QoS SOLUTIONS FOR VIDEOCONFERENCING

By

Anis Zaihasmy Bin Zainal Abidin

Dissertation submitted in partial fulfillment of
the requirement for the
Bachelor of Technology (Hons)
(Information Technology)

JANUARY 2006

Universiti Teknologi PETRONAS
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

QoS SOLUTIONS FOR VIDEOCONFERENCING

By

Anis Zaihasmy Bin Zainal Abidin (3205)

A project dissertation submitted to the
Information Technology Programme
Universiti Teknologi PETRONAS
In partial fulfillment of the requirements for the
BACHELOR OF TECHNOLOGY (Hons)
(INFORMATION TECHNOLOGY)

Approved by,

(Mr.Anang Hudaya Muhamed Amin)

UNIVERSITI TEKNOLOGI PETRONAS
TRONOH, PERAK
JANUARY 2006

CERTIFICATE OF ORIGINALITY

This is to certify that I am responsible for the work submitted in the project, that the originality work is my own expect as specified in the references and acknowledgements and the original work contain herein have not been undertaken or done by unspecified sources or persons.

Anis Zaihasmy Bin Zainal Abidin

ABSTRACT

This project is intended to gain knowledge and apply the theory learnt about the need of QoS in videoconferencing and the various options available. Today's conferencing applications are now IP friendly, it can run on either dedicated lines (like ISDN or telephone lines) or IP networks. However, as most network administrators know, conferencing applications can wreak havoc on unprepared corporate networks. The key to successfully deploying conferencing applications is the activation of Quality of Service (QoS). QoS refers to a network's ability to reliably and consistently provide a certain level of throughput and performance. QoS for conferencing typically involves network availability, bandwidth, end-to-end delay, jitter, and packet loss. Simply stated, if the network doesn't conform to the minimum requirements in any of these areas, the conferences are doomed to fail. QoS can be achieved in a variety of ways, including over-provisioning (deploying additional bandwidth), data prioritization, and the use of QoS-enabled overlay or converged networks. Organizations have two main options for deploying QoS within their organizations; convergence or overlay. Convergence requires the use of QoS-capable WAN links throughout the organization. In many cases, this requires a fork-lift upgrade and migration of all network resources, which can place convergence out of reach of many cost-sensitive organizations. On the other hand, overlay networks allow a step-by-step migration from a non-QoS to a QoS network without the high cost and inherent risk of major network reconfigurations. In this way, overlay networks are a first step toward convergence.

ACKNOWLEDGEMENTS

First and foremost, thanks to the Lord Almighty for given me strength, wisdom and patience to complete this project.

I am indebted to many individuals who helping me through the completion of this project where their presence are the essence to make my project successful. They are people of my respects who involves directly or indirectly throughout this project.

First of all, I would like to express a lot of thank to Allah S.W.T to make my project smooth and successful. I also would like to express my gratitude to FYP Committee as they have managed to help me to be well prepared for my project.

As a most gracious mentor and guide, I would like to thanks my supervisor, Mr. Anang Hudaya Muhamed Amin for the tremendous support and guidance during this project. To all my colleagues, a bunch of thank for their time in giving me help and share their knowledge on this project.

Last but not least, I would like to express a special thank to my family members for their priceless support, encouragement, constant love, valuable advices and their understanding of me. Without all of them, I would not go further like where I standing right now. I hope the experience I have gained during the completion of this project will be beneficial, and bring warm and sweet memories to me.

TABLE OF CONTENTS

CERTIFICATION OF APPROVAL i

CERTIFICATE OF ORIGINALITY ii

ABSTRACT iii

ACKNOWLEDGEMENTS iv

TABLE OF CONTENTS v

CHAPTER 1: INTRODUCTION 1

1.1 Background 1

1.2 Problem Statement 2

1.2.1 Problem Identification . . . 2

1.2.2 Significance of Project . . . 3

1.3 Objective and Scope of Study . . . 3

CHAPTER 2: LITERATURE REVIEW AND THEORY . 5

2.1 QoS 5

2.1.1 QoS Measurements . . . 5

2.1.2 Why QoS 6

2.2 QoS – An End-to-End Concept . . . 8

2.2.1 QoS on the Local Area Network (LAN) 8

2.2.2 QoS on the Last Mile . . . 10

2.2.3 QoS on the Wide Area Network (WAN) 11

2.3 H.323 12

2.4 Gatekeeper 13

2.4.1 13

CHAPTER 3: METHODOLOGY AND PROJECT WORK . 15

3.1 Procedure Identification 16

3.1.1 Planning and Preliminary Data Gathering 16

3.1.2 Research and Data Collection . . 16

3.1.3 Data Compilation and Analysis . . 16

3.1.4 Simulation and Testing . . . 17

3.1.5 Implementation and Evaluation . . 17

3.2 Tools 17

CHAPTER 4: RESULT AND DISCUSSION . . . 18

4.1 Videoconferencing 18

4.1.1 Videoconferencing Architecture . 20

4.1.2 Characteristics of Successful Videoconferencing . . . 20

4.1.3 Summary of ITU Videoconferencing Standards 23

4.2 QoS 25

4.2.1 The Need for QoS . . . 25

4.2.2 Important QoS Parameters . . 26

4.3 QoS Solution Options 29

CHAPTER 5: CONCLUSION AND RECOMMENDATION . 35

REFERENCES 37

APPENDICES 38

CHAPTER 1

INTRODUCTION

1.1 Background

Videoconferencing, a technology that was once viable only for organizations with big budgets and dedicated staffing, is now readily available at price points that will attract even home-based business professionals and consumers. For the technology manager, videoconferencing represents a strategic technology that can deliver value for them and their organization by making people more productive and it doesn't mean just high-level decision-makers. Today's IT-oriented worker bees can also leverage videoconferencing to collaborate and communicate with colleagues and customers across town or across the globe.

Effective videoconferencing technology selection and deployment is a significant challenge. This is much more than an exercise in network capacity planning and desktop systems management. It's a business planning exercise as well. And with the unusual variation in videoconferencing alternatives (with major differences in quality, price, flexibility and functionality) the task of matching business needs and opportunities against available technologies is no easy task. The variation in videoconference systems architectures (including the end points and the network) also demands a careful review of existing and anticipated technology infrastructure, making this a technologically challenging assignment as well. Even though most people will be mounting a significant effort to properly deploy videoconferencing, they will need to realize what a great opportunity this can be for them and their organization and that it will be worth the effort to identify those applications where videoconferencing will work and work well.

1.2 Problem Statement

Quality of service (QoS) is the ability for an application to obtain the network service it requires for successful operation. Quality of Service for videoconferencing is really only noticed when the Best Effort service encounters congestion. A common question is why not provision more bandwidth, use Best Effort, and do away with complicated QoS architectures.

1.2.1 Problem Identification

i. Videoconferencing

Study about available videoconferencing technologies and understand about the difference approaches use in the real world. Research will be done to gain understanding about the technology (videoconferencing) and also about the characteristic of successful videoconferencing.

ii. QoS and why is it needed

This study will identify the real meaning of QoS use in videoconferencing and find the reasons about why QoS is needed for a successful videoconference. Other than that this study will also try to explain about the advantages of using QoS compared to others available solutions use to increase the performances of videoconferencing applications.

iii. QoS solutions

To identify and apply various options for QoS available solutions. This will be the main focused of this study.

1.2.2 Significance of Project

Acquiring and implementing one or two videoconference systems won't require a major overhaul of the network infrastructure. However, if planning to ramp up to deploy more than a few systems, we'll want to think through the implications for the WAN, LAN or Intranet infrastructure. Performance, flexibility, pricing and staff support are the key factors that we'll need juggle when arriving at an effective configuration. Videoconferencing based on today's data networks poses serious challenges, and only those organizations with the staff resources and commitment to state-of-the-art network technologies will be up to the task. Most of the rest of us will roll out videoconferencing more slowly, with ISDN playing a central role.

1.3 Objective and Scope of Study

The relevancy of this project is basically to study how videoconferencing work and implement QoS solution on it. The studies will include:

- Identify typical videoconferencing applications.
- Identify standard protocol use in videoconferencing.
- Identify videoconference system alternatives.
- Research on characteristics of successful videoconference solutions.
- Network consideration for videoconferencing.
- Identify common problem occurred.

All the information gathered will be use to design and implement QoS solution for videoconferencing systems. Basically there will be no specific product developed, but only simulation and testing will be conducted.

The objectives of this project are:

1. Able to understand of how videoconferencing work and why QoS is needed to ensure a successful videoconferencing.
2. Successfully deploying the appropriate level of QoS for videoconferencing in simulated environment.

CHAPTER 2

LITERATURE REVIEW AND THEORY

2.1 QoS

QoS, which stands for Quality of Service, is an overused term that describes the overall performance of a data network. Basically, QoS refers to how well and consistently a network can deliver predictable results. In other words, if a piece (or packet) of data enters a network in one location, just how well will that network be able to host that packet's travels from its point of origin to its final destination.

2.1.1 QoS measurements

Network quality of service is evaluated by measuring four key parameters: bandwidth, end-to-end delay, jitter, and packet loss.

- **Bandwidth:** The average number of bits per second that can travel successfully through the network.

- **End-to-end delay:** The average time it takes for a packet to traverse the network from a sending device to a receiving device.

- **Jitter:** The variation in end-to-end delay of sequentially transmitted packets.

- **Packet loss:** The percent of transmitted packets that never reach the intended destination.

For IP voice and video communications systems to work properly, the bandwidth should be as large as economically possible while the end-to-end delay, jitter, and packet loss should be minimized. Lower end-to-end delay leads to a more satisfactory, natural communications experience, while large delay values lead to unnatural conversations with long pauses between phrases or sentences.

2.1.2 Why QoS?

There must be adequate bandwidth in the network to meet the demands of the offered load. Even then, there could be contention for network bandwidth for short periods of time. This occurs because traffic in the network is not evenly spread during all times. When traffic arrives at a network device, the devices processes and forwards the traffic. The amount of traffic that a device can forward is limited by the capacity of its interfaces. There are certain times when too many packets arrive at a device at the same time. At such times, the device cannot forward all the packets immediately due to the limited capacity of its interfaces. These excess packets are either queued in a buffer or dropped. This causes congestion and results in delay and loss of packets.

Some ways to handle congestion are:

- **Over-provision the network**

One could add more bandwidth and over-provision the network to ensure that the need for bandwidth can be satisfied at all times. With over-provisioning, it is possible to prevent any conflict for resources. All incoming traffic can be serviced immediately since there is always sufficient capacity in the network. This may sound like an ideal solution. However, over provisioning leads to enormous wastage of valuable resources because the degree of over provisioning may need to be a factor of 10 or 100 the capacity needed to service the load successfully. Consequently, over-provisioning may not be the most desirable solution. [1]

- **Separate networks**

Separate networks can be set up for each application type so that there is no resource conflict between traffic types. For instance, an organization can have a network separate for voice, video and data. Like over provisioning, this results in poor utilization of resources. In addition, this only solves the problem of multimedia applications interfering with data applications. It does not solve the problem of having more voice traffic than there is bandwidth on the voice network, unless it is combined with over-provisioning. Therefore, the trend is to consolidate more and more applications over a single IP network. [1]

- **Quality of Service (QoS)**

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. During peak times, any device might delay and/or drop some packets to relieve congestion. For this solution to be effective, the QoS network devices must be able to differentiate among classes of arriving traffic and satisfy their individual requirements. QoS mechanisms provide a set of tools that can be used to do that. It enables the network to recognize traffic belonging to certain users and applications such that preferential services may be provided to them. (This is why QoS is also known as "managed unfairness"). Some QoS mechanisms also enable applications to provide information to the network to aid the devices in performing traffic classification. [1]

QoS is therefore the best way to handle contention for network resources when the network is intended to service widely varying types of traffic. It is important to emphasize that there should be sufficient network capacity to start with. QoS does not create any additional capacity. It just helps to manage the available resources according to policies set out by the network administrator.

2.2 QoS – An End-to-End Concept

In order to enjoy quality of service performance during a conference, that quality of service must be in place from one end of the conference to the other. In this way, quality of service is an end-to-end concept, and the QoS provided by a network is only as good as the weakest link in the network chain. This can have a dramatic impact on the scope of work, cost, and reality of activating QoS on a particular network.

When running time-sensitive applications on an IP network, one must realize that Ethernet networks were not designed to provide guaranteed levels of performance. Therefore, achieving quality of service requires that some combination of hardware, software, and/or intelligence be deployed throughout the following three parts of the network; the LAN, the "last mile," and the WAN.

