Trends in Wide Area IP Traffic Patterns

A View from Ames Internet Exchange

Sean McCreary (mccreary @ caida.org)
kc claffy (kc @ caida.org)
University of California, San Diego
Cooperative Association for Internet Data Analysis (CAIDA)
U.S.A.

Contents

Abstract

We report results from a longitudinal analysis of the IP traffic workload seen at a single measurement site inside a major Internet traffic exchange point. Using data collected by the NLANR/MOAT Network Analysis Infrastructure (NAI) project [NAI] and analysis software from CAIDA's CoralReef project [CoralReef], we present trends in application usage seen at the NASA Ames Internet Exchange over 10 months, from May 1999 through March 2000. We show changes in the fraction of traffic from streaming media and online gaming, as well as an increase in traffic from new applications such as Napster and IPSEC tunneling. We also show that our data does not indicate any overall change in the TCP/UDP traffic ratio at the Ames Internet Exchange during this period, or significant differences from the analyses by MCI Worldcom and CAIDA in 1998.

Introduction

Over the years there has been a great deal of ‘common wisdom’ developed about the nature of wide area Internet traffic. Unfortunately, these rules of thumb have developed in the absence of observations about the composition of actual traffic carried in the Internet backbone. Many analyses of Internet traffic behavior require accurate knowledge of the traffic characteristics in the backbone today, for purposes ranging from the optimization of future networking equipment to modeling the effects of new protocols on the existing traffic mix. CAIDA aims to fill this gap, supplying accurate information about backbone traffic characteristics to both industry and the academic community.

Other studies [Feldmann98] have used Internet traffic trace data as input for evaluation of specific protocol performance issues, but have not concentrated on characterizing the overall workload contained in the traces. There are also several ongoing projects [Feldman98, AIXstats] that monitor the utilization of network links at our measurement site in terms of the number of packets and bytes transferred over time. However, these monitoring projects do not attempt to provide a finer grained picture of the link utilization in terms of the protocols in use on the links.

Earlier workload analysis studies in the NSFnet backbone [Heimlich89, Claffy93, Merit95] included course-grain estimates of the fraction of traffic due to the most popular applications before the advent of web browsers. This included basic statistics about the prevalence of FTP, e-mail, netnews, telnet, DNS, and a single category for ‘other’ TCP and UDP applications. Several studies detailing the workload presented at the border of large organizations [Caceres89, Caceres91, Paxson94, WISCstats] have included traffic breakdowns by protocol as well. These site-specific studies form a complement to backbone studies, as they can reveal differences in the way different kinds of organizations use the Internet.

Previous studies of backbone traffic [Apisdorf97, Thompson97, claffy98] have analyzed the workload presented at two sites inside the Internet MCI backbone (AS3561), now owned by Cable and Wireless. These studies spanned a relatively short period of time, ranging from a single day to a full week. These short ‘snapshots’ of backbone traffic are not long enough to accurately determine trends in the traffic mix, as we see a large amount of variability on these time scales. In this paper we present an analysis of the workload seen at AIX over a much longer period, spanning more than 10 months.

NLANR/MOAT’s Datacube project [MOAT99] is a framework for storing and analyzing traces collected from a set of Coral monitors at HPC sites. The three dimensions of the ‘cube’ are: data origin (measurement location where the data originated); project name (e.g., analysis method); and data collection date. MOAT makes the public data available on its web server via this DataCube structure, to allow data exploration along each dimension of the cube.

In the next section, we present background information about our data collection site and the tools we used to collect and analyze the data. We then present some sample results from our study, an analysis of the distribution of packet lengths, and some trends in the protocol mix seen at our sampling site. We conclude with a summary of the challenges we face in continuing and extending our measurement program at CAIDA.

Background

The Monitor Site

The traces used for this study were collected from the NASA Ames Internet exchange (AIX) in Mountain View, CA [AIX] as part of an NSF/NASA collaborative effort with NLANR/MOAT. They were collected from one of four (now five) OC-3 ATM links that interconnect AIX and MAE-West in San Jose, CA.

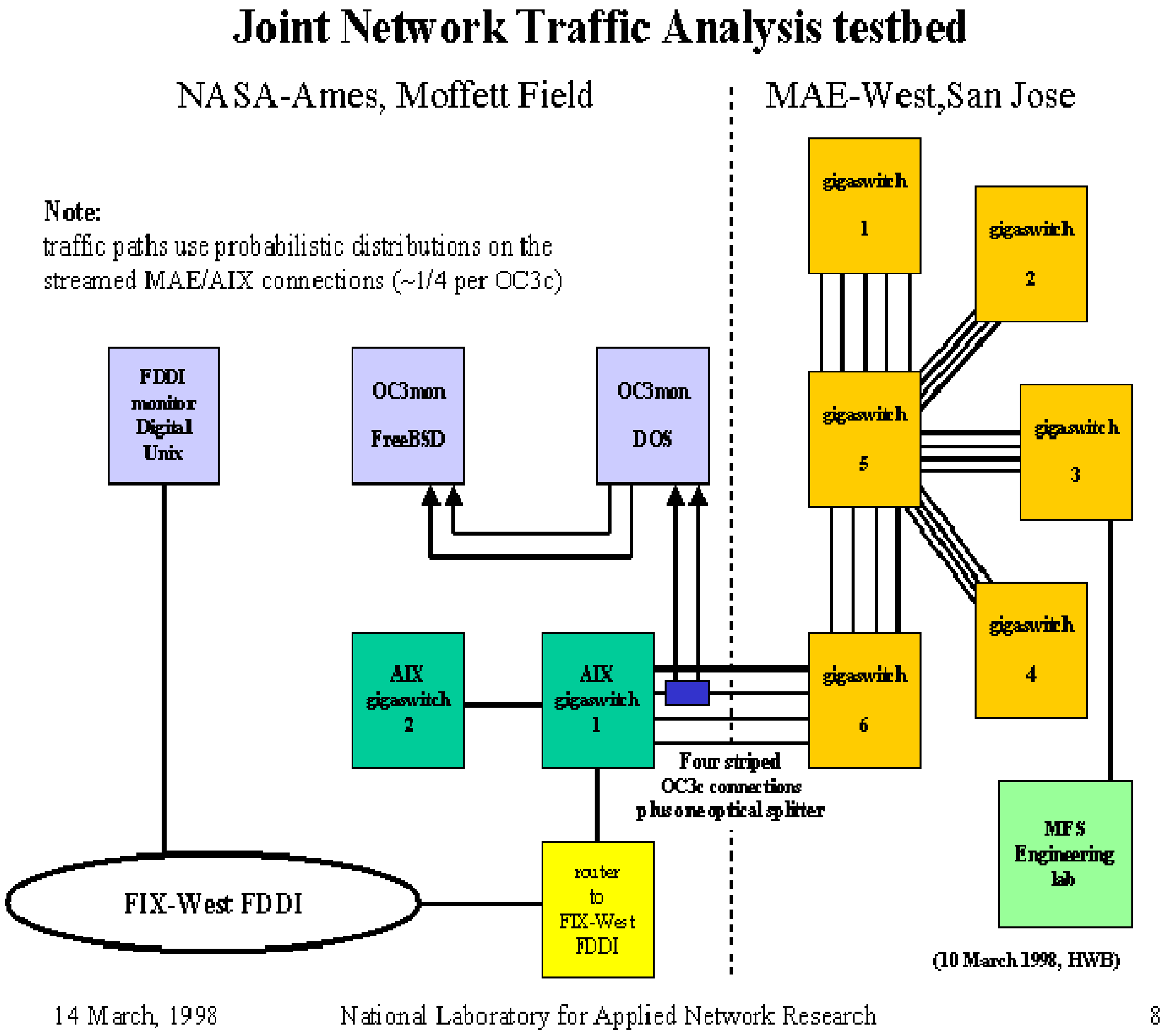

Fig 1: A diagram showing the location of the optical splitter used to collect the data. Note that there are currently five links between NASA-Ames and MAE-West. Thanks to Hans-Werner Braun and NLANR/MOAT for use of this figure.

This group of links form a striped connection between two DEC Gigaswitches, with an aggregate bandwidth of approximately a single OC-12 link. The Gigaswitches use a proprietary scheduling algorithm for sending packets across this link, but each packet is sent across an individual link inside an AAL5 PDU. This means the scheduling inside the Gigaswitches happens at the packet level, since all cells from a PDU are sent over the same link.

Consequently, the data we collect from this site is essentially sub-sampled from the actual data traversing this link using the proprietary scheduling algorithm inside the Gigaswitches. This algorithm is approximately round-robin, but also depends on internal load characteristics in the Gigaswitch switching fabric. However, we know that the distribution of packets among the OC-3 links is not entirely uniform, since measurements of the link utilizations show two of them carry approximately twice the traffic of the other two (measured by byte volume, not packet volume) [Feldman98]. However, we assume that the Gigaswitch scheduling algorithm is independent of the encapsulated protocol, e.g. not dependent upon packet length.

Because of this complex scheduling algorithm we are not able to accurately estimate the number of conversations traversing the monitored links, or the length of these conversations in packets or bytes. Consequently, we only characterize the workload observed at AIX in terms of relative fractions of packets and bytes.

Monitoring Methodology and Tools

The data collection system is essentially similar to the one used in [Thompson97]. A Coral/OC3mon platform was connected to one link in each direction using optical splitters. The traces we studied were collected as part of NLANR/MOAT’s Network Analysis Infrastructure (NAI) project [Braun98]. For each packet that passes the monitor, only the first ATM cell from the AAL5 PDU is captured and written to disk. The first cell contains the first 40 bytes of each packet, which is usually enough to extract the TCP or UDP port numbers from the transport layer headers. However, the monitor does not verify that the entire AAL5 PDU is carried by the link, and so estimates of the data rate carried by the link may be inflated in the presence of cell loss. Six to eight traces were collected each day, usually with a duration of 90 seconds each. The starting time for each trace was set at equal intervals during the 24 hour period, and randomized over a range of an hour at the beginning of each interval.

