NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

INTERNET TELEPHONY

by

Richard Perri

December 1999

Thesis Advisor:	Bert Lundy
Second Reader:	Wolfgang Baer

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 1999	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE: Internet Telephony

5. FUNDING NUMBERS

6. AUTHOR(S) Perri, Richard Paul

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION/AVAILABILITY STATEMENT: Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE:

13. ABSTRACT *(maximum 200 words)*

During the mid- '90s, data and voice began to merge, propelled by advances in compression technology. The ubiquity of routed Internet Protocol (IP) networks, and the desire to trim telephony costs are the major driving forces of the deployment of Voice over IP (VoIP).

One major advantage of VoIP technologies is that they leverage existing network resources and dramatically reduce, or eliminate telephone costs. If there is an existing Wide Area Network (WAN) then VoIP could be employed over the WAN. However, a WAN link may not be available at each node location. Then only local point of presence (POP) for router based Internet connectivity would be required for VoIP over the Internet. The Internet could be the part of the backbone for the routing of the voice packets.

The advantages of deployment of VoIP are evident. The issue of whether or not to deploy VoIP is more concerned with technical implementation and Quality of Service (QoS) that with a cost-benefit analysis.

This thesis analysis some of the technical issues surrounding the use of Internet Telephony. Specifically, the Internet Architecture and required QoS for reliable voice, and issues that arise from a dynamic network such as the Internet, and both software and hardware approaches to workstation solution to Internet Telephony.

14. SUBJECT TERMS Internet Telephony, Voice Over Internet Protocol Networks

15. NUMBER OF PAGES 66

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

(THIS PAGE INTENTIONALLY LEFT BLANK)

Approved for public release; distribution is unlimited.

INTERNET TELEPHONY

Richard Perri
Lieutenant Commander, United States Navy
B.S., SUNY Maritime College

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 1999

Author: ______________________
Richard Perri

Approved by: ______________________
Bert Lundy, Thesis Advisor

____
Wolfgang Baer, Second Reader

____
Dan Boger, Chairman
Department of Computer Science

(THIS PAGE INTENTIONALLY LEFT BLANK)

ABSTRACT

During the mid- '90s, data and voice began to merge, propelled by advances in compression technology. The ubiquity of routed Internet Protocol (IP) networks, and the desire to trim telephony costs are the major driving forces of the deployment of Voice over IP (VoIP).

One major advantage of VoIP technologies is that they leverage existing network resources and dramatically reduce, or eliminate telephone costs. If there is an existing Wide Area Network (WAN) then VoIP could be employed over the WAN. However, a WAN link may not be available at each node location. Then only local point of presence (POP) for router based Internet connectivity would be required for VoIP over the Internet. The Internet could be the part of the backbone for the routing of the voice packets.

The advantages of deployment of VoIP are evident. The issue of whether or not to deploy VoIP is more concerned with technical implementation and Quality of Service (QoS) than with a cost-benefit analysis.

This thesis analyses some of the technical issues surrounding the use of Internet Telephony, specifically, the Internet Architecture and required QoS for reliable voice, and issues that arise from a dynamic network such as the Internet, and both software and hardware approaches to workstation solution to Internet Telephony.

(THIS PAGE INTENTIONALLY LEFT BLANK)

TABLE OF CONTENTS

LIST OF FIGURES

(THIS PAGE INTENTIONALLY LEFT BLANK)

LIST OF TABLES

(THIS PAGE INTENTIONALLY LEFT BLANK)

I. INTRODUCTION

A. BACKGROUND

Voice over Internet Protocol (VoIP) means the transmission of voice traffic in packets over a network utilizing the Internet Protocol (IP). We can transmit voice over IP networks that are privately owned or publicly utilized. If we have the technology to transmit Voice over the Internet then why not use Internet Telephony? This would encompass VoIP, which utilizes the large backbone of the Internet.

Internet Telephony is viewed by some to be an effective technology and by others as nothing more than an irritant. The irritating aspect stems from those people who have used the public Internet to make telephone calls. In most cases, they are not happy with the quality of the speech and the overall ability of the Internet to support voice traffic.

Why then is Internet Telephony of such keen interest to the communications industry, in view of its relatively poor performance in the support of voice traffic?

There are four major reasons for the interest, and for the deployment of Internet Telephony: Economics of Networks, Universal Presence of IP, Maturation of Technologies, and the shift to Data Networks.

1. The Economics of Networks

This first reason for Internet Telephony can be summed up by the following three areas: integration of voice and data, bandwidth consolidation, tariff arbitrage.

Clearly the *integration of voice and data* traffic will be demanded by multi-application software resulting in the inevitable evolution to Web servers capable of interacting with the customer with data, voice, and video images.

Integration of voice and data allows for *bandwidth consolidation*, which effectively fills the data communications channels more efficiently. The telephone legacy of channeled voice slots, are inefficient for the support of data applications.

The commonsense approach is to migrate away from the rigid telephony based time division multiplexing (TDM) scheme wherein a telephone user is given bandwidth continuously, even when the user is not talking. Since voice conversations entail a lot of silence using the data communications scheme of Statistical TDM (STDM) yields a much more efficient use of the bandwidth. Simply put, STDM uses the bandwidth when it needs it or the bandwidth is made available to other talkers who need it at that instant.

Consider that 50 percent of a normal speech pattern is silence. Voice networks that are built on TDM use bandwidth to carry those silent periods, but data networks do not. In addition, 20 percent of speech consists of repetitive patterns that can be eliminated through compression algorithms, but TDM operations do not exploit this compression technology.

Lastly, *Tariff arbitrage* means by passing the public switched telephone networks' toll service and utilizing the Internet backbone. This approach avoids the costly long distance charges incurred in the tariffed telephone network in contrast to lower costs of the untariffed Internet or privately owned IP networks.

An argument can be made that VoIP will not be attractive if or when the Federal Communications Commission (FCC) removes the Enhanced Service Provider (ESP) status that is granted to Internet Service Provider (ISP). The effect of this status is that ISPs are not required to pay local access fees to use the telephone company (telco) local access facilities. This special status gives ISPs a huge advantage in competing for voice customers. Access fees are the most expensive part of a long distance call, up to 50 percent of the cost for a long distance call.

If the ESP status was removed, this would certainly level the playing field largely and there would be less hype about VoIP. However, the fact remains that conventional circuit-switched telephone networks cannot compete with packet –switched networks on a cost and efficiency basis. This fact stems partly from the concept of bandwidth consolidation, speech compression and the next three major reasons for VoIP.

2. Universal Presence Of IP

The second major reason for Internet telephony is the universal presence of IP and associated protocols in user and network equipment. Of essential importance is the fact that IP resides in the end-user workstation. Although this may be possibly a subtle point, this gives IP a decided advantage over other existing technologies that are not resident in the user end station. Moreover, IP operates in both wide area networks (WAN) and local area networks (LAN), whereas Frame Relay and Asynchronous Transfer Mode (ATM) normally operate in the wide area network. Occasionally ATM will find its way to the desktop, but this is the exception rather than the rule.

3. Maturation Of Technologies

The third major reason for the deployment of Internet telephony is the maturation of technologies that now make IP telephony feasible.

Much of the *Hardware Technology* is supported by wide-scale deployment of digital signal processors (DSPs). The DSPs are found in codecs (voice coders and decoders) and high speed modems. DSPs are now high performance, mass produced and relatively inexpensive.

Another aspect of the maturation of technologies is the increase sophistication of *user applications*. Increasingly, we will use applications supporting three-dimensional, real-time, voice, full-motion video, and data displays.

4. The Shift To Data Networks

Finally, the fourth major reason for the assured success of VoIP and other data networks is the fact that the world is experiencing a shift away from circuit-based networks to packet-based networks. Some market forecasters place the ratio of data networks-to-circuit networks at 80 to 20 percent by the year 2005.

B. SCOPE OF THIS THESIS

This thesis is to examine a workstation solution to Internet Telephony. In particular, focus will be on the architecture of Internet networks, issues of a dynamic network such as the Internet, and both software and hardware approaches to a workstation solution to Internet Telephony, as shown in Figure 1.1.

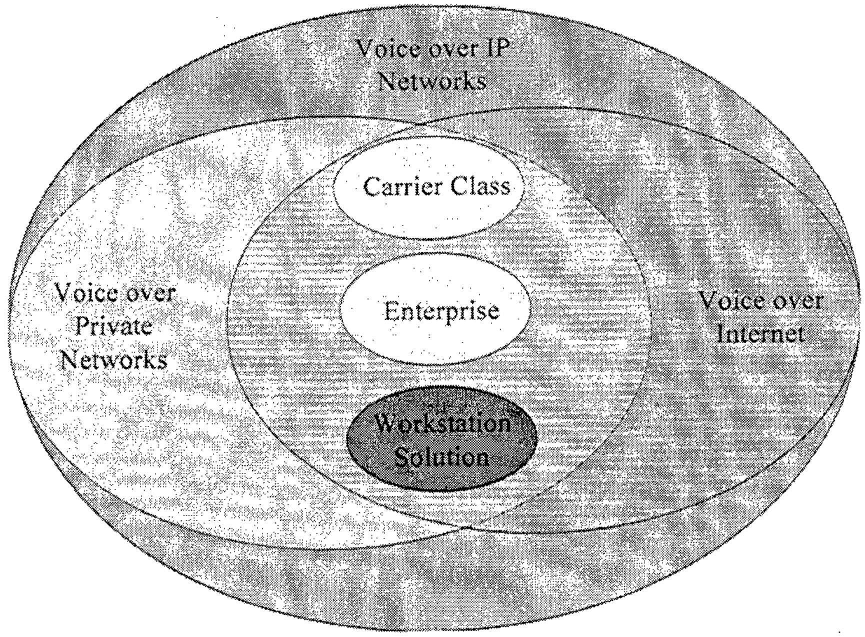

Figure 1.1 A Workstation solution to Internet Telephony

A workstation solution is defined as bringing the IP datagrams to the end user. Here, the workstation will decide how to handle and possess the ability to handle any type (Voice, Data) of IP packets. The main advantage to this solution is it fully utilizes the IP network because it contains no legacy interfaces with a Public Switched Telephone Network (PSTN).

The Carrier Class and Enterprise solutions are not discussed in this thesis other than this brief description. *Carrier Class* a large scale network that interfaces an IP network with a legacy PSTN through the use of "gateways" which reside at the Telephone Central Offices. *Enterprise Solution* is a smaller scale Carrier Class solution. An organization that has several different geographical locations, which are linked together by an IP Network, may use gateways at the different geographical locations to employ VoIP.

C. ORGANIZATION

This thesis is divided into six chapters. Chapter I is the Introduction which addresses the purpose, background and organization of this thesis. Chapter II deals with the H.323 Model and Voice over an Internet Protocol (IP) Network, and analog to digital and packetizing. Chapter III deals with an H.323 Gatekeeper for the Internet, and possible solutions such as: Internet Locator Service (ILS) and I seek you (ICQ). Chapter IV describes the Internet Telephony, and the Architecture of Internet, and performance of Internet as it relates to Internet Telephony. Chapter V is a description of experiments conducted. Chapter VI is the conclusions and areas for future work.

(THIS PAGE INTENTIONALLY LEFT BLANK)

II. H.323 MODEL FOR VOIP

This chapter describes the Voice over Internet Protocol (VoIP) H.323 model and its components. It also describes the factors which affect generic digitized voice over an IP network.

