Simulation and Monitoring of a University Network for Bandwidth Efficiency Utilization

Samuel N. John[1], Charles Ndujuiba[2], Robert Okonigene[3], Ndeche Kenechukwu[4]
[1,2,4]Department of Electrical and Information Engineering, Covenant University, Ota, Ogun State, Nigeria.
[3]Department of Electrical and Electronics Engineering, Ambrose Alli University, Ekpoma, Edo State, Nigeria.
[1]samuel.john@covenantuniversity.edu.ng, [2]charles.ndujiuba@covenantuniversity.edu.ng,
[3]robokonigene@yahoo.com, [4]kene.ndeche@gmail.com

Abstract - *As organization networks grow, it is essential that network administrators have knowledge of the different types of traffic traversing their networks and the methods of monitoring such traffic. Traffic monitoring and analysis is essential in order to troubleshoot and resolve issues as they occur in order not to bring the network to a total collapse. There are numerous tools and methods available for network traffic monitoring and analysis, no administrator can effectively carry out such activities without in-depth knowledge of the traffic on the network. The inefficient management of the network traffic may result into network collapse or degradation and these may negatively affect the network performance of the Corporate or University networks. This paper therefore, proposed a developed network topology and simulation to monitor the network performance. Therefore, achieving an effective management and controlling of the increase traffic flows in the network. The result obtained shows a better network performance in the bandwidth usage and utilization of the University network.*

Keywords: Network Monitoring, Simulation, Performance, Utilization, Efficiency.

1. Introduction

In today's IT-driven world, network administrators are tasked with the challenge of coping with increasingly expanding networks and providing excellent network performance around the clock in order to reduce down time to the barest minimum and thereby increasing business process with high productivity and maintaining or increasing revenue.

"Networking" is the buzz word of our times, networks are all around us. Networks are the key to
our life – virtually anything is connected with something other: Persons, corporations and their shareholders, our private and public life. Any structure that emerges from the mutual ties of its components may be conceived as a network [1, 2]. Network Monitoring is an active network communications practice for diagnosing problems and gathering statistics for administration and fine tuning, resulting in efficient bandwidth utilization and increasing the efficiency of data exchange in the network [3, 4]. Network monitoring for a corporate network is a critical IT function that can save money in network performance, employee productivity and infrastructure cost overruns. A network monitoring system monitors an internal network for problems. It can find and help resolve snail-paced webpage downloads, lost-in-space e-mail, questionable user activity and file delivery caused by overloaded, crashed servers, dicey network connections or other devices [5, 6].

Network monitoring can be achieved using various types of software or a combination of plug-and-play hardware and software appliance solutions. Virtually any kind of network can be monitored. It doesn't matter whether it's wireless or wired, a corporate LAN, VPN or service provider WAN. Devices on different operating systems with a multitude of functions, ranging from BlackBerrys and cell phones, to servers, routers and switches can be monitored. These systems can help in identifying specific activities and performance metrics, producing results that enable a business to address various and sundry needs, including meeting compliance requirements, stomping out internal security threats and providing more operational visibility [7, 8].

Network simulation, on the other hand, is a technique where a program models the behavior of a network either by calculating the interaction between the different network entities (hosts/routers, data links, packets, etc). using mathematical formulas, or actually capturing and playing back observations from a production network. The behavior of the network and the various applications and services it supports can then be observed in a test laboratory; various attributes of the environment can also be modified in a controlled manner to assess how the network would behave under different conditions [10, 12, 14].

Network simulators attempt to model real world networks. The idea being that if a system can be modeled, then features of the model can be changed and the results analyzed. As the process of model modification is relatively cheap and where a wide variety of scenarios can be analyzed at low cost (relative to making changes to a real network) [9, 11].

This project covers an investigation and recommendation of a network monitoring system for Covenant University. During the course of this project, research was conducted into the systems used by other organizations and the attitude and practices of both users and administrators on the network.

Since making changes to the networks are expensive and mistakes can cost a lot of money to rectify, Covenant University (CU) has a need for information regarding its network and this project aims at solving the challenges arising from the services provided by the Network Operating Center (NOC). By its nature the CU network contains a large number of computers connected wired and wireless which are not under direct control of the NOC. Also, a small percentage of the users on the network engage in illegal practices and do not adhere to the rules and regulations of the university network policy. It is known that, a good percentage of the students' downloaded files (often large files such as movies, videos and games) not only slowing the network but putting the institution at risk of prosecution from the legitimate/copyright owners of such files. Hence, the creation of a network monitoring system controlled by and created specifically for the academic needs of the institution cannot be overemphasized for an effective and efficient usage of bandwidth.