After collection, the traces are processed to remove any information that might compromise the privacy of the individuals generating the traffic. This processing masks the source and destination IP addresses, and deletes all data from the IP payload except for a TCP or UDP header (if present), or the ICMP or IGMP type and code fields. If the packet carries enough bytes of IP header options, then the TCP or UDP port numbers may not be present in the first cell of the PDU. In this case, we ignore that packet in subsequent application workload analysis. Since the fraction of packets with IP header options is typically less than 0.003%, this doesn’t seriously impact our measurements of the traffic fraction generated by the most popular TCP and UDP applications.

Analysis Methodology and Tools

We used CoralReef [CoralReef] to reduce each raw trace to a set of summary tables that we archived for later analysis. The tables include aggregate numbers such as the number of packets and bytes in the trace as well as distributions of packet lengths and the number of packets and bytes seen for each IP-layer protocol.

For TCP and UDP, we analyze application usage using port address pairs. The packet traces available from the NAI archive [Braun98] only include IP and transport layer headers, so our methodology does not use encapsulated data to identify the application that generated the packets. Traces in the NAI archive have had all payload data removed to protect the privacy of Internet users.

In most cases, we have assumed that packets sent between any port number higher than 1023 and a well-known port number below 1023 are generated by the same protocol (e.g., HTTP on port 80). This matches typical end host behavior, in which clients allocate ephemeral ports from the range 1024 to 32767 [Stevens94].

For some of the protocols, we have condensed ranges of port numbers in both the source and destination fields. For example, the RealAudio category in the UDP table includes all traffic with destination ports between 6970 and 7170 inclusive [RealNetworks]. Unfortunately, this range also includes the ports used by AFS, and so we are potentially confusing an unknown amount of AFS traffic with RealAudio. However, the majority of RealAudio traffic appears on UDP ports 6970, 6971, and 6972, none of which are used by AFS. By only considering traffic on UDP ports from this range that are not used by AFS, the amount of RealAudio traffic can be estimated independently from the amount of AFS traffic that may be present as well.

We are currently investigating better techniques for differentiating RealAudio and AFS traffic using packet size distribution and packet inter arrival patterns, and we hope to be able to conclusively differentiate between the two in the future. A recent analysis of the traffic patterns exhibited by RealAudio traffic [Mena00] has shown several parameters that may be used to differentiate between RealAudio and other protocols. A further study characterizing AFS traffic patterns needs to be undertaken to identify the best metrics to use to separate the two.

For both TCP and UDP traffic, there is a significant fraction of traffic that cannot be mapped to applications using well known port numbers. Many protocols do not depend on well-known port numbers, but either use a well-known service for negotiating the port numbers used by secondary connections, or use arbitrary but fixed port numbers that are not registered with IANA. The most popular application with negotiated port numbers is passive-mode FTP, in which the client sends the port number to use for a data connection over the command channel. There are many other protocols that use similar behavior, such as Napster and Internet telephony applications.

Most online games do not register well-known ports with IANA, but use arbitrary port numbers above 5000. We have collected the port numbers used by several of the popular games and use this information to estimate the fraction of traffic generated by them. Our analysis of online game traffic includes game traffic on the following UDP ports:

Half Life	any to or from 27005	any to or from 27015
Quake 3: Arena	any to or from 27960	
Starcraft	6112 to 6112	
Quake II	any to or from 27901	any to or from 27910
QuakeWorld	any to or from 27500	any to or from 27001
Unreal	any to or from 7777	

Table 1: UDP ports used by Online Games

As is the case with RealAudio and AFS, there are many possibilities for confusion between game traffic and other applications when only port numbers are used to make the classification. We assume that there are no other protocols that preferentially use these same ports, and that applications that ephemerally use these ports contribute equal amounts of traffic across all traffic categories. This assumption carries significant risks, and needs further analysis to fully evaluate its impact on our data.

Results

Packet lengths

The following graphs show the distribution of IP packet sizes seen at AIX. These distributions are built from two approximately one week periods near the beginning and end of our study. They contain contributions from the different workloads carried by the network at different times of day, and so they should represent more of an ‘average’ picture of the packet size distribution than any individual trace. However, no attempt has been made to normalize the contributions of individual traces. The distributions presented here are simply those of the concatenated traces.

Additionally, these distributions have only been plotted for packet sizes less than 1600 bytes. This allows the structure of the distributions to be presented in greater detail, but hides the very small fraction of larger packets that appear in these traces (typically less than 0.005% of packets).

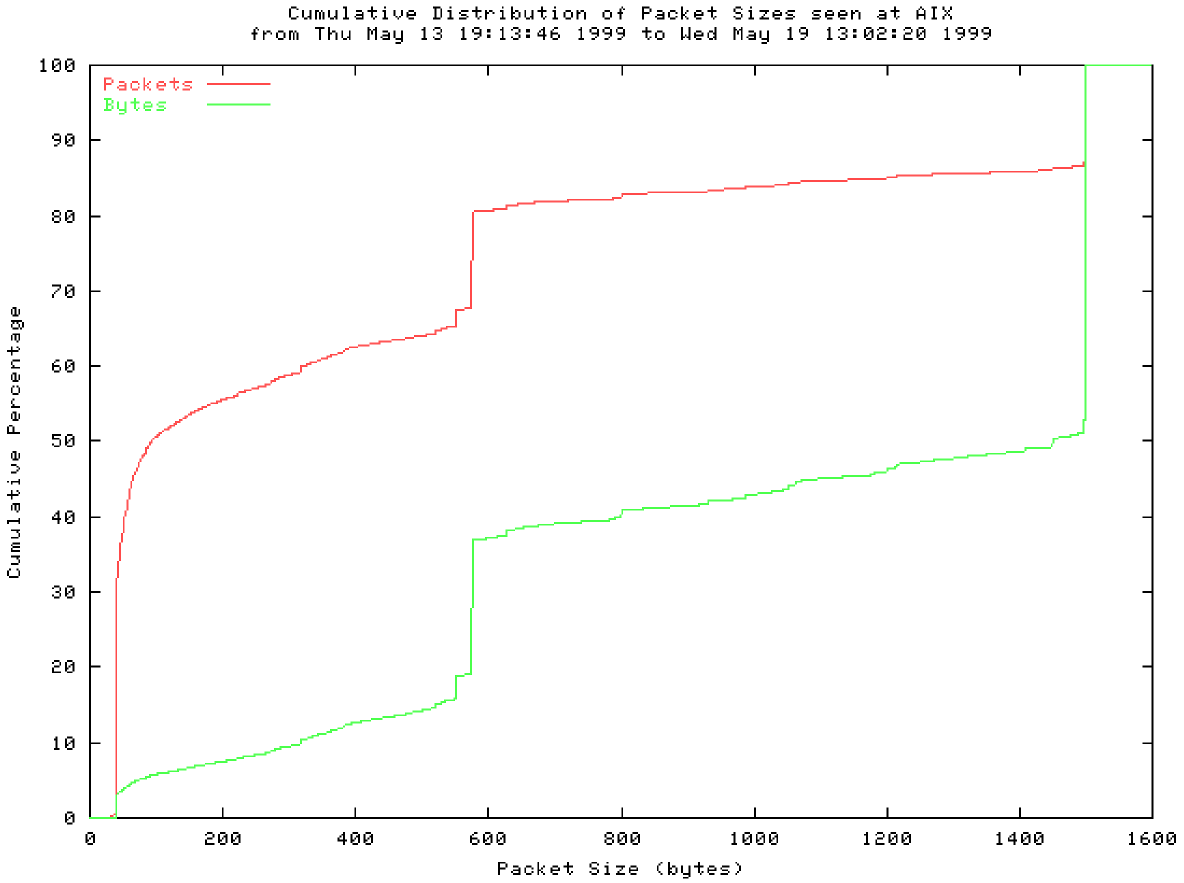

Fig 2: IP packet length distribution from 39 trace files captured between Thursday, May 13th 1999 at 19:14:36 PDT and Wednesday, May 19th 1999 at 13:02:20 PDT, over an interval of almost six days.

Statistics for the underlying packet length distribution:

```
Mean: 413 bytes, Standard Deviation: 509 bytes
Median: 93 bytes, Percentiles: 5th 40 bytes, 25th 40 bytes, 75th 576 bytes, 95th 150
Number of Observations: 127 million packets [127710031 packets]
```

These numbers correspond to the upper curve in the figure above.