A. ARCHITECTURE OF H.323 VOIP MODEL

The H.323 architecture and protocol assumes the transmission path between the telephony users and passes through at least on local area network such as an Ethernet or token ring. It further assumes that the Local Area Network may not provide any guaranteed quality of service (QoS) needed to support the telephony traffic.

There are three major components of the H.323 architecture model used for VoIP are the Terminal, Gateway, and Gatekeeper.

H.323 terminal is shown in the below Figure 2.1. The end user box provides real-time two-way voice communications with another H.323 terminal. The terminal can also communicate with an H.323 Gateway if the voice traffic is changing to a non-H323 network such as the Public Switched Telephone Network (PSTN).

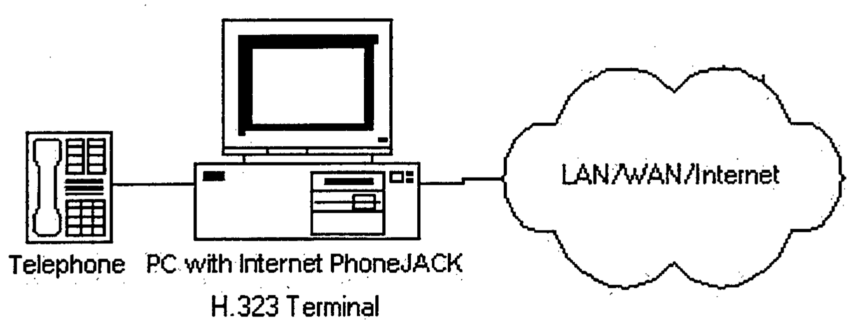

Figure 2.1 H.323 Terminal

H.323 Gatekeeper is shown in the below Figure 2.2. The Gatekeeper provides the control features such as call establishment and tracking of active terminals on the network.

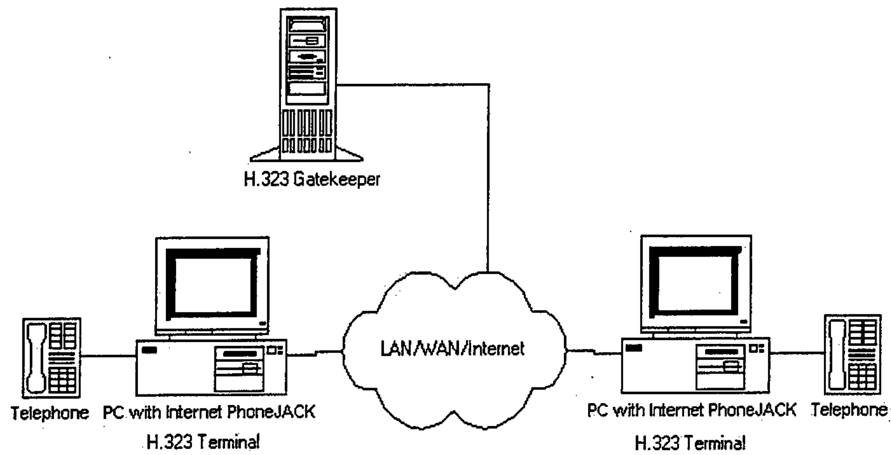

Figure 2.2 H.323 Gatekeeper

H.323 Gateway is shown in Figure 2.3. It is the node that will bridge the gap between a H.323 network and a non-H.323 network. I have shown the connection of a data H.323 network to the local Public Switched Telephone Network.

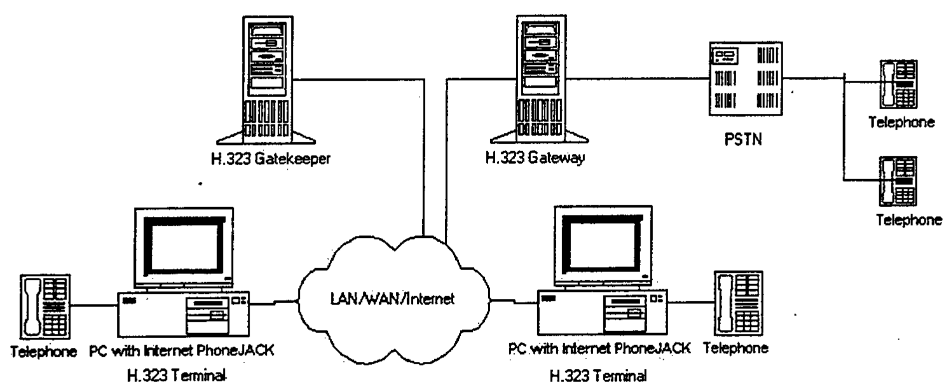

Figure 2.3 H.323 Gateway to Public Switched Telephone Network

The H.323 components will be used as the nodes for the research and experiments conducted within this thesis.

B. THE H.323 PROTOCOL STACK

H.323 protocol consists of several standards and cites the use of many others. These are depicted below in the Figure 2.4. The VoIP platform encompasses a vast ensemble of technologies and protocols. Some of those other protocols are: Internet Protocol (IP), User Datagram Protocol (UDP), Real Time Protocol (RTP), the Media Gateway Control Protocol (MGCP), the Resource Reservation Protocol (RSVP), H.323 and many others to provide a "VoIP Platform" to the end-user. [CSCO99] An overview of the IP and UDP protocol is provided.

<table>
<tr><th>Audio</th><th>Video</th><th>Data</th><th colspan="3">System Control</th></tr>
<tr><td>G.711</td><td rowspan="5">H.281
H.283</td><td rowspan="6">T.120</td><td rowspan="6">Call Control H.225</td><td rowspan="6">RAS Control H.225</td><td rowspan="6">H.245 Control</td></tr>
<tr><td>G.722</td></tr>
<tr><td>G.723</td></tr>
<tr><td>G.728</td></tr>
<tr><td>G.729</td></tr>
<tr><td colspan="2">RTP/RTCP</td></tr>
<tr><td colspan="2">UDP</td><td colspan="4">UDP or TCP</td></tr>
<tr><td colspan="6">IP</td></tr>
<tr><td colspan="6">L-2 Varies</td></tr>
<tr><td colspan="6">L-1 Varies</td></tr>
</table>

Figure 2.4 H.323 Protocol Stack

For audio applications, the G.711 speech Codec is required. However, newly developed Codecs such as G.723 and G.729 continue to improve VoIP applications. Chapter V deals with the testing and experimenting with these three codecs.

The principal function of a voice coder is to encode pulse code modulation (PCM) user speech samples into a small number of bits (a frame). This is done in such a manner that the speech is robust in the presence of link errors, jittery networks, and bursty transmissions. At the receiver, the frames are decoded back to the PCM speech samples, and then converted to the waveform.

1. Overview of IP

Only an overview of IP is required for this thesis, and I emphasize only the aspects of IP that are important for the support of voice traffic.

IP is an example of a connectionless service. It permits the exchange of traffic between two host computers without any prior call setup. However, these two computers must share a common connection-oriented transmission port protocol. Since IP is connectionless, it is possible that the datagrams could be lost between the two end-user's stations. For example, the IP gateway hardware enforces maximum queue length; if this queue length is violated, the buffers will overflow. In this situation, the additional datagrams are discarded in the network.

Since IP is an unreliable, best-effort datagram-type protocol, it has no retransmission mechanism. It provides no error recovery for the underlying subnetworks. It has no flow-control mechanisms. The user datagrams may be lost, duplicated, or even arrive out of order. It is not the job of IP to deal with most of these problems. For this reason, a higher-level transport layer protocol (TCP) is required.

These low-level characteristics of IP translate into an effective means of supporting real-time voice traffic. Assuming the routers are fast, and sufficient bandwidth is available, IP does not introduce significant overhead to the support of VoIP. Again, the universal presence of IP is the largest selling point.

2. Overview of UDP

Layer 4 of the OSI model is where User Datagram Protocol (UDP) operates. UDP is a connectionless protocol and does not provide sequencing or acknowledgements. Since it has no reliability, flow control, nor error-recovery measures, UDP serves principally as a multiplexer/demultiplexer for receiving traffic into and out of an application.

UDP uses the port concept to direct the datagrams to the proper upper-layer application. The UDP datagram contains a destination port number and source port number. The destination number is used by UDP and the operating system to deliver the traffic to the proper application.

Recently, routers have begun examining the port numbers in order to determine the type of traffic in the user payload. For example, a destination port number might identify a real time application and the router could then treat this traffic as a high-priority unit.

C. BARRIERS FOR SUCCESSFUL DEPLOYMENT OF VoIP

Deployment of VoIP is not a trivial matter. The main reason is that the IP suite (and the hardware for data networks) is not designed to accommodate synchronous, real time traffic, such as voice. In addition, the traffic loss experienced in IP networks as well as the amount and variability of delay militates against effective support of voice traffic. Factors such as the variable delay, non-cooperative, and the connectionless nature of an IP networks are discussed.

Variable delay is onerous to speech. It complicates the receiver's job of playing out the speech image to the listener. Furthermore, the delay of the speech signal between the talker and the listener can be excessively long. This will result in the loss of information; the digital-to-analog converter cannot use the last-arriving samples.

Another factor to be considered in the public Internet is the "*non-cooperative nature.*" The Internet is amalgamation of disparate networks and service providers who have formed associations in an evolutionary and somewhat fragmented manner. It may not grant the user's bandwidth requirements. Sometimes the user will get the service needed and sometimes not.

Another point is the *connectionless nature* of the IP networks, which may detract from effective voice communications. The challenges in supporting synchronous voice traffic over the Internet would have to be met with such tools as priority scheduling, upper-layer resource reservation and source routing to simulate the aspects of a connection-oriented technology.

D. EVALUATING FACTORS IN PACKETIZED VOICE

There are three main factors to evaluate in packetized voice are packet delay, bandwidth requirements, and computational effort. Each plays an important role in the overall quality of voice over an IP network.

Packet delay describes how long it takes to send the packet from the sender to the receiver. Two aspects of packet delay should be known. The first aspect is how long it takes to send the traffic from the sender to the receiver. The second aspect is the variation in time of the arrival of the packets at the receiver. The variation in delay is called *jitter*.

For packetized voice to be translated back to an analog signal in a real-time mode, the two-way delay for voice packets must be constant and generally must be low-usually less than 300 ms. The two-way delay measures how long it takes:

(a) for A's speech to reach B
(b) for B to hear the speech
(c) for B to talk back
(d) for A to hear B's response

If the delay becomes too long (approx. 400-500 ms) the conversation appears phony, almost like a half-duplex connection where the two people are taking turns talking, but waiting a while before taking the turn to talk.

Voice transmissions exhibit a relatively higher tolerance for errors than pure data transmissions. If an occasional packet is distorted, lost, or discarded by the network, the fidelity of the voice reproduction is not severely affected. If the total of the wayward packets is less than 10 percent of the total packets transmitted it will not severely affect voice fidelity.

The second factor deals with how much *bandwidth is required* to support the voice transmission. The bandwidth calculation must factor in the bits required to represent the speech signal as well as the overhead headers (protocol control information) that are used to support the signals. At a minimum this includes the Layer 2 header, the IP header, the UDP header, the Layer 7 header and the headers created by the voice coder. All totaled, they add significant overhead to the voice packet and this protocol control information is a big drain on the available bandwidth.