2. Specification of the Network Parameters

In performing this task, the following specifications/requirements were set for the proposed network:

- Traffic graphs,
- Details of data packet generation per time including packet flow and size,
- Graphic warning of any possible packet collisions observed,
- Details of traffic on critical ports or channels,
- Details of other dubious traffic or odd traffic patterns.

In order to generate a detailed report on the network performance it is imperative to have knowledge of the following performance metrics: Latency, Packet Size, Bandwidth, Throughput etc [7, 8].

3. Methodology

The processes involved with the implementation of this work were outlined and the different segments presented. Details regarding the technologies and tools utilized in developing the system, particularly the software implementation are also discussed with an overview of reports generated from the monitoring system.

The model follows a real topology of a section of Covenant University network and the performance characteristics of the model were to be ascertained. To determine this, server applications were modeled over the internet and local intranet and their performances evaluated.

Network simulation software was used in the simulation of the network and measurement of device performance and management applications in a virtual, scalable network environment [13]. This simulation package runs under Windows environment and it comprises a set of decision supporting tools, providing a comprehensive development environment for specification, simulation and performance analysis of communication networks, computer systems and applications.

4. Current Covenant University Network Layout

The Covenant University network is an enterprise class network with several network segments and hierarchies. Internet is provisioned on the network through two radio links terminated at two different service provider ports. The first service provider 21st Cenury GUAP-SAT1 (Google) provides 25Mbps of download traffic to the staff segment of the network while the second is eTranzact (MainOne) which provides a bandwidth of 60Mbps to the student segment as shown in Figure 1. The network has a 4-layer hierarchy which is broken down into the student segment and the staff segment. Dedicated elements are used in each segment not beyond the distribution switch. The network itself is based on a cascaded topology and all remote buildings are linked up to a central office as shown in Figure 2. As a campus there are central buildings and switches installed per building. Thus the switches can be seen as the connection point and an identity for each building.

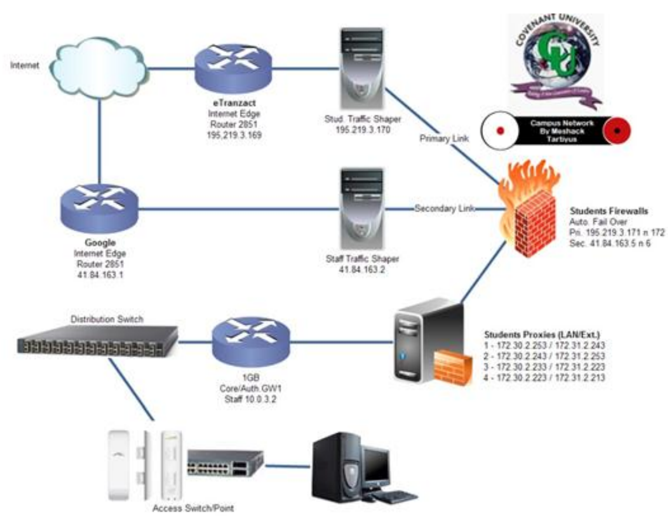

Figure 1. The Core Topology of the Covenant University Network

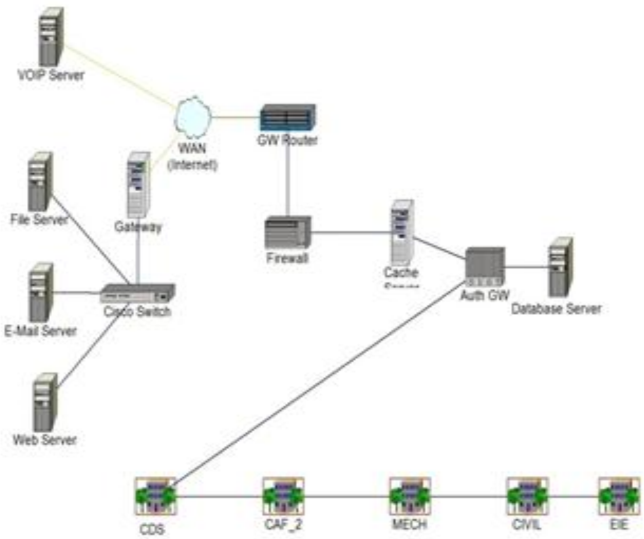

Figure 2. Current Covenant University Cascaded Network Topology

The current model is divided into 2 sections at the Gateway (GW) Router: the outside internet and the University network. The outside internet is represented by the VoIP, Web, Email and File servers (Figure 1). The University internet has a firewall which is designed to filter packets coming into the network. The Authentication Gateway router is connected to the Cache Server, The Database Server and the buildings. The buildings are linked to one another in a cascade arrangement with a link connecting the CDS building to the Authentication Gateway router (Figure 2). This means that packets from the gateway router to the various buildings must pass through the CDS building.

