| Solutions | Products | Ordering | Support | Partners | Training | Corporate |

Tech Notes

Implementing QoS Solutions for H.323 Video Conferencing over IP

Document ID: 21662

Help us help you.

Please rate this document.

○ Excellent

○ Good

○ Average

○ Fair

○ Poor

This document solved my problem.

○ Yes

○ No

○ Just browsing

Suggestions for improvement:

(256 character limit)

Send

Contents

Introduction

H.323 is the standard with global acceptance for multimedia conferences in an IP network. This document discusses tools to implement Quality of Service (QoS) for H.323 video conferences over an enterprise WAN with relatively low-speed links.

Prerequisites

Requirements

Readers of this document should have knowledge of these topics:

- The components of an H.323-compliant system. Components include, but are not limited to, terminals, gateways, gatekeepers, multipoint controllers (MCs), multipoint processors (MPs), and multipoint control units (MCUs). Refer to White Paper: Deploying H.323 Applications in Cisco Networks for more information.

- Cisco H.323 video conference solutions, which include MCUs and gateways as well as the Multimedia Conference Manager (MCM) gatekeeper and proxy. See the Related Information section of this document for links to information on Cisco video conference solutions.

- H.323 zone designs. The group of H.323 endpoints occurs in zones, which are administrative conveniences similar to a Domain Name System (DNS). Each zone has one gatekeeper that manages all endpoints.

- Dialing plans. Refer to *Chapter 5: Dial Plan Architecture and Configuration* of Cisco AVVID Solution, IP Telephony: Cisco CallManager Release 3.0(5) for more information.

- Call Admission Control (CAC) techniques, which include signaling of resource requirements via Resource Reservation Protocol (RSVP).

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Background Information

Most networks today support one or more of these video traffic types:

Video Type	Traffic Characteristics
Video conference	Live, two-way, small groups bandwidth: One or more streams per user
Video on demand	One-way, point-to-point (pull model) bandwidth: One stream per user
Broadcast video (scheduled)	One-way, one-to-many (push model) bandwidth: One stream to unlimited users (IP multicast)

At the same time, many enterprises examine the existing and often separate data, voice, and video network infrastructures to determine the most efficient ways to bring these networks together across an IP infrastructure. In these converged networks, QoS is mandatory at any potential congestion point in the network. QoS ensures that delay- and drop-sensitive traffic, real-time video, and voice pass through unimpeded, relative to the drop-tolerant data applications. In particular, QoS is crucial at the WAN edge router. There, hundreds of megabits of potential traffic aggregate into slower-speed links in the kilobits or low megabits-per-second range.

H.323

Many IP video conference applications use the H.323 suite of protocols. The International Telecommunications Union (ITU) H.323 defines an international standard for multimedia over IP. ITU approved the first version of the H.323 standard in 1996. The current version is 4. Many applications now commonly deploy LAN-based H.323 video systems. An example application is Microsoft NetMeeting, which utilizes H.323 for video conference and shared collaboration.

Previously, video conference systems with H.320 as a basis were common. Each system had its own Public Switched Telephone Network (PSTN) connection. As the left side of the figure in this section shows, today you can use video gateways for communication between the converged H.323 network and the legacy video network. The right side of the figure shows how you can use video terminal adapters to link individual H.320 endpoints seamlessly in an H.323 network.
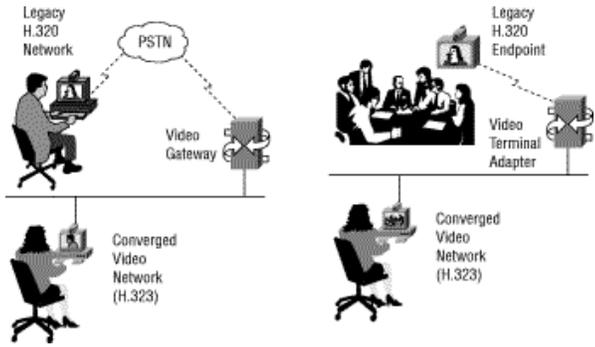
Characterization of Video Conference Traffic

