DEVELOPMENT OF AN ACCEPTABLE USE POLICY FRAMEWORK FOR IBBUL COMMUNICATION NETWORK

BY

Muhammad DANGANA

Department of Electrical and Computer Engineering

Faculty of Engineering

Ahmadu Bello University

Zaria, Nigeria

JANUARY, 2016

DEVELOPMENT OF AN ACCEPTABLE USE POLICY FRAMEWORKFOR IBBUL COMMUNICATION NETWORK

BY

DANGANA Muhammad, B.Eng. (FUT, Minna) 2006

(MSc/ENG/1376/2011-2012)

dangana@ibbu.edu.ng

modanji@yahoo.com

A DISSERTATION SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES, AHMADU BELLO UNIVERSITY,

ZARIA

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF A MASTER OF SCIENCE (MSc) DEGREE IN TELECOMMUNICATION ENGINEERING

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

FACULTY OF ENGINEERING

AHMADU BELLO UNIVERSITY,

ZARIA

JANUARY, 2016

DECLARATION

I, DANGANA Muhammad, hereby declare that this dissertation titled **"Development of an Acceptable Use Policy Framework for IBBUL Communication Network"** was carried out by me as part of the requirements for the award of Master of Science in Telecommunication Engineering, AhmaduBello University, Zaria. To the best of my knowledge, this research work has never been submitted anywhere for the award of any certificate. All literatures used and cited in this report, are duly acknowledged by means of references.

DANGANA Muhammad _____ _____

Signature **Date**

CERTIFICATION

This dissertation titled “Development of an Acceptable Use Policy Framework for IBBUL Communication Network” meets the requirements for the award of degree of Master of Science (MSc) in Communication Engineering by Ahmadu Bello University, Zaria and it is approved for its contribution to knowledge and literature.

Chairman, Supervisory Committee		
(Dr. S.M. Sani)	**Signature**	**Date**
Member, Supervisory Committee		
(Dr. A. D. Usman)	**Signature**	**Date**
Head of Department		
(Dr. Y. Jibril)	**Signature**	**Date**
Dean Postgraduate School		
(Prof. K. Bala)	**Signature**	**Date**

DEDICATION

I dedicate this research work to God, the Lord of the Universe.

ACKNOWLEDGEMENT

All praises be to the LORD of the UNIVERSE, Who shape things the way HE wants it. I thank God Who Has included this certificate in my achievements, I shall always be grateful to Him.

My gratitude also goes to my parents; Alhaji Suleiman Dangana and Mallama Zainab Muhammad for thecontinuous support they have been giving me. I also thank them for their love.

I sincerely appreciate the support of my dear wife, (Hafiza)Zainab Muhammad Swasu. Her support has always put me on the fast lane. Your patience, encouragement, care and love shall never be forgotten. I always thank God for you because ladies like you are hard to come by. My sincereappreciation also goes to my lovely son, AbdulBasit Ashraf Muhammad, may ALLAH continue to guide him and may he achieve greater things in life. To my family, I love you all.

I shall forever be grateful to the chairman of my supervisory team,Dr. S. M. Sani for all his encouragement and professionalism in supervising my work. He single handedly pulled me back into this MSc programme after all hopes were dashed. May the Lord of the Universe reward him without measure. He shall always be in my memory. I sincerely appreciate my co-supervisor Dr. A. D. Usman for not relenting in his support to me. May ALLAH reward him for all his advice and efforts.

My special appreciation also goes to the Head of the Department Prof. M.B Mu`azu for all his advice. I shall also be grateful to Dr. S. Garba for all his encouragements, time and advices. His contribution to the success of this work is profound, may ALLAH reward him. My appreciation also goes to Dr. A.EAdedokun for all his supports.

My gratitude also goes to the PG Coordinator, Dr. A. M. S. Tekanyi, who, despite hisenormous tight schedules, still find time to see that this work conform to the set standards. I also thank him for all his advice. I appreciate the contributions of Prof. B. G. Bajoga, Dr.K.A. Abubilal, Prof.Jimoh, Dr. J.Y. Oricha for creating the time to go through my manuscripts. I am also indebted to Engr. E. Okafor, and Engr. Adamu for their advice. Most especially, I am grateful to all the lecturers in the Department whose names could not be

mentioned. My esteem appreciation goes to MallamAbdullahiTukur for all the administrative support.

Finally, I shall never forget the understanding and support of my siblings: AbdullahiNdagi, Umar Saba, IsahYaya, HadizaTalatu, Hussaina and Hassana, Bintu and my uncle Barr. Ibrahim Dangana. May Allah keep the love; give us good health and prosperity.

DANGANA Muhammad

January, 2016.

ABSTRACT

Bandwidth utilization in a campus network if not properly managed,may leads to the congestion of the network bandwidth. This research work presents bandwidth control system implemented at the access layer of a campus network which is aimed at reducing the processing time at the core of the network. Ibrahim BadamasiBabangidaUniversity Lapai (IBBUL) campus network was monitored and data were collected on daily basis between 12am to 11pm over a period of 60 days (from 1st September, 2014 to 30th October, 2014). Analyses of these data were carried out which include: (i) peer-to-peer (p2p) activities, (ii) user traffic analysis and,(iii) web analysis. The analyses revealed the highest and lowest p2p activities of the users across the monitored nodes, as well as the time-of-day they occurred. It also revealed the nodes with the highest traffic and the time-of-day it usually occurred. Based on these results, IBBUL network scenario was modelled and simulated using Graphical Network Simulator 3 (GNS3). A star network topology with a Juniper EX4200 core was modelled. Juniper EX2200 series switches were modelled as the access layers. A number of host computers with various specifications were also attached to these switches and all the devices were configured appropriately. Traffic shaping technique was employed to implement bandwidth regulation on the access layer switches. The results obtained were validated by comparing it with the monitored data collected. From the results it was noticed that the developed model performed better by reducing the average processing time of the core to 6.00ms when bandwidth management was implemented at the access layer as compared to the average processing time of 9.950ms when bandwidth management was implemented at the core. This represents about 40% reduction in processing time. The average rate of download and upload speeds of the network users increased by 203.76Kb/s and 110.07Kb/s respectively. This represents about 95% improvement in the download and upload speeds.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Acronyms	Definition
CLI	Command Line Interface
GUI	Graphical User Interface
IBBUL	Ibrahim BadamasiBabangida University, Lapai
ICT	Information and Communications Technology
LAN	Local Area Network
VCS	Virtual Chassis Switch
ISP	Internet Service Providers
NSMExpress	Network System Monitor Express
WLC	Wireless Local Controller
BYOD	Bring Your Own Device
QoS	Quality of Service
WANO	Wide Area Network Optimization
GNS3	Graphical Network Simulator 3
RAS	Remote Access Server
VPN	Virtual Private Network
PING	Packet Inter-Network Groper
MRC	Maximum Rate Control

LBFS	Low-Bandwidth File System
AUP	Acceptance Use Policy
SDN	Software Defined Networking
P2P	Peer-to-Peer
JNM	Juniper Network Monitor
MAC	Media Access Control
URL	Unified Resource Locator
Mbps	Mega bits Per Second
HTTP	Hypertext Transfer Protocol
TCP	Transmission Control Protocol
UTM	Unified Threat Management
RED	Random Early Detection
WRED	Weighted Random Early Detection
VM	VirtualBox Machine
RTT	Round Trip Time
ICMP	Internet Control Message Protocol

CHAPTER ONE

INTRODUCTION

1.1 Background

This chapter discusses the network structure of IBBUL, the type of devices use in the network, as well as the challenges facing the network with respect to bandwidth management.

1.1.1 IBBUL Network Structure

With the use of wired or wireless connectivity, instant access to email, the Internet and other IT services has dramatically changed the way people live, work and study. To this end, students, staff and visitors always expect easy access to most information and services of an institution.

While academic institutions are characterized by high rate of electronic file sharing and Internet surfing, Ibrahim BadamasiBabangida University, Lapai (IBBUL) as a fast growing institution is not exempted from such demand. These demands can only be met effectively with a robust bandwidth management policy.

The current population of IBBUL comprising both students and staff is about ten thousand, nine hundred and seventy five (12,975) (Ibrahim, 2015). In the year 2006, IBBUL network bandwidth was 1Mbps/1Mbps (1Mbps uplink and 1Mbps downlink) used for its online academic activities. This was gradually increased to its present size of 45Mbps uplink and 45Mbps downlink in order to provide adequate resource sharing among its academia (Ibrahim, 2015)

Figure 1.1 shows the current network structure of IBBUL (Ibrahim, 2014). From Figure 1.1 it can be seen that the Information and Communications Technology (ICT) Center houses the data centre that provides all the Internet connectivity and Intranet services through optic fiber backbone network to other buildings on the campus. This fiber optic backbone is single-mode with 10Gbps capability and covers a distance of 10km. A star topology is used for the network where every network device is connected to a central point. IBBUL network infrastructure comprises of the following devices: Juniper Networks products (45%), Cisco Systems, Inc (35%), Ubiquitous Networks (15%) and D-Link (5%).

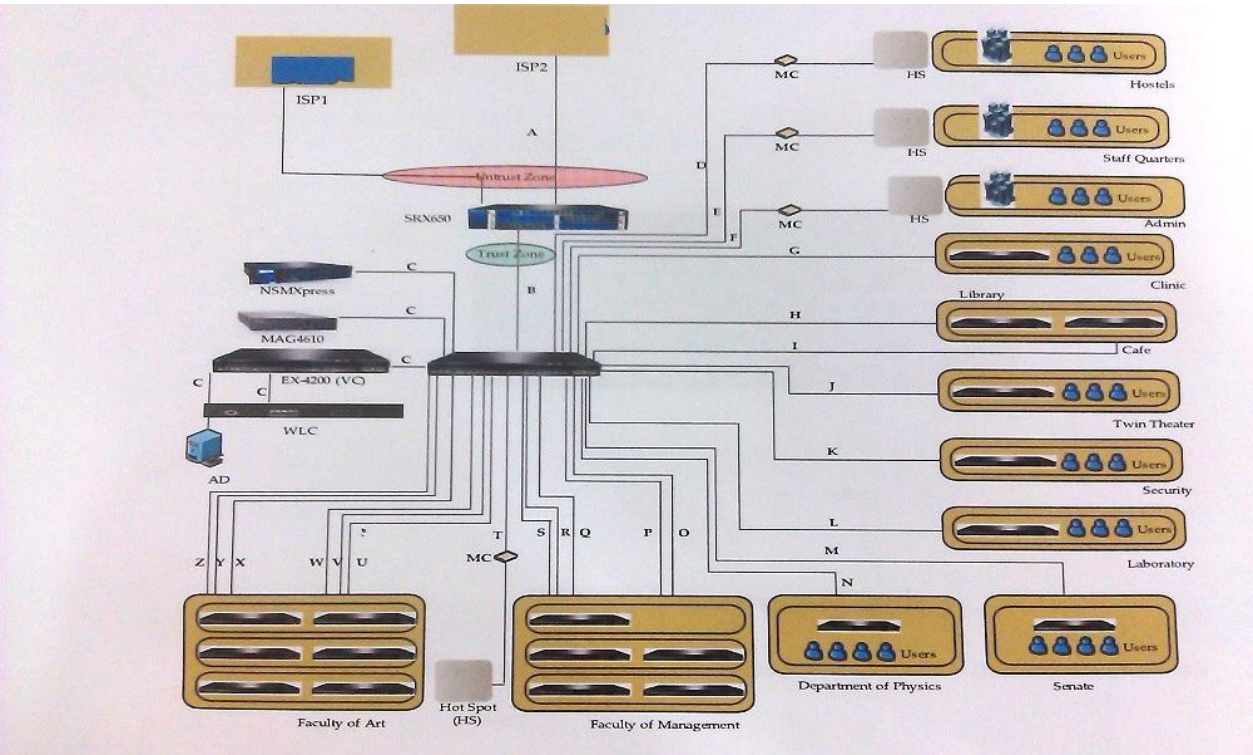


Figure 1.1: Network Structure of IBBUL (Topology)(ICT Center, IBBUL)

As shown in Figure 1.1, each Department in a Faculty such as Faculty of Arts, Management and Social Science, as well as other buildings such as: the Central Laboratory, the Security Office, Senate Building, Library, School Clinic and twin theatre have Ethernet Local Area Network (LAN) structure. Multi-Layer switches (Juniper EX 2200 series) are used to connect the LANs in these buildings. Optical fibre cables (i.e B-Z) are used to connect other devices to the Virtual Chassis Switch (Core).

The IBBUL network is interfaced with the Internet through a secure and reliable Juniper SRX 650 Firewall device. This firewall is capable of accommodating up to four (4) different Internet Service Providers (ISPs) into a single network depending on the internal distribution of the service. Also connected to the Virtual Chassis Switch is the Juniper Network System Monitor Express (NSMExpress). This NSMExpress has Orion Network Performance Monitoring software installed on it for network monitoring. The Wireless Local Controller (WLC) which controls all the wireless devices in IBBUL network is directly connected to the Virtual Chassis Switch.

Figure 1.2 (ICT Center, IBBUL) shows the hot spot devices in the IBBUL environment. One hot spot is located between Faculty of Sciences and the Faculty of Management, the hostel

and staff quarters have one hotspot each. Hotspots typically provide Internet access through wireless access points for laptops, smart phone, etc. These hotspots have about 30m coverage range. In addition to the LAN in some of these buildings, hotspots are provided to increase the number of connected users. These buildings include: ICT Centre, Library and Senate building. These hotspots are connected to the Virtual Chassis Switch using an interface called the Media Converter.

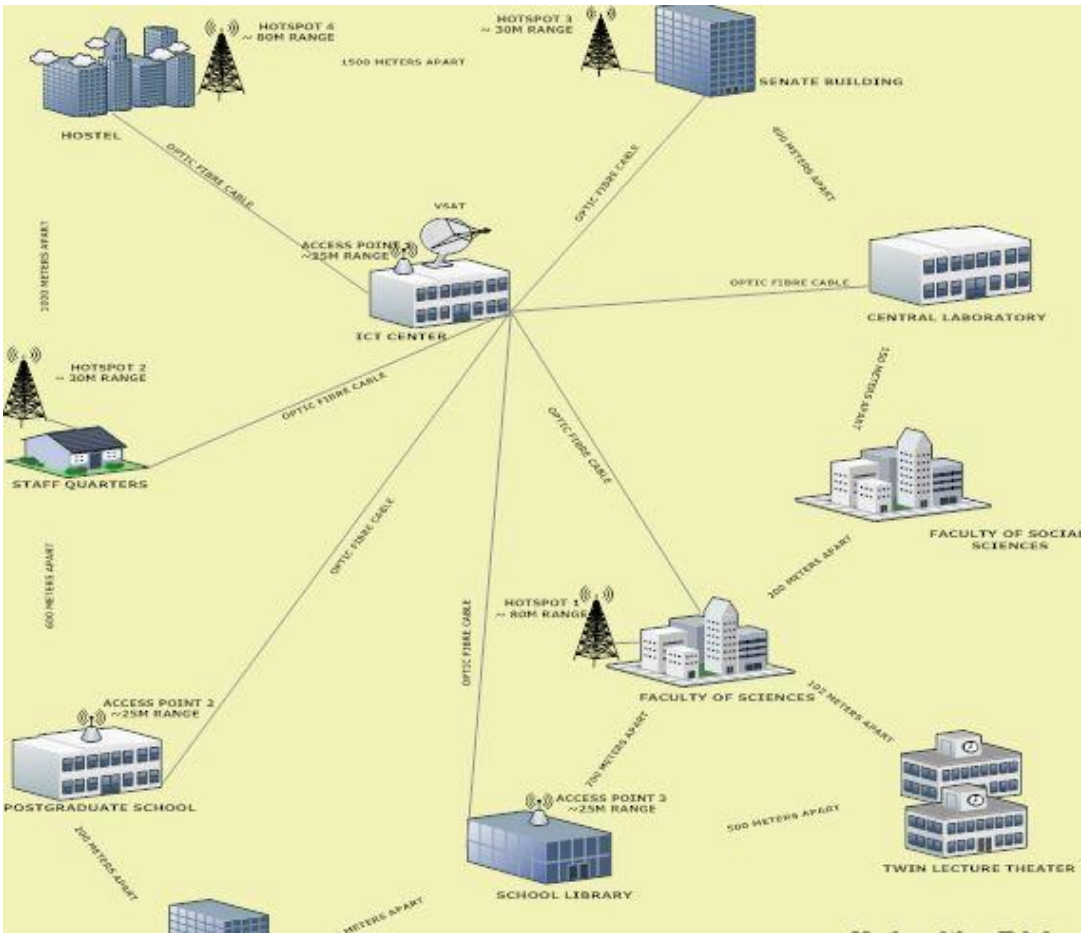


Figure 1.2: Network Structure of IBBUL (Buildings and Hotspots)(ICT Center, IBBUL)

The VSAT in Figure 1.2 connects IBBUL network to its Internet Service Provider (ISP).

Nevertheless, with the current bandwidth size of 45Mbps as compared to the current staff and student population of about 12,975 in IBBUL and the trend in Bring Your Own Device (BYOD) technology (such as smart phones, notepads, etc.) among students as well as University staff, the institution network is being congested. Thus, the need for effective bandwidth management policy. This policy is intended to facilitate effective and enhanced learning within and outside the classroom(s); and support a broad range of multidisciplinary

research activities that would deliver innovative academic and business solutions and serve as a source of revenue for the IBBUL University.

The major challenges experienced by IBBUL are:

(i) students' overuse of undesired applications;

(ii) lack of prioritization of traffic or applications;

(iii) use of multiple devices to access the network by students` and staff;

(iv) long connectivity durations by users;

(v) automation of connectivity by users` devices such as laptops, smart phones, tablets, etc;

(vi) poor application performance such as Windows updater, etc;

Apart from the limited bandwidth, the improper use of existing connectivity is a major challenge. Inappropriate use of existing bandwidth, due to absence of bandwidth management strategies promotes bandwidth wastage on unwanted traffic such as viruses; music and movie download by some users. The largely unrestricted access exposes the University Internet connectivity to bandwidth-hogging applications such as media streaming. No matter how much more bandwidth is bought, it will quickly get exhausted if no bandwidth management policy is in place.Hence, the need for an effective and efficientbandwidth management policy.

1.2 Aim And Objectives

The aim of this dissertation is thedevelopment of decentralized bandwidth utilization management model for access layer in order to improve the performance of IBBUL campus network that will meet the demands of IBBUL community as a multidisciplinary institution.

This will be achieved through the following objectives:

(i) To reduce the work load and processing time at the core of the network in order to achieve improvement in the network performance.

(ii) Development of a traffic classification based bandwidth management system which will aid in effective utilization of the bandwidth.

(iii) To improve the network performance of IBBUL in order to have reliable access by all users.

1.3 Problem Statement

Regardless of the type of network (wired or wireless) being accessed by users, bandwidth is a scarce resource that needs to be controlled among its users. In IBBUL, the use of multiple devices by users to access the network, their long connectivity durations and the current lack of bandwidth management policy have led to the congestion of the University network especially at peak hours. It is therefore important that the University network has an accountable bandwidth management policy. This research is therefore aimed at developing an acceptable use bandwidth management policy for IBBUL network.

1.4 Methodology

The following methodology was adopted in carrying out this research work:

I. Monitoring and collection of data traffic flowing through the network. The data traffic was collected from the monitoring server between 12am to 11pm daily for a period of 60 days (from 1st September, 2014 to 30th October, 2014). A packet capturing software (Juniper Network Monitor) was used for the collection of the data;

II. Analysis of the collected traffic for traffic classifications; using PRTG software;

III. Bandwidth regulations (or resizing), traffic filtering and traffic priority setting usingtraffic shaping as a bandwidth management technique was used;

IV. Implementation of step III at Access Layer levels;

V. Modelling and simulation of network scenario;

VI. Validation of results by comparing the simulation results and that of the data collected before simulation;

VII. Proposing an acceptable bandwidth utilization policy based on results obtained for optimization of IBBUL network.

1.5 Significant Contributions

Quite a number of research work have been carried out in the direction of bandwidth management, however, to the best of my knowledge, these works have focused on managing bandwidth at the core layer of the networks. While this approach is common, this research has chosen to implement bandwidth management on the access layer of the network. This is aimed at reducing the data processing time of the core. The significant contributions of this work include: (i) reduction of the processing time at the core of the network, (ii) improvement of the browsing experience by users of the network, and (iii) development of an acceptable use policy.

1.6 Dissertation Organization

Chapter one of this dissertation presents the general introduction. The review of similar works as well as relevant fundamental concepts about bandwidth and its management, bandwidth categorization, types of bandwidth management techniques and hierarchical network structure are presented in chapter two. Chapter three presents the materials and methods used in carrying out the research such as network monitoring and data collection, modelling and simulation. The results obtained from the monitored network areanalysed, simulated and discussedin chapter four. Chapter five presents the conclusions and recommendations of the dissertation. References lists and appendices are also presented at the end of this dissertation.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This section reviews some of the paramount theoretical concepts and similar research works that are relevant to this research. These will give a clear understanding of the research undertaken and help in designing an effective approach to solving bandwidth congestion.

2.2 Review of Fundamental Concepts

This part gives a brief description on the following: the importance of bandwidth and its management, categorization of bandwidth management, the various types of bandwidth management techniques and policies (such as traffic shaping, congestion avoidance, etc), comparative analysis of simulators and hierarchical network structure.

2.2.1 Bandwidth and its Management

Bandwidth can simply be thought of as a representation of the capacity of the communication media (especially network devices: switches, routers, Ethernet cables, fibre optic cables, etc.) to transfer data from source to destination(Athicha, et al., 2010).The wider the route or path for data transmission, the more the packets of information will be transmitted to the user's Internet enabled devices (Athicha, et al, 2010). Bandwidth is also a gross measurement, taking the total amount of data transferred in a given period of time at a particular rate, without taking into consideration the quality of the signal itself(McGuigan, 2010).

Bandwidth is measured in bits per second (bps) and there are various Internet connections with different bandwidth standards. For instance, the traditional dial-up Internet connection provides a very narrow bandwidth limit of about 56 kbps, also some broadband connections allow data transfer at much higher speed ranging from (128 kbps to 2Mbps, as well as STM-1 which offers 155Mbps).Improving the performance of the information delivery chain is urgent if researchers and students are to benefit from the Internet and take part in the international academic communitywork (Rosenberg, 2010). The performance of the existing

Internet connections can be enhanced by monitoring and control mechanism and this is known as bandwidth management. Bandwidth management is a process of controlling and measuring communication (traffic, or packets) on a network link in order to avoid network congestion and poor performance(Dualwan, 2010). It is possible that a University with a small bandwidth connection will still have its Internet access. However, if the bandwidth connection is increased and the bandwidth management strategyis removed, useful access to the Internet will decrease immediately and soon become impossible(Rosenberg, 2010). A bandwidth management functions by sorting outbound network traffic into various classes according to service and application types. Traffic is then planned out according to the minimum and maximum bandwidth that is configured for each of the traffic types (Dualwan, 2010).

2.2.2 Bandwidth Management Categorization

Components of bandwidth management are classified into three broad categories, if any one ofthese activities or categories are missing, then the management of bandwidth is significantly compromised. These activities inform and reinforce each other for better utilization of scare bandwidth(Rosenberg, 2010).

Figure 2.1 shows the relationship among bandwidth management activities.

