ASHESI UNIVERSITY COLLEGE

ASHESI NETWORK TRAFFIC ANALYSIS

UNDERGRADUATE THESIS

B.Sc. Management Information Systems

Husein Shahadu

2017

ASHESI UNIVERSITY COLLEGE

Ashesi Network Traffic Analysis

Undergraduate Thesis

Undergraduate Thesis submitted to the Department of Computer Science, Ashesi University College in partial fulfilment of the requirements for the award of Bachelor of Science degree in Management Information Systems

Husein Shahadu

April 2017

DECLARATION

I hereby declare that this Undergraduate Thesis is the result of my own original work and that no part of it has been presented for another degree in this university or elsewhere.

Candidate's Signature:

…….

Candidate's Name:

…… ……

Date:

…..……...

I hereby declare that preparation and presentation of this Thesis were supervised in accordance with the guidelines on supervision of Undergraduate Thesis laid down by Ashesi University College.

Supervisor's Signature:

…….

Supervisor's Name:

…….

Date:

…….

ACKNOWLEDGEMENT

First and foremost, I thank almighty GOD for making this work attainable. I would like to thank my thesis advisor Dr Charles W. Jackson of the Faculty of Computer Science and Faculty of Engineering Department at Ashesi University College. The door to Dr Jackson`s office was continually open for discussions or whenever I had an issue concerning my study. Dr systematically allowed this work to be my very own, however navigated me within the right direction whenever I called upon him or whenever he thought I needed it.

I would also thank the Ashesi Network Directors. They assisted and were involved in gathering data for this project: Mr David Asumadu-Boateng, Mr Ato Yawson, and Mr Daniel Nii Tettey Botchway. While not their fervid participation and input, the information gathering process and also the reports from MainOne could not have been possible.

I additionally offer my respect to the authors of the many tools I employed in this thesis like NetBalancer for watching and monitoring network traffic on my own system, Wi-Fi Analyser for analysing signal strengths of the various subnets of the Ashesi network system and google maps for determining latitude and line of longitude of varied locations across Ashesi.

Last but not least, I offer my earnest appreciation and acknowledgement to my revered instructors: Dr Nathan Amanquah, Dr Aelaf Dafla, Dr Ayorkor Korsah, Mr Kwadwo Gyamfi Osafo-Maafo, Mr David Amatey Sampah, and Antoinette Doku and also the speakers who took time to guide us during our seminars. I am gratefully indebted to your guidance, comments and feedbacks on this work. Thank you very much!!!

ABSTRACT

The web has evolved from an information exchange system to a data mining, knowledge creation or Knowledge dissemination platform where the internet is viewed as a critical and vital component of success by students, lecturers and researchers in higher institutions particularly within universities and colleges. There is thus pressure on network directors managing network services within these institutions to provide regular and correct utilization of the available bandwidth. Network directors are being pressured to ensure that there is sufficient bandwidth available for every network user and also ensure the bandwidth is used productively. With the expansion of digitally made contents and Internet computing demands in the last couple of years, network users often complain of insufficient bandwidth available to completely satisfy their wants. In an attempt to attend to users complains, network directors ought to determine the main objective or purpose of the offered bandwidth and identify unproductive applications eating the bandwidth. In this paper, an attempt is made to investigate network traffic on the Ashesi University network system and to prioritize applications on the network based on user needs and based on what the bandwidth is purchased for. A policy framework is additionally outlined for best utilization and management of the university`s network system. The findings of the study indicate that there is the need to prioritize applications on the network because it was made clear that users access certain types of applications during school hours and some other type of applications after school hours. There is also the need to install certain servers locally in alternative to scaling back the traffic caused during peak days and also during peak hours of the Ashesi network system.

Keywords: *Bandwidth, Internet Access Policy, Viruses, Spam, Peer-to-Peer File-Sharing, Network Traffic, Optimization, Prioritization, Applications, Monitoring tools, Network analysers*

Table of Contents

FIGURES

LIST OF ACRONYMS

ADSL: Dynamic Host Configuration Protocol.

FTP: File Transfer Protocol

CPU: Central Processing Unit

HTTP: Hypertext Transfer Protocol

IP: Internet Protocol

MRTG: Multi Router Traffic Grapher

P2P: Peer to Peer

Mbps: Megabits per Second

TCP: Transmission Control Protocol

ISP: Internet Service Provider

Kbps: Kilobits Per Second

LAN: Local Area Network

NTOP: New Technology Option Pack Read

WWW: World Wide Web

SQL: Structured Query Language

SNMP: Simple Network Management Protocol

HTML: Hypertext Mark-up Language

ATP – AppleTalk Transaction protocol

CUDP – Cyclic UDP

DCCP – Datagram Congestion Control Protocol

RDP – Reliable Datagram Protocol

POP – Post Office Protocol

TLS – Transport Layer Security

NTP – Network Time Protocol

Chapter 1: Introduction

Campus-wide network systems and access to network information resources are in increasing demand and have really become more important in completing a meaningful research in any instructional setting. The campus-wide network has become one among a necessary assets to facilitate the success of any university. In view of this, Ashesi University College is not an exception. Ashesi University is an institution where a seat of higher learning is happening, including administrative as well as facilities for research and teaching. Internet access is so in high demand and is made possible through allotted bandwidth provided by MainOne – Ashesi University main ISP.

Stable Internet access is crucial for college students and other network users to connect with the outside world, participate and publish research works. Network directors are aware within the method of providing a stable connection, various unwanted congestion caused by the flood of IP/TCP traffic happens (Vikas, Vikram, & Balvir, 2011).

To manage the traffic, information and bandwidth measure becomes the core to focus on since it is the bandwidth that permits interaction of users on the network. Additionally, while not proactive management techniques, a network capability is crammed with viruses, worms or extra traffic caused by many harmful users. This affects the performance of the network that makes bandwidth management and monitoring terribly necessary.

Bandwidth is said to be the capability of a communication line to transfer information from a source to a destination (Flickenger, 2006). The methods, techniques or policies adopted to confirm effective consumption of the offered bandwidth is termed bandwidth management (Flickenger, 2006).

In this study, to ensure the bandwidth is used for the purpose that it was absolutely purchased, network traffic is discussed in details using Ashesi University College as a case study.

1.1 Background of the Study

Bandwidth represents the capability of a communication line to transfer data from source to destination (Aline, Pierre-Andre, & Claude). The broader the route or channel for packet transmission, the lot of packets transmitted. In observing the performance of a network`s bandwidth, the entire quantity of information transferred in a given amount of time at a selected period is set, analysed and evaluated (Carter & Crovella, 1996).

Bandwidth is also responsible for the speed of data transmission. The larger the bandwidth quota, the higher the connection speed thus the quicker to upload and download information. The fundamental unit for measuring bandwidth is bits per second (bps), however, the bandwidth may also be measured in kilobits, megabits or gigabits per second (gbps) (Vikas, Vikram, & Balvir, 2011). From research, it was noted that numerous internet connections follow different bandwidth standards or protocols. For instance, ancient dial-up connection provides slim bandwidth limit of about 56 kbps, while broadband connections enable information transfer at a better speed ranging from 128 kbps to 2mbps (Vikas, Vikram, & Balvir, 2011).

There are different Transport/Network layer protocols to transport packets on the network. Examples include ATP, CUDP, DCCP, RDP, POP, TLS, NTP, etc. However, the TCP/IP protocol is that which is widely used as a result of its ability to permits moderately economical and error-free transmission of packets (ANDREW & DAVID, 2011).

.

Furthermore, bandwidth is claimed to be comparatively expensive in developing countries and this is often because of variety of things starting from the poor power supply to connection via satellite in developing countries. Connection via satellite is way costlier than a reference to cable (Venter, 2003). These challenges lead to the high price of bandwidth in the developing world. As a result of this problem, several institutions have engaged network directors to watch and optimize consumption of network bandwidth.

In Ashesi University, there are network directors to monitor and evaluate the performance of the Ashesi network. To ensure faculty, students and other network users get pleasure from the complete advantage of the web and be able to participate within the international academic community, performance of the web information delivery system should be deliberate (Diana, 2005).

The internet network performance is increased through monitoring and putting in place policies to guard usage and consumption of the bandwidth. This is often called bandwidth management - improving the performance of a web Internet connection through removal of unnecessary traffic.

Bandwidth works sort of a pipe. If the flow of the fabric within the pipe is not monitored and managed properly, the pipe can choke with unwanted traffic - viruses, spam, peer-to-peer file-sharing or something that reduces the flow of information from one point to another (Flickenger, 2006).

In today`s internet world, bandwidth has become an important resource for institutions and once not monitored well, might jeopardize the everyday operations of an establishment like Ashesi whose daily activities largely depends on the internet. The bandwidth is often devoured by unproductive applications which can be costly to sight while not correct monitoring (Diana, 2005).

In monitoring and analysing bandwidth, traffic is sorted into various classes according to service and application types and the period users access these applications. The traffic is then prioritised and planned out accordingly to the minimum and maximum bandwidth that is configured for each of the traffic types (Bandwidth Management and Traffic Optimization, 2017).

In implementing a bandwidth management strategy, 3 activities are required: (i) Policy, (ii) Monitoring, and (iii) Implementation. Neglecting any of these activities hugely compromises the management process for these activities inform and reinforce one another (Diana, 2005). The Fig. 1 shows the relationship among these activities.