Unlike voice, video has a very high and extremely variable packet rate with a much higher average maximum transmission unit (MTU). This figure illustrates a typical packet size breakdown of video conference traffic:
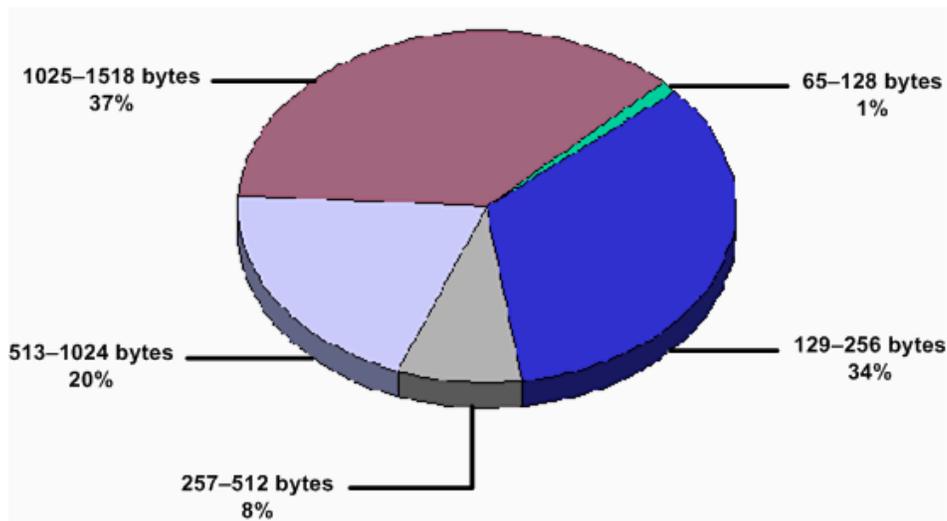
A stream of video conference traffic consists of two types of frames, as this figure illustrates:
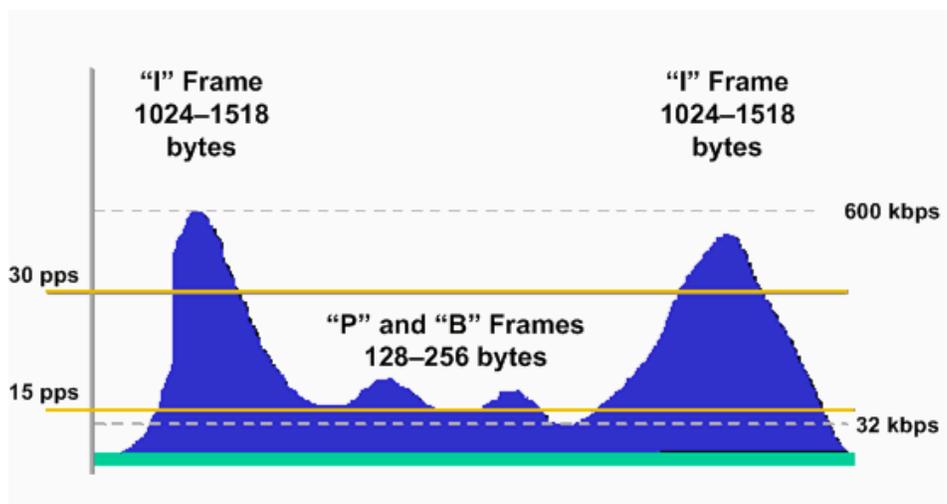
The "I" frame is a full sample of the video. The "P" and "B" frames use quantization via motion vectors and prediction algorithms.

Capacity Planning

Before you place video traffic on a network, ensure that adequate bandwidth exists for all necessary applications. First, calculate the minimum bandwidth requirements for each major application, for example, voice, video, and data. The sum represents the minimum bandwidth requirement for any specific link. This amount should consume no more than 75 percent of the total bandwidth available on that link. This 75 percent rule assumes that some bandwidth is necessary for overhead traffic. Examples of overhead traffic include routing protocol updates and Layer 2 keepalives, as well as additional applications, such as e-mail and HTTP traffic. Have voice and video traffic occupy no more than 33 percent of link capacity. This Example Scenario explains capacity planning on a converged network.

