TELKOMNIKA, Vol.16, No.5, October 2018, pp.2073~2081
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v16i5.7326

Performance of MPLS-based Virtual Private Networks and Classic Virtual Private Networks Using Advanced Metrics

Kennedy Okokpujie*[1], Olamilekan Shobayo[2], Etinosa Noma-Osaghae[3], Okokpujie Imhade[4], Obinna Okoyeigbo[5]
[1,2,3,5] Department of Electrical and Information Engineering, Covenant University, Ota, Nigeria
[4]Department of Mechanical Engineering, Covenant University, Ota, Nigeria
*Corresponding author, e-mail:kennedy.okokpujie@covenantuniversity.edu.ng

Abstract

Multiprotocol Label Switching (MPLS) is effective in managing and utilizing available network bandwidth. It has advanced security features and a lower time delay. The existing literature has covered the performance of MPLS-based networks in relation to conventional Internet Protocol (IP) networks. But, too few literatures exist on the performance of MPLS-based Virtual Private Networks (VPN) in relation to traditional VPN networks. In this paper, a comparison is made between the effectiveness of the MPLS-VPN network and a classic VPN network using simulation studies done on OPNET®. The performance metrics used to carry out the comparison include; End to End Delay, Voice Packet Sent/Received and Label Switched Path's Traffic. The simulation study was carried out with Voice over Internet Protocol (VoIP) as the test bed. The result of the study showed that MPLS-based VPN networks outperform classic VPN networks.

Keywords: *MPLS, VPN, performance metrics, load, throughput*

1. Introduction

The Internet provides real-time applications that require the minimum possible end-to-end delay. Voice and video conferencing are great examples of such applications. A great deal of bandwidth and special connections are required to get the needed speed and minimal delay for these applications. It is not cost effective to directly implement these high speed networks. Thus, there is a need to provide a new measure to operate these applications whilst preserving the need for minimal end-to-end delay at no additional network enhancement costs [1]. For example, video applications usually require an end-to-end delay of less than 250ms. These applications usually use VPNs for their security needs. VPNs are connectivities deployed on shared communication infrastructure with private network policies. This shared infrastructure may not utilize the public internet but can make use of the Internet Protocol and Frame Relay provided by Internet Service Providers [2,3].

VPNs provide a cost efficient and effective way of making users on physically separated networks appear as though they are on a single network [4]. VPNs can be classified on the basis of their protocol levels as Layer-2 (L2) and Layer-3 (L3) VPNs. Layer-2 VPNs can provide secured point-to-point transport services for two nodes and $n(n-1)$ links for enterprise applications. The cost of L2 links increases substantially when the value of n is small. L3 VPNs connect different end users using an MPLS enabled routing network. MPLS-based VPN can be used to provide end-to-end infrastructure consolidation that can support data, voice and video services for dissimilar networks [5]. MPLS-based VPNs have the ability to support any-to-any connectivity, retain existing IP addresses and allow for site-to-site or data centre scalability [6]. These are major enterprise network advantages.

As stated in [7], MPLS, Reservation Protocol (RSVP) and Differentiated Services (Diffserv) are the three models suggested by the Internet Engineering Task Force (IETF) for the servicing of Quality of Service (QoS) requests [8]. The MPLS has fast packet forwarding and traffic engineering that beats the best that conventional IP can offer. MPLS is the primary integration technology for transporting voice, video and data traffic within a network. MPLS-VPN

Received September 17, 2017; Revised March 7, 2018; Accepted September 6, 2018

can combine the advantages of IP and other network protocols to deliver the QoS desired [9]. This has led to the proliferation of ISPs that provide MPLS-VPN services and the growing number of businesses that use MPLS-VPNs. The sophisticated nature of MPLS-VPNs has also given room for sustainable security solutions for MPLS-VPNs [10].

Programs have also been developed to provide solutions for the use of VPNs utilizing MPLS backbone in public networks. A VPN does not provide a second layer of information because it cannot perform automatic encryption and thus, finds it difficult to connect easily especially when there are errors caused by interruption of information disclosure protocol and other issues [11]. Label Switching Paths (LSPs) are the means by which traffic demands are routed in MPLS networks. LSPs have dynamic routing capabilities that can handle rapidly varying traffic demands. Some LSPs are removed from the network when traffic demands are low and created when traffic demands are high. The creation and deletion of LSPs due to vary traffic demands could lead to bandwidth underutilization. Rerouting LSPs using a better configuration has been proposed as a way of checkmating bandwidth underutilization in MPLS networks. Rerouting is usually performed offline and at a time when the network is stable. The services the LSP supports, the desired Quality of Service informs the way and manner in which LSPs are confiured to prevent bandwidth underutilization. One way to improve the situation at any instance is to reroute the present LSP to a known and better global configuration. This rerouting process is performed ‘‘off-line’’ during a quiet period when the network state is stable. To achieve this, the desired Quality of Service is taken into serious consideration as rerouting has its own unique effect on network traffic.

1.1. Related Work

It is common knowledge that MPLS-based network infrastructure is quite efficient. Authors In paper [12], looked closely at how MPLS is implemented on VPNs. An architectural model was clarified and a proposal was made for a unique model that allows a design and implementation procedure for MPLS on VPNs. The authors elucidated on the various QoS that must be considered when designing MPLS-VPN schemes. In paper [13] a detailed description was given on how to simulate a MPLS scheme using OPNET$^{®.}$ The authors focused on describing the functionality of MPLS architecture through a simulation model.

The authors in [14] explained a rerouting technique that used three levels of QoS requirements to tackle the issue of network resource wastage. The technique involved the use of an algorithm that gave priority to medium quality LSPs over low quality LSP when rerouting. The technique considers low quality LSPs only after all medium quality LSPs has been rerouted. The technique was a two pronged one that tried to keep reroutings to the barest minimum. The authors supported their findings with some numerical results.

In [15] a distortion factor was used to represent the varied network streams that are usually found at the node of a network. This enabled the authors to use MPLS to address what-if scenerios that are dependent on anticipated traffic demands. A problem known as a distortion-aware non-linear discrete optimization was created to view how the MPLS can be used to reroute traffic from a heterogenous data stream.The main problem was splited into two phases. The frist phase was used to break down the major problem into micro-problems and the second stage was used to show how the non-linear distortion aware problem was solved.

1.2. The problem

A lot of literature exists on comparions between conventional IP and MPLS networks. The authors in [16] used the performance metrics of end-to-end delay, voice packet delay, received and sent voice packets and voice packet jitter to evaluate the comparative performance of IP and MPLS networks. Voice over VoIP was used as the test bed for the simulation study. The simulation study’s result showed that MPLS-based networks outperform conventional IP networks. However, the study was not carried out on VPNs.The authors in [17] implemented the MPLS technology for a different test bed known as Vehicular Ad-hoc Networks (VANETS) and were able to show the comparative effieciency of IP and MPLS networks using QoS parameters such as packet loss, round trip delays and fault tolerant paths. The result of the study showed that MPLS-based networks perform better than their IP counterpart. But security measures were not considered in the study. The study carried out by the authors in [7] incorporated security and VPNs. The comparative study used frame relay as a performance metric. The study showed that MPLS-VPNs are better in performance than IP based networks. However, their test bed was only meant to cater to data sevices [18].

1.3. Proposed Solution

Since most work done in this area have already been able to show that for efficient management in traffic engineering, MPLS backbone provides better peformance than it's IP conterpart, and also VPN based MPLS is the best security scheme to be used, the later was only justified for data networks, voice and video was not considered. Since real life infrastructure will carry video, voice and data, this work is going to compare the performance of MLPS-VPNs with classic VPNs using VoIP as the test bed [19,20].

2. Research Method

2.1. Experiment Description

This section describes the overall network design for the simulation study.Transmission and switching using the VPN-MPLS backbone is simulated and compared with the classic VPN only. The simulation study shows the location of network devices and their optimum connection matrix. The simulations study is carried out in:

a. A simple MPLS-VPN network
b. A traditional VPN network.

The network components as used in this paper from OPNET® library include:

a. Ethernet_wkstn: This is the OPNET® element that is used to simulate the total number of network users. It consists of ethernet connections at a selected rate. It is controlled by the underlying medium used to connect to an ethernet switch.
b. Ethernet_server: This is used to simulate the service server in the network.
c. Cisco 7200 router: This is the Cisco router model that is capable of supporting MPLS traffic management technology.
d. 100BaseT: This link provides a full duplex capability with speeds up to 100Mbps for connecting the Cisco router to the Ethernet_server and Ethernet_wkstn.
e. PPP_E3: This is used to provide a point to point duplex link connecting two workstations or nodes and it can deliver an IP rate of speeds amounting to 34.36Mbps. It is also used for connecting the Cisco 7200 series router.
f. MPLS_E-LSP_STATIC: This is configured so that the static LSPs are not signaled during startup. This helps to ensure total control of the routing process.
g. Application Config: This network component is used to direct OPNET® to the application that contains the underlying framework for the simulation study. Only one application configuration is for OPNET® to deal with multiple network applications. Application parameters for different application types being observed are configured in this element.
h. Profile Config: This is used to represent the different traffic patterns of users on a network. It can be used to show the different applications a user might or will be using in some time duration, i.e. (simulated period). There is no limit to the number of profiles that can be simulated. The simulated profiles can be viewed on assigned networks and observations can be made. User profiles vary from one user to the other and in this study; users were assigned to profiles that were configured for the needed application.
i. MPLS_Config_Object: This element is used for the configuration of MPLS Forwarding Equivalence Class (FEC) and Traffic Trunk. The specifications are implemented at the Ingress Edge router. The main purpose of the implementation is to reroute traffic flows and allocate distinct LSPs to different application traffic. The utmost intention of the simulated OPNET® implementation was to provide a networking environment with traffic flow that can be related to an ISP network. The model site simulated can provide the networking capabilities of Servers, Workstations, Routers and Link Models. At the edges of the networks, Cisco 7200 series routers were provided to deal with the traffic ingress and egress from the servers and workstations.

2.2. Description of the Topology

The profiles discussed in the earlier section were used to configure two applications that use Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) as their transport protocols. The simulation study ensures the routing of these network traffic types through the shortest paths possible.The choice of UDP and TCP as the transport protocols for the simulation study was informed by its wide use in IP systems. During configuration, two minutes was assigned to allow for sufficient flooding of the network with TCP and UDP traffic. The two minutes' convergence time allows enough time for the network components such as the routers to exchange Hello packets, thereby, helping to build the topology tables and routing paths. At the start of the second minute, the application responsible for the transfer of data is triggered, allowing TCP packets to move across the network.

The maximum TCP packets allowed to be downloaded from the file server was capped at 50MB. The application that provides UDP packets on the network starts one minute after the TCP packets have reached an assigned threshold. The maximum traffic load for the UDP packets was set at 3MB. The default Maximum Transmission Unit (MTU) value used was 1500 bytes for Ethernet connections. This specifies the amount of IP datagram packets that can be carried in a frame.

2.3. MPLS SIMULATION SCENARIO

The TCP and UDP traffics generated were controlled by installing LSPs that labeled the packets and made rerouting easy. A total amount of four LSPs were created between the edge router allowing traffic into the network (i.e. ingress router (PE_1)) and the router taking packets out of the network (i.e. egress router (PE_2)). The flow specification for TCP and UDP traffic entering into the network was configured for router (PE_1). The LSP traffic was made to pass through two traffic trunks as shown in Figure 1. Trunking was configured on the LSP links to engineer the packets from the File Transfer Protocol (FTP) clients (CE_1) to the server hosting the FTP protocol application. The simulation is shown in Figure 1. For the MPLS scenario, the maximum transfer rate was recorded for the TCP and UDP protocols. The throughput between the routers was measured and finally the queuing delay was also considered.

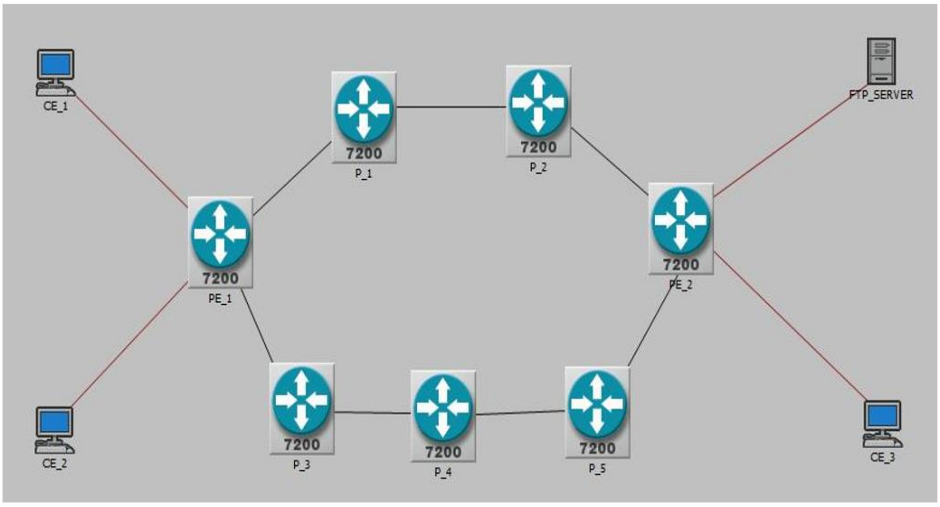


Figure 1. MPLS Simulation Scenario

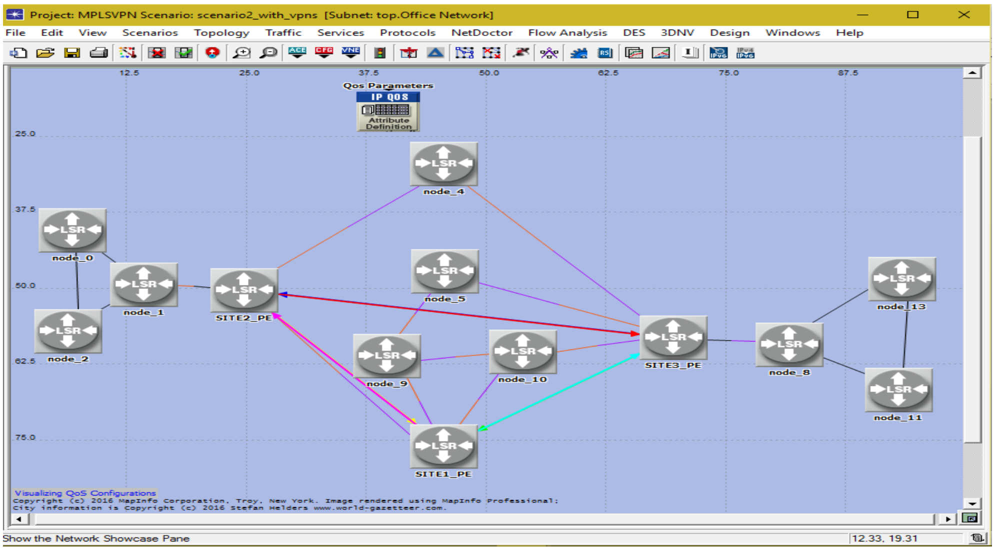
2.4. VPN-MPLS SIMULATION SCENARIO

The network components for the VPN-MPLS simulation study include: The Autonomous System 1 (AS-1) that contains four provider routers (P) and three provider Edge routers (PE). The autonomous System 2 (AS-2) was modeled as an enterprise network named Enterprise 1. Enterprise 1 was created and divided into two (2) sites, namely, site 1 and 2 respectively. Site one consists of two Customer routers (C) and one Customer Edge router (CE). Site 2 also contains the same amount of Customer Routers and Customer Edge Routers. The configuration is shown in Figure 2.

The VPN in this simulation study is named "Yellow_VPN". The routers are interlinked by using PPP_SONET_OC3 links. The desired IP QoS is implemented on every router in the MPLS backbone with the following parameters:

a. QoS Scheme: Priority Queuing
b. QoS profile: Protocol Based.

The results were analyzed based on VPN delay and VPN load/throughput (in bits/seconds and packet/seconds).



Project: MPLSVPN Scenario: scenario2_with_vpns [Subnet: top.Office Network]

Visualizing QoS Configurations
Copyright (c) 2016 MapInfo Corporation, Troy, New York. Image rendered using MapInfo Professional;
City information is Copyright (c) 2016 Stefan Helders www.world-gazetteer.com.

Show the Network Showcase Pane 12.33, 19.31

Figure 2. VPN-MPLS simulation Scenario

3. Results and Analysis

3.1. VPN Simulation Scenario

Figure 3 is the result got for the MPLS scenario. By observation, it was discovered that the maximum transfer rate was obtained at the 594th second, with a value of 1923004.16 bits/second. After one minute, the UDP traffic generated from the CE_2 reached a maximum transmission rate of 3017570.37 bits/second after a period of about 594 seconds. The values were got from the traffic moving towards the (PE_1) router. It was also observed that the intensity of traffic from the UDP packets in the network had some effect on the traffic intensity recorded by the TCP protocol. These effects were noticeable throughout the simulation period.

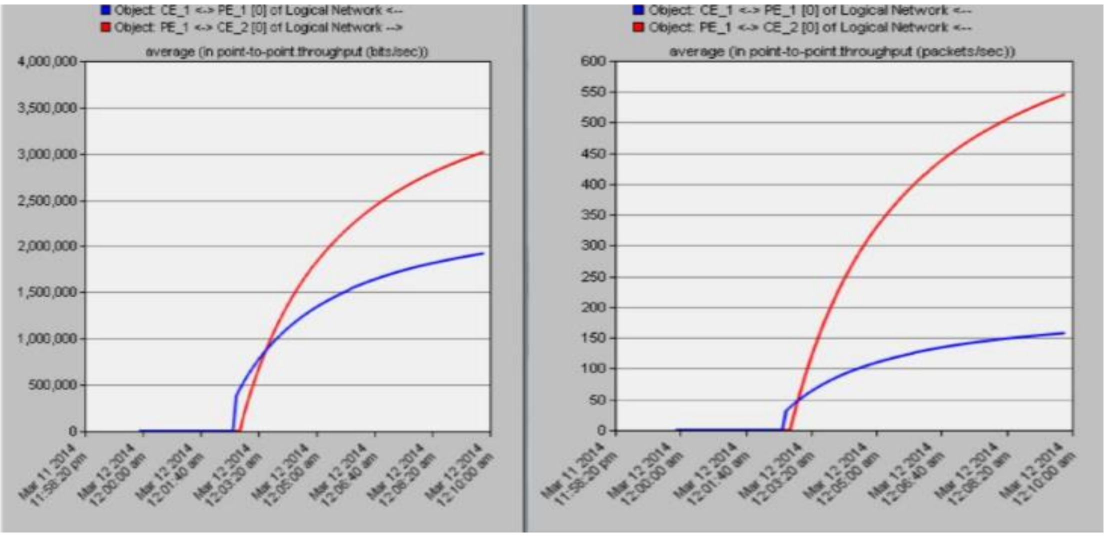


Figure 3. UDP Traffic Analysis

To obtain the TCP parameters, the simulation was allowed to continue for another 168 seconds and a minimum TCP value was obtained. The minimum TCP value obtained was 388712.82 bits/second. A maximum value of 1923004.16 bits/second was obtained at the 594th second. This is shown in Figure 4. The transients can be attributed to TCP acknowledgements travelling back and forth from the server to the client along the shortest path. Transients appeared in the result for the ingress router in charge of traffic forwarding to other areas of the network from the (PE_1). For packets to be rerouted or engineered to move in a specific path, it must adhere to the LSPs policy and path reservation so configured.

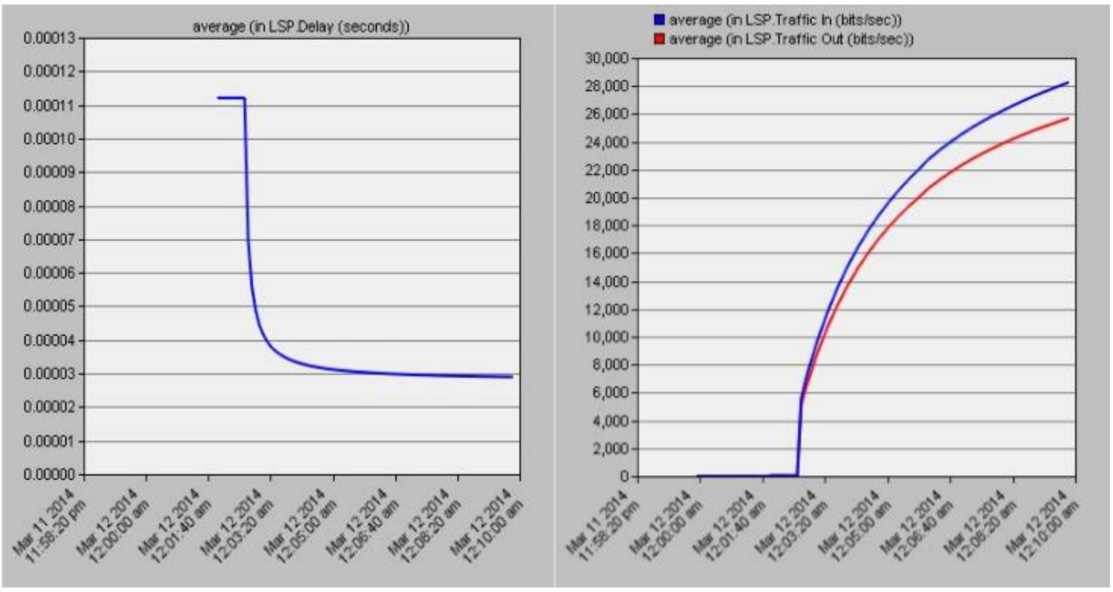


Figure 4. TCP Traffic Analysis

For proper working of the LSP configuration, packet routing for a particular specification of LSP must be established. This gives sole control of packet rerouting to the PE_1 ingress router on the edge of the network. The PE_1 ingress router also has the ability to supervise the average bit rate permitted by the flow specification predefined by the LSP. The flow specification configured and implemented for UDP traffic permitted bits averaging 4214400 bits/sec. It was noticed that some UDP traffic exceeded the specified average at some point due to increased traffic intensity. The LSP, configured at the ingress router, provided the queuing mechanism to control the amount of UDP packets to the specified value. This delay, caused by the LSP had some influence on the flow of TCP packets.

Experimentations done on the MPLS also yielded results based on the maximum throughput of the system which was measured by the routers that were configured to handle traffic flows. Compared to the earlier simulation, it was observed that the throughput measured between the routers that combines the shortest path and the longest path experienced load balancing. While in the earlier simulation, there were some nodes that had to carry more load than others. The throughput measured for the TCP traffic travelling along the ingress and egress routers reached a maximum value of 28247.78 bits/second. It was noticed that the throughput starts to rise after a period of 120 seconds from the beginning of the simulation.

From the result of the simulation study, it was noticed that long paths were utilized better i.e. the traffic engineering qualities of the MPLS was more evident with such paths. It was observed that there was no throughput at the non-shortest path without the traffic engineering provided by the MPLS. Without the traffic engineering of the MPLS, TCP traffic would experience more bandwidth deprivation when competing with its UDP counterpart along the shortest path. The MPLS reduces congestion on the network because it carries more UDP traffic by default whenever edge routers have shortest path configurations.

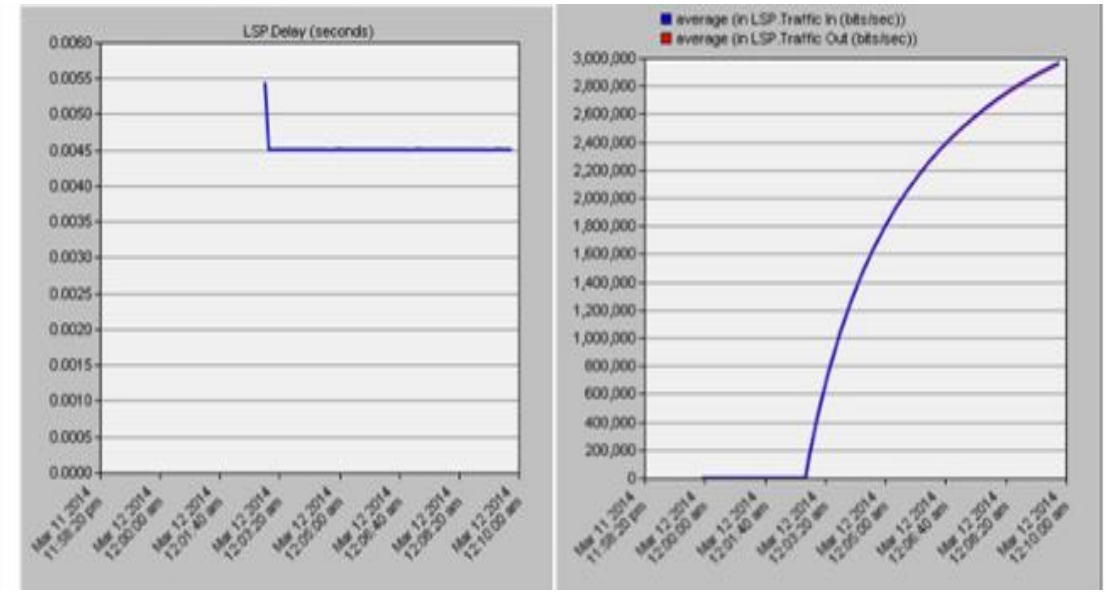


Figure 5. Showing the Impartation of the LSP

3.2. VPN-MPLS SIMULATION SCENARIO RESULT

For the VPN-MPLS simulation Scenario, The VPN delay statistics gives the end-to-end delay for traffic through an MPLS VPN network. This delay is measured as the time elapsed between traffic entering the Provider's network through the Ingress PE and traffic departing the Provider's Network through the Egress PE. Figure 6 illustrates the VPN delay for 500 calls per hour. The sample mean of the VPN delay is 4.69E-006.

The network throughput and load are main parameters that reflect the network capability. By definition, the load is the amount of VPN traffic that enters the Provider's network through the Ingress PE while the throughput is the amount of VPN traffic that leaves the Provider's network through the Egress PE. Figure 7 shows the MPLS VPN load for 500 calls. It was observed that the sample mean for the load was 3814132 bit/s. From Figure 8, it was observed that the sample mean of the VPN throughput was 3822233.94 bit/s.

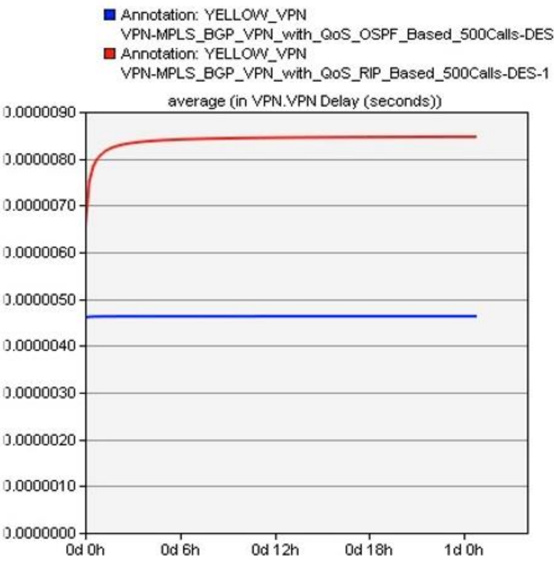


Figure 6. MPLS-VPN delay

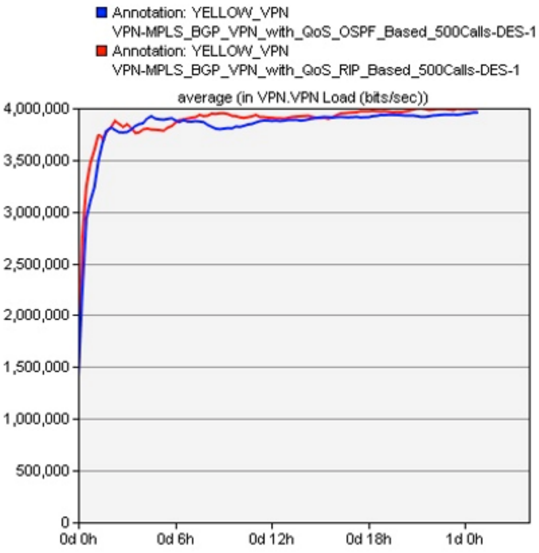


Figure 7. MPLS-VPN load

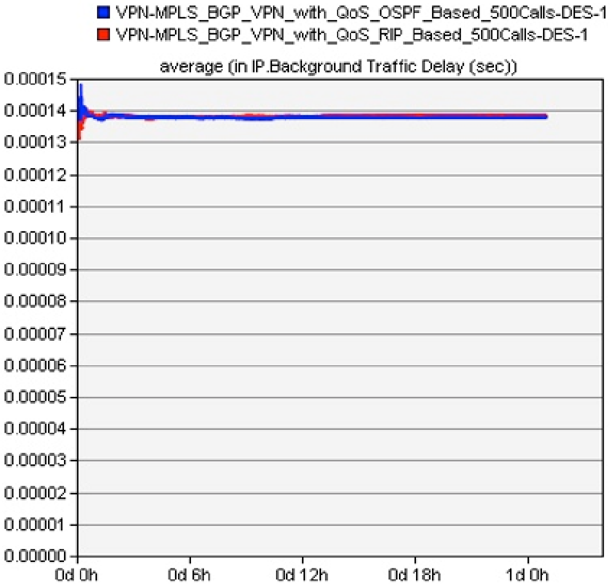


Figure 8. VPN-MPLS throughput

4. Conclusion

This simulation study aims to analyze and compare the performance metrics of an MPLS based VPN to that of a traditional VPN network using VoIP as the test bed. The analysis and comparison is followed by presenting an approach in OPNET® modeler 14.5 to obtain the performance metrics.

In this paper, a combination of theoretical research and empirical research were used. It began with a literature review of the relevant state-of-the-art in MPLS, VPN and MPLS-VPN. The simulation study yielded observations about the following areas:

a. The challenges in MPLS based VPN network with respect to IP QoS
b. How MPLS based VPN with IP QoS influences delay in VoIP network
c. The best scenario for VoIP traffic.

It was found that MPLS VPN based on the interior routing protocol (OSPF) and exterior routing protocol (BGP) with IP QoS is the best scenario for VoIP traffic. MPLS VPN architecture is scalable and flexible enough to provide well organized voice packet transmission, load balancing, consistency, data security, network isolation from other networks and end to end controlled connectivity with guaranteed QoS.

References

[1] GK Widi, ML Baihaqi, AS Nugroho, SS Hidayat. The Efficiency Test of Additional Multi Protocol Label Switching Network Protocol Over Open Shortest Path First Network Using Graphic Network Simulator 3. *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS).* 2015; 15: 100-106.

[2] MY Hariyawan. Comparison analysis of recovery mechanism at MPLS network. *International Journal of Electrical and Computer Engineering (IJECE).* 2011; 1: 151.

[3] NE Rikli, S Almogari. Efficient priority schemes for the provision of end-to-end quality of service for multimedia traffic over MPLS VPN networks. *Journal of King Saud University-Computer and Information Sciences.* 2013; 25: 89-98.

[4] MN Soorki, H Rostami. Label switched protocol routing with guaranteed bandwidth and end to end path delay in MPLS networks. *Journal of Network and Computer Applications.* 2014; 42: 21-38.

[5] M Kolhar, MM Abualhaj, F Rizwan. QoS Design Consideration for Enterprise and Provider's Network at Ingress and Egress Router for VoIP protocols. *International Journal of Electrical and Computer Engineering (IJECE).* 2016; 6: 235.

[6] BG Józsa, M Makai. On the solution of reroute sequence planning problem in MPLS networks. *Computer Networks.* 2003; 42: 199-210.

[7] YQ Fan, H Fan, C Sun. OPNET-Based Computer Simulation of MPLS VPN Security Solutions. *Applied Mechanics and Materials.* 2011: 361-365.

[8] SI Popoola, AA Atayero, N Faruk, JA Badejo. Data on the key performance indicators for quality of service of GSM networks in Nigeria. *Data in Brief.* 2018; 16: 914-928.

[9] A Ezenwoke. Design of a QoS-based Framework for Service Ranking and Selection in Cloud E-marketplaces. *Asian Journal of Scientific Research.* 2018; 11: 1-11.

[10] H Ifijeh, F Idachaba, I Oluwafemi. *Performance Evaluation of The Quality of VoIP Over WLAN Codecs.* Proceedings of the World Congress on Engineering. 2015.

[11] D Grayson, D Guernsey, J Butts, M Spainhower, S Shenoi. Analysis of security threats to MPLS virtual private networks. *International Journal of Critical Infrastructure Protection.* 2009; 2: 146-153.

[12] DO Awduche, B Jabbari. Internet traffic engineering using multi-protocol label switching (MPLS). *Computer Networks.* 2002; 40: 111-129.

[13] IM Yelmo, D Larrabeiti, I Soto, P Pacyna. Multicast traffic aggregation in MPLS-based VPN networks. *IEEE Communications Magazine.* 2007; 45.

[14] S Srivastava, A van de Liefvoort, D Medhi. Traffic engineering of MPLS backbone networks in the presence of heterogeneous streams. *Computer Networks.* 2009; 53: 2688-2702.

[15] R Mishra, H Ahmad. Comparative Analysis of Conventional IP Network and MPLS Network over VoIP Application. *International Journal of Computer Science and Information Technologies.* 2014; 5: 4496-4499.

[16] KN Qureshi, AH Abdullah. Multiprotocol Label Switching in Vehicular Ad hoc Network for QoS. *Information Management & Business Review.* 2014; 6.

[17] KN Qureshi, AH Abdullah, AN Hassan, DK Sheet, RW Anwar. Mechanism of Multiprotocol Label Switching for Forwarding Packets & Performance in Virtual Private Network. *Middle-East Journal of Scientific Research.* 2014; 20: 2117-2127.

[18] O Obinna, O Kennedy, O Osemwegie, N Nsikan. Comparative Analysis of Channel Estimation Techniques in SISO, MISO and MIMO Systems. *International Journal of Electronics and Telecommunications.* 2017; 63: 299-304.

[19] AA Atayero, OI Sheluhin, YA Ivanov. Modeling, simulation and analysis of video streaming errors in wireless wideband access networks. in *IAENG Transactions on Engineering Technologies*, ed: Springer. 2013: 15-28.

[20] Okokpujie KO, Okoyeigbo O, Okhaifoh JE, Osemwegie O, Nkordeh N. Performance Analysis and Modeling of MIMO Systems. *International Journal of Applied Engineering.*