The third factor is the *computational effort* needed to support the coding, transport, and decoding for the speech images in each machine in the network. The term computational effort refers to the expense and complexity involved in supporting services to the audio application. In simple terms, it refers to the Millions of Instruction per

Second (MIPS) required to support the operation, as well as the amount of memory needed.

As an example of computational efficiency, a conventional 64-kbit/s-voice signal can be produced in a high quality manner by the use of a 2-MIPS machine. A 15-20 MIPS machine can significantly reduce the requirement to 8 kbit/s for a high-quality reproduction of voice. Currently, the ITU-T is examining a standard for a 4-kbit/s machine that is excepted to require a 40-50 MIPS machine.

E. SUMMARY

The H.323 model has become the industry standard for VoIP and Internet Telephony. We have discussed the components that are utilized for VoIP and the factors which affect generic digitized voice over an IP network. The next chapter will deal with how the H.323 Gatekeeper can be implemented for Internet Telephony.

(THIS PAGE INTENTIONALLY LEFT BLANK)

III. H.323 GATEKEEPER FOR INTERNET

The H.323 model makes the basic assumption that there will be at least the basic H.323 nodes for effective communications. That is, it assumes two or more end users (H.323 terminals) and a H.323 Gatekeeper. However, when dealing with a public domain such as the Internet, who will setup and maintain the Gatekeeper?

This chapter deals with two programs, which can be used on the Internet or a private domain to provide the required control processes and the functionality of a H.323 Gatekeeper.

A. INTRODUCTION

Locator services are a relatively new concept to the Internet. There are two types of locator services: Internet Directory Services and Internet Locator Services. The *Internet Directory Services* lets a user find **static** information about other users on the Internet (for example, telephone numbers and e-mail addresses). The *Internet Locator Services* allow you to find **dynamic** information about people who are currently logged onto the Internet. They store the information about a user that is changing or that is available only when they are logged on (for example, IP address).

The current sets of Internet Locator Servers have been limited in scope, and without standard protocols for communication with real time applications, such as Internet telephony. Consequently, the Internet has lacked a standards-based Locator service that could be used by an organization both as an internal locator and for access to global location information.

I have implemented two types of Internet Locator Servers for comparison and testing. The Microsoft Internet Locator Server (ILS) is discussed first and the I seek you (ICQ) implementation is discussed second.

B. ILS SOLUTION

Overall, the components of the Microsoft Internet Locator Server (ILS) provides a flexible system that offers a dynamic (location) directory services to a variety of different client applications.

Dynamic directory information is handled by the Internet Locator Server. A person's IP address, which can be different every time a user logs on to the Internet, is an example of dynamic directory information that other users may want to retrieve.

When users connect to the Internet, they can register their names and IP addresses with the ILS server. Throughout their time online, client applications send periodic refreshes to the server to keep user ILS entries valid. When the client application terminates for any reason, the ILS server deletes user entries after the refresh period has elapsed, thereby protecting against stale directory information.

Because of the frequency of client refreshes, ILS stores its information in a RAM database. This provides better performance than if the information was in a disk-based database. Clients can access the directory through the ILS Locator Directory Application Protocol (LDAP) interface, or through a Web page. Both the HTTP and LDAP interfaces are discussed.

1. ILS Interfaces

ILS has two interfaces for gaining access to its contents: a standard HTTP interface for HTML Web pages, and a standards-based LDAP interface for ILS to access the dynamic directory information.

A service provider can use the *HTTP interface* to design a dynamic member directory that users access through their Web browser, as shown below in Figure 3.1. Figure 3.2 shows the results of a search for currently online users.

The ILS *LDAP interface* provides Internet standards-based access protocol that allows any third party Internet client to access the ILS servers for dynamic directory information, such as a user's current IP address. This facilitates the construction of point-to-point Internet communication sessions. A listing of all users currently logged onto the server is shown below in Figure 3.3.

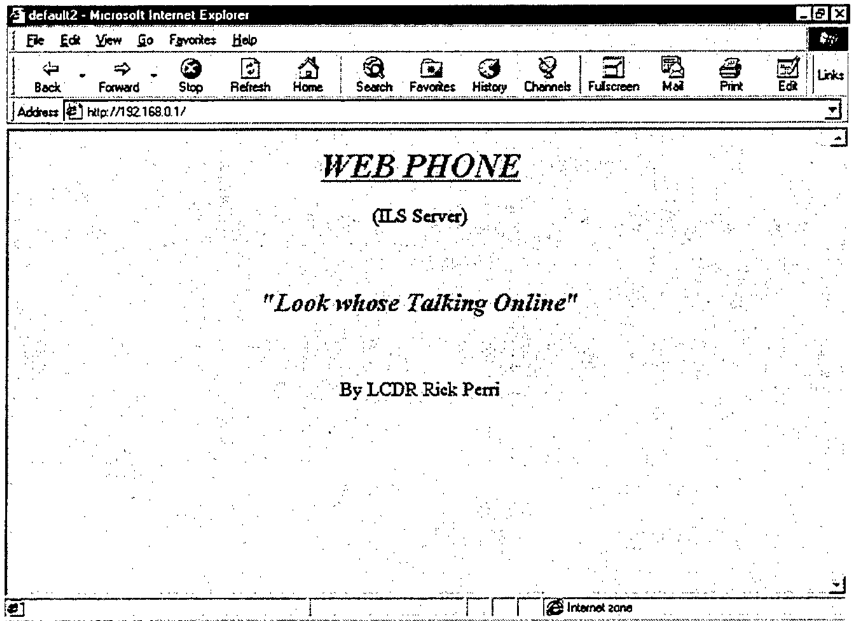

Figure 3.1 HTTP interface (Web page)

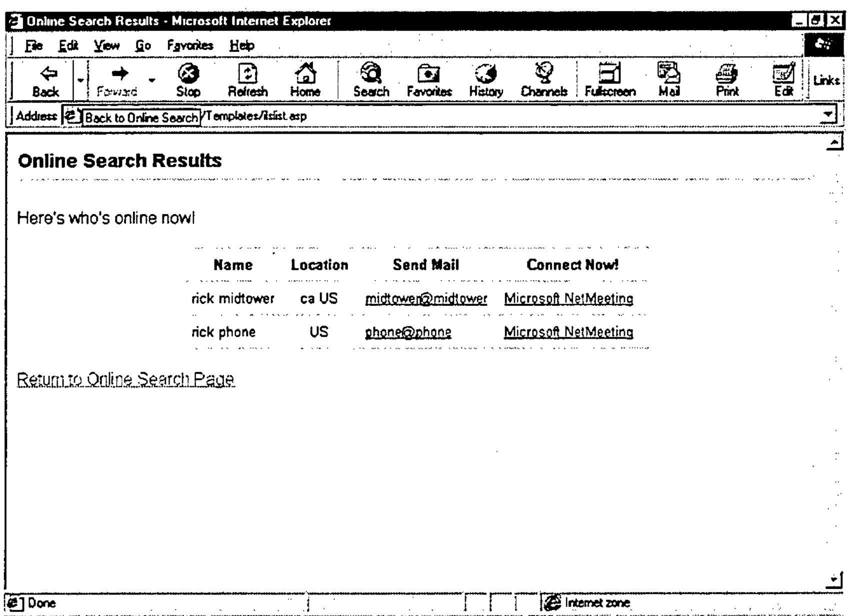

Figure 3.2 HTTP interface search results

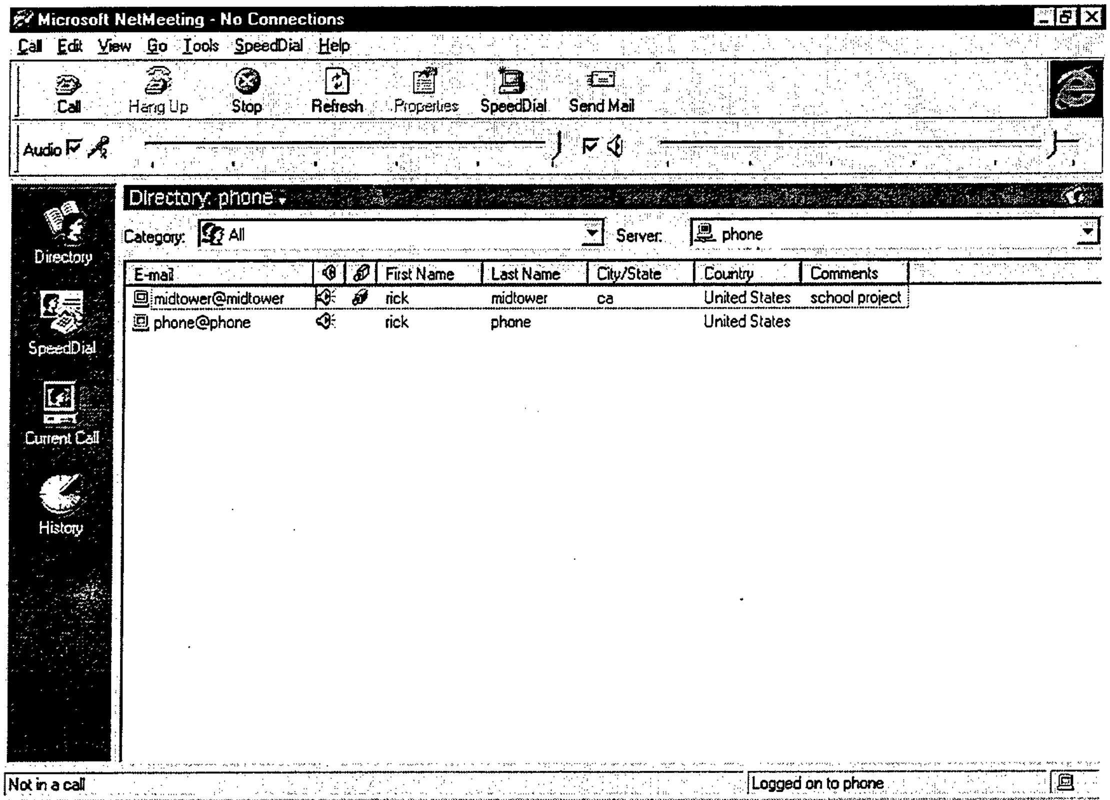

Figure 3.3 ILS LDAP interface showing users logged onto the server [OPG96]

2. ILS Hardware Architecture

The following Figure 3.4, shows a possible network topology of an ILS system. As described in Chapter V, this network was establish for testing of Internet Telephony calls.

