Journal of Computer Science Review and Engineering | ***ISSN 1694-4488***
Published by AIR JOURNALS | *https://airjournal.org/jcsre*
16/18 Avenue des Longaniers, Quatre Bornes, Mauritius
airjournals@gmail.com; enquiry@airjournal.org

RESEARCH ARTICLE

Simulation Analysis of Network Metrics on Virtual Private Network Through Multi-Protocol Label Switching

Ogbu, Mary Nnenna C[1*]; Okpala, Etomochi[2] and Ezeagwu, Christopher Ogwugwuam PhD[3]
[1&2]Department of Computer Engineering, Caritas University Amorji-Nike Enugu, Nigeria
[3]Department of Electronic and Computer Engineering Nnamdi Azikiwe University, Awka

Citations - APA

Ogbu, M. N. C., Okpala, E. & Ezeagwu, C. O. (2023). Simulation Analysis of Network Metrics on Virtual Private Network Through Multi-Protocol Label Switching. *Journal of Computer Science Review and Engineering, 7(2) 1-13. DOI: https://doi.org/10.5281/zenodo.8245033*

ABSTRACT

Multi-Protocol Label Switching is one of the packet-switching technology that uses fixed-length identifier labels to transmit traffic efficiently. The three main services an MPLS supports are Quality of Service (QoS), Traffic Engineering (TE), and Virtual Private Network (VPN). The forwarding mechanism and scalability features of this technology make it more suitable for carrying out real-time application traffic. This paper evaluated the network performance metrics for time-sensitive (video, voice) and Best-effort traffic (FTP, email) in an MPLS-enabled network. The functionality of the MPLS system was performed through the simulation approach using the Riverbed OPNET tool. Analysis of simulated results about network performance metrics shows that there was an improvement in the performance of Time-sensitive in Best-effort traffic on a Virtual Private Network over the MPLS backbone.

Keywords: *Multiple Protocol Label Switching Technology; Virtual Private Network; Time-sensitive; Best-effort Traffic; Network Metrics*

Introduction

The enormous rapid growth in the use of the Internet had made a big impact on the type of services requested from Virtual Private Network (VPN) enterprise customers. This also influences the kind of performance the VPN users demand from the Service Providers (SPs). Most Internet Service Providers and telecommunication operators had plans of improving their IP-based network infrastructures in terms of Quality of Service (QoS) performance. Multi-Protocol Label Switching technology is among the IP-based network. It is a data transmission technology that transmits packets from one network node to another using a four-byte length identifier label. This MPLS is an emerging generation technology that ensures reliable delivery of data services to various VPN users. The forwarding mechanism, packet control and scalability features of MPLS technology made this network more worthy for implementing real-time applications like voice and video. MPLS operates by integrating layer 2 information such as bandwidth utilization of a given network link into layer 3 elements of the network. The main routing mechanism of an MPLS which involves the transmission of IP packets from one node to another through an MPLS cloud can be classified into the following actions: the creation and distribution of label; the creation of a table at each router; the creation of label switched path; the insertion of a label; the forwarding of the packet.

Creation and Distribution of Label: An unlabeled packet from the customer network goes into an MPLS domain after the packet were classified into Forwarding Equivalence Class (FEC) by the LER. This LER creates the label and uses its LDP signaling to initiate the distribution of the label to the packet. It decides the binding of the label to the specific FEC. Abinaiya and Jayagetha (2015) clearly stated that an MPLS label can be created either during the construction of an MPLS architecture, the introduction of a new user (as a VPN customer) in the existing MPLS network, or the creation of new routers.

Creation of Table at each Router: Label Distribution Protocol exchanges labels and stores them in a table known as Label Information Base (LIB). The content of the table contains the mapping information between the input port and incoming port label table to an output port and outgoing label table. Table 1 below shows a sample of the LIB table. For instance, the LDP signaling at ingress LSR will assign a prefix of 101 to the packet transmitting from the VPN user with port number 2 and map it to the destination port number 5 which has 218 prefixes attached to it in the table.

