

California Video Over IP Project - CalVIP

Quality of Service Configuration for TCP/IP Video Conferencing

White Paper

Written by Cassidy D. Smith, PlanNet Consulting
Published on September 2, 2003

Abstract

As the CalVIP project rolls out new H.323 IP Based Videoconferencing technologies, it is important for campuses to ensure quality delivery of this service. This paper discusses Quality of Service (QoS) network configuration practices and includes specific command line examples for Cisco Powered Networks that can be used by campuses and therefore meet that goal.

Note: Do you have the latest version of this document? [Check Here](#)

© 2003 PlanNet Consulting LLC. All rights reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

CONTENTS

INTRODUCTION	1
Scope	1
End-to-End QoS for Video Conferencing	1
CONSIDERATIONS FOR VIDEO CONFERENCING OVER IP	2
QoS issues and Technologies	2
QoS issues	2
QoS enabling technologies	2
Non-QoS issues that can affect quality	3
Cisco MCM Considerations	3
Ethernet Speed and Duplex issues	3
Spanning Tree	3
Codecs	3
Peripherals	3
Firewalls	4
IMPLEMENTING CAMPUS QOS	5
Campus QoS Configuration Recommendations	5
QoS Configuration	5
Access Layer Switches	5
Distribution Layer Switches	6
Core Layer Switches	6
Cisco QoS Configuration	7
Cisco Manual Layer 3 Marking and Classification (Optional)	12
Cisco AutoQOS configuration	13
WAN QOS	13
APPENDIX A – CISCO QOS SAMPLE CONFIGURATION	14
APPENDIX B - REFERENCES	15
CENIC Publications	15
Resources	15
Bibliography	15
For More Information	15
APPENDIX C – GLOSSARY	16
DOCUMENT CONTROL.....	19

INTRODUCTION

The CalVIP Videoconferencing project will be implementing new H.323 technologies to replace the older ISDN/ATM based H.320 technology. Video over IP is sensitive to delay and Jitter that can occur on IP networks. It is important for campuses to ensure quality delivery of this service.

Scope

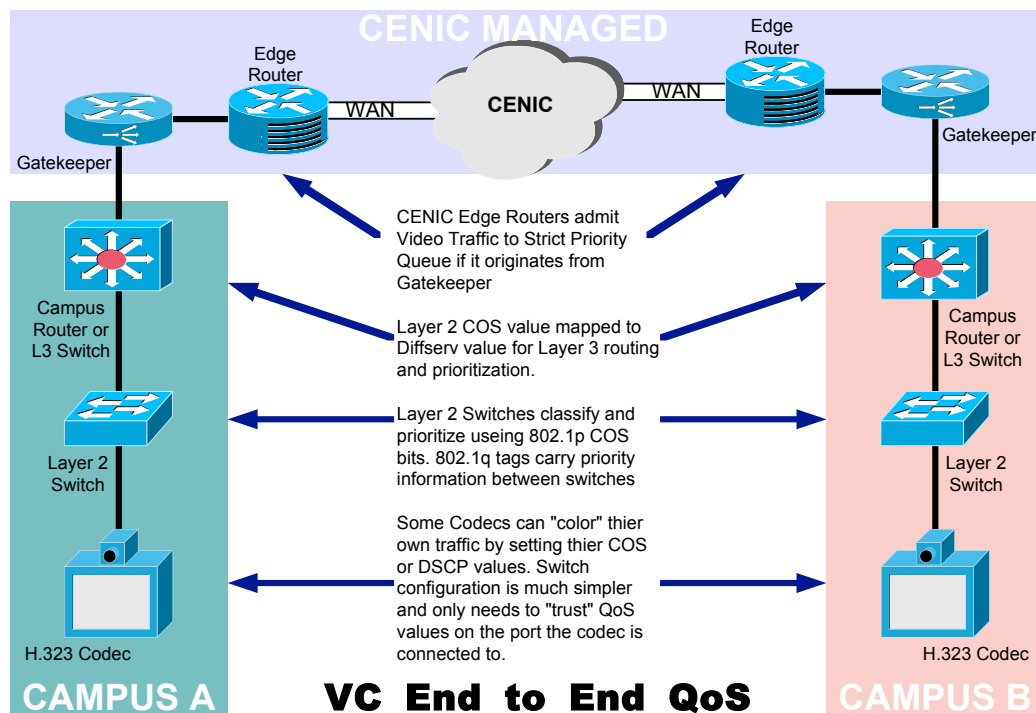
This white paper describes the network configuration requirements to implement End-to-End Quality of Service (QoS) for H.323 Video Conferencing. Some mention of WAN QoS will be made however the CENIC CalVIP operations group provides management of WAN QoS. The gatekeeper is the demarcation point. Campuses will implement QoS within their own Layer 2 and Layer 3 campus network devices.