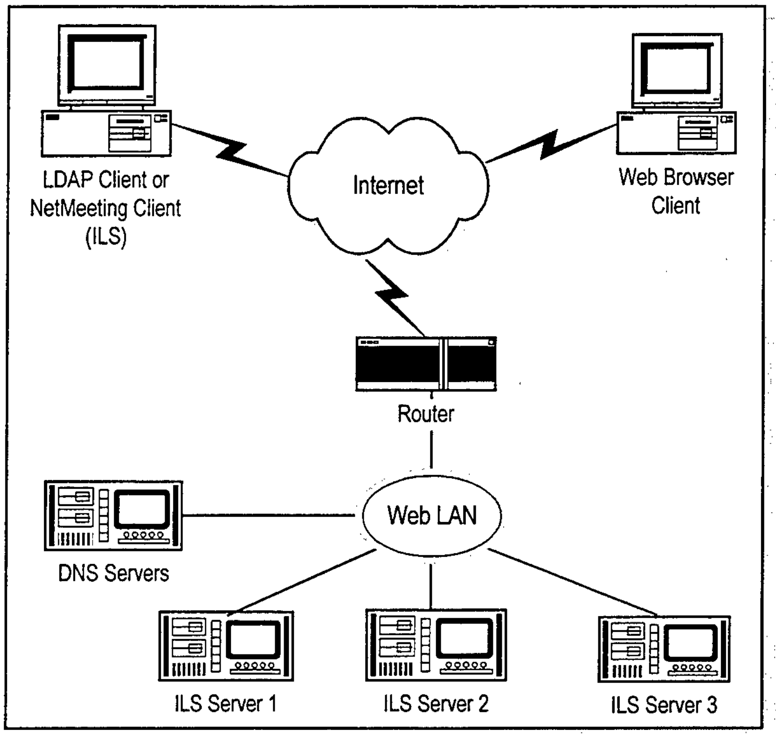

Figure 3.4 ILS Server Architecture [WAG96]

3. ILS Software Architecture

At a very high level, the following components are involved in these processes:

- The **Web Browser Client** is an end-user computer running software using one or more of the LDAP or HTTP interfaces to retrieve directory information.

- The **Active Server Pages** processor executes ASP scripts on the server to produce HTML for the client browser. The ILS ActiveX server component is used by ASP scripts to interact with ILS: it is the Web author's interface for the ILS database DLL.

- The **HTTP Interface** gives Web browsers the ability to manipulate and query the ILS database. Through the Active Server Pages feature of Internet Information Server version 3.0, access to ILS is provided from a Web page.

- The **LDAP Interface** is a service of the Internet Information Server framework. This service allows LDAP clients to manipulate and query the ILS database.

- The **ILS Database** is a memory-resident database where dynamic directory information is stored. Entries are kept in the ILS database as long as clients refresh them periodically. This ensures that other clients have access to the most current information about each user's Internet location.

4. Process Relationships

This section describes the ILS process flow and shows how the hardware and software components work together. This section includes an overview of the process, detailed flow descriptions, and a preview of how to administer the ILS processes.

ILS acts as the server in a client-server network system. As a server, it responds to client requests for information. The requests are typically carried by either HTTP or LDAP protocols. When a client application requests information-using HTTP, ILS uses the Active Server Pages framework to respond with HTML pages that can be viewed with a standard Web browser. When a client application makes an ILS LDAP request, ILS generates LDAP responses that contain directory information or error codes.

Queries from the LDAP interface are passed through the ILS directory Dynamic Link Library (DLL) to the ILS DataBase Dynamic Link Library. Queries from the HTTP interface are handled by an ActiveX server component that reformulates the query for the ILS directory DLL. For HTTP queries, an Active Server Pages (ASP) script on the server composes the query results into an HTML page, which is then returned to the user.

5. ILS Key Processes

The ILS Server has the following key processes:

- **ILS/HTTP** Web browser clients accessing dynamic (location) directory information.
- **ILS/LDAP** LDAP clients accessing dynamic (location) directory information.

Figure 3.5 illustrates how ILS handles a query from a client. Note that ILS/HTTP and ILS/LDAP are both running within the same instance of ILS.

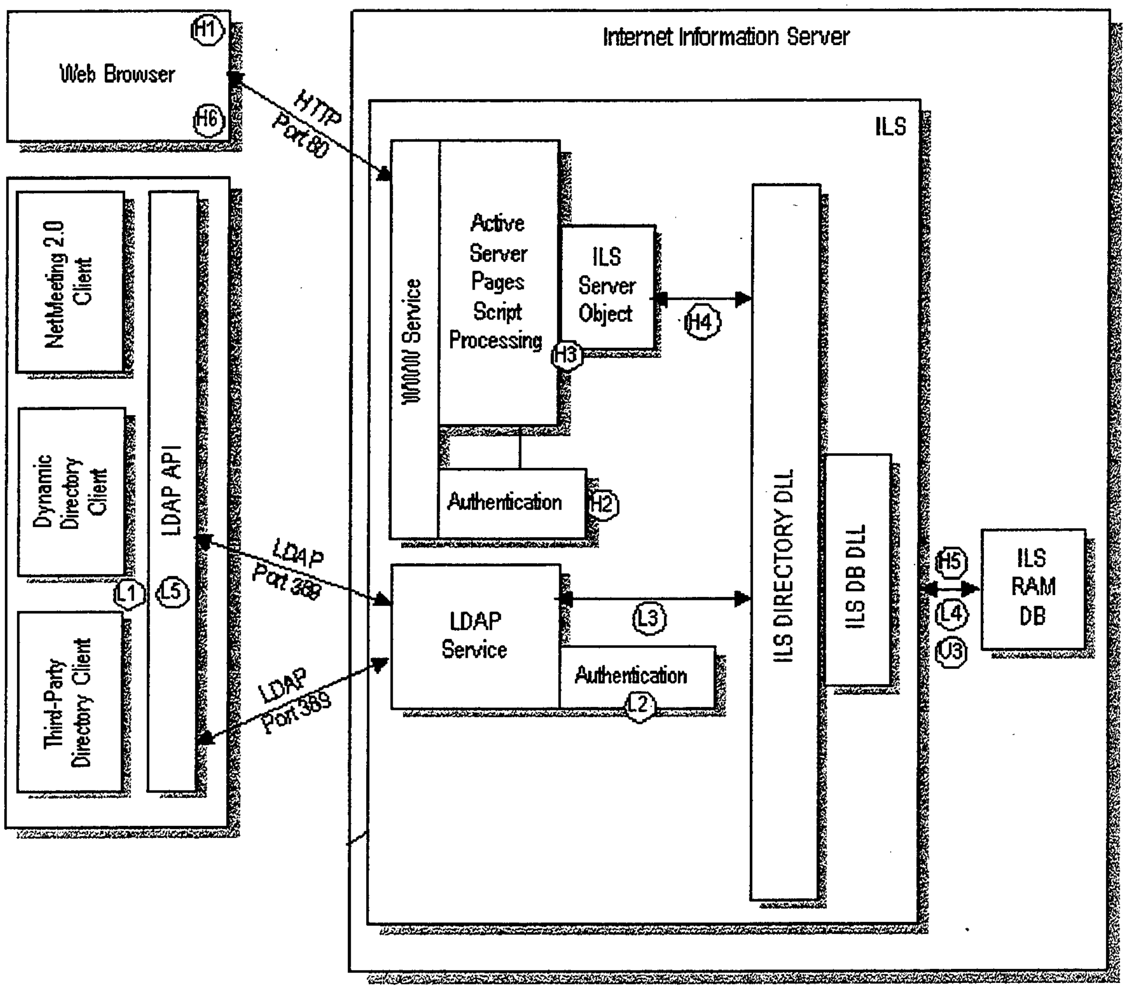

Figure 3.5 Relationship of Key Processes [OPG96]

In the following section, the identifiers (H1, H2, L1, L2, and so on) correspond to process steps in the preceding diagram. [OPG96]

When a directory request is received from *a Web browser client (HTTP Process)*, the following process takes place:

- (H1) The user submits a query to the ILS/HTTP service through a standard HTML form.

- (H2) If the system is set up for security authorization, the query must be accepted by the authentication system.
- (H3) If the authentication is necessary and succeeds, the query is routed through the script interpreter, which loads the ILS ActiveX server component to handle the query.
- (H4) The server component issues a reformulated query to the ILS directory DLL.
- (H5) The ILS directory DLL issues a query to the ILS dynamic database.
- (H6) The ILS database returns the query results through the ILS database DLL, which in turn routes the results through the server component back to the user in HTML format.

When a directory request comes from *an Internet client application (LDAP Process)*, such as Microsoft NetMeeting or Intel Internet Phone, the following process takes place:

- (L1) Using an ILS LDAP client, the user submits a query to the LDAP service.
- (L2) If the system is set up for user authentication, the query must be accepted by the authentication system.
- (L3) If the authentication is necessary and succeeds, the LDAP service passes the query to the ILS directory DLL.
- (L4) The ILS database DLL issues a query to the ILS database.
- (L5) The ILS database returns the query results through the ILS database DLL, which in turn routes the results through the LDAP service and back to the client.

C. ICQ SOLUTION

The second implementation of a Internet Locator Server was the I seek you (ICQ) server. The ICQ (I seek you) network is a global instant contact system that lets you detect if others are connected to the Internet and then allows you to connect directly to them. This works similarly to a telephone number except that an ICQ # tracks both your IP address and your telephone number. The ICQ number is one of a kind and cannot be duplicated; it is individual to you. The ICQ user can connect with voice, email or data chat services. Using an ICQ number instead of an ILS or other such public log-in directories gives the user quick and efficient connectivity. There is no searching through long lists to find people; a single number is all you need. As an ICQ user, you can control who can or cannot reach you.

ICQ is a free contact directory available to anyone who wishes to utilize the Internet for communication. Using ICQ the user can collaborate over the Internet using data chat and initiate voice calls using multiple telephone applications. As long as you are connected to the Internet, you can be reached at your PC. ICQ allows you to bypass ILS servers and other public directory servers used for PC to PC communication to connect in a more time efficient manner. The ICQ number replaces the need for a location server by allowing you to be identified on the ICQ network when you are running the ICQ application.

ICQ works by installing a small client application program on each of the end user terminals. This client application program runs continuously in the background and provides an updated status to the remote ICQ server. The updates are frequent enough for the ICQ server to propagate a status down to a fraction of a second.

ICQ Hardware Architecture is shown in two examples below: PC to PC, and PC to PSTN Gateway configuration. Again, these network configurations were implemented and described in Chapter V.

In the example below, there are three steps to the basic process of using a communication application to call from *PC to PC* using an ICQ number. The first step is the dialing of an ICQ number to attempt to reach an associate. Step two is the query of the ICQ server to locate the person's current IP address and location. If the recipient of the call is logged onto the Internet, the communication is placed to their PC. The third step is the communication connected to their PC begins to ring letting them know there is an incoming communication. The PC to PC configuration is shown below in Figure 3.6.

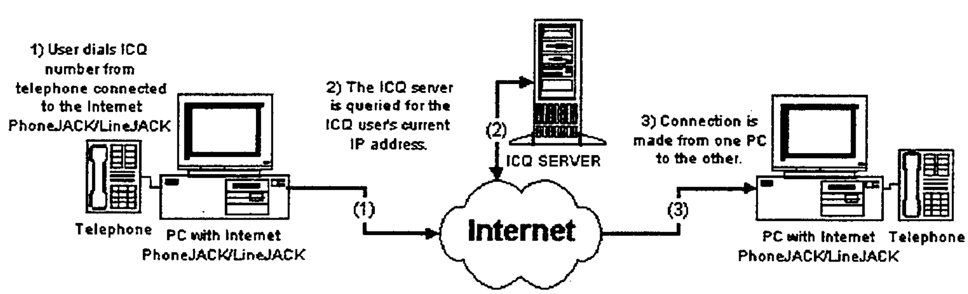

Figure 3.6 ICQ Architecture for PC to PC

In the next example, there are three steps to the basic process of using a communication application to call from *PC to PSTN* using an ICQ number. The first step is the dialing of an ICQ number to attempt to reach an associate. Step two is the query of the ICQ server to locate the person's current IP address and location. If the recipient of the call is not logged onto the Internet, the communication is via a PSTN Gateway server. The third step is the communication connected to standard phone begins to ring letting them know there is an incoming communication. The PC to PSTN configuration is shown below in Figure 3.7.

