Network Traffic Analysis: A Case Study of ABU Network

SB .A. Mohammed
Department of Electrical and
Computer Engineering,
ABU, Zaria, Nigeria

Dr.S.M Sani
Senior Lecturer, Department of
Electrical and Computer Engineering,
ABU, Zaria, Nigeria

Dr. D.D. DAJAB
Director ICT, ABU Zaria
Electrical and Computer Engineering,
ABU, Zaria, Nigeria

Abstract

The Internet is being viewed as a critical component of success by the researchers, teachers and students in the Universities and Colleges. The Objectives of thesis is to identify unproductive network based applications responsible for consuming valuable bandwidth of University network system and to enhance utility of productive applications on a University network. This research work, geared towards analysis on the internet traffic network's of Ahmadu Bello University (ABU), Zaria as a case study. the monitoring of network traffic was conducted by bandwidth monitoring software, a packet sniffer (using Wireshark Version 165, SVR Rev 40429) configured as a gateway between the University network system and the internet over a 90-day monitoring period in a schedule of 15 minutes daily, 30 minutes weekly and 2 hours monthly. The data (packets) captures was further analysed using MATLAB which is a tool for graphing network data from which conclusions from the graphs was drawn that ABU's current network traffic is underutilized and far from optimal in terms of Internet Inbound/Outbound traffic generated by its users (staff/students). It has also been observed that defensive bandwidth management is insufficient in respect to the institution's aims and objectives on its network usage. This emphasises the need for improved bandwidth management and optimization.

Keyword: Network monitoring traffic, Monitoring software (packet sniffer), Packet capture and Traffic analysis.

1. Introduction

The rapid growth of the Internet in size, complexity and traffic types has made network management a challenging task. The ability of a monitoring system to provide accurate information about the nature and type of the network traffic cannot be over emphasized. Information about who is generating the most traffic, what protocols are in use, where is the traffic originating from or where is the destination of the traffic can be very important to solving congestion problems. Many network administrators spend a lot of time trying to know what is degrading the performance of their network [4]. A typical solution to congestion problem is to upgrade network infrastructure, i.e. replace servers with high end servers and increase the bandwidth. This solution is expensive, short term and does not scale. As soon as the upgrade is done the congestion problem will improve for a while and later gradually deteriorate as the users change their behavior in response to the upgrade. The alternative solution to this problem is to deploy a scalable network traffic monitoring and analysis system, in order to understand the dynamics of the traffic and changes in the internet and overall stability of the network. In addition to knowing the health status of the network, monitoring of network activity also has the benefits of detecting denial of service (DoS) and bandwidth theft attacks. In order to conduct analysis of wide range of network behaviors, it is necessary to collect network traffic on a continuous basis rather than as a onetime event which only captures transient behaviors that provides insight into network problems. Collecting long term network traffic data will provide valuable information for improving and understanding the actual network dynamics [1]

2. Background

The type of connectivity used to link the Institution to the Internet Service Provider are Leased Line – Fiber and Leased Line – Radio link/Wireless Satellite/VSAT (3.88m Dish). The University connects to the Cisco router, and the capacity connection for two satellite i.e. Intelsat satellite

(Downlink: 3.5Mbps/ Uplink: 512Kbps) and I- direct satellite (Downlink: 1.5Mbps/ Uplink: 512Kbps) and currently connect to the Line – Fiber with Synchronous Transport Module level-1(SMT-1) from GLO which has a bit rate of 155.52 Mbps. The Overall capacity is**:**
Uplink (Mbps):156.52Mbps