This paper discusses QoS network configuration practices and includes specific command line examples for Cisco Powered Networks that can be used by campuses and therefore meet that goal.

This paper does not discuss the merits of QoS; it assumes the campus has already decided to implement it and has QoS capable equipment.

End-to-End QoS for Video Conferencing

The following diagram is the basic network architecture that will implement Video Conferencing over IP, and as such it contains the network elements that will need to implement various QoS techniques to ensure End-to-End Quality of Service. The rest of this document will focus on each element and what needs to occur at that point within the network.



CONSIDERATIONS FOR VIDEO CONFERENCING OVER IP

QoS issues and Technologies

While there are QoS issues and technologies the following sections review only the relevant information for the CalVIP project.

QoS issues

The primary issues for Video Conferencing are Available Bandwidth, Packet Loss, Delay and Jitter (Delay Variance). See the Appendices for details.

QoS enabling technologies

Layer 2: Layer 2 frames do not natively have any ability to indicate priority, however you can use the 3 Class of Service (COS) bits in the 802.1p field, which is part of the 802.1q tag, and can be transmitted to other switches via Trunk Ports.

Layer 3: IPv4 packets have always had the ability to indicate priority, in the Type of Service Byte (TOS) 3 bits are used for IP Precedence, the TOS byte has been re-purposed to be used by the DSField that contains the DiffServ Code Point (DSCP), which is a 6 bit value that enables traffic classification. The DSField is backwards compatible with IP Precedence.

Layer 2 and 3 Mapping: Layer 3 DSCP and Layer 2 COS are independent QoS technologies. Mapping is required to preserve quality End-to-End. QoS values are translated between Layer 2 COS values and Layer 3 DSCP values. In table 1 below is an example of what values might be mapped. There is no standard for what priority various traffic types should get; therefore the values in the table are only recommendations.

<i>Traffic Type</i>	<i>Layer 2 CoS</i>	<i>Layer 3 IP Precedence</i>	<i>Layer 3 DSCP</i>	
Reserved	7	7	-	(56)
Reserved	6	6	-	(48)
Voice	5	5	EF	(46)
Videoconferencing	4	4	AF41	(34)
Call Control	3	3	AF31	(26)
High Priority Data/Streaming Video	2	2	AF21	(18)
Medium Priority Data	1	1	AF11	(10)
Best Effort Data	0	0	BE	(0)

Table 1.

Non-QoS issues that can affect quality

Cisco MCM Considerations

The H.323 Gatekeeper will consist of a Cisco Router with several 10/100 Ethernet ports and 1 1000BaseT copper GigEthernet port. The router will run MCM software to perform the gatekeeper function for Campuses. The MCM should be placed near both the network backbone and the CENIC edge router. Ideally the MCM will be directly connected to a core switch and the no more than one hop away from the edge router. If placement is going to be relatively far from a core switch the campus should work with CalVIP Operations to ensure that a GBIC, such as a LX GBIC supporting the longer distance and or single mode fiber is purchased. CalVIP Operations will review any changes or special needs.

Ethernet Speed and Duplex issues

Use a manually set 100Mbps "full-duplex" Ethernet connection. Even just one 384Kbps call on a 10Mbps half-duplex connection produced visible video artifacts, albeit minor. In addition, even when devices are capable of full-duplex, they cannot auto-negotiate correctly, resulting in mismatched duplexes and a failed videoconference. The best way to get reliable quality is to use equipment capable of setting the speed and duplex features manually.

Spanning Tree

Spanning tree convergence time can affect perceived quality by simply being slow to converge after an outage or link change. Every effort should be made to enable faster convergence. Vendors that support RSTP and MST will generally have much faster convergence and therefore video calls can commence faster. For Cisco environments technologies such as, Uplinkfast, MST, and Rapid PVST can be used to shorten convergence time.