2.2.1 QoS on the Local Area Network (LAN)

Many people believe that quality of service is not an issue on the LAN due to the emergence of 10mbps, 100mbps, and Gigabit LANs. While true that most LANs do have adequate bandwidth to carry IP videoconferencing traffic, adequate bandwidth alone does not guarantee consistent conferencing performance.

To understand this, we must consider that many networking companies recommend limiting LAN traffic to 30% or 40% of rated capacity. Therefore, a 100 mbps segment can actually handle only 30 mbps of traffic. Recognizing that a single LAN segment may actually serve 100 or more users, we can see how this segment could fill up very quickly. In fact, if even a few users activated bandwidth hungry applications (like FTP or even a web browser), conferences in progress may be impacted. There are two common solutions for this problem:

Option 1 – Intelligent Subneting

LAN contention can be managed by intelligently engineering and planning the network routing. For example, a company could choose to place all videoconferencing systems on only certain subnets to avoid co-mingling conferencing traffic with other LAN traffic. However, this is easier said than done and may involve a total re-design of the network and new IP address assignments. This is further complicated by the fact that in some cases a user's workstation is also their videoconferencing system. In the end, this is a costly, time consuming, and typically short-term solution.

Option 2 – The V-LAN

To minimize the commingling of data and conferencing traffic on the LAN, many companies choose to create a totally separate overlay network, often called a Video-LAN. Note that due to the similar nomenclature, many people confuse Video-LANs with Virtual-LANs (or V-LANs). However, while a Virtual-LAN is a software-based grouping of workstations and servers, a Video-LAN involves a totally separate, parallel network and therefore provides total isolation of conferencing traffic from other LAN data. Since most organizations have a limited number of videoconferencing systems deployed in each facility, creating a Video-LAN is relatively inexpensive compared to the cost of deploying other QoS management schemes on the LAN.

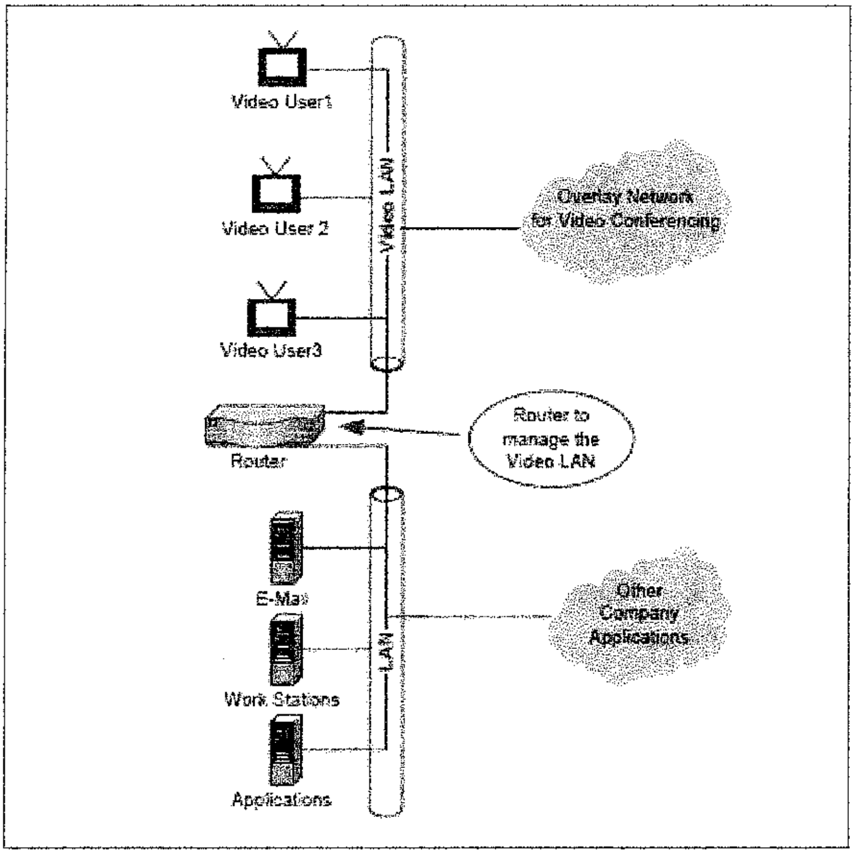

Video User1
Video User 2
Video User3
Video LAN
Overlay Network for Video Conferencing
Router
Router to manage the Video LAN
E-Mail
Work Stations
Applications
LAN
Other Company Applications

Figure 1: **Typical Video-LAN Configuration**

2.2.2 QoS on the Last Mile

QoS must also be maintained on the connections between the corporate LAN and the WAN. These connections, sometimes called the "local loop" or "last-mile" connection, typically consist of dedicated lines running from the end-user facility to the nearest point of presence (POP) of the network provider.

The type of last mile connection utilized depends upon a number of factors including the required bandwidth and the types of lines available. However, typical connections include T1s, T3s, DSL, frame relay, and ATM. Each of these connections can provide varying amounts of bandwidth and QoS control, and therefore the last mile is another area of concern for network designers.

2.2.3 QoS on the Wide Area Network (WAN)

For financial reasons, most companies purchase their WAN bandwidth from network service providers (NSPs) or telephone service providers (Telco's). To do so, they contact the provider and request a network connection, of a certain capacity, and QoS level, between certain locations. As one might imagine, larger pipes, higher QoS levels, and longer distances increase the monthly price for those lines.

It should come as no surprise that NSPs can only monitor and manage performance of network segments under their control. Therefore, network providers will often provide QoS guarantees only for network traffic traveling between their network points of presence (or POPs). This part of the provider's network is called the network backbone or core. In some cases, the NSP's scope of responsibility, or demarcation, ends at the point where the traffic leaves their POP. Alternatively, if the NSP provides both the WAN and the last-mile, the NSP's scope of responsibility may include the last-mile connections and perhaps even the switch/router on the customer's premises. It is important for conferencing and network managers to clearly understand the NSP's scope of responsibility.

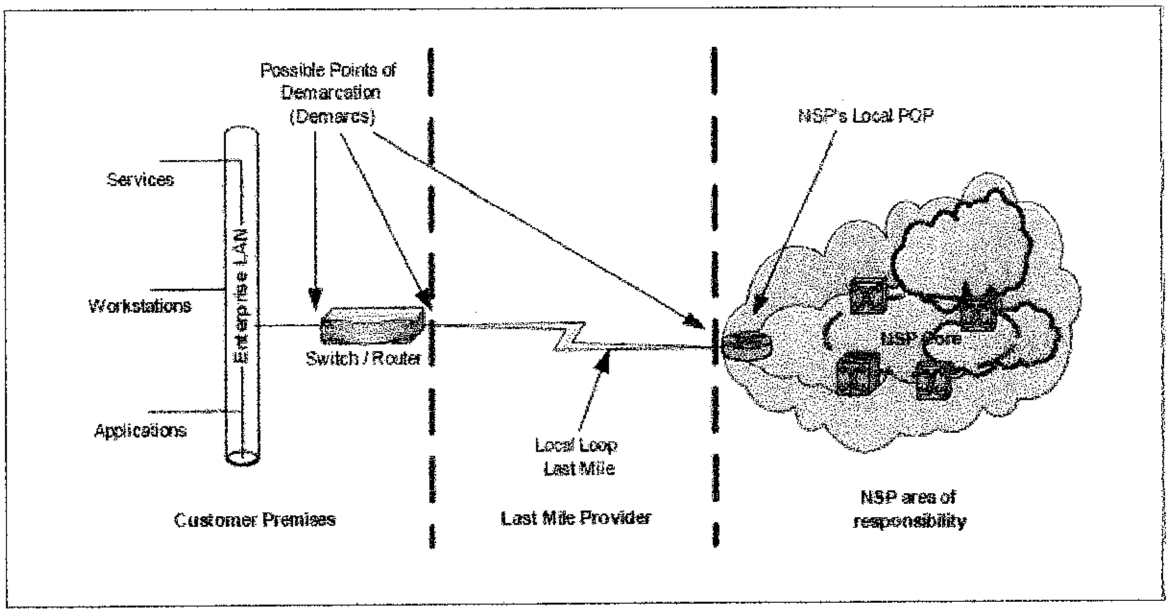


Figure 2: **Typical LAN / WAN Network**

2.3 H.323

Many IP video conference applications use the H.323 suite of protocols. The International Telecommunications Union (ITU) H.323 defines an international standard for multimedia over IP. ITU approved the first version of the H.323 standard in 1996. The current version is 4. Many applications now commonly deploy LAN based H.323 video systems. An example application is Microsoft NetMeeting, which utilizes H.323 for video conference and shared collaboration. [2]

H.323 Components

- H.323 Terminal
- H.323 MCU (Multipoint Control Unit)
- H.323 Gateway
- H.323 Gatekeeper
- H.323 Proxies

Previously, video conference systems with H.320 as a basis were common. Each system had its own Public Switched Telephone Network (PSTN) connection. As the left side of the ***figure 3*** shows, today we can use video gateways for communication between the converged H.323 network and the legacy video network. The right side of the ***figure 3*** shows how we can use video terminal adapters to link individual H.320 endpoints seamlessly in an H.323 network.

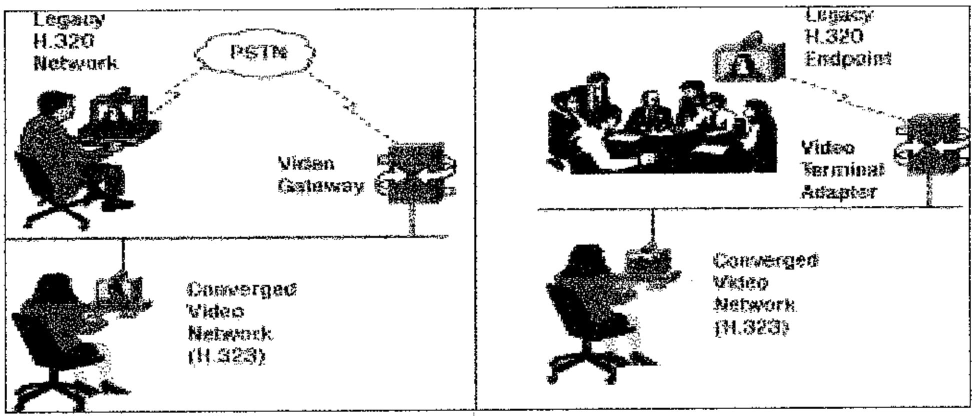


Figure 3

2.4 Gatekeeper

A gatekeeper provides services such as address translation and network access control for H.323 terminals, gateways, and MCUs. A gatekeeper can provide other services such as bandwidth management, and accounting. With a gatekeeper, dial plans can be centralized to provide scalability. Gatekeepers are optional in a H.323 network, but if a gatekeeper is present endpoints must use the services provided by it.

A zone is the collection of H.323 nodes such as gateways, terminals, and MCUs registered with the gatekeeper. There can only be one active gatekeeper per zone. Zones can overlay subnets and one gatekeeper can manage gateways in one or more subnets. [3]

2.4.1 Gatekeeper functions:

- Address Translation - translate H.323 IDs (such as abc1@domain.com) and E.164 numbers (standard telephone numbers) to endpoint IP addresses.

- Admission Control - control endpoint admission into the H.323 network via H.225 Registration, Admission, and Status (RAS) messages

- Bandwidth Control - manage endpoint bandwidth requirements via H.225 RAS messages.

- Zone Management - provide zone management for all registered endpoints in the zone, e.g. control endpoint registration.

- Call Authorization - Restrict access to certain terminals or gateways, possibly based on time of day.

- Call Management - Maintain active call information and use it to indicate busy endpoints or redirect calls.

- Bandwidth Management - Reject admission when the required bandwidth is not available.