Table 1: Sample of Label Information Base Table

Input Port	Incoming (input) Port Label	Output Port	Outgoing (output) Port Label
2	101	5	218
3	29	3	27

Creation of Label Switched Path:
LDP dynamically creates the Label Switched Path (LSP) - a unidirectional traffic path by which any labeled packet passes to reach the ingress LSR for a particular FEC. For the efficiency of the network, multiple LSP is usually established throughout any given network. Note that LSP is normally created in the opposite direction to the creation of an entry in the LIB.

Insertion of Label:
To find the next hop and request a label for the specific FEC, the first LER uses the LIB table created. It then inserts the label and forwards the IP packet to LSR. In a continuous process, the subsequent routers will use the label to find the next hop and forward the packet to it.

Forwarding of Packet:
Packet forwarding is the summary of the above-mentioned actions in which LER classify unlabeled packet, create label, table, and LSP, insert the created label, and finally forward the packet to the LSR. Then the subsequent LSR will examine the label in the received packet, substitute it with the outgoing label and forward it till the packet reaches the last hop where it will be removed. As soon as the label is removed from the packet, the packet will be out of the MPLS cloud then it will be delivered to the destination host as ordinary IP forwarding as shown in Fig. 1.

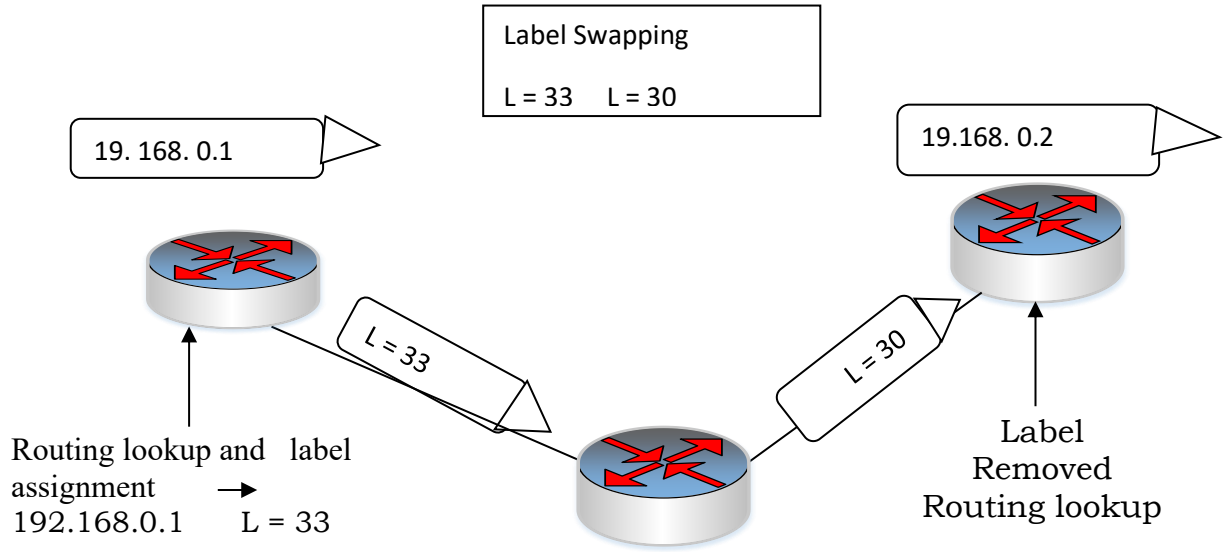


Fig. 1: Illustration of MPLS Packet Forwarding

However, the IP packet forwarding action does not depend on the longest address match as in the IP-VPN mechanism rather it depends on the label. This means that the MPLS mechanism helps routers to forward network traffic by looking at the label attached to the packet and not the destination IP address.

All these actions of MPLS can be summarized into three simple instructions namely:

I. **PUSH** (label Imposition)
II. **SWAP** (label switching)
III. **POP** (label disposition)

These three MPLS operational actions with instructions are illustrated in Fig. 2. The figure depicted how host VPN customer A sent an IP packet that passes to PE through the CE device. The LER (PE device) does layer 3 lookup, classifies the packet, creates a label, and distributes the packet toward the LSR (P device) till it reached egress LER of destination host B. Then the P device does label lookup, switches the label 1 (L_1) created to label 2 (L_2) and then forward the packet to the next hop. Also, the next hop PE device removes the label and forwards the label as an ordinary IP packet to the CE device that will deliver the packet to host B.