Codecs

Not all codecs are created equal; several quality issues can arise from badly performing or non-compliant codecs. Some codecs allow you to hard code the speed and duplex settings for the Ethernet port. Some codecs have the ability to mark their own packets with priority values in either the COS or DiffServ field. Tandberg and Polycom's higher end codecs can do both and also have the ability to hide minor packet loss.

Peripherals

Cameras, Microphones, and Speakers if not working properly can all affect the perceived quality of the Video Conference and should not be overlooked during troubleshooting.

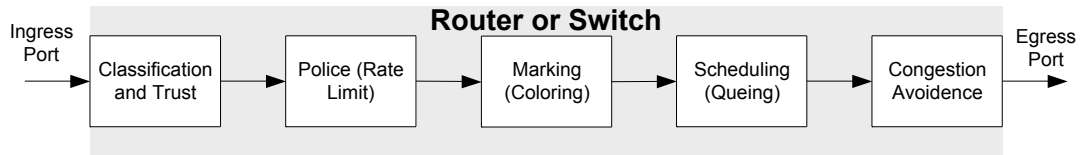
Firewalls

Firewalls only recently began supporting H.323. And while this support is welcome most firewalls introduce considerable delay. At the time of this writing, there none of the major firewall providers support QoS. This means that they have no means of providing preferential treatment to real time traffic. For the highest quality Videoconferencing it is recommended that no firewall be used. Private subnets or VLANs protected by ACL's should provide enough security on the campus side. The gatekeeper has admission control and a proxy function that will only allow the authorized codecs to communicate across the WAN.

IMPLEMENTING CAMPUS QOS

Campus QoS Configuration Recommendations

The QoS operations are based on the DiffServ architecture and use DSCP values internally. This value is determined by an ingress port's "trust" state, and is carried throughout the QoS process. Along its path to an egress port, the DSCP value can be used to Rate Limit, Color, determine queuing priority or traffic shape to avoid congestion. The diagram below shows the basic QoS process flow.



QoS is managed hop by hop or in other words on every device in the communication path. The following sections will discuss manual configuration at layer 2 and Layer 3 boundaries, and will also contain configuration examples that can serve as a starting point for Cisco Powered networks. There are QoS policy tools that allow you to configure multiple devices at a time, but that is beyond the scope of this paper.

Bandwidth: There must be sufficient bandwidth for the overall quantity of traffic, QoS techniques can only manipulate and schedule the usage of that bandwidth.

QoS Configuration

Most campus networks are hierarchal and have three distinct levels of network devices. The levels are the Access, Distribution and Core. They generally physically placed in the IDF, BDF, and MDF respectively. We will follow this hierarchy as we configure QoS.

Access Layer Switches

The access layer is used to connect end user equipment such as Codecs, PC's and IP Phones. The following QoS features can be applied at the Access Layer:

<i>Trust</i>	<i>Untagged Classification</i>	<i>Ingress Policing</i>
<i>Congestion Management</i>	<i>Weighted Round Robin</i>	<i>Egress queue mapping</i>

At the access layer we either want to Trust QoS values coming from the end user device (Codec) or override existing or untagged QoS values. Then we want to schedule or queue the traffic accordingly.

Cisco Access Layer Configuration

See the section entitled "Cisco QoS Configuration" and perform the following tasks:

- Either Trust or Set COS value of 4 on Ports connected to Codecs.
- Trust COS on Trunk uplink ports.
- If available enable WRR egress queuing.
- If Available enable Mapping for COS to "internal" DSCP.
- If Available enable Mapping for COS to Egress Queue.

Distribution Layer Switches

The Distribution layer is used to connect the Access Layer to the backbone network and the Core Switches. The following QoS features can be applied at the Distribution Layer:

<i>Trust DSCP</i>	<i>RE-Classification</i>	<i>Strict Priority Queuing</i>
	<i>Weighted Round Robin</i>	

At the distribution layer we primarily want to Trust DSCP values. Then we want to schedule or queue the traffic accordingly.

Cisco Distribution Layer Configuration

See the section entitled "Cisco QoS Configuration" and perform the following tasks:

- Trust COS on Trunk uplink ports.
- If available enable WRR egress queuing.
- If Available enable Mapping for COS to "internal" DSCP.
- If Available enable Mapping for COS to Egress Queue.