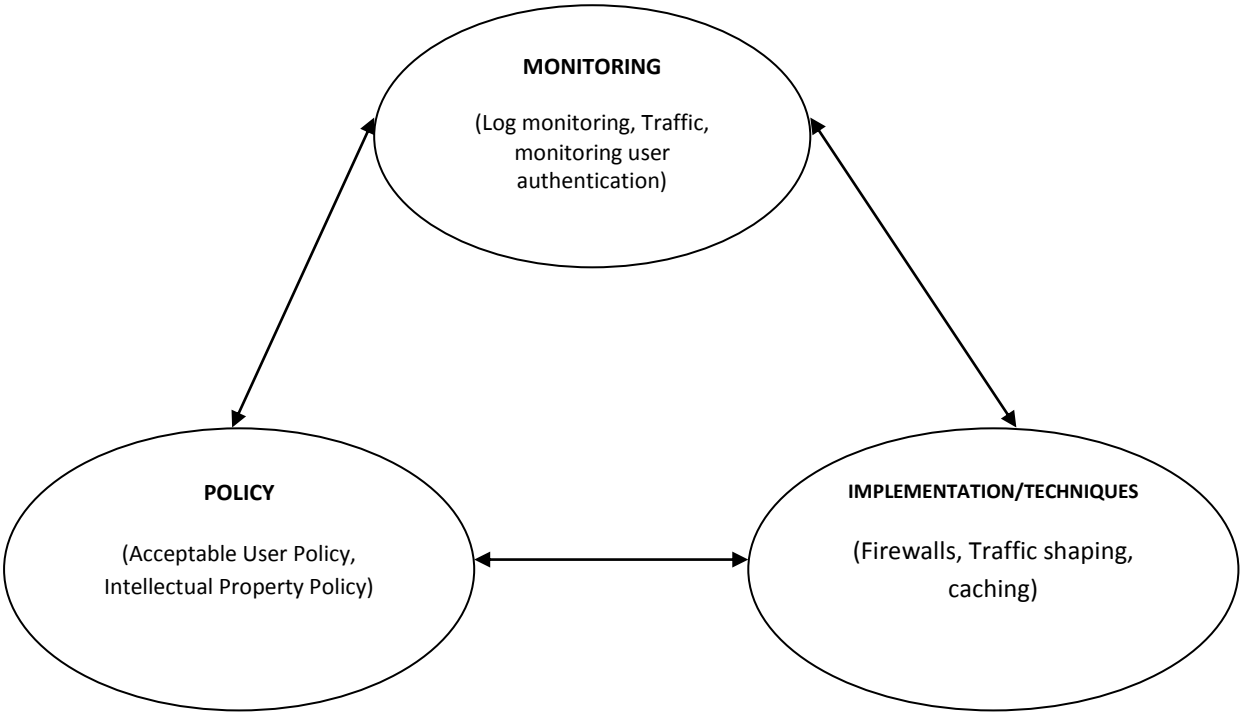


Figure 2.1: Components of Bandwidth Management Activities(Lockias, 2012)

Figure 2.1 is a simple illustration of the components or categorization of bandwidth management activities. The direction of the arrows shows how these components are linked. It is obvious that policy is an essential component of any bandwidth management strategy. Technical solutions will be difficult to implement without it. Policies are essential in that they provide the framework for defining how a network is to be used and detail how technical solutions should be implemented. Without a policy, users will not understand what they are doing or why, and will complain or subvert administrative actions instead of helping administrators to achieve the bandwidth management goal. Policy-based management allows a University to control which network services and resources are available to its users in accordance with its Information Technology strategy(Rosenberg, 2010). Without an Acceptable Usage Policy (AUP)for the Internet no amount of bandwidth is enough to satisfy the demands of an unrestricted user community. Individuals downloading music and other files for their personal use can use up an institution's bandwidth. Frequently it is the minority that consumes the majority of available bandwidth(Athicha, *et al*, 2010).

The institution's policy needs to be understood and enforced. It therefore becomes the responsibility of the network administrators to find out which users are not adhering to the policy and to find a suitable penalty on the user. While policies are being formed, respect for intellectual properties should be considered. This is to avoid the use of some Internet material that the institution do not have right to accesseither by the students or staff. Monitoring involves both technical and physical check on the network. These checks help in the enforcement of policy, faults diagnosis and accurate troubleshooting on the network. Nevertheless, network monitoring generates the process ofcreating an enforceable policy that reflects the actualneeds of the user group. In monitoring, users authentications or right to access the network are being observed. This will help to identify unauthorized network users and to know how the network authentication system handles that. Monitoring how network users log into the network and how their traffic transverse the network will give network administrators an insight on usage patterns.

Implementation of the policy requires a number of tools and techniques that would helpnetwork administrators to ensure that bandwidth is being managed properly and policy is adhered to.The key components include (Dualwan, 2010):

(i) Network Analysers for monitoring traffic

(ii) Firewallsfor blocking malicious and unwanted traffic

(iii) Anti-Virusfor protecting network servers against viruses

(iv) Cachesfor efficientbandwidth utilization

(v) Traffic Shapersfor prioritizing and controlling traffic

(vi) Quota Systemsfor managing user behaviour

(vii) Bandwidth capping for pegging individual use of the network bandwidth.

2.2.3 Types of Bandwidth Management Techniques

Many bandwidth management techniques have been developed and some of these techniques are discussed as follows:

(i) Traffic Shaping

This is a form of bandwidth management technique that limits the bandwidth size that will be available to certain data streams. This is done by limiting the bandwidth utilization of a particular application or limiting the bandwidth utilization of each user. Example of traffic shaping is to specify that traffic from file-sharing software never exceed 250 Kbps. Traffic shaping have the advantage of handling these routine evasive manoeuvres by inspecting each packet of data carefully.However, limiting by the type of application (or port number in some cases) is occasionally difficult because software (applications) can be designedto use random port numbers to communicate in order to evade traffic shapers (Bill, 2012).

(ii) Congestion Avoidance

These are algorithms that reduce the congestion being experienced over a network link. The algorithms function by either reacting to the detection of a congestion on a link (due to packet loss or explicit notification), or by simply anticipating congestion through monitoring traffic levels. The following are types of congestion avoidance methods: Random Early Detection (RED), whichis a discipline for a network scheduler suited for congestion avoidance and Weighted Random Early Detection (WRED), which is a method where a single queue may have several different queue thresholds. For the latter, each queue threshold is associated with a particular traffic class for the congestion avoidance(Barry, 2011). The minimization of congestion on network links improves the overall performance, however, packet loss and delay resulting from congested links usually requires retransmission of the data by the sending host, this might also exacerbate the situation.

(iii) **Quality of Service (QoS) Assignment**

This is used to refer to the features that allow network administrators to configure specifications for the delivery of services over a network along the lines of integral QoS features (usually related to IP traffic) in networks. QoS is implemented as a series of queues on routers to manage traffic by either dropping or delaying packets. These queues are managed by a number of queuing mechanisms which act on the traffic held in the queues with the aim of effecting a measure of management and implementation of QoS(Barry, 2011).

(iv) **Wide Area Network (WAN) Optimization**

This technique does not discriminate between traffic streams as found in packet shapers and QoS devices. However, WAN optimizers use a variety of techniques to strip out the inefficiencies and redundancies from network traffic. WAN optimizers are designed to speed up all the traffic that passes through it.

In this dissertation work, it proposed to use the traffic shaping specification as a bandwidth management technique. This is because of its features such as the flexibility of assigning limitations on bandwidth usage.

2.2.4 Comparative Analysis of Network Simulators

Network simulators are used to test different network parameters before the real-life deployment of such a network (Jim, 2013). Different types of network simulators such as: OPNET, OMNet++, QualNet, Network Simulator-2, GNS3, Packet tracer etc, are compared in terms of availability, complexity, result presentation, number of tuneable network parameters and Graphic User Interface (GUI). Table 2.1 summarizes a comparative analysis among the types of simulators in use.

Table 2.1: Comparative Analysis of Some Simulators (Jim, 2013)

Name of Simulator	Availability	Complexity	Result Presentation	No. of tuneable network parameters	GUI	Support for Access Layer
MATLAB	License required	Average	Good	Average	Average	No
OPNET	License required	Average	Fair	Low	Fair	No
Network Simulator - 2	Freeware	High	Fair	Low	Low	Yes
GNS3	Freeware	Average	Good	Good	Good	Yes

MATLAB is a performance language for technical computing. It integrates computation, visualization and programming. Typical uses include: Modelling, simulation, and prototyping, data analysis, exploration, visualization, math and computation, algorithm development, scientific and engineering graphics,and application development, including graphical user interface building(Hansel and Boul, 2011).

OPNET simulator is a tool used in the simulation of the behaviour and performance of a network. The main difference with other simulators lies in its power and versatility. This simulator makes possible working with Open Systems Interconnection (OSI) model, from layer 7 to the modification of the most essential physical parameters(Jaw, 2003).

Network Simulator 2 supports networking research and education with the following features (Ke, 2014):

(i) protocol design to formulate a protocol

(ii) traffic studies to analyse and study network traffic

(iii) protocol comparison can be used to compare the performance of protocols

(iv) it supports new network architecture designs;

(v) it is freely distributed and open source;

Graphical Network Simulator 3 (GNS3) is an open source simulator with the capabilities of designing and optimizing a state-wide telecommunications network. GNS3 can design and build networks of any size. GNS3 can provide a multi-vendor virtual environment. GNS3 is not vendor specific, since real networks are not vendor specific. It can supportCisco, Juniper, HP, Arista, Citrix and Brocade products. GNS3 canintegrate a wide variety of networking systems and simulation can gain access to a growing list of freely available virtual networking appliances. GNS3 also provides graphical user interface that runs on traditional PC hardware and can be used on multiple operating systems, including Windows, Linux, and MacOS X.

Due to the features of GNS3 and its advantages against others (such as its complexity level and result presentation), it shall be used for this research work.

2.2.5 Hierarchical Network Structure

The common hierarchical network structures that exist usually simplify the traffic routing in a network. Hierarchical network models comprise of main components such as: access network, distribution network (convergence/aggregation network) and core network (backbone network). The functions of these layers or networks are discussed in the following sections:

1 Core Layer Functions

The core layer provides a high-speed backbone to forwards all traffic in the network. It also provides very strong routing and forwarding capability and wide bandwidth. Functions and attributes of the core layer include the following (Kurose & Ross, 2011):

i. The implementation of redundancy in both network devices and network links in order to avoid the existence of any point of failure; allow this layer to provide a high speed, reliable and available backbone.
ii. Using quick-converging routing protocols, it also provides quick adaptation to network changes.

2 Aggregation Layer Functions

This aggregation layer is responsible for interfacing between the core and access layers. Its functions include:

i. Traffic between the access and core layers are being routed through this layer;
ii. Provides redundant connections, both to access devices and to the core devices.

3 Access Layer Functions

Access layer is the point of entrance of the users to the network. Users can be local or remote. Local users typically access the network through connections to a LAN switch. Remote users might access the network through the Internet, Remote Access Server (RAS) using VPN connections. Access layer functions include:

i. Provides workgroup/user access to the network;
ii. Implement Quality of Service mechanism.

One of the advantages of using a network structure based on layers is modularity, which means designing a network based on modules. Modularity is a very important characteristic in network since it allow easy scalability and it allows devices that have similar and well-defined functions to be grouped at each layer, which makes it easy to add, replace and remove individual devices (Tavares, 2011)

With IBBUL network having a star topology, it is obvious that the core (Virtual Switch) handles all information for processing. Decentralization of bandwidth management using traffic shaping technique from the core to the access layers shall relieve the core long processing time and provide better bandwidth management. This was tested using the Packet Inter-Network Groper (PING) Test.

2.3 Review of Prior Works

This section presents a review of some works that have been carried out with respect to bandwidth management.

Jeng.et al., (2006) wrote a research paper that addressed the problem of bandwidth allocation under the weighted maximum rate constrained link sharing policy (an important management feature for service providersand many applications). The paper also proved a key theory in the condition of allocation termination. Three algorithms of weighted Maximum Rate Control (MRC) fair queuing were proposed. They include: WMRC-Intuitive, WMRC-Sorting and WMRC-Partition. These algorithms have different running time complexities which were implemented on a PC-based platformto find the best-practice algorithm which was WMRC-Partition. In this research work also, the average case complexity was reduced but the authors did not relate its work to bandwidth management policy.

Dejan.et al., (2007) wrote a research paper that proposed, implemented and evaluated a mesh based high bandwidth data dissemination system under both static and dynamic network conditions. This technique was found to out perform previous technigues. The system was designed tokeepitsincomingpipefullofuseful datawithaminimalamountofcontroloverheadfroma dynamicsetof peers. In the process, they defined the importantaspects of the general data dissemination problem andexploredseveralpossibilitieswithineachaspect. The results found show that each ofthese

tenets of file distributionis animportantconsiderationinbuildingfile distributionsystems. Adaptive strategies where employed by the system which can adjust over time toself-tunetoconditionswhichwillperformwellinamuchwiderrangeofconditions,andindeedin manyscenariosof dynamically changing conditions. While the system helped in maintaining high bandwidth under dynamic network conditions, the paper did not discuss how this bandwidth can be managed and implemented on Access Layer Switches.

Yongpei.et al., (2008) wrote a research paper that was aimed at maximizing Internet Service Provider`s (ISP) revenue by presenting a decentralized auction-based scheme for bandwidth allocation and pricing in a differentiated service-based network. This is achieved by a mathematical formulations. For a multiple bottleneck link case, a heuristic algorithm is developed to solvethe problem. In this research paper, clients are allowed to bid on the price they are willing to pay and the service theyrequire. The service provider decides the resources (bandwidth) to allocate to each individual as well as thresholds for each differential service class based on the clients' bids, in a way that aims to maximize his revenue. The paper also considered a single bottleneck link network as well as a larger network scope, which can contain hundreds to thousands of nodesand huge number of bottleneck links. For alarge-scale network, they proposed a heuristic algorithm and showed the results of various simulations, which comparedthe revenues generated by the auction approach with the flat-rate pricing approach. The results show that overall theauction approach brings the service provider more revenue than the flat-rate pricing approach. This paper proposed a bandwidth management scheme for revenue maximization which is targeted at ISPs. However, the paper did not discuss this bandwidth management at the Access Layer levels.

Athicha. et al., (2010) wrote a research paper that presentsLow-Bandwidth File System (LBFS); anetworkfilesystemdesignedfor low-bandwidth networks. LBFS exploits similarities betweenfiles or versions of the same file to save bandwidth.It avoids sending data over the network when the same datacanalreadybefoundintheserver'sfilesystemortheclient'scache. Usingthistechniqueinconjunctionwithconventionalcompression and caching, LBFS consumed very low bandwidth as compared to traditional network file systemson common workloads. It is this low bandwidth comsumption that makes LBFS practical forsituations where other file systems cannot be used. In manysituations, LBFS makes transparent remote file access a viable and less frustrating alternative to running interactiveprograms on remote machines. This paper discussed how LBFS can be used to share small network files over a low-

bandwidth network. However, it did not discuss how bandwidth management policy can save a situation where limited bandwidth is demanded by numerous users.

John. et al., (2011) wrote a research paper that examined the management of a network with respect to congestion in both the Local Area Network (LAN) and on the Internet backhaul. In this research work, three approaches were used: (i) NetCracker Professional Software® was used to simulate aWAN scenario in which files of various sizeswere copied across the WAN links from a serverto a remote desktop. The latency for the different file sizes was noted; (ii) an IBM Trivoli,whats-up-gold and PRTG® software were used to obtainreadings of bandwidth, latency, throughput, andCPU utilization as well as user voice and videoexperience on a life, corporate network runningon fiber links; (iii) the testing of user's perceptionwhen copying big files, watching videos, playinginteractive games and making concurrent calls across WAN links. From the analyzed results obtained, the research concluded that as the offered load in a network increases, the throughput decreases. It also recommended that since choice of protocol to be used in any file transfer depends on thetype of packet to be routed, then protocol optimization canbe used to improve the efficiency of traffic that usesCIFS, FTP, HTTP, MAPI and TCP protocols. However, this paper did not discuss how bandwidth management and policy can be used to continually optimize this scarce resource.

Aloi and Pace, (2012) wrote a research paper that focused on new benefits of applying an adaptive period inventory managementpolicy to a wireless cognitive telecommunications scenario. Systematic supply of bandwidth is done in order to maximize both economic profit andquality of service offered to wireless users. The paper also designed a wise-cost effective supplying bandwidth policy, with the aim of extending the soundness of the techniques to to different application scenarios. The research developed a bandwidth supplying module and the results obtained shows that the module performed well in both static and dynamic operation conditions. This made the overall communication architecture more attractive and effective. However, this paper is focused on Internet Service Providers (ISP) for cost effectiveness and effective bandwidth sharing. The paper did not extend its discussion to bandwidth consumers such as Universities.

Lockias, (2012) investigated the issue of bandwidth maximization in some universities. The research surveyed a sample of five universities and catalogued their experiences. A mixed

methods approach was used to gather relevantdata. The first was information (data) gathering on ICT governanceand policy issues. The targeted respondents were personnel from the Information Technology Servicesdepartment, Computer Centres or other related departments. Principal authorities, including ViceChancellors, Librarians and Registrars. The second was an administration of emailed questionnaire and phone interviews. The questionnaire incorporateda series of questions about campus infrastructure, including the number of computers that werenetworked or connected to the Internet, bandwidth management strategies used and thechallenges faced. The results found showed that most of the Universities sampled do not have an official Acceptance Use Policy (AUP) to assist with bandwidth management. However, the research did not sample the universities that implement bandwidth management at Access Layer levels.

Maduka, (2012) researchedon evidence-based policy-making of bandwidthoptimization in a university network, giving rise to improved network performance and cost savings. Theresearch data were based on network event logs (network monitoring) from a campus network. A post-data-collection was done by conversion of collected logs into database entries which were then analyzed. This analysis was done to drawuseful insights about the needs and behavioural patterns of users on the network. The results found suggested that optimum bandwidth management is achievable by means of evidence based policyresearch and implementation and policy recommendationswere made for the campus network. However, the research did not suggest the implementation of this bandwidth management at Access Layer levels in a campus network.

Devajit. et al., (2013) developed an application based bandwidth management tool. This development tool is used to combat the challenges that are facing the easy flow of data transmission in network designs. PHP, MySQL, Notepad++ and Apache where the application system design tools that where used to simulates a simple wirelessbased intranet network environment which calculates thesize of any file that is to be sent over the network. When thefile size exceeds the allotted bandwidth by the administrator,the transfer process is terminated. The system also enablesan administrator to change the allowed network bandwidthbased on preferences. Clients systems are allowed to shareand transfer files as long as they are within the allowed bandwidth range. This research work did not cover to large scale organizations such as Universities (which have both Intranet and Internet connectivities) in the management and control of their network bandwidth.

Andrew, (2013) developed a bandwidth management scheme using traffic shaping on a campus network. Prioritization of users with less daily usage than those with heavy usage was carried out. Users with less Internet usage were assigned faster speed than those whose usage is high. While users, who always download something from the Internet, were punished (they were assigned slower speed). The strategy used was simply to identify those users with high traffic and putting them in a certain group/pool with limited speed. This was achieved using the following steps: (i) User based Authentication System (hotspot) with external radius server, custom perl script and Mikrotik`s radius attributes. (ii) Each client bandwidth usage with the radius server accounting system was recorded. (iii) A running script was created on the server to calculate user`s total bandwidth of the day. (iv) The script is made to send a radius attributes to Mikrotik to assign users in different HTB pools based on their usage. (v) The script was run for every minute. (vi) Another script was created that will reset the counters and groups at certain time. This technique improved bandwidth utilization management on the campus network however; this was implemented at the core of the network.

Wang.et al., (2013) proposed a bandwidth adaptation algorithm that is based on per class degradation for bandwidth management in heterogeneous wireless network. They compared the performance of this approach with another method via simulation experiments. They found out that there were some trade – offs between the two methods. The per-class method generally has better fairness than the per flow method, since it degrades all the flows in certain class and thus has better fairness than the per flow method. It also provides computation simplicity and executed faster, which is important to the admission control component. Applying QoS means treating some traffic in preference to others, and this implies the ability to reject traffic, hence, prioritization of traffic through classification is paramount which is not the case in this work.

Deepika & Rama, (2014)used a Software Defined Networking (SDN)to estimate path loss rate and latency for effective bandwidth utilization in a college campus network. SDN adapts it send rate to the estimated bandwidth, while using active measurement techniques to measure the path loss and latency between two nodes. This method allows the calculation of loss and latency using the initial packet separation and the time stamps as input. Comparison of bandwidth measurements was done using iperf between traditional network and SDN, results obtained from simulation using mininet shows better performance in SDN than

traditional network. The drawback in the proposed SDN framework was that, as the number of switches increases the performance decreases.

Zaghloul, (2014) presented a research work on the importance of having prioritization of mission-and time-critical traffic for optimum utilization of bandwidth for high-value applications and maintenance of quality of service (QoS) levels. This was carried out by developing a computer program which was stored on a computer system ROM, this computer program operated when manage link bandwidth is executed to manage link bandwidth in a communication network having a plurality of routing. Also in this application, in order to compensate an unusual traffic, a reservation factor was used for this., especially in jamming environment that are not captured by the standard Connection Admission Control (CAC) algorithm. Traffic classification was also done in order to recognize packets moving across a network as part of an application or flow. The program makes decisions based on prioritization of traffic for QoS delivery. However, the program was not evaluated on routing and switching devices to be implemented on access layer network environment.

In conclusion, a lot of researches have been carried out to improve bandwidth efficiency and management. However, to the best of my knowledge, these researches did not implement bandwidth management at the Access Layer Switch levels.

This dissertation therefore, contributes to knowledge by developing a bandwidth allocation or management policy at Access Layer Switch levels for a multidisciplinary university network like IBBUL. This shall be achieved through the use of Traffic shaper bandwidth management technique and developing an Acceptable Use Policy (AUP).

CHAPTER THREE

MATERIALS AND METHODS

3.1 Introduction

This chapter describes in detail the materials and the methods used in carrying out bandwidth utilization management system at the access layer of the network.

3.2 Method of Data Collection

The Network monitoring was carried out by logging a selection of activities that where of interest to bandwidth utilization on the network. This was carried out over a period of 60 days (from 1st September, 2014 to 30th October, 2014) and between 12am to 11pm daily. The collection of these logs where done using a packet capturing software (Juniper Network Monitor) across some selected nodes in the main campus. Since these research nodes are setup on a Tier -2 standards, the challenge of stable electric power supply to these nodes where eliminated. At the end of the monitored period, the collected logs were then analyzed to see its relationship with bandwidth utilization.

The loggings of selected network activities or events for this work include those activities of the network users that are considered to consume a large part of the bandwidth. The following event logs were carried out and then further analyzed: Peer-to-Peer (p2p) events and analysis. This was carried out to simply know the amount of bandwidth utilized by p2p events. Web–proxy events and analysis. This was used to understand the web resources that are of interest and frequently used by users. Finally, the hotspot events and analysis, which was used to discover patterns in network use within the University.

A packet capturing based log repository (Juniper Network Monitor) is capable of collecting log messages from distant devices on a network and cataloguing them based on message type and source. A twelve (12) number access layer switch were being monitor (two-third of the total). These Access Layer Switches (Node A, B … L) have an in-built utility for packet based logging. This facility enables the forwarding of log messages from each node to a remote server. The type of messages been forwarded include: firewall logs generated when p2p traffic is detected; web-proxy logs (URLs visited by users); and user session statistics (hot spot messages).

The hotspot session information or statistics includes details such as: user session start and end time, total downloaded and uploaded bytes, MAC-address of each device used, hotspot login parameters, and the node and client IP addresses. At the establishment of each session, which is initiated by a login, a custom router-embedded script (managed by Juniper MAG device) collects initial parameters of the client. This is then forwarded to the server for use in creating a new session entry in the catalogue. The initial parameters includes: the client's IP and MAC addresses, time of login and the network node.

3.3 Data Monitoring

Figure 3.1 is a simple illustration of the network monitoring setup.

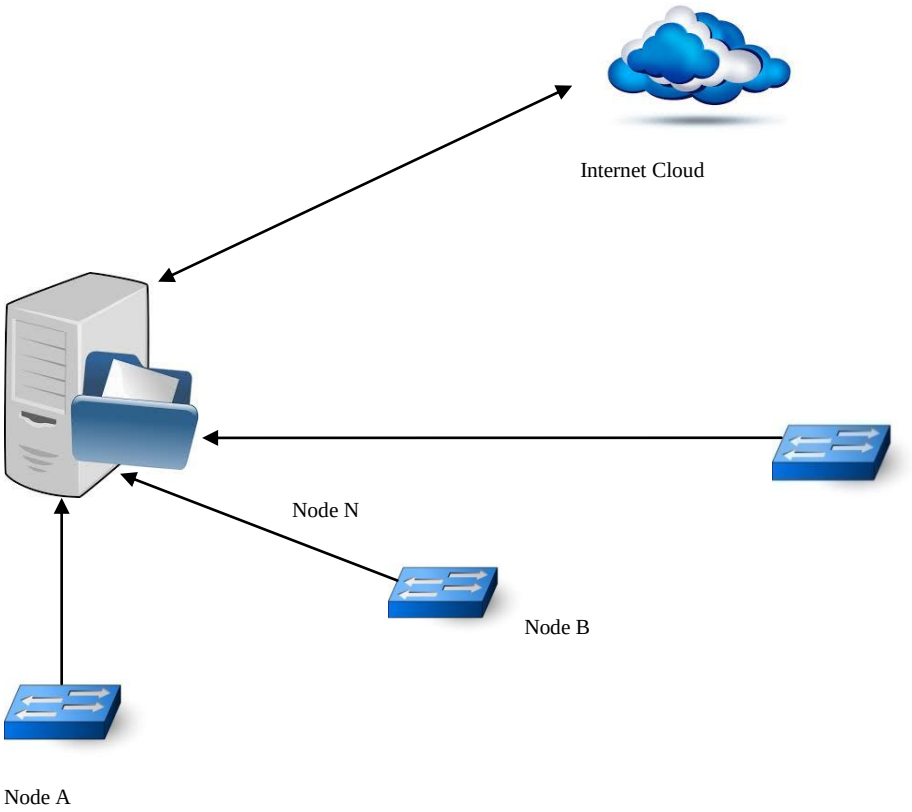


Figure 3.1: A Schematic of the Network Monitoring Setup

The logs from the selected nodes are collected into the server for analysis. Grouping of the entries in the log files were done based on their sources. The groups include: access layer switch (hotspot), web proxy and firewall. The messages related to each of these groups were processed accordingly as shown in Table 3.1:

Table 3.1: Messages and their Related Entries

S/N	Messages	Entries
1	Access Layer (Hotspot)	Start and End-of-session times Total Bytes (Download and Upload) IP Address MAC Address
2	Web Proxy	IP Address of source URL Visited
3	Firewall	P2p indication Time of occurrence

3.4 Installations and Configurations

An open source Graphical Network Simulator 3 (1.3.1 all-in-one) was downloaded from http://www.gns3.com and installed in 8.1 Windows operating system. A general configuration of the simulator was carried out at the edit and preference tab. This was done by selecting the specifications that are required for the simulation. These specifications are provided at the edit tab and the preference tabs. These general configurations include: the IOS Image directories, style, classic etc. Oracle VirtualBox Machine (VM) software was also downloaded from https://www.virtualbox.org/wiki/Downloads alongside an extension pack 4.0.3. These where installed on the same system and configured. The installation was done by following the procedures of the software after meeting its requirements. Juniper IOS Image software called JunOS Olive was downloaded from: https://community.gns3.com/thread/7020 and was also installed.

