SEAMLESS VIDEO TRANSMISSON OVER NETWORK

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
ÇANKAYA UNIVERSITY

BY

SERDAR YURT

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
COMPUTER ENGINEERING

MAY, 2012

Title of the Thesis: **Seamless Video Transmission over Network**

Submitted by **Serdar YURT**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University

Prof. Dr. Taner ALTUNOK
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Asst. Prof. Dr. Murat SARAN
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Asst. Prof. Dr. Reza HASSANPOUR
Supervisor

Examination Date: 11.05.2012

Examining Committee Members:

Prof. Dr. Mehmet Reşit Tolun	(TED Univ.)	
Asst. Prof. Dr. Reza Hassanpour	(Çankaya Univ.)	
Asst. Dr.Abdülkandir Görür	(Çankaya Univ.)	

STATEMENT OF NON-PLAGIARISM

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: Serdar YURT

Signature :

Date : 11.05.2012

ABSTRACT

SEAMLESS VIDEO TRANSMISSION OVER NETWORK

YURT, Serdar

M.Sc., Department of Computer Engineering

Supervisor: Asst. Prof. Dr. Reza HASSANPOUR

May 2012, 48 pages

Traditionally different types of traffic are not distinguished. Traffic suffers from increasing delay, packet loss and variable delay. In order to deal with these issues QoS (Quality of Service) schemes have been proposed. The primary goal is to provide a testbed and platform for investigating characteristics of real time internet traffic on heterogeneous networks. QoS techniques for transmission of real time video may be based on DiffServ (Differentiated Service) architecture. In the QoS testbed, this is implemented using an efficient bandwidth agent to allocate bandwidth, a Hiererchical Token Bucket queuing scheme at the output interface of routers, and a policing mechanism at the incoming of the edge switch. The characteristic of real time video traffic using MPEG-4 streaming and Telepresence devices are studied to that we will have a good idea what bandwidth and burst size is required to stream MPEG4 video through the QoS Diffserv domain. We use the testbed to investigate how real time streams behave in QoS scheme and provide a realistic recommendation to manage the available bandwidth for both the Q0S provider and clients. Test were conducted with Telepresence. From this test we observe that telepresence streaming require a certain size of burst to properly be transmitted.

Keywords: DiffServ, Telepresence, Hierarchical Token Bucket, Delay, Packet Loss

ÖZ

NETWORK ÜZERİNDEN KESİNTİSİZ VİDEO İLETİMİ

YURT, Serdar

Yükseklisans, Bilgisayar Mühendisliği Anabilim Dalı

Tez Yöneticisi: Asst. Prof. Dr. Reza HASSANPOUR

Mayıs 2012, 48 sayfa

Geleneksel internet trafiği ayırt edilmemekte ve farklı türde ki trafikler gecikmelerin artmasından ve paket kayıplarından kaynaklı mağdur olmaktadır. Paketlerin daha düzenli dağıtımı ve iletimi için QoS mekanizması önerilmiştir. Temel amac test ortamı oluşturularak gerçek zamanlı trafiğin simule edilmesi ve uyguladığımız Qos mekanizması DiffServ modeli ile etkilerinin görülmesidir. OoS icin oluşturduğumuz test ortamında anahtarlama ve yönlendirme cihazların da konfigurasyonlar tanımlanmış ve cihazlarda bulunan kuyruk ve denetleme mekanizmalarından yararlanılmıştır. Gercek zamanlı trafik icin MPEG-4 formatındaki Telepresence cihazları kullanılmıştır. Biz bu sağladığımız test ortamında telepresence görüntü aktarımları için ihtiyac duyulan bandwidth ve burst değerleri ile birlikte düzgün bir şekilde iletildiğini gözlemledik.

Anahtar Kelimeler: DiffServ, Telepresence, Gecikme, Paket Kaybı, HTB Kuyruk

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my supervisor Asst. Prof. Dr. Reza HASSANPOUR for his guidance, advices and support during the research. It has been pleasure to work with him. I also thank Prof. Dr. Mehmet Tolun REŞİT for their suggestions and comments.

I especially thank to my family and R. Teoman KOÇER for their patience and support while the period of study.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

CHAPTER 1

1. INTRODUCTION

Tremendous increase in network capacity leads increase of consumption of this capacity at the same time. Web traffic, voice over IP and other multimedia application such as video phones, video conferencing, on-line lectures, Telepresence, video on demand so on. These real time video streaming services have become important on the Internet, and have also been gradually expanding the service field. However, these applications require large amount of bandwidth besides specialized service on network with respect to latency and loss. Therefore performance of some mission critical applications degrades in the network [1].

One of these applications is Telepresence. To provide good quality performance, Telepresence requires significant bandwidth with minimal delay, jitter and loss. For this we first need to have QoS (Quality of Service) mechanisms, and resource management to support QoS for real time streaming applications. However, QoS is not guaranteed because the internet currently is designed for best effort delivery by default. Because different service of internet traffic are not distinguished the congestion occurs which means that increasing delay and packet drops .In order to solve these problems DiffServ (Differentiated Service) model is applied. The main goal of DiffServ is a more scalable and manageable architecture for service differentiation in IP networks [2]. This study describes a solution in providing network Quality of Service (DiffServ) to Telepresence application.

1.1. Problem Definition

Real time video applications require some of streaming techniques. These streaming techniques display video data by transmitting once small portions of video files. However, real time streaming applications require minimum bandwidth and guaranteed QoS whereas traditional network applications such as e-mail, web, ftp, bandwidth and delay are not important issues. Some applications, such as FTP, HTTP and email, are not sensitive to delay and jitter. On the other hand applications such as interactive voice and video are vulnerable to loss, delay and jitter. Real time internet traffic such as video and audio is always required more bandwidth and delay sensitive.

In present IP Networks both the traditional and real time traffic use FIFO (First In First Out) by default. In this case, it is difficult the design an efficient real time transport system because best effort delivery would not satisfy these issues in IP network [3].

During peak times of traffic, networking devices might delay and/or drop some packets to avoid a possible congestion. At this point, the QoS network devices must be able to differentiate among classes of arriving traffic and satisfy their individual requirements. QoS mechanisms providing a set of tools that can be used to do that play a critical role. It enables the network to recognize traffic belonging to certain users and applications such that preferential services may be provided to them. Some QoS mechanisms also enable applications to provide information to the network to assist the devices in performing traffic classification. QoS is therefore the best way to handle contention for network resources when the network consists of widely varying types of traffic. The network IP capacity should be sufficient depending on the reality that QoS does not create any additional capacity. It just helps to manage the available resources according to policies set out by the network administrator [4].

1.2. Objectives

The work of this thesis is referred to previous MCS thesis for format and guide and is used to TT infrastructure. The main goals of this thesis are to investigate Telepresence application for monitoring the packet traffic through a network within QoS System (DiffServ Model).

We set an efficient test bed to investigate how real time streams behave in the QoS scheme and to provide a realistic recommendation to manage the available bandwith for both QoS provider and clients.

This thesis evaluates QoS techniques for transmission of real time video that use a Differentiated Service mechanism. The DiffServ mechanism provides QoS guarantees on Internet Protocol (IP) networks. This DiffServ mechanism includes an efficient bandwidth agent to allocate bandwidth on heterogeneous networks, a Hierarchical Token Bucket (HTB) queuing scheme at the output interface of Router, and policing mechanism at the incoming interface of Edge router in a test bed.

The test bed consist of TT networks to find the characteristics of real time video traffic (Using Telepresence, include MPEG4) and to determine what bandwidth and burst size is required to stream MPEG4 video through the QoS DiffServ domain.

1.3. Thesis Organization

The rest of the thesis is organized into several chapters. Chapter 2 discusses application and describes related to QoS. Chapter 3 discusses some of the previous work on QoS at the network layer and the application layer. Chapter 4 describes QoS test bed design and shows the result of test and analysis. Conclusion and future work are discussed in Chapter 5.

CHAPTER 2

2. CONSEPTS and TERMINOLOGIES

Communication systems such as data, audio, images and video must provide QoS. Real time video streaming will be more popular in the near future [5]. But during the achievement of this process there will be some challenges we have to overcome. In order to overcome these challenges, a well designed QoS should be implemented. In this chapter, we introduce application (teleperence) and its characteristics, so we will understand the telepresence application in a better way. But meanwhile we need to investigate the characteristics of Telepresence to provide QoS.

2.1. Telepresence Concept

Normally, the meetings can be at same or distant locations to discuss problems or any kind of need. What Telepresence enable is to meet face to face meeting without all participations come together [6]. Telepresence requires various pieces of equipments such as cameras, microphones, user interface, network connections, codec, screen, communication server. Why we need these devices because we want to provide good audio and video to end user. In order to give end user best audio and video quality we need to achieve acceptable service from network to eliminate this problem the best mechanism is implement QoS in the network. While providing QoS network delay should be as small as possible as compared to the total allowable system latency. When we want to send video and audio packets over networks which do not have enough bandwidth among packets, these packets will arrive late or out of order. This causes delay, jitter and packet loss resulting bad performance.

