MULTICAST VIDEOCONFERENCE TOOLS AND TECHNOLOGIES

A University Thesis Presented to the faculty

Of

California State University, Hayward

In Partial Fulfillment

Of the Requirements for the Degree

Of Master of Science in Telecommunications

By

Rick Kovacic

ACKNOWLEDGEMENTS

This Thesis research was begun in September, 2000 and continued through the publication of this document in June, 2001. The vast majority of network and telecommunications research was conducted at TELCOT Institute in San Ramon, California through the gracious support of Dr. Alex Bordetsky, Ph.D., Telecommunications Division, School of Business and Economics at California State University, Hayward. Without Dr. Bordetsky's on-going support and enthusiasm this project would have never taken form.

I would also like to thank those instructors, staff and administrators at CSUH who helped me achieve a program of study technically intensive and content pertinent during my studies. I would like to extend special thanks to those persons who shared my vision of participating in a degree program and research studies that would be recognized as credible in the Telecommunications industry.

I would like to personally thank the following persons for their contributions to my Thesis Project:

- Mr. Bruce Bagnoli, Facilities and Planning Office
- Mr. Charles Hintz, Instructional Media Center
- My wife, Lonny, for her continued support and belief in my abilities

Rick Kovacic
June, 2001

TABLE OF CONTENTS

MULTICAST VIDEOCONFERENCE TOOLS AND TECHNOLOGIES

APPROACH

This Thesis study was centered around the use of multicast tools, specifically video conference tools, in conjunction with various network technologies. Integration of software applications and features for enduser ease-of-use was a major consideration during test procedures. To achieve the stated goals, several general transmission approaches were planned and utilized during the study:

- Utilize dedicated connections to MBone routers to send & receive multicast traffic;
- Download and install proprietary videoconference software applications on local machines;
- Installed dedicated multicast hardware on the LAN to send and receive multicast traffic, or simulate such capabilities through web-based interfaces using the same technologies
- Utilize existing vendor web-based software solutions available.

A variety of test sessions were devised to explore the viability of each of these approaches. A standardized format was created for test sessions and a schedule implemented that would allow persons in different time zones to participate in sessions at their convenience. The session format would include:

- Capabilities to exchange text, real-time speech and video images
- Sessions scheduled at different times and days of the week

- Sessions would require no encryption or login procedure for the client
- Sessions would be advertised on the widest scale possible (globally).

Multiple platforms were also available to utilize in the tests at the TELCOT Institute facility. These included:

- SUN Ultra10 Unix workstations running Solaris operating system
- Dell PCs running Windows 98 and Windows 2000 OS;
- Dedicated Zydacron comStation PC running NT v4 OS.

These workstations were part of the extended Telcot LAN connected to a dedicated T1 phone line between a local ATM router and routers on the CSUH main campus. Throughputs of up to 1.544 mbps were anticipated on workstations at Telcot during tests. A graphic representation of the entire California State University network is provided below; CSU-Hayward is a LAN on this larger WAN or Intranet as shown on the following page.

The TELCOT LAN afforded a high-speed, dedicated T1 connection to the main network routers on the CSU-Hayward campus some 20 miles away and an ATM switch for routing of all packets across the line; one multicast router was available on the main campus LAN as well.
At a remote location were additional workstations to be utilized for testing, including a Macintosh PowerPC G3 running OS9.1 and a Win98 PC with aDSL high-speed network access; data transmission rates of 393kbps were consistently available on this system. Both workstations provided the opportunity to test the various solutions explored from a remote location with

different network characteristics. Initial tests were to be conducted using MBone tools, discussed below.

Test Preparation

Video conference sessions were created via MBone session tools from the "Phoenix" SUN Ultra10 machine at TELCOT; this machine is configured as the LAN multicast router to send and receive multicast traffic on the network (IP address = 134.154.162.41). Its configuration included three multicast 'tunnels' to dedicated multicast routers outside of the primarily Telcot LAN:

- one to a 2nd multicast router at Telcot (134.154.162.40),
- another to Dr. Kevin Brown's Linux router on the CSUH main campus (134.154.160.18),
- and a third to a multicast router at the Information Sciences Institute (http://www.isi.edu/) at the University of Southern California (128.9.160.194).

These tunnels would allow multicast packets originating from and received by the Phoenix machine at Telcot to be routed directly to other MBone multicast routers globally. The configuration file on this Sun Ultra10 (IP address of 134.154.162.41) is called "mrouted.conf" and is located at /usr/multicast; parameters in this file regulate the flow of multicast packets in and out of the machine at specific threshold rates to limit total network bandwidth consumed by the traffic. The specific parameters of this file are shown below:

```
#  This is the mrouted.conf setup for the TELCOT Instititues.
#  An example copy of the /etc/mrouted.conf can be found at
#  /etc/mrouted.conf.old.
#
#  Setup name boundary
#name LOCAL 239.0.0.0/16

#  Setup the phyint to reflect the primary interface
```

```
#phyint hme0 metric 1
#phyint hme0 boundary LOCAL

#  Setup a tunnel with Dr. Brown's system (wamcom) in CSUH network.
tunnel 134.154.162.41 134.154.160.18 metric 1 threshold 1 rate_limit
1000

#  Setup a tunnel with the other mbone router, 134.154.160.40
#tunnel 134.154.162.41 134.154.162.40 metric 1 rate_limit 900

#  Setup a tunnel with the outside world.
tunnel 134.154.162.41 128.9.160.194 metric 1 threshold 1 rate_limit 900
```

The tunnel IP addresses for the originating and endpoint routers are both specified, along with metric, threshold, and data rate limits in this file. The ‘rate_limit‘ figure of 900kbps shown above was reduced to 500kbps later in the tests to reduce network load.

All other personal computers and workstations on the LAN could (theoretically) send and receive multicast packets through this machine. Video conference hardware and MBone software were installed on Windows98, Windows2000, and Win NT4.0 PCs at the facility to for this purpose. Additionally, a second Sun Ultra10 was configured to participate in video conference tests (but never utilized due to time constraints). At the ‘home office’, the Win98 PC was configured with MBone session tools to send and receive multicast traffic; research into MBone tools for the Macintosh PowerPC showed few tools being available for this platform.

Test Procedures: MBone

MBone sessions were originated from the Phoenix machine at Telcot using the SDR session tool. Sessions were ‘advertised’ each Wednesday afternoon from 1500-1800 hours PST, with the following parameters:

- Sessions were setup as Meetings
- No encryption was established
- Sessions included audio, video and text exchange features
- Sessions were advertised globally

Session times scheduled were varied throughout the course of the test to accommodate users with different work schedules, researchers located in other time zones and parts of the world, and users at the Telcot facility. Multiple sessions were held on Tuesdays and Thursday mornings and afternoons, as well as during specific weekend hours on occasion.