Downlink (Mbps):160.52Mbps

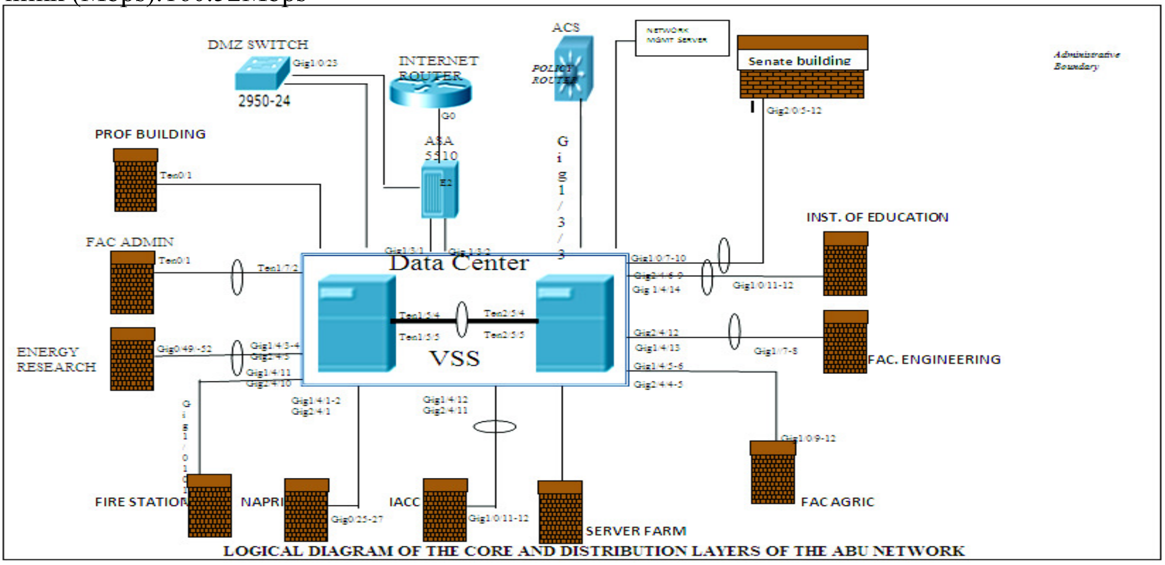


Figure 1: Logical Diagram of the core and Distribution Layers of the ABU Network

Figure 1 shows the core and distribution layer of the entire ABU network diagram based on the Cisco 3-layer model. It shows has shown the major nodes and connection points in the distribution layer of the institution's network and shows a direct connection of the Layer 3 Switch (MLS or ACS) to the Data Center backbone on interface Gig 1/3/3.The connections between the network nodes are implemented with optical fibers links (i.e. Single Mode cable) which interlink the nodes of the , Senate building, Institutes of Education, Faculty of Engineering, Agric, Art, Administration, Energy Research and NAPRI e.t.c

The backbone network is based on **Gigabit Ethernet technology.** These connections are implemented via single-mode optical fiber which has the following features;

i. Relatively narrow diameter, through which only one mode will propagate typically 1310 or 1550nm.

ii. Higher transmission rate

The small core and single light-wave virtually eliminate any distortion that could result from overlapping light pulses, providing the least signal attenuation and the highest transmission speeds of any fiber cable type. The TCP/IP suite of protocols is the set of protocols used to communicate across the internet. It is also widely used on many organizational networks due to its flexibility and wide array of functionality provided [4].These TCP/IP suites of protocols are the sources of different networked application. TCP/IP suites of protocols are assessed by showing the percentage each of the network protocols. Moreover, the TCP/IP protocols analysis can be used to clearly show the percentage of traffic consumption which can be used as input for bandwidth allocation in intercampus network. The TCP/IP suites of protocols that is interested in are: FTP, Telnet, SMTP, HTTP, TCP, UDP, ICMP, ARP, DNS, eDonkey, SNMP, DHCP, SSH, Telnet, NetBIOS, and POP3.

2.1 Network monitoring:

Is the ongoing process of collecting information about various aspects of network operations. By carefully analyzing this data, you can identify faults; find cases of waste and unauthorized access, and spot trends that may indicate future problems. Implementation is the step of implementing traffic shaping, filtering, caching, and other technologies within your network to help bring actual usage in line with policy. The actions you need to take are indicated by the data collected through monitoring and analysis, and are constrained by the network policy. Many people expect to begin the task of bandwidth management by starting with this step. But without good monitoring techniques, network administrators are effectively blind to the problem [5]

2.2 Network Traffic Analysis Tools

Monitoring tools are selected out of a variety of tools (Ntop, Iptarf, MRTG, Nagios and Web sense) available today. The following features have been considered while making the selection:

i. Appropriateness
i. Affordability
ii. Lightweight
iii. Flexibility,
iv. Graphical support
v. Data retention
vi. User friendly and
vii. Feature richness

In this research, packet sniffer is selected because it is a piece of software capable of monitoring all network traffic. It has the following features that most monitoring tools do not posses.

i. It is an open source tool with extensive support.
ii. It stores data for a long time.
iii. It is able to capture all incoming and outgoing traffic for example clear-text passwords, user names and other private or sensitive details. Internet bandwidth use by host and protocol, point to point traffic are crucial to know in order to manage and optimize the bandwidth.