According to Eze *et al.* (2014), the main operation of LSR in an MPLS network is to push.

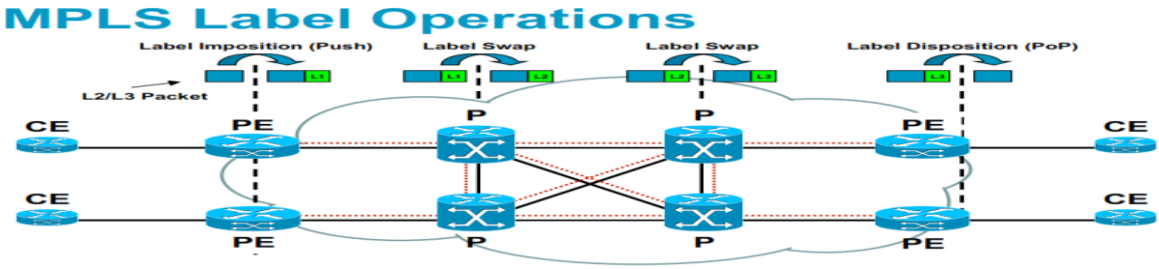


Fig. 2: Illustration of MPLS Operational action (Dasgupta 2010)

Adewale, et al. (2016) described routing as the transfer of a packet from a device on one network to another on a different network. Note that all PE and P routers run label-switching functions so that they can build MPLS label

Switched Path (LSP) from each PE to the next. (Almofary, *et.al*. 2013). With the evolution of the worldwide Internet Engineering Task Force (IETF) Kaur and Kumur (2010) emphasized that the MPLS concept was an additional range of IP-VPN which can provide enterprises with ease of management, reliability, price performance, and integrated end-to-end mobility.

Related Works

Abinaiya and Jayageetha (2015) carried out a survey work about the introduction of MPLS by the IETF group. According to the authors, IETF introduced MPLS as a standard–based transmission technology which made it available to every network vendor like CISCO, ALCATEL, and JUNIPER. This standard feature of MPLS ensures interoperability of different productions of vendors in a large network. Ibikunle, Oloja, and Esi (2013) in their work used MPLS to create VPN to virtualize campus networks that allow the isolation of multiple systems over a shared physical network. A layer 3 routed core in which other architectural building blocks were connected was used by the authors as the physical test bed. From the research work, distribution blocks of 1 to 3 were physically shared into two distributed switches and acted as PE devices in an MPLS core of the test-bed network. The test-bed network consisted of two of six CISCO 3725 Ether-Switch routers both for the distribution layers and access layer, also four CISCO 7200 routers used for edge routers. VPN was created in MPLS with virtualization which improved utilization (bandwidth /resources) and reduced the network delay. The authors recommended the implementation of Traffic Engineering in the Service Providers' MPLS network, especially when they are creating VPNs to boost and increase the overall efficiency of the networks.

Adewale, et al. (2014) created and simulated the performance of MPLS using two network topologies of Covenant and Landmark Universities. Traffic Engineering was implemented in the enabled MPLS and non-MPLS networks. It was observed that when MPLS was disabled, there was a lot of packet loss and delay unlike when it was enabled. The result of the simulation showed that MPLS-TE reduced routing path thereby ensuring an enhanced network performance by minimizing the traffic on a network segment and increasing the network throughput.

Aggarwal and Dhall (2015) studied the performance measures of an MPLS-TE network and a traditional IP network about real-time multimedia (video conferencing and voice-over IP) and non-real-time applications (FTP). Their work was characterized for both MPLS and traditional IP networks in different scenarios which are MPLS network with Traffic Engineering and IP network without Traffic Engineering. The work was experimentally done by considering two different network loads (during heavy and lighter load networks) in the two scenarios (MPLS-TE and Non-MPLS scenarios). The work equally evaluated the performance metrics like delay variations, end-to-end delay, throughput, packet drop, and page response time for different types of traffic (video, voice, & data) in a congested network for both MPLS and Non-MPLS networks. After simulation, it was observed that MPLS-TE was able to handle incoming traffic over several Label Switched Paths according to Forwarding Equivalence Class, unlike the Conventional IP network.