To establish an MBone session, commands are accessed in the various menus of SDR. Menus and features are described below:

New menu

- Create advertised session – allows a user to designate the name, time and duration, scope, encryption method, and tools for sessions originating from a users machine
- Quick Call – allows parameters to be established to establish a point-to-point multicast session to a specific IP address

Calendar

- Shows monthly listings of advertised MBone sessions seen by the workstation receiving multicast traffic via SDR

Prefs

- Sessions – options for displaying session
- Interface – styles for creating sessions, viewing, session listings and label details
- Tools – shows the media formats and the MBone applications associated with each
- Web – parameters for accessing Internet resources while using SDR
- You – specific information about the user as name, email address, and phone number; additionally, a nickname and web URL can be designated to expedite MBone sessions between users
- People – acts as an Address Book for listing names and IP addresses of frequently called MBone users

- Security – parameters to encryption used in sessions; PGP (Pretty Good Privacy) is the built-in security feature used by SDR.

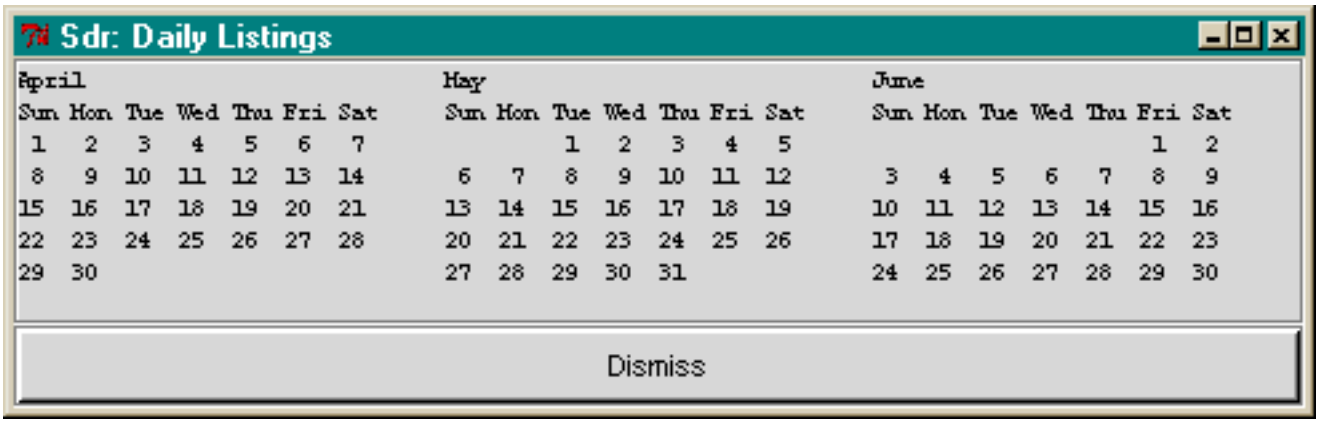
Help

- Sdr Help – a built in help guide reference for users of SDR
- Key setup – information on encryption parameters for PGP

Quit

- A method of ending sessions and exiting the SDR software.

When sessions were scheduled or 'advertised', a listing of upcoming sessions is shown in the calendar menu; days which sessions are scheduled are highlighted and information on these sessions can be obtained by choosing the appropriate day. The Calendar window is shown below:



To join a session, a user chooses a session listing in the main SDR window or in the Calendar, and is provided with a number of choices, including the tools to use, a method of inviting other parties, and particulars of the SDR session. For a more in-depth discussion of how to use the SDR session tool, download and real the SDR User Guide located at the University of London Networked Multimedia Research Group web site (http://www-mice.cs.ucl.ac.uk/multimedia/software/ - user_guides).

Instructions for use of other MBone session tools as nSDR are available at the Open Mash User Groups web site (http://www.openmash.org/users/index.html).

MBone Test Details

Numerous tests were conducted weekly over a 6 month period from September, 2000 through March, 2001. Impressions of these tests and excerpts from various test procedures follow.

Initially, there were no apparent problems in establishing MBone sessions from the Phoenix multicast router machine. The configuration of the local multicast router was in question, however, as settings in the "mrouted.conf" file had been altered by students in previous research projects. Once verified, as discussed previously, sessions were schedule on a weekly basis.

Complications on other machines on the Telcot LAN recognizing and joining advertised sessions were immediately apparent. Some of the machines would recognize the MBone sessions, access their contents, and show other participants; audio and video packets could be sent to other participants on these machines. Software used by these machines during tests included MBone tools as SDR, VIC, VAT and NTE; operating systems used by participating machines was Windows 98.

Other machines on the Telcot LAN would see MBone sessions in SDR but could not join them. This included the Zydacron comStation running OS NT4.0; although sessions were readily recognized the video drivers and hardware incorporated into this machine were unable to

interface with the MBone session tools; thus sessions could be watched but no participation possible due to the lack of video transmitting capabilities to the machine. Curiously, audio reception was also a problem on this machine, despite manufacturer OEM audio boards featuring multiple inputs and outputs being installed on the machine.

Further complications were displayed by two PCs on the Telcot LAN which could not recognize or participate in MBone sessions advertised locally. These two PCs were located physically in the same room but used different IP addresses on the network; they were both connected to the same ATM switch as other machines on the LAN. Additionally, each used a different operating system: one was running Windows98 and the other Windows2000 Server edition. Both machines displayed the same characteristics when launching MBone tools:

- The SDR session tool would launch correctly
- No SDR sessions would be listed in the main session window
- When advertising sessions from these machines, no other workstation would recognize sessions announced. [This was later determined to be an inappropriate action, as no session could be announced from any other machine except the multicast router Sun ("Phoenix").]

The only sessions recognized by the workstations at Telcot included those advertised locally from the Phoenix machine, weather Broadcasts supplied by NASA, and specialized one-time announcements from government entities and other parties. These second (NASA) sessions were advertised daily and consisted of television broadcast of the Weather channel digitized and delivered over MBone in real-time. Video frame rates were in the 6-10 fps range; images were

recognizable but full motion video not achieved. Audio was broken and patchy at best; it was not possible to listen to the broadcast and recognize what information was being transmitted.

Traffic Monitoring

During tests multicast traffic could be monitored through the multicast router from remote stations. Remote stations were chosen for this purpose as a) the procedure would allow monitoring from any location with network access, and b) monitoring was desired from a general, publicly-available platform (e.g. Windows OS) other than the specific machine configured as the LAN mrouter. The general procedure for doing this consisted of:

- establishing a remote connection to the router via Telnet;
- logging onto the multicast router as "root";
- using a Unix command tool to locate, filter and list multicast packets traveling through the router.

