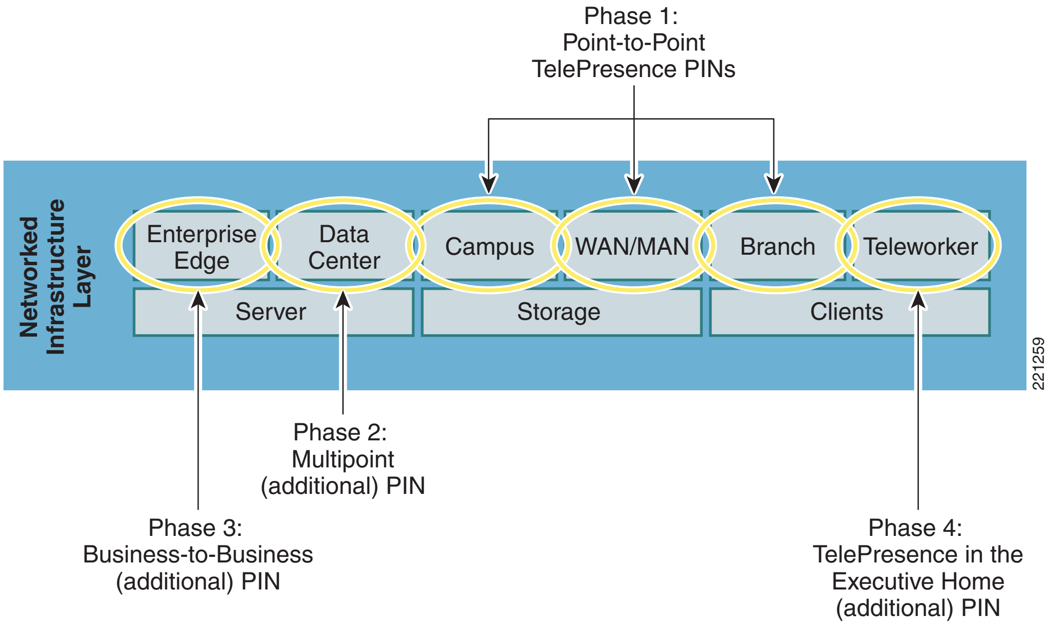
The next phase of TelePresence deployments will begin with the release of the Business-to-Business TelePresence solution, enabling enterprises to move to a Inter-Enterprise Deployment Model (as described in Chapter 3, "TelePresence Network Deployment Models"). These Inter-Enterprise deployments may be Point-to-Point or Multipoint. With this additional functionality, a new enterprise

PIN, the enterprise edge, will require design modifications. Additionally, service providers will need to develop shared services domains to provide the necessary connectivity, security, and QoS services required to enable this solution. Early Field Trials (EFT) of B2B services have begun. However, the Inter-Enterprise Deployment Model has not yet received CVD certification.

Finally, TelePresence systems are already emanating considerable executive-perk appeal, especially CTS-1000 systems that are designed for an executive's office. Already some executives are deploying TelePresence systems within their homes, taking advantage of very high-speed residential internet access options, like fiber optics to the home. Therefore, an inevitable fourth phase of TelePresence deployments will undoubtedly include the executive teleworker PIN. Early Field Trials (EFT) of TelePresence systems deployed in executive homes has begun. However, the Executive-Class Teleworker Deployment Model has not yet received CVD certification.

The relevant enterprise PINs for the above deployment models, based on the Service Oriented Network Architecture (SONA), specifically the Networked Infrastructure Layer, are illustrated in Figure 4-7.

Figure 4-7 SONA Networked Infrastructure Layer—Places in the Network (PINs) for Phases 1-4 TelePresence Deployments



The following chapters discuss and detail QoS designs for deploying TelePresence in each of these enterprise PINs. Information is provided on components pending CVD certification to allow customers to plan their network designs and deployment strategies accordingly. However, where detailed CVD design guidance is not yet available, note that the information provided is subject to change pending CVD certification.

CHAPTER 5

Campus QoS Design for TelePresence

Overview

The campus is the primary Place-in-the-Network (PIN) where TelePresence endpoints connect to the network infrastructure. Specifically, the 10/100/1000 NIC on the TelePresence primary codec connects —typically via an Intermediate Distribution Frame (IDF)—to the campus access-layer edge switch port. It is at this switch port that the initial QoS polices required to support TelePresence are enabled. Additional QoS policies are also required on all campus inter-switch links. Let's consider each of these port-specific QoS requirements.

Access Edge Switch Port QoS Considerations

The first QoS operation that needs to be performed is to define the trust boundary. The trust boundary is the point in the network at which 802.1Q/p CoS markings and/or IP DSCP markings are accepted or overridden by the network.

At the access-layer, the network administrator can enable the infrastructure to:

- Trust the endpoints (CoS and/or DSCP)
- Not trust the endpoints and manually re-mark TelePresence traffic using administratively-defined policies within the access-edge switch
- Conditionally trust the endpoints (trust is extended only after a successful CDP negotiation)

In Phase 1 deployments of Cisco TelePresence (Intra-Enterprise Point-to-Point Deployment Models, as discussed in Chapter 3, "TelePresence Network Deployment Models") it is recommended to have a dedicated Communications Manager (CUCM) to support TelePresence. By default, CUCM marks any and all video traffic (including TelePresence) to AF41. It is recommended that this parameter be modified to mark video (i.e., TelePresence only, in this dedicated CUCM context) to CS4.

Note The reason behind this recommendation is that CUCM does not (yet) have the ability to distinguish between different types of video. Therefore CUCM by default marks both generic Videoconferencing/Video Telephony (from applications like Cisco Unified Video Advantage, for example) as well as TelePresence to AF41.

If a dedicated CUCM is being used for managing TelePresence endpoints, and it has been configured to mark video (i.e., TelePresence) traffic to DSCP CS4, then the TelePresence primary codec marks all TelePresence call traffic (both video and audio) to CS4, but Call-Signaling traffic to CS3. The Cisco

7970G IP Phone similarly marks DSCP values correctly, marking VoIP traffic to EF and Call-Signaling to CS3. Therefore, the switch port connecting to the TelePresence primary codec can be configured to trust DSCP.

Alternatively, the access switch ports can be set to trust CoS, as both the Cisco 7970G IP Phone and the TelePresence primary codec are assigned to the Voice VLAN (VVLAN) and tag their traffic with 802.1Q/p CoS values. The 7970G IP Phone marks VoIP traffic to CoS 5 and Call-Signaling traffic to CoS 3. The Cisco TelePresence codec marks TelePresence traffic (both video and audio) to CoS 4 and Call-Signaling traffic to CoS 3.

However, if the switch port is configured to trust CoS, then it generates an internal DSCP value for all traffic flows via the CoS-to-DSCP map. Only one change is recommended to be made to the default CoS-to-DSCP map, which is to map CoS 5 to EF (46) instead of leaving the default mapping of CoS 5 to CS5 (40). The recommended CoS-to-DSCP map for access-switches connecting to Cisco TelePresence primary codecs is illustrated in Table 5-1.

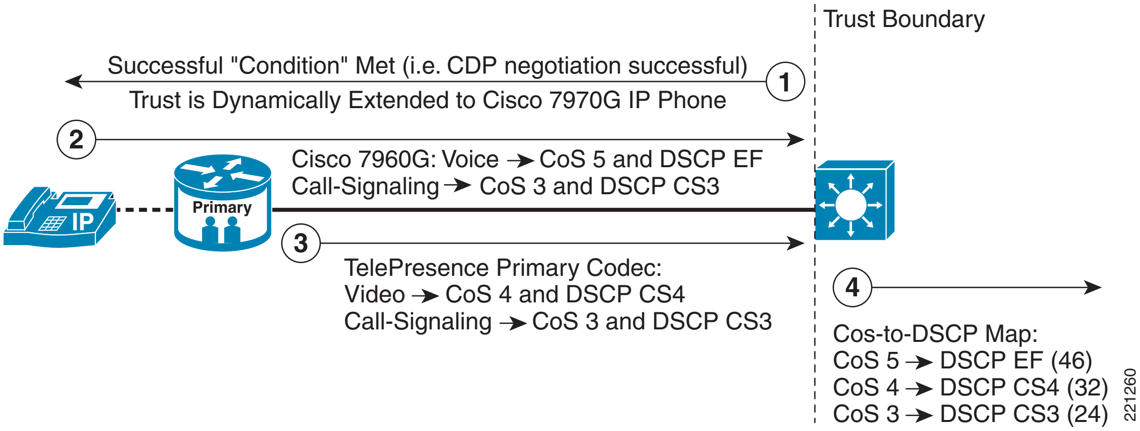
Table 5-1 Recommended Global CoS-to-DSCP Mapping for TelePresence Access-Edge Switches

CoS Value	DSCP Value	PHB	Application
7	56	-	Network Control
6	48	CS6	Internetwork Control
5	46	EF	Voice
4	32	CS4	TelePresence
3	24	CS3	Call-Signaling
2	16	CS2	Management
1	8	CS1	Scavenger
0	0	DF	Default Forwarding/Best Effort

Finally, the access switch may be set to conditionally trust the TelePresence endpoint. This is because Cisco IP Telephony devices, including the Cisco Unified 7979G IP phone that is an intrinsic part of the TelePresence endpoint system, have the ability to identify themselves, via Cisco Discovery Protocol (CDP) to the network infrastructure. Upon a successful CDP negotiation/identification, the network infrastructure dynamically extends trust to the endpoints, which include both the Cisco Unified 7970G IP phone and the TelePresence primary codec. The primary functionality that conditional trust brings is to allow for user-mobility within the IP Telephony-enabled enterprise (users can add/move/change where their IP Phones are connected and the network automatically adapts without requiring an administrator to manually change switch port trust policies). This user-mobility is not a crucial functionality to support TelePresence, since TelePresence units are rarely moved around (due to sheer size). Nonetheless, this conditional trust functionality is supported by TelePresence codecs and adds a minor element of security in the event that the TelePresence codec is physically disconnected from the wall network jack by an unknowing and/or disgruntled individual, who then connects some other device (such as their laptop) to this trusted switch port. In this case, by using a conditional trust policy, the abuser's traffic would no longer be trusted.

The operation of conditional trust policies, as well as endpoint CoS markings and the CoS-to-DSCP mappings of the access-edge switch for TelePresence scenarios, is illustrated in Figure 5-1.

Figure 5-1 Conditional Trust, CoS Markings, and Mappings for TelePresence


Trust Boundary
Successful "Condition" Met (i.e. CDP negotiation successful)
Trust is Dynamically Extended to Cisco 7970G IP Phone
1
2
Cisco 7960G: Voice → CoS 5 and DSCP EF
Call-Signaling → CoS 3 and DSCP CS3
IP
Primary
3
TelePresence Primary Codec:
Video → CoS 4 and DSCP CS4
Call-Signaling → CoS 3 and DSCP CS3
4
Cos-to-DSCP Map:
CoS 5 → DSCP EF (46)
CoS 4 → DSCP CS4 (32)
CoS 3 → DSCP CS3 (24)
221260

Note that if trust CoS is used (as opposed to conditional trust), steps 2, 3, and 4 still apply. The only difference is that the switch would skip step 1; the port would always be trusted regardless of CDP.

An optional recommendation for the access-edge switch port connecting to a TelePresence primary codec is to configure a policer to prevent network abuse in case of a compromise of this trusted port. Similar to the example previously given, this recommendation is to prevent an unknowing and/or disgruntled individual that gains physical access to the TelePresence switch port and decides to send rogue traffic over the network that can hijack voice or video queues and easily ruin call or video quality. Therefore, the administrator may choose to limit the scope of damage that such network abuse may present by configuring access-edge policers on TelePresence switch ports to drop (or remark to Scavenger - CS1) out-of-profile traffic originating on these ports. This is not only a Cisco recommended best practice, but is also reflected in RFC 4594 which recommends edge policing the Real-Time Interactive service class via a single-rate policer.

If such a policer is configured, it is recommended to use Per-Port/Per-VLAN policers, whenever supported. In this manner, a set of policers may be applied to the Voice VLAN to ensure that voice, video, and call signaling traffic are performing within normal levels and a separate, more stringent, policer can be applied to the data VLAN.

Note When configuring policers for TelePresence, make sure you allow for the appropriate burst intervals, as defined in Burst Requirements in Chapter 4, "Quality of Service Design for TelePresence."

Finally, to ensure guaranteed levels of service, queuing needs to be configured on all nodes where the potential for congestion exists, regardless of how infrequently it may occur.

In Catalyst switches, queuing (along with all other QoS operations) is performed in hardware. Therefore, there are a fixed number of hardware queues that vary by platform, as well as by linecards. The nomenclature for Catalyst queuing is 1P*x*Q*y*T, where:

- 1P represents a strict priority (Expedite Forwarding) queue
- *x*Q represents a number of non-priority queues
- *y*T represents a number of drop-thresholds per queue

Note As discussed, due to the strict service levels required by Cisco TelePresence, it is recommended to assign TelePresence flows to a strict priority queue, whether this is implemented in Cisco Catalyst hardware or in Cisco IOS software. However, some older Catalyst platforms and linecards do not support a strict priority queue. For example, some Catalyst 6500 linecards support only a 2Q2T egress queuing model and as such would not be recommended within a Cisco TelePresence campus network design.

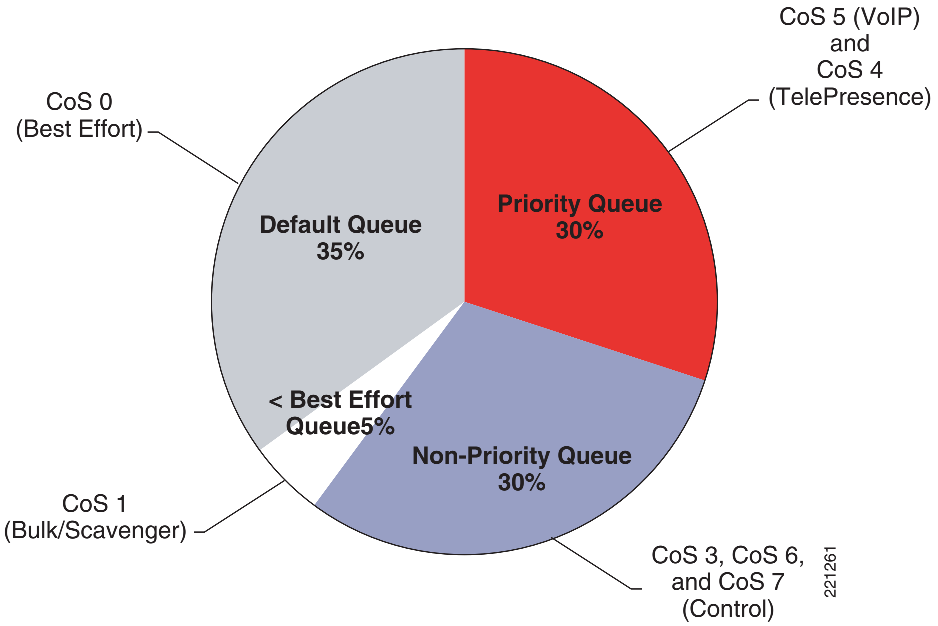
It is highly recommended that all Catalyst switches and linecards within a Cisco TelePresence campus design support a 1PxQyT queuing model.

For example, a Catalyst 6500 48-port 10/100/1000 RJ-45 Module (WS-X6748-GE-TX) has a 1P3Q8T, meaning 1 strict priority queue (which, incidentally, on this linecard is Queue 4) and 3 additional non-priority queues each with 8 configurable Weighted Random Early Detect (WRED) drop thresholds per queue.

Cisco Enterprise Systems Engineering (ESE) testing has shown that the optimal and most consistent service levels for TelePresence are achieved when TelePresence is provisioned with strict-priority hardware queuing (typically in conjunction with VoIP Telephony traffic), provided that the total bandwidth assigned to these realtime applications is less than 33% of the link—but this is virtually always the case on high-speed campus links in the range of 100 Mbps to 10 Gbps Ethernet. For example, consider a Catalyst 6513 provisioned with 11 x 48-port linecards, with each port configured to support G.711 VoIP (128 kbps max per port). Such a configuration would only require 67.584 Mbps or 6.8% of a GigE uplink. Even if a CTS-3000 system were connected to each of the 11 linecards, the total realtime bandwidth would be [(11 x 15 Mbps) + (11 x 48 x 128 kbps)] 232.584 Mbps or 23.3% of a GigE uplink (which is still within the 33% LLQ Rule allowance).

As a generic campus queuing guide, it would be recommended to assign CoS values 4 (TelePresence) and 5 (VoIP) to the strict priority queue, CoS 3 (Call-Signaling) to a (non-default) non-priority queue, and CoS 0 (Best Effort) to the default queue. Finally, CoS 1 (Bulk and/or Scavenger traffic) should be assigned to a (minimally provisioned) less than Best Effort non-priority queue. These guidelines are illustrated in Figure 5-2.

Figure 5-2 Generic Campus Queuing Provisioning and Mapping Guidelines



Campus Inter-Switch Link QoS Considerations

Once the trust boundary has been established and optimal access-edge policers have been enabled, then the DSCP values on all other inter-switch links and campus-to-WAN hand off links can be trusted. Therefore, it is recommended to trust DSCP (not CoS) on all inter-switch links, whether these are uplinks/downlinks to/from the distribution layer, uplinks/downlinks to/from the core layer, intra-core links, or links to WAN Aggregation routers.

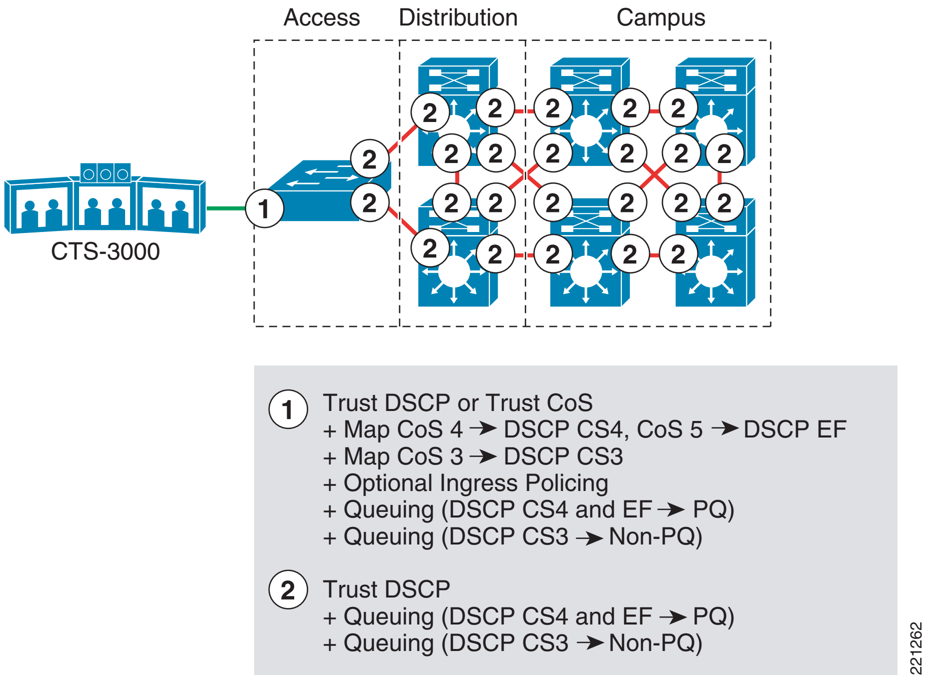
The reason it is recommended to trust DSCP and not CoS is two-fold: first, because marking granularity is lost every time a node is set to trust CoS. For example, if TelePresence endpoints are marking traffic to CS4 and Unified Video Advantage (or other Videoconferencing/Video Telephony endpoints) are marking their traffic to AF41 and the distribution-layer is set to trust CoS from the access-layer, then these flows both appear the same (as CoS 4) to the distribution-layer switch and are indistinguishable from each other from that node forward. Secondly, because trusting CoS implies using 802.1Q trunking between switches. Today, most enterprise campus networks are designed to be Layer 3 and thus 802.1Q is not used on inter-switch links.

Queuing is likewise recommended to be enabled on every node along the path. Note that this document generally focuses only on the QoS requirements for TelePresence. The actual QoS policies may be more complex than those shown here due to the myriad of other data, voice, and video applications on the network. It is recommended that customers use the information provided in this document in concert with

- *Enterprise QoS Solution Reference Network Design Guide*, Version 3.3, November 2005
- Szigeti, Tim and Hattingh, Christina. *End-to-End QoS Network Design: Quality of Service in LANs, WANs, and VPNs*. Indianapolis: Cisco Press, 2004. ISBN-10: 1-58705-176-1; ISBN-13: 978-1-58705-176-0.

A summary of the minimum QoS design requirements within an enterprise campus supporting TelePresence are illustrated in Figure 5-3.

Figure 5-3 ***Enterprise Campus QoS Design Recommendations for TelePresence***



1 Trust DSCP or Trust CoS
+ Map CoS 4 → DSCP CS4, CoS 5 → DSCP EF
+ Map CoS 3 → DSCP CS3
+ Optional Ingress Policing
+ Queuing (DSCP CS4 and EF → PQ)
+ Queuing (DSCP CS3 → Non-PQ)

2 Trust DSCP
+ Queuing (DSCP CS4 and EF → PQ)
+ Queuing (DSCP CS3 → Non-PQ)

TelePresence Campus Access-Layer QoS Designs

Now that campus-specific considerations have been addressed, we can look at how these policies can be configured on specific platforms. Before we identify the platforms, let's briefly review some of the key network and QoS-related features required by campus platforms at the access-layer. These include: 10/100/1000 connectivity, adequate dedicated or shared buffering to accommodate TelePresence traffic rates and sub-second bursts, granular policing, and 1PxQyT queuing. Optionally, it would be preferred to have support for conditional trust, Per-Port/Per-VLAN policing, as well as DSCP-to-Queue mapping (as opposed to CoS-to-Queue mapping).

Given these requirements, the following currently-shipping Catalyst platforms have been validated by Cisco Enterprise Systems Technical Marketing for TelePresence access-edge support:

- Catalyst 3560G and 3750G (and by extension the 3650-E and 3750-E)
- Catalyst 4500 and 4948
- Catalyst 6500 (Although only certain linecards are recommended. Some older linecards do not have the requisite buffer to handle TelePresence traffic rate and burst requirements.)

Platform-specific configurations for each of these series of switches are provided in subsequent sections.

Catalyst 3560G/3750G and 3650-E/3750E

The Cisco Catalyst 3560G is a fixed-configuration switch that supports up to 48 10/100/1000 ports with integrated Power over Ethernet (PoE), plus 4 Small Form-Factor Pluggable (SFP) ports for uplinks. The 3560 has a 32 Gbps backplane, which is moderately oversubscribed (52 Gbps theoretical maximum input vs. 32 Gbps backplane yields an oversubscription ratio of 1.625:1 or 13:8). Additionally, the 3560G supports IP routing (including IPv6), multicast routing, and an advanced QoS and security feature-set.

The Catalyst 3750G is nearly identical, with only a few additional key features, including the support for a stackable configuration (via Stackwise technology), allowing for the 32 Gbps backplane (comprised of dual counter-rotating 16 Gbps rings) to be extended over multiple 3750G switches (up to 9). Additionally, the 3750G provides support for 10 Gigabit Ethernet (10GE) connectivity. Obviously, however, the more switches in the stack, as well as the use of 10 GE connectors, increases the oversubscription ratio accordingly.

The 3560-E and 3750-E represent the next evolution of these switches. As before, the 3560-E is a fixed configuration switch, but now with a 128 Gbps backplane and 10 GE port support. Similarly, the 3750-E supports a 128 Gbps backplane with dual 10GE port support, as well as the support for a stackable configuration (via Stackwise Plus technology, allowing a 64 Gbps interconnect between stacked switches).

As the 3560G, 3750G, 3560-E, and 3750-E share virtually identical feature parity (the main differences being the backplane throughput and uplink port speeds), we consider them as a single switch and abbreviate the reference to simply C3560G/3750G.

From a QoS perspective, some of the relevant features of the C3560G/3750G/E include conditional trust, Per-Port/Per-VLAN policers (via Hierarchical QoS policies), DSCP-to-Queue mapping, 2Q3T or 1P1Q3T ingress queuing, and 4Q3T or 1P3Q3T egress queuing. Additionally, these platforms provide (minimally) 750 KB of receive buffers and 2 MB of transmit buffers for each set of 4 ports. These buffers can be allocated, reserved, or dynamically borrowed from a common pool, on a port-port, per-queue basis, depending on the administrative configurations chosen.

Let’s begin leveraging these features into the validated best-practice designs for this switch family for supporting TelePresence at the campus access-layer.

As QoS is disabled by default on these switches, the first step that we must take is to globally enable QoS. We can do this by issuing the global command:

```
mls qos
```

With QoS enabled, we can configure the access-edge trust boundaries. As discussed previously, we have three options: trust DSCP, trust CoS, or conditional trust. It is recommended that ports used for data and VoIP Telephony be configured to conditionally trust CoS, while ports used for TelePresence be configured to either trust DSCP, trust CoS or conditionally trust CoS. Trusting DSCP on these ports is the simplest operationally. The interface command to configure DSCP trust is fairly straightforward:

```
mls qos trust dscp
```

Note While Cisco IOS allows the configuration of trust CoS and conditional trust on uplink ports, uplink ports should be set to trust DSCP (only). This is required on the C3560G/3750G/E for two reasons: first, to preserve marking granularity between switches (as previously discussed in Campus Inter-Switch Link QoS Considerations), as well as to activate the DSCP-to-Queue mapping (versus the CoS-to-Queue mapping) on the uplink switch ports.

If you choose to trust CoS or conditionally trust CoS, ensure that the fifth parameter in the global CoS-to-DSCP map —which corresponds to the DSCP mapping for CoS 4—is set to 32 (CS4). Additionally, to support IP Telephony properly, the global CoS-to-DSCP mapping table should be modified such that CoS 5 (the sixth parameter in the CoS-to-DSCP map) is mapped to 46 (EF)—which is not the default (the default setting is 40/CS5). These settings are achieved via the following global and interface commands:

```
mls qos map cos-dscp 0 8 16 24 32 46 48 56
interface Gigx/y
 mls qos trust cos
```

If you choose to implement conditional trust on the TelePresence ports, it can be enabled with the following interface command:

```
mls qos trust device cisco-phone
```

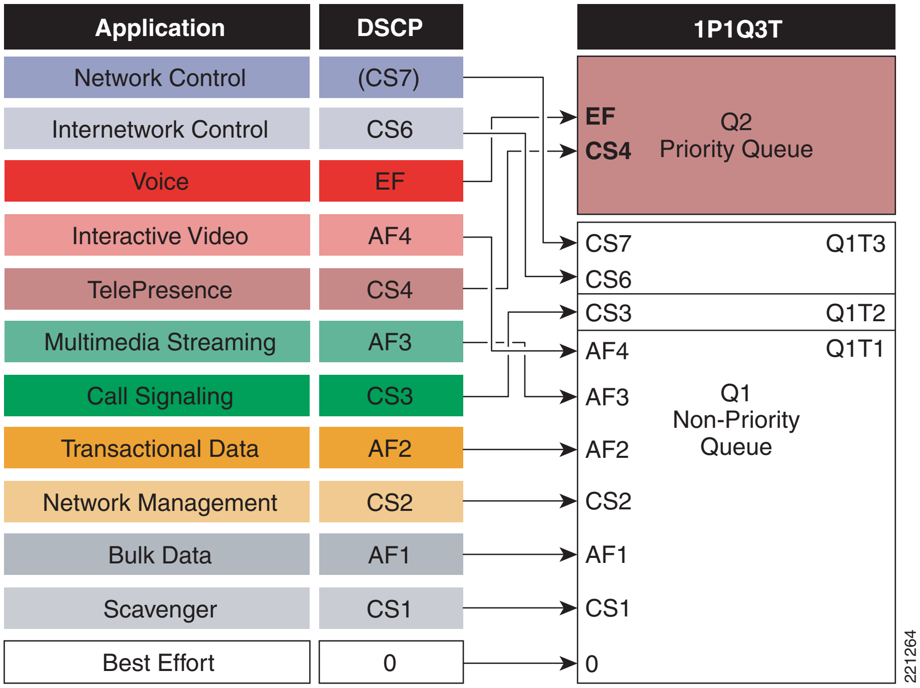
Note If conditional trust policies are to be used, then make sure that the TelePresence codec software is running version 1.1.0 (256D) or higher, as software version 1.0.1 (616D) incorrectly marks TelePresence audio traffic to CoS 5 (not CoS 4).

These configuration commands can be verified with the following commands:

- show mls qos
- show mls qos map cos-dscp
- show mls qos interface

Next, as the C3560G/3750G/E platforms have architectures based on oversubscription, they have been engineered to guarantee QoS by protecting critical traffic trying to access the backplane/stack-ring via ingress queuing. Ingress queuing on this platform can be configured as 2Q3T or 1P1Q3T. As we've already established the requirement for strict-priority servicing of TelePresence (and VoIP) traffic, it is recommended to enable the 1P1Q3T ingress queuing structure with DSCP EF (VoIP) and CS4 (TelePresence) being mapped to the ingress PQ (Q2). The configurable thresholds in the non-priority queue can be used to protect control traffic. For example, Network Control traffic (such as Spanning Tree Protocol) associated with DSCP CS7 and Internetwork Control traffic (such as Interior Gateway Protocols, including EIGRP and OSPF) marked DSCP CS6 can be explicitly protected by assigned these to Q1T3. Additionally, a degree or protection can be offered to Call-Signaling traffic (which is essentially control traffic for the IP Telephony infrastructure), which is marked CS3. All other traffic types can be provisioned in Q1T1. The recommended ingress 1P1Q3T queuing configuration for the C3560G/3750G/E platforms is illustrated in Figure 5-4.

Figure 5-4 Catalyst 3560G/3750G/E(1P1Q3T) Ingress Queuing Recommendations for TelePresence Deployments



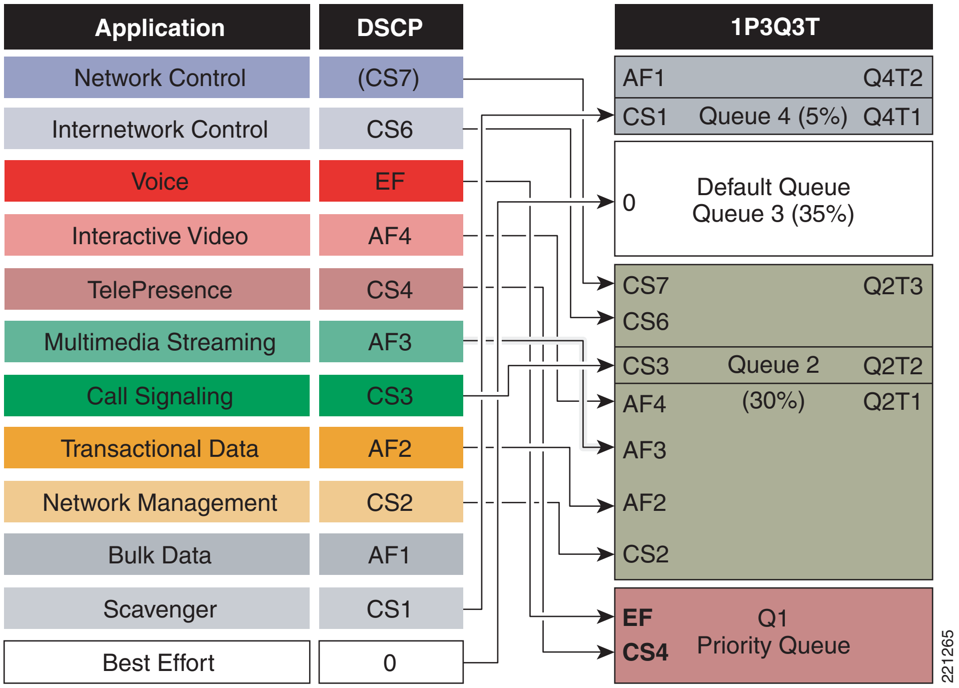
Based on Figure 5-4, the recommended configuration for ingress queuing on the C3560G/3750G/E for TelePresence deployments is as follows:

```
! This first section modifies the CoS-to-DSCP for VoIP

mls qos map cos-dscp 0 8 16 24 32 46 48 56
 ! Modifies CoS-to-DSCP mapping to map CoS 5 to DSCP EF


! This section configures the Ingress Queues and Thresholds for 1P1Q3T

mls qos srr-queue input buffers 70 30
 ! Configures the Ingress Queue buffers such that Q2 (PQ) gets 30% of buffers
mls qos srr-queue input priority-queue 2 bandwidth 30
 ! Configures the Ingress PQ (Q2) to be guaranteed 30% BW on stack ring
mls qos srr-queue input bandwidth 70 30
 ! Configures SRR weights between Ingress Q1 and Q2 for remaining bandwidth
mls qos srr-queue input threshold 1 80 90
 ! Configures Ingress Queue 1 Threshold 1 to 80% and Threshold 2 to 90%
 ! Ingress Queue 1 Threshold 3 remains at 100% (default)
 ! Ingress Queue 2 Thresholds 1, 2 and 3 remain at 100% (default)


! This section configures the Ingress CoS-to-Queue Mappings for TelePresence ports using
trust-CoS

mls qos srr-queue input  cos-map  queue 1 threshold 1 0 1 2
 ! Maps CoS 0, 1, 2 and 4 to Ingress Queue 1 (Q1T1)
mls qos srr-queue input  cos-map  queue 1 threshold 2 3
 ! Maps CoS 3 to Ingress Queue 1 Threshold 2 (Q1T2)
mls qos srr-queue input  cos-map  queue 1 threshold 3 6 7
 ! Maps CoS 6 and 7 to Ingress Queue 1 Threshold 3 (Q1T3)
mls qos srr-queue input  cos-map  queue 2 threshold 1 4 5
 ! Maps CoS 4 (TelePresence) and CoS 5 (VoIP) to Ingress-PQ Threshold 1 (Q2T1)
! This section configures the Ingress DSCP-to-Queue Mappings for TelePresence ports using
trust-DSCP

mls qos srr-queue input  dscp-map queue 1 threshold 1 0 8 10 12 14
 ! Maps DSCP 0, CS1 and AF1 to Ingress Queue 1 Threshold 1 (Q1T1)
mls qos srr-queue input  dscp-map queue 1 threshold 1 16 18 20 22
 ! Maps DSCP CS2 and AF2 to Ingress Queue 1 Threshold 1 (Q1T1)
mls qos srr-queue input  dscp-map queue 1 threshold 1 26 28 30 34 36 38
 ! Maps DSCP AF3 and AF4 to Ingress Queue 1 Threshold 1 (Q1T1)
mls qos srr-queue input  dscp-map queue 1 threshold 2 24
 ! Maps DSCP CS3 to Ingress Queue 1 Threshold 2 (Q1T2)
mls qos srr-queue input  dscp-map queue 1 threshold 3 48 56
 ! Maps DSCP CS6 and CS7 to Ingress Queue 1 Threshold 3 (Q1T3)
mls qos srr-queue input  dscp-map queue 2 threshold 1 32 46
 ! Maps DSCP CS4 (TelePresence)& EF (VoIP) to Ingress-PQ Threshold 1 (Q2T1)
```

Note Non-Standard DSCP values can also be mapped to their respective queues (using the CoS-to-Queue Map as a reference); however, for the sake of simplicity, non-standard DSCP-to-Queue Mappings have not been shown in these configurations.

