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. NLANR PMA data includes approximately 90-second packet trace samples collected at a number of academic, research, and commercial sites during years 1998-2001. We consider four metrics of traffic: bytes, packets, flows, and number of source-destination pairs over time, and we analyze correlation among these metrics. We also analyze the composition of traffic by application.

Keywords—Network operations, Internet traffic workload characterization, Traffic scaling, Applications

I. Introduction

Internet traffic is the result of interaction among millions of users, hundreds of heterogeneous applications, and 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. Many assumptions and assertions have been made about the nature of wide area Internet traffic. Both industry and the research community need to have as accurate knowledge of its characteristics as possible. Their interests include optimization of network components, modification of protocols to enhance their performance, modeling the effects of emerging applications on the existing architecture, planning and facilitating future growth and development of the Internet, and others. 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 two and a half years (1999-2001) period.

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 fraction of fragmented traffic was on the rise. They also considered emerging traffic categories such as streaming media, online gaming and Napster.

An earlier (1997) study by Thompson, Miller and Wilder [2] discussed patterns and 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. 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. However, the results of this paper also are derived from data collected over a 24-hour period in the middle of 2001. They provide a snapshot of the traffic characteristics typical for the Sprint IP backbone, but cannot be generalized to 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]).

We note that our results represent a unique long-term view of Internet traffic from multiple observation points and depict the evolution of this community of Internet users during years 1998-2001. We strive to provide the Internet research and operational community with reliable data that represent diverse types of users and can serve as a basis for modeling Internet traffic behavior and assessing future infrastructural needs.

The rest of the paper is organized as follows. Section II discusses the data collection, the methodology of our analysis and limitations of the available data. Section III presents our results. Section IV highlights conclusions and directions of future work.

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]. The archive contains traffic samples collected at various campus, research, and commercial sites listed in table I. A detailed description of the sites and the current status of measurements is available at [6]. We have analyzed traces captured at these sites during the period from November 1998 through May 2001. Three types of network interface cards were used for traffic monitoring: ForeRunner PCA-200E ATM [7], which we will refer to as FATM; Applied Telecom POINT OC12c PoS [8]; and University of Waikato Dag3.2 OC3c/OC12c ATM/PoS [9]. Note that the FATM card was not designed for high precision measurements and is prone to frequent inaccuracies in timestamping (see Section II-C).

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 duration of each trace ranges
from approximately 80 to 130 seconds. 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. To satisfy privacy requirements, IP addresses in the traces have been encrypted. While we do not know the actual IP addresses, we can count the total number of unique addresses observed in a trace.

The traces (and corresponding files in the NLANR archive) are named as `<Site Abbreviation>-<Capture Time>.<data format>.enc.gz`. Capture time is measured in UNIX time, i.e. seconds since 1970-01-01 00:00:00 GMT [10]. Files are in two formats: `.crt` (from FATM card) and `.tsh` (from POINT and DAG cards). The `.enc` and `.gz` extensions indicate that headers have been encrypted and that the data have been gzipped, respectively.

### 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 the `flow key` tuple of source IP address, source port, destination IP address, destination port, and protocol. 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. This definition of flow by the key and timeout mechanism and interval is similar to the one adopted in [11] and makes 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. We 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 [12] software suite to reduce raw traces. When studying the traffic metrics listed above, we divide traces into 30 s intervals and analyze each interval independently. We count the number of bytes, packets, and flows in each interval. Flows expire at interval boundaries; no timeout is used. We then collapse 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 80 and 130 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 applications, 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 application. 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 application per month.
C. Issues with the data

Since 1995 NLANR has been collecting IP packet header traces to support research in understanding Internet traffic workload characteristics. In the course of many months of analyses we noticed several problems in the raw data, making experimental results prone to errors and misinterpretations. We have developed solutions in the CoralReef software for known problems that would otherwise have affected the results of this paper.

A small percentage of archived traces are corrupt at the gzip level and yield an immediate error on input to CoralReef. They are unsuitable for further analysis and are discarded.