Furthermore, Telepresence solution's main component is the codec. The Codec provides the inputs for high definition cameras and outputs for high definition displays. The Codec also provides the audio inputs for microphones and audio outputs for speakers and compresses the video and audio inputs with H.264 compression into IP packets for delivery on the IP network. The Codec is a two way real-time communications platform so that you can see and hear the far end at the same time they are seeing and hearing you. The rapid delivery of the information is very important. Real time communications must have very low delay and uniform delivery of the packets across the network [7]. QoS is very important to the Telepresence solution.

The codec which is packaged in a complete Telepresence solution offers two different packages; the CTS-3000, and CTS-1000.

CTS-3000: The high-end Telepresence system has three Codec's (1 primary and two secondary) three cameras and monitors. It also uses a 7970 color IP telephone for user operation.

Figure 1 General View of Telepresence

The Telepresence system is an IP only solution based on SIP (Session Initiation Protocol). As such the main considerations must be given to bandwidth, Call Manager integration, QoS and security.

2.2. Call Concept

The combination of the 7970 and the Telepresence endpoint in the room should present to the user a seamless environment where both devices should act as if they are a single entity. The intent here is that to have a phone (the 7970) in the room acting as the user interface for both the phone and the Telepresence device. The following call scenarios are defined:

2.2.1. Inbound Call

Upon reception of an inbound call request, the units master will use its local end-user interface and the phone user interface to prompt the user to answer the call. If the user accepts the call the units will auto-negotiate the highest quality available. Note that it is also possible to have the units configured to automatically accept an inbound call.

2.2.2. Outbound Call

To initiate an outbound call in an Ad Hoc fashion, the end-user uses the standard IP phone mechanisms (keypad, speed-dial, or directory). If the remote site offers video capabilities, and the unit is not engaged in an active call it will use SIP to transfer the call to the Telepresence endpoint and renegotiate the call media. The IP phone will drop out of the call [8].

2.3. QoS Concept

The main purpose of the QoS is to treat packets differently trough a network device based on package content. The tasks in which QoS configuration provides depend on the direction of traffic flow of the device performing the QoS functionality.

QoS policies classify and mark each packet at the access layer on the network to which IP packet first enter the network. The rules defined in the policies are applied in the inbound path on access layer interface.

When the packet has been market on the inbound path it can be used on outbound path to give each packet access to the appropriate amount of resources.
After the packets have been marked, the policies in each device based on marked packages do not need to do deep analysis of the content packet.

In order to efficiently utilize the company's network resources, it should be considered which network traffic is critical and allocate appropriate resources to support those traffic stream.

If video stream exists in the network, it must get priority over all data .If we don't give priority, the video stream will freeze and have bad quality. Video and voice application are jitter and delay sensitive. A good QoS policy will give the video stream packet priority access to the interface queue and will be processed first [9].

2.4. Architecture of QoS

Early attempt to introduce QoS in to IP (Layer 3) was TOS (Type of Service) but it never really used on a large and complexity networks. That is way it has been supersede by DiffServ model. To support multimedia real time application the architecture should control traffic and layer 3 switches in the network. The two methods for IP network are DiffServ (Differentiated Services) and IntServ (Integrated Services).

2.4.1. Differentiated Service

In The DiffServ model traffic is classified into flows although the reservation is not required IP packet are marked using the DiffServ field. This field uses same field as the ToS field although each bit has different meaning. DiffServ's main advantage is an admission control mechanism at the ingress of network. Typically functions performed in a DiffServ network are ;

- Traffic is classified in to flows
- A network policy is applied to the classified flows, so it shapes traffic to meet the requirement of the particular flow .If the traffic is intense the packet the low priority flow are discarded.

- When the traffic is shaped, the IP header DiffServ field is marked with the appropriate DSCP (Differentiated Service Code Point)
- When it is passed through DiffServ network the DSCP triggers a selected per hop behavior from the interior of the network.

2.4.2. Integrated Service

Integrated Services is similar to ATM because it defines an end to end pathway through a network for each application's packet. It does this using the RSVP (Resource Reservation Protocol) which dynamically maintains a path using the resources with lightest load. This is maintained as a flow with appropriate policies for admitting traffic to the network so this pre determined packet handles characteristics at each hop [10].

2.5. Jitter, Delay and Latency

Latency is the delay in data transmission from source to destination.
Jitter is the variation in latency. Admission control is to determine which applications and users are entitled to network resources. These mechanisms specify how, when, and by whom network resources on a network segment (subnet) can be used. Traffic control is to which applications and users are entitled to network resources.
These mechanisms specify how, when, and by whom network resources on a network segment (subnet) can be used [11].

2.6. Qos and Queuing

Queue management is a fundamental issue for QoS. It enables bandwidth control (admission control) and ensures that traffic is dealt with as its priority requires. To achieves this;

- **Weighted Fair Queuing**

It sets max and min bandwidth limits. It ensures that lower priority application cannot borrow bandwidth from other application.

- **Priority**

This ensures that high priority traffic is given priority over other traffic. So it causes less delay [12].

2.7. DiffServ Domain for Telepresence

It is assumed that Telepresence will support 802.1p/q CoS (Class of Service) Layer 2) packet marking for QoS. Telepresence must also support DiffServ code point (DSCP - Layer 3) marking for QoS. This involves marking packets based on the configured IP Type of Service values (ToS) for the different classes of sourced traffic: audio, video, call signaling and network management.

Marking of Audio (Voice) Signal

Layer 2: CoS = 5

Layer 3: DSCP = 46 (EF, Expited Forwarding)

Marking of Video (TelePresence) Signal

Layer 2: CoS = 4

Layer 3: DSCP = 32 (CS4, Class Selector)

Marking of Signaling Traffic

Layer 2: CoS = 3

Layer 3: DSCP = 24 (CS3) or DSCP = 26 (AF31, Assured Forwarding)

Telepresence endpoints rely on CUCM to perform location based Call Admission Control (CAC).

A main aspect of a high-quality experience is low-latency between endpoints. Both the local and the remote endpoints contribute some degree of latency, as does the network that lies between the endpoints. One-way network latency alone can easily be 70 ms when the remote destination is a great physical distance from the local endpoint. The Telepresence system understands this and has adjusted the latency warning’s alert to reflect this, however for the most optimal experience it is still recommended that the units be within 70 ms of each.

A key performance criteria of a high-quality conferencing experience is good synchronization between the media streams. Voice and Video streams are sent separately over the WAN. Telepresence must provide for synchronization between media streams and make sure that they never vary by more than 20 ms from the original media synchronization.

2.8. Compression Techniques

Compression is reduction in size to save space. Hence transmission bandwidth and time will be reduced. Therefore, it is necessary to compress a video. Because of video files consist of components which are container and codec video format confusing. Codecs are used inside to container. Codec is a compression algorithm that performs encoding and decoding on a digital data stream or signal. MPEG-1, MPEG-2, MPEG-4 are the well known codec. Here we are going to use H.264 (also known as MPEG-4 Part 10/AVC for Advanced Video Coding) compression standard.

The container, on the other hand, is computer file format that describes the structure of the file. It can have various types of data. The container identifies data type and carries all of the information the computer needs [13]. Video compression techniques are categorized by bit rate. Constant Bit Rate (CBR) video is compress and transmit at a constant bit rate but the variable bit rate (VBR) video transmit at a variable bit rate.

2.8.1. H264 Compression Technique

H.264 is a video encoding and compression standard jointly developed by the Telecommunication Standardization Sector (ITU-T) Video Coding Experts Group

(VCEG) and the International Organization for Standardization/International Electro technical Commission (ISO/IEC) Moving Picture Experts Group (MPEG). It was originally completed in 2003, with development of additional extensions continuing through 2007 and beyond.

H.264 is equivalent to, and also known as, MPEG-4 Part 10, or MPEG-4 AVC (Advanced Video Coding). These standards are jointly maintained so that they have identical technical content and are therefore synonymous. Generally speaking, PC-based applications such as Microsoft Windows Media Player and Apple QuickTime refer to it as MPEG-4, whereas real-time, bidirectional applications such as video conferencing and Telepresence refer to it as H.264 [14].

2.9. Characteristics of Video

We need compression technique because of the limitation bandwidth capacity and to save store space. Telepresence resolution is 1920 by 1080 pixels. In video there are 3 colors to make each frame element; red, green, blue.

Each color is 8 bits precision which means that each picture requires 6.220 Kbytes, (1920x1080x3) of storage space. Normally 30 frames per second are needed to show a continues image on the screen [15] 1.5 Gbps (6.220Kbytesx1024x 8 bits /picturex30picture/seconds) which means that we need a network in which throughput is greater than 1.5 Gbps in order to send one second of video to the destination in real time. Therefore each TP screen needs approximately 570 of storage space. That is why real time streaming video should be compressed efficiently. In case video signal is of variable size and has a VBR which causes problems that are the characteristics of compressed video signals. We will investigate the traffic characteristic if video stream which are compressed based on the MPEG-4 standard.

2.9.1. Burst

As we already know compression techniques are divided into CBR and VBR. Burst occurs because of high compression rate and variance bits per frame in VBR compression. Since burst properties are an important factor in VBR streaming it needs to be understood for QoS. In order to achieve QoS allowing bandwidth and congestion control should be carefully exanimate for real time multimedia communications. Burst behavior of the VBR video has a significant impact and congestion control. This is obvious because the burst behavior of the VBR usually generates various amounts data (various video signals or high rate time scales) during different time periods [16].

Besides the impact on the bandwidth congestion control it also causes packet delay and packet loss.