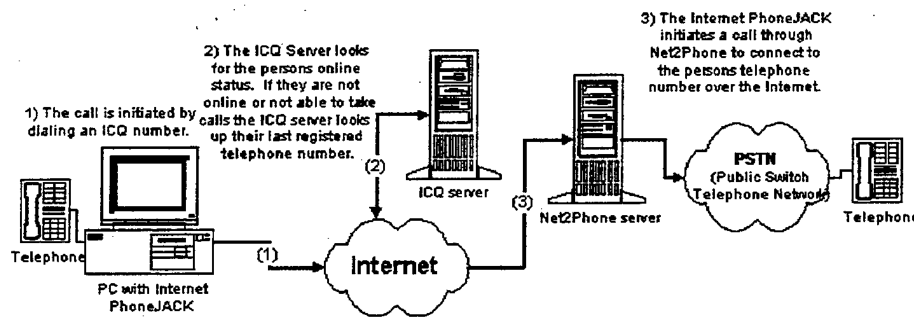

Figure 3.7 ICQ Architecture for PC to PSTN

D. COMPARISON OF ILS AND ICQ SOLUTIONS

A brief comparison of the two implementations (ICQ and ILS) of an H.323 Gatekeeper for Internet telephone is described.

The advantages of the ICQ implementation are the disadvantages of the ILS implementation:

- **One number ID.** Each ICQ number is unique per person. That uniqueness enables a user location to be determined no matter where on the Internet or forwarded to the PSTN . ILS can not forward communications to the PSTN automatically.
- **Server Information is shared.** No matter which of the many ICQ servers you are communicating with, your online status is replicated to all the ICQ servers on the Internet. This allows the sharing of a user status world wide and not to a specific server. ILS servers due not share information. Therefore, a user logged onto one ILS server has no idea of a user logged onto another ILS server.

- **Ease of use**. Once the client program is installed and running it is transparent to the end user. The end user can locate an other user on the Internet automatically or manually. ILS servers require the user to log on/off in order to join or leave the server.

- **Instantaneous status feed back**. Since the client programs continuously sends out updates to the server via an Internet connection, the user's status is known instantaneously to other Internet users. ILS feedback of a user's status is often inaccurate and outdated.

E. SUMMARY

Setting up and maintaining a H.323 Gatekeeper in a public domain can be a relatively hard process. If you are successful, you will soon be swamped with users, and your system needs to be *scalable* to handle millions of users. Difficulties will be experienced by end users trying to communicate with *different software applications* and *different versions* that may not work as advertised. In addition, if you were in business, the Gatekeeper functionality has to provide for billing and charges. Currently none of the Internet Gatekeepers charges for their service. However, some servers are proprietary in which an end user would have to have that companys application program to log onto the server.

(THIS PAGE INTENTIONALLY LEFT BLANK)

IV. INTERNET TELEPHONY

This chapter starts out with a brief description of the Internet's architecture and discussion on the point of presence (POP) for most dial-up users is provided. It then follows with a discussion of attributes of the Internet such as Round Trip Time (RTT), packet loss, non-fixed routing, and the size and protocol type of packets currently being sent on the Internet. Performance characteristics and a case study for VoIP over the Internet conclude this chapter.

A. ARCHITECTURE OF THE INTERNET

Today, the Internet is a complex collage of regional and national networks that are interconnected together with routers. The communication links used by the Internet Service Providers (ISP) are leased lines from the telephone system usually DS1 or DS3 lines, and increasingly SONET lines. The basic Internet connections and the many ISPs are illustrated in Figure 4.1.

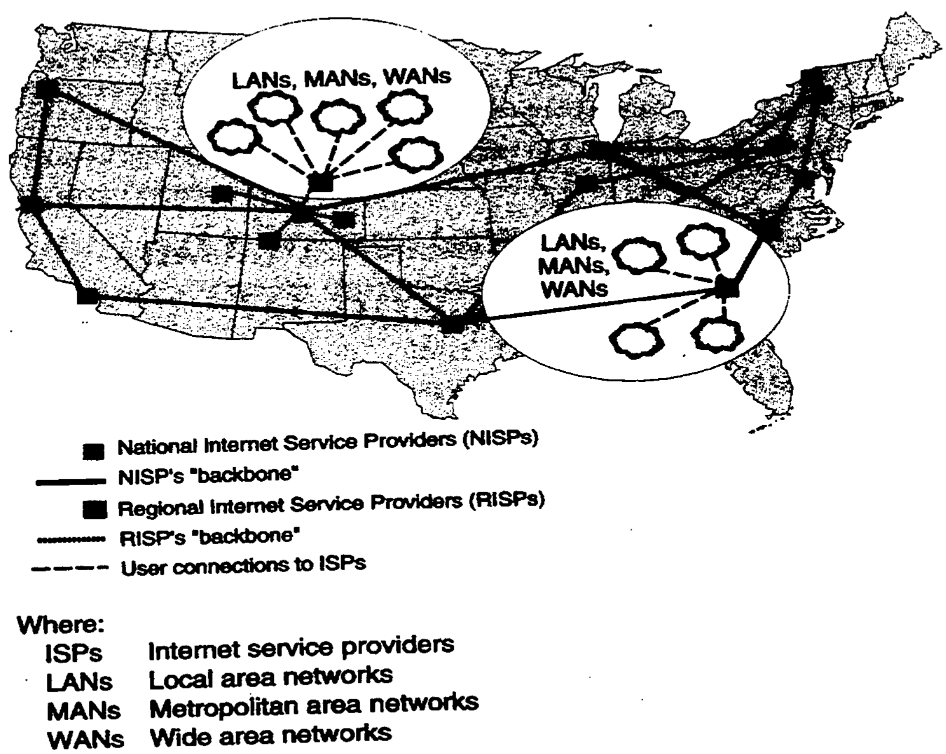

Figure 4.1 Internet Overview [BLAK99]

The Internet Service Providers (ISP) provide the access into the Internet. They provide this access through the telephone network, and the Internet will connect to the ISPs through the telco local exchange carrier (LEC), and the exchange carrier's central office (CO).

The telephone companies are required to provide the ISPs with a connection to the telephone company's customers. The connections are provided at the telephone companies Central Office (CO). These connections from the customer to the central office's Main Distribution Frame (MDF) may be patched to the local switch or to a digital cross. Commonly, the connection from the CO to the ISP is attained through a digital cross connect (DCS) machine.

A typical Internet user employs a conventional V series modem to modulate the analog signals on the local loop to the local telephone office, shown in Figure 4.2. At the telephone office the signals are digitized in some type of T1 frame and sent through the telephone digital backbone to a designated ISP. The Telephone Company performs the analog-to-digital (A/D) and digital-to-analog (D/A) conversions operations. Therefore the interface between the telephone system and the ISP node is digital if the telco backbone is used.

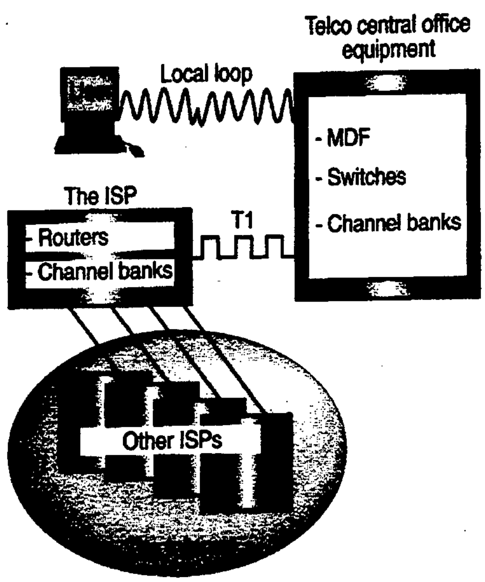

Figure 4.2 Typical dial-up user connection to Internet [BLAK99]

The ISPs connect to each other through the eleven nationwide Network Access Points (NAPs). The NAP's job is to exchange traffic between ISPs and other networks. NAPs must operate at link speeds of 100 Mbit/s and thus their local networks have been implemented with Fiber Distributed Data Interface (FDDI), 100 Base-T (Fast Ethernet at 100 Mbit/s), or 1000 Base-T (Gigabit Ethernet at 1 Gbit/s). Many of them have ATM switches and SONET links to other NAPs and the larger ISPs.

The ISP or NAP node can range from a simple configuration to one that has scores of routers, servers, LANs, and ATM/Frame Relay switches. A typical ISP site will have high speed LANs, multiple servers and high-speed access to the wide area networks. This is where the bottlenecks can often occur. If the LANs inside the ISP site are not fast enough, or if the routers become overloaded, then bottlenecks can occur. If the server farm is not large enough, then the servers may be buffering the data too long. In order to deliver steady streams of traffic into and out of an ISP it must frequently tune itself.

B. ATTRIBUTES OF THE INTERNET

The Internet was developed to transfer traffic by using adaptive routing features. This means that the traffic may take different routes through the Internet depending on the condition at a specific time. As stated earlier, the Internet is designed as a connectionless system, which means that there are no "affiliations", established between the machine in the Internet. Consequently, the Internet does not maintain an ongoing knowledge of the user's traffic routes.

The Internet is a "best effort" delivery network. The Internet will attempt to deliver the data traffic, but if problems occur, the traffic will be discarded.

Finally, the current Internet supports either unicast (one-to-one) or multicasting (one-to-many) operations.

Internet attributes such as the local loop, Round Trip Time (RTT), packet loss, packet routing, packet size and protocol type are discussed.

The biggest problem in deploying high-quality Internet Telephone is the limited *bandwidth on the local loop.*

For today's analog voice transport systems, the present structure on the local loop provides adequate capacity, but that capacity is insufficient for other application, such as data and video. Voice has a modest bandwidth requirement of about 3.5 kHz of the frequency spectrum. The local loop is designed to support voice bandwidth.

The problem is that many applications that are now in the market place, or are being developed, are significantly handicapped by local loop bottlenecks.

Round-trip time (RTT) is a measure of the time it takes to send a packet to a destination node and receive a reply for the node. RTT includes the transmission time in both direction and the processing time at the destination node.

Most RTTs in the Internet are within the range of 70 -160 ms, although larger variations to RTT do occur. Due to the asynchronous nature of the Internet, RTT is not consistent. During periods where Internet traffic is heavy, the RTT may exceed 300 ms.

The ITU-T G.114 recommendation limits RTT to 300 ms or less for telephone traffic. This performance factor is based on many studies and observations; they conclude that longer delays in a telephone-based conversation give the impression to a voice user that they are using a half-duplex circuit, which is an unsatisfactory connection.

Another Internet characteristic that is important in Internet Telephony is *Packet Loss*. The two factors involved are (a) how often packet loss occurs and (b) how many successive packets are affected.

Packet loss is important to Internet telephone, since the loss may affect the outcome of the decoding process at the receiver, and may be detected by the end-users ears.

Today's voice coders can produce high-quality voice signals with about a 10 percent loss of the voice packets, if the packet losses are random and independent. The G723.1 compensates for this loss by using the previous packet to simulate the characteristics of the vocal signal that was in the lost packet.

Traffic loss in the Internet is bursty: large packet losses occur in a small number of bursts. This characteristic of the Internet behavior complicates the support of Internet telephony, because packetized voice works best if the packet loss is random and independent.