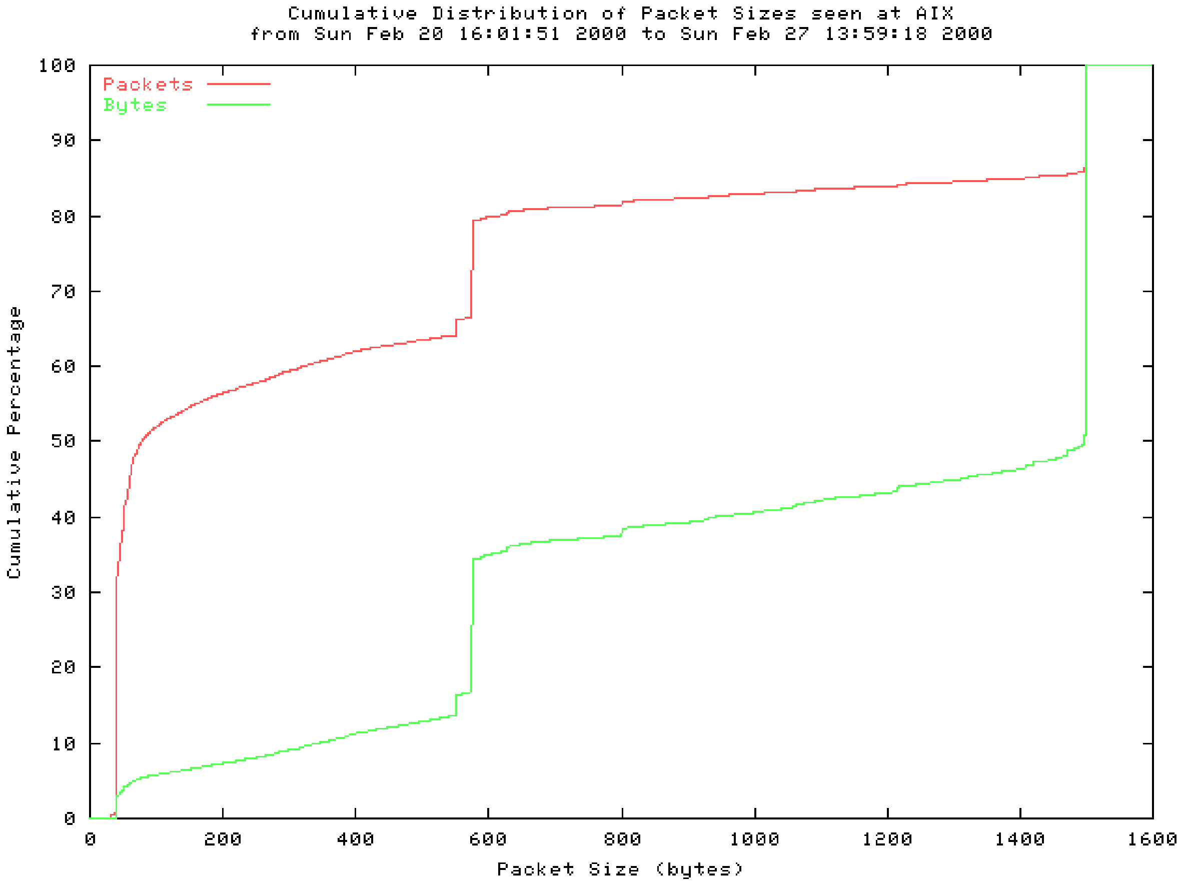

Fig 3: IP packet length distribution from 43 trace files captured between Sunday, February 20th 2000 at 16:01:51 PST and Sunday, February 27th 2000 at 13:59:18 PST, over an interval of almost 7 days.

Statistics for the underlying packet length distribution:

```
Mean: 420 bytes, Standard Deviation: 521 bytes
Median: 78 bytes Percentiles: 5th 40 bytes, 25th 40 bytes, 75th 576 bytes, 95th 1500
Number of Observations: 84 million packets [84415871]
```

These numbers correspond to the upper curve in the figure above.

The primary features of this distribution originate in the way common TCP implementations divide a data stream into packets. Approximately 85% of the traffic in these traces is TCP, and a large proportion of this TCP traffic is generated by bulk transfer applications such as HTTP and FTP. Consequently, the majority of the packets seen are one of three sizes: 40 byte packets (the minimum packet size for TCP) which carry TCP acknowledgments but no payload; 1500 byte packets (the maximum Ethernet payload size) from TCP implementations that use path MTU discovery; and 552 byte and 576 byte packets from TCP implementations that do not use path MTU discovery.

These two distributions are strikingly similar despite the fact that the second is based on data collected more than 9 months after the first. The second distribution has a slightly larger contribution from packets smaller than 100 bytes, but the difference is quite small. The following graph shows how the mean and median values of the packet size distribution vary over the entire duration of our study.

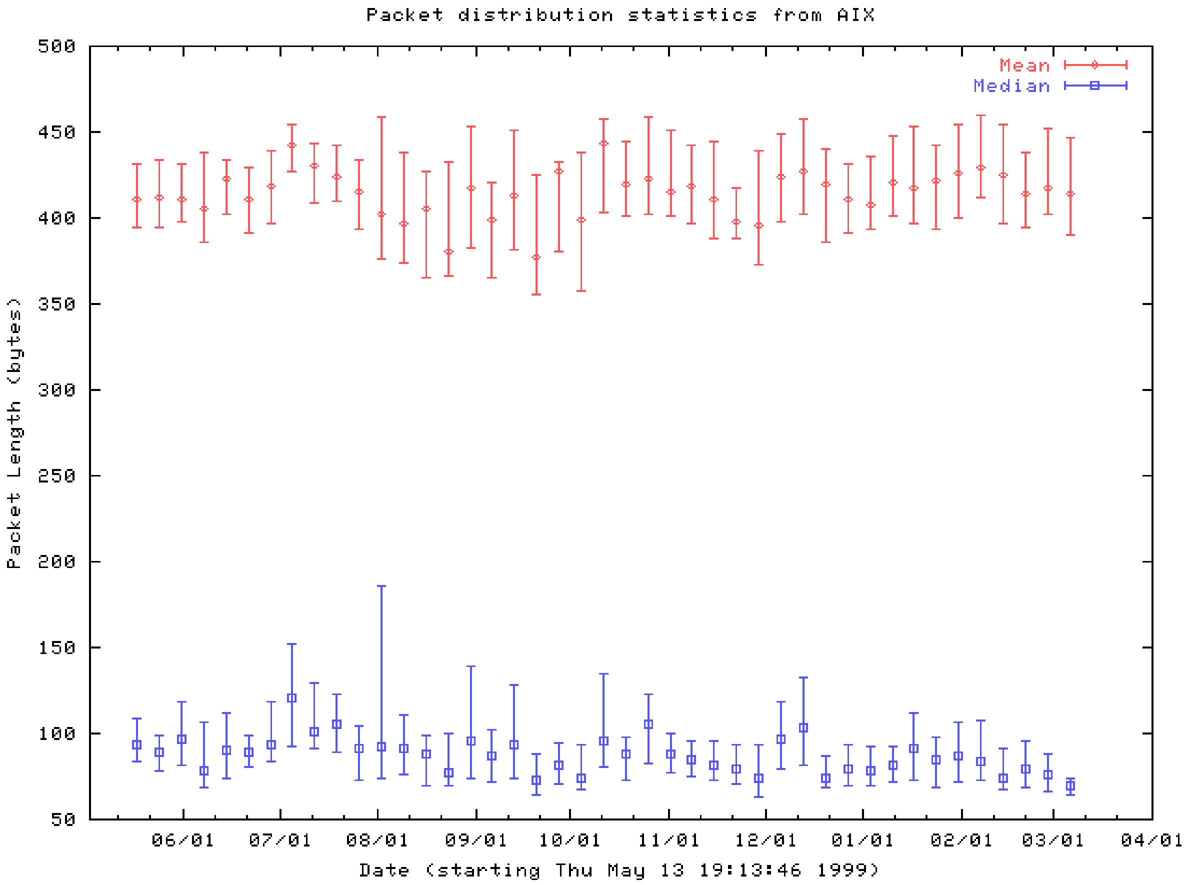

Fig 4: Mean and median packet length values for each packet trace collected between Thursday, May 13th 1999 at 19:14:36 PDT and Sat Mar 11 13:57:38 PST 2000. Values have been binned by week, and the median for each bin is plotted with first and third quartile error bars.

It is not surprising that these parameters do not show any significant long term trend. As long as TCP is the dominant protocol in use in the Internet, the packet length distribution is unlikely to change very much unless the TCP protocol itself changes.

Protocol Mix

Raw Data

In the tables below, we provide some sample data from the month of February, 2000. Each of the 216 traces from this period were concatenated, and the summary information presented below is for all the traces combined.

Total IP Bytes	193692014407
Total IP Packets	451971619
Total Duration of Traces	24345 sec
IP packets with DF set	329241464
Fragments of IP Datagrams	1023206
Fragments of UDP Datagrams	597228
Fragments of TCP Datagrams	9702
IP Packets with options	3213
Non-IP packets	462085

Table 2: Aggregate totals for all traces collected in February, 2000

Table 3 presents the top 10 IP layer protocols seen in these traces. TCP and UDP typically account for almost all of the traffic seen in any trace, with GRE and ICMP as the next two most popular protocols

Protocol	Number	Packets	Bytes	Average Size
TCP	6	374801201	176706563104	471
UDP	17	62456731	9842511709	157
GRE	47	7566415	5272240819	696
ICMP	1	5938044	1350011401	227
ESP	50	517353	197216792	381
IP in IP	4	265103	179257606	676
AH	51	74423	43454671	583
IPIP	94	143502	41707350	290
SKIP	57	117050	41633952	355
IGMP	2	68404	7729038	112

Table 3: Top 10 protocols seen during February, 2000

In the next two tables, we have consolidated the TCP and UDP port address pairs into categories by application. As described previously, we have assumed that traffic between any port number higher than 1023 and a well-known port number below 1023 is exclusively generated by the same protocol (e.g. HTTP on port 80). We denote the condensed set of port numbers in the table with the label ‘0’.

For some of the protocols, we have condensed ranges of port numbers in both the source and destination fields. For example, the RealAudio category in the UDP table includes all traffic with destination ports between 6970 and 7170 inclusive, represented with the label ‘7070’.

Note that a significant portion of both TCP and UDP traffic falls into a category labeled with ‘0’ in both the source and destination fields. This includes all the traffic that was not mapped to a specific protocol using our methodology. This traffic is either generated by protocols that use negotiated port numbers at both ends (e.g., passive-mode FTP), or by new applications that use unregistered fixed ports. We continue to add port utilization profiles for new protocols as we obtain new and updated information.

Protocol	Source	Destination	Packets	Bytes	Average Size
HTTP	80	0	140780543	100044030753	710
	0	0	45319842	17319763013	382
NNTP	0	119	17895481	15992967942	893
HTTP	0	80	94578965	7844163850	82
FTP Data	20	0	6728097	6689611587	994
SMTP	0	25	8878925	6071084052	683
NNTP	119	0	8857217	5399672480	609
HTTP/Web Proxy	8080	0	2331669	2327032104	998
Napster	0	6699	3331109	1838804438	552
HTTPS	443	0	3035809	1535037132	505
Napster	6699	0	3377828	1528188686	452
FTP Data	0	20	5498097	1262294037	229
Napster	6688	0	1230335	935883810	760
	1755	0	1182358	908626624	768
POP3	110	0	1820887	798255125	438
Hotline	5501	0	685536	787122008	1148
RTSP	554	0	754508	616087123	816
Napster	0	6688	1149382	348845629	303
SMTP	25	0	6438672	339788020	52
RealAudio	7070	0	445551	298598442	670
Shoutcast	8000	0	353545	296161291	837
Web Cache	3128	0	325447	280739543	862
HTTPS	0	443	2635048	280418901	106
NetBIOS SSN	139	0	312658	264965212	847
	2189	0	294654	174140223	590

Table 4: Top 25 TCP application categories seen during February, 2000

Protocol	Source	Destination	Packets	Bytes	Average Size
	0	0	15108822	2568130721	169
RealAudio	0	7070	4610070	2029483625	440
DNS	53	53	9290872	1064980650	114
DNS	53	0	3444558	638796849	185
Half Life	27015	27005	2199098	452384485	205
DNS	0	53	5286554	332598249	62
	0	6770	619334	230280312	371
Starcraft	6112	6112	4167625	217783755	52
EverQuest	9001	9000	908432	171755388	189
Half Life	27005	27015	2754416	160806176	58
RealAudio	6970	0	532356	154663054	290
Unreal	7777	0	1109005	141327485	127
EverQuest	9005	9000	777485	138637166	178
Unreal	0	7777	1892613	107613279	56
Quake 3: Arena	27960	27960	784258	80146922	102
Half Life	27015	0	424614	77756002	183
Quake II	27901	27910	946674	58842583	62
Half Life	0	27005	317735	58062692	182
	0	22	50337	45995046	913
	28001	0	255081	44789873	175
NetBIOS NS	137	137	509854	43996075	86
Quake II	27910	27901	232865	43942438	188
	0	371	46531	40574996	871
CU-SeeMe	7648	7648	136843	39681727	289
Quake II	27901	0	601427	37327785	62
Half Life	27005	0	498300	29191062	58

Table 5: Top 25 UDP application categories seen during February, 2000

Long Term Trends

In each of the time series graphs below, we have collected the data values into week-long bins, and we plot only the median and first and third quartiles for each bin. For graphs with more than one data series, we have introduced a slight offset to the bins for each series to prevent overlap.