3. Statement of Problem

The ABU network is expected to have growing number of hosts with the growing number of staff and students, the following problems are encountered:

i. A way of giving priority to traffic based on users classes, applications or time of the day to make maximum utilization and optimization of bandwidth has not been implemented,
ii. A mechanism that makes sure that the University bandwidth is used for the intended purpose (Academic and research related) and discovering when it is not in place are not available
iii. In addition bandwidth is often consumed by low priority, bandwidth-hungry uses for non-educational purposes.
iv. Peer-to-Peer (P2P)-based network congestion; the primary cause of the bandwidth problems is P2P file-sharing software (such as Morpheus, Gnutella, and KaZaa). These programs allow an individual to connect to a network of other users and exchange music, video, and other types of files.

4. Methodology

The methodology used in this research will focus on how to enhance the Internet users experience by eliminating processes caused by improper management and control of bandwidth. To identify unproductive web applications responsible for consuming valuable bandwidth of University network system through the following;

i. **Selection of Monitoring Software**: A software that will monitor and adequately report in details the
network usage, identified and preferably an open source software to take care of licensing and virus issues [6]

ii. **Installation and Configuration of Monitoring Software**: Packet sniffers is installed and configured as a monitoring server on the network. It can be accessible from any part of the network

iii. **Verification of the Configuration**: The server tested on a small office network to ensure that the configuration works well.

iv. **Installation of Software on Live Network**: The software is installed on the University network operating centre.

v. **Data collected (packet traffic):** Data is collected from the monitoring server daily over a period of 90 days continuously.

vi. **Extraction of data**: Since the research is interested in the analysis of the network usage , a detailed analysis of data is done using **MATLAB (Simulink**) to figure out the type classification of applications as productive (academic and research related) and unproductive (personal, non academic and non research related) activities in addition to applications which are consuming high bandwidth [9].

5. Results and Discussion

This begins with the preparation and collection of data, which includes both transmitted and received rates per daily (15 Minute average), weekly (30 Minute average) and monthly (2 Hours average) of the various access points in the networks, at over the period of three months.

A programme using M files and communication toolbox in MATLAB was used to plot the bandwidth utilization (Traffic IN and traffic OUT) of the daily, weekly and monthly bandwidth usage