Currently studies are underway to capture statistics and discover the incidences of misordered *packet arrival.* Several studies show that out-of-sequence arrival is common. In a voice application, arrival order is important because packets that arrive out of sequence may arrive too late to be useful. They may be discarded and handled as a lost or delayed packet.

Hop count is a term used to describe the number of hops between a sender and a receiver. It is a critical aspect in Internet telephony because more hops means more delay, and more variable delay. Hop count must consider round-trip time (RTT), because of the interactive, real-time nature of telephone conversations. Figure 4.3 shows several aspects of hop count and RTT, and it affects the quality of voice applications.

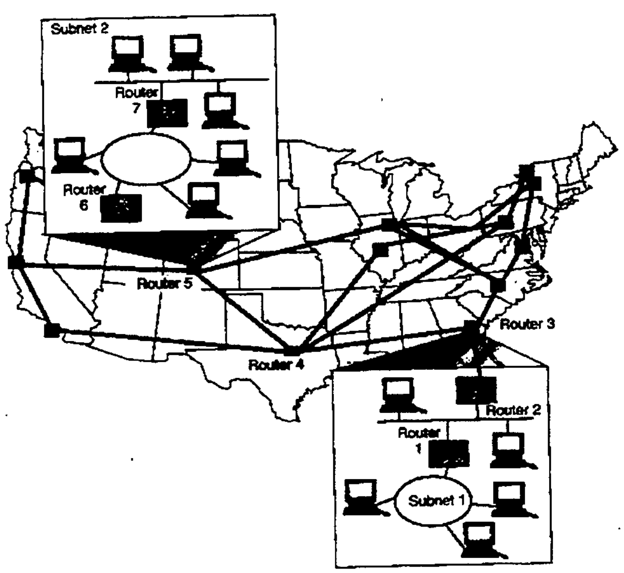

Figure 4.3 Subnet Hop count [BLAK99]

The traffic is to be sent from a host on subnet 1 to a host on subnet 2. The IP datagrams must be processed by both hosts as well as all the routers on the path between the hosts. Let us assume the traffic traverses through the fewest number of hops, which in this case means the datagrams are processed by seven routers, numbered router 1 through router 7 in Figure 4.3. Thus, the datagrams are sent thorough nine hops. If the routers are not heavily loaded with traffic, then queuing delay will be short, and the delay at each router, while variable, will not create a major problem when the traffic arrives at the receiver. However, if traffic is heavy and /or the routers are not performing their datagram forwarding operations efficiently; then the accumulated and variable delay will result in the inability of the receiver to reconstitute the real-time voice signal.

Several studies also reveal that it is clear that geographical distance cannot be correlated to round-trip delay. Indeed in one study, a short distance of only 477 miles, but with a hop count of 21 resulted in a 500 ms round-trip delay. Therefore to emphasize, hop count is an essential factor in delay and geographical distance is less of a factor.

Fixed routing is a desirable feature for real-time traffic. However, how necessary its it?

Studies conducted on the routing behavior of the Internet reveal that most of the traffic between two or more communicating parties remains on the same physical path during the session. In fact, route alteration is more an exception than the rule.

One study on Internet "routing persistence" is summarized in Table 1 [PAXS97].

Duration of traffic flow	% of routes that change	Comments
Seconds	N/A	Used in load balancing
Minutes	N/A	In tightly-coupled routers
10's of minutes	4	Changes usually through different cities or autonomous systems
Hours	9	Usually intranetwork changes
6+ Hours	19	Usually intranetwork changes
Days	68	(a) 50 % of these routes persist for <7 days (b) Other 50 % persist for >7 days

Table 1: Routing Persistence [PAXS97]

Paxson defines routing persistence as how long a route endures before changing. Although in the Internet routing, changes occur over a wide range of time. Most of the routes in the Internet do not change much.

Note: The N/A entries in Table 1 represent situations in which routing fluctuations do occur in the Internet but they are not a factor in the "big picture".

The most common *packet size* traveling on the Internet is 40 bytes, which accounts for TCP acknowledgements (ACKs), finish messages (FINs), and reset messages (RSTs). Overall, the average packet sizes vary from 175 to about 400 bytes, and 90 percent of the packets are 576 or smaller. Ten percent of the traffic is sent in 1500-byte sizes, which reflects traffic from Ethernet-attached hosts. Figure 4.4 breaks down the occurrence of the common size packets traveling on the Internet.

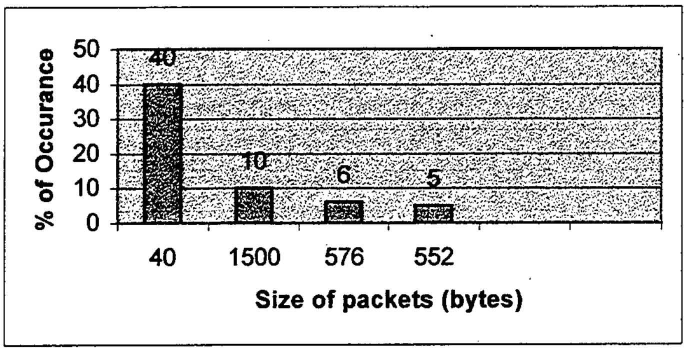

Figure 4.4 Most Common Sized Packets Traveling on Internet

In Figure 4.5, the *packet protocol* type carried by IP is shown. Almost all the traffic is TCP, followed by UDP, then ICMP. Other encapsulated directly in IP accounts for very little of the Internet traffic.

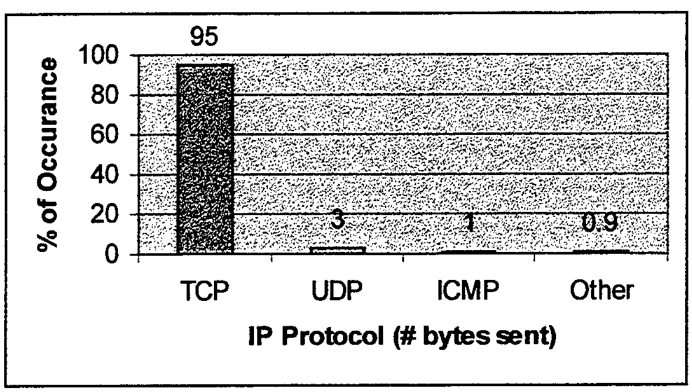

Figure 4.5 Most Common Protocols Travelling over Internet

The significance of these facts to VoIP is as follows. First, it is important to use small packets for voice traffic. If a packet is lost in the network, the small packet is less likely to contain significant parts of a speech signal. The idea is to divide and conquer. Most low-bit rate voice coders are designed to produce very short voice packets, usually no more than 10-30 ms in duration, and 10-30 bytes in length.

The other reason for small packet is that it permits the processing node, such as a router, to examine and operate on a small unit of information quickly. The router does not have to wait very long for the bits to propagate through the incoming interface. In contrast, a long packet means it takes a while for the bits of the entire transmission to arrive and therefore to be processed.

As shown in the Figure 4.4, the Internet has been calibrated to use relatively large packets. The fact that almost 50 percent of the packets transported in the Internet are only 40 bytes is not significant. They are not for user traffic, but for connection management operation for TCP.

If a substantial amount of Internet traffic becomes voice traffic, it will require an increase in Internet capacity, because the smaller packets will consume significantly more of the overall bandwidth. The ratio of overhead to user payload will increase.

A potentially bigger problem is the increased load on the routers in the Internet. The router has to spend as much time processing the fixed-length header of a 10-byte packet as it does in processing the same length header of a larger packet. This will be alleviated with the migration of high-speed gigabit routers, and the overall latency in the Internet will continue to improve.

C. PERFORMANCE

As discussed earlier, the larger the packet loss, the worse the audio quality will be at the receiver. On the other hand, large packet sizes increase the delay and so do large buffers. This section looks into packet loss, packet delay, packet size and buffer size considerations.

First, let's consider the *loss* of user traffic. The *size of the packet* is quite important for speech because of the concept of packet length. Packet length is a function of the number of bits in the packet, and the coding rate of the signal. Studies reveal that losing traffic that is around 32-64 ms (for G.711 traffic) in duration is disruptive, because it means the loss of speech phonemes. On the other hand, cell loss of duration of some 4-16 ms is neither noticeable nor disruptive to the listener. Therefore, a payload size of anywhere around 32-64 octets would be acceptable to an audio listener. The actual perception of audio loss is a function other factors such as the compression algorithms used, etc.

Next, consider *buffer size*. A larger buffer will increase *delay*, and decrease the loss rate, because the larger buffer allows more flexibility in playout, and the machine does not have to discard as many packets. However, the continued decrease of the buffer size, while decreasing delay, means more packets will be discarded. In effect, as the buffer size approaches 0, the machine operates at wire speed, but will experience more loss of traffic.

So, there is a trade off between buffer size and delay. The voice packet should be small, in order to reduce latency and improve quality. However, there is a point of diminishing returns where the overhead of headers to the smaller user packets is so high that it negates any chance of an efficient network. The newer codes G.729 and G.729a have found 10 ms bundles to be efficient.

D. CASE STUDY FOR VOIP OVER THE INTERNET

This section is a description of a test conducted by 3Com on the performance of VoIP over the public Internet. The source of the study is [COX98] .

The study entailed sending and receiving traffic between three nodes: University of California, Davis; University of Illinois, Chicago; and DePaul University. The geographical distance for the farthest leg was about 2/3 the length of the USA. The tests were run for a six-month period in 1998. During these tests, a client would transmit once per hour to a server for three minutes. Observations were made in the evenings as well as various times during the business day and on weekends. The transmission involved a trace that allowed the analysts to judge RTT and packet loss. The data representing RTT does not include analog-to-digital conversion, Codec operations, or other factors that would be required for a VoIP application.

Codecs G.723.1 and G.729a were employed for PC-to-PC communications and VoIP gateway communications.

Several important aspects of the study can be summarized in Figure 4.6. Figure 4.6 compares the average RTT (ms) in relation to the hop count. The hop count represents the number of nodes traversed between the client and the server.

- The first fact is that RTT can exceed 200 ms
- The second fact is that the delay is highly variable. On occasion a delay going through the same number of nodes is 100 ms and another occasion it may be 200 ms.
- Lastly, the geographical distance (miles) have been placed on the graph. The distance represents the miles between the sender and receiver of the tested trace. It is clear that geographical distance cannot be correlated to RTT. Therefore, hop count is an important factor in delay and geographical distance is less of a factor as shown below in Figure 4.6.

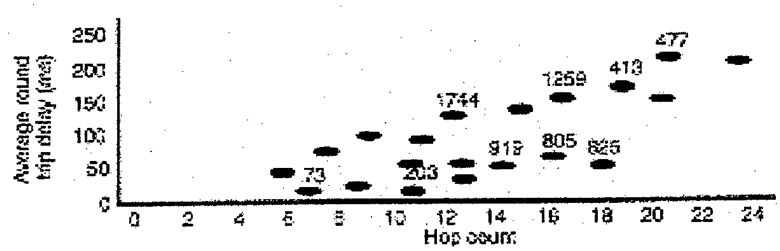

Figure 4.6 Round Trip Delay vs Hop Count (Geographical Distance) [KOST98]

E. SUMMARY

Is Internet technologically feasible? Yes, but the Cox study demonstrates that VoIP over the public Internet is marginal now. Nevertheless, the attractive features of Internet telephone, such as one link to the home, integration of voice and data, and lower costs will continue to push the technology further.

