CMU-ITC-86-046

Monitoring Local Area Networks at Carnegie-Mellon University: Tools for Network Planning

Bryan Striemer
Mark Lorence

Information Technology Center
Carnegie-Mellon University
Pittsburgh, PA. 15213

May 16, 1986

Table of Contents

Table of Figures

Table of Tables

Introduction

In February 1982 a task force for the future of computing at Carnegie-Mellon University issued a report in which they said, "The Task Force believes this [the Local Area Network] is the single most important technical step that can be taken to enhance the computational environment at C-MU." [1] Six months later a joint project was started between the university and the IBM Corporation to develop a computing technology to support C-MU's needs by the fall of 1986 [2]. In the first three months of 1985 a prototype of this system was deployed on campus making use of, and expanding, installations of the Ethernet [3] Local Area Networks already on campus. By the end of this year the university plans to complete a campus-wide installation of a token ring [5] cabling system and will begin large-scale deployment of this new computing facility.

The new system has been given the name *Andrew*, after two benefactors of C-MU; Andrew Carnegie and Andrew Mellon. Since the fall of 1985 the Information Technology Center - the group responsible for the development of Andrew - has been monitoring utilization of various local area networks on campus and has recently developed a new monitor that traces specific traffic patterns. This paper briefly describes the tools we are using and presents some of the data we have collected. We hope our network analysis will be useful in the planning that is currently taking place for the expansion of Andrew.

The Network Monitors

All our network monitoring is done with IBM PC products. To watch the Ethernet we use the Ungermann-Bass PC/NIC network adapter and to monitor the IBM token ring we use the IBM 6100 token ring adapter. The token ring adapter is built to use the 16-bit I/O bus so this card can be used only in the AT personal computers. The Ethernet adapter can be used in any PC having an eight bit card slot.

The monitors transmit no data, they simply listen to all traffic on the network. The token ring adapter provides an error log that keeps a count of any packets not received. The Ungermann-Bass adapter enables us to determine if packets have been missed, but not how many. Because we save only a small amount of information about each packet we have been able to receive all network information and not miss any packets. We know this on the token ring by periodically reading and saving the error log. Measuring the accuracy of the Ethernet tools was done by running another piece of equipment in parallel and then comparing the results. The verification tool we used was the LANalyzer Ethernet Network Monitor made by EXELAN, Inc. [6] which has the ability to monitor total packet and byte count without missing information.

Another difference between the ring and Ethernet cards is that the PC is responsible for moving information into and out of the Ethernet card. The token ring adapter has an on-board microcontroller and the ability to gain control of the I/O bus. The token ring adapter is responsible for: managing its own memory resources, communicating with other adapters on the ring, and moving information in and out of the attaching host. The only affect this difference has had is that packet interarrival times on the ring are more varied than on the Ethernet.

Network Utilization Monitor

There are two programs running in the utilization monitor, one is an interrupt handler that gets invoked when the network adapter signals the arrival of a packet. The second program runs in the background, updates the screen and, at midnight, saves the collected information onto a floppy diskette. The data is reduced on a separate machine.

The number of bytes and the number of packets are collected on each four minute boundary of the day. Along with these numbers, added over the entire day, is a distribution of packet size and interpacket arrival times. (The interpacket arrival times are kept only if an AT personal computer is used. PC and XT machines lack a unique high speed counter that is used to capture this information.) If you are using a token ring adapter an error log is checked every four minutes and a missed packet count is recorded.

The real-time display consists of the date, time, bytes and packets received, and network utilization. The screen is updated each second. The display information is most useful in checking that the monitor is functioning normally, but it can also be used for problem determination. Recently we had a event where one machine stopped the entire ring. Figure 1 shows a record of the event. At the time of the failure the monitor was displaying the fact that the network was inactive. This enabled the network maintainers to know immediately that the problem was on the ring rather than with the machine that connects the ring to the rest of the campus network.

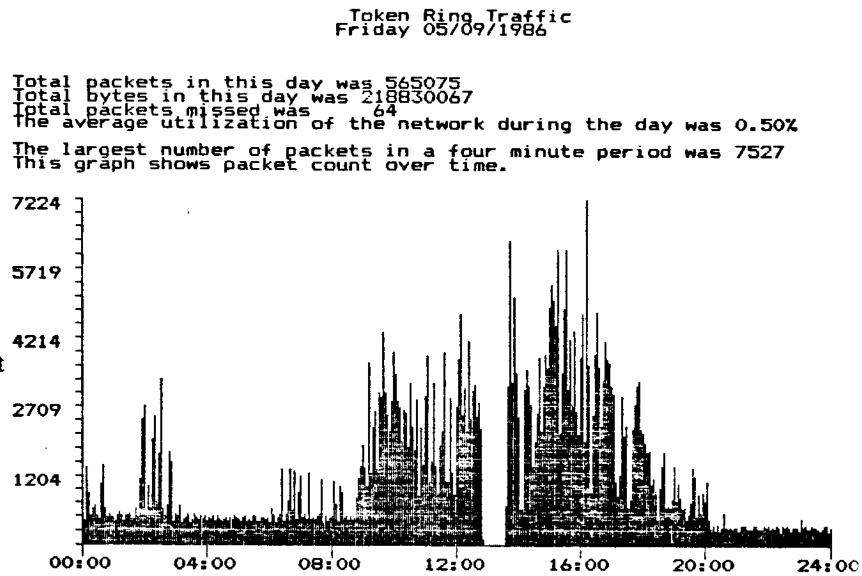


Figure 1.
Recorded Ring Network Outage

Traffic Pattern Monitor

Like the utilization monitor, the traffic pattern monitor has an interrupt handler and a background task. This monitor is different in that it looks at the information field of incoming packets and takes action based on what it finds.

This monitor accumulates information on unidirectional communication paths based on the Internet Protocol address fields.[10] A large table is built with each entry listing the machine that generated the packets and the machine that received the packets, as well as the number of packets and bytes that were sent for this one way communication path over the entire sampling period. If two machines establish a connection between each other it would show up as two entries in this table. There are a finite number of entries in which to store statistics; the monitor can accumulate numbers on 1,792 connections. The number of connections can increase exponentially depending on how much inter-machine communication exists, but typically our workstations establish links with only about three other machines. The monitor is built so that the collected data can be dumped to diskette at any time. The operator may want to save the data and restart the monitor if the table fills up. In the event that the table does overflow, there will be a byte count and packet count of information that was received and not recorded. An accumulated total of non-IP bytes and packets is kept as well.

Even though this tool saves much more information than the utilization monitor, we have measured it receiving all frames. A hashing mechanism is used to index into the data table and an "elastic buffer" is used to pass information between the interrupt handler and the background task. As bursts of traffic appear on the network this elastic buffer will fill up absorbing the spikes of high utilization. A counter is kept of the number of times the interrupt handler found the elastic buffer filled up. The highest number of missed packets that has been recorded is 1558 packets missed in a run involving 1.5 million packets. There will be a point when this tool will fall short of recording all frames, but we have not found that point on the networks we have been monitoring.

A minimal amount of information is displayed on the screen. Along with the date and time, the number of connections being monitored is shown.

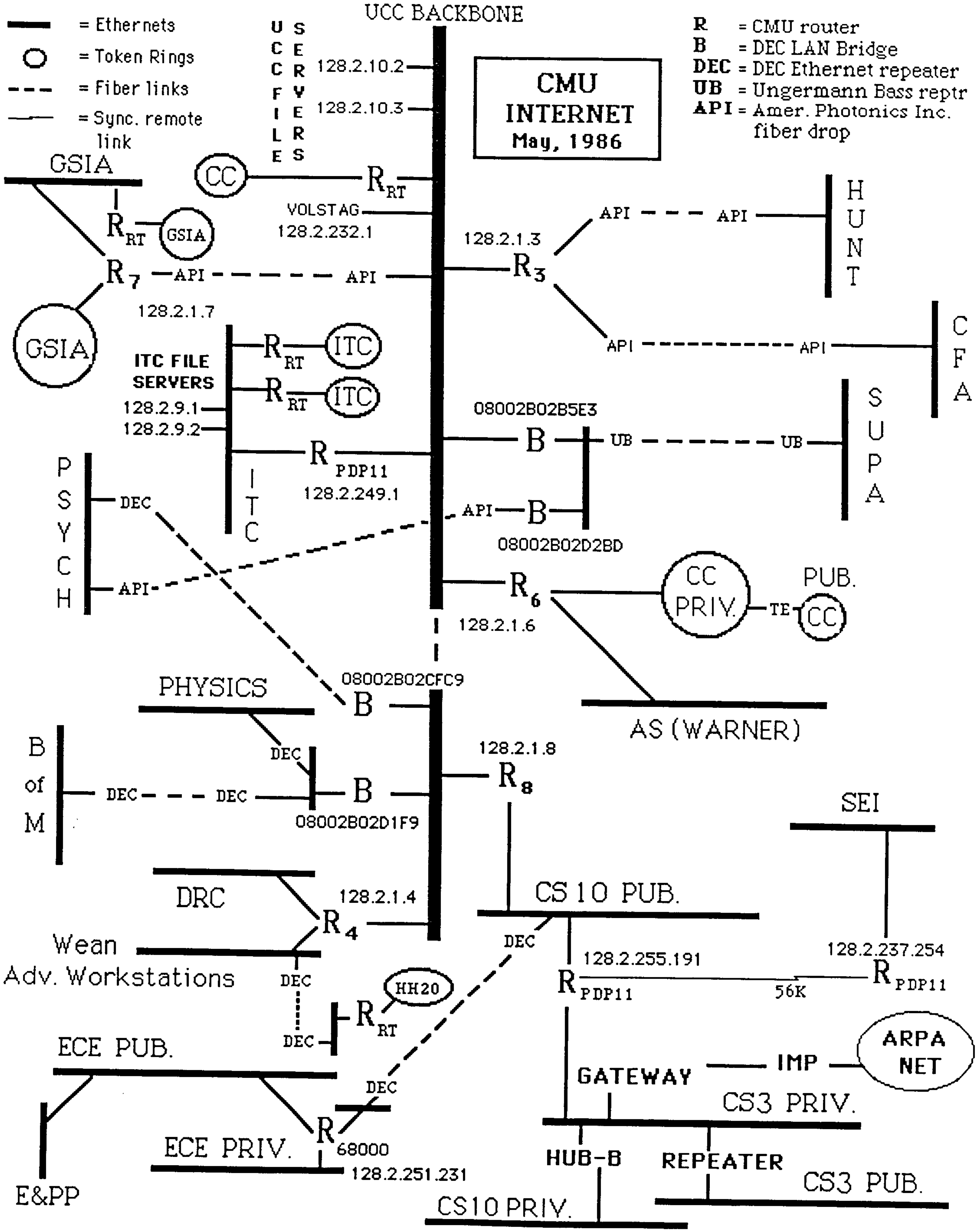


Figure 2.
Campus Network Configuration

LAN Computing Environment

The Andrew computing system consists of central file servers attached to a network supporting two classes of machines: high function workstations and personal computers. The high function machine is characterized as having a multitasking UNIX[tm] operating system, bit mapped graphics display, and virtual memory. (Machines currently being used are IBM RT PCs, SUN Microsystem Inc. model 120s and DEC MicroVax II workstations.) The IBM personal computer can also access a central file server over the network through one of these larger machines running a special server program called PC Server.

Local Area Networks and network protocols existed on this campus long before Andrew. In fact, our ability to deploy Andrew machines to the far reaches of the campus was only possible because these existing networks were extended to a central building and attached to a backbone Ethernet. [4] These 17 Ethernets and 2 ProNet ring networks were built up over the years and now support over 600 non-Andrew computers.

The ITC LAN Configuration

The ITC has one Ethernet and two token rings which are interconnected with machines that route information between them - called routers [9]. The ITC has approximately 45 Andrew workstations which are distributed evenly on the two rings while the file servers and another 15 Andrew workstations reside on the Ethernet. One of these Andrew workstations acts as a PC Server for about a dozen IBM PCs.

The University LAN Configuration

There are just over 200 Andrew workstations on campus today (including the ITC). For many years the central computing center has been using several DEC 2060 machines. Different areas of the campus are using VAX systems, PERQ computers, Hewlett-Packard machines and personal computers from Apple, IBM and other manufacturers. Figure 2 (courtesy of the campus Data Communications Department) shows the inter-connection of Local Area Networks. Some of these machines use the IP protocols which we can monitor, but there are other network protocols co-existing with IP on the campus networks.

Observations on Utilization

Our first development system consisted of SUN Microsystems Inc. model 100 diskless workstations with SUN model 150 disk servers. Early in the development of Andrew it was decided that we would not support diskless workstations [7] and

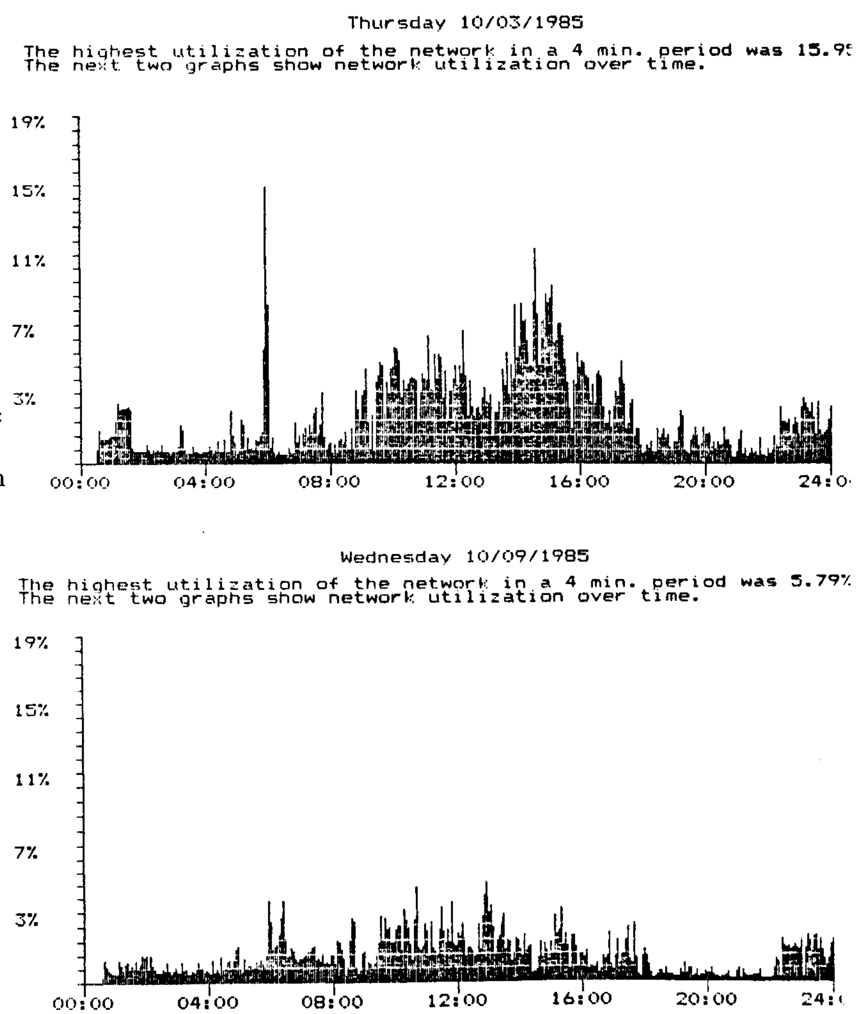


Figure 3.
Utilization Past and Present

eventually phased these diskless machines off the Ethernet. As we eliminated these machines the utilization monitor showed a significant drop in network utilization (figure 3) giving us real data justifying our earlier decision.

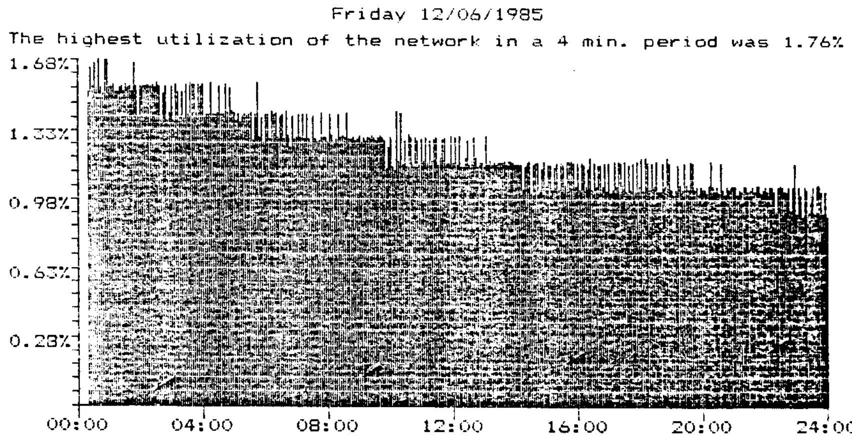


Figure 4.
Decreasing Network Utilization

As we brought up our first token ring we tested it with performance testing software designed to stress our file servers. Over the course of a couple days the monitor showed the network utilization steadily dropping (figure 4) when the test should have remained at a constant level of network utilization. Closer inspection revealed a bug in released software.

At the end of January 1986, right after IBM's announcement of the IBM RT PC, a new public machine room was opened which contained twenty-four new Andrew workstations. The utilization of the campus backbone Ethernet (figure 5) nearly doubled in the next four weeks.

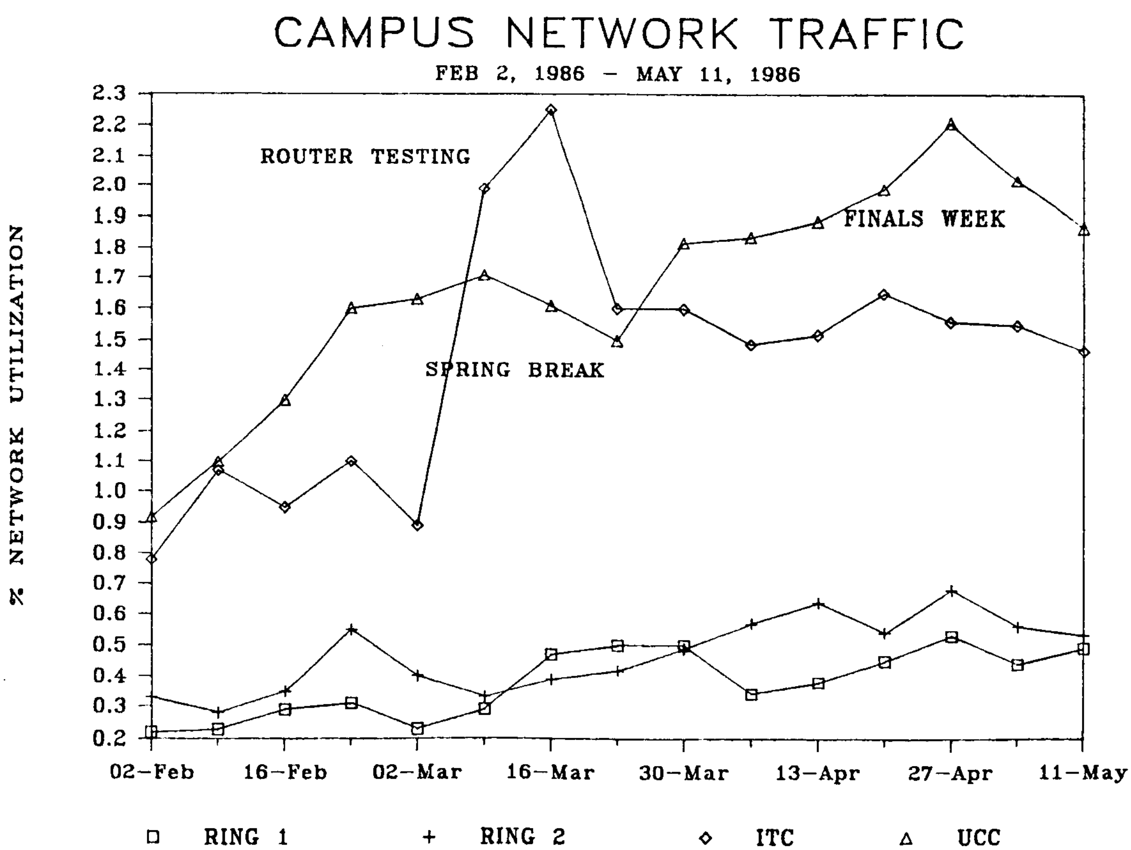


Figure 5.
Utilization of Four Major Networks

Isolated Configuration

The two token rings in operation at the ITC are probably the best examples of pure and complete Andrew workstation configurations. There are no file servers on these rings (all communication with the file servers for each ring is done through a single router) there are no tape back up machines, these networks are not used as a data path for other systems, it's all simply Andrew workstations. In addition, one of the rings has a PC Server that connects all the ITC personal computers to the central file server - another important part of the Andrew system. (See figure 7.)

The utilization monitor can help us understand what we must expect from our routing machines as well as the load each workstation puts on the file server. On Friday April 25, 1986 between 4:12 pm and 4:16 pm we recorded the highest network utilization sustained over any four minute period since the beginning of the year. The utilization number was 5.85% (figure 6). During this heavily used period there were an average 64 packets per second and 29,278 bytes per second. There were 19 Andrew workstations and 11 PCs attached to this ring at the time. During this peak four minute period of network utilization each machine required 976 bytes each second.

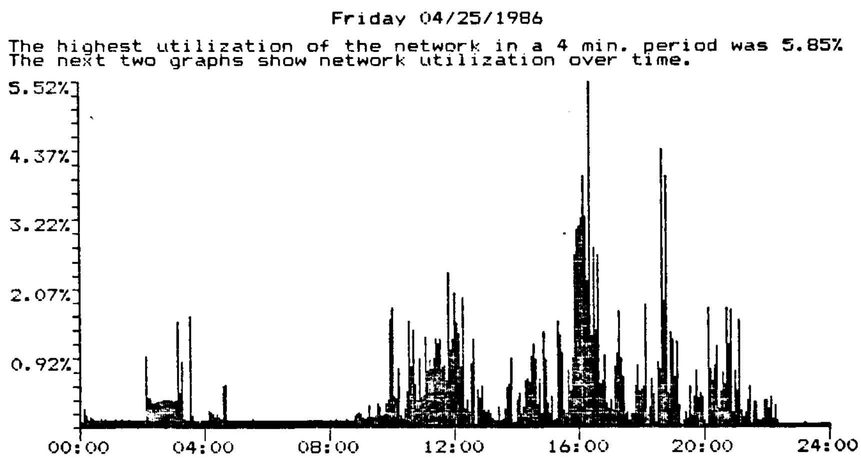


Figure 6.
Peak Utilization of the Ring

Between 10 am and 6 pm there were an average of 13 packets per second and 5,157 bytes per second. This is an average of 172 bytes per workstation per second during the busiest eight hours of the day.

Each member of the ITC has an Andrew workstation and some have PCs as well. It is probably the case that the PCs are relatively inactive. This means that the average network load was closer to 270 bytes per second per workstation, and the peak load was 1,500 bytes/machine/sec.

Observations of Traffic Patterns

For this report both the campus backbone Ethernet and ITC Ethernet were watched for two days. The backbone network was monitored Wednesday May 7th and Thursday May 8th. The ITC network was monitored on Monday May 12th and Tuesday May 13th. Each day was broken into three parts: midnight to 8 am, 8 am to 5 pm, and 5 pm till midnight. (Portions of the results of the data reduction, for each of the twelve sample periods, are listed in appendix B.) Early morning hours are used to analyze the amount of traffic generated when information is sent to our tape back-up machines. The mid-day runs are used to study file server and workstation loads.

File Servers and Workstations

In a single session an Andrew user will establish connections to more than one of the file servers. This is because different files and utilities reside on different machines. Also, since

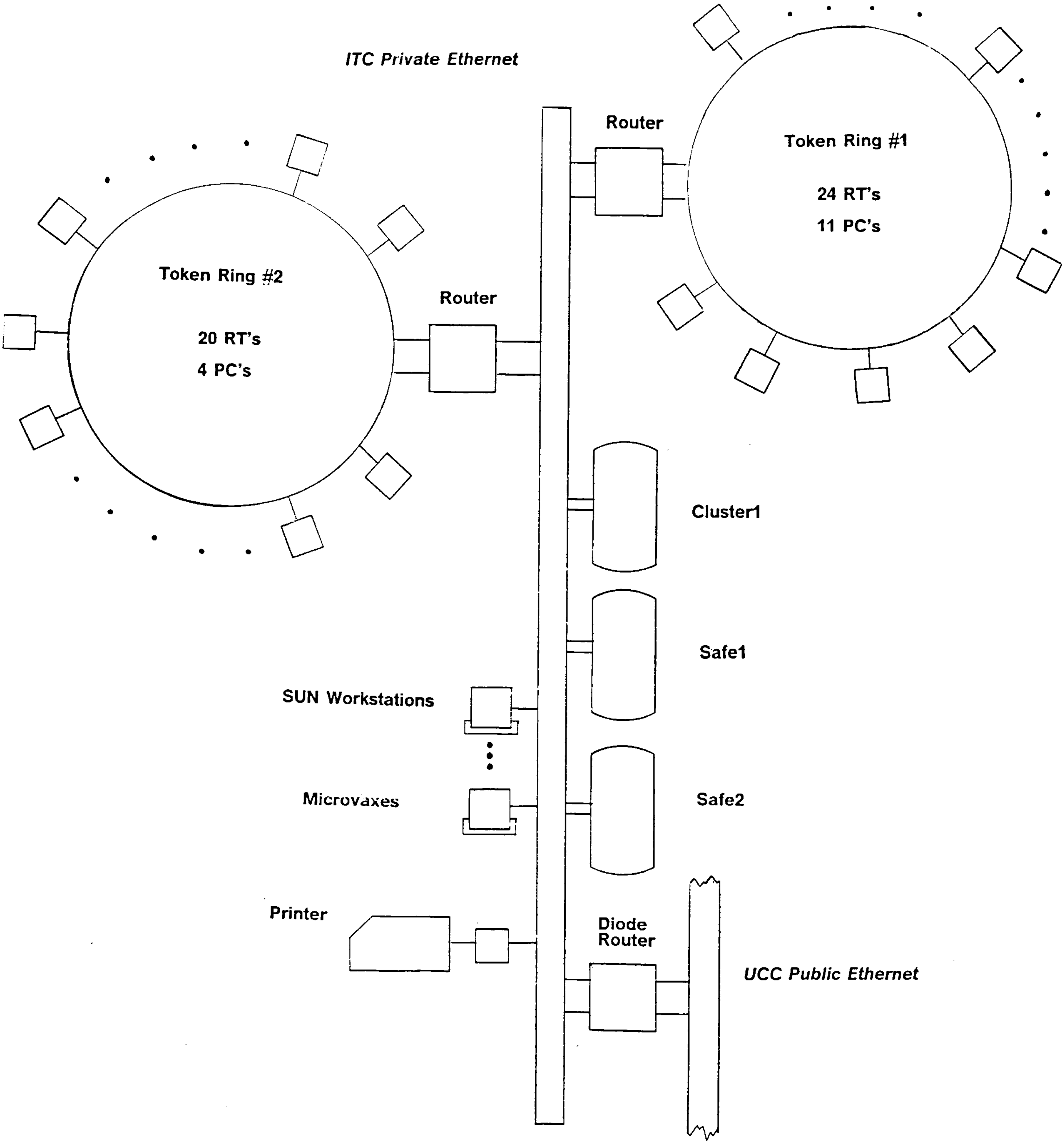


Figure 7.
ITC Network Configuration

we are in the early stages of deployment we have far more users than workstations and people rely heavily on public machines. As different people use the same machine and access different file servers the likelyhood of more connections per machine increases.

The four Andrew file servers used by the campus are called vice2 through vice5. Within the ITC we have servers named safe0, safe1 and safe2. Of the two days sampled, Thursday was the most active for the backbone network and Monday was the day of most traffic on the ITC Ethernet. Table 1 shows the total number of packets, bytes and network utilization for each file server between 8 am and 5 pm on the busiest day monitored (byte and packet count are the number which the machine both received and transmitted). The connections count represents one way communication and since machines usually establish two way connections you can divide this number in half and get an accurate count of the number of machines using each server.

Backbone Ethernet
Thursday May 8th, 1986

Machine	Packets	Bytes	# of connections	% Bytes
vice2	443129	207499584	332	22.37 %
vice3	257406	116304553	284	12.54 %
vice4	230750	80410185	344	8.67 %
vice5	365742	226454086	321	24.42 %

ITC Ethernet Traffic
Monday May 12th, 1986

Machine	Packets	Bytes	# of connections	% Bytes
safe0	28668	17816265	4	1.90 %
safe1	336779	131463008	151	14.03 %
safe2	350764	210408395	149	22.45 %

Table 1.
Campus and ITC file server traffic

On the backbone network the file server/client connections amounted to 60% of all bytes and 39% of all packets. There were about 162 Andrew workstations monitored. To support all of these machines it took 565 million bytes over nine hours or 6.4K bytes each minute for each workstation or roughly 107 bytes a second per workstation.

On the ITC network the file server/client connections amounted to 63% of all bytes and 63% of all packets. There were about 67 Andrew workstations monitored. To support all these machines it took 593 million bytes over nine hours or 16K bytes each minute for each workstation or roughly 273 bytes a second per workstation.

File Server Controller

One machine, called Cluster1, takes on the role of communicating with all the file servers. Software updates are given to Cluster1 and it is then Cluster1's responsibility to copy the information to all the file servers. Password changes are also propagated through Cluster1. This eliminates the need for an operator to contact every file server; something that is important now and will become even more important when Andrew expands to a hundred file servers.

The status of any file server can be monitored with a program that can be run on any Andrew workstation. Information is given on how long the server has been running, how many people are connected and what the file request demand has been. Rather than have an arbitrary number of machines putting requests on the file servers for this information, Cluster1 collects the statistics and passes them on to anyone requesting it.

For these reasons Cluster1 shows up as a big user of network bandwidth.

Appendix C shows the results of a sampling run of the ITC network on Tuesday May 13th between 8 am and 5 pm. Cluster1 contributed more than any other machine to the total network utilization. It was also a major user of the network in it's communication with single machines. There were four machines that were used to monitor file server status: bowerhill, moon, whitaker, and scranton. Of these four, bowerhill was run continuously. In nine hours bowerhill and cluster1 exchanged 40 million bytes of information, or 1,248 bytes each second.

Workstations

Much of the activity on Andrew at this point is applications development. If we look at the workstations used to develop programs that will be widely used in the future we will be able to make better predictions on future network bandwidth requirements.

Table 2 shows the ten connections that contributed most to overall traffic on the backbone Ethernet on Thursday May 8. The machine "glenfield" belongs to one of the people in the computer science department who is working with the ITC to get a data base application running on our system. The first pass of this program runs with very few changes to our file system. This is rather inefficient because our file system never transmits less than an entire file [8]. A great deal of work is being done to reduce the amount of file system traffic that this program generates including modifications to the whole-file transfer function.

Source	Destination	Packets	Bytes	% of all Network Bytes
glenfield	vice3	18769	19969218	2.15 %
glassport	vice2	22999	19948654	2.15 %
hickman	vice3	13338	13040624	1.41 %
cluster1	vice5	9601	8106290	0.87 %
vice5	apollo	6805	8088278	0.87 %
ishmael	vice3	10674	7589175	0.82 %
vice2	norristown	8808	7482856	0.81 %
coraopolis	vice4	10774	7259516	0.78 %
brookville	vice4	7038	6677684	0.72 %
cmu-4	vice4	8795	6658827	0.72 %

Table 2.
Highest Single Direction Communication Paths

The amount of information going from glenfield to vice3 alone averaged 616 bytes/second. The total amount of traffic for glenfield amounted to 930 bytes/second.

Andrew workstations have the ability to connect and communicate with each other without going through a central facility, as do all machines that run the IP protocols. System maintainers use this function to control and diagnose problems on machines remotely. Other people find this capability useful when they want to move information to and from other machines on campus. Unused machines can be accessed over the network and used when people are looking for extra computing resources.

The May 7th mid-day sample of the backbone network showed that inter machine communication accounted for 27% of all connections, 24% of all packets and 6% of all bytes. On the second day of sampling this traffic accounted for 28% of all connections, 14% of all packets and 5% of all bytes.

Non IP Traffic

The campus backbone Ethernet is used as a communication link for non-Andrew machines. On the first day of sampling, during the nine hours between 8 am and 5 pm, the non-IP traffic accounted for 29% of all bytes and 63% of all packets. On the second day non-IP traffic was 11% of all bytes and 29% of all packets.

Printing

There are two Andrew printers on campus and one in the ITC. The busiest printer was at the ITC on Monday May 12th between 5 pm and midnight. The average network traffic was about 400 bytes each second. The most active campus printer was on Wednesday May 7th in the evening hours when it averaged 250 bytes each second. The average for all printers for all days was 150 bytes a second.

Tape Backup

Each morning, in the first few hours of the day, information is sent from the file servers to a back up machine. On Wednesday morning, May 7, between midnight and 8 am the tape back up system - CMU-4 - sent and received 63% of all network traffic (Table 3). The total Ethernet utilization for this sample period was 2.3% making the back up system 1.45% of the Ethernet. There were 515 million bytes exchanged averaging 17.9K bytes each second.

File servers are backed up in two ways: saving only those files that have been changed that day and, every nine times the server has been saved incrementally, a complete copy of the disks is made. The full disk backup saves much more data than the incremental approach. There is no attempt to synchronize the file server's full disk backup in or out of step with each other. For this reason the amount of tape activity changes quite a bit from day to day. On May 8th the tape activity was half that measured the previous day.

Machine	Packets	Bytes	# of connections	% Bytes
cmu-4	843110	515037472	12	62.94 %

Source	Destination	Packets	Bytes	% Bytes
cmu-4	vice3	137066	8244221	1.01 %
cmu-4	vice2	91090	5486669	0.67 %
cmu-4	vice4	79510	4795654	0.59 %
cmu-4	vice5	7771	466435	0.06 %
cmu-4	cluster1	1022	61320	0.01 %
cmu-4	maytag	242	14520	0.00 %
vice3	cmu-4	228048	218105767	26.65 %
vice2	cmu-4	151840	143623652	17.55 %
vice4	cmu-4	132070	10461849	14.72 %
vice5	cmu-4	13176	12889311	1.58 %
cluster1	cmu-4	1028	717866	0.09 %
maytag	cmu-4	247	170208	0.02 %

Table 3.

Wednesday May 7th, 1986. Midnight to 8 am. Tape back up of the file servers.

Conclusions

Having the ability to simply count packets and bytes and chart this information can uncover problems in software, help in system design decisions and assist in simple maintenance. Having more complex tools, like our traffic pattern monitor, can be used to determine something as simple as average network utilization or give you details about how much traffic each individual workstation generates.

Determining the number of Andrew workstations that can be put on an isolated network will depend largely on the router machine's capabilities. To ensure that there is no disruption of service during peak network loads the router should be able to handle approximately 1,500 bytes each second for each Andrew workstation.

During a random day on the backbone Ethernet the average bytes each Andrew workstation required each second was 107. Traffic patterns within the ITC show loads of around 270 bytes/second for each machine. The most active Andrew machine averaged 930 bytes/second over a nine hour period. Those machines running the special file server monitor program were measured to generate as much as 1,248 bytes of network traffic each second over extended periods of time.

We just recently completed the development of the IP monitor and it is somewhat unfortunate that the development of this tool coincides with the end of the school year. We have always suspected that the Andrew developers, using Andrew workstations all day, generate more network traffic than the average machine on campus. That's what this analysis shows, but we believe the large difference is due partly to the fact that the samples were made at the end of the school year. We recommend that people doing network planning lean more towards the numbers seen measuring ITC workstations.

The bandwidth of Ethernet is 10 megabits/second or 1.25 million bytes/second. Four hundred Andrew workstations each averaging 300 bytes of data each second would drive the Ethernet to about 10% Utilization. If the peak load went to 1,500 bytes/second for each of the 400 workstations the Ethernet utilization would hit approximately 50%.

The tape backup activity changed by 100% between the two days that we sampled. On the most active morning the Ethernet utilization was 1.45% averaged over an eight hour period or 17.9K bytes/second. Expanding the number of file servers could generate significant network loads during the backup process in the early morning hours.

To fully understand the network resources needed by the Andrew computing system, and the other systems on campus, we will need to conduct many more experiments. Doing this analysis will not only help us prevent the network from becoming overloaded, but will give us data enabling us to balance the load on file servers, locate inefficient applications and assist in network maintenance.

Appendix A

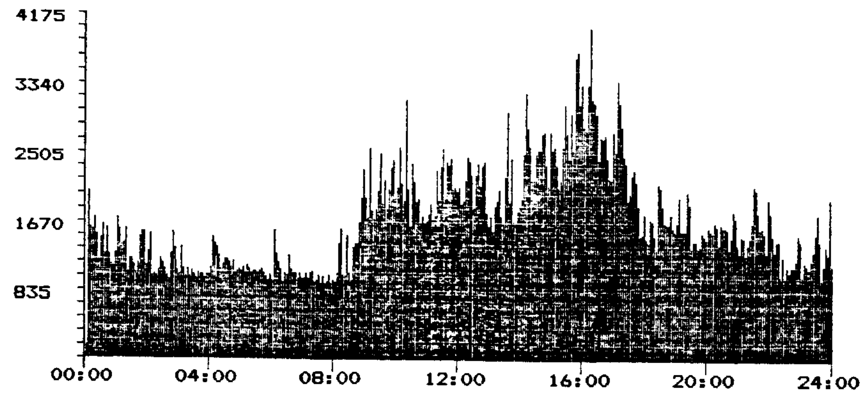
Network Utilization
A Weekly Average

We picked the week of April 20th to show average utilization numbers because it was a time when the campus was in a fairly normal state. Spring break was over, spring finals were two weeks away and utilization was on the rise (figure 5).

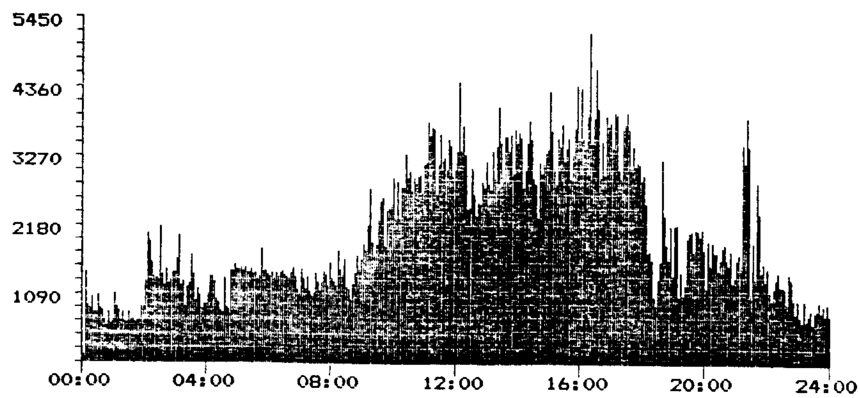
Notice that the token ring and Ethernet graphs, for Network Utilization Versus Time of Day, have different values along the 'y' coordinate. The charts were normalized to a fixed scale so that we would be able to more easily compare them. Remember also that percent utilization between the ring and Ethernet does not equate the same number of bytes. The speed of Ethernet is 10 million bits per second while the token ring speed is 4 million bits per second.

Average Daily Network Traffic
April 20th 00:00 am to April 26th 23:56 pm 1986
Packets Versus Time of Day

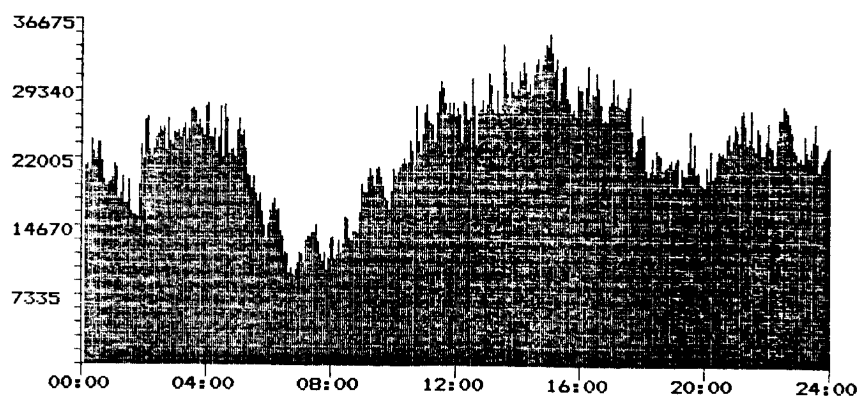
ITC Token Ring 1



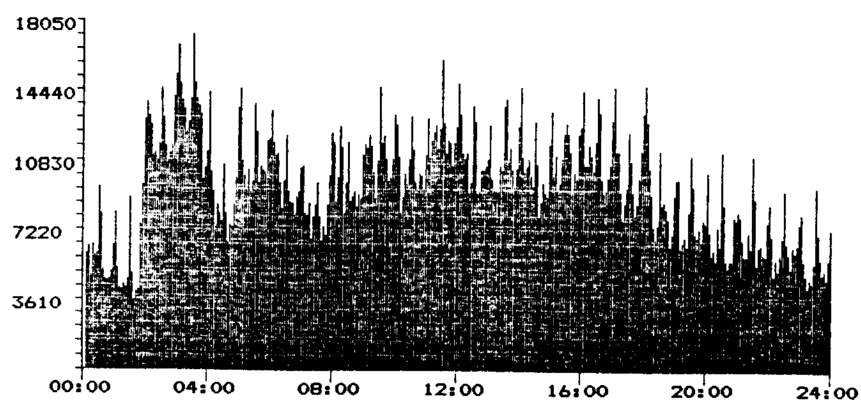
ITC Token Ring 2



Backbone Ethernet

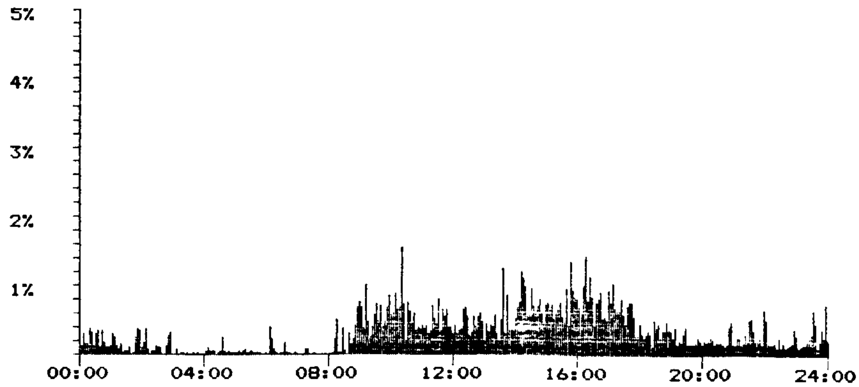


ITC Ethernet

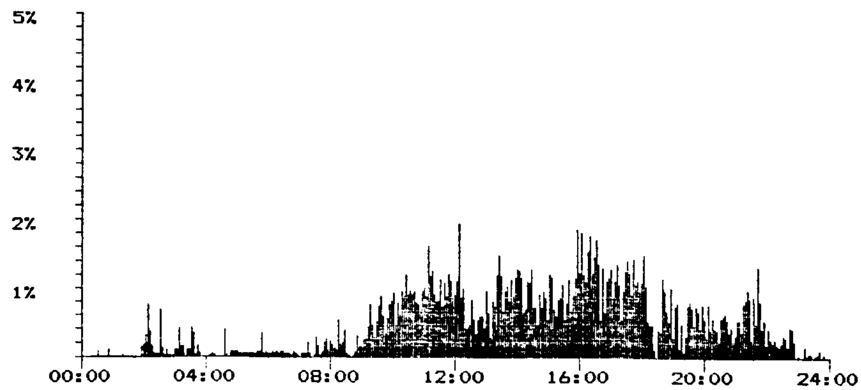


Average Daily Network Traffic
April 20th 00:00 am to April 26th 23:56 pm 1986
Network Utilization Versus Time of Day

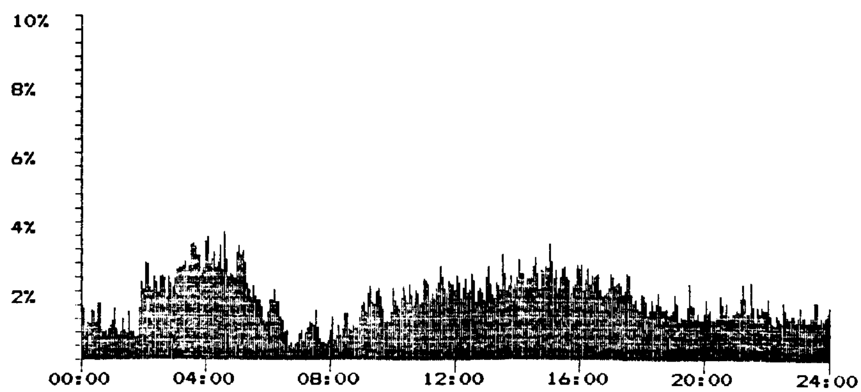
ITC Token Ring 1



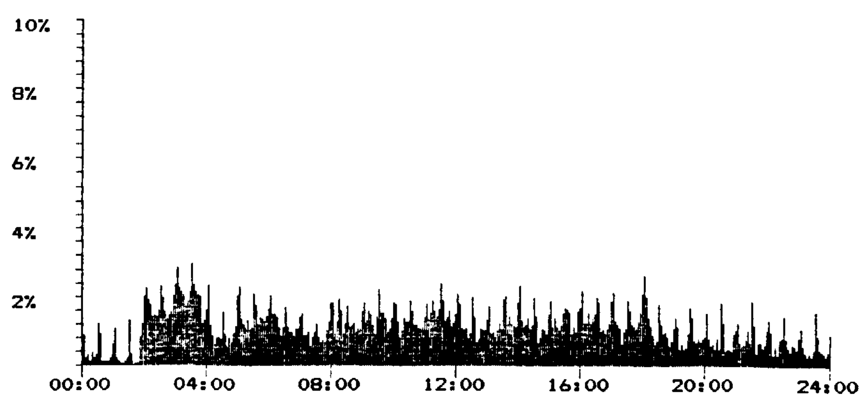
ITC Token Ring 2



Backbone Ethernet

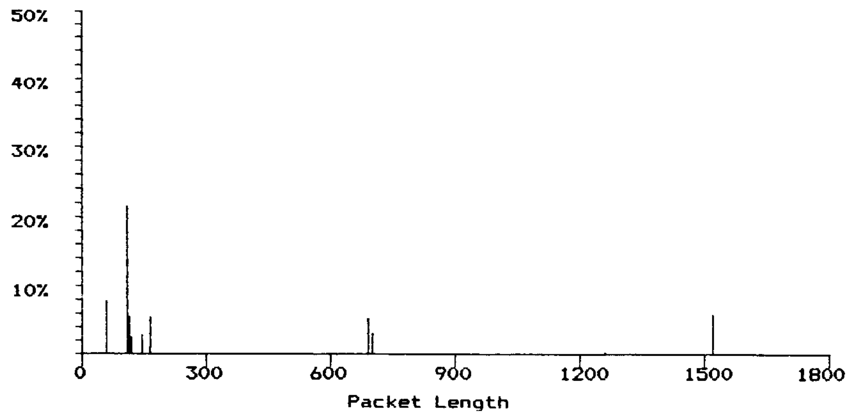


ITC Ethernet

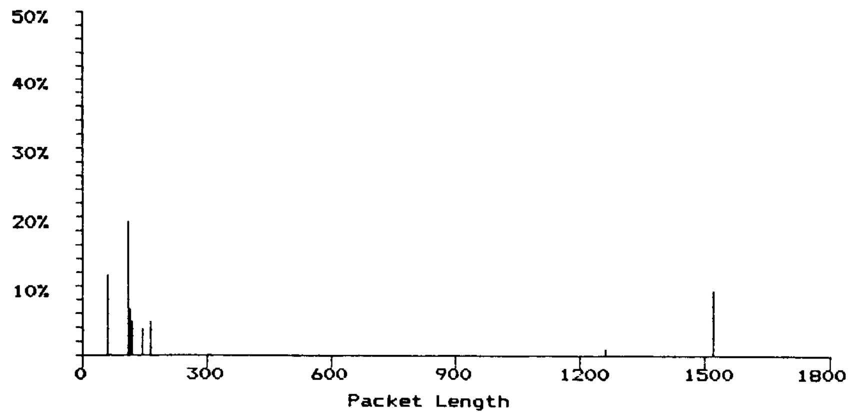


Average Daily Network Traffic
April 20th 00:00 am to April 26th 23:56 pm 1986
Percentage of Packets Versus Packet Length

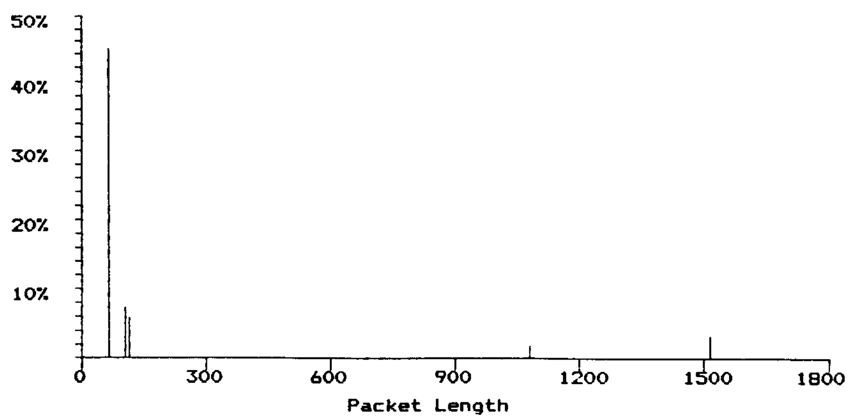
ITC Token Ring 1



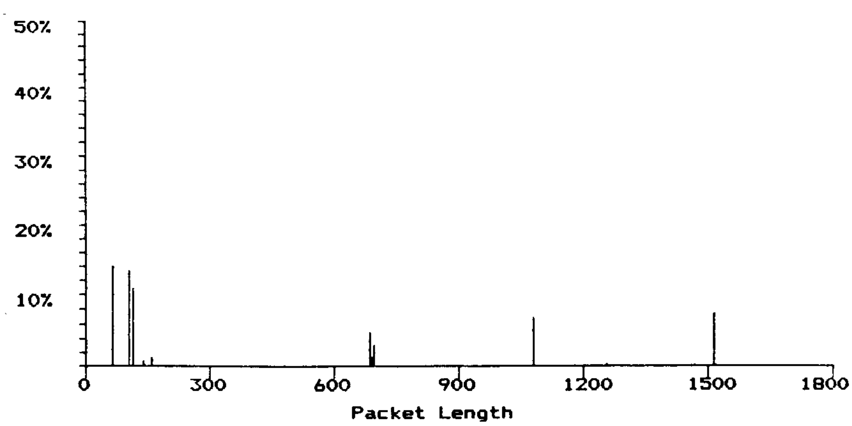
ITC Token Ring 2



Backbone Ethernet

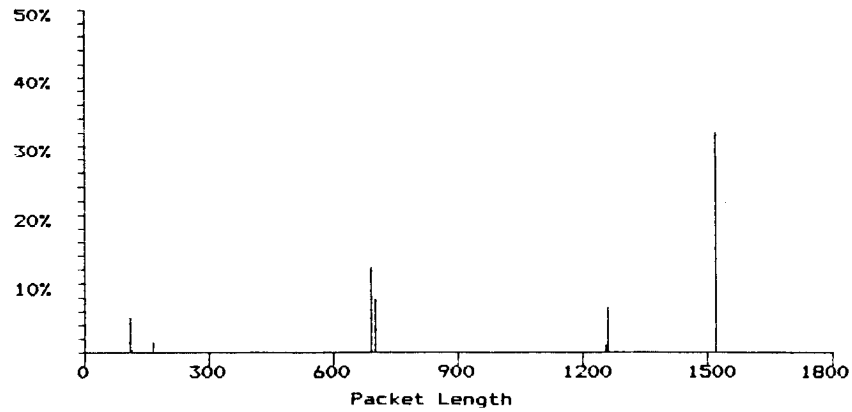


ITC Ethernet

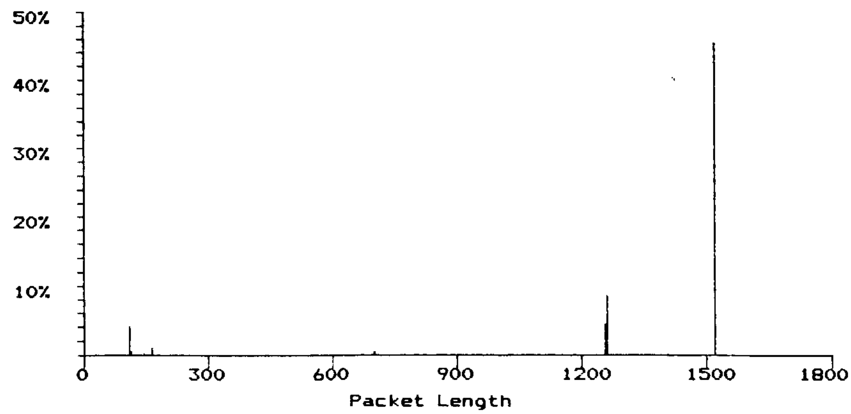


Average Daily Network Traffic
April 20th 00:00 am to April 26th 23:56 pm 1986
Percentage of Bytes Versus Packet Length

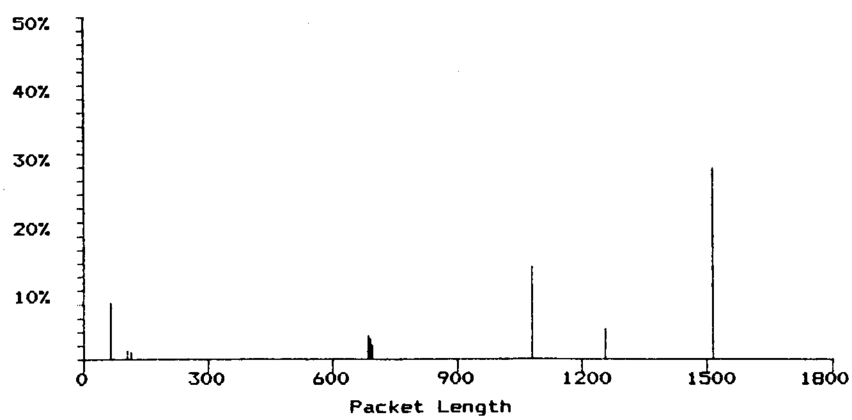
ITC Token Ring 1



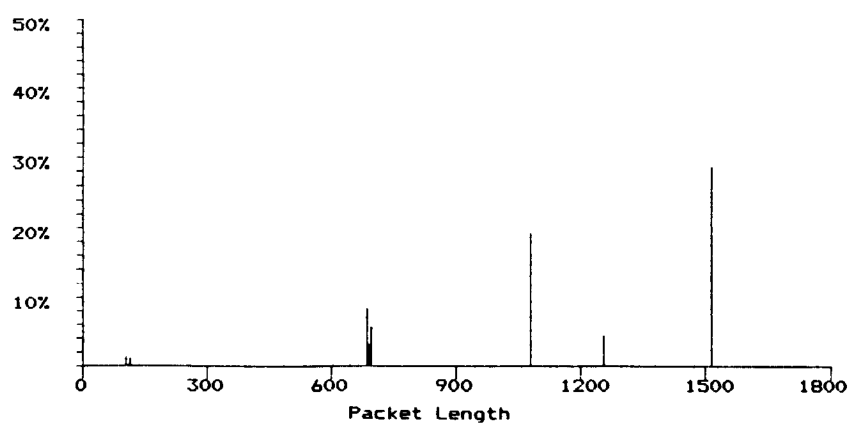
ITC Token Ring 2



Backbone Ethernet



ITC Ethernet

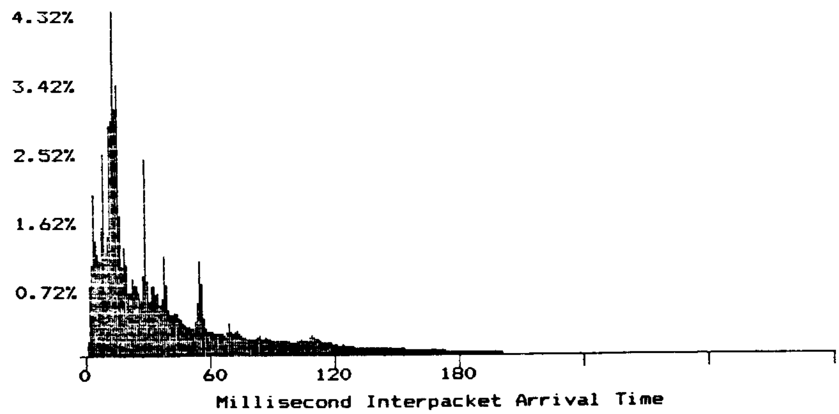


Average Daily Network Traffic

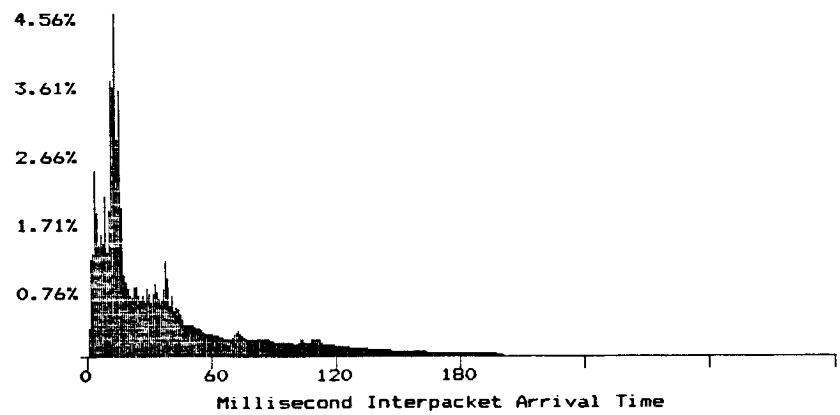
April 20th 00:00 am to April 26th 23:56 pm 1986

Percentage of Packets Versus Interpacket Arrival Time

ITC Token Ring 1



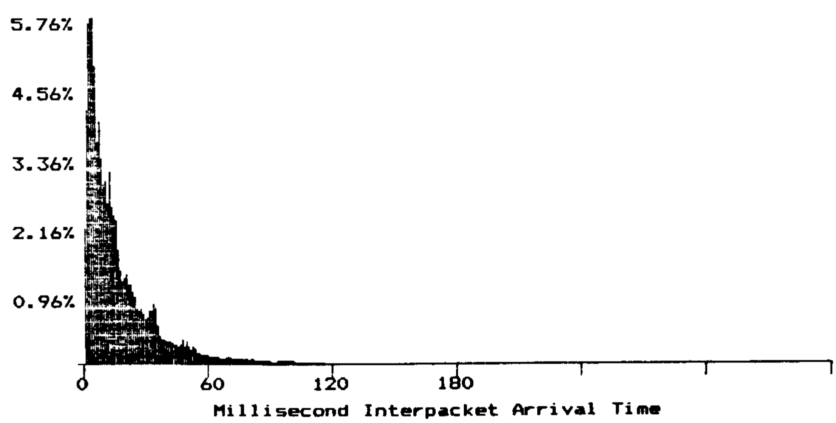
ITC Token Ring 2



Backbone Ethernet

A PC, rather than the AT, was used to monitor this nework. The PC lacks a unique high speed counter to collect interpacket arrival times.

ITC Ethernet



Appendix B

IP Traffic Patterns
Heading, List by Machine, List by Connection
Sorted by highest byte count/first 10 entries

Campus Backbone Ethernet
Ethernet IP Address Traffic Capture
Wednesday 05/07/1986

Start time 00:00:05 End time 07:47:22
Elapse time 07:47:17
Number of packets missed because the tables were full was 0
Number of bytes missed because the tables were full was 0
Number of non-IP packets was 587377
Number of non-IP bytes was 61624280
Elastic buffer full count = 12
Number of connections monitored = 1649
The number of machines monitored was 268.
The total number of bytes monitored was 756722078.
The total number of packets monitored was 1695029.
Percent of bytes missed because the tables were full was 00%.
The total number of bytes on the network was 818346358.
The total number of packets on the network was 2282406.
Average utilization for this run was 2.34 %

Machine	Packets	Bytes	# of connections	% Bytes
cmu-4	843110	515037472	12	62.94 %
vice3	469385	255817539	254	31.26 %
vice2	387800	193149370	310	23.60 %
vice4	362306	164961702	336	20.16 %
cluster1	140720	88353791	20	10.80 %
vice5	153192	74100553	316	9.05 %
scranton	48229	29095334	12	3.56 %
vice6	15340	10180546	2	1.24 %
apollo	29877	8191896	9	1.00 %
larimer	9326	7652763	6	0.94 %

Source	Destination	Packets	Bytes	%Bytes
vice3	cmu-4	228048	218105767	26.65 %
vice2	cmu-4	151840	143623652	17.55 %
vice4	cmu-4	132070	120461849	14.72 %
cluster1	scranton	22877	15057382	1.84 %
scranton	cluster1	22936	13725640	1.68 %
vice5	cmu-4	13176	12889311	1.58 %
cluster1	vice5	13397	12138062	1.48 %
cluster1	vice3	11429	9561810	1.17 %
cluster1	vice2	11038	9397900	1.15 %
cluster1	vice4	11563	9383013	1.15 %

Campus Backbone Ethernet
Ethernet IP Address Traffic Capture
Wednesday 05/07/1986

Start time 07:59:20 End time 17:00:02
Elapse time 09:00:42
Number of packets missed because the tables were full was 351014
Number of bytes missed because the tables were full was 64443224
Number of non-IP packets was 1206074
Number of non-IP bytes was 121279191
Elastic buffer full count = 0
Number of connections monitored = 1792
The number of machines monitored was 292.
The total number of bytes monitored was 710484747.
The total number of packets monitored was 1900231.
Percent of bytes missed because the tables were full was 09%.
The total number of bytes on the network was 896207162.
The total number of packets on the network was 3457319.
Average utilization for this run was 1.99 %

Machine	Packets	Bytes	# of connections	% Bytes
vice5	358092	224373417	330	25.04 %
vice2	407379	172889802	329	19.29 %
vice4	321335	124241749	342	13.86 %
cluster1	163822	99337309	22	11.08 %
vice3	219828	87915088	270	9.81 %
coraopolis	53240	44930913	6	5.01 %
scranton	61055	33670785	22	3.76 %
apollo	65481	23703013	13	2.64 %
federal	69694	12101845	10	1.35 %
norristown	68571	11568294	14	1.29 %

Source	Destination	Packets	Bytes	%Bytes
coraopolis	vice4	22398	23176490	2.59 %
cluster1	scranton	26154	16581152	1.85 %
scranton	cluster1	26327	15413082	1.72 %
cluster1	vice5	16610	14401214	1.61 %
cluster1	vice2	13853	11612136	1.30 %
cluster1	vice4	14557	11310306	1.26 %
cluster1	vice3	13634	11255480	1.26 %
vice5	apollo	8897	10870274	1.21 %
coraopolis	vice5	9291	10052725	1.12 %
millvale	tech11	10405	7797415	0.87 %

Campus Backbone Ethernet
Ethernet IP Address Traffic Capture
Wednesday 05/07/1986

Start time 17:00:13 End time 23:59:50
Elapse time 06:59:37
Number of packets missed because the tables were full was 161822
Number of bytes missed because the tables were full was 17081942
Number of non-IP packets was 626098
Number of non-IP bytes was 63593786
Elastic buffer full count = 61
Number of connections monitored = 1792
The number of machines monitored was 288.
The total number of bytes monitored was 387523790.
The total number of packets monitored was 1358741.
Percent of bytes missed because the tables were full was 04%.
The total number of bytes on the network was 468199518.
The total number of packets on the network was 2146661.
Average utilization for this run was 1.49 %

Machine	Packets	Bytes	# of connections	% Bytes
vice2	240452	101677577	327	21.72 %
vice5	169075	86605413	324	18.50 %
cluster1	123354	76792158	22	16.40 %
vice4	180866	63581023	340	13.58 %
vice3	122775	42769277	269	9.13 %
scranton	42267	25399832	13	5.43 %
media	25201	13224622	12	2.82 %
mercer	117463	12821158	20	2.74 %
allisonpark	18534	11794399	10	2.52 %
federal	147704	11058652	12	2.36 %

Source	Destination	Packets	Bytes	%Bytes
cluster1	scranton	19862	12847108	2.74 %
scranton	cluster1	19937	11770510	2.51 %
cluster1	vice5	11897	10693830	2.28 %
media	vice2	11411	9029090	1.93 %
cluster1	vice3	9903	8483876	1.81 %
cluster1	vice2	9637	8131745	1.74 %
cluster1	vice4	9981	8044628	1.72 %
cluster1	vice6	8450	7867954	1.68 %
cmu-4	vice4	8597	6661158	1.42 %
vice5	bedford	4373	5101466	1.09 %

Campus Backbone Ethernet
Ethernet IP Address Traffic Capture
Thursday 05/08/1986

Start time 00:00:05 End time 08:00:41
Elapse time 08:00:36
Number of packets missed because the tables were full was 0
Number of bytes missed because the tables were full was 0
Number of non-IP packets was 528560
Number of non-IP bytes was 57272827
Elastic buffer full count = 7
Number of connections monitored = 1723
The number of machines monitored was 275.
The total number of bytes monitored was 435017460.
The total number of packets monitored was 1232088.
Percent of bytes missed because the tables were full was 00%.
The total number of bytes on the network was 492290287.
The total number of packets on the network was 1760648.
Average utilization for this run was 1.37 %

Machine	Packets	Bytes	# of connections	% Bytes
cmu-4	303802	172078067	12	34.95 %
vice5	225740	120877478	320	24.55 %
vice3	209431	93060977	274	18.90 %
cluster1	140758	88612485	18	18.00 %
vice2	204669	76937359	316	15.63 %
vice4	193830	70367333	338	14.29 %
scranton	47345	29079294	12	5.91 %
buenavista	17097	12299549	6	2.50 %
vice6	16461	10750590	4	2.18 %
jefferson	16469	9762616	8	1.98 %

Source	Destination	Packets	Bytes	%Bytes
vice3	cmu-4	62926	56151967	11.41 %
vice5	cmu-4	47443	46316496	9.41 %
vice2	cmu-4	36202	31196078	6.34 %
vice4	cmu-4	37501	30361946	6.17 %
cluster1	scranton	22852	15079896	3.06 %
scranton	cluster1	22918	13833324	2.81 %
cluster1	vice5	13430	12124675	2.46 %
cluster1	vice2	11207	9650848	1.96 %
cluster1	vice6	10127	9493434	1.93 %
cluster1	vice4	11382	9151926	1.86 %

Campus Backbone Ethernet
Ethernet IP Address Traffic Capture
Thursday 05/08/1986

Start time 08:00:48 End time 17:08:09
Elapse time 09:07:21
Number of packets missed because the tables were full was 441543
Number of bytes missed because the tables were full was 79282325
Number of non-IP packets was 951902
Number of non-IP bytes was 98804657
Elastic buffer full count = 46
Number of connections monitored = 1792
The number of machines monitored was 288.
The total number of bytes monitored was 749421067.
The total number of packets monitored was 1876146.
Percent of bytes missed because the tables were full was 10%.
The total number of bytes on the network was 927508049.
The total number of packets on the network was 3269591.
Average utilization for this run was 2.26 %

Machine	Packets	Bytes	# of connections	% Bytes
vice5	365742	226454086	321	24.42 %
vice2	443129	207499584	332	22.37 %
vice3	257406	116304553	284	12.54 %
cluster1	172507	99762827	22	10.76 %
vice4	230750	80410185	344	8.67 %
scranton	66391	30642942	19	3.30 %
volstag	58716	30486288	20	3.29 %
glenfield	39780	30155644	8	3.25 %
glassport	41332	24623516	12	2.65 %
hickman	44378	24239404	8	2.61 %

Source	Destination	Packets	Bytes	%Bytes
glenfield	vice3	18769	19969218	2.15 %
glassport	vice2	22999	19948654	2.15 %
cluster1	volstag	26675	16703826	1.80 %
scranton	cluster1	25334	15047168	1.62 %
cluster1	scranton	24856	13911156	1.50 %
hickman	vice3	13338	13040624	1.41 %
volstag	cluster1	25830	12961912	1.40 %
cluster1	vice5	9601	8106290	0.87 %
vice5	apollo	6805	8088278	0.87 %
ishmael	vice3	10674	7589175	0.82 %

Campus Backbone Ethernet
Ethernet IP Address Traffic Capture
Thursday 05/08/1986

Start time 17:08:16 End time 23:59:50
Elapse time 06:51:34
Number of packets missed because the tables were full was 83929
Number of bytes missed because the tables were full was 10160546
Number of non-IP packets was 632422
Number of non-IP bytes was 65809618
Elastic buffer full count = 10
Number of connections monitored = 1792
The number of machines monitored was 287.
The total number of bytes monitored was 336902420.
The total number of packets monitored was 952204.
Percent of bytes missed because the tables were full was 03%.
The total number of bytes on the network was 412872584.
The total number of packets on the network was 1668555.
Average utilization for this run was 1.34 %

Machine	Packets	Bytes	# of connections	% Bytes
cluster1	168009	100308295	28	24.30 %
vice2	201730	75414897	334	18.27 %
vice3	154429	66477880	268	16.10 %
vice5	149104	64379821	322	15.59 %
vice4	137290	45396812	334	11.00 %
volstag	45846	24693352	20	5.98 %
scranton	40137	23062615	14	5.59 %
ishmael	26007	15172026	8	3.67 %
allisonpark	28426	12483346	34	3.02 %
wright	41761	9097354	6	2.20 %

Source	Destination	Packets	Bytes	%Bytes
cluster1	volstag	21225	13863354	3.36 %
scranton	cluster1	19307	11804298	2.86 %
cluster1	scranton	19087	10995606	2.66 %
cluster1	vice5	12253	10680232	2.59 %
volstag	cluster1	20359	10313490	2.50 %
ishmael	vice3	11477	9905731	2.40 %
cluster1	vice4	9985	8077178	1.96 %
cluster1	vice2	9708	7923132	1.92 %
cluster1	vice3	10066	7707120	1.87 %
cluster1	vice6	8007	7373818	1.79 %

ITC Ethernet
Ethernet IP Address Traffic Capture
Monday 05/12/1986

Start time 00:00:05 End time 08:00:02
Elapse time 07:59:57
Number of packets missed because the tables were full was 0
Number of bytes missed because the tables were full was 0
Number of non-IP packets was 14130
Number of non-IP bytes was 847816
Elastic buffer full count = 11
Number of connections monitored = 730
The number of machines monitored was 107.
The total number of bytes monitored was 305979601.
The total number of packets monitored was 778859.
Percent of bytes missed because the tables were full was 00%.
The total number of bytes on the network was 306827417.
The total number of packets on the network was 792989.
Average utilization for this run was 0.76 %

Machine	Packets	Bytes	# of connections	% Bytes
cluster1	274807	162764947	49	53.05 %
safe2	145836	75850642	133	24.72 %
maytag	122520	67098406	8	21.87 %
safe1	194371	53263867	132	17.36 %
bowerhill	72189	42484101	18	13.85 %
moon	59571	36206704	10	11.80 %
scranton	49639	31171466	2	10.16 %
vice5	35709	12561560	106	4.09 %
vice2	49990	12122569	101	3.95 %
apollo	40389	11852332	14	3.86 %

Source	Destination	Packets	Bytes	%Bytes
safe2	maytag	63160	61845331	20.16 %
cluster1	bowerhill	33788	22921332	7.47 %
bowerhill	cluster1	34135	18612610	6.07 %
cluster1	moon	28171	18138978	5.91 %
moon	cluster1	28285	17302198	5.64 %
cluster1	scranton	24720	15918224	5.19 %
scranton	cluster1	24919	15253242	4.97 %
cluster1	vice5	7688	6487568	2.11 %
cluster1	vice2	6915	5333396	1.74 %
cluster1	vice3	6547	5070916	1.65 %

ITC Ethernet
Ethernet IP Address Traffic Capture
Monday 05/12/1986

Start time 07:59:51 End time 17:02:52
Elapse time 09:03:01
Number of packets missed because the tables were full was 0
Number of bytes missed because the tables were full was 0
Number of non-IP packets was 24533
Number of non-IP bytes was 1510948
Elastic buffer full count = 63
Number of connections monitored = 1374
The number of machines monitored was 254.
The total number of bytes monitored was 935831463.
The total number of packets monitored was 1919066.
Percent of bytes missed because the tables were full was 00%.
The total number of bytes on the network was 937342411.
The total number of packets on the network was 1943599.
Average utilization for this run was 2.07 %

Machine	Packets	Bytes	# of connections	% Bytes
cluster1	483656	280387721	133	29.91 %
safe2	350764	210408395	149	22.45 %
vice5	258065	190228470	121	20.29 %
safe1	336779	131463008	151	14.03 %
vice2	188586	83134400	125	8.87 %
moon	119279	59465165	15	6.34 %
vice4	114861	52580568	135	5.61 %
vice3	84689	51555850	93	5.50 %
bowerhill	72167	40882032	21	4.36 %
coraopolis	62627	38971269	36	4.16 %

Source	Destination	Packets	Bytes	%Bytes
cluster1	bowerhill	34340	21538876	2.30 %
mooncrest	safe2	17383	19302666	2.06 %
bowerhill	cluster1	35096	18904992	2.02 %
pitcairn	safe2	19982	17444608	1.86 %
coraopolis	vice5	13286	17212598	1.84 %
cluster1	vice5	19734	17045680	1.82 %
cluster1	vice0	16886	16273050	1.74 %
cluster1	safe0	16287	16192044	1.73 %
scranton	cluster1	26596	15554976	1.66 %
cluster1	scranton	26400	15549848	1.66 %

ITC Ethernet
Ethernet IP Address Traffic Capture
Monday 05/12/1986

Start time 17:00:00 End time 00:00:00
Elapse time 7:00:00
Number of packets missed because the tables were full was 0
Number of bytes missed because the tables were full was 0
Number of non-IP packets was 11949
Number of non-IP bytes was 717128
Elastic buffer full count = 0
Number of connections monitored = 889
The number of machines monitored was 135.
The total number of bytes monitored was 458890522.
The total number of packets monitored was 921755.
Percent of bytes missed because the tables were full was 00%.
The total number of bytes on the network was 459607650.
The total number of packets on the network was 933704.
Average utilization for this run was 1.45 %

Machine	Packets	Bytes	# of connections	% Bytes
cluster1	258181	158702765	59	34.53 %
safe2	197106	107142051	142	23.31 %
cheswick	111813	95311731	16	20.74 %
presto	100866	87268515	14	18.99 %
safe1	137354	49914079	139	10.86 %
vice5	73122	44034184	115	9.58 %
vice3	56465	38484256	74	8.37 %
bowerhill	60854	35638234	18	7.75 %
scranton	43381	26686562	2	5.81 %
duquesne	40104	25915996	23	5.64 %

Source	Destination	Packets	Bytes	%Bytes
cheswick	presto	51918	52404423	11.40 %
presto	cheswick	31847	22390692	4.87 %
cluster1	bowerhill	29373	19657438	4.28 %
bowerhill	cluster1	29670	15743100	3.43 %
cheswick	safe2	12873	13830675	3.01 %
cluster1	scranton	21611	13696074	2.98 %
scranton	cluster1	21770	12990488	2.83 %
duquesne	vice3	9398	11871113	2.58 %
cluster1	vice5	12458	11168433	2.43 %
cluster1	safe2	11999	10442854	2.27 %

ITC Ethernet
Ethernet IP Address Traffic Capture
Tuesday 05/13/1986

Start time 00:00:05 End time 08:11:35
Elapse time 08:11:30
Number of packets missed because the tables were full was 0
Number of bytes missed because the tables were full was 0
Number of non-IP packets was 23467
Number of non-IP bytes was 1408156
Elastic buffer full count = 4
Number of connections monitored = 755
The number of machines monitored was 101.
The total number of bytes monitored was 887126132.
The total number of packets monitored was 1564395.
Percent of bytes missed because the tables were full was 00%.
The total number of bytes on the network was 888534288.
The total number of packets on the network was 1587862.
Average utilization for this run was 2.41 %

Machine	Packets	Bytes	# of connections	% Bytes
maytag	995091	629980263	26	70.90 %
safe1	728158	435947445	136	49.06 %
safe2	442875	269775695	132	30.36 %
cluster1	299653	184105701	41	20.72 %
bowerhill	71660	42373863	16	4.77 %
scranton	51196	31838376	2	3.58 %
vice5	48804	21220214	108	2.39 %
vice4	54585	19060860	121	2.15 %
vice2	53516	17162197	102	1.93 %
vice3	40055	15661278	72	1.76 %

Source	Destination	Packets	Bytes	%Bytes
safe1	maytag	397130	391546290	44.07 %
safe2	maytag	219754	212394687	23.90 %
cluster1	bowerhill	34449	23217090	2.61 %
bowerhill	cluster1	34842	18833732	2.12 %
cluster1	scranton	25498	16331564	1.84 %
scranton	cluster1	25698	15506812	1.75 %
maytag	safe1	229359	14419904	1.62 %
safe2	cheswick	10379	12295584	1.38 %
cluster1	vice5	13612	12269653	1.38 %
cluster1	safe1	12386	10739523	1.21 %

ITC Ethernet
Ethernet IP Address Traffic Capture
Tuesday 05/13/1986

Start time 08:12:13 End time 17:08:00
Elapse time 08:55:47
Number of packets missed because the tables were full was 0
Number of bytes missed because the tables were full was 0
Number of non-IP packets was 31066
Number of non-IP bytes was 1865000
Elastic buffer full count = 1570
Number of connections monitored = 1558
The number of machines monitored was 258.
The total number of bytes monitored was 734699307.
The total number of packets monitored was 1503488.
Percent of bytes missed because the tables were full was 00%.
The total number of bytes on the network was 736564307.
The total number of packets on the network was 1534554.
Average utilization for this run was 1.65 %