5. The Proposed Covenant University Network Layout

The proposed network model is analogous to the current network topology setup except that the internal network distribution from the Authentication Gateway Router through the Cache Server, and the Database Server to the buildings is in star topology as shown in Figure 3. The buildings therefore, are now connected directly to the Authentication gateway router which means that packets from the gateway are transmitted directly to the various buildings of the University.

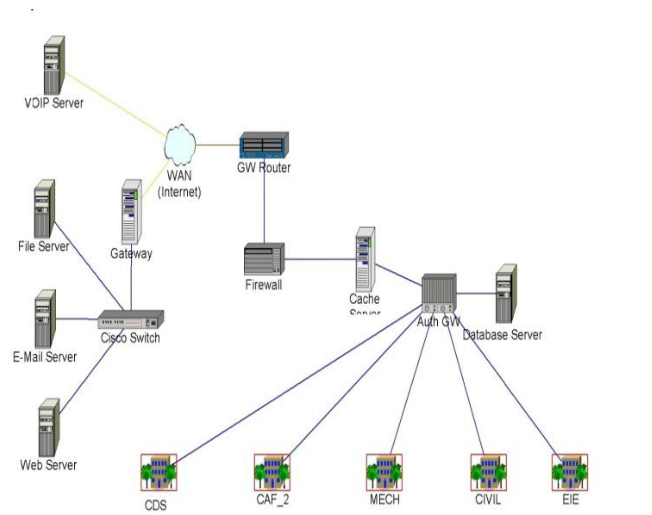

Figure 3. Diagram of the Proposed Covenant University Star Network Topology

6. Implementation and Testing

Each building network is composed of 19 systems distributed across 3 switches out of which one is selected for the report statistics. The applications modeled were VoIP Server, File Server, Email Server and Web Server. Two models were simulated, the current Covenant University network model showing critical areas of the network and an improved model based on the current model correcting bottlenecks and increasing efficiency on the network as shown in Figure 4.

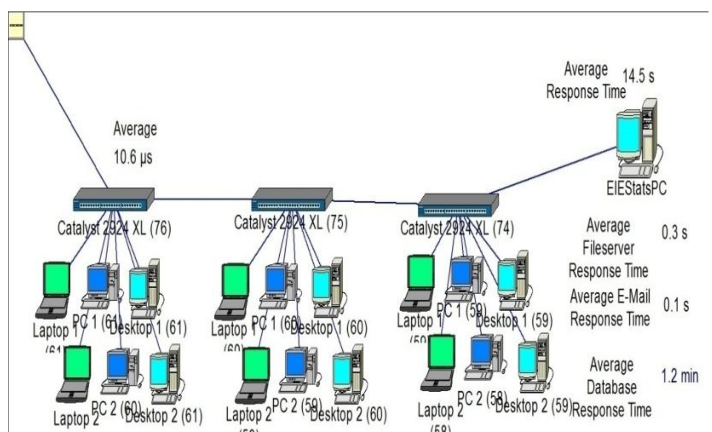

Figure 4. Average Response Time of a Sample Building System Distribution for the Current Network

The average response time on the EIE Stats PC is 14.5s while the average response time for file server, Email and Database applications are 0.3seconds, 0.1 seconds and 1.2 minutes respectively. Also, the average response time on the CDS Stats PC is 12.5s while the average response time for file server, Email and Database applications are 343.9

milliseconds, 51.4 milliseconds and 70.8 seconds respectively. Figure 5, shows the result and average response time of sample system distribution for the proposed network topology.