Core Layer Switches

The Core layer is used to connect the Distribution to the rest of the backbone network and the WAN (Edge router and Gatekeeper). The following QoS features can be applied at the Core Layer:

<i>Trust DSCP</i>	<i>RE-Classification</i>	<i>Strict Priority Queuing</i>
<i>Police</i>	<i>Weighted Round Robin</i>	<i>Congestion Avoidance</i>

At the Core layer we primarily want to Trust DSCP values. Then we want to schedule or queue the traffic accordingly.

Cisco Core Layer Configuration

See the section entitled "Cisco QoS Configuration" and perform the following tasks:

- Trust COS on Trunk uplink ports.
- If available enable WRR egress queuing.
- If Available enable Mapping for COS to "internal" DSCP.
- If Available enable Mapping for COS to Egress Queue.

Cisco QoS Configuration

For Cisco example configurations the following legend will explain which commands to use for a given device:

XL	2900XL and 3500XL series with 12.0 Layer 2 IOS
C4	CatOS systems for 4000/4500 with Supervisor 2.
C5	CatOS systems for 2926 and 5000 (With NFFC II) Series.
C6	CatOS systems for 6000/6500
I4	Native IOS Systems for 4000/4500 with SupIII or SupIV.
I2	Native IOS Systems for 2950/3550
I6	Native IOS Systems for 6000/6500.
IOS	Any Generic IOS Routing device

IOS commands with a preceding word in (parentheses) indicate which configuration mode you need to be in.

Enable QoS

XL I2	<i>Enabled by default (3550 must enable like I6 below)</i>
C4/5/6	SET QOS ENABLE
I4	(global) QOS
I6	(global) MLS QOS

Trust

If your codec can set it's own DSCP (34) or COS (4) value, set the port it is connected to for trust. Depending on switch model you may be able to trust DSCP or COS or both, make sure the device on the other end is sending the type you expect to trust. All Trunk or uplink ports should trust

COS, access ports should only trust if the end device (codec) can send a value to be trusted.

XL	<i>Not able to trust port</i>
C4	<i>Beware 4000 CatOS systems trust COS on ALL ports!!</i>
C5	<i>5000 CatOS systems always trust DSCP on all ports, not capable of trusting COS</i>
C6	SET PORT QOS {mod/port} TRUST {trust-cos trust-dscp}
I4	(interface) QOS TRUST {dscp cos}
I2 I6	(interface) MLS QOS TRUST {dscp cos}

Untagged "Default COS"

On the port the Codec is connected to set untagged incoming packets or frames with COS 4 for video conferencing.

XL	(interface) SWITCHPORT PRIORITY DEFAULT COS 4
C4	<i>4000 CatOS systems cannot selectively set COS or DSCP per port, it can only be set globally, which is of little value. Use a downstream switch or the Codec itself to set COS.</i>
C5 C6	SET PORT QOS {mod/port} COS 4
I4	(interface) QOS COS 4
I2 I6	(interface) MLS QOS COS 4

Override

To override existing COS or DSCP values, first complete untagged "default" cos configuration step then set the same port to "override".

XL	(interface) SWITCHPORT PRIORITY override
C4	<i>4000 CatOS systems cannot override.</i>
C5 C6	<i>5000 and 6000 CatOS systems cannot override.</i>
I4	<i>Overrides by default.</i>
I2 I6	(interface) MLS QOS COS override

Layer 2 to 3 Mapping

Configure COS to DSCP mapping to maintain correct priority across layer 2 and 3 domains.

XL	<i>No mapping available</i>
C4	<i>No mapping available</i>
C5	<i>No Mapping available</i>
C6	SET QOS cos-dscp-map 0 10 18 26 34 46 48 56
I4	QOS MAP cos 0 to dscp 0 QOS MAP cos 1 to dscp 10 QOS MAP cos 2 to dscp 18 QOS MAP cos 3 to dscp 26 QOS MAP cos 4 to dscp 34 QOS MAP cos 5 to dscp 46 QOS MAP cos 6 to dscp 48 QOS MAP cos 7 to dscp 56
I2 I6	(global) MLS QOS MAP cos-dscp 0 10 18 26 34 46 48 56

Layer 3 to 2 Mapping (Optional)

Some campus may have H.323 traffic that traverses a Layer 3 border router. The following is an example of a configuration for IOS devices that will Map Layer 3 DSCP values to a layer 2 COS value. In this example only values for H.323 Control, VoIP and Video Conferencing are shown.