We present only the fraction of traffic contributed by each application or application group rather than absolute measurements of traffic volume in any category. Shifts in the relative fractions among multiple protocols or applications over time represent changes in how the network is used, rather than how busy our measured link is at any given time. However, during the period of this study, the monitored link had a median utilization of approximately 85 Mb/s.

Median and quartile values have been calculated using the methodology described in [RFC2330]. Specifically, the quartile values are actual data points and not interpolated values, and the median is either an actual data point or the average of the two middle values. Each weekly bin typically contains 40-50 observations.

The first graph shows the fraction of packets due to TCP and UDP seen at AIX. The graph does not show any clear long term shifts in the balance between these two dominant transport layer protocols. Despite the increase in the number of UDP applications in recent years, growth in the total amount of UDP traffic is offset by growth in TCP traffic as well.

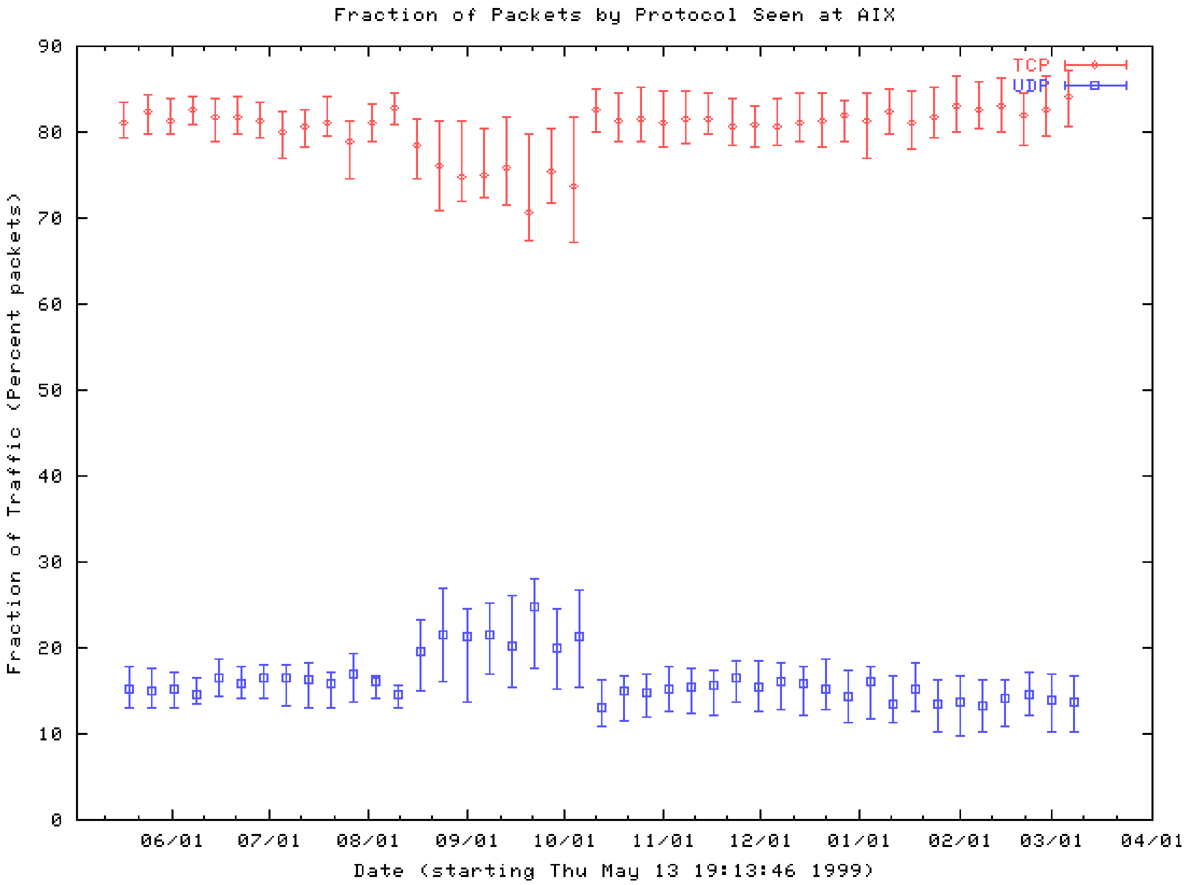

Figure 5: Fraction of TCP and UDP packets seen at AIX. Traces are collected into weekly bins, and the median and first and third quartiles for each bin are plotted.

This next graph shows the fraction of IPSEC traffic seen at AIX, including both authentication header (AH) and encapsulating security payload (ESP) traffic. The graph shows an increase of almost an order of magnitude during the first 5 months of our study, but then levels off or even declines slightly. This suggests that after an initial period of serious interest, IPSEC traffic has stopped growing faster than non-IPSEC traffic.

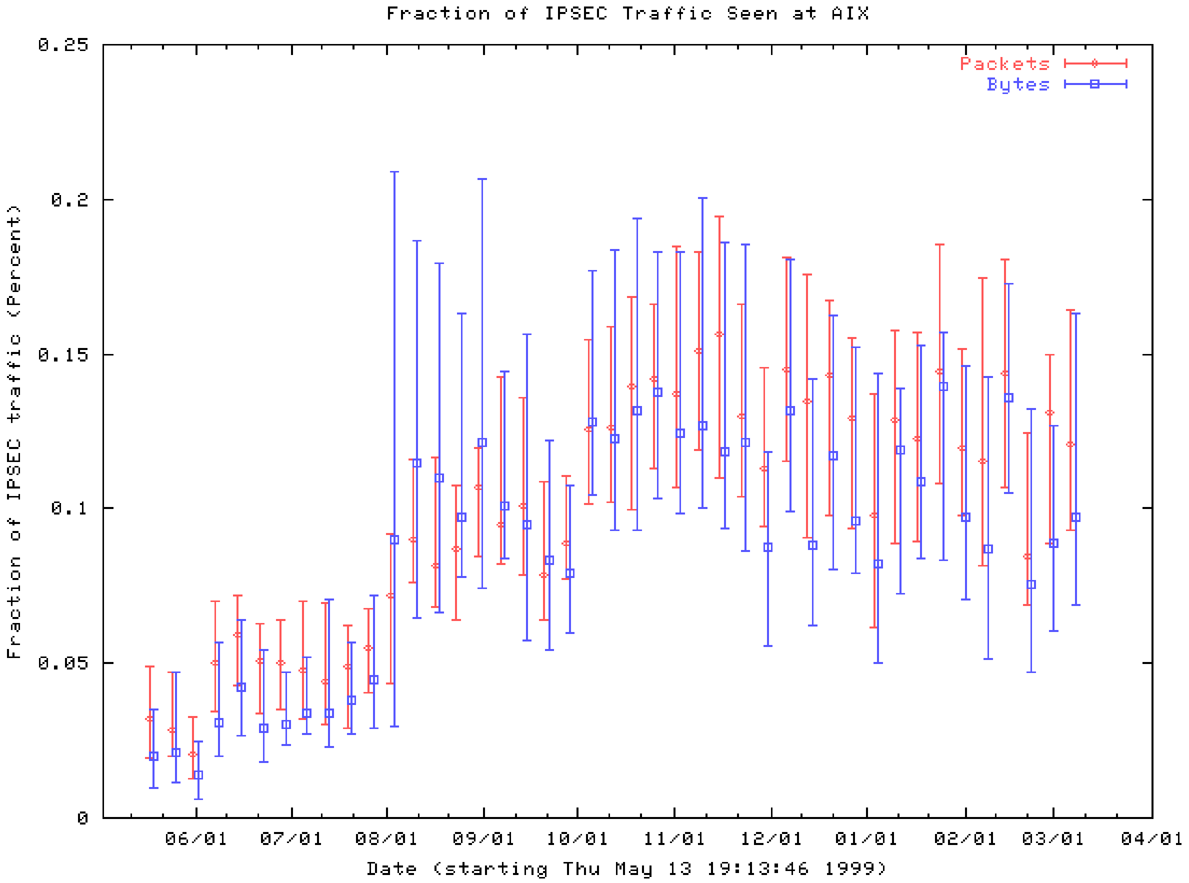

Figure 6: Fraction of authentication header (AH) and encapsulating security payload (ESP) traffic seen at AIX. Traces are collected into weekly bins, and the median and first and third quartiles for each bin are plotted.

The amount of fragmented traffic in wide area networks has been a topic of great interest in the past few months, especially as it relates to IP traceback techniques [Savage00]. Our data indicates that the fraction of fragmented traffic is on the rise, and that the majority of this growth is in the form of UDP packets. We need to perform further analysis to determine which UDP protocols are generating these fragments. Not surprisingly, TCP traffic is virtually never fragmented. Most likely this is due to widespread deployment of path MTU discovery combined with TCP’s relatively small default packet size.