Following ingress queuing configuration, we can now proceed to configuring the egress queues. The C3560G/3750G/E supports either 4Q3T or 1P3Q3T egress queuing configurations. As the need for an EF PHB has already been established, both for VoIP and for TelePresence, it is recommended to enable the 1P3Q3T egress queuing configuration, with Q1 as the PQ. Then both VoIP (DSCP EF) and TelePresence (DSCP CS4) should be mapped to Q1 (the PQ). Default traffic can be assigned to Q3 and Q4 can be designated as a less than Best Effort queue, servicing Bulk (AF1) and Scavenger (DSCP CS1) traffic, being assigned to Q4T2 and Q4T1, respectively. Network Control (DSCP CS7) and Internetwork Control (DSCP CS6) can be mapped to the highest threshold of the preferential non-priority queue (Q2T3), while Call-Signaling (DSCP CS3) can be mapped to the second highest threshold in that queue (Q2T2). All other applications can be mapped to Q2T1. The recommended 1P3Q3T egress queuing configuration for the C3560G/3750G/E platforms is illustrated in Figure 5-5.

Figure 5-5 Catalyst C3560G/3750G/E (1P3Q3T) Egress Queuing Recommendations for TelePresence Deployments



Application	DSCP
Network Control	(CS7)
Internetwork Control	CS6
Voice	EF
Interactive Video	AF4
TelePresence	CS4
Multimedia Streaming	AF3
Call Signaling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	0

Based on Figure 5-5, the recommended configuration for egress queuing on the C3560G/3750G/E for TelePresence deployments is as follows:

```
! This section configures the Output CoS-to-Queue Maps for TelePresence ports using
trust-CoS

mls qos srr-queue output cos-map queue 1 threshold 3 4 5
 ! Maps CoS 4 (TelePresence) and CoS 5 (VoIP) to Egress Queue 1 Threshold 3 (PQ)
mls qos srr-queue output cos-map queue 2 threshold 1  2
 ! Maps CoS 2 to Egress Queue 2 Threshold 1 (Q2T1)
mls qos srr-queue output cos-map queue 2 threshold 2  3
 ! Maps CoS 3 (Call-Signaling) to Egress Queue 2 Threshold 2 (Q3T2)
mls qos srr-queue output cos-map queue 2 threshold 3  6 7
 ! Maps CoS 6 and CoS 7 (Net Control) to Egress Queue 2 Threshold 3 (Q2T3)
mls qos srr-queue output cos-map queue 3 threshold 3  0
 ! Maps CoS 0 (Best Effort) to Egress Queue 3 Threshold 3 (Q3T3)
mls qos srr-queue output cos-map queue 4 threshold 3  1
 ! Maps CoS 1 (Bulk/Scavenger) to Egress Queue 4 Threshold 3 (Q4T3)


! This section configures the Output DSCP-to-Queue Maps for TelePresence ports using
trust-DSCP

mls qos srr-queue output dscp-map queue 1 threshold 3 32 46
 ! Maps DSCP CS4 (TelePresence) and EF (VoIP) to Egress Queue 1 (PQ)
mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22
 ! Maps DSCP CS2 and AF2 to Egress Queue 2 Threshold 1 (Q2T1)
mls qos srr-queue output dscp-map queue 2 threshold 1 26 28 30 34 36 38
 ! Maps DSCP AF3 and AF4 to Egress Queue 2 Threshold 1 (Q2T1)
mls qos srr-queue output dscp-map queue 2 threshold 2 24
 ! Maps DSCP CS3 to Egress Queue 2 Threshold 2 (Q2T2)
mls qos srr-queue output dscp-map queue 2 threshold 3 48 56
 ! Maps DSCP CS6 and CS7 to Egress Queue 2 Threshold 3 (Q2T3)
mls qos srr-queue output dscp-map queue 3 threshold 3 0
```

```
 ! Maps DSCP DF to Egress Queue 3 Threshold 3 (Q3T3 - Default Queue)
mls qos srr-queue output dscp-map queue 4 threshold 1 8
 ! Maps DSCP CS1 to Egress Queue 4 Threshold 1 (Q4T1)
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
 ! Maps DSCP AF1 to Egress Queue 4 Threshold 2 (Q4T2)


! This next section configures the WRED min and max thresholds for Q1

mls qos queue-set output 1 threshold 2 80 90 100 100
 ! Sets Egress Queue 2 Threshold 1 (Q2T1)Ò 80% and Threshold2 (Q2T2)Ò 90%
mls qos queue-set output 1 threshold 4 60 100 100 100
 ! Sets Egress Queue 4 Threshold 1 (Q4T1) Ò 60% and Threshold 2 (Q4T2)Ò 100%



! This section configures trust-DSCP and queuing on TelePresence access port and uplink
ports

interface GigabitEthernet1/0/1
 description TelePresence or Uplink port
 mls qos trust dscp
  ! Assigns the TelePresence port and/or uplink port to trust DSCP
 queue-set 1
  ! Assigns interface to Queue-Set 1 (default)
 srr-queue bandwidth share 1 30 35 5
  ! Q2 gets 30% of remaining BW (after PQ); Q3 gets 35% & Q4 gets 5%
 priority-queue out
 ! Expedite queue is enabled for TelePresence and VoIP
!


! This section configures conditional-trust and queuing on TelePresence access ports

interface GigabitEthernet1/0/2
 description IP Telephony and/or Data port
 mls qos trust device cisco-phone
  ! Configures conditional trust based on the CDP advertisements of the TelePresence
system and attached 7970G IP phone
 queue-set 1
  ! Assigns interface to Queue-Set 1 (default)
 srr-queue bandwidth share 1 30 35 5
  ! Q2 gets 30% of remaining BW (after PQ); Q3 gets 35% & Q4 gets 5%
 priority-queue out
 ! Expedite queue is enabled for TelePresence and VoIP
!
```

Note As before, non-Standard DSCP values can also be mapped to their respective queues (using the CoS-to-Queue Map as a reference); however, for the sake of simplicity, non-standard DSCP-to-Queue Mappings have not been shown in these configurations.

These configuration commands can be verified with the following commands:

- show mls qos queue-set
- show mls qos maps cos-input-q
- show mls qos maps dscp-input-q
- show mls qos maps cos-output-q
- show mls qos maps dscp-output-q

- show mls qos interface
- show mls qos interface buffers
- show mls qos interface queueing
- show controllers ethernet-controller port-asic statistics

Catalyst 4500 and 4948

The Cisco Catalyst 4500 series switches are midrange modular platforms with chassis options to support 3, 6, 7, and 10 slots; these models include the Catalyst 4503, 4506, 4507R, and 4510R, respectively (the latter two models supporting a redundant supervisor option). The Catalyst 4500 family of switches provides Layer 2 through Layer 4 network services, including advanced high-availability, security, and QoS services in addition to integrated PoE to support unified communications. The linecards that meet the requirements (at the time of writing) outlined in TelePresence Campus Access-Layer QoS Designs for the Catalyst 4500 include the 4448 and the 4548 series linecards (specifically, the WS-X4448-GB-RJ45 and the WS-X4524-GB-RJ45V or WS-X4548-GB-RJ45V).

On the other hand, the degree of oversubscription and buffering capabilities on the C4500 series linecards varies by linecard. Some linecards are entirely non-blocking, while others, such as the 4448 and the 4548, provision a single 1 Gbps uplink to the switch fabric for every 4 or 8 (10/100/1000) ports, which equates to an 4:1 (for the 4524) or an 8:1 (4448 and 4548) theoretical oversubscription ratio. As such, the 4448 and 4548 series linecards, while suitable at the campus access-edge, would not be recommended to be used as uplinks nor within the distribution and core layers of a TelePresence-enabled campus.

The Catalyst 4948 series provides an advanced feature set of intelligent network services, but is engineered and optimized to support high-performance wirespeed switching for data center server traffic. Thus the Catalyst 4948 has a completely non-blocking architecture and as such would be suitable at any layer (access, distribution, or core) within a TelePresence-enabled campus network. Specifically, the Catalyst 4948 provides 96 Gbps of switching fabric for its fixed configuration 48 x 10/100/1000 ports plus 4 SFP ports (which may be GE or 10 GE). Additionally, the Catalyst 4948 provides approximately 16 MB of buffering which is shared among all 48 ports.

As the Catalyst 4500 and 4948 share virtually identical feature parity (the main differences being the backplane throughput and buffer architectures), we consider them as a single switch and abbreviate the reference to simply C4500/4948.

From a QoS perspective, some of the relevant features of the C4500/4948 include conditional trust, an elegant Per-Port/Per-VLAN policer implementation, DSCP-to-Queue mapping, 4Q1T or 1P3Q1T queuing support. and an advanced congestion algorithm (Dynamic Buffer Limiting or DBL).

Let’s begin leveraging these features into the validated best-practice designs for this switch family for supporting TelePresence at the campus access-layer.

The first thing to note is a minor syntactical difference when configuring QoS features on the C4500/4948; specifically, QoS commands on this platform do not include the mls prefix used on the C3560G/3750G/E and the C6500 series platforms. For example, to globally enable QoS on the C4500/4948 (which is disabled by default), the command is not mls qos, but simply:

```
qos
```

With QoS enabled, we can configure the access-edge trust boundaries. As discussed previously, we have three options: trust DSCP, trust CoS, or conditional trust. It is recommended that ports used for data and VoIP Telephony be configured to conditionally trust CoS, while ports used for TelePresence be configured to either trust DSCP, trust CoS or conditionally trust CoS. Trusting DSCP on these ports is the simplest operationally.

```
qos trust dscp
```

If you choose to trust CoS or conditionally trust CoS, then CoS 5 must be explicitly mapped to DSCP EF prior to the port being configured to trust CoS. All other CoS-to-DSCP mappings can be left at their respective default values. These functions can be achieved via the following global and interface commands:

```
qos map cos 5 to 46
!
interface Gigx/y
 qos trust cos
```

If you choose to implement conditional trust on the TelePresence ports, it can be enabled with the following interface command:

```
qos trust device cisco-phone
```

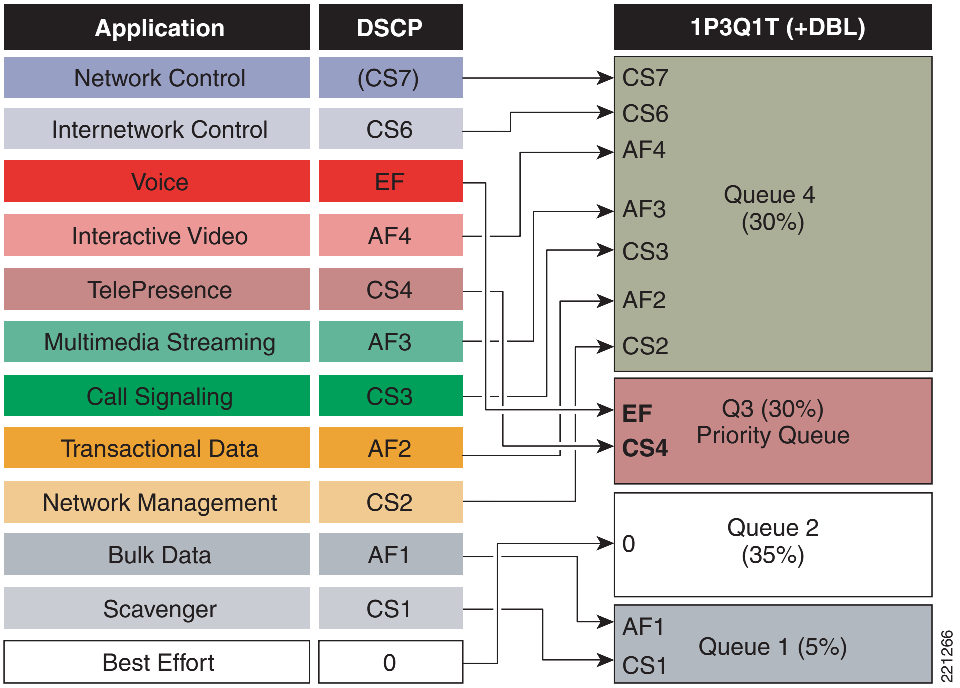
Note If conditional trust policies are to be used, then make sure that the TelePresence codec software is running version 1.1.0 (256D) or higher, as software version 1.0.1 (616D) incorrectly marks TelePresence audio traffic to CoS 5 (not CoS 4).

As with configuration commands, the C4500/4948 omits the mls prefix in the corresponding verification commands. These configuration commands can be verified with the following commands:

- show qos
- show qos maps
- show qos interface

As the C4500/4948 does not support ingress queuing (although it bears mentioning that the internal servicing architectures have been tested and found to be adequate in protecting TelePresence traffic even in the event of oversubscription), we can move on to configuring egress queuing. The C4500/4948 can be configured to operate in a 4Q1T mode or a 1P3Q1T mode, the latter of which is recommended for VoIP Telephony and TelePresence deployments. On the C4500, however, the strict priority queue, when enabled, is Q3. As the C4500/4948 supports DSCP-to-Queue mappings, we can distinguish between applications such as generic Videoconferencing/Video Telephony (AF4) and TelePresence (CS4), even though these share the same CoS and IP Precedence values (Cos/IPP 4). Given these abilities, it is recommended to enable 1P3Q1T queuing on the C4500/4948, with VoIP (EF) and TelePresence (CS4) assigned to the strict-priority queue (Q3). Q2 may be dedicated to service default traffic and Q1 can be used to service less than Best Effort Scavenger (CS1) and Bulk (AF1) traffic. All other applications can be mapped to Q4, the preferential queue. The recommended (1P3Q1T + DBL) egress queuing configuration for the C4500/4948 platform is illustrated in Figure 5-6.

Figure 5-6 Catalyst C4500/4948 (1P3Q1T + DBL) Egress Queuing Recommendations for TelePresence Deployments



Note As before, non-Standard DSCP values can also be mapped to their respective queues; however, for the sake of simplicity, non-standard DSCP-to-Queue Mappings have not been shown in these configurations.

As previously mentioned, the C4500/4948 supports an advanced congestion avoidance algorithm—Dynamic Buffer Limiting (DBL)—rather than Weighted Tail Drop (WTD) or Weighted-Random Early-Detect (WRED). Therefore no DSCP-to-Threshold mappings are required on the C4500/4948. However, to leverage DBL, it must be globally enabled (as it is disabled by default). This is achieved with the following global command:

```
qos dbl
```

Optionally, DBL can be configured to operate to support RFC 3168 IP Explicit Congestion Notification (IP ECN or simply ECN), which utilizes the remaining 2 bits of the IPv4/IPv6 Type of Service (ToS) Byte (the DSCP value uses the first 6 bits of the ToS Byte). The following global command enables ECN for DBL:

```
qos dbl exceed-action ecn
```

Note For more information on IP ECN, refer to RFC 3168 (at www.ietf.org/rfc/rfc3168) and Szigeti, Tim and Hattingh, Christina. *End-to-End QoS Network Design: Quality of Service in LANs, WANs, and VPNs*. Indianapolis: Cisco Press, 2004. ISBN-10: 1-58705-176-1; ISBN-13: 978-1-58705-176-0.

Additionally, to leverage DBL (with/without ECN) on a per-interface basis, a service policy applying DBL to all flows must be constructed and applied to each interface. This can be done by using the following basic policy-map:

```
policy-map DBL
```

```
 class class-default
  dbl
!
interface Gig x/y
 service policy output DBL
```

However, at this point, an important consideration pertaining to DBL much be taken into account, namely DBL (when enabled and configured as per the above recommendations) is active on all flows, including flows destined to the PQ (Q3)—which in our case includes VoIP and TelePresence traffic. As DBL introduces dynamic drops, especially on bursty, large-packet flows, this is detrimental to TelePresence call-quality. Therefore, to explicitly disable DBL on PQ traffic, the following amendments can be made to the previous policy:

```
class-map PQ
 match ip dscp ef
 match ip dscp cs4
policy-map DBL
 class PQ
 class class-default
  dbl
!
interface Gig x/y
 service policy output DBL
```

In this modified policy, the class-map PQ identifies traffic destined to the Priority Queue, specifically EF (VoIP) and CS4 (TelePresence) traffic. In the policy-map, the PQ-class receives no action (DBL or otherwise) and serves only to exclude these flows from the following class-default policy of applying DBL to all (other) flows. It is highly recommended to use this modified policy on C4500/4948 platforms supporting TelePresence in conjunction with DBL; otherwise DBL drops negatively impact TelePresence call-quality.

Piecing this together, the C4500/4948 egress queuing recommendation, shown in Figure 5-6, is as follows:

```
!This section enables DBL globally and excludes DBL on PQ flows

qos dbl
 ! Globally enables DBL
qos dbl exceed-action ecn
 ! Optional: Enables DBL to mark RFC 3168 ECN bits in the IP ToS Byte
class-map PQ
 match ip dscp ef
 match ip dscp cs4
  ! Classifies traffic mapped to PQ for exclusion of DBL-policy
policy-map DBL
 class PQ
  ! No action (DBL or otherwise) is applied on traffic mapped to PQ
 class class-default
  dbl
  ! Enables DBL on all (other) traffic flows


! This section configures the DSCP-to-Transmit Queue Mappings

qos map dscp 0 to tx-queue 2
 ! Maps DSCP 0 (Best Effort) to Q2
qos map dscp 8 10 12 14 to tx-queue 1
 ! Maps DSCP CS1 (Scavenger) and AF11/AF12/AF13 (Bulk) to Q1
qos map dscp 16 18 20 22 to tx-queue 4
 ! Maps DSCP CS2 (Net-Mgmt) and AF21/AF22/AF23 (Transactional) to Q4
qos map dscp 24 26 28 30 to tx-queue 4
 ! Maps DSCP CS3 (Call-Sig) and AF31/AF32/AF33 (MultiMedia) to Q4
```

```
qos map dscp 34 36 38 to tx-queue 4
 ! Maps DSCP AF41/AF42/AF43 (Interactive-Video) to Q4
qos map dscp 32 46 to tx-queue 3
 ! Maps DSCP CS4 (TelePresence) and EF (VoIP) to Q3 (PQ)
qos map dscp 48 56 to tx-queue 4
 ! Maps DSCP CS6 (Internetwork) and CS7 (Network Control) to Q4

! This section configures queues, activates the PQ and applies DBL

interface range GigabitEthernet1/1 - 48
 tx-queue 1
 bandwidth percent 5
  ! Q1 gets 5% BW
 tx-queue 2
 bandwidth percent 35
  ! Q2 gets 35% BW
 tx-queue 3
 priority high
  ! Q3 is PQ
 bandwidth percent 30
  ! Q3 (PQ) gets 30% BW
 shape percent 30
  ! Shapes/limits PQ to 30% BW
 tx-queue 4
 bandwidth percent 30
  ! Q4 gets 40%
 service-policy output DBL
  ! Applies DBL to all flows except VoIP & TelePresence
!
```

Note As before, non-Standard DSCP values can also be mapped to their respective queues; however, for the sake of simplicity, non-standard DSCP-to-Queue Mappings have not been shown in these configurations.

These configuration commands can be verified with the following commands:

- show qos dbl
- show qos maps dscp tx-queue
- show qos interface

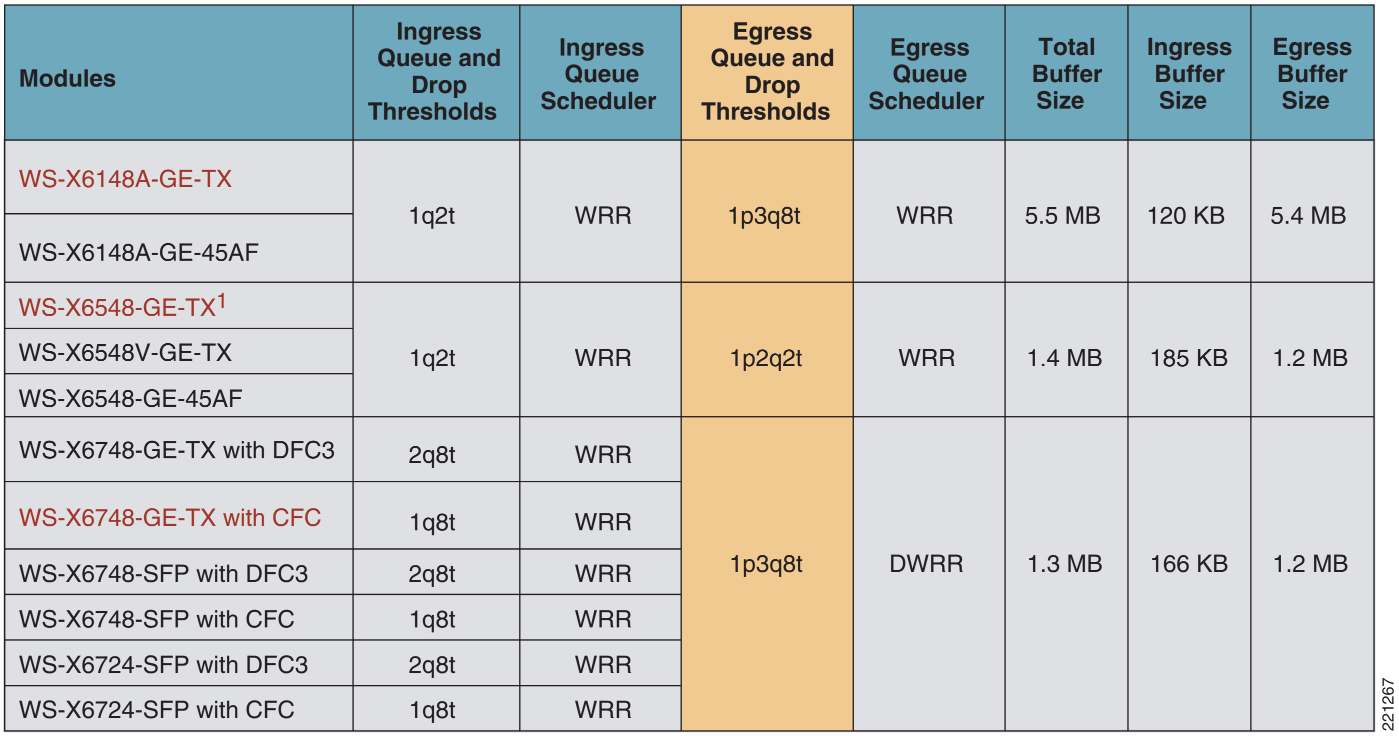
Catalyst 6500

The Cisco Catalyst 6500 series switches represent the flagship of Cisco's switching portfolio, delivering innovative secure, converged services throughout the campus, from the access-edge wiring closet to the distribution to the core to the data center to the WAN edge. The Catalyst 6500 platform is available in 3, 4, 6, 9, or 13 slot combinations; these models include the 6503, 6504, 6506, 6509 (regular or Network Equipment Building System [NEBS] compliant), and 6513. Additionally, these chassis options are also available in Enhanced models, designated by a -E suffix (such as 6503-E, 6504-E, etc.) for additional feature functionality and performance (except the 6513 at the time of writing).

Overall, the Catalyst 6500 provides the highest performance switching plane, supporting a 720 Gbps switching fabric and the option to run either centralized or distributed forwarding to achieve optimal performance. Additionally, the Catalyst 6500 provides leading-edge Layer 2-Layer 7 services, including rich High-Availability, Manageability, Virtualization, Security, and QoS feature sets, as well as integrated PoE, allowing for maximum flexibility in virtually any role within the campus.

The linecards that meet the requirements (at the time of writing) outlined in TelePresence Campus Access-Layer QoS Designs for the Catalyst 6500 include the 6148A, 6548, and the 6748 series linecards (specifically, the WS-X6148A-GE, the WS-X6548-GE, and the WS-X6748-GE families of linecards). These linecards support per-port buffers (which vary in size according to linecard) as well as ingress and egress queuing structures (which similarly vary according to linecard). The buffering and queuing details of these linecards are shown in Table 5-2.

Table 5-2 TelePresence Access-Layer 6500 Linecard Specifications



Modules	Ingress Queue and Drop Thresholds	Ingress Queue Scheduler	Egress Queue and Drop Thresholds	Egress Queue Scheduler	Total Buffer Size	Ingress Buffer Size	Egress Buffer Size
WS-X6148A-GE-TX	1q2t	WRR	1p3q8t	WRR	5.5 MB	120 KB	5.4 MB
WS-X6148A-GE-45AF							
WS-X6548-GE-TX[1]	1q2t	WRR	1p2q2t	WRR	1.4 MB	185 KB	1.2 MB
WS-X6548V-GE-TX							
WS-X6548-GE-45AF							
WS-X6748-GE-TX with DFC3	2q8t	WRR	1p3q8t	DWRR	1.3 MB	166 KB	1.2 MB
WS-X6748-GE-TX with CFC	1q8t	WRR					
WS-X6748-SFP with DFC3	2q8t	WRR					
WS-X6748-SFP with CFC	1q8t	WRR					
WS-X6724-SFP with DFC3	2q8t	WRR					
WS-X6724-SFP with CFC	1q8t	WRR					

[1] There are several other linecards in the Catalyst 6500 Series that may meet the requirements, but have not received CVD certification at the time of writing.

It is important to note that the 6148A-GE and the 6548-GE are both engineered with 8:1 oversubscription ratios and as such, while suitable at the access-layer, these linecards would not be recommended to deploy as uplinks or within the distribution and core layers of the TelePresence-enabled campus network. On the other hand, the 6748-GE is virtually non-blocking, supporting a dual 20 Gbps connection to the switch fabric for its 48 (10/100/1000) ports, which equates to a minimal 6:5 oversubscription ratio.

From a QoS perspective, some of the relevant features of the C6500 include port-trust, linecard-dependant queuing options, and WRED support. Let’s examine how these features can be leveraged into validated best-practice designs for the Catalyst 6500 (which we will abbreviate to C6500) at the access-edge.

As with the previously discussed switch platforms, QoS is disabled by default and must be explicitly enabled globally on the C6500 for any configured policies to take effect. The command to globally enable QoS on the C6500 is:

```
mls qos
```

With QoS enabled, we can configure the access-edge trust boundaries. At the time of writing, on the C6500, we have only two port-trust options: trust DSCP and trust CoS.

Note While trusting IP Precedence is a configurable option, this functionality is superseded by trusting DSCP. Additionally, at the time of writing, conditional trust is not available on the C6500.

When considering which trust option to configure, there is an important relationship between trust and ingress queuing on the C6500 to consider, namely, if a port is set to trust CoS, then ingress queuing is automatically enabled. This becomes an especially relevant consideration on linecards with high oversubscription ratios, such as the 6148A and 6548 (both with 8:1 oversubscription ratios). Therefore, it is recommended to set the ports connecting to TelePresence systems to trust CoS. However, keep in mind that if CoS is to be trusted, then ensure that the fifth parameter in the global CoS-to-DSCP map —which corresponds to the DSCP mapping for CoS 4—is set to 32 (CS4). Additionally, to support IP Telephony properly, the global CoS-to-DSCP mapping table should be modified such that CoS 5 (the sixth parameter in the CoS-to-DSCP map) is mapped to 46 (EF), which is not the default (the default setting is 40/CS5). These settings are achieved via the following global and interface commands:

```
mls qos map cos-dscp 0 8 16 24 32 46 48 56
interface Gigx/y
 mls qos trust cos
```

However, on all inter-switch link ports (uplinks/downlinks, etc.) it is recommended to set port-trust to trust DSCP to preserve marking granularity and Diffserv Per-Hop Behaviors. For this same reason, it is highly recommended to set port-trust to trust DSCP (or better yet, to use service policies with policers) on ports connected to endpoints that may be generating generic Videoconferencing/Video Telephony traffic (marked AF41); otherwise the DSCP value (AF41) for these flows will be lost and will be remapped to CS4 (since the CoS-to-DSCP map maps CoS 4 to DSCP CS4), eliminating your ability to distinguish between them on subsequent switch/router hops along the network path. The interface command to configure DSCP trust on an interface is as follows:

```
mls qos trust dscp
```

These configuration commands can be verified with the following commands:

- show mls qos
- show mls qos maps | begin Cos-dscp map
- show queueing interface gigabitethernet x/y | include trust

Before we describe linecard-specific queue recommendations, it bears mentioning that the queuing structures on the C6500—both ingress and egress—are CoS-based (with the sole exception, at the time of writing, of the WS-X6708-10GE, which supports DSCP-based queuing). This presents a challenge to network administrators deploying both generic Videoconferencing/Video Telephony (marked AF41 per RFC 4594) and TelePresence (marked CS4 per RFC 4594), as these applications both share the same CoS value of 4. As such, TelePresence and generic Videoconferencing/Video Telephony traffic are indistinguishable from one another with a CoS-based queuing scheme, with both applications always being mapped to the same queue. Since TelePresence requires an Expedited Forwarding Per-Hop Behavior (as explained in Chapter 4, "Quality of Service Design for TelePresence" and as allowed for by RFC 4594), both TelePresence and Videoconferencing/Video Telephony must be assigned to the strict-priority hardware queue on C6500 linecards (along with VoIP). Therefore, while this technical limitation exists, network administrators are encouraged to configure the hardware strict-priority queues on their C6500 platforms to adequately provision for their VoIP, TelePresence, and Videoconferencing/Video Telephony traffic.

While this may sound a bit complicated or excessive, in practice it is not that difficult to do, especially when considering that VoIP is such a lightweight application. For example, consider a Catalyst 6513 with redundant supervisors and 11 x 48-port linecards. If each of these ports supported VoIP, a total of only 68 Mbps of PQ would be required on the uplink (6.8% of a GigE link). Additionally, if a generic

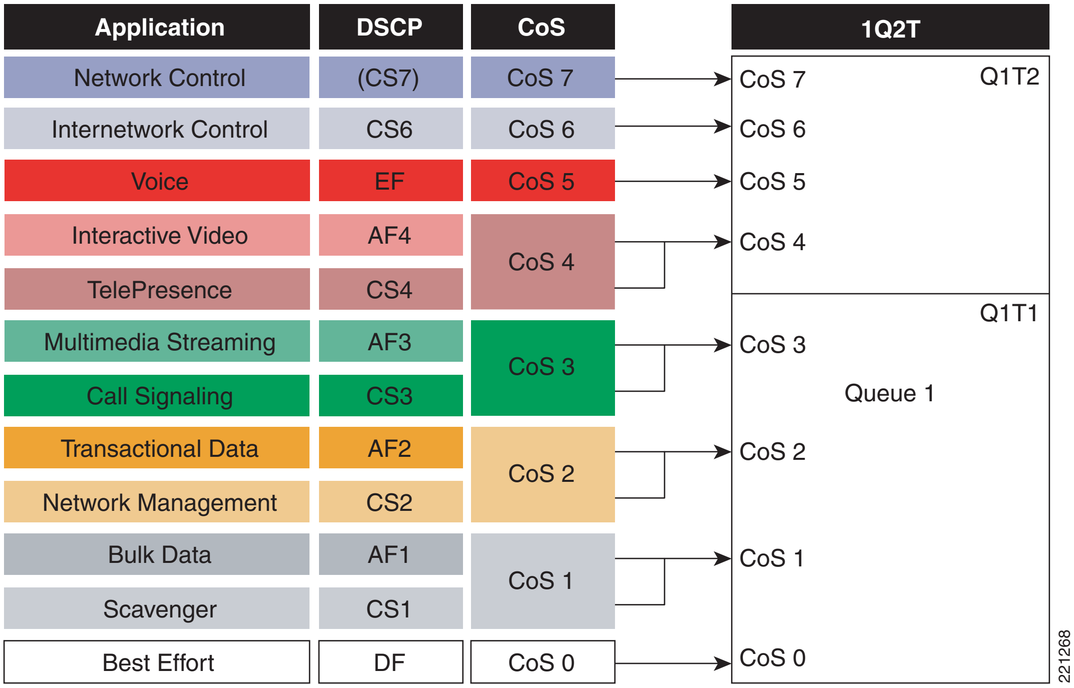
Videoconferencing/Video Telephony application was provisioned on each port that would permit 384 Kbps of AF41 video traffic per port, the combined total would be 270 Mbps (27% of a GE uplink). This leaves enough PQ traffic to support 2 separate CTS-3000 systems connected to the same chassis and still be at a theoretical maximum of only 30% of a single GE uplink.

