RUFORUM Working Document Series (ISSN 1607-9345) No. 14 (2): 215-219
Available from *http://repository.ruforum.org*

Research Application Summary

A mechanism for controlling incoming Internet Traffic into Multi service Networks

Kato, J.
Regional Universities Forum for Capacity Building in Agriculture (RUFORUM) Plot 151/155 Garden Hill, Makerere University Main Campus, P. O. Box 16811, Kampala, Uganda
Corresponding author: j.kato@ruforum.org

Abstract

Controlling of incoming internet traffic is very challenging in today's computer networks because network administrators have limited control over incoming traffic. Prioritizing incoming traffic in public institutions such as universities is challenging as students often tend to misuse internet by initiating a lot of traffic with non-academic interaction including downloading entertainment materials such as movies amidst limited bandwidth for those focused on research. The Explicit Congestion Notification mechanism enables the Universities' network administrators to control incoming internet traffic without help from the Internet Service Provider (ISP) as well as installing special devices on the network. The low priority traffic is controlled before leaving the sender by tricking the sender to think that the network is congested by using Explicit Congestion Notification (ECN) signal and adjusting the congestion window size of the low priority traffic. This will free bandwidth for high priority traffic needs such as research. This mechanism has proven efficient in securing and making available 80% of the total bandwidth for high priority traffic.

Key words: High priority traffic, low priority traffic, Transport Control Protocol

Résumé

Le contrôle du trafic Internet entrant est très difficile dans les réseaux informatiques d'aujourd'hui parce que les administrateurs de réseau ont un contrôle limité sur le trafic entrant. Prioriser le trafic entrant dans les institutions publiques telles que les universités est difficile comme les étudiants ont souvent tendance à abuser de l'internet en initiant beaucoup de trafic qui sortent du ressort académique y compris le téléchargement de matériel de divertissement tels que les films au milieu de la bande passante limitée pour ceux qui sont axés sur la recherche. Le mécanisme explicite de notification de congestion permet aux administrateurs réseau des universités de contrôler le trafic Internet entrant sans aide du fournisseur de services Internet (ISP), ainsi que l'installation de dispositifs spéciaux sur le réseau. Le trafic de faible priorité est contrôlé avant de quitter l'expéditeur en incitant l'expéditeur de penser que le réseau est congestionné en utilisant un signal de notification explicite de congestion (REC) et en ajustant la taille de la fenêtre de congestion du trafic de faible priorité. Ceci va libérer la bande pour les besoins de trafic hautement prioritaires tels que la recherche. Ce mécanisme a prouvé son efficacité dans la sécurisation et la mise à disposition de 80% de la bande totale pour le trafic de haute priorité.

Mots clés : Trafic de haute priorité, trafic de faible priorité, protocole de contrôle du transport

Introduction

In multi-service computer networks, the nature of internet traffic directed to most of universities networks has greatly changed (Guo *et al.*, 2004; Sairam *et al.*, 2010). An increase of multimedia traffic such as: the transfer of large video and audio files, video conferencing, online games, and streaming videos, among others, has brought competition for the limited bandwidth often available in universities (Saad, 2004). There is limited effort within organizations on controlling incoming internet traffic as network administrators often tend to focus outgoing traffic through permanently blocking unwanted traffic.

Makerere University, a premier university in Uganda, operates a multi-service internet and computer networks system to facilitate its robust internet dependence with in the ten colleges and several administrative units. The University decentralized internet service management under the Directorate of Information, Communications and Technology Support (DICTS) serves as a central coordinating unit. Accordingly, each college prioritizes traffic differently depending on the niche areas. For example The College of Computing and Information Science (CoCIS) considers real time traffic (video and voice conferencing) more critical traffic than other types of traffic, while other Colleges may consider Simple Mail Transfer Protocol (SMTP) traffic more important than real –time traffic (Joachim, 2004).

Makerere University has over 35,000 students with a growing emphasis on the utilization of on-line learning and remote computer access within the university. As such the density of computers within the university has increased and so has internet use and demand. However, like in many universities in the developing world, Makerere University and its constituent colleges is faced with the challenge of internet rationalization due to limited bandwidth. Further, the youthful population in the universities often tend to shift their priorities to low priority traffic (Saad, 2004). The recent surge in the utilization of the Transport Control Protocol (TCP) supported applications such as Gnutella, Napster and Bit Torrent have put a huge burden on most universities networks as these distort bandwidth available for high priority traffic (Sen, 2004, Saroiu *et al.,* 2012). Accordingly universities have to innovate on how to protect the central focus of universities as research institutions and thereby make the limited internet bandwidth available for high priority traffic activities such as research and innovatively control low traffic internet access without affecting system performance. This study focused at controlling the low traffic before it leaves the sender side.