Example Scenario

A site has a link capacity of 1.544 Mbps and contains two video terminals that support a maximum data rate of 256 kbps each. Although the rate of the two video calls equals 512 kbps, add 20 percent to the data rate of the call to account for overhead. Twenty percent is a conservative percentage that ensures proper capacity planning in most environments. You can start with an extra 20 percent for overhead and then adjust this value, higher or lower, with the results of your monitor as a basis.

Provision the priority queue for sufficient bandwidth to allow both video terminals to have an active call across the WAN simultaneously without the possibility of an overrun of the priority queue. In this example scenario, if you add a third video terminal, you need to implement some form of CAC.

Determine Per-Call Bandwidth Consumption

With capacity planning, one of the most critical concepts to understand is how much bandwidth you use for each call. This section lists the bandwidth that each coder-decoder (codec) uses. Refer to Voice over IP - Per Call Bandwidth Consumption for more information.

H.323 Audio

Audio signals contain digitized, compressed sound (usually speech). H.323 supports proven ITU-standard audio codec algorithms. The algorithms with support include:

- G.711—3.1 kilohertz (kHz) at 48, 56, and 64 kbps (normal telephony)

- G.722—7 kHz at 48, 56, and 64 kbps

- G.728—3.1 kHz at 16 kbps

- G.723—5.3 and 6.3 kbps modes

Selection of the right codec reflects tradeoffs between speech quality, bit rate, compute power, and signal delay.

H.323 Video

According to the H.323 standard, video capabilities in H.323 terminals are optional. However, when you implement the H.323 terminals, the terminals must support the H.261 codec, with optional support for the H.263 standard.

- H.261—Video codec for audiovisual services at multiples of 64 kbps. H.261-compliant devices fully encode initial frames. The devices then code only the differences between the initial and subsequent frames for minimal packet transmissions. Optional motion compensation improves image quality.

- H.263—Video codec for video plain old telephone service (POTS). The H.263 standard is a backward-compatible update to the H.261 standard. H.263 significantly enhances picture quality with a half-pixel motion estimation technique, which is a requirement. Enhancements also come from predicted frames and a Huffman code table, with optimization for low bit-rate transmissions. The H.263 standard defines five standard picture formats, as Table 1 shows in the document White Paper: Deploying H.323 Applications in Cisco Networks.

Classification

To provide the appropriate QoS guarantees to video traffic, network devices need to be able to identify such traffic.

The differentiated services (DiffServ) model of QoS uses DiffServ code point (DSCP) values to separate traffic into classes. DiffServ defines these two sets of DSCP values:

- Expedited Forwarding (EF)—Provides a single DSCP value (101110) that gives marked packets the highest level of service from the network. Cisco implements EF service via low latency queueing (LLQ). Generally, EF keeps the high-priority queue very small to control delay and to prevent starvation of lower-priority traffic. As a result, packets can drop, if the queue is full. Usually, EF is most appropriate for VoIP.

- Assured Forwarding (AF)—Provides four classes, each with three drop precedence levels.

For more information on DSCP, refer to Implementing Quality of Service Policies with DSCP.

Generally, Cisco design guides recommend AF41 (DSCP value 100010) for video. There is no advantage if you treat the audio portion of the video streams better than the video packets in an IP video conference application. Therefore, use AF41 as the DSCP value for both voice and video media in a video conference.

At Layer 2, you can use the 3 class of service (CoS) bits in the IEEE 802.1p field, which is part of the IEEE 802.1Q tag.