With this in mind, let’s now consider the best practice ingress and egress queuing configurations for the 6148A, 6548 and 6748 linecards.

Ingress Queuing Design—1Q2T

As shown in Table 5-1, both the 6148A and 6548 linecards support a CoS-based ingress queuing structure of 1Q2T which can be leveraged to offset their oversubscription ratios. The 1Q2T ingress queuing structure uses Tail-Drop thresholds, which by default are set at 80% of the queue (Q1T1) and at 100% of the queue (Q1T2 which, incidentally, is non-configurable). By default, CoS values 0 through 4 are mapped to Q1T1 and CoS values 5 through 7 are mapped to Q1T2. The only improvement we can make on this default configuration to optimize TelePresence traffic on these oversubscribed linecards is to map CoS 4 (TelePresence) to the second threshold (Q1T2), along with CoS 5 (VoIP) and CoS 6 and 7 (Network Control traffic). The recommending ingress 1Q2T queuing configuration for C6500 6148A and 6548 linecards is illustrated in Figure 5-7.

Figure 5-7 Catalyst 6500 (1Q2T) Ingress Queuing Recommendations for TelePresence Deployments



Application	DSCP	CoS
Network Control	(CS7)	CoS 7
Internetwork Control	CS6	CoS 6
Voice	EF	CoS 5
Interactive Video	AF4	CoS 4
TelePresence	CS4	
Multimedia Streaming	AF3	CoS 3
Call Signaling	CS3	
Transactional Data	AF2	CoS 2
Network Management	CS2	
Bulk Data	AF1	CoS 1
Scavenger	CS1	
Best Effort	DF	CoS 0

The configuration for the C6500 1Q2T ingress queuing structure (for the 6148A and 6548 linecards) illustrated in Figure 5-7 is as follows:

```
interface GigabitEthernet x/y
 rcv-queue cos-map 1 1 0 1 2 3
  ! Maps CoS values 0-3 to Q1T1
 rcv-queue cos-map 1 2 4 5 6 7
  ! Maps CoS values 4-7 to Q1T2
```

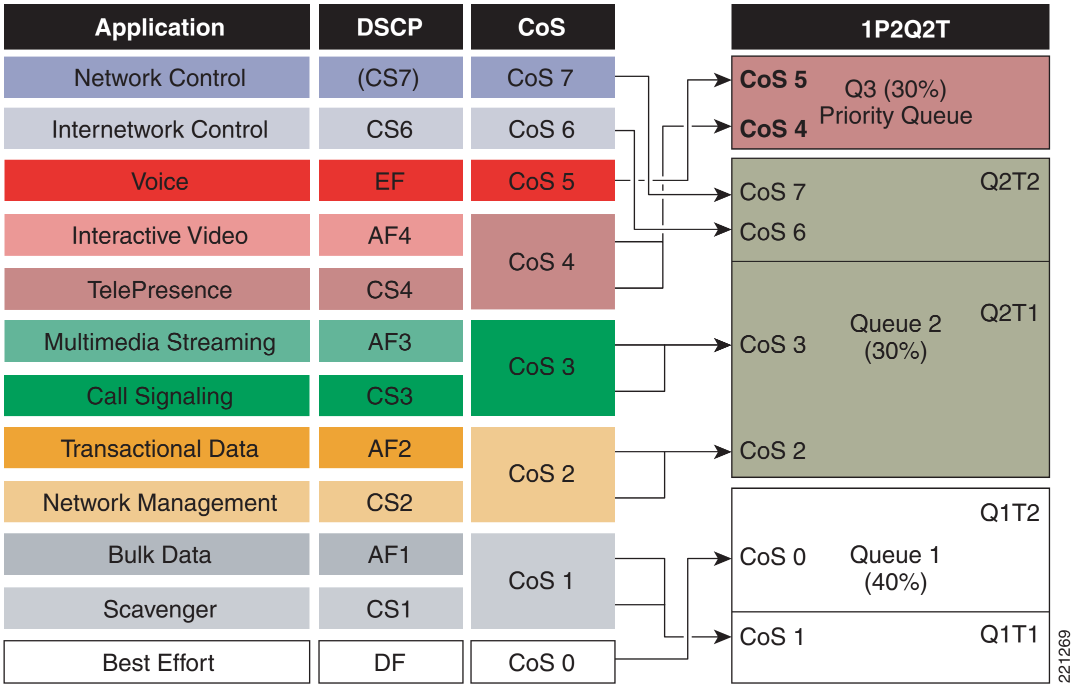
These configuration commands can be verified with the following command:

- show queueing interface GigabitEthernet x/y

Egress Queuing Design—1P2Q2T

As shown in Table 5-1, the 6548 linecards support a CoS-based egress queuing structure of 1P2Q2T, which uses WRED as a congestion avoidance mechanism. Under such a queuing structure, TelePresence traffic, along with VoIP, is recommended to be mapped to the strict-priority queue. Furthermore, because the egress queuing is CoS-based, Videoconferencing/Video Telephony (AF41) will also be assigned to the strict-priority queue. For non-realtime classes, the per-queue WRED thresholds can be configured to allow for granular QoS within a given queue. Specifically, Q1T1's minimum WRED threshold is set to 40% and its maximum threshold to 80%; then by mapping CoS 1 (Scavenger/Bulk) to Q1T1, we are restricting such traffic within Q1, with the remaining buffers (Q1T2) being exclusively reserved for CoS 0 (Best Effort traffic). Similarly, we can set Q2T1's minimum WRED threshold to 70% and maximum threshold to 80%; then by mapping CoS 2 (Transactional/Network Management) and CoS 3 (Call-Signaling/Multi-Media Streaming) to Q2T1, we are restricting these flows to a maximum of 80% of Q2, with the remaining buffers (Q2T2) being exclusively reserved for CoS 6 and 7 (Network Control traffic). The recommending egress 1P2Q2T queuing configuration for C6500 6548 linecards is illustrated in Figure 5-8.

Figure 5-8 Catalyst 6500 (1P2Q2T) Egress Queuing Recommendations for TelePresence Deployments



Application	DSCP	CoS
Network Control	(CS7)	CoS 7
Internetwork Control	CS6	CoS 6
Voice	EF	CoS 5
Interactive Video	AF4	CoS 4
TelePresence	CS4	
Multimedia Streaming	AF3	CoS 3
Call Signaling	CS3	
Transactional Data	AF2	CoS 2
Network Management	CS2	
Bulk Data	AF1	CoS 1
Scavenger	CS1	
Best Effort	DF	CoS 0

The configuration for the C6500 1P2Q2T egress queuing structure (for the 6548 linecards) illustrated in Figure 5-8 is as follows:

```
!
interface GigabitEthernet x/y

! This section sets the queue limits and bandwidth allocations
 wrr-queue queue-limit 40 30
```

```
  ! Sets the buffer allocations to 40% for Q1 and 30% for Q2
  ! Also implicitly sets PQ (Q3) to 30%)
 wrr-queue bandwidth 40 30
  ! Sets the WRR weights for 40:30 (Q1:Q2) bandwidth servicing

! This section sets the Min and Max WRED thresholds for Q1
 wrr-queue random-detect min-threshold 1 40 80
  ! Sets Min WRED Thresholds for Q1T1 and Q1T2 to 40 and 80, respectively
 wrr-queue random-detect max-threshold 1 80 100
  ! Sets Max WRED Thresholds for Q1T1 and Q1T2 to 80 and 100, respectively

! This section sets the Min and Max WRED thresholds for Q2
 wrr-queue random-detect min-threshold 2 70 80
 ! Sets Min WRED Thresholds for Q2T1 and Q2T2 to 70 and 80, respectively
 wrr-queue random-detect max-threshold 2 80 100
 ! Sets Max WRED Thresholds for Q2T1 and Q2T2 to 80 and 100, respectively

! This section maps the CoS values to the Queues/Thresholds
 wrr-queue cos-map 1 1 1
  ! Maps CoS 1 (Scavenger/Bulk) to Q1 WRED Threshold 1
 wrr-queue cos-map 1 2 0
  ! Maps CoS 0 (Best Effort) to Q1 WRED Threshold 2
 wrr-queue cos-map 2 1 2 3
  ! Maps CoS 2 (Trans-Data & Mgmt) and CoS 3 (Call-Sig + Multimedia) to Q2T1
 wrr-queue cos-map 2 2 6 7
  ! Maps CoS 6 (Routing) and CoS 7 (STP) to Q2 WRED Threshold 2
 priority-queue cos-map 1 4 5
  ! Maps CoS 4 (TelePresence & Interactive-Video) and CoS 5 (VoIP) to the PQ
!
```

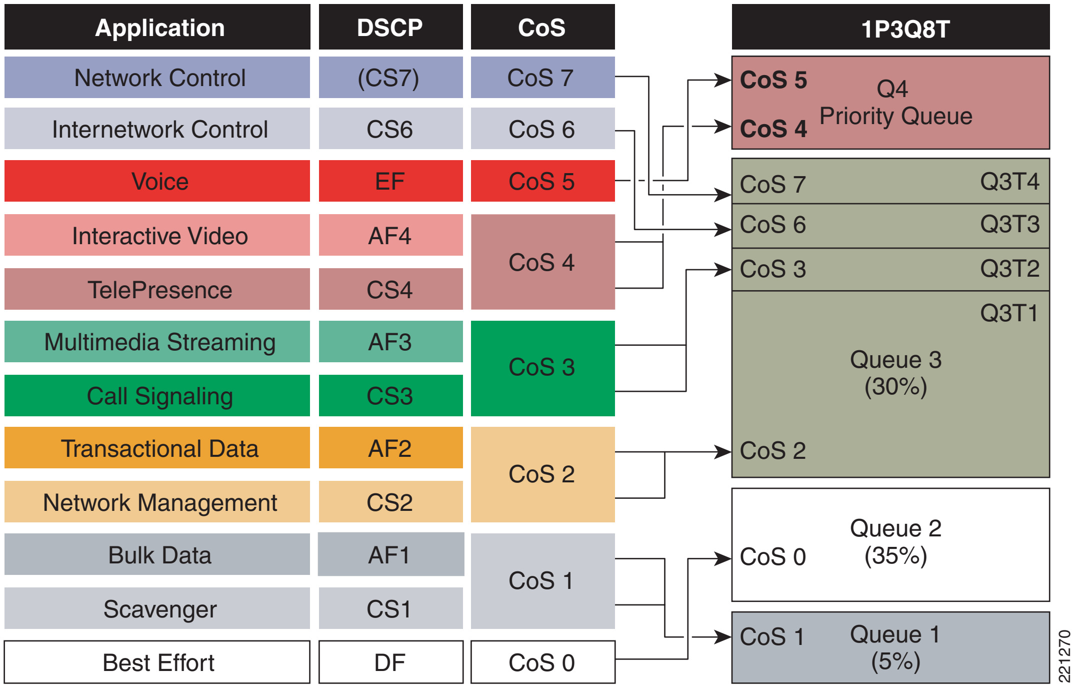
These configuration commands can be verified with the following command:

- show queueing interface GigabitEthernet x/y

Egress Queuing Design—1P3Q8T

As shown in Table 5-1, both the 6148A and 6748 linecards support a CoS-based egress queuing structure of 1P3Q8T, which uses WRED as a congestion avoidance mechanism. Under such a queuing structure, TelePresence traffic, along with VoIP, is recommended to be mapped to the strict-priority queue. Furthermore, because the egress queuing is CoS-based, Videoconferencing/Video Telephony (AF41) is also assigned to the strict-priority queue. CoS 1 (Scavenger/Bulk) can be constrained to a less than Best Effort queue: Q1. Q2 can then be dedicated for the default class (CoS 0). To minimize TCP global synchronization, WRED can be enabled on the non-realtime queues for congestion avoidance (technically, the congestion avoidance behavior is RED, as only one CoS weight is assigned to each queue). However, in Q3 the WRED thresholds can be set to give incremental preference to Network control traffic (CoS 7 and 6), followed by Call-Signaling traffic (CoS 3), and finally by Network Management traffic (CoS 2). The recommended egress 1P3Q8T queuing configuration for C6500 6148A and 6748 linecards is illustrated in Figure 5-9.

Figure 5-9 Catalyst 6500 (1P3Q8T) Egress Queuing Recommendations for TelePresence Deployments



The configuration for the C6500 1P3Q8T egress queuing structure (for the 6548 linecards) illustrated in Figure 5-9 is as follows:

```
interface GigabitEthernet x/y

! This section sets the queue limits and bandwidth allocations
 wrr-queue queue-limit 5 35 30
  ! Allocates 5% for Q1, 35% for Q2 and 30% for Q3
 priority-queue queue-limit 30
  ! Allocates 30% for the Strict-Priority Queue (Q4)
 wrr-queue bandwidth 5 35 30
  ! Sets the WRR weights for 5:35:30 (Q1:Q2:Q3) bandwidth servicing

! This section enables WRED on Q1, Q2 and Q3
 wrr-queue random-detect 1
  ! Enables WRED on Q1
 wrr-queue random-detect 2
  ! Enables WRED on Q2
 wrr-queue random-detect 3
  ! Enables WRED on Q3

! This section sets Q1T1 WRED Thresholds to 80% (min) and 100% (max)
 wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100
  ! Sets Min WRED Threshold for Q1T1 to 80% and all others to 100%
 wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100
  ! Sets Max WRED Threshold for Q1T1 to 100% and all others to 100%

! This section sets Q2T1 WRED Thresholds to 80% (min) and 100% (max)
 wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100
  ! Sets Min WRED Threshold for Q2T1 to 80% and all others to 100%
 wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100
  ! Sets Max WRED Threshold for Q2T1 to 100% and all others to 100%
! This sectin sets Q3T1 to 60:70, Q3T2 to 70:80, Q3T3 to 80:90 and Q3T4 to 90:100
 wrr-queue random-detect min-threshold 3 60 70 80 90 100 100 100 100
  ! Sets Min WRED Threshold for Q3T1 to 60%, Q3T2 to 70%, Q3T3 to 80%
  ! Q3T4 to 90%, and all others to 100%
 wrr-queue random-detect max-threshold 3 70 80 90 100 100 100 100 100
  ! Sets Max WRED Threshold for Q3T1 to 70%, Q3T2 to 80%, Q3T3 to 90%
  ! and all others to 100%

! This section maps CoS values to egress Queues/Thresholds
 wrr-queue cos-map 1 1 1
  ! Maps CoS 1 (Scavenger/Bulk) to Q1 WRED Threshold 1
 wrr-queue cos-map 2 1 0
  ! Maps CoS 0 (Best Effort) to Q2 WRED Threshold 1
 wrr-queue cos-map 3 1 2
  ! Maps CoS 2 (Net-Mgmt and Transactional Data) to Q3 WRED T1
 wrr-queue cos-map 3 2 3
  ! Maps CoS 3 (Call-Signaling and Mission-Critical Data) to Q3 WRED T2
 wrr-queue cos-map 3 3 6
  ! Maps CoS 6 (Routing) to Q3 WRED T3
 wrr-queue cos-map 3 4 7
  ! Maps CoS 7 (Spanning Tree) to Q3 WRED T4
 priority-queue cos-map 1 4 5
  ! Maps CoS 4 (TelePresence & Int-Video) and CoS 5 (VoIP) to the PQ
!
```

These configuration commands can be verified with the following command:

- show queueing interface GigabitEthernet x/y

Distribution and Core QoS Considerations and Design

The current Cisco Verified Design (CVD) certified testing of the Intra-Enterprise Deployment Model is limited to point-to-point TelePresence deployments. As such, aggregation scenarios—such as found in the distribution and core layers of the campus network where multiple point-to-point calls may traverse a single link—as well as the deployment of multipoint resources, have not yet received CVD certification.

Note Additional Place in the Network (PIN) design chapters for TelePresence, such as WAN/VPN design, will be added as Cisco Validated Design results become available.

CHAPTER 6

Branch QoS Design for TelePresence

TelePresence Branch QoS Design Overview

The primary business advantages of TelePresence systems include:

- Reduced travel time and expense
- Improved collaboration and productivity
- Improved quality of work/life (due to reduced travel)
- The green advantage of a reduced carbon footprint

However, these business advantages are not fully realized if TelePresence systems are connected solely via an Intra-Campus Deployment Model (as illustrated in Figure 3-1); rather, gaining these advantages requires TelePresence systems to be deployed over wide area networks, whether these are private WANs or Virtual Private Networks.

WANs or VPNs may be used to interconnect large campuses to each other or may be used to connect one or more large campuses with smaller branch offices (as illustrated in Figure 3-3). To simplify these permutations, we refer to all TelePresence connections over a wide area as Branch Places-in-the-Network (PINs).

Branch PINs serve as boundary points between local area and wide area networks and, as such, these are often the most bottlenecked PINs and therefore have the most critical QoS requirements within the network infrastructure. To help select the best policies to be used at these critical PINs, it is beneficial to review some important considerations, which we discuss next.

LLQ versus CBWFQ Considerations

Probably the most controversial decision relating to TelePresence deployments is whether to provision TelePresence traffic over the WAN/VPN in a strict-priority Low-Latency Queue (LLQ) or in a dedicated bandwidth-guaranteed Class-Based Weighted-Fair Queue (CBWFQ).

In campus networks, placing TelePresence in the strict-priority hardware queues yielded superior results during testing, especially in terms of protection against packet loss during momentary periods of congestion, which occur regularly in campus networks even under normal operating conditions. Additionally, placing TelePresence traffic in these strict-priority queues does not involve any incremental or ongoing monetary expense (beyond initial configuration), as this potential for strict-priority servicing already exists within the campus network infrastructure and the exercise simply becomes a matter of re-configuring existing queuing structures to enable strict-priority queuing for TelePresence.

Therefore, the decision to service TelePresence with strict-priority queues within the campus is relatively straightforward.

However, the corresponding decision becomes more complicated over the WAN/VPN due to three main considerations:

- The cost of subscribing to realtime SP services
- The "33% LLQ Rule"
- The potential effect of TelePresence on VoIP

Let us look at each of these considerations in turn. The first and foremost consideration is the ongoing cost of subscribing to realtime services from a service provider. Service providers generally charge enterprise customers premium rates for the amount of traffic they want serviced within a realtime class. At times, these additional premiums may make it cost prohibitive to provision TelePresence traffic within a realtime SP class. At the very least, such expensive premiums could diminish the overall business cost savings that TelePresence can provide an enterprise (versus employee travel expenses).

The second consideration is the potential impact of the "33% LLQ Rule" (referenced in Chapter 4, "Quality of Service Design for TelePresence" in the section Queuing TelePresence). At times, administrators cannot provision adequate amounts of bandwidth for TelePresence and remain within this conservative design recommendation. This is generally the case when dealing with (45 Mbps) T3/DS3 links. According to the "33% LLQ Rule," no more than 15 Mbps of traffic of such a link should be assigned for strict-priority servicing. However, if a network administrator already has VoIP provisioned (quite properly) in an LLQ on such a link, and is looking to also provision TelePresence with strict-priority servicing, then they have a decision to make. For example, if they wish to deploy a CTS-3000 at 1080p-Best (requiring 15 Mbps just for TelePresence), then they either have to upgrade the link's bandwidth capacity (which is often cost-prohibitive, as generally the next tier of bandwidth is OC3) or they violate this design rule to accommodate all of their realtime traffic.

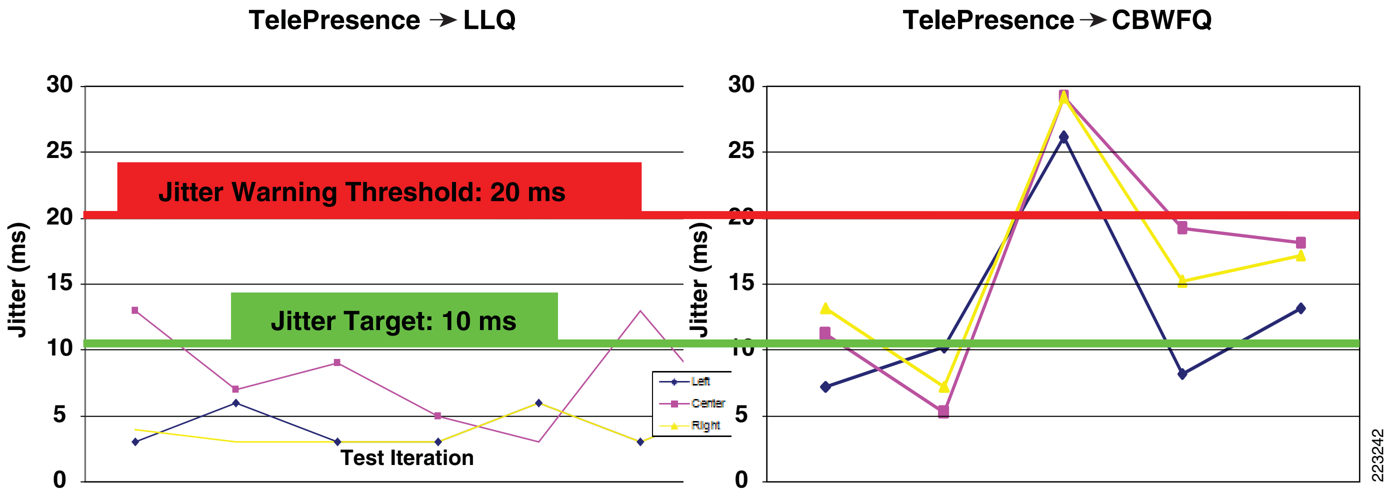
At this point, it bears repeating that the "33% LLQ Rule" is a conservative design recommendation, with the intent of reducing the variance in application response times of non-realtime applications during periods that the realtime classes are being utilized at maximum capacity. This is an exceptionally relevant concern when dealing with a high-bandwidth realtime application such as TelePresence.

For example, let us reconsider a (45 Mbps) T3/DS3 link configured to support two separate CTS-3000 calls, both configured to transmit at full 1080p-Best resolution. Each such call requires 15 Mbps of realtime traffic. Prior to TelePresence calls being placed, non-realtime applications would have access to 100% of the bandwidth (to simplify the example, we are assuming there are no other realtime applications, such as VoIP, on this link). However, once these TelePresence calls are established, realtime TelePresence calls would suddenly dominate more than 66% of the link and all non-realtime applications would just as suddenly be contending for less than 33% of the link. TCP windowing for many of these non-realtime applications would begin slow-starting, resulting in many data applications hanging, timing out, or becoming stuck in a non-responsive state. Such network behavior, changing from one minute to the next, generally translates into users calling the IT help desk complaining about the network (which happens to be functioning properly, albeit in a poorly-configured manner).

That being said, it bears repeating that the "33% LLQ Rule" rule is not to be viewed as a mandate, but is simply a best practice design recommendation. There may be cases where specific business objectives cannot be met while holding to this recommendation. In such cases, enterprises must provision according to their detailed requirements and constraints. However, it is important to recognize the tradeoffs involved with over-provisioning realtime traffic classes in conjunction with the negative performance impact this has on non-realtime-application response times.

Quite naturally then, to make such provisioning decisions, a network administrator might wonder about the tradeoffs involved in TelePresence application performance when TelePresence is placed in a LLQ versus a CBWFQ. In such a comparison, the most sensitive service level attribute is jitter, as both policies can be configured to completely prevent packet loss. As one might suspect, provisioning TelePresence in a LLQ results in lower peak-to-peak jitter values, as compared to provisioning TelePresence in a CBWFQ, which is shown in Figure 6-1.

Figure 6-1 Jitter Comparisons Between LLQ and CBWFQ WAN Edge Queuing Policies



Cisco Enterprise System Engineering testing showed that a 12-class RFC 4594-based QoS policy on a fully-congested T3 link—with TelePresence being serviced in a LLQ—yielded between 3-13 ms of peak-to-peak jitter to TelePresence; whereas an identical test—but with TelePresence being serviced in a CBWFQ—yielded between 5-29 ms of peak-to-peak jitter to TelePresence. As detailed in Chapter 4, "Quality of Service Design for TelePresence," TelePresence has a one-way peak-to-peak jitter target of 10 ms and a warning threshold of 20 ms of peak-to-peak jitter, which if exceeded over an extended period can generate warning messages on the screen. During some of the CBWFQ tests, this warning message was observed on the screen, indicating that network congestion was affecting the TelePresence call quality.

Note These tests were performed using TelePresence codec software version 1.1.0 (256D). Newer versions of CTS software have superior traffic smoothing capabilities as well as deeper de-jitter buffering, both of which amount to less overall sensitivity of TelePresence to jitter. Therefore the advantage of LLQ over CBWFQ queuing policies is less with newer versions of CTS software.

Therefore, while a moderate performance advantage to TelePresence can be observed when it is provisioned in a LLQ versus a CBWFQ, the advantage is not so great as to preclude recommending provisioning TelePresence in a CBWFQ when it is not viable to be provisioned with a LLQ. In other words, from a purely technical standpoint, **the best performance levels for TelePresence can be achieved when it is provisioned in a LLQ**. However, when other factors (such as additional ongoing costs or over-provisioning constraints for realtime bandwidth, etc.) need to be taken into account and render provisioning TelePresence in an LLQ unviable, then **the next best levels of service can be achieved by provisioning TelePresence in a dedicated CBWFQ**.

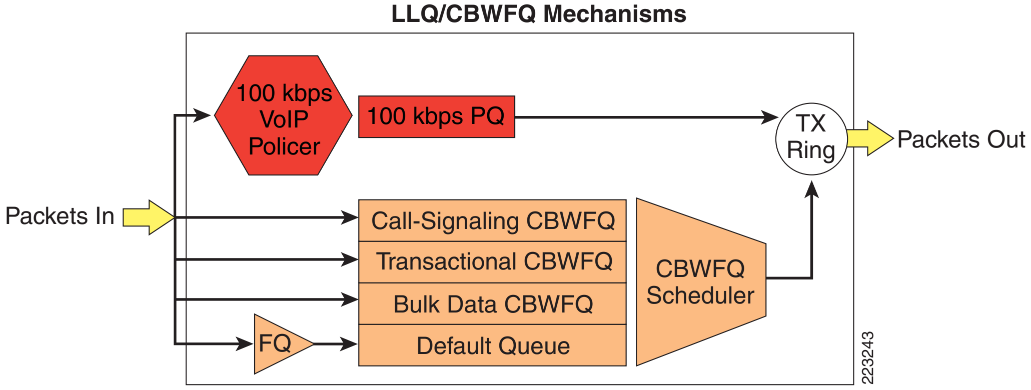
The third main consideration of whether to use LLQ or CBWFQ is the potential effect of TelePresence traffic on VoIP traffic if both are to be serviced in a strict-priority queue. To better understand how these realtime applications can be provisioned with strict-priority servicing and protected from interfering with each other, we must take a closer look at Cisco's IOS LLQ/CBWFQ mechanisms. To do so, let us consider a simple LLQ/CBWFQ policy.

Example 6-1 Simple LLQ/CBWFQ Policy

```
policy-map WAN-EDGE
 class VOIP
  priority 100
 class CALL-SIGNALING
  bandwidth percent 5
 class TRANSACTIONAL
  bandwidth percent 20
 class BULK
  bandwidth percent 10
 class class-default
  fair-queue
```

The underlying mechanisms for this LLQ/CBWFQ policy are graphically represented in Figure 6-2.

Figure 6-2 Cisco IOS LLQ/CBWFQ Mechanisms—Part 1



Note For the sake of simplicity, some Layer 2 subsystems (including Link Fragmentation and Interleaving) have been omitted from Figure 6-2, as these mechanisms simply are not relevant at the link speeds required by TelePresence.

In Figure 6-2, we see a router interface that has been configured with a 5-class LLQ/CBWFQ policy, with VoIP assigned to a 100 kbps LLQ and additional three explicit CBWFQs defined for Call-Signaling, Transactional Data, and Bulk Data respectively, as well as a default queue that has a Fair-Queuing pre-sorter assigned to it. There are two additional underlying mechanisms that may not be obvious from the configuration, but are shown in Figure 6-2:

- An implicit policer attached to the LLQ
- A final output buffer called the Tx-Ring

Let us first take a look at the implicit policer attached to the LLQ. The threat posed by any strict priority-scheduling algorithm is that it could completely starve lower priority traffic. To prevent this, the LLQ mechanism has a built-in policer. This policer (like the queuing algorithm itself) engages only when the interface is experiencing congestion. Therefore, it is important to provision the priority classes properly. In this example, if more than 100 kbps of VoIP traffic was offered to the interface and the interface was congested, the excess VoIP traffic would be discarded by the implicit policer. However, traffic admitted by the policer gains access to the strict priority queue and is handed off to the Tx-Ring ahead of all other CBWFQ traffic.

The Tx-Ring is a final output buffer that serves the purpose of always having packets ready to be placed onto the wire so that link utilization can be driven to 100%. It is actually a full Tx-Ring that signals the Cisco IOS software to indicate that an interface is experiencing congestion and as such the LLQ/CBWFQ algorithms need to be engaged.

Now, let us consider the case of servicing not just VoIP with strict-priority queuing, but also TelePresence.

Note For the sake of example and illustration simplicity, let us assume TelePresence only requires 400 kbps of traffic for these next two examples only.

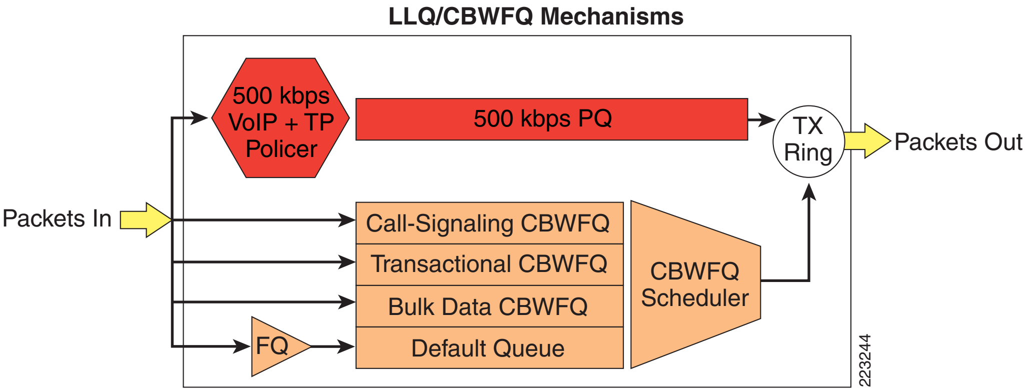
Two options exist to the network administrator. The first is to admit both VoIP and TelePresence to the same LLQ. Thus our example policy becomes:

Example 6-2 VoIP and TelePresence in a Single LLQ Policy

```
class-map match-any REALTIME
 match dscp ef                ! Matches VoIP
 match dscp cs4               ! Matches TelePresence
…

policy-map WAN-EDGE
 class REALTIME
  priority 500                ! 100 kbps for VoIP + 400 kbps for TelePresence
 class CALL-SIGNALING
  bandwidth percent 5
 class TRANSACTIONAL
  bandwidth percent 20
 class BULK
  bandwidth percent 10
 class class-default
  fair-queue
```

The corresponding IOS mechanisms for Example 6-2 are illustrated in Figure 6-3.

Figure 6-3 Cisco IOS LLQ/CBWFQ Mechanisms—Part 2



In Figure 6-3, we can see that not only has the LLQ been expanded in size (to 500 kbps), but also the implicit policer (for the combined VoIP and TelePresence class) has been increased to 500 kbps. Such a policy continues to protect VoIP from data as well as TelePresence from data. However, this policy does potentially allow TelePresence to interfere with VoIP. This is because traffic offered to the LLQ class is serviced on a first-come, first-serve basis. Therefore, should TelePresence traffic suddenly burst, then it is possible—even likely—that VoIP traffic would be dropped.

At this point, we can realize another benefit of the implicit policer for the LLQ: not only does this mechanism protect non-realtime queues from bandwidth-starvation, but also it allows for Time-Division Multiplexing (TDM) of the LLQ. TDM of the LLQ allows for the configuration and servicing of "multiple" LLQs, while abstracting the fact that there is only a single LLQ "under-the-hood," so to speak. Pertinent to our example, by configuring two LLQs, not only are VoIP and TelePresence protected from data applications, but VoIP and TelePresence are also protected from interfering with each other.