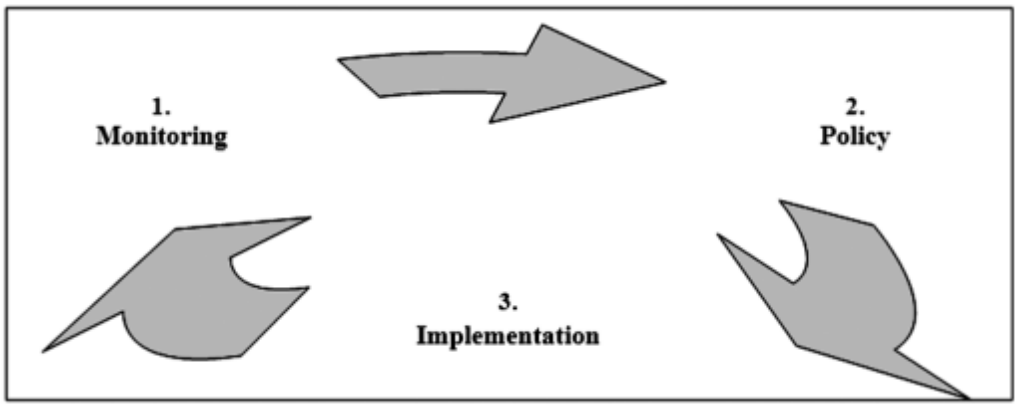

Figure 1: Bandwidth management activities

- **Monitoring:** This can be necessary for enforcing the policy because it reflects the real needs of users. Monitoring serves as a proactive measure to detect faults and troubleshoot problems before they occur.
- **Policy:** Policy refers to rules or laws place in situ to guide user behavior on the network. Without a suitable user policy, no amount of bandwidth is enough to satisfy users particularly once users are students. Students can continuously notice new ways to misusing the internet. They will download music, videos, stream videos online and

others will access bandwidth-hungry applications some of which can hijack the bandwidth from other important services.

- **Implementation:** Implementation is actually ensuring the policy designed is implemented and is obeyed by all users.

In designing a policy especially for students, user education is way lot productive than technical solutions. The policy needs to be understood and enforced. It is, therefore, the responsibility of administrators to check users and find out which policy suits them and ensure they adhere to the policy.

There are varied tools available to monitor and analyse a network`s bandwidth performance. Main features that ought to be conceded when deciding on a tool are : (i) Network Analysers—for monitoring traffic; (ii) Firewalls—for interference of malicious and unwanted traffic; (iii) Anti-Virus-for protective network; (iv) Caches—for efficiently using bandwidth, (v) Traffic Shapers—for prioritizing and controlling traffic; and (vi) Quota Systems—for managing user behaviour (Vikas, Vikram, & Balvir, 2011).

1.2 Problem Statement

Ideally, one main focus of Ashesi University College which is also a part of the learning goals of the school is technological competency. This is often mostly achieved through stable and reliable internet connection. The Internet is made available so as to boost students learning expertise both in-class and the out-of-class expertise. Sadly, instability in internet connection in Ashesi became a major concern for internet users in the last two semesters of 2016. The population of students keeps rising and users are also identifying news ways of consuming more bandwidth - cloud computing. The present bandwidth management system permits all applications and services on the network to possess equal priorities in a particularly fast and discretional manner. Continuing with this current

management system prevents optimization of traffic since there is less information to be able to prioritized services based on user needs - classify applications as high priority or low priority depending on what application or service is required by users on what day and at what time. The inability to prioritise applications leads to superfluous congestion that affects the network performance and inhibits Ashesi from fully enjoying the full advantage of cloud computing.

1.3 Research Study

I would wish to explore choices for a new bandwidth management strategy that will concentrate on prioritization of services on the network. To do this, I will work with the Ashesi network management team to observe user behaviours on the internet by studying the sorts of traffic generated, the top visited applications and the time, the day or the period within which users visit these applications.

1.4 Objectives of the Study

- To identify unproductive network based applications responsible for consuming valuable bandwidth of the Ashesi network system.
- To design a bandwidth management policy framework to reinforce the utility of productive applications on the network.
- To rank applications on the network based on user daily traffic trend or analysis

1.5 Scope of Study

This study is meant to be executed within a particular timeframe and so restricted to analysing network traffic on the Ashesi network and prioritising applications based on day and time of day in which they are accessed.

1.6 Significance of Study

There is presently no policy limiting users on the Ashesi network. This study can aid in formulating a policy and setting priorities for services on the network. It will also conjointly weigh down superfluous traffic generated by making certain that what is required by users at a specific period or day is what is given higher priority and that which is less required is given low priority. This can prevent the situation where few users hijack the internet from the larger group. Furthermore, it will also aid in designing a policy to monitor and control negative behaviours on the Ashesi network.

1.7 Thesis Outline

Chapter two covers literature review and theoretical framework; it reviews printed and unpublished works, journals, and books to gather data for the study. It also gives background knowledge about network traffic, network protocol distribution, bandwidth management and weblog analysis. Chapter three demonstrates the methodology employed to carry out this study. Chapter 4 discusses the outcome of the study and traffic on the Ashesi network. Chapter 5 provides detailed recommendation and conclusion for this project.

Chapter 2: Literature Review

This study is concentrated on network traffic analysis of college bandwidth. The researcher conducted a literature review to assess major issues and concepts in network traffic analysis, network protocol distribution, Weblog analysis, bandwidth management and network monitoring tools. To manage network traffic, you must first understand the source of the traffic. Internet traffic is an aggregate of traffic from many local area networks (LAN). Various related works, journals, books and articles were consulted to assess the importance of network traffic analysis and the need for network monitoring tools. Keywords that were used in researching the topic were bandwidth, traffic, IP, TCP, the internet, transmission, congestion, workload, ISP, Optimization, etc. The search considered a total of twenty- five resources which included eight journals, seven articles, and ten books.

1.1 Overview of Study

Network traffic is classified into connection-level traffic, World Wide Web (WWW) traffic and user behaviour traffic. Connection level traffic occurs when many users try to transmit bytes or packets simultaneously. A situation like that makes bandwidth demand exceeds bandwidth supply thereby slowing down the rate at which people connect to the internet (Behrouz, 2010).

A connection point is formed when a machine/packet gets the following parameters right: source IP address, destination IP address, source port number and destination port number (Behrouz, Catherine, & Sophia, 1998). The diagram below indicates a network`s connection point.

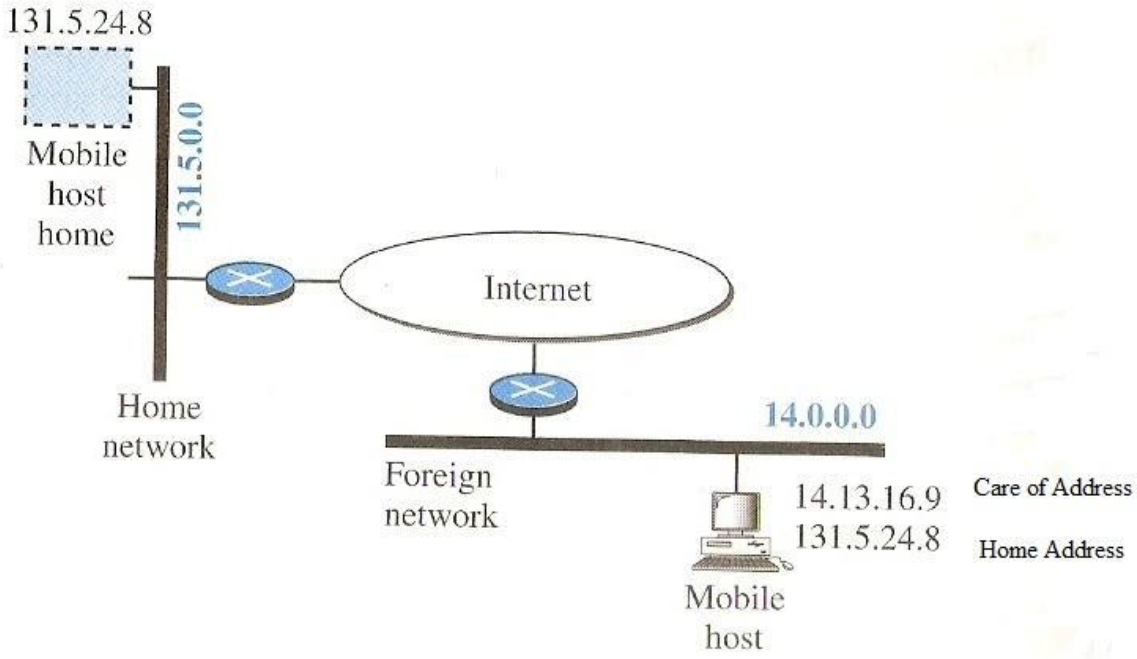

Figure 2: Internet connection point

When these four unique addresses close, a communication link is created and a connection is formed.

World Wide Web (WWW) traffic is most frequently caused by malicious worms or through sharing or distribution of files on the network (Lance, Martin, & Carey, 2003).

User behaviour traffic is the result of activities of internet users. Every network gets healthy and unhealthy users. Healthy users are those that use the internet for what it had been purchased for. Harmful users engage in activities that hurt or misuses the network bandwidth. They can hijack a network bandwidth from all other users if they are not checked. They engage in activities like peer-to-peer file sharing, streaming online videos, music or accessing bandwidth-hungry applications.