Co

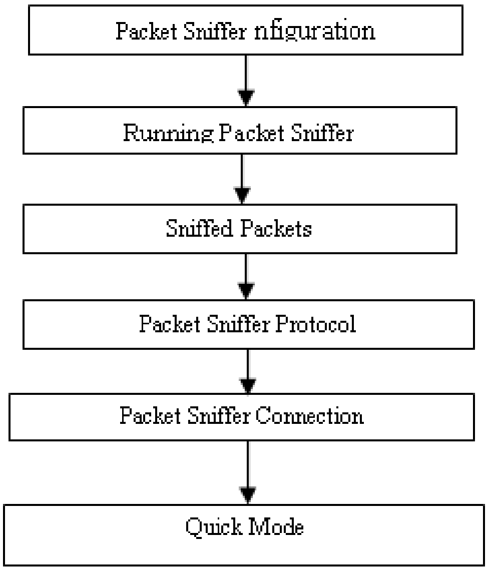


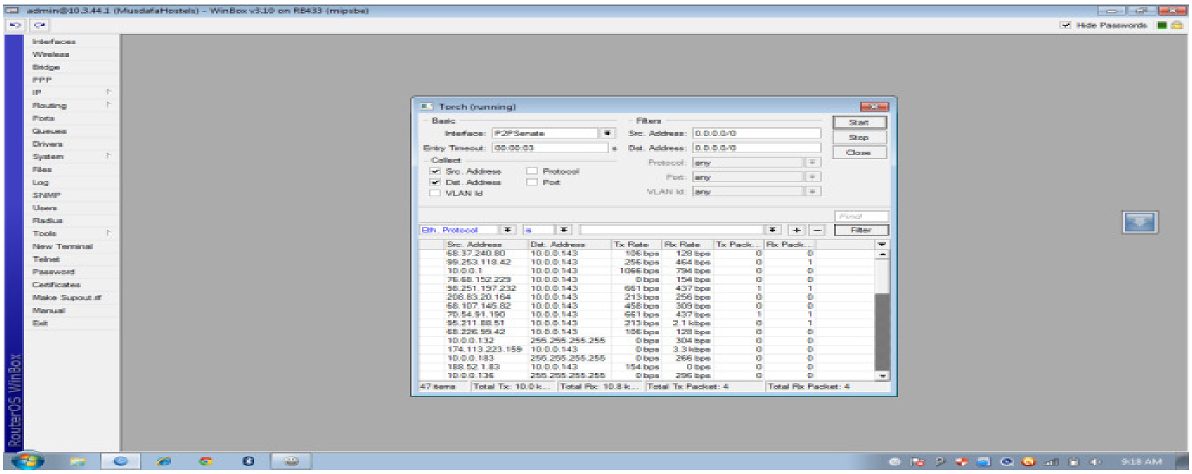
Fig.2.Chart configuration

5.1 Verification of the Configuration

After the configuration the software is tested on the server. The following tasks are verified:

i. Search for clear-text usernames and passwords from the network,
ii. Convert network traffic into human readable form,
iii. Analyze networks to detect bottlenecks and detect network intruders.

iv. Packets captured from a local area network and the capture network traffic is based on application.



Torch (running)

Basic
Interface: P2PSenate
Entry Timeout: 00:00:03 s

Collect
☑ Src. Address ☐ Protocol
☑ Dst. Address ☐ Port
☐ VLAN Id

Filters
Src. Address: 0.0.0.0/0
Dst. Address: 0.0.0.0/0
Protocol: any
Port: any
VLAN Id: any

Eth. Protocol is

Src. Address	Dst. Address	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
68.37.240.80	10.0.0.143	106 bps	128 bps	0	0
99.253.118.42	10.0.0.143	256 bps	464 bps	0	1
10.0.0.1	10.0.0.143	1066 bps	794 bps	0	0
76.68.152.229	10.0.0.143	0 bps	154 bps	0	0
98.251.197.232	10.0.0.143	661 bps	437 bps	1	1
208.83.20.164	10.0.0.143	213 bps	256 bps	0	0
68.107.145.82	10.0.0.143	458 bps	309 bps	0	0
70.54.91.190	10.0.0.143	661 bps	437 bps	1	1
95.211.88.51	10.0.0.143	213 bps	2.1 kbps	0	1
68.226.99.42	10.0.0.143	106 bps	128 bps	0	0
10.0.0.132	255.255.255.255	0 bps	304 bps	0	0
174.113.223.159	10.0.0.143	0 bps	3.3 kbps	0	0
10.0.0.183	255.255.255.255	0 bps	266 bps	0	0
188.52.1.83	10.0.0.143	154 bps	0 bps	0	0
10.0.0.136	255.255.255.255	0 bps	296 bps	0	0

47 items | Total Tx: 10.0 k... | Total Rx: 10.8 k... | Total Tx Packet: 4 | Total Rx Packet: 4

Figure 3 shows a Packet captured from local Area Network

The matlab programme was run and the result was as shown in the following Figures; 3.1, 3.2 and 3.3.

1- Figure 3.1 gives the line chart of plot of daily average bandwidth utilization of different number of users of the various access points that are found within the network.

2- Figure 3.2 gives the line chart of plot of weekly average bandwidth utilization of users of the various access points that are found within the network.