Currently, there are no standards that describe which value is most appropriate for IP video conference. However, Cisco normally recommends this marking scheme for multiservice networks:

Traffic Type	Layer 2 CoS	Layer 3 IP Precedence	Layer 3 DSCP
Voice RTP[1]	5	5	EF
Voice control	3	3	AF31
Video conference	4	4	AF41
Streaming video (IP/TV)	1	1	AF13
Data	0-2	0-2	0-AF23

[1] RTP = Real-Time Transport Protocol

This table assigns streaming video and video conference separate classification and marking values. Streaming video has a better ability to buffer streams and deal with delay and jitter. Therefore, streaming video requires different QoS levels.

In addition, you can separate the control and data portions of the video conference streams. To separate these two portions of the streams, mark control with AF31 and data with AF41. However, this design is not the best design. Not all endpoints allow you to mark bearer and control traffic differently, and a Cisco Proxy marks all video conference traffic with one value. In addition, control traffic bit rates are negligible, relative to the video call bit rates.

Perform classification as close to the source as possible. Third-party video partners VCON, PictureTel, and Polycom can set the IP precedence bits. If your H.323 terminal does not set any header values, you can mark the packets at these points in the network:

- A Layer 3 switch port

  Refer to Configuring QoS for more information.

- A Cisco IOS® router that uses class-based marking

  Refer to Configuring Class-Based Packet Marking for more information.

- A Cisco IOS router that uses the Cisco MCM feature

- An H.323 gatekeeper/proxy that runs on a remote WAN router

Select a Fancy Queuing Mechanism

Cisco IOS Software now includes several queueing mechanisms. These mechanisms meet the needs of the type of traffic that enters the network and the wide-area media that the traffic traverses. On either the campus or the WAN, any time there is a potential congestion point in the network, the application of proper queuing techniques is necessary. The queue ensures that delay- and drop-sensitive traffic, such as voice and real-time video, pass through unimpeded, relative to the drop-tolerant data applications. An interruption is typical at the WAN edge router. There, hundreds of megabits of potential traffic aggregate into slower-speed links in the kilobits or low megabits-per-second range.

Configure the newer queue methods with the commands of the modular QoS command-line interface (CLI) (MQC). With the MQC, specify a minimum bandwidth guarantee with the **bandwidth** command. Specify strict priority dequeueing to the interface level queue with the **priority** command. The **bandwidth** command implements class-based weighted fair queueing (CBWFQ), and the **priority** command implements LLQ. Refer to Comparing the bandwidth and priority Commands of a QoS Service Policy for more information.

Model/Prioritization Scheme

Cisco recommends this model or prioritization scheme on a multiservice network:

Data Link Type	Minimum Cisco IOS Software Release	Classification	Prioritization	LFI[1]	Traffic Shaping
Serial lines	Cisco IOS Software Release 12.0(7)T	DSCP = EF for voice; DSCP = AF41 for all video conference traffic; DSCP = AF31 for voice control traffic; other classes of traffic have a unique classification.	LLQ with CBWFQ	MLP[2]	—
Frame Relay	Cisco IOS Software Release 12.1(2)T	DSCP = EF for voice; DSCP = AF41 for video; DSCP = AF31 for voice control traffic; other classes of traffic have a unique classification.	LLQ with CBWFQ	FRF.12	Shape traffic to CIR[3].
ATM	Cisco IOS Software Release 12.1(5)T	DSCP = EF for voice; DSCP = AF41 for video; DSCP = AF31 for voice control traffic; other classes of traffic have a unique classification.	LLQ with CBWFQ	MLP over ATM	Shape traffic to guaranteed portion of bandwidth.
		DSCP = EF for voice; DSCP = AF41 for		MLP	Shape

ATM and Frame Relay	Cisco IOS Software Release 12.1(5)T	video; DSCP = AF31 for voice control traffic; other classes of traffic have a unique classification.	LLQ with CBWFQ	over ATM and Frame Relay	traffic to guaranteed portion of bandwidth on slowest link.

[1] LFI = Link Fragmentation and Interleaving

[2] MLP = multilink PPP

[3] CIR = committed information rate

This list explains some key points of the model/prioritization scheme.

