ISSN 2047-3338

Issues of Implementation of Voice over IP with Quality of Service: An Overview

E. Dar[1] and M. Latif[2]

[1]Technical University of Vienna, Institute of Software Technology and Interactive System, Austria
[2]Department of Computer Science, University of London, United Kingdom

***Abstract*— This project explores various aspects regarding to the implementation of voice over Internet Protocol (IP) with Quality of Service and gives a detailed insight into this. Internet telephony utilizes the Internet medium to transfer audio between two or more clients in real time, thus allowing the clients to make conversations simultaneously on telephones. Converged voice and data using a packet based transport offers flexible, scalable, and cost efficient services. Emphasis is put on the efficient voice communication over the IP network so that Quality of Service (QoS) is maintained. Packet voice quality issues and strategies for minimizing the packet loss are described and implemented.**

***Index Terms*— Voice Over IP, Issues, Quality of Service and Strategies**

I. INTRODUCTION

VOICE over Internet Protocol [1] technology is designed to break down the barrier between traditional Public Switched Telephone Networks (PSTN) [3] and VoIP networks. For the carrier, the opportunity of voice over Packet technologies lies in optimizing network infrastructure and in extending customer reach beyond PSTN subscribers, while at the same time maintaining end-to-end service capabilities and service offerings.

QoS [2] measurements for packet networks carrying real-time voice are significantly different from those for networks that carry data only. Data networks are concerned solely with minimizing data error rates while voice channels, however, depend on the perceived quality of the resultant speech. Because users of public switched-telephone networks have come to expect high perceptual speech quality (toll quality) and service reliability, it is important in most applications that VoIP systems do not degrade voice quality or incur much delay. VoIP networks emphasis is put on the question how voice can efficiently be forwarded in a packet network so that Quality of Service (QoS) is maintained [5].

Thus, the main problem is to define a way to carry voice calls over an IP network including the digitization and packetization of the voice streams with QoS and describes a networking environment where voice, video and data transmissions are integrated within a single, unified system (often referred to as a multi-service network). The merger of packet switching technology with, telephony signaling and call-processing intelligence; allowing carriers to consolidate typically separate voice and data overlay networks, and provide new communication services, however, drawbacks of separate voice and data networks, brings out the solution of converged networks; transmitting voice, video and data over same packet based network.

The rest of the paper is organized as: In section II, we discussed the background history and related work of the research. In section III, we discussed the different issues regarding implementation of VoIP with QoS. We conclude our work in section IV.

II. BACKGROUND

VoIP [4] stands for Voice over Internet Protocol. With new technological advances, voice can be transferred across the Internet, and it is the ability, which has lead to Internet telephony, or the transfer of voice over Internet protocol (IP) networks, rather than over public switched telephone networks (PSTN) [8]. Voice over IP [10] is a form of communication much different than circuit switching because VoIP sends information through IP packets over the Internet. Years ago it was found that sending a signal to a remote destination could also be done digitally which brought about the evolution of VoIP [6]. A typical VoIP call uses an ADC or analog to digital converter, then transmits the data over the internet in packets and at the end of transmission formats the data again with a DAC or digital to analog converter [9]. Basically VoIP digitalizes voice in data packets, sends them and reconverts them in voice at the call destination.

The packet switching is more efficient than the circuit switching PSTN because the information is sent in groups and there is no dead air time, and one is not being charged for the dead air time on the line through the utilization of the Internet medium to transfer audio between two or more clients in real time, Internet telephony [7] has several advantages with its technology, primary the offering of low-cost long distance "telephone" service, but also still carries several disadvantages with it, only to be improved through future technological advancement [11].

The Internet telephony [7] technology first became a reality in February 1995 when VocalTec, Inc. first announced its Internet telephony software product, the VocalTec Internet Phone; which allows for conversation between users over the

Internet. This software was originally designed to operate on a PC with a 486/33-MHz processor or higher, where a user would be able to utilize the PC's modem, sound card, speakers and microphone to hold a conversation with another user by talking into the microphone and listening via the speakers [11]. With this technology, conversation was limited to only two computer users and it was essential that both parties were using the Internet Phone software and Internet telephony was limited to PC-to-PC connection only.