3.5 Simulation

For the simulation, the Oracle VM VirtualBox Manager was launched first. The JunOS Olive 12.1.r.1.9 IOS Image software was imported into the VM. To import this IOS images, this was carried out through the file menu tab, the import appliance was clicked and the prompted page was used to navigate to the location of the IOS Image file. All the necessary settings including checking the *Reinitialize the MAC address of all network cards box*. This is shown in Figure 3.2

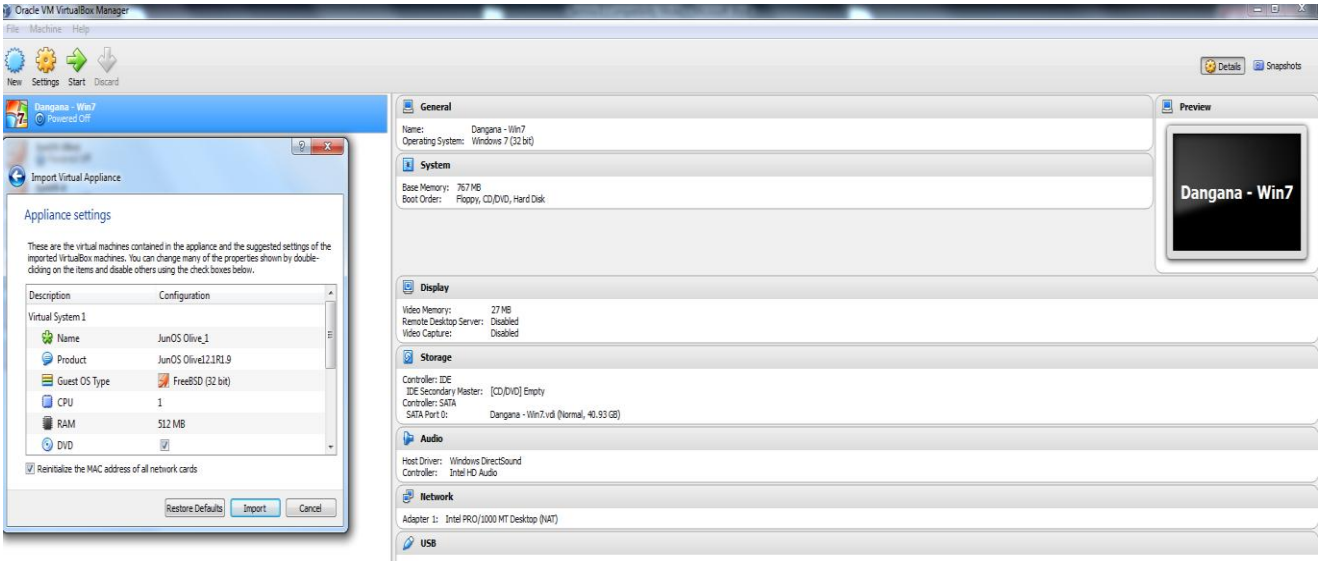


Figure 3.2: Importing JunOS IOS to VM

Since multiple juniper devices will be used for the simulation, several clones of the IOS Images were made to allow for this purpose. This was achieved using the clone tab on the Oracle VM as shown in Figure 3.3

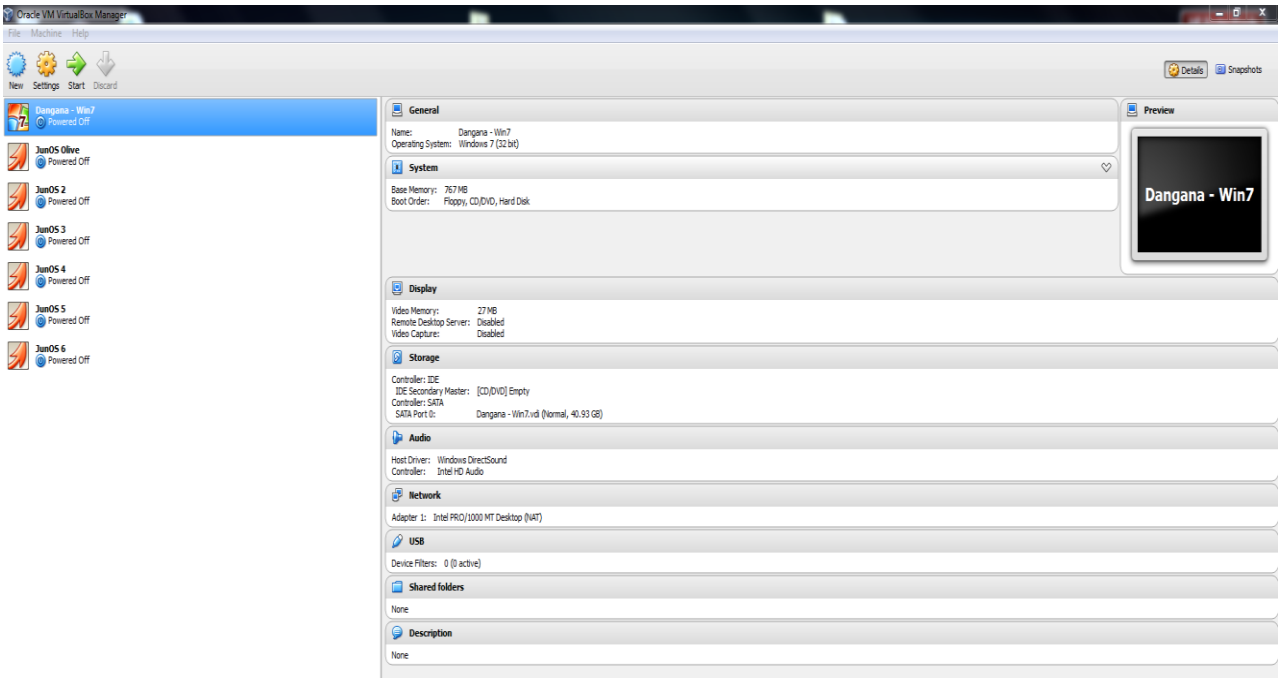


Figure 3.3.: Clones of IOS on VM

GNS3 was then launched, using the preference tab on GNS3, all the needed JunOS Olive IOS Images were imported from Oracle VM to the GNS3. With all the devices in place, the

desired network structure was modelled on the topology page of the GNS3 simulator as shown in Figure 3.4

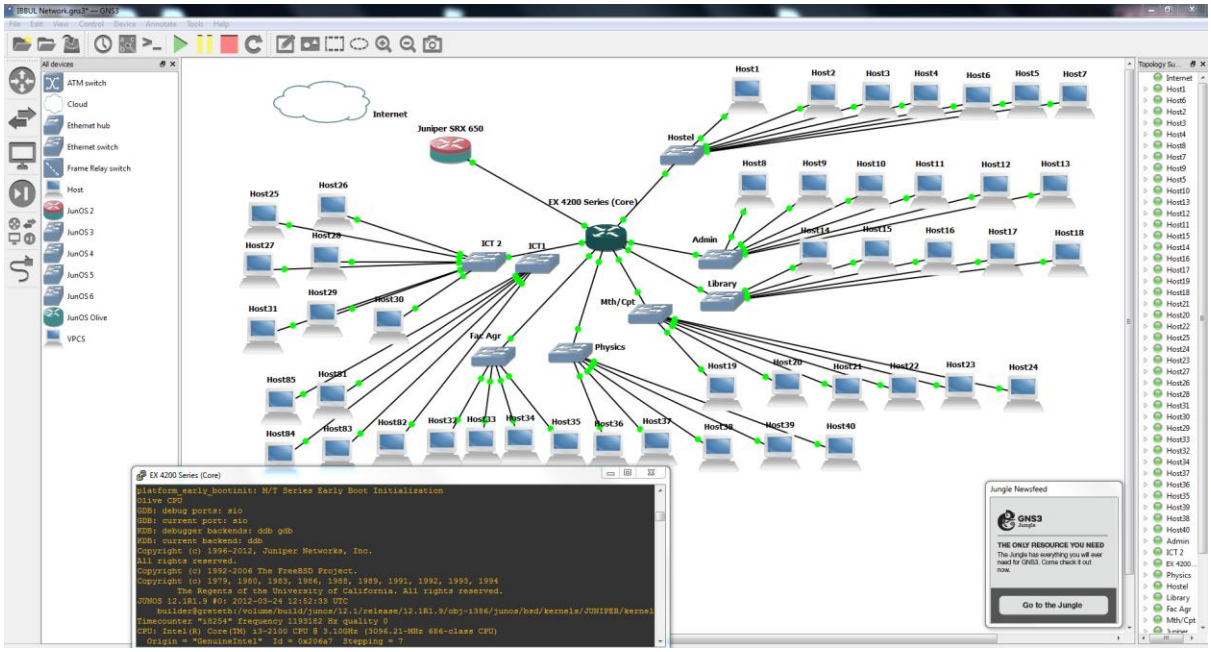


Figure 3.4: Simulated Network Scenario

With the modelled network, all the necessary configuration of the Juniper network devices was made and simulations were carried out. Simulation involving the retrieval of Internet resources by the users without any bandwidth management in place and another simulation that involves the retrieval of Internet resources with bandwidth management in place were both carried out. The bandwidth management was carried out using traffic shaping technique on the access layer of the network.

3.5.1 Simulation Parameters

The research is based on some parameter specifications which include:

I Network Structure: This indicates the topology of the network which includes the core;

II Access Layer Capability: This defines the level of intelligence of the access layer;

III Rate Limit: This specifies the bandwidth limit configured which was achieved using traffic shaping technique.

3.5.2 Traffic Filtering (Web Filtering)

Web filtering allows the management of bandwidth and Internet usage by preventing access to inappropriate Web content. However, from the user behavioral pattern and the number of sites been visited by these users, a classification of traffic was made. This include: Academic Sites and Non-academic Sites. This classification was made based on the fact that IBBUL is an academic institution.

To enhance traffic filtering, the classification of traffic based on the most visited sites is presented in Table 3.2.

Table 3.2: Classification of sites

S/N	Academic sites	Non-academic sites
1	Yahoo mail	Pornography
2	Gmail	Exclusive
3	Institution mail	Windows update
4	Institution portal	Olufamous
5	Wikipedia	Gambling
6	MSN	Naijapals
7	News	

Although, some sites cannot be easily classified as academic or non-academic because they can be used for both. Example of these web sites includes Facebook and Youtube. While it is obvious that these sites consume much bandwidth, they cannot be filtered or blocked completely. In order to manage the available bandwidth without blocking these sites, certain policies can be attached to these sites such as allowing the traffic of these specific URL at certain time-of-day coupled with the regulated traffic shaping technique in place.

This traffic filtering was targeted at every user and not to any specific group of users, and as such, this was carried out at the Firewall level (see figure 1.1). To achieve this traffic filtering, an Integrated Web filtering solution was used. The integrated Web filtering solution intercepts every HTTP request in a TCP connection. And in this case, the decision making is done on the device (firewall) after it identifies the category for a URL either from user-defined categories or from a category server (SurfControl Content Portal Authority provided by Websense). The configuration of traffic filtering was accomplished using a J-Web interface solution. The J-Web interface is a Graphic User Interface (GUI) that allows the

traffic filtering. It is easy to use and it also allow the filtering of traffic both in specified URL or grouped URL.

3.5.3 Steps for Traffic Filtering

1. Configuration of Global Web Filtering Options
2. Creation of Profile
3. Creation of Unified Threat Management (UTM) Policy
4. Attachment of UTMPolicy to Security Policy

3.5.3.1 Configuration of Global Web Filtering Options

To configure the Web Filtering feature profile, the following steps are involve:

i. **Configure>Security>UTM>WebFiltering**.

ii. On the **Globaloptions**.

iii. a**Juniperenhanced**tab was made active.

iv. In the **Cachetimeout**, the timeout (in minutes) for the expiration of cache entries was entered. A cache timeout of 21600 was used.

v. For the **Cache Size**, the maximum number of kilobytes (KB) for the cache was entered. A cache size of 1000KB was used.

vi. For the Server Host, **rp.cloud.threadseeker.com**as the Surf Control server name was entered.

vii. For the **Server Port**, number 80 was entered as the port number that will be used to communicate with the Surf Control server.

viii. The configuration was then committed using the action drop down menu.

Figure 3.5 shows the steps (i to viii) involved in the configuration of global web filtering options.

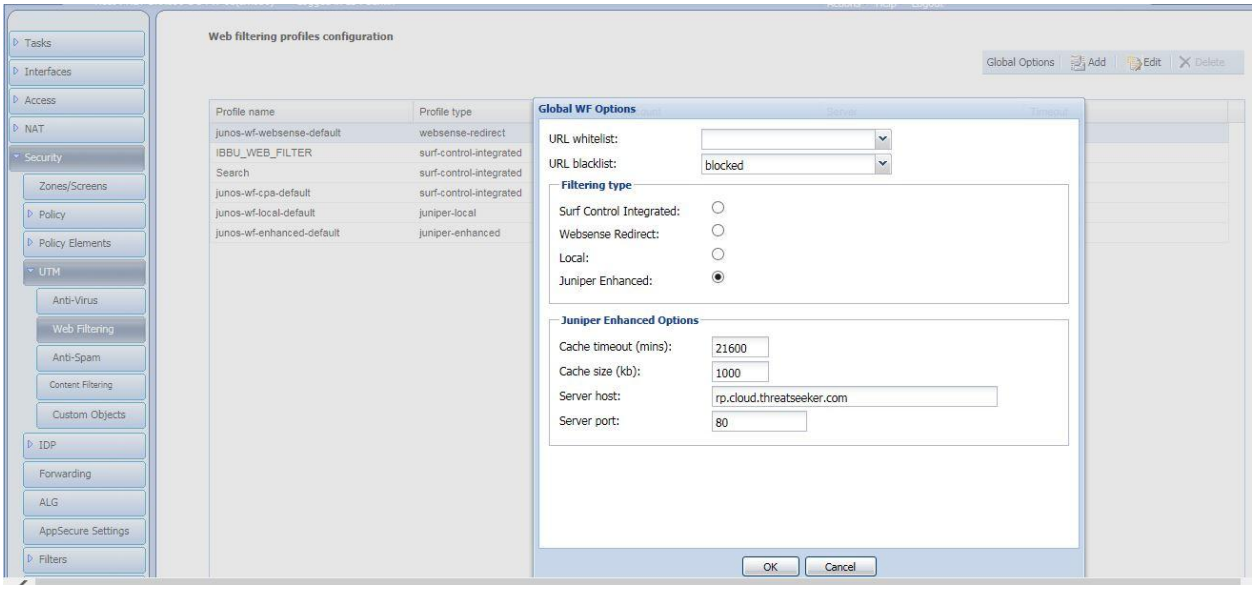


Figure 3.5: A Snapshot of the Configuration of Global Web Filtering Option

3.5.3.2 Creation of Profile

To create a profile name and to select a category from the included white list and blacklist categories, the following steps were carried out:

i. **Configure > Security > UTM > Web Filtering**.

ii. On the **Add**tab**,** a custom profile name (ibbul_ewfprofile01) was entered as the **Profile name**,

Figure 3.5.1 shows the steps (i-ii) involved in the creation of profile name.

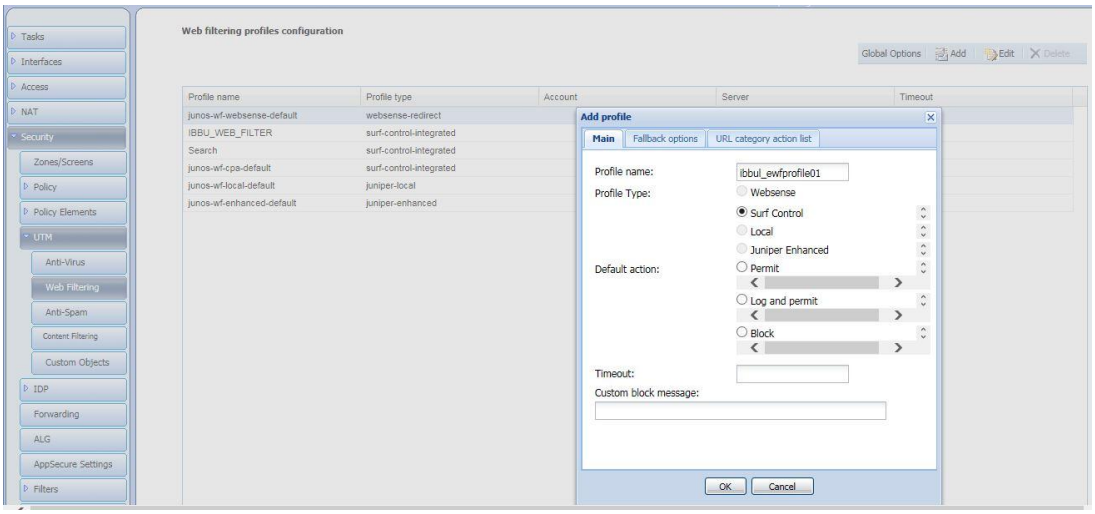


Figure 3.5.1: A Snapshot of Profile Name Creation

iv. The created profile ibbul_ewfprofile01 was then selected from the profile list.

v. From the **URL category action** list, the category and the action that is associated with the category were selected. Using the **Add tab,** more categories and associated actions was added. These categories and actions include: gaming, Adult_Sexually_Explicit, Criminal Skills, Advertisement, Hacking, etc.

Figure 3.5.2 shows the selected URL categories to filter. These URLs are not allowed in the network and are blocked to the network users.

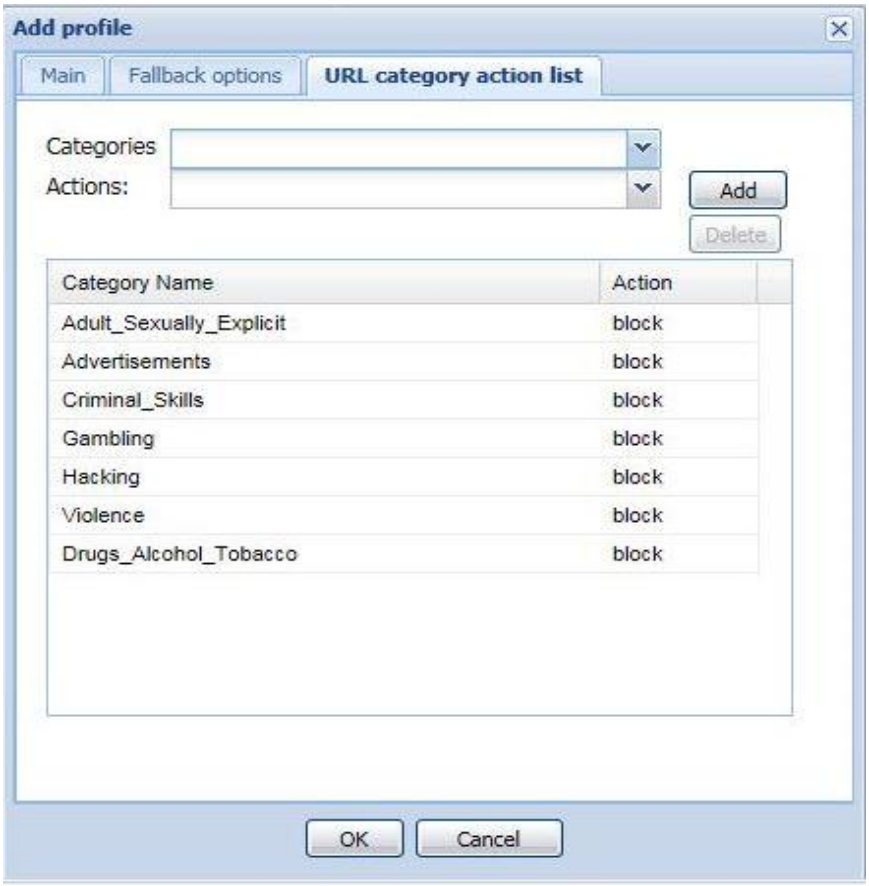


Figure 3.5.2: A Snapshot of Filtered Websites

vi. The **Site Reputation Action** and the **Log and permit** for all or required actions were then performed.

Figure 3.5.3 shows the reputation action of other sites that are allowed in the network.

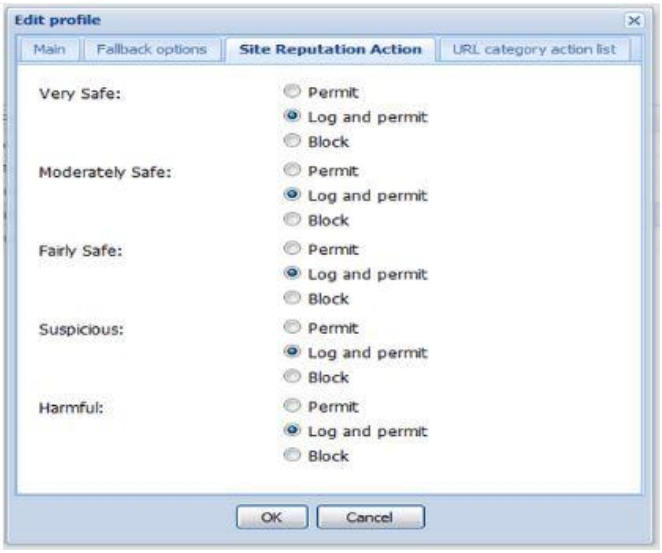


Figure 3.5.3: A Snapshot of Required Actions

This action (step vi) is necessary because it gives the permission to allow any other traffic through the network excluding the blocked ones.

vii. At the **Main tab**, under the **Default action**, **Log and permit were** selected.

Figure 3.5.4 shows the default action. The step allows the acceptance of all traffic before filtering take place.

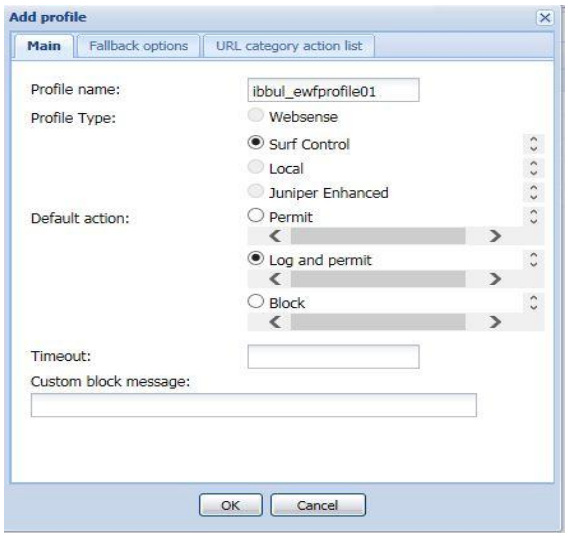


Figure 3.5.4: A Snapshot of Default Action

3.5.3.3 Creation of UTM Policy

To configure a UTM policy for Enhanced Web Filtering, the following steps were carried out:

i. **Configure > Security > Policy > UTM Policies**.

ii. On the **Add Policy** window is the main tab.

iii. In the **Policy Name** text field, a unique name for the UTM policy (ibbul_**policy**) was entered.

iv. In the **Session per client limit** text field with a session limit of 0 to 20000, a session per client limit of 12000 for this UTM policy was entered.

v. For the **Session per client over limit**, A **Block**was selected. This is the action that the device takes, when the session per client limit for thisUTM policy is exceeded.

Figure 3.5.5 shows the steps (i-v) involved in the creation of Unified Threat Management policy.

