Journal of Research in Science, Technology, Engineering and Management (JoRSTEM)
ISSN: 2456-0197

Internet Traffic Measurement: An Overview

Atul Kumar

B. Tech., Department of CSE, Malla Reddy Engineering College, Secunderaba.

Abstract - ***This tutorial article discusses the role of network traffic measurement in the design, testing, and evaluation of Internet protocols and applications. As the number of Internet users increasing rapidly in this world, Internet traffic is also increased. In computer network traffic measurement is the process of measuring the amount and type of traffic on a particular network. Internet traffic measurement and analysis are mostly used to characterize and analysis of network usage and user behaviour, but faces the problem of scalability under the explosive growth of Internet traffic and high speed access. To analyse this traffic multiple tools are available. But they do not perform well when the traffic data size increase. As data grows it is necessary to increase the necessary infrastructure to process it. The article begins with some background information on Internet traffic measurement, and then proceeds to discuss the "tools of the trade", including examples of both hardware-based and software-based approaches to network traffic measurement.***

Keywords – Internet, Traffic Measurement, Applications, Network Troubleshooting, Workload Characteristics.

I. INTRODUCTION

The evolution of the Internet over the last thirty years has been accompanied by the development, growth, and use of a wide variety of network applications. Network monitoring and measurement have become more and more important in a modern complicated network. Few applications range from text-based utilities such as file transfer, remote login, electronic mail, and network news from the early days of the Internet, to the advent of desktop videoconferencing, multimedia streaming, the World-Wide Web, and electronic commerce on today's Internet. In the past, administrators might only monitor a few network devices or less than a hundred computers. Now they need more sophisticated network traffic monitoring and analysis tools in order to maintain the network system stability and availability such as to fix network problems on time. Using specialized network measurement hardware or software, a networking researcher can collect detailed information about the transmission of packets on the network, including their timing structure and contents. Moreover, they have to regularly check the network performance if the network devices are overloaded. Before a failure due to the overload, information about network usage can be used to make a network plan for short-term and long-term future improvement.

II. APPLICATION

A. Network Troubleshooting

Computer networks are not infallible. Often, a single malfunctioning piece of equipment can disrupt the operation of an entire network, or at least degrade performance significantly. Examples of such scenarios include "broadcast storms", illegal packet sizes, incorrect addresses, and security attacks. In such scenarios, detailed measurements from the operational network can often provide a network administrator with the information required to pinpoint and solve the problem.

B. Protocol Debugging.

Developers often want to test out "new, improved" versions of network applications and protocols. Network traffic measurement provides a means to ensure the correct operation of the new protocol or application, its conformance to required standards, and (if necessary) its backward-compatibility with previous versions, prior to unleashing it on a production network.

C. Workload Characterization.

Network traffic measurements can be used as input to the workload characterization process, which analyzes empirical data (often using statistical techniques) to extract salient and representative properties describing a network application or protocol. Knowledge of the workload characteristics can then lead to the design of better protocols and networks for supporting the application.

D. Performance Evaluation.

Finally, network traffic measurements can be used to determine how well a given protocol or application is performing in the Internet. Detailed analysis of network measurements can help identify performance bottlenecks. Once these performance problems are addressed, new versions of the protocols can provide better (i.e., faster) performance for the end users of Internet applications.

At the first sight, measuring network characteristics by observing network traffic looks like doing things the hard way. After all, a network is man-made system whose component characteristics are known so it should be possible to construct an exact model for simulations. However, there are several reasons why this is not as trivial as it looks. Network operators have knowledge of their network structure and configuration, but this information is usually for their own use only and not published. Network topology, physical locations and detailed information, such as equipment hardware and software versions and configuration parameters, are kept secret both for security and competitive reasons. Furthermore, several changes take place in networks daily, making it even more difficult to acquire consistent snapshot of the network. The network characteristics are also changed abruptly by failures, which are difficult to model because of their random nature and unknown parameters. Another unknown factor in networks is the characteristics of network traffic. New applications emerge and proportion of each application of total traffic changes. Network users adopt quickly new applications if they find them useful. Even distribution of traffic flow directions may change, the latest example being peer-to-peer sharing applications where communication is mesh-like rather than server-centric. Additional traffic sources are malicious worms, which spread either automatically or human assisted utilising Security Problems in Software.

III. CONCLUSION

Being able to monitor and analyze networks is vital in the job of Network Administrators. They must strive to keep the networks they oversee in good health as to not disrupt productivity within a company and to not disrupt any essential public services. As summarized throughout this paper several routers based and non-router based techniques are available to assist Network Administrators in the day to day monitoring and analysis of their networks. When choosing a particular tool to use for monitoring, an Admin must first decide if they would like to use a more proven system or a newer system.

REFERENCES

[1] M. Arlitt and C. Williamson, “Internet Web Servers: Workload Characterization and Performance Implications”, IEEE/ACM Transactions on Networking, Vol. 5, No. 5, pp. 815-826, October 1997.

[2] P. Barford and M. Crovella, “Measuring Web Performance in the Wide Area”, ACM Performance Evaluation Review, Vol. 27, No. 2, pp. 37-48, September 1999.

[3] L. Breslau, P. Cao, L. Fan, G. Phillips, and S. Shenker, “Web Caching and Zipf-like Distributions: Evidence and Implications”, Proceedings of the IEEE Infocom Conference, New York, NY, pp. 126-134, March 1999.

[4] R. Caceres, P. Danzig, S. Jamin and D. Mitzel, “Characteristics of Wide-Area TCP/IP Conversations”, Proceedings of ACM SIGCOMM, Zuric ¨ h, Switzerland, pp. 101-112, September 1991.

[5] J. Cao, W. Cleveland, D. Lin, and D. Sun, “On the Nonstationarity of Internet Traffic”, Proceedings of ACM SIGMETRICS, Cambridge, MA, pp. 102-112, June 2001.

[6] M. Crovella and A. Bestavros, “Self-Similarity in World Wide Web Traffic: Evidence and Possible Causes”, IEEE/ACM Transactions on Networking, Vol. 5, No. 6, pp. 835-846, December 1997.