3- Figure 3.3 gives the line chart of plot of monthly average bandwidth utilization of users of the various access points that are found within the network

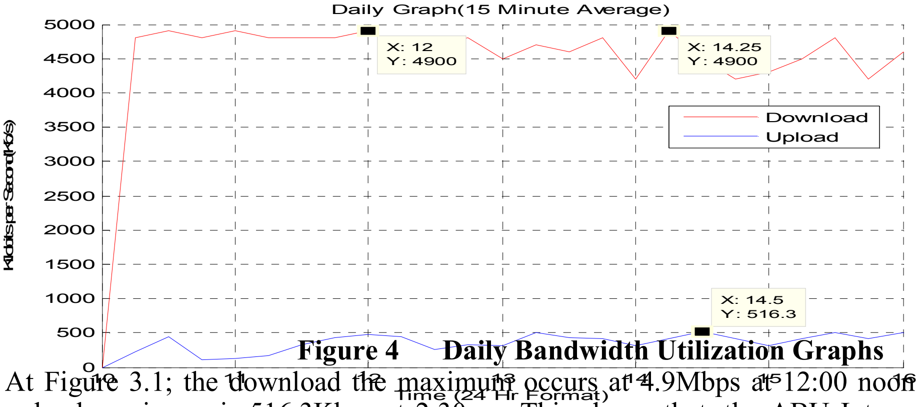


Figure 4 Daily Bandwidth Utilization Graphs

At Figure 3.1; the download the maximum occurs at 4.9Mbps at 12:00 noon while the upload maximum is 516.3Kbps at 2:30pm. This shows that, the ABU Internet gateway saturate very quickly from 10:00 a.m. up to 4:00 p.m. this emphasises the need for improved bandwidth management and optimization.

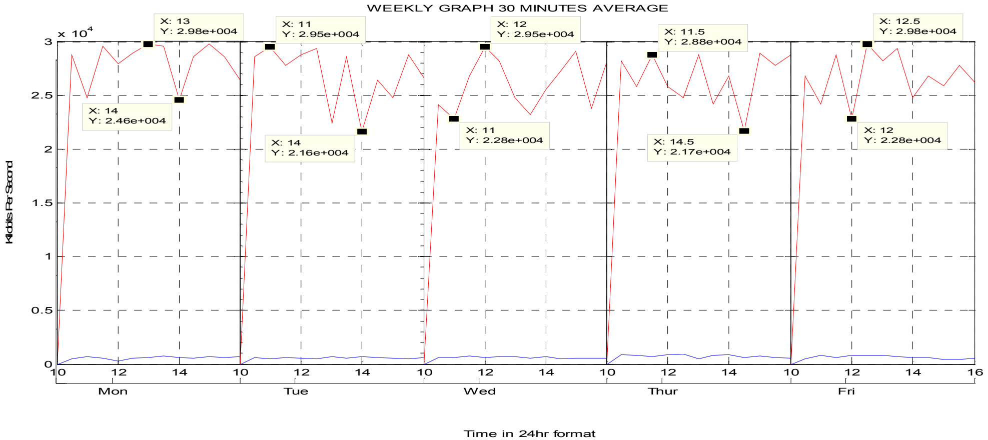


Figure 5 Weekly Bandwidth Utilization Graphs of Week 24 of 201

Figure 3.2 shows that, from Monday to Friday the maximum are download 29.4Mbps at different time i.e. 1:00pm, 11:00am, 12:00am, 11:55am and 12.05am, and a very percentage of the university community run windows operating systems which need daily updates of both the operating system and the antivirus software on them.