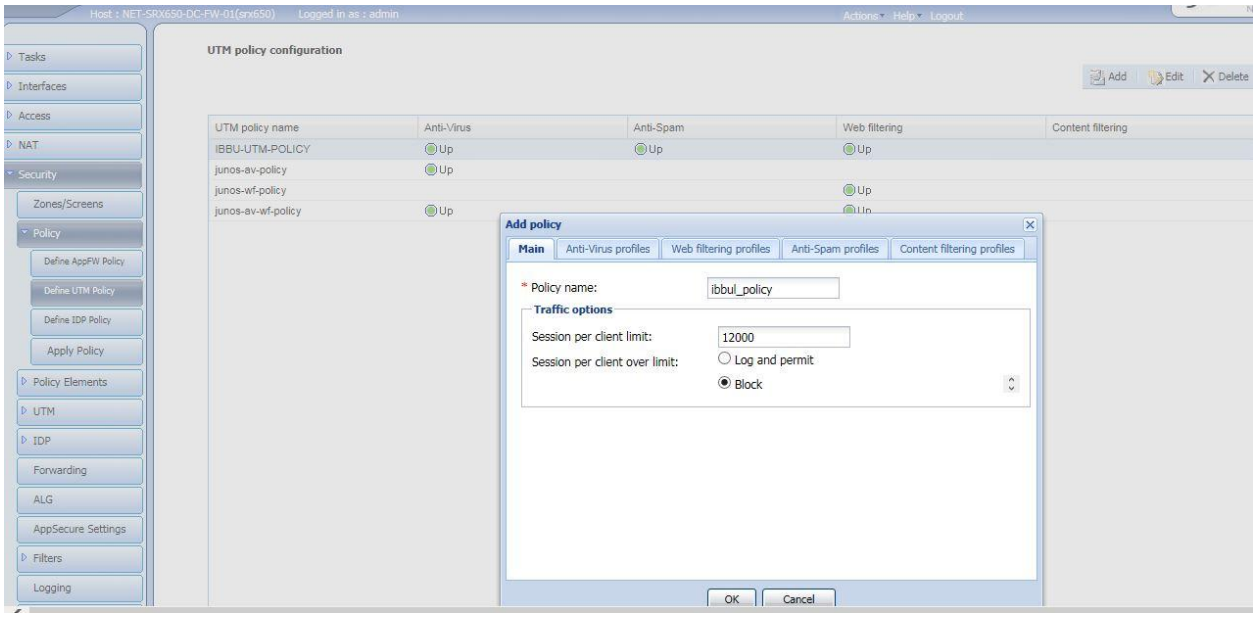


Figure 3.5.5: A Snapshot of Creation of UTM Policy

vi. On the web filtering profile tab, next to the **HTTP profile**, **ibbul_ewfprofile01** was selected.

Figure 3.5.6 shows the selection of the profile name.

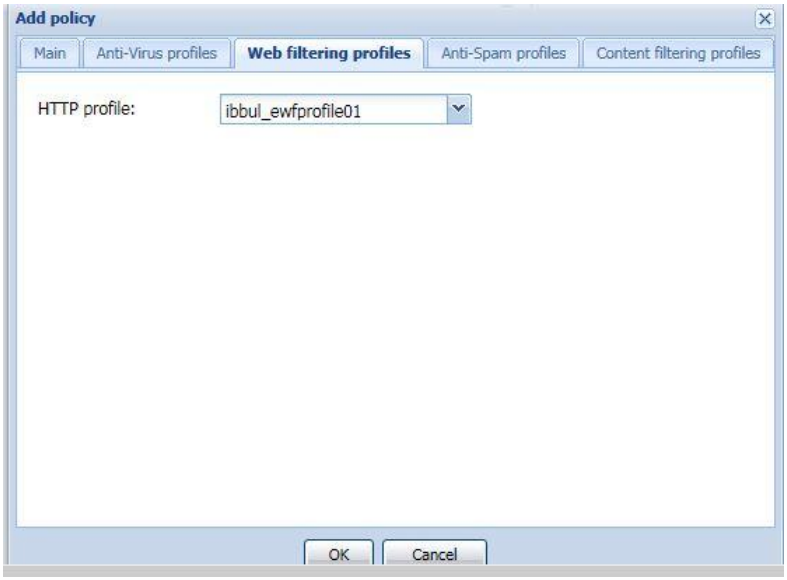


Figure 3.5.6: A Snapshot of Profile Selection

3.5.3.4 Attachment of UTM Policy to Security Policy

In order to attach a UTM policy to a security policy, the following steps were carried out:

i. **Configure > Security > Policy > FW Policies**.

ii. Using the **Policy** tab on the **Add Policy** window,

iii. In the **Policy Name** text field, the name of the policy (**web-filter**) was entered.

iv. Next to **From Zone**, a **trust**zone was selected from the list.

v. Next to **To Zone**, **untrust**zone was selected from the list.

vi. **any**was selected as the source address.

vii. **any**was also selected as destination address.

Figure 3.5.7 shows step (i-vii) involved in the attachment of UTM to security policy

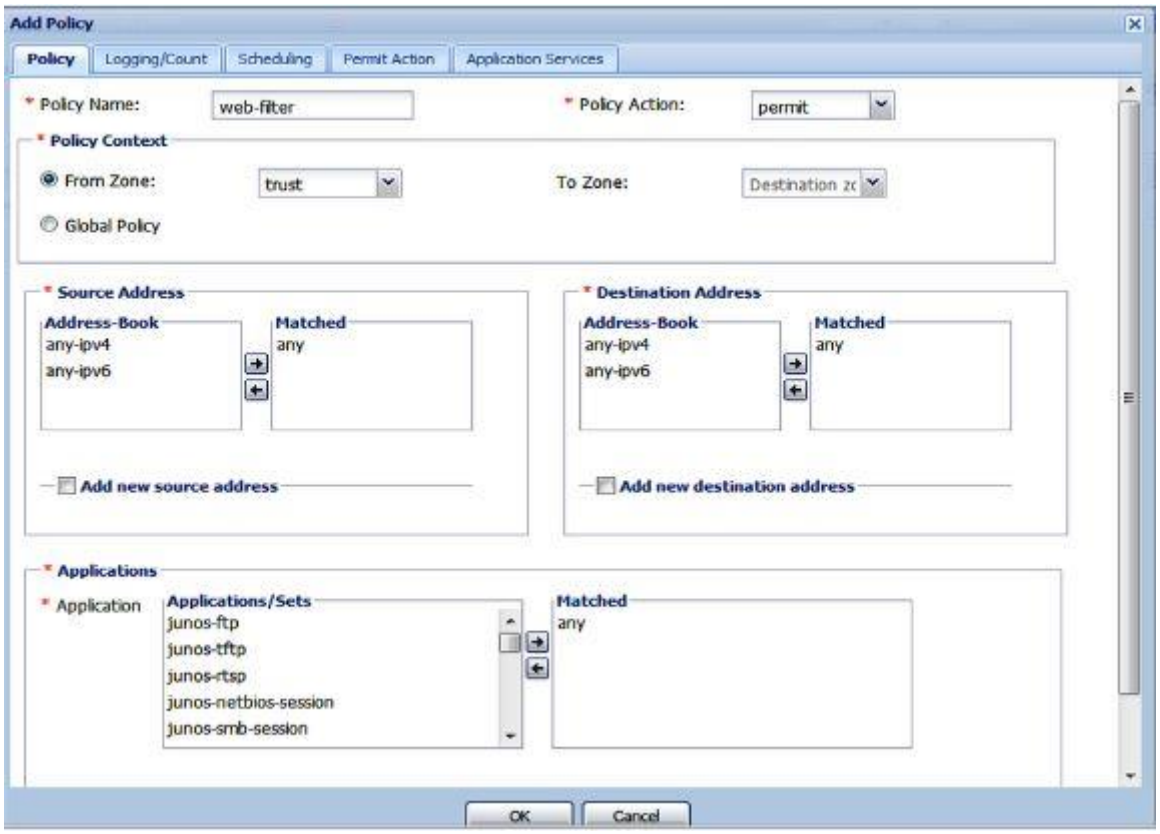


Figure 3.5.7: A Snapshot of Attachment of UTM Policy to Security Policy

viii. On the **Application Services** tab and next to **UTM Policy**, the UTM policy to be attached to the security policy was selected.

ix. Finally a configuration commit was made.

Having filtered these web sites considered to be non-academic and observing the bandwidth usage over some time, it was found out that about 25% of the network bandwidth was saved. This also resulted into a better browsing experience by the users.

3.6 Traffic Shaping Technique

Traffic shaping which is also known as Packet Shaping is simply the practice of regulating network data transfer to assure a certain level of performance or quality of service (QoS) (Margaret, 2013). In other words, traffic shaping, or traffic management, controls the bandwidth available and sets the priority of traffic processed by the policy to control the volume of traffic for a specific period (bandwidth throttling) or controls the rate at which

traffic is sent. Traffic shaping attempts to normalize traffic peaks. However, there are thresholds that need to be maintained, these include the amount of data which can be buffered and the length of time which this can occur. Once these thresholds have been surpassed, frames and packets will be dropped, and sessions will be affected in other ways (Fortinet, 2011).

This section will explain the procedure used in applying traffic shaping on the access layer switches.

3.6.1 Application of Traffic Shaping Technique on Access Layer Switches

The analysis of network traffic in section 4.2 has provided an insight on how to apply traffic shaping technique on individual nodes as a means of bandwidth regulation for the IBBUL network. Having identified the nodes with high traffic rate, it is now easier to apply bandwidth limit on these nodes. However, to achieve this, the Command Line Interface (CLI) procedure was employed. The CLI allows the configuration of the access switches to ones specifications. In other words, CLI allows the implementation of bandwidth regulation of any size as long as the thresholds are been maintained.

To apply bandwidth regulation on the switches the following steps were used:

1. Configuration of Firewall Filter
2. Configuration of Policers
3. Specification of Policers in a Firewall Filter Configuration
4. Application of the configured Firewall Filter with a Policer

3.6.1.1 Configuration of Firewall Filter

In order to configure Firewall Filter, the required details, such as type of family for the firewall filter, firewall filter name, match conditionsetc, were implemented.

The following steps were carried out in firewall filter configuration:

i. Configuration of the family address type for the firewall filter

   [edit firewall]

   admin@EX_2200-ADMIN-SW10# set family inet

ii. Specifying the family name to be applied on multiple interfaces and name individual firewall counters specific to each interface.

   [edit firewall family ethernet-switching filter ingress-port-filter]

admin@EX_2200-ADMIN-SW10# set interface-specific

iii. Specifying a term name

[edit firewall family ethernet-switching filter ingress-port-filter]

admin@EX_2200-ADMIN-SW10# set term term-one

iv. Specifying the match conditions to match on packets that contain a specific source-address and source-port for the firewall filter term

[edit firewall family ethernet-switching filter ingress-port-filter term term-one]

admin@EX_2200-ADMIN-SW10# set from source-address any

admin@EX_2200-ADMIN-SW10# set from source-port 80

v. Specifying filter action

[edit firewall family ethernet-switching filter ingress-port-filter term term-one]

admin@EX_2200-ADMIN-SW10# set then discard

admin@EX_2200-ADMIN-SW10# set then count counter-one

admin@EX_2200-ADMIN-SW10# set then forwarding-class expedited forwarding

vi. Committing the configuration

admin@EX_2200-ADMIN-SW10# commit

3.6.1.2 Configuration of Policers

The policer which performs the rate-limit traffic on the switches was configured using the following steps:

i. Specifying the policer`s name

[edit firewall]

admin@EX_2200-ADMIN-SW10# set ibbulpolicerpolicer-one

ii. Configuring rate limit for the policer

a) Specifying the bandwidth limit in bit per second (bps), this is to control the traffic rate on the interfaces

[edit firewall policerpolicer-one]

admin@EX_2200-ADMIN-SW10# set if-exceeding bandwidth-limit 1m

b) Specifying the maximum allowable burst size, this will control the amount of traffic bursting

[edit firewall policerpolicer-one]

admin@EX_2200-ADMIN-SW10# set if-exceeding burst-size-limit 2m

iii. Specifying the policer action to discard packets that exceed the rate limits

[edit firewall policer]

admin@EX_2200-ADMIN-SW10# set policer-one then discard

3.6.1.3 Specification of Policers in a Firewall Filter Configuration

In order to reference a policer, a configuration of the filter term that includes the policer action was carried out.

[edit firewall family ethernet-switching]

admin@EX_2200-ADMIN-SW10# set filter limit-hosts term term-one from source-address any

admin@EX_2200-ADMIN-SW10# set filter limit-hosts term term-one then policerpolicer-one

3.6.1.4 Application of the configured Firewall Filter with a Policer

To apply the firewall filters to filter packets that are entering or exiting the interfaces with a policer the following was carried out:

i. [edit interfaces]

admin@EX_2200-ADMIN-SW10#set ge-0/0/0 unit 0 family inetsource-address any filterinput ingress-router-filter

admin@EX_2200-ADMIN-SW10# set ge-0/1/0 unit 0 family inetsource-address any filter output egress-router-filter

Based on the configurations implemented above, the bandwidth utilization on the access switches was limited to 1Mbps. In order words, each port on the switch is limited to 1Mbps. This implies that users are subjected to 1Mbps and cannot exceed this rate.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Introduction

In this chapter, the data collected from the network were analysed, these were also simulated in a modelled network scenario for improved bandwidth utilizationand the results obtained are presented.

4.2 Results

The results obtained from the analysis carried out are presented in this sub-section. Four major data were monitored and collected from the network which includes: (i) peer-to-peer activities, (ii) traffic events, (iii) web events and (iv) userbehaviouralpattern. Each of these events was viewed from two perspectives, events based on individual nodes and events based on time-of-day as they occurred. The simulation results were also presented based on (i) evaluation of the processing time of the core (ii) evaluation of bandwidth utilization rate with increase in network users (iii) evaluation of downloading and uploading speed among users.

4.2.1 Peer-to-Peer (p2p) Analysis

Since firewalls or packet filter exist both as a software solution and as a hardware appliance and is considered as a network securitysystem that controls the incoming and outgoing network traffic based on an applied rule set(Rouse, 2010), a firewall rule was then set up to indicate a p2p traffic across each monitored node. In order to derive the intensity of p2p activity in each node at any given time of the day, these p2p events were monitored. In the results obtained, nodes with prominent p2p activities were identified and the corresponding time of the day in which they were more pronounced.

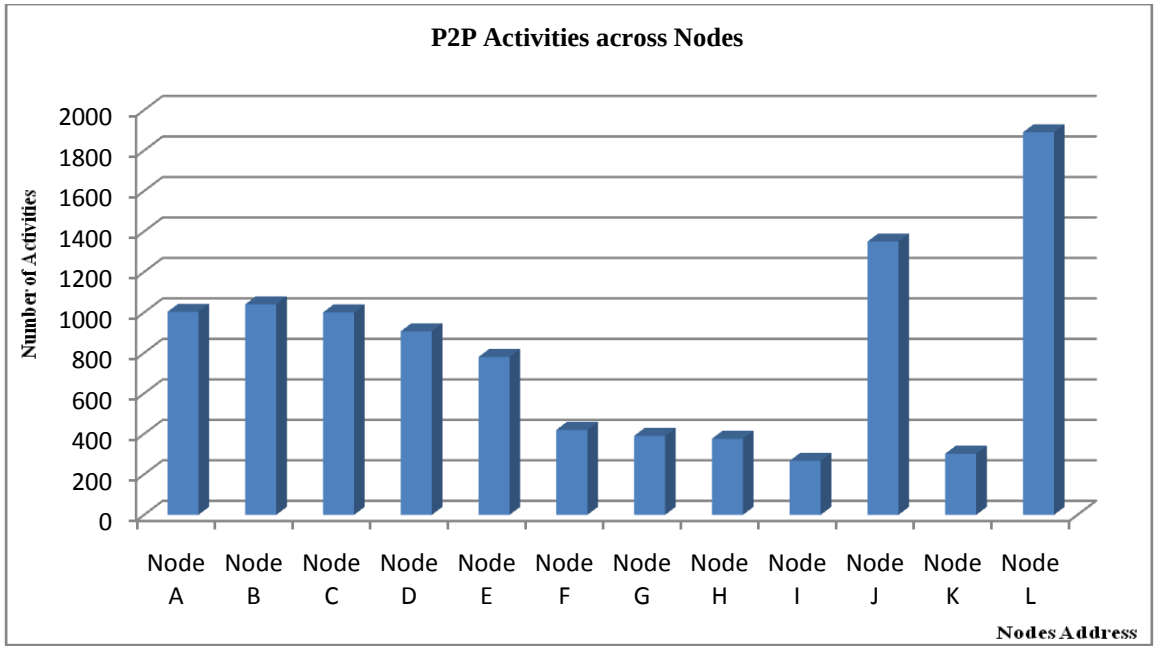


Figure 4.1: The Distribution of p2p Activities across the Selected Nodes

Figure 4.1 shows the average number of p2p activities at the selected node in the network. The horizontal axis indicates the nodes while the vertical axis indicates the number of p2p activities. The p2p activities are most pronounced at node J and node L. This is because node J provides hotspot services to the users while node L is the hostel hotspot. In other words, node J usually has significant number of users connected to it. Node Iis located in the Mathematics department and records the lowest p2p activities. Since p2p activities usually consumes significant amount of bandwidth, it is therefore paramount to understand the p2p activities of the network users. This analysis therefore gives an insight on how to manage the bandwidth with respect to p2p activities.

Figure 4.2 illustrates the trend in p2p activities of users on a time-of-day bases.

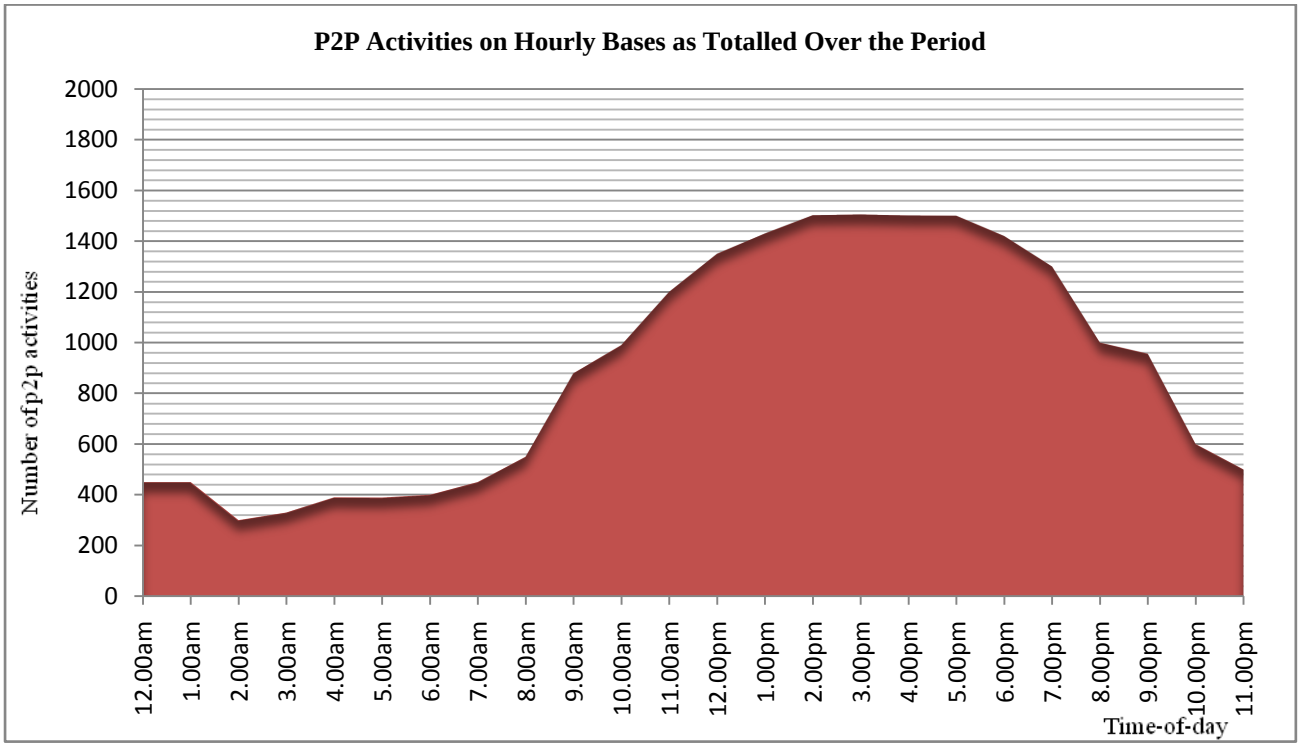


Figure 4.2: P2P Activities on Hourly Bases of the Day

The p2p activities are at the lowest from 1am -6am daily. The activities gradually pick up and reach the highest at about 12pm-6pm. P2P applications run 24 hours in the background, constantly downloading content and are left unattended for days at a time(Brat, 2010). It is to this end that it has become important to understand the time-of-day p2p activities of the users in order to factor this constant bandwidth consumption rate into the bandwidth management policy.

Table 4.1 also shows the list of the active devices (Nodes) involved.

Table 4.1: The Selected Nodes for Monitoring

S/N	ACTIVE DEVICE	NODE
1	ICT CENTER SWITCH 4	Node A
2	ICT CENTER SWITCH 2	Node B
3	ICT CENTER SWITCH 3	Node C
4	ICT CENTER SWITCH 1	Node D
5	ADMIN SWITCH	Node E
6	LIBRARY SWITCH	Node F
7	DEANAGE FAC. OF NATURAL SCI.	Node G
8	FAC. OF AGRIC	Node H
9	MATHS/COMP. DEPT	Node I
10	BIOLOGICAL SCIENCES	Node J
11	PHYSICS DEPT	Node K
12	HOSTEL SWITCH	Node L

4.2.2 Traffic Analysis

With the Junos Pulse Access Control monitoring software, the traffic utilization statistics of all user sessions were logged throughout the period been monitored (See Appendix A). This statistics enabled the calculation of the amount of total bandwidth (upload and download) that was consumed. The total traffic usage at each monitored node was also calculated. More so, at various time-of-days the overall traffic distribution across the entire network was determined.

Figure 4.3 illustrate graphically the total traffic (in megabytes) of users by time of day.

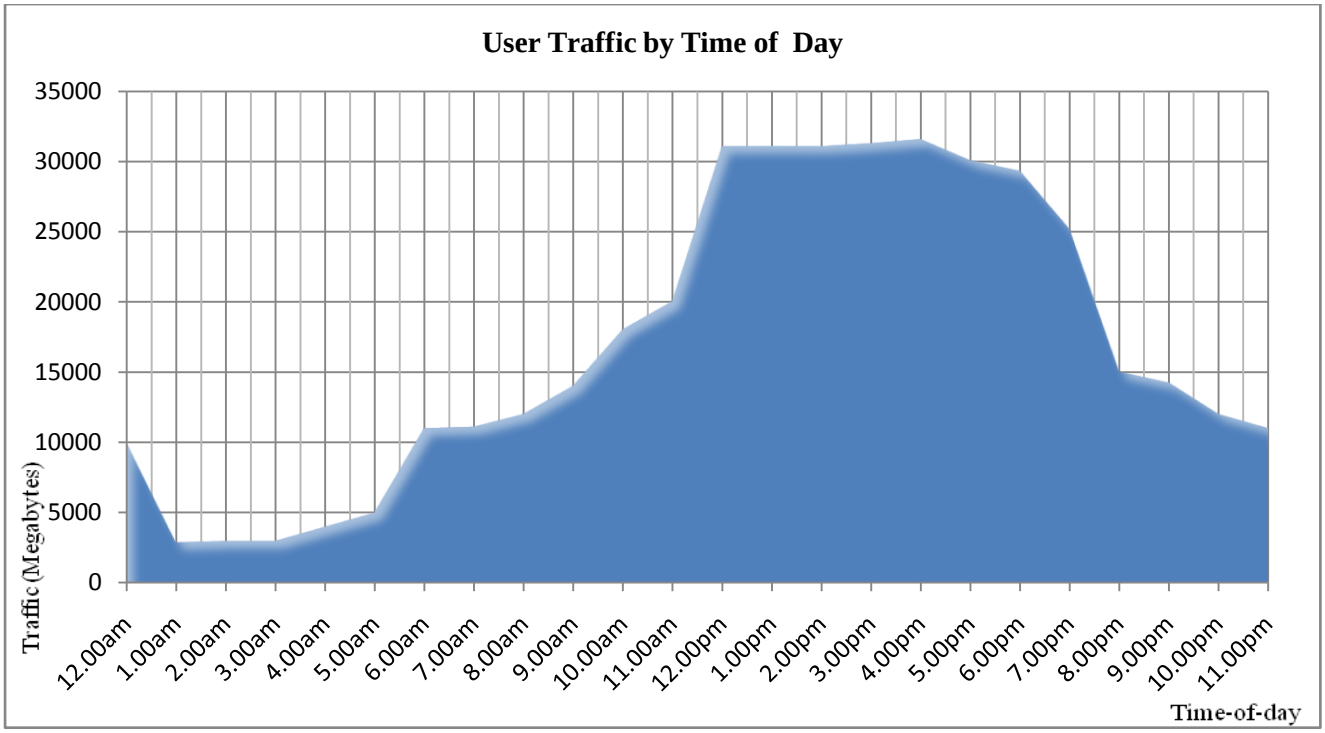


Figure 4.3: Total User Traffic (In Megabytes) by Time of Day.

The number of traffic on the vertical axis is plotted against the time of day (hourly) on the horizontal axis. The traffic was found to be at the lowest within the period of 1am-6am. While the traffic start to pick up between the period of 10am-5pm daily. Knowing the rate at which traffics traverse the network at time-of-day gives an idea on how to properly manage the available bandwidth on daily bases. More so, understanding the traffic rate in the network easily helped in the implementation of the required bandwidth management strategy and policies.

Figure 4.4 is a representation of the number of traffic across individual node.