1.2 Network Traffic Analysis Tools

1.2.1 Ntop

Ntop is used to monitor, analyse and measure network traffic (Deri et al., 2000). It has embedded HTTP server features that support various network media types across various platforms and can store traffic information into an SQL database system. It is however limited by its high memory requirements when operating in a continuous monitoring environment (N, Monowar, R, D, & J, 2014).

Ntop uses the same packet capture library to obtain network data. It is multi-user based and capable of collecting archives and analysing network data captured. It however does not have a web interface to display results.

1.2.2 Multi Router Traffic Grapher

MRTG is a tool for graphing network data. It can run on a Web server. It reads inbound and outbound octet counter of the gateway router after every five minutes, and then logs data to generate graphs for web pages. The graphs can then be viewed using a web browser. Although MRTG gives a graphical overview, it, however, does not give details about the host and protocol responsible for the traffic (Tobias, 2001).

1.2.3 Weblog Analysis

Web analysis studies user behaviour on a Website. By collecting various Web analytics metrics, one can develop key performance indicators (KPIs) that measure visitor trends (Bernard, Amanda, & Isak, 2009).

Network managers can use weblog statistics to discover the types of people who visit their sites, and the pages that they visit (Robert, Bamshad, & Jaideep, 1999).

Server logs consist of transfer logs, error logs, referrer logs, and agent logs. Transfer log provides a list of all hits on the server and the times at which they occurred. The error log lists all errors that were made to the server. The referrer log provides a list of the locations from which users came before entering the site, and the pages that the users hit first within the site. The agent log lists the search engines used by the users on the site (Rob, Shanshan, & Dimitrios, 2010).

According to (Roger, Alberto, & Ee-Peng, 2005), Web sites are generating a big amount of Weblogs data that contain useful information about the user behaviour. IT administrators can use this information to analyse and classify network traffic to ensure adequate bandwidth and server capacity on their web sites.

Chapter 3: Research Methodology

To study daily network traffic and also identify unproductive applications responsible for eating valuable bandwidth of the Ashesi network system, the Ashesi network was monitored using Fort iGATE as a gateway between Ashesi and the outside world. A period of 7 days was set to watch the behaviour of Internet Users and their bandwidth utilization trend for 24hrs. The following resources and tools were used to gather and retrieve traffic data:

(i) Ashesi network report from MainOne

(ii) Traffic reports from Fort iGATE

(iii) Bandwidth usage graphs from the Fort iGATE device, assisted by Ashesi network management team.

The Fortinet device delivered complete range of network traffic from applications to security features such as;

- Top viruses by IP
- Top attacked sources
- Top attacked victims
- Top spam sources and spam destinations
- Firewall status
- VPN (Virtual Private Network)
- Gateway anti-virus, anti-spyware and gateway anti-spam.

A detailed analysis of the reports was completed followed by categorization and classification of applications as productive (academic and research related) and unproductive (personal and non-academic and non-research related) activities in addition to

high consumption bandwidth applications and sessions by application. R and tableau were used as data analysis tools to analyse the reports and the traffic generated per day. After analysing the reports, a bandwidth utilization policy framework was then designed by throttling unproductive works and prioritizing applications or services on the network.

Chapter 4: Discussion and Results

1.1 Ashesi Network Physical Structure and Bandwidth Utilization

The Ashesi network contains a multi-tiered design integrated from where MainOne hands over service to Ashesi campus through end-user connection points. Fibre, radio, switches and routers are used to link or convey the network from one end to another across the school. Ashesi also has installed Access Points (AP) and their controllers for seamless access to network services via Wi-Fi. The network currently connects to the Internet on 310Mbps downlink and 250Mbps maximum uplink bandwidth. The main service points of the Ashesi network are;

- Edge network,
- Cisco AS1K Router
- Fortinet Firewall,
- Admin 3 Switch and
- On Dell Switch where the access points are connected.

These are switches to provide connection for users. There are also planted PoEs across Ashesi campus to support internet connection via wireless access points.

Below is a diagram of the Ashesi network layout. The network topology is star shape as can be seen from the diagram.

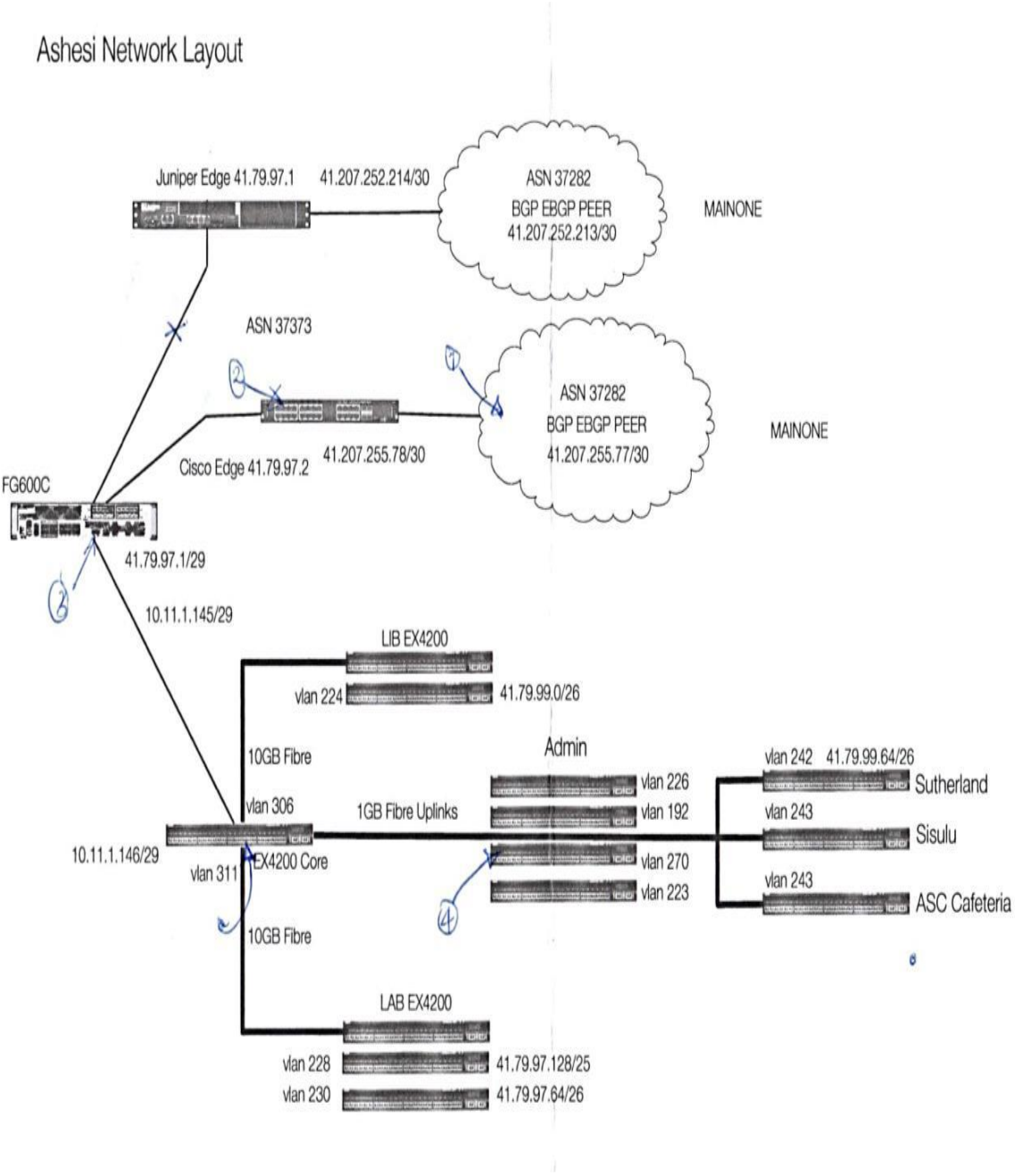

Figure 3: Ashesi network topology

1.2 Ashesi Network Subnets and Signal Strength

The Ashesi network is split into different subnets to facilitate management of wireless connections. The main subnets are explained below;

AshesiAir: AshesiAir is one of the subnets of the Ashesi network system. Its signal is strong around Warren Library, Ghana Climate Innovation Center and the Office of Diversity in International Programs (ODIP). People around these locations in Ashesi University are assured of high network signal on the AshesiAir subnet.

Student: The Student subnet has high network signal around Norton Motulsky, the Engineering Staff area, Old Hostel, Lecture Hall 216/217 and round the Samory Toure Greene Lounge area.

Staff&Faculty: People round the Computer Laboratory - 221/222, Electronic Laboratory, Administration, Lecture Halls, and Akorno will get high signal strength through the staff&faculty subnet.

Ashesi Guest: Ashesi guest has robust signal around Akorno, Administration, Electronic Lab, Design Lab, New Hostel, Health Center and at Norton Motulsky.

Sisulu Air: Sisulu air is by choice designed for Water Sisulu hostel. However other subnets like Student and Ashesi Guest also are robust in this area.

Berekuso Air: The Berekuso air subnet is only found around the hostel front desk area.

