IP Traffic Characterization for Planning and Control
V. Bolotin, J. Coombs-Reyes, D. Heyman, Y. Levy and D. Liu
AT&T Labs, 200 Laurel Avenue, Middletown, NJ 07748, U.S.A.

IP traffic modeling and engineering is a challenging area that has attracted an extensive research effort in recent years. Many studies show that the packet-level traffic from data networks, such as LANs, WANs, ATM, Frame Relay, Internet, etc., exhibits slowly decaying autocorrelation or long range dependence. In this paper, we discuss the key differences between traditional voice traffic and the IP traffic, and the challenging issues in IP traffic engineering and modeling. By using packet data collected on a corporate Intranet, we make several observations and recommendations that are new and have significant implications for the future of IP traffic characterization. We find that the slowly decaying autocorrelation phenomenon is mostly caused by flows of correlated packets and the existence of some periodic network management traffic. On the control time scale, we propose to identify the sources of the peaks that cause most of the performance problems, partition the traffic into classes of similar applications, and do characterization by class. On the planning time scale, we characterize traffic variations by a mixture of distributions that closely fit the empirical histogram formed from round-the-clock measurements during a fixed calendar period.

1. Introduction
As diverse data networks, each dedicated to a specific set of applications, are converging towards unified global networks based on the Internet Protocol (IP), the need to manage the performance of these networks and to deliver the required Quality of Service (QoS) to a wide range of applications becomes critical. The statistical properties of IP traffic are considerably different from the statistical properties of conventional voice traffic. A number of studies of different types of data networks (LANs, WANs) and services/applications (ATM, Frame Relay, WWW, etc.) have shown that the aggregated carried traffic, at the packet level, exhibits slowly decaying autocorrelation or Long Range Dependence (LRD) (e.g., [4, 5, 10]). However, these studies have not examined the nature of the traffic components and have not led to a practical methodology that can be used for planning and engineering.

The goal of traffic characterization is to develop an understanding of the nature of the traffic and devise tractable models that capture the important properties of the data and can eventually lead to accurate performance prediction. Which properties are important may depend on the traffic questions one wants to answer. The primary uses of traffic characterization are for

- long-range planning activities, such as network planning, design, and capacity management
- performance prediction, real-time traffic management, and network control.

These uses require different traffic characterizations. Network planning is concerned with the amounts and kinds of facilities that need to be deployed. This type of engineering decision usually is based on the stochastic nature of the traffic observed over long periods. The time scales for traffic

---

1 The work of this author was performed while on a summer internship at AT&T Labs. He is currently a Ph.D. student at School of Industrial and Systems Engineering, Georgia Institute of Technology.
characterizations that typically arise in network planning are denominated in minutes; 30 min and 1 hour are typical measurement intervals. We shall refer to such as *large time-scale characterization.*

On the other hand, traffic management and network control are concerned with real-time management of network resources, and the stochastic nature of the traffic over short time intervals is of paramount importance. Detailed models are needed that relate load over short intervals to network performance measures, such as packet loss rates and link delays, and application response times. The same models are used to determine critical occupancy levels for network components, which are in-turn used for planning and engineering. The time scales for this type of traffic characterization are denominated in seconds and fractions of a second. Accordingly, we refer to those as *small time-scale characterization.*

While most papers to date have attempted to model the aggregate packet or byte stream observed over a link, and a few papers (e.g. [2]) quantified the behavior of particular applications, in this paper we study the traffic of a corporate IP network on both large and small time scales. The aim here is to understand better the traffic characteristics, answer a few fundamental questions on the characteristics of IP traffic, and draw conclusions that can affect the planning and engineering of IP networks. For example, rather than just observing that the traffic exhibit long-range dependence, as manifested by slowly decaying autocorrelations at the packet level, we analyze the data and find that this behavior can be attributed to a few applications that generate periodic traffic, as well as the obvious correlation within packet flows. We note, however, that our study should be viewed as a first step in a long process that would eventually lead to a solid methodology for managing IP networks.

Our analysis is based on hourly data from several links on a corporate IP network, as well as a 7.5-hour packet trace from one WAN link connecting two major sites. We make several observations and recommendations that are new and have significant implications for the future of IP traffic characterization. For large-scale characterization, we propose the use of a mixture of normal distributions to capture the traffic behavior over all hours of the day. This can lead to a more accurate prediction of peak loads. On the issue of the critical time scale for capturing small time-scale behavior and modeling the queueing dynamics, our analysis indicates that it is on the order of one second. One of the most distinct phenomena in IP networks is the short bursts of packets generating peaks that can be an order of magnitude larger than the average traffic level and are the main source of performance degradation. We find that each of these peaks is usually generated by a single application, and that a few applications (two in our case) account for most of the peaks. The same observation holds for the behavior of the autocorrelation function, which is dominated by applications with large variance, typically the same applications that generate the large peaks. Our conclusion is that the partitioning of the traffic into classes of applications with similar behavior is a promising approach towards the effective modeling and control of IP traffic. The partitioning can be based on protocol, with special need to separate the control traffic from the data, and/or on groups of applications with similar behavior or performance requirements. In addition, due to the packet-level correlations, modeling at a higher level, like flow or session, is likely to be more effective. This approach is pursued in another paper [12] that uses a hierarchical two-class model separating TCP and UDP traffic.

The paper is organized as follows. The key differences between the traditional voice traffic and the IP traffic, and the challenging issues in IP traffic engineering and modeling are summarized in Section 2. In Section 3, we study the packet trace, examine the sources of short peaks, and shed some light on what is causing the slowly decaying autocorrelation function. In Section 4, we investigate the issue of the critical time scale for traffic management for IP traffic. Results on large time-scale characterization are summarized in Section 5. The conclusion and topics for further study are given in Section 6.
2. Overview of IP traffic characterization issues

The Poisson model of traffic that has worked well for voice traffic does not apply to IP traffic. Figure 2.1 shows five minutes of typical measured IP traffic from a corporate IP LAN and of simulated Poisson traffic for the packet arrivals. The average bit rate of the trace is 42.5 Kbps. The packet rate is 56.3 per sec for both the trace and the Poisson traffic. The peak to mean ratio of the Poisson traffic is 1.4; it's 4.1 for the IP traffic (in packets per sec). This is manifested in the figure by the larger range in the IP traces than in the Poisson trace. The auto-correlation function (ACF) plot shows that the number of bytes in 100ms intervals is correlated significantly, and the correlation can last longer than a minute. This means that periods of peak demands are likely to last for several seconds, and they are separated by (statistically) longer periods, as indicated in Figure 2.1.

![Figure 2.1 IP traffic and Poisson traffic](image)

The peak periods are analogous to the engineering or busy periods in voice traffic engineering. In traditional voice traffic, long-term peaks in the arrival rate correspond to surges in the number of calls, last for 15 min or longer, and usually occur at predictable times of the day. The lengths and arrival times of a few isolated calls do not have a big impact on the offered load. In contrast, with IP traffic, one large file download or database update (essentially one connection/session/transaction) can cause a huge burst in the traffic. Moreover, such small time-scale peaks can occur at any time during the day and the busiest hour may not contain the busiest seconds. Therefore, the concept of busy period does not work well with IP traffic. We shall illustrate this in detail in Section 5.

There is little interaction between congestion in voice networks and the offered traffic (except for extreme overloads that the network is not designed to handle when admission control is triggered). IP technology allows applications to seek more bandwidth when the network is lightly loaded. When there is congestion, packets are dropped and window flow-control may throttle the throughput to a lower rate, leading to longer transaction completion times. The transport layer protocol also may respond to congestion, so there is significant interaction between congestion in an IP network and the offered traffic (at the packet level).

IP networks serve a diverse set of applications, as opposed to circuit-switched networks, which serve mainly voice traffic as well as an ever-increasing demand for fax and Internet access. Clearly, if an IP network would be dedicated to voice traffic, or even to video conferencing traffic, its analysis and
design would be relatively simple. It is the unknown mix of applications and the unknown characteristics of many applications that make the task much more difficult for general IP networks.

As opposed to signaling traffic in circuit-switched networks, control packets in IP networks share resources with data packets. The control packets include both those that are used to set up and maintain connections, as well as a significant amount of packets that are used for routing and network management. On some network segments we observed, the percentage of control packets at times exceeded 30% of the total traffic. This raises the challenge of characterizing this traffic, as well as the question of how to classify and manage it.

In addition to all the differences mentioned above, the voice traffic has relatively stable growth and traffic pattern. On the other hand, IP traffic is complex in nature; the diverse connections (modem, LAN, cable, XDSL, satellite), the ever changing applications (HTTP is the dominant application today, but what is next?), and the tremendous growth of the traffic volume – all impose new challenges for traffic characterization and performance modeling of IP traffic.

3. Small Time-Scale Analysis

The heterogeneity of the IP traffic calls for the need to partition the traffic. Traffic from different applications, e.g. FTP, Telnet, IP voice, DNS, NTP, HTTP exhibit very different characteristics. In addition, there is a keen demand for preferential services for some business critical applications. To provide differentiated services based on the QoS class, understanding the traffic characteristics per class is the key to effective management of network resources.

The data we used for this study is a 7.5-hour WAN IP traffic trace from a corporate network. We chose a day with relatively light traffic so that the traffic characteristics are not altered much by the network. As an initial step, we divided the traffic into 4 classes and found that most of the peaks are caused by two applications. By looking at the autocorrelation of the byte counts of the applications, we found that the slowly decaying autocorrelation phenomenon is mostly caused by streams of correlated packets between source and destination sockets and the coexistence of some periodic network management traffic in the data.

3.1 Where do peaks come from?

We partition the data into 4 classes based on the port number used. The partition is done by the traffic volume and the distinct traffic behavior we observed. The classes are NTP, DNS, a Sybase application, and the rest. Table 3.1 is a summary of some statistics of the 4 classes.

<table>
<thead>
<tr>
<th>Bytes</th>
<th>Packets</th>
<th>Peak/mean ratio of Kbytes/sec</th>
<th>Variance and Coefficient of variation of Kbytes/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>MB</td>
<td>%</td>
<td>packets</td>
<td>%</td>
</tr>
<tr>
<td>All</td>
<td>134.2</td>
<td>100</td>
<td>914,558</td>
</tr>
<tr>
<td>NTP</td>
<td>26.8</td>
<td>20</td>
<td>352,780</td>
</tr>
<tr>
<td>Sybase</td>
<td>32.6</td>
<td>24</td>
<td>38,579</td>
</tr>
<tr>
<td>DNS</td>
<td>23.5</td>
<td>18</td>
<td>47,562</td>
</tr>
<tr>
<td>Rest</td>
<td>51.2</td>
<td>38</td>
<td>475,637</td>
</tr>
</tbody>
</table>

Table 3.1 Summary statistics for different applications

We see from Table 3.1 that NTP has significant traffic volume but small variance. This suggests that NTP generates relatively regular traffic. In contrast, the traffic from the Sybase application is highly bursty. It contains about 24% of the bytes, but only 4% of the packets. DNS exhibits similar behavior, though less variable than Sybase, and the rest is relatively regular.
One important observation to make here is that the variance is almost additive. We computed the correlation coefficient for each pair of applications and concluded that the traffic streams from different applications are not correlated.

Figure 3.1

Figure 3.1 shows the bytes per second for the different applications. The Sybase application usually consists of large file downloads, therefore the average packet size is much larger than the others. DNS has a mixture of some file downloads and some regular activity. We make two observations here. Firstly, each individual peak in Figure 3.1 is mostly caused by a single application. Secondly, only few applications generate the peaks. In this particular trace, it is mostly DNS and Sybase that account for the peaks. If traffic from Sybase and DNS is excluded, the remaining traffic is a lot smoother.

3.2 The myths about autocorrelation function in IP traffic

Many studies show that the packet level traffic from data networks, LANs, WANs, ATM, Frame Relay, WWW, etc., exhibits significant autocorrelation and long range dependence. We illustrate here through real network traffic traces that the slowly decaying autocorrelation phenomenon is mostly caused by streams of correlated packets between source and destination sockets and the coexistence of some periodic network management traffic in the data.

Figure 3.2 shows the autocorrelation functions (ACF) for the different applications. The large file downloads in Sybase lead to the short-range high autocorrelation. The pattern also manifests itself in the plot for All Traffic. The ACF for NTP clearly shows the regular periodic behavior. There is a 64-second timer, which causes the small spikes at multiples of 64. The periodic nature of the traffic
leads to the high and slowly decaying autocorrelation. It is easy to show that ACF of a superposition
is the weighted sum of the ACFs of its components, where a component’s weight is the proportion of
its variance to the sum of variances of all the components. This is the reason the slowly decaying part
of the ACF is more pronounced when the traffic from DNS and Sybase is excluded. The ACF for the
rest of the traffic seems to be well behaved.

![ACF Graphs for Different Applications](image)

**Figure 3.2** The ACFs for bytes per second for different applications

It is interesting to note that the weight of a given application in the ACF of the superposition is only
proportional to its variance and is independent of the traffic volume. Hence, a small fraction of the
traffic could potentially alter the ACF of the superposition.

The results of this section have many implications. Firstly, they suggest that modeling the traffic by
partitioning is a logical and promising approach. The example shows that one can gain insight by
partitioning the traffic into just 4 classes, analyzing them along with the superimposed process.
Secondly, based on this data set, the slowly decaying variance piece comes from NTP, which is the
most regular component of the traffic. Traffic from NTP clearly is not the cause for higher loss or
longer delay than the other traffic. It is the traffic from Sybase that would be the most damaging to
the performance of critical applications. This is another case where the short-range, high correlation
is more dominant in the queueing behavior than the long range dependent traffic ([8], [9]). Thirdly,
traffic from non-critical applications could be and should be controlled (e.g. by assigning to a low
priority class) to assure that critical applications meet their performance requirements.
4. Critical time scale for traffic engineering

The engineering time scale is the largest measurement interval that can be used for accurate traffic engineering. The trace collection tools can provide time granularity of 1 or 10 microseconds. In order to manage the data efficiently, some level of aggregation on the data is needed. It is evident that the smaller the measurement interval, the more information we need to collect, store, and analyze. On the other hand, the longer the measurement interval is, the less of the traffic characteristics remain. Hence, the trade-off is between the accuracy of the traffic characterization and the cost of obtaining and processing the data.

The data we use for this study is the same 7.5-hour WAN IP traffic trace used for the analysis in Section 3. Since we have time stamps at a granularity smaller than a millisecond, we can calculate what the measurements would have been had they been taken over intervals of 100ms, 1s, 1min, 15 min, etc. Figure 4.1 shows how different measurement intervals would describe the traffic (in Kbytes per second). A key observation here is that the peaks in the plots in the top row are at least five times as large as the peaks in the plots on the bottom row. The peaks of the 1s measurements are an order of magnitude larger than the peaks of the 15-minute measurements.

**Figure 4.1** Kbytes per second measurements averaged over different time intervals
In order to address the question of critical time scale, we use the technique of local Poissonification, as discussed in [11] and [13]. Suppose that measurements are taken in intervals of $T$ units of time. We obtain the packet counts in consecutive intervals of length $T$. For each interval, since the spacing within the measurement intervals is unknown, we distribute the packets independently and uniformly within the interval. By doing so, we form a point process which is referred to as the local poissonification of the original process. It is easy to see that the smaller the measurement interval, the closer the new process is to the original trace. The new process tends more and more to a Poisson process as the measurement interval increases.

The purpose of this construction is to reduce the behavior of the trace to that of a Poisson process within each measurement interval, while preserving interval counts, thereby retaining some of the “morphology” of the trace over longer intervals. The key idea here is to investigate the importance of the local spacing of the packets within the measurement interval.

In order to evaluate how well these processes represent the original trace, we simulate the performance of a router interface with these input processes and deterministic service time to determine the engineering time scale. The model is a single server queue with a finite buffer. The mean length of the packet queue (which is proportional to the mean packet-delay) and the proportion of packets that overflow the buffer are computed under different offered loads. We assume the buffer size to be 100 packets. The service time is adjusted to reflect the various offered loads. The baseline case uses the trace as the input to the queue. The Poissonification of the trace over intervals of 100ms, 1 second, 10 seconds, 30 seconds and 1 minute are also fed into the same queueing system. The results are shown in Figures 4.2.

From Figure 4.2, we see that 1-second counts are the largest interval that leads to good performance prediction over the load region of interest. The general consensus is that packet loss of 5% or higher is not acceptable. The smaller the measurement interval, the closer are the results to those of the traffic trace. These results indicate that the critical time scale for understanding the queueing dynamics is in the range of 100 ms to 1 second. Measurement intervals of larger size will lead to underestimation of the packet loss probability and queueing delay.

![Figure 4.2](image.png)

**Figure 4.2** Loss probability as a function of offered load
5. Patterns and Methods in Large Time-Scale Traffic Variation

As discussed in the introduction, traffic characterization is needed for two major goals: tracking and forecasting traffic demand and relating traffic demand to grade of service for engineering. While the second goal usually needs references to loads higher than the average loads, the demand characterization cannot be achieved accurately enough unless it is based on average loads: high loads are too volatile and occur rarely.

5.1. Traditional Methods – Busy Period and Extreme Value Engineering

Historically, one hour has become the base time interval for traffic characterization. Accordingly, traditional characterization of large-scale time variability of traffic has been based on the concept of busy hour. It had been long understood that the busy-hour representation of traffic variability obscures some peak traffic values that may occur outside the busy hour. Therefore alternative engineering techniques, generically called extreme value engineering, were developed (see, e.g., [6]). Serious inadequacies of extreme value engineering caused some Bell operating companies to revert to the busy-hour based engineering.

The extreme value techniques are based on probability models for extreme value statistics (e.g., [7]). There is no relation between the extreme value re-evaluation sample and overall hour-to-hour traffic distribution within the control time period (e.g., all 24 hours during all working days of one month). Thus, there is no relation between traffic description for tracking and forecasting traffic demand and traffic description for engineering. In contrast to this, our large-scale traffic characterization derives peak traffic values as part of the overall distribution, and prescribes continuous re-evaluation of the overall distribution.

This characterization method can be applied to traditional circuit-switching networks, but, as we show in this paper, it is of critical need for IP networks. Analysis of a large corporate IP network traffic indicated that variability of traffic over the time of day and from one day to another has so much volatility that it cannot be described in terms of extreme value engineering, much less in terms of busy periods. Moreover, due to such volatility the notion of large time-scale needs to be reduced from hours to minutes, and the proposed method is equally applicable to such time scales.

5.2. Probability Distribution Characterization of Large-Scale Traffic Variability

Figure 5.1 illustrates the volatility phenomenon as observed on a corporate WAN link with 2 Mbps capacity. Figure 5.1 is based on measurements of the hourly bit rate for all hours on 22 weekdays in April, 1998. Thus, the total number of measurement points is 24x22=528, and about 5% of those (28 points), with the highest bit rates, are positioned in the graph according to their day and hour. To discriminate further, the 28 points are divided into four groups: the seven highest (about 1.3% of all 528 hours), the next seven highest etc. One can observe that there is no specific pattern in the distribution of these points over days and clock hours, i.e., there is no distinct busy
Thus, we propose another representation of large-scale time variability patterns that do not have a distinct busy period. The analysis is based on the natural concept that in any large traffic sample set, formed as described above, there exist “homogeneous” subsets such that the points of a subset may be viewed as a sample from one distribution. This model was introduced in [1] in application to circuit-switched traffic. In that application, a subset is a sample of one-hour load on all weekdays of one month and can be described by a normal distribution with good accuracy. The total set is then a sample from a mixture of many distributions with different parameters. From the practical point of view, it is important that often a mixture of just two normal distributions is sufficient.

We characterize the traffic by a mixture of distributions that closely fit the empirical histogram formed from round-the-clock measurements during a fixed calendar period (e.g., four weeks). This method is applicable to any base interval, as large as the traditional one hour and as small as one second, which is critically needed for characterizing IP data traffic variability, as discussed in section 4. The characterization is illustrated below for one-hour and one-second base intervals.

To illustrate this approach we use more data on the same corporate link as in figure 5.1. The sample consists of hourly rates, in Mbps, measured from 12/97 to 4/98, 24 hours each day on 102 weekdays, the total of 2448 hour traffic points (the 4/98 data used in figure 5.1 is included). The histogram of this sample is shown in figure 5.2. Also shown in figure 5.2 is the model based on a mixture of two normal distributions. The three curves are the two normal components of the mixture and the mixture distribution. It is critical to make the distinction between the natural actual mixture of many distributions and its model by a mixture of two distributions. First, the two distinct peaks in the middle of the histogram indicate that the mixture-of-two model does not exactly match those two distinctive parts of the total set (each part is, in turn, a mixture of many distributions). Notwithstanding the differences, the cumulative distribution function in figure 5.2 indicates an excellent degree of overall approximation that provides a basis for three major applications of the mixture-of-two model:

-...
1. Demand estimation

2. Extreme value estimation – figure 5.2 indicates that the model is good enough for estimating the tail probabilities. This approach is conceptually different from extreme value methodologies, in which extreme traffic values had always been considered as independent of the rest of the distribution. The new approach establishes relations between the distribution and its peak values.

3. Trend tracking – continuous re-evaluation of the empirical distribution and its mixture-of-two model with time will make it possible to track changes not only with regard to the average demand, but with regard to the form of the distribution and its model, including extreme values. Note that essential changes in the core of the distribution can be noticed long before changes in extreme values – sufficient statistical data for those would require significantly more time.

5.3. Practical Considerations

When the characterization method is applied, very large traffic peaks cannot be and should not be taken into account. The following classification helps to separate those peaks. Peak traffic values on an IP link can be classified into predictable and unpredictable. The latter occur as a result of unusual events (market conditions, weather conditions etc.); obviously these peak values cannot be accounted for. Although the predictable peaks are quantifiable, some very large ones are normally not taken into account because of economical considerations – it would be too expensive to engineer the network otherwise. Any congestion during these rare peaks is usually handled by giving priority to the most important traffic, by designing the equipment to maintain reasonable throughput, etc. The remaining peak traffic is to be characterized by a probability distribution as described above.

To conclude, traffic characterization by a distribution over all clock hours during a fixed calendar period (a month, 8 weeks etc.) solves the two major problems:

- It resolves the problem of traffic engineering and traffic management in a traffic environment without a distinct busy period, especially in case of small base time interval
- It allows establishing more precise relations between peak values and the core of the distribution (in comparison with the traditional empirical characteristics, such as high-day-to-average-busy-season ratio).

5.4. Analyzing Gap between Large-Scale and Small-Scale Characterization

Figure 5.3 serves as the introduction to the issue. In this case, the sample is the second-by-second bit rate recorded by continuous seven-hour measurements. That includes all traffic on the LAN, local, domestic and global, and many traffic classes. There are so many different traffic sources, each contributing a very small fraction of the total traffic, that it would be natural to think of the total traffic distribution as a mixture of many distributions. Figure 5.3 indicates that this mixture of many distributions has been accurately described by a mixture of just three normal distributions. Since the second-by-second traffic counts are correlated, the one-second scale cannot be used to bridge the small-scale and large-scale characterization.
However, these results show the same normal-mixture phenomenon both on the hour scale and on the second scale. In addition, this phenomenon was observed in regard to the sets of five-minute rates, where each five-minute rate is the highest within its clock hour. Therefore, it is reasonable to expect a normal-mixture distribution of rates on other scales between one second and one hour.

That expectation provides the basis for further analysis. The larger the interval, the less is the correlation between the rates in adjacent intervals. Therefore, gradually increasing the time scale from one second, one can find the smallest time interval without significant correlation. This interval will serve as the basis for large-scale traffic characterization.

6. Conclusion

Based on data from a corporate IP network, we presented several new observations and recommendations on IP traffic characterization. The findings and proposals are on the practice rather than theory track, and they provide significant progress towards effective methods for traffic characterization, performance modeling, and planning and engineering. Future work needs to first validate our findings with data from other networks, and then to further develop the methods into automated tools for traffic analysis and performance models. Of particular interest is similar analysis of links with higher load and higher capacity.

Although not directly addressed in this paper, one of the major challenges facing the operators of IP networks is the need to provide different quality of service (QoS) grades, or at least differentiated service levels, to specified classes of applications. Since the results reported here are based on partitioning of the traffic into classes of applications with similar behavior and/or requirements, they can lead to a successful approach to the modeling and engineering of QoS-capable networks.

References