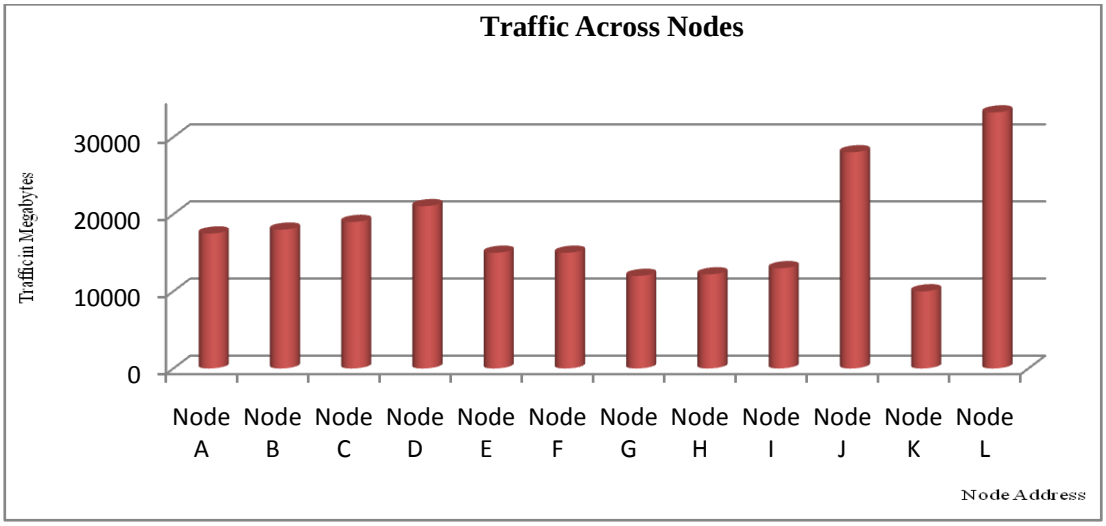


Figure 4.4: User Traffic (In Megabytes) across Individual Node.

The Vertical axis shows the amount of traffic (in megabytes) against the nodes at the horizontal axis. Nodes J and L (Biological Sciences switch and Hostel Switch) carry the most traffic. This can be associated with the fact that these switches provides hotspots to network users which in turn provides more connectivity and hence the volume of traffic. Node K and G (Physics and Deanage Faculty of Natural Sciences switches) have the lowest amount of traffic traversing them. This is because access to the network using these switches is basically through cable and limited numbers of these are available.

It is obvious that users connect to the network through the access layers (nodes); therefore, analyzing these nodes in order to understand the traffic rate across them is important. This is because a view of the traffic per node enables the implementation of bandwidth regulation using the traffic shaping technique. This is also implies that a bandwidth regulation can be implemented on a per node bases.

During the monitoring period, 5483 separate user sessions were noticed. A session for a specific user begins when a network user uses his/her username and password to sign into the campus network; it also ends at a time when that same user signs out intentionally. The user can sign out intentionally by simply following a log out or sign out link, or unintentionally by a hard disconnection from the network. A hard disconnection is when a user leaves a coverage area of a hotspot or unplugs its cable and this usually prompts or triggers a session timeout event. During any session initialization, details on the user are collected and uploaded to a central database server for a specific period of time. These details include: username, user IP address, MAC address, the network node at which the user is connected through, and the timestamp (at session initialization). Usually a session termination message is sent to a log file when a user ends its session. This message contains the duration of the session, the timestamp (at session termination), and the traffic statistics of that user session.

4.2.3 User Behavioural Pattern

In order to justify the amount of traffic that traverse through the network at the various nodes, it became necessary to analyze the user sessions in the network (the behavioural pattern). Figure 4.5 is a simple representation of the number of active user session with respect to the nodes.

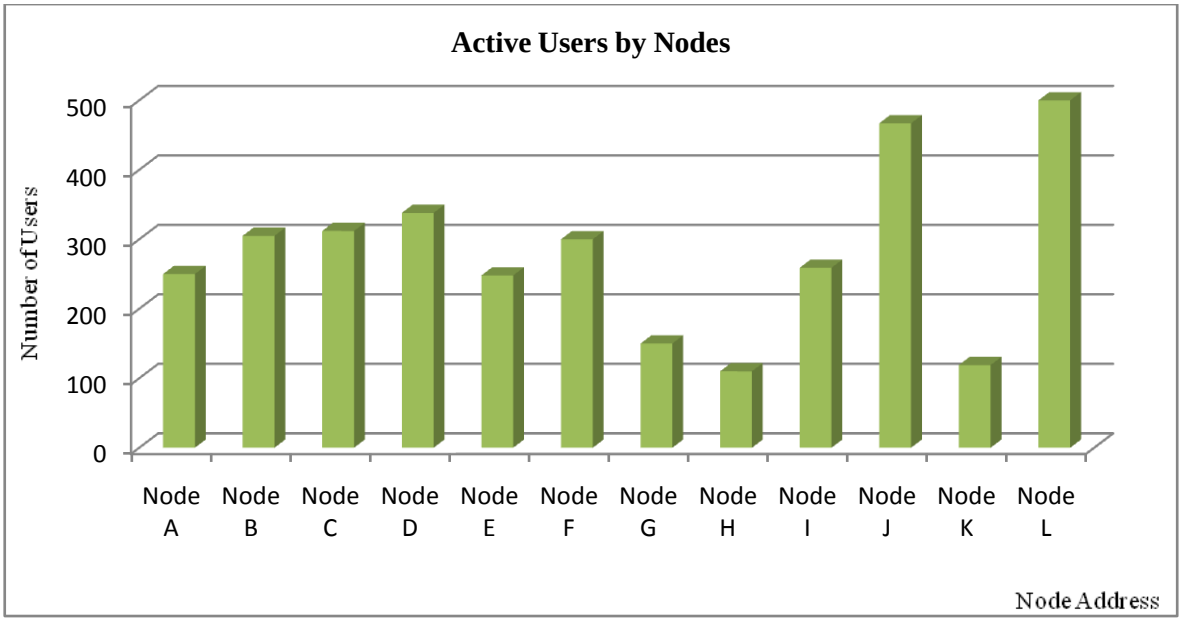


Figure 4.5: User Session by Node.

The vertical axis is the number of users and is plotted against the horizontal axis which represents the nodes. Node L (Hostel Switch) records the highest user session while node H (Faculty of Agriculture) records the lowest user session.

Figure 4.6 is a simple graphical representation of the average hourly peak load of users in the network. It shows the behavioural pattern of the users on a daily bases.

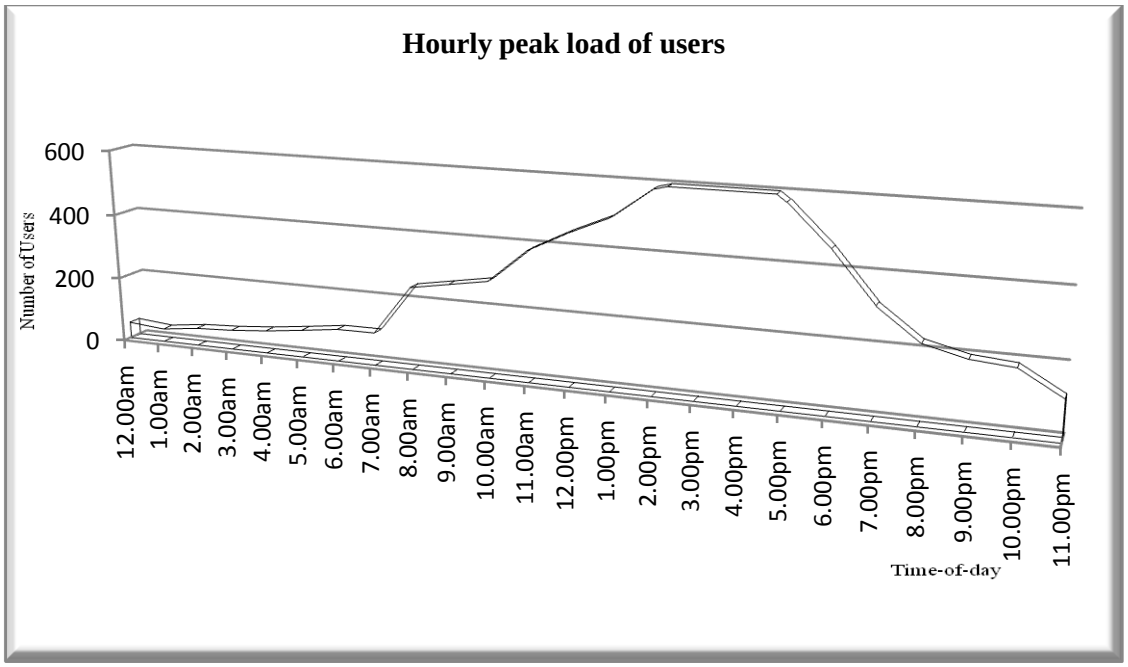


Figure 4.6: Average Hourly Peak Load of Users.

The vertical axis (number of users) is plotted against the horizontal axis (time of day).

The load is at its peak at about 10am-4pm while at its lowest at about 12am-5am daily. Understanding the user behavioural pattern is important as this affects the amount of traffic in

a network which also helps to shape the implementation of bandwidth regulation in the network.

Table 4.2 shows the average count of user sessions by their nodes and time-of-day.

Table 4.2: Count of User Session by Nodes and Hour of Day

Time/ Node	10.10. 10.28	10.10 .10.6	10.10 .10.7	10.10 .10.5	10.10. 10.10	10.10. 10.12	10.10. 10.17	10.10. 10.18	10.10. 10.19	10.10. 10.21	10.10. 10.23	10.10. 10.27	To tal s
12am	11	12	10	15	2	25	45	18	20	50	14	104	32 6
1am	9	8	15	4	2	15	20	12	21	61	40	78	28 5
2am	7	5	9	5	3	10	20	10	13	57	43	64	24 6
3am	5	4	9	1	-	8	11	6	12	36	25	40	15 7
4am	-	-	2	-	-	5	8	5	7	-	-	50	77
5am	-	-	-	-	-	7	3	1	5	-	-	70	86
6am	-	-	-	-	-	2	6	1	6	4	1	73	93
7am	-	12	-	-	-	8	9	1	3	12	2	40	87
8am	9	6	4	7	3	2	4	2	1	8	5	15	66
9am	5	3	4	5	1	3	7	4	2	4	7	13	58
10am	7	9	10	12	12	11	13	7	1	2	5	20	10 9
11am	9	8	11	15	10	8	12	9	6	3	10	27	12 3
12pm	12	6	15	17	16	13	14	11	9	8	13	20	15 4
1pm	16	11	20	17	15	9	18	10	8	11	18	35	18 8
2pm	20	18	21	19	22	13	11	14	10	9	20	41	21 8
3pm	22	17	23	16	17	9	7	16	12	14	11	48	21 2
4pm	18	15	26	19	18	14	9	23	17	15	19	56	24 9
5pm	23	22	18	28	10	18	13	21	24	19	28	59	28 3
6pm	26	20	21	30	19	24	17	19	29	31	32	65	33 3
7pm	25	22	20	28	26	21	29	22	18	28	25	81	34 5

8pm	27	24	29	21	31	37	19	20	17	35	28	96	385
9pm	33	36	32	39	42	48	27	22	23	27	21	107	457
10pm	35	32	31	37	40	41	39	27	28	36	28	127	501
11pm	25	30	28	32	38	31	29	27	20	31	21	133	445
Totals	335	320	338	367	327	382	390	308	312	487	416	1 462	5483

The number of user session per node per hour was counted and the total calculated. A total average of 5483 count was calculated. This user behavioural pattern as shown in Table 4.2 is with respect to the nodes the users are connected as well as the time-of-day. This table reveals the node with the highest number of users and the time-of-day which it usually occurs. This in turn helps to shape the decision to be taken on bandwidth regulation.

4.2.4 Web Analysis

During the monitoring period, the Unified Resource Locator (URLs) visited by users on the network were also tracked. These URLs were analyzed and the popular online utilities on campus and domains were revealed.

Table 4.3 shows among the network users, a list of some of the most popular or visited utilities.

Table 4.3: Most Popular Sites Visited by Users on the Network

S/N	Most Popular:	Utility
1	Mail servers	Yahoo Mail, and Gmail
2	News site	Naijapals,
3	Search engine	Google, Yahoo
4	Social Network Site	Facebook, Twitter
5	Educational	Wikipidia
6	Peer-to-peer sites	Bit Torrent, KazaA
7	Streaming Site	YouTube

Figure 4.7 is a simple illustration of the most important domain hits.

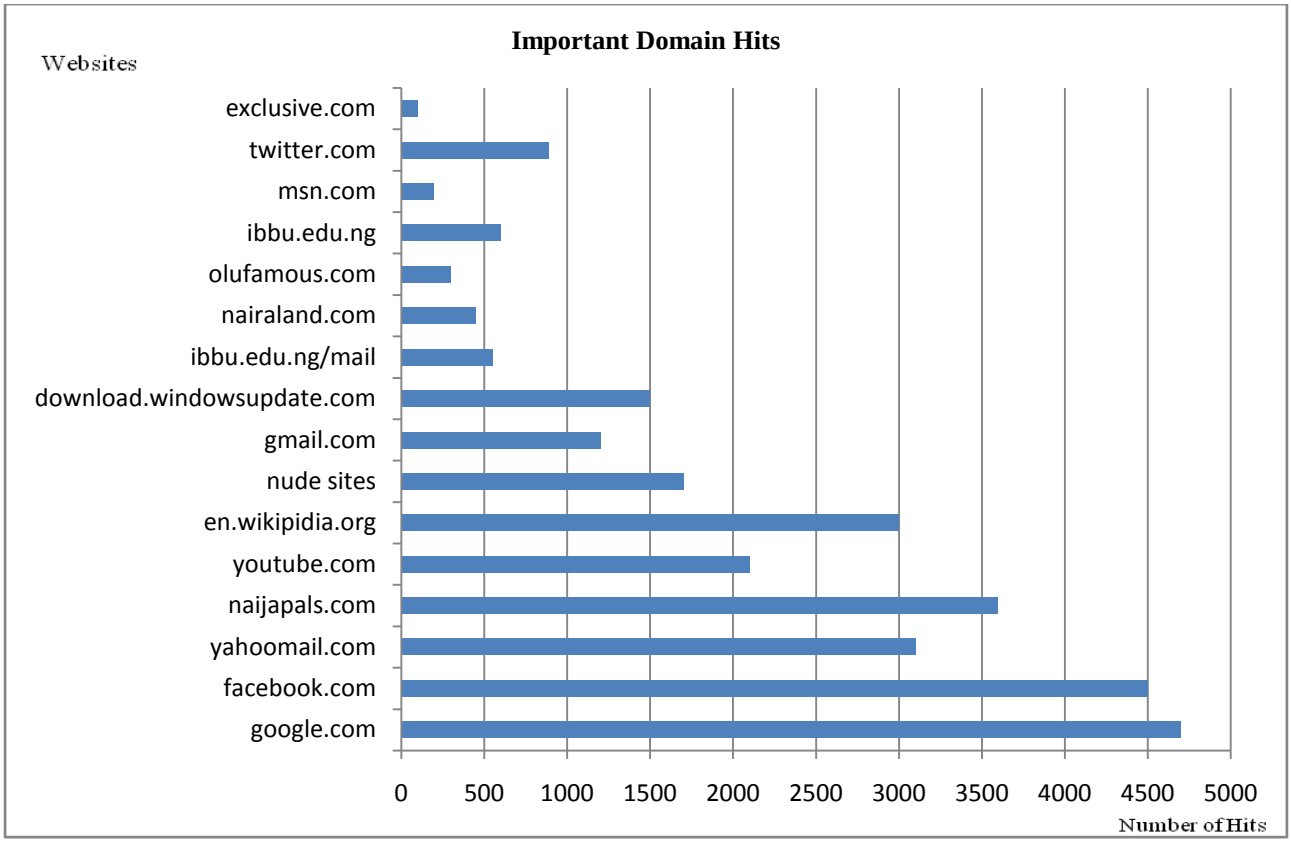


Figure 4.7: Important Domain Hits by Users on the Network

The vertical axis represents the sites visited by the users while the horizontal axis represents the number of hits. The domain hit is also shown in Appendix C. The most frequent among them is google.com. The understanding of the most frequently hit website is necessary in web analysis because it enable a proper web filtering. In other words, knowing the frequently visited websites enables the classification of these sites for web filtering which is an important tool for bandwidth management.

4.2.5 Bandwidth Utilization Rate across Nodes

An evaluation of the upload to download ratio of traffic revealed an estimate of the bandwidth utilization of the users on the network. This data is useful because it gives an insight on the bandwidth utilization patterns in the activities of the users. This is also important as it is an evident for Internet bandwidth expansion in the future. Table 4.4 is a summary of the average bandwidth utilization rate. As shown in Table 4.4, an average user session duration is about 66.09 Minutes and this gives an insight into the behavioral usage pattern of the network users. The download/upload activities of the users is represented in Figure 4.8 and also summarized in Table 4.4. Meanwhile, from Figure 4.7, we observe a keen

interest in Wikipidia.org and YouTube.com, which can be classify as a rich educational sources. As shown in Table 4.4, it is evident that the users will hardly have a very smooth browsing experience going by the average rate of download and by comparing user distribution over nodes and over time. In addition, from Figure 4.7, the average hits on the University domain (ibbu.edu.ng) fluctuates as it is most visited at the beginning of a new session. It can be seen in Figure 4.7 that Yahoomail.com is most frequent for mail services and preferred to the institutional mail service and Gmail.com. Social networking on Facebook is also a very prominent activity on the campus network. Unexpectedly, however, visits to research oriented domains are unremarkable.

Figure 4.8 is a graphical presentation of the average bandwidth utilization across the selected nodes.

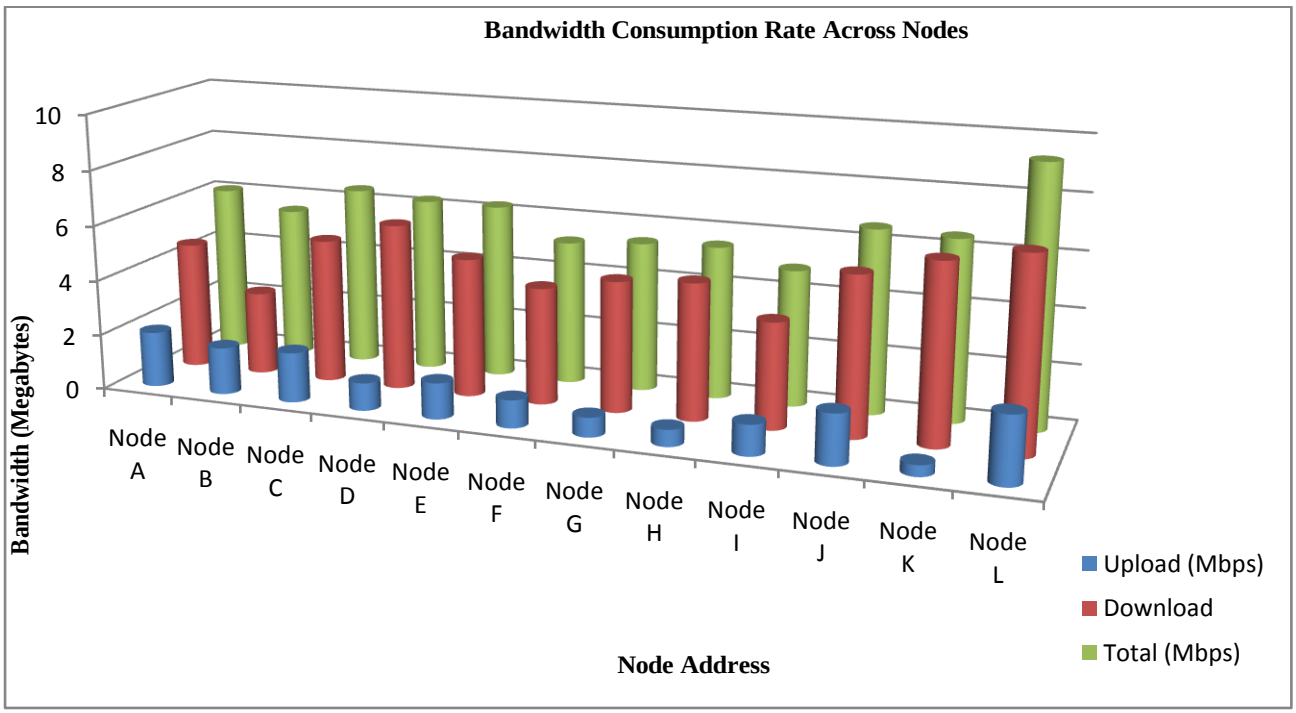


Figure 4.8: Bandwidth Utilization Distribution across the Nodes

As shown in figure 4.8, node L utilizes more bandwidth as compared to other nodes. The bandwidth consumption rate across these nodes gives an insight on how to implement the bandwidth regulation on the nodes. Using the traffic shaping technique, different bandwidth regulation or resizing can be implemented on individual nodes which could depend on the level of importance.

Table 4.4 shows a summary of the average traffic statistics during the monitored period.

Table 4.4: Summary of traffic statistics

No. of Distinct Sessions	Total Average Download Traffic (KB)	Total Average Upload Traffic (KB)	Average Rate of Download (KB/s)	Average Rate of Upload (KB/s)	Average Session Duration (Minutes)
6 723	467 346 727.932	189 762.425	9.67	4.97	66.09

As shown in table 4.4, the average duration of users on the network is about 66.09 minutes. With the average rate of download been recorded, it is evident that the browsing experience of the users are hardly smooth. This also implies that without bandwidth management on the network, users will not have fair access to this scarce resource (bandwidth).

Figure 4.9 also shows the bandwidth utilization at port ge-0/0/0 of the network firewall at the datacenter.

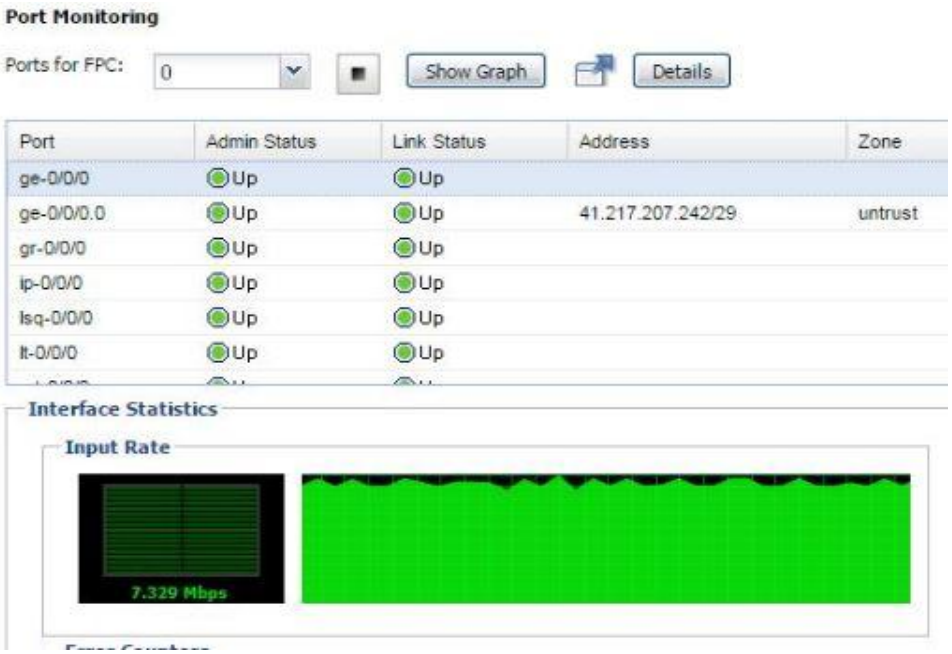


Figure 4.9: Total Bandwidth Utilization on Port ge-0/0/0 of the Firewall

Figure 4.9 shows the bandwidth utilization monitoring interface. It reveals a constant maximum utilization of the bandwidth by the network users. This requires constant bandwidth utilization monitoring for adequate bandwidth management. With bandwidth management in place, more users with better browsing experience shall be expected.

4.2.6 Relationship between Number of User, P2P Intensity and Overall Traffic

It is evident from the results obtained and shown in Figure 4.1 and Figure 4.2;the p2p activities are more prominent in two nodes: node J (Biological Science Switch) and L (Hostel Switch). From Figures 4.4 and 4.5, node D, J and L also experience high traffic. Finally, the nodes with the highest users are J and L. The relationship between the number of users andp2p activity shows that the contributing factor to traffic statistics is the concurrent number of users on the network. It is also evident that the node with the highest number of users also records the highest number of p2p activities. The node with few numbers of users records the least traffic. Meanwhile, two main factors have been observed to influence traffic flow on the network and therefore affect user bandwidth availability. These include: the number of active users and the intensity of p2p activity on that node. Intense p2p activity starts around mid-day, peaks between 1pm and 4pm, and continues high until around 6pm. On the other hand, there is a decline in the number of users at midnight (12am), hitting the peak between 11am and 5pm, and then declining fairly steadily until midnight.

4.2.7 Bandwidth Management

Bandwidth management is a general term given to a collection of tools and techniques that an institution can use to allocate bandwidth to its users or reduce the demand on critical segments of the network. More often, bandwidth management may be applied on the Wide Area Network (WAN) segment that connects the institution to the greater Internet. It may be applied on critical internal segments, such as segments connecting the campus residence halls to the rest of the network (Linda, 2012). This section will focus and discuss application of bandwidth management at the WAN segment (access layers) that connects the institution to the greater Internet. This section will also discuss the methods used to manage the bandwidth available to the institution: blocking of unauthorized traffic (web filtering) and traffic shaping (bandwidth regulation).

4.3 Evaluation of the Processing Time of the Core

The evaluation of the processing time of the core was carried out using Packet Inter-Network Groper Test. Two scenario of the test was carried out and the first includes a test when the bandwidth management configuration was implemented at the core of the network. This scenario assigned the responsibility of bandwidth regulation to the network users at the core and the processing time to treat a request was evaluated. The summary of the processing time is shown in Table 4.5.

Table 4.5: Summary of the Round Trip Time (ms) of the Processing Time

Total ICMP (Echo-Request)	**Round Trip Time (ms)**			
	Minimum	**Maximum**	**Average**	
2420	2.000	2037.172	9.950	

From Table 4.5, the total Internet Control Message Protocol (ICMP) sequence is the total echo request messages sent by the user to the core for processing. The Round Trip Time (RTT) also called Round-Trip Delay is measured in milliseconds, and it is the time required for an echo request message to travel from a specific source (host) to a specific destination (core) and back again. The minimum RTT is the lowest RTT recorded in the total number of echo messages sent. While the maximum RTT is the highest RTT recorded in the total number of echo messages sent. The average RTT is the average RTT calculated in the total messages sent. From Table 5.1, it implies that a total number of 2420 echo request messages were sent to the core and 2ms was recorded as the minimum RTT while 2037.172ms was recorded as the maximum RTT. An average RTT of 9.950ms was also recorded. These values were obtained and calculated by the ping test software.

A portion of the summarized processing time in Table 4.5 was plotted and this is presented in Figure 5.0

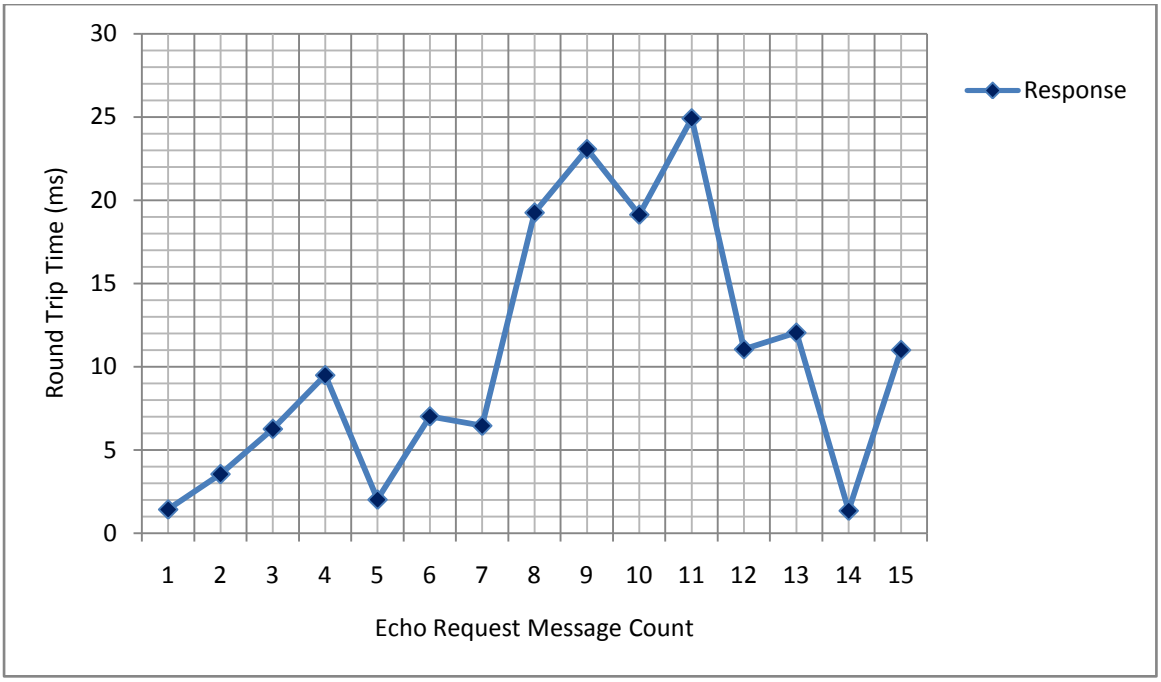


Figure 5.0: Processing Time When Bandwidth Management is applied at the Core

Figure 5.0 shows a graphical presentation of the response time of the core. Although low response times were noticeable, (1.425ms and 1.350ms at echo request 1 and 14 respectively), more of high response time were recorded (24.905ms, 23.058ms, 19.245ms and 19.124ms at echo request 11, 9, 8 and 10 respectively). While the processing time fluctuates in Figure 5.0, a high average processing time was recorded. This is because the core was also tasked with bandwidth regulation as well as other traffic processing.

The second scenario involves a test when the bandwidth management configuration was implemented at the access layer of the network. The summary of the processing time is shown in Table 4.6.

Table 4.6: Summary of the Round Trip Time (ms) of the Processing Time

Total ICMP (Echo-Request)	**Round Trip Time (ms)**		
	Minimum	**Maximum**	**Average**
2524	1.403	182.000	6.000

From Table 4.6, a total of 2524 echo request messages were sent, the minimum and maximum RTT recorded were 1.403ms and 182ms respectively. The average RTT recorded

was 6ms. This implies that the average RTT representing the processing time of the core is lower when bandwidth management was implemented at the access layer levels.

A portion of the summarized processing time in Table 4.6 was plotted and this is presented in Figure 5.1.

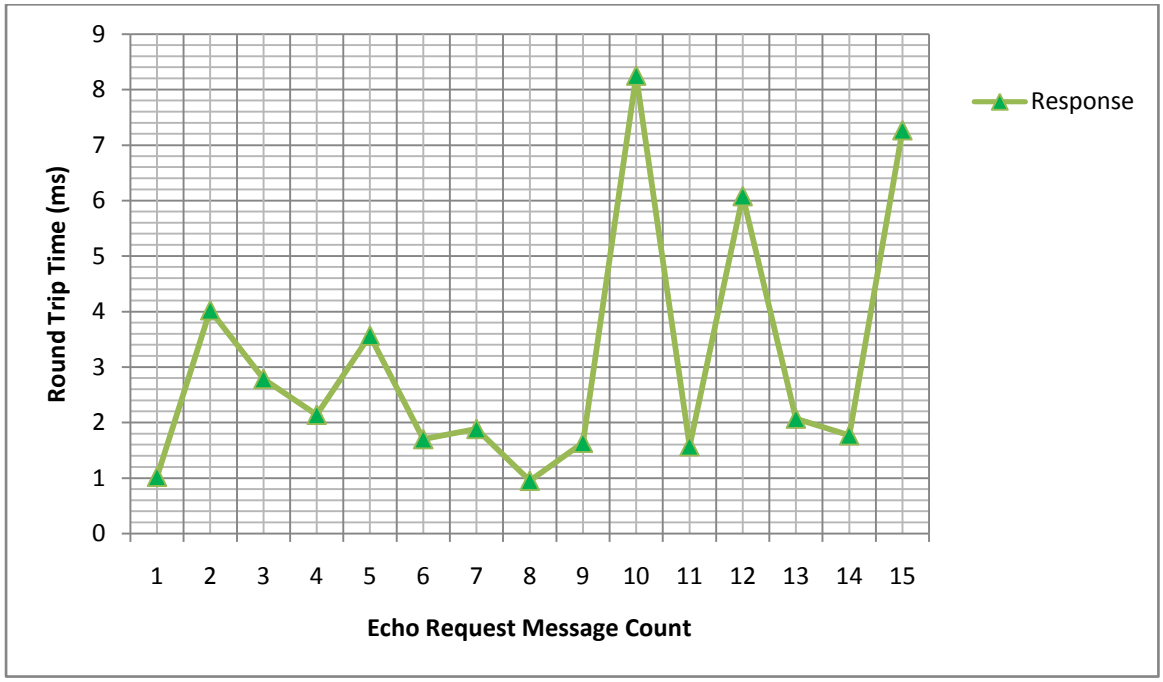


Figure 5.1: Processing Time when Bandwidth Management is applied at the access layer

A graphical presentation of the processing time of the core when bandwidth was applied at the access layer is shown in Figure 5.1. Less process time is recorded throughout on the graph. The highest recorded time (8.254ms at echo request 10) is less than the highest time recorded (24.905ms at echo request 11) in Figure 5.0. This implies that, with the implementation of bandwidth management at the access layers, the core processes data at a faster rate.

From Table 4.5 and Table 4.6, the average times taken by the core to process a request from a user are 9.950ms and 6.000ms respectively. It is therefore observed that it take the core a longer duration to process the request of a user on the network when the same core is responsible for bandwidth management but lesser time for the core to process request from users when the bandwidth management responsibility is transferred to the access layer switches. An approximate 40% improvement in the processing time is recorded as shown in Equation 4.1.

T_{imp}= [{$t_{avg(Bc)}$ – $t_{avg(Ba)}$}]/$t_{avg(Bc)}$ X 100 (4.1)

= [{9.950 – 6.000}] / 9.950 X 100

= 40%

Where:

$T_{imp}$is the percentage improvement in processing time;

$t_{avg(Bc)}$is the processing time of the core when bandwidth management is applied at core;

$t_{avg(Ba)}$is the processing time of the core when bandwidth management is applied at the access layer switches.

4.4 Evaluation of Bandwidth Utilization Rate with Increase in Network Users

The rate of bandwidth utilization when traffic shaping was not implemented in the simulated network is shown in Figure 5.2.

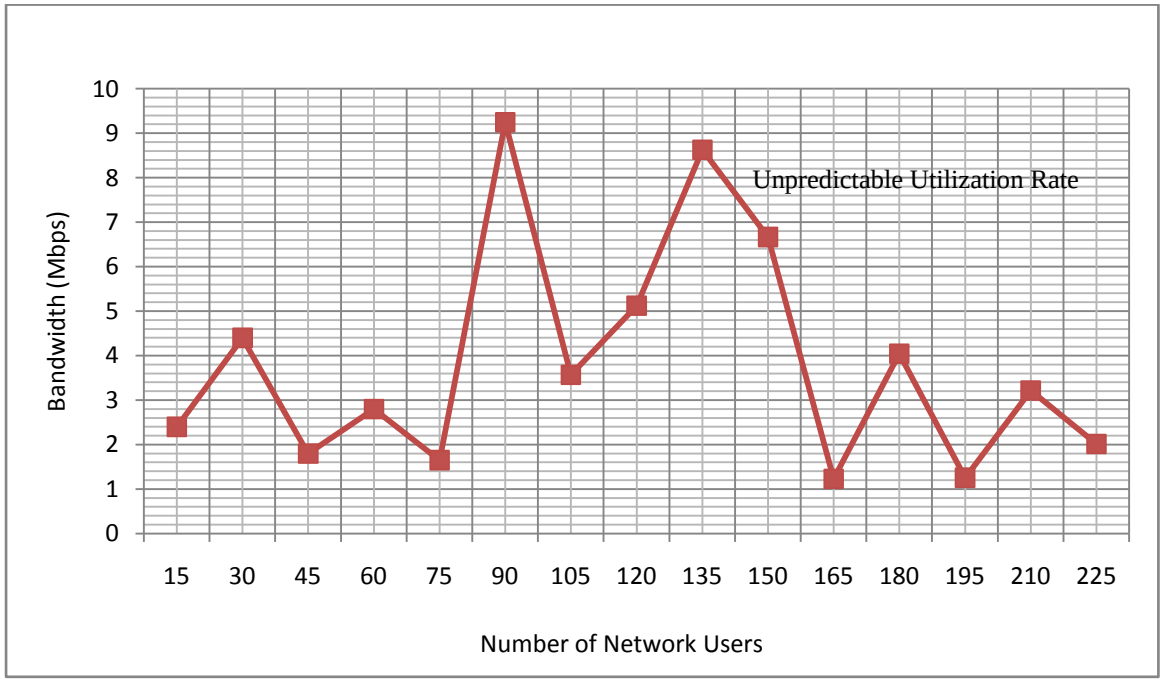


Figure 5.2: Bandwidth Consumption Pattern without Regulation

From Figure 5.2, the bandwidth utilization follows an unpredictable pattern. This is because: (i) there was no implementation of bandwidth management. Bandwidth management was neither implemented at the core or at the access layers. (ii) the capability of user devices differ. As a result of this, the bandwidth is frequently congested. It is observed that the

bandwidth utilization rose to 9.246Mbps and 8.630Mbps at 90 and 135 network users respectively, this can be attributed to the capacity of the devices. A single network user with high capable device can pull large amount of the bandwidth while leaving the rest of the network users with low capacity devices to utilize little bandwidth.

4.5 Evaluation of Downloading and Uploading Speed among Users

The download andupload speed recorded among users as simulated is presented in Table 4.7.

Table 4.7: Summary of Downloading and Uploading Speed

No. of Network Users	Total Average Download (KB)	Total Average Upload (KB)	Average Rate of Download (KBps)	Average Rate of Upload (KBps)
35	167 135 516.811	72 621.316	213.43	115.04

Table 4.7 shows the simulated results obtained as the download and upload speeds of the users. The total average download represents the amount of data downloaded by users over specific period of time and the total average upload represent the amount of data uploaded by users. The average downloads and uploads rates shows the average speeds the users used in downloading and uploading data. 213.43KBps and 115.04KBps were recorded as the downloading and uploading speeds of the users respectively.

4.6 Evaluation of the Network Traffic per Node

The result of the network traffic per node of the simulation is presented in Figure 5.3

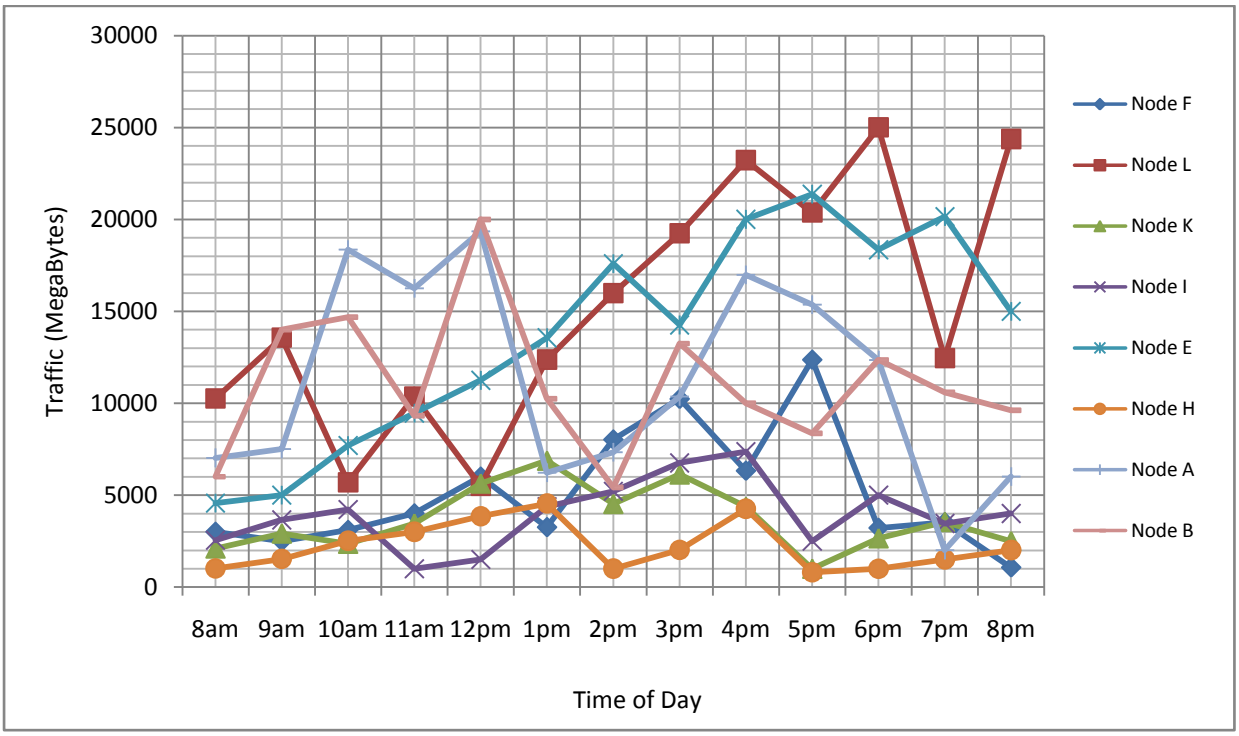


Figure 5.3: Network Traffic per Node

Figure 5.3 shows the occurrence of traffic at time of day per individual access layer. While traffic are generated by the hosts attached to the access layers, the simulated network shows that the hostel access layer switch generated the most traffic which reached its peak of 25GB at about 6pm while Faculty of Agriculture generated the least traffic with a traffic peak of 4.5GB at about 1pm and 4pm.

4.7 Validation

Validation of the proposed technique (bandwidth regulation using traffic shaping technique at the access layer) was carried out and comparisons were made. Comparisons were made in terms of: (i) processing time of the core. The processing time of the core when bandwidth regulation was implemented at the core was compared with the processing time of the core when bandwidth regulation was implemented at the access layers. (ii) the downloading and uploading speeds of users. The monitored download and upload speeds of the network users were compared with the simulated download and upload speeds of the users.

The comparison of the processing time of the core when bandwidth limit was applied at the core and when it was applied at the access layers is presented in Figure 5.4.

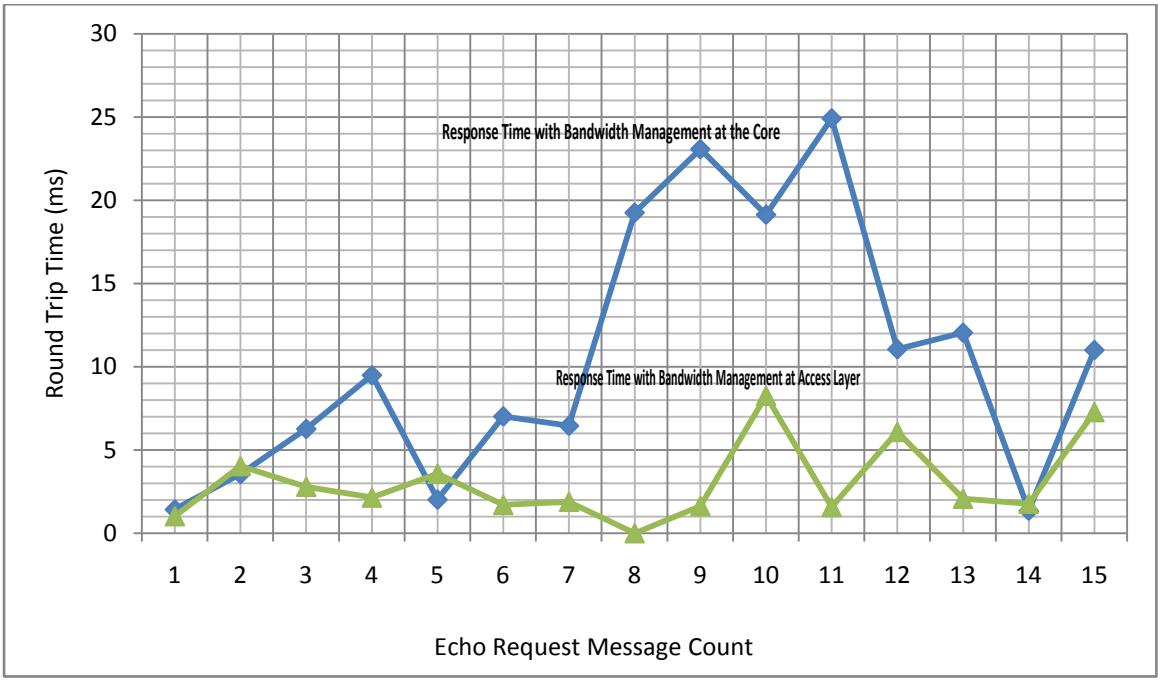


Figure 5.4: Processing Time of the core at Different situations

From Figure 5.4, it can be observed that the processing time recorded when bandwidth was applied at the access layer levels were less as compared to the time recorded when the same was applied at the core. The trend in the time recorded for the access layer bandwidth implementation is less (with the highest time record at 8.254ms at 10 echo request message) as compared to the trend of time recorded for bandwidth implementation at the core. The highest time occurred at 24.905ms at 11 echo request message. About 40% improvement in the processing time of the core was recorded.

Table 4.8 compares the download and upload statistics obtained during the monitored period of IBBUL campus network and the simulated statistic of the same network.

Table 4.8: Comparison of Downloading and Uploading Statistic

	Total Average Download (KB)	Total Average Upload (KB)	Average Rate of Download (KB/s)	Average Rate of Upload (KB/s)
Monitored	467 346 727.932	189 762.425	9.67	4.97
Simulated	167 135 516.811	72 621.316	213.43	115.04

The average downloads and uploads speeds of the users when simulated (bandwidth management applied at the access layers) shows improvement in the browsing experience of the network users. Comparing the monitored statistics (in terms of average download and upload speeds) and the simulated statisticof the users, about 95% of improvement in the download speed was recorded and about 96% improvement in the upload speed was recorded as shown in equations 4.2 and 4.3 respectively.

$$D_{imp} = [\{d_{avg(S)} - d_{avg(M)}\}]/t_{avg(S)} \text{ X } 100 \quad (4.2)$$

$$= [\{213.43 - 9.67\}] /213.43 \text{ X } 100$$

$$= 95\%$$

$$U_{imp} = [\{u_{avg(S)} - u_{avg(M)}\}]/u_{avg(S)} \text{ X } 100 \quad (4.3)$$

$$= [\{115.04 - 4.97\}] / 115.04 \text{ X } 100$$

$$= 96\%$$

Where:

$D_{imp}$is the percentage improvement in download speed;

$d_{avg(S)}$is the simulated average download speed;

$d_{avg(M)}$is the monitored average download speed.

$U_{imp}$is the percentage improvement in upload speed;

$u_{avg(S)}$is the simulated average upload speed;

$u_{avg(M)}$is the monitored average upload speed.

In order to capture the download and upload speeds statistics in the simulation, resources were retrieved from the system to represent download while resources were sent to the system to represent upload.

4.8 Life Network Scenario of Bandwidth Management Implementation

The implementation of bandwidth management using traffic shaping technique was carried out on a segment of the IBBUL network. This was carried out during the period that traffic was at its peak (7pm to 12am). Traffic was diverted to the test access layer switch; this enabled high traffic to travers through this test switch.

4.9 Network Scenario Setup

Figures 5.5 and 5.6 showa snapshot of the network scenario setup.

Figure 5.5: A snapshot of Network Scenario Setup

Figure 5.5 shows the configuration computer, test switch, fibre connection cable, core layer switch and the fibre cabinet. The fibre cabinet link or connect the core layer to the access layer switches at their various locations or departments. However in this test, direct connection is made between the test switch and the core. Using the configuration computer and traffic shaping technique, the bandwidth management was implemented on the test switch.

Figure 5.6: Connections to Switch Snapshot

Figure 5.6 shows a snapshot of all the connections made to the test switch.These connections include: all the wireless access points and hotspots in the ICT Centre, configuration computer and EX4200 core switch.

4.10 Evaluation of the Processing Time of the Life Network Scenario

Based on this test, the processing time of the core was carried out using the ping test. A number of echo request messages were sent and the Round Trip Time (RTT) in milli-seconds was recorded. The result revealed that;

An average RTT of 10.06ms was recorded when bandwidth management was implemented on the access layers as against an average RTT of 12.01ms when bandwidth management was implemented on the core layer. This represents about 16.23% reduction in the processing time of the core layer.

4.11 Proposing an Acceptable Use Policy (AUP) on Bandwidth Utilization for IBBUL Network

Proposing an AUP for a multidisciplinary Institution like IBBUL, care is taken to meet the satisfaction of all quotas. Hence, the following is proposed:

4.11.1 Policy Title: Bandwidth Regulations for IBBUL Network Users

4.11.2 Policy Purpose: This is to ensure that the University's network bandwidth connection continues to effectively meet instructional needs,serve the University's academic mission and also meet the needs of the campus community with fairness among users.

4.11.3 Application: This policy is directed to members of the University community. These include the staff, students and authorized visitors.

4.11.4 Policy Statement: IBBUL Information and Communication Technology Centre is saddled with the responsibility of ensuring that the University's network connections and bandwidth resources are available for use when needed with fairness and are properly managed.Without any policies or prioritizations in place bandwidth hungry applications shown in the report and users with high capacity devices would deplete available bandwidth capacity. When bandwidth is depleted leading to its congestion, users will experience difficulty in accessingacademic content. In order to ensure that the network bandwidth is available for all institutional needs the ICT Centre has put in place a bandwidthmanagement system. This bandwidth management system regulates the network bandwidth and the system can also block spurious non-academic traffic and only allow some traffic at stipulated times.

4.11.5 Bandwidth Tiers: This explains the levels of the bandwidth system put in place.

4.11.5.1First Tier: Blocking of traffic that are considered non-academic traffic and video streaming. This includes non-academic web browsing sites, non-academic video and audio messaging and collaboration, and gambling traffic. Examples of such include: Pornography sites, naijabet.com etc. Sports sites can be access at specified time.

4.11.5.2 Second Tier: This involves the transfers of large files including updates. The downloading and uploading rate of all users has been pegged at 1Mbps maximum.

4.11.5.3 Third Tier: Peer-to-peer activities are also limited to the rate specified and only certified peer-to-peer engines are allowed as any uncertified engines are blocked.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusions

Bandwidth utilization management system has been proposed and implemented at the access layer of a campus network. This was achieved using traffic shaping technique due to its flexibility and simplicity. The data collected after 60 days of monitoring of IBBUL campus network were analysed; this gave insight on how to simulate the modelled IBBUL network. The results obtained revealed the highest and lowest p2p activities of the users across the monitored nodes as well as the time-of-day they occurred. It also revealed the nodes with the highest traffic and the time-of-day it usually occurred. The web analysis revealed the most visited sites by the users. The results obtained shows about 40% noticeable reduction in the processing time of the core layer (an average of 6.00ms as against the average of 9.950ms), increased in the download and upload speeds of about 203.76KB/s and 110.07KB/s respectively. It can therefore be concluded that the implementation of bandwidth regulation at the access layer using traffic shaping technique reduces the processing time of the core layer as well as improves the browsing experience of the network users.

5.3 Recommendations for Further Work

Bust traffic shaping technique is recommended for future work. This could be implemented at the access layers as a means of bandwidth regulation. Bust traffic shaping technique allows more bandwidth usage from pool when network users are few.

REFERENCES

Abdullahi, M. B. (2014).*The Study of The Policy Based Bandwidth Management in The Core Network: A Case Study of ABU Network. Zaria.* Zaria: Department of Electrical and Computer Engineering. Ahmadu Bello University, Zaria, Nigeria.

Andrew, P. (2013). Badnwidth Management for University Campus Network. *Internation Journal for Sciences* , 2-32.

Athicha, M., Benjie, C., & David, M. (2010).*A Low-bandwidth Network File System.* San Diego: Defense Advanced Research Projects Agency (DARPA).

Barry, V. W. (2011).*Bandwidth Management and Monitoring for IP Network Traffic: An Investigation.* Retrieved September 14, 2014, from Academia: http://www.academia.edu/502587/Bandwidth_Management_and_Monitoring_for_IP_Network_Traffic_An_Investigation

Bill, M. (2012).*Bandwidth Management Techniques — Tips and Actions*. Retrieved September 15, 2014, from Techsoup for Libraries: https://www.techsoupforlibraries.org/cookbook-3/networking-and-security/tools/bandwidth-management-techniques-tips-and-actions

Brat, N. (2010).*Managing Peer-To-Peer Traffic With Cisco Service Control Technology.* Retrieved September 11, 2014, from Cisco SCE 1000 Series Service Control Engine: http://www.cisco.com/c/en/us/products/collateral/service-exchange/sce-1000-series-service-control-engine/prod_white_paper0900aecd8023500d.html

Deepika, M., & Rama, M. B. (2014). An approach to Effective Bandwidth Utilization using Software Define Networking . *(IJCSIT) International Journal of Computer Science and Information Technologies,* , 5571-5574.

Dejan, K., Ryan, B., Charles, K., Erik, V., James, W. A., Snoeren, A. C. (2007). *Maintaining High Bandwidth under Dynamic Network Conditions.* New York, USA: Center for Networked Systems.

Devajit, M., Majidu, l. A., & Utpal, J. B. (2013). A Study of Bandwidth Management in Computer Networks. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* , 70-73.

Dualwan. (2010).*Bandwidth Management and Traffic Optimization*. Retrieved June 22, 2014, from dualwan: <http://dualwan.org/bandwidth-management.html>

Fortinet, J. (2011).*Fortgate: Traffic shaping* . Retrieved January 15, 2015, from Forttech: http://docs.fortinet.com/uploaded/files/1049/fortigate-traffic-shaping-40-mr3.pdf

Aloi G., and Pace, P.(2012). A wise cost-effective supplying bandwidth policy for multilayer wireless cognitive networks. *Computers & Operations Research* , 2836–2847.

Hansel, Drew; Boul, Yous. (2011).*MATLAB: The Language of Technical Computing.* Retrieved November 10, 2014, from MathWorks: www.mathworks.com/fisica.unav.es/~angel/matlab/getstart_r12.pdf

Ibrahim, B. B. (2014).*Facts about IBBUL ICT Unit.* Retrieved September 13, 2014, from Ibrahim Badamasi Babangida Univesity, Lapai: http://www.ibbu.edu.ng/ictfacts-pdf.php

Ibrahim, B. B. (2013).*Students` record.* Retrieved September 21, 2014, from Ibrahim Badamasi Babangida Univesity, Lapai: http://www.ibbu.edu.ng/studentrecords-infounit.pdf.php

James, A., Michel, O., Delfin, Y. M., & Zhonghui, Y. (2001). WINTRAC: a TCP window adjustment scheme for bandwidth management. *Performance Evaluation* , 1-44.

Jaw, K. (2003).*OPNET Simulator.* Retrieved November 9, 2014, from OPNET Solution: http://users.salleurl.edu/~zaballos/opnet_interna/pdf/OPNET%20Simulator.pdf

Jeng, F. L., Meng, C. C., Ming, T. K., & Wan, j. L. (2006). Bandwidth allocation algorithms for weighted maximum rate constrained link sharing policy. *Information Processing Letters* , 238–243.

Jim, G. (2013).*Designing WLANs with Simulation*. Retrieved May 6, 2014, from Wi Fi Planet: http://www.wi-fiplanet.com/tutorials/article.php/2246571/Designing-WLANs-with-Simulation.htm

Joel K, Y. (2007).*Mixing Multiple Wireless Technologies*. Retrieved May 1, 2014, from Sensor: http://www.sensorsmag.com/networking-communications/wireless-sensor/mixing-multiple-wireless-technologies-1435

John, S., Okonigene, R., Matthews, V., Akinade, B., & Chukwu, I. (2011). Managing and Improving Upon Bandwidth Challenges in Computer Network. *Journal of Emerging Trends in Engineering and Applied Sciences (JETEAS)* , 482-486.

Johnsson, A. (2005).*Bandwidth Measurements in Wired and Wireless Networks.* Vasteras: Department of Computer Science and Electronics, Malardalen University, Sweden.

Kurose, J and Ross, K (2011). Top - Down Approach Featuring the Internet, 3rd Edition. *Journal of Computer Networking, 734 - 736.*

Ke, L. (2014).*Network Simulator 2: Introduction.* Retrieved November 9, 2014, from Simulators: http://www.cs.binghamton.edu/~kliu/cs580t/ns2pre.pdf

Linda, D. (2012). Bandwidth Management Tools, Strategies and Issues. *Educause Constituent Group* , 34-39.

Lockias, C. (2012). Bandwidth management in universities in Zimbabwe: Towards a responsible user base through effective policy implementation. *International Journal of Education and Development using Information and Communication Technology* , 62-76.

Maduka, K. A. (2012).*Bandwidth management: the public policy approach in a university campus network.* Ibadan, Nigeria: DiploFoundation.

Margaret, R. (2013).*Traffic Shaping.* Retrieved January 12, 2015, from Techtarget: http://searchnetworking.techtarget.com/definition/traffic-shaping

McGuigan, B. (2010).*What is bandwidth*. Retrieved June 22, 2014, from WiseGeek: <http://www.wisegeek.com/what-is-bandwidth.htm>

Ravi, P., Constantinos, D., Margaret, M., & kc, c. (2003). Bandwidth Estimation: Metrics, Measurement Techniques, and Tools. *IEEE Network* , pp. 27-35.

Rosenberg, D. (2010). Digital Libraries. *International Network for the Availability of Scientific Publications (INASP)* , 66-71.

Rouse, M. (2010).*Enterprise Firewall Protection.* Retrieved August 20, 2014, from TechTarget: http://searchsecurity.techtarget.com/definition/firewall

Wang, X. G., Geyong, M., John, M., & Khalid, A.-B. (2013). A QOS-BASED BANDWIDTH MANAGEMENT SCHEME IN HETEROGENEOUS WIRELESS NETWORK. *International Journal of Simulation*, 9-17.

Wei, C., & Mostafa, A. B. (2003). Virtual Private Network Bandwidth Management with Traffic Prediction. *Computer Networks* , 765-778.

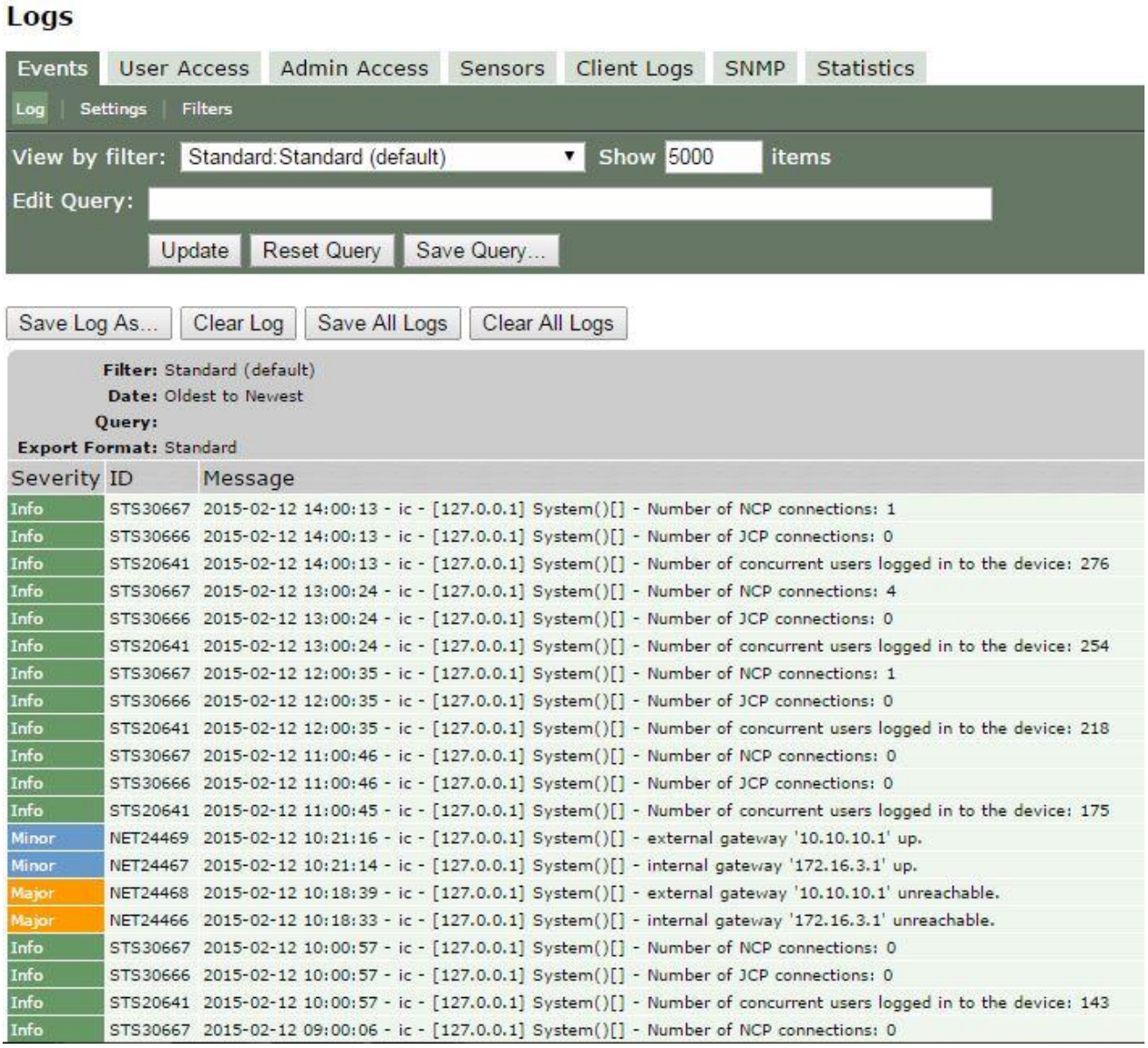
Yingfei, D., & Xiaojiang, L. (2010). Novel dynamic delay allocation adjustment for improving bandwidth efficiency. *Computer Communications* , 463–476.

Yongpei, G., Weilai, Y., Henry, O., & Douglas, M. B. (2008). A pricing approach for bandwidth allocation in differentiated service networks. *Computers & Operations Research* , 3769 – 3786.

Zaghloul, M. (2014). Applying Quality of Service Technique for Bandwidth Mnagement in Jamming Environment System. *IMPACT: International Journal of Research in Engineering and Technology (IMPACT: IJRET)* , 57-62.

Appendix A

A Snap Shot of the Juniper Junos Pulse Access Control Software



Logs

Events | User Access | Admin Access | Sensors | Client Logs | SNMP | Statistics

Log | Settings | Filters

View by filter: Standard:Standard (default) Show 5000 items

Edit Query:

Update | Reset Query | Save Query...

Save Log As... | Clear Log | Save All Logs | Clear All Logs

Filter: Standard (default)
Date: Oldest to Newest
Query:
Export Format: Standard

Severity	ID	Message
Info	STS30667	2015-02-12 14:00:13 - ic - [127.0.0.1] System()[] - Number of NCP connections: 1
Info	STS30666	2015-02-12 14:00:13 - ic - [127.0.0.1] System()[] - Number of JCP connections: 0
Info	STS20641	2015-02-12 14:00:13 - ic - [127.0.0.1] System()[] - Number of concurrent users logged in to the device: 276
Info	STS30667	2015-02-12 13:00:24 - ic - [127.0.0.1] System()[] - Number of NCP connections: 4
Info	STS30666	2015-02-12 13:00:24 - ic - [127.0.0.1] System()[] - Number of JCP connections: 0
Info	STS20641	2015-02-12 13:00:24 - ic - [127.0.0.1] System()[] - Number of concurrent users logged in to the device: 254
Info	STS30667	2015-02-12 12:00:35 - ic - [127.0.0.1] System()[] - Number of NCP connections: 1
Info	STS30666	2015-02-12 12:00:35 - ic - [127.0.0.1] System()[] - Number of JCP connections: 0
Info	STS20641	2015-02-12 12:00:35 - ic - [127.0.0.1] System()[] - Number of concurrent users logged in to the device: 218
Info	STS30667	2015-02-12 11:00:46 - ic - [127.0.0.1] System()[] - Number of NCP connections: 0
Info	STS30666	2015-02-12 11:00:46 - ic - [127.0.0.1] System()[] - Number of JCP connections: 0
Info	STS20641	2015-02-12 11:00:45 - ic - [127.0.0.1] System()[] - Number of concurrent users logged in to the device: 175
Minor	NET24469	2015-02-12 10:21:16 - ic - [127.0.0.1] System()[] - external gateway '10.10.10.1' up.
Minor	NET24467	2015-02-12 10:21:14 - ic - [127.0.0.1] System()[] - internal gateway '172.16.3.1' up.
Major	NET24468	2015-02-12 10:18:39 - ic - [127.0.0.1] System()[] - external gateway '10.10.10.1' unreachable.
Major	NET24466	2015-02-12 10:18:33 - ic - [127.0.0.1] System()[] - internal gateway '172.16.3.1' unreachable.
Info	STS30667	2015-02-12 10:00:57 - ic - [127.0.0.1] System()[] - Number of NCP connections: 0
Info	STS30666	2015-02-12 10:00:57 - ic - [127.0.0.1] System()[] - Number of JCP connections: 0
Info	STS20641	2015-02-12 10:00:57 - ic - [127.0.0.1] System()[] - Number of concurrent users logged in to the device: 143
Info	STS30667	2015-02-12 09:00:06 - ic - [127.0.0.1] System()[] - Number of NCP connections: 0

Appendix B

A Snap Shot of User Session Details

Severity	ID	Message
Info	EAM24805	2015-02-12 20:17:30 - ic - [127.0.0.1] anonymous(IBBU_REALM)[ADMIN, STAFF, CAFE, DEANAGE_FONS, FACULTY HOTSPOT, ICT_CENTER, PHYSICS, LIBRARY, HOSTEL] - RADIUS authentication was resumed for anonymous (realm 'IBBU_REALM') from location-group 'LIBRARY' and attributes are: NAS-IP-Address = 172.22.12.2,NAS-Port = 92,NAS-Port-Type = 15
Info	EAM24459	2015-02-12 20:17:30 - ic - [172.22.12.15] sameze(IBBU_REALM)[ADMIN, STAFF, CAFE, DEANAGE_FONS, FACULTY HOTSPOT, ICT_CENTER, PHYSICS, LIBRARY, HOSTEL] - User assigned to vlan (VLAN='141')
Info	EAM24805	2015-02-12 20:17:15 - ic - [127.0.0.1] anonymous(IBBU_REALM)[ADMIN, STAFF, CAFE, DEANAGE_FONS, FACULTY HOTSPOT, ICT_CENTER, PHYSICS, LIBRARY, HOSTEL] - RADIUS authentication was resumed for anonymous (realm 'IBBU_REALM') from location-group 'LIBRARY' and attributes are: NAS-IP-Address = 172.22.12.2,NAS-Port = 92,NAS-Port-Type = 15
Info	EAM24459	2015-02-12 20:17:15 - ic - [172.22.12.15] sameze(IBBU_REALM)[ADMIN, STAFF, CAFE, DEANAGE_FONS, FACULTY HOTSPOT, ICT_CENTER, PHYSICS, LIBRARY, HOSTEL] - User assigned to vlan (VLAN='141')
Info	EAM24805	2015-02-12 20:17:14 - ic - [127.0.0.1] sqeezy100(IBBU_REALM)[] - RADIUS authentication accepted for sqeezy100 (realm 'IBBU_REALM') from location-group 'WIRELESS' and attributes are: NAS-IP-Address = 172.16.3.30,NAS-Port = 18268,NAS-Port-Type = 19
Info	EAM24459	2015-02-12 20:17:14 - ic - [127.0.0.1] sqeezy100(IBBU_REALM)[LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT] - User assigned to vlan (VLAN='125')
Info	AUT24414	2015-02-12 20:17:14 - ic - [127.0.0.1] sqeezy100(IBBU_REALM)[LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT] - Agent login succeeded for sqeezy100/IBBU_REALM from E4-D5-3D-9F-08-12.
Info	AUT24326	2015-02-12 20:17:14 - ic - [127.0.0.1] sqeezy100(IBBU_REALM)[] - Primary authentication successful for sqeezy100/System Local from E4-D5-3D-9F-08-12
Info	EAM24460	2015-02-12 20:17:11 - ic - [127.0.0.1] egba01(IBBU_REALM)[] - Authentication failed because the maximum number of concurrent users for the realm has been reached
Info	AUT24326	2015-02-12 20:17:11 - ic - [127.0.0.1] egba01(IBBU_REALM)[] - Primary authentication successful for egba01/System Local from A4-DB-30-4C-0E-14
Info	EAM24805	2015-02-12 20:17:05 - ic - [127.0.0.1] u12fmspad051(IBBU_REALM)[] - RADIUS authentication accepted for u12fmspad051 (realm 'IBBU_REALM') from location-group 'WIRELESS' and attributes are: NAS-IP-Address = 172.16.3.30,NAS-Port = 18264,NAS-Port-Type = 19
Info	EAM24459	2015-02-12 20:17:05 - ic - [127.0.0.1] u12fmspad051(IBBU_REALM)[LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT] - User assigned to vlan (VLAN='125')
Info	AUT24414	2015-02-12 20:17:05 - ic - [127.0.0.1] u12fmspad051(IBBU_REALM)[LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT] - Agent login succeeded for u12fmspad051/IBBU_REALM from 00-26-C6-80-3A-5E.
Info	AUT24326	2015-02-12 20:17:05 - ic - [127.0.0.1] u12fmspad051(IBBU_REALM)[] - Primary authentication successful for u12fmspad051/System Local from 00-26-C6-80-3A-5E
Info	EAM24805	2015-02-12 20:16:59 - ic - [127.0.0.1] anonymous(IBBU_REALM)[ADMIN, STAFF, CAFE, DEANAGE_FONS, FACULTY HOTSPOT, ICT_CENTER, PHYSICS, LIBRARY, HOSTEL] - RADIUS authentication was resumed for anonymous (realm 'IBBU_REALM') from location-group 'LIBRARY' and attributes are: NAS-IP-Address = 172.22.12.2,NAS-Port = 92,NAS-Port-Type = 15
Info	EAM24459	2015-02-12 20:16:59 - ic - [172.22.12.15] sameze(IBBU_REALM)[ADMIN, STAFF, CAFE, DEANAGE_FONS, FACULTY HOTSPOT, ICT_CENTER, PHYSICS, LIBRARY, HOSTEL] - User assigned to vlan (VLAN='141')
Info	EAM24805	2015-02-12 20:16:56 - ic - [127.0.0.1] u12fnscsc053(IBBU_REALM)[] - RADIUS authentication accepted for u12fnscsc053 (realm 'IBBU_REALM') from location-group 'WIRELESS' and attributes are: NAS-IP-Address = 172.16.3.30,NAS-Port = 18262,NAS-Port-Type = 19
Info	EAM24459	2015-02-12 20:16:56 - ic - [127.0.0.1] u12fnscsc053(IBBU_REALM)[LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT] - User assigned to vlan (VLAN='125')
Info	AUT24414	2015-02-12 20:16:56 - ic - [127.0.0.1] u12fnscsc053(IBBU_REALM)[LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT] - Agent login succeeded for u12fnscsc053/IBBU_REALM from 30-AA-BD-17-B2-A4.
Info	AUT24326	2015-02-12 20:16:56 - ic - [127.0.0.1] u12fnscsc053(IBBU_REALM)[] - Primary authentication successful for u12fnscsc053/System Local from 30-AA-BD-17-B2-A4
Info	EAM24805	2015-02-12 20:16:49 - ic - [127.0.0.1] u13fnscsc063(IBBU_REALM)[] - RADIUS authentication accepted for u13fnscsc063 (realm 'IBBU_REALM') from location-group 'WIRELESS' and attributes are: NAS-IP-Address = 172.16.3.30,NAS-Port = 18257,NAS-Port-Type = 19
Info	EAM24459	2015-02-12 20:16:49 - ic - [127.0.0.1] u13fnscsc063(IBBU_REALM)[LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT] - User assigned to vlan (VLAN='125')
Info	AUT24414	2015-02-12 20:16:49 - ic - [127.0.0.1] u13fnscsc063(IBBU_REALM)[LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT] - Agent login succeeded for u13fnscsc063/IBBU_REALM from 04-F7-E4-38-6E-DE.
Info	AUT24326	2015-02-12 20:16:49 - ic - [127.0.0.1] u13fnscsc063(IBBU_REALM)[] - Primary authentication successful for u13fnscsc063/System Local from 04-F7-E4-38-6E-DE
Info	EAM24460	2015-02-12 20:16:46 - ic - [127.0.0.1] egba01(IBBU_REALM)[] - Authentication failed because the maximum number of concurrent users for the realm has been reached
Info	AUT24326	2015-02-12 20:16:46 - ic - [127.0.0.1] egba01(IBBU_REALM)[] - Primary authentication successful for egba01/System Local from A4-DB-30-4C-0E-14

(i) Users session details

Active Users

Overview | Active Users

Show users named: * Show 200 users Update

Delete Session... | Delete All Sessions... | Refresh Roles | Disable All Users...

