Longitudinal study of Internet traffic in 1998-2003

Marina Fomenkov, Ken Keys, David Moore, and k claffy

Abstract

There is growing interest in capturing and analyzing Internet traffic characteristics in pursuit of insights into its evolution. We present a study of one of the few sources of publicly available long-term Internet traffic workload data, namely the NLANR PMA archive of packet header traces. More than 4000 trace samples were collected at a number of academic, research, and commercial sites during years 1998-2003. We consider four metrics of traffic: bytes, packets, flows, and number of source-destination pairs. We also analyze the composition of traffic by protocol.

Keywords

Internet traffic workload characterization, Traffic scaling, flows, TCP, UDP

I. Introduction

Internet traffic is the result of interaction among millions of users, hundreds of heterogeneous applications, and dozens of sophisticated protocols. The technical components of the Internet are complex in themselves, and they are augmented by a general unpredictability and diversity of the human components. Both industry and the research community benefit from accurate knowledge of wide area Internet traffic. Their interests include optimization of network components, modification of protocols to enhance their performance, modeling the effects of emerging applications on the existing architecture, and facilitating future growth of the Internet. However, reliable and representative measurements of wide area Internet traffic are scarce. Our study aims to help fill this gap by presenting a longitudinal study of traffic behavior at a number of academic, research and commercial sites observed over four and a half years (1998-2003).

In a previous study, McCreary and Claffy [1] analyzed IP traffic workload seen at a single measurement site at NASA Ames Internet eXchange point (AIX) from May 1999 through March 2000. They found no significant change in the overall packet size distribution, nor in the ratio of TCP to UDP traffic during this period, but the proportion of fragmented traffic was on the rise.

An earlier (1997) study by Thompson, Miller and Wilder [2] discussed characteristics of wide area Internet traffic samples collected on MCI's commercial Internet backbone. Their interval of observations ranged from a single day to a week and hence their data cannot be used for assessing any long-term trends.

Fraleigh *et al.* [3] describe the IPMON traffic monitoring system and report observations of traffic on OC-12 links in the Sprint E-Solutions backbone network over a 24-hour period in the middle of 2001. This is the first published traffic study from OC-12 links in a commercial backbone network. They found that on some links over 60% of the traffic is generated by new applications such as distributed file sharing and streaming media, while only 30% is web traffic. The results of this paper provide a snapshot of traffic characteristics typical for the Sprint IP backbone, but it is unclear if they are representative of other networks.

The WAND network research group of the University of Waikato conducts bidirectional measurements on the OC3 access link that connects the University of Auckland to the public Internet [4]. Since July 1999 they have collected several comprehensive data sets spanning periods from one week up to seven months. The data are publicly available and have been used in a number of studies (see review in [4]).

II. Data

A. Data collection

Our study surveys a publicly available archive of traces collected and maintained by the National Laboratory for Applied Network Research (NLANR) [5]. Monitors obtained more than 4000 traffic samples at various academic and research sites connected to High Performance Computing (HPC) networks (table I). A detailed description of the sites and the current status of measurements is available at [6].

All authors are with: CAIDA, SDSC, UC San Diego, La Jolla CA 92093-0505, USA. E-mail: {marina,kkeys,dmoore,kc}@caida.org.

Support for this work is provided by NSF grants ANI-0137121 and ACI-9619020.

TABLE I. MONITORED SITES (LISTED ALPHABETICALLY).