During the beginning months of 1996, the VocalTec announced that it would be working with another company, Dialogic, to produce a piece of hardware, known as a gateway, that allows for PC-to-Phone and Phone-to-Phone connections by bridging the Public Switched Telephone Network (PSTN) [8] with the Internet [11]. It was the creation of the gateway that allowed for Internet telephony [7] to become a success as the first technology that combined both the Internet and PSTN worlds. Before the creation of the gateway, several companies had worked and created various forms of Internet telephony software as solutions to place "telephone" calls over the Internet, but it was the functionality of the gateway that was essential to truly make Internet telephony work.

The PSTN or network where telephone calls are transferred is a circuit-switched network where a direct single path route is created between the caller and callee. The network resources (e.g. link bandwidth) are allocated to each call for the duration of the call. Thus, no resource sharing occurs between separate calls and a resource piece is idle if it is not being used by its owning call. However, this telephone connection network is different from the Internet connection network in that the Internet connection network follows a packet-switching network scheme. With packet-switching, each data stream to be transferred over the Internet medium is divided into packets, or simply smaller portions of the entire data, where all users connected to the Internet share all of the networks resources. Each packet uses the full link bandwidth, and network resources are only used as needed. The development of gateways made it possible to converge two distinct networks.

The second primary obstacle the gateway overcame is the means of addressing, or accessing a user on a PC, which could be located anywhere around the world. Prior to the deployment of the gateway, in order to access a remote PC, a user needed to know the PC's IP address, an address that is not easily obtainable if one has not had prior contact to the remote PC. However, the gateway overcame this problem by allowing a user to access a remote PC that was equipped with any gateway by only knowing the contactee's phone number. A phone number is a more easily obtainable piece of information than an IP [11] address, thus the gateway's functionality now overcame two primary obstacles; network bridging and addressing.

Upon receipt of a standard telephone voice signal, the gateway first digitizes the analog voice signal, compresses the new digital signal, pocketsize the signal into the standard data transfer blocks of the Internet, known as IP packets [11], and moves the packets onto the Internet for transport to the destination gateway, where this gateway reverses the process. With this gateway technology, it is possible to place three different types of calls using Internet telephony; PC-to-PC, PC-to-Phone, and Phone-to-Phone.

Standards have been developed for Internet telephony to create a uniform operation method and for interoperability between the vast numbers of products that are available. For instance, companies such as Deltathree, Net2Phone, and VocalTec Inc. offer different products and services relating to Internet telephony. To overcome the primary software interoperability problem that existed with VocalTec's Internet Phone, where a VOIP call could only be placed if both users were using this same software, standards were put in place so that one user, using one company's software, could contact another person who might be using another company's software. Thus, with the H.323 standard and G.723 audio codec standard, users with different software products are able to communicate using Internet telephony [11]. Now, keeping these PC standards in mind, as well as the PSTN standards, gateway producers are able to create a gateway product to fulfill these specified requirements.

III. ISSUES OF IMPLEMENTATION OF VOIP WITH QOS

A. QoS Requirements for VoIP

For VoIP to be a realistic replacement for standard PSTN telephony services, customers need to receive the same quality of voice transmission they receive with basic telephone services – meaning consistently high quality voice transmissions [15]. End user expectations for carrier grade telephony are:

- Once a call has been accepted by call control and resources allocated to it the call should be carried to completion with the required voice quality.
- Established calls must be protected from network disturbances as for as physically possible. One implication of this requirement, when applied to a connectionless packet network, is that stable calls must not be adversely affected by sudden loads caused by the re-routing of traffic from other parts of the network.
- The network must be capable of supporting very high levels of call setup attempts. Existing narrowband exchanges may support millions of busy hour call attempts and a VoIP network must be able to support comparable volumes.
- In the event of focused overload, calls that cannot be carried must be rejected without degrading the call carrying capacity of the network. The PSTN and thus any replacement packet network will occasionally be subjected to very high volumes of calls far beyond that which can be carried (TV and radio phone-in competitions or ticket sales for major events are prime drivers for this sort of overload), any resource reservation mechanisms must be able to deal effectively with this type of event.
- Mechanisms must be available to ensure that emergency calls and high priority calls receive preferential treatment.
- Call setup latency must be comparable to the existing network. The resource reservation mechanisms chosen

must not introduce delays that mean the user notices a worse setup time on a packet network than they would on a traditional TDM network

- The network must be secure from denial of service attacks and spoofing. For example, only the call that has been allocated the resource must be able to use it and when the call is released the resource must again be available to the network.
- Some networks may require the support for call pre-emption. In certain cases it may be required for a network to de-allocate resources that have been reserved for an existing call and re-allocate them to a new call.