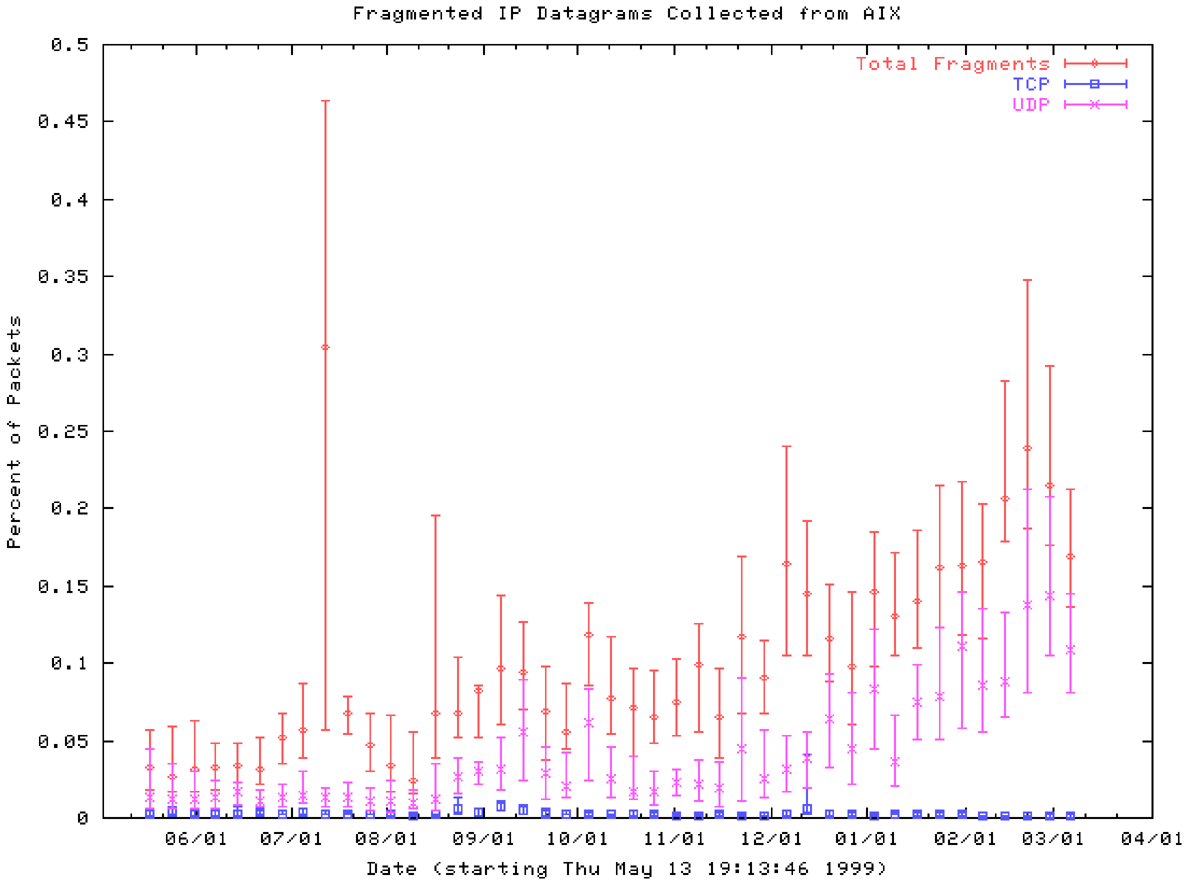

Figure 7: Fraction of fragmented traffic. Traces are collected into weekly bins, and the median and first and third quartiles for each bin are plotted.

FTP is the traditional bulk transfer protocol widely used before the advent of HTTP and the web. However, we see a clear decline in the contribution of FTP to the overall traffic mix since October 1999. This decline may actually be due to a shift from active to passive mode FTP associated with an increase in packet filtering firewalls in the Internet, or it may be due to a shift away from FTP to alternative protocols for file transfer. However, the graph of HTTP traffic fraction over this same time period does not show a corresponding increase.

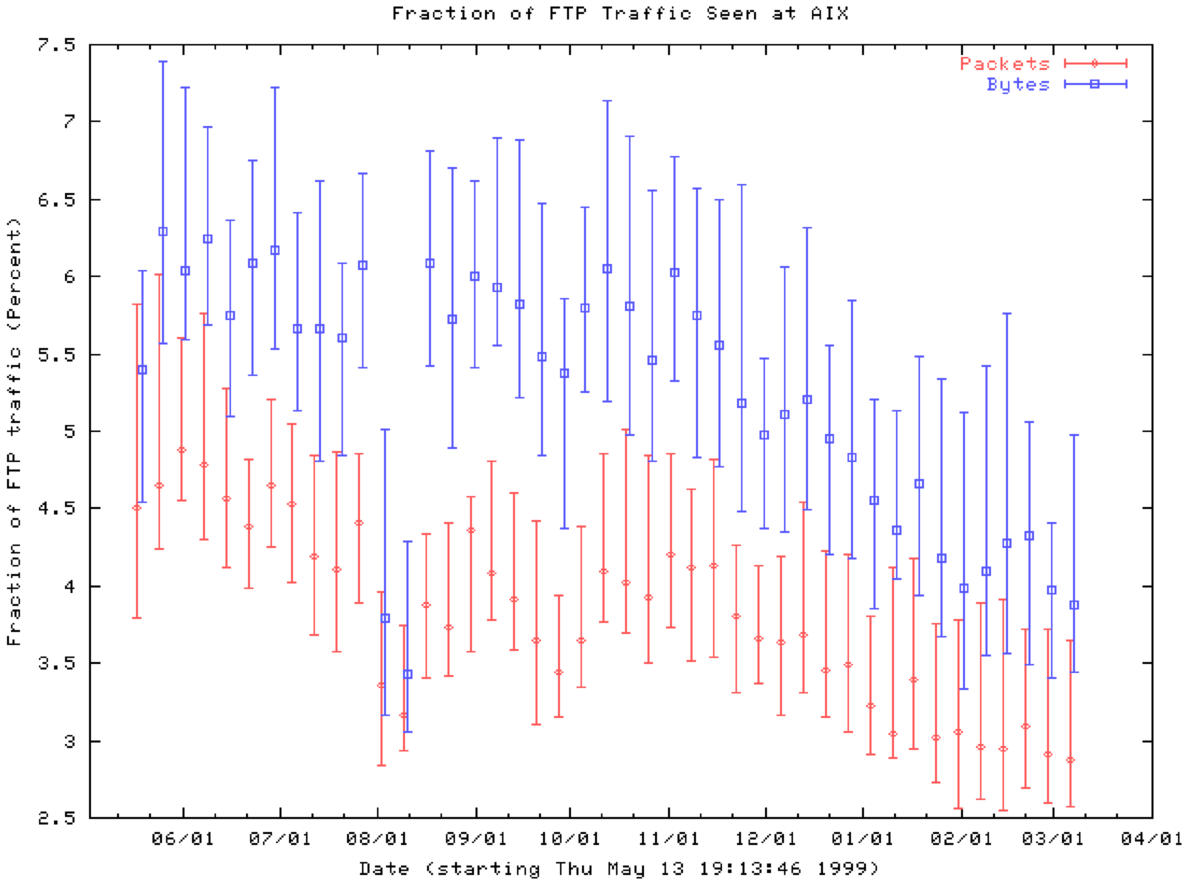

Figure 8: The fraction of active mode FTP traffic is declining. Traces are collected into weekly bins, and the median and first and third quartiles for each bin are plotted.

The following graph shows a relatively surprising decrease in the fraction of RealAudio traffic seen at AIX. Both TCP and UDP RealAudio traffic have decreased in packet volume compared to non-RealAudio traffic, although this trend seems to have flattened out in the last few months of our study.

Although RealNetworks has released newer versions of their RealPlayer software since this study began, the new versions use the same set of TCP and UDP ports as the old versions, with the addition of TCP port 554 for RTSP traffic [RealNetworks]. Consequently, the trend we observe is not due to a shift from the older software to the newer versions, but represents either a slowing in the growth of RealAudio traffic or a decline relative to the growth in non-RealAudio traffic.

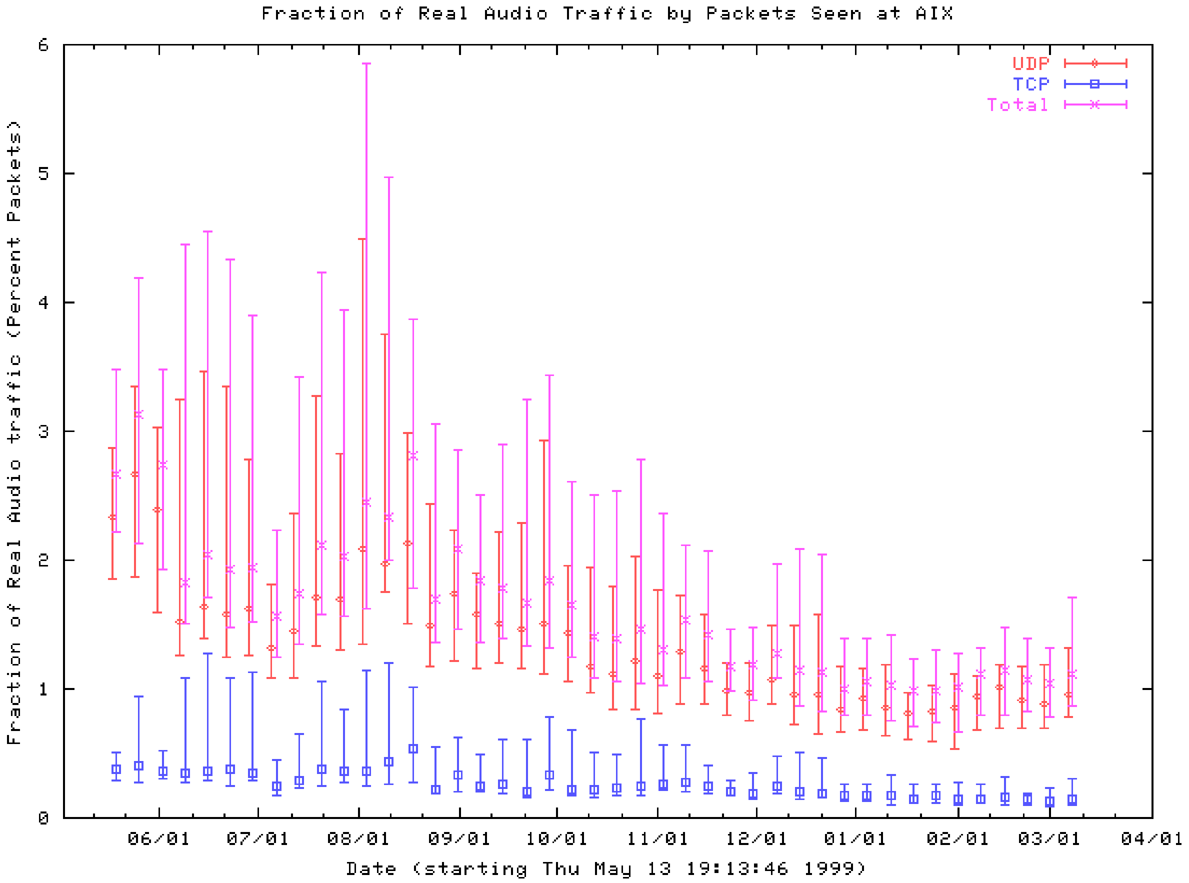

Figure 9: The fraction of RealAudio traffic has declined over the past 10 months. Traces are collected into weekly bins, and the median and first and third quartiles for each bin are plotted.