Snoop

One of the tools used for monitoring traffic is "Snoop". Snoop is a command-line tool that allows multicast traffic to be recognized, filtered and listed with various attributes. Below is a list of Snoop commands and attributes:

```
Usage:  snoop
      [ -a ]              # Listen to packets on audio
      [ -d device ]         # settable to le?, ie?, bf?, tr?
      [ -s snaplen ]        # Truncate packets
      [ -c count ]        # Quit after count packets
      [ -P ]              # Turn OFF promiscuous mode
      [ -D ]              # Report dropped packets
      [ -S ]              # Report packet size
      [ -i file ]         # Read previously captured packets
      [ -o file ]         # Capture packets in file
      [ -n file ]         # Load addr-to-name table from file
```

```
        [ -N ]              # Create addr-to-name table
        [ -t  r|a|d ]       # Time: Relative, Absolute or Delta
        [ -v ]              # Verbose packet display
        [ -V ]              # Show all summary lines
        [ -p first[,last] ]    # Select packet(s) to display
        [ -x offset[,length] ]  # Hex dump from offset for length
        [ -C ]              # Print packet filter code

        [ filter expression ]
```

Example:

```
        snoop -o saved  host fred

        snoop -i saved -tr -v -p19
```

Using this tool traffic rates could be monitored, source and destination IP addresses discovered, and quality of transmission shown (in the way of amounts of packets lost). This tool was used on numerous occasions to detect traffic during sessions and monitor the amount of load placed on the local network when using MBone tools. Below is a snoop session performed during one of the weekly MBone session multicasts:

```
login: rick
Password:
Last login: Wed Feb 21 18:52:49 from 134.154.162.100
Sun Microsystems Inc.   SunOS 5.7       Generic October 1998
$ su root
Password:
# snoop -c20 -V multicast
Using device /dev/hme (promiscuous mode)
_____________________________________
     phoenix -> 224.2.235.50 ETHER Type=0800 (IP), size = 168 bytes
     phoenix -> 224.2.235.50 IP  D=224.2.235.50 S=134.154.162.41 LEN=154,
ID=29578
     phoenix -> 224.2.235.50 UDP D=57160 S=48424 LEN=134
_____________________________________
198.10.49.50 -> 239.198.10.49 ETHER Type=0800 (IP), size = 898 bytes
198.10.49.50 -> 239.198.10.49 IP  D=239.198.10.49 S=198.10.49.50 LEN=884,
ID=18548
198.10.49.50 -> 239.198.10.49 UDP D=22222 S=1035 LEN=864
_____________________________________
198.10.49.50 -> 239.198.10.49 ETHER Type=0800 (IP), size = 282 bytes
198.10.49.50 -> 239.198.10.49 IP  D=239.198.10.49 S=198.10.49.50 LEN=268,
ID=18577
198.10.49.50 -> 239.198.10.49 UDP D=22222 S=1035 LEN=248
_____________________________________
          ? -> (multicast)  ETHER Type=0000 (LLC/802.3), size = 52 bytes
_____________________________________
     phoenix -> 224.2.235.50 ETHER Type=0800 (IP), size = 165 bytes
```

```
     phoenix -> 224.2.235.50 IP  D=224.2.235.50 S=134.154.162.41 LEN=151,
ID=29579
     phoenix -> 224.2.235.50 UDP D=57160 S=48424 LEN=131
_____________________________________
198.10.49.50 -> 239.198.10.49 ETHER Type=0800 (IP), size = 890 bytes
198.10.49.50 -> 239.198.10.49 IP  D=239.198.10.49 S=198.10.49.50 LEN=876,
ID=18582
198.10.49.50 -> 239.198.10.49 UDP D=22222 S=1035 LEN=856
_____________________________________
140.173.165.126 -> 239.198.10.49 ETHER Type=0800 (IP), size = 130 bytes
140.173.165.126 -> 239.198.10.49 IP  D=239.198.10.49 S=140.173.165.126
LEN=116, ID=41185
140.173.165.126 -> 239.198.10.49 UDP D=22223 S=1362 LEN=96
_____________________________________
           ? -> (multicast)  ETHER Type=0000 (LLC/802.3), size = 52 bytes
_____________________________________
           ? -> (multicast)  ETHER Type=0000 (LLC/802.3), size = 52 bytes
_____________________________________
198.10.49.50 -> 239.198.10.49 ETHER Type=0800 (IP), size = 252 bytes
198.10.49.50 -> 239.198.10.49 IP  D=239.198.10.49 S=198.10.49.50 LEN=238,
ID=18618
198.10.49.50 -> 239.198.10.49 UDP D=22222 S=1035 LEN=218
_____________________________________
sportster.east.isi.edu -> 239.140.173.5 ETHER Type=0800 (IP), size = 102
bytes
sportster.east.isi.edu -> 239.140.173.5 IP  D=239.140.173.5 S=38.245.76.176
LEN=88, ID=31615
sportster.east.isi.edu -> 239.140.173.5 UDP D=55555 S=1044 LEN=68
_____________________________________
     phoenix -> 224.2.235.50 ETHER Type=0800 (IP), size = 156 bytes
     phoenix -> 224.2.235.50 IP  D=224.2.235.50 S=134.154.162.41 LEN=142,
ID=29580
     phoenix -> 224.2.235.50 UDP D=57160 S=48424 LEN=122
_____________________________________
           ? -> (multicast)  ETHER Type=0000 (LLC/802.3), size = 52 bytes
_____________________________________
198.10.49.50 -> 239.198.10.49 ETHER Type=0800 (IP), size = 987 bytes
198.10.49.50 -> 239.198.10.49 IP  D=239.198.10.49 S=198.10.49.50 LEN=973,
ID=18638
198.10.49.50 -> 239.198.10.49 UDP D=22222 S=1035 LEN=953
_____________________________________
     phoenix -> 224.2.240.162 ETHER Type=0800 (IP), size = 102 bytes
     phoenix -> 224.2.240.162 IP  D=224.2.240.162 S=134.154.162.41 LEN=88,
ID=15224
     phoenix -> 224.2.240.162 UDP D=19711 S=48422 LEN=68
_____________________________________
     phoenix -> 224.2.235.50 ETHER Type=0800 (IP), size = 146 bytes
     phoenix -> 224.2.235.50 IP  D=224.2.235.50 S=134.154.162.41 LEN=132,
ID=29581
     phoenix -> 224.2.235.50 UDP D=57160 S=48424 LEN=112
_____________________________________
198.10.49.50 -> 239.198.10.49 ETHER Type=0800 (IP), size = 1031 bytes
198.10.49.50 -> 239.198.10.49 IP  D=239.198.10.49 S=198.10.49.50 LEN=1017,
ID=18665
198.10.49.50 -> 239.198.10.49 UDP D=22222 S=1035 LEN=997
_____________________________________
198.10.49.50 -> 239.198.10.49 ETHER Type=0800 (IP), size = 934 bytes
198.10.49.50 -> 239.198.10.49 IP  D=239.198.10.49 S=198.10.49.50 LEN=920,
ID=18704
198.10.49.50 -> 239.198.10.49 UDP D=22222 S=1035 LEN=900
_____________________________________
```

```
     phoenix -> 224.2.235.50 ETHER Type=0800 (IP), size = 466 bytes
     phoenix -> 224.2.235.50 IP  D=224.2.235.50 S=134.154.162.41 LEN=452,
ID=29582
     phoenix -> 224.2.235.50 UDP D=57160 S=48424 LEN=432
_____________________________________
198.10.49.50 -> 239.198.10.49 ETHER Type=0800 (IP), size = 550 bytes
198.10.49.50 -> 239.198.10.49 IP  D=239.198.10.49 S=198.10.49.50 LEN=536,
ID=18735
198.10.49.50 -> 239.198.10.49 UDP D=22222 S=1035 LEN=516
snoop: 20 packets captured
#
```