Ahmad, Alatky, and Jafar (2015) analyzed and evaluated the integration of MPLS and DiffServ mechanism. The work involved the integration of MPLS forwarding and DiffServ quality mechanisms to enhance the performance of most real-time applications. The DiffServ quality scheme helped to mark all the IP packets with different DiffServ Code Points (DSCP) at the LER routers. They presented a QoS performance analytical study of applications like video conferencing, mail, voice, and web over DiffServ with MPLS in IPv4 and IPv6 networks using the Optimized Network Engineering Tool (OPNET). The network performance was analyzed using the core of two virtual network environments (i.e. MPLS over core IPv4 and IPv6 network). The network topology used to carry out the simulation contains three routers as LER, five routers as LSR, two servers for FTP, and a database under four different applications (video, voice, data, and FTP). Weight Fair Queue class based on QoS techniques was implemented in the enabled MPLS IPv4 and IPv6 networks. The simulation results show that IPv6 performed better than IPv4 over the MPLS network in terms of throughput, delay, and jitter (Ahmad, Hamdani, & Magray, 2015). Ahmed and Basit (2014) and Khan (2012) said that Traffic Engineering (TE) was one of the services MPLS networks provide. In the work, TE was implemented in an MPLS network using the GNS3 simulation tool. The result showed how the TE improved the bandwidth and guarantee less delay in the network. The authors' emphasized how Traffic Engineering if implemented in an MPLS-enabled network helps to engineer traffic flow in a large ISP network.

Almofary, Moustafa, and Zaki (2013) explained the concept of Border Gateway protocol in MPLS-VPN concerning scalability. The authors used the OPNET modeler to study how Route-Reflector (RR) can be used to solve scalability problems in a network. Full mesh BGP topology was used between PE routers to enable MPLS and also RR. After simulation, the MPLS-VPN backbone including IGP with or without RR was compared. The results showed that the one with Route Reflector improved very well.

Banu and Ramachandran (2013) proposed the MPLS load balancing technique to improve the QoS for Voice over IP applications. An effective flow classification load balancing scheme was the technique implemented in the research work. Also, the priority of the network bandwidth utilization and arrival rate of voice packets based on the traffic flow was considered. Load unbalanced situations and congestion increases that resulted due to the failure of the network link were enhanced with the proposed technique. Free congestion and Label Switched Paths (LSPs) for multipath dispersion were created using Rainbow Fair Queuing mechanism. The technique was incorporated into the MPLS LSR router during the simulation. The results gave an efficient load-balancing improvement in the network. Using video streaming as the interactive real-time application of the proposed technique was recommended as further research work.

Efendi (2012) carried out simulation work to analyze how network parameters like latency and packet loss appear when multi-virtual routing and forwarding were implemented in an MPLS-VPN network. It was observed that the latency of data transmission and the percentage of packet loss were very small especially when IPSec tunneling was enabled in the network. And these metrics could not be increased by encapsulation and encryption process.

In the research work, Eze, *et al.* (2014) investigated an MPLS testbed called Multi Console MPLS-VPN model to ensure that the real-time services were delivered reliably with lower delays and high transmission speed. The implementation of Traffic Engineering into the MPLS model for efficient use of available resources and improvement of quality of service was carried out. The authors used only the simulation approach in the characterized physical testbed model as the research methodology. Their work evaluated the comparative performance analysis of multimedia traffic over MPLS-VPN by deriving several system models with a Label Switched Path (LSP) flow algorithm which was simulated in OPNET IT guru for both network scenarios. With this approach, the simulated results showed that multimedia traffic over MPLS-VPN performed better than conventional IP.

