Journal of Ubiquitous Systems & Pervasive Networks
Volume 7, No. 1 (2016) pp. 01-06

Performance Evaluation of Routing Protocols for Video Conference over MPLS VPN Network

Abdullah Al Mamun, Tarek R. Sheltami, Hassan Ali, Sultan Anwar

College of Computer Science & Engineering
King Fahd University of Petroleum and Minerals
Eastern Province, Dhahran 31261, Saudi Arabia

Abstract

Nowadays video conferencing is a highly demanding facility in order to its real time characteristics, but faster communication is the prior requirement of this technology. Multi Protocol Label Switching (MPLS) IP Virtual Private Network (VPN) addresses this problem and it is able to make a communication faster than others techniques. However, this paper studies the performance comparison of video traffic between two routing protocols namely the Enhanced Interior Gateway Protocol (EIGRP) and Open Shortest Path First (OSPF). The combination of traditional routing and MPLS improve the forwarding mechanism, scalability and overall network performance. We will use GNS3 and OPNET Modeler 14.5 to simulate many different scenarios and metrics such as delay, jitter and mean opinion score (MOS) value are measured. The simulation result will show that OSPF and BGP-MPLS VPN offers best performance for video conferencing application.

Keywords: *OSPF, BGP, EIGRP, MPLS, Video conference, Provider router, edge router, layer3 VPN*

1. Introduction

Video conferencing connects people in real time through audio and video communication over broadband networks allowing visual meetings and cooperation on digital documents and shared presentations [1] [2]. In previous, members connected between central meeting rooms prepared with video conference hardware, but new technologies allow participants to connect remotely over a network through multiple devices like laptops, desktops, smart phones and tablets [1]. To support this scenario, we need delay less and reliable technology to transfer data packet quickly. This is why, it is driven to develop such technology that can give us chance to send video packets in real time with minimum delay and jitter. Moreover, video conferencing is a transmission technology that presents an economical and trustworthy tool for video and voice [2], [3] and [4]. The protocol H.393 is used that describes in a such a way that it supports dual stream in case of video conferencing, usually one for live video, the other for still images[4]. However, video conferencing needs some binding Quality of Service (QoS) requirements such as low, delay, less jitter and packet loss [5]. Committing the optimum QoS parameters is obligatory for video conferencing service [5], thus using MPLS in this area is better solution now a days because it proves to perform better than Non-MPLS networks.

More technically, Aside from forwarding efficiency, it has to remember that, in traditional packet-switched IP networks, almost everything is done based solely on the destination IP address in the packet. Since an MPLS label is added to the packet after a host sends it, he can associate a label with more than just the specific destination of the end host. For example, if one wanted, he could associate traffic that needed low latency service with destination ABC with label 12345. He could also associate traffic only requiring normal service with the same destination ABC with label 23456. Going back to the post office example, one series of digits might be media mail to his house, whereas another series of digits represents next day air to his home. Both labels point to the same destination, but they represent different ways of being handled as they are being sent there.

Another non-efficiency-related benefit that MPLS brings to those who use it is its flexibility in controlling the path that a given packet will take. It is LSP, which stands for label switched path which is shown in fig 1. An LSP is a specific path from the ingress MPLS router to the egress MPLS router. When a MPLS header is added to a packet, the label in that header is associated with a specific LSP. All packets going over the same LSP are going to follow the exact same path through

* Corresponding author. Tel.: +966-13-860-4678
Fax: +9876543210; E-mail: tarek@kfupm.edu.sa

DOI: 10.5383/JUSPN.07.01.001

the network, with a few exceptions outside the scope of this document. Through the use of traffic-engineering mechanisms (also beyond the scope of this document), or by simply adjusting some underlying protocols, it can be influenced what that path will be, on both a primary and secondary basis. There are many ramifications of being able to control the end-to-end path through the MPLS network. For example, let's say someone has two tiers of service, gold and silver. His gold service is supposed to provide enhanced throughput with lower latency and jitter to customers. His silver service provides service to customers where the consistently greater throughput and enhanced forwarding are not guaranteed. By using MPLS LSPs, it can specify that the gold traffic uses its more expensive backbone circuits, whereas the silver traffic uses the less expensive ones.