This graph shows a decline the in the fraction of traffic generated by several popular online games over the first 8 months of our study. The online games included in this graph are Starcraft, Quake II, and QuakeWorld (a variant of Quake II). These games were popular when we started collecting our data, but as the graph shows, their popularity has declined fairly steadily since July, 1999.

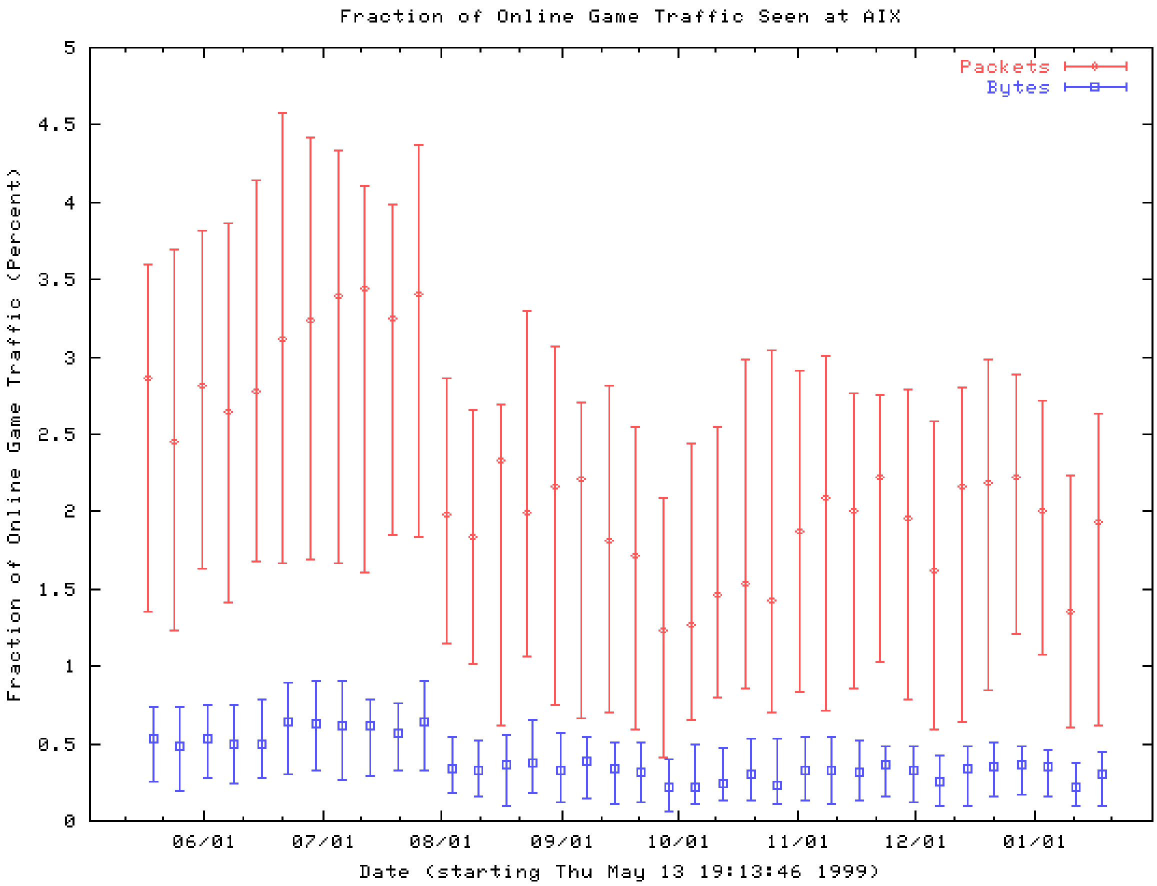

Figure 10: Fraction of online game traffic, including Quake II, QuakeWorld, and Starcraft. Traces are collected into weekly bins, and the median and first and third quartiles for each bin are plotted.

This second graph of online gaming traffic shows quite a different trend from the previous graph. Unlike the previous graph, this one includes traffic from several newer games in addition to the older ones. The new graph includes traffic generated by Half Life, Quake 3: Arena, and Unreal in addition to Starcraft, Quake II, and QuakeWorld. Although there is not enough data to determine a trend, the median traffic fractions are much higher on this graph than the previous one. Hence, the overall fraction of online game traffic seems to be on the rise, but it is a moving target. The increase is primarily generated by new games as they gain popularity, while older games seem to decrease in popularity over time.

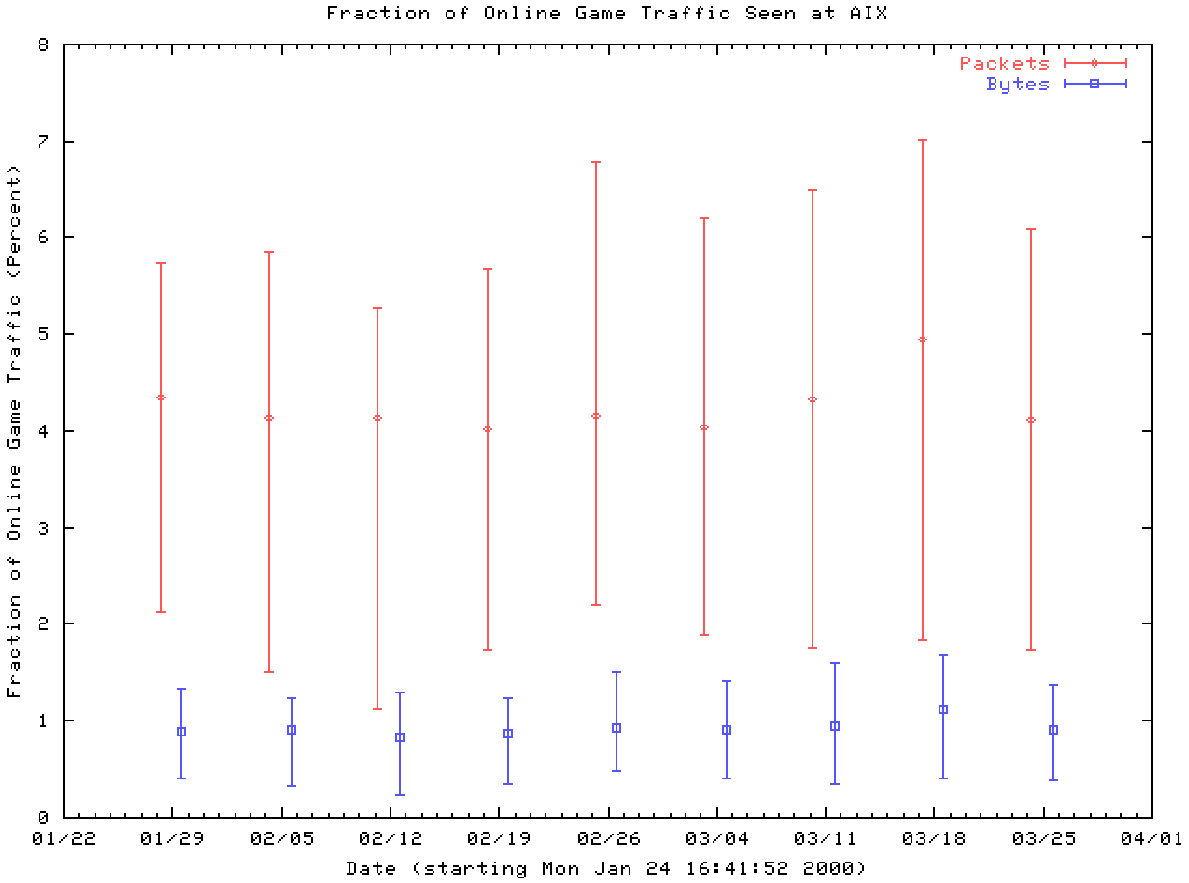

Figure 11: Fraction of online game traffic, including Half Life, Quake II, QuakeWorld, Quake 3: Arena, Starcraft, and Unreal. Traces are collected into weekly bins, and the median and first and third quartiles for each bin are plotted.

Although Napster does not use a fixed set of ports for file transfers, we identified the three most commonly used TCP ports in use in late January: TCP ports 6688, 6697, and 6699. Bulk transfer traffic may be either sent to or received from these ports, since Napster supports both active and passive mode transfers [Napster]. As Universities and other sites move to block traffic on these ports, Napster traffic will undoubtedly migrate to others. However, the short term trend clearly shows dramatic growth, increasing by over 50% in the last two months of our study.