- Voice enters a queue with priority queuing (PQ) capabilities and receives a bandwidth of 48 kbps. The entrance criterion of this queue is the DSCP value of EF, or an IP precedence value of 5. Traffic in excess of 48 kbps drops if there is interface congestion. Therefore, use an admission control mechanism to ensure that traffic does not exceed this value.

- Video conference traffic enters a queue with PQ capabilities and receives a bandwidth of the call data rate plus 20 percent. The entrance criterion to this queue is a DSCP value of AF41, or an IP precedence value of 4. Traffic in excess of the call data rate drops if there is interface congestion. Therefore, as in the case of voice, you **must** use an admission control mechanism to ensure that traffic does not exceed this value. Use the proxy for queue access, particularly if you have not configured trust on every switch port. For queue access at small sites with only a few video terminals, use access control lists (ACLs) with the video terminal IP address as a basis. The use of ACLs protects against rouge users who mark traffic with IP precedence 4. This mark bypasses the gatekeeper, or CAC, and affects all the video in the PQ.

  Note: One-way video traffic, such as IP/TV, should use CBWFQ via the **bandwidth** command. The delay tolerances are higher.

- The congestion of the WAN links can completely starve the voice control signaling protocols. In this case, the IP phones cannot complete calls across the IP WAN. Voice control protocol traffic, such as H.323 and the Skinny Client Control Protocol, requires its own class-based weighted fair queue with a minimum configurable bandwidth equal to a DSCP value of AF31. This DSCP value correlates to an IP precedence value of 3.

- Systems Network Architecture (SNA) traffic enters a queue with a specified bandwidth of 56 kbps. The queueing operation within this class is FIFO, with a minimum bandwidth allocation of 56 kbps. Traffic in this class that exceeds 56 kbps enters the default queue. The entrance criterion to this queue can either be TCP port numbers, a Layer 3 address, IP precedence, or a DSCP.

All traffic that remains can enter a default queue. If you specify a bandwidth, the queuing operation is FIFO. Alternatively, if you specify the keyword fair, the operation is weighted fair queuing (WFQ).

In addition, do not video conference on link speeds of less than 768 kbps. On low bit-rate links, the use of compressed RTP (cRTP) and LFI can reduce the effects of serialization and queueing delay.

Do not use cRTP with IP video conferences. This list provides best practices for cRTP:

- Use cRTP only with low bit-rate voice codecs, such as G.729. If you use G.711 as the audio codec for a voice or video conference call, the statistical throughput gains that you achieve with cRTP are not significant enough to merit use of cRTP.

- Use cRTP only when low bit-rate voice is a significant percentage of the offered load. In general, this feature is only beneficial when low bit-rate voice is greater than 30 percent of the offered load to a circuit.

- cRTP can affect forwarding performance. Monitor CPU utilization when you have enabled the feature.

Should Voice and Video Share LLQ?

A frequent consideration with multiservice QoS service policies is whether to configure voice and video conference traffic as priority classes. This consideration comes from the fact that LLQ presently supports a single strict-priority queue, even when you have configured multiple classes for prioritization. When you configure the VoIP and video classes with priority, the traffic from both of these classes goes into a single queue. Therefore, these reasons can cause you to choose not to place video in the priority queue:

- Video packets are much larger than voice packets. Video packets are usually as large as the maximum link MTU size. With the EF mark, video packets can enter the same priority queue as voice. If a small VoIP packet enters the queue behind a large video packet, or behind several such packets, the delay in the VoIP packet increases. The delay can be substantial, and it adversely affects the performance of VoIP applications.

- Because most EF queues are very small, they can lead to packet drop when you use them for video traffic.

Cisco has performed tests that placed video in the priority queue. The tests were with link speeds greater than 768 kbps and with proper CAC to avoid oversubscription. Cisco found that the placement of video in the priority queue did not introduce a noticeable increase in delay to the voice packets.