In this example, a connection was established to the Sun Phoenix machine and the user became 'root'. Then a command of "snoop -c20 -V multicast" was input to the multicast router; this command stipulated:

- a snoop command was to be performed on the multicast router;
- a specific number of multicast packets was to be monitored (in this case '20');
- all summary information on each packet was to be shown ('-V');
- a filter for multicast traffic was applied ('multicast'), allowing the user to monitor only the multicast packets traveling over the network.

Complete details on snoop tests can be found in Appendix D: Multicast Network Statistics.

Netstat

Another monitoring technique involved using a 'netstat' command line input for gathering and displaying network traffic during multicast sessions. Netstat allows a user to monitor the overall network traffic based on the type and amount of traffic, the current network and maximum network loads, the cumulative total packets during the monitor time, and allocation failures. Below is a sample of a netstat monitoring session for multicast only traffic on the Telcot multicast router:

```
# netstat -m
streams allocation:
                                                cumulative  allocation
                        current   maximum          total    failures
streams                     318       336         152367           0
queues                      857       884         456100           0
mblk                        606      4445         281374           0
dblk                        588      4920      186376214           0
linkblk                       8       169             66           0
strevent                      8       169        1038558           0
syncq                        17        67            272           0
qband                         0         0              0           0

971 Kbytes allocated for streams data
#
```

In this test, the 'netstat' command included a filter attribute for multicast traffic only ('-m'). Additional attributes may be applied to the netstat command during monitoring sessions to gain information on overall network traffic, portions of traffic, or traffic during specific time periods. For more information on using netstat, consult the Hacking Truths web site at http://hackingtruths.box.sk/netstat.htm. Complete details on netstat tests can be found in Appendix D: Multicast Network Statistics.

Route Trace

An additional monitoring activity found useful was to trace the route of multicast traffic during sessions from a non-participating workstation using the NeoTrace software package. NeoTrace allows a user to input a destination IP address or DNS name and then locate the routers, switches and bridges traffic encounters between the source (client) and destination machines. This information is useful in analyzing multicast traffic when tunneling to a router outside of the local

area network, in determining network delay due to hop count, and the location and distance of multicast routers being used during an MBone session.

To perform a trace, a user:

- downloads and installs a tracing software program as NeoTrace;
- launches the NeoTrace software application;
- inputs a DNS or IP address into the location box;
- chooses a Ping command to trace the route from the source machine.

When pinging, a representation of the path or route of the trace packets is shown, either in graphic or text form. Information about each hop on the route is available in a secondary application window, and textual information can be saved during a session. Below is a summary of information from a NeoTrace session done during an MBone session:

```
NeoTrace  Version 3.01 - TRIAL (December 20 2000) Trace Results
Target: 239.198.10.49
Date: Thu Feb 15 20:43:17 2001
Nodes: 2


Node Data
Node Net Who IP Address      Location            Node Name
   1   -   - 134.154.162.100 37.755N, 121.953W   Dell210
   2   1   - 239.198.10.49   Unknown


Packet Data
Node High Low  Avg  Tot  Lost
   1    0    0    0    1    0
   2    1    0    0   11    0


Network Data
Network id#: 1
University of Southern California (NET-MCAST-NET)
   Information Sciences Institute

   4676 Admiralty Way

   Marina Del Rey, CA 90292-6695
```

```
Whois Data
_____
NeoTrace Copyright ©1997-2000 NeoWorx Inc
3a8cafe5
98 94
```

There is no direct correlation or relationship between the MBone session and the NeoTrace function being performed, other than establishing a path that multicast packets may take between the local mrouter machine and a multicast router outside the LAN.

Complete details on trace routing tests can be found in Appendix D: Multicast Network Statistics. For more information on obtaining and using NeoTrace, visit the NeoWorx web site at http://www.neoworx.com/products/neotrace .