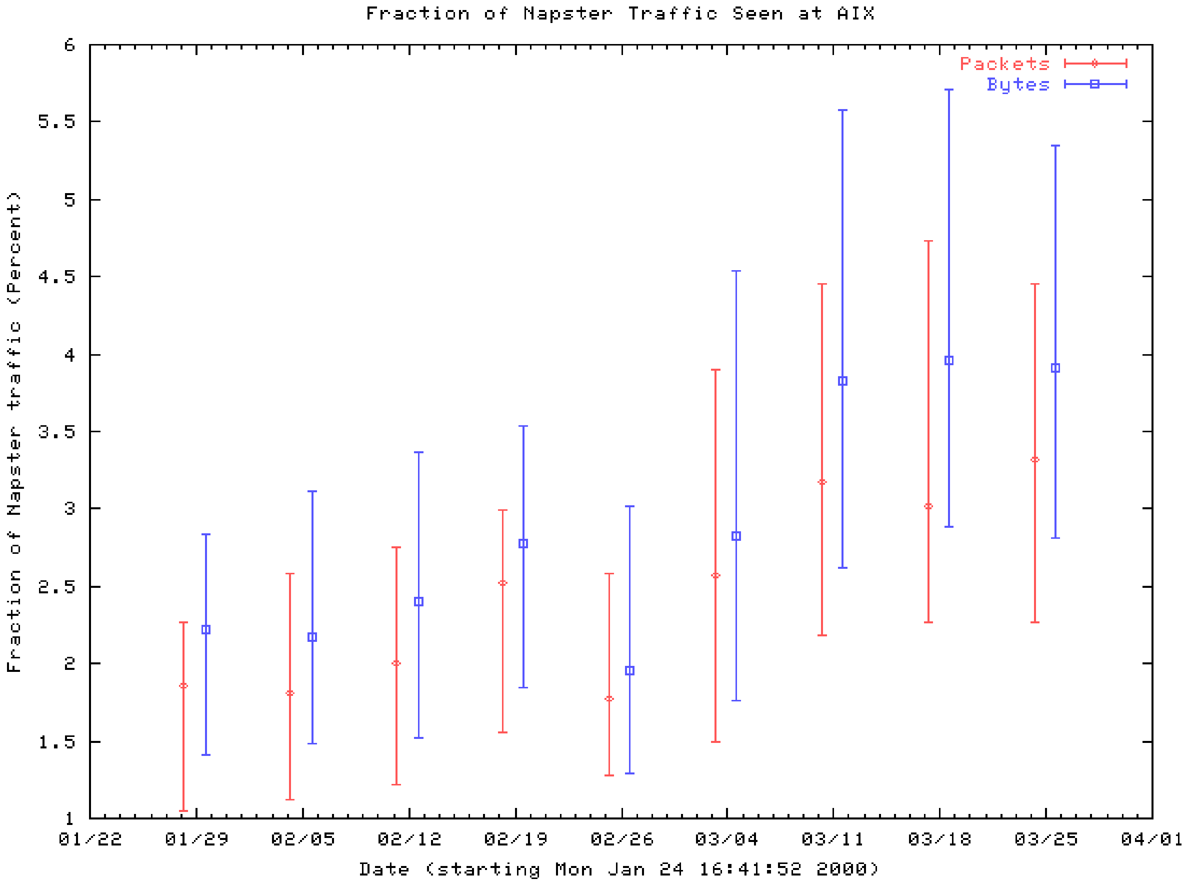

Figure 12: Fraction of Napster bulk-transfer traffic seen at AIX. Traces are collected into weekly bins, and the median and first and third quartiles for each bin are plotted.

Shorter Term Trends

Some shorter term trends can be easily associated with common user behavior. For example, the fraction of email traffic (SMTP packets to or from TCP port 25) increased significantly in November and early December, only to drop off again during the holidays at the end of December. Perhaps this was related to online commerce, as many people used the Internet to purchase their Christmas gifts?

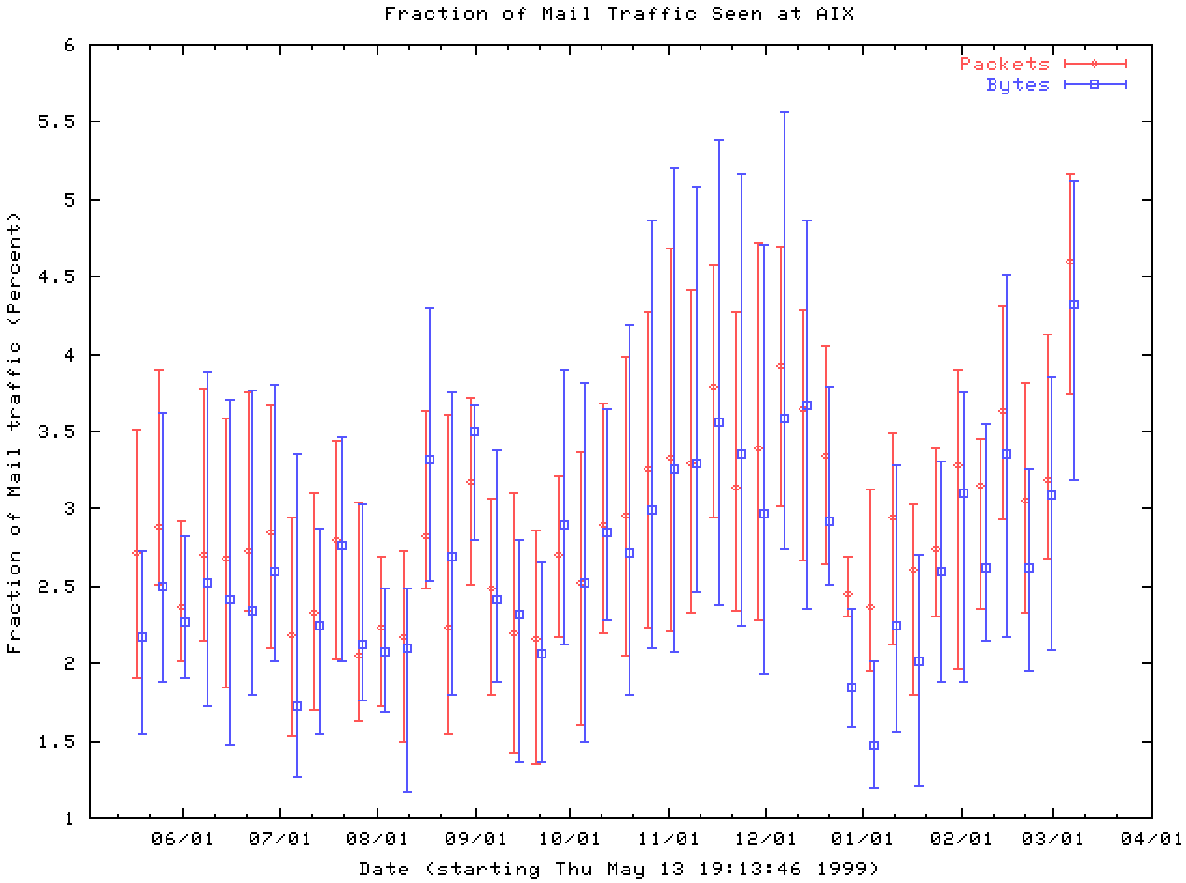

Figure 13: Fraction of mail traffic seen at AIX, showing a peak in usage just before the Christmas holidays. Traces are collected into weekly bins, and the median and first and third quartiles for each bin are plotted.

Online gaming is clearly more popular on weekends, as the following graph shows. The fraction of game traffic can nearly double on weekends compared to the typical weekday. This change in workload over the course of a week has been smoothed out in our previous graphs by our choice of bin size.

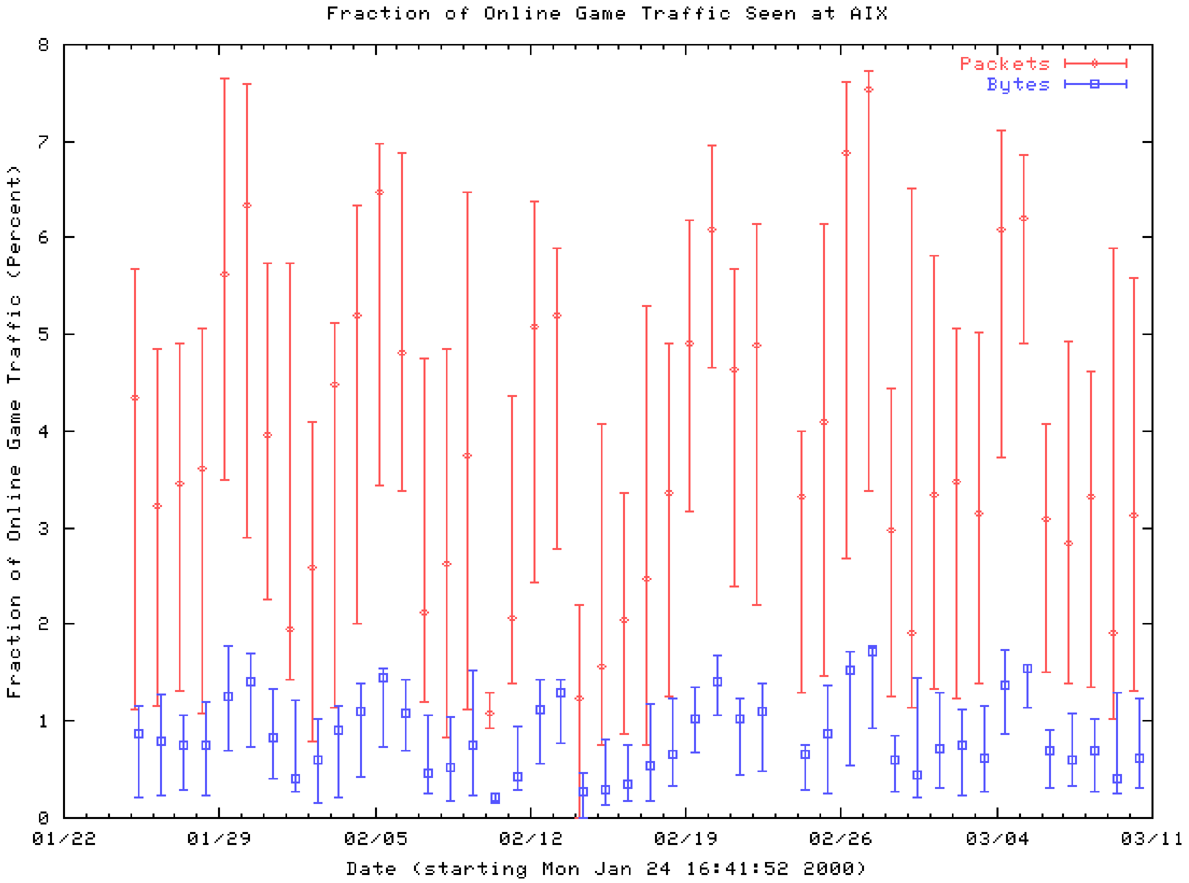

Figure 14: Weekly variations in the fraction of online gaming traffic seen at AIX. Traces are collected into daily bins, and the median and first and third quartiles for each bin are plotted.