Simulation Approach

The developed schematic diagram of Cloud-Based MPLS-VPN (CBMV) tunneling representing what happened in one of the ISP networks in Nigeria is shown in Fig. 3. Each of the different partner sites is represented as one of the bank branches. They were symbolically represented as g_1, g_2, g_3, and g_4, then g_{chqts} as the corporate headquarter nodes. It was observed from the experimental results of the studied network analyzed in chapter four that the system cannot provide a robust network QoS performance. However, a simplified scheme that will drive a scalable MPLS-VPN with up to $K = 2^{10}$ remote sites/offices were proposed in this study. To achieve this, a discrete event simulation approach was used in the RIVERBED OPNET simulation modeler.

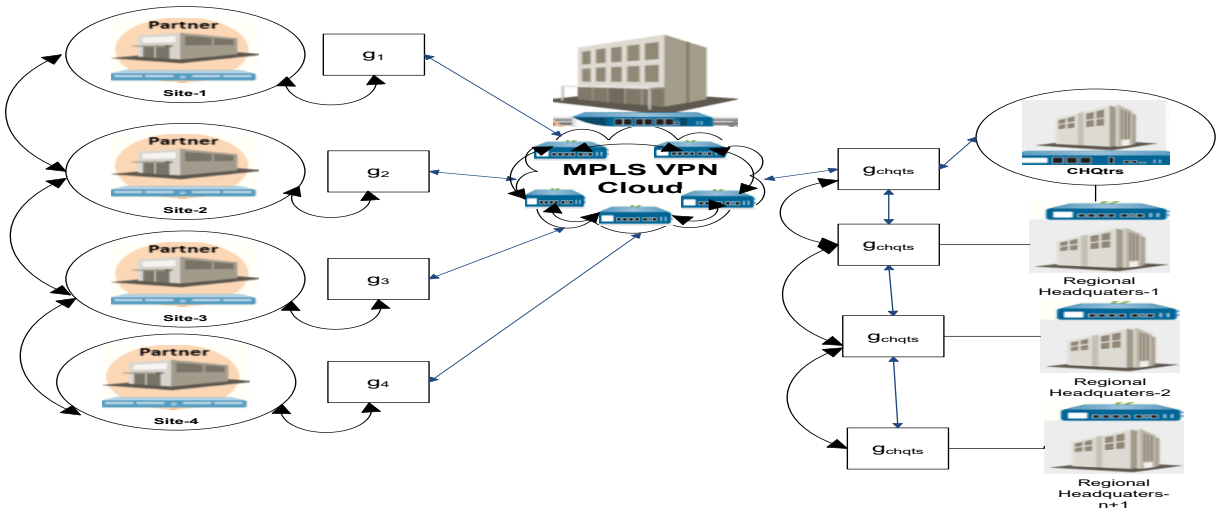


Fig. 3: Developed Cloud-Based MPLS-VPN Tunneling

Multiple MPLS services were enabled in the network as shown in Fig. 3. The schematic diagram of CBMV label stacking used in the simulation is shown in Fig. 4.

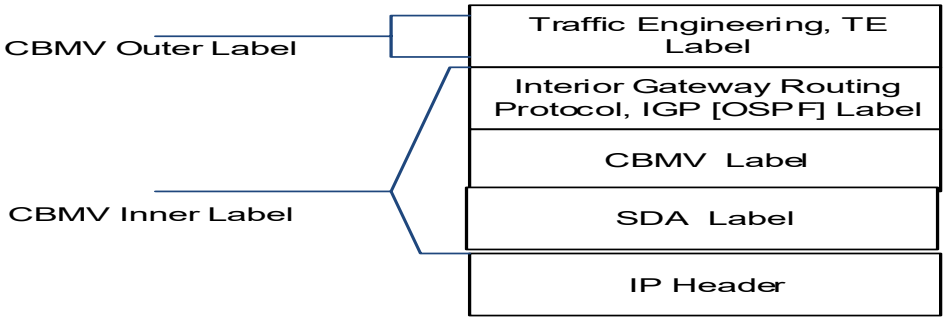


Fig. 4: CBMV Label Stacking for Optimal Traffic Tunneling

The CBMV service in Fig. 4 allows the support of the user multicast traffic in a Border Gateway Protocol (BGP) environment. IP-header gives support to multicast video, voice, and data traffic within the VPN which was used in the simulation testbed environment shown in Fig. 5. The label stacking of the MPLS IP header will help to improve QoS. This label stacking was used to study the behavior of MPLS-based networks and also to determine the impact of QoS metrics on MPLS-VPN performance.