Ping

Finally, command line 'ping' tests were conducted during MBone sessions to determine the state of remote clients and routers which were attempted to be involved in MBone sessions, test cameras and connections, and the like. The ping command tools allows a user to send a signaling packet across the network connection to a predetermined IP or DNS address to verify the DTEs and actual route of traffic from a distance source. In these tests, ping commands were used specifically to determine the location of multicast routers and the source of multicast traffic from other parties participating in MBone sessions. An example of the results of a ping command session is shown below:

```
PolyCom Station IP addressbook: test
Microsoft(R) Windows 98
   (C)Copyright Microsoft Corp 1981-1998.
C:\WINDOWS>ping 216.81.250.253
Pinging 216.81.250.253 with 32 bytes of data:
Request timed out.
Request timed out.
```

```
Request timed out.
Request timed out.

Ping statistics for 216.81.250.253:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\WINDOWS>ping 216.54.150.16
Pinging 216.54.150.16 with 32 bytes of data
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 216.54.150.16:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

Complete details on PING tests can be found in Appendix D: Multicast Network Statistics.

Other Monitoring Tools

Additional tests were conducted using ‘mping’ and ‘mtrace’ commands in a DOS window, with no satisfactory results to report. These tests were not continued during test sessions. To learn more about these two monitoring commands, see the Multimedia Project research at Microsoft Research web site (http://research.microsoft.com/barc/mbone/mping.htm) and the Mtrace information at Lawrence Berkeley Labs web site (http://www-itg.lbl.gov/mbone/mtrace.tips.html) .

Other monitoring tools as "map MBone" are available for Sun Solaris and other Unix operating systems, but were not used for monitoring in this test. For more information on these tools visit the USC ISI MBone web site at http://www.isi.edu/scan/mbone.html .

MBone Test Conclusions

The large number of variables in sending, receiving and monitoring multicast traffic during MBone sessions tools lead this researcher to a variety of conclusions and suggestions concerning the use of the technology. These conclusions and suggestions are outlined below:

- multicast traffic is highly unpredictable and thus unreliable for daily business and communication applications;
- reliability can be established by using dedicated multicast hardware and software on a LAN;
- propriety MBone tools available from software and hardware manufacturers limit the average user to 'free' technology that is rapidly becoming outdated and underdeveloped;
- there is limited support for users on 'alternative' platforms to utilize MBone multicasting;
- alternatives exist which allow multipoint videoconference sessions and related tools to be conducted without the large investment required for dedicated hardware.

Multicast Traffic: Unreliable

When establishing multicast sessions using SDR or nSDR, it was virtually impossible to detect whether the multicast traffic being generated was actually traveling outside of the LAN's multicast router. Parties outside of the Telcot LAN that were invited to participate in sessions were (apparently) not able to see the sessions or join in a session; in one particular case a person invited located at the CSUH main campus was unable to participate in or see sessions using the same MBone tools as the source machine. After discussion, we concluded that there was likely multicast traffic filtering algorithms placed on the main CSUH network routers, and without

tunneling directly to a multicast router, there was no way MBone sessions could be utilized. This general principle applies to virtually all network workstations that are attempting to utilize public MBone tools on networks without dedicated multicast routers: there is little or no guarantee that multicast traffic will be accessible because of the individual's lack of network control. Control of multicast packet routing on the LAN is considered essential of VC sessions are to be conducted for daily business or professional purposes.

Further study is warranted in this area.

MBone Tools: Compatibility

The Zydacron comStation was an example of a dedicated VC hardware platform exhibiting hardware conflicts with multicast traffic. Test results gathered on from machine lead to a number of conclusions being drawn about its inability to participate in MBone sessions:

- the audio codecs are not compatible with the multicast traffic being received;
- the transmission & reception rate of packets on the LAN is not sufficient to allow synchronous playback;
- the audio packets being received were being assembled intermittently, with numerous packet losses, allowing for only partial playback of audio information.

Discussions with engineers and representatives of Zydacron resulted in a consensus there were, indeed, hardware conflicts with the codecs installed in the comStation, but no readily available solutions to the problem existed. Development of the hardware, and work with drivers and the comStation software application, are warranted to develop a working solution that can interface with MBone and other multicast networking protocols.

MBone Tools: Propriety vs. Public

Most of the free MBone tools have not been developed or had further support since the late 1990's, limiting their effectiveness and compatibility with new operating systems, infrastructure developments and changes in network configurations. Research done during this study indicated that few universities or non-profit organizations were continuing development in MBone tools, providing support to the idea that their effectiveness and usability is limited in time and scope. With current operating systems, these tools provide limited usefulness and reasonable quality of service, but not in a time-sensitive or project-critical environment.

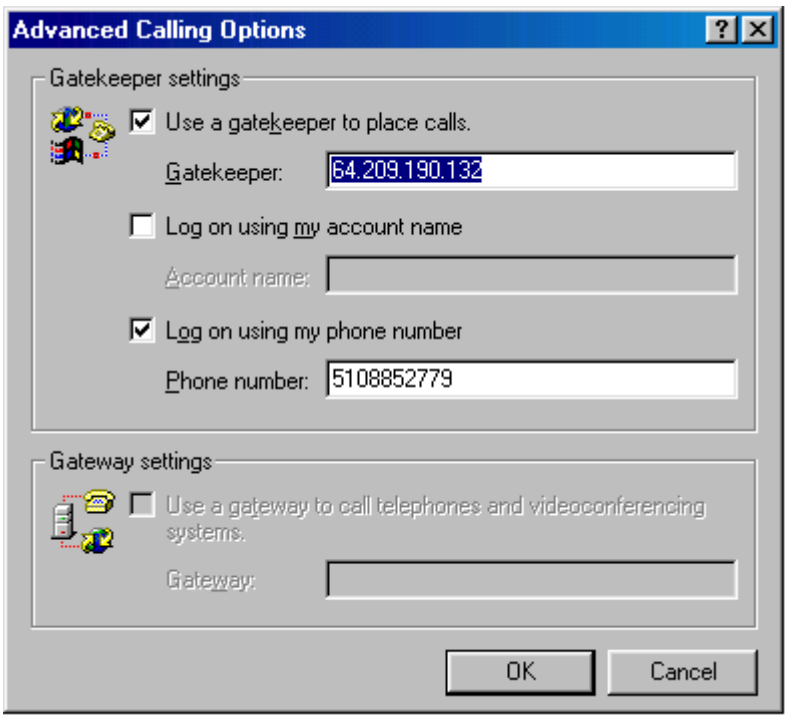
Complete notes on MBone testing are found in Appendix A: General MBone Test notes at the end of this paper. See Appendix B: Zydacron comStation 160 Tests for details on test procedures of this workstation.

Test Procedures: Web-based Multicast Videoconferencing

Another alternative offering that is a low-cost solution to MBone or dedicated hardware & software packages is web-based, multipoint videoconferencing services offered by software manufacturers and specialized vendors. These browser-based video portals require certain software and network configurations to be workable; examples include FVC's Clicktomeet.net service and Evoke Communications Web Conferencing. Both systems were tested during this study.

The ClickToMeet system is highly scalable, as hundreds or even thousands of simultaneous users in a variety of geographical locations can participate. By ‘grouping’ multicast sessions, numerous individual users can participate in separate sessions, further scaling the system to a global scope. Access is greatly expanded, as persons with the required hardware, software and network access can utilize the service. Finally, this alternative is extremely cost-efficient; there are no actual service fees involved in using the web-based conferencing tools. This feature alone guarantees the feasibility and popularity of such a system.