In general, you can select one of these models. Cisco has tested both models:

- Voice, video, and audio in the priority queue and provision appropriately

- Voice in the priority queue, with video and audio in a bandwidth queue

A third approach is to separate the audio component of the video conference. In other words, place the audio component in the priority queue and the video component in a bandwidth queue. However, video coders tend to have longer coding delays than voice coders. Therefore, if you give the audio streams of a video conference absolute priority, the audio streams arrive early and are held in order to achieve lip sync. So, there is no advantage if you place voice packets associated with a video conference in a queue with better service than the service that the video packets receive.

If you choose to place video and voice in the priority queue, mark the traffic types with different DSCP values. If you mark the traffic types with different DSCP values, you can use a different priority statement in your QoS service policy to control video. In particular, video can require a larger burst parameter.

CAC

The prioritization of traffic only solves part of the challenge of QoS provision for video over IP. A complete solution requires CAC.

CAC, or bandwidth control, is necessary to avoid the oversubscription of network resources. With video conferencing, a rejection of a video terminal that requests network resources is necessary to maintain the quality of existing video streams if the new terminal exceeds the available bandwidth. In other words, CAC protects video from video.

In general, there are three schemes for CAC provision for video calls:

- Limit the number of video terminals. In particular, at remote sites without an H.323 gatekeeper, there is only one way to control the use of bandwidth for video across a particular link, such as a WAN. In this case, you need to physically limit the number of video terminals at remote sites. Provision sufficient bandwidth in the priority queue to support the maximum data rate of all video endpoints at a particular site.

  Note: Provision the priority queue for the maximum data rate of the video terminals plus 20 percent. The additional 20 percent allows for IP and transport overhead.

- Use gatekeeper CAC to set bandwidth limits for interzone and intrazone calls on a per-session basis. You can combine gatekeeper CAC with a proxy, which provides a single access point into the priority queue. This single access point prevents an oversubscription of the priority queue by unauthorized video streams. You must register video terminals with the gatekeeper to obtain access to the proxy. The gatekeeper configuration allows a maximum video bandwidth outside the local zone. This maximum bandwidth needs to match the bandwidth provision of the priority queue to ensure

proper queueing functionality. These guidelines apply only to hub and spoke environments. Gatekeepers use direct mode and do not allow intermediate gatekeepers to deduct bandwidth from links.

- Implement endpoints for which you have enabled RSVP. The endpoints use RSVP messages to describe the traffic profile and request the necessary service. RSVP-aware network devices along the end-to-end path read these RSVP messages and decide whether to grant or deny the reservation request. The devices communicate their decision to the endpoint via another RSVP message. The endpoint and its application then decide whether to adapt to the available network conditions through a discontinuation of the conference or a reduction of the requirements.

Appendix II of the H.323 version 4 standard outlines an approach for the use of RSVP. The main points are:

- When you place a call, an endpoint communicates the ability of the endpoint to reserve resources to the gatekeeper. The gatekeeper then indicates whether an endpoint resource reservation attempt is advisable.

- During the H.245 phase, the endpoints indicate whether they can signal resource reservations. With this information, the endpoints decide whether to proceed with the call.

- The send of RSVP reservation messages can occur after the open of the logical channels but before the use of the logical channels for data packets.

Traffic Shaping

The use of Frame Relay for WAN connectivity introduces another QoS requirement. Specifically, when a higher-speed central site feeds one or more lower-speed remote sites, the central site can overrun both the physical bandwidth and the CIR bandwidth of the remote site. To prevent the send of too much bandwidth to a remote site, implement traffic shaping on the central-site router. Refer to these resources for more information on Frame Relay traffic shaping:

- Configuring Frame Relay Traffic Shaping on 7200 Routers and Lower Platforms

- VoIP over Frame Relay with Quality of Service (Fragmentation, Traffic Shaping, LLQ / IP RTP Priority)

Interworking with H.323 Terminals

H.323 video conference networks typically consist of five functional components:

- Video terminals

- Gatekeepers

- Gateways

- MCUs

- Proxies

Cisco offers product solutions for all these components, except video terminals. Proof shows that Cisco H.323 products interoperate with third-party H.323 terminals.