CHAPTER 3

METHODOLOGY AND PROJECT WORK

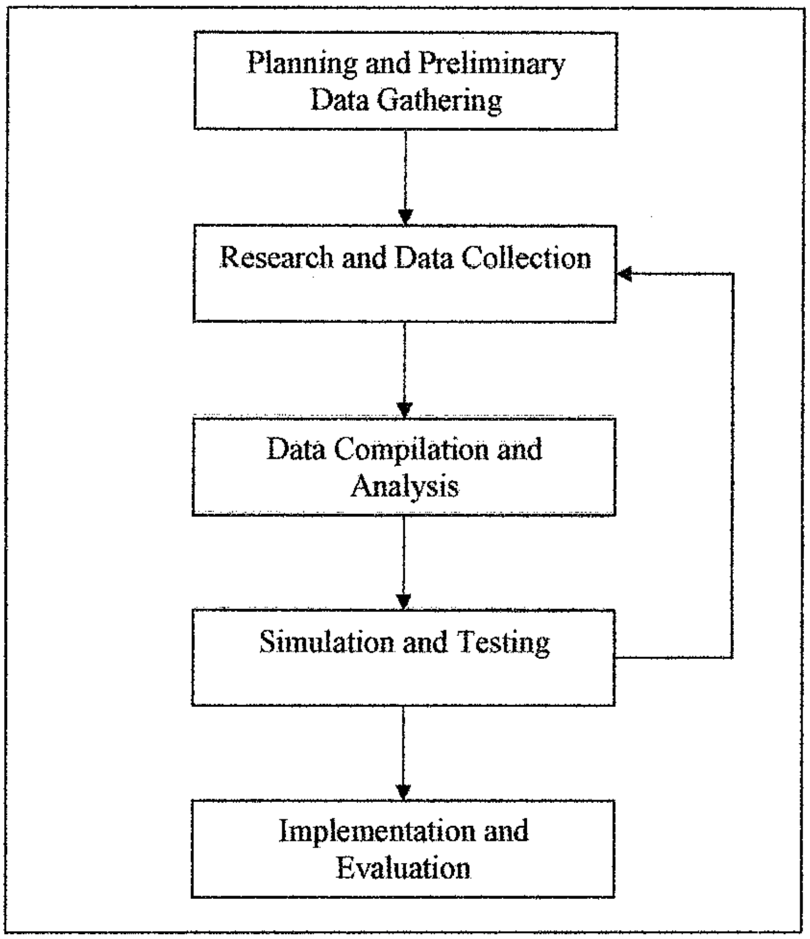

Planning and Preliminary Data Gathering
Research and Data Collection
Data Compilation and Analysis
Simulation and Testing
Implementation and Evaluation

Figure 4: **Project Methodology**

Figure 4 describes the flow of procedures that are planned for this project. The project begins with planning and preliminary data gathering and ended with implementation of the system and the evaluation.

3.1 Procedure Identification

3.1.1 Planning and Preliminary Data Gathering

This is the first phase of the project whereby all the essential activities that have to be done in order to ensure the effectiveness and smoothness of the flow of the project. All data need in research is gathered first to have the clear view of the project and understand more on the videoconferencing process. A timeline is also being prepared so that the flow of the project can be controlled and deadlines can be set.

3.1.2 Research and Data Collection

This phase is where further detail of all the important data from the preliminary data gathering is collected. More deep research are done to ensure good understanding about the topic and also to get familiar with all the technical terms used. The importance of this phase is to gain as much knowledge and understanding as possible especially on the QoS that applied on videoconferencing.

3.1.3 Data Compilation and Analysis

The result obtained upon the completion of the research procedures are conformed and analyzed. All the data are sorted and evaluated. The most important features and details will be put into account during the simulation and testing process.

3.1.4 Simulation and Testing

After analyze all the information and data gathered, the project will continue with simulation and testing phase. This is the most importance phase in the project because in this phase, it will determined whether all the theoretically information and data gathered can be apply into a real simulation or not.

Basically in this phase, all the QoS solution identified during the research process will be tested. If there any problem occurred during this phase, more research and data collection may need to be done again.

3.1.5 Implementation and Evaluation

This phase only can be done if the simulation and testing phase are successful. In this phase, all the successful test that have been done will be evaluate in order to make sure it meet all the project requirements and make any corrections if there any flaws encountered.

3.2 Tools

- Videoconferencing terminal.
  A pc equipped with camera, speaker, microphone and software for videoconferencing.
- Switch/router
- Multipoint Control Unit (MCU)
- Network performance monitoring software
- Windows 2000 operating system

CHAPTER 4

RESULT AND DISCUSSION

4.1 Videoconferencing

In telecommunication, the term videoconferencing has the following meaning:

1. A teleconference (live exchange of information among persons and machines remote from one another but linked by a telecommunication system) that include video communication.
2. Pertaining to a two-way electronic communication system that permits two or more persons in different locations to engage in the equivalent of face-to-face audio and video communications. Videoconferencing may be conducted as if all of the participants are in the same room.

Video conferencing has in the past been relatively expensive, but prices are now coming down considerably, as it is possible for anyone with a fast enough internet connection to operate a video conference. Sometimes the conferencing takes place over a private network or VPN, which guarantees better performance, but there will be a trend towards running video conferences over the public internet as technology improves.

Videoconferencing can be used for:

- conducting interviews
- holding meetings
- setting up meetings
- giving lectures

Videoconferencing has the advantage that it can reduce the need for travel. Basically, using a network, a camera and a headset with videoconferencing people can interact as if they were talking face to face in a room. There are two types of videoconferencing. One is called point to point conferencing which basically is a communication link between any two locations. Another is multipoint conferencing which is a link between varieties of locations (more than two). Multi point conferences can further be classified as two types, LAN and MCU (multi control unit). LAN provides links between different locations or groups. In a Multi Control Unit environment, audio and video signals are automatically switched during conferencing (perhaps to attend to bandwidth issues).

4.1.1 Videoconferencing Architecture

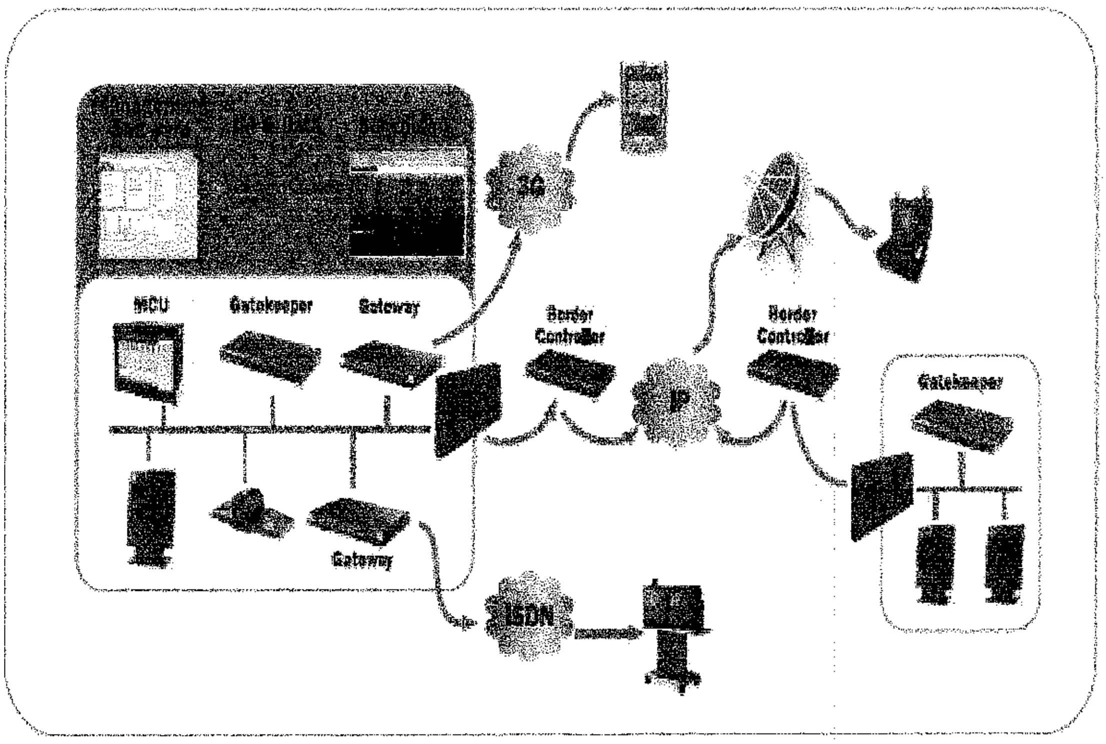


Figure 5: **Videoconferencing Architecture**

4.1.2 Characteristics of Successful Videoconferencing

The goal of any videoconferencing system is to provide an illusion, so that people look and feel like they are all sharing the same space, with each location an extension of the other sites that is seen through the monitor or other display device being used. Success is attained when technology is no longer noticeable and fades into the background and videoconference participants are able to focus on their conversation and their work.

The first factor affecting the ability of a system to achieve the illusion is the perceived quality of video and audio, and this is one of the primary factors to consider when evaluating any videoconferencing technology. This means rich, full-duplex audio with no echo or noticeable delays. Video quality is a function of frame rate, pixel resolution and monitor size. Video should be clear with rich colors, and it should be free of jerky movement, ghosting, freeze frames, or other visual anomalies.

Digitizing audio and video results in large amounts of data, which is extremely expensive to transmit across public or private networks. As a result, videoconferencing systems use some sort of lossy compression for digital audio and video. The ability of video and audio compression engines (codecs) to deliver good quality audio and video, given network bandwidth constraints, is partly responsible for the resulting perception of quality. Another important factor determining the perceived video/audio quality is the network itself. Unreliable or slow connections can destroy video and audio quality, no matter how good the monitor, or the speakers, or the codec, though some codecs will respond to these conditions better than others.

The quality issue is directly related to another prominent feature of alternative videoconference systems, which is price. This relationship can be stated plainly: The more we pay, the better the quality we'll see and hear. Videoconference systems at the low end include inexpensive desktop computer and plain old telephone system (POTS)-based systems that cost a few hundred dollars and offer postage stamp, jerky video and half-duplex audio. At the other extreme is the executive room system costing hundreds of thousands of dollars that has multiple cameras, microphones and monitors and offers near-broadcast quality video and audio across the WAN or the pubic switched network.

Another key characteristic is flexibility. The ability to interoperate with videoconference users on other systems, the ability to use the public switched network, the ease with which a system can service large numbers of participants, and the ability to share applications and documents as well as video and audio, are all considerations that determine the overall flexibility and functionality of systems we'll be evaluating.

Directly related to the flexibility issue, is adherence to standards. The International Telecommunications Union (ITU) has been very active in defining standards for videoconferencing over circuit switched digital networks, POTS, and packet networks

(LAN/intranet/Internet). The ITU standards define compression algorithms for video and audio, document and applications sharing, bandwidth aggregation and multipoint conference control. The standards enable interoperability, thereby ensuring a degree of flexibility that is an important consideration at all videoconference system price points.

Videoconference network requirements and their impact on existing and planned network applications is the other key characteristic on which you'll need to focus. Videoconferencing systems can consume large amounts of bandwidth, so it's critical to plan accordingly, whether it's bandwidth on the enterprise LAN and WAN or bandwidth obtained on demand from the public switched network.

Successful videoconferencing depends on the underlying network to deliver three important performance characteristics:

1. Isochronous transmission

Video and audio delivery must be sent and received continuously and in a synchronized fashion. Any irregularities in the transmission of either or both media streams will have a perceptible negative impact on the quality of the video and audio at the end points.

2. Bandwidth

For any reasonable quality video and audio, a sizable chunk of bandwidth is required. 128 Kbps is probably the minimum threshold for achieving any degree of audio/video quality.

3. Low Latency

Because a conference is interactive, any delay in the transmission of audio and video is quite noticeable. This is different from some audio/video broadcast applications, which are much less sensitive to transmission delays.

4.1.3 Summary of ITU Videoconferencing Standards

H.320 A suite of standards defining videoconferencing interoperability over ISDN. These standards define rules for establishing communications, framing and synchronizing media, and inverse multiplexing ISDN channels. H.320 also includes the following video and audio coding standards:

- **H.261** A video compression standard for bandwidth multiples of 64 Kbps
- **G.711** Basic audio compression at 48 Kbps to 64 Kbps -- low computation pulse code modulation technique same as used in regular telephony
- **G.722** Higher quality audio at the same bandwidths using more sophisticated audio processing
- **G.728** Lower bit rate audio compression -- 16 Kbps

H.323 A suite of standards defining interoperability of videoconferencing over packet switched networks with no guaranteed quality of service (QoS). These standards define the packetization and synchronization of media over non-QoS packet networks and a gateway for the interoperability of H.320 and H.323 systems. The following video and audio coding standards are part of H.323:

- **H.261** Same video compression standard also used in H.320 and H.323
- **H.263** An alternative compression standard for low bit rate communications
- **G.711, G.722, G.728** -- audio compression standards also used in H.320
- **G.723** Audio compression for 5.3 Kbps and 6.5 Kbps

H.324 A suite of standards defining videoconferencing interoperability over POTS that establishes low-bandwidth multiplexing/control protocols. H324 includes the following standards:

- **H.263** Although H.261 is included in the standard, H.263 is commonly used since it can compress video for very low bit rate transmission.
- **G.723** H.324 incorporates only low bit rate audio compression

- **V.80** Standard application interface for developing H.324 systems that convert synchronous data streams to modem asynchronous, enable rate adjustments during a call, and notify client software of lost packets

T.120 A suite of videoconferencing data collaboration standards that is included in the three H.32x standards described above. T.120 includes:

- **T.124** Conference control standard
- **T.126** Standard for sharing still images
- **T.127** Binary file transfer standard

4.2 QoS

Within a converged network, Quality of Service (QoS) is by far the most important implementation consideration. QoS is a networking term that specifies a guaranteed network data performance level. In practical terms, QoS is a mechanism to assure that audio and video data traverse the network with minimum delay. If network QoS is not in place, videoconferencing calls will be unreliable, inconsistent, and often unsatisfactory.

