American Journal of Engineering and Applied Sciences

Original Research Paper

# Policy-Based Network Management in BIUST Network

**[1]Thato Solomon, [2]Adamu Murtala Zungeru,**
**[1]Rajalakshmi Selvaraj, [3]Olefile Phakedi and [1]Ontiretse Bagwasi**

*[1]Department of Computer Science and Information Systems,*
*[2]Department of Electrical, Computer and Telecommunication Engineering,*
*[3]Department of Information Communication Technology,*
*Botswana International University of Science and Technology, Palapye, Botswana*

*Article history*
Received: 3-05-2017
Revised:14-06-2017
Accepted: 20-06-2017

Corresponding Author:
Adamu Murtala Zungeru
Department of Electrical, Computer and Telecommunication Engineering, Botswana International University of Science and Technology, Palapye, Botswana
Email: zungerum@biust.ac.bw

**Abstract:** Policy-Based Network Management (PBNM) is one of the approaches used by network administration groups for Quality of Service (QoS) and administration on the internet. This paper seeks to propose the adoption of a Policy Creation Model for Policymaking in some organizations. The model will then be applied to a real scenario Botswana International University of Science and Technology (BIUST) network. A combination of technical computer skills, effective network monitoring and a workable policy helps in attaining effective bandwidth management by the users. This study extends one of our researches in network traffic monitoring in BIUST network.

**Keywords:** Quality of Service, Internet, Network Administration Groups, Policy-Based Network Management, Policy Creation Model

## Introduction

The process used to determine the type and value of traffic of a network's traffic measure is very important particularly on effective management of bandwidth in computer networks. Effective bandwidth management occurs only if there is a combination of effective network monitoring, computer skills that are applied and utilitarian policy that is comprehensible. Figure 1 shows components of network performance management.

### *Network Analysis and Planning (NAP)*

In NAP, network monitoring software's are used to collect data for network management applications. Monitoring of network is important because it helps to capture all useful information of the network for control and management of network usage. Network devices are remotely located. It is not easy to monitor statuses of network devices because it is unusual for these devices to have direct connected terminals. This makes the network management application to be difficult. Techniques developed to help in the management of network usage make it easy for network administrators to monitor network usage on their network devices Wong (2000).

### *Network Modelling*

Network traffic modelling is used as the basic for the network applications and for capacity planning of network systems. Given the impact of poor choices in this arena, it is clear that the validity of the underlying models is of critical importance Wilson (2006). There are a wide number of mathematical models that could be used to model network traffic depending on the type of network to be modelled. Factors which are used to examine a network are enrolled directly from the fundamental traffic model.

### *Bandwidth Policy-Based Management*

The Policy based networking is the administration of a network system to allow different types of traffic such as data, voice and video to get bandwidth availability that is expected to serve the system's clients. Integrating data, phone and video traffic in the same system helps in testing organizations to oversee activities to avoid a situation where one administration blocks another. Utilizing policy statements, system network administrators can indicate which type of services to prioritize and at what times of day and on what parts of their Internet Protocol (IP)-based network. This type of administration is commonly referred to as Quality of Service (QoS). It is controlled with policy based networking.

Most policy based systems administration software requires a great deal and more definite and system mindful proclamation. As of now, the Internet Engineering Task Force (IETF) is drafting a standard policy framework and other related protocols, Yavatkar

*et al*. (2000; Astrudillo *et al*., 2011). Figure 2 shows components of a distinctive policy-based network and the components are pronounced as:

- A Policy Management Tool (PMT) at which strategies are entered, altered, or called from a Policy Repository (PR)
- Policy Decision Point (PDP): A server that recovers approaches from the arrangement archive and follows up on the strategies for the benefit of Strategy Requirement Focuses (PEPs)
- The Policy Enforcement Points (PEPs): These are switches, routers and other system devices that implement the policies, employing access control list, queue management algorithms and so on
- The PR: Server of policies which is used as a directory. It relies on the Lightweight Directory Access Convention (LDAP)