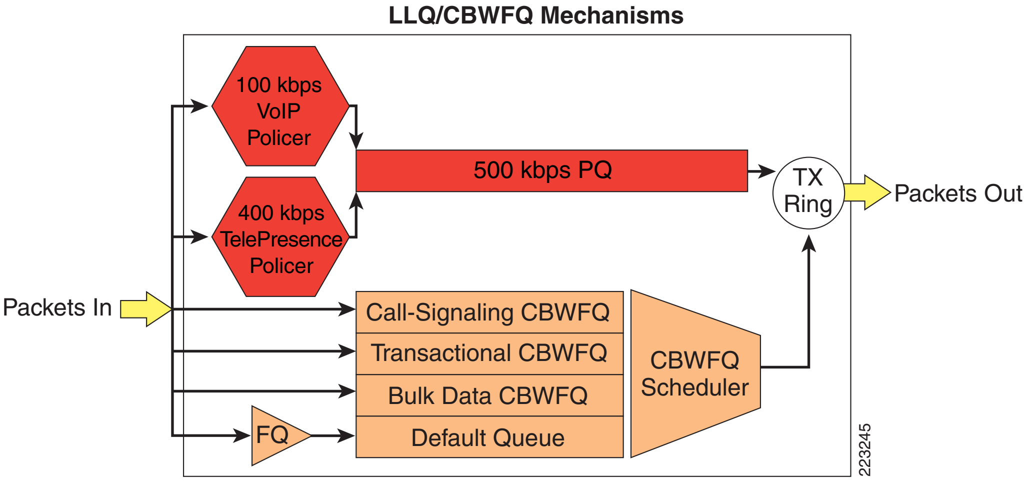
Let us take a look at our final policy example to cover this point. In Example 6-3, a dual-LLQ design is used, one each for VoIP and TelePresence.

Example 6-3 VoIP and TelePresence in a Dual-LLQ Policy

```
class-map match-all VOIP
 match dscp ef                 ! Matches VoIP
class-map match-all TELEPRESENCE
 match dscp cs4                ! Matches TelePresence
…

policy-map WAN-EDGE
 class VOIP
  priority 100                 ! 100 kbps LLQ for VoIP
class TELEPRESENCE
  priority 400                 ! 400 kbps LLQ for TelePresence
 class CALL-SIGNALING
  bandwidth percent 5
 class TRANSACTIONAL
  bandwidth percent 20
 class BULK
  bandwidth percent 10
 class class-default
  fair-queue
```

The corresponding IOS mechanisms for Example 6-3 are illustrated in Figure 6-4.

Figure 6-4 Cisco IOS LLQ/CBWFQ Mechanisms—Part 3



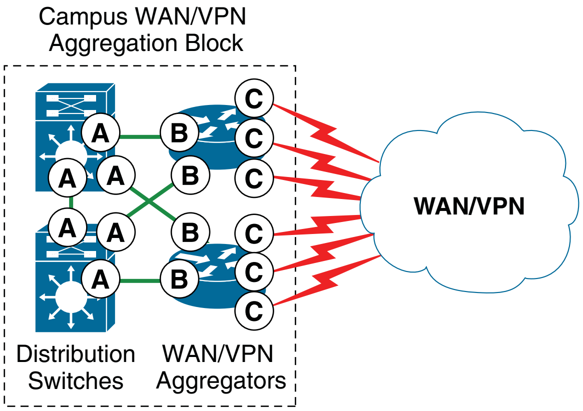
In Figure 6-4, we see that two separate implicit policers have been provisioned, one each for the VoIP class (to 100 kbps) and another for the TelePresence class (to 400 kbps), yet there remains only a single strict-priority queue, which is provisioned to the sum of all LLQ classes, in this case to 500 kbps (100 kbps + 400 kbps). Traffic offered to either LLQ class is serviced on a first-come, first-serve basis until the implicit policer for each specific class has been invoked. For example, if TelePresence attempts to burst beyond a 400 kbps rate (remember, this rate has been reduced in order to simplify this example, both textually and also graphically), then it is dropped.

Therefore, to sum up this final consideration regarding whether or not to use LLQ for TelePresence: **if strict priority servicing for TelePresence is desired and viable, and if another realtime class (such as VoIP) has already been configured with a LLQ, then a dual-LLQ design would be recommended** in order to protect VoIP and TelePresence from interfering with each other.

Campus WAN/VPN Block Considerations

Typically the first step in connecting a branch to a campus is to build out a WAN/VPN aggregation block at the main campus site. An example enterprise campus WAN/VPN aggregation block is illustrated in Figure 6-5.

Figure 6-5 Enterprise Campus WAN/VPN Aggregation Block QoS Design Recommendations for TelePresence



A **Interswitch Link Policies:**
Trust DSCP
+ Queuing (CoS 4 and 5 → PQ)
+ Queuing (CoS 3 → Non-PQ)

B **Router LAN Edge Policies:**
Trust DSCP (default)
+ LLQ for VoIP (EF)
+ LLQ for TelePresence (CS4)
+ CBWFQ for Call-Signaling (CS3)

C **WAN/VPN Edge QoS Policies:**
Trust for VoIP (EF)
+ LLQ or CBWFQ for TelePresence (CS4)
+ CBWFQ for Call-Signaling (CS3)

Interswitch links are shown in Figure 6-5 as points labeled A. While technically-speaking some of these links are interconnecting switches to routers, however their role and configuration are the same as the interswitch links described and defined in Chapter 5, "Campus QoS Design for TelePresence." To be completely technically accurate, we could refer to these links as LAN-to-LAN non-edge links , but this term becomes a bit wordy and unwieldy, and as such we continue to use the simpler term interswitch links, but with a broadened meaning to include these switch-to-router links as well.

Note As noted above, the term used here as interswitch links in this context refers to LAN-to-LAN non-edge links, not (necessarily) trunked links encapsulated with Cisco InterSwitch Link (ISL) trunking protocol.

As previously detailed (in Chapter 5, "Campus QoS Design for TelePresence"), all interswitch links should be configured to trust DSCP and perform hardware queuing, such that CoS 4 (TelePresence) and CoS 5 (VoIP) are assigned to the strict priority hardware queue and CoS 3 (Call-Signaling) is assigned to a non-priority queue within the platform/linecard's 1PxQyT queuing structure.

Next, it would be recommended to enable LLQ/CBWFQ (or hardware queuing policies, if supported) on the router's LAN edges, labeled as points B in Figure 6-5. This is recommended when the levels of WAN/VPN aggregation may make it theoretically possible to oversubscribe these WAN-to-LAN links. For example, if the WAN/VPN aggregation router was homing seven individual OC3 circuits (totaling 7 * 155 Mbps or 1.085 Gbps), but connecting to the distribution switches via GigabitEthernet links, then the potential for oversubscription on these WAN-to-LAN links would exist. Therefore, these links should be protected with a queuing policy, as a queuing policy would be the only way to provide service level **guarantees** on these links, regardless of how rarely these queuing policies would engage. As discussed in the previous section, if LLQ is to be used for VoIP and TelePresence, then these should be configured with a dual-LLQ policy, similar to the simplified example provided in Example 6-3 (but with different bandwidth values for both VoIP and TelePresence, based on how many calls of each type were being supported over these links).

Finally, WAN/VPN edge QoS policies would be required on all points labeled C in Figure 6-5. The specifics of these WAN/VPN edge policy permutations are discussed in detail in this chapter.

TelePresence Branch LAN Edge

The LAN edge of the branch PIN performs essentially the same QoS services as does the campus access edge, namely the enforcement of a trust boundary, CoS-to-DSCP mapping (if required), optional TelePresence policing (to prevent network abuse of a trusted switch port), and queuing. However, there are some design considerations unique to the branch LAN edge discussed below.

TelePresence Branch LAN Edge QoS Design Considerations

Depending on the platform(s) used at the branch, QoS functions may be performed in hardware, in software, or in a combination of both. This is because Cisco IOS-based routers perform QoS in software, while Cisco Catalyst switches perform QoS in hardware. Additionally, some devices, such as the Cisco Integrated Services Routers, combine functionality from both product families within a single platform (for example, a Cisco ISR equipped with a Cisco EtherSwitch network module).

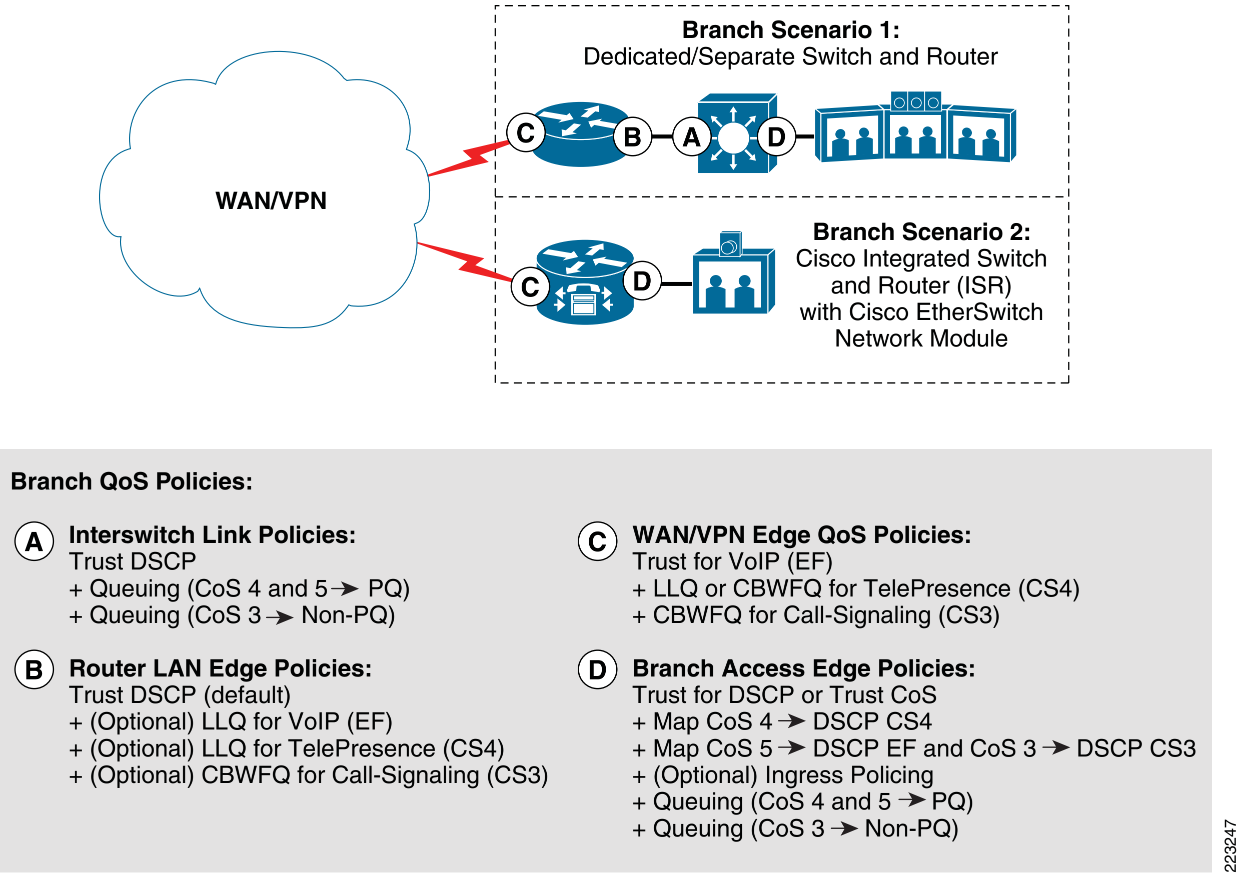
A general rule of thumb relating to QoS design is to **always enable QoS policies in hardware, rather than in software**, whenever a choice exists. This is because QoS policies performed in software require (marginal) incremental CPU loads to enforce (the actual incremental load varies according to platform, line rates, policy complexity, traffic patterns, and other variables). However, QoS policies performed in hardware are performed at line rates (GE or 10GE) without **any** incremental load to the CPU. Therefore, it is generally more efficient and effective to design QoS policies to be performed within hardware whenever possible.

Applying this rule of thumb to the branch LAN edge would typically result in one of two scenarios:

- The first scenario consists of a Cisco router on the WAN edge connecting to a Cisco Catalyst switch, which then connects to the branch endpoints, including the TelePresence system.
- The second scenario consists of a Cisco Integrated Services Router equipped with an EtherSwitch module performing all QoS functions within a single box.

These scenarios and their respective placements of QoS policies are illustrated in Figure 6-6.

Figure 6-6 Enterprise Branch QoS Design Recommendations for TelePresence


Branch Scenario 1:
Dedicated/Separate Switch and Router
WAN/VPN
C
B
A
D
Branch Scenario 2:
Cisco Integrated Switch and Router (ISR) with Cisco EtherSwitch Network Module
C
D
223247

Branch QoS Policies:

(A) Interswitch Link Policies:
Trust DSCP
+ Queuing (CoS 4 and 5 → PQ)
+ Queuing (CoS 3 → Non-PQ)

(B) Router LAN Edge Policies:
Trust DSCP (default)
+ (Optional) LLQ for VoIP (EF)
+ (Optional) LLQ for TelePresence (CS4)
+ (Optional) CBWFQ for Call-Signaling (CS3)

(C) WAN/VPN Edge QoS Policies:
Trust for VoIP (EF)
+ LLQ or CBWFQ for TelePresence (CS4)
+ CBWFQ for Call-Signaling (CS3)

(D) Branch Access Edge Policies:
Trust for DSCP or Trust CoS
+ Map CoS 4 → DSCP CS4
+ Map CoS 5 → DSCP EF and CoS 3 → DSCP CS3
+ (Optional) Ingress Policing
+ Queuing (CoS 4 and 5 → PQ)
+ Queuing (CoS 3 → Non-PQ)

We can see that for the most part the QoS policies deployed in the branch are reflective of the policies deployed at the campus WAN block. For example, the WAN/VPN edge QoS policies are applied to the branch router's WAN interface (to complement the WAN edge policies on the WAN/VPN aggregator's WAN edge). These are shown as points labeled C in Figure 6-6. The considerations and details of these WAN/VPN edge policies are discussed in detail throughout this chapter.

In the case of a branch PIN using dedicated/separate switch(es) and router(s), the administrator has two additional policy points to configure: the router's LAN edge (shown the point labeled B in Figure 6-6) and the switch-to-router link (shown as the point labeled A in Figure 6-6). A queuing policy on the router's LAN edge (point B) is optional, as in many cases it may be theoretically impossible to congest this interface in the WAN-to-LAN direction: this interface would likely be a GigabitEthernet interface, and as such, well above the access rate of the WAN/VPN link. If it is to be configured with a queuing policy, then a dual-LLQ policy would be recommended, such that VoIP and TelePresence are assigned to separate LLQs and Call-Signaling is protected with a CBWFQ. Such a policy would be similar to the simplified example provided in Example 6-3 (but with different bandwidth values for both VoIP and TelePresence, based on how many calls of each type were being supported over these links).

Next, the administrator would need to configure the switch-to-router links, labeled as point A. These ports are essentially serving the same roles as campus interswitch links (as previously discussed in Chapter 5, "Campus QoS Design for TelePresence"). These ports should be configured to trust DSCP and perform hardware queuing, such that CoS 4 (TelePresence) and CoS 5 (VoIP) are assigned to the strict priority hardware queue and that CoS 3 (Call-Signaling) is assigned to a non-priority queue within the platform/linecard's 1PxQyT queuing structure.

The final policy points are the branch access edges, which are shown as points labeled D in Figure 6-6. These ports should be configured with either static or conditional trust of either DSCP or CoS (as described in detail in Chapter 5, "Campus QoS Design for TelePresence"" in Access Edge Switch Port QoS Considerations).

If CoS is trusted, then the necessary CoS-to-DSCP mappings must be in place, such that CoS 4 (TelePresence) is mapped to (the default value of) DSCP CS4 (32), CoS 5 (VoIP) is mapped to (the non-default value of) DSCP EF (46), and CoS 3 (Call-Signaling) is mapped to (the default value of) DSCP CS3 (24).

An optional recommendation for the branch access edge switch port connecting to a TelePresence primary codec is to configure a policer to prevent network abuse in case of a compromise of this trusted port. This recommendation helps prevent an unknowing and/or disgruntled individual that gains physical access to the TelePresence switch port from sending rogue traffic over the network that can hijack voice or video queues and easily ruin voice or video quality. Therefore, the administrator may choose to limit the scope of damage that such network abuse may present by configuring access edge policers on TelePresence switch ports to drop (or remark to Scavenger - DSCP CS1) out-of-profile traffic originating on these ports. This is not only a Cisco recommended best practice, but is also reflected in RFC 4594, which recommends edge policing the Real-Time Interactive service class via a single-rate policer. If such a policer is configured, it is recommended to use Per-Port/Per-VLAN policers, whenever supported. In this manner, a set of policers may be applied to the Voice VLAN to ensure that voice, video, and call signaling traffic are performing within normal levels and a separate, more stringent policer can be applied to the data VLAN.

Note Access Edge policers are described in detail on a platform-by-platform basis in Chapter 2, "Campus QoS Design" of the QoS SRND at www.cisco.com/go/srnd.

Additionally, the recommended burst parameter for TelePresence policers is discussed in detail in TelePresence Branch WAN Edge LLQ Policy.

Finally, it is recommended to enable queuing on these branch access edge links in the case of congestion. While the likelihood of such an event is rare, these may occur during DoS/worm attacks; therefore, provisioning queuing policies on these links is mandatory to provide service level guarantees in **any** event.

In the case of a branch PIN using an ISR with an EtherSwitch module, the only real twist is that the administrator would configure the WAN/VPN edge policies in the router console mode, and then switch to the EtherSwitch console mode (using the **service-module gigabitEthernet** *module/number* **session** IOS command) to configure hardware QoS policies on the EtherSwitch module (which is essentially a Cisco Catalyst 3750 switch), using the Catalyst 3750 configuration recommendations provided in Chapter 5, "Campus QoS Design for TelePresence."

TelePresence Branch LAN Edge QoS Designs

The configuration details for branch LAN edge policies are identical to the platform- and linecard-specific policies used in the campus access edge, which have already been covered in detail in Chapter 5, “Campus QoS Design for TelePresence” and as such it would be redundant to again detail these designs in this chapter.

TelePresence Branch WAN Edge

The WAN edge of the branch is likely the most congested node within the network and as such requires the most attention from a QoS perspective. Let us now recap some of the considerations of the WAN edge and then delve into design detail.

TelePresence Branch WAN Edge Design Considerations

In a private WAN design, the principal decision that the administrator needs to make has already been covered in detail, namely whether to service TelePresence with a LLQ or a CBWFQ. A point to keep in mind with respect to private WAN scenarios is that additional costs are typically not incurred when provisioning additional traffic with strict priority servicing and, as such, these scenarios are generally more conducive to provisioning TelePresence in a LLQ then other VPN scenarios.

Once the LLQ versus CBWFQ decision is made, then the WAN edge policies are fairly straightforward and are a function of this decision coupled with the number of traffic classes that have been defined by the enterprise’s strategic business QoS objectives (as discussed in Chapter 4, “Quality of Service Design for TelePresence”).

TelePresence Branch WAN Edge QoS Design

To recap, LLQ provides superior levels of service for TelePresence as compared to CBWFQ, yet may entail additional costs or other constraints. Therefore, each administrator must make an informed decision as to which WAN edge queuing strategy (LLQ or CBWFQ) to employ. Both configuration options are presented in detail in the following sections.

TelePresence Branch WAN Edge LLQ Policy

If TelePresence is to be assigned to an LLQ, then in addition to adequately provisioning priority bandwidth to the LLQ, one additional design parameter needs to be calculated: the burst parameter of the implicit policer of the LLQ.

The implicit policer for the LLQ is a token-bucket algorithm policer (like any other IOS or Catalyst policer) and as such needs a burst parameter to be defined in order to police to a sub-line rate. To better understand why this is so, let us briefly recap how token-bucket policers work.

To regulate transmissions at sub-line rates, the concept of an interval must be applied. An interval is a sub-second period of time during which an application may send traffic. For example, if a policer was to limit an application to 15 Mbps of a 45 Mbps circuit, then the policer would allow the application to transmit for a total of 333 ms per second (15 / 45 Mbps) and it would drop any packets offered during the remaining 667 ms per second. Now, if the application sent all its traffic in a single burst, this could tie up the circuit for up to one-third of a second, which may cause excessive jitter and/or drops to other applications. Therefore, rather than allowing a single interval per second for an application to send traffic, it is generally more efficient to configure policers that allow for transmission over multiple sub-second intervals. The amount of traffic that an application can transmit during a sub-second interval is called the committed burst or Bc. The time interval itself is referred to as the time constant or Tc. The relationship between the burst, the interval, and the overall policing rate is:

Bc = Policing Rate * Tc

Now let us apply this theory to TelePresence traffic patterns so that we can define an optimal value for the burst parameter of the LLQ's implicit policer.

TelePresence codecs, whether operating at 720p or 1080p resolution, display 30 frames per second. Put differently, TelePresence codecs send information representing one frame every 33 ms (1 second/30 frames-per-second). We can use this information as a starting point, as it directly correlates to our interval (Tc).

Now, if TelePresence had a fixed packet size and a constant packetization rate (like VoIP), then we could simply divide the per second bandwidth requirements (shown in Table 4-1 in Chapter 4, "Quality of Service Design for TelePresence") by 30 (fps) to arrive at our burst parameter. For example, under this assumption, a CTS-3000 transmitting at 1080p-Best would need a burst parameter of 62,500 Bytes (15 Mbps / 30 fps / 8 bits).

Note However, while a fixed packet size and a constant packetization rate might make burst calculations a bit simpler, these would result in exponentially higher bandwidth requirements for TelePresence. As discussed in Chapter 4, "Quality of Service Design for TelePresence," if TelePresence were uncompressed, it would result in 1.5 Gbps of bandwidth per display, rendering TelePresence virtually undeployable—especially over wide area networks.

However, TelePresence does not have a fixed packet size, nor a constant packetization rate, as it utilizes advanced video compression techniques to achieve compression rates of over 99%, thus massively reducing the bandwidth requirements for TelePresence and rendering it more deployable, even over WANs. Notwithstanding, these high compression algorithms within TelePresence systems do have a direct impact in burst calculations for policers, such as the implicit policer within LLQ.

Therefore, to configure the policing burst such that it does not drop TelePresence traffic, we have to analyze what would be the maximum transmission (in Bytes) within a 33 ms interval—in other words, the worst-case scenario per frame of TelePresence video. In H.264 video, which TelePresence systems utilize, this worst-case scenario would be the full screen of (spatially-compressed) video, which is periodically sent, known as the Instantaneous Decoding Refresh (IDR) frame. The IDR frame is the key frame that subsequent video frames reference, sending only differential information between subsequent frames and the IDR frame, rather than the full-picture again.

Note For more information about H.264 video encoding, refer to RFC 3964 "RTP Payload Format for H.264 Video" at http://www.ietf.org/rfc/rfc3984.

The maximum IDR frame sizes observed during extensive testing of TelePresence systems (using CTS software version 1.1.0 [256D]) was 64 KB. Therefore, the LLQ burst parameter should be configured to permit up to 64 KB of burst per frame per screen. In the case of a triple-display CTS-3000 systems, we should allow for 192 KB of burst (3 * 64 KB) in the rare event of a "triple-IDR storm," where all three codecs send IDR frames simultaneously.

Note If Cisco design recommendations for TelePresence room lighting and other environmental variables are not followed, then IDR frame sizes may vary in size beyond 64 KB, which may in turn affect the network QoS policies.

However, it bears mentioning that the version of CTS software used in this phase of testing (1.1.0 [256D]) did not support an auxiliary video stream. If newer versions of CTS software are being used or if the use of an auxiliary video stream (for sharing PowerPoint presentations, etc.) is planned, then a larger value of TelePresence burst would be required. Subsequent testing has shown that a value of 256 KB is sufficient to support TelePresence with an auxiliary video stream (192 KB for worst-case primary video + 64 KB for worst-case auxiliary video). Therefore, the examples that follow utilize this higher burst value to adequately provision for the use of TelePresence with an auxiliary video stream; if, on the other hand, such use is not planned, then a value of 192 KB is sufficient for TelePresence burst provisioning.

Now let us put this all together into a configuration. To quickly recap, the full syntax of the LLQ command in Cisco IOS is:

priority {*bandwidth-kbps* | **percent** *percentage*} [*burst*]

As can be seen, the burst parameter is an optional parameter that can be explicitly defined as part of the **priority** command. If the burst is not explicitly defined, then it defaults to a value computed as 200 ms of traffic at the configured LLQ bandwidth rate. However, it is important to note that the burst value is expressed in Bytes (not bits).

For example, if **priority 1000** was configured for a class, then the default burst parameter would be set to 25000 Bytes (1000 kbps * 200 ms / 8 bits). This value would not appear in the configuration, but could be verified with a **show policy map interface** verification command.

Let us look at the worst-case burst for a CTS-1000 system. Applying the IDR as the worst-case burst scenario for TelePresence primary video (at 64 KB) coupled with an allowance of auxiliary video bursting of the same amount (64 KB), the configuration to provision a branch WAN edge queuing policy that provisions a TelePresence CTS-1000 system running at 1080p-Best (with the optional support of an auxiliary video stream) to a LLQ with an optimal burst parameter (of 128 KB) is shown in Example 6-4.

Example 6-4 Dual-LLQ Branch WAN Edge Policy for VoIP and TelePresence (CTS-1000 at 1080p-Best with Auxiliary Video)

```
policy-map WAN-EDGE
 class VOIP
  priority percent 10         ! LLQ for VoIP (example amount of BW)
 class TELEPRESENCE
  priority 5500 128000        ! LLQ for CTS-1000 (1080p-Best + aux video)
 class DATA
  ...
```

Likewise, the configuration to provision a branch WAN Edge queuing policy that provisions a TelePresence CTS-3000 system running at 1080p-Best (with the optional support of an auxiliary video stream) to a LLQ with an optimal burst parameter (of 256 KB) is shown in Example 6-5.

Example 6-5 Dual-LLQ Branch WAN Edge Policy for VoIP and TelePresence (CTS-3000 at 1080p-Best with Auxiliary Video)

```
policy-map WAN-EDGE
 class VOIP
  priority percent 10         ! LLQ for VoIP (example amount of BW)
 class TELEPRESENCE
  priority 15000 256000       ! LLQ for CTS-3000 (1080p-Best + aux video)
 class DATA
  ...
```

These configurations can be verified with the following command:

- **show policy-map interface**

TelePresence Branch WAN Edge CBWFQ Policy

If, on the other hand, TelePresence is to be assigned to a CBWFQ, then in addition to adequately provisioning guaranteed bandwidth to the CBWFQ, one additional design parameter needs to be considered, the length of the CBWFQ.

By default, Class-Based Weighted Fair Queues are 64 packets deep. Extensive testing has shown that this default queue-depth has at times resulted in tail-drops when provisioned to protect TelePresence flows. Therefore, on most interfaces it is recommended to increase the default queue-depth for the TelePresence queue to 128 packets, using the **queue-limit 128** command in conjunction with the CBWFQ **bandwidth** command.

An example policy provisioning a TelePresence CTS-3000 system running at 1080p-Best (with the optional support of an auxiliary video stream) to a CBWFQ, with an extended queue-depth to 128 packets, is shown in Example 6-6.

Example 6-6 CBWFQ Branch WAN Edge Policy for TelePresence (CTS-3000 at 1080p-Best with Auxiliary Video)

```
policy-map WAN-EDGE
 class VOIP
  priority percent 10         ! LLQ for VoIP (example amount of BW)
 class TELEPRESENCE
  bandwidth 15000             ! CBWFQ for CTS-3000 (1080p-Best + aux video)
  queue-limit 128             ! Extended queue-limit for TelePresence CBWFQ
 class DATA
  ...
```

This configuration can be verified with the following command:

- **show policy-map interface**

TelePresence Branch T3/DS3 WAN Edge Design

When configuring a WAN edge policy for TelePresence, there are a couple of additional considerations that need to be taken into account when using T3 interfaces, namely, adjusting the hold-queue size (if needed) to accommodate all LLQ/CBWFQs and tuning the Tx-Ring to minimize TelePresence jitter on converged links.

The total number of buffers that the IOS software allocates for queuing per interface (regardless of whether the interface is configured with FIFO, LLQ, or CBWFQ) is called the output queue or hold-queue. The size of the output queue and can be adjusted with the **hold-queue** interface command to a value between 0 and 4096 packets; the default output queue size of a T3 serial interface is 1000 packets.

Normally the default hold-queue size is sufficient for a T3 interface. Consider our worst-case example, where we have a 12-class RFC 4594-based QoS policy and let us choose the option with TelePresence assigned to a CBWFQ. Besides TelePresence, there are 10 CBWFQs, each a default queue-depth of 64 packets, for an output queue depth of, so far, 640 packets. Additionally, there is the 128 packet extended queue-depth for the TelePresence CBWFQ, bringing our running total output queue depth to 768 packets which, even factoring a moderate allowance for LLQ queue depth, is well below our default value of 1000 packets for this T3 interface.

However, should the administrator—for whatever reason—require expanding the queue depths of each CBWFQ to 128, then the output queue depth requirement would be at least (11 * 128) 1408 packets, not even factoring a moderate allowance for the LLQ. In such a scenario, LLQ traffic could be impacted if the output queue size was not expanded accordingly. For instance, in such a case, the network administrator could increase the size of the output queue to 1500 packets by using the **hold-queue 1500** interface command.

Earlier in this chapter we introduced the Tx-Ring. To quickly recap, the Tx-Ring represents the size of the final output buffer (a FIFO queue) that maximizes physical link bandwidth utilization by matching the outbound packet rate on the router with the physical interface rate. The Tx-Ring also serves to indicate interface congestion to the IOS software. Prior to interface congestion, packets are sent on a FIFO basis to the interface via the Tx-Ring. However, when the Tx-Ring fills to its queue-depth/limit, then it signals to the IOS software to engage any LLQ/CBWFQ policies that have been attached to the interface. Subsequent packets are then queued within IOS according to these LLQ/CBWFQ policies, dequeued into the Tx-Ring, and then sent out the interface in a FIFO manner. These operations are illustrated in Figure 6-2, Figure 6-3, and Figure 6-4.

The Tx-Ring can be configured on certain platforms, such as the Cisco PA-T3+ port adapter interface, with the **tx-ring-limit** interface command. The value of the **tx-ring-limit** number can be from 1 to 32,767 packets. The default for serial interfaces on the PA-T3+ is 64 packets.

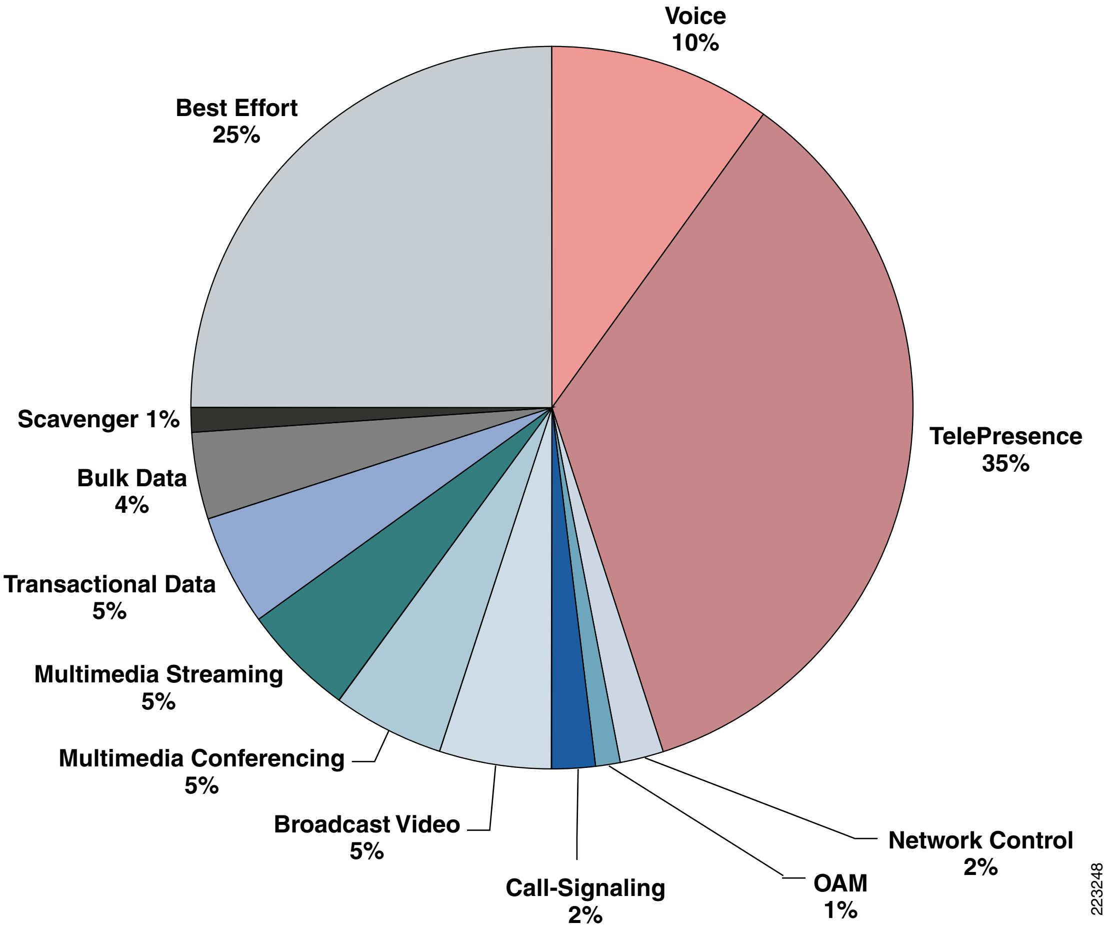
During testing it was observed that the default tx-ring-limit limit of 64 packets was shown to cause somewhat higher jitter values to TelePresence traffic during fully-congested scenarios. The reason for this is the bursty nature of TelePresence traffic. Even though TelePresence traffic is prioritized when LLQ/CBWFQ policies are active, if there are no TelePresence packets to send, the FIFO Tx-Ring is filled with other traffic. When a new TelePresence packet arrives, even if it gets priority treatment from the Layer 3 LLQ/CBWFQ queuing system, the packet are dequeued into the FIFO Tx-Ring when space is available. However, with the default settings, there can be as many as 63 (non-TelePresence) packets in the Tx-Ring in front of that TelePresence packet. In such a worst-case scenario it would take as long as 17 ms to transmit these non-TelePresence packets out of the T3 interface. This 17 ms of instantaneous delay (i.e., jitter) exceeds the jitter target for TelePresence.