Abbreviation	Full Name	Card	Start date	End date
12NCS	NCSA OC12mon vBNS connection	POINT	June, 1999	May, 2001
12SDC	SDSC OC12mon vBNS connection	POINT	May, 1999	May, 2001
ADV	Advanced Networks and Services	DAG3.2	February, 2001	November, 2002
AIX	MAE-West interconnection at NASA-Ames	DAG3.5	May, 1999	March, 2003
ANL	**Argonne Natl Lab to STARTAP connection**	**FATM**	**November, 1998**	**April, 2003**
APN	**APAN connection at STARTAP**	**FATM**	**November, 1998**	**April, 2003**
BUF	University of Buffalo	DAG3.2	October, 2001	March, 2003
BWY	Columbia University (BroadWaY)	DAG3.2	June, 2000	April, 2003
COS	Colorado State University	DAG3.2	May, 2000	March, 2003
FLA	Florida universities GigaPOP	FATM	November, 1998	May, 2001
FRG	Front Range GigaPOP	FATM	March 2000	September, 2000
IND	Indiana university GigaPOP	DAG3.2	July, 2001	December, 2002
MEM	University of Memphis	DAG3.2	November, 2000	April, 2003
MRA	Merit Abilene	DAG3.2	January 2002	April, 2003
MRT	Michigan universities (Merit)	FATM	January 1999	May, 2001
NCA	National Center for Atmospheric Research	FATM	November, 1998	April, 2001
NCL	North Caroline RTP universities GigaPOP	FATM	November, 1998	May, 2001
NRN	NASA NREN connection at the AIX	FATM	December, 1998	April, 1999
ODU	**Old Dominion University**	**FATM**	**November, 1998**	**April, 2003**
OSU	**Ohio State University**	**FATM**	**November, 1998**	**April, 2003**
SDC	SDSC commodity connection	FATM	November, 1998	May, 2001
TAU	Tel Aviv University	FATM	December, 1999	May, 2002
TXG	Texas universities GigaPOP, OC12	DAG3.2	May, 2002	April, 2003
TXS	Texas universities GigaPOP, OC3	FATM	November, 1998	September, 2002

Sites shown in **bold** have the longest monitoring period.

At each site packet headers were captured at two interfaces between one and eight times daily once per month, usually on the 15th day of each month. The starting hour for each trace was set at constant intervals during the 24-hour period but randomized within the hour at the beginning of each interval. The average duration of each measurement ranges between approximately 60 and 120 seconds.

B. Analysis methodology

We consider the following four metrics of measured traffic: number of bytes, number of packets, number of flows, and number of source-destination pairs. The first two metrics are primary since they are directly measured. Packets are actual quanta of traffic recorded by monitoring cards and each packet contains a certain number of bytes. The number of flows and the number of source-destination pairs are secondary metrics since they derive from data processing and aggregation.

A *flow* is a sequence of packets in which each packet has the same value for a 5-tuple of source IP address, source port, destination IP address, destination port, and protocol *flow key*. Flows expire at periodic intervals measured from the beginning of the trace, or after a specified timeout period during which no packets matching the flow key are observed. These definitions of flow and timeout mechanisms (similar to the ones adopted in [7]) make it highly likely that all packets of a flow originate from the same application and in the same episode of network use. Therefore, a flow intuitively corresponds to a unit of human activity on the net although many flows can map to the same activity (e.g. downloading a URL with many embedded objects). The number of flows is a measure of the number of connections (or sessions) passing through the monitored link. Note however that the count of flows observed in a trace is not an objective characteristic since this number will be different depending on the chosen flow key and expiry mechanism.

The *number of source-destination pairs* (or the *number of IP pairs*) represents the next step in data aggregation. Although IP addresses in the traces have been encrypted to satisfy privacy requirements, we can count the number of unique combinations of <source IP address> and <destination IP address> observed within a specified time interval. Port numbers and protocols are ignored. This metric measures the number of Internet hosts communicating via the monitored link.

We used the CAIDA CoralReef [8] software suite to reduce raw traces. When studying the traffic metrics

listed above, we divide traces into 30 s intervals and count the number of bytes, packets, and flows in each interval independently. Flows expire at interval boundaries; no timeout is used. We then aggregate each table of flows to a table of IP pairs. Data in the incomplete interval at the end of each trace are discarded. Since the traces are usually between 60 and 120 s long, we obtain 2 or 3 valid 'sub-traces' from each trace. If a trace contains measurements from two interfaces, we process each independently.

When studying the stratification of traffic by protocols, we consider the whole trace and use a flow expiry timeout of 64 s. First, CoralReef routines create a separate summary table for each monitored interface. The table shows the numbers of {bytes, packets, flows} attributed to a given protocol. Next we find the precise duration of measurements at each interface from timestamps and use these values to convert absolute counts to rates. Finally, we average the rates of both interfaces for all traces recorded on the same date. This procedure yields a single data point for each parameter {bytes, packets, flows} for each protocol per month.