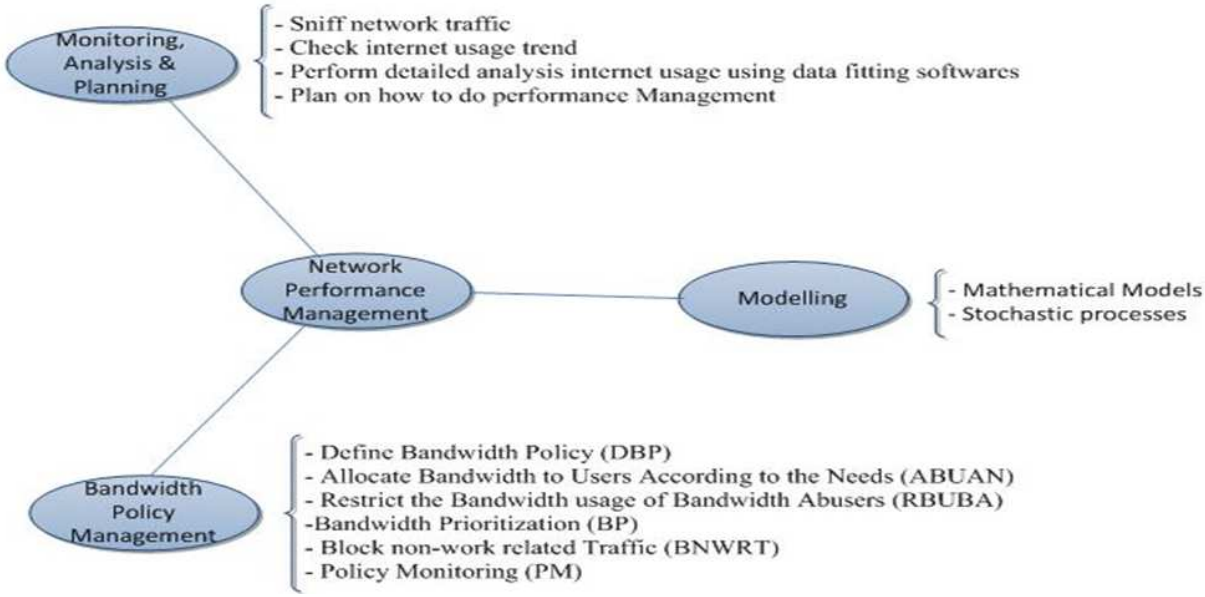


Fig. 1. Components of network performance management

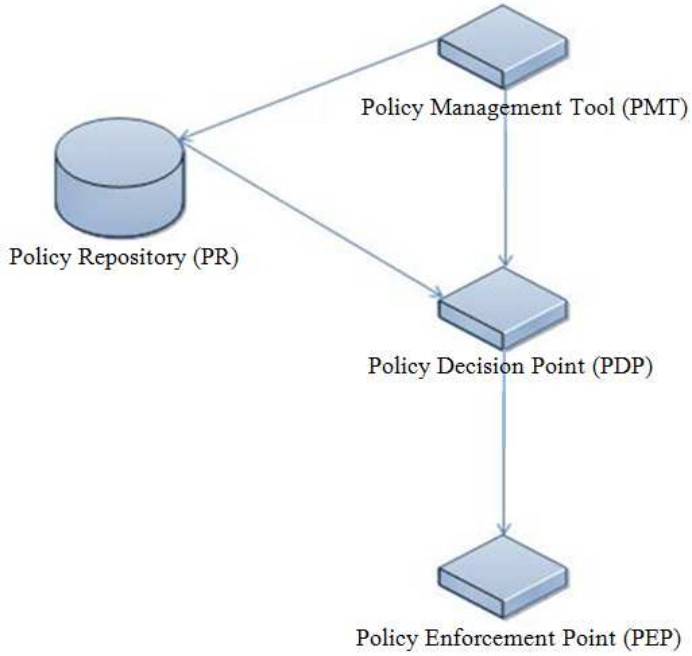


Fig. 2. IETF Policy-Based Management components

This research paper proposes the adoption of a Policy Creation Model that will be applied to a case of BIUST network. The adopted model is anticipated to address the requirements and needs of ICT department at BIUST and allowing the department to achieve wise bandwidth utilization in the campus network, which will greatly improve the research strength of the research intense university (BIUST). This study extends one of our researches in network traffic monitoring in BIUST network (Solomon *et al*., 2016). This will be archived through the following:

- Guaranteed bandwidth which is used for the intended purposes (Academic and research related)
- Reduced traffic congestion due to restrictions in bandwidth usage of bandwidth abusers
- Increased network efficiency in the campus network as required bandwidth is allocated to users according to the needs
- Increased worker's productivity as non-work related traffic will be block and required bandwidth will be allocated to work-critical users

This remainder of the paper is organized as follows: Section 2 describes related studies in bandwidth management through a policy based approach. Then in section 3, we present the adopted policy creation model and in section 4, the model is applied to a real scenario. Results and discussions are presented in section 5. Finally, in section 6, the conclusions are discussed.