4.2.1 The Need for QoS

QoS helps us deal with contention between different users and applications for network resources. In this context, contention occurs when multiple applications simultaneously attempt to use the same network resources. Note that modern day networks are designed to operate well under a certain level of contention. However, when that contention reaches beyond an acceptable level, performance issues arise. Therefore QoS is needed to control the impact that applications can have on other applications.

There are two major factors that generate network contention; shared bandwidth and limited bandwidth.

- **Shared bandwidth**

  Contention is a byproduct of sharing network resources and bandwidth with other applications and users. Therefore, it is logical that in situations without shared bandwidth (e.g. dedicated lines that are used to support each application), one need not worry about contention. In this way, ISDN videoconferencing users and POTS (plain old telephone system) analog line audio conferencing users avoid contention by using dedicated lines for their applications.

- **Limited bandwidth**

  Since contention is caused by competition for existing network resources, it stands to reason that the greater your network resources, the less contention you will have. Taken to an extreme, one can all but eliminate the impact of contention just by providing adequate bandwidth. In fact, some organizations may find that over-provisioning their network is a less expensive and better short-term option than enabling QoS. One must understand, however, that deploying additional bandwidth without QoS control will not provide performance guarantees. In addition, it stands to reason that using high bandwidth applications (like videoconferencing) will contribute to network contention.

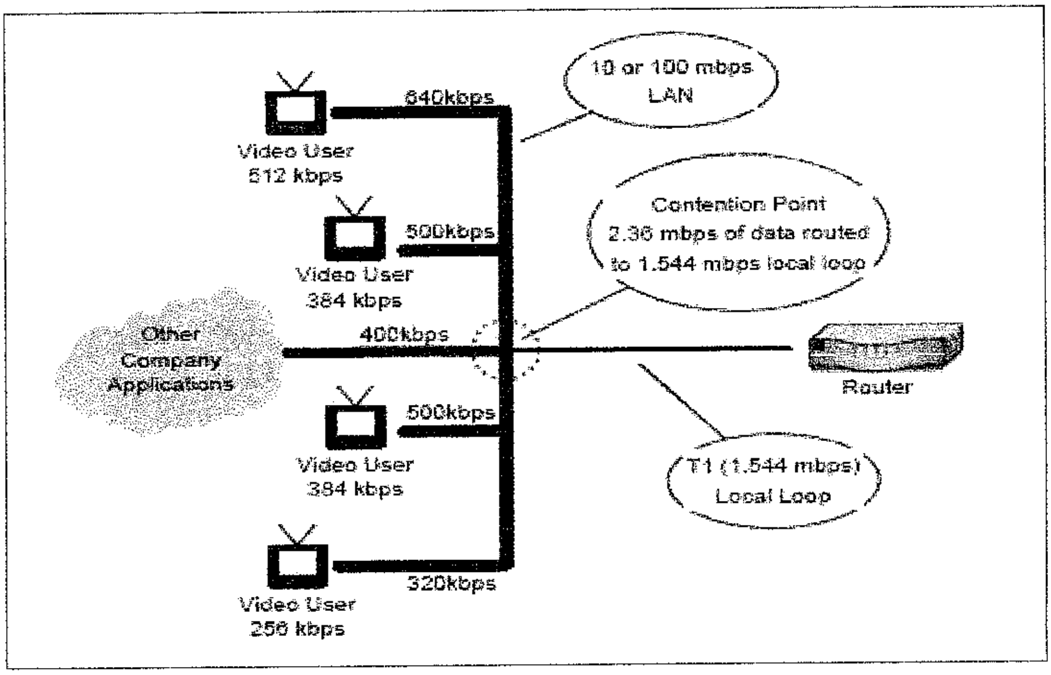


Figure 6: **Example of Network Contention**

4.2.2 Important QoS Parameters

For conferencing applications, we typically focus on five key performance parameters:

- **Availability** (uptime)

Availability refers to the percentage of time that the network is "up and running" and available to host data traffic. Measured in percentage of uptime, high quality network providers often provide three nines (99.9%), four nines (99.99%) or even five nines (99.999%) uptime guarantees. As a reference, a guarantee of "four nines of availability" indicates that the network will be down (or unavailable) for less than five seconds per month.

- **Bandwidth**

Bandwidth, also known as throughput, describes the capacity of an entire network or a portion of a network. Because the individual pieces of data that traverse a network are called bits, bandwidth is typically specified in bits per second (bps), kilobits per second (kbps), or megabits per second (mbps). For example, earlier modems provided a throughput of 300 bits per second. However, in today's conferencing networking environment, common network capacities include 384 kbps and 1.544 mbps, which can carry 384,000 and 1,544,000 bits simultaneously.

- **End-to-end delay**

End-to-end delay, often called latency, refers to the average time it takes for a piece of data to travel successfully through the network from the point of origin to the destination. Note that one unavoidable source of latency is the transmission delay involved in the physical transmission of the piece of data. Since a piece of data cannot travel faster than the speed of light, the transmission delay for a bit to travel from **location A** to **location B**, assuming a straight connection between those locations, would be 18.6 milliseconds (or .019 seconds). Additional delays are introduced by routers and other processing equipment in the network.

- **Jitter**

Jitter is a measurement of the variation in the end-to-end delay between consecutive packets of information. In other words, if it takes packet "A" 31ms (milliseconds) and packet "B" 44 ms to traverse the network, the jitter will be 13ms. Network ratings often include a maximum (i.e. not to exceed) value, in milliseconds, for jitter.

- **Packet loss**

Packet loss is a measurement of the percentage of packets that will, for a variety of reasons, not reach their destination. Typically, packet loss is the result of congestion within the network when too many pieces of information arrive simultaneously at a network router or switch. In most cases, networks will simply re-transmit lost packets, but for real-time applications (like conferencing), this form of recovery is not acceptable.

4.3 QoS Solution Options

- **Option 1 - Best Effort (Lack of QoS)**

The first option is really the choice not to deploy quality of service at all. In effect, these users are choosing to accept the problems associated with running conferencing traffic over a non-QoS-enabled network.

- **Option 2 – Intelligent Queuing**

As data traverses a network, it travels between devices called switches and routers. Similar to toll booths on an expressway, these network devices act as traffic cops directing traffic from one location to another. By controlling the priority these devices give to certain types of traffic, network designers can yield improved performance for certain applications.

When data arrives at a switch or router, it enters a queue (or a waiting line), and waits to be sent on its way. In addition, if too many pieces of data arrive at a single device simultaneously, the device may simply discard the newly arrived data to focus on processing the items already in the wait queues. Waiting in queues and overloading of switches and routers are common sources of latency (delay) and packet loss on data networks.

To improve performance, some network devices have multiple queues designed to process only certain types of traffic. Which queue a piece of network traffic reaches is determined by the value of certain bits in the packet's header, which are set by the originating device or another device on the source network. Through this priority queuing methodology, time-sensitive voice and video data is processed more quickly than non-real time data, resulting in improved QoS performance for those applications.

The two most common forms of intelligent queuing are IP precedence and DiffServ. Both IP precedence and DiffServ utilize bits of the data packet's header for prioritization. IP precedence modifies bits 9 – 11 in the header, or ID label, of the IP data packet and provides eight different classifications, ranging from a highest priority of seven to a lowest priority of zero. DiffServ uses bits 9-14 of the IP packet header and provides up to 64 different classifications, called types of service (TOS). Many videoconferencing endpoints, including current products from Polycom, TANDBERG, VCON, and Sony, have the ability to set the IP precedence and TOS bits during IP video calls. For endpoints without this capability, external QoS management devices can be deployed to set these priority bits. However, in environments utilizing either IP precedence or DiffServ, QoS will not be achieved unless all switches and routers in the network have the ability to process these prioritization requests. Therefore, devices that can't process these priority tags must be upgraded. For this reason, the deployment of IP precedence and/or DiffServ can be expensive and time consuming for many organizations.

- **Option 3 – Multi Protocol Level Switching (MPLS)**

Technically speaking, MPLS is a packet switching protocol defining how information traverses a data network. However, for the purposes of this project, we will focus on MPLS' inherent QoS capabilities and the performance enhancements MPLS offers compared to other QoS methods.

In conventional networks, packets forwarding (routing) decisions are made by each router in the packet's path from source to destination. This requires each router to perform the following tasks:

1. Receive the packet in the main input queue
2. Open the packet header
3. Analyze the packet's priority bits – if QoS is enabled (IP precedence or DiffServ)

4. Move the packet to the appropriate priority queue – if QoS is enabled
5. Look up the routing information from a lookup table
6. Forward the packet to the next router

The above process, and especially the look up in step five, can cause delays, bottlenecks, and even lost packets depending upon the flow of traffic to this router.

In MPLS networks, the data packets are tagged (labeled) with more descriptive headers that include both priority and routing (destination) information. In effect, the packet's path through the network is pre-defined when it enters the network. Therefore, when the packet arrives at a router, the router can make forwarding decisions based on the contents of the packet header (or label) instead of a time-consuming look up.

As is the case with other QoS options, MPLS must be enabled on all routers and switches throughout the network in order to be effective. This may require hardware and/or software upgrades throughout the network. Once activated, MPLS provides a significant performance improvement and allows for effective convergence of voice, video, and data over a single data network. However, it is important to understand that MPLS, like the other queuing options, does not in itself guarantee packet delivery. Should network traffic exceed the capacity of the network routers, MPLS networks will experience delays and dropped packets. In effect, MPLS could be considered an intelligent form of best-effort and a solid mixture of performance and cost-effectiveness.

Due to the high cost, complexity, and the need to outfit the entire network, MPLS tends to be out of reach of most enterprise networks. However, a number of service providers have deployed MPLS over all or part of their network. By purchasing services from these companies, enterprise organizations can enjoy the benefits of MPLS on their WAN without the need to build an MPLS network.

- **Option 4 – ATM**

The QoS options described previously have involved the prioritization of data traffic within network switches and routers. In many situations, these "best effort" methodologies will yield the desired performance on the data network. However, when performance guarantees are required, ATM networks may be a better option. ATM, which stands for asynchronous transfer mode, is a switching technology designed for high-performance multimedia networking. For our purposes, there are four important aspects of ATM as follows; virtual circuits, class of service, fixed-cell length, and hardware switching.

Virtual Circuits -- ATM allows the creation of virtual circuits (or VCs), which according to the International Engineering Consortium, is an end-to-end connection with defined end points and routes, but without any dedicated bandwidth. Bandwidth for virtual circuits can be configured either as static (called a permanent virtual circuit or PVC) or dynamic (called a switched virtual circuit or SVC). The use of VCs means that data traveling across an ATM network rides on a virtual dedicated highway, totally segregated from other traffic. For this reason, ATM networks are able to provide performance guarantees and a level of QoS beyond that provided by best-effort, DiffServ, IP Precedence, and MPLS networks.