IOS	<pre> class-map H323-CONTROL-COS match cos 3 ! class-map H323-VIDEO-COS match cos 4 ! class-map H323-VOICE-COS match cos 5 ! class-map H323-CONTROL-DSCP match ip dscp 26 ! class-map H323-VIDEO-DSCP match ip dscp 34 ! class-map H323-VOICE-DSCP </pre>
-----	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

```

match ip dscp 46
!
policy-map H323-COS-DSCP
class H323-CONTROLL-COS
set ip dscp 26
class H323-VIDEO-COS
set ip dscp 34
class H323-VOICE-COS
set ip dscp 46
class class-default
set ip dscp 0
!
policy-map H323-DSCP-COS
class H323-CONTROLL-DSCP
set cos 3
class H323-VIDEO-DSCP
set cos 4
class H323-VOICE-DSCP
set cos 5
class class-default
set cos 0
!
interface fastethernet x/y.10
encapsulation dot1Q 10
service-policy input H323-COS-DSCP
service-policy output H323-DSCP-COS
!
interface fastethernet x/y.1
encapsulation dot1Q 1 native
end

```

Weighted Round Robin (WRR)

Configure WRR to distribute packets amongst available Queues.

XL	<i>No WRR available</i>
C4	<i>No WRR available</i>
C5	<i>No WRR Available</i>
C6	<i>No Change, use Default.</i>

I4	(interface) tx-queue 3 Priority High
I2	(global) wrr-queue bandwidth 30 50 80 100
I6	<i>No Change, use Default.</i>

Queue Mapping

Map Packets with particular COS or DSCP values to specific egress queues.

XL	<i>Has hard coded COS mappings to High and Low priority queue</i>
C4	SET QOS MAP 2q1t 2 1 COS 4-7
C5	<i>No Change, use Default queue mappings.</i>
C6	<i>No Change, use Default queue mappings.</i>
I4	<i>No Change, use Default queue mappings.</i>
I2	(global) wrr-queue cos-map 1 0 1 (global) wrr-queue cos-map 2 2 3 (global) wrr-queue cos-map 3 4 (global) wrr-queue cos-map 4 5 6 7
I6	<i>No Change, use Default queue mappings.</i>

Cisco Manual Layer 3 Marking and Classification (Optional)

In some cases a campus may not have access switches that are capable of any QOS functions whatsoever, or there is a situation where marking needs to be preformed at a Layer 3 boundary. The following is an example of a configuration for IOS devices that will Mark and Classify as needed.

I2	ip access-list extended H323-TRAFFIC
I4	permit udp any any range 16384 37276
I6	deny ip any any
	!
	ip access-list extended H323-CONTROLL
	permit tcp any eq 1720 any
	permit tcp any any eq 1720
	deny ip any any
	!
	class-map match-all H323-TRAFFIC
	match access-group name H323-TRAFFIC
	class-map match-all H323-CONTROLL
	match access-group name H323-CONTROLL
	!
	policy-map H323
	class H323-TRAFFIC
	set ip dscp 46
	class H323-CONTROLL
	set ip dscp 26
	class class-default
	set ip dscp 0
	!
	interface fastethernet x/y
	service-policy input H323
	!
	interface gigabit x/y
	service-policy input H323
	end

Cisco AutoQOS configuration

Cisco AutoQOS is a relatively new feature that essentially configures all of the above and more for QoS with a few much simpler commands. At the time of this writing only the 2950, 3550, 4000 running IOS and 6500/CatOS 7.5.1 and above support AutoQOS. Native IOS for the 6500 is scheduled to have AutoQOS support by the end of 2003.