Ashesi student council: This subnet is robust around Efua Sunderland Hall, Ephraim Amu Hall and the Bill and Jeanne Bliss Student Lounge.

Surfinn: The surfinn subnet provides internet connection for Engineering Workshop, down the Health Center.

Ashesi north: The Ashesi north subnet is strong round the registrar`s area. There is also the **hostel lobby** subnet providing accessibility for folks around the hostel front desk area. The diagram below is a map of Ashesi University showing the various subnets and the areas they have strong signals.

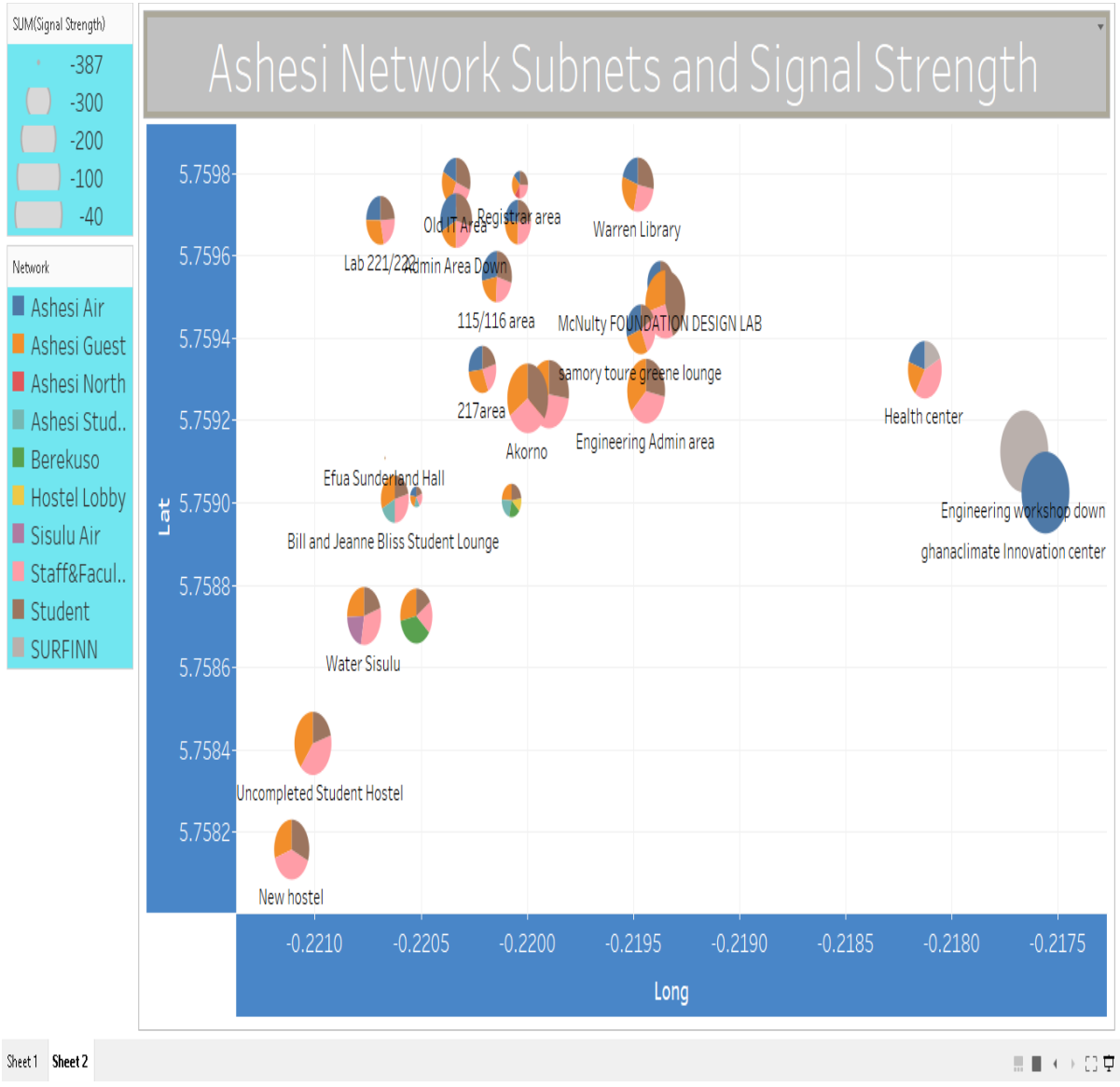

Figure 4: Ashesi network subnets and signal strength

The study considered top three subnets in every location and the map above shows the top three subnets per location in every chart. The signal strengths were recorded as

negative numbers thus the smaller the size of a subnet on the chart, the higher the signal strength of that particular subnet in the area. For example, at the Warren Library, the top three subnets in the area were staff&faculty, AshesiAir and Ashesi Guest. From the map and from the Warren Library pie chart, AshesiAir has the smallest size thus the subnet with the highest signal strength at the library. The data used to contracts the map above is found in appendix Fig 13.

The following facts were additionally deduced from users experience with the various subnets:

- Students need to be clear on the location or where to access each subnet. They need network directors to clearly designate areas of access for each subnet. E.g. Staff&faculty for administration area, students for hostels, AshesiAir for campus, etc.
- Students additionally suggested that IT differentiate subnets based on what one must on the web. Say one subnet designated for academic resources, another for social media applications or YouTube or web applications, etc.
- There is increasing peer-to-peer (P2P) file sharing among students. Some students suggested that a subnet can be designated to handle P2P activities.

1.3 Analysing Traffic on the Ashesi Network

The goal of monitoring and managing network traffic is to have the right amount of bandwidth in the right place at the right time for the right set of users and applications. Managing network traffic requires that the load or capacity relationship of key facilities are understood. To ensure effective analysis of bandwidth consumption, network traffic bottlenecks are identified and dealt with on a case-by-case or day by day basis, based on business priorities (CRUZ, 2000).

The graph below shows traffic trend on the Ashesi network based on day and time in which traffic occurs. The smaller the size of the rectangle, the lower the network traffic generated and vice versa for both the period and the day traffic is generated.

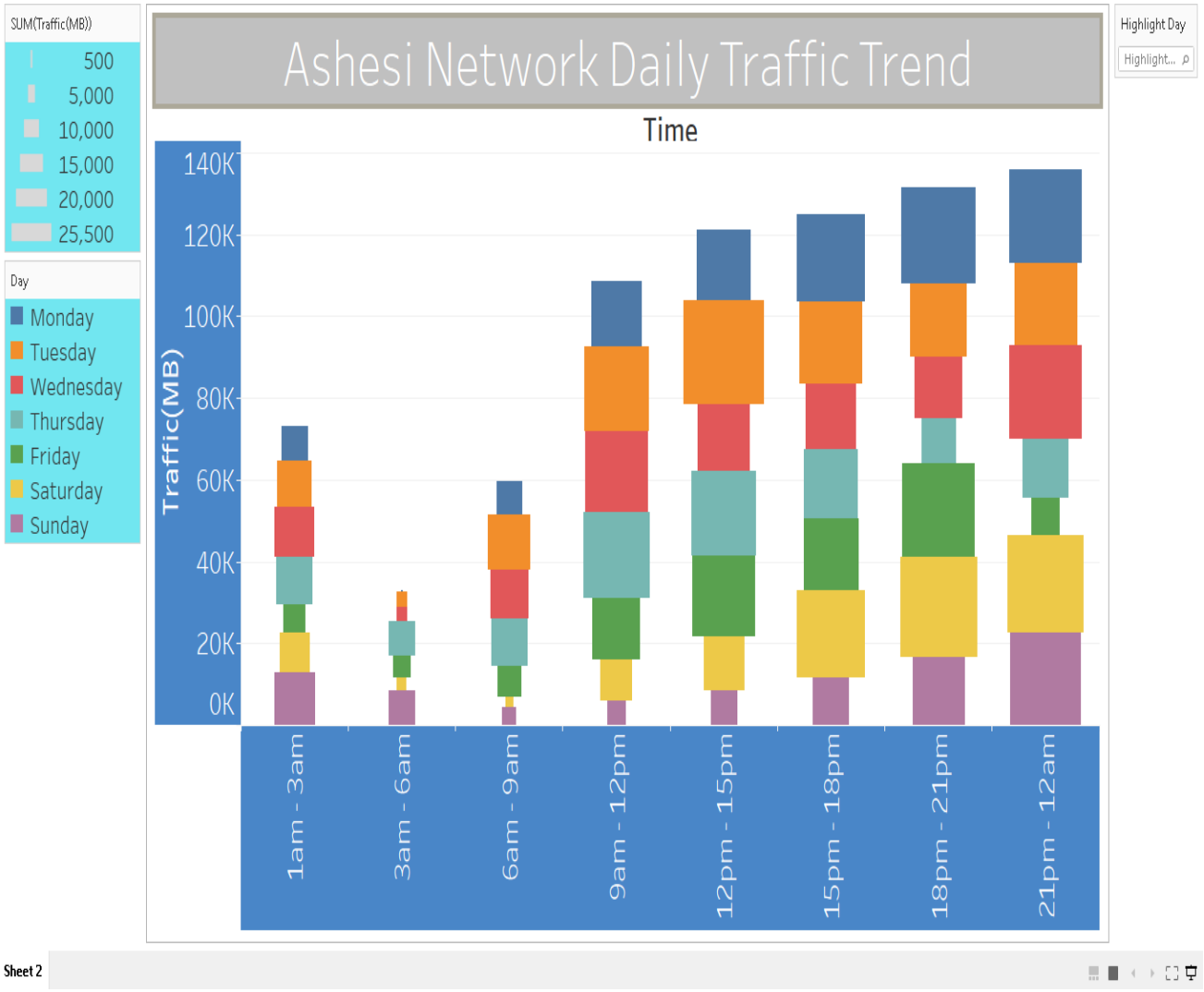

Figure 5: Daily network traffic trend

The columns represent the time of day traffic is generated and also the rows indicate the amount of traffic (MB) generated within the period. The colours represent days and since the network was monitored for a week for 24hrs, we have seven colours representing traffic trend for each day and for each time range. Sum of traffic ranges from 500 to 25, 500 (MB). From the graph, it can be observed that the busy days of the Ashesi network are Mondays, Tuesdays, Wednesdays, Thursdays and Sundays. These are the days the most traffic is generated. Approximately, traffic reaches its peak between 9:00 am – 15:00 pm during school hours and comes down after students are done with class work and workers close

offices for their homes. After school hours, the peak of traffic is approximately around 9:00 pm – 12:00 am when students have rested and are back to the classrooms for studies.