Additionally, a lower Tx-Ring results in the IOS software engaging congestion management policies sooner and more often, resulting in lower overall jitter values for priority traffic, such as TelePresence. On the other hand, setting the value of the Tx-Ring too low may result in significantly higher CPU utilization rates, as the processor is being continually interrupted to engage queuing policies, even when congestion rates are just momentary bursts and not sustained rates. Thus when tuning the Tx-Ring, a trade-off setting is required such that jitter is minimized, but not at the expense of excessive CPU ultilization rates. Therefore, extensive testing has shown that setting the Tx-Ring to a value of 10 packets is optimal on converged T3 inks supporting TelePresence and other applications (such as voice, data, and other video applications). This can be achieved by using the **tx-ring-limit 10** interface command.

Note As explained above, tuning the Tx-Ring to value of 10 is only required on converged links that support additional applications beyond TelePresence. On T3 circuits that are dedicated to TelePresence, lowering the Tx-Ring to a non-default value is not required; in fact, such tuning can actually deteriorate the quality of TelePresence calls on such dedicated T3 circuits. It is important to keep in mind that in the case of dedicated circuits, it is not other applications that could potentially fill the Tx-Ring, but rather other TelePresence flows. Furthermore, when properly provisioned, dedicated links should not generate sustained congestion scenarios.

Now let us put this all together into a full example. In this 12-class RFC 4594-based case-study example, it was decided to service TelePresence traffic over the branch T3 WAN edge in a CBWFQ, as provisioning both VoIP and TelePresence in a dual-LLQ design would, in this case, require 45% of priority queuing, which would cause excessive variations in application response times to the other 10 application classes. The WAN edge bandwidth allocations for this case-study example are shown in Figure 6-7.

Figure 6-7 Case Study Example Bandwidth Allocations of a RFC 4594-Based LLQ/CBWFQ Policy Over a Branch T3 WAN Edge



The corresponding configuration for this case study example is shown in Example 6-7.

Example 6-7 Case Study Example Configuration of a RFC 4594-Based LLQ/CBWFQ Policy (with TelePresence in a CBWFQ) Over a Branch T3 WAN Edge

```
!
class-map match-all VOICE
  match dscp ef                          ! Voice marking
class-map match-all TELEPRESENCE
  match dscp cs4                         ! TelePresence marking
class-map match-all NETWORK-CONTROL
  match dscp cs6                         ! IP Routing marking
class-map match-all OAM                  ! Operations / Administration
  match dscp cs2                         ! and Management marking
class-map match-all CALL-SIGNALING
  match dscp cs3                         ! Call-Signaling (Cisco)
class-map match-all BROADCAST-VIDEO
  match dscp cs5                         ! Broadcast Video (Cisco)
class-map match-all MULTIMEDIA-CONFERENCING
  match dscp af41 af42 af43              ! Video-Conferencing marking
class-map match-all MULTIMEDIA-STREAMING
  match dscp af31 af32 af33              ! Streaming-Video marking
class-map match-all TRANSACTIONAL-DATA
  match dscp af21 af22 af23              ! Transactional Data markings
```

```
class-map match-all BULK-DATA
  match dscp af11 af12 af13                  ! Bulk-Data markings
class-map match-all SCAVENGER
  match dscp cs1                             ! Scavenger marking
!


!
policy-map WAN-EDGE-T3
 class VOICE
  priority percent 10                        ! LLQ for VoIP
class TELEPRESENCE
  bandwidth percent 35                       ! CBWFQ for TP (CTS-3000)
  queue-limit 128                            ! Expanded Queue-Limit for TP
class NETWORK-CONTROL
  bandwidth percent 2                        ! CBWFQ for Routing
class OAM
  bandwidth percent 1                        ! CBWFQ for Ops/Admin/Mgmt
class CALL-SIGNALING
  bandwidth percent 2                        ! CBWFQ for Call-Signaling
class BROADCAST-VIDEO
  bandwidth percent 5                        ! CBWFQ for Broadcast Video
class MULTIMEDIA-CONFERENCING
  bandwidth percent 5                        ! CBWFQ for IP/VC
  random-detect dscp-based                   ! DSCP-WRED for IP/VC
class MULTIMEDIA-STREAMING
  bandwidth percent 5                        ! CBWFQ for Streaming-Video
  random-detect dscp-based                   ! DSCP-WRED for Stream-Video
class TRANSACTIONAL-DATA
  bandwidth percent 5                        ! CBWFQ for Trans-Data
  random-detect dscp-based                   ! DSCP-WRED for Trans-Data
class BULK-DATA
 bandwidth percent 4                         ! CBWFQ for Bulk Data
  random-detect dscp-based                   ! DSCP-WRED for Bulk Data
class SCAVENGER
  bandwidth percent 1                        ! Minimum CBWFQ for Scavenger
class class-default
  bandwidth percent 25                       ! CBWFQ for Best Effort
  random-detect                              ! WRED for Best Effort
!
…
!
interface Serial6/0
 description BRANCH-TO-CAMPUS-T3
 ip address 192.168.2.9 255.255.255.252
 tx-ring-limit 10                            ! Tuned T3 Tx-Ring
 dsu bandwidth 44210
 framing c-bit
 cablelength 10
 serial restart-delay 0
 max-reserved-bandwidth 100                  ! LLQ/CBWFQ BW Override
 service-policy output WAN-EDGE-T3           ! Attaches policy to T3 int
!
```

Note Since this policy supports a less-than Best Effort Scavenger-class, it requires an explicit CBWFQ to be configured on class-default (the Best Effort class); otherwise, the queuing algorithm robs bandwidth from class-default to service Scavenger traffic. Additionally, when class-default is configured with an explicit **bandwidth** command, then the **max-reserved-bandwidth** interface command must also be configured on the outgoing interface. Additional details on this behavior can be found in the QoS SRND at www.cisco.com/go/srnd on pages 3-8 and 3-9.

Optionally, if the network administrator chooses to use LLQ instead of CBWFQ, then the only change to the above policy would be to the TELEPRESENCE class within the WAN-EDGE-T3 policy-map, as shown in Example 6-8.

Example 6-8 Policy Amendment to Example 6-7 to Provision TelePresence in a Dual-LLQ Policy Over a T3 Branch WAN Edge

```
!
policy-map WAN-EDGE-T3
 class VOICE
  priority percent 10                   ! LLQ for VoIP
class TELEPRESENCE
  priority percent 35 256000            ! LLQ for CTS-3000 (1080p-Best + aux video)
class NETWORK-CONTROL
…
```

These configurations can be verified with the following commands:

- **show interface**
- **show policy-map interface**
- **show controllers Serial** *module/interface* **| include tx_limited**

TelePresence Branch OC3-POS WAN Edge Design

When configuring a WAN edge policy for TelePresence, there are a couple of additional considerations that need to be taken into account when using OC3-POS interfaces, such as the Cisco 7600 SPA-2XOC3-POS. Both of these considerations relate to Low-Latency Queuing:

- There is a 35% hard limit to the amount of traffic that can be configured with priority queuing.
- There is different configuration syntax for enabling LLQ on these interfaces.

Let us discuss these considerations in more detail.

The first consideration is fairly straightforward: on these OC3-POS interfaces, there is a hard limit of 35% for the sum of all traffic that can be configured with LLQ. This means that either a single LLQ class can be configured with a maximum of 54.25 Mbps or the sum of all LLQ classes can be configured for a combined maximum of 54.25 Mbps. This hard-limit, incidentally, is quite consistent with Cisco's "33% LLQ Rule."

The second consideration has to do with a change in syntax for configuration of LLQ on these OC3-POS interfaces. The configuration syntax for strict priority queuing on an OC3 POS interface is such the **priority** command does not include a bandwidth parameter, either as an absolute value (defined in kbps) or as a percentage of the link's bandwidth. That being said, there is correspondingly no implicit policer within the LLQ **priority** command, but rather an explicit policer must be configured on the policy-map class and then the **priority** command can be applied to the class. This difference is not limited to syntax only, but also affects behavior, as an implicit policer only engages when the LLQ is active (i.e., during periods of congestion), but an explicit policer, such as required for a LLQ class on an OC3-POS interface, is always on.

Note The always-on nature of explicit policers is advantageous from an Admission Control perspective. For example, without a comprehensive, network-aware Call Admission Control system in place, there would be no way to always enforce limits on TelePresence traffic without explicit policers (remember, implicit policers, like those included within LLQ, are only active during congestion scenarios). Admission Control considerations and designs are discussed in more detail in Chapter 8, "Capacity Planning and Call Admission Control."

The configured explicit LLQ policer may be either a single-rate or a dual-rate policer. When applied to TelePresence traffic, only a single-rate policer is relevant (as we are not interested in marking down excess TelePresence traffic, which we could do with two levels of granularity via a dual-rate policer). Additionally, testing has shown that using a dual-rate policer offers no performance advantages whatsoever; therefore it is recommended to configure a single-rate policer on the TelePresence LLQ class.

As with an implicit policer, a committed burst parameter is required when defining an explicit policer. As discussed in TelePresence Branch WAN Edge LLQ Policy, the recommended value for TelePresence committed burst for a CTS-3000 system running 1080p-Best (with optional auxiliary video support) is 256 KB.

Reflecting the foregoing points, the configuration syntax for creating a single-rate explicit policer and applying it to a TelePresence LLQ class (for a CTS-3000 system running at 1080p-Best with auxiliary video) LLQ is shown in Example 6-9.

Example 6-9 TelePresence LLQ Policy Over a OC3-POS Branch WAN Edge

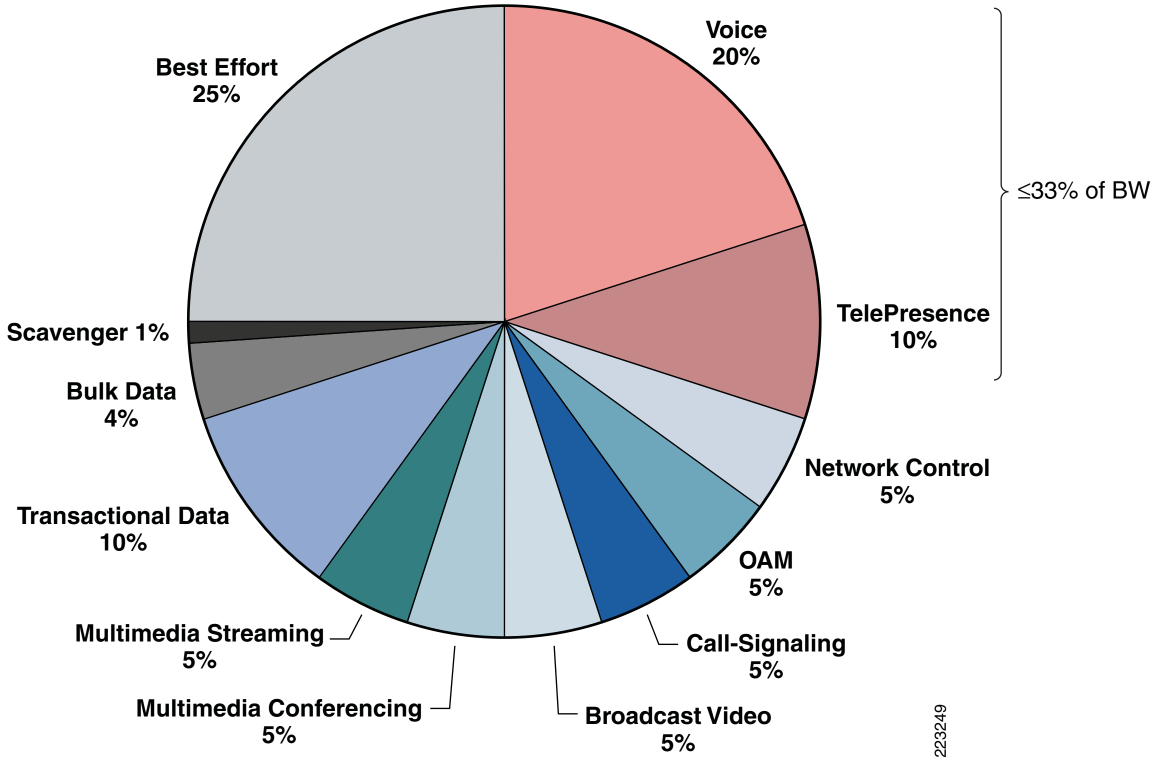
```
!
policy-map WAN-EDGE
 class TELEPRESENCE
  police cir 15000000                     ! TP is policed to 15 Mbps
    bc 256000                             ! Bc is 256 KB
    conform-action transmit               ! Conforming action --> transmit
    exceed-action drop                    ! Single-Rate Policing action
  priority                                ! LLQ command for OC3-POS
!
```

This configuration can be verified with the following command:

- **show policy-map interface**

Now let us again put this all together into a full example. In this 12-class RFC 4594-based case-study example, it has been decided to service TelePresence traffic over the branch OC3-POS WAN edge in a dual-LLQ design, along with voice. The WAN edge bandwidth allocations for this case-study example are shown in Figure 6-8.

Figure 6-8 Case Study Example Bandwidth Allocations of a RFC 4594-Based LLQ/CBWFQ Policy Over a Branch OC3-POS WAN Edge



The corresponding configuration for this second case study example is shown in Example 6-10 (the class-maps are not repeated, as these do not change).

Example 6-10 Case Study Example Configuration of a RFC 4594-Based LLQ/CBWFQ Policy (with TelePresence in a Dual-LLQ) Over a Branch OC3-POS WAN Edge

```
!
policy-map WAN-EDGE-OC3-POS
 class VOICE
  police cir 31000000                 ! Voice is policed to 31 Mbps (20%)
    bc 15500                          ! Bc is 15.5 KB
    conform-action transmit           ! Conforming action --> transmit
    exceed-action drop                ! Single-Rate Policing action
  priority                            ! LLQ command for OC3-POS
 class TELEPRESENCE
  police cir 15000000                 ! TP is policed to 15 Mbps
    bc 256000                         ! Bc is 256 KB
    conform-action transmit           ! Conforming action --> transmit
    exceed-action drop                ! Single-Rate Policing action
  priority                            ! LLQ command for OC3-POS
class NETWORK-CONTROL
  bandwidth percent 5                 ! CBWFQ for Routing
class OAM
  bandwidth percent 5                 ! CBWFQ for Network Management
class CALL-SIGNALING
  bandwidth percent 5                 ! CBWFQ for Call-Signaling
class BROADCAST-VIDEO
  bandwidth percent 5                 ! CBWFQ for Broadcast Video
class MULTIMEDIA-CONFERENCING
  bandwidth percent 5                 ! CBWFQ Video-Conferencing
  random-detect dscp-based               ! DSCP-WRED for Video-Conferencing
class MULTIMEDIA-STREAMING
  bandwidth percent 5                    ! CBWFQ for Streaming-Video
  random-detect dscp-based               ! DSCP-WRED for Streaming-Video
class TRANSACTIONAL-DATA
  bandwidth percent 10                   ! CBWFQ for Transactional Data
  random-detect dscp-based               ! DSCP-WRED for Transactional Data
class BULK-DATA
 bandwidth percent 4                     ! CBWFQ for Bulk Data
  random-detect dscp-based               ! DSCP-WRED for Bulk Data
class SCAVENGER
  bandwidth percent 1                    ! Minimum CBWFQ for Scavenger
class class-default
  bandwidth percent 25                   ! CBWFQ for Best Effort
  random-detect! WRED for Best Effort
!
…
interface POS3/0/1
 description BRANCH-TO-CAMPUS-OC3-POS
 ip address 192.168.5.1 255.255.255.252
 clock source internal
 service-policy output WAN-EDGE-OC3-POS  ! Attaches policy to OC3-POS
!
```

Note No Tx-Ring tuning is required on the OC3-POS link; neither is a **max-reserved-bandwidth 100** interface command required.

Optionally, if the network administrator chooses to use CBWFQ instead of LLQ for TelePresence, then the only change to the above policy would be to the TELEPRESENCE class within the WAN-EDGE-OC3-POS policy-map, as shown in Example 6-11.

Example 6-11 Policy Amendment to Example 6-10 to Provision TelePresence in a CBWFQ Over an OC3-POS Branch WAN Edge

```
!
policy-map WAN-EDGE-OC3-POS
 class VOICE
  police cir 31000000                    ! Voice is policed to 31 Mbps (20%)
   bc 15500                              ! Bc is 15.5 KB
   conform-action transmit               ! Conforming action --> transmit
   exceed-action drop                    ! Single-Rate Policing action
  priority                               ! LLQ command for OC3-POS
 class TELEPRESENCE
  bandwidth percent 10                   ! CBWFQ for TelePresence
 class NETWORK-CONTROL
…
```

Note Testing has shown that extending the TelePresence CBWFQ queue-limit beyond the default value of 64 packets is not required on OC3-POS interfaces because of the extremely fast serialization rate—relative to TelePresence transmission rates—of these interfaces.

These configurations can be verified with the following command:

- **show policy-map interface**

TelePresence Branch IPSec VPN Edge

In the initial releases of Cisco TelePresence software, native encryption within the codecs was not supported. Nonetheless, for certain enterprises, encryption is a business requirement for all IP communications. This business requirement can be achieved by performing IPSec encryption and decryption within the network infrastructure, such as at the branch WAN/VPN edges over a private WAN or an MPLS VPN infrastructure. However, it is good to review some design considerations relating to IPSec and QoS interaction prior to examining the configuration details required for these deployments.

Note Cisco does not recommend deploying TelePresence over the Internet—with or without IPSec encryption—as critical service level parameters, such as latency, jitter, and loss, cannot be guaranteed over the Internet. These IPSec designs for TelePresence are intended for use over private WAN and/or MPLS VPN scenarios.

TelePresence Branch IPSec VPN Edge Considerations

One of the first considerations is that IPSec adds network overhead to the packets. How much overhead depends on the encryption and tunneling options defined within the security associations. For example, a typical IPSec configuration uses IPSec Tunnel Mode with **esp-3des** and **esp-md5-hmac**, which results in an overhead of 56 bytes, accounted for as shown in Table 6-1.

Table 6-1 IPSec Network Overhead Breakdown

Component	Overhead in Bytes
IPSec header (bytes)	20
ESP Header (bytes SPI)	4
ESP Header (bytes Sequence)	4
IOS ESP-DES/3DES (bytes IV)	8
ESP-DES/3DES 64-bit) (bytes pad)	6
ESP Trailer (byte PAD length)	1
ESP Trailer (byte Next Header)	1
ESP MD5 96 digest (bytes)	12
Total IPSec Overhead	56

This being the case, since the average packet size for TelePresence is around 1200 Bytes, encryption overhead is typically <5%. Table 6-2 shows a detailed breakdown of the respective encrypted bandwidth requirements for all TelePresence motion-handling and resolution options.

Table 6-2 TelePresence Bandwidth Requirements with IPSec Encryption

Motion Handling	**Best**	**Better**	**Good**	**Best**	**Better**	**Good**
Resolution	**1080p**	**1080p**	**1080p**	**720p**	**720p**	**720p**
CTS 1000						
Max with IPSec overhead (Kbps)	5,792	5,194	4,596	4,596	3,400	2,204
CTS 3000						
Max with IPSec overhead (Kbps)	15,360	13,566	11,772	11,772	8,184	4,596

Another important consideration is the interaction of IPSec and QoS, particularly with respect to Anti-Replay. In order to understand this interaction implication, it is beneficial to briefly recap the purpose and function of IPSec Anti-Replay.

IPSec offers inherent message-integrity mechanisms to provide a means to identify whether an individual packet is being replayed by an interceptor or hacker. This concept is called connectionless integrity. IPSec also provides for partial sequence integrity, preventing the arrival of duplicate packets.

Note Anti-Replay concepts are outlined in RFC 2401, “Security Architecture for the Internet Protocol” at www.ietf.org/rfc/rfc2401.

When ESP authentication is configured in an IPSec transform set, for each security association, the receiving IPSec peer verifies that packets are received only once. Because two IPSec peers can send millions of packets, a 64-packet sliding window is implemented to bind the amount of memory required to tally the receipt of a peer’s packets. Packets can arrive out of order, but they must be received within the scope of the window to be accepted. If they arrive too late (outside the window), they are dropped.

The operation of the Anti-Replay window protocol is as follows:

1. The sender assigns a unique sequence number (per security association) to encrypted packets.
2. The receiver maintains a 64-packet sliding window, the right edge of which includes the highest sequence number received.
3. The receiver evaluates the received packet’s sequence number:
   - If a received packet’s sequence number falls within the window and was not received previously, the packet is accepted and marked as received.
   - If the received packet’s sequence number falls within the window and previously was received, the packet is dropped and the replay error counter is incremented.
   - If the received packet’s sequence number is greater than the highest sequence in the window, the packet is accepted and marked as received, and the sliding window is moved “to the right.”
   - If the received packet’s sequence number is less than the lowest sequence in the window, the packet is dropped and the replay error counter is incremented.

While Anti-Replay is useful in validating message integrity, in a converged IPSec VPN implementation with QoS enabled, lower-priority packets are often delayed so that higher-priority packets receive preferential treatment, which has the unfortunate side effect of sufficiently reordering packets so they are out of sequence from an IPSec Anti-Replay perspective. Therefore, there is a concern that through the normal QoS prioritization process, the receiver might drop packets as Anti-Replay errors, when, in fact, they are legitimately sent or received packets.

Traffic assigned to CBWFQ classes is much more sensitive to Anti-Replay than traffic assigned to a LLQ. This is because LLQ traffic is always sent in order, with strict priority; but CBWFQ traffic may be delayed by other CBWFQ flows and be sent in gaps exceeding the receiver's 64-packet sliding Anti-Replay window. Furthermore, by default, each CBWFQ class receives a queue with a length of 64 packets. Meanwhile, the receiving IPSec peer has a single 64-packet Anti-Replay window (per IPSec Security Association) with which to process packets from **all** LLQ and CBWFQ bandwidth classes. Therefore, a mismatch is created between the queue depths on the sender's output interface (multiple queues of 64 packets each) as compared to the width of the receiver's Anti-Replay window (a single sliding window of 64 packets per SA). As more bandwidth classes are defined in the sender's policy map, this mismatch increases. This is an inefficient use of expensive WAN/VPN bandwidth, as many packets are transmitted only to be dropped before decryption.

Cisco IOS allows the Anti-Replay window to be expanded (up to a maximum value of 1024 packets) or, alternatively, to be disabled entirely.

During testing it was observed that when TelePresence was provisioned within a dual-LLQ design, with a default-sized Anti-Replay window (of 64 packets), Anti-Relay errors did not affect either TelePresence or voice flows; however, there were significant Anti-Replay errors occurring on CBWFQ classes, inline with the behavior described above. These errors were reduced as the Anti-Replay window was enlarged, to the maximum of 1024 packets, yet were only eliminated altogether when Anti-Replay was disabled.

Additionally, when TelePresence was provisioned with a CBWFQ, with a default-sized Anti-Replay window, significant replay errors occurred on TelePresence flows, resulting in unusable call-quality. Replay errors were still noticed even when the Anti-Replay sliding window was set to the maximum of 1024 packets and were only eliminated when the Anti-Replay feature was disabled.

Therefore, when encrypting TelePresence over the private WAN and/or MPLS VPN, it is recommended to assign TelePresence to a LLQ and/or to disable Anti-Replay.

TelePresence Branch IPSec VPN Edge QoS Design

As discussed in the previous section, it is not recommended to deploy TelePresence over IPSec VPNs over the Internet, due to the lack of service level guarantees of the Internet in general. But rather, if required due to business reasons, IPSec encryption via the network infrastructure provides an additional security overlay to private WANs or MPLS VPNs for TelePresence calls.

If TelePresence is to be deployed over IPSec VPNs over private WANs or MPLS VPNs, then three additional points should be kept in mind:

- Provision the additional bandwidth required by encryption, according to Table 6-2.
- Provision TelePresence traffic into a LLQ (or a dual-LLQ, along with voice).
- Either maximize or disable Anti-Replay.

The first bullet is straightforward and the second bullet has already been covered (see Example 6-5 and Example 6-9). The third bullet, however, requires some new commands that we have not yet detailed.

To minimize Anti-Replay errors or to eliminate them completely, Cisco IOS introduced a pair of commands in 12.3(14)T that could either enlarge the Anti-Relay window (to a maximum of 1024 packets) or disable it entirely, the **set security-association replay window-size** and the **set security-association replay disable** commands, respectively.

Let us consider two examples to illustrate these options. In Example 6-12, a dual-LLQ QoS policy (with modified priority bandwidth for the TelePresence class) is applied in conjunction with a native IPSec tunnel (including a maximized Anti-Replay window) to a branch T3 WAN/VPN edge interface.

Example 6-12 Dual-LLQ Design with Native IPSec Tunnel and Maximized Anti-Replay Window

```
!
policy-map WAN-EDGE-IPSEC
 class VOIP
  priority percent 10             ! LLQ for VoIP (example amount of BW)
 class TELEPRESENCE
  priority 15360 256000           ! LLQ for CTS-3000 with IPSec (1080p-Best + aux video)
 class DATA
  ...
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key CTS address 192.168.2.10
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set CTS-IPSEC esp-3des esp-md5-hmac
!
crypto map CMAP local-address Serial6/0
crypto map CMAP 10 ipsec-isakmp
 set peer 192.168.2.10
 set security-association replay window-size 1024! Maximizes A/R
 set transform-set CTS-IPSEC
 match address BRANCH-TO-CAMPUS
 qos pre-classify
!
!
interface Serial6/0
 description BRANCH-TO-CAMPUS-T3
 ip address 192.168.2.9 255.255.255.252
 tx-ring-limit 10                                ! Tunes T3 Tx-Ring
 dsu bandwidth 44210
 framing c-bit
 cablelength 10
 serial restart-delay 0
 crypto map CMAP
 max-reserved-bandwidth 100                      ! LLQ/CBWFQ BW Override
 service-policy output WAN-EDGE-IPSEC            ! Attaches Dual-LLQ Policy
!
!
ip access-list extended BRANCH-TO-CAMPUS
 permit ip 10.16.0.0 0.0.255.255 10.17.0.0 0.0.255.255
!
```

In Example 6-13, a dual-LLQ QoS policy (with modified priority bandwidth for the TelePresence class) is applied in conjunction with a GRE IPSec tunnel (with a disabled Anti-Replay window) to a branch T3 WAN/VPN edge interface.

Example 6-13 Dual-LLQ Design with GRE IPSec Tunnel and Disabled Anti-Replay Window

```
!
policy-map WAN-EDGE-IPSEC
 class VOIP
  priority percent 10                        ! LLQ for VoIP (example amount of BW)
 class TELEPRESENCE
  priority 15360 256000                      ! LLQ for CTS-3000 with IPSec
 class DATA
  ...
!
```