If we increased the bandwidth it would be wasted and network usage would be reduced. Because it will cause packet loss and packet drops if the bandwidth is less than largest required bandwidth.

Increasing bandwidth is not a complete solution with the burst Because when the packet gets to a router they must compete for priority.

2.9.2. Constant Bit Rate and Variable Bit Rate

CBR and VBR are used for compression. The main characteristics of CBR is that output bit rate of the encoder is held constant by means of feedback loop control. Output of the VBR's bit rate variable but the quality of the video is held approximately constant [17].

As we know earlier VBR video signals causes some problems. One of the problems is too determined to required bandwidth. Typically video streams compressed before transmitted .Normally video signals are compressed using the technique called MPEG-4 [15] which inherently uses VBR.

Scene content and coding algorithm are very important for VBR. The encoder is the key component of transmission over the network. Normal data transmission cannot change the original data. But video encoder modifies that data by adjusting an number of parameter which is found in coding algorithms such as frame rate and resolution [18].

2.9.3. Summary

In this chapter we discussed Telepresence conferencing to provide good quality by using QoS mechanism. We also mentioned compression techniques like MPEG-4 (H264) which reduced size of the file but causes transmission to have VBR with burst. Therefore following chapter will calculate how to deal with characteristics of Telepresence to provide QoS.

CHAPTER 3

3. PREVIOUS WORK

When they consider video and audio traffic on the internet we need to provide QoS. QoS is not always guaranteed while increasing bandwidth. That's why we are going to investigate QoS under the following issues.

3.1. Quality of Service at The Network Layer

3.1.1. Integrated Services

According to the IETF principles, one of the techniques to guarantee QoS is integrated service model. Here, there is a signaling protocol called The Resource Reservation Protocol which makes per flow reservation to guarantee QoS.

Although IntServ guarantees differentiated services there are some drawbacks to using this model. In order to provide QoS the requirements of classification and forwarding policies for each flow along network path, all of the communication equipment such as routers should support RSVP along the path to set up per flow reservation. However, each data flow is complex and needs large resources for routers.

That's why IntServ has problem to handle complexity and scalability. Therefore Differentiated Service model has been proposed.

3.1.2. Differentiated Services

The difference IntServ between DiffServ is DiffServ works aggregate traffic [19]. DiffServ is based on packet marking technique to provide differentiated service by aggregating classification states aggregates traffic classification rather than per flow states. Scalability is achieved by using packet marking technique to be easier. In order to understand scalable QoS support, a packet IP header field called ToS for IPv4 and flow label for Ipv6 must be marked. We focused on the IPv4 DiffServ model. Here 6 bits from 8 bits ToS field in IP header are labeled by Differentiated Service Code Point (DSCP). DSCP provides DiffServ with PHB (per hop behavior) to identify and classify packet. So, PHB knows how to forward the received classified and marked packets for DiffServ.

DiffServ architecture consists of a scheduler who manages network resources and Edge Router (ER) to regulate traffic. In order to provide guaranteed service, the futures such as admission control, resource reservation and packet scheduling should be implemented. Duan, Zhang, Hou and Gao [20] tell in their research the bandwidth scheduler architecture admission control should be on a per domain basis rather than a hop by hop basis. This approach shows that complexity of the admission control algorithms is reduced.

There are two types of Router in DiffServ domain. One of the routers is ER. ERs marks packages on the DSCP depending client request. it is responsible to accept and filter incoming packages.ER in DiffServ network include policy mechanism in the ingress interface and packet scheduling in the outgoing interface to provide Differentiated Service according to SLA (Service Level Agreement) which is a mutually agreement between client(requester) and a network [19]. ER (Edge Router) and CR (Core Router) characterize, police, and marks IP traffic. ER and CR can be used as traffic policer in DiffServ domain. Traffic policer drop packages if data stream exceeds limit specified in SLA.

Routers forward packages which are defined in every PHB by using the code point in IP header. The Expedited Forwarding PHB is used to provide services such as low loss, low jitter, low latency and assured bandwidth though the QoS DiffServ domain. Assured Forwarding PHB provides least bandwidth and least loss.AF PHB forwards almost all packages if traffic doesn't exceed the defined subscribed information rate. Best Effort forwarding doesn't provide QoS.

Fifo is not suitable to provide DiffServ. Because it gives all the packet the same QoS. Therefore it is necessary to change existing packet scheduling and Hierarchical Token Bucket packet transmission has been suggested within DiffServ domain.
Zhang and Wu [21] take into account both Class Based Queuing (CBQ) and HTB for a bandwidth limiting scheduler. They concluded that HTB leads a better shaping result than CBQ .For marked packages, HTB has different priorities classes to distinguish packages.

In our study is designed an IPv4 test bed by DiffServ Domain. Streaming Video traffic and Background Traffic have sent through the QoS network to see if the domain could provide QoS. However Our DiffServ domain did not have a BB (Bandwidth Broker) for admission control or QoS reservation maintenance and had no communication between a client and the network. We manually configured the router to mark the incoming video packets at the interfaces. We marked video packets, used the Cisco router IOS (Internetwork Operating System) facilities, as mark EF, CS3 and background traffic as mark AF11, 21, 22, 23. In front of the HTB, there was a filter to check the IP header, distinguish between video traffic and background traffic based on the mark and put each type of traffic in its own class in the HTB. We verified that the HTB supports guaranteed services on the router.

At the TungaBaskaroRao study [22], QoS agent BB , QoS client, signaling are used for DiffServ domain. Routers here are configured by the QoS agent to mark IP packets. The packets are marked based on source IP, destination IP, source port number, destination port number and protocol. When the QoS agent runs, it statically sets up the HTB in the output interface of the router. Once the QoS agent receives a request from a Q0S client, the QoS agent first checks the network environment then replies back. If the reply is positive, then QoS agent dynamical sets the policer with source, destination IP, source port, destination port, protocol and the required bandwidth at the router.

This mechanism is important. Because it can control the band with for EF marked packets. Monitoring video traffic bandwidth is an issue when the client asks for a certain amount of bandwidth for real time video streaming and send more data than required bandwidth request. Therefore policing mechanism is necessary to protect against overflow and to achieve maximum utilization of resource. However TungaBaskaroRao only sent CBR data through the QoS network which means that data quality would be maintained at whichever the policer set. However if the data were VBR real time video stream then TungaraBaskaraRao's DiffServ domain wouldn't work well because of the bursts.

In their study if the data were VBR real time video stream, their DiffServ domain wouldn't work well because of the burst. Therefore it is necessary to know characteristics of video applications for VBR to provide QoS in a different way.

Kuang and Williamson [23] tried different real time applications for streaming on a Wireless LAN (Local Are Network). They used a real media server to send different real time applications. They discovered burst in the traffic while testing this application. They realized that the burst is generated not only from compression techniques but also from multimedia applications.

Ahmed, Mehaoua and Buridant [24] suggest that IP DiffServ with AF PHB can support real time video communication with packet marking and scheduling mechanism. They investigated QoS interaction by sending MPEG-4 video applications through a network. They mark the packets at the video sender before transmission. But their domains also have ERs to accept and filter incoming packets. However it is necessary to discover the actual required average rate and burst size to satisfy QoS.

3.2. Quality of Service at the Application Layer

There are a lot of studies on the Application Layer to provide QoS. One of them is the Real player example [23]. It sends burst packages to fill the buffer at the receiver to provide QoS.

It is technique possible to provide QoS unlike ftp and e-mail .It would be safer if the application sent burst packets to receiver's buffer at the beginning. Because other packets would have extra time to reach the destination after the burst packets. To support QoS Sheu and Fang [25] investigated how to calculate the receiver's initial buffer size. When the server send burst packets it might be dropped because overflow If buffer size is not large enough.

Some of the researchers used different techniques to find a solution for burst traffic. Some work on compression algorithms the other worked on multimedia applications. Zubari,El Shaikh and Mahmoud [26] used a traffic shaper at the output interface of a video Server. But there was a gap between packets. These makes a protection against overflow at the receiver and control the transmission packet speed at the Server.

Li, Liu and Zhang [16] worked on how to measure burst. They found that burst is an important property for real time video because it has a significant impact on bandwidth allocation and congestion control. That's why to measure and optimized bandwidth is difficult. In order to handle this problem to solution is to allocate highest peak burst rate. It seems an easy way to solve the problem. It consumes resources. Therefore it is not recommended.

In the study of Tunali and Anar [27] the way to solve the measure of the bandwidth is possible during the playing of the video from time to time. But it brings some problems during the checking of the bandwidth because it generates more data flow on the internet.

3.2.1. Summary

All researchers mentioned here insist on working application layers to provide QoS along with problem during their studies. Some of them have succeeded in their study because they found solutions to provide QoS. They seem reasonable to get good quality streaming but in order to satisfy QoS, to work in application layer is not enough.

The network layer should also be considered to eliminate congestion to satisfy QoS. Because if the congestion occurred they would not guarantee QoS. In order to provide guarantee QoS, we need to work not only application layer but also at the network layer. Because current network environment doesn’t guarantee enough bandwidth and doesn’t eliminate packet delay.

My study deals with DiffServ on network environment. The study mainly consists of real time packages defined by DSCP (classification, marking and forwarding of packages) rather than other packages (e-mail, ftp, specific data...). The network resources is tried to use efficiently to provide good quality streaming.