The deployment of high-speed access technologies at the local loop will further push Internet telephony. Once end users have access to high-speed local loop devices the equations changes.

First, overhead (headers and trailers) is not as significant a factor, since the increased bandwidth can support this overhead. Second, new PCs will be upgraded to support faster voice coders to take advantage of the higher-speed local loop. Third, the increase pipes into and out of the Internet will force an upgrading of the Internet's capacity. Fourth, the increase of voice traffic will also force the Internet to look more and more like a telephone network, but with significantly enhanced multi-application capabilities.

(THIS PAGE INTENTIONALLY LEFT BLANK)

V. DESCRIPTION OF EXPERIMENT

This chapter describes in detail the experiments that were conducted for Internet Telephony. Two PCs were used for H.323 terminals and were utilized in various network configurations. Commercial off the shelf software and hardware VoIP applications were used and tested. Telephone calls were placed on both the Internet and Intranet networks. In addition, a H.323 Gateway was utilized to place Internet Telephone calls over the Public Switched Telephone Network (PSTN). Both PC to PC and PC to PSTN telephone calls were tested.

A. HARDWARE AND OPERATING SYSTEMS

1. Equipment Used in Experiment

Two standard PCs were used:

PC One was an Intel Pentium 300 MHz CPU with 32 MB of RAM. It utilized Microsoft Windows 98 operating system. Loaded on the computer was Microsoft NetMeeting version 2.1 and Netscape Navigator version 4.0. For the voice interface, a standard sound card with speakers and a microphone were used.

PC Two was an Intel Pentium 400 MHz CPU with 64 MB of RAM. PC Two had a removable Hard Disk Drive (HDD) bay. This enabled two completely separate "C" drives. The two "C" drives were configured as follows:

Alpha: It utilized Microsoft Windows NT 4.0 operating system with option pack 4.0, service pack 3.0, Microsoft Internet Information server 3.1, Internet Locator Server 2.0 installed. NT server also had the Domain Name Service (DNS) and Window Internet Name Service (WINS) running. This configuration provided for the H.323 Gatekeeper functionality for testing of various Internet Telephone applications.

Bravo: It utilized Microsoft Windows 98 operating system. Loaded on the computer was Microsoft NetMeeting version 2.1 and Netscape Navigator version 4.0.

Network interfaces:

Both computers had Baynetworks 10/100MB-network interface cards (NIC) installed and were connected through a SVEC fast Ethernet hub (100 MB). This LAN was used for local and controlled testing.

Both computers also had 56k v.90 modems for access to the Internet via Internet Service Providers (ISP). The Internet was used for testing of various configurations and introduced real world latency and errors.

Sound Interface Cards:

PC One always had a standard sound card with speakers and a microphone for voice communications.

PC Two had two configurations:

First configuration is with a standard sound card, speakers and a microphone.

The second was with the *QuickNet LineJack Interface Card.* The LineJack card is a full duplex audio card designed to convert the analog human voice to the final digitized and packetized data for transport over an IP network. It has an onboard Digital Signal Processors (DSP) and Codecs, which eliminates the computer's CPU from having to be utilized for voice coding and decoding. It also has built in echo cancellation which eliminates the "echo effect" associated with the standard sound card, speaker and microphone setup. The freeing up of the general purpose computer's CPU coupled with the echo cancellation allows a PC based telephone to approach the clarity of a standard telephone line, see Figure 5.1 below. Another feature of the LineJack is that it allows for a standard telephone (RJ-11 type) to be plugged directly into the interface card. This allows the use of a standard telephone set for the speaker and microphone. It also allows the standard telephone keypad to be used when dialing a telephone number or IP address. The LineJack can also be used as a H.323 Gateway, in which a single line can be converted from the IP data network to the PSTN and vice versa. The H.323 Gateway was utilized in the third experiment.

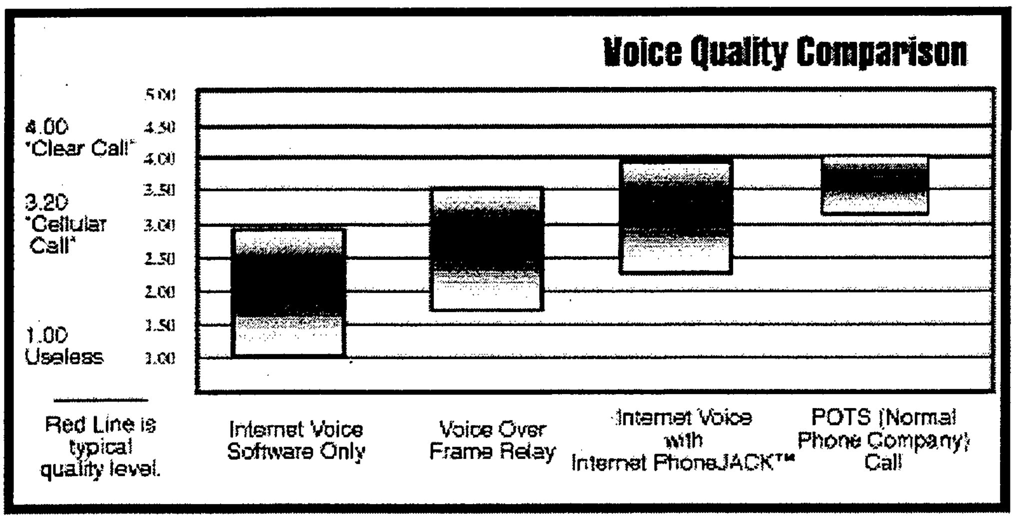

Figure 5.1 Voice Quality Comparison Chart [LIN99]

B. TESTED CONFIGURATIONS

1. Software to Software (PC to PC VoIP)

The first configuration was a PC to PC connection via the LAN or Internet and tested a software Internet Telephone application, as shown below in Figure 5.2. The application tested was Microsoft NetMeeting version 2.1. Both PCs acted as H.323 terminals. *PC One* was configured with a sound card, speakers and a microphone. *PC Two* acted as the H.323 Gatekeeper; it was configured with the Alpha HDD and a standard sound card with speakers and a microphone.

The test procedure was as follows:

- Both PCs log onto ILS, H.323 Gatekeeper (Figure 3.3).
- Either PC can initiate a call via point and click on a member of the directory (Figure 3.2 or Figure 3.3).
- Called PC answers incoming call via mouse click.
- Call is setup and continues.
- Either H.323 terminal can close call.

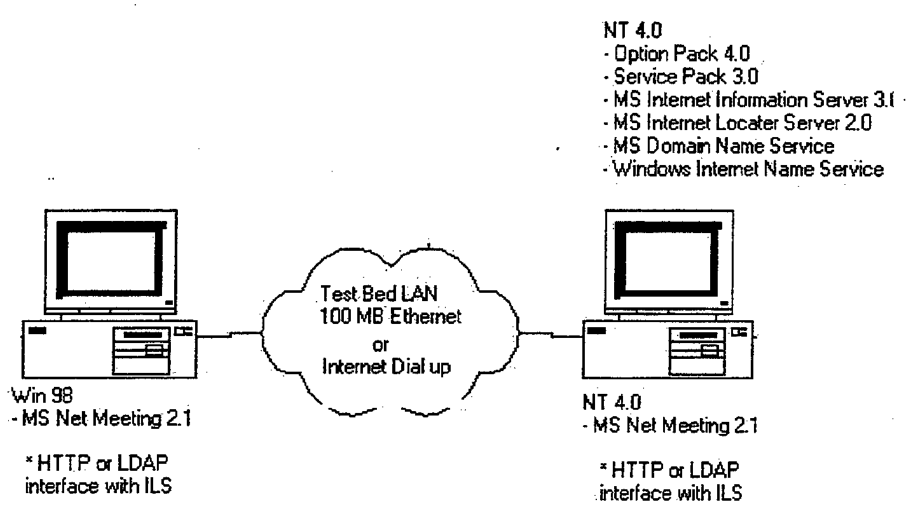

Figure 5.2 ILS Software to Software (Alpha)

2. **Software to Hardware (PC to PC VOIP)**

The second configuration was a PC to PC connection via the LAN or Internet. It tested a software Internet telephone application to a hardware processed application, as shown below in Figure 5.3. The application tested was Microsoft NetMeeting version 2.1. Both PCs acted as H.323 terminals. There was no H.323 Gatekeeper in this test. Instead both terminal's IP addresses were fixed and known. *PC One* was configured with a sound card, speakers and a microphone. *PC Two* was configured with the QuickNet LineJack interface card with a standard telephone. It was running the Internet Switchboard version 3.1 program that is required for the LineJack interface card.

The test procedure was as follows:

- Either PC can initiate a call by entering the IP address of the PC to be called. *PC One* enters the IP address via keyboard. *PC Two* enters the IP address via telephone keypad.
- *PC Two* can answer incoming call by lifting receiver in normal telephone fashion.
- Call is setup and continued.
- Either H.323 terminal can close call.

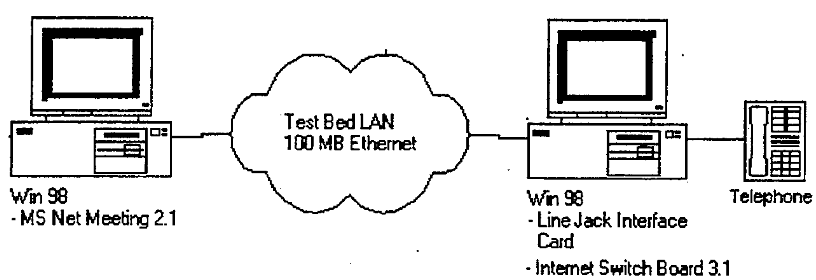

Figure 5.3 Software to LineJack Hardware (Bravo)

3. Software to Local H.323 Gateway (PC to PSTN)

The third configuration was a PC to PSTN connection via the LAN. It tested an Internet telephone software application to a local H.323 Gateway, as shown below in Figure 5.4. The application tested was Microsoft NetMeeting version 2.1. Both PCs acted as H.323 terminals. There was no H.323 Gatekeeper in this test. Instead both terminal's IP addresses were fixed and known. *PC One* was configured with a sound card, speakers and a microphone. *PC Two* was configured with the QuickNet LineJack interface card with a standard telephone. There was also a PSTN line connected to the LineJack. This was to be used for the H.323 Gateway to the PSTN. It was running the Internet Switchboard version 3.1 program that is required for the LineJack interface card.

The test procedure was as follows:

- *PC Two* was setup to be the H.323 Gateway.
- *PC One* initiated a call by entering the IP address of the H.323 Gateway and the PSTN telephone number to be called.
- *PC Two* answers the initial call from *PC One*. *PC Two* then automatically dials the PSTN telephone number on the PSTN line connected to the LineJack.
- The PSTN connection is made and *PC One* is then talking over the PSTN line via the IP network.
- Either the H.323 terminal or Gateway can close the call.