<i>Cisco Catalyst 2950E1</i> <i>Cisco Catalyst 3550</i>	<i>Cisco IOS Software Release 12.1(12c)EA1</i>
Cisco Catalyst 4500	Cisco IOS Software Release 12.1(19)E
Cisco Catalyst 6500	Cisco Catalyst Operating System 7.5.1

WAN QOS

As mentioned earlier the WAN is managed by the CENIC and CalVIP operations team. The WAN and each of the campuses or District offices is their own QoS administrative domain. If a campus wants to implement QoS they need to only concern themselves with their own campus. Once this is complete the only question will be whether the other campuses are also implementing QoS. For true End-To-End QoS all parties must have implemented QoS. QoS is cumulative meaning that all improvements are helpful to the final perceived quality.

APPENDIX A – CISCO QOS SAMPLE CONFIGURATION

In the example below most of the non-QoS related items have been removed for clarity. The 4500 and 6500 IOS configurations are similar.

```
2950 version 12.1
hostname TEC-C2950-IDF3
!
wrr-queue bandwidth 30 50 80 100
wrr-queue cos-map 1 0 1
wrr-queue cos-map 2 2 3
wrr-queue cos-map 3 4
wrr-queue cos-map 4 5 6 7
!
mls qos map cos-dscp 0 10 18 26 34 46 48 56
spanning-tree uplinkfast
!
interface FastEthernet0/1
switchport access vlan 2
switchport mode access
mls qos cos 4
mls qos cos override
spanning-tree portfast
!
interface FastEthernet0/2
switchport access vlan 2
switchport mode access
mls qos trust cos
spanning-tree portfast
!
interface GigabitEthernet0/1
description Link from TLB-C6509-MDF-1 3/1
switchport trunk native vlan 900
switchport mode trunk
mls qos trust cos
udld aggressive
!
end
```

APPENDIX B - REFERENCES

CENIC Publications

<http://www.cenic.org/Pubs.html>

Resources

Several Avaya QoS papers are available:

http://www1.avaya.com/enterprise/news/docs/thought_leadership/qos.html

Several Cisco QoS papers are available:

<http://www.cisco.com/go/qos>

Several QoS papers at the H.323 Forum:

<http://www.h323forum.org/papers/>

Packeteer white papers for Video Over IP QoS are available:

http://www.packeteer.com/resources/prod-sol/deploying_videoIP.pdf

http://www.packeteer.com/resources/prod-sol/protecting_videoip.pdf

Several QoS papers for Cisco environments From NetCraftsmen:

<http://www.netcraftsmen.net/technology/QoS/QOS.htm>

Several Published documents are available at the Internet 2 Commons site:

<http://commons.internet2.edu/>

Bibliography

1. Quality of Service - Ferguson and Huston, Wiley, 1998
2. IP Quality of Service - Srinivas Vegesna, Cisco Press, 2001
3. Cisco Catalyst QoS - Flannagan, Froom, and Turek, Cisco Press, 2003
4. Cisco Field Manual: Catalyst Switch Configuration – Hucaby and McQuerry, Cisco Press, 2003
5. Cisco DQOS: Exam Certification Guide – Odom and Cavanaugh, Cisco Press, 2003

For More Information

Additional information about the CalVIP Project is available at the following Web site:

<http://www.csu.net/CALVIP/index.htm>

APPENDIX C – GLOSSARY

Administrative domain: A collection of networks that are under the same administrative control.

Admission Control: This is the mechanism that decides whether the network device has sufficient resources to supply the requested QoS.

Application Quality of Service (AQoS): The facilities provided within an application to provide Quality of Experience to users. Implemented to provide a quality user experience.

ARQ: Address request

Available Bandwidth: The transmission capability. Generally measured in megabits per second (Mbps). Also known as capacity.

Behavior aggregate (BA): A collection of packets with the same DS codepoint crossing a link in a particular direction.

Classifier: An entity that selects packets based on the content of packet headers according to defined rules.

Common Open Policy Service (COPS): Client/Server protocol to support policy control.

Congestion Avoidance: This is a method of predictively managing queues and buffers to avoid congestion on a given link.

DBA: Dynamic bandwidth allocation

Delay: See **Latency**

Differentiated Services Code Point (DSCP): The DSCP is a six-bit field, which spans the fields formerly known as the type-of-service (ToS) fields. It can also refer to the specific value of the DSCP portion of the DS field, used to select a PHB.

DS field: The IPv4 header ToS octet or the IPv6 Traffic Class octet when interpreted in conformance with the definition given in [DSFIELD]. The bits of the DSCP field encode the DS codepoint, while the remaining bits are currently unused.