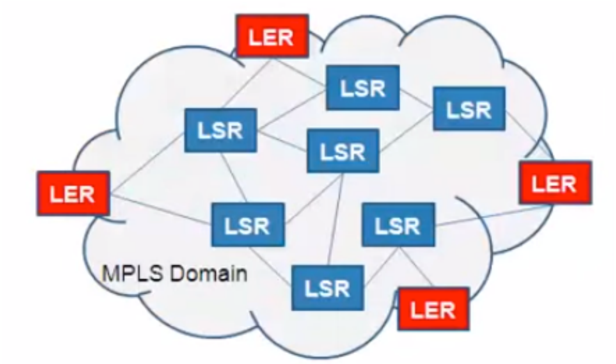

Fig. 1. Example Provider Network.

Finally, it is a best packet switching technology which ensures QoS, convenient for multimedia applications, efficient and reliable use of network resources. This paper discusses the best design for protocol suits for multimedia application for different routers such as Label switch router (LER) that in the middle of the Service provider network that uses label to perform routing is label switch router that is a combination of switch and router. Also known as Provider router and Label Edge Router. However, a sample provider backbone network is shown in fig 1 where LER and LSR are connected internally. The routers those are located at the boarder of a MPLS network known as Provider Edge router. However, the proposed style is applied in a SP infrastructure and applies techniques of DiffServ [6] and MPLS [7]. Simulation results of delay, jitter, and throughput and packet loss with this strategy are presented and discussed. The main contribution of this paper are configure MPLS LDP in the service provider network, configure VRF in the Provider Edge (PE) routers, configure BGP VPNv4 peering between routers, configure Peering between PE routers to customer routers and finally compare routing protocol in case of video conferencing.

2. Methodology

The simulation of video conferencing on MPLS VPN is accompanied using OPNET Modeler 14.5. The codec chosen for the video conferencing simulation is H.320 scheme and interactive voice with delay, throughput and reliability for establishing the video calls. Fig 2 shows the BGP-MPLS VPN network topology for the video conferencing simulation in GNS3. There are two LER respectively R1 and R4 that are connected to the customer AS router CUSTAR1 and CUSTAR2. CUSTAR1 is connected to the interface f0/1 of R1s interface which ip is 15.15.15.0/32 whereas CUSTAR2 is connected with the interface f0/1 of R4s interface that ip is 46.46.46.0/24. Router R2 and R3 are LSR in this scenario. OSPF area 0 is covers all provider backbone area. Also Provider network BGP AS 65001 is shown in fig 2. MPLS operates using the protocol called LDP (Label Distribution Protocol) which assigns labels ranging from 16 to 1,048,575 (0-15 reserved and cannot be used in Cisco routers) to IP prefixes/subnets in the routing table. LDP relies on the routing table in order for it to form its LIB (Label Information Base) and LFIB (Label Forwarding Information Base). LSR (Label Switch Routers) are routers in the middle of the Service provider network that uses label to perform routing. LER (Label Edge Routers) are routers that are entry and exit points of the network. They are generally the Provider Edge (PE) routers. The three general operations of LDP when dealing with labeling packets Push - means that the incoming packet has no label and has to assign a new label to it. Ingress LER do this operation. SWAP - basically changing the label to a different label. LSR do this operation. POP removes the label. Egress LER does this operation. The ingress PE actually appends two MPLS labels in the header. First, a lookup is done in the BGP table to find the VPN label. Then, the path label is put on top of that. The path label is what you use to get to the egress PE router, and the VPN label is what the egress PE uses to send it out the right interface. Now, on to yet another term is PHP. PHP stands for penultimate hop popping. Before I define what PHP is, I need to understand a problem seen by the developers of MPLS. To get a packet ready to send toward a customer, two things have to be done. First, I have to remove the path label. Second, I have to do a lookup on the VPN label to determine which interface to send it out through. Rather than have the egress PE router do both of these tasks, PHP is done. All PHP does is have the router connected to the egress PE remove the path label prior to sending it to the egress PE. In this way, the workload is distributed. The last P router before the egress PE removes the outer path label, while the egress PE removes the inner VPN label and sends it towards its final destination.

3. Experimental Work

In this section, we experimentally evaluated the performance and capabilities of above method. The experiment was carried using hardware and software tools such as GNS3, OPNET and MatLab. The main configuration of routers is given below.