The legacy PSTN network supports all of these requirements today using TDM narrowband switches. Additionally some network operators have migrated their TDM voice platforms onto ATM which is a relatively straight forward evolution because ATM is both connections oriented and rich in quality of service features. Where VoIP is considered, however, the underlying network is very different and it poses a number of challenges to operators wishing to support a toll quality voice service.

B. Packet Voice Quality Issue

High end-to-end voice quality in packet transmission depends principally on these factors:

- Voice Encoding *I* Decoding (Codec)
- End-to-end delay across the network and variation in the delay (jitter)
- Packet loss across the channel
- Echo control

Selecting the right speech codec is essential. Codec performance includes the baseline quality (that is, without impairments) and the performance with impairments present, such as background noise and lost/late packets. To prevent excessive degradation from transcoding, it is necessary to control whether and where transcodings occur and what combinations of codecs are used [9].

It is also essential to control the end-to-end delay. When end-to-end delay exceeds 150—200 milliseconds one-way (300—400 milliseconds round-trip), the connection is noticeably impaired. Anyone who has talked on a call with a single satellite hop has experienced this effect. (A geostationary satellite connection adds about 300 milliseconds of one-way delay.

In packet transmission, packets sometimes get "lost." These packets may have been late or may have been discarded in the network because of congestion. The missing information degrades the output signal, and a Packet Loss Concealment (PLC) may be needed to smooth over the gaps. The delay through the packet network exacerbates any echo that may be present. Echo control with the right characteristics at the appropriate places in the connection protects against echo at both ends. Echo control becomes essential when packet network equipment is interconnected with circuit switched equipment operating with two-to-four-wire conversions or "hybrids."

There are other parameters that can affect performance. For example, an end device that doesn't support the designated loss/level plan may not provide a usable voice connection.

Voice quality issues in packet transmission are similar to those in digital wireless transmission. Wireless networks use low bit-rate codecs and are susceptible to channel impairments and increased end-to-end delay. Echo control within the wireless network and at the interface between the wireless and wireline networks is essential.

The following sections describe the effects of the four performance factors, where and how they interact, the range of acceptable operation, and how they can be managed in the packet network environment.

1). Voice Encoding / Decoding (Codec)

A codec (coder-decoder) converts the analog voice signal to a digitized bit stream at one end of a call and returns it to its analog state at the other (codecs are also used to convert from one digital form to another, a process known as "transcoding"). In telephone networks, one of two techniques is generally used: waveform coding or CELP (code excited linear predictive) coding. Waveform codecs directly or indirectly code the amplitude of the signal at each point, while CELP codecs are based on a model of the acoustics of the vocal tract during speech production. ITU Rec. G.711 defines the PCM (pulse code modulation) coding that is used in much of the circuit-switched (TDM) digital network.

G.711 is a waveform codec, and operates at 64 kbps in almost all telephony applications. G.726 defines ADPCM (Adaptive Differential Pulse Code Modulation), also a waveform codec. G.726 reduces the data rate, but also degrades the quality of the reproduced signal. The processing delay for both of these codecs is less than 1 millisecond, which is negligible. The main delay associated with the use of these codecs in packet networks is the packetization delay.

This delay is equivalent to the duration of signal contained in each packet, typically between 10 and 40 milliseconds.

Packet transmission offers the flexibility to use different codecs as needed.

In choosing a code for a particular call or application, there are several considerations:

- the compression rate needed
- the desired voice quality
- the delay that the codec adds to the connection
- how well the codec allows missing packets to be smoothed over, and
- whether a packet loss concealment algorithm must be added externally or is already built into the codec.

The encoding delay of the codec is an integral component of the end-to-end delay. Because compression codecs add significant delay, the delay budget defining the distribution of allowable delay to the various network elements may require adjustment to accommodate a long encoding delay. Table 1 shows some of the characteristics of the codecs most commonly chosen for point-to-point Voice over IP applications [16].

Table 1: Characteristics of Speech Codecs Commonly Used in Packet Networks

Codec	Type	Bit Rate	Frame Size Total Delay		Other Information
G.711	PCM	64 Kbps	Depends on Packet size		Codec of choice for high-quality. PSTN equivalent voice service
G.726	ADPCM	32 Kbps	Depends on Packet size		Often used for multiplexing on 64 Kbps "toll" quality voice channels.
G.729	ACELP	8 Kbps	10 ms	25 ms	ITU-s 8 Kbps coding standard. Good delay characteristics and acceptable voice quality.
G.729A	ACELP	8 Kbps	10 ms	25 ms	Reduced-complexity version of G.729.