C. Issues with the data

We have discovered that traces captured with an FATM card [9] (files with extension .crl in the NLANR archive) often have problems with the accuracy of time measurements. In general, the start epoch and drift rate of FATM clocks are not synchronized at inter-packet timescales with an accurate time source, the CPU clock, or clocks of other FATM cards. Therefore absolute times of any packets and inter-packet arrival times from different cards are unreliable.

FATM cards also have a problem that delays the increment of their 32 bit high-order firmware clock when their 16 bit 40 MHz low-order hardware clock wraps. ATM cells that arrive between the low-order wrap and the corresponding high-order increment will have timestamps 2.62144 ms less than the correct value. CAIDA's CoralReef library can automatically detect a failed FATM firmware clock increment and compensate for it, reporting the correct timestamp.

We also found that NLANR FATM traces often have apparent clock resets (cell timestamps jumping to near zero) on one or both interfaces. In particular, almost all traces of *.crl* type showed a reset on interface 0 after timestamps have reached a little over 14 s, which could be after as many as 11 blocks of data, and a reset on interface 1 after timestamps had reached about 6 s. Some traces also contain multiple large discontinuities in timestamps, both before and after the last apparent clock reset. We treat all cells before the last discontinuity as unreliable and eliminate them from our analysis.

The duration of measurements may be different for each interface within the same trace or data from one interface can be completely lost. Careful normalization is required in order to combine or compare data from different interfaces. We solve this problem by a) checking timestamps and determining time intervals as accurately as possible; b) properly converting absolute counts to rates; c) averaging the rates.

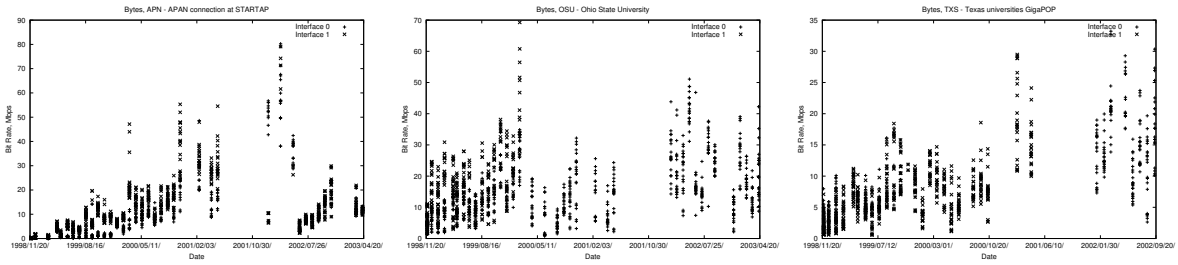
III. Results

A. Bit rate and Packet rate

We will now discuss basic properties of the two primary traffic metrics: bytes and packets. For this analysis we present all values as rates, that is counts of a certain metric (for example, the number of packets) divided by the length of the sampling interval. The default length of the sampling interval is 30 seconds. We also convert byte rate into the more commonly used bit rate.

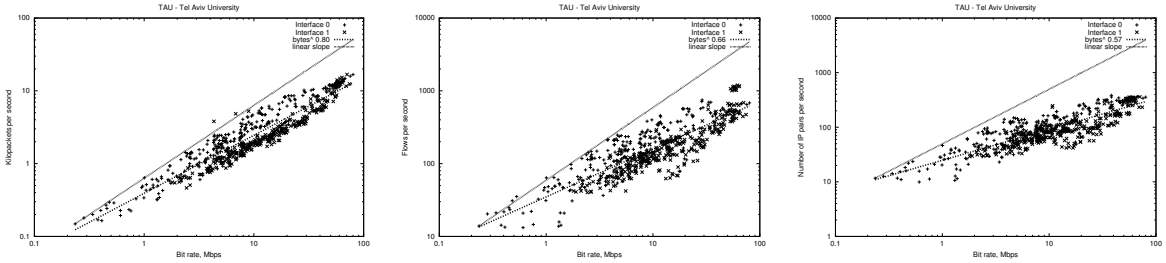
Out of 24 sites listed in Table I, only four sites have been consistently monitored for the whole four and a half year period that we analyze (although there are some gaps in coverage); two more sites have almost four years of data. We considered these data (examples in Figures 1) in order to make inferences about the rate of Internet traffic growth in 1998-2003.