Machine	Packets	Bytes	# of connections	% Bytes
cluster1	407503	236941578	113	32.17 %
safe2	285110	164570138	146	22.34 %
vice5	195150	140006548	124	19.01 %
safe1	230633	93724695	147	12.72 %
vice2	187754	76821338	124	10.43 %
vice4	113824	55890901	134	7.59 %
whitaker	67059	33223481	16	4.51 %
volstag	57803	31799651	2	4.32 %
mooncrest	40778	29920117	19	4.06 %
scranton	50559	29320855	4	3.98 %

Source	Destination	Packets	Bytes	%Bytes
cluster1	volstag	29944	19379724	2.63 %
mooncrest	safe2	14363	16618740	2.26 %
scranton	cluster1	25380	15054124	2.04 %
cluster1	vice5	16482	14809865	2.01 %
cluster1	scranton	25176	14266464	1.94 %
cluster1	safe2	15306	13021230	1.77 %
cluster1	vice2	16327	12917362	1.75 %
cluster1	bowerhill	20926	12543492	1.70 %
volstag	cluster1	27859	12419927	1.69 %
cluster1	vice3	14023	11946300	1.62 %

ITC Ethernet
Ethernet IP Address Traffic Capture
Tuesday 05/13/1986

Start time 17:08:07 End time 23:59:50
Elapse time 06:51:43
Number of packets missed because the tables were full was 0
Number of bytes missed because the tables were full was 0
Number of non-IP packets was 11053
Number of non-IP bytes was 663296
Elastic buffer full count = 0
Number of connections monitored = 937
The number of machines monitored was 159.
The total number of bytes monitored was 395777681.
The total number of packets monitored was 841689.
Percent of bytes missed because the tables were full was 00%.
The total number of bytes on the network was 396440977.
The total number of packets on the network was 852742.
Average utilization for this run was 1.28 %

Machine	Packets	Bytes	# of connections	% Bytes
cluster1	281403	174011070	68	43.89 %
safe1	184680	84156057	139	21.23 %
vice5	117344	69192990	119	17.45 %
safe2	119970	60266051	139	15.20 %
moon	69183	42910620	12	10.82 %
scranton	58202	36659623	4	9.25 %
vice4	88972	29900432	120	7.54 %
pitcairn	102254	29854506	41	7.53 %
freeport	32210	25085422	12	6.33 %
buenavista	43814	24020062	18	6.06 %

Source	Destination	Packets	Bytes	%Bytes
cluster1	moon	33010	22162896	5.59 %
moon	cluster1	33052	19998728	5.04 %
cluster1	scranton	28973	19229086	4.85 %
scranton	cluster1	29055	17419738	4.39 %
keown	safe1	12713	17111382	4.32 %
freeport	safe1	14367	15517638	3.91 %
cluster1	vice5	12581	11477639	2.90 %
mooncrest	safe2	9549	11137367	2.81 %
whiteoak	vice5	11378	11014050	2.78 %
cluster1	safe2	9638	8654379	2.18 %

Appendix C

File Server Controller

MONDAY May 12, 1986
8 am to 5 pm
ITC Ethernet

15 machines (of 254) contributing most to network traffic.

IP Address	Packets	Bytes	# of connections	% Bytes
cluster1	483656	280387721	133	29.91 %
safe2	350764	210408395	149	22.45 %
vice5	258065	190228470	121	20.29 %
safe1	336779	131463008	151	14.03 %
vice2	188586	83134400	125	8.87 %
moon	119279	59465165	15	6.34 %
vice4	114861	52580568	135	5.61 %
vice3	84689	51555850	93	5.50 %
bowerhill	72167	40882032	21	4.36 %
coraopolis	62627	38971269	36	4.16 %
mooncrest	54004	36850544	18	3.93 %
whitaker	69568	33446643	14	3.57 %
pitcairn	65582	33406378	23	3.56 %
buenavista	60496	31498147	27	3.36 %
scranton	53452	31133464	6	3.32 %

20 connections (of 1374) contributing most to network traffic.

IP Source	IP Destination	Packets	Bytes	%Bytes
cluster1	bowerhill	34340	21538876	2.30 %
mooncrest	safe2	17383	19302666	2.06 %
bowerhill	cluster1	35096	18904992	2.02 %
pitcairn	safe2	19982	17444608	1.86 %
coraopolis	vice5	13286	17212598	1.84 %
cluster1	vice5	19734	17045680	1.82 %
cluster1	vice0	16886	16273050	1.74 %
cluster1	safe0	16287	16192044	1.73 %
scranton	cluster1	26596	15554976	1.66 %
cluster1	scranton	26400	15549848	1.66 %
buenavista	safe2	17694	14869480	1.59 %
cluster1	safe2	20544	14633695	1.56 %
cluster1	moon	25973	14593134	1.56 %
cluster1	vice3	17054	14395499	1.54 %
cluster1	vice2	17519	14172012	1.51 %
moon	cluster1	26227	14057740	1.50 %
cluster1	vice4	16978	13535363	1.44 %
cluster1	vice6	14034	13107653	1.40 %
moon	whitaker	21347	12179252	1.30 %
whitaker	safe2	10233	11114435	1.19 %

Cluster1 single direction communication
25 most active out of 133

IP Source	IP Destination	Packets	Bytes	%Bytes
cluster1	bowerhill	34340	21538876	2.30 %
bowerhill	cluster1	35096	18904992	2.02 %
cluster1	vice5	19734	17045680	1.82 %
cluster1	vice0	16886	16273050	1.74 %
cluster1	safe0	16287	16192044	1.73 %
scranton	cluster1	26596	15554976	1.66 %
cluster1	scranton	26400	15549848	1.66 %
cluster1	safe2	20544	14633695	1.56 %
cluster1	moon	25973	14593134	1.56 %
cluster1	vice3	17054	14395499	1.54 %
cluster1	vice2	17519	14172012	1.51 %
moon	cluster1	26227	14057740	1.50 %
cluster1	vice4	16978	13535363	1.44 %
cluster1	vice6	14034	13107653	1.40 %
cluster1	safe1	13972	11043331	1.18 %
safe2	cluster1	16954	7869779	0.84 %
cluster1	volstag	12005	7496778	0.80 %
volstag	cluster1	11622	5289839	0.56 %
vice5	cluster1	14377	3822860	0.41 %
vice4	cluster1	10944	3782075	0.40 %
vice3	cluster1	10427	3229320	0.34 %
vice2	cluster1	10932	2872947	0.31 %
dallas	cluster1	6294	2739319	0.29 %
cluster1	dallas	6039	2632516	0.28 %
cluster1	maytag	2651	1911748	0.20 %

Appendix D

Utilization Monitor Data Format

The machines used to collect network data are the PC products from IBM. These machines use the Intel CPU architecture which give us the attribute of byte reversal. We don't have to worry about confusing single byte pieces of information. Two byte counters are placed in memory with the least significant byte first and four byte counters are the same with the least significant two bytes appearing before the most significant two bytes. (Example: 12345678 hex would appear in consecutive locations of memory as 34 12 78 56.) The format for the network data is as follows:

8-byte Header

bytes	description
1,0	year
2	day
3	month
4	day of the week (0 = Sun, 6 = Sat)
5,6,7	reserved

360 entries for each 4 minute period of the day
9 bytes for each entry = 3,240 bytes
First entry

# of bytes	description
4	Number of packets
4	Number of bytes
1	reserved

360 entries for the size of packets
4 bytes for each entry = 1440 bytes
Entries represent 5 byte increments
First entry

# of bytes	description
4	# of packets between 1 and 5 bytes in length

200 entries for interpacket arrival time
4 bytes for each entry = 800 bytes
Entries represent 1 millisecond increments

# of bytes	description
4	Number of packets with 0 millisecond IPA time
4	Number of packets with 1 millisecond IPA time
4	Number of packets with 199 millisecond IPA time

Total number of bytes in the data set is 5488.

Appendix E

IP monitor data formats

Primary Directory (stored results)

Size = 57,344 bytes, Header and each entry = 32 bytes, 1,792 total entries

Header

Bytes	
0 - 1	Year
2	Day
3	Month
4	Day of the week
5	Start Time Hour
6 - 7	Start Time Minutes * 18.2
8	End Time Hour
9 -10	End Time Minutes * 18.2
11	Reserved
12-15	Non IP Packet Count (Least significant byte first)
16-19	Non IP Byte Count
20-23	Packet Count not Monitored (Primary Directory Full)
24-27	Byte Count not Monitored (Primary Directory Full)
28-31	Elastic Buffer Full Count

Data (first entry starts at offset 32)

Bytes	
0 - 3	IP Source Address
4 - 7	IP Destination Address
8 -11	Number of Packets
12-15	Number of Bytes
16-29	Reserved
30-31	Chain Pointer (0 = End of Chain)

Elastic Buffer (internal data structure)

Size = 1024 bytes, Each entry is 16 bytes, 64 total entries

First Entry

Bytes	
0 - 3	Source IP Address
4 - 7	Destination IP Address
8 - 9	Packet Length (MSB: 1 - Valid, 0 - Not Valid)
10-15	Reserved

Hash Table (internal data structure)

Size = 2048 bytes, Each entry is 2 bytes, 1024 total entries

First Entry

Bytes	
0 - 1	Offset to first entry in the chain (0 = Not Used)

References

[1] The Task Force for the Future of Computing
A Newell (Chairman)
The Future of Computing at Carnegie-Mellon University
Available from authors

[2] James H. Morris, Mahadev Satyanarayanan, Michael H. Conner, John H. Howard, David S. H. Rosenthal, and F. Donelson Smith
Andrew: A Distributed Personal Computing Environment
Communications of the ACM, Volume 29 Number 3, 184 - 201, March 1986

[3] Technical Committee Computer Communications of the IEEE Computer Society
Carrier Sense Multiple Access with Collision Detection (CSMA/CD), ANSI/IEEE Std 802.3-1985
The Institute of Electrical and Electronic Engineers, 1985

[4] John Leong
Data Communication at C-MU, Tech. Rep. CMU-ITC-85-043, July 1985
Information Technology Center and Computation Center
Carnegie-Mellon University, Pittsburgh, Pa. 15213

[5] Technical Committee Computer Communications of the IEEE Computer Society
Token Ring Access Method and Physical Layer Specifications, ANSI/IEEE Std 802.5-1985
The Institute of Electrical and Electronic Engineers, 1985

[6] LANalyzer EX 5000E Ethernet Network Analyzer User Manual
Excelan, Inc. 2180 Fortune Drive, San Jose, Ca. 95131

[7] Michael J. West, Mahadev Satyanarayanan
Why Deployed SUNs Should Have Disks, Tech. Rep. CMU-ITC-84-009, July 10, 1984
Information Technology Center
Carnegie-Mellon University, Pittsburgh, Pa., 15213

[8] Mahadev Satyanarayanan, John H. Howard, Alfred Z. Spector, Michael J. West, David Nichols, Bob Sidebotham
The ITC Distributed File System: Principles and Design
In Proceedings of the 10th ACM Symposium on Operating System Principles, Dec. 1985

[9] Mike Accetta
A Network Router
Department of Computer Science
Carnegie-Mellon University, Pittsburgh, Pa., Sept. 1983

[10] Mike Accetta
DARPA Internet Protocol Service on the C-MU Local Area Networks
Department of Computer Science
Carnegie-Mellon University, Pittsburgh, Pa., June 24, 1983