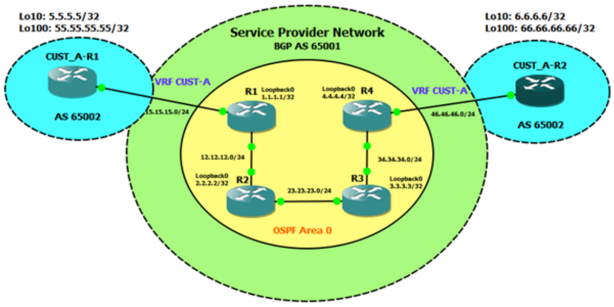

Fig. 2. MPLS VPN Topology in GNS3 Simulator.

2.1. Configuration of MPLS LDP in the Service Provider Network

The command mpls ip is required to form LDP neighbors. It is only configured in interfaces that are inside the service provider network. Any interfaces such as loopbacks or those facing the customer are not required to be configured because LDP is not required between customer and PE routers. Though the customer is connected to the MPLS network, it is a common practice for service providers not to make their network visible to the customer.

The mpls label range command in the routers sets the number of labels only. I configured it that way so it will be easier to explain later how LDP works. In the example configuration, the number of labels that can be assigned for each router only amounts to 1000. If the network has more than 1000 prefixes, the rest of the prefixes will not be labeled and will be routed using IP. The total labels of range are shown in table I.

The mpls ldp router-id loopback0 force command enforces the LDP to use the IP address of Loopback0 as its ID. The force keyword will tear down existing LDP sessions and clear all the current bindings and applies the changes to the LDP ID. If force is not used, the router will wait until the current interface of the LDP ID goes down before it applies the new LDP ID specified in the command.

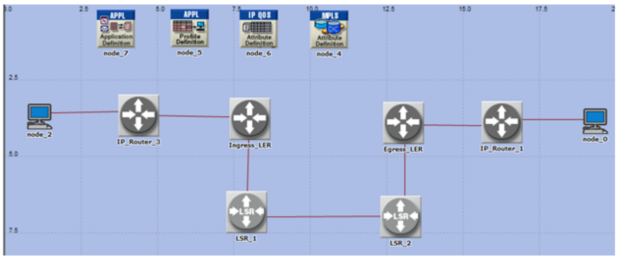

Fig. 3. MPLS VPN Topology in OPNET Simulator.

Table 1. Label Range

Router	Interface	label range
Router 1	Fast Ethernet 0/0	1000-1999
Router 2	Fast Ethernet 0/0	1000-1999
Router 2	Fast Ethernet 0/1	2000-2999
Router 3	Fast Ethernet 0/1	2000-2999
Router 3	Fast Ethernet 0/0	3000-3999

2.2. Configuration of VRF in PE Routers

VRF (Virtual Routing and Forwarding) is comparable to a VLAN in a switch. VRF is used to create different routing tables that are separated from each other. Since one VRF can't see what routes are in another VRF, the same IP prefix can exist in different VRFs. However, duplicate IP prefixes will have an issue when it comes to route-leaking between VRFs.

2.3. Configuration of BGP VPN v4 Peering between R1 and R4

VPNv4 is an address-family of Multiprotocol BGP. To explain it simply, VPNv4 is a collection of all routes from different VRFs that were marked with the extended community route-target. This is the address-family where route-leaking can be performed. Route-leaking is simply sharing a route from one VRF to another. Common application for this is, one company wants to connect to other company's servers and they happen to be connected to the same MPLS provider.

2.4. Configuration of Peering between PE and Customer Routers

Configure Peering between PE routers R1 and R4 to customer routers CUSTA-R1 and CUSTA-R2. Announce Loopback 10 and 100 in the CE routers.

However, The BGP-MPLS VPN simulations are directed using two beset interior routing protocol namely EIGRP and OSPF on similar topology as in fig 3. The rate of a video call call is fixed at 500, 2500 and 4000 calls/hour. Average call duration is set to 10 minutes and the voice flow duration is set to 3 hours. The simulations are beset to measure the voice packet end-to-end delay, voice jitter and mean opinion score as to define the overall video and voice quality in both scenarios during the three following scenarios.

4. Result and Analysis

Each experiment is repeated 10 times for perfect accuracy. The detail simulation result is presented in following sub sections.
As we can see, there is full reach ability between the CE routers but the trace route shows the path it took inside the service provider core network. This is not an advisable behavior, normally service provider from the customer any information about its core network. Let's configure a way to do that. After executing no mpls ip propagate-ttl command and run exactly the same trace out command.