In some cases, these terminals offer QoS tools to ensure the satisfaction of the delay and loss parameters of video traffic in the face of unpredictable data flows. For example, the Polycom Viewstation keeps track of all video packets after the establishment of a call. The Polycom Viewstation reports average latency as well as the number of lost video or audio packets. This tool also supports debugs with readable output. These debugs can help indicate the source of a problem that is not detectable through the analysis of the video output. For more information, refer to the document How to Configure Video over IP for Polycom Video Units.

Sample Configuration

This sample configuration demonstrates how to apply LLQ to video conference traffic that traverses a WAN link:

Sample Configuration

```
Sample Configuration
class-map Video-Conf
  match access-group 102
class-map Streaming-Video
  match access-group 103
!
policy-map QoS-Policy
  class Video-Conf
    priority 450 30000
  class Streaming-Video
    bandwidth 150
class class-default
    fair-queue
!
! -- Video-Conf Traffic
access-list 102 permit ip any any dscp cs4
access-list 102 permit ip any any dscp af41
!
! -- Streaming Traffic
access-list 103 permit ip any any dscp cs1
access-list 103 permit ip any any dscp af13
```

After you create a QoS policy map, apply the policy with the **service-policy** command. The type of interface to which you apply the policy determines the places of application of the command. Here are some examples:

Interface Type	Configuration Example
Leased line	`line interface multilink1` `   service-policy output QoS-Policy`

ATM PVC[1]	`interface atm 1/0.1 point`
	`  pvc 1/50`
	`    service-policy output QoS-Policy`

Frame Relay VC[2]	`map-class frame-relay vcofr`
	`   frame cir 128000`
	`   frame mincir 64000`
	`   frame bc 1000`
	`   frame frag 160`
	`   service-policy output QoS-policy`
	
	Note: On the Cisco 7500 series with distributed QoS, use DTS[3] commands. Refer to Frame Relay Traffic Shaping With Distributed QoS on the Cisco 7500 Series.

[1] PVC = permanent virtual circuit

[2] VC = virtual circuit

[3] DTS = distributed traffic shaping

NetPro Discussion Forums - Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums - Featured Conversations for RP
Service Providers: MPLS
Default route in VPN - Mar 3, 2005 Two routers as CPE - Mar 3, 2005

6500 & VRF-Lite - Mar 3, 2005
Is MPLS possible on a 1721? - Mar 3, 2005
MPLS versus Switched network - Mar 3, 2005

Virtual Private Networks: Services

VPN Client not working at remote location - Mar 2, 2005
Trying to find the highest possible MTU - Feb 25, 2005
ISP with QoS - Feb 24, 2005
WRED Maximum-thresholds default value - Feb 20, 2005
831 Dual VPN setup Problem - Feb 18, 2005

Virtual Private Networks: Security

split-tunnel issue - Mar 3, 2005
Cisco IOS/PIX Radius Attributes Doubt - Mar 3, 2005
EZVPN PhaseII NEM - Unable to proceed to ISAKMP Phase II - Mar 3, 2005
Issue in VPN tunnels between 1700 (hub) and 1700 and PIX (spokes) - Mar 3, 2005
Unable to add Cisco VPN 3000 concentrator to CW - Mar 2, 2005

Related Information

- **ITU H.323 Standard**
- **White Paper: Technical Considerations for Converging Data, Voice, and Video Networks**
- **Video Broadcast/Video-on-Demand Product Directions**
- **Cisco IP/TV Video Streaming Applications**
- **Cisco IP/VC Videoconferencing**
- **Call Admission Control for H.323 VoIP Gateways**
- **Internetworking Technology Overview: Quality of Service Networking**
- **QoS Support Page**
- **Technical Support - Cisco Systems**

| Home | How to Buy | Login | Profile | Feedback | Site Map | Help |

Updated: Mar 03, 2005   Document ID: 21662