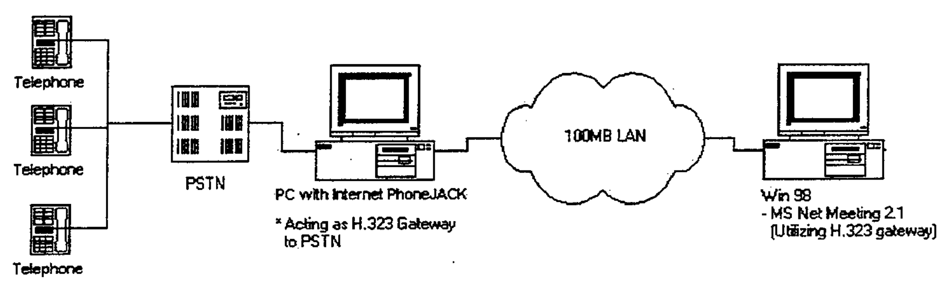

Figure 5 4 Software to a local H.323 Gateway (Bravo/PSTN)

4. Hardware to Remote H.323 Gateway (PC to PSTN)

The last configuration was a PC to PSTN connection via the Internet. It tested an Internet telephone software application to a remote H.323 Gateway, as shown below in Figure 5.5. The application tested was the Net-to-Phone application. A Net-to-Phone account was setup and utilized for testing. The Net-to-Phone server was the remote H.323 Gateway and Gatekeeper in this test. That is, the Net-to-Phone Gatekeeper was responsible for call setup and establishment. In addition, the Net-to-Phone Gateway was utilized to transition from the IP data network to the PSTN in the local calling area. The Net–to-Phone network has Gateways throughout the US. The test calls' data packages traveled on the Internet until they would hop off onto the PSTN. There they would be placed as local calls.

PC Two acted as a H.323 terminal and was connected to the Internet via a 56K v.90 modem. *PC Two* was configured with the QuickNet LineJack interface card with a standard telephone. It was running the Net-to-Phone application and the Internet Switchboard version 3.1 program that is required for the LineJack interface card.

The test procedure was as follows:

- *PC Two* was an H.323 terminal with the Net-to-Phone application and account information.
- *PC Two* initiated a call by entering the PSTN telephone number to be called.
- *PC Two* automatically launches the Net-to-Phone application and connects to the Net-to-Phone server.
- The Net-to-Phone Gatekeeper determines which local Gateway to establish the call through and proceeds with the setup.
- The PSTN connection is made and *PC Two* is then talking over the PSTN line via the IP network.
- Either the H.323 terminal or Gateway can close the call.

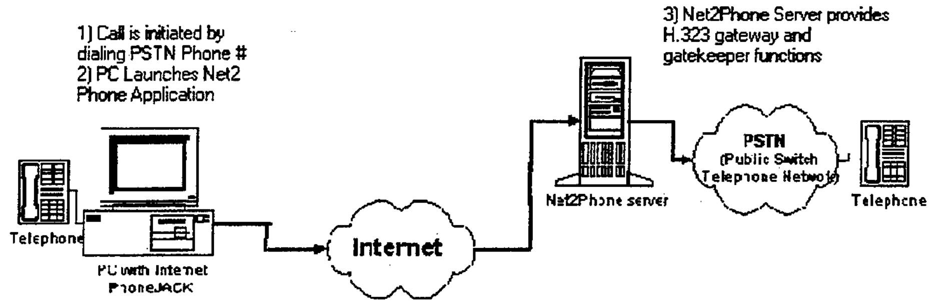

Figure 5.5 Hardware to a remote H.323 Gateway (PC to Telephone VOIP)

C. OBSERVATIONS ON TESTING

Testing of the above four configurations was completed. The ability of a H.323 terminal to conduct Internet Telephony met with varying degrees of success. Having no way to empirically measure the various aspects of voice quality, I subjectively determined the quality of the current off the shelf technology.

The crux of this thesis was not a comparison of software or hardware packages, but the implementation of the H.323 components required to provide Internet Telephony services.

The H.323 Gatekeeper services were provided by the software packages ICQ and ILS. A detailed description of the ILS and ICQ servers was provided in Chapter III.

The H.323 Internet Telephony software packages utilized were Microsoft NetMeeting and the Net-to-Phone application. These software applications enabled a standard PC to become a complaint H.323 terminal. Both software packages were able to provide PC to PC and PC to PSTN communications.

The QuickNet LineJack interface card worked as advertised. It enabled Internet telephone calls utilizing a standard telephone vice a sound card, speakers and a microphone. Its dedicated hardware for voice digitizing and packetizing relieved the general purpose CPU from those tasks and provided for clearer voice communications. It also provided for a one line H.323 Gateway to the PSTN for traditional telephone calls. Tests were conducted successfully with both a local and remote H.323 Gateway.

VI. CONCLUSIONS AND FUTURE WORK

A. SUMMARY

This thesis does not attempt to provide an all-inclusive list of commercial Internet Telephony applications. This research study however intends to serve as an overview of a workstation solution to Internet telephony. It worked from the industry standard H.323 model and implement various workstation solutions to Internet Telephony. It also addresses issues surrounding using the Internet as part or the entire IP network. Details and conclusions were provided in Chapter IV.

A workstation solution for IP Telephony must address issues such as dedicated hardware, software applications and existing network infrastructure. The H.323 model issues were addressed in Chapters II and III. Implementation of the software and hardware to support the H.323 model was detailed in Chapter V.

The main advantage of a workstation solution is that it provides the greatest flexibility of all the Internet Telephony solutions. Both the Carrier and Enterprise class solutions rely on legacy fits to existing circuit switched networks. Only the workstation solution provides for all voice traffic to originate and terminate on a data network. This may seem simplistic; however, assuming a completely data oriented network then expansion and scalability issues are trivial. If you bring the IP packets to the workstation and the workstation can determine if it is voice or video or data then you truly have data convergence.

Sound quality is the number one determining factor for continued use of any voice system. Internet telephony is no exception. Currently Internet telephony quality varies depending mostly on network bandwidth. Private networks continue to outperform public networks. Continued speed enhancements in the local loop will narrow the gap between the two network types.

The Internet and much of the technology around the backbone were not designed around real-time requirements. A large part of the Internet's appeal is that it is a group effort. Even the smallest carrier can source traffic for delivery anywhere in the world through another carrier's network. No one is surprised that its current performance characteristics are not quite always suitable for real-time applications.

The Internet continues to hold great promise not only in reducing costs of global communications, but also in enabling the types of applications, which requires many loosely affiliated nodes to communicate with voice and data.

In general, the public will rely on the Internet for voice traffic only when it proves to be reliable. Internet Telephony is maturing and will become more reliable later. My own opinion is based loosely on Moore's Law, "computer processing power doubles every eighteen months". If we consider Internet telephony half way to being usable then we have approximately eighteen months to go.

B. CURRENT INDUSTRY TECHNOLOGY

During the author's research, he was able to attend the Internet Telephony exposition in San Diego, CA in the fall of 1999. The trip was invaluable and worth mentioning the current industry highlights in the final chapter of this thesis.

Most of the current industry implementations of Internet Telephony rely heavily on legacy connections to the existing local PSTN. Many of the Internet Telephony Carrier Class companies are focused on building a large data network backbone. The large backbone is US nationwide and spreading to overseas and foreign territories. The backbone is interfaced with the local PSTN via large capacity H.323 Gateways at the local Telephone Company switching offices. The end user still uses the local PSTN to dial into the Gateway where the voice is packetized and sent over the data network to the local Gateway of the termination area.

This implementation may be adopted during the transition between VoIP and traditional telephone system. However, it should be viewed as a temporary fix and possibly a burden in the future, a burden because instead of building a total data network, it is a hybrid of packet and circuit switch. The hybrid network does not fully utilize the flexibility of a data network and it does not address the large bottleneck of the local loop. It also requires the end user to maintain two networks, a telephone and a data, and therefore does not support the idea of data convergence.

A data network that delivers the IP packets to the end user provides for the most flexible and most robust network. The end user terminal must be able to handle every type of packet: voice, data and video. If the network has the infrastructure to handle data and voice initially, then the addition of video would be relatively easy and true data convergence can be achieved.

There were only a few companies that designed their networks around the workstation solution to Internet Telephony. They had a true data network backbone and their model delivered all the IP packets to the end user terminal. The terminal was able to handle the each type of packet, data or voice accordingly. This model provided for a very robust network that was easily scalable. Each node attached to the network could function independently and could provide any service such as data, voice, beeper, fax or interface with a wireless network.

The author feels that this later implementation will be the winner in the future for the following reasons:

- Local access points can be made through any type of data connection.
- If high-speed access technologies are available such as DSL or cable modem then they may be used.
- It addresses the proliferation of IP devices and allows for the expansion of new IP devices.
- It is also the most scalable network design and allows for true data convergence.

C. FUTURE WORK

Future work for the workstation solution for Internet Telephony should address increasing speed at the local loop, refined hardware processing and data convergence.

For the near term, the local loop will continue to be the largest bottleneck of the Internet. Advances in technologies that allow for faster data rates will allow the continued expansion and use of Internet Telephony.

Dedicated hardware for voice digitizing and packetizing will continue to out perform generic software attempts of general-purpose computer systems. Advances in this field will provide for clearer voice reproduction.

Data convergence will continue to move forward at the workstation level. Voice, video and data will arrive via the network and the end box needs to be able to accommodate the various data types. Once this happens, a cultural change will further the use of Internet Telephony and communications.

LIST OF REFERENCES

[BLAK99] Uyless Black, *Voice Over IP*, Prentice Hall Series, Upper Saddle River New Jersey, 1999.

[COX98] Cox, R. V., Hassle, B.G., Lacuna, A., Shahraray, B., and Rabiner, L., "On the Applications of Multimedia Processing to Communications," *Proceedings of the IEEE*, vol. 86, No. 5 May 1998.

[CSCO99] Chris Lewis, *Cisco TCP/IP Routing Professional Reference*, Mc Graw Hill, New York 1999.

[GON98] Marcus Goncalves, *Voice Over IP Networks*, Mc Graw Hill, New York 1998.

[KOST98] Kostas, T. J., Borella, M.S. Sidhu, I. Shuster, G.M., Grabiec, J. and Mahler, J., "Real-Time Voice Over Packet Switched Networks", *IEEE Network*, January 1999.

[LIN99] Quick Net, *Line Jack Documentation*, Quicknet Technologies, San Francisco , California, 1999.

[MON98] D. Monoli and E. Monoli, *Delivering Voice over IP Networks,* Wiley Computer Publishing, Lancaster PA, 1998.

[OPG96] Microsoft, *Internet Locator Server Operations Guide, 1996.*

[PAXS97] Paxson, Vern. *IEEE/ACM Transactions on Communications*, "End-to-End Routing Behavior in the Internet." Vol. 5, No.5 October 1997.

[PHO99] Quick Net, *Phone Jack Documentation*, Quicknet Technologies, San Francisco , California, 1999.

[SHAP98] Jeffrey R. Shapiro, *Computer Telephony Strategies,* IDG Books, Foster City CA, October 1998.

[WAG96] Microsoft, *Internet Locator Server Web page Author's Guide, 1996.*

(THIS PAGE INTENTIONALLY LEFT BLANK)

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Road, Ste 0944
   Ft. Belvoir, Virginia 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, California 93943-5101

3. Chairman,Code CS 1
   Computer Science Department
   Naval Postgraduate School
   Monterey, California 93940-5000

4. Prof Bert Lundy 1
   Computer Science Department, Code CS/Ln
   Naval Postgraduate School
   Monterey, California 93943-5100

5. Prof Wolfgang Baer 1
   Computer Science Department, Code CS/Bn
   Naval Postgraduate School
   Monterey, California 93943-5100

6. LCDR Rick Perri 4
   EODMU TWELVE
   1050 Remount Rd. Bldg 3115
   North Charleston, SC 29406