The ClickToMeet services require an H.323 compliant endpoint machine that is configurable and compatible with the FVC gatekeeper. AS mentioned earlier, a dedicated VC workstation can be configured to work with this system; this was also done on a remote Windows platform by configuring Microsoft's NetMeeting as a software endpoint to interface with the web-based video portal. This was accomplished by inputting the assigned gatekeeper and E.164 endpoint specifications into the Advanced Calling option fields of NetMeeting, as seen in the graphic below:



Additionally, network firewall configurations must allow multicast packets to freely travel across the transmission path from the source machine to the video portal. An online, Java-based test allows a user to test any firewalls on their network connection (at home or ISP) to detect any blocks in the network path. This was conducted on a remote Windows machine connected to an aDSL service with firewall protection; tests were conducted with the local software firewall turned on and off with no apparent effect. Results of those tests are shown below:

The results of this test are summarized as follows:

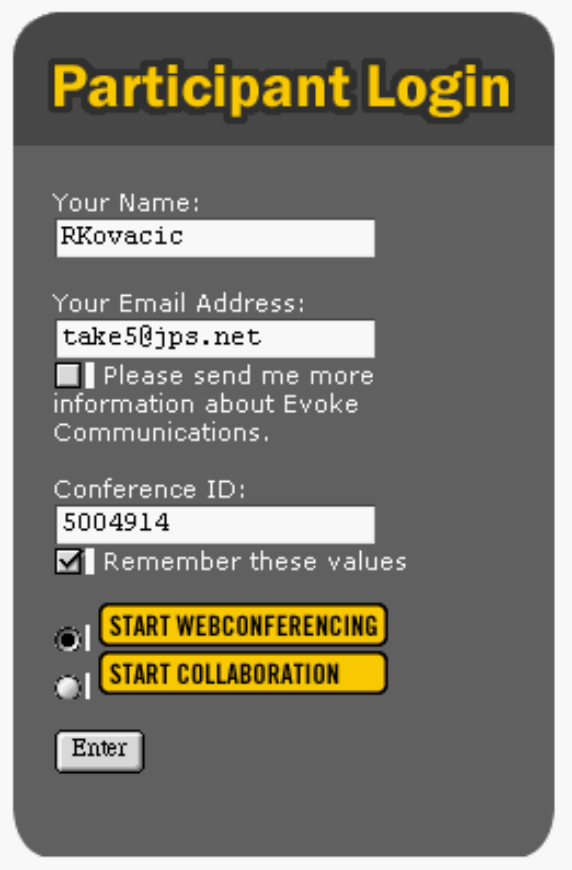
- Failure of UDP protocol in accepting Incoming packets failed on all logical ports, indicating that their is a problem in receiving multicast traffic from a source outside of the ISP and/or LAN networks;
- TCP Outgoing packet route was capable of transmitting multicast packets from the local source machine;
- Outgoing packets using UDP protocol could also be sent from the local machine.

This problem prevented any connections to be made using the Clicktomeet.net service, although the service allowed this user to login to the video portal and attempt calls to technical parties and demo destinations established at the service. Attempts to make connections with other parties ultimately failed, due to the inability of the video portal to accept packets sent from the local machine. Technical support was sought from the ISP of the aDSL service used at this remote location; no satisfactory solution was found to this problem and further talks with engineers at the service provider were pending at the end of this study.

The same overall impressions apply to the CuSeeMeWorld virtual video community, but the intended audience is more consumer-oriented than business. This service has merged with FVC and now work from a common customer base. Though technically different in operation, both services are attempting to provide similar services to the enduser and require similar network configurations. CuSeeMe requires the VC software to be downloaded or purchased and installed on a client machine before accessing any of the services; this was accomplished using a free 'trial' version of the software for Windows available from the company web site.

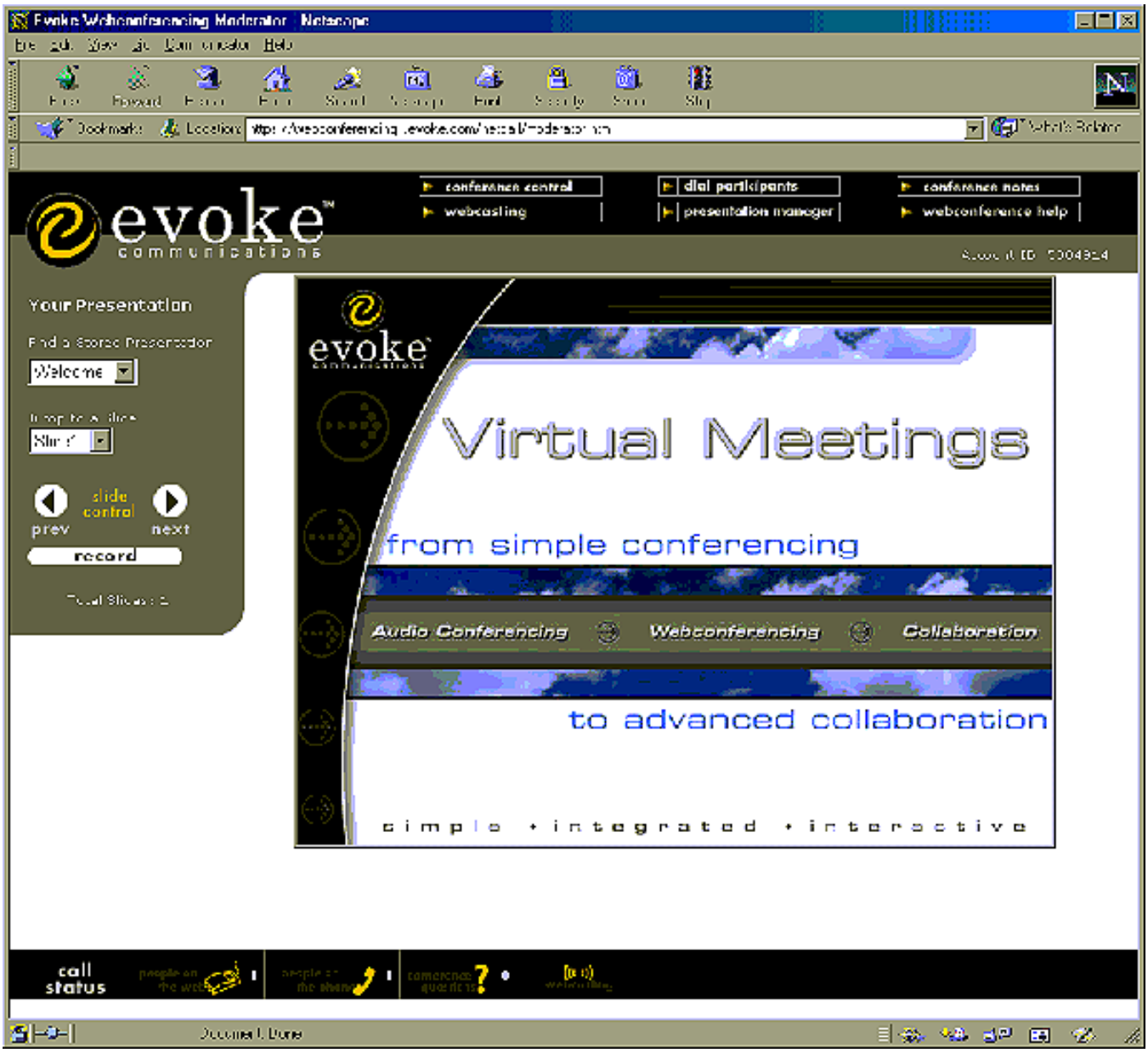
The Evoke Communications solution was also included in these tests; this service is more of a collaborative tools and presentation medium than a method of video conferencing. It required registration and payment method to be validated upon registering. A 'free' demo offer was in effect at the time of these tests, allowing a 'moderator' to host a webconference meeting with up to five participant with no fees. The user did have to incur any telephony costs involved in logging onto the service, 9 minutes of such fees were incurred during testing in this study to gain knowledge of the service and interface.

To begin or join a session a user had to logon to the service either as a Moderator or Participant. Shown to the right is the login screen for a participant; the moderator login is identical with the exception a user's PIN is required to begin a webconference session.



Once the login procedure is accomplished, a moderator may begin a webconference or a user may join any listed sessions. To start a web session, the portal requires a phone connection to be made between the service portal and the 'host' or moderator machine; this can be accomplished by dialing an 888 number from the web interface, or having the video portal call the local machine phone number. During this test, the 888 number was called to the portal to establish a connection after logging on to the service as a moderator. After several prompts, the session was established via phone connection and the web interface reacted by updated web interfaces.

The interface allowed a variety of controls to be manipulated for voice and data access, and outside user interfacing with the session. Controls also allowed the moderator to view the participants of a session and end a session via a popup browser window. Below is the standard interface presented to a moderator of a webconference session:



Additional status icons at the bottom of the window allowed for monitoring of session, users phoning into the session for audio only, and the like. The controls on the left of the interface allow a moderator to present preexisting slides or documents for viewing, and to record a conference session. At the top of the window are icons for accessing additional characteristics of the session as monitoring dial-in participants, creating and recording a webcasting feature, and accessing a built-in Help guide.

Test Conclusions: Web-based Multicast Videoconferencing

Web-based multicast services have been tailored towards specific business applications and consumer needs. For true real-time videoconferencing with collaborative tools no web-based service tested in this study proved to be completely satisfactory in meeting the expectations of the researcher. Some of the solutions network requirements were too limited for the average consumer to utilize; other features as software memory and cpu processing requirements proved difficult for users of pre-Pentium or PowerPC machines to use effectively. Other solutions proved to have features that only a limited number of specific users as business managers might want to utilize, restricting the overall market appeal of the produce. Finally, no one solution provided the easy of use, OS and hardware compatibility, tools, features and network requirements deemed satisfactory to this researcher.

Following are comments and conclusions on each of the web-based conferencing packages tested:

- **FVC ClickToMeet**: this video portal has a well-developed set of software tools and is the closest of the solutions tested to an everyday useable webconferencing service for business. But the network requirements are too restrictive for the average user; a user would need an unrestrictive path to the video portal from their LAN router, a network configuration many system administrators would not allow. This solution also supports Windows OS only, limiting the service to a specific demographic and technical group.

- **CuSeeMeWorld**: this web interface is the most developed of the solutions tested for general consumer use. A free trial version of the software and web interface plugins are available for download and installation on a local machine. An Installation Wizard assists in tailoring the software preferences for the various features. Test features in the web portal include firewall and network connection testing. And a Web Companion set of software applications allow you to access web channels, obtain up-to-date news on the software, store favorite video chat areas and the like.