CHAPTER 4

4. TEST BED ARCHITECTURE

In this chapter, we describe all of the components for the test bed architecture needed to full understand, designing a test bed among Telepresence systems which are used in our existing network environment. This Telepresence system is often used efficiently for meeting purposes.

4.1. Test Bed Architecture for Existing Network Environment

QoS domain is configured manually in our network environment to satisfy QoS. For this, existing network structure of router's IOS is used. In this architecture there are 3 routers. They communicate each other by using enhanced routing protocol. QoS is implemented among these routers as QoS agent and Client. The architecture includes signaling protocol between a client and QoS agent.

When the QoS agent executed, it configure the HTB at the egress interface of the router. This way, the QoS model is scalable and allows aggregation of flow. The client's request is in XML (Extensible Markup Language) format includes source and destination IP address, source and destination port, amount of bandwidth and the protocol.

When the client sends a request to QoS agent, the QoS agent process this request based on the EF, AF, and CS3 bandwidth available in the QoS domain.

So The QoS agent controls admission. The QoS agent is a backbone Router in the DiffServ domain. An image comes from Telepresence devices is the QoS client for us.

Our domain has three routers which include policer at the ingress interface to control traffic and HTB at the egress at the interface to manage bandwidth. If there is enough EF DiffServ bandwidth available for the client’s request, the Backbone router configures the policer to monitor packets and marks a packet DSCP-EF in the IP Header when the packet matches the six criteria’s mentioned above. If there is no enough bandwidth QoS agent gives a message ‘bandwidth is not available’ and ‘reservation Rejection’. Then QoS Agent maintains the packets for reservation and repeats reservation request every 15 seconds until reservation expires. This process works automatically on router structure.

If the reservation expires, QoS agent deletes the reservation and disables the policer and removes the packet marker from the router. All of these actions occurred between routers in DiffServ by establishing a secured connection.

Network and application topology are illustrated below for our test bed.

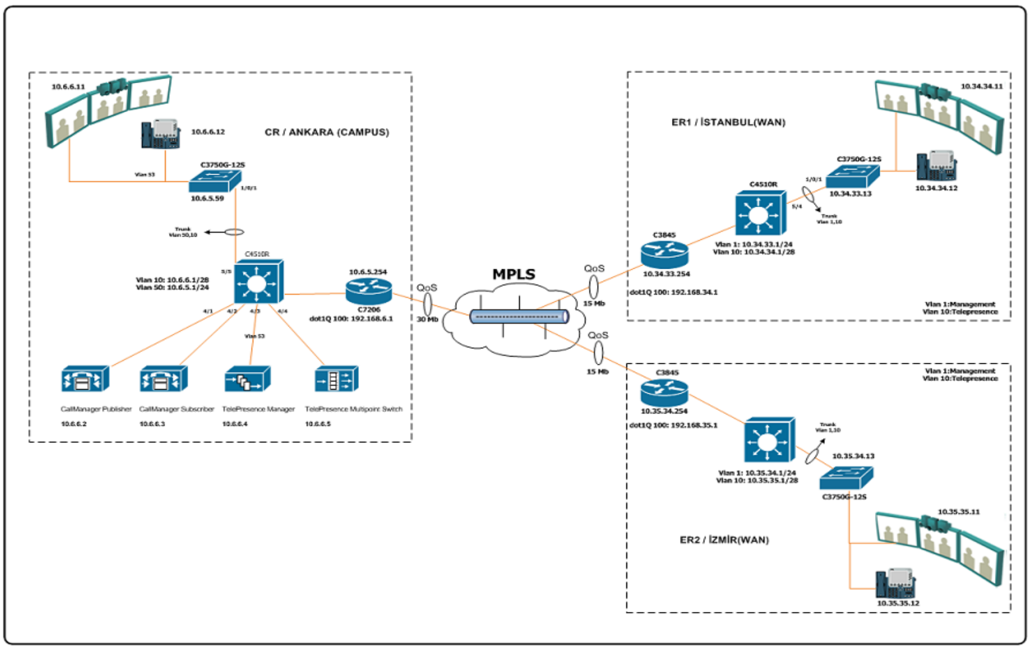


Figure 2 Network Topology

In Figure 2, the test bed contains four different links; the 192.168.6.1, 192.168.34.1, 192.168.35.1 respectively CR, ER1, ER2. This test bed contains wired network using a 1 Gbps fiber cable, 100 Mbps Switch. In order to provide end to end QoS, it is necessary to investigate the traffic characteristics of Telepresence on wired network .To guarantee QoS over a wired network is an issue because real time internet traffic is always required more bandwidth and delay sensitive.

In Figure 3, our application consists of servers and endpoints. Servers are CUCM, CTMS and VCS. Endpoints are CTS, VC. We are interested in streaming between CTS devices. Communication Servers are used for different purposes .CUCM is used for call control. CTMS is used for conferencing. Each CTS device is registered to CUCM via SIP. If point to point call wanted between CTS devices. First, they are communicated via CUCM. And then RTP streaming is established between them. If there is conference between more than two CTS , CTMS is used for bridging.

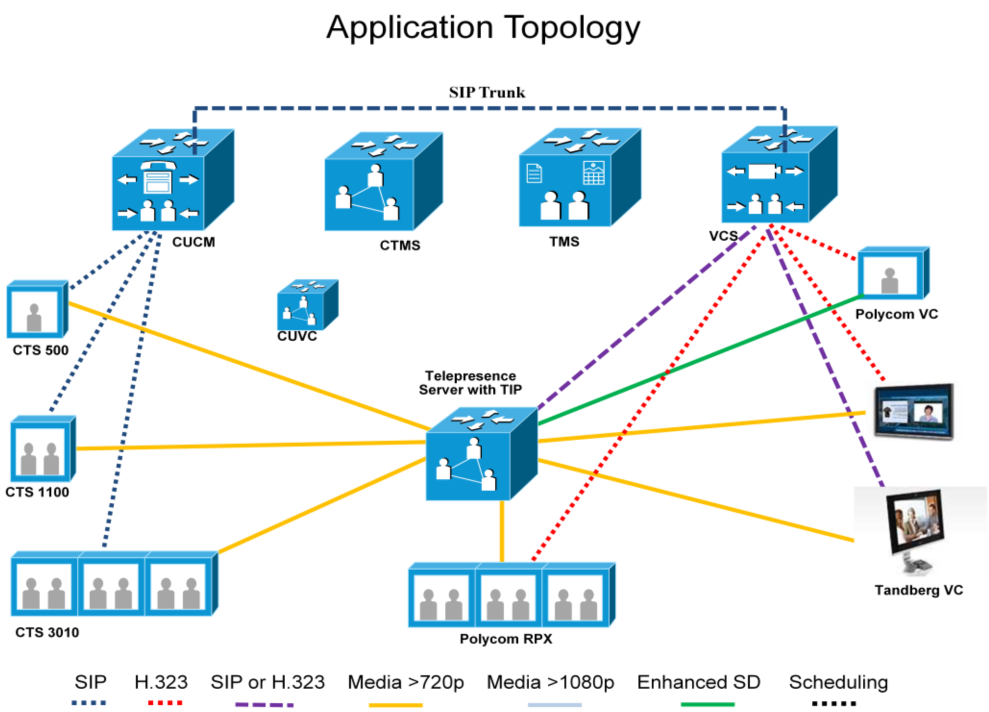


Figure 3 Application Topology

4.2. Network Design In DiffServ Domain

In Figure 2, the single sites (Ankara, Istanbul, Izmir) are interconnected via Ethernet links over Turk Telekom's MPLS network. The network structure of the single sites is depicted respectively in Figure 4, Figure 5 and Figure 6.

Our DiffServ architecture has three routers which are located tree different areas respectively ER1, ER2 and CR. In our DiffServ domain, each ER is configured using 15 Mbps bandwidth whereas the CR is configured to use 30 Mbps bandwidth. The remaining configuration (marking) is left same. Because we use multipoint switch in CR location to make multi conference. If we have more than two conference between ER locations. We will use Multipoint switch at the CR location. Now we are ready to investigate both ER and CR How the DiffServ domain provides guaranteed service. The CR and ER in DiffServ domain are evaluated for the differentiated services and traffic forwarding.

Ankara Campus network topology is summarized below in Figure 4. It shows our campus environment. It is called name CR. Here we have Server and CTS 3010 device. Our CTS is connected to 3750 location switch which is connected to Backbone switch called 4500 switch. Servers are also connected to BBS. Finally all devices through router which has 1 Gbps line speed enter to MPLS network.