2). Delay

The end-to-end delay (sometimes called "latency") is the time between the generation of a sound at one end of a call and its reception at the other end. VoIP is extremely bandwidth- and delay-sensitive [15].

There are two distinct types of delay: fixed and variable.

- Fixed delay components add directly to the overall delay on the connection.
- Variable delays arise from queuing delays in the egress trunk buffers. These buffers create variable delays, called jitter, across the network. Variable delays are handled via the de-jitter buffer at the receiving side.

Delay causes two different impairments. First, as delay increases, echo becomes more noticeable. Second, when the delay becomes long enough, it disrupts conversation dynamics, making communication difficult.

Some delay factors are given:

- Processing Delay
- Packetization Delay
- Serialization Delay
- Propagation Delay/Network Delay
- Buffering Delay/Accumulation Delay

3). Echo Impairment and Control

Echo in the network results from coupling between the transmit path and the receive path, which causes the outgoing speech to be sent back to the talker. The severity of an echo depends on two factors: the amplitude of the echoed signal and the time it takes to return to the talker. Amplitude is a function of the strength of the coupling between the transmit and receive channels. It is characterized as the "echo path toss," which is the difference in level (in dB) between the original input speech and the echoed signal. For a given echo path loss (i.e., constant level), the longer the time between the original speech and the returning echo, the louder the echo will seem. Echo that is inaudible in the circuit-switched network may become noticeable with packet transmission because of the increased delay. Interconnections between packet networks and circuit-switched networks are especially susceptible to echo impairment. Reflections from two- to four-wire hybrids used on analog lines in circuit-switched networks create strong echo; loss planning in the PSTN and rules for private networks connecting to the PSTN are largely intended to keep hybrid and other echoes below the threshold of audibility.

The delay associated with packet transmission violates the engineering assumptions of the circuit-switched network. Therefore, echo control at the interface between the networks is essential to protect users at both ends from hearing echo. While fully digital networks have no echo paths in the network, they can still be subject to echo from coupling in the end devices. Acoustic coupling, where the microphone picks up the output of the receiver, is one potential source. Electrical pickup between analog circuits (crosstalk) is another. Such echo is usually lower level than hybrid echo, but may be audible with long delay.

Following are descriptions of several echo-reduction techniques. They can be used alone or in combination, depending on the application and the level of echo expected.

- Echo Cancellers
- Echo Suppressors
- Loss/level planning

4). Packet Loss

In the traditional circuit-switched telephone network, a call is assigned a physical connection between end-points, and the circuit remains dedicated to that channel for the duration of the call. In contrast, packet networks break voice, fax, and data into small samples or packets of information. Each packet has a header that identifies where the packet is going and provides information for reassembly when the packet arrives at the destination. Packets travel independently and they are interspersed with packets from other network traffic along the way. Travel time through the network varies for individual packets.

Unless the network is precisely matched to the peak traffic load, packets sometimes fail to arrive at the destination. These lost packets create gaps in voice communications, which can result in clicks, muting, or unintelligible speech. In transmitting data, the remedy for packet loss is to resend the missing packets, but this solution doesn't work for time-sensitive voice conversations. Generally, there are two ways to lose packets. They can be lost at network nodes because of an over-flow in the buffer or because a congested router deliberately discards them to reduce congestion. These packets are truly gone, and will never arrive at the destination. Network outages from disabled devices or fiber cuts can also result in lost packets. These events may result in large packet losses; these will be spread across the many different virtual channels that the network is handling at that time.

Second, packets can be delayed if they take a longer route or spend time in a device queue, causing variability in arrival time at the receiving end. The jitter buffer is used to smooth out the variability by holding packets for input to the decoder. The delay introduced by the jitter buffer is tuned to the

expected network delay variation. That delay determines the longest time that a packet can take to arrive and still be in time to be decoded. Packets arriving after the prescribed delay lose their turn and are as good as lost, since the voice playout cannot wait for the late packets to show up. In a network running without call admission control, and without a quality of service (QoS) protocol enabled, packet loss is uncontrollable in the face of congestion. The consequences of congestion depend on the type of network, the proportion of voice and data traffic, the number of hops, and the duration of the event. The number of late packets can be minimized by increasing the size of the jitter buffer. However, a longer jitter buffer increases the end-to-end delay.