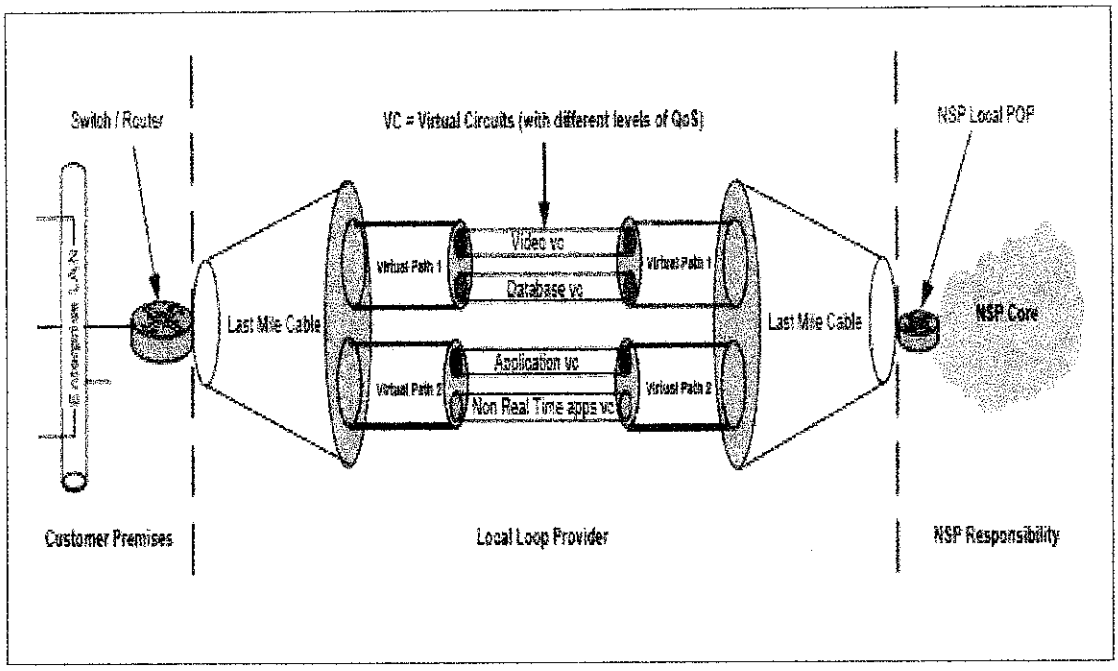


Figure 7: **Virtual Circuits in an ATM Transmission Link**

In this figure, the video traffic is traveling along a virtual circuit (labeled "Video vc") within virtual path 1 and provides a specific level of Quality of Service. The database traffic, application traffic, and non-real time application traffic are segregated in their own virtual circuits, and therefore the data will not commingle with other traffic.

- **Option 5 – Non-Standard Based Solutions**

Although IP Precedence, DiffServ, MPLS, and ATM CoS are the most common "standards-based" forms of QoS delivered today, there are many other non-standards based solutions, each of which approach QoS problems from a different direction. For example, one company offers time-based packet sequencing as a means of scheduling packet delivery through IP networks. This requires the installation of specialized hardware throughout the network, but provides increased throughput and certain performance guarantees. Another company offers a QoS monitoring engine that analyzes network performance and re-routes traffic, in-real time, onto secondary (or overlay) networks to circumvent QoS issues. For example, using this technology a company could run its priority traffic over the Internet (using a secure, encrypted VPN) and divert it onto a more-expensive dedicated network when the Internet's performance falls below a certain threshold. By using the Internet to carry much of their traffic, companies can significantly decrease their bandwidth requirements and networking costs.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

For many organizations, the only way to successfully host conferencing applications on their LAN / WAN will be to activate quality of service on their network. This is a must to ensure that bandwidth hungry applications, like videoconferencing, do not step on other mission critical data applications.

As described in this document, QoS is an end-to-end concept. In other words, QoS must be in place on all network links in the data path in order to be effective. In effect, network performance is only as strong as the weakest link in the data chain. Therefore, the benefits of a QoS enabled WAN may be blocked by an inadequate local loop or enterprise LAN. This means that network administrators must view QoS from a bird's-eye view in order to plan a successful QoS project.

Depending upon network topology and cost limitations, organizations can choose between a variety of QoS options including prioritization (DiffServ and IP Precedence), MPLS, and ATM networks. In most cases, higher performance networks are more expensive than those with lower levels of QoS. Therefore, organizations should carefully evaluate their requirements and plan their networks accordingly.

As a recommendation, for the future, this kind of project should try to develop own network monitoring system that able to monitor all the QoS aspects to make it easy for network administrators to monitor their videoconferencing and network performances.

REFERENCES

Subha Dhesikan, June 2001. ***Quality of Service for IP videoconferencing, Engineering White Paper.*** CISCO Press.

Dr. Peter J. Welcher, 2003. ***Quality of Service (QoS) and H.323 Gatekeepers for IP Video Conferencing.*** Chesapeake Netcraftsmen.

Ira M. Weinstein, December 2004. ***Making the Best of ISDN-Based Videoconferencing.*** Wainhouse Research.

Sue Spielman, Liz Winfeld, 2003. ***The Web Conferencing Book: Understand the Technology.*** AMACOM.

Sanjay Jha, Mahbub Hassan, 2002. ***Engineering Internet QoS.*** Artech House.

Zheng Wang, 2001. ***Internet QoS: Architecture and Mechanism for Quality of Service.*** Morgan Kaufmann.

Mike Flannagan, Richard Froom, Kevin Turek, 2003. ***Cisco Catalyst QoS: Quality of Service in Campus Network.*** CISCO Press.

David McDysan, 2000. ***QoS & Traffic Management in IP & ATM Networks.*** Mc Graw Hill.

Tim Szigeti, Christina Hattingh, 2004. ***End-To-End QoS Network Design: Quality of Service in LANs, WANs and VPNs.*** CISCO Press.

H. Jonathan Chao, Xiaolei Guo, 2001. ***Quality of Service in High-Speed Networks.*** IEEE.

Online References:

http://www.cisco.com
http://www.ciscopress.com
http://www.conferzone.com/
http://www.radvision.com
http://www.opalsoft.net/qos/
http://video-conferencing-guides.com/
http://www.webopedia.com/TERM/V/videoconferencing.htm
http://www.aarnet.edu.au/engineering/networkdesign/qos/what.html
http://www.ja.net/developement/qos/janet-qos-1.doc
http://www.ivci.com/videoconferencing-the-need.html

APPENDIX

DEPLOYING QoS TO ENHANCE MULTIMEDIA NETWORK PERFORMANCE
(http://www.microsoft.com/windows2000/techinfo/reskit/deploymentscenarios/scenarios/qos_install_qos_packetscheduler.asp)

1. Installation of QoS Packet Scheduler

QoS Packet Scheduler must be installed on all end-systems (clients) that make reservations on subnets. It is also possible to install QoS Packet Scheduler on the servers running QoS ACS. This allows priority to be given to the RSVP messages that are processed on the server. We installed QoS Packet Scheduler on each of the Windows 2000 Server computers running QoS ACS.

Note For RSVP packets to be generated from the clients that are using NetMeeting, you must have a sound card, video card, and PC video camera installed.

The following procedure was used to install QoS Packet Scheduler on the computers running Windows 2000 Professional and Windows 2000 Server, with QoS ACS installed, in both the Seattle and Milan sites.

Note You need Administrator rights on the local machine to install QoS Packet Scheduler

To install QoS Packet Scheduler

- From the **Start** menu, point to **Settings**, and then click **Network and Dial-up Connections**.
- Click the Local Area Connection on which you want to install QoS Packet Scheduler, and then on the **File** menu, click **Properties**.
- Click **Install**, click **Service**, and then click **Add**.
- Click **QoS Packet Scheduler**, and then click **OK**.
- Click **Close** twice.

2. Installation of QoS Admission Control Service

We installed QoS Admission Control Service on two separate computers running Windows 2000 Server in the same subnet in the Seattle office, and then installed QoS ACS in a different subnet for the Milan office. This ensures that subnet resources are managed, even when the primary QoS ACS server is not available.

The following procedure was used to install QoS Admission Control Service on the computers running Windows 2000 Server in both the Seattle and Milan sites.

Note You need Administrator rights on the local machine to install QoS Admission Control Service.

To install QoS Admission Control Service

- From the **Start** menu, point to **Settings**, click **Control Panel**, and then double-click **Add/Remove Programs**.
- Click the **Add/Remove Windows Components** icon, select **Networking Services**, and then click **Details**.
- Select the **QoS Admission Control Service** check box, and then click **OK**.
- Click **Next**.
- Click **Finish** to close the Windows Components Wizard.
- Click **Close** twice.
- Click **Close.**

After installing QoS Admission Control Service in the Seattle site, we then configured QoS Admission Control Service for the subnet 172.16.20.0/22.

3. Configuration of QoS Admission Control Service for the Seattle Site

We performed the following tasks when configuring QoS Admission Control service for subnet 172.16.20.0/22 in the Seattle site:

- Creation of a subnet object
- Configuration of traffic properties for the subnet
- Selection of QoS ACS Servers
- Configuration of logging settings
- Configuration of enterprise settings

Creation of a Subnet Object for the Seattle Site

Note You need Enterprise Administrator rights and Administrator rights on the local computer to create a subnet object and configure its properties. This can be configured by using the **Computer Management** program located in **Administrative Tools**.

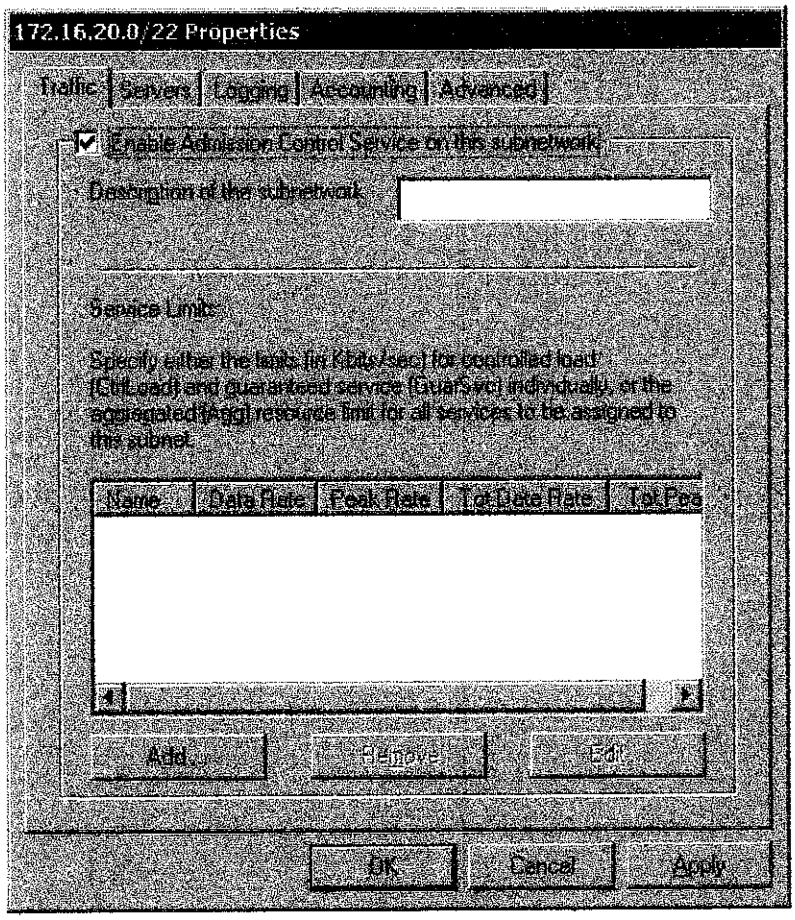
By creating a subnet object, we applied a common set of properties to all QoS-enabled clients managed by QoS ACS on that physical subnet. The following procedure was used to create a subnet object.

To create a subnet object

- From the **Start** menu, point to **Programs**, click **Administrative Tools**, and then click **QoS Admission Control**.
- Right-click the **Subnetwork Settings** folder, and then click **Add subnetwork**.
- In the **Create Subnetwork** box, type **172.16.20.0/22**.
- Click **OK** to close the **172.16.20.0/22 Properties** dialog box.

Note It is also possible to create the subnet objects through the **Active Directory Sites and Services** MMC snap-in. Then, after the **Enable Admission Control Service on this subnetwork** box has been selected for that subnet object by using **QoS Admission Control**, as shown in Figure 1, the subnet object in **Active Directory Sites and Services** can be distinguished from the other, non-QoS ACS–configured subnet objects, by the ACS container.