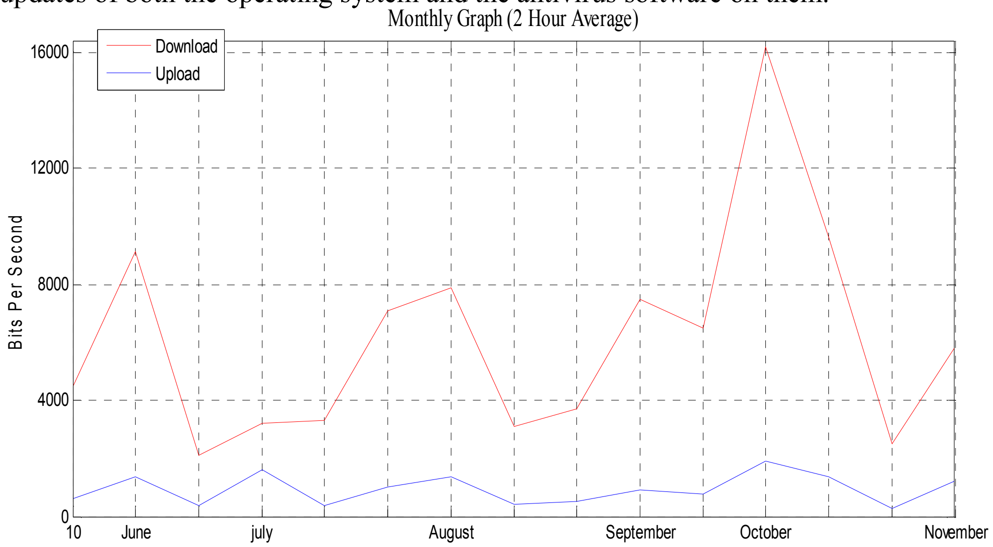


Figure 6 Monthly Bandwidth Utilization Graphs at 2011

i. Finally looking Figure 3.3 reveals that there are peer-to-peer connections using ABU context which indicates that there are users with download manager software in their computers. These software enable heavy down loaders congest internet connection restricting internet access to other users and servers that need global accessibility.
ii. Websites accessed by each user of the network was identified and was found that bulk of Internet traffic is peer to peer access and downloads of music, video and Anti-virus updates and access of free e-mail services Although, is acknowledge that peer to peer access and download of music, video and Anti-virus updates and free e-mail services might be important for academic purpose.

6 Conclusion

This network traffic analyses show there is unwise bandwidth utilization in the campus network, and is a serious and emerging challenge for almost all organisations in the present world information technology. Lack of appropriate bandwidth management is preventing useful Internet access which in turn yielding low quality of academic and research works. Better management of bandwidth makes Internet access wider especially for those who need it in actual. Unfortunately there is relatively little understanding about the importance of managing bandwidth because of low awareness, lack of technical staff, improper implementation of Internet usage policy, non supportive attitude of authorities, etc. Bandwidth is a very valuable and limited resource, so there is a need to enhance awareness level among all stakeholders- students, researchers and staff within the university education system in addition to implement a common acceptable policy. Policy should encourage academic and research related activities and throttle of unproductive and individual centric activities [10]. The ICT professionals responsible for management of university network system have to monitor network traffic and users' behaviour continuously on network followed by analysis of web applications eating valuable resource. Furthermore, provision of trainings and technical tools is not sufficient for bandwidth management but there is a need to have a rich coordination among all stakeholders, authority and ICT staff on a common acceptable Internet access policy.

Hence, it is a necessary condition to implement appropriate bandwidth management so as to reduce the bandwidth starvation in the campus network.

7 Acknowledgments

This paper is a part of M.Sc. research work of the first author and the author gives sincere thanks to both his Major and Minor supervisors who are also the other two authors of this work. The author also gives thanks to the management of Ahmadu Bello University ICT for their support of this work.

8 References

[1] A practical guide to Bandwidth Management and Optimization Using Open Source Software, in October 2006

[2] Bandwidth management position paper, (Aptivate, June 2007); How to accelerate your internet,

[3] Bo Yu"Based on the network sniffer implement network monitoring Computer Application and System Modeling (ICCASM), 2010 International Conference on Volume: 7, 2010, Page(s): V7-1 - V7-

[4] Dualwan (2009) Bandwidth Management and Traffic Optimization (2010). http://dualwan.org/ bandwidth-management.html

[5] Flickenger, R. (2006). How to accelerate your Internet: A Practical Guide to Bandwidth Management and Optimization, Accessed on 20th November, 2010

[6] Graham, Robert. "Sniffing (network wiretap, sniffer) FAQ". Version 0.3.3. 14 September 2011

[7] Ansari, Rajeev S.G. and Chandrasekhar H.S, "Packet Sniffing: Brief Introduction", *IEEE* Potentials,
Dec 2002- Jan 2003, Volume: 21 Issue: 5, pp: 17 – 19

[8] A. Dabir, A. Matrawy, "Bottleneck Analysis of Traffic Monitoring Using Wireshark", *4th* International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov. 2007, Page(s):158 – 162

[9] A scalable architecture for network traffic monitoring and analysis using free open source software.

[10] S. Floyd and V. Jacobson, Link-sharing and resource management models for packet networks, IEEE Trans. Networking, vol. 3, 1995.