## Related Work

In the course of recent years, the developing enthusiasm for the field of bandwidth management through a policy based approach is prove by a few innovative work endeavors in both the educated community and industry, working gatherings driving institutionalization endeavors, new specialized meetings and new ad items supporting strategy policy-based administration. In any case, utilizing bandwidth management policies as a part of network administration is not new; the original idea is known to have evolved in the early 1970s and the research was aimed to monitor and control the access rights of resources in large distributed systems (Gakio, 2006).

From that point forward, with the development of the Internet, the expanding complexities and heterogeneity of present technology innovations and the expansion of the network infrastructure to be overseen, it is not astonishing that the policy based approach to deal with computerizing network administration has turned out to be so mainstream. The policy based approach can be utilized to oversee diverse parts of a network, regularly known as policy disciplines.

A policy based bandwidth management designs and controls the different operational attributes of a network all in all, furnishing the network administrator with a streamlined, intelligently brought together and robotized control over the whole network.

A policy can be explained as "an unmistakable goal, course or strategy for activity to direct and decide current and upcoming choices." In overall, policies can be seen as arrangements of an organization to accomplish its goals. This may include an arrangement of guidelines to govern the behavior of its network and its components (users, applications, resources and so forth.) and the detail of an arrangement of activities to be executed.

As stated in some of the researches by Lymberopoulos *et al*. (2003; Snir *et al*., 2001), the IETF Policy working group outlined a framework for overseeing QOS inside network. They don't have a dialect for indicating policies. However, they are utilizing the X.500 catalog pattern. IETF policies are of the structure if < set of conditions > then do < a set of actions >. Directories are utilized for storing policies yet not for gathering subjects and targets, Lymberopoulos *et al*. (2003).

They don't have the ideas of subject and focus on that can be utilized to decide to which parts a policy applies, so the mapping of approaches to segments must be finished by different means (i.e., interface roles). Besides, they don't bolster strategy decides that can be powerfully activated by occasions to reconfigure the managed system as indicated by evolving situations. The policy work in the IETF is by all accounts concentrated just in the network layer and they have not considered the connection amongst application and network policy, Lymberopoulos *et al*. (2003).

In a study presented by Astrudillo *et al*. (2011), a novel model for creating management policies in telecommunications networks was presented. The proposed model incorporated actors, policy creation process, policy abstraction levels and a way for creating policies. Usage of the proposed model over the technology division at University of Cauca was then incorporated. The authors recognize actors or individuals that are included in the policy creation process and roles of them where classified. The proposed abstraction levels to oversee telecommunications network systems uncovered that policies cannot be seen as a solitary substance or statically, as in these new environments of dynamic network systems and particular prerequisites for every system client. The policies must be made and actualized at various levels inside the administration plane of the network system. A standout amongst the most critical results was policy creation method which permits creation through strides in every stage required in this procedure. Also, this procedure was linked with

policy abstraction levels and actors and an application illustration was created.

Another study by Mohammed *et al*. (2013a) presented a bandwidth management and optimization using a case study of Ahmadu Bello University (ABU) Zaria. A policy-based bandwidth scheme for ABU Zaria was used to articulate this work. A fibre-based STM-2 links was leased by ABU Zaria from Glo-1 to provide the university with a complete duplex bandwidth of 155 Mbps. The university had approximately 4000 student and staff. There was a fibre ring backbone network that links the three campuses at Samaru, Shika and Kongo. This involved 90-days of data collection and analysis of traffic data. Packet sniffer was also used for the advancement of the bandwidth optimization that is focused on policy-based strategies. The GNS3 was used for simulation of the effect of policies on a segment of the network. A small network was used to validate the results of the simulation. The outcomes proved that when the developed policies were brought about, bandwidth utilization decreased. It moved from 3.9 to 2.9 Mbps, saving 1.0 Mbps in bandwidth. This is an indication that when brought about on the live network, bandwidth management can be enhanced, Adami *et al*. (2001).

## Adoption of a Policy Creation Model

This study proposes the adoption of a policy creation model which was presented by Mohammed *et al*., (2013b) to be applied to a case of BIUST Network. Fortigate firewall was used for simulation of the effect of the policies on a segment of the network. The authentication of results of the simulation was done on the BIUST network. The pertinent steps of the adopted model are.

### *Define High-Level Abstract Policies*

The main thing to do in the policy life-cycle is to procure the necessities or administration prerequisites which are gathered by Policy Makers. Through this approach policies for bandwidth management will be created.

### *Specify High-Level Goals*

It states the goals to be obtained by the management system. It is significant to note that a goal approach is used to create policies. Therefore, it is important for the high-level goals that fulfill the necessities and requirements to be defined into the high-level abstract policies. Now define the high-level goal G 1-1: "Bandwidth optimized for both incoming and outgoing Internet traffic congestion "which represents the major objective to be obtained by the management system policies by Gakio (2006).

### *Define Sub-Goals*

It is in this step that the Sub-Goal (SG) extracts and generates a subtle distinction hierarchy. To get this done, there are things to be taken into consideration. These includes: Unlimited resources and information about the management environment. It is preferable to take into consideration the services, the sources consumed by each service and the priority to be prone to each resource, according to the role played in the institutional mission at the university.

Fig. 3 shows the refinement hierarchy generated for our particular case, while Table 1 gives detail of subject and targets contributions, where:

G 1-1: "Bandwidth optimized for both incoming and outgoing internet traffic “which represents the main objective that should be achieved by the management system.
SG2-1: Allow access to the Services and/or Applications.
SG2-2: Set a Bandwidth for Services and/or applications by defining thresholds (Minimum -Maximum).
SG2-3: Ensure a Bandwidth for Services and/or Applications.
SG3-1: Set a minimum bandwidth of 500Kbps for incoming and outgoing connections of computers that have urgent downloads.
SG3-2: Ensure Guarantee access to the VoIP server with high priority and guaranteed bandwidth of 5000 Kbps.
SG3-3: Ensure a bandwidth of 512 Kbps per connection for incoming and outgoing traffic of videoconference equipment.
SG3-4: Ensure a bandwidth of 512 Kbps for incoming connection to the Web Server.
SG3-5: Set the maximum bandwidth allowed per connection for outgoing traffic from Web Servers.
SG3-6: Set a lowest limit bandwidth of 1024 Kbps for ongoing traffic to crucial websites.
SG3-7: Guarantee a maximum bandwidth of 4000 Kbps for each connection for outgoing traffic from streaming servers.
SG3-8: Set a minimum bandwidth of 512 Kbps for incoming traffic to proxy servers.
SG3-9: Set a minimum bandwidth of 512 Kbps for outgoing traffic from proxy servers.
SG3-10: Allow web filtering to specify access for sites of different categories.
SG3-11: Deny access to restricted websites.
SG3-12: Allow priority use of network services for selected users/groups of users.

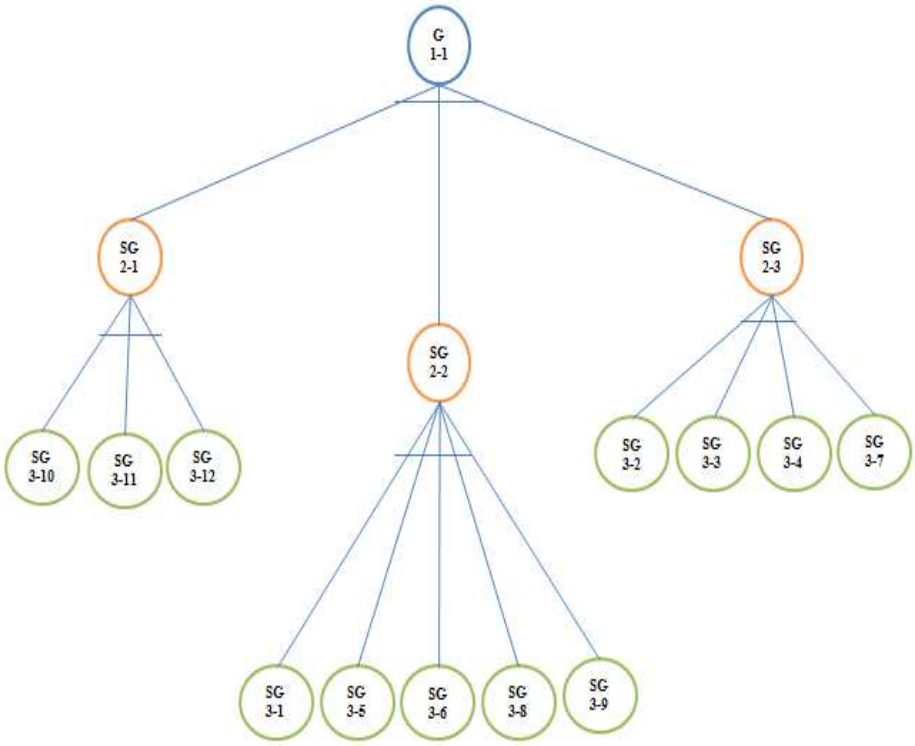


Fig. 3. Refinement Hierarchy

Table 1. Subject and targets

| | Contribution | | | |
|---|---|---|---|---|
| Sub goal | Source | Destination | Service | Time |
| $SG_{3\text{-}1}$ | Hosts with Important downloads | Any destination | All IP | Anytime |
| $SG_{3\text{-}2}$ | VoIP Server | Any destination | VoIP | Anytime |
| $SG_{3\text{-}3}$ | Videoconference Equipment | Any destination | All IP | Anytime |
| $SG_{3\text{-}4}$ | Web Servers | Any destination | All IP | Anytime |
| $SG_{3\text{-}5}$ | Any source | Any destination | All IP | Anytime |
| $SG_{3\text{-}6}$ | Any source | Any destination | Web applications All IP | Anytime |
| $SG_{3\text{-}7}$ | Streaming Servers | Any destination | All IP | Anytime |
| $SG_{3\text{-}8}$ | Any source | Any destination | All IP | Anytime |
| $SG_{3\text{-}9}$ | Proxy Servers | Any destination | All IP | Anytime |
| $SG_{3\text{-}10}$ | Web filtering | Any destination | All IP | Anytime |
| $SG_{3\text{-}11}$ | Any source | Any destination | All IP | Anytime |
| $SG_{3\text{-}12}$ | Selected users/groups of users | Any destination | | Anytime |

### *Generating Strategies*

Strategy is defined as a plan of action designed to achieve the overall aim or high-level goal. It can be converted in one or more mid-level policies. Therefore; it should allow low-level aims so as to obtain the high-level ones. The procreated strategy is named S1:

$$S1 = SG_{3-1}\Delta SG_{3-2}\Delta SG_{3-3}\Delta SG_{3-4}\Delta SG_{3-5}\Delta$$
$$SG_{3-6}\Delta SG_{3-7}\Delta SG_{3-8}\Delta SG_{3-9}\Delta SG_{3-10}\Delta$$
$$SG_{3-11}\Delta SG_{3-12}$$

### *Identify Conditions*

In this step, all conditions which aid each sub aim to be obtained on the system should be identified. This is done by taking into consideration the functionality that the system supports and ascertaining the source and place of traffic, the type of service and the time in which each sub goal is launched.

### *Identifying the Subject and Target*

It is worth noting that it is important to identify the subject and target that will be specified in the end of

policy rules. The subject is an individual unit or objects that are responsible for implementing the activities involved in the policy. The targets are elements influenced by the policy actions.

### *Define Policies which will be Deployed by the System*

It is preferable to describe this in a mid-level policy layout for this; it uses all the elements achieved in previous steps (for instance, sub goals, conditions, target and subject). The following defined policies are used to compose the strategy S1:

- P1 (Based on): If "the source address belongs to any host of pressing downloads group, Destination address is whichever, anytime 'Then' designate a minimum bandwidth of 512 kbps for both inbound and outbound connection to that computer and give a high priority (9)"
- P2 (Based on): If "the source address is the VoIP server, anytime 'Then' Guarantee access to the VoIP server with high priority and guaranteed bandwidth and designate a high priority (9)"
- P6 (Based on $SG_{3\text{-}6}$): If "the source address is whichever, destination address is one of the crucial websites, anytime 'Then' set a minimum bandwidth of 1024 Kbps"
- P7 (Based on $SG_{3\text{-}7}$): If "the source address is one of the streaming servers, destination address is whichever, anytime 'Then' Assure a bandwidth of 4000 Kbps per connection and designate a low priority (4)"
- P8 (Based on): If "the source address is whichever, the destination address is one of the representative severs, anytime 'Then' set a minimum bandwidth of 512 kbps and designate a middle priority (7)"
- P9 (Based on): If "the source address is one of the representative servers, destination address is whichever, anytime 'Then' set a minimum bandwidth of 512 Kbps and designate a middle priority (5)"
- P10 (Based on): Web filtering policy to specify access for sites of different categories
- P11 (Based on): Deny access to restricted websites
- P12 (Based on): Allow priority use of network services for selected users/groups of users

The ranges established to determine the priority assigned to each policy are as follows:

- From 1 to 4, low priority
- From 5 to 7, middle priority
- Finally from 8 to 9, high priority John and Morgan (2004)

## Results and Discussion

Figure 4 shows daily utilization of bandwidth in the BIUST network on 08.09.2015 before implementation of the policy. It had come to a concern that, around 0815 h (hrs.), much traffic is generated with maximum of 9821.893 Kbps. The curve also should rapid increase in traffic generated within 1451 and 1521 h as it increased from 2978.084 to 9048.664 Kbps at 1511 h and back to 3050.338 Kbps at 1521 h. Figure 5 shows daily bandwidth utilization in the BIUST network on 08.09.2016 after implementation of the policy. It was observed that, within the hours of 9:41, 11:00, 11:21, 12:00, 12:30, 13:45, 15:00 and 16:11, much traffic is generated, with maximum of 52.419 Kbps. When Fig. 5 is equated with Fig. 4, it has come to an attention that bandwidth is protected and pre-owned more carefully, as a result, optimization is obtained.

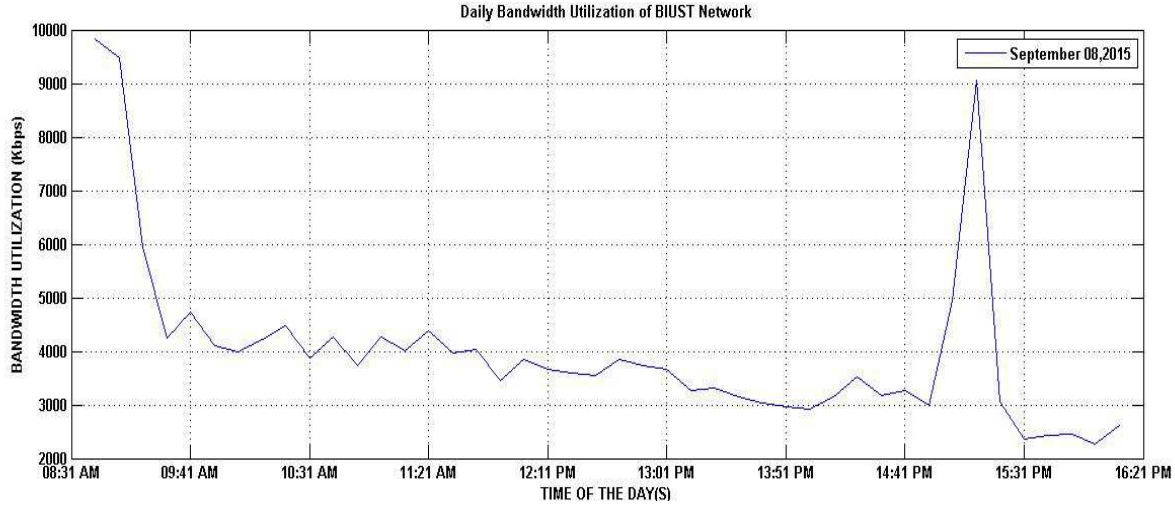


Fig. 4. Daily bandwidth utilization before policy implementation

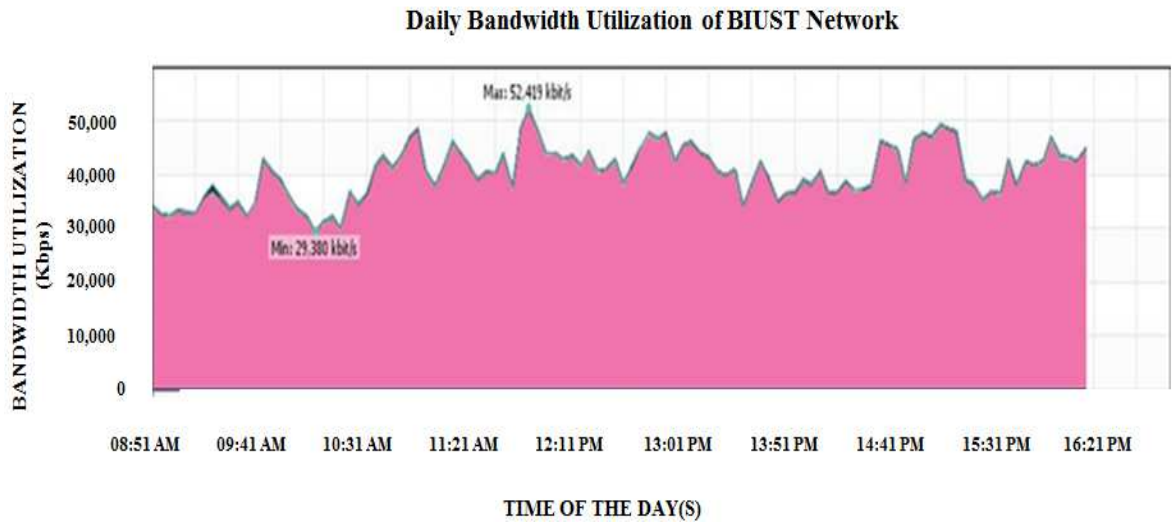


Fig. 5. Daily bandwidth utilization after policy implementation

## Conclusion

In this study, we proposed adoption of a policy creation model for policy making in an organization. The proposed approach has been applied in BIUST network and proved its efficiency based on presented results. Policy based networking is considered of awesome interest within research intense and academic universities due to its benefits of benefits of delivering consistent, correct and understandable network systems. Results obtained after policy implementation showed that there is the need for policy implementation in BIUST network system as bandwidth was conserved and used more efficiently as compared to results before the policy was implemented.

## Acknowledgement

I am very much grateful to the management of Botswana International University of Science and Technology (BIUST) for the sponsorship and their support throughout the research.

## Funding Information

This research was carried out within the frame of a master's project funded by BIUST.

## Author's Contributions

All authors contributed equally to the implementation of the present paper.

## Ethics

This article is original and contains unpublished Material, the corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues involved.

## References

Adami, D., M. Marchese and L.S. Ronga, 2001. TCP/IP-based multimedia applications and services over satellite links: Experience from an ASI/CNIT project. IEEE Personal Commun., 8: 20-27. DOI: 10.1109/98.930093

Astrudillo, C.A., A.M. Gustin and O.J. Calderon, 2011. Policy creation model for policy-based management in telecommunications networks. Proceedings of the IEEE Latin-American Conference on Communications, (ACC' 11).

Gakio, K., 2006. African Tertiary Institutions Connectivity Survey (ATICS). Gaborone, Botswana: Cyberplex Africa.

Lymberopoulos, L., E. Lupu and M. Sloman, 2003. An adaptive policy-based framework for network services management. J. Netw. Syst. Manage., 11: 277-303. DOI: 10.1023/A:1025719407427

Mohammed, S.B.A., S.M. Sani and D.D. Dajab, 2013a. Network traffic analysis: A case study of ABU network. Comput. Eng. Intell. Syst., 4: 33-40.

Mohammed. S.B.A., D.D. Dajab and M.B. Mu'zu, 2013b. Policy creation model for policy based bandwidth management in the core network (A case study of Abu data network). Int. J. Comput. Applic., 68: 1-6. DOI: 10.5120/11564-6855

Snir, Y., Y. Ramberg, J. Strassner and R. Cohen, 2001. Policy QoS information model <draft-ietf-policy-qos-info-model-03.txt>.

Solomon, T., A.M. Zungeru and R. Selvaraj, 2016. Network traffic monitoring in an industrial environment. Proceedings of the 3rd International Conference on Electrical, Electronics, Computer Engineering and their Applications, Apr. 21-23, IEEE Xplore Press, pp: 133-139. DOI: 10.1109/EECEA.2016.7470779

Wilson, M., 2006. A historical view of network traffic models.

Wong, E., 2000. Fundamentals of network monitoring.

Yavatkar, R., D. Pendarakis and R. Guerin, 2000. A framework for policy-based admission control. RFC.