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key telep address 192.168.2.10
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set CTS-IPSEC esp-3des esp-md5-hmac
!
crypto map CMAP local-address Serial6/0
crypto map CMAP 10 ipsec-isakmp
 set peer 192.168.2.10
 set security-association replay disable ! Disables Anti-Replay
 set transform-set CTS-IPSEC
 match address BRANCH-TO-CAMPUS
 qos pre-classify
!
!
interface Tunnel0
 ip address 10.18.1.1 255.255.255.252
 tunnel source 192.168.2.9
 tunnel destination 192.168.2.10
!
interface Serial6/0
 description BRANCH-TO-CAMPUS-T3
 ip address 192.168.2.9 255.255.255.252
 tx-ring-limit 10                        ! Tunes T3 Tx-Ring
 dsu bandwidth 44210
 framing c-bit
 cablelength 10
 serial restart-delay 0
 crypto map CMAP
 max-reserved-bandwidth 100              ! LLQ/CBWFQ BW Override
 service-policy output WAN-EDGE-IPSEC    ! Attaches Dual-LLQ Policy
!
!
ip access-list extended BRANCH-TO-CAMPUS
 permit gre host 192.168.2.9 host 192.168.2.10
!
```

These configurations can be verified with the following command:

- **show policy-map interface**
- **show crypto engine accelerator statistic** *module*

TelePresence Branch MPLS VPN

MPLS VPN architectures are comprised of customer edge (CE) routers, provider-edge (PE) routers, and provider (P) routers. MPLS VPNs provide fully-meshed Layer 3 virtual WAN services to all interconnected CE routers. Let us discuss some of the critical QoS design considerations pertaining to MPLS VPNs and then translate these considerations into configuration examples.

Note MPLS VPN architectures are defined in RFC 2547 “BGP/MPLS VPNs” at www.ietf.org/rfc/rfc2547.

TelePresence Branch MPLS VPN Edge Considerations

The advent of MPLS VPN service offerings that inherently offer full-mesh connectivity has shifted the QoS administration paradigm. Under traditional hub-and-spoke Layer 2 WAN designs, the enterprise network administrator controlled all the QoS policies by configuring these on the WAN aggregator routers' and branch routers' WAN edges, as previously discussed. However, under a full-mesh topology, it is the service provider's QoS policies on the PE edges routers that ultimately determine how traffic enters a branch and these SP policies may be different from the enterprise's policies on the (unmanaged) CE edges.

Therefore, to ensure end-to-end service levels, enterprise administrators must choose service providers that offer compatible policies to meet their business objectives; furthermore, enterprises must fully understand the SP's QoS policies and map their policies to match in a complementary manner.

First, let us briefly discuss service provider selection based on SLA requirements. As brought out in Chapter 4, "Quality of Service Design for TelePresence," the bandwidth and service level requirements of TelePresence (including latency, jitter, and loss requirements) are very high—some are even higher than the SLAs of VoIP. Therefore, to achieve these tight end-to-end SLAs, it is mandatory that the SP be able to guarantee a subset of these SLAs from PE-edge-to-PE-edge.

In the past, to facilitate VoIP deployments over MPLS VPNs, Cisco initiated a Cisco Powered Network (CPN) "IP Multiservice Service Provider" designation that required SPs to offer (independently-verified) PE-to-PE SLA guarantees that would enable enterprise customers to fulfill the end-to-end SLA requirements of VoIP. This initiative was well received by both enterprise customers and SPs, as enterprise customers did not have to do as much research and testing to validate potential SP networks to support their VoIP deployments and SPs, in turn, received a competitive advantage in marketing their networks that could meet VoIP SLAs.

Subsequently, this initiative has similarly been applied to TelePresence. Cisco is in the process of validating various service providers that can meet a subset of the stringent SLAs required by TelePresence, so that enterprise customers can provide end-to-end SLA guarantees for TelePresence.

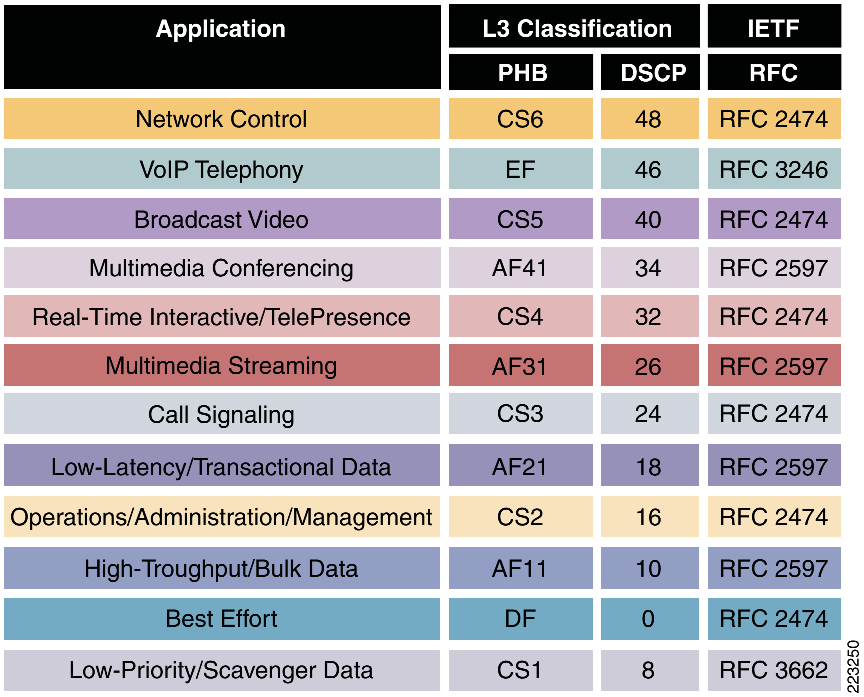
Second, let us turn our attention to enterprise-to-service provider mapping, which usually involves three main points to consider:

1. The number of enterprise traffic classes versus the number of service provider traffic classes; and if collapsing is required, how to perform this efficiently.
2. Marking or remarking requirements on CE egress to gain admission to the desired SP traffic class; and (optional) remarking requirements on CE ingress to restore enterprise traffic markings for provisioning, accounting, or management purposes.
3. Non-traditional WAN access media, such as sub-line-rate Ethernet access, and the QoS implications these pose.

Let us discuss each of these in turn, beginning with the number of traffic classes.

The number of traffic classes within an enterprise network is a function of its business objectives (as discussed in detail in Chapter 1 of the QoS SRND at www.cisco.com/go/srnd). As an informational guide, RFC 4594 "Configuration Guidelines for DiffServ Service Classes" (www.ietf.org/rfc/rfc4594), outlines up to 12 classes of traffic that may be present within an enterprise. This is not to say that it is mandatory for enterprises to have 12 traffic classes today; but rather that the potential exists in enterprise networks for up to 12 traffic classes and—given the trends in emerging new applications and evolving business objectives—even if enterprises are not deploying 12 class models today, they may need to in the near future. For configuration and testing purposes, we can use this 12-class enterprise model as a worst-case scenario, providing maximum disparity between the number of enterprise traffic classes versus the number of service provider traffic classes. The Cisco-modified 12-class RFC 4594 enterprise model is shown in Figure 6-9.

Figure 6-9 Cisco-Adapted 12-Class RFC 4594-based Enterprise Classification and Marking Model

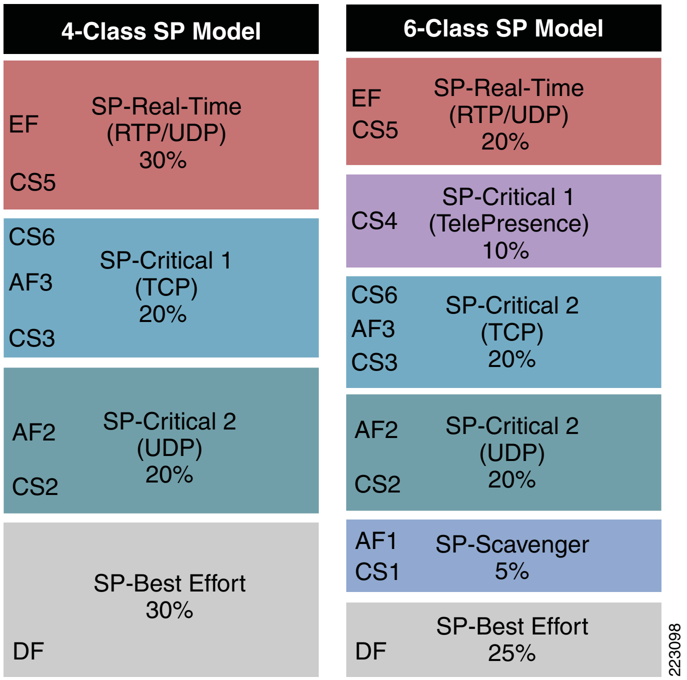


Application	L3 Classification		IETF
	PHB	DSCP	RFC
Network Control	CS6	48	RFC 2474
VoIP Telephony	EF	46	RFC 3246
Broadcast Video	CS5	40	RFC 2474
Multimedia Conferencing	AF41	34	RFC 2597
Real-Time Interactive/TelePresence	CS4	32	RFC 2474
Multimedia Streaming	AF31	26	RFC 2597
Call Signaling	CS3	24	RFC 2474
Low-Latency/Transactional Data	AF21	18	RFC 2597
Operations/Administration/Management	CS2	16	RFC 2474
High-Troughput/Bulk Data	AF11	10	RFC 2597
Best Effort	DF	0	RFC 2474
Low-Priority/Scavenger Data	CS1	8	RFC 3662

Note Some of the application class names show both the RFC 4594 names as well as the better known, but less wordy, Cisco QoS Baseline application class names. For example, “Low Latency Data,” “High Throughput Data,” and “Low Priority Data” are generally more easily referred to as “Transactional Data,” “Bulk Data,” and “Scavenger,” respectively. Nonetheless, the names can be viewed as synonymous.

Now let us look at service provider class models. At the time of writing, in North America, most service providers offer 3- or 4-class QoS models, although some are planning 6-class models. In EMEA or Asia Pacific, some providers offer even more classes. Rather than presenting models for each number of SP classes, we consider just two, a 4-class and a 6-class model, and the principles applied to these enterprise-to-SP mapping examples can be extended to other traffic class models. These 4-class and 6-class examples are graphically illustrated in Figure 6-10.

Figure 6-10 Example 4-Class and 6-Class MPLS VPN SP QoS Models



Comparing Figure 6-7 to Figure 6-8 highlights the fact that, more often than not, there are generally fewer SP traffic classes than enterprise classes, and thus there are times when more than one enterprise traffic class is assigned to the same SP class. When such collapsing has to be done, it is recommended to **avoid mixing TCP-based applications with UDP-based applications within a single service provider class**. This is due to the behavior of these respective protocols during periods of congestion.

Specifically, due to TCP transmission guarantees and its windowing behavior, TCP transmitters throttle back flows when drops are detected. In contrast, most UDP transmitters are completely oblivious to drops and, therefore, never lower transmission rates because of dropping. When TCP flows are combined with UDP flows within a single service provider class and the class experiences congestion, TCP flows continually lower their transmission rates, potentially giving up their bandwidth to UDP flows that are oblivious to drops. This effect is called TCP starvation/UDP dominance. Even if WRED is enabled on the service provider class, the same behavior would be observed because WRED (for the most part) manages congestion only on TCP-based flows. Granted, it is not always possible to separate TCP-based flows from UDP-based flows, but it is beneficial to be aware of this behavior when making such application-mixing decisions within a single service provider class.

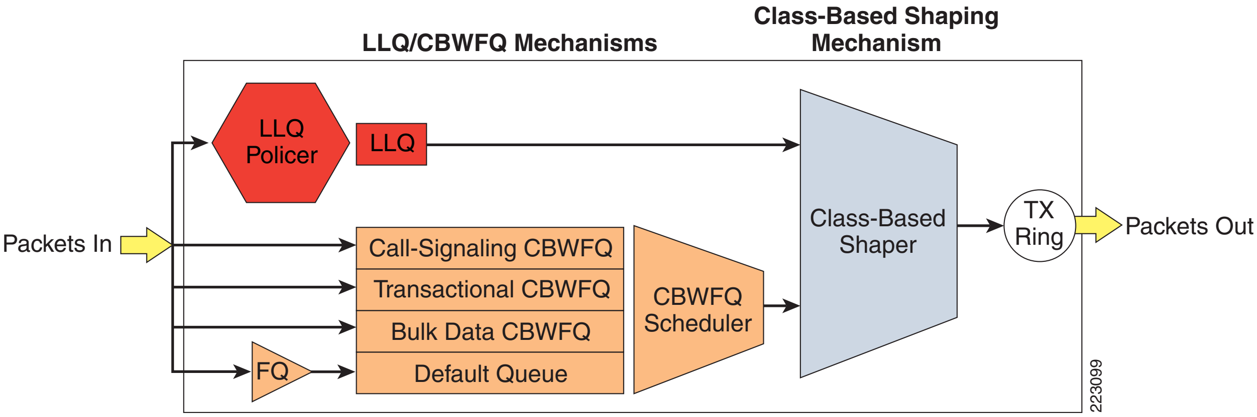
Now let us look at traffic marking and remarking requirements. As can be seen in Figure 6-8, DSCP values serve as the admission criteria per SP class. These DSCP values likely vary from one provider to another, therefore it is important for the enterprise subscriber be fully informed of the DSCP admission criteria for each SP class. At times applications may need to be remarked in order to gain admission to the desired SP class. When such is the case, **remarking should be done as the final operations on the (unmanaged) CE egress edge**. Otherwise, if remarking is done at an earlier node, say the campus access edge, then changes to the SP QoS policies or migration to another SP would be much more difficult to manage, as would using multiple SPs for redundancy (each with its own marking scheme).

Also, there may be times when the enterprise has a business requirement to maintain DSCP markings in the branch, perhaps for traffic accounting purposes or for other reasons. In such cases, the enterprise subscriber may choose to make the MPLS VPN appear DSCP-transparent by **restoring enterprise DSCP markings on the CE ingress edge**.

Additionally, each SP class is likely policed on the PE ingress edge. Excess traffic may either be remarked or dropped. Again, it is important for the enterprise subscriber to know exactly how excess traffic is treated on a per-class basis. Understanding SP policing policies is an especially important consideration for the TelePresence class. As we have already discussed in TelePresence Branch WAN Edge LLQ Policy, TelePresence requires 256 KB of committed burst from a policer. **Therefore, it is essential to confirm with the service provider that whatever class TelePresence traffic is assigned to is being policed with at least 256 KB of burst.**

And finally, let us discuss the QoS implications of non-traditional WAN access-media, such as Ethernet. As previously discussed, queuing policies only engage when the physical interface is congested (as is indicated to IOS software by a full Tx-Ring). This means that queuing policies never engage on media that has a contracted sub-line rate of access, whether this media is Frame Relay, ATM, or Ethernet. In such a scenario, **queuing can only be achieved at a sub-line rate by introducing a two-part policy**, sometimes referred to a **Hierarchical QoS (HQoS) policy** or nested QoS policy, **wherein 1) traffic is shaped to the sub-line rate, and 2) traffic is queued according to the LLQ/CBWFQ policies within the sub-line rate**. With such an HQoS policy, it is not the Tx-Ring that signals IOS software to engage LLQ/CBWFQ policies, but rather it is the Class-Based Shaper that triggers software queuing when the shaped rate has been reached. Such an HQoS policy is graphically illustrated in Figure 6-11.

Figure 6-11 Hierarchical QoS Policy—Shaping to a Sub-Line Rate with Queuing within the Shaped Rate

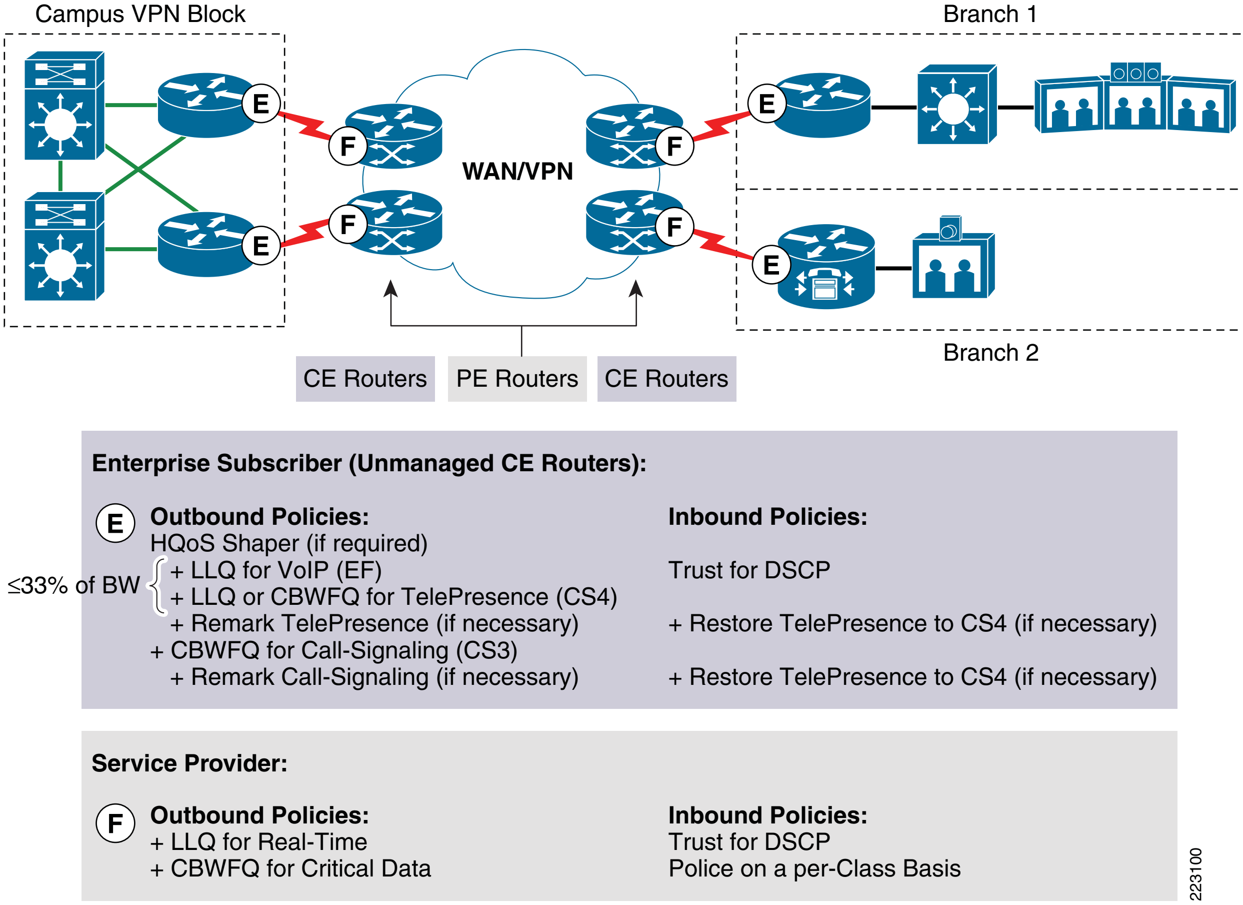


Let us consider a practical example in which an SP offers an enterprise subscriber a GigabitEthernet handoff, but with a (sub-line rate) contract for only 50 Mbps. Normally, queuing policies only engage on this GE interface when the offered traffic rate exceeds 1000 Mbps. However, the enterprise administrator wants to ensure that traffic within the 50 Mbps contracted rate is properly prioritized prior to PE handoff. Therefore, they configure an HQoS policy, such that the interface shapes all traffic to the contracted 50 Mbps rate and attaches a nested queuing policy to the shaping policy, such that traffic is properly prioritized within this 50 Mbps sub-line rate.

The only other consideration an administrator should keep in mind with HQoS policies is their potential performance impact. When performed in IOS software on routers, then these policies generate a marginal CPU load; the actual amount of the load depends on platforms, speeds, policy complexity, traffic rates, and other factors. A rule of thumb, however, is to always keep CPU levels below 75% during normal operating conditions, as this allows some cycles to always be available to process network events. Some platform guidance for HQoS policies are presented, along with detailed configurations, in TelePresence Branch MPLS VPN QoS Designs.

Finally, let us take a look at how all these QoS policies fit together for a TelePresence-enabled branch subscribing to a MPLS VPN, as illustrated in Figure 6-12.

Figure 6-12 Enterprise and Service Provider MPLS VPN QoS Design Recommendations for TelePresence


Campus VPN Block
Branch 1
Branch 2
WAN/VPN
E
F
CE Routers
PE Routers
CE Routers
Enterprise Subscriber (Unmanaged CE Routers):
E Outbound Policies:
HQoS Shaper (if required)
≤33% of BW
+ LLQ for VoIP (EF)
+ LLQ or CBWFQ for TelePresence (CS4)
+ Remark TelePresence (if necessary)
+ CBWFQ for Call-Signaling (CS3)
+ Remark Call-Signaling (if necessary)
Inbound Policies:
Trust for DSCP
+ Restore TelePresence to CS4 (if necessary)
+ Restore TelePresence to CS4 (if necessary)
Service Provider:
F Outbound Policies:
+ LLQ for Real-Time
+ CBWFQ for Critical Data
Inbound Policies:
Trust for DSCP
Police on a per-Class Basis
223100

As shown in Figure 6-12, the enterprise subscriber provisions LLQ/CBWFQ policies for VoIP and TelePresence (in conjunction with HQoS sub-line rate shapers, if required) and performs any application-class remarking on the CE egress edges. Optionally, if required, the enterprise may restore their markings on the CE ingress edges for any traffic that required remarking over the MPLS VPN.

In turn, the service provider polices traffic on a per-class basis on their PE ingress edges and provisions LLQ/CBWFQ policies according to their class-models on the PE egress edges. They may also perform QoS and/or MPLS Traffic Engineering within their core; however, such policies are beyond the scope of our enterprise-centric designs.

Note Due of the explicit ingress policing on PE edges of MPLS VPNs, it cannot be overemphasized that the enterprise subscriber needs a comprehensive Call Admission Control system in place to limit the amount of TelePresence traffic over the MPLS VPN; otherwise the call-quality of **all** TelePresence calls over the MPLS VPN may degrade to the point of unusability.

TelePresence Branch MPLS VPN QoS Designs

Having reviewed the many design considerations for MPLS VPNs, let us now put them into practice by constructing configuration policies to meet the requirements of several specific scenario examples, including a 4-class SP model, a 6-class SP model, and a sub-line rate access example.

TelePresence 4-Class MPLS VPN SP Model QoS Design

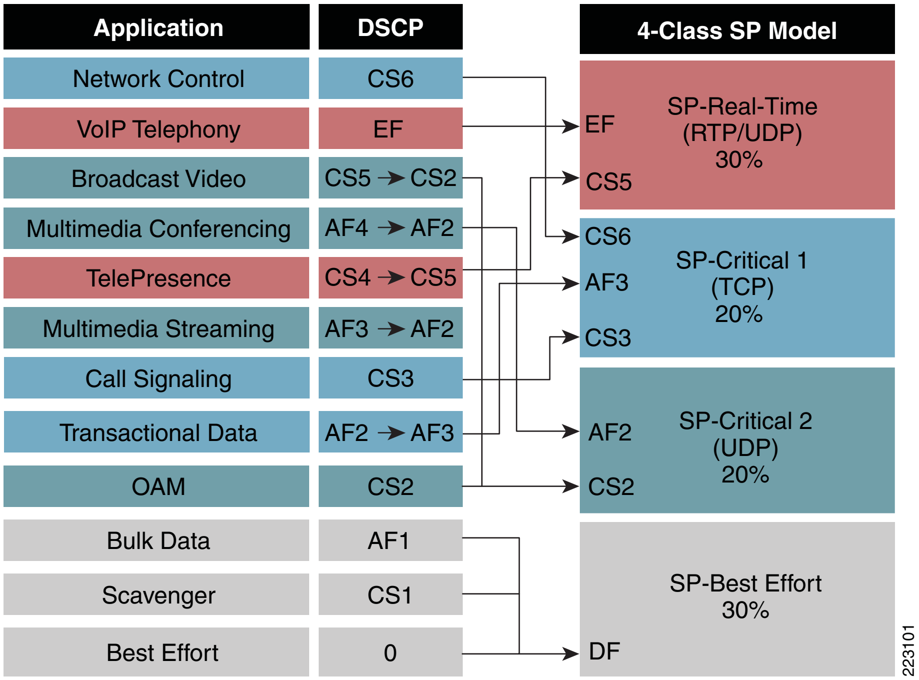
Let us begin by constructing a CE edge policy to support a 4-class SP model example. In this example, since there are so few classes to choose from, TelePresence may need to be combined with another application. **It is highly recommended not to combine TelePresence with any unbounded application** (i.e., an application without any admission control) **within a single SP class**, since this could lead to class congestion, resulting in TelePresence drops (with or without WRED enabled on the SP class), which would ruin TelePresence call quality. Therefore, in such a design two choices exist:

- Assign TelePresence into the SP-Realtime class along with voice.
- Assign TelePresence to a dedicated non-priority SP class.

We consider the option of assigning TelePresence into the SP-Realtime class for this example and then consider the option of assigning it to a non-priority class in the following (6-class SP model) example.

Given the 4-Class SP model illustrated in Figure 6-10, we have a Realtime class, a default Best Effort class, and two additional non-priority traffic classes. In this case, the enterprise administrator may elect to separate TCP-based applications from UDP-based applications by using these two non-priority SP traffic classes. Specifically, if voice and TelePresence are the only applications to be assigned to the SP Realtime class, then Broadcast Video, Multimedia Conferencing, Multimedia Streaming, and Operations/Administration/Management (OAM) traffic (which is largely UDP-based) can all be assigned to the UDP SP-class (SP-Critical 2). This leaves the other non-priority SP class (SP-Critical 1) available for control plane applications, such as Network Control and Call-Signaling, along with TCP-based Transactional Data applications. Figure 6-13 shows the per-class remarking requirements from the CE edge to gain access to the classes within the 4-class SP model, with TelePresence assigned to the SP-Realtime class, along with voice.

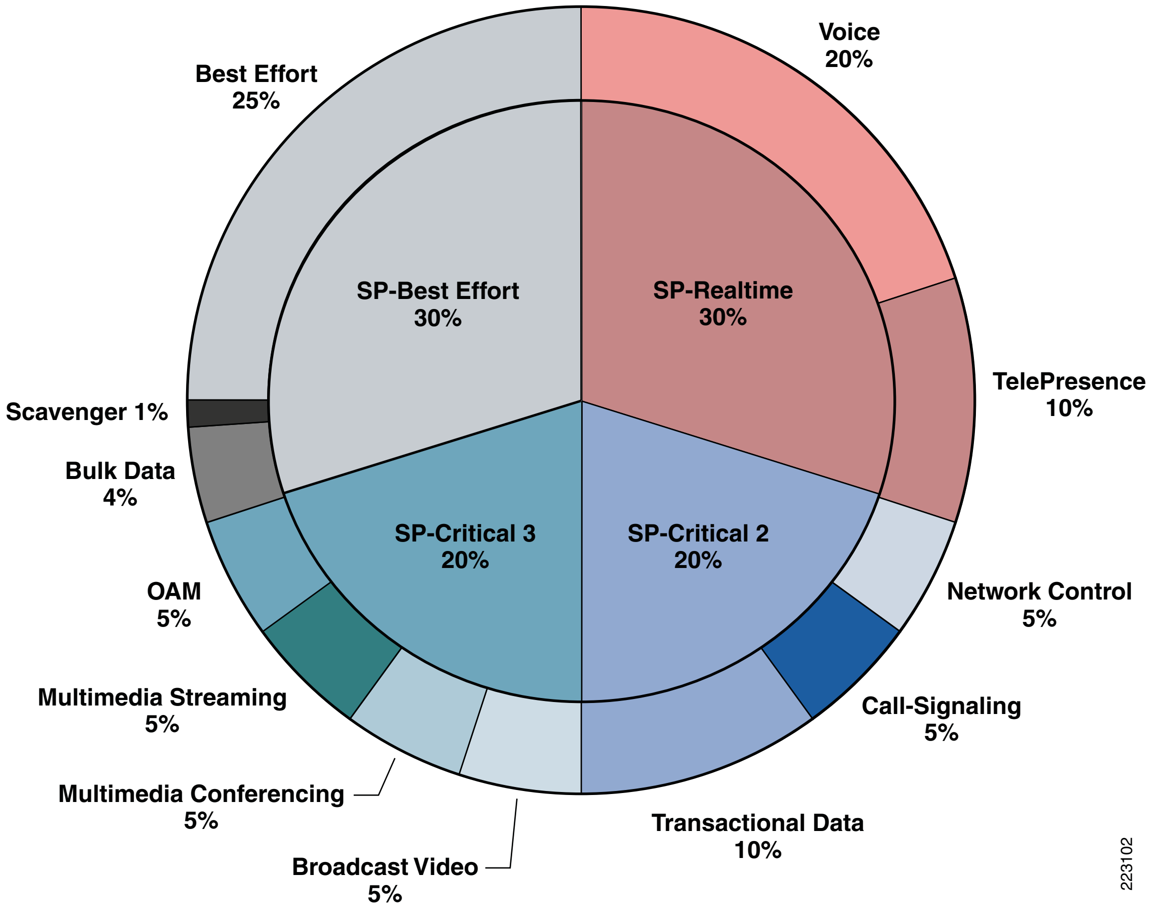
Figure 6-13 Enterprise-to-SP Mapping—4-Class SP Model Example with TelePresence Assigned to the Realtime Class Along with Voice



As shown in Figure 6-13, in this example TelePresence traffic must be remarked on the CE egress edge to CS5 to gain access to the SP's Realtime class. Also, Broadcast Video must be remarked to CS2 to assign it to the UDP SP class (SP-Critical 2). Similarly, Multimedia Conferencing and Multimedia Streaming must be remarked to AF2 to assign these also to the UDP SP class. Correspondingly, Transactional Data traffic must be remarked to AF3 to gain access into the TCP SP class (SP-Critical 1). All other traffic does not require remarking to gain admission to the desired classes; this includes Bulk and Scavenger, as these default to the SP-Best Effort class without any explicit remarking.

Additionally, the relative per-class bandwidth allocations need to be aligned, such that the enterprise CE edge queuing policies are consistent with the SP's PE edge queuing policies to ensure compatible Per-Hop Behaviors (PHBs). Compatible bandwidth allocations are illustrated in Figure 6-14, where the inner pie-chart represents the SP's per-class bandwidth allocations and the outer pie-chart represents the enterprise's per-class bandwidth allocations over an OC3 link.

Figure 6-14 Enterprise-to-SP Bandwidth AllocationC4-Class SP Model Example with TelePresence Assigned to the Realtime Class Along with Voice



The CE egress edge configuration for this policy is shown in Example 6-14.

Example 6-14 Enterprise-to-SP Mapping—4-Class SP Model Example with TelePresence Assigned to the Realtime Class Along with Voice

```
policy-map CE-EDGE-4CLASS-OC3-POS
 class VOICE
  police cir 31000000                    ! Voice is policed to 31 Mbps (20%)
   bc 15500                              ! Bc is 15.5 KB
   conform-action transmit               ! Conforming action --> transmit
   exceed-action drop                    ! Single-Rate Policing action
  priority                               ! LLQ command for OC3-POS
class TELEPRESENCE
police cir 15000000                      ! TP is policed to 15 Mbps
    bc 256000                            ! Bc is 256 KB
    conform-action transmit              ! Conforming action --> transmit
    exceed-action drop                   ! Single-Rate Policing action
  priority                               ! LLQ command for OC3-POS
  set dscp cs5                           ! Remark TelePresence to CS5
class NETWORK-CONTROL
  bandwidth percent 5                    ! CBWFQ for Routing
class CALL-SIGNALING
  bandwidth percent 5                    ! CBWFQ for Call-Signaling
class TRANSACTIONAL-DATA
  bandwidth percent 10                   ! CBWFQ for Transactional Data
  random-detect dscp-based                   ! DSCP-WRED for Transactional Data
  set dscp af31                              ! Remark Transactional Data to AF31
class BROADCAST-VIDEO
  bandwidth percent 5                        ! CBWFQ for Broadcast Video
  set dscp cs2                               ! Remark Broadcast Video to CS2
class MULTIMEDIA-CONFERENCING
  bandwidth percent 5                        ! CBWFQ Video-Conferencing
  random-detect dscp-based                   ! DSCP-WRED for Video-Conferencing
  set dscp af21                              ! Remark Video-Conferencing to AF21
class MULTIMEDIA-STREAMING
  bandwidth percent 5                        ! CBWFQ for Streaming-Video
  random-detect dscp-based                   ! DSCP-WRED for Streaming-Video
  set dscp af21                              ! Remark Streaming-Video to AF21
class OAM
  bandwidth percent 5                        ! CBWFQ for Network Management
class BULK-DATA
 bandwidth percent 4                         ! CBWFQ for Bulk Data
  random-detect dscp-based                   ! DSCP-WRED for Bulk Data
class SCAVENGER
  bandwidth percent 1                        ! Minimum CBWFQ for Scavenger
class class-default
  bandwidth percent 25                       ! CBWFQ for Best Effort
  random-detect                              ! WRED for Best Effort
!
…

…
interface POS3/0/1
 description BRANCH-CE-EDGE-OC3-POS
 ip address 192.168.5.1 255.255.255.252
 clock source internal
 service-policy output CE-EDGE-4CLASS-OC3-POS! Attaches policy
!
```

Optionally, the original markings for TelePresence, Transactional Data, Broadcast Video, Multimedia Conferencing, and Multimedia Signaling can be restored on the CE ingress edges to make the MPLS VPN appear completely DSCP-transparent to the enterprise, despite the remarking requirements of the service provider. The TelePresence and Transactional Data remarking policies are 1:1 DSCP mappings (one DSCP is changed to another DSCP) and as such are easy to undo with a reversing 1:1 mapping operation. However, the remarking operations performed on Broadcast Video, Multimedia Conferencing, and Multimedia Signaling are 2:1 mappings (two DSCP values are changed to a single DSCP value); specifically Broadcast Video and OAM now share DSCP CS2 and Multimedia Conferencing and Multimedia Signaling share DSCP AF21. These 2:1 DSCP mappings require additional classification policies to identify the discrete applications now sharing a single codepoint. These additional classification policies can include NBAR or access-lists.

In Example 6-15, TelePresence and Transactional Data are restored to their original enterprise-marked DSCP values via a simple 1:1 reverse-mapping. Broadcast Video is separated from OAM by referencing an ACL that identifies the source IP address of the Broadcast Video servers. Multimedia Streaming, in this example, consists of streaming RealAudio and VDO Live stateful protocols, both of which can be identified via NBAR and thus sifted apart from Multimedia Conferencing. An optional DSCP restoration policy for the CE ingress edge is shown in Example 6-15.

Example 6-15 Optional Enterprise DSCP Marking Restoration Policies for CE Ingress Edges

```
class-map match-all SP-TELEPRESENCE
 match dscp cs5                                  ! Remarked value for TelePresence
class-map match-all SP-TRANSACTIONAL-DATA
 match dscp af31 af32 af33                       ! Remarked value(s) for Trans-Data
class-map match-all SP-BROADCAST-VIDEO
```

```
 match dscp cs2                              ! Shared DSCP for Bdcst Video + OAM
 match access-group name BROADCAST-VIDEO-SERVERS! References ACL
class-map match-all SP-MULTIMEDIA-STREAMING-REALAUDIO
 match dscp af21 af22 af32                   ! Shared DSCP for MM-Stream + Conf
 match protocol realaudio                    ! NBAR PDLM for RealAudio
class-map match-all SP-MULTIMEDIA-STREAMING-VDOLIVE
 match dscp af21 af22 af32                   ! Shared DSCP for MM-Stream + Conf
 match protocol vdolive                      ! NBAR PDLM for VDOLive
class-map match-all SP-MULTIMEDIA-CONFERENCING
 match dscp af21 af22 af32                   ! All other AF2 is MM-Conf only
!
policy-map CE-EDGE-IN
 class SP-TELEPRESENCE
  set dscp cs4                               ! Restores original marking for TP
 class SP-TRANSACTIONAL-DATA
  set dscp af21                              ! Restores original marking for TD
 class SP-BROADCAST-VIDEO
  set dscp cs5                               ! Restores original marking for BV
 class SP-MULTIMEDIA-STREAMING-REALAUDIO
  set dscp af31                              ! Restores original marking for MMS
 class SP-MULTIMEDIA-STREAMING-VDOLIVE
  set dscp af31                              ! Restores original marking for MMS
 class SP-MULTIMEDIA-CONFERENCING
  set dscp af41                              ! Restores original marking for MMC
!