Variations in bit rate are large and mostly without obvious trends. The wide scattering of data points reflects a well-known property of Internet traffic burstiness [10]. We observed neither a clear diurnal pattern in the measured traffic nor consistent long-term growth. At APAN-STARTAP connection (Figure 1(a)), traffic appears to grow for the first three years of observations, and then drops considerably. At the Ohio State University (Figure 1(b)), it fluctuates. At Texas Universities GigaPOP (Figure 1(c)), the traffic rate increases first, but seems to stabilize after the summer of 2001. Other sites [11] also exhibit diverse behavior



(a) APAN-STARTAP (b) Ohio State (c) Texas universities

Fig. 1. Average bit rates sampled at interfaces 0 and 1 in 30 s intervals.



(a) Packet rate (b) Flow rate (c) Number of IP pairs per second

Fig. 2. Traffic metrics vs. bit rate, Tel Aviv University. All rates are averages of 30 s intervals.

of traffic and none has had a consistent growth throughout the whole period of monitoring.

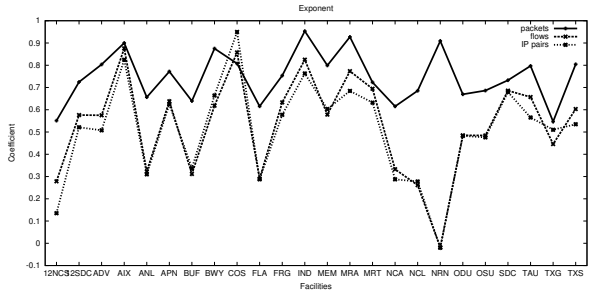
Unfortunately, the quality of available data is often insufficient for any more quantitative estimates. For example, in each particular case, traffic fluctuations can be explained by a variety of local reasons, i.e. changes in preferred routing, technical problems with data collection, lower usage of university links during summers, etc., rather than by global decline of Internet traffic. However, assuming that the NLANR trace measurements are at least somewhat representative of the overall Internet traffic evolution during the last five years, we conclude that these data do not support the claim of Internet traffic universally and rapidly increasing both before and after the Internet bubble burst in 2000-2001 [12].

Packet rates [11] fluctuated over time similarly to bit rates. The packet rate is a sublinear function of the bit rate (Figure 2(a)). This observation suggests that as traffic grows, the average packet length increases.

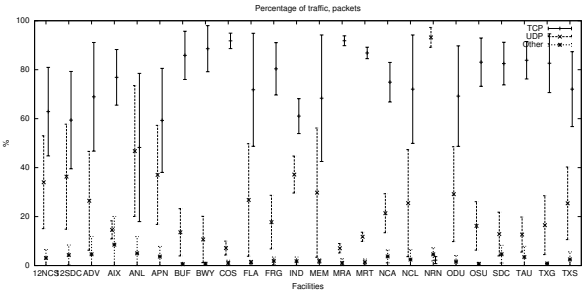
B. Number of flows and source-destination pairs

Although there is no consistent growth of bandwidth usage in the majority of monitored links during the period of our observations, the bit rate and the packet rate fluctuate by as much as a few orders of magnitude at the majority of sites. The large dynamic range of values allows us to study the scaling of secondary traffic parameters with the increase in usage of a link. We have considered the dependence of the number of flows and the number of IP pairs (both normalized to the length of the measurement interval) on the bit rate; figures 2(b) and 2(c) provide examples. Results for other sites are in [11]. The growth of these two parameters with the bit rate is even slower than that of the packet rate discussed above.