Methodology

The Transport Control Protocol (TCP) used to control the flow of low priority traffic by using Explicit Congestion Notification (ECN) signal was used in this study. The ECN has the ability to confuse the sender of low priority traffic to think that there is congestion on incoming link and reduce on the sending rate by adjusting the congestion window size by half (Jacobson, 1988; Saad, 2004). Proposed proxy flow control mechanism focuses on controlling the inbound traffic by tempering with the window size on every acknowledgement coming from low priority traffic. The receiver of low priority traffic advertises on each TCP acknowledgement the available space in its input buffer using a 2 byte field window size. In situations where the low priority traffic is using more than allocated bandwidth, the algorithm will control the low priority traffic and allow high priority traffic bandwidth users access to adequate internet. This is operationalized by algorithm either increasing or decreasing the coefficient of scale that will in turn increase or reduce the advertised window size of the low priority traffic.

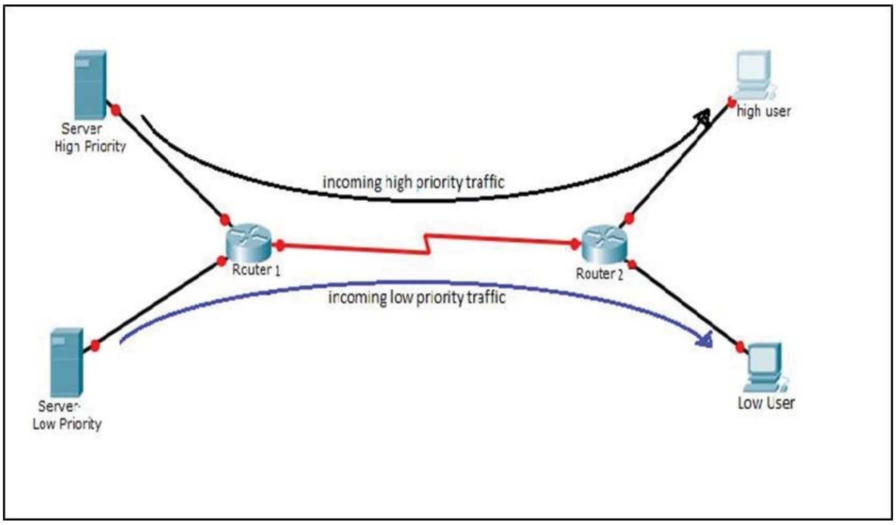

Figure 1: Shows the Network Topology

A network model is presented in Figure 1: the black arrow represents a flow of high priority traffic and blue arrow represents a flow of low priority traffic into a university network. Most administrators focus on controlling incoming traffic at the edge router (Router 2) inside the network. This however is a poor decision because the low priority traffic would have already consumed the limited bandwidth on the main link before being dropped at the edge router (Router 2). Controlling low priority traffic before leaving the server offers the best bet solution as it would limit the flow to low priority traffic on the main link (Router 1 – Router 2). In this study, the focus was on reducing the flow rate of low priority traffic before consuming the bandwidth on the main link. The Explicit Congestion Notification signal was used to control the incoming traffic. In ECN framework, when the Router 2 described above detects a congestion build-up on the network, it marks all the packets in order to signal the sender of low priority traffic of emerging congestion. The receiver of the low priority traffic sends a Congestion Experienced (CE) signal on the TCP acknowledgments to the sender who reacts appropriately to Congestion Experienced (CE) signal. This technique tricks the sender of low priority traffic by making the user feel that the incoming link is congested. In that regard, should the sender react to the ECN signals, it will then be possible to slow down the sending rate of the low priority traffic by setting the ECN-Echo flag on TCP acknowledgments. The fake ECN controller tampers with the TCP flags instead of tampering with the window size field (Saad, 2004).