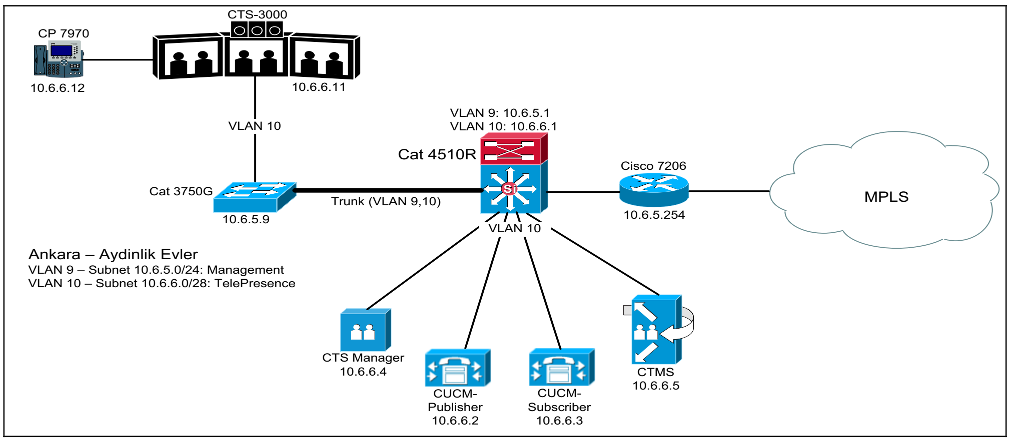


Figure 4 Ankara Campus Network Topology

In Figure 5, the other is area WAN environment which is located in Istanbul , It has same configuration as in campus area. The only difference is there are no servers. And also is called name ER1.

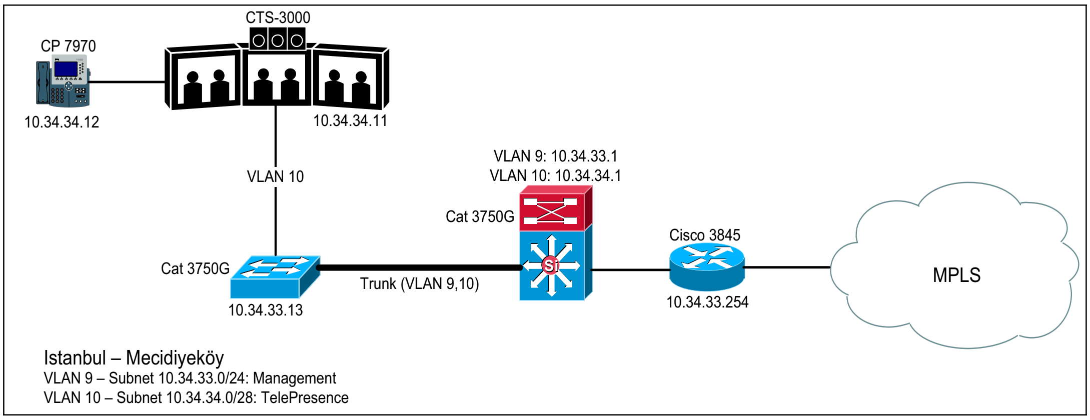


Figure 5 Istanbul WAN Topology

In Figure 6, the other is area WAN environment which is located in Izmir , It has same configuration as in campus area. Izmir are called name ER2.

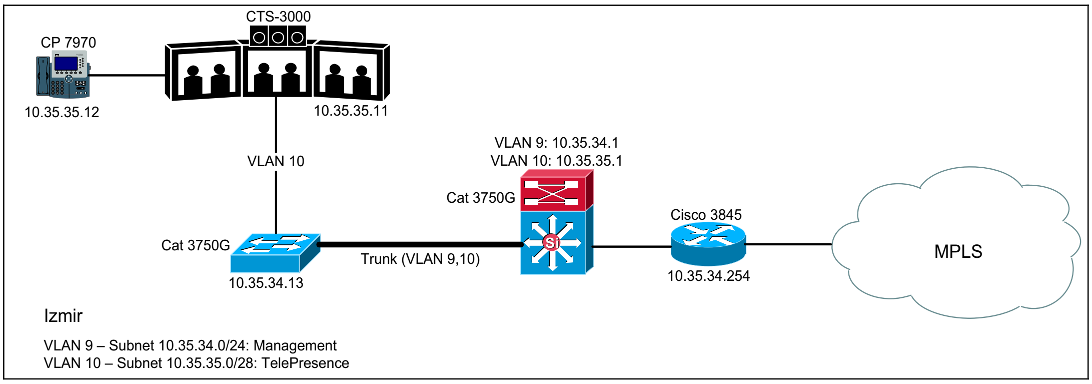


Figure 6 Izmir WAN Topology

4.2.1. Host Specification

There are three routers. These are labeled ER/CR. Three of them are ER respectively ER1, ER2, The other is CR located near the Multipoint Switch. ER and CR are connected through MPLS. ER interface IP addresses are 192.168.34.1, 192.168.35.1, respectively and CRs is 192.x.x.1.

In this test bed, QoS Agent and QoS client run on CR and ER .Here, client means real time traffic derive from Telepresence device. Or Client is called real time traffic coming from Telepresence device. Tables 1 through Table 3 contain information about the systems for test bed architecture.

Table 1 CR Router Specification

Name	Cisco 7206 VXR
RAM	512 KB
Version	12.4-11.bin, Cisco IOS Software
IP Address	Gigaeth0, 192.168.6.1 and GigaEth1, 10.6.5.254

Table 2 ER1 Router Specification

Name	Cisco 3845
RAM	256 KB
Version	12.4-11.bin, Cisco IOS Software
IP Address	GigaEth0,192.168.34.1 and GigaEth1,10.34.33.254

Table 3 ER2 Router Specification

Name	Cisco 3845
RAM	256 KB
Version	124-2.T5.bin,Cisco IOS Software
IP Address	Gigaeth0,192.168.35.1 and GigaEth1,10.35.34.254

4.2.2. Link Specification

There are four links in the QoS domain. Each specification of these links is as follows;

192.168.6.1/30, a 1 Gbps fiber cable, CR is connected to MPLS.
192.168.34.1/30, a 1 Gbps fiber cable, ER1 is connected to MPLS.
192.168.35.1/30, a 1 Gbps fiber cable, ER2 is connected to MPLS.

4.3. Quality of Service Design

In Consideration of QoS for Telepresence, there are two areas in the network that we need to look at independently. The first area is in the Campus environment, and the second area is in the WAN environment.

In the campus environment, the recommendations for QoS configurations are relatively simple. First we need to ensure that the traffic from the Telepresence codec is trusted such that the QoS markings are not rewritten. The next step is to ensure that Telepresence traffic is placed into the layer 2 priority queue of all the switches that it passes through. This is accomplished by ensuring that CoS4/AF41 traffic is mapped into the priority queue at each switch.

The diagram are illustrated below in Figure **7** depicts a typical Telepresence deployment and shows all the points in the network that need to trust the CoS/DSCP values as well as where priority queuing is needed.

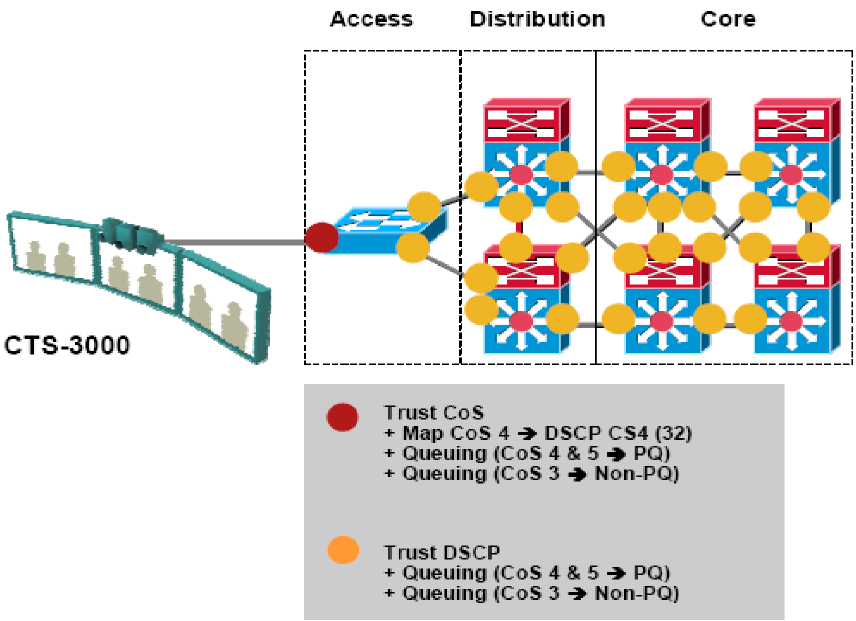


Figure 7 Campus QoS Design Recommendation for Telepresence

4.3.1. QoS Recommendation Catalyst 3750G

General Settings

!Enable of QoS on switch

mls qos

TelePresence Port Settings

!Trust DSCP value (no 802.1Q)

interface Gigx/y

mls qos trust dscp

OR

!Mapping CoS to DSCP values

mls qos map cos-dscp 0 8 16 24 32 46 48 56

!Trust CoS value

interface Gigx/y

mls qos trust cos

!Trust CoS value only if Cisco TelePresence/IP Phone is attached

mls qos trust device cisco-phone

Uplink/Router Port Settings

!Trust DSCP value (no 802.1Q)

interface Gigx/y

mls qos trust dscp

OR

!Trust CoS value

interface Gigx/y

mls qos trust cos

Ingress Queue Settings

The following in Figure 8 shows the mapping of the different traffic types to the corresponding ingress queues of the switch:

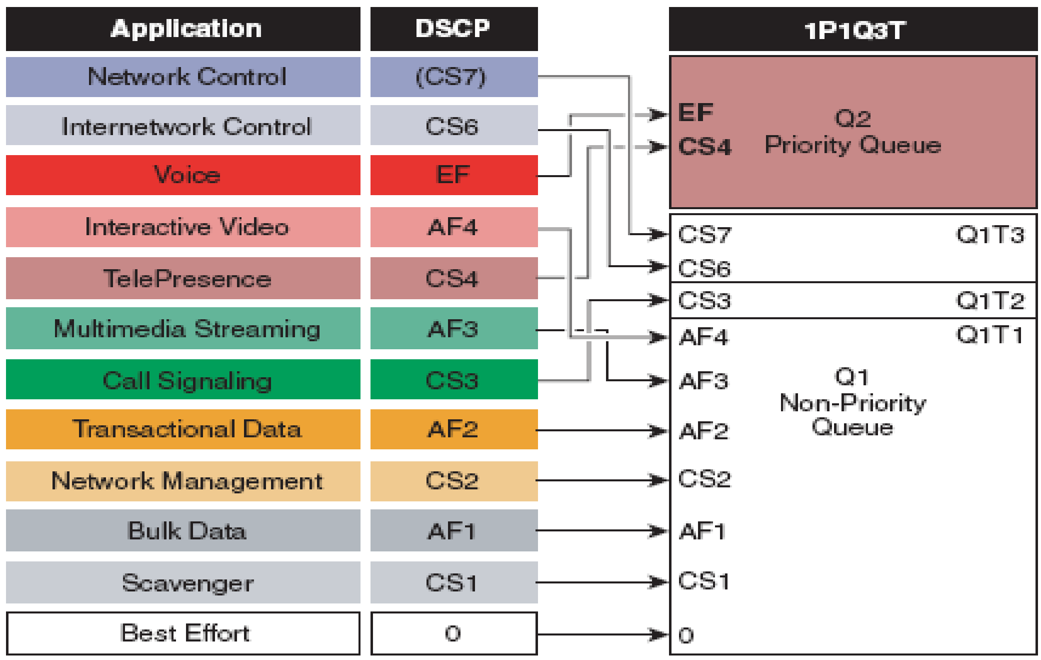


Figure 8 Switch 3750G Ingress Queuing Recommendation for Telepresence

The following shows the config [28]:

! 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 (no 802.1Q)

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)

Egress Queue Settings

The following in Figure 9 shows the mapping of the different traffic types to the corresponding egress queues of the switch:

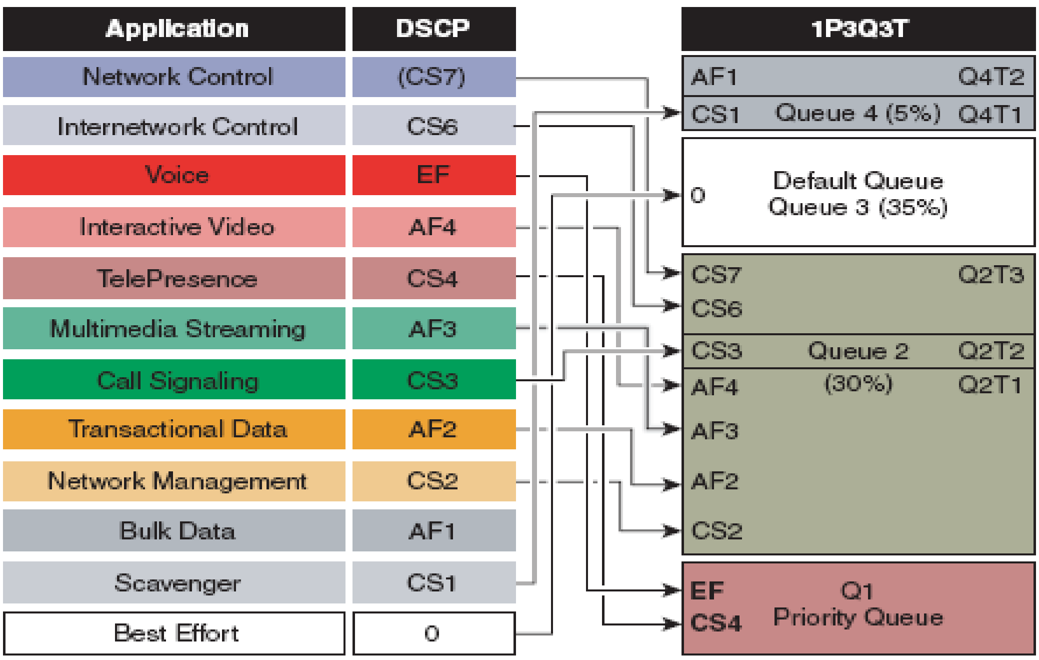


Figure 9 Switch 3750G Egress Queuing Recommendations for Telepresence

The following shows the config [28]:

! 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 (no 802.1Q)

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

4.3.2. QoS Recommendation Catalyst 4500

General Settings

!Enable of QoS on switch

qos

TelePresence Port Settings

!Trust DSCP value (no 802.1Q)

interface Gigx/y

qos trust dscp

OR

!Mapping CoS to DSCP values (only necessary for voice traffic others left to

! their default values

qos map cos 5 to 46

!Trust CoS value

interface Gigx/y

qos trust cos

!Trust CoS value only if Cisco TelePresence/IP Phone is attached

qos trust device cisco-phone

Uplink/Router Port Settings

!Trust DSCP value (no 802.1Q)

interface Gigx/y

qos trust dscp

OR

!Trust CoS value

interface Gigx/y

qos trust cos

Ingress Queue Settings

The Catalyst 4500 does not support ingress queuing – but tests have resulted in that the architecture is adequate for Telepresence.

Egress Queue Settings

The following in Figure 10 shows the mapping of the different traffic types to the corresponding egress queues of the switch:

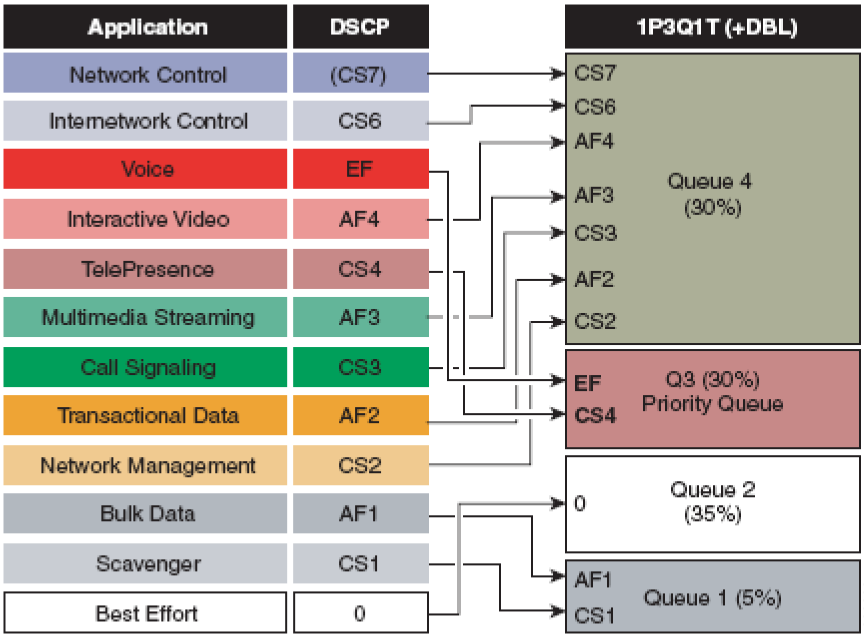


Figure 10 Switch 4500 Egress Queuing Recommendations for Telepresence

The following shows the config [28]:

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 Voice & TelePresence

4.3.3. WAN QoS Recommendation

The connection between Ankara and the both site in Istanbul are realized with Ether links using the MPLS Backbone from Turk Telekom. The needed bandwidth must be shaped to the Telepresence requirements. Following shows a configuration [28] example for the WAN router:

class-map match-all VOIP

match dscp ef =>Voice marking

class-map match-all TELEPRESENCE

match dscp cs4 =>TelePresence marking

class-map match-all CALL-SIGNALING

match dscp cs3 => Call-Signaling (Cisco)

match dscp af31

policy-map TP_BW_QOS

class VOIP

priority 100 =>LLQ for VoIP (1 Voice Call)

class TELEPRESENCE

priority 15000 256000 =>LLQ for CTS-3000 (Burst of 256000 Bytes for optimal TelePresence video signal transmission)

class CALL-SIGNALING

bandwidth 100 (100 kbitps must be more than sufficient)

policy-map TP_MAIN_POLICY

class class-default

shape average 3000000 60000 => **Bc=Shaped Rate*Tc** (optimal result for for TelePresence with Tc=20ms)

service-policy TP_BW_QOS

interface Port-channel1.250

description TELEPRESENCE_YENI_VLAN

bandwidth 30000

encapsulation dot1Q 250

ip address 200.200.200.1 255.255.255.0

service-policy output TP_MAIN_POLICY

4.4. Testing and Analysis

4.4.1. Bandwidth Requirement

For the bandwidth usage, we first need to define the nature of the bandwidth and how to quantify it, including any burst nature of the bandwidth . The bandwidth usage will be restricted on a rolling window basis to a target bandwidth. This bandwidth can burst up to 20% higher to a ceiling over this rolling window. So, assuming that the rolling window is 1s and the target bandwidth is 4Mbps, then in any given period of 1s the total bandwidth should average out to 4Mbps. (The rolling window means that the 1s window can be arbitrarily picked). The ceiling dictates that within the rolling window, we will never go above 20% higher than the target average. So, the maximum burst in a 1s rolling window could be as high as 4.8Mbps in this example (but will not be sustained at this rate). The burst is only on the Variable Bit-Rate (VBR) video stream and not the Constant Bit-Rate (CBR) audio stream. Also note that the rolling window is currently defined as 1s in the product, but is subject to change.