Also, it may be noted that there is typically less traffic on the network from 1:00 am – 9:00 am. This can be as a result of the fact that several users will either be sleeping, prepare for classes or offices will be setting up for workers to start work. On weekends too, there is usually less work on the network during the day especially from morning till 15:00 pm. The traffic begins to generate after 15:00 pm when students have rested and set out for studies. Fig 11 in Appendix provides the data for this graph.

After analysing the traffic trend, the applications or services causing the traffic were also analysed. This was to determine what keeps the network busy especially during the peak hours and peak days.

The graph below shows the days, the time-range and the applications causing the most traffic on the Ashesi network. The graph gives information on the applications that are accessed during the day or school hours and applications accessed after school. The goal here is to be able to prioritize the applications based on users demand and also to avoid unnecessary competition from unimportant applications. This information is important to classify applications as high priority or low priority based on the time and the day internet users access the application.

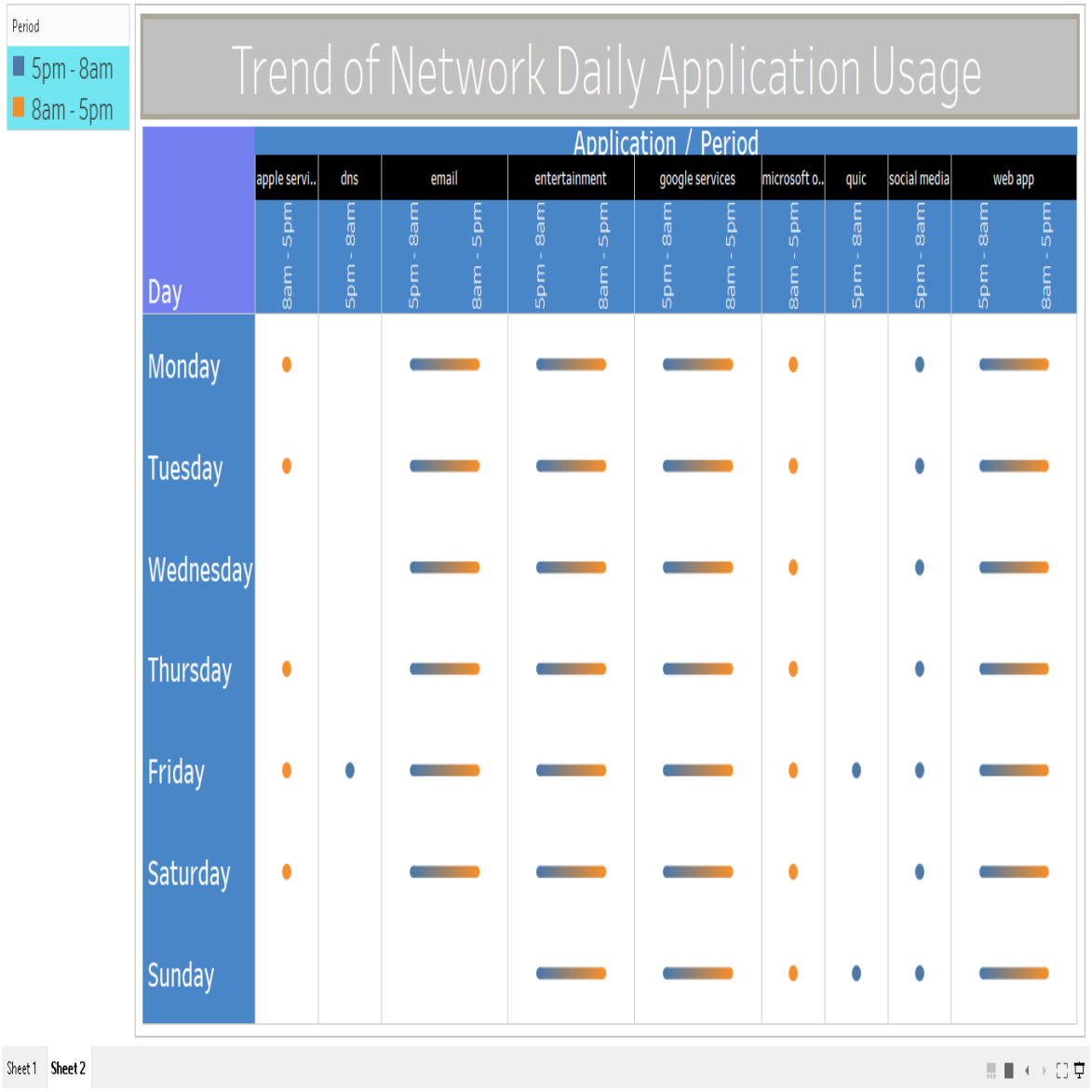

Figure 6: Top applications on Ashesi network

The graph above shows rows as day and columns as applications. The black colour represents the applications or services on the network and the blue beneath the black represents the period of time. There are two time-range, (8:00 am – 5:00 pm) for school hours and (5:00 pm – 8:00 am), after school or work hours. The yellow colour represents applications accessed during the day and the blue represents applications accessed after work hours. From the graph, it can be seen that applications such as apple services and the Microsoft office applications are mostly accessed during the day thus it would be good to

have these applications on high priority during the day. The DNS, QUIC, and social media are accessed after work or school hours thus these applications can be put on low priority during the day and high priority after work hours. The services which combine both colours are the busy applications on the network. They are accessed almost 24hrs. It would be good to have these applications between high and low or either high or low priority depending on the situation of the network. Fig 12 in appendix is the data for the graph above

1.4 Bandwidth Consumption by Application

In the Fort iGATE report, the top applications that contributed significant bandwidth load are shown in the graph below. Almost 50% of the total bandwidth for the week was consumed by google services. Google services include google search engine, YouTube, google downloader or any other service provided by google. Web applications or web pages was the next consuming application on the network after google taking about 15% of the total bandwidth for the week. The chart shows the applications and the maximum bandwidth each application consumed.

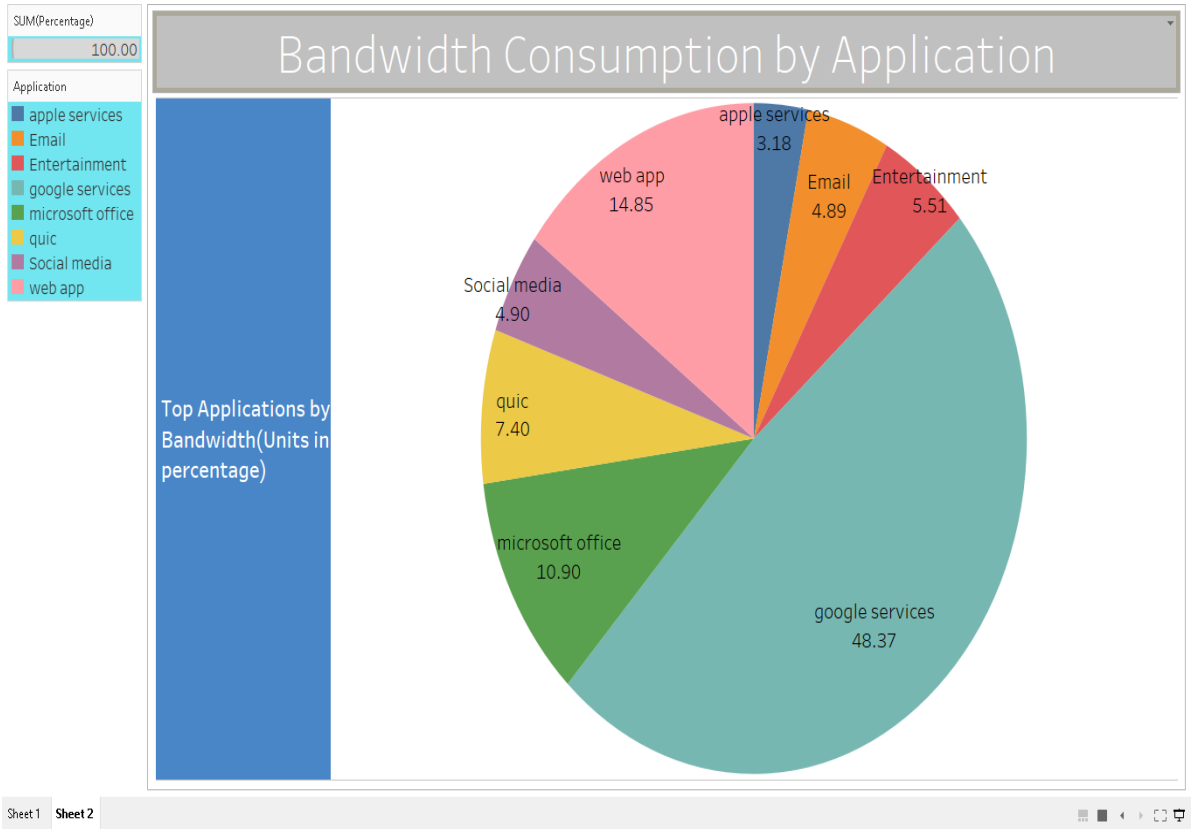

Figure 7: Top applications by bandwidth

Social media and entertainment (Facebook, Instagram, skype, twitter, torrent, online video or music streaming) were of the first rank in the list of top ten applications on the network by bandwidth. Together, social media and entertainment consumed about 10% of the total bandwidth for the week representing 7.04GB as seen in the appendix Fig 9.