Results and discussion

Three focus actions: target horizontal line, No Action, and Explicit Congestion Notification (ECN) curves are presented in Figure 2. The target horizontal line illustrates a percentage of bandwidth targeted to allocate to high priority traffic and targeted percentage is 80% of the total bandwidth. The ECN curve showed an improvement in bandwidth allocation to high priority traffic when the mechanism was applied as the no action curve tended to move along the horizontal line with increase in time. Further, as time increased from 0 to 39 seconds, the high priority traffic consumed over 81% of the total bandwidth. It was also noted that an increase of time from 40 to 76 seconds led to 78% of bandwidth dedicated to high priority traffic. Time-bandwidth allocation generally fluctuated within the system.

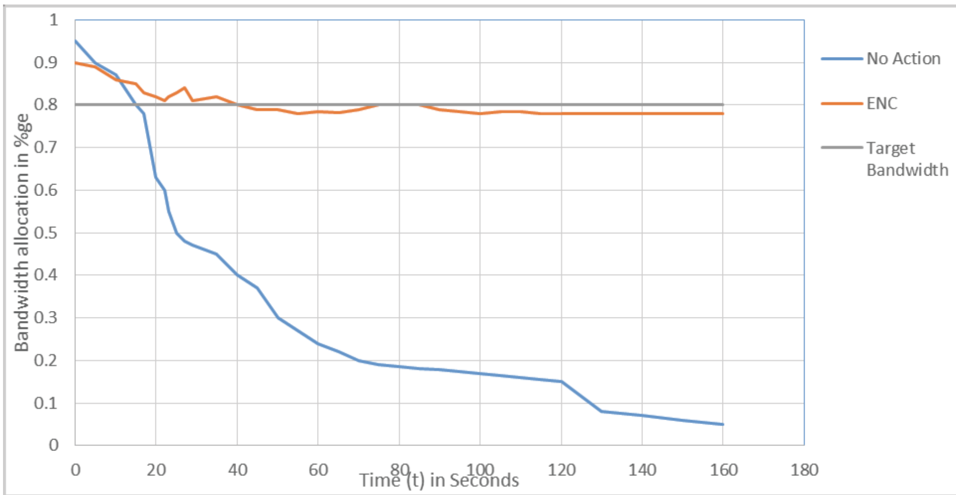

Figure 2: Bandwidth allocation to high traffic priority with increase in time

Research application

This study has shown that high priority traffic consumed more bandwidth than the targeted bandwidth (0 – 39 seconds), hence affecting low priority traffic's quality of service. There is need to improve the performance of the mechanism within this time range. It was observed that between 40 to 160 seconds, high priority traffic used its proposed percentage share (78% - 80%) hence achieving the objective of the study.

Acknowledgement

This paper is a contribution to the 2016 Fifth African Higher Education Week and RUFORUM Biennial Conference.

References

Saad Biaz, 2004. Controlling Inbound Traffic. Auburn University.

Novak, D. C. 2008. Managing bandwidth allocations between competing recreational and non-recreational traffic on campus networks. *Decision Support Systems* 45 (2): 338-353.

Guo, F., Chen, J., Li, W. and Chiueh, T. C. 2004. Experiences in building a multihoming load balancing system. *IEEE INFOCOM* 2:1241-1251.

Singh, A. S. and Barua, G. 2010. Load balancing inbound traffic in multihomed stub autonomous systems. Guwahati, India.

Joachim, D. 2004. University Gets Tough on P2P. Internetweek.com.

Saroiu, S., Gummandi, K. P. and Gribble, S. D. 2012. A measurement study of peer-to-peer file sharing systems. Multimedia Computing and Networking (MMCN).

Sen, S. and Wang, J. 2004. Analyzing peer-to-peer traffic across large networks. *IEEE/ACM Transactions on Networking* 12 (2): 219-232.

Bukhari, I. F., Harwood, A. and Karunasekera, S. 2015. Effect of similarity distribution on the convergence of decentralized similarity overlays. In: Proceedings of the 13th Australasian Symposium on Parallel and Distributed Computing.

Jacobson, V. 1988. Congestion avoidance and control: ACM Computer Communication Review. Proceedings of the Sigcomm in 88 Symposium in Stanford, CA. 18 (4): 314-329.

Gupta, J. D., Howard, S. and Howard, A. 2006. Traffic Behavior of VoIP in a Simulated Access Network. World Academy of Science, Engineering and Technology.