Figure 1 Enabling QoS Admission Control Service



☑ Enable Admission Control Service on this subnetwork

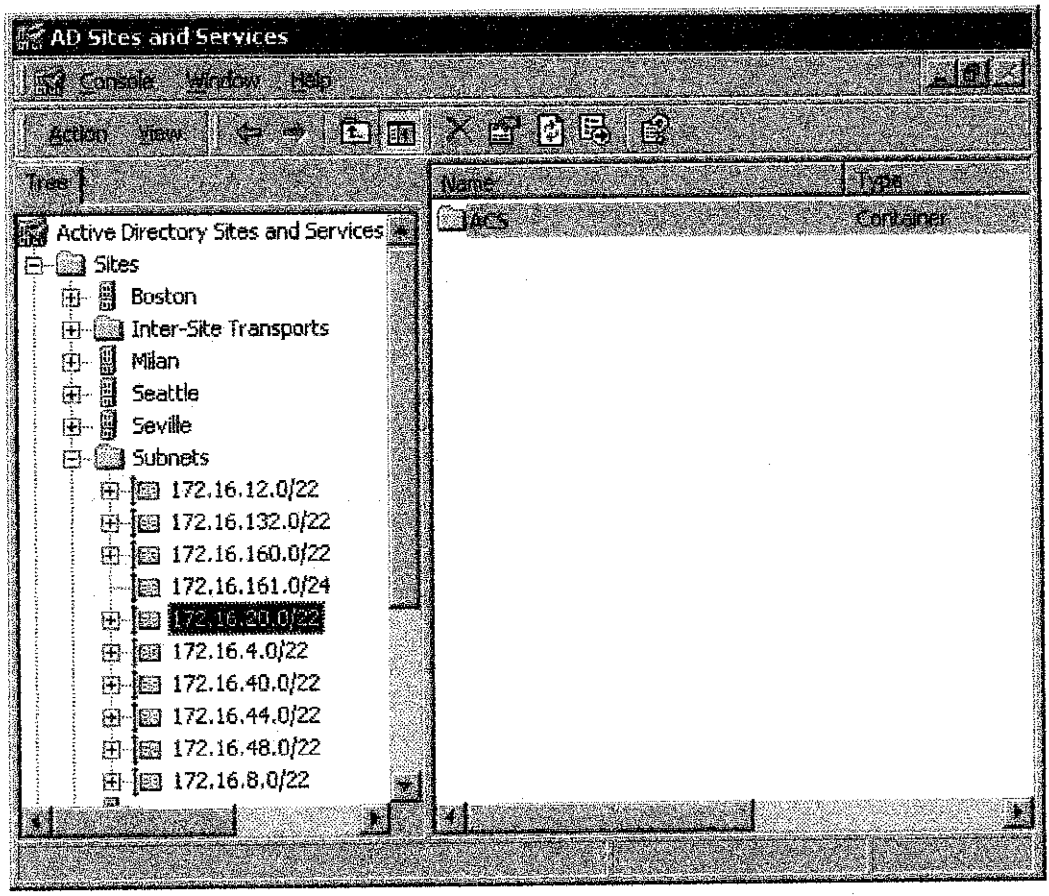
Description of the subnetwork:

Service Limits:

Specify either the limits (in Kbits/sec) for controlled load (CtrlLoad) and guaranteed service (GuarSvc) individually, or the aggregated (Agg) resource limit for all services to be assigned to this subnet.

Name	Data Rate	Peak Rate	Tot Data Rate	Tot Pea

Figure 2 QoS ACS container for subnet in Active Directory Site and Services snap-in



Configuration of Traffic Properties for the Seattle Site

Because the newly-created subnet object is linked to the physical subnet, we can control the traffic limits for the subnet. When we configured the traffic properties for subnet 172.16.20.0/22, we assumed the following:

- 100 megabits per seconds (Mbps) Ethernet is used for the LAN in both Seattle and Milan.
- Each NetMeeting video conferencing session (point-to-point) does not use more bandwidth than 500 kilobits per second (Kbps), even during peak flows.
- On average, in subnet 172.16.20.0/22, no more than two users at a time will use NetMeeting for a video conferencing session.

Analyze traffic on your LAN to ensure that the values entered in the traffic properties correctly reflect your specific network environment.

The following procedure was used to configure the traffic limits for subnet 172.16.20.0/22.

To configure traffic limits for 172.16.20.0/22

- From the **Start** menu, point to **Programs**, click **Administrative Tools**, and then click **QoS Admission Control**.
- In QoS Admission Control, highlight **Subnetwork Settings**, and then double-click on the subnet address **172.16.20.0/22**.
- Click the Traffic tab and verify that the Enable Admission Control Service on this subnetwork box is checked.
- Click **Add**, and then in the **Service Type** list, click **Aggregate**.

We selected **Aggregate** because of the real-time traffic needs (video and voice) of the video conferencing software. If we needed QoS for video only, without voice, then we would've selected **Controlled Load.** On the other hand, if we needed QoS for voice only, then we would've selected **Guaranteed Service**.

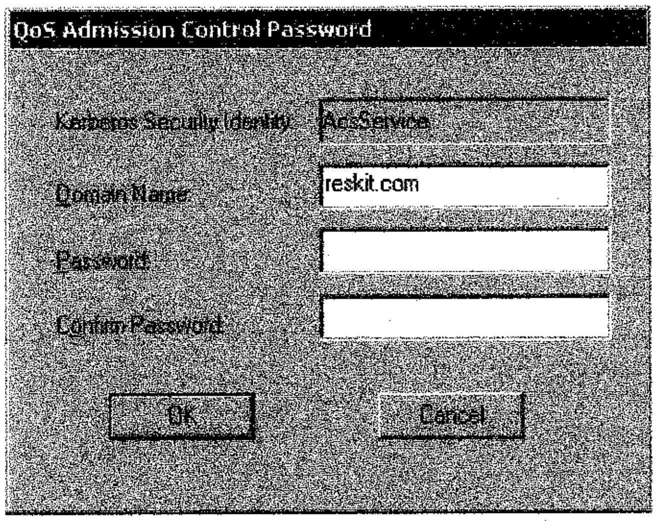
- Click **Data rate per flow**, and then type **500** in the text box.
- Click **Peak data rate per flow**, and then type **500** in the text box. This value must be equal to or greater than **Data rate per flow**.
- Click **Aggregate data rate**, and then type **2000** in the text box. This value must be equal to or greater than **Peak data rate per flow**.
- Click **Aggregate Peak data rate** and then type **2000** in the text box. This value must be equal to or greater than **Aggregate data rate**.
- Click **OK**.

Selection of QoS ACS Servers

It is necessary to select which Windows 2000 servers are allowed to run QoS Admission Control.

- From the **Start** menu, point to **Programs**, click **Administrative Tools**, and then click **QoS Admission Control**.
- In QoS Admission Control, highlight **Subnetwork Settings**, and then double-click on the subnet address **172.16.20.0/22**.
- Click the **Servers** tab, and then click **Add**.
- Select **SEA-NA-FP-04**, click **Add**, and then click **OK**.
- In the **Domain Name** box type **reskit.com**, as shown in Figure 3.

Figure 3 AcsService account dialog



QoS Admission Control Password

Kerberos Security Identity: AcsService

Domain Name: reskit.com

Password:

Confirm Password:

Important It is necessary to enter the root domain name, reskit.com, even though the QoS ACS server is installed on a computer in the child domain of noam.reskit.com. This is also true when configuring the other QoS ACS servers, SEA-NA-FP-05, MIL-EU-FP-03, and MIL-EU-FP-04. You must always create the AcsService account in the root domain of an enterprise.

- In the **Password** and **Confirm Password** boxes, type a strong password for the AcsService account, and then click **OK**.
- Click **Apply**, and then click **OK**.

From the same computer used to access and configure SEA-NA-FP-04, we followed the same steps to add SEA-NA-FP-05, which acts as a backup QoS ACS server for fault tolerance.

Configuration of Logging Settings

We enabled QoS logging so we can assess network bandwidth needs and monitor the number of users who regularly reserve resources on the network.

To enable RSVP message logging

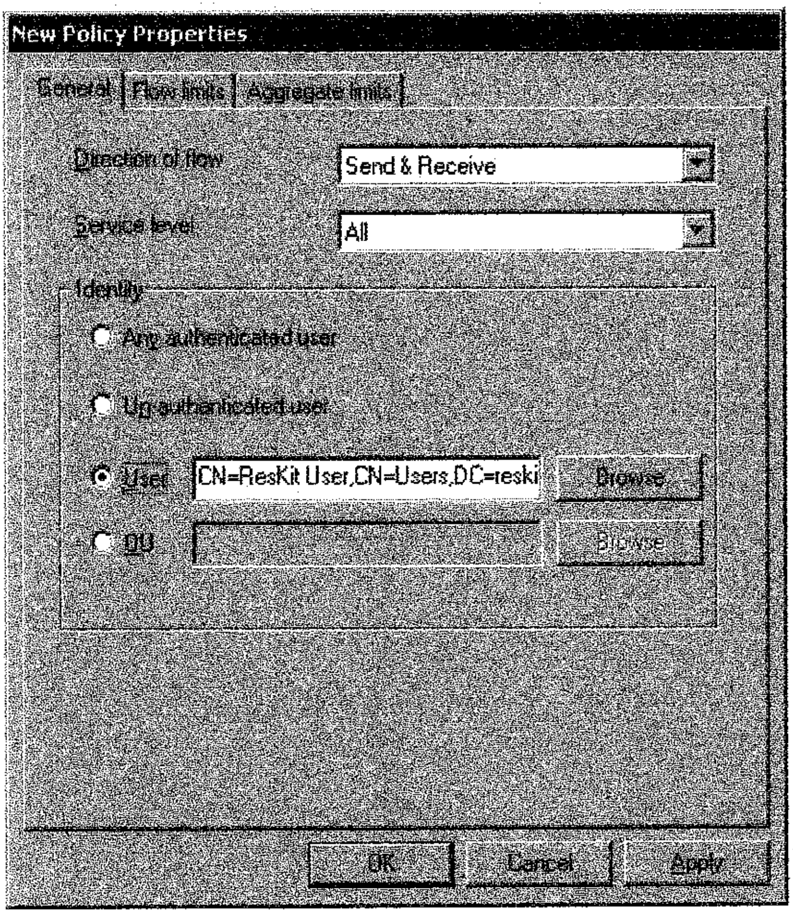
- From the **Start** menu, point to **Programs**, click **Administrative Tools**, and then click **QoS Admission Control**.
- In QoS Admission Control, highlight **Subnetwork Settings**, and then double-click on the subnet address **172.16.20.0/22**.
- Click the **Logging** tab, select **Enable RSVP message logging**, and then click **OK**.

Configuration of Enterprise Settings

Enterprise settings are for controlling the policies of QoS users on the subnets that are managed by QoS ACS. The majority of QoS users will have the same policies and because we know that all QoS client users have the same QoS-related bandwidth needs, we accepted the default settings already configured in both of the default polices, **Un-Authenticated User** and **Any Authenticated User**.

If there were any users or groups of users that needed exceptions to the default polices, then we can set a specific policy for that user or group by adding a new policy under Enterprise Settings. For example, by adding a new policy under **Enterprise Settings**, it is possible to assign policies to a specific user, as shown in Figure 4.

Figure 4 New Policy Properties — User



Direction of flow: Send & Receive

Service level: All

Identity

○ Any authenticated user

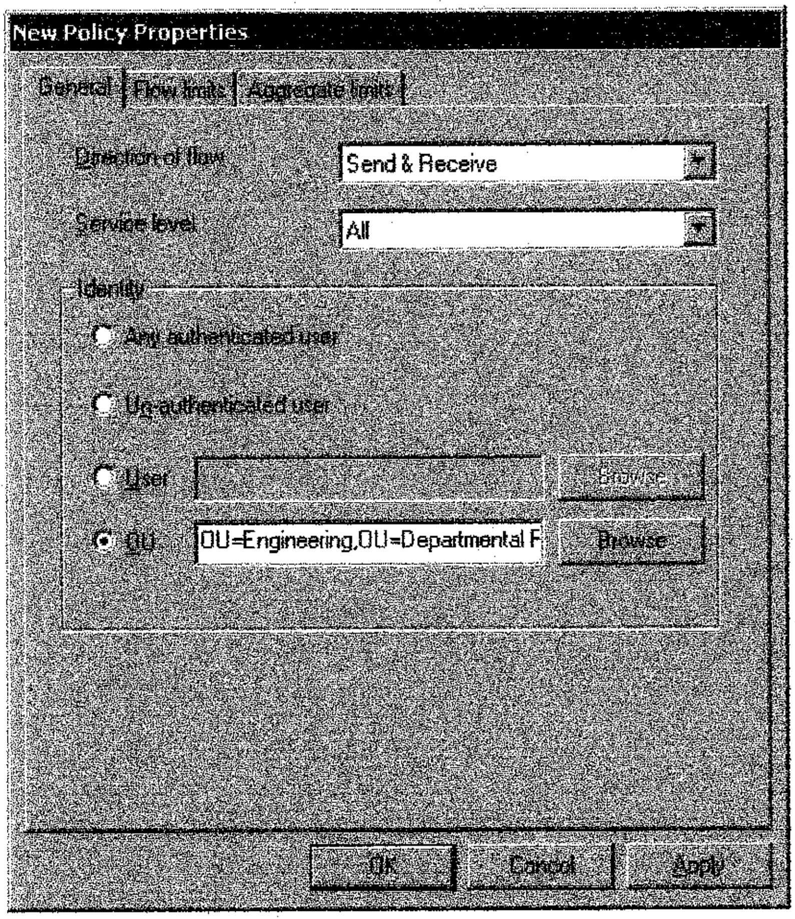
○ Un-authenticated user

● User CN=ResKit User,CN=Users,DC=reski

○ OU

Or, it is possible to assign policies to a group of users or computers by using organizational units (OUs) in Active Directory®, as shown in Figure 5.