In figure 2 dotted lines show linear regression of the data in logarithmic space. In linear space these lines represent an approximation by power law function of type $y \sim x^{\alpha}$, where x is the bit rate and y is either the packet rate, or the number of flows per second, or the number of IP pairs per second. Solid lines correspond to linear dependence $y \sim x$. Figure 3(a) shows the value of exponent α for packets, flows, and IP pairs for all monitored sites. The average values for all sites excluding the NASA NREN connection at the AIX (NRN) are: $\alpha_{packets} = 0.74 \pm 0.11$; $\alpha_{flows} = 0.56 \pm 0.19$; $\alpha_{IPpairs} = 0.53 \pm 0.20$. From Figure 3(a) it is clear that properties of traffic at the NRN site are very different from those at all other sites. This difference



(a) The exponent for power law approximation of three traffic metrics vs. bit rate.



(b) Percentage of packets by protocols.

Fig. 3. Aggregated characteristics of traffic.

Metric	TCP, %	UDP, %	Other, %
Bytes	(83 ± 11)	(16 ± 11)	(1 ± 1)
Packets	(75 ± 12)	(22 ± 11)	(3 ± 2)
Flows	(56 ± 15)	(33 ± 10)	(11 ± 7)

TABLE II. COMPOSITION OF TRAFFIC BY PROTOCOLS FOR DIFFERENT METRICS.

is explained below in Section III-C.

Arnaud [13] considered an N^2 phenomenon of Internet growth. He argued that if N is the number of simultaneous connections between computers then the capacity at the core of any Internet network should grow as N^2 to support the expected traffic growth. In our framework, the number of flows corresponds to the number of connections and the bit rate is the bandwidth used. At first sight our experimental data seem to confirm the N^2-hypothesis: number of flows is approximately proportional to a square root of bit rate, or bit rate grows as the square of number of flows. However, this interpretation is misleading. As stated in Section II-B, bit rate is a primary parameter representing the objective measure of traffic. It cannot exceed the physical capacity of a given link. The number of flows is a derived metric that depends on the bit rate, not vice versa. Reversing the X and Y axes in Figure 2, i.e., putting the dependent variable on the X axis and the independent variable on the Y axis, would produce a result that has no physical meaning.

C. Traffic by protocols

We considered the traffic mix by protocols using the following categories: TCP, UDP, ICMP, IGMP, IP_in_IP, GRE, ESP, AH, SKIP, IPIP and other. A protocol of each packet is determined by the value of the protocol field in its IP header (i.e., 6 = TCP, 17 = UDP, etc.). At most sites, TCP is the predominant transport protocol (examples are at [11]). Some grid computing sites (NCSA, SDSC, ANL) may carry significant amounts of UDP traffic. The NASA NREN connection at AIX is the only link heavily dominated by UDP traffic during all six months of monitoring.

For each site, we calculated overall average percentages of its protocol mix using three main categories $\{$TCP, UDP, Other$\}$ and three metrics of traffic $\{$bytes, packets, flows$\}$. Figure 3(b) shows fractions of traffic by packets attributed to each of the categories. Typically, TCP traffic is between 60% and 90% of the total load, UDP traffic is between 10% and 40%, and all other protocols combined produce less than 5%. The nature of traffic observed at NRN is clearly different from all other sites (2% TCP, 93% UDP, 5% other). The aggregated average composition of traffic by protocols at all sites but NRN is shown in the Table II.

In their analysis of traces collected at AIX in 1999-2000, McCreary and Claffy [1] found that median fractions of packets (derived from weekly bins) were $> 80\%$ TCP, and $< 20\%$ UDP. These fractions did not change appreciably during 10 months of monitoring. Averaging monthly measurements of AIX traffic from May 1999 till March 2003 yields fractions of traffic by packets as $(77 \pm 17)\%$ TCP, $(14 \pm 4)\%$ UDP, and $(9 \pm 11)\%$ other. Our results are very close to [1] indicating continuing stability of the protocol mix over time despite the increase in the number of UDP applications in recent years.

IV. Conclusions and future work

We have presented an overview of Internet traffic as seen from multiple observation points. The NLANR PMA archive of traces is one of the largest and diverse collection of Internet traffic samples available to the research community for longitudinal studies of Internet traffic. Although different types of cards were used to captured the traffic, we were able to process the data in a uniform manner and derived aggregated characteristics of traffic observed at different sites.