Also, about 10% of the traffic was due to updates of various Microsoft office applications. It would be beneficial to have these services on a local server to reduce the amount of bandwidth and request time spent in accessing these services. A major contributor in the Microsoft office was windows update and this can definitely be a host on a local server. Also, apple services consumed about 3% of the bandwidth feed and about 5% was due to downloads from web pages or web browsers. There was also a significant load of about 8% on the bandwidth due to QUIC (Quick UDP Internet Connections) queries. The

above information is clearly indicating that nearly more than 50 percent traffic on the Ashesi network is due to the unproductive practice of applications which are not correlated with academic or research works. Fig 9 in appendix supplies data for the above pie chart.

1.5 Number of Connections by Application

In terms of individual visits or connections per application, web pages (Firefox Mozilla browser pages, chrome pages), social media platforms (Instagram, twitter, Facebook) and entertainment (YouTube, torrent, online video streaming) were the most visited services by session. This suggests that though google services might be the highest bandwidth-consuming application on the network, very few people might be hijacking the network with google applications. This shows how the bandwidth of an academic institution like Ashesi can be monopolized by very few people. It also points out that the academic purpose of the Ashesi network is not reflected both in terms of bandwidth consumption and in terms of the number of connections or sessions by application. Fig 10 in appendix is the data for graph below.

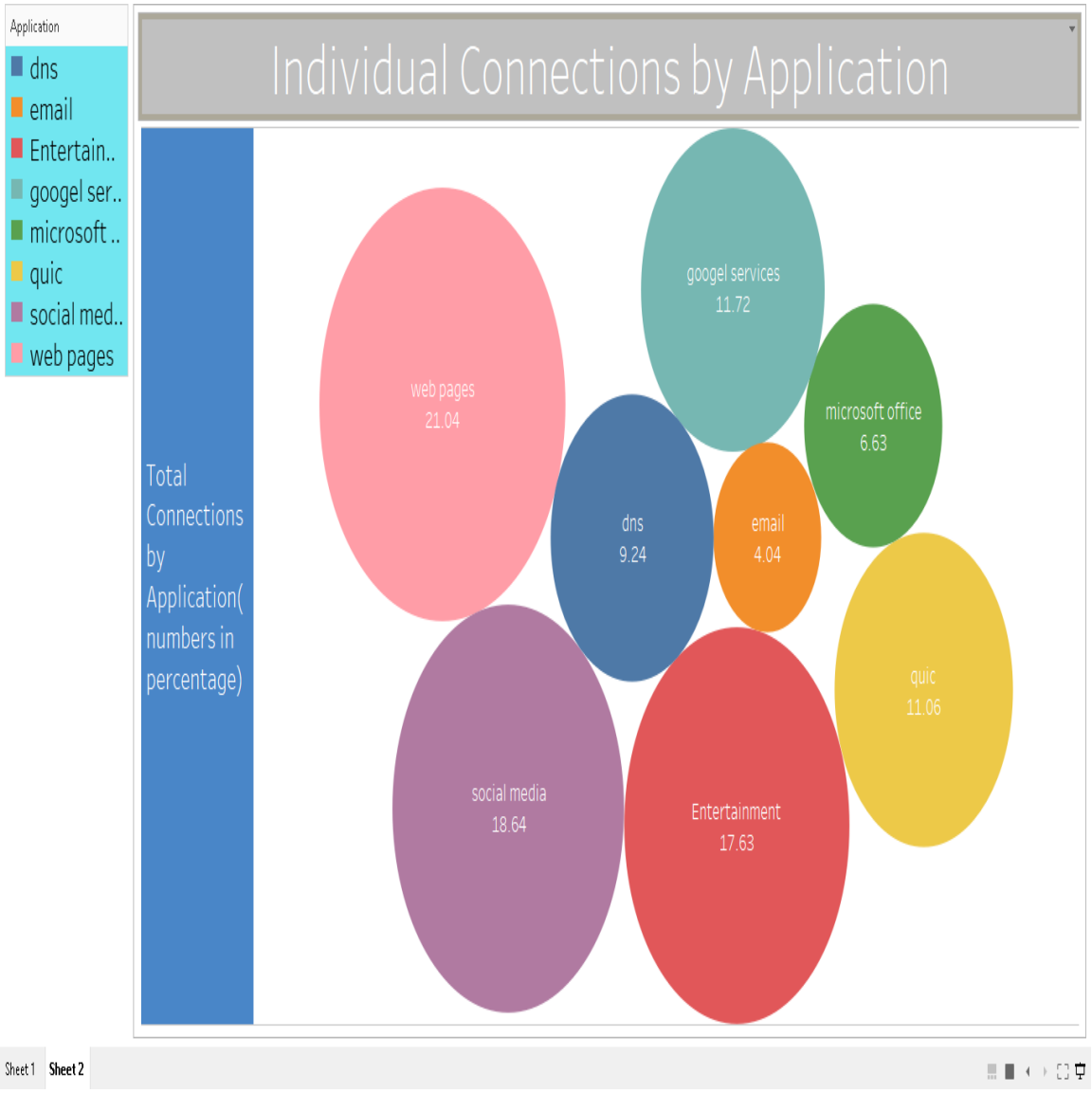

Figure 8: User sessions by application

Chapter 5: Recommendations and Limitations

Bandwidth management is a difficult task for most institutions in the present world of Information Technology. The inability to adequately manage bandwidth is leading to poor Internet Access which in turn leads to low quality of academic and research works. The ability to monitor, analyse and correct superfluous bandwidth consumption improves access to the Internet especially when users have enough time on the internet and are less supervised (Venter, 2003).

There is relatively little understanding of the importance of bandwidth management and this is as a result of low awareness, lack of technical staff, improper implementation of Internet Usage Policy and non-supportive attitude of authorities (Venter, 2003).

The bandwidth is a valuable but limited resource and as such, there is the need to enhance communication or awareness of the judicious use of it among all stakeholders-students, researchers and staff within Ashesi in addition to implementing a commonly acceptable policy.

The policy agreed on should encourage academic and research related activities and throttle unproductive and individual-centric activities. Also, the professionals responsible for managing the network have to monitor traffic and users' behaviour continuously in order to be able to check new strategies adopted by users which abuse the bandwidth.

1.1 Formulation of Policy for Stable Internet Access

Having completed the analysis with the above mentioned bandwidth utilisation facts which became clear during the traffic monitoring and analysis phase, a policy whose main aim is to ensure the Ashesi Internet is stable and reliable to achieve or sustain the Ashesi learning goal of technological competence was formulated.

Using the internet for personal reasons is not a crime but it becomes a problem when personal usage slows or halts down important network services for the greater good. As a result, it is recommended that all personal Internet use be put on low priority especially during the day or school hours when there is already too much traffic on the network. There are various open source tools on the internet with application prioritization features. An example is NetBalancer. NetBalancer has three classifications for prioritizing applications – High, Normal and Low priority. As such it can be a good tool to prioritize the applications or issues identified.

The analysis also indicates that there is the need to have apple services and Microsoft services (office 365, windows update, etc.) put on the high priority between 8:00 am – 5:00 pm every day.

In addition to the above, services from social media (Facebook, Instagram, twitter, etc.), domain name system (DNS) and QUIC are to be on low priority during school hours from 8am – 5pm and high priority after school hours from 5:00 pm – 8:00 am. This will reduce congestion and traffic on the network since there would be less competition for the limited bandwidth. Web mail, entertainment sites (YouTube, video streaming, music, online games), google services (google store, google play, google search engine) and web pages (http browsers, Firefox Mozilla, etc.) are demanded both during school hours and after

school hours as such these services are to be on high priority at all times or can be scheduled on normal when NetBalancer is used.

From the study, the DNS address resolution appears to be generating too much traffic. It generated almost 10% of the total traffic for the week by session. The DNS was ranked in the top ten major causes of traffic on the network. In order not to halt the resolution of addresses by the DNS by putting it on low priority during the day, it is advised Ashesi installs its own DNS server if this is already not done.

