Improving the Performance of a Network by Managing the Bandwidth Utilisation with squidGuard: A Case Study

[1]S. Akpah, [1]D. Mireku-Gyimah and [1]F. L. Aryeh
[1]University of Mines and Technology, P. O. Box 237, Tarkwa, Ghana

Akpah S., Mireku-Gyimah D., and Aryeh F. L. (2017), "Improving the Performance of a Network by Managing the Bandwidth Utilisation with squidGuard: A Case Study", *Ghana Journal of Technology,* Vol. 1, No. 2, pp. 9 - 17.

Abstract

The University of Mines and Technology (UMaT) has a Local Area Network (LAN) with a download and upload bandwidth capacity of 60 MB, which is connected to a Network Operating Center by fibre optic cable and distributed to about 3000 users in the UMaT community via Cat 6 Ethernet cables and wireless access connections. The primary purpose of the internet facility is to support teaching and learning, research and sharing of information. Unfortunately, even though the capacity of the bandwidth is considered sufficient, the LAN had two main challenges: the network appears to be slow; and sometimes it gave signals of insecurity from virus attacks. This paper seeks to study the behaviour patterns and bandwidth utilisation trends of the network users using Squid Analysis Report Generator; identify the causes of the challenges and deploy effective bandwidth management control policies using squidGuard. The results of the study revealed that the challenges of the LAN are attributable to: misuse of the bandwidth mainly by some students on low-priority, bandwidth-hungry websites and applications such as pornographic and other useless websites and peer-to-peer applications; and lack of effective bandwidth management control policies. After the installation of a squidGuard on the firewall server and definition of access protocols and policies to effectively monitor and control the network traffic by giving priority access to legitimate users and restricting access to low-priority, bandwidth-hungry websites and applications, there was a significant increase in the speed and security of the LAN. It is recommended that the installed software packages must be upgraded periodically to sustain the performance of the LAN; the bandwidth capacity could also be increased to 100 MB as the students' number increases.

Keywords: Local Area Network, Bandwidth Management Control Policies, Peer-to-Peer Applications

1 Introduction

Reliable internet connectivity has become a prerequisite for universities to provide quality education and undertake quality research works. This is made possible by the vast amounts of information available on the global information highway (Internet). Most universities including University of Mines and Technology (UMaT) continue to spend huge sums of money to increase their current bandwidth capacity and undertake network infrastructure upgrades. Despite these considerable investments, some universities continue to find themselves having unreliable and unusable internet access. This is mostly attributed to the annual increase in student enrolment, increasing use of electronic gadgets to enhance teaching and learning and the widespread use of desktop applications that practically consume any amount of available bandwidth. Other causes are as a result of the overreliance on peer-to-peer network traffic (Kondakci, 2003; Gummadi *et al*. 2003; Anon. 2002), which contains low-priority, bandwidth-hungry interactive contents filled with inappropriate web traffic and viruses, leaving the bandwidth hopelessly bogged down to a point when the network becomes slow and very insecure. As the usage of heavy bandwidth consuming applications continue to grow and the network usage patterns of users continue to change, there is a need for more resolute and well co-ordinated effort to monitor the usage patterns of users and implement effective bandwidth management strategies to improve Quality of Service (QoS) to the entire university community. In most cases, the ideal thing to do is to entirely restrict the usage of this strategic resource; however, restricting this altogether will lead to frustration on the part of end users. Since bandwidth is a strategic but scarce resource, priority must be placed on its efficient usage and management. Without effective bandwidth management, applications that are deemed critical and considered to have much academic worth would be starved of the available bandwidth thus disrupting services that impact the operational activities of these universities. The ultimate challenge is how to make available more bandwidth and how to manage the limited bandwidth in the most efficient way. Apart from the technical issues relating to bandwidth management, the biggest challenge is to continually advocate the importance of preserving this strategic resource (bandwidth) and the need to responsibly use it.

*Manuscript received December 28, 2016
Revised version accepted March 17, 2017

Bandwidth represents the capacity of a communication media used to transfer network packets from one point to another over a given time. This means that the wider the channel, the more the data packets that will be transmitted and vice versa. Bandwidth is usually expressed in bits per second (bps), kilobits per second (kbps), megabits per second (mbps) or gigabits per second (gbps). Various Internet Service Providers (ISPs) are offering different bandwidth standards at different prices. Currently most universities are struggling to have reliable, usable internet access. According to Rosenberg (2008), researchers and students can benefit immensely from good internet connectivity and collaborate with other international academic communities with a reliable information delivery chain. By this, the performance of an existing network infrastructure can further be enhanced by deploying a monitoring and control mechanism primarily known as bandwidth management. Bandwidth management is classified as the process of efficiently distributing and controlling bandwidth resources to mission critical applications on a particular network. The primary aim of bandwidth management is to improve network performance by monitoring and removing unnecessary web traffic. According to Sharma, *et al*. (2011), the goal of network management is to be able to apportion bandwidth to the right applications, at the right place and at the right time. Literally, bandwidth can be described as a hollow tube and if contents or materials inside the tube are not constantly monitored, the tube will be congested with inappropriate contents. Anon. (2009) describe bandwidth management as a process of controlling data packets on a network to avoid filling up the transmission medium which could result in network congestion, poor performance and network insecurity. Managing a bandwidth comprises defining and enforcing policies on a network to ensure that the right users are getting access for the right purposes and also ensure satisfactory network performance. It also ensures that bandwidth is not wasted on low-priority applications which consume much more bandwidth. Without clearly defined policies, technical solutions will be difficult to implement. Network policy frameworks are critical as they guide network usage; user access issues and other implementation procedures for technical solutions to be deployed. Implementing policy-based management strategies affords university network administrators the privilege to control the amount of bandwidth which should be allocated to which network services and resources. A policy-based framework can be an Acceptable Use Policy (AUP) document which defines acceptable procedures of network access, guidelines for dealing with network problems, appropriate sanctions to be applied and so on. These rules must be configured into the various network resources, most importantly, firewall servers or other devices. Further views shared by Rosenberg (2008) are that bandwidth management stems from three (3) key activities namely policy, monitoring and implementation. Rosenberg (2008) continues that the goal of efficiently managing bandwidth will be severely compromised should any one (1) of these key activities be missing from the process since each one of these activities are dependent on, and enforce, one another. According to Sharma, *et al.* (2011), due to the increasing number of network users, no amount of bandwidth can be said to be enough to satisfy the ever growing demands of the user community. It has therefore become very crucial to implement bandwidth usage policies to specify how the available bandwidth should be allocated to support the core mandate of the university. Making sure that the available bandwidth is widely accessible to the entire university community requires the commitment from all stakeholders to drive home the need to deploy policy frameworks on the existing campus network. This paper proposes an approach that places emphasis on deploying appropriate network policies to encourage proper bandwidth saving practices among all users. It also proposes ways to control and manage the many noncritical, bandwidth-hungry applications that consume majority of bandwidth that is available. The ultimate goal is to ensure that mission critical applications and services are carried out as efficiently as possible.

The aim of this paper is to study the challenges of the network on UMaT campus that affect its speed and security and propose efficient bandwidth management control policies to assist the network administrators to improve the performance of the network.

The paper sought to answer the following questions:

(i) What is the current state of the Internet connectivity at UMaT?
(ii) What are the UMaT bandwidth usage trends and the behaviour patterns of network users?
(iii) What bandwidth management strategies are deployed at UMaT and their effectiveness?

The significance of the study lies in the fact that the outcomes would assist the university authorities to formulate and implement bandwidth management strategies to improve network performance by eliminating unnecessary traffic and making internet access available to all legitimate users.

2 Resources and Methods Used

2.1 Resources

The UMaT Internet Infrastructure, the users comprising students and staff, Squid Analysis Report Generator (SARG) and squidGuard are the main resources used for this study.

The study was conducted at UMaT campus which is located at Tarkwa, 89 kilometers from Takoradi, the Western Regional capital of Ghana, West Africa. Currently UMaT has two Faculties, namely: the Faculty of Mineral Resource Technology (FMRT), which has six (6) academic departments and the Faculty of Engineering (FOE), which has four (4) academic departments. There are also the School of Postgraduate Studies (SPS) which coordinates all activities of postgraduate education and the Center for Communication and Entrepreneurship Skills (CENCES) which currently serves as the nucleus of the future Faculty of Integrated Management Sciences. Apart from FMRT, FOE, SPS and CENCES, the internet infrastructure is extended to the Administration Block, UMaT Basic School, the clinic, the Maintenance Unit, the University Radio Station, the three (3) Student Halls on campus and one (1) Student Hall off-campus which is about 2 km away.

The UMaT Network Architecture is shown in Fig. 1. It spans a maximum distance of approximately 1.39 km. The main LAN backbone which is located at the Network Operation Centre (NOC) also doubles as the main base station. The Internet Service Provider (ISP) provides a point to point internet connection with download and upload bandwidth stream of 60 MB which is connected by fiber optic cable to an AN-FM-PCM30 switch. It is then connected by Cat 6 Ethernet cables to a LAN switch. The LAN switch is then connected by Cat 6 Ethernet cables through a Trendnet 24 port switch to a Linux box which serves as a firewall and doubles as a Proxy Server. The LAN is connected by way of Cat 6 ethernet cables through an Hp Procurve switch to the Proxy Server, Mail Server and Application server. The LAN backbone then serves as a transmitter by receiving network signals from the main NOC and appropriately transmits them to the other base stations located at their respective points. A Cisco Aironet 1300 wireless bridge/access point with 12 dBi omni-antenna serving as the WLAN base station is connected to the LAN switch to bridge all the other six (6) Cisco Aironet 1300 outdoor units. At these six locations, the Cisco Aironet 1300 bridges are connected directly to one of the ethernet ports of a Dynamic Host Control Protocol (DHCP) server with two (2) network cards performing IP Address distribution and Network Address Translation (NAT). The LAN is further extended using wireless network adaptors via Access Points to mobile users.

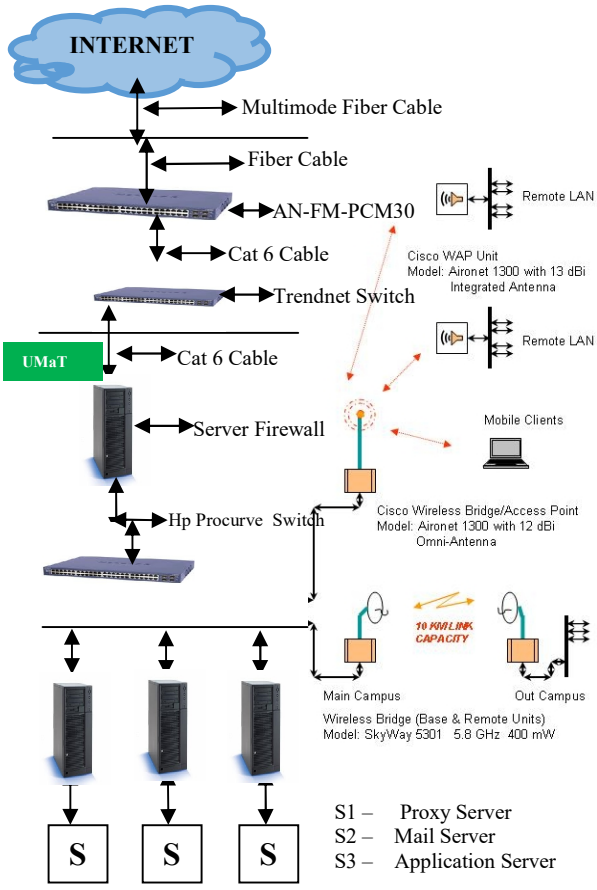

Fig. 1 UMaT Network Architecture

2.2 Methods Used

The analysis of the bandwidth usage trends and behaviour patterns of network users was undertaken using Squid Analysis Report Generator (SARG) which, according to Ravi (2015), is an open source squid proxy log analysis tool which analyses web based log files and generate reports based on the bandwidth consumption rates of users. This was done by logging all user access to the network over a period of six (6) weeks. The bandwidth usage reports generated over the period revealed credible facts that supported the need for the implementation of bandwidth management control policies to help prioritise academic and research related activities. The generated reports were classified as follows; productive applications (contain much academic worth) and unproductive (personal, non-academic and non-research related) activities which included all the applications that consume practically any amount of bandwidth. A second open source software known as squidGuard

was installed. According to Haland (1998), squidGuard which is a Uniform Resource Locator (URL) redirector software was used to control web contents accessed by users on the Proxy Server. It was integrated into the firewall environment to implement blacklist rules and content control by defining sites for which access may be redirected or restricted entirely.

2.2.1 Data Analysis

Detailed analysis was performed on the user log files that were generated with the help of the SARG over the monitoring period. The analysis was grouped as follows:

2.2.2 Peer-to-Peer (p2p) Analysis

To efficiently monitor all p2p web traffic on the network, a policy was defined and configured into the firewall to analyse and derive the impacts of p2p activities within given intervals throughout the monitoring period. The results showed the prominence of p2p activities on the network and the time of the day that they were more prominent. Fig. 2 identifies the nodes with the highest p2p activities and Fig. 3 shows the prominence of the p2p activities.

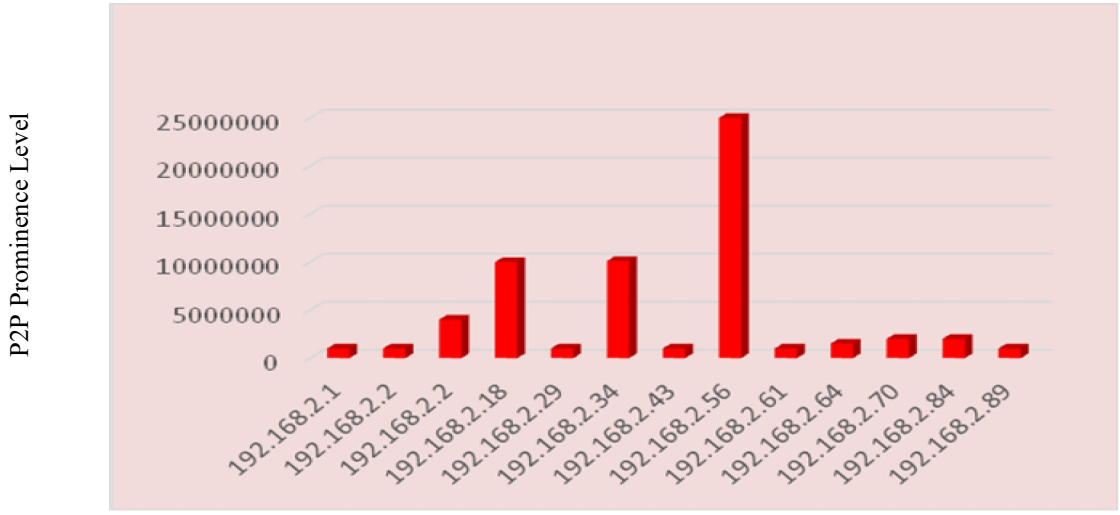

Fig. 2 Distribution of P2P Activities Across Computers

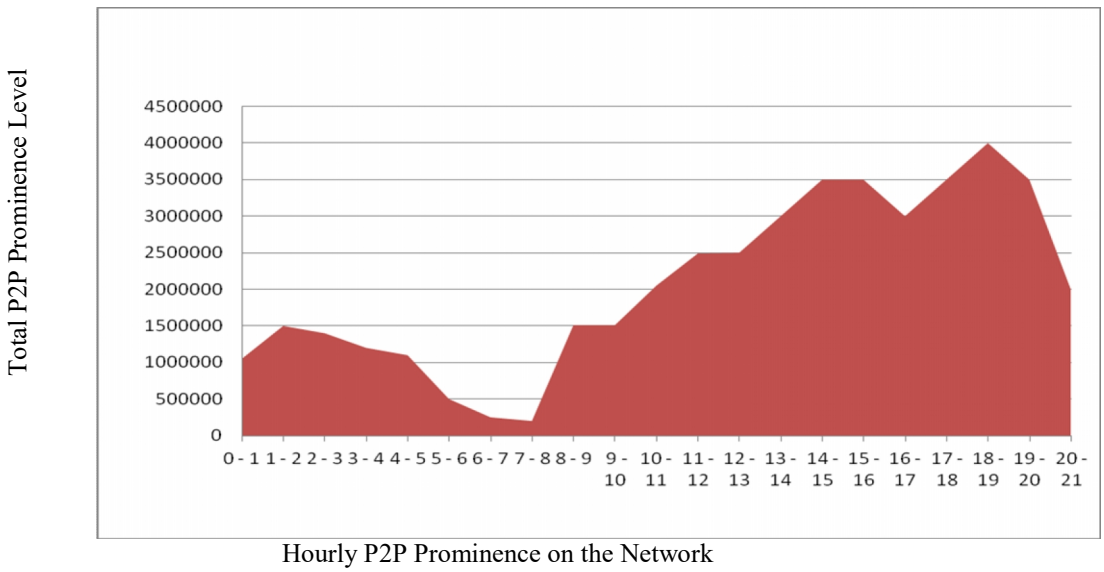

Fig. 3 Total P2P Activity Over the Period

2.2.3 Bandwidth Traffic Analysis

Bandwidth traffic usage statistics of all user activities were logged by the SARG throughout the monitoring period. This enabled the researchers to ascertain the total bandwidth (upload plus download) consumed by each user throughout the period. Determining the overall traffic distribution across the entire network was also made possible at various times of the day. Fig. 4 shows the total bandwidth clearly indicating the peak traffic period. Fig. 5 shows all the nodes that contributed to the overall traffic distribution.

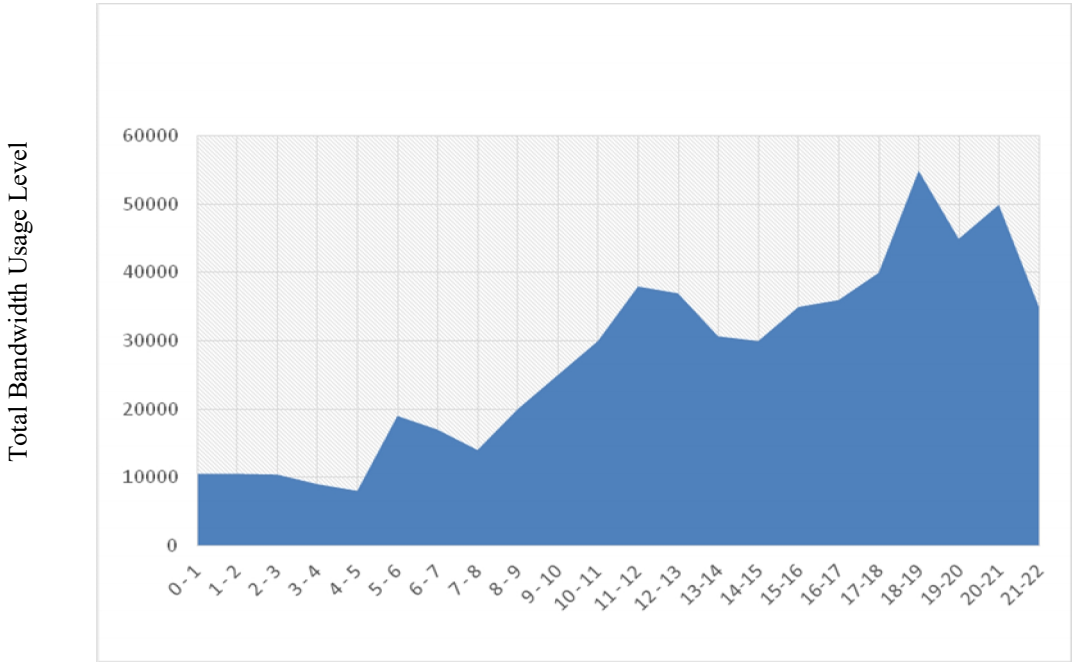

Fig. 4 Total Bandwidth Traffic by Time of Day

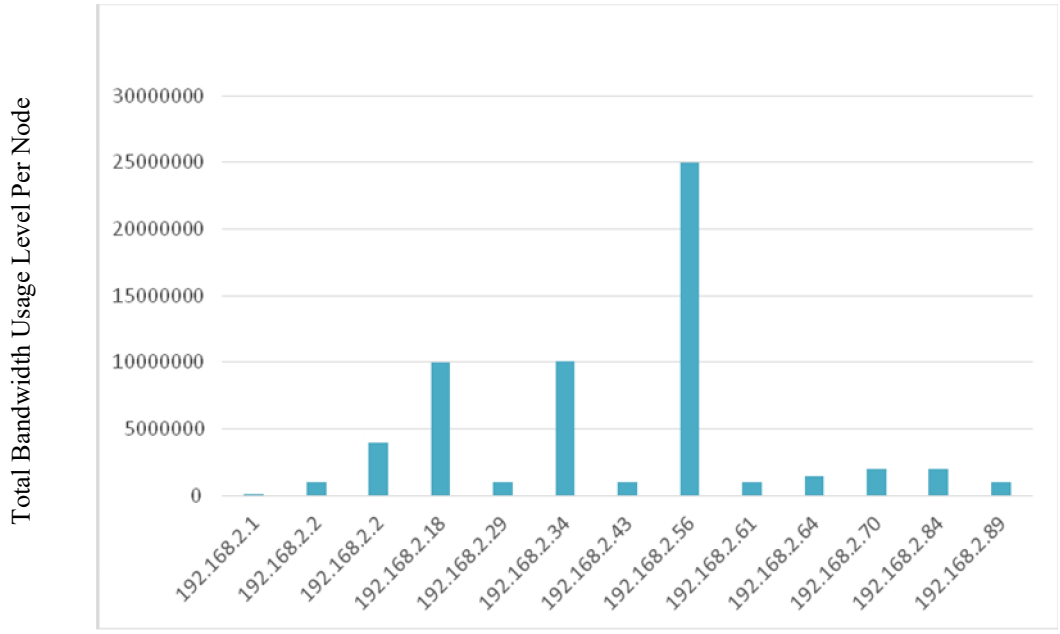

Fig. 5 Total Traffic Across All Nodes

2.3 URL Analysis

A web proxy server was setup on the network to relay URL requests from clients to the server and vice versa. This enabled the network administrators analyse URL logs which gave unobtrusive insights to the behavior patterns of network users and also provided an overview of the internet usage on campus. The analysis further revealed popular URLs visited by users on the network within the monitoring period. Table 1 shows a list of some of the most popular internet utilities accessed by users on the network. Fig. 6 shows the domain names with the highest hits throughout the monitoring period. Table 2 shows a list of some websites and applications that were considered to be productive and unproductive.

Table 1 List of Most Popular Internet Utilities

Most popular mail servers	GMail, Yahoo Mail, UMaT Mail
Most popular search engine	Google
Most popular news sites	Peacefmonline.com, myjoyonline.com, bbc.com, yahoo news
Most popular computer brands	Hp, Dell and Lenovo
Most popular Instant Messaging Platforms	Whatsapp, Skype, Facebook,

Table 2 List of Productive and Unproductive Websites and Applications

Productive Apps	**Unproductive Apps**
Dreamweaver	Kazaa
Arc GIS	Bit Torrent
Whittle	Freecast
Surpac	Limeware
Microsoft Visual Studio	Shareaza
Arc Info	UTorrent
Ilwis Software	Whatsapp
MatLab	
Productive Websites	**Unproductive Websites**
Googlescholat.com	Facebook.com
Slideshare.com	Youtube.com
Google.com	Pornographic Websites
UMaT Library Websites	Dating Websites
News Websites	Hacking Websites
Amazon.com	Gambling Websites
Ghana Institute of Engineers Website	Online Market Websites
Australian Institute of Engineers Website	Ocultic Websites

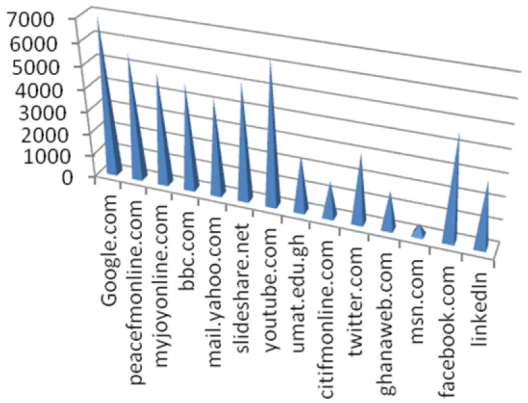

Fig. 6 Domain Names with Highest Hits

3 Results and Discussion

The results as presented by the SARG show the list of users who accessed the network during the monitoring period. It also depicted clearly the total amount of bandwidth consumed by the topmost users in that order. Fig. 7 shows the total bandwidth consumption rates of the users. It also shows the various URLs accessed by a particular user and the number of times the user accessed that particular website, the amount of bandwidth consumed by a particular website and the time spent accessing webpages on the website.

Squid User Access Report
Period: 2015 May 25
Sort: bytes, reverse
Top users

USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	
192.168.0.63	62.98K	2.29G	10.39%	80.72%	19.28%
192.168.0.61	63.60K	1.98G	9.00%	79.36%	20.64%
192.168.0.51	56.08K	1.94G	8.80%	82.69%	17.31%
192.168.0.60	57.62K	1.91G	8.67%	78.39%	21.61%
192.168.0.53	54.43K	1.86G	8.44%	81.02%	18.98%
192.168.0.62	53.38K	1.66G	7.54%	77.22%	22.78%
192.168.0.50	51.24K	1.64G	7.46%	77.27%	22.73%
192.168.0.58	64.95K	1.49G	6.79%	58.05%	41.95%
192.168.0.64	40.23K	1.24G	5.66%	79.72%	20.28%
192.168.0.52	40.12K	1.21G	5.50%	77.82%	22.18%
192.168.0.59	64.93K	1.20G	5.45%	66.99%	33.01%
192.168.0.55	54.73K	970.83M	4.40%	70.90%	29.10%
192.168.0.57	46.92K	874.34M	3.96%	57.10%	42.90%
192.168.0.56	40.45K	852.87M	3.87%	78.26%	21.74%
192.168.0.54	19.26K	497.52M	2.26%	72.60%	27.40%
192.168.0.65	14.63K	386.71M	1.75%	71.85%	28.15%
192.168.0.46	475	17.43M	0.08%	0.00%	100.00%
192.168.1.9	2	7.35K	0.00%	0.00%	100.00%
192.168.1.13	2	251	0.00%	0.00%	100.00%
TOTAL	786.10K	22.06G		75.70%	24.30%
AVERAGE	41.37K	1.16G			

Fig. 7 Total Bandwidth Consumption Rates

The reports generated by the SARG helped in analysing all nodes which were prominent with p2p activities. As depicted in Figs. 2a and 2b, three (3) nodes with IP addresses 192.168.2.3, 192.168.2.34 and 192.168.2.56 were classified the highest when it comes to p2p activities. The analysis also helped the network administrators to uncover that the intensity of p2p activities starts around 10:00 am and peaks around 5:00 pm getting to the close of work. This continues to somewhere around 9:00 pm before reducing around 11:00 pm as depicted in Figs. 3a and 3b. After clearly understanding the behaviour patterns of users on the network, the squidGuard helped define access control rules on the Proxy Server to blacklist or whitelist access to websites which were deemed not to have much academic worth thus such websites were either redirected or entirely blacklisted. The squidGuard also helped the network administrators to define time schedules which controlled time periods within which users especially students could gain access to certain websites. Websites such as Tumbir, Twitter, Pinterest, Twoo, Google+, etc, which are deemed to consume a lot of the bandwidth were redirected to the UMaT webpage. Other low-priority websites and applications such as pornographic websites, peer-to-peer file sharing software (i.e. BitTorrent, uTorrent, Tribler, Babelgum, etc), websites with aggressive and abusive contents, gambling, alcohol and drug related contents just to mention a few were completely blacklisted. Fig. 8 shows a pornographic website redirected to the UMaT webpage whilst Fig. 9 shows a pornographic website completely blacklisted.

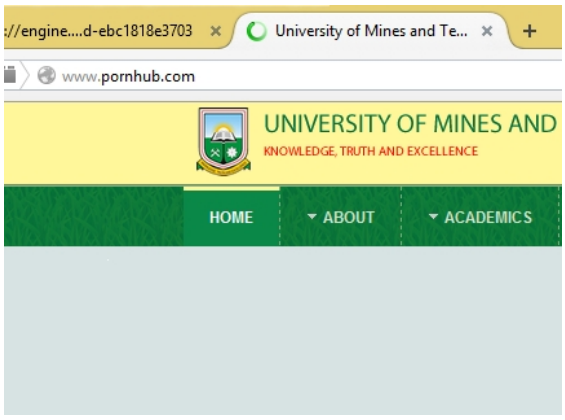

Fig. 8 Redirected Pornographic Website

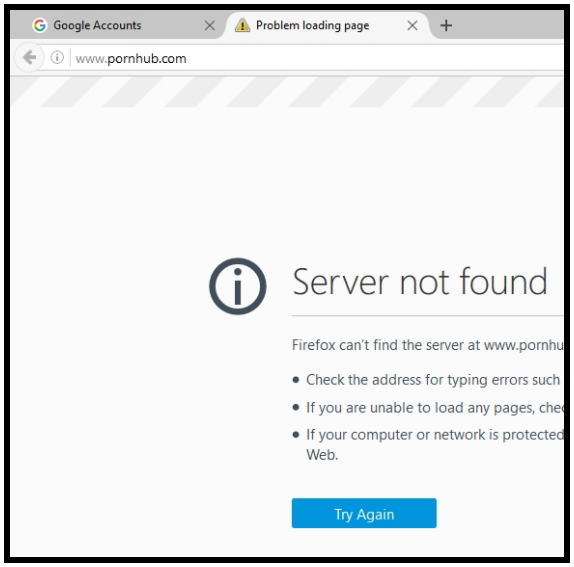

Fig. 9 Completely Blacklisted Website

Results from the research clearly showed that even though the network administrators on UMaT campus deploy some techniques to control access and manage the bandwidth, the users especially students are always finding new ways to overcome this hurdles.

3.2 Suggested Useful Practices

From the foregoing discussions, it is clear that there was an urgent need to block certain websites or web applications. All social media websites, p2p file sharing applications, chatting websites, were whitelisted and redirected to the university's website. All whitelisted websites must be redirected during working hours between the hours of 8:00 am to 5:00 pm, Pornographic, dating, hacking, gambling, tobacco, abusive websites were to be completely blocked. It is also proposed that updates of applications such antivirus and operating system be scheduled for late hours where normal working hours are over. To minimize unnecessary network traffic and make available more bandwidth to the entire university community, it is also proposed that the network administrators make adequate use of the Proxy Server, Mail Server and Application Server. The following are worth noting:

1) The Proxy Server or a web cache proxy server provides proxy and cache services for Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), File Transfer Protocol (FTP), and many other protocols. It also reduces bandwidth congestion and improves response times by caching and reusing frequently-requested web pages. It is able to act as an intermediary by passing the client's

request on to the server and saving a copy of the requested object. This will reduce the amount of bandwidth used by clients and go a long way to save the institution money and keep the bandwidth requirements lower and more manageable.

2) The Institutional Mail Server receives incoming emails from local users (people within the same domain) and remote senders and forwards outgoing emails for delivery. UMaT can use its domain email addresses (i.e.flaryeh@umat.edu.gh) as their primary email service as compared to other email services such as yahoo.com, hotmail.com, inbox.com, iCloud mail, just to mention a few which consume greater portions of the university bandwidth due to the numerous multimedia adverts they display.

3) It is also proposed that the UMaT put in place a Network Acceptable Use Policy which will provide detailed guidelines on network user access and usage. The policy must be used to determine and govern issues such as:
   (i) Using the LAN for the core purpose for which it was put in place;
   (ii) Monitoring the internet usage patterns and enforcing the appropriate sanctions where necessary; and
   (iii) Protecting all campus computers connected to the LAN from virus and spam attacks.

4) The Application Server can also be used to host a number of applications that network users can fall on when needed without necessarily accessing the internet for such applications. This will also help to reduce unnecessary load on bandwidth during peak hours.

4 Conclusions and Recommendations

4.1 Conclusions

From the study, the following conclusions were drawn:

Even though UMaT has a good LAN infrastructure and sufficient bandwidth, there were two (2) main challenges:
(i) The network appeared to be slow; and
(ii) The network gave signals of insecurity.

The challenges were attributable to two (2) main issues:
(i) Misuse of the bandwidth mainly by some students on low-priority, bandwidth-hungry websites and applications; and
(ii) The lack of effective bandwidth management control policies.

After the installation of the squidGuard the problems were eradicated, resulting in better performance of the network, specifically:
(i) The speed of the LAN increased significantly; and
(ii) The security of the LAN was also improved.

4.2 Recommendations

From the work that has been carried out, the following are recommended:

(i) The installed software packages should be upgraded periodically; and
(ii) Even though the upload and download capacity of 60 MB is considered sufficient, UMaT can consider increasing the bandwidth of the LAN to at least 100 MB. This will effectively cater for the annual increase in student enrolment for the next five years after which time another upgrade can be considered.

References

Anon. (2010), "The Need for Bandwidth Management: Taking Control of your Internet Connection". *http://www.internetwk.com/links-/elron.html* Accessed: August 5, 2016.

Anon. (2002), Peer-to-Peer File Sharing: The Impact of File Sharing on Service Provider Networks, *Industry White Paper.* Sandvine Inc., Ontario, 29 pp.

Anon. (2009). "Bandwidth Management and Traffic Optimization", *http://dualwan.org/ bandwidth-management.html.* Accessed: Oct 8, 2016.

Gummadi, K. P., Dunn, R. J., Saroiu S, Gribble, SD, Levy, HM and Zahorjan, J. (2003), Measurement, modeling, and analysis of a peer-to-peer file-sharing workload. *In SOSP'03: Nineteenth ACM Symposium on Operating Systems Principles*, 2003, pp. 314–329.

Haland, L. E. (1998), "pfSense - Squid + Squidguard / Traffic Shapping Tutorial", *https://www.howtoforge.com/pfsense-squid-squidguard-traffic-shaping-tutorial,* Accessed: September 17, 2016.

Kondakci, S. (2009), "A concise cost analysis of Internet malware". *Computers & Security*, Volume 28, Issue 7, October 2009, pp. *648-659.*

Sharma V., Kumar, V. and Thakiu, B. S. (2011), Need of Bandwidth management and

formulation of policy framework for Effective utilisation of Internet services within a University campus. *International Journal of Computer Science and Communication* 2(1), pp. 173-178.

Rosenberg, D. (2008), "Evaluating Electronic Resource Programmes and Provision: Case Studies from Africa and Asia, INASP Research and Education Case Studies, 3", *www.inasp.info/file/c85e1f2bd439dd5aa2c350814e81c4cf/evaluating-electronic-resource-programmes-and-provision-case-studies-from-africa-and-asia.html*, Accessed: September 10, 2016.

Ravi, S. (2015), "Squid Analysis Report Generator and Internet Bandwidth Monitoring Tool", *http://www.tecmint.com/sarg-squid-analysis-report-generator-and-internet-bandwidth-monitoring-tool*, Accessed November 7, 2016.

Authors

S. Akpah is an Assistant Lecturer at the Computer Science and Engineering Department of the University of Mines and Technology. He holds a BSc and MSc in Information Technology from Ghana Technology University College and Kwame Nkrumah University of Science and Technology respectively. His research interest inludes Local Area Network Infrastructure Design and Deployment, Wireless Securities and Open Source Firewalls.

D. Mireku-Gyimah is a Professor of Mining Engineering and a Consulting Engineer currently working at the University of Mines and Technology, Tarkwa, Ghana. He holds the degrees of MSc from the Moscow Mining Institute, Moscow, Russia, and PhD and DIC from the Imperial College of Science, Technology and Medicine, London, UK. He is a member of Institute of Materials, Minerals and Mining of UK and New York Academy of Sciences and also a fellow of Ghana Institution of Engineers and the Ghana Academy of Arts and Science. His research and consultancy works cover Mine Design and Planning, Mine Feasibility Study, Operations Research, Environmental Protection and Corporate Social Responsibility Management.

F. L. Aryeh is an Assistant Research Fellow at the Computer Science and Engineering Department of the University of Mines and Technology. He holds a BSc in Statistics and Computer Science from the University of Ghana and an MSc in Information Technology from Kwame Nkrumah University of Science and Technology. His research interest inludes Wireless and Wired Network Securities, Web Applications and Internet Technologies.