Conclusions and Future Directions

In our long term study of the traffic workload at the Ames Internet Exchange, we found no significant trends over time in either the overall packet size distribution or changes in the ratio of TCP to UDP traffic. We did find an order of magnitude increase in the volume of IPSEC traffic, and a strong increasing trend in the volume of fragmented UDP traffic. Some other interesting trends include decreases in the volume of active-mode FTP and RealAudio traffic, and increases in the volume of online gaming and Napster traffic. We also found short term trends, including a transient increase in the volume of e-mail traffic during the holiday shopping season, and a strong weekday/weekend variation in the volume of online gaming traffic.

The collection of backbone traffic statistics has been severely impacted by the breakup of the network core into a number of mutually competitive organizations. Data collection efforts must now protect both the privacy of individual Internet users and the proprietary interests of the host organizations. CAIDA is in a unique position to monitor and analyze traffic collected from backbone links, as it has ongoing relationships with several core ISPs and exchange point providers.

Our workload characterization efforts also face additional technical challenges, both in extending our methodology to increase the accuracy of our measurements, and in coping with the introduction of new protocols. Our port based traffic classification scheme has some severe limitations, as illustrated by the volume of traffic it fails to map to any specific protocol. Additional techniques are necessary to further differentiate this traffic, as well as reduce confusion among protocols that use the same set of source or destination ports.

Furthermore, in order to accurately classify protocols that use negotiated ports on both ends it will be necessary to correlate multiple traffic streams from the same host to the same or different destinations [Plonka00]. However, these techniques may have limited usability in the Internet core where the measurement site is far away from both the source and destination of the traffic. Consequently, we may be unable to effectively sort this traffic by protocol without using techniques that monitor the all traffic exchanged on the associated control channels, as these channels typically use a well-known port at one end even if the data channel does not.

IPSEC represents another potential problem for workload analysis, as ESP traffic encrypts the source and destination ports we use for traffic classification. If use of ESP becomes widespread, we may lose the ability to estimate how the network is being utilized altogether. [Bellovin99] proposes a modification to ESP that sends clear text port numbers for encapsulated traffic. If this modification was adopted, ESP would not pose such a problem for our measurements.

The interconnection link between AIX and MAE-West has recently been upgraded to a single OC-12 Packet over SONET (POS) link. This will improve the data collection site, and allow us to perform packet flow analysis since every packet sent between AIX and FIX West will be visible to our monitor. However, it will also require POS support for Coral/OCXmon hardware. Development of additional hardware and software to support POS links at OC-3 and OC-12 speeds is currently under way at CAIDA, and we hope to continue this analysis after the link upgrade with minimal interruption in data collection.

CAIDA is also interested in other backbone sampling points for comparison against the workload seen at AIX. Previous studies done with data collected by MCI [claffy98, Apisdorf97, Thompson97] bear some similarities to our results, but more data collection must be performed before any conclusions can be drawn about how representative our results are of other wide-area Internet infrastructure.

Acknowledgments

This analysis would not have been possible without the work of Hans-Werner Braun and the National Science Foundation’s NLANR/MOAT project for collecting and archiving Internet traffic traces. The particular monitor that we used at the AMES Internet Exchange (AIX) exists as a result of a collaboration among NASA, NLANR, and CAIDA. We are grateful to Bill Jones, Lance Tatman, Bobby Cates, and Jeff Osbourne (all from NASA-Ames), and to Steve Feldman (previously at MCI/Worldcom) for their continued support and maintenance of this and other traffic monitors at the exchange points. We would also like to thank Ken Keys, David Moore, and the rest of the CoralReef team for the analysis library used throughout this project.

References

1. [AIX] **Ames Internet eXchange,** http://aix.arc.nasa.gov/ .
2. [AIXstats] **Ames Internet eXchange Link Utilization Statistics,**

http://aix.arc.nasa.gov/graphlink.html .

3. [Apisdorf97] J. Apisdorf, k claffy, K. Thompson, and R. Wilder. **OC3mon: Flexible, Affordable, High-Performance Statistics Collection,** http://www.isoc.org/isoc/whatis/conferences/inet/97/proceedings/F1/F1_2.HTM .
4. [Bellovin99] S. Bellovin. **Transport-Friendly ESP,** http://www.research.att.com/~smb/talks/tfesp-ndss/index.htm
5. [Braun98] H.-W. Braun. **Towards a systemic understanding of the Internet organism: a framework for the creation of a Network Analysis Infrastructure,** http://moat.nlanr.net/NAI .
6. [Caceres89] R. Caceres. **Measurements of Wide-Area Internet Traffic.** UCB/CSD 89/550, University of California, Berkeley, CA, December 1989, http://sunsite.berkeley.edu/Dienst/UI/2.0/Describe/ncstrl.ucb/CSD-89-550 .
7. [Caceres91] R. Caceres, P. Danzig, S. Jamin, and D. Mitzel **Characteristics of wide-area TCP/IP conversations** Proceedings of ACM SIGCOMM '91, September 1991, http://www.acm.org/pubs/citations/proceedings/comm/115992/p101-caceres .
8. [CAIDA] **Cooperative Association for Internet Data Analysis,** http://www.caida.org .
9. [claffy93] K. Claffy and H.-W. Braun and G. Polyzos. **Long-term traffic aspects of the NSFNET,** Proceedings of INET'93. http://wwwdev.caida.org/outreach/papers/lta.html .
10. [claffy95] K. C. Claffy, Hans-Werner Braun, George C. Polyzos. **A parameterizable methodology for Internet traffic flow profiling,** IEEE JSAC April 1996, http://wwwdev.caida.org/outreach/papers/pmi.html .
11. [claffy97] k claffy and T. Monk. **What's next for Internet data analysis?** IEEE Special Issue on Communications in the 21st Century **85,** 1563-1571 (1997). .
12. [claffy98] k claffy, G. Miller, and K. Thompson. **the nature of the beast: recent traffic measurements from an Internet backbone,** http://www.isoc.org/inet98/proceedings/6g/6g_3.htm .
13. [claffy99] kc claffy. **Internet measurement and data analysis: topology, workload, performance and routing statistics,** , NAE 99, http://wwwdev.caida.org/outreach/papers/Nae/ .
14. [CoralReef] **CoralReef home page,** http://www.caida.org/Tools/CoralReef .
15. [Feldman98] S. Feldman. **MAE-West Link Utilization Statistics,** http://www.mae.net/~feldman/gigaswitch/ames
16. [Feldmann98] A. Feldmann, J. Rexford, and R. Caceres. **Efficient policies for carrying Web traffic over flow-switched networks,** , IEEE/ACM Transactions on Networking, December 1998, pp. 673-685, http://www.research.att.com/~jrex/papers/ton98.ps
17. [Heimlich89] H. Heimlich. **Traffic Characterization of the NSFNET Backbone,** , USENIX Conference Proceedings, Winter 1989, http://www.research.att.com/~jrex/papers/ton98.ps
18. [Merit95] **NSFNET Statistics** , Merit Network, Inc., 1995, http://www.merit.edu/merit/archive/nsfnet/statistics .
19. [Mena00] A. Mena and J. Heidemann. **An Empirical Study of RealAudio Traffic,** , IEEE INFOCOM 2000, http://www.ieee-infocom.org/2000/papers/84.ps .
20. [MOAT] **National Laboratory for Applied Network Research (NLANR)/ Measurement and Operations Analysis Team (MOAT),** http://moat.nlanr.net/ .
21. [MOAT99] National Laboratory for Applied Network Research (NLANR)/ Measurement and Operations Analysis Team (MOAT), **Data analysis based on Coral packet traces** http://moat.nlanr.net/Datacube .
22. [Napster] **Napster Protocol Specification,** http://opennap.sourceforge.net/napster.txt .
23. [OC3mon] **Coral/OC3 Monitoring Hardware,** http://moat.nlanr.net/OC3mon-monitors .

24. [OC3mon-sw] **OC3mon Data Collection Software,** http://moat.nlanr.net/Software/OC3mon .
25. [RFC2330] V. Paxson. **Growth Trends in Wide-Area TCP Connections,** IEEE Network, 8(4), pp. 8-17, July/August 1994. ftp://ftp.ee.lbl.gov/papers/WAN-TCP-growth-trends.ps.Z .
26. [Plonka00] D. Plonka. **UW-Madison Napster Traffic Measurement,** http://net.doit.wisc.edu/data/Napster/ .
27. [RealNetworks] **RealNetworks RealSystem Firewall Support,** http://service.real.com/firewall/adminfw.html .
28. [RFC2330] V. Paxson, G. Almes, J. Mahdavi, and M. Mathis. **Framework for IP Performance Metrics** RFC 2330, ftp://ftp.isi.edu/in-notes/rfc2330.txt .
29. [Savage00] S. Savage, D. Wetherall, A. Karlin and T. Anderson. **Practical Network Support for IP Traceback,** , *in submission*. Currently available as UW-CSE-00-02-01. .
30. [Stevens94] W. Richard Stevens. **TCP/IP Illustrated, Volume 1: The Protocols** Addison-Wesley, 1994.
31. [Thompson97] K. Thompson, G. Miller, and R. Wilder. **Wide Area Internet Traffic Patterns and Characteristics** IEEE Network, Vol. 11 No. 6, pp. 10-23, Nov/Dec 1997. http://www.vbns.net/presentations/papers/MCItraffic.ps .
32. [WISCstats] D. Plonka. **University of Wisconsin Network Usage Statistics,** http://wwwstats.net.wisc.edu/ .

For more information: info @ caida.org *last update:*

this page: