Policy Creation Model for Policy based Bandwidth Management in the Core Network (A Case Study of Abu Data Network)

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

D. D. Dajab, PhD.
Director ICT, A.B.U Zaria
Senior Lecturer, Department of Electrical and Computer Engineering,

M.B Mu'azu, PhD.
Head of Department, Electrical and Computer Engineering,
Engineering, ABU, Zaria
Nigeria

ABSTRACT

Bandwidth management and optimization are very critical to any organization especially universities and research organizations. This work is aimed at the development of a policy- based bandwidth scheme for ABU Zaria (as a case study). ABU Zaria currently has a fibre-based STM-1 links leased from Glo – I, thus providing the university with a full duplex bandwidth of 155Mbps. The university has a student – staff population of about 40000 currently and a fibre ring back-bone network linking the three campuses at Samaru, Shika and Kongo. The work involved collection and analysis of traffic data over a 90-day period using Packet Sniffer, for the development of the policy- based strategies for bandwidth optimization. Simulation of the effect of the policies on a segment of the network was carried out using the GNS3 and validation of results of the simulation was done on a small network. The results showed as improvement in bandwidth utilization from 3.9Mbps to 2.9Mbps thus saving 1.0Mbps in bandwidth when the developed policies were implemented. This is an indication that when implemented on the live network there will be better management of the bandwidth. [2]

General Terms

Policy based - bandwidth management implementation, Design a model, simulated in a GNS3.

Keywords: Policy Creation Process, Configuration and simulation.

1. INTRODUCTION

ABU Zaria has a staff- student population of about 40,000 with varied interests (academic and non-academic) for utilizing bandwidth is insatiable and without proper management it will not be optically utilized in line with the mission and vision of the network. This thus necessitates the need to develop a comprehensive bandwidth management policy, in this case, policy – based.

The proposed model is expected to meet the needs of campus ICT department who need to offer their campus community proper internet services through as follows:

i. Guaranteed bandwidth for education applications in the campus network.

ii. Reduce traffic congestion and increase network efficiency in the campus network.

iii. Control users and applications in their access to network resources. [1]

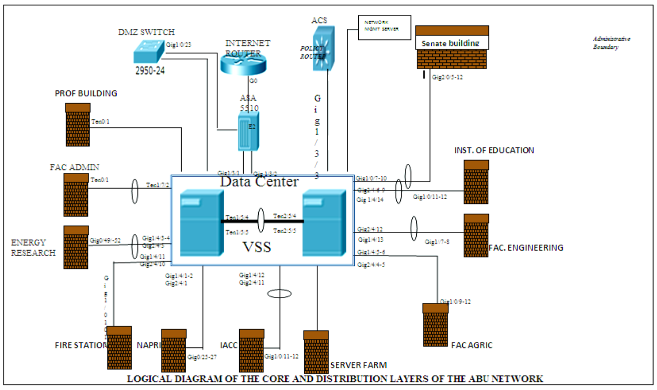


Figure 1: Logical Diagram of the core and Distribution Layers of the ABU Network

2. BACKGROUND

Bandwidth is the maximum amount of data that can travel a communications path in a given time.

Bandwidth is typically measured in bits per second. If you think of the communications path as a pipe, then bandwidth represents the width of the pipe that determines how much data can flow through it all at once [3] Inbound traffic is data that is received by your computer from another computer. Outbound traffic is data that is sent from your computer to another computer. With the ever-increasing number of users that use high bandwidth for broadband multimedia traffic over the Internet, such as interactive games, videoconference, High-Definition Television (HDTV) and other high-speed services, high growth of access network is the most glaring issue in the communication industry

3. STATEMENT OF PROBLEM

There are about 40000 students and staff in ABU Zaria which is multi- campus based (Samaru, Shika and Kongo). On the average there are about 6000 – 7000 concurrent users on the ABU network at any particular time (especially during the hours of 8:00am to 4:00pm). These users have varied interacts and reasons for being in the network (academic and non - academic).

Most traffic activities on the network are mostly on the Internet compared to the intranet (which is robust and fast since it is on fibre). This implies bandwidth usage and even though ABU Zaria is on STM-1 link via fibre from GLO –I (full duplex bandwidth of 155Mps), Lack of a comprehensive bandwidth management policy can lead to a non –optimal usage of such bandwidth.

4. POLICY CREATION MODEL METHODOLOGY

The pertinent steps in designing the proposed model are as follows:

- **i.** Defining High-Level Abstract Policies
- **ii.** Specifying High-Level Goals
- **iii.** Defining Sub-Goals
- **iv.** Generating Strategies
- **v.** Identifying Conditions
- **vi.** Identifying the Subject and Target
- **vii.** Defining the Policies which will be deployed by the System

4.1 Defining high-level abstract policies

In this phase the management objectives are extracted. The aim of this approach is to create policies to manage the internet traffic, because it is necessary to use effectively the Internet links according to the services that it offers. This requirement is needed so that there would not be a 'bottleneck' within the network. In this sense, the following needs /requirements are observed:

- **i.** Videoconferencing and streaming services should be prioritized and must ensure adequate bandwidth for their proper functioning.
- **ii.** Access to sites of institutional interest must always be guaranteed.
- **iii.** Services of non-institutional interesting should have low priority and be restricted during working hours.
- **iv.** Hosts that have special permits should be having unlimited bandwidth.
- **v.** Web servers must be accessed at any time and at a good speed, regardless of the amount of traffic which they arise [2]

4.2 Specifying high-level goals

It expresses the aims to be achieved by the management system in general way (abstract level). Since it uses a goal approach for creating policies, it needs to define high-level goals that fulfill the necessities and requirements defined into the High-Level Abstract Policies. Now define the high-level goal **G $_{1\text{-}1}$:** "Bandwidth optimized for both incoming and outgoing internet traffic "which represents the main objective that should be achieved by the management system policies [3]

4.3 Defining sub-goal

In this step, is to extract the sub goals (**SG**) and generate a refinement hierarchy. This is done taking into account the management needs/requirements, available resources and information about the management environment. It is necessary to take into account the services, there sources consumed by each service and the priority to be given to each of these resources, according to the role in the institutional mission at the university. Figure 1.1 shows the refinement hierarchy generated for this particular case, where

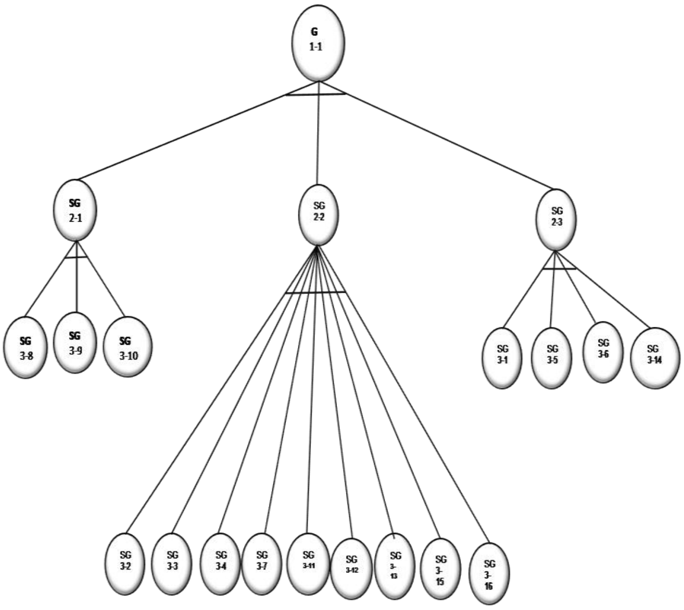


Figure 2: Refinement hierarchies

G $_{1\text{-}1}$: "Bandwidth optimized for both incoming and outgoing internet traffic "which represents the main objective that should be achieved by the management system.

SG$_{2\text{-}1}$: Allow access to the Services and/or Applications.

SG$_{2\text{-}2}$: Set a Bandwidth for Services and/or applications by defining thresholds (Minimum -Maximum).

SG$_{2\text{-}3}$: Ensure a Bandwidth for Services and/or Applications.

SG$_{3\text{-}1}$: Ensure a bandwidth of 256kbps per incoming connection to mail servers.

SG$_{3\text{-}2}$: Set the maximum bandwidth allowed per outgoing connections from mail servers.

SG$_{3\text{-}3}$: Set a minimum bandwidth of 512kbps for incoming and outgoing connections of computers that have urgent downloads.

SG$_{3\text{-}4}$: Ensure a bandwidth of 1024kbps for incoming and outgoing connections to streaming Server.

SG$_{3\text{-}5}$: Ensure a bandwidth of 512kbps per connection for incoming and outgoing traffic of videoconference equipments.

SG$_{3\text{-}6}$: Ensure a bandwidth of 512kbps for incoming connection to the Web Server.

SG$_{3\text{-}7}$: Set the maximum bandwidth allowed per connection for outgoing traffic from Web Servers.

SG$_{3\text{-}8}$: Deny access to RapidShare during working hours.

SG$_{3\text{-}9}$: Deny access to P2P applications during working hours.

SG$_{3\text{-}10}$: Allow access to P2P applications during non-working hours.

SG_{3-11}: Set a minimum bandwidth of 64kbps to internet access for equipment with public IP address.

SG_{3-12}: Set a maximum bandwidth of 512kbps for outgoing traffic from FTP server.

SG_{3-13}: Set a minimum bandwidth of 1024kbps for outgoing traffic to important web sites.

SG_{3-14}: Ensure a bandwidth of 1024kbps per connection for outgoing traffic from streaming servers.

SG_{3-15}: Set a minimum bandwidth of 512kbps for incoming traffic to proxy servers.

SG_{3-16}: Set a minimum bandwidth of 1024kbps for outgoing traffic from proxy servers.

4.4 Generating strategies

Strategy is called the sequence of sub-goals that should be implemented to obtain the high-level goal in the management system. The strategy can be encoded in one or more mid-level policies). Therefore, it must meet allow-level goals in order to achieve the high-level ones. The generated strategy is called S1.

S1 = SG_{3-1} Λ SG_{3-2} Λ SG_{3-3} Λ SG_{3-4} Λ SG_{3-5} Λ SG_{3-6} Λ SG_{3-7} Λ SG_{3-8} Λ SG_{3-9} Λ SG_{3-10}Λ SG_{3-11} Λ SG_{3-12} Λ SG_{3-13} Λ SG_{3-14} Λ SG_{3-15} Λ SG_{3-16}

4.5 Identifying conditions

.In this step should be identified all conditions that help each Sub Goal to be achieved in the system taking into account the functionality that the system supports, determining the source and destination of traffic, the type of service and time in which each Sub Goal is executed.

4.6 Identify the subject and target

It is necessary to identify the subject and target that will be specified in the final policy rules. The Subject refers to the entity responsible for implementing the actions involved in the policy or the objects that are permitted or prohibited in the actions. The Target refers to the elements affected by the policy actions.

Table 1. Summary of Conditions Identified for each Sub-Goal

Sub-Goal	**Conditions**			
	Source	**Destination**	**Services**	**Time**
SG_{3-1}	Mail Servers	Any destination	Mail	Any time
SG_{3}-2	Any source	Mail Server	Mail	Any time
SG_{3-3}	Hosts with Important Downloads	Any destination	All IP	Any time
SG_{3-4}	VoIP Server	Any destination	VoIP	Any time
SG_{3-5}	Videoconference Equipments	Any destination	All IP	Any time
SG_{3-6}	Web Servers	Any destination	All IP	Any time
SG_{3-7}	Any source	Web Server	All IP	Any time
SG_{3-8}	Any source	RapidShare Servers	Web Applications	Working Hours
SG_{3-9}	Any source	Any destination	P2P Applications	Working Hour
SG_{3-10}	Any source	Any destination	P2P Applications	Non Working Hours
SG_{3-11}	Host with NAT or Public IP	Any destination	All IP	Any time
SG_{3-12}	FTP server	Any destination	FTP	Any time
SG_{3-13}	Any source	Important Web Sites	Web Applications	Any time
SG_{3-14}	Streaming Servers	Any destination	All IP	Any time
SG_{3-15}	Any source	Proxy Servers	All IP	Any time
SG_{3-16}	Proxy Servers	Any destination	All IP	Any time

Table 1.1 summarizes all identified conditions that help each Sub Goal to be achieved in the system. That is, the source and destination of traffic, the type of service and time in which each Sub Goal is executed.

4.7 Defining the Policies which will be specified in the System

In order to deploy a policy in a management system, it is necessary to define this in a mid-level policy format for this; it uses all the elements obtained in the previous steps (e.g. sub goals, conditions, target, and subject). The following are the defined policies that make up the strategy S1:

P1 (Based on SG_{3-1}): If “The Service is email, the Source Address is mail servers, Destination Address is whichever, anytime” Then “Ensure a bandwidth of 256kbps to mail servers, and assign a medium priority (6)”.

P2 (Based on SG_{3-2}): If “The Service is email, the Source Address is whichever; the Destination Address belongs to one of the mail servers, anytime” Then “Assign a medium priority(6) and give the maximum available capacity to service”.

P3 (Based on SG_{3-3}): If “The Source Address belongs to any host of urgent downloads group, Destination Address is whichever, anytime” Then “Assign a minimum bandwidth of 512 kbps for both inbound and outbound connection to that computer, and give a high priority (9)”.

P4 (Based on SG_{3-4}): If “The Source Address and Destination Address is the VoIP server, anytime” Then “Ensure a bandwidth of 1024 kbps for both inbound and outbound connection to that server, and assign a high priority (9)”.

P5 (Based on SG_{3-5}): If “The Source Address or Destination Address belongs to any video conference equipments, anytime” Then “Ensure a bandwidth of 512 kbps for both inbound and outbound connections to these hosts and assign a medium priority (6)”.

P6 (Based on SG_{3-6}): If “The Source Address is whichever, the Destination Address belongs to one of the web servers, anytime" Then "Ensure a bandwidth of 512kbps for incoming connection to these servers and assign a middle priority (7)".

P7 (Based on SG_{3-7}): If "The Source Address belongs to one of the web servers, Destination Address is whichever, anytime "Then "Give the maximum available bandwidth for outgoing connection from these servers and assign a low priority (4)".

P8 (Based on SG_{3-8}): If "The Source Address is whichever, the Destination Address is one of the RapidShare servers, the Service is a web application, anytime" Then "Discard traffic from and to those servers".

P9 (Based on SG_{3-9}): If "The source address is whichever, the Application is P2P, at working hours" Then "Deny Access to those applications".

P10 (Based on SG_{3-10}): If "The Source Address and Destination Address is whichever, the Application is P2P, at non-working hours" Then "Accept traffic to and from those applications".

P11 (Based on SG_{3-11}): If "The Source Address belongs to one host with NAT or Public IP, Destination Address is whichever, anytime" Then "Assign a maximum bandwidth of 64 kbps to these hosts and assign a middle priority (7)".

P12 (Based on SG_{3-12}): If "The Source Address belongs to one of the FTP servers, Destination Address is whichever, anytime" Then "Set a maximum bandwidth of 512 kbps for outgoing traffic from FTP servers and assign a low priority(4)".

P13 (Based on SG_{3-13}): If "The Source Address is whichever, Destination Address is one of the important web sites, anytime "Then "Set a minimum bandwidth of 1024 kbps".

P14 (Based on SG_{3-14}): If "The Source Address is one of the streaming servers, Destination Address is whichever, anytime" Then "Ensure a bandwidth of 1024 kbps per connection and assign a middle priority (6)".

P15 (Based on SG_{3-15}): If "The Source Address is whichever, the Destination Address is one of the proxy servers, anytime "Then "Set a minimum bandwidth of 512 kbps and assign a middle priority(7)".

P16 (Based on SG_{3-16}): If "The Source Address is one of the proxy servers, Destination Address is whichever, anytime "Then "Set a minimum bandwidth of 512 kbps and assign a middle priority (5)".

The ranges established to determine the priority assigned to each policy are like follow:

i. From 1 to 4, low priority,

ii. From 5 to 7, middle priority and

iii. Finally from 8 to 9, high priority [5

5. RESULTS AND ANALYSES

All the policies set on the objectives of the research work is implemented on the MLS using GNS3. [5]

Figure 3 is the flow chart showing the design and the implementation process of the bandwidth optimization (**G_{1-1}**) policies in a tree form. At the apex, it shows the ultimate goal of bandwidth optimization with the sub goals (SGs) beneath shown in a series of conditional statement which determines which policy is to be implemented at a point and which one not is implemented considering some important differences in the sub goals.

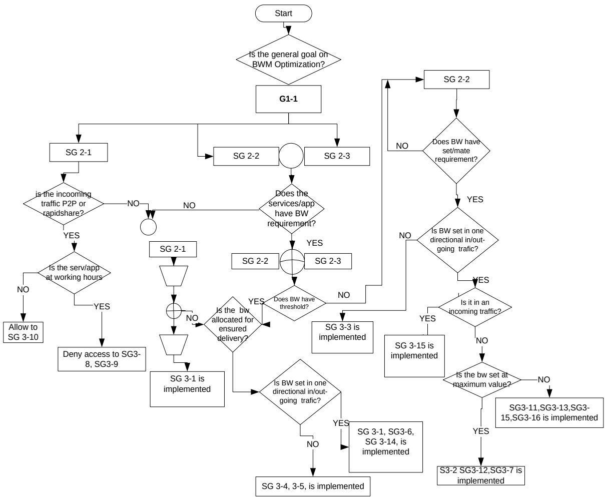

Start
Is the general goal on BWM Optimization?
G1-1
SG 2-1
SG 2-2
SG 2-3
is the incooming traffic P2P or rapidshare?
NO
YES
Is the serv/app at working hours
NO
YES
Allow to SG 3-10
Deny access to SG3-8, SG3-9
NO
Does the services/app have BW requirement?
YES
SG 2-1
SG 2-2
SG 2-3
NO
Is the bw allocated for ensured delivery?
YES
Does BW have threshold?
NO
SG 3-1 is implemented
SG 3-3 is implemented
Is BW set in one directional in/out-going trafic?
YES
NO
SG 3-1, SG3-6, SG 3-14, is implemented
SG 3-4, 3-5, is implemented
SG 2-2
Does BW have set/mate requirement?
NO
YES
Is BW set in one directional in/out-going trafic?
NO
YES
Is it in an incoming traffic?
YES
NO
SG 3-15 is implemented
Is the bw set at maximum value?
NO
YES
SG3-11,SG3-13,SG3-15,SG3-16 is implemented
S3-2 SG3-12,SG3-7 is implemented

Figure 3: Configuration and Implementation of the policies flowchart

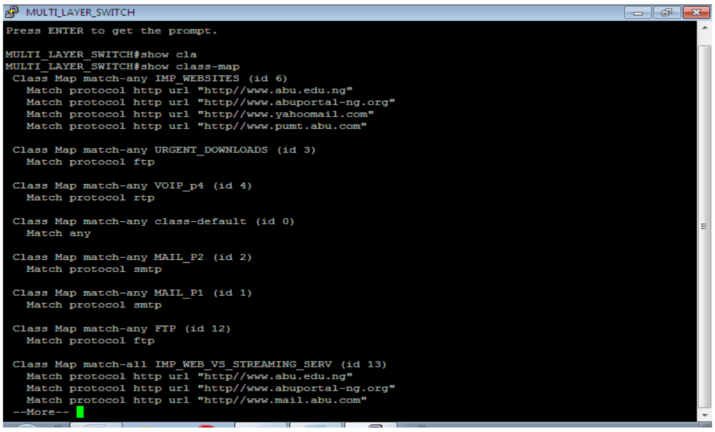
5.1 The Simulation Results

The polices are simulated on Graphical Network Simulator (GNS3) based on the following:

a. Class map

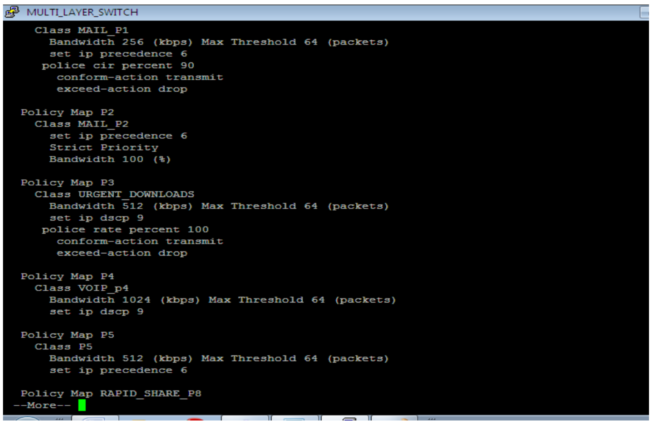
b. Policy map

c. Access list



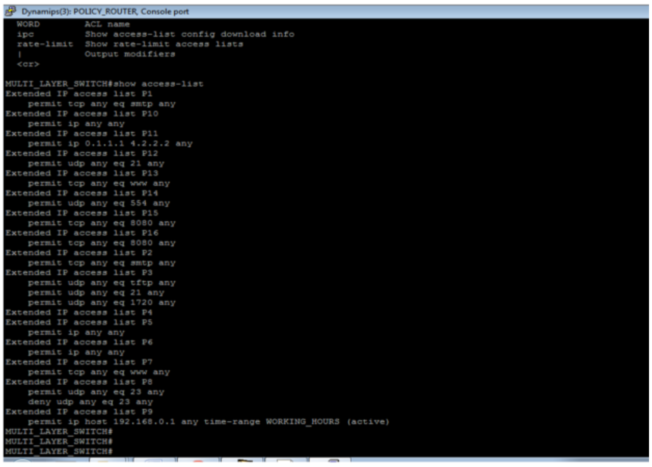
```
Press ENTER to get the prompt.

MULTI_LAYER_SWITCH#show cla
MULTI_LAYER_SWITCH#show class-map
 Class Map match-any IMP_WEBSITES (id 6)
   Match protocol http url "http//www.abu.edu.ng"
   Match protocol http url "http//www.abuportal-ng.org"
   Match protocol http url "http//www.yahoomail.com"
   Match protocol http url "http//www.pumt.abu.com"

 Class Map match-any URGENT_DOWNLOADS (id 3)
   Match protocol ftp

 Class Map match-any VOIP_p4 (id 4)
   Match protocol rtp

 Class Map match-any class-default (id 0)
   Match any

 Class Map match-any MAIL_P2 (id 2)
   Match protocol smtp

 Class Map match-any MAIL_P1 (id 1)
   Match protocol smtp

 Class Map match-any FTP (id 12)
   Match protocol ftp

 Class Map match-all IMP_WEB_VS_STREAMING_SERV (id 13)
   Match protocol http url "http//www.abu.edu.ng"
   Match protocol http url "http//www.abuportal-ng.org"
   Match protocol http url "http//www.mail.abu.com"
 --More--
```

Figure 4: Class map Configuration



```
   Class MAIL_P1
     Bandwidth 256 (kbps) Max Threshold 64 (packets)
     set ip precedence 6
    police cir percent 90
      conform-action transmit
      exceed-action drop

 Policy Map P2
   Class MAIL_P2
     set ip precedence 6
     Strict Priority
     Bandwidth 100 (%)

 Policy Map P3
   Class URGENT_DOWNLOADS
     Bandwidth 512 (kbps) Max Threshold 64 (packets)
     set ip dscp 9
    police rate percent 100
      conform-action transmit
      exceed-action drop

 Policy Map P4
   Class VOIP_p4
     Bandwidth 1024 (kbps) Max Threshold 64 (packets)
     set ip dscp 9

 Policy Map P5
   Class P5
     Bandwidth 512 (kbps) Max Threshold 64 (packets)
     set ip precedence 6

 Policy Map RAPID_SHARE_P8
--More--
```

Figure 5: Policy map Configuration



```
  WORD         ACL name
  ipc          Show access-list config download info
  rate-limit   Show rate-limit access lists
  |            Output modifiers
  <cr>

MULTI_LAYER_SWITCH#show access-list
Extended IP access list P1
    permit tcp any eq smtp any
Extended IP access list P10
    permit ip any any
Extended IP access list P11
    permit ip 0.1.1.1 4.2.2.2 any
Extended IP access list P12
    permit udp any eq 21 any
Extended IP access list P13
    permit tcp any eq www any
Extended IP access list P14
    permit udp any eq 554 any
Extended IP access list P15
    permit tcp any eq 8080 any
Extended IP access list P16
    permit tcp any eq 8080 any
Extended IP access list P2
    permit tcp any eq smtp any
Extended IP access list P3
    permit udp any eq tftp any
    permit udp any eq 21 any
    permit udp any eq 1720 any
Extended IP access list P4
Extended IP access list P5
    permit ip any any
Extended IP access list P6
    permit ip any any
Extended IP access list P7
    permit tcp any eq www any
Extended IP access list P8
    permit udp any eq 23 any
    deny udp any eq 23 any
Extended IP access list P9
    permit ip host 192.168.0.1 any time-range WORKING_HOURS (active)
MULTI_LAYER_SWITCH#
MULTI_LAYER_SWITCH#
MULTI_LAYER_SWITCH#
```

Figure 6: Access List Configurations

The validation of the policy was completed when comparisons of the plots were made between the data captured after the policy was implemented with that which was previously captured before the policies were implemented at specific intervals of time and in overall which shows a great difference between both. From such comparisons, it is safe to say that the policies implemented have help optimized the traffic flow of the network hence the entire network is optimized.

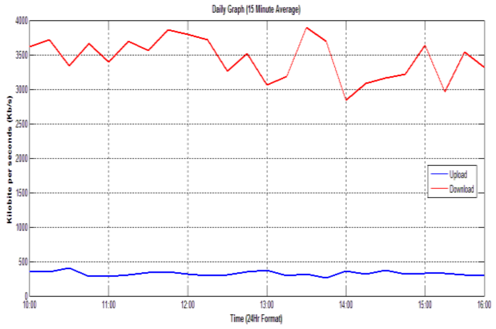


Figure 7 Daily bandwidth utilization graphs before policy is implemented

Figure 7 shows the plots of data captured before the policy was implemented, at the download the maximum occur at 3.9Mbps at 1:30pm while the upload maximum is 499kbps at 10:30am

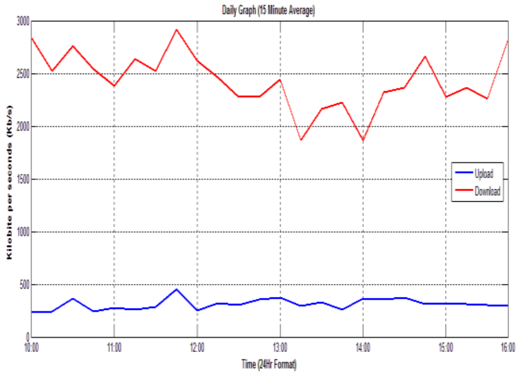


Figure 8: Daily bandwidth utilization graphs after policy are implemented

Figure 8 shows the plot of data captured after the policy was implemented, at the download the maximum occurs at 2.9Mbps at 11:45am noon while the Upload maximum is 498kbps at 11:45am. When this figure s compared with figured 4.8, It is observed that bandwidth is conserved and used more efficiently hence, optimization is achieved.

6. CONCLUSION

A campus network such as that covered by this research work has an enormous and urgent need of a policy-based bandwidth management implementation which was achieved by the research work through a range of technologies. One of the most important results of this work is the procedures adopted for creating the various policies, which allowed development through steps, with critical and careful decisions made at each phase involved in this process. To be able to achieve the desired goal of paying a large sum of money for bandwidth by the University management and to justify the usage of such capital-intensive acquisition of the said bandwidth which should be mainly for academic and research purpose some measure need to be put in place to check unwanted and unnecessary network traffic most likely to be encountered on such campus network (Bandwidth policies). It should however, be noted that while such denials and limited permissions are put in place some (though very few) important University activities may also be affected but can always be easily detected and logically resolved when ever such problems are noted.

7. ACKNOWLEDMENTS

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

8. REFERENCES

[1] Bandara, N. Damianou, E. Lupu, M. Sloman and N. Dulay (2009), "Policy-Based Management" in Handbook of Network and System Management.

[2] D. Adami, M. Marchese, and L. S. Ronga (2010), "Tcp/ip-based multimedia applications and services over satellite links .Personal Communications, *IEEE*, vol. 8 (3) pp. 20–27, 16.

[3] Gakio (2006) African Tertiary Institutions Connectivity Survey (ATICS): Full Repor

[4] Rodriguez, Phil, et al. The Bandwidth Issue: Different Solutions to a Common Challenge." Presentation delivered at ResNet Symposium. J (2008)

[5] Strassner J.C (2004), “Policy-based network management: solutions for the next generation,” Morgan Kaufmann, San Francisco, 2004, pp. 10-24

[6] SuperJANET is the UK academic high-speed high-bandwidth backbone of the JANET.

[7] Shankaraiah; Venkataram, P "Bandwidth management in a hybrid wireless network: For superstore applications," Communication Systems (ICCS), 2010 IEEE International Conference on, vol., no., pp.517-521, 17-19 Nov. 2010