Furthermore, in addition to the above solutions, it was also observed that the following servers be installed: Mail Server, Web Cache Server, Windows Update Server, Antivirus Update Server, in order to minimize traffic on the network by resolving users' request locally.

- **Mail server**: Mail servers often receive incoming emails from local users and local senders (people within Ashesi). Having a local email server in Ashesi University will allow fast and concise communication among multiple users in addition to an efficient method of information dissemination. Emails can be checked out anytime and anywhere locally thereby facilitating the reduction of traffic generated.
- **Web Cache Server:** A web cache server caches web documents (e.g., HTML pages, graphics or images) in an attempt to minimize bandwidth-consumption and server workload. The server operates between web servers and clients by saving copies of the responses coming from web servers to the clients. When a client request for the same URL he requested before, the saved response is reused instead of asking the original server for it again. This reduces the amount of bandwidth used by clients and also reduces the response time of pages requested. It saves time and money by keeping the bandwidth requirements lower and more manageable (Venter, 2003).

- **Windows Update Server**: From the analysis, it became clear that from the Microsoft services, windows update generated the most traffic. Out of 12% traffic from Microsoft services, windows updates contributed about 8%. In view of this, it is recommended that windows update server be installed to provide regular updates locally to users. With this server, the unnecessary traffic created by windows update will be eliminated. The server can be configured to get updates during night hours to avoid individual rush during peak hours. This will help save the bandwidth during work hours.
- **Antivirus Update Server**: An antivirus update server can also be installed to reduce the unnecessary anti-virus update traffic during the day. A single system anti-virus updates can bring the whole network performance to a halt. Having this server installed locally will reduce unnecessary load on bandwidth during peak hours and will also prevent halting the whole system as a result of a single antivirus update (Venter, 2003).

1.2 Recommendation for Library

The target of this study was to get to the specifics to identify the amount of traffic generated from the library, the computer labs and any other place students' have access to computers. However, it was difficult to get data for specific applications due to limited network infrastructure at Ashesi network room. For instance, I wanted to know how much traffic is specifically generated from YouTube, outlook, Facebook, google search engine, etc. but the device currently used to monitor the network grouped the applications into services such as Microsoft services, google services, http browsers, etc.

Ashesi library has enough computers where students can access the Internet. Most often librarians are required to provide library services which often is related to information distribution over the Internet. For these reasons, librarians typically have an interest in network optimization and control. As a result, it will be good for the library to have its own

proxy server for reasons of optimization and control and also to be able to specifically deal with traffic from the library. When this is done, librarians will have access to daily or weekly Web access logs and statistics of internet usage at the library. They will be able to tell what the computers in the library are being used for by monitoring and analysing traffic in the library.

The Library may also see the need for a usage policy specifically for the library if certain library-specific issues need to be addressed. Also, there may be the need to make a case for more bandwidth to the library especially when Ashesi finally adopts the bandwidth quota system.

1.3 Limitations

There were several challenges this study faced in an attempt to get a full overview of the Ashesi network performance. The following were major limitations that prevented the study from capturing traffic from major consumption areas across Ashesi;

- The monitoring device could not get data for specific applications such as traffic generated from Facebook, twitter, YouTube, etc. The applications were grouped into services thus traffic was related to Microsoft office traffic, google services traffic, apple services traffic, etc. This affected the analysis in determining how much traffic was generated from specific applications and managing traffic based on application based.
- Network directors also lacked the needed infrastructure to specifically determine traffic generated from the library, the computer laboratories or traffic from workers offices. This limitation greatly affected the study because a major aspect of the study was to analyze and control traffic coming from these areas.

Chapter 6: Conclusion

This study presented an analysis of how applications or services on the Ashesi network can be prioritized so as to minimise traffic generated especially during peak hours. The daily traffic trend of the network was observed and analysed in order to determine peak hours and down periods of the network. The services were also classified into most accessed services during school hours and those accessed after schools hours. This information is important for prioritization of services on the network. The study also touched on bandwidth consumption by application and it was clear google services were the most consuming services on the Ashesi network. Network directors may rely on this information to make google applications accessible on a local server. This will save the bandwidth and also reduce traffic on the network.

More so, the signal strength of the various subnets of the Ashesi network were determined and analysed thus network directors can now assign subnets based on signal strength across various locations in Ashesi University. This information will also be helpful when Ashesi finally adopts a bandwidth quota system.

The graphs generated in the analysis provides details of the network traffic, services, subnets signal strengths and insight into problems that could lead to congestion and poor network performance. Future work will focus on application based monitoring and intrusion detection monitoring module and pre-emptive intrusion control.

Appendix

Application	Bandwidth	Bandwidth(GB)	Percentage
Entertainment	3727.3	3.73	5.51
google services	32700	32.7	48.37
Email	3305	3.3	4.89
web app	10041.5	10.04	14.85
apple services	2153	2.15	3.18
Social media	3314.4	3.31	4.90
quic	5000	5	7.40
Microsoft office	7367.2	7.37	10.90
Total	67608.4	67.6	100.00

Figure 9: Data for application by bandwidth graph

Application	Connections	Percentage
web pages	3894757	21.04
google services	2169346	11.72
quic	2046470	11.06
dns	1710548	9.24
Microsoft office	1227287	6.63
email	747162	4.04
social media	3449916	18.64
Entertainment	3262310	17.63
Total	18507796	100.00

Figure 10: Data for session by application graph

id	Day	Time	Traffic(MB)
0	Monday	1am - 3am	8,500
0	Monday	3am - 6am	500
0	Monday	6am - 9am	8,000
0	Monday	9am - 12pm	16,000
0	Monday	12pm - 15pm	17,000
0	Monday	18pm - 21pm	23,500
0	Monday	21pm - 12am	23,000

1	Tuesday	1am - 3am	11,000
1	Tuesday	3am - 6am	3,500
1	Tuesday	6am - 9am	13,500
1	Tuesday	9am - 12pm	20,500
1	Tuesday	12pm - 15pm	25,500
1	Tuesday	15pm - 18pm	20,000
1	Tuesday	18pm - 21pm	18,000
1	Tuesday	21pm - 12am	20,000
2	Wednesday	1am - 3am	12,500
2	Wednesday	3am - 6am	3,500
2	Wednesday	6am - 9am	12,000
2	Wednesday	9am - 12pm	20,000
2	Wednesday	12pm - 15pm	16,500
2	Wednesday	15pm - 18pm	16,000
2	Wednesday	18pm - 21pm	15,000
2	Wednesday	21pm - 12am	23,000
3	Thursday	1am - 3am	11500
3	Thursday	3am - 6am	8500
3	Thursday	6am - 9am	11500
3	Thursday	9am - 12pm	21000
3	Thursday	12pm - 15pm	20500
3	Thursday	15pm - 18pm	17000
3	Thursday	18pm - 21pm	11000
3	Thursday	21pm - 12am	14500
4	Friday	1am - 3am	7,000
4	Friday	3am - 6am	5,500
4	Friday	6am - 9am	7,500
4	Friday	9am - 12pm	15,000
4	Friday	12pm - 15pm	20,000

4	Friday	15pm - 18pm	17,500
4	Friday	18pm - 21pm	23,000
4	Friday	21pm - 12am	9,000
5	Saturday	1am - 3am	9500
5	Saturday	3am - 6am	3000
5	Saturday	6am - 9am	2500
5	Saturday	9am - 12pm	10000
5	Saturday	12pm - 15pm	13000
5	Saturday	15pm - 18pm	21500
5	Saturday	18pm - 21pm	24500
5	Saturday	21pm - 12am	24000
6	Sunday	1am - 3am	13000
6	Sunday	3am - 6am	8500
6	Sunday	6am - 9am	4500
6	Sunday	9am - 12pm	6000
6	Sunday	12pm - 15pm	8500
6	Sunday	15pm - 18pm	11500
6	Sunday	18pm - 21pm	16500
6	Sunday	21pm - 12am	22500

Figure 11: Data for traffic trend graph

id	Day	Period	Application
0	Monday	8am - 5pm	apple services
0	Monday	8am - 5pm	entertainment
0	Monday	8am - 5pm	google services
0	Monday	8am - 5pm	Microsoft office
0	Monday	5pm - 8am	social media
0	Monday	5pm - 8am	email
0	Monday	5pm - 8am	web app

1	Tuesday	8am - 5pm	apple services
1	Tuesday	8am - 5pm	google services
1	Tuesday	8am - 5pm	email
1	Tuesday	8am - 5pm	Microsoft office
1	Tuesday	5pm - 8am	entertainment
1	Tuesday	5pm - 8am	social media
1	Tuesday	5pm - 8am	web app
2	Wednesday	8am - 5pm	Microsoft office
2	Wednesday	8am - 5pm	web app
2	Wednesday	8am - 5pm	google services
2	Wednesday	8am - 5pm	email
2	Wednesday	5pm - 8am	entertainment
2	Wednesday	5pm - 8am	social media
2	Wednesday	5pm - 8am	email
3	Thursday	8am - 5pm	entertainment
3	Thursday	8am - 5pm	web app
3	Thursday	8am - 5pm	google services
3	Thursday	8am - 5pm	Microsoft office
3	Thursday	8am - 5pm	apple services
3	Thursday	5pm - 8am	web app
3	Thursday	5pm - 8am	social media
3	Thursday	5pm - 8am	google services
3	Thursday	5pm - 8am	email
4	Friday	8am - 5pm	entertainment
4	Friday	8am - 5pm	web app
4	Friday	8am - 5pm	apple services
4	Friday	8am - 5pm	google services
4	Friday	8am - 5pm	Microsoft office
4	Friday	5pm - 8am	web app
4	Friday	5pm - 8am	social media
4	Friday	5pm - 8am	dns
4	Friday	5pm - 8am	quic
4	Friday	5pm - 8am	email
5	Saturday	8am - 5pm	entertainment
5	Saturday	8am - 5pm	web app
5	Saturday	8am - 5pm	Microsoft office
5	Saturday	8am - 5pm	google services
5	Saturday	8am - 5pm	apple services
5	Saturday	5pm - 8am	web app
5	Saturday	5pm - 8am	google services