The discrete event simulation approach is an approach that involves the use of trigger events and scenarios to create process nodes, traffic statistics nodes, and object nodes. With this discrete event approach network topology, network model, and network operation scenarios were created in the simulation platform. Application, profile, IP attribute, configuration, and failure recovery windows were loaded in the simulation platform. All these were configured in the platform and MPLS services were enabled.

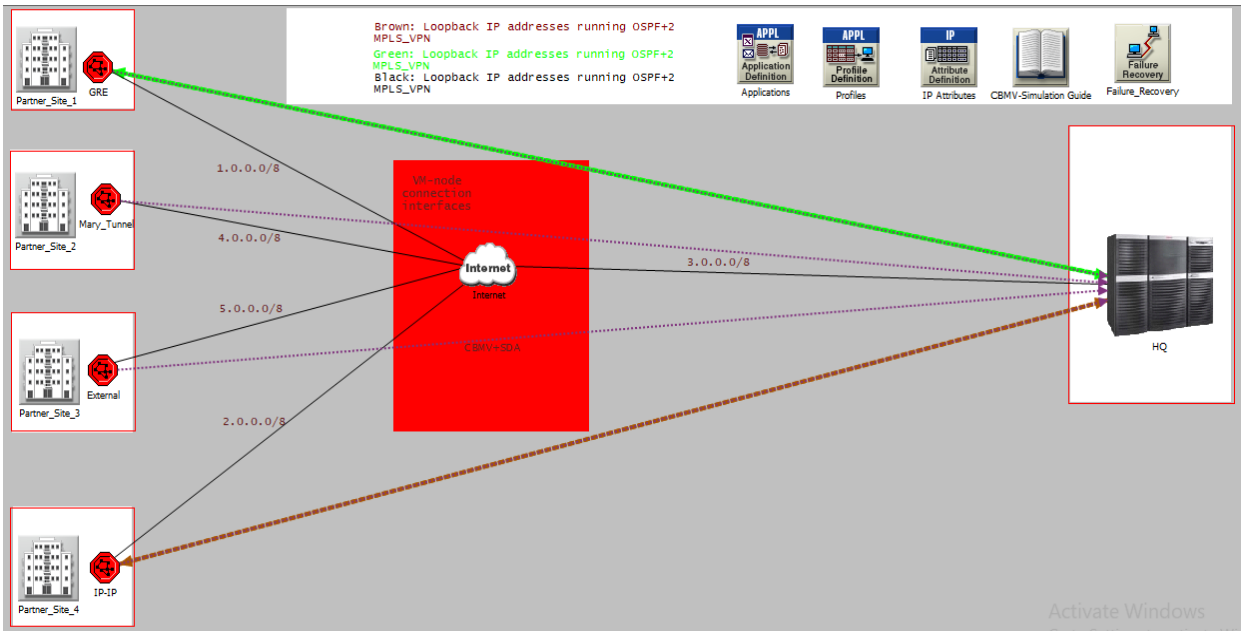


Fig. 5: MPLS-VPN Simulation Testbed

The testbed environment used for the simulation as a generic template for running this MPLS-VPN network was developed using RIVERBED OPNET modeler software version 17.5 as a simulation tool. RIVERBED was used to create the configuration of the networks. Riverbed OPNET modeler is a powerful simulation software that supports several protocols for the simulation of heterogeneous network contexts. It offers an easy way to implement an accurate and more versatile environment for carrying out complex network-related research. It is a high-level event-based network simulation tool that operates at the packet level.

This Riverbed OPNET modeler software version 17.5 is divided into three main hierarchies:
network domain, node domain, and process domain. In developing the CBMV network simulation, several modules from the Riverbed model library were used. These were highlighted below

I. Riverbed Modeler 17.5 simulator software with C++ engine.
II. The Compaq_Personal_Workstation_500 node models where both the server and client application are running were used for the workstation purposes.
III. Ethernet2_slip8_ler (LER) and Ethernet2_slip_lsr (LSR) node model.
IV. MPLS_LSP_Static model was used to create a Label Switched Path (LSP). This model was used to create static forwarding Tables.
V. Application_Config contains information on several parameters of real-time-sensitive and best-effort (non-real-time) applications and was referred to as the Profile_Config object. This element was used to tell the simulation tool the type of application that was modeled upon the network.
VI. MPLS_Config, QoS_Config, and Profile_Config functions were enabled.
VII. Four VPN_ sites/subnets were employed with their Media Access Control (MAC) controller, application data blocks, and LERs.
VIII. CISCO IOS Image that supports the MPLS features was enabled.
IX. Distance between LSR1 and LSR3, LSR2 and LSR3 is about 40 km while LSR1 and LSR2 are 5 km apart.

All these requirements and components were enabled and used in the simulation of system performance. Full system simulation with best-effort (FTP, data) and time-sensitive (video, voice) applications were carried out. The VPN edge routers were connected with VPN workstations with a ppp_adv link whereas the LSR core routers were connected with a ppp_ds3 link. To facilitate the determination of QoS metrics performance for both real-time-sensitive and best-effort dynamic traffic scenarios, the ppp_adv link was used as it supports variable data rates. Also, the ppp_ds3 link was used for interconnection between LER and LSR core routers. To visualize the impact of QoS

parameters in the presence of traffic variants, a PPP_ds3 link that supports a data rate of 1Gbps was employed. The network comprises workstations on which both the client and server applications are running for FTP/TCP, Video, and VoIP applications. From the five MPLS LSR routers at one end was an egress router (LSR node-2) and at the other end was an ingress router (LSR node 0). The other three routers are label switch compliant and hence referred to as MPLS-enabled LSR routers. In the simulation design, the LSPs were configured and set for designating the traffic path links. The profile configuration was set up for creating user profiles that map the application configuration. The application configuration describes the application running in different VPN sites, the remote load balancers, and VPN headquarters servers as well as the protocols used for the application. Now, the MPLS attribute definition responsible for configuring the traffic trunks and Forward Equivalence Class (FEC) were enabled.

This was done to check the performance of the MPLS-VPN. From the system architecture of the CBMV testbed, four VPN workstations were connected to the edge routers (LERs g1 to g4). Five clouds-based MPLS high-density routers (LSR 0 to LSR 5) were connected as shown in Fig. 5. The network topology used to carry out this research objective contains components of CISCO 6500 series routers with the same configurations for both non-MPLS and MPLS networks. All these routers were connected by point-to-point OSPF + 2 links working at a data rate of 1Gbps. OSPF +2 is an Open Shortest Path First of version two. Both traffic patterns were routed severally from headquarters to the corporate office for 90 seconds at any interval. Traffic workloads were generated based on the total number of packets sent. Each simulation reading was repeated a minimum of ten times and the mean value (average) of these samples was collected.

Simulation Parameters

All the configured and enabled parameters for the MPLS-enabled network are tabulated in Table 2.

Table 2: Simulation Parameters

Parameter	Values	Remarks
Number of VPN Workstations	4	Connected with ppp_adv link
Number of LER	12	connected by ppp_ds3 link
Number of LSR	5	connected by ppp_ds3 link
Number of Load balancer instances	3	Virtual Instantiation
Number of remote VPN Nodes	3	Virtual Instantiation
Traffic Types	Best-effort and Time-sensitive Traffic	Voice, Video and Data
Data rate	100Kbps	
MPLS Attribute Definition	Enabled for FIB	Traffic Trunks and FEC
Routing Protocols	OSPF+2, IP header	
Maximum Translation Unit (MTU)	1000 Packets MTU	
QoS Profile	Protocol based	
Link Capacity	1.5Mbps	
Network Architecture	MPLS-VPN	
Packet Rate	100Mbps	
Maximum Translation Unit (MTU)	1000 Packets MTU	
Packet Discard Ratio (PDR)	0.0%	
Profile Configuration	Enabled	
Application Configuration	Enabled	
Failure Recovery	Enabled	
IP QoS Attribute Block	Enabled	

Ethernet 4_Slip8_gateway (Cisco 39000 series routers- ISR) was employed in all the locations via PPP_ds1 links. This runs on Cisco IOS software for transporting IP traffic. The simulation compilation window is represented in Fig. 4. In each case, the OSPF+2 routing protocol was configured to run on the VPN tunnels to exchange routing information between the various VPN sites via the cloud core. Encapsulation and encapsulation delays were

configured on tunnels. Ethernet4_Slip8_gateway which runs on the IOS release 15.4 version was used. The IP header was used in the tunneling process into the LSR cloud domain.