  But the chat areas tend to be crowded with people without any purpose of being there except to experience the phenomena of multicast over IP. There appears to be no moderator of any of the sessions, and privacy can only be guaranteed if a user creates a session that has access restrictions in place. This service is undesirable from the standpoint of its lack of purpose and generic orientation toward use of the technology, but useful for family members and individuals wanting to communicate with relatives or business associates on a one-on-one format.

- **Evoke Communications**: the 'webconference' service provided by this vendor has no video capabilities, thus rendering it to more of a collaborative public workspace. Meetings must be preplanned and any materials to be presented must be pre-packaged. A user must dial-in to the service, something that creates something of a paradox with a web-based service; a user can send and receive information via TCP/IP but must establish a circuit-switched connection to access the services. There are also phone charges associated with the phone connections with the service's host machines. This researcher found the features to be somewhat low-tech and the application of the service attractive only to businesses that had no other way of collaborating with remote offices or business associates.

Test Procedures: dedicated Multicast Hardware

One dedicated VC installation was conducted during the course of this study. This involved the purchase and installation of two Polycom ViewStation group videoconference systems in locations in San Francisco and Van Nuys, California. The purpose of the installation was for two-way VC educational sessions involving an instructor in San Francisco to be multicast to a separate facility with capabilities of transmitting full-motion video and voice in real-time, with additional video sources as whiteboard, copystand and cpu screen switchable during sessions. The proposed transmission method chosen was three B-ISDN (Basic Rate ISDN) with a total bandwidth of 384kbps at each location.

Equipment chosen for this installation was the Polycom ViewStation 512, which could provide H.323 multicast traffic and accommodate both TCP/IP and ISDN transmission links. Features[1] of this system include:

- Full-motion video at 30 frames per second in point-to-point calls
- Full duplex digital audio with noise suppression and echo cancellation
- An embedded Web server handles diagnostics and simple software upgrades over the Net
- Web-based presentation system makes it easy to share graphics and slides
- Address book records numbers frequently dialed
- Voice tracking camera and track-to-preset function automatically focus on the speaker
- Simple GUI makes setup fast and foolproof

[1] Polycom ViewStation web site, http://www.polycom.com/products/video_medium.html

The installation included dual monitors at both locations to provide student and instructor viewing of video traffic and a room microphone for ambient and instructor voice audio.

Test Conclusions: dedicated Multicast Hardware

The Polycom ViewStation was easy to install and setup, and performed as expected during initial tests done at both facilities. Test calls were made between the San Francisco and Van Nuys locations successfully with all features of the VC system operational. Both audio and video streams were transmitted by both locations; setup of the system software via on-screen menus using the IR remote was matched between the locations to eliminate any conflicts with the systems.

One problem became apparent during testing, however; the transmission links at the Van Nuys facility showed only one of the BISDN lines operational. A provision in the Polycom software allows for testing of local loop and end loop links; this test and online monitoring tools showed only one of the 3 ISDN lines installed was actually transmitting traffic. Thus, this facility was limited to a 128kbps bandwidth for sending and receiving multicast traffic, not considered acceptable for the system application. The service provider was contacted and informed of the problem; initial tests at the Central Office of the provider indicated the service was intact. These reports conflicted with the local system tests, and a trouble ticket was opened with the repair division of the provider. No further work has been done or problems reported on this system since the installation. Complete notes on this installation are available in Appendix C: SATI Polycom Installation at the end of this paper.

Tests were not conducted on dedicated server hardware due to its lack of availability; no conclusions are drawn concerning this method of multicasting.

Test Procedures: Proprietary Multicast Software

Proprietary software solutions are attractive to the desktop user interested in conducting private VC sessions for business or personal use. One such solution emerging on the marketplace is iVisit software from Eyematic Interfaces. This software is similar to previous releases from CuSeeMe and other vendors and provides a number of different features. It is also available for both Windows and Macintosh OS, allowing for a larger user base than solutions ported to only a single platform.

A free 6-month trial version of iVisit was available during this test. This software was downloaded and installed on different platforms and multiple machines in different locations for test purposes. Private and group calls were made between Telcot, CSUH, a remote home office and other users throughout the USA and world using the software. The package is easy to install, use and understand, with icon-driven commands and multiple windows for monitoring users, video and audio transmission, and network statistics. Both Windows and Macintosh versions were tested in this study.

Test Conclusions: Proprietary Multicast Software

iVisit allows a user to create a private one-on-one call with another user, or to join a group or 'community' of users for multipoint interaction. Both approaches were used in testing this software package. This researcher was particularly interested in the cross-platform compatibility of the product, and conducted most of these tests using a Macintosh G3 PowerPC from a remote location connected to an aDSL transmission link.

Successful VC sessions were made between the remote location and users at CSUH and Telcot. The software was found to be fully functional but cpu and memory intensive; on a G3 Macintosh running OS9.1 with 224 mb of RAM video frame rates of 12-25fps were transmitted regularly but occasional paused or 'frozen' video feeds were experienced. An accompanying Pentium IImmx Windows98 PC with limited (64mb) of RAM experienced numerous software freezes and low video frame rates (4-8fps), making the software nearly unusable for extended periods of time. Users installing on older pre-Pentium or pre-PowerPC machines may find the processor load and memory requirements too taxing for such systems; installing of this software package on older machines is not suggested.