We have discovered that traces captured with an FATM card [7] (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. Note that the FATM clock problems, if not carefully addressed, may significantly influence the accuracy and validity of any results derived from packet timestamps (for example, estimates of the round-trip times for connections that traverse a given link [13]).

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 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. Analysis of TCP sequence numbers in these traces showed positive and negative jumps in the sequence numbers similar to those in the timestamps, at the same positions in the trace, indicating that it is not just the timestamps that are incorrect but that the cells are actually out of order. Often the timestamp discontinuities occur on block boundaries and a few hundred cells past a block boundary, with timestamps at the end of one monotonically increasing segment matching the timestamps at the beginning of a previous segment. This observation suggests that there was some mismanagement of blocks and the write pointer in the driver. Therefore we treat all cells before the last discontinuity as unreliable and eliminate them from our analysis.

CAIDA’s CoralReef version 3.5 handled clock resets in the first block by discarding cells before the reset. CoralReef 3.6 can also detect the other kinds of discontinuities, in any block, and can be configured to discard all data before the last discontinuity or just issue a warning about each discontinuity. Note that earlier versions of CoralReef (and possibly NLANR software) did not detect these errors and so may provide invalid results, especially when timestamps are involved in calculations, e.g. in determining traffic rates.

After a clock reset (which is probably caused by a firmware reload or reset), timestamps of the next several hundred cells increase at a rate much lower than in the rest of the trace. The different rate indicates that these packets were held in a buffer early in the card’s pipeline before they were timestamped, and then they were timestamped in quick succession. This problem affects packets received over a period of only a few microseconds at the beginning of the trace, which has negligible effect when measuring packet rates on scales of tens of seconds as in 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. Therefore, one cannot directly add together (or compare) absolute counts of {bytes, packets, flows} observed at different interfaces, and cannot interpret them as statistically independent uniform measurements of the same parameter. Data from different interfaces should always be treated separately and careful normalization is required in order to combine or compare them. In our analysis we solved 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.

Despite the data limitations described in this subsection, the NLANR archive of traces is currently the only long-term archive of data available for longitudinal studies of Internet traffic. It spans more than a three year time period and continues to grow. Measurements at different sites all take place on the same day of the month and, after encryption, collected traces are archived together. Although different types of cards captured the traffic at different times and locations, we were able to process the data in a uniform manner and derived four quantitative metrics of the Internet traffic. The uniform processing enables us to compare and contrast characteristics of traffic at different sites.

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.

Traffic from the monitored facilities (cf. Table I) exhibits diverse behavior. During the monitoring period some sites have had consistent growth, some have remained stable, and some have fluctuated between growth and reduction (cf. examples in figures 1). Packet rates (not shown) behaved similarly to bit rates.

We observed neither a clear diurnal pattern in the measured traffic nor consistent long-term growth. The data suggest that the common notion of Internet traffic universally and rapidly
increasing is not always true. 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 [14]. An unambiguous trend such as the steady increase in traffic at APAN in Figure 1(a) is an exception rather than a rule.

The dependence of the packet rate on the bit rate (examples in Figure 2) is close to linear for all monitored facilities. Therefore the inverse slope of the linear approximation line drawn through the data represents the mean packet length. Our data show that the mean packet length varies between 500 and 1000 bytes per packet for the majority of our sites (Figure 3). Note that mean values should be treated with caution when modeling traffic characteristics since the distribution of packet length is not Gaussian but rather a tri-modal distribution with maxima (in decreasing order) at 40, 1500, and 576 bytes per packet [2], [1], [15]. However, the mean packet length of these studies appears consistent with our results.

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 some 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 4 and 5 provide examples. While the packet rate scales linearly with the bit rate (Figure 2), the growth in the number of flows and the number of IP pairs is much slower. In both figures dashed 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 number of flows per second or the number of IP pairs per second. Solid lines correspond to linear dependence \( y \sim x \).

Figure 6 shows the value of exponent \( \alpha \) for packets, flows, and IP pairs for all monitored sites. In all cases the exponent is less than 1, and for flows and IP pairs it is usually about 0.5 or less. Clearly, the observed growth of these two metrics with the increased usage of a link is considerably slower than linear.