Figure 5 New Policy Properties — OU



New Policy Properties

General | Flow limits | Aggregate limits

Direction of flow: Send & Receive

Service level: All

Identity

○ Any authenticated user

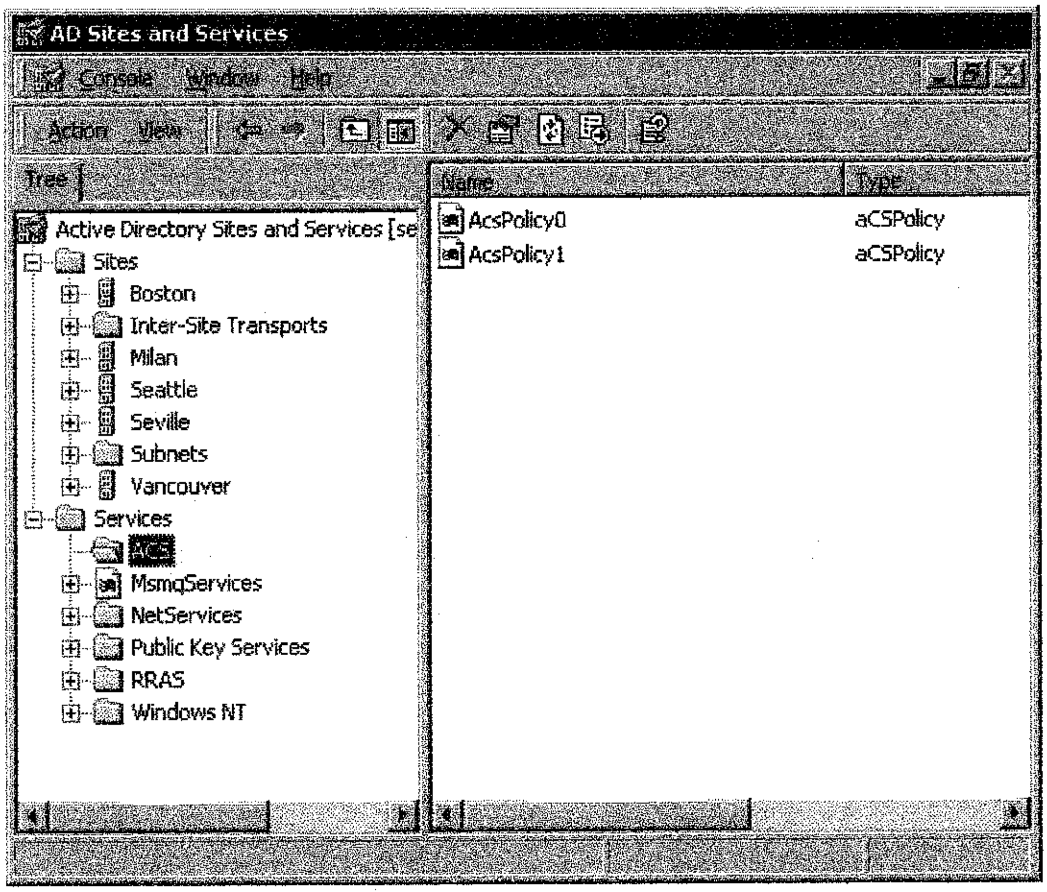
○ Un-authenticated user

○ User

● OU OU=Engineering,OU=Departmental F

All polices are written to the configuration container located in **Active Directory Sites and Services** MMC snap-in shown in Figure 6.

Figure 6 QoS ACS configuration container



- Active Directory Sites and Services [se
  - Sites
    - Boston
    - Inter-Site Transports
    - Milan
    - Seattle
    - Seville
    - Subnets
    - Vancouver
  - Services
    - MsmqServices
    - NetServices
    - Public Key Services
    - RRAS
    - Windows NT

Name	Type
AcsPolicy0	aCSPolicy
AcsPolicy1	aCSPolicy

4. Configuration of QoS Admission Control Service for the Milan Site

When we configured QoS Admission Control Service for the subnet in Milan, we performed the same steps we used in Seattle except for the different subnet address (172.16.132.0/22) and computer names (MIL-EU-FP-03 and MIL-EU-FP-04).

5. Configuration of the Seattle Cisco Layer 3 Switch, SEA-NA-CISCO-02

To ensure an end-to-end QoS RSVP solution we also configured the two Cisco Catalyst 6006 layer 3 switches, SEA-NA-CISCO-02 and SEA-NA-CISCO-03, for RSVP. We added the following command to each interface needed to support RSVP on the layer 3 switch, SEA-NA-CISCO-02:

```
ip pim dense-mode
ip rsvp bandwidth 1024 1024
```

We also added the following command to the global commands on the Cisco Catalyst 6006 layer 3 switch, SEA-NA-CISCO-02:

```
ip multicast-routing
```

ip dvmrp route-limit 20000

To configure QoS RSVP on layer 3 switch SEA-NA-CISCO-02

From the **Start** menu, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.

At the command prompt, type **telnet 172.17.21.22**, and then press ENTER. Provide the password when prompted. This will start a Telnet session with SEA-NA-CISCO-02.

- Type **enable** and press Enter. Provide the password when prompted.
- Type **config terminal** and press Enter.
- At the command line, type each of the following commands:
- **ip multicast-routing**
- **ip dvmrp route-limit 20000**
- **interface Vlan100**
- **ip address 172.17.21.22 255.255.255.252**
- **ip pim dense-mode**
- **ip rsvp bandwidth 1024 1024**
- **interface Vlan140**
- **ip address 172.17.21.25 255.255.255.252**
- **ip pim dense-mode**
- **ip rsvp bandwidth 1024 1024**

Press ENTER, exit configuration mode, and then log off the router.

6. Configuration of the Seattle Cisco Layer 3 Switch, SEA-NA-CISCO-03

We added the following command to each interface needed to support QoS RSVP on the layer 3 switch, SEA-NA-CISCO-03:

```
ip pim dense-mode
ip rsvp bandwidth 1024 1024
```

We also added the following command to the global commands on the Cisco Catalyst 6006 layer 3 switch, SEA-NA-CISCO-03:

```
ip multicast-routing
ip dvmrp route-limit 20000
```

To configure QoS RSVP on router SEA-NA-CISCO-03

From the **Start** menu, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.

- At the command prompt, type **telnet 172.17.21.26**, and then press ENTER. Provide the password when prompted.
- Type **enable**, and then press ENTER. Provide the password when prompted.
- Type **config terminal**, and then press ENTER.
- At the command prompt, type each of the following commands:
- **interface Vlan200**
- **ip address 172.17.21.26 255.255.255.252**
- **ip pim dense-mode**
- **ip rsvp bandwidth 1024 1024**
- **interface Vlan230**
- **ip address 172.16.20.1 255.255.252.0**
- **ip pim dense-mode**
- **ip rsvp bandwidth 1024 1024**
- Press ENTER, exit configuration mode, and then log off the router.

We added the following commands to each interface needed to support QoS RSVP on the Cisco 7513 router, SEA-NA-CISCO-01:

ip rsvp bandwidth 1024 1024
ip pim dense-mode

We also added the following command to the serial interface on the Cisco 7513 router, SEA-NA-CISCO-01:

no fair-queue

We also added the following command to the global commands on the Cisco 7513 router, SEA-NA-CISCO-01:

ip multicast-routing

To configure QoS RSVP on router SEA-NA-CISCO-01

- From the **Start** menu, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
- At the command prompt, type **telnet 172.17.21.21**, and then press ENTER. Provide the password when prompted.
- Type **enable**, and then press ENTER. Provide the password when prompted.

- Type **config terminal**, and then press ENTER.
- At the command prompt, type each of the following commands:
- **ip multicast-routing**
- **interface GigabitEthernet5/0/0**
- **ip address 172.17.21.21 255.255.255.252**
- **load-interval 30**
- **negotiation auto**
- **ip rsvp bandwidth 1024 1024**
- **interface Serial9/2**
- **bandwidth 1544**
- **ip address 172.17.21.1 255.255.255.252**
- **ip pim dense-mode**
- **no fair-queue**
- **ip rsvp bandwidth 1024 1024**

Press ENTER, exit configuration mode, and then log off the router.

8. Configuration of the Milan Cisco Router

We added the following command to each interface needed to support QoS RSVP on the Cisco 7507 router, MIL-EU-CISCO-01:

ip pim dense-mode
ip rsvp bandwidth 1024 1024

We also added the following command to the serial interface on the Cisco 7507 router, MIL-EU-CISCO-01:

no fair-queue

We also added the following command to the global commands on the Cisco 7507 router, MIL-EU-CISCO-01:

ip multicast-routing

To configure QoS RSVP on router MIL-EU-CISCO-01

- From the **Start** menu, point to **Programs**, point to **Accessories**, and then click **Command Prompt**.
- At the command prompt, type **telnet 172.16.132.1**, and then press ENTER. Provide the password when prompted.
- Type **enable**, and then press ENTER. Provide the password when prompted.
- Type **config terminal**, and the press ENTER.

- At the command prompt, type each of the following commands:
- **interface Ethernet1/0**
- **ip address 172.16.132.1 255.255.252.0**
- **ip pim dense-mode**
- **ip rsvp bandwidth 1024 1024**
- **interface Serial5/0**
- **bandwidth 1544**
- **ip address 172.17.21.2 255.255.255.252**
- **ip pim dense-mode**
- **no fair-queue**
- **ip rsvp bandwidth 1024 1024**

Press ENTER, exit configuration mode, and then log off the router.

9. Verifying Operation of QoS RSVP

After installing QoS Packet Scheduler on the clients and QoS ACS servers, installing and configuring QoS ACS on the servers, and configuring the routers and layer 3 switches for RSVP, we were ready to verify that QoS RSVP was working. To verify this, we started a Microsoft NetMeeting session between the client in Seattle and the client in Milan. Because this application is QoS-aware, it issued a request for priority bandwidth allocation for the session. Then, to verify that an actual reservation was being made between the two clients in Seattle and Milan, we used the Microsoft Windows 2000 Server Resource Kit tool, Traffic Control Monitor (Tcmon).

To install NetMeeting on SEA-NA-CLNT-01 and MIL-EU-CLNT-01

- From the **Start** menu, point to **Programs**, point to **Accessories**, point to **Communications**, click **NetMeeting**, and then click **Next**.
- Type information in the **First name**, **Last name**, and **E-mail address** boxes, and then click **Next**.
- On the next screen, clear the **Log on to a directory server when NetMeeting starts** check box, because for testing purposes it is not necessary. Click **Next**.
- Select **Local Area Network**, and then click **Next**.
- Continue through the **Audio Tuning Wizard**, and then click **Finish** at the completion of the wizard. The NetMeeting application appears on the desktop.
- In NetMeeting, click **Tools**, click **Options**, click **Video**, and then verify that both **Automatically send video at the start of each call** and **Automatically receive video at the start of each call** are selected. Click **OK**.

Note For NetMeeting to establish QoS flows, a video card, PC video camera, and sound card must be installed on each client.

By installing the *Windows 2000 Server Resource Kit* tool, Tcmon, we were able to monitor and verify when we received QoS on the NetMeeting flows.

To install the Windows 2000 Server Resource Kit tool,Tcmon, on SEA-NA-CLNT-01 and MIL-EU-CLNT-01

- Insert the *Windows 2000 Server Resource Kit* companion CD. The *Windows 2000 Server Resource Kit* setup wizard is displayed.

  Note If the setup wizard does not automatically appear upon insertion of the CD, manually start the wizard by opening a command prompt, designating your CD-ROM drive letter, and typing SETUP.