The best way to prevent late and lost packets is to engineer the network to preclude or minimize delays and other contributing factors. This means that congestion control (call admission control) must be in place to prevent the router queues from filling, which causes variation in delay and possibly overflow.

Strategies for minimizing lost packets are given.

- QoS Protocols
- Call Admission Control
- Adaptive Jitter Buffer
- Interleaving
- Sending Duplicate Data
- Concealing Missing Data

C. VoIP QoS Mechanisms

There are various mechanisms that can be used to provide quality of service for packet networks, few of them are [1]:

- Resource Reservation Protocol (RSVP)
- Integrated Services (lntserv)
- Differentiated Services (Diffserv)
- MPLS Traffic Engineering (MPLS-TE)

1). Resource Reservation Protocol (RSVP)

Resource Reservation Protocol (RSVP) is an IETF standard that allows a host to request a specific Quality of Service (QoS) requirement from the network, on behalf of an application data stream. RSVP carries the request through the network, visiting each node the network uses to carry the stream. At each node, RSVP attempts to make a resource reservation for the stream, before reporting back to the application and allowing the call/communication.

To make a resource reservation at a node, the RSVP daemon communicates with two local decision modules, “admission control” and “policy control”.

- Admission Control: It determines whether the node has sufficient available resources to supply the requested QoS.
- Policy Control: It determines whether the user has administrative permission to make the reservation.

2). Integrated Services (lntserv)

The integrated services provide quality of service by explicitly reserving bandwidth on a per flow basis and the protocol used is, RSVP.

It is important to distinguish between RSVP itself and Intserv. RSVP is a signaling mechanism that is used to realize the intserv architecture. It is possible to use RSVP for other reasons, one example is RSVP-TE where it is used to facilitate traffic engineering for MPLS networks.

When used as part of Intserv, RSVP provides a method for a user to request a particular quality of service for a session, in effect this reserves the bandwidth throughout the network for the duration of the session. In the case of a voice session the sender of the voice flow would send an RSVP path message through the network to the receiver. Each node along the path identifies that the Path message signifies a new RSVP session and checks its resources before sending on (a possibly modified) path message. Each Intserv capable node along the path is required to store a soft state for the session and RSVP path refreshes must be sent periodically through the network to hold a particular reservation. Once the Path message reaches the user, the traffic parameters contained within the path message are checked and if the user can support such a session, or wishes to modify the session, an RSVP reservation message is sent back through the network to the sender.

3). Differentiated Services (Diffserv)

The Diffserv approach to provide QoS support differs fundamentally from lntserv in that it does not refer to a specific protocol for providing quality of service but rather an architectural framework designed to facilitate QoS.

Diffserv proposes that QoS should be provided by the setting and enforcing of policy within a network, to provide a set of Service Level Specifications (SLS) between networks (or customers and networks), effectively service level agreements (SLA). The key features of the Diffserv architecture are as follows.

- The network is divided into one or more Diffserv domains.
- Sources and sinks of traffic outside of the Diffserv domain are considered customers and would typically have an appropriate Service Level Specification that defined how much traffic and of what type they could pass into, and receive from the Diffserv domain.
- The edge of the diffserv domain is made up of Diffserv boundary routers. A Diffserv boundary router performs traffic classification and traffic conditioning and policing. It must provide functions for admission control, policy enforcement.
- Unlike Intserv, Diffserv QoS functions are not applied to a single flow from a customer. Diffserv classifies traffic into a series of classes (otherwise known as per hop behaviours) and applies the same treatment to all traffic within a class.
- The core of a diffserv domain is made up of Diffserv core routers. Diffserv core routers are intended to concentrate solely on traffic handling, processing each packet based on how the packet was marked at the Diffserv boundary.

Because Diffserv is architecture rather than a complete solution, supplementary elements must be added to the solution in order for it to be suitable for supporting a voice service. A key aspect of this is, admission control and one way of providing it is, to deploy bandwidth managers within the

network.

4). *MPLS Traffic Engineering (MPLS-TE)*

Multiprotocol Label Switching (MPLS) provides a mechanism for engineering network traffic patterns that is independent of routing tables. MPLS assigns short labels to network packets that describe how to forward them through the network. MPLS is independent of any routing protocol and can be used for uni-cast packets [9].