interface POS3/0/1
 description BRANCH-CE-EDGE-OC3-POS
 ip address 192.168.5.1 255.255.255.252
 service-policy output CE-EDGE-OC3-POS       ! Attaches egress policy
 service-policy input CE-EDGE-IN             ! Attaches ingress policy
!
...
!
ip access-list extended BROADCAST-VIDEO-SERVERS! Reference ACL
permit ip any 10.200.200.0 0.0.0.255         ! Broadcast Video Server Subnet
!
```

These configurations can be verified with the following command:

- **show policy-map interface**

We can note a few important policy elements in Example 6-15:

- It is important to give the remarked traffic classes unique names from the original enterprise-marked traffic classes, otherwise these interfere or overwrite each other. For example class “TELEPRESENCE” matches on the enterprise marking value for TelePresence (CS4), but class “SP-TELEPRESENCE” matches on the remarked value for TelePresence (CS5).
- Because of the default **match-all** operand on class-maps, we have to have two separate class maps to sift, [traffic marked AF2 and using the realaudio protocol] or [traffic marked Af2 and using the vdolive protocol]. If a single class-map was used, then the **match-all** operand would preclude any match (because the protocol in use cannot be both realaudio and vdolive at the same time; these protocols are unique and represent mutually exclusive criterion). Furthermore, a **match-any** operand on a combined class-map for AF2 **or** realaudio **or** vdolive would not work either, because this would fail the logical requirement that the traffic must be [marked AF2 **and** realaudio] or [marked AF2 **and** vdolive], and thus would result in false-positive matches on Multimedia Conferencing traffic marked AF2.
- It is important to keep in mind that classification logic, like ACL logic, is based on the first-true-match rule. Therefore, the order of classification and sifting must be given careful consideration in order to ensure that traffic marking gets restored properly.

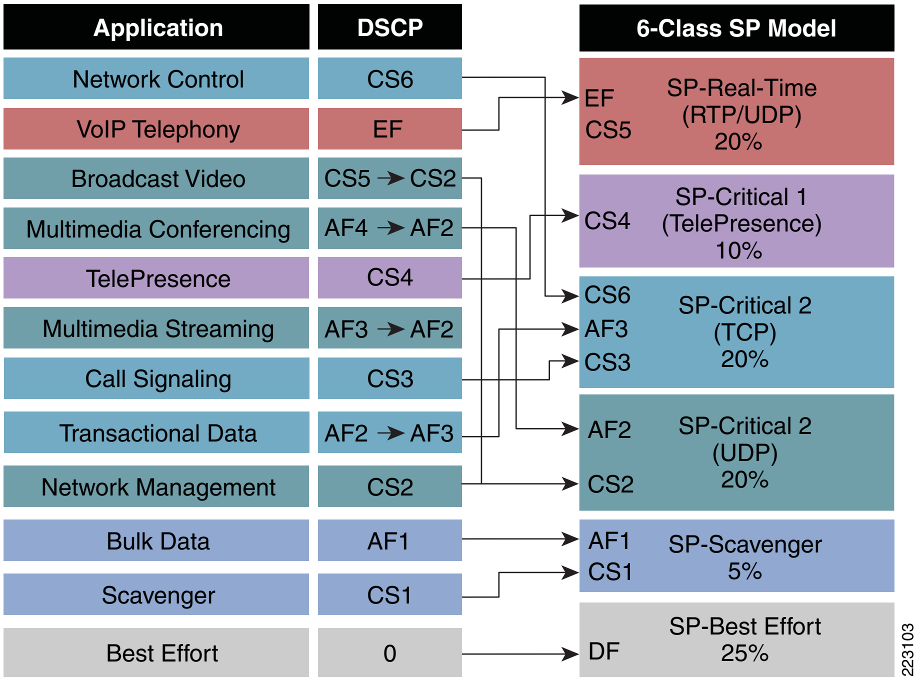
TelePresence 6-Class MPLS VPN SP Model QoS Design

Now let us turn our attention to the 6-Class SP model, also illustrated in Figure 6-10. In this model, we have a Realtime class, a default Best Effort class, a "less-than Best Effort" Scavenger class, and three additional non-priority traffic classes. Furthermore, to illustrate more design options, we assign TelePresence to a non-priority SP-class in this example; but of course TelePresence can also assigned, in combination with voice, to the SP-Realtime class, as has already been detailed in the previous section.

In this case, the enterprise administrator can dedicate one of the non-priority classes (such as SP-Critical 1) for TelePresence. Again, it bears reiteration that it would not be recommended to assign TelePresence in conjunction with any unbounded application into a single SP class, as the other application could potentially cause the combined class to congest, resulting in TelePresence drops and loss of call-quality.

This leaves two additional non-priority classes, which again allows the administrator to separate TCP-based applications from UDP-based applications. Specifically, Broadcast Video, Multimedia Conferencing, Multimedia Streaming, and Operations/Administration/Management (OAM) traffic can all be assigned to the UDP SP-class (SP-Critical 3). This leaves the other non-priority SP class (SP-Critical 2) available for control plane applications, such as Network Control and Call-Signaling, along with TCP-based Transactional Data applications. Figure 6-15 shows the per-class remarking requirements from the CE edge to gain access to the classes within the 6-class SP model, with TelePresence assigned to a non-priority SP class.

Figure 6-15 Enterprise-to-SP Mapping—6-Class SP Model Example with TelePresence Assigned to a Dedicated, Non-Priority SP-Class

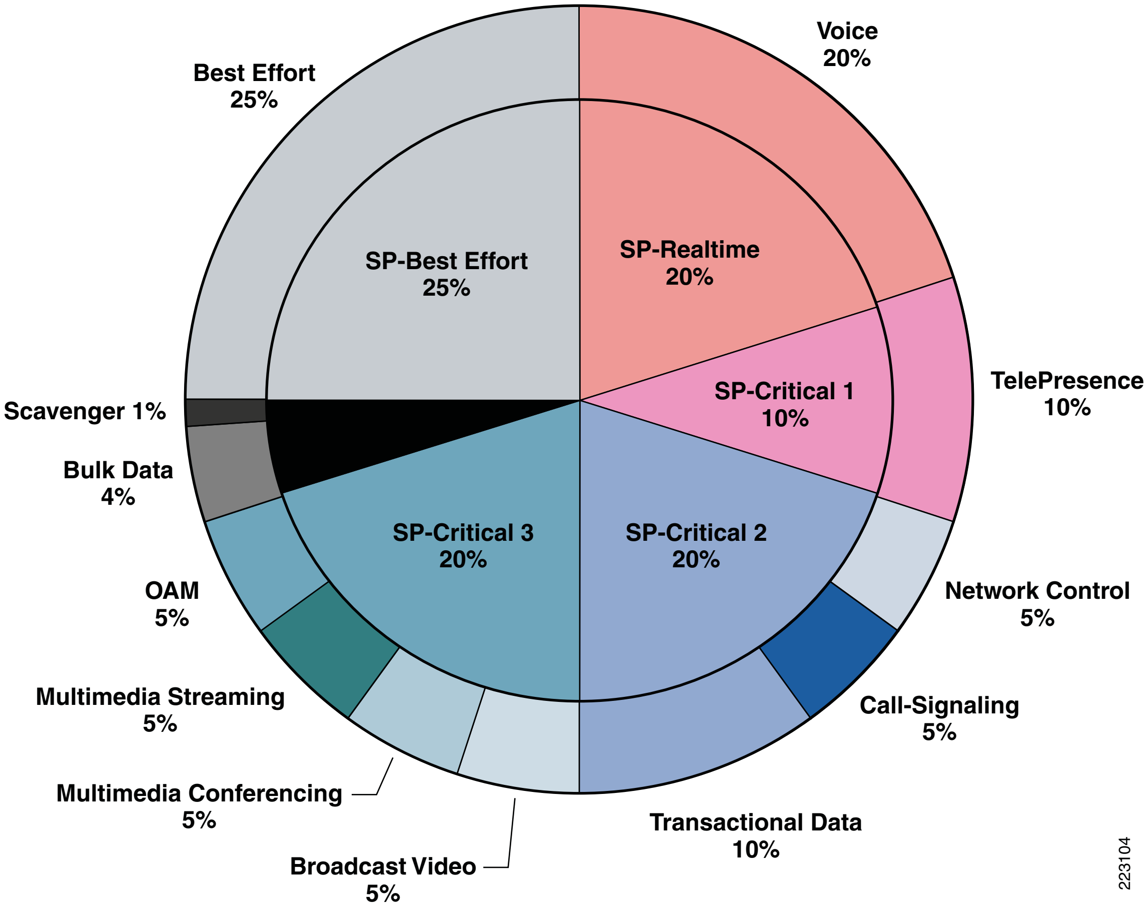


Application	DSCP
Network Control	CS6
VoIP Telephony	EF
Broadcast Video	CS5 → CS2
Multimedia Conferencing	AF4 → AF2
TelePresence	CS4
Multimedia Streaming	AF3 → AF2
Call Signaling	CS3
Transactional Data	AF2 → AF3
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	0

As shown in Figure 6-15, in this second example TelePresence traffic does not need to be remarked to gain access to the dedicated, non-priority SP class to which it is assigned (SP-Critical 1). However as before, Broadcast Video must be remarked to CS2 to assign it to the UDP SP class (SP-Critical 3); Multimedia Conferencing and Multimedia Streaming must be remarked to AF2 to assign these also to the UDP SP class. Correspondingly, Transactional Data traffic must be remarked to AF3 to gain access into the TCP SP class (SP-Critical 2). All other traffic does not require remarking to gain admission to the desired classes. However, it may be noted that Bulk and Scavenger no longer default to the SP-Best Effort class, but rather now default to the SP-Scavenger class, which is the desired policy to bind these potentially bandwidth-hogging applications.

Additionally, the relative per-class bandwidth allocations again need to be aligned, such that the enterprise CE edge queuing policies are consistent with the SP's PE edge queuing policies. Compatible bandwidth allocations are illustrated in Figure 6-16, where the inner pie-chart represents the SP's per-class bandwidth allocations and the outer pie-chart represents the enterprise's per-class bandwidth allocations over an OC3 link.

Figure 6-16 Enterprise-to-SP Bandwidth Allocation—6-Class SP Model Example with TelePresence Assigned to a Dedicated, Non-Priority SP-Class



The CE egress edge configuration for this policy is shown in Example 6-16.

Example 6-16 Enterprise-to-SP Mapping—6-Class SP Model Example with TelePresence Assigned to a Dedicated, Non-Priority SP-Class

```
policy-map CE-EDGE-6CLASS-OC3-POS
 class VOICE
  police cir 31000000                          ! Voice is policed to 31 Mbps (20%)
   bc 15500                                    ! Bc is 15.5 KB
   conform-action transmit                     ! Conforming action --> transmit
   exceed-action drop                         ! Single-Rate Policing action
  priority                                    ! LLQ command for OC3-POS
class TELEPRESENCE
```

```
  bandwidth percent 10                           ! CBWFQ for TelePresence
 class NETWORK-CONTROL
  bandwidth percent 5                            ! CBWFQ for Routing
 class CALL-SIGNALING
  bandwidth percent 5                            ! CBWFQ for Call-Signaling
 class TRANSACTIONAL-DATA
  bandwidth percent 10                           ! CBWFQ for Transactional Data
  random-detect dscp-based                       ! DSCP-WRED for Transactional Data
  set dscp af31                                  ! Remark Transactional Data to AF31
 class BROADCAST-VIDEO
  bandwidth percent 5                            ! CBWFQ for Broadcast Video
  set dscp cs2                                   ! Remark Broadcast Video to CS2
 class MULTIMEDIA-CONFERENCING
  bandwidth percent 5                            ! CBWFQ Video-Conferencing
  random-detect dscp-based                       ! DSCP-WRED for Video-Conferencing
  set dscp af21                                  ! Remark Video-Conferencing to AF21
 class MULTIMEDIA-STREAMING
  bandwidth percent 5                            ! CBWFQ for Streaming-Video
  random-detect dscp-based                       ! DSCP-WRED for Streaming-Video
  set dscp af21                                  ! Remark Streaming-Video to AF21
 class OAM
  bandwidth percent 5                            ! CBWFQ for Network Management
 class BULK-DATA
  bandwidth percent 4                            ! CBWFQ for Bulk Data
  random-detect dscp-based                       ! DSCP-WRED for Bulk Data
 class SCAVENGER
  bandwidth percent 1                            ! Minimum CBWFQ for Scavenger
 class class-default
  bandwidth percent 25                           ! CBWFQ for Best Effort
  random-detect                                  ! WRED for Best Effort
!
```

This configuration can be verified with the following command:

- **show policy-map interface**

Optionally, if the original markings for Transactional Data, Broadcast Video, Multimedia Conferencing, and Multimedia Signaling need to be restored, these can be done in a similar manner as demonstrated in Example 6-15, with the exception of not requiring TelePresence traffic to be restored (as it does not get remarked in this 6-class model example).

TelePresence Sub-Line Rate Ethernet Access QoS Designs

As previously discussed, to enforce CE edge queuing policies at sub-line rates, an HQoS policy must be used such that a shaper smooths out traffic to the sub-line rate and forces queuing to occur if this rate is exceeded.

As with policers, Cisco IOS shapers operate on a token-bucket principle, achieving sub-line rates by allowing traffic through in specified bursts (Bc) per sub-second intervals (Tc). As shaping introduces delay to packets above the burst value, it is important to properly size the bursts and intervals to minimize potential shaping jitter. For example, as previously discussed, 1080p sends 30 frames of video per second or, phrased differently, a frame's worth of information every 33 ms. However, if the shaping interval is set too low, say to 5 ms, then a frame's worth of information may be delayed over 3-5 shaping intervals (depending on the amount of frame information). Extensive lab testing has shown that configuring a shaping interval of 20 ms has resulted in the most consistent and minimal jitter values to support a CTS-3000 call.

The interval parameter cannot be set directly, but is set indirectly by explicitly configuring the burst parameter. The relationship between the interval, burst, and shaped rate is given as:

Tc = Bc/Shaped Rate

Or:

Bc = Shaped Rate * Tc

For example, on a FE or GE interface configured to support a sub-line rate of 50 Mbps, a burst value of 1 megabit (50 Mbps * 20 ms) would result in an optimal shaping interval for TelePresence.

Note For Cisco IOS Shapers, like the Class-Based Shaper, the burst is expressed in bits (not in Bytes, as is the case with policers).

Translating this into an HQoS policy yields the following configuration, as shown in Example 6-17.

Example 6-17 HQoS Policy to Queue and Shape TelePresence Traffic to a 50 Mbps Sub-Line Rate Over a GigabitEthernet Interface

```
policy-map CE-EDGE                         ! CE Edge queuing policy
 class VOICE
  ...
 class TELEPRESENCE
  ...                                      ! Either a dual-LLQ or CBWFQ policy for TP
...
!
policy-map HQoS-50MBPS                     ! CE Edge HQoS Shaping policy
  class class-default
    shape average 50000000 1000000         ! Rate=50Mbps; Bc=1Mb, Tc=20ms
    service-policy CE-EDGE                 ! Forces queuing at sub-line rate
!
...
!
interface GigabitEthernet0/1
 description CE-EDGE-GE
 ip address 192.168.1.50 255.255.255.252
 no ip redirects
 no ip proxy-arp
 duplex auto
 speed auto
 media-type rj45
 negotiation auto
 service-policy output HQoS-50MBPS         ! Attaches HQoS policy to GE int
!
```

This configuration can be verified with the following command:

- **show policy-map interface**

The final point of consideration for this chapter is the performance impact of HQoS policies on various platforms. As previously discussed, when QoS is performed in hardware, such as on Catalyst switches, then there is no performance impact of QoS policies on the CPU. However, when QoS policies are performed in software, then there is a performance impact that depends on several factors, such as the platform, speed, traffic mix, QoS policy, etc.

At speeds up to 150 Mbps, Cisco IOS routers, like the 3800 series ISR or the Cisco 7200-VXR, may be used to enforce HQoS policies on Ethernet-based access-media. Before we look at the performance impact on these platforms, it bears mentioning that it is not primarily the speed that affects the CPU performance, but rather the Packets-per-second (PPS) rate.

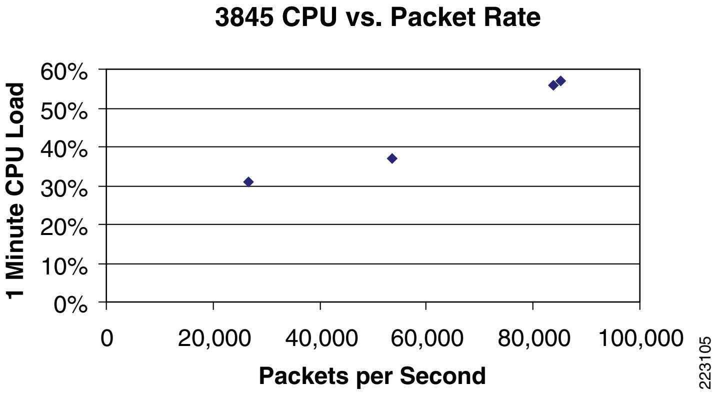
That being said, Table 6-3 shows the performance of a Cisco 3845 router enforcing HQoS policies at rates ranging from 50 Mbps through 150 Mbps.

Table 6-3 *Cisco 3845 Platform Performance of HQoS Policies at 50 Mbps Through 150 Mbps Traffic Rates (26KPPS Through 84 KPPS)*

Bidirectional Target Data Load	Actual Data Load	CPU	PPS	Video Quality
50 Mbps	50 Mbps Out / 48 Mbps In	31%	26,568	Near Perfect
100 Mbps	87 Mbps Out / 88 Mbps In	37%	53,633	Near Perfect
150 Mbps	145 Mbps Out / 147 Mbps In	57%	85,214	Near Perfect
150 Mbps	145 Mbps Out / 140 Mbps In	56%	83,879	Near Perfect

The corresponding performance graph for Table 6-3 is shown in Figure 6-17.

Figure 6-17 *Cisco 3845 Platform Performance of HQoS Policies at 50 Mbps Through 150 Mbps Traffic Rates (26KPPS Through 84 KPPS)*



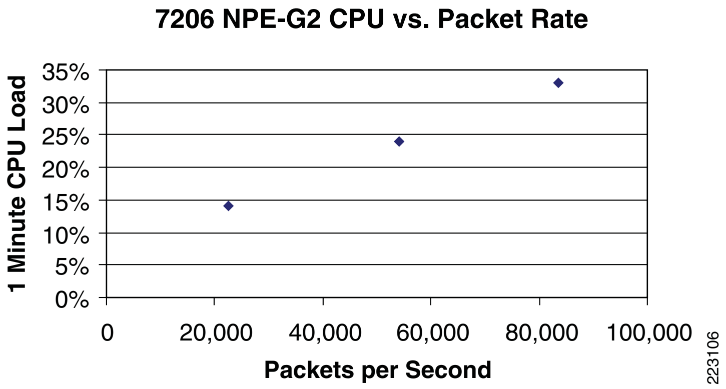
Additionally, Table 6-4 shows the performance of a Cisco 7200VXR router with a Network Processing Engine (NPE) G2 enforcing HQoS policies at rates ranging from 50 Mbps through 150 Mbps.

Table 6-4 *Cisco 7200VXR with NPE-G2 Platform Performance of HQoS Policies at 50 Mbps Through 150 Mbps Traffic Rates (22KPPS Through 84 KPPS)*

Bidirectional Target Data Load	Actual Data Load	CPU	PPS	Video Quality
50 Mbps	50 Mbps Out / 45 Mbps In	14%	22,634	Near Perfect
100 Mbps	96 Mbps Out / 96 Mbps In	24%	54,011	Near Perfect
150 Mbps	142 Mbps Out / 147 Mbps In	33%	83,631	Near Perfect

The corresponding performance graph for Table 6-4 is shown in Figure 6-18.

Figure 6-18 Cisco 7200VXR with NPE-G2 Platform Performance of HQoS Policies at 50 Mbps Through 150 Mbps Traffic Rates (22KPPS Through 84 KPPS)



Both of these platforms are able to support HQoS policies for TelePresence at these speeds (50 Mbps through 150 Mbps). The goal, however, is to keep CPU levels below 75% during normal conditions, so that the router always has some cycles available to process network events.

For higher speeds, HQoS policies should be performed in hardware (such as on the Catalyst 3750-Metro switch with Enhanced Services modules) or on a hybrid hardware/software platform like the Cisco 7600 SIP/SPA combination.

CHAPTER 7

Call Processing Overview

Overview

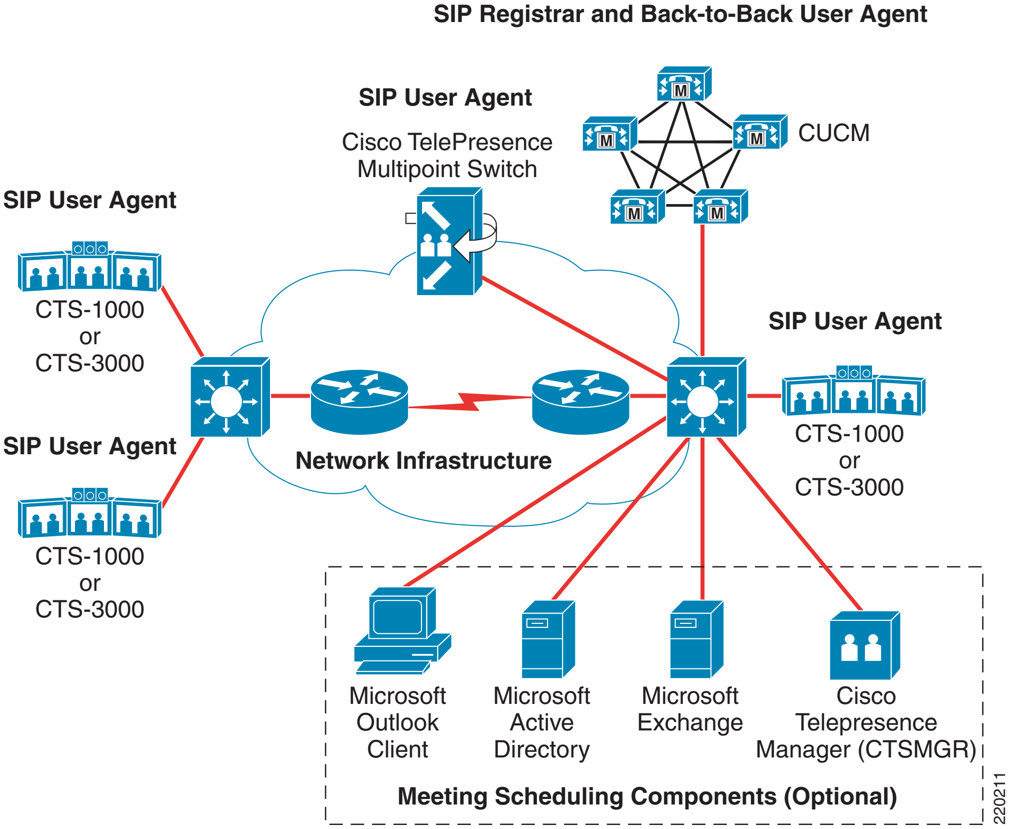
This chapter discusses the Session Initiation Protocol (SIP) and call processing design for Cisco TelePresence, including:

- How the Cisco TelePresence suite of virtual meeting solutions integrates with Cisco Unified Communications Manager (CUCM)
- CUCM software version requirements
- Current CUCM cluster design recommendations
- How the Cisco TelePresence Codecs use Session Initiation Protocol (SIP) and how they register using a shared line appearance with the Cisco Unified 7970G IP phone
- How Cisco TelePresence multipoint resources, such as the Cisco TelePresence Multipoint Switch (CTMS), are configured as a SIP trunk to CUCM and how multipoint calls are routed

Call Processing Components

Figure 7-1 shows the components involved in point-to-point and multipoint TelePresence meetings.

Figure 7-1 Cisco TelePresence Solution Components



These components consist of:

- Two or more Cisco TelePresence systems (any combination of CTS-3000s or CTS-1000s), each with a Cisco Unified 7970G IP phone (not shown in Figure 7-1) which functions as the user interface for launching, controlling, and concluding the meeting
- One CUCM Cluster

  TelePresence release 1.0 requires CUCM version 5.1.1 or higher, with version 5.1.2 recommended for support of the Auto Collaborate feature of TelePresence.
- One or more Cisco TelePresence Multipoint Switches (required for multipoint TelePresence meetings)
- IP network infrastructure over which the signaling, video, and audio media are transported
- Meeting scheduling components (optional):
  - Microsoft Exchange 2003 server
  - Microsoft Active Directory 2000 or 2003 server
  - Microsoft Outlook client
  - Cisco TelePresence Manager (CTSMGR)

  These components are only required for scheduled TelePresence meetings. Ad hoc and permanent TelePresence meetings do not require them.

TelePresence Endpoint Interface to CUCM (Line-Side SIP)

CUCM is the core call processing software for the Cisco TelePresence solution as well as all other Cisco IP telephony devices. CUCM functions as both a SIP registrar and Back to Back User Agent (B2BUA). TelePresence Codecs and 7970G IP phones use SIP for call signaling and control, functioning as SIP user agents which register with a CUCM cluster. Cisco TelePresence Systems use TCP for their SIP signaling to/from CUCM. It should be noted that TelePresence devices are currently not supported by the Survivable Remote Site Telephony (SRST) feature of Cisco router platforms, which is often used to provide resiliency in CUCM deployments with remote sites.

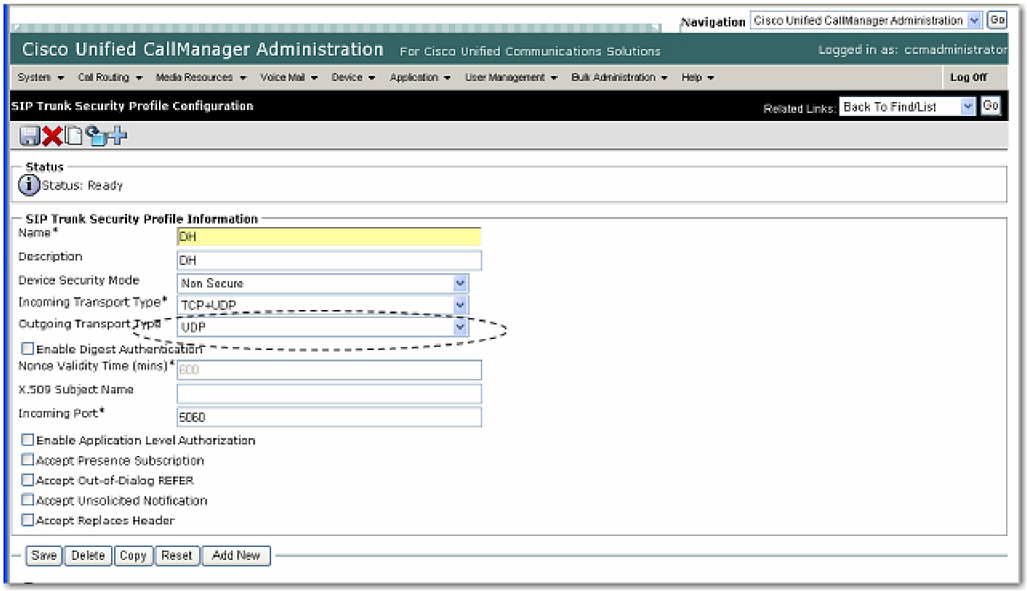
The following sections provide an overview of how TelePresence components register with CUCM, initiate a meeting, and then conclude a meeting.

TelePresence Multipoint Switch Interface to CUCM (Trunk-Side SIP)

The Cisco TelePresence Multipoint Switch (CTMS) multipoint solution connects to CUCM by way of a SIP Trunk. SIP trunks do not use the SIP REGISTER method, and thus for trunks CUCM functions solely as a Back-to-Back User Agent (B2BUA). Route Pattern(s) are configured to route multipoint calls to the SIP trunk(s) of the multipoint switch(es). At the time of writing, CTMS uses UDP for SIP signaling to/from CUCM.

Therefore the outgoing transport type on the CUCM SIP Trunk Security Profile Configuration must be set for UDP for CTMS. This is shown in Figure 7-2.

Figure 7-2 CUCM SIP Trunk Security Profile Configuration



SIP Trunk Security Profile Configuration

Status

Status: Ready

SIP Trunk Security Profile Information

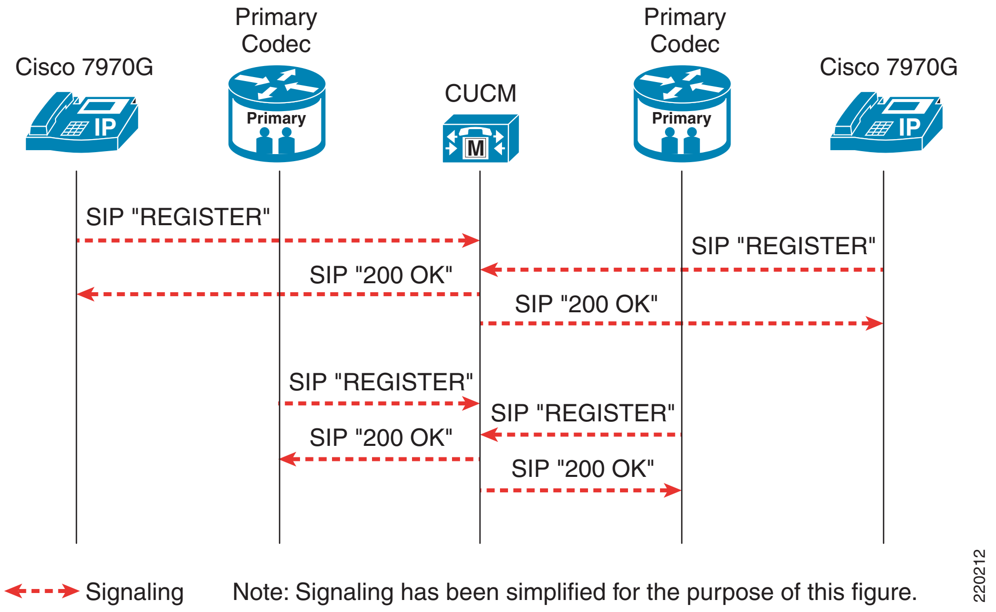
Name*	DH
Description	DH
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type*	UDP
□ Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	
Incoming Port*	5060

□ Enable Application Level Authorization
□ Accept Presence Subscription
□ Accept Out-of-Dialog REFER
□ Accept Unsolicited Notification
□ Accept Replaces Header

TelePresence Endpoint Device Registration

For Release 1.0 of the TelePresence solution, it is recommended that all TelePresence devices in a deployment register to a single CUCM cluster. Although TelePresence devices can be registered across multiple CUCM clusters, Cisco TelePresence Manager (CTSMGR), which performs meeting scheduling, can only support a single CUCM cluster in the current release. The 7970G IP phones which function as the user interface for the TelePresence solution also register with CUCM, sharing the same dial extension as the TelePresence Codecs. Figure 7-3 shows an example of the high-level data flows in the registration process.

Figure 7-3 Cisco TelePresence Device Registration

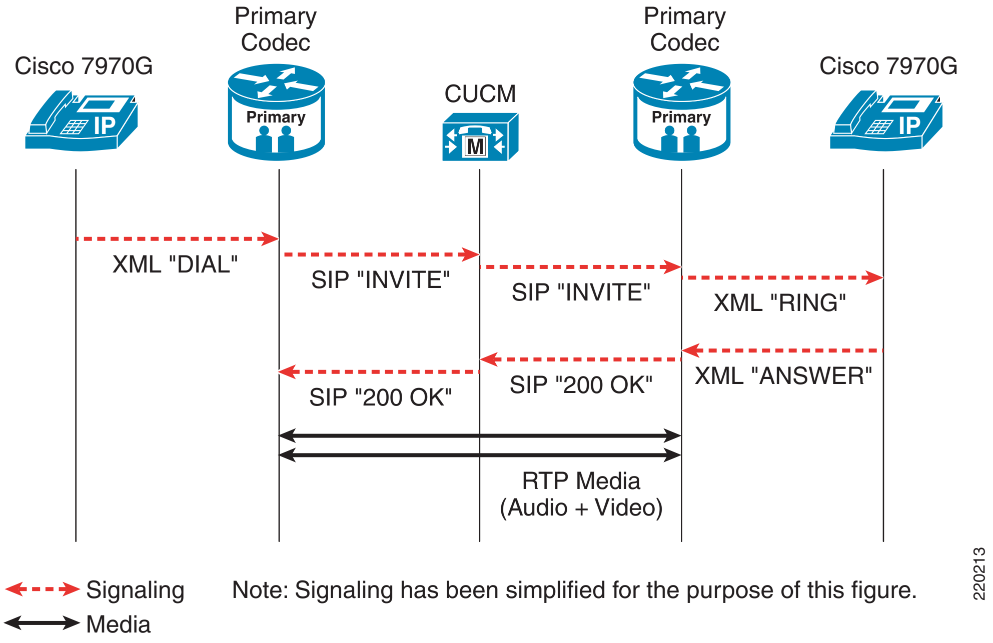


By default CUCM listens on TCP and UDP port 5060 for SIP-related signaling. Cisco TelePresence Systems and Cisco 7970G IP Phones use TCP and hence connect to CUCM on TCP port 5060. The contact header within the SIP REGISTER provides the IP address, transport protocol, port number, and the dial extension for CUCM to reach the TelePresence Codecs and 7970 IP phones.

Call Setup

Once registration is complete, meetings may be established between any two Cisco TelePresence systems or between any TelePresence System and a multipoint switch. Figure 7-4 shows a high-level overview of the call establishment signaling between TelePresence Codecs, their associated 7970G IP phones, and the CUCM cluster.

Figure 7-4 Point-to-Point Cisco TelePresence Call Setup



To make the SIP signaling easier to understand, it has been greatly simplified in Figure 7-4. SIP SUBSCRIBE and NOTIFY messages have been removed from the call flow. These messages are used primarily to update the 7970G IP phones and TelePresence Codecs regarding the status of the call. Finally, HTTP messages between TelePresence Codecs and the Cisco TelePresence Manager have also been removed. These messages inform the Cisco TelePresence Manager of the beginning and ending of a TelePresence meeting.

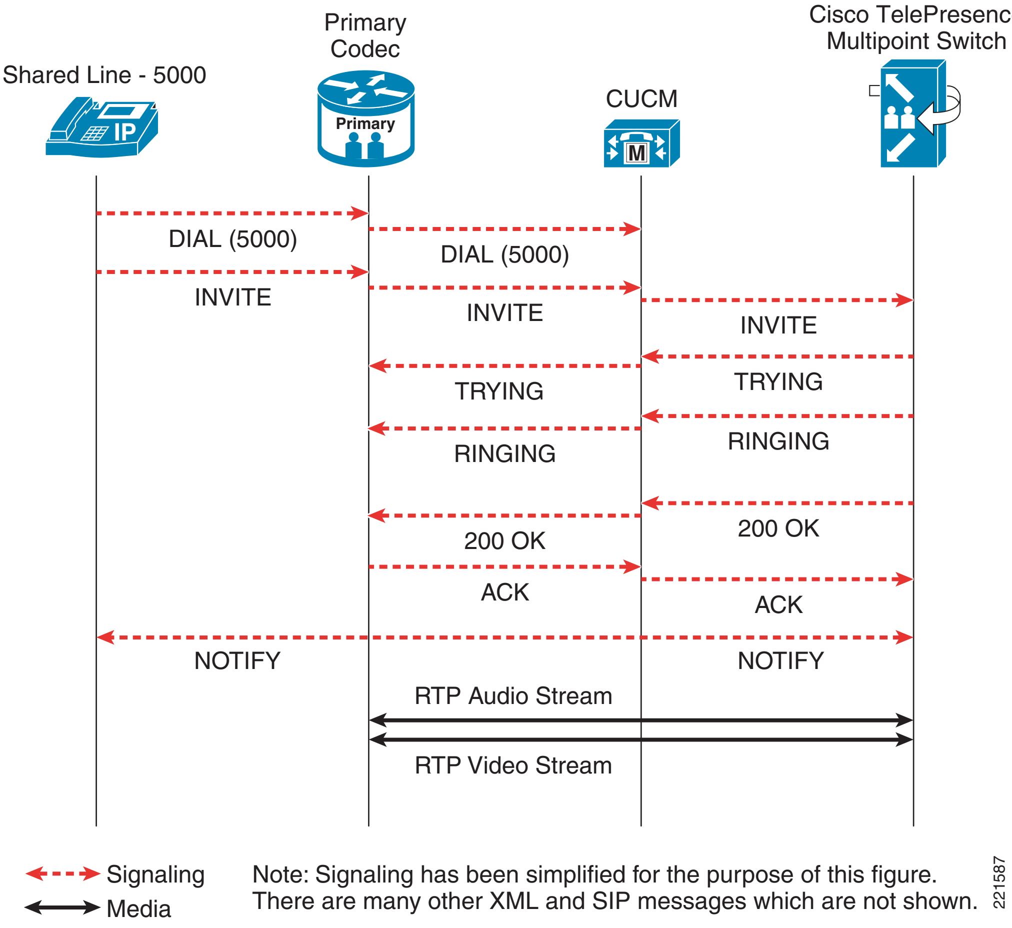
Call setup is initiated when the end user enters or selects, via the touch-screen user interface of the 7970G IP phone, the remote TelePresence location to which he or she wishes to establish a meeting. This causes the 7970G IP phone to generate an XML message to the TelePresence Codec. The XML message instructs the TelePresence Codec to generate a SIP INVITE, which is sent to the CUCM cluster. Within the initial SIP INVITE, the TelePresence Codec uses the Session Description Protocol (SDP). SDP, discussed in IETF RFC 2327, allows two endpoints which are configured for different audio or video modes to negotiate a common set of media parameters for the call. This is accomplished primarily through the use of the media (m=…), attribute (a=…), and bandwidth (b=…) lines. The quality parameter within the TelePresence device configuration in CUCM determines what media capabilities are offered in the initial SDP.

Upon receiving an INVITE from one TelePresence System and determining the destination endpoint (based on the number dialed), CUCM generates a new SIP INVITE to the remote TelePresence Codec. Upon receipt of the SIP INVITE, the TelePresence Codec informs the 7970G IP phone of the incoming call via an XML message. The end user at the remote location accepts the incoming call via the touch-screen user interface of the 7970G phone. This causes a final XML message to be sent to the remote TelePresence Codec, informing it to answer the call. After that, the audio and video media streams begin. Optionally, the TelePresence codec may be configured (in CUCM) to automatically answer all incoming calls, in which case the XML message sequence to/from the phone is skipped and the call is answered immediately. Incidentally, it should be noted that since the same dial extension is shared between the remote TelePresence Codec and the remote 7970G IP phone which functions as its user interface, CUCM generates the new SIP INVITE message to both remote devices. This allows the user to answer the call using the **handset** of the IP Phone (in which case the call is established as an audio-only call). Under normal conditions though, the TelePresence Codec is the one to answer the call and the SIP INVITE to the 7970G IP Phone is canceled.

CUCM acts as a back-to-back user agent (B2BUA), processing requests as a user agent server (UAS) and generating requests as a user agent client (UAC). Unlike a proxy server, CUCM maintains dialog state and participates in all requests sent on the dialogs it establishes. Since CUCM functions as a B2BUA, it sees the SDP information regarding the media capabilities of both sides of the TelePresence call. It determines what audio and video parameters are used for the meeting based on the parameters that are common to both TelePresence devices and what is allowed via the configuration within CUCM. The configuration parameters for the allowed audio and video rates are based on two things: the Quality Setting for each TelePresence System (e.g. 1080p-Best, 1080p-Better, 1080p-Good, 720p-Best, 720-Better and 720p-Good) and the region settings of the device pool to which the TelePresence devices belong. This allows CUCM to set up a call between two TelePresence devices which are configured for different video modes. For example, if one TelePresence device is configured for 1080p-Best while another is configured for 720p-Good, CUCM specifies 720p in the outgoing SIP message to the 1080p system, thereby negotiating the call down to 720p in both directions.

Multipoint calls are no different than point-to-point calls in that each TelePresence System dials the number of the multipoint switch in a point-to-point fashion. In other words, a multipoint call is nothing more than several point-to-point calls all landing on the same destination device (the multipoint switch). The differences are that instead of matching the dialed number to a Directory Number assigned to a registered endpoint, CUCM matches the dialed number to a Route Pattern assigned to a SIP trunk. The signaling and media negotiation sequences are otherwise the same.

Figure 7-5 Multipoint Cisco TelePresence Call Setup

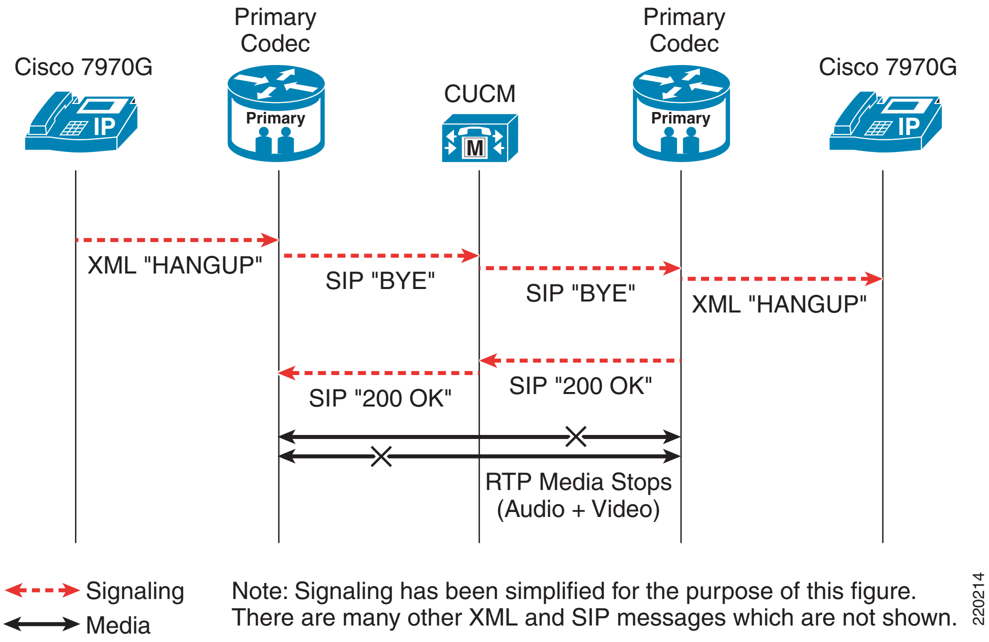


TelePresence utilizes a single AAC-LD over RTP audio stream and a single H.264 over RTP video stream in each direction, for a total of four RTP media streams per bi-directional point-to-point TelePresence meeting. This holds regardless of the model of Cisco TelePresence system device. With CTS-3000 devices, the video streams from the multiple cameras are multiplexed into a single RTP stream. Likewise, the audio streams are multiplexed into a single audio stream. The auxiliary video and audio streams are also multiplexed into these streams.

Call Teardown

Figure 7-6 shows a high-level overview of the call termination signaling between TelePresence Codecs, the 7970G IP phones which function as their user interfaces, and the CUCM cluster.

Figure 7-6 Cisco TelePresence Call Termination


Cisco 7970G
Primary Codec
Primary
CUCM
M
Primary Codec
Primary
Cisco 7970G
IP
XML "HANGUP"
SIP "BYE"
SIP "BYE"
XML "HANGUP"
SIP "200 OK"
SIP "200 OK"
RTP Media Stops (Audio + Video)
Signaling
Media
Note: Signaling has been simplified for the purpose of this figure.
There are many other XML and SIP messages which are not shown.
220214

To make the SIP signaling easier to understand, it has again been greatly simplified in Figure 7-6. Call termination begins when the end user at one end of a TelePresence meeting uses the touch-screen user interface of the 7970G IP phone to end the meeting. This causes the 7970G IP phone to send an XML message to the TelePresence Codec, instructing it to hang up the call by generating a SIP BYE message. The SIP BYE message is sent to CUCM, which then generates a new SIP BYE message to the remote TelePresence Codec. The remote TelePresence Codec informs the 7970G phone at the remote site that the call is terminating. Upon receipt of the SIP 200 OK messages from the TelePresence Codecs, the audio and video media streams stop.

Since CUCM functions as a B2BUA which maintains state of all SIP calls initiated and terminated through it, it can capture call detail records of when TelePresence meetings start and stop. This may be necessary for management systems and for billing charges for TelePresence meetings back to individual departments.

Firewall and NAT Considerations

TelePresence embeds the audio and video media endpoint addresses within the SIP call signaling messages. This has implications for firewalls and network address translation. For a firewall to determine the IP addresses and ports to dynamically open to allow the audio and video media through, the firewall may need to monitor the SIP signaling flow. Also, any IP address translation within the network may pose a problem, since the addressing received by the remote TelePresence device may not represent a routable IP address to the routers and Layer 3 switches at the remote site. Therefore, for Release 1.0 of the Cisco TelePresence solution, it is assumed and recommended that no address translation devices or firewalls exist between TelePresence endpoints.

CHAPTER 8

Capacity Planning and Call Admission Control

Overview

The Cisco TelePresence suite of virtual meeting solutions supports three different types of meetings which may be implemented within the Intra-Enterprise Deployment Model:

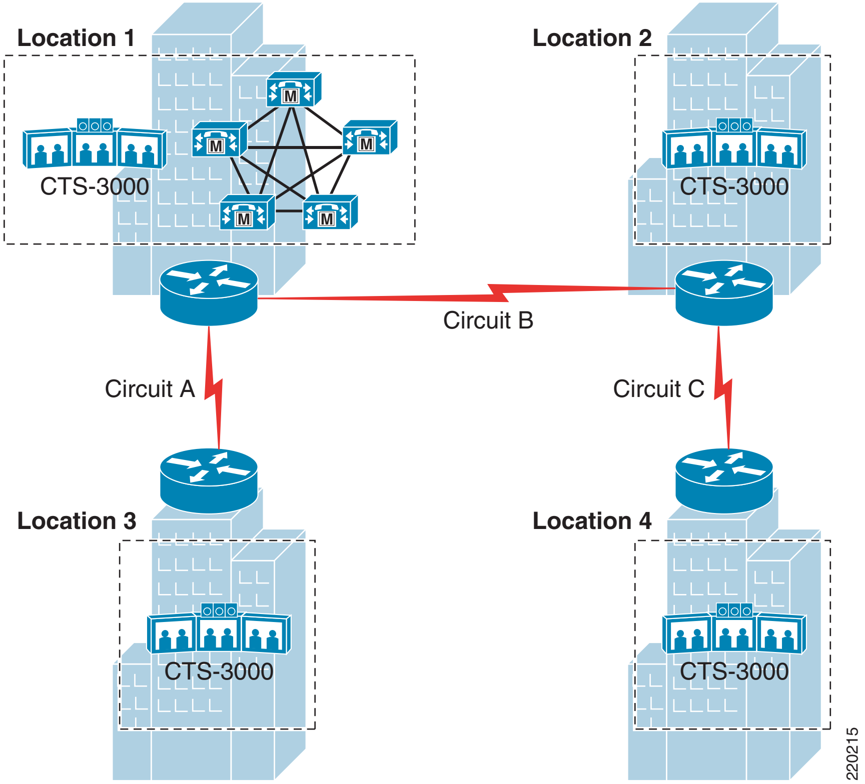
- Ad hoc meetings—An end-user simply dials the extension of the Cisco TelePresence system at the other end through the 7970G IP phone that functions as the user interface to the Cisco TelePresence system. There is no scheduling involved.
- Permanent meetings—Remain up at all times. An example of a permanent TelePresence meeting is the use of a remote receptionist. Also, in scenarios where there are only two TelePresence systems deployed and they are heavily used, it may be desirable to simply leave the meeting up continuously.
- Scheduled meetings—Scheduled in advance of the meeting through the company's groupware application (e.g., Microsoft Exchange/Outlook).

With the current release of the Cisco TelePresence Solution, there is no automated mechanism for reserving network bandwidth or performing call-by-call Call Admission Control (CAC). Therefore, if the number of TelePresence rooms deployed at a given site exceed the bandwidth available to/from that site, it is possible that too many TelePresence meetings could occur simultaneously and QoS policies in the network will begin dropping TelePresence packets, resulting in poor audio and video quality for all calls traversing that network link. Existing CAC techniques, which are Locations-based CAC or Resource ReserVation Protocol (RSVP), both of which are administered by Cisco Unified Communications Manager (CUCM), are not recommended or supported for Cisco TelePresence. Therefore, the current recommendation is to use manual capacity planning to provide sufficient bandwidth to support all possible TelePresence meetings simultaneously occurring across the network infrastructure. However, due to the limitations of this approach, more advanced CAC mechanisms for TelePresence are being developed and evaluated.

Manual Capacity Planning

Manual capacity planning relies on having sufficient bandwidth within the network to support all possible TelePresence meetings occurring simultaneously and so guarantee 100% call completion. Since all TelePresence meetings are always allowed onto the network, this technique may also be referred to as having no CAC. The physical topology of the network infrastructure impacts how much and where bandwidth needs to be provisioned. Figure 8-1 shows an example of this technique with four locations in a partially-meshed network topology.

Figure 8-1 Bandwidth Provisioning Example



One technique for determining the amount of bandwidth required across each circuit is to simply list all possible combinations of simultaneous TelePresence meetings between locations and the number of meetings each circuit must handle, as shown in Table 8-1.

Table 8-1 Circuit Requirements Example

Meetings Between Locations	Circuit Requirements
Location 1 to Location 2 and Location 3 to Location 4	Circuit A-1 Meeting Circuit B-2 Meetings Circuit C-1 Meeting
Location 1 to Location 3 and Location 2 to Location 4	Circuit A–1 Meeting Circuit B–0 Meetings Circuit C–1 Meeting
Location 1 to Location 4 and Location 2 to Location 3	Circuit A–1 Meeting Circuit B–2 Meetings Circuit C–1 Meetings

However, for the simple network topology shown in Figure 8-1, it is obvious by simply visualizing the network that circuit B must be provisioned with sufficient bandwidth to support two TelePresence meetings, while circuits A and C must be provisioned with sufficient bandwidth to support one TelePresence meeting. Note that for converged networks, this bandwidth is in addition to any other VoIP or video applications, as well as all data traffic. Also, for simplicity, all the devices in Figure 8-1 are shown as CTS-3000 units. The amount of bandwidth required per Cisco TelePresence meeting depends on the Cisco TelePresence system models (CTS-1000 or CTS-3000) involved in the call and the video mode (1080p or 720p) which the units are configured to use. The network administrator must take these issues into consideration when determining the amount of bandwidth that must be provisioned to support TelePresence meetings across the network infrastructure. See Table 4-1 in Chapter 4, "Quality of Service Design for TelePresence" for a detailed list of bandwidth requirements per system type.

The design objective of 100% call completion for all scheduled, ad hoc, and permanent TelePresence meetings is feasible and desirable for current deployments consisting of dozens to hundreds to systems. However, as the number of TelePresence endpoints deployed increases into the hundreds or even thousands, the amount of bandwidth required to support it may become cost prohibitive. Cisco is in the process of addressing this concern by enhancing the CAC mechanisms provided by CUCM (Locations and RSVP) to support TelePresence. This functionality is scheduled for a future release of CUCM. As information about these enhancements becomes available, this document will be revised appropriately.

CHAPTER 9

Call Processing Deployment Models

Overview

For the current release of the Cisco TelePresence Solution and the Intra-Enterprise Deployment Model, a single Cisco Unified Communication Manager (CUCM) cluster is recommended to support all TelePresence devices within the enterprise. TelePresence meetings currently can only be scheduled across a single cluster by the Cisco TelePresence Manager (CTSMGR) scheduling server because CTSMGR only supports a single CUCM cluster. Although devices can register across multiple CUCM clusters, and ad hoc and permanent meetings can be established between clusters, this design is not currently recommended for customers deploying CTSMGR. For customers not deploying CTSMGR, this restriction is not applicable. Furthermore, a future release of CTSMGR is planned to support multiple CUCM clusters, at which point this restriction will be removed.

In addition, in environments where TelePresence is deployed along with other generic Videoconferencing/Video Telephony devices on the same cluster, CUCM cannot instruct Videoconferencing/Video Telephony to use the recommended AF41 QoS marking and TelePresence to use the recommended CS4 QoS marking. The marking of audio and video traffic by CallManager is handled at the cluster level and not at the device level, because the marking of audio and video traffic is a cluster-wide (i.e., global) parameter and CUCM offers only a single parameter for video, which by default is set to AF41. For this reason it is recommended that TelePresence be placed on a separate cluster from all other Videoconferencing / Video Telephony applications. Finally, Cisco TelePresence requires CUCM release 5.1.1 or higher, with version 5.1.2 recommended to support the Auto Collaborate endpoint feature of TelePresence. Therefore, to summarize the guidance based upon the above three criteria, if a customer has a single existing cluster running version 5.1.1 or higher deployed for IP telephony and has no other Videoconferencing/Video Telephony devices, it is acceptable to integrate TelePresence devices onto that cluster. However, since the vast majority of deployments are not expected to meet these criteria, it is recommended that a separate CUCM cluster be deployed to support TelePresence and the guidance contained in this document is based upon that approach.

Dial-Plan Recommendations

For the current release of TelePresence, it is recommended that the Cisco Unified 7970G IP phones that serve as the user interface to the Cisco TelePresence system endpoints be marked to indicate that they should not be used for emergency services calls. A separate IP Phone registered to the production IP Telephony CUCM cluster should be deployed in the same room to provide access to emergency services.

To support functionality such as the ability to bridge audio participants into the TelePresence meeting via the audio add-in feature of the TelePresence System, the CUCM cluster which supports the TelePresence deployment may require additional components: either one or more voice gateways connecting the TelePresence CUCM cluster to the customers PBX or to the PSTN, and/or one or more Inter-Cluster Trunks (either H.323 or SIP) between the TelePresence CUCM cluster and the existing IP Telephony CUCM cluster(s).

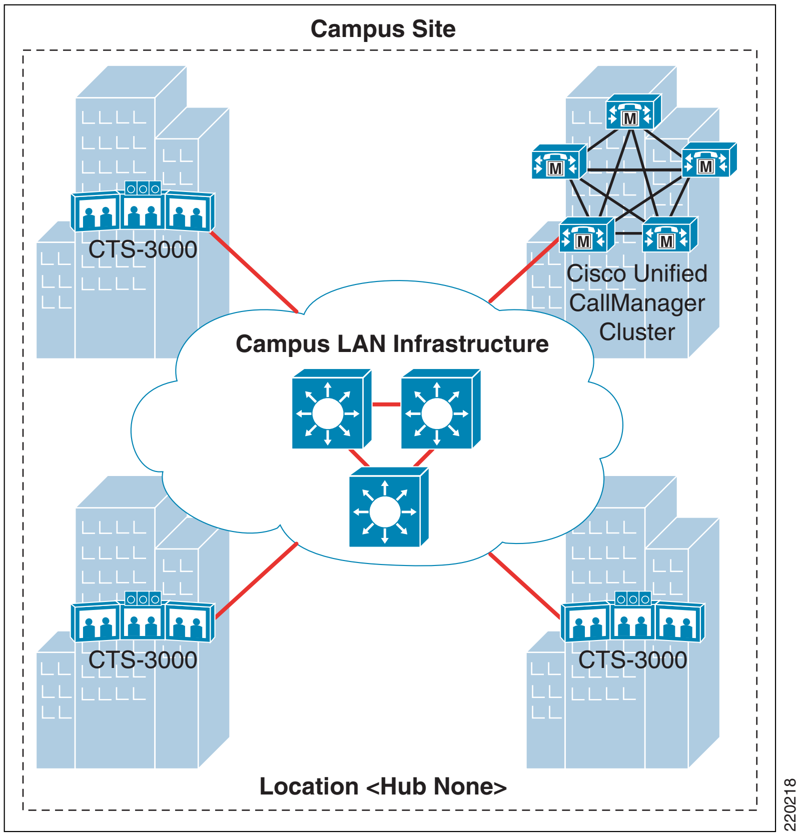
In either scenario, the TelePresence dial plan must be selected carefully and call routing set up appropriately to allow the TelePresence systems to reach and to be reached by other phones, audio conferencing bridges, and the PSTN. Therefore, the dial plan, Directory Numbers, Partitions, and Calling Search Spaces allocated to the TelePresence systems should be consistent with the rest of the enterprise to provide full support for current and future capabilities.

All current TelePresence deployments use either a single-site call processing model or a multi-site WAN with centralized call processing model. In both of these models, the CUCM cluster which supports the TelePresence devices resides at one location, such as a main campus. All communications with devices at remote locations takes place over the IP network infrastructure.

Single-Site Call Processing Model

The single-site call processing model applies to Cisco TelePresence deployments within a single campus and to deployments across MANs with LAN speed (i.e., Gigabit Ethernet) connectivity between sites. Figure 9-1 shows an example of this deployment model.

Figure 9-1 Cisco TelePresence Single-Site Deployment

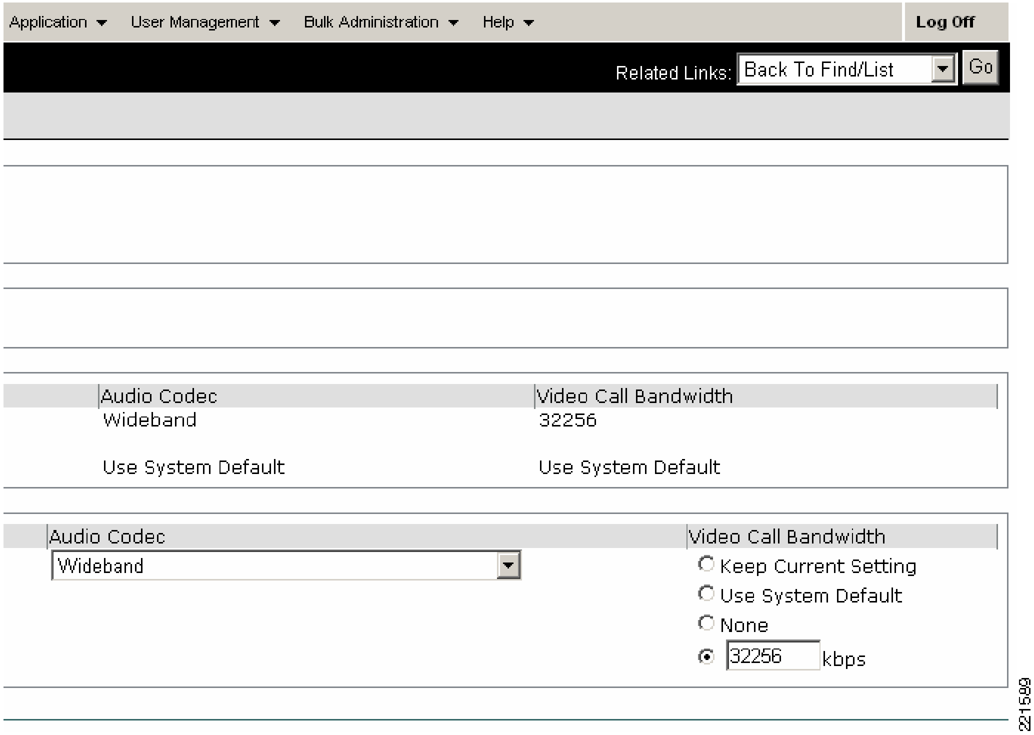


Call Admission Control

In a single-site design, it is assumed that a high-speed LAN provides connectivity between all devices. CAC is typically not an issue, since the LAN can easily be scaled to provide sufficient bandwidth to simultaneously support all possible TelePresence meetings. TelePresence devices can be left within the default Hub_None location within the CUCM configuration, which provides no bandwidth restrictions on the total amount of video and audio traffic.

The region settings within the CUCM configuration are used to control the audio codec and the amount of video bandwidth used per call within a region and between regions. Since there are no other video devices in a standalone TelePresence deployment, all TelePresence devices can be placed in a single region. The region should be configured for AAC/Wideband audio (which as of release 5.1.1 of CUCM permits up to 256 Kbps of audio per call) and a video bandwidth of at least 12500 Kbps (12.5 Mbps). As of release 5.1.1 of CUCM, the maximum video bandwidth permitted is 32,256 Kbps. These settings are illustrated in Figure 9-2.

Figure 9-2 Recommended CUCM Region Settings for TelePresence



Audio Codec	Video Call Bandwidth
Wideband	32256
Use System Default	Use System Default

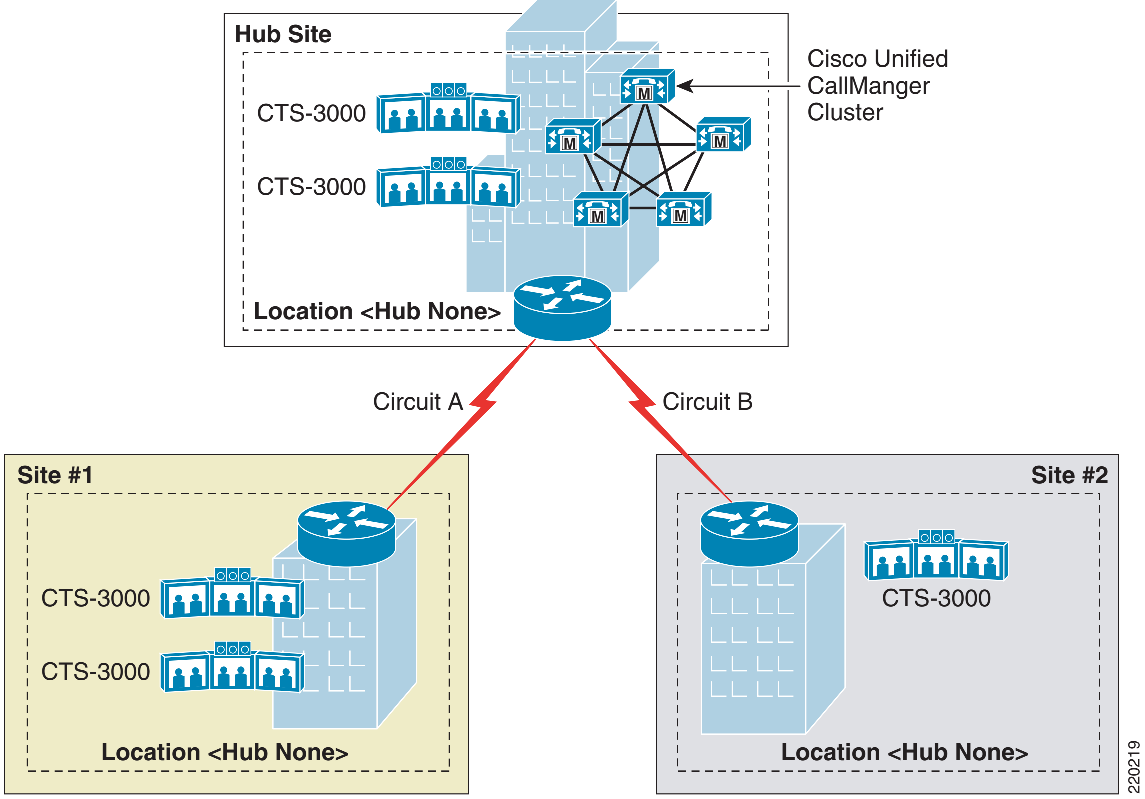
Audio Codec: Wideband

Video Call Bandwidth:
○ Keep Current Setting
○ Use System Default
○ None
● 32256 kbps

Multi-Site WAN with Centralized Call Processing Model

In a multi-site WAN with centralized call processing model, a single CUCM cluster is deployed at a central site. This acts as the call processing agent for TelePresence devices both at the local and remote sites. Figure 9-3 shows an example of this deployment model over a hub-and-spoke network topology.

Figure 9-3 Cisco TelePresence Multi-Site Deployment

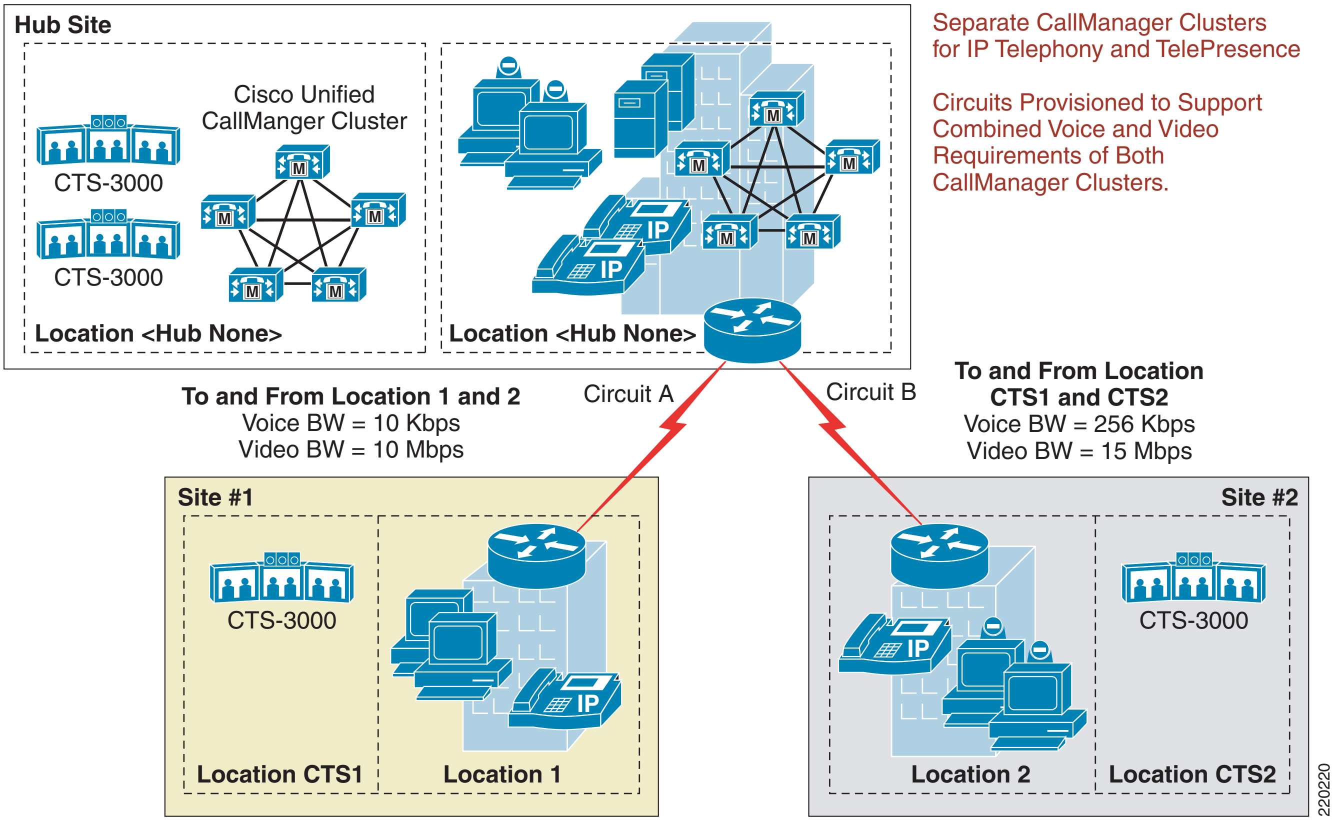


Call Admission Control

For current TelePresence deployments it is recommended that sufficient WAN bandwidth be provisioned to support all possible simultaneous meetings within the network. Refer to Chapter 8, "Capacity Planning and Call Admission Control" for details regarding the use of manual capacity planning to guarantee 100% call completion. For this design, all TelePresence devices can be left in the default Hub_None location which provides no bandwidth restrictions on the total amount of video and audio traffic (as shown above). Alternatively, TelePresence devices at each remote site can be assigned to a different location and the video and audio bandwidth between locations set to unlimited.

When implementing Cisco TelePresence alongside an existing CUCM deployment dedicated for IP telephony, the WAN circuits must be provisioned with sufficient bandwidth to take into account the CAC requirements of both CUCM clusters. An example of this is shown in Figure 9-4.

Figure 9-4 Separate Cisco Unified CUCM Design Example



As can be seen in Figure 9-4, separate CUCM clusters are deployed for TelePresence and for IP telephony (both dashed boxes). Each CUCM configuration has a different location configured for each remote site with a certain amount of bandwidth configured between each location for audio and video. In this scenario, the WAN circuits must be provisioned to accommodate the aggregate bandwidth pools configured in both CUCM clusters, since they operate independently of each other. Otherwise, the potential exists for oversubscribing the circuits and degrading the quality of voice, desktop video, and TelePresence meetings.

It should also be noted that the Survivable Remote Site Telephony (SRST) feature of Cisco router platforms do not currently support Cisco TelePresence system devices. Therefore in a multi-site WAN with a centralized call processing TelePresence design, SRST cannot be used to provide redundancy if the connection to the TelePresence CUCM cluster fails. However in the design shown in Figure 9-4, where a separate CUCM cluster is deployed for IP telephony devices, SRST works well for the IP phones and other devices which are supported.