- Click **Install Resource Kit**.
- Click **Next**.
- Select **I Agree**, and then click **Next**.
- Enter your information in the **Name** and **Organization** boxes, and then click **Next**.
- Click **Custom** to install a subset of all tools and documentation.

  Note To install all features of the *Microsoft® Windows® 2000 Professional Resource Kit* CD, click **Typical**.

- Perform the following steps for every option except **Tool Documentation** and **Network Management Tools**:
  - Click the option.
  - Select **Entire feature will not be available**.
- Click **Next** two times, and then click **Finish**.
- Click **Exit** to close the *Windows 2000 Resource Kit* setup wizard.

After installing Traffic Control Monitor from the *Windows 2000 Server Resource Kit* companion CD, we then started Tcmon to monitor the QoS flows.

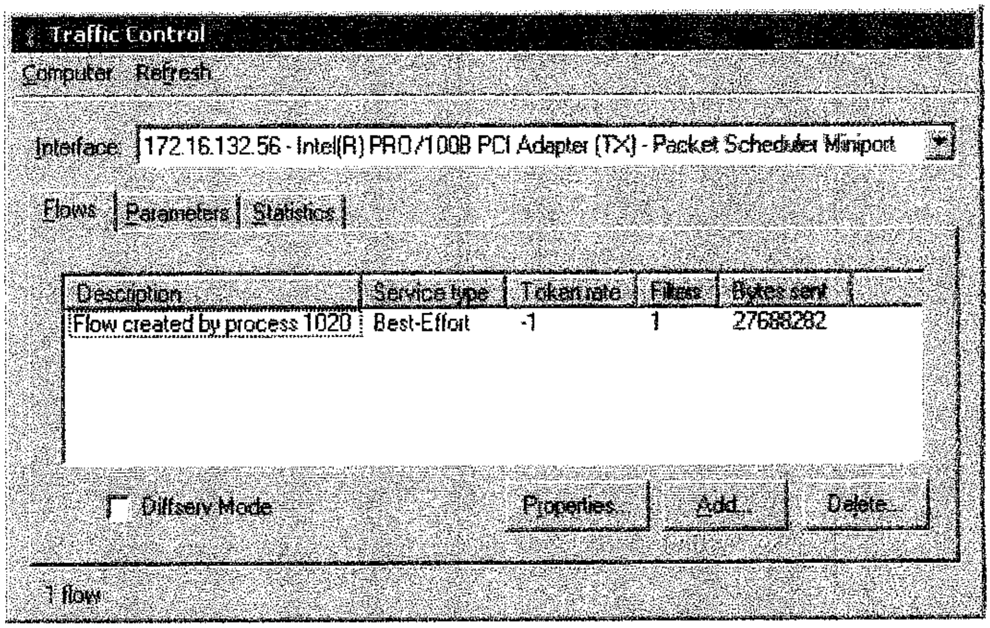
To start Tcmon on SEA-NA-CLNT-01 and MIL-EU-CLNT-01

Note You need Administrator rights on the local machine to run Tcmon.

- From the **Start** menu, point to **Programs**, point to **Windows 2000 Resource Kit**, and then click **Tools**.
- Double-click **Network Management Tools**, and then double-click **Traffic Control Monitor**.

Figure 1 shows Tcmon on MIL-EU-CLNT-01 before a NetMeeting session is opened.

Figure 1 Tcmon before a QoS-enabled NetMeeting session is established



Interface: 172.16.132.56 - Intel(R) PRO/100B PCI Adapter (TX) - Packet Scheduler Miniport

Description	Service type	Token rate	Filters	Bytes sent
Flow created by process 1020	Best-Effort	-1	1	27688282

□ Diffserv Mode

1 flow

After having installed and started Tcmon, and opened NetMeeting on both clients, we then established a QoS-enabled NetMeeting session between SEA-NA-CLNT-01 and MIL-EU-CLNT-01.

To establish a NetMeeting session

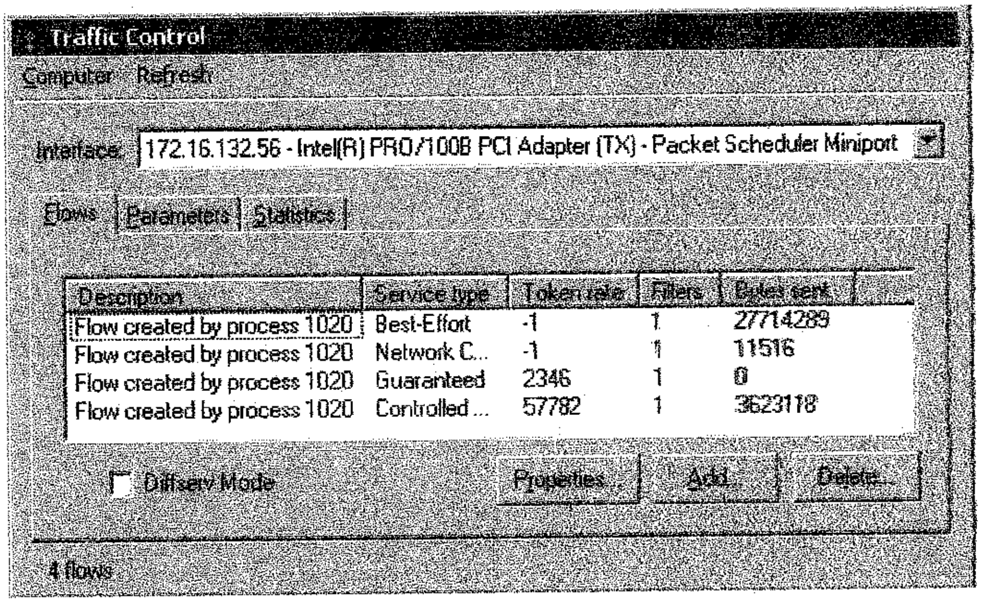
Note In NetMeeting, on the client you are calling, click **Call**, and then click **Automatically Accept Calls**. This will allow the client to automatically accept the call without manual intervention.

- From the **Start** menu, point to **Programs**, point to **Accessories**, point to **Communications**, and then click **NetMeeting**.
- In NetMeeting, on either SEA-NA-CLNT-01 or MIL-EU-CLNT-01, click **Call**, and then click **New Call**.
- Enter the IP address of the client you are calling, and then click **Call**.

After a NetMeeting session has been established between the two clients, you can then verify whether or not QoS RSVP has been applied to the newly-created flows for the NetMeeting session. On each client, for each QoS-enabled NetMeeting session, three different flows are created: one flow is used for QoS signaling, one flow is used for video, and the other is used for audio.

Several seconds after the session has been established you should see the following in Tcmon, as seen on MIL-EU-CLNT-01 in Figure 2:

Figure 2 Tcmon on MIL-EU-CLNT-01after a QoS-enabled NetMeeting session is established



Interface: 172.16.132.56 - Intel(R) PRO/100B PCI Adapter (TX) - Packet Scheduler Miniport

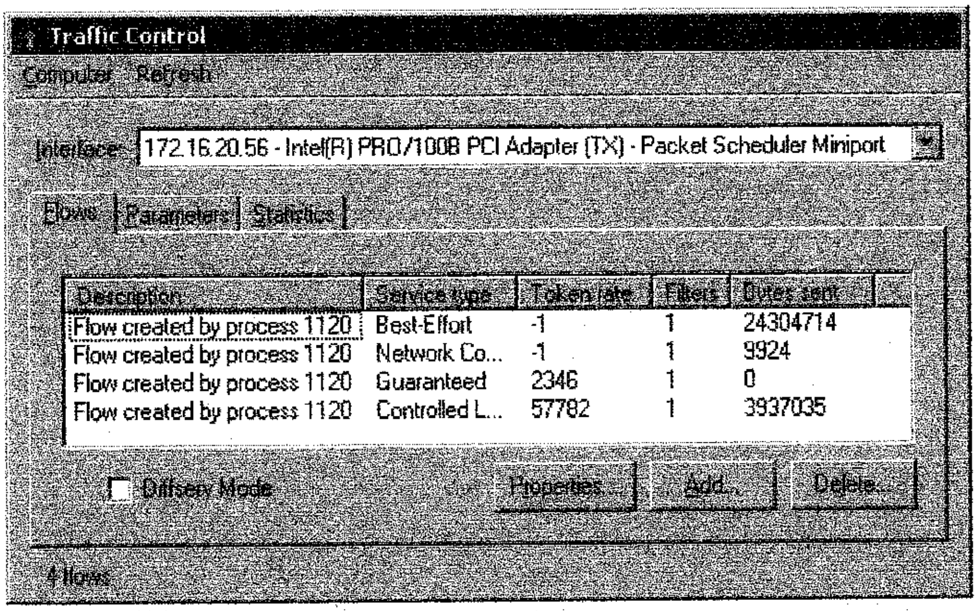
Description	Service type	Token rate	Filters	Bytes sent
Flow created by process 1020	Best-Effort	-1	1	27714289
Flow created by process 1020	Network C...	-1	1	11516
Flow created by process 1020	Guaranteed	2346	1	0
Flow created by process 1020	Controlled ...	57782	1	3623118

☐ Diffserv Mode

The Network Control flow is used for QoS signaling; the Guaranteed flow is for QoS audio; and the Controlled Load flow is for QoS video. If QoS RSVP is not established for the audio and video flows, the Service type is listed as Best Effort.

After verifying that QoS RSVP was working on the Milan client, MIL-EU-CLNT-01, we then verified through Traffic Control Monitor that RSVP QoS was working on the Seattle client, SEA-NA-CLNT-01, as shown in Figure 3.

Figure 3 Tcmon after a QoS-enabled NetMeeting session is established



Traffic Control

Interface: 172.16.20.56 - Intel(R) PRO/100B PCI Adapter (TX) - Packet Scheduler Miniport

Description	Service type	Token rate	Filters	Bytes sent
Flow created by process 1120	Best-Effort	-1	1	24304714
Flow created by process 1120	Network Co...	-1	1	9924
Flow created by process 1120	Guaranteed	2346	1	0
Flow created by process 1120	Controlled L...	57782	1	3937035

□ Diffserv Mode

4 flows

Figure 4 shows a user in the Seattle site in a NetMeeting session over the congested WAN link between the Seattle and Milan sites without Windows 2000 QoS RSVP.

Figure 4 NetMeeting without QoS RSVP

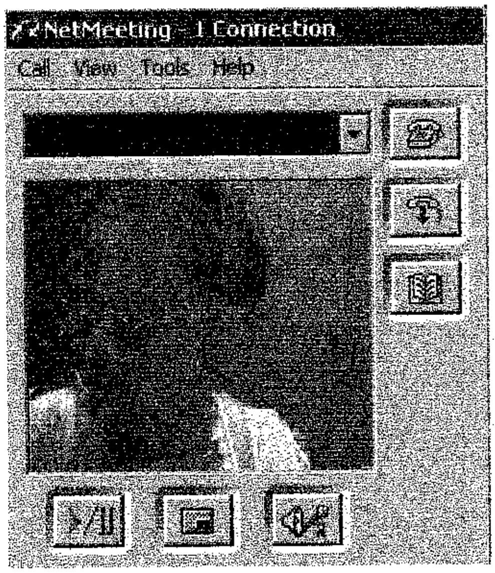
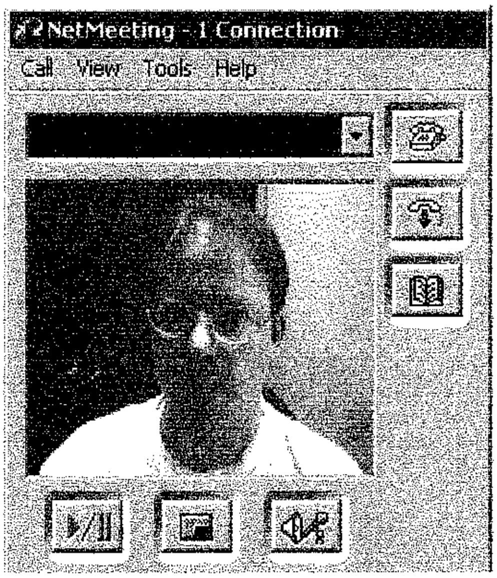


Figure 5 shows the same user in the Seattle site in a NetMeeting session over the congested WAN link between the Seattle and Milan sites with Windows 2000 QoS RSVP.

Figure 5 NetMeeting with QoS RSVP


NetMeeting - 1 Connection
Call View Tools Help