Arnoud [16] considered the \( N^2 \) phenomenon of the 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, hence the bit rate grows as the square of the number of flows. However, this interpretation is misleading. As stated in II-B, bit rate is a primary parameter measured in the network. It represents the objective measure of traffic and 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 our plots, i.e., putting the dependent (derived) variable on the X axis and the independent variable on the Y axis, would produce a result that has no physical meaning.

C. Usage Patterns

We now discuss the composition of traffic by application and trends in application use over time. Using CoralReef software we mapped the (protocol, source port, destination port) tuple of each IP packet in our traces to an application as found in CAIDA’s passive monitor report generator application list [17]. The list has been compiled by CAIDA from multiple sources among which is the IANA port assignment list [18] for well
known ports. There are currently 101 applications in our list. We further aggregated applications into 13 applications categories based on the similarity of their purpose and use. For example, such web-related applications as HTTP, HTTPS, and SQUID are combined into one category WWW; file-sharing applications such as NAPSTER, EDONKEY, GNUTELLA and similar ones constitute the P2P (peer-to-peer) category, etc.

Port numbers that we could not directly map to an application were aggregated in three unclassified categories based on the protocol used: Unclassified_TCP, Unclassified_UDP, and Unclassified_ICMP. A few of the grid computing sites (NCSA, SDSC, ANL) did carry significant amounts of Unclassified_UDP, likely a specialized grid application. The rest of the sites had negligible Unclassified_UDP traffic, and no site had significant Unclassified_TCP or Unclassified_ICMP traffic.

Altogether we used 16 groups of applications for the analysis below. Figure 7 presents the composition (in bytes, packets, and flows) of traffic observed at the SDSC commodity connection. Proportions of the various applications calculated for packets are similar to those for bytes, but are rather different if calculated for flows. Some applications generate more flows than others. For example, an ftp connection (belongs to our File_Transfer category) creates one data flow per file, while a single http connection (group WWW) may create many flows per single web click. Therefore, the proportion of WWW traffic counted in flows (Figure 7(c)) is higher than when counted in bytes or packets (Figures 7(a) and 7(b)).

The composition of traffic varies significantly from site to site. However it appears that the share of WWW traffic reached its maximum sometime between late 1999 and early 2000 and has been steady or decreasing since. Interestingly, this phenomenon coincides with the onset of noticeable amounts of P2P traffic in the Internet, probably indicating a genuine shift in Internet users’ interests.

IV. CONCLUSIONS AND FUTURE WORK

We have presented an overview of Internet traffic as seen from multiple observation points. Despite the limitations of the data, the publicly available NLANR PMA archive of traces offer useful insights into short-term variations and long-term evolution of Internet traffic.

We considered four 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 (see also discussion in [19]).

While the packet rate scales almost linearly with the bit rate,
the counts of flows and IP pairs grow considerably slower than the bit rate. This observation indicates a potential possibility of storing these parameters as part of a router’s state: the memory necessary for storage should grow slower than the CPU power required to process traversing packets.

We also found that a commonly accepted claim of Internet traffic constantly increasing at a high rate is not true for the prevailing majority of the monitored sites.

The mean packet length varies between 500 and 1000 bytes at different monitored sites. We are unable to study distributions of flow length from the NLANR archive because the traces are not long enough. Samples of traffic must last at least 24 hours in order to even approach capturing representative statistics of flow length distribution [20].

We have studied the mix of applications at the monitored sites in terms of three metrics: bytes, packets, and flows. The proportions of different groups of applications are highly variable from site to site. It appears that the growth of WWW traffic stopped at the end of 1999 when peer-to-peer traffic took off.

At present CAIDA is conducting regular measurements of a commercial OC-48 backbone link at the Metromedia Fiber Network (MFN) in San Jose. We have obtained several traces, each approximately one hour long. Analysis methodology and preliminary results are at [21]. Other research groups [4], [22] also are working to build passive monitoring equipment for use at high speed links. We will extend the analysis presented in this paper to new data as they become available.

REFERENCES