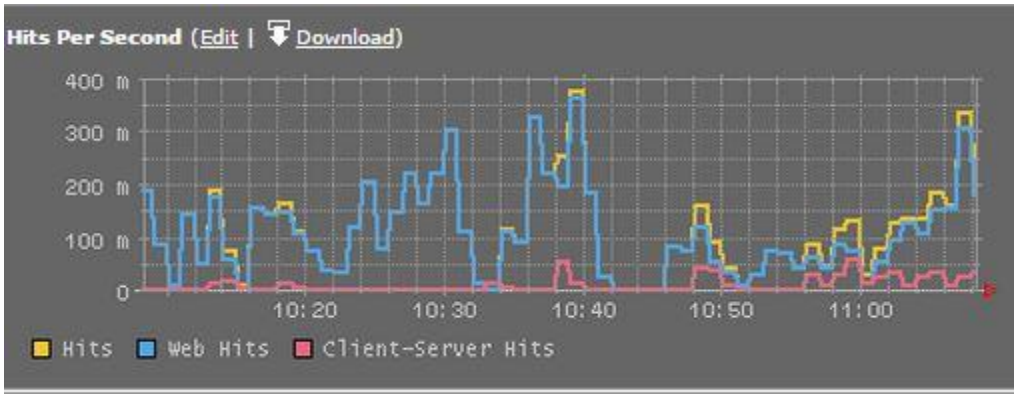
Number of Users: 321

	!	User	Realm	Roles	Signed in	Signed in IP	MAC Address	Agent Type	Agent Version	Endpoint Security Status
		01librarian	IBBU_REALM	ADMIN, STAFF, CAFE, DEANAGE_FONS, FACULTY HOTSPOT, ICT_CENTER, PHYSICS, LIBRARY, HOSTEL	2015/2/12 15:38:24		64-89-9a-86-51-aa			Not Applicable
		02librarian	IBBU_REALM	ADMIN, STAFF, CAFE, DEANAGE_FONS, FACULTY HOTSPOT, ICT_CENTER, PHYSICS, LIBRARY, HOSTEL	2015/2/12 15:23:53		bc-f6-85-ac-a4-ac			Not Applicable
		04security	IBBU_REALM	SECURITY, ADMIN, FACULTY HOTSPOT, ICT_CENTER	2015/2/12 15:20:50		f4-b7-e2-41-ae-0d			Not Applicable
		abbeyolaa	IBBU_REALM	LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT	2015/2/12 19:58:30		00-82-84-bd-06-0a			Not Applicable
		abdul28	IBBU_REALM	LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT	2015/2/12 19:07:46		3c-18-9f-02-90-19			Not Applicable
		abdul28	IBBU_REALM	LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT	2015/2/12 12:48:55		b8-b4-2e-d8-35-bb			Not Applicable
		abdul9672	IBBU_REALM	LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT	2015/2/12 20:23:38		b8-98-f7-16-41-6a			Not Applicable
		ABmalik	IBBU_REALM	LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT	2015/2/12 16:53:36		00-1a-73-d7-12-df			Not Applicable
		Adamsay	IBBU_REALM	LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT	2015/2/12 11:00:39		38-aa-3c-86-6c-20			Not Applicable
		adamu001	IBBU_REALM	LIBRARY, HOSTEL, ICT_CENTER, FACULTY HOTSPOT	2015/2/12 14:07:37		94-00-70-cb-84-67			Not Applicable

(ii) Active users' session details

Appendix C

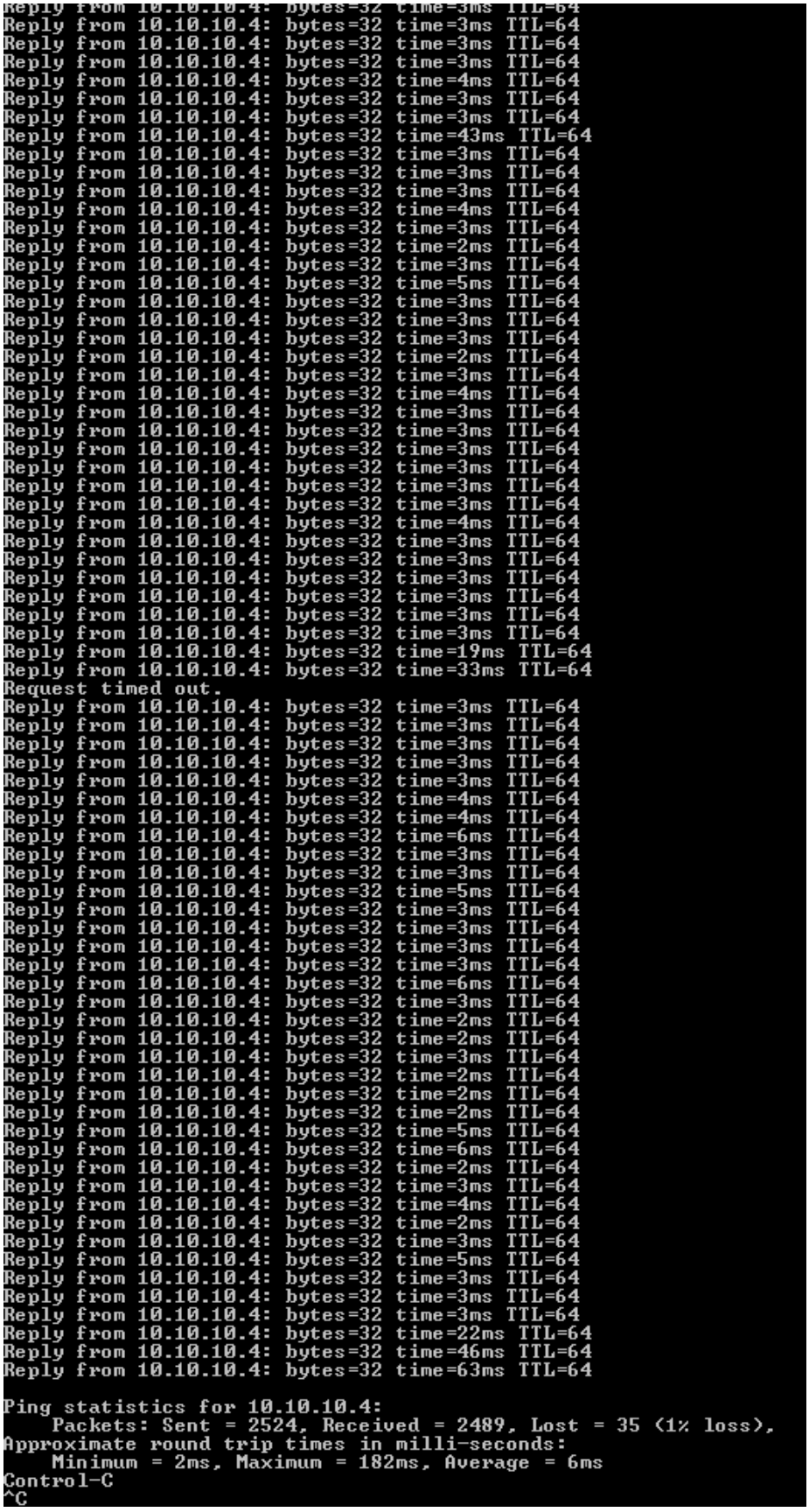
Domain Hits per Second



APPENDIX D

```
64 bytes from 10.10.10.4: icmp_seq=2363 ttl=64 time=2.357 ms
64 bytes from 10.10.10.4: icmp_seq=2364 ttl=64 time=1.679 ms
64 bytes from 10.10.10.4: icmp_seq=2365 ttl=64 time=10.451 ms
64 bytes from 10.10.10.4: icmp_seq=2366 ttl=64 time=7.318 ms
64 bytes from 10.10.10.4: icmp_seq=2367 ttl=64 time=6.424 ms
64 bytes from 10.10.10.4: icmp_seq=2368 ttl=64 time=1.615 ms
64 bytes from 10.10.10.4: icmp_seq=2369 ttl=64 time=1.657 ms
64 bytes from 10.10.10.4: icmp_seq=2370 ttl=64 time=1.748 ms
64 bytes from 10.10.10.4: icmp_seq=2371 ttl=64 time=2.213 ms
64 bytes from 10.10.10.4: icmp_seq=2372 ttl=64 time=1.808 ms
64 bytes from 10.10.10.4: icmp_seq=2373 ttl=64 time=1.774 ms
64 bytes from 10.10.10.4: icmp_seq=2374 ttl=64 time=1.701 ms
64 bytes from 10.10.10.4: icmp_seq=2375 ttl=64 time=1.990 ms
64 bytes from 10.10.10.4: icmp_seq=2376 ttl=64 time=1.822 ms
64 bytes from 10.10.10.4: icmp_seq=2377 ttl=64 time=1.642 ms
64 bytes from 10.10.10.4: icmp_seq=2378 ttl=64 time=18.931 ms
64 bytes from 10.10.10.4: icmp_seq=2379 ttl=64 time=2.456 ms
64 bytes from 10.10.10.4: icmp_seq=2380 ttl=64 time=2.148 ms
64 bytes from 10.10.10.4: icmp_seq=2381 ttl=64 time=34.973 ms
64 bytes from 10.10.10.4: icmp_seq=2382 ttl=64 time=1.876 ms
64 bytes from 10.10.10.4: icmp_seq=2383 ttl=64 time=2.010 ms
64 bytes from 10.10.10.4: icmp_seq=2384 ttl=64 time=1.803 ms
64 bytes from 10.10.10.4: icmp_seq=2385 ttl=64 time=1.750 ms
64 bytes from 10.10.10.4: icmp_seq=2386 ttl=64 time=2.671 ms
64 bytes from 10.10.10.4: icmp_seq=2387 ttl=64 time=1.609 ms
64 bytes from 10.10.10.4: icmp_seq=2388 ttl=64 time=7.305 ms
64 bytes from 10.10.10.4: icmp_seq=2389 ttl=64 time=1.877 ms
64 bytes from 10.10.10.4: icmp_seq=2390 ttl=64 time=2.936 ms
64 bytes from 10.10.10.4: icmp_seq=2391 ttl=64 time=1.711 ms
64 bytes from 10.10.10.4: icmp_seq=2392 ttl=64 time=3.480 ms
64 bytes from 10.10.10.4: icmp_seq=2393 ttl=64 time=2.291 ms
64 bytes from 10.10.10.4: icmp_seq=2394 ttl=64 time=3.399 ms
64 bytes from 10.10.10.4: icmp_seq=2395 ttl=64 time=3.341 ms
64 bytes from 10.10.10.4: icmp_seq=2396 ttl=64 time=8.260 ms
64 bytes from 10.10.10.4: icmp_seq=2397 ttl=64 time=2.747 ms
64 bytes from 10.10.10.4: icmp_seq=2398 ttl=64 time=1.766 ms
64 bytes from 10.10.10.4: icmp_seq=2399 ttl=64 time=2.330 ms
64 bytes from 10.10.10.4: icmp_seq=2400 ttl=64 time=1.560 ms
64 bytes from 10.10.10.4: icmp_seq=2401 ttl=64 time=1.772 ms
64 bytes from 10.10.10.4: icmp_seq=2402 ttl=64 time=1.859 ms
64 bytes from 10.10.10.4: icmp_seq=2403 ttl=64 time=1.897 ms
64 bytes from 10.10.10.4: icmp_seq=2404 ttl=64 time=1.688 ms
64 bytes from 10.10.10.4: icmp_seq=2405 ttl=64 time=1.627 ms
64 bytes from 10.10.10.4: icmp_seq=2406 ttl=64 time=8.455 ms
64 bytes from 10.10.10.4: icmp_seq=2407 ttl=64 time=8.853 ms
64 bytes from 10.10.10.4: icmp_seq=2408 ttl=64 time=2.214 ms
64 bytes from 10.10.10.4: icmp_seq=2409 ttl=64 time=7.282 ms
64 bytes from 10.10.10.4: icmp_seq=2410 ttl=64 time=1.610 ms
64 bytes from 10.10.10.4: icmp_seq=2411 ttl=64 time=1.740 ms
64 bytes from 10.10.10.4: icmp_seq=2412 ttl=64 time=33.055 ms
64 bytes from 10.10.10.4: icmp_seq=2413 ttl=64 time=1.826 ms
64 bytes from 10.10.10.4: icmp_seq=2414 ttl=64 time=1.696 ms
64 bytes from 10.10.10.4: icmp_seq=2415 ttl=64 time=1.787 ms
64 bytes from 10.10.10.4: icmp_seq=2416 ttl=64 time=1.906 ms
64 bytes from 10.10.10.4: icmp_seq=2417 ttl=64 time=1.961 ms
64 bytes from 10.10.10.4: icmp_seq=2418 ttl=64 time=1.553 ms
64 bytes from 10.10.10.4: icmp_seq=2419 ttl=64 time=1.659 ms
^C
--- 10.10.10.4 ping statistics ---
2420 packets transmitted, 2420 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.403/9.950/2037.172/73.497 ms
```

(a) Ping Test I



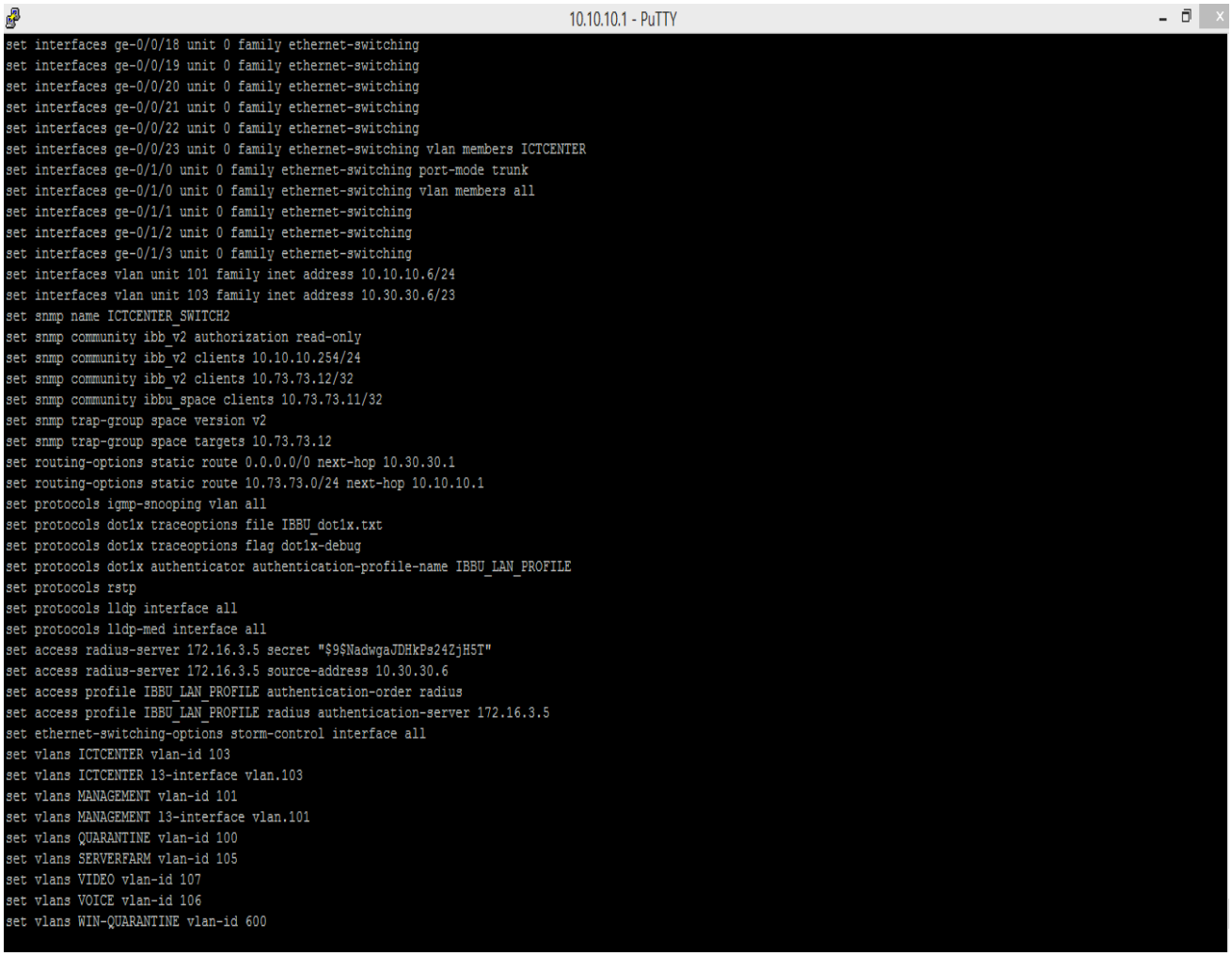
(b) Ping Test II

APPENDIX E

```
set security pki ca-profile ca enrollment retry-interval 1800
set security ike proposal ike-phase1-proposal authentication-method pre-shared-keys
set security ike proposal ike-phase1-proposal dh-group group2
set security ike proposal ike-phase1-proposal authentication-algorithm sha1
set security ike proposal ike-phase1-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-phase1-policy mode main
set security ike policy ike-phase1-policy proposals ike-phase1-proposal
set security ike policy ike-phase1-policy pre-shared-key ascii-text "$9$oMZDk5Qnp0I.P0IEcvMaZUj.PTz39tu"
set security ike gateway gw-LAYER3 ike-policy ike-phase1-policy
set security ike gateway gw-LAYER3 address 41.217.207.67
set security ike gateway gw-LAYER3 external-interface ge-0/0/0.0
set security ipsec proposal ipsec-phase2-proposal protocol esp
set security ipsec proposal ipsec-phase2-proposal authentication-algorithm hmac-sha1-96
set security ipsec proposal ipsec-phase2-proposal encryption-algorithm aes-128-cbc
set security ipsec policy ipsec-phase2-policy perfect-forward-secrecy keys group2
set security ipsec policy ipsec-phase2-policy proposals ipsec-phase2-proposal
set security ipsec vpn LAYER3-VPN bind-interface st0.0
set security ipsec vpn LAYER3-VPN ike gateway gw-LAYER3
set security ipsec vpn LAYER3-VPN ike ipsec-policy ipsec-phase2-policy
set security utm custom-objects url-pattern blocked value http://www.yahoo.com
set security utm custom-objects custom-url-category blocked value blocked
set security utm feature-profile anti-virus type kaspersky-lab-engine
set security utm feature-profile anti-virus kaspersky-lab-engine profile IBBU_ANTIVIRUS scan-options scan-mode all
set security utm feature-profile web-filtering url-blacklist blocked
set security utm feature-profile web-filtering type surf-control-integrated
set security utm feature-profile web-filtering surf-control-integrated cache size 500
set security utm feature-profile web-filtering surf-control-integrated profile IBBU_WEB_FILTER category Hacking action block
set security utm feature-profile web-filtering surf-control-integrated profile IBBU_WEB_FILTER category Adult_Sexually_Explicit action block
set security utm feature-profile web-filtering surf-control-integrated profile IBBU_WEB_FILTER category Chat action block
set security utm feature-profile web-filtering surf-control-integrated profile IBBU_WEB_FILTER category Sports action block
set security utm feature-profile web-filtering surf-control-integrated profile IBBU_WEB_FILTER category blocked action block
set security utm feature-profile web-filtering surf-control-integrated profile IBBU_WEB_FILTER custom-block-message "******************SITE NOT ALLOWED IN IBBU!!!! ACCE
SS DENIED 8:00am to 5:00pm, MONDAYS to FRIDAYS**********************"
set security utm feature-profile web-filtering surf-control-integrated profile Search category Search_Engines action block
set security utm feature-profile web-filtering surf-control-integrated profile Search default block
set security utm feature-profile web-filtering surf-control-integrated profile Search custom-block-message "Not allowed for now"
set security utm feature-profile web-filtering surf-control-integrated profile Search fallback-settings default log-and-permit
set security utm feature-profile web-filtering surf-control-integrated profile Search fallback-settings server-connectivity log-and-permit
set security utm feature-profile web-filtering surf-control-integrated profile Search fallback-settings timeout log-and-permit
set security utm feature-profile web-filtering surf-control-integrated profile Search fallback-settings too-many-requests log-and-permit
set security utm feature-profile web-filtering surf-control-integrated profile Search_Engines category Search_Engines action block
set security utm feature-profile web-filtering surf-control-integrated profile Search_Engines default block
set security utm feature-profile web-filtering surf-control-integrated profile Search_Engines custom-block-message "NOT ALLOW FOR NOW"
set security utm feature-profile web-filtering surf-control-integrated profile Search_Engines fallback-settings default block
```

10.10.10.1 - PuTTY

```
set security utm feature-profile web-filtering surf-control-integrated cache size 500
set security utm feature-profile web-filtering surf-control-integrated profile IBBU_WEB_FILTER category Hacking action block
set security utm feature-profile web-filtering surf-control-integrated profile IBBU_WEB_FILTER category Adult_Sexually_Explicit action block
set security utm feature-profile web-filtering surf-control-integrated profile IBBU_WEB_FILTER category Chat action block
set security utm feature-profile web-filtering surf-control-integrated profile IBBU_WEB_FILTER category Sports action block
set security utm feature-profile web-filtering surf-control-integrated profile IBBU_WEB_FILTER category blocked action block
set security utm feature-profile web-filtering surf-control-integrated profile IBBU_WEB_FILTER custom-block-message "******************SITE NOT ALLOWED IN IBBU!!!! ACCE
SS DENIED 8:00am to 5:00pm, MONDAYS to FRIDAYS**********************"
set security utm feature-profile web-filtering surf-control-integrated profile Search category Search_Engines action block
set security utm feature-profile web-filtering surf-control-integrated profile Search default block
set security utm feature-profile web-filtering surf-control-integrated profile Search custom-block-message "Not allowed for now"
set security utm feature-profile web-filtering surf-control-integrated profile Search fallback-settings default log-and-permit
set security utm feature-profile web-filtering surf-control-integrated profile Search fallback-settings server-connectivity log-and-permit
set security utm feature-profile web-filtering surf-control-integrated profile Search fallback-settings timeout log-and-permit
set security utm feature-profile web-filtering surf-control-integrated profile Search fallback-settings too-many-requests log-and-permit
set security utm feature-profile web-filtering surf-control-integrated profile Search_Engines category Search_Engines action block
set security utm feature-profile web-filtering surf-control-integrated profile Search_Engines default block
set security utm feature-profile web-filtering surf-control-integrated profile Search_Engines custom-block-message "NOT ALLOW FOR NOW"
set security utm feature-profile web-filtering surf-control-integrated profile Search_Engines fallback-settings default block
set security utm feature-profile web-filtering surf-control-integrated profile Search_Engines fallback-settings server-connectivity block
set security utm feature-profile web-filtering surf-control-integrated profile Search_Engines fallback-settings timeout block
set security utm feature-profile web-filtering surf-control-integrated profile Search_Engines fallback-settings too-many-requests block
set security utm feature-profile web-filtering juniper-enhanced cache timeout 1800
set security utm feature-profile web-filtering juniper-enhanced cache size 500
set security utm feature-profile web-filtering juniper-enhanced profile my_ewfprofile01 default log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile my_ewfprofile01 fallback-settings default log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile my_ewfprofile01 fallback-settings server-connectivity log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile my_ewfprofile01 fallback-settings timeout log-and-permit
set security utm feature-profile web-filtering juniper-enhanced profile my_ewfprofile01 fallback-settings too-many-requests log-and-permit
set security utm feature-profile anti-spam sbl profile junos-as-defaults sbl-default-server
set security utm feature-profile anti-spam sbl profile junos-as-defaults spam-action block
set security utm feature-profile anti-spam sbl profile junos-as-defaults custom-tag-string ***SPAM***
set security utm utm-policy IBBU-UTM-POLICY anti-virus http-profile IBBU_ANTIVIRUS
set security utm utm-policy IBBU-UTM-POLICY anti-virus smtp-profile IBBU_ANTIVIRUS
set security utm utm-policy IBBU-UTM-POLICY anti-virus pop3-profile IBBU_ANTIVIRUS
set security utm utm-policy IBBU-UTM-POLICY web-filtering http-profile IBBU_WEB_FILTER
set security utm utm-policy IBBU-UTM-POLICY anti-spam smtp-profile junos-as-defaults
set security utm utm-policy mypolicy web-filtering http-profile my_ewfprofile01
set security utm utm-policy mypolicy traffic-options sessions-per-client limit 1000
set security utm utm-policy mypolicy traffic-options sessions-per-client over-limit block
set security flow traceoptions file LAYER3-VPN
set security flow traceoptions file files 2
set security flow traceoptions file world-readable
set security flow traceoptions flag basic-datapath
```


10.10.10.1 - PuTTY
set interfaces ge-0/0/18 unit 0 family ethernet-switching
set interfaces ge-0/0/19 unit 0 family ethernet-switching
set interfaces ge-0/0/20 unit 0 family ethernet-switching
set interfaces ge-0/0/21 unit 0 family ethernet-switching
set interfaces ge-0/0/22 unit 0 family ethernet-switching
set interfaces ge-0/0/23 unit 0 family ethernet-switching vlan members ICTCENTER
set interfaces ge-0/1/0 unit 0 family ethernet-switching port-mode trunk
set interfaces ge-0/1/0 unit 0 family ethernet-switching vlan members all
set interfaces ge-0/1/1 unit 0 family ethernet-switching
set interfaces ge-0/1/2 unit 0 family ethernet-switching
set interfaces ge-0/1/3 unit 0 family ethernet-switching
set interfaces vlan unit 101 family inet address 10.10.10.6/24
set interfaces vlan unit 103 family inet address 10.30.30.6/23
set snmp name ICTCENTER_SWITCH2
set snmp community ibb_v2 authorization read-only
set snmp community ibb_v2 clients 10.10.10.254/24
set snmp community ibb_v2 clients 10.73.73.12/32
set snmp community ibbu_space clients 10.73.73.11/32
set snmp trap-group space version v2
set snmp trap-group space targets 10.73.73.12
set routing-options static route 0.0.0.0/0 next-hop 10.30.30.1
set routing-options static route 10.73.73.0/24 next-hop 10.10.10.1
set protocols igmp-snooping vlan all
set protocols dot1x traceoptions file IBBU_dot1x.txt
set protocols dot1x traceoptions flag dot1x-debug
set protocols dot1x authenticator authentication-profile-name IBBU_LAN_PROFILE
set protocols rstp
set protocols lldp interface all
set protocols lldp-med interface all
set access radius-server 172.16.3.5 secret "9NadwgaJDHkPs24ZjH5T"
set access radius-server 172.16.3.5 source-address 10.30.30.6
set access profile IBBU_LAN_PROFILE authentication-order radius
set access profile IBBU_LAN_PROFILE radius authentication-server 172.16.3.5
set ethernet-switching-options storm-control interface all
set vlans ICTCENTER vlan-id 103
set vlans ICTCENTER l3-interface vlan.103
set vlans MANAGEMENT vlan-id 101
set vlans MANAGEMENT l3-interface vlan.101
set vlans QUARANTINE vlan-id 100
set vlans SERVERFARM vlan-id 105
set vlans VIDEO vlan-id 107
set vlans VOICE vlan-id 106
set vlans WIN-QUARANTINE vlan-id 600