5	Saturday	5pm - 8am	entertainment
5	Saturday	5pm - 8am	social media
5	Saturday	5pm - 8am	email
6	Sunday	8am - 5pm	web app
6	Sunday	8am - 5pm	entertainment
6	Sunday	8am - 5pm	Microsoft office
6	Sunday	5pm - 8am	web app
6	Sunday	5pm - 8am	social media
6	Sunday	5pm - 8am	quic
6	Sunday	5pm - 8am	google services

Figure 12: Data for daily application usage

id	Location	Network	Signal Strengt	Lat	Long
0	Motulsky Area	Student	-40	5.7592625000	-0.21989640000
0	Motulsky Area	Staff&Faculty	-52	5.7592625000	-0.21989640000
0	Motulsky Area	Ashesi Guest	-56	5.7592625000	-0.21989640000
1	Warren Library	Staff&Faculty	-63	5.7597718000	-0.21947775000
1	Warren Library	Ashesi Guest	-60	5.7597718000	-0.21947775000
1	Warren Library	Ashesi Air	-48	5.7597718000	-0.21947775000
2	Lab 221/222	Student	-64	5.7596852000	-0.22069000000
2	Lab 221/222	Staff&Faculty	-59	5.7596852000	-0.22069000000
2	Lab 221/222	Ashesi Air	-66	5.7596852000	-0.22069000000
3	Water Sisulu	Student	-44	5.7587236000	-0.22076690000
3	Water Sisulu	Ashesi Guest	-55	5.7587236000	-0.22076690000
3	Water Sisulu	Sisulu Air	-46	5.7587236000	-0.22076690000
4	Oteng	Student	-38	5.7587236000	-0.22052110000
4	Oteng	Staff&Faculty	-44	5.7587236000	-0.22052110000
4	Oteng	Ashesi Guest	-65	5.7587236000	-0.22052110000
5	Health center	Ashesi Guest	-43	5.7593220500	-0.21812597000
5	Health center	SURFINN	-40	5.7593220500	-0.21812597000
5	Health center	Ashesi Air	-45	5.7593220500	-0.21812597000
6	New hostel	Student	-63	5.758156	-0.221108
6	New hostel	Staff&Faculty	-80	5.758156	-0.221108
6	New hostel	Ashesi Guest	-60	5.758156	-0.221108
7	Engineering workshop d	SURFINN	-40	5.7591234500	-0.21765764000
8	ghanaclimate Innovatior	Ashesi Air	-42	5.7590234500	-0.21755764000
9	Electronic lab/Design LA	Student	-48	5.7594807000	-0.21934830000
9	Electronic lab/Design LA	Staff&Faculty	-52	5.7594807000	-0.21934830000
9	Electronic lab/Design LA	Ashesi Guest	-43	5.7594807000	-0.21934830000
10	Registrar area	Ashesi Guest	-88	5.7597718000	-0.22003290000
10	Registrar area	Ashesi Air	-48	5.7597718000	-0.22003290000
10	Registrar area	Ashesi North	-40	5.7597718000	-0.22003290000
11	Admin Area	Student	-67	5.7596844000	-0.22033330000
11	Admin Area	Staff&Faculty	-51	5.7596844000	-0.22033330000
11	Admin Area	Ashesi Guest	-43	5.7596844000	-0.22033330000
12	115/116 area	Staff&Faculty	-56	5.7595482000	-0.22014160000
12	115/116 area	Ashesi Guest	-54	5.7595482000	-0.22014160000
12	115/116 area	Ashesi Air	-70	5.7595482000	-0.22014160000
13	217area	Student	-58	5.7593228000	-0.22020970000
13	217area	Staff&Faculty	-60	5.7593228000	-0.22020970000
13	217area	Ashesi Air	-73	5.7593228000	-0.22020970000
14	samory toure greene lou	Student	-45	5.7594202100	-0.21946335000
14	samory toure greene lou	Ashesi Guest	-72	5.7594202100	-0.21946335000
14	samory toure greene lou	Staff&Faculty	-66	5.7594202100	-0.21946335000
15	Bill and Jeanne Bliss Stu	Student	-58	5.7590078000	-0.22062230000
15	Bill and Jeanne Bliss Stu	Staff&Faculty	-78	5.7590078000	-0.22062230000
15	Bill and Jeanne Bliss Stu	Ashesi Student Cou	-50	5.7590078000	-0.22062230000
16	ephraim amu hall	Student	-72	5.7590132000	-0.22052110000
16	ephraim amu hall	Staff&Faculty	-78	5.7590132000	-0.22052110000
16	ephraim amu hall	Ashesi Student Cou	-52	5.7590132000	-0.22052110000
17	Efua Sunderland Hall	Ashesi Guest	-82	5.7591072000	-0.22066880000
17	Efua Sunderland Hall	Ashesi Student Cou	-53	5.7591072000	-0.22066880000
17	Efua Sunderland Hall	Hostel Lobby	-80	5.7591072000	-0.22066880000
18	Hostel Front Desk	Ashesi Student Cou	-73	5.7590044000	-0.22007230000
18	Hostel Front Desk	Hostel Lobby	-43	5.7590044000	-0.22007230000
18	Hostel Front Desk	Berekuso	-60	5.7590044000	-0.22007230000
19	Akorno	Student	-48	5.7592525000	-0.21999640000
19	Akorno	Ashesi Guest	-46	5.7592525000	-0.21999640000
19	Akorno	Staff&Faculty	-44	5.7592525000	-0.21999640000

Figure 13: network signal strength data

References

Aline, F., Pierre-Andre, F., & Claude, G. (n.d.). Adaptive bandwidth allocation method for non-reserved traffic in a high-speed data transmission network, and system for implementing said method. *EP0781068A1.* Cisco Technology, Inc., New York.

ANDREW, S. T., & DAVID, J. W. (2011). *COMPUTER NETWORKS.* Library of Congress Cataloging-in-Publication Data.

Bandwidth Management and Traffic Optimization. (2017, March Saturday). Retrieved from dualwan.org: http://dualwan.org/ bandwidth-management.html

Behrouz, A. F. (2010). *TCP/IP Protocol Suite.* New York: McGraw-Hill.

Behrouz, A. F., Catherine, C., & Sophia, C. F. (1998). *DATA COMMUNICATIONS and NETWORKING.* New York: The McGraw-Hill Companies.

Bernard, J. J., Amanda, S., & Isak, T. (2009). *Handbook of Research on Web Log Analysis.* New York: Information science reference.

Carter, R., & Crovella, M. (1996). *Dynamic Server Selection using Bandwidth Probing in Wide-Area Network.* Boston University.

CRUZ, P. (2000). ADOPTING A BUSINESS-ORIENTED APPROACH TO BANDWIDTH MANAGEMENT. *Computer Technology Review*.

Diana, R. (2005). *Towards the digital library: findings of an investigation to establish the current status of university libraries in Africa.* UK: International Network for the Availability of Scientific Publications (INASP) Oxford.

Flickenger, R. (2006). *How To Accelerate Your Internet.* INASP/ICTP.

Lance, T., Martin, A., & Carey, W. (2003). *A Performance Comparison of Dynamic Web Technologies.* Calgary: University of Calgary, Calgary, AB.

N, H., Monowar, H. B., R, C., D, K. B., & J, K. K. (2014). Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications* , Pages 307-324 .

Rob, L., Shanshan, Q., & Dimitrios, B. (2010). Progress in tourism management: A review of website evaluation in tourism research. *Tourism Management*, Page 297–313.

Robert, C., Bamshad, M., & Jaideep, S. (1999). Data Preparation for Mining World Wide Web Browsing Patterns. *Knowledge and Information Systems*, Page 5-32.

Roger, H. L., Alberto, H. F., & Ee-Peng, L. (2005). Report on the Fifth ACM International Workshop on Web Information and Data Management (WIDM 2003) . *ACM* (pp. 277-278). ACM SIGIR Forum.

Tobias, O. (2001). Monitoring Your IT Gear: The MRTG Story. *Journal of IT Professionals, IEEE Educational Activities Department Piscataway, NJ, USA*, Page 44-48.

Venter, G. (2003). *Optimising Internet Bandwidth in Developing Country Higher Education.* Oxford, U.K.: International Network for Availability of Scientific Publications.

Vikas, S., Vikram, K., & Balvir, S. T. (2011). NEEDO FB ANDWIDTHM ANAGEMENT ANDF ORMULATIONO FP OLICYF RAMEWORKF OR. *International Journal of Computer Sciencea ndC ommunication*, pp. 173-178.