Table 2. End-To-End delay before MPLS

Route	Delay 1(s)	Delay 2(s)	Delay 3(s)	Avg. Delay(s)
46.46.46.4	224	428	320	324
34.34.34.3	1188	992	1100	1093
23.23.23.2	1108	992	880	993
12.12.12.1	880	968	1172	1007
15.15.15.5	888	888	880	885

Table 3. End-To-End delay after MPLS

Route	Delay 1(s)	Delay 2(s)	Delay 3(s)	Avg. Delay(s)
46.46.46.4	268	428	356	351
15.15.15.5	1072	980	920	961

Now, the service provider network has been hidden through the no mpls ip propagate-ttl command. It clearly observed that first test shows the path from one customer to another end. In this case, all ip and reach time are shown that is indication of before MPLS deployment. When second test is done after configuring all LER and LSR router, it shows only customer interface. As a result ip addresses are hidden due to MPLS where label is used to increase throughput and decrease RTT and packet loss.

However, we got various experimental simulation results after running exactly the same topology in OPNET simulator varying the routing protocols which are describes below sequentially.

2.1. End to End Packet Delay

The amount of time taken for transmitted a packet across a network from source to destination is shown in fig 4-6. The line graph of fig 4 presents the packet delay for 500 calls per/hours using both EIGRP and OSPF. Initially, the delay is same for both protocols that are almost zero but it is start to increase suddenly at 890s for EIGRP whereas OSPF is remain unchanged.

Similarly, the fig 5 shows that the traffic delay for 2500 calls per hour where delay is start to increase immediately after 960s for EIGRP protocol whereas OSPF shows regular zero all most.

In the same way, fig 6 represents the packet delay for 4000 calls per hour. In this case, EIGRP protocol offers a little change that delay is start a bit later to go to pick of 990s but delay for OSPF protocol is still zero for this large traffic too.

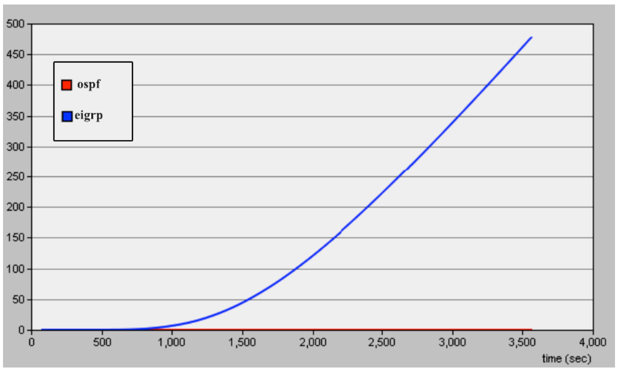

Fig. 4. Traffic Delay for 500 video calls per hour.

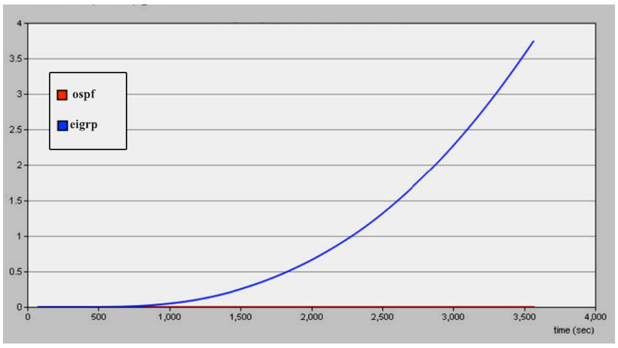

Fig. 5. Traffic Delay for 2500 video calls per hour.

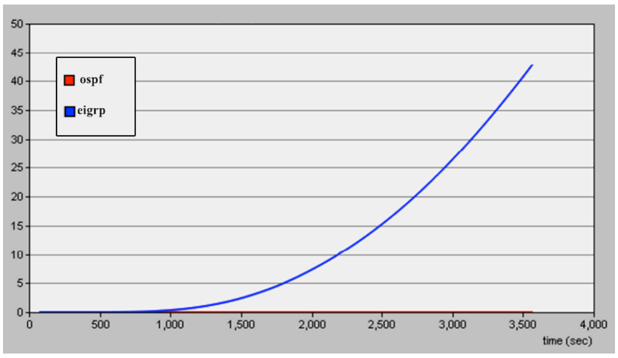

Fig. 6. Traffic Delay for 4000 video calls per hour.

2.2. Jitter

Time difference between two frames due to transmission latency is shown in fig 7-9, Jitter for 500 calls per hour is shown in fig 7 where jitter is start to happen from less than 500s for EIGRP whereas OSPF is remaining unchanged to the last frame.

In the same manner, jitter for 2500 calls per hour is shown in fig 8 where jitter is start to increase from 480s and it became saturated after a while in EIGRP protocol, but almost zero jitter is experienced though a little changed happens initially while same setup ran with OSPF protocol.

Again, fig 9 is shows the jitter for 4000 calls per hour where jitter goes high quickly at little bit earlier than previous experiment which is 470s whereas OSPF is still unchanged.

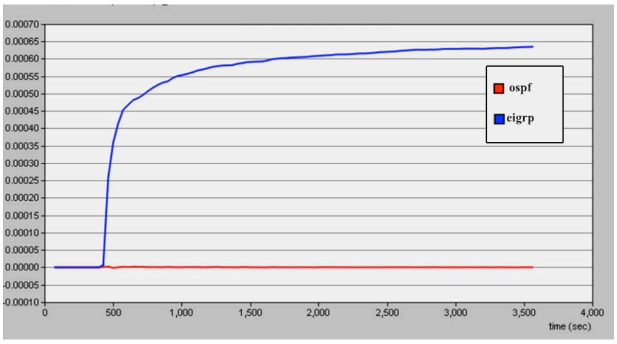

Fig. 7. Jitter for 500 video calls per hour.

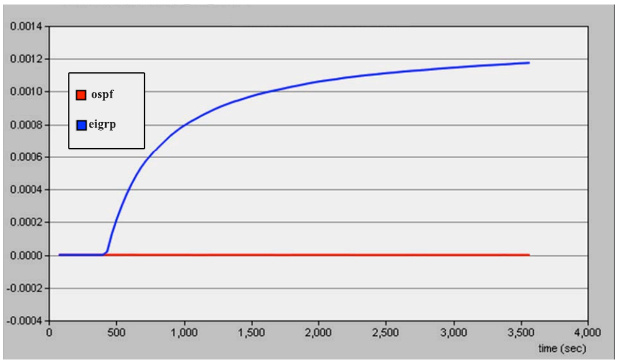

Fig. 8. Jitter for 2500 video calls per hour.

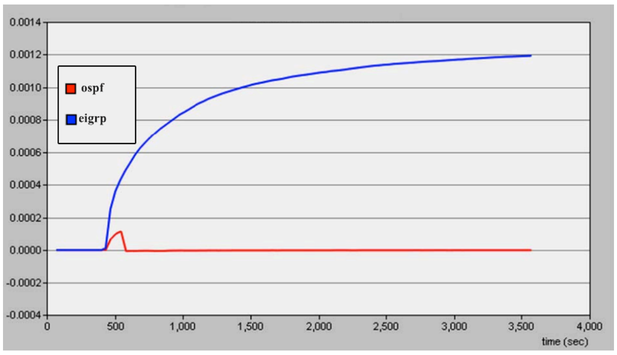

Fig. 9. Jitter for 4000 video calls per hour.

2.1. Mean Opinion Score (MOS)

In voice communications, particularly Internet telephony, the mean opinion score (MOS) provides a numerical measure of the quality of human speech at the destination end of the circuit [8]. MOS scores are shown below according to this experimental sequence. However, fig 10 displays the MOS score for 500 calls per hour where score is start to drop for both EIGRP and OSPF at the same time which is less than 500s from 3.7 units of MOS and it does not recovered until simulation end.

In the same fashion, the MOS score for 2500 calls per hour is shows in fig 11 where score is start to drop from the 3.55 units when time was less than 500s for both EIGRP and OSPF. Finally, fig 12 displays the MOS score for 4000 calls per hour where score is again start to go down from the 3.6 units at 480s.

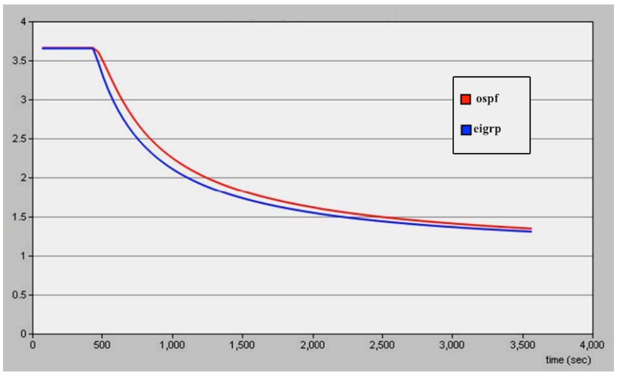

Fig. 9. MOS for 500 video calls per hour.

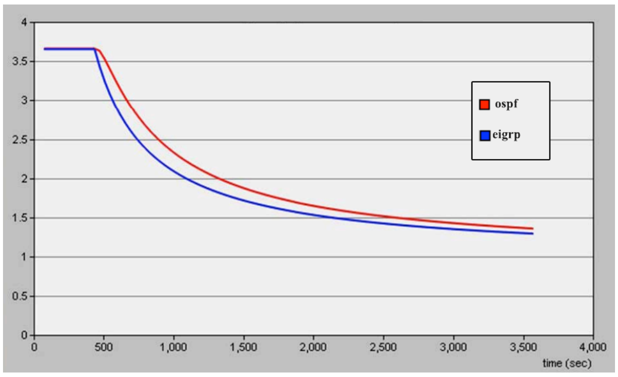

Fig. 9. MOS for 2500 video calls per hour.

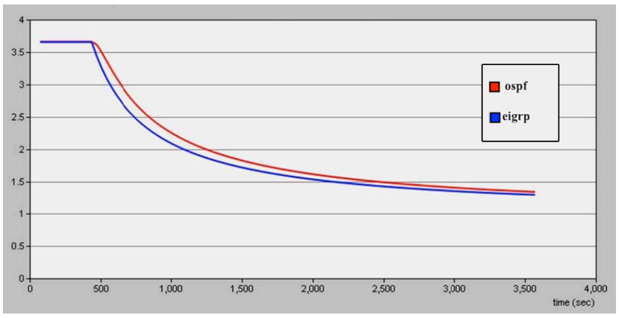

Fig. 9. MOS for 4000 video calls per hour.

5. Related Works

So far many researches has been done on video conferencing multi-cast and broadcast over MPLS are [9], [10] and [11] but few of them are comparison study among router protocols in MPLS VPN [1]-[4] and [12]. Relative comparison of network model infrastructure for delivering data over MPLS networks [2]-[4] shows MPLS perform better. Among many performance metric, end to end delay is considered in the paper [4] [13], jitter cite5and [14], voice packet delay variation is shown, voice packet send and receive [4], packet loss [6], throughput putc[14] and MOS[15] and [16]. In video conferencing, performance measures shown in case of voice codec in paper [2] and [3]. However, G.711 is used as most popular codec for VoIP call in [17], [18] that is also discussed about security in multimedia communication. How many types of routing protocols is implemented in VoIP application is shown in paper [6]-[13]. Comparison of many well-known routing protocols such as RIP, OSPF and EIGRP is presented in the paper [16]-[19]. Determining the best routing protocol is complex task, here they are discussed how can it does easily based on convergence time and queuing delay in the paper [7] and [13].

6. Conclusion

This paper introduced a performance evaluation of video conferencing application using two different routing protocol respectively EIGRP and OSPF over MPLS VPN network. The empirical simulation result shows that router configuration on each provider router is successfully done and it can hide the PE router while data is traversing router to router. Moreover, it is clearly observed that the best performance is recorded in case of OSPF protocols in every scenario. We have planned to continue our research in large scale in future.

Acknowledgment

Department of Computer Engineering, King Fahd University of Petroleum & Minerals, KSA.

References

[1] Windstream, "Mastering network design with mpls," *http://www.windstreambusiness.com/media/663859/masteringnetworkdesign-with-mpls.pdf)*, 2012.

[2] R. S. Naoum and M. Maswady, "Performance evaluation for voip over ip mpls," *World Comp. Sc. and Inf. Tech. J.(WCSIT)*, vol. 2, no. 3, pp. 110–114, 2012.

[3] R. Yunos, S. A. Ahmad, N. M. Noor, R. M. Saidi, and Z. Zainol, "Faculty of computer and mathematical sciences, uitm malaysia, selangor, malaysia," in *Systems, Process & Control (ICSPC), 2013 IEEE Conference on*. IEEE, 2013, pp. 139–143.

[4] ——, "Uitm malaysia, selangor, malaysia," in *Systems, Process & Control (ICSPC), 2013 IEEE Conference on*. IEEE, 2013, pp. 139–143.

[5] E. Kim, W. Chun, Y. Jang, and S. Rha, "Traffic measurements supporting end-to-end qos requirements in mpls networks," in *Advanced Communication Technology, 2004. The 6th International Conference on*, vol. 2. IEEE, 2004, pp. 862–867.

[6] R. Yunos, N. M. Noor, and S. A. Ahmad, "Performance evaluation between ipv4 and ipv6 on mpls linux platform," in *Information Retrieval & Knowledge Management,(CAMP), 2010 International Conference on*. IEEE, 2010, pp. 204–208. http://dx.doi.org/10.1109/infrkm.2010.5466916

[7] A. Hinds, A. Atojoko, and S. Y. Zhu, "Evaluation of OSPF and EIGRP routing protocols for ipv6," *International Journal of Future Computer and Communication*, vol. 2, no. 4, pp. 287–291, 2013. http://dx.doi.org/10.7763/IJFCC.2013.V2.169

[8] R. Serral-Gracia, L. Jakab, and J. Domingo-Pascual, "Measurement based call quality reporting," in *Local Computer Networks, 2007. LCN 2007. 32nd IEEE Conference on*. IEEE, 2007, pp. 997–1008. http://dx.doi.org/10.1109/lcn.2007.76

[9] J.-H. Cui, J. Kim, A. Fei, M. Faloutsos, and M. Gerla, "Scalable qos multicast provisioning in diff-serv-supported mpls networks," in *Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE*, vol. 2. IEEE, 2002, pp. 1450–1454.

[10] S. A. A. Shah and L. Ahmed, "Mpls feasibility for general and core ip networks using open-source systems," in *Electrical Engineering, 2008. ICEE 2008. Second International Conference on*. IEEE, 2008, pp. 1–6. http://dx.doi.org/10.1109/icee.2008.4553931

[11] I. Rozic, "Multicast state scalability in qos mpls networks," in *Software in Telecommunications and Computer Networks, 2006. SoftCOM 2006. International Conference on*. IEEE, 2006, pp. 320–325. http://dx.doi.org/10.1109/softcom.2006.329774

[12] S. Ali and B. Z. Rana, "Opnet analysis of voip over mpls vpn with ip qos," *Blekinge Institute of Technology, Sewden*, 2011.

[13] K. Mirzahossein, M. Nguyen, and S. Elmasry, "Analysis of rip, OSPF, and EIGRP routing protocols using opnet," *Simon Fraser University, School of Engineering Final Year Project, ENCS 427: Communication Networks*, 2013.

[14] R. Yasinovskyy, A. L. Wijesinha, R. K. Karne, and G. Khaksari, "A comparison of voip performance on ipv6 and ipv4 networks," in *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*. IEEE, 2009, pp. 603–609. http://dx.doi.org/10.1109/aiccsa.2009.5069388

[15] E. S. Myakotnykh and R. A. Thompson, "Adaptive speech quality management in voice-over-ip communications," in *Telecommunications, 2009. AICT'09. Fifth Advanced International Conference on*. IEEE, 2009, pp. 64–71. http://dx.doi.org/10.1109/aict.2009.17

[16] X. Che and L. J. Cobley, "Voip performance over different interior gateway protocols," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 1, no. 1, 2009.

[17] N. Aoki, "A semi-lossless steganography technique for g. 711 telephony speech," in *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on*. IEEE, 2010, pp. 534–537. http://dx.doi.org/10.1109/iihmsp.2010.136

[18] T.-Y. Huang, P. Huang, K.-T. Chen, and P.-J. Wang, "Could skype be more satisfying? a qoe-centric study of the fec mechanism in an internet-scale voip system," *Network, IEEE*, vol. 24, no. 2, pp. 42–48, 2010. http://dx.doi.org/10.1109/MNET.2010.5430143

[19] I. Kaur and M. Sharma, "Performance evaluation of hybrid network using EIGRP & OSPF for different applications," *International Journal of Engineering Science and Technology (IJEST)*, vol. 3, no. 5, pp. 3950–3960, 2011.