For a CTS-3000 at 1080 p with best motion handling, we have the following [28] one way bandwidth:

- 3 primary video streams (4000 kbps each): 12Mbps
- 3 primary audio streams (64Kbps each): 192Kbps
- 1 auxiliary audio stream: 64Kbps
- 1 auxiliary video stream: 500Kbps
- TOTAL (Average): 12,756Mbps
- TOTAL (Burst and Overhead): 15,3Mbps

For a CTS-3000 at 720p with best motion handling, we have the following [28] one way bandwidth:

- 3 primary video streams (2250 kbps each): 6.75Mbps
- 3 primary audio streams (64Kbps each): 192Kbps
- 1 auxiliary audio stream: 64Kbps
- 1 auxiliary video stream: 500Kbps
- TOTAL (Average): 7,506Mbps
- TOTAL (Burst and Overhead): 9,0Mbps

These burst 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 motion handling averages only 10-12 Mbps.

For all configurations, there is also an additional VoIP call of 64 Kbps possible that can be made from the Telepresence system IP Phone to another IP Phone or to the PSTN (if deployed and configured), but this traffic will not be between the two Telepresence endpoints in the call.

Bandwidth Consumption

Understanding bandwidth requirements of the calls based on codecs and video quality. At this bandwidth usage, TT has been visited on March 14, 2011 Cisco Office at San Jose, ABD.

Purpose of this visit is better understanding Telepresence solution, know how sharing and testing. Finding values in the Table-4, PoC report [29] have also been used.
It is given generally values [28] together calculated burst and overhead in Table-5.

Table 4 Test Data

Screen	Codec	Motion	Presentation	Bandwidth
3	1080p	Best	*	12.5M
3	1080p	Best	5 fps	15.0 M
3	1080p	Good	-	9.5M
3	1080p	Good	5 fps	11.5M
3	720p	Best	-	6.1M
3	720p	Best	5 fps	9 M
3	720p	Good	-	3.5M
3	720p	Good	5 fps	4.5M

Table 5 Product Data in Detail

Bandwith Consumption Kilobits Per Seconds(Kbps)				
Resolution	**1080p**	**1080p**	**720p**	**720p**
Motion Handling	Best	Good	Best	Good
Video Stream	4000	3000	2250	1000
Audio Stream	64	64	64	64
Video Channel (5fps)	500	500	500	500
Audio Channel	64	64	64	64
Single Screen Systems	4628	3628	2878	1628
Total Audio and Video	4756	3756	3006	1756
TOTAL (Average)	12756	9756	7506	3756
TOTAL(Burst and Overhead)	15307	11707	9007	4507

4.4.2. Burst Requirement

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 motion handling 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.

Determine the burst size 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.

The maximum IDR frame sizes observed during extensive testing of Telepresence systems was 64000 bytes. Therefore, the LLQ burst parameter should be configured to permit up to 64000 bytes of burst per frame per screen.

In the case of a triple-display CTS-3000 system, we should allow for 192000 bytes of burst (3 * 64000 bytes) in the rare event of a “triple-IDR storm,” where all three codec send IDR frames simultaneously. If the use of an auxiliary video stream is planned (e.g. for sharing PowerPoint presentations) additional 64000 bytes must be taken into consideration.

Recommended burst parameters:

CTS-1000:

Rate R = 5500 Kbits

Burst B = 128000 bytes (1080-best + aux video)

CTS-3000:

Rate R = 15000 Kbits

Burst B = 256000 bytes (1080-best + aux video)

CTMS:

Rate R = 198000 Kbits

Burst B = 4608000 bytes (1080-best + aux video)

For CTMS multiply CTS-1000 rate and burst with 36 (max of 36 segments per CTMS). Because for the current project only 3 CTS-3000 systems are used it will be sufficient to multiply CTS-1000 rate and burst with 9 (max of 3 x 3 = 9 segments in the project).

Configuration for policing, shaping and queuing:

Policing:

police bps [burst-max] conform-action action exceed-action action

police 15000000 256000 conform-action transmit exceed-action drop

The **policing rate** is indicated in **bitps** and the **burst** is indicated in **bytes** with this command.

Shaping:

shape [average | peak] mean-rate [[burst-size] [excess-burst-size]]

shape average 15000000 2048000

The **shaping rate** is indicated in **bitps** and the **burst** is indicated in **bits** with this command.

Queuing:

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

priority 15000 256000

The **queue bandwidth** is indicated in **Kbits** and the **burst** is indicated in **bytes**.

4.4.3. Latency Requirement

Cisco Telepresence has a network latency target of 150 ms one way (from codec Ethernet port to codec Ethernet port) [28]. We further divide that into 80% for the service provider (SP) and 20% for the enterprise. The 80% for the SP is from demarc to demarc (including the last-mile access circuit). So the SP gets 120 ms end-to-end from demarc to demarc. Those are the targets that the network should be engineered to. We established a threshold at 200 ms end-to-end (160 ms demarc to demarc) at which point it will trigger an alarm on the Telepresence system and generate a warning message to the user. This threshold is what the SPs Service Level Agreement (SLA) should be based on. Find Table-6 the recommended SLA (one way) and threshold behaviour:

Table 6 Recommended and Threshold Values for Latency

	Target	Warning Message	2nd Warning Message
End to End	≤150 ms	>200 ms	>400 ms
Service Provider	≤120 ms	>160 ms	>320 ms

80/20 split between Service Provider and Enterprise

80% allocated to the SP is from demarc to demarc - including the CE-PE link

20% allocated to the Enterprise

Service Provider should engineer their network to the Targets, but the Service Level Agreements (SLAs) should be based on the first threshold

Threshold behavior:

200 ms: “Experiencing network delay” warning message is displayed by the Telepresence system.

400 ms: “Experiencing severe network delay” warning message is displayed by the Telepresence system.

4.4.4. Jitter Requirement

Jitter within the system should be less than 5 ms peak, for a total of 10ms peak to peak [28]. Meaning, for example, if the average latency is 50ms, then the min and max latency should not be outside of 45-55 ms (or 10ms peak to peak). Controlling jitter in a Telepresence environment is extremely a key to a successful Telepresence deployment. Telepresence video is extremely sensitive to jitter, and video quality degrades very quickly in the face of jitter. Find Table-7 the recommended SLA (one way) and threshold behaviour:

Table 7 Recommended and Threshold Values for Jitter

	Target	Warning Message	2nd Warning Message
End to End	≤10 ms	>20 ms	>40 ms
Service Provider	≤5 ms	>10 ms	>20 ms

50/50 split between Service Provider and Enterprise

50% allocated to the SP is from demarc to demarc - including the CE-PE link

50% allocated to the Enterprise

Service Provider should engineer their network to the Targets, but the Service Level Agreements (SLAs) should be based on the first threshold.

Threshold behavior:

20 ms: “Experiencing network congestion” warning message is displayed.

40 ms - Step 1: System will lower motion handling from Best to Good.

40 ms - Step 2: If condition persists the call will be disconnected and "Call could not Proceed due to excessive network congestion" error message will be displayed.

4.4.5. Packet Loss Requirement

Packet loss should be under 0.05% [28]. If packet loss is above this number then the quality of your video will degrade significantly. Video in general is extremely sensitive to packet loss, and Telepresence video is even more sensitive. Packet losses along with jitter are the two most important factors that should be monitored in the network for Telepresence. Find Table-8 the recommended SLA (one way) and threshold behaviour:

Table 8 Recommend and Threshold Values for Packet Loss

	Target	Warning Message	2nd Warning Message
End to End	≤0,05 %	>0,1 %	>0,2 %
Service Provider	≤0,025 %	>0,05 %	>0,1 %

50/50 split between Service Provider and Enterprise
50% allocated to the SP is from demark to demark – including the CE-PE link
50% allocated to the Enterprise

Service Provider should engineer their network to the Targets, but the Service Level Agreements (SLAs) should be based on the first threshold.
Threshold behavior:
0, 1%: "Experiencing network congestion" warning message is displayed.
0, 2% - Step 1: System will lower motion handling from Best to Good.
0, 2% - Step 2: If condition persists the call will be disconnected and "Call could not proceed due to excessive network congestion" error message will be displayed.

CHAPTER 5

5. CONCLUSION

5.1. Summary

There are different types of traffic on the internet. But it is not easy to distinguish this traffic. When the talk about internet traffic, main problem is increasing delay and packet loss.

That is Why QoS is an important mechanism to distinguish packages which mean marking, regulating and scheduling and managing bandwidth.