Logging onto the various communities listed in the Directory of the software allowed for multipoint connections to be made with persons around the globe. Calls were made to and received from users on various continents around the globe, with acceptable video frame rates for interaction. Text exchange was the most effective way of communicating, as many users do not have microphones and/or sound cards installed at their locations. Audio was received

intermittently from users with microphones, the quality appearing to be a function of the distance the users were from each other. Audio received from Europe, as an example, was not synchronized with the video image; audio received during one-to-one connections with users at CSUH were synchronized and easily understood. This enhanced the real-time nature of the VC sessions tremendously.

A problem with sending audio from the remote location was experienced, however. The conclusion made here is this was not a problem with the software itself, but a hardware problem within the local machine being used. Further research is warranted to remedy the problem.

Conclusion

The overall goal of this study was to explore video conference tools in an attempt to achieve acceptable quality levels and integration of video, audio, text exchange, and collaborative tools sharing within existing and available telecommunications infrastructures. A variety of session and application tools were found that achieved the quality and ease-of-use stated in this study's objectives for everyday business, professional and personal use. These tools and solutions included:

- **Proprietary conferencing software from Eyematic Interfaces, Inc.**

  The set of iVisit integrated applications are easy to use and install; allow video, audio, text exchange and network statistics monitoring during sessions; and is ported to both Windows and Macintosh platforms. The software tested was 'demo' software the vendor provided without charge for a 6 month test period.

- **Dedicated Multicast VideoConference systems from Polycom, Inc.**

  These integrated systems were found to be the most user-friendly and easy to install & operate group systems in this test. The system chosen could accommodate a variety of input sources and transmission links. Equipment provided was high-quality and exceeded the expectations of this research study. Solutions are moderately to high-end priced; substantial volume discounts are available for large companies and institutions, however.

- **Web-based conferencing solutions from First Virtual Communications and CuSeeMe.**

  Both vendors provide integrated, web-based tools that are easy to operate. Local Area

Network configurations can affect the effectiveness of these services, as use may limited by firewall and packet filtering schemes on the LAN. Access to these proprietary tools is also limited; registration with their services requires a payment method and user authentication for each session. But the tools and features are well-developed, and each has an individual market application for either business or consumer use.

The following tools were found to be less satisfactory for everyday use for the reasons stated:

- **Web-based conferencing solutions from Evoke Communications.**

  This vendor's conferencing and collaboration tools are easy to access and use, and are readily available on the Internet anytime. There is no real-time video feature, however, limited the application of the service to prepared material presentation. Registration with the service , payment and user authentication is required for each session, and coordination among users is required for successful conferencing. A free 'demo' license was utilized for these tests, with the user having to incur the per-minute telephone charges for dialup access to the service (ranging from 21-27¢ per minute) plus additional fees for any presentation uploads and conference recording features tested. These costs were found to be a detriment to the overall appeal of the service.

- **Public MBone session tools.**

  A variety of session tools are freely available for interfacing with multicast routers but have not been developed the past several years, lack state-of-art interfaces and user features. A LAN workstation must be configured as an multicast router for traffic to be sent and received, or tunneling protocols must be established on individual

workstations wishing to participate in MBone sessions. Tunneling is limited to UNIX or Linux-based machines, presenting a problem for Windows and Macintosh users. Quality of and access to multicast sessions is greatly affected by LAN switch and router configurations.

The following tools were found to be desirable but untestable for the reasons stated:

- **Dedicated server hardware solutions from First Virtual Communications and Cisco.**

  FVC's ClickToMeet dedicated multicast server and Cisco's IP/TV conferencing solutions both allow in-house, web-based conferencing hosting endpoints to be established at a client's business or home, with multipoint user capabilities. These solutions are both costly, however, and were not available for evaluation during this study's testing period.

Software and hardware solutions continue to be developed by multiple vendors. Many of these solutions presently exhibit satisfactory levels of quality and performance for everyday use. This 'push technology' is placing more pressure on network and telecommunication providers to expand transmission services to accommodate the needs of real-time communications. Publicly available tools are widely available, but some require further development to again mass business and consumer acceptance.

Network infrastructure available on the Telcot LAN, CSU-Hayward LAN, Internet WANs in the United States and selected countries of Europe were utilized for test purposes. Configurations of

all these networks were found to limit the effectiveness of the software and hardware solutions tested, leading to the following conclusions:

- Minimum network throughput of 384kbps is required to transmit and receive audio/video streams at frame rates above 15fps with accompanying uninterrupted audio (speech or sound).
- TCP/IP packet routing is attractive due to its availability and low cost; leased lines (as B-ISDN) provide dedicated and guaranteed bandwidth but are more costly than public TCP/IP routing.
- Firewalls and multicast packet filtering on networks severely restrict the effectiveness of all multicast solutions to deliver QoS at expected levels, and should be researched prior to purchasing or installing any solution.
- High-speed public TCP/IP packet routing is effective for multicasting if network configuration is controlled locally by system administrators familiar with network requirements of multicast traffic.

Real-time videoconferencing and collaboration is highly dependent on network and telecommunications infrastructures. Expansion of the telecommunications infrastructure is necessary for all users, business, educational and private, to use the various VC tools with acceptable QoS on a daily basis. Local Area Network and telecommunications infrastructure capabilities are the biggest limitations currently effecting the performance of available software and hardware tools.