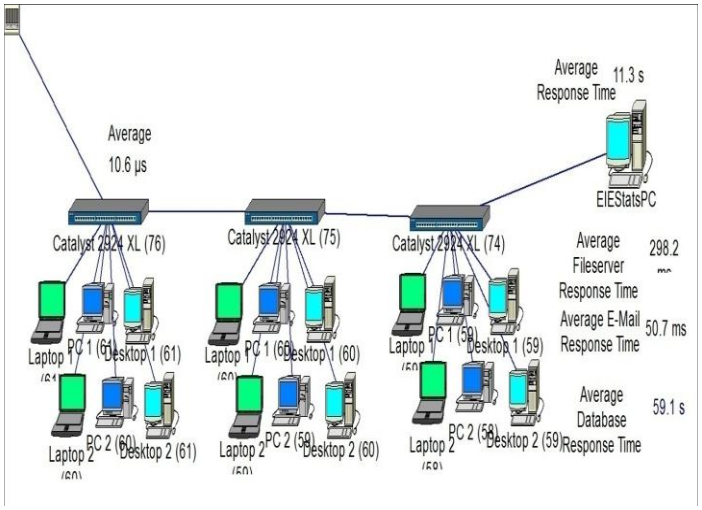

Figure 5. Average Response Time of a Sample Building System Distribution for the proposed Network

7. Results and Analysis

The results measured at the Authentication Gateway for the Networks are shown in Table 1, Table 2 and Table 3 shows the comparison between the application response times of EIE building and CDS building.

Table 1. Metrics Measurement Results at the Authentication Gateway for Current Network.

Packet Size (Kbytes)	Average Delay (μs)	No. of Packets	Throughput (Mbps)
10	23.1	3691	4.1
30	41.3	5035	3.4
40	53.7	4881	2.8
50	66.9	4339	2.6
60	75.9	5271	2.5

Table 2. Metrics Measurement Results at the Authentication Gateway for Proposed Network.

Packet Size (Kbytes)	Average Delay (μs)	No. of Packets	Throughput (Mbps)
10	12.5	4160	1
20	13	4116	1
30	12.5	4587	1.1
40	13.1	4707	1.1
50	12.4	5385	1.1
60	12.2	5257	1.2

Table 3. Comparison between the Application Response Times of EIE Building and CDS Building.

Metrics	**Current Model**	**Improved Model**
Average Response Time (EIE)	14.5 s	11.3 s
Average File Server Response Time (EIE)	300 ms	289.2 ms
Average Email Server Response Time (EIE)	100 ms	50.7 ms
Average Database Server Response Time (EIE)	72 s	59.1 s
Average Response Time (CDS)	12.5 s	11.1 s
Average File Server Response Time (CDS)	343.9 ms	290.8 ms
Average Email Server Response Time (CDS)	51.4 ms	50.8 ms
Average Database Server Response Time (CDS)	70.8 s	59.6 s

Figure 6 shows the measurement of throughput against packet size for current and proposed networks of the University. This result indicates that as the packets sizes increases, the throughput for the current network decreases while the throughput for the proposed network increases. This trend shows a better bandwidth utilization and efficiency in the proposed star network than in the current cascaded network topology.

In Figure 7, the average delay of the proposed network topology is relatively constant with an optimized characteristic while the average delay of the current network topology increases as the packet sizes increase. This will result into a better bandwidth utilization and network performance of the proposed network than the current network.

8. Conclusion

For network operators and administrators, network monitoring and analysis provides the means of being proactive (i.e. ability to detect faults prior to a network experiencing downtime). It also allows them manage service level contracts, to be assured of day-to-day operations and to validate system changes. The result of this work shows a highly improved network performance in the proposed star network topology than in the current cascaded network topology. This is an evidence of an optimized characteristic shown by the proposed star network topology

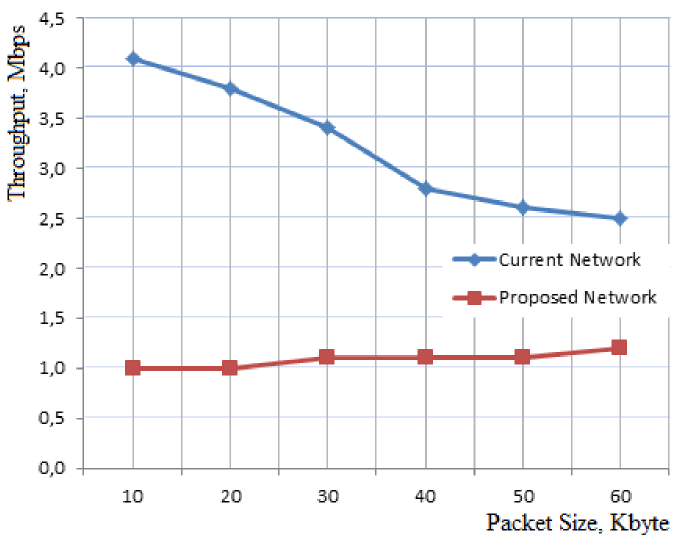

Figure 6. Measurement of Throughput against Packet size for Current and proposed Networks

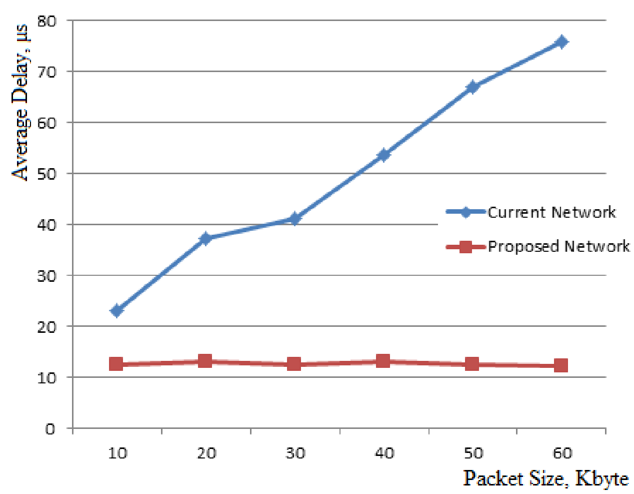

Figure 7. Measurement of Average Delay against Packet size for Current and proposed Networks

9. References

[1] Douglas Comer, Computer Networks and Internets , page 99 ff, Prentice Hall 2008.

[2] Kurose, James F. & Ross, Keith W. (2007), "Computer Networking: A Top-Down Approach" ISBN 0-321-49770-8.

[3] John S. N., Anoprienko A. A., Okonigene R. E.: “Developed Algorithm for Increasing the Efficiency of Data Exchange in a Computer Network”: International Journal of Computer Applications (0975 – 8887), Volume 6– No.9, pp. 16-19, September 2010, Foundation of Computer Science, USA Impact Factor = 0.835: www.ourglocal.com/journal/?issn=09758887.

[4] John S.N., Okonigene R.E., Matthews V.O., Akinade B., Chukwu I.S.: “Managing and Improving upon Bandwidth Challenges in Computer Network”, Journal of Emerging Trends in Engineering and Applied Sciences (JETEAS 2011) (Volume 2 Number 3) ISSN: 2141-7016, UK.

[5]http://www.masswerk.at/netmonitor2/netmonitor_1_en_help/intro.html., “An Introduction to Networks”. *Masswerk Website*. [Online] 2011. [Cited: December 20, 2011].

[6] Fred Halsall, Introduction to data communications and computer networks, page 108, Addison-Wesley, 1985.

[7] S.N. John, F.A. Ibikunle, A.A. Adewale: “Performance Improvement of Wireless Network Based on Effective Data Transmission”, The International Conference on Wireless, Mobile and Multimedia Networks organized by IET, 11-12 January 2008, IEEE Xplore Digital Library Journal: ISSN 0537-9989, pp.134-137, @ IEEE Xplore Digital Library, 2008, USA.

[8] John S.N., Akinade B.A., Chukwu I.S.: Wide Area Network Efficiency Through Optimization of Key Performance Indices: Proceedings: International Conference NIGERCON 2010, June 17 -19, 2010, pp., Rockview Hotel, Abuja.

[9] Penttinen A., Chapter 9 – Simulation, Lecture Notes: S-38.145 - Introduction to Teletraffic Theory, Helsinki University of Technology, Fall, 1999.

[10] Kennedy I. G., Traffic Simulation, School of Electrical and Information Engineering, University of the Witwatersrand, 2003.

[11] John S.N., Atayero A. A.: “Simulation of the Effect of Data Exchange Mode Analysis on Network Throughput», European Journal of Scientific Research ISSN 1450-216X,

Vol.24 No.2 (2008), pp.244-252, © EuroJournals Publishing, Inc. 2008.

[12] Anoprienko A.Y., John S.N.: "Basic Approaches to Simulation and Research of Network Infrastructure", Proceedings: "3rd International Scientific Technical Conference", (Integrated Computer Technology in Machine Construction), IKTM): Kharkov National Aeronautic University, Kharkov, Ukraine, Nov. 24th-27th, pp. 98, 2003.

[13] Netcraker Professional 4.1, http://www.netcracker.com/en/services/overview/ 2013.

[14] Flood, J.E. Telecommunications Switching, Traffic and Networks, Chapter 4: Telecommunications Traffic, New York: Prentice-Hall, 1998.