Echo: A perceptible problem typically in a voice call whereby some of the originating senders voice signal is bounced back to them after a small delay.

Flow: A flow is a set of packets belonging to one instance of the application identified by some combination of source address, source port, destination address, destination port, and protocol identifier.

Global Synchronization: Is a phenomenon that occurs when thousands of TCP flows encounter congestion at approximately the same time and subsequently

back off and go into slow start at the same time. Without intervention the TCP flows will cycle between congestion and back off which is not efficient use of the available bandwidth. RED and WRED are used to eliminate the problem by adding random packet drops when congestion is eminent.

Jitter: The variability in latency between parts of the transmission. Jitter can be measured in various ways (e.g., the difference between the highest latency and the lowest latency, the standard deviation of the latency, the statistical probability of a given delay variance, etc.), so it is often given a qualitative value. Also called delay variation.

Latency: The average time between transmission and reception. Generally measured in milliseconds (ms). Also called delay.

Marker: A device that performs marking.

Marking: The process of setting the IP Precedence or DS code point in a packet based on defined rules; pre-marking, re-marking. This is also known as “coloring” the packet.

Network Availability: The probability that any communication can occur. Generally given as a percent. Also known as uptime.

Network Device: This refers to a device in the network that handles traffic. Routers and switches are examples of network devices.

Network Quality of Service (NQoS): Typically referred to as IP QoS. Derived from Integrated services (IETF Intserv working group) and/or Differentiated Services (RFC 2475).

Over-provisioning: This refers to applying more bandwidth to the problem than is required.

Packet Loss: Percent of the transmission that does not arrive correctly.

Per Hop Behavior (PHB): This refers to a forwarding action taken by a routing or switching device when determining what to do with a given packet. An example might be putting real time traffic in a high priority queue or it may simply be setting the next hop to which the packet will be sent. It can also refer to the forwarding behavior applied at a DS-compliant node to a DS behavior aggregate.

Policing: This is the process of enforcing the policies, which could result in delaying or dropping packets.

Policy: This is a set of rules that define the criteria for allowing access to a network resource. Rules used to classify the response afforded a marked packet, Behavior Aggregate, PHB group.

Policy control: The application of policies to make a decision whether to allow access to a resource.

Policy Decision Point (PDP): A COPS acronym. This is the device where the policy decisions are made. The PDP has usually a global knowledge of all the network policies that pertain to one administrative domain.

Policy Enforcement Point (PEP): This is the device where the policy decisions are enforced.

Quality of Experience (QoE): The measure of the facilities of Quality of Service applied to a voice/video communication session. Application QoS or network alone or a combination of the two.

Quality of Service(QoS): This refers to the type of service provided by the network devices.

Queuing: The act of storing packets where they are held for subsequent processing. Queuing may occur during either input or output on a given router or switch interface. Several types of queue scheduling exist: First In First Out(FIFO), Priority Queuing (PQ), Class Based Queuing (CBQ), and Weighed Fair Queuing (WFQ).

RAS: Registration, Admission, and Status

Resource: This refers to all the factors in the network device that affect the forwarding of packets such as bandwidth on an interface, queues, processing power etc.

RIP: Request in progress

RR: Receiver report

RTP: Real-time Transport Protocol

RTCP: Real-time Transport Control Protocol

Scheduling: See "Queuing" above.

Sequence Error: The probability that a packet will arrive out of sequence and thus must be buffered prior to reassembly. Generally given as a percent of out-of-sequence packets over the total number of packets.

Traffic Shaping: The practice of controlling the volume of traffic being sent into the network, and the rate at which it is transmitted. Two shaping algorithms exist: Leaky Bucket and Token Bucket.

Traffic: Traffic refers to one or more flows that traverse through the network.

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

DOCUMENT CONTROL

This Document is	Controlled X Uncontrolled
Version Control Website	http://itrp.calstate.edu/vc/

DOCUMENT HISTORY

Version	Date	Author	Comments
1	09/02/03	Cassidy D. Smith	

CONTACTS

Original Author	Cassidy D. Smith, <i>PlanNet Consulting</i> , 714.271.4000, csmith@plannet.net
Author	
Revisions	

DISTRIBUTION

Name/Distribution list	Email address/Maintainer	Phone

CONFIDENTIALITY

--