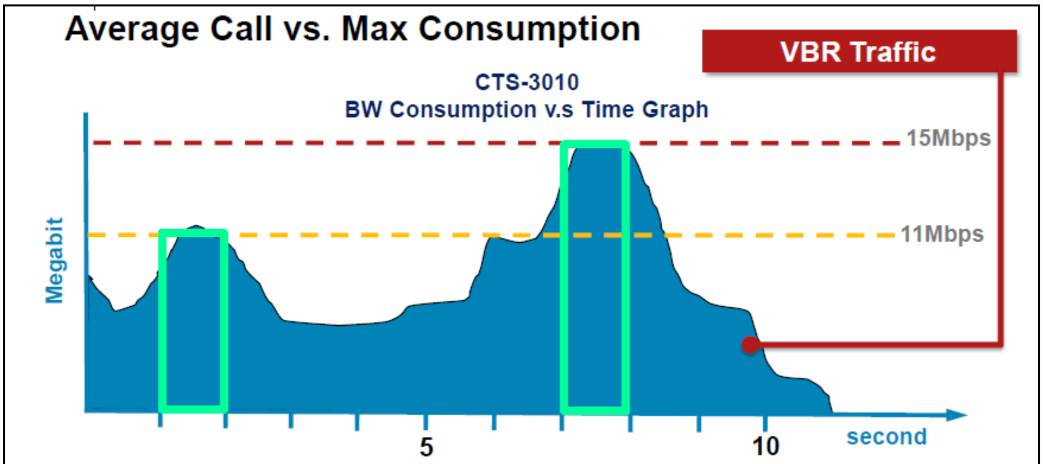
In our test bed mentioned in chapter 4, for our QoS scheme we used DiffServ, Class Based Fair Queuing with HTB, policer, Telepresence systems. Our DiffServ domain to provide QoS was used CBR and VBR in existing network.
Characteristic of HTB was observed by configuring rate and ceiling parameter as the PHB mechanism which provide packet scheduling and packet forwarding on the Router.

Policer mechanism regulates packet by setting up rate and burst parameter while transmitting video data.

In Figure 11, our pattern video content are changing with different transmission rate. Finally it was observed that a shaper eliminates burst traffic so result is good quality video.

QoS schemes are necessary because of bandwidth and delay. Telepresence systems use generally 1.5 Gbps lines. Using special code tolerates this bandwidth but it is not enough for transmitting video. At the same time it requires correct QoS mechanism.

The goal of this thesis is to establish good quality streaming video through DiffServ domain. So we calculated how much bandwidth is required for real time streaming video. To manage this bandwidth characteristic of real time video, compression scheme, multimedia application and content of the video are investigated.



"Average Call" Bandwidth Consumption Per Second							
Resolution	1080p	1080p	1080p	720p	720p	720p	720p
Motion Handling	Best	Better	Good	Best	Better	Good	Lite
CTS-500/1X00 *average* bandwidth (Mbps) *includes Layer 2- 4 overhead*	4 Mbps	3.5 Mbps	3 Mbps	3 Mbps	2.5 Mbps	1.5 Mbps	1 Mbps
CTS-30X0/32X0 *average* bandwidth (Mbps) *includes Layer 2- 4 overhead*	11 Mbps	10 Mbps	8 Mbps	8 Mbps	6 Mbps	3 Mbps	-

Figure 11 Average Call vs. Max Consumption

5.2. Future Work

In Order to understand well QoS Mechanism there are some recommendation such as;

How QoS performance will be affected by using different compression techniques with different video format?

If different compression technique is used (MPE2) behavior of the video would been change depending of compression technique in this case we have to deal with burst at the beginning of the video.

How will be the signaling for multi QoS Environment?

In our case one signal QoS agent is evaluated .This Agent is responsible for managing available bandwidth in DiffServ domain. But it also should be investigated in detail how it behaves in more than one QoS domain to understand how to communicate each other provide QoS.

How IPV6 versus IPV4 will affect QoS performance?

IPv4 has some limitations like less address space. IPv6 has been preferred due to larger address space, better mobility support, better auto configuration and aggregating router structure.

Therefore it would be useful to determine the QoS performance of real time video streams during transmission with the use of IPv4 and IPV6 networks together.
These topics will need further investigation.

REFERENCES

[1] **DHESIKAN, S.** (2001), *Quality of Service for IP Videoconferencing Engineering White Paper,* Cisco System, June 2001.

[2] **DOVROLIS C., RAMANATHAN P.** (1999), *A case for Relative Differentiated Services and the Proportional Differentiation Model*, University of Wisconsin-Madison, IEEE Network Journal, September-October 1999

[3] **PARK S.** (2008) *Quality of Service for Video Transmission.* University of New Brunswick, Faculty of Computer Science, August 2008.

[4] **DHESIKAN, S.** (2001), *Quality of Service for IP Videoconferencing Engineering White Paper*, Cisco System, June 2001.

[5] **ZHEN, L. et.al.** (2002) *Consideration and Research Issues for the Future Generation of Mobile Communication*, Canadian Conference on Electrical and Computer Engineering, vol. 3, pp. 1276-1281, 2002.

[6] http://en.wikipedia.org/wiki/Telepresence

[7] **HIRCHE, S., BUSS, M.** (2004) *Telepresence Control in Packet Switched Communication Networks*. Proceedings of the 2004 IEEE, International Conference on Control Applications, vol. 1, pp.236–241, 2004.

[8] **HOEGER R.** (2007), Telepresence Installation for Turk Telekom by Dimension Data, Project Document.

[9] **GARDINER, B.** (2008) *Expert Reference Series of White Paper*, Global Knowledge, 2008.

[10] http://www.alliedtelesis.com/media/pdf/qos_wp.pdf , pp. 8

[11] http://technet.microsoft.com/en-us/library/cc757120(v=ws.10)

[12] http://www.alliedtelesis.com/media/pdf/qos_wp.pdf , pp.10

[13] http://www.digitalpreservation.gov/formats/fdd/video_fdd.shtml

[14] **SZIGETI, T. et.al.** (2009), *Cisco Telepresence Fundamentals*, Cisco Press, 2009

[15] **YEOM, H.Y. et.al.** (1997), *An Efficient Transmission Mechanism for Stored Video*, Protocols for Multimedia Systems, Multimedia Networking, IEEE *Conference* on, pp. 122-130, 1997.

[16] **LI, H. et.al.** (2003), *An effective burstiness estimation model for VBR video stream,* Multimedia and Expo, 2003.ICME'03 Proceeding, 2003 International conference on, pp. 57-60, 2003

[17] **ROSE, O.** (1997), *Traffic Modeling of Variable Bit Rate MPEG Video,* University of Wurzburg, Department of Computer Science.

[18] **LAKSHMAN, T.V. et.al.** (1998), *VBR Video: Tradeoffs and Potentials,* Proceedings of the IEEE, vol. 86, pp. 952-973, 1998.

[19] **GIORDANO, S. et.al.** (2003), *Advanced QoS Provisioning in IP networks: The European premium IP projects.* IEEE Communication Magazine, vol. 41, pages 30-36, 2003

[20] **DUAN, Z.et.al.** (2004), *A core Stateless Bandwidth Broker Architecture for Scalable support of Guaranteed Services*, IEEE Transactions on Parallel and Distributed Systems vol. 15, pp. 167-182, 2004

[21] **ZHANG, H.Q., WU, Z.M** (2005), *Traffic Control in Linux-based Routers*, Ruan Jian Xue Bao/ Journal of Software vol. 16, pp. 462-471, 2005

[22] **TUNGABASKARARAO, V.** (2007), *End-to-End QoS Signaling for Real Time Data Streams*, MCS Thesis Faculty of Computer Science, University of New Brunswick, February 2007.

[23] **KUANG, T., WILLIAMSON, C.** (2002), *A Measurement Study of RealMedia Streaming Traffic*, Proceeding of SPIE-The International Society for Optical Engineering vol. 4865, pp. 68-79, 2002.

[24] **AHMED, T.et.al.** (2001), *Implementing MPEG-4 Video on demand over IP Differentiated Services.* Conference Record / IEEE Global Telecommunications Conference vol. 4, pp. 2489-2493, 2001.

[25] **SHEU, T.L., FANG, J.T.** (2000), *A buffer allocation mechanism for VBR video playback,* Communication Technology Proceedings, 2000. WCC-ICCT 2000, International Conference on vol. 2, pp. 1641-1644, 2000.

[26] **ZUBAIRI, J.et.al.** (2002). On Shaping and Handling VBR Traffic in a DiffServ Domain*,* ATS, Simulation Series vol. 33, pp. 10-15, 2002

[27] **T.TUNALI, T., ANAR, K.** (2006), *Adaptive available bandwidth estimation for Internet video streaming*, Signal Processing: Image Communication vol. 21, pp. 217-234, 2006

[28] Cisco Systems (2009), *Cisco Telepresence Network Systems 2.0 Design Guide*, March 5, 2009

[29] Turk Telekom (2011), *Proof of Concept Report,* 14 March 2011

APPENDICES

A. CURRICULUM VITAE

PERSONEL INFORMATION

Surname, Name **:** YURT, Serdar
Date and Place of Birth **:** 19.03.1974, ANKARA
Phone **:** 0 532 5489734
E-mail **:** syurt156@gmail.com

EDUCATION

Degree	**Institution**	**Year of Graduation**
BS	HU Statistical	1997
High School	Aydınlıkevler High School	1992

WORK EXPERIENCE

YEARS	**COMPANY**	**ENROLLMENT**
11.2008 - present	Türk Telekom A.Ş.	Team Leader
01.2003 - 11.2008	Fintek A.Ş.	Project Leader
01.1999 - 01.2003	Halkbank IT	Specialist

FOREIGN LANGUAGES

Advanced English