In the traditional Level 3 forwarding paradigm, as a packet travels from one router to the next, an independent forwarding decision is made at each hop. The network layer header is analyzed, and the next-hop is chosen based on this analysis and on the information in the routing table. In an MPLS environment, the analysis of the packet header is performed just once, when a packet enters the MPLS cloud. The packet then is assigned to a stream, which is identified by a *label,* which is a short (20-bit), fixed-length value at the front of the packet. Labels are used as lookup indexes into the label-forwarding table. For each label, this table stores forwarding information. You can associate additional information with a label—such as class-of-service (CoS) values- that can be used to prioritize packet forwarding.

MPLS traffic engineering extends the capabilities of MPLS to incorporate quality of service and as such provides a potentially useful tool to a network operator looking to support voice services. MPLS can be used inside a network to setup label switched paths between ingress and egress points in the network; in effect this creates tunnels down which appropriately tagged traffic flows. By assigning a bandwidth to the label switched path on establishment it is possible to ensure that traffic being carried over a label switched path is guaranteed to be delivered to the egress point provided that the total traffic admitted to the label switched path does not exceed the bandwidth allocated to it.

This is a useful tool for IP networks carrying voice as it allows what effectively is an aggregate reservation between two points down which many individual flows can be carried without requiring the explicit reservation of resources for each individual flow. Furthermore this aggregate reservation can be varied with time to allow for fluctuating traffic flows in a network and when combined with MPLS fast re-routing it allows for a resilient network to be created where even significant network failures have very limited impact on the traffic being carried by a particular label switched path.

IV. CONCLUSION

Although VoIP is an attractive alternative to traditional voice systems and PSTN voice services, deploying VoIP is not a simple process. Before choosing a solution, organizations should consider both the required functionality and the potential issues. These considerations drive the protocol and equipment choices in designing the VoIP solution. Although the wide range of VoIP protocols has caused some confusion in the marketplace, it is precisely this protocol flexibility that makes VoIP-based systems so much more useful than legacy voice systems.

In this thesis, we have discussed the different security and quality of service issues for voice over IP networks. We have also proposed some solutions for these problems and issues discussed in this research thesis. In designing their VoIP solution, organizations also need to consider how their networks will address the latency, jitter, bandwidth, packet loss, reliability, and security issues raised in this paper. By working with vendors that can provide VoIP solution flexibility, companies can take advantage of the efficiencies of VoIP, while enhancing the scalability and reliability of their network for the next generation of applications and services. As VoIP becomes commonly deployed, some traditional data firewalls will add support for VoIP. Alternatively, we have the option of using VoIP firewalls to address VoIP's unique issues.

REFERENCES

[1]. Jonathan Davidson, Voice over IP Fundamentals, 1st Edition, 2000

[2]. Quality of Service for Voice over IP, http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/qossol/qosvoip.htm

[3]. William Stallings, Data & Computer Communication, 6Th Edition, 2000

[4]. Bhumip Khasnabish, Implementing Voice over IP, 1st Edition, 2003

[5]. Voice and Fax over Internet Protocol (V/FoIP), http://www.iec.org/online/tutorials/vfoip/

[6]. Dan Newland, Networking Essentials, 2nd Edition, 1999

[7]. Internet Telephony and VoIP, http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group8/

[8]. PSTN and Comparisons to Voice over IP, http://www.ciscopress.com/content/images/chap01_1578701686/elementLinks/1578701686CH01.pdf

[9]. Lawrence Harte, Internet Telephone, 1st Edition, 2001,

[10]. Introduction to VOIP, The future of cheap communication, http://people.smu.edu/akashc/VoIP_paper.pdf

[11]. Internet Telephony, http://www.homepagez.com/chaffee009/ECE494/intro.htm

[12]. Voice over IP Applications, http://www.it.iitb.ac.in/drona/beprj/web/Iassignment/voip4/assign1/projectVOIP1.htm

[13]. Quality of Service for Voice over IP, http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/qossol/qosvoip.htm

[14]. Designing a Long-Distance VoIP Network, http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/longd.htm

[15]. Voice over Internet Protocol, http://focus.ti.com/pdfs/bcg/online_voip_chapter.pdf

[16]. Voice over the Internet Protocol Applications, http://www.privateline.com/clayton/voice