We considered four quantitative metrics of traffic: number of bytes, number of packets, number of flows and number of source-destination pairs. The first two metrics are primary as they represent quantities that are actually recorded in captured traces. They are objective measures of the actual traffic. The third and fourth metrics are secondary since we derive them from observed packets in conjunction with definitions we accept in performing the analysis.

We found that a commonly accepted claim of Internet traffic constantly increasing at a high rate is not true for the majority of sites in our survey. However, the creditableness of this observation may be limited by intrinsic problems of the data set itself. First, the choice of sites for monitoring was restricted to HPC sites. Second, infrastructure changes that may have occurred at some sites to direct a portion of traffic to different links have not been properly documented.

We found that packet rate is a sublinear function of bit rate, $packet\_rate \sim (bit\_rate)^{0.75}$. Counts of flows and IP pairs behave approximately as $(bit\_rate)^{0.5}$. This observation indicates that routers may be able to keep track of active flows since the memory necessary for storage would grow slower than the CPU power required to process traversing packets.

We have studied the mix of traffic at the monitored sites by protocol in terms of three metrics: bytes, packets, and flows. We found that proportions of TCP and UDP traffic on average is about 5 to 1 by bytes, or 3 to 1 by packets. This ratio has not changed appreciably over the period of observations.

In 2001 CAIDA began collecting data at two OC48 links in the networks of Tier 1 providers Verio and MFN. We welcome researchers to use these data in their analysis of Internet traffic properties. Other groups [4], [14] also are working to build passive monitoring equipment for use at high speed links. We continue to improve our data collection and analysis methodologies and will extend the analysis presented in this paper to new data as they become available.

References

[1] S. McCreary and kc claffy, "Trends in wide area IP traffic patterns: a view from Ames Internet eXchange," in *13th ITC specialist seminar: IP Traffic measurement, modeling and management*, Sept. 2000.

[2] K.Thompson, G. Miller, R. Wilder, "Wide area Internet traffic patterns and characteristics," *IEEE Network*, vol. 11, 1997.

[3] C. Fraleigh, S. Moon, C. Diot, B. Lyles, F. Tobagi, "Packet-level traffic measurements from a tier-1 IP backbone," Sprint technical report TR-01-110101.

[4] J. Micheel, I. Graham, N. Brownlee, "The Auckland data set: an access link observed," in *Proceedings of the 14th ITC specialists seminar on access networks and systems*, 2001.

[5] "National Laboratory for Applied Network Research," http://www.nlanr.net/.

[6] "NLANR. Passive Measurement and Analysis: Site configuration and status," http://pma.nlanr.net/PMA/Sites/.

[7] k claffy, H. Braun, G. Polyzos, "A parameterizable methodology for internet traffic flow profiling," *IEEE JSAC*, vol. 13, 1995.

[8] K. Keys, D. Moore, R. Koga, E. Lagache, M. Tesch, kc claffy, "The architecture of coralreef: an internet traffic monitoring software suite," in *PAM2001 - A workshop on Passive and Active Measurements*, 2001.

[9] "ForeRunner 200E Network Interface Cards," http://www.marconi.com/html/solutions/forerunner200enics.htm.

[10] D.Clark, W. Lehr, I. Liu, "Provisioning for bursty Internet traffic: implications for industry and Internet structure," 1999, http://ana.lcs.mit.edu/anaweb/.

[11] M. Fomenkov, "Traffic workload trends from 1998-2003 NLANR traces," 2003, http://www.caida.org/~marina/NLANR/.

[12] A. Odlyzko, "Internet traffic growth: Sources and implications," 2003, http://www.dtc.umn.edu/ odlyzko/doc/itcom.internet.growth.pdf.

[13] B. St. Arnaud, "Scaling issues on Internet networks," 2001, http://www.canet3.net/library/papers/scaling.pdf.

[14] G.Iannaccone, C. Diot, I. Graham, N. McKeown, "Monitoring very high speed links," in *ACM SIGCOMM Internet Measurement Workshop*, 2001.