Results and Analysis

The statistics of the selected QoS metrics as well as the HF and IPSec security issues were obtained and discussed later in the previous section. The virtualized load balancer sink was where all the QoS metrics were obtained while the window compiled the results which were imported into the MATLAB environment for easy graphical representations.

Throughput Analysis

From CBMV throughput data sets, given the network packet sizes as the simulation observation time, the average throughput of time-sensitive and best-effort traffic were analyzed. Recall that in the previous section of this chapter, it was stated that throughput response varies proportional to the packet rate of the transmission. Figure 6 illustrates the impact of the CBMV load balancer with VM Scheduling, as well as VLAN TE as shown in the corresponding variation of throughput as against packet rates. Both time-sensitive (voice and video) and best-effort (email) traffic were transmitted from the VPN branch partner site to headquarters.

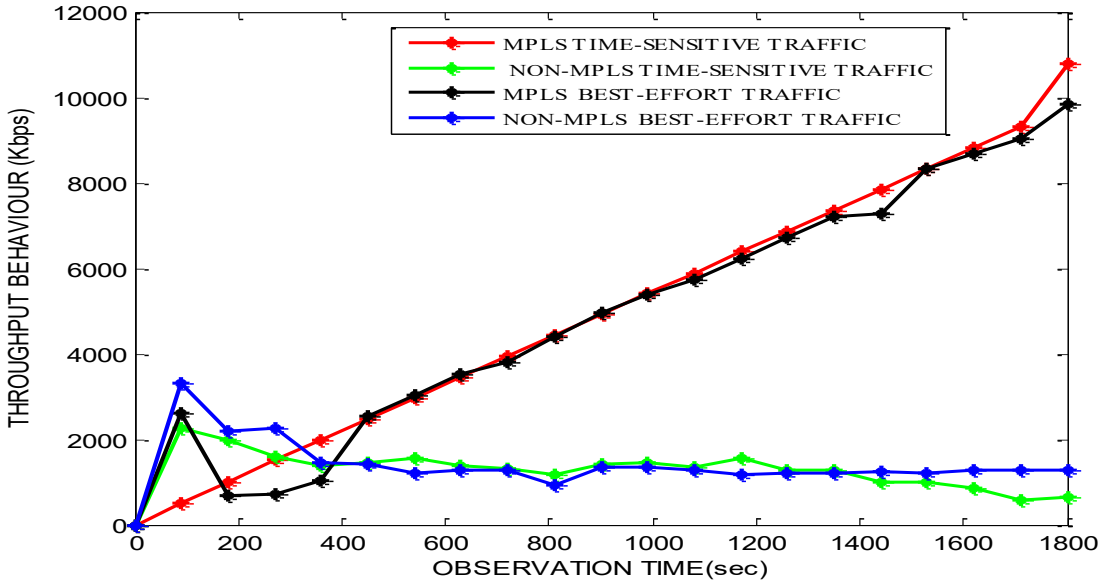


Fig. 6: Comparison of Throughput on Time-sensitive and Best-effort Traffic for MPLS and Non-MPLS Network

The throughput values for both time-sensitive and best-effort traffic increased as the traffic intensity (observation time) increased. Also, the logical mapping of the address in LSR in Fig. 6 reduces network density and ensures optimal traffic flow. In an MPLS-VPN network, the time-sensitive and best-effort traffic offered throughput responses of 51.20% and 48.80% respectively out of the available 110,000Mbits/sec throughput generation. The plot generally shows that the time-sensitive traffic offered better throughout compared with the best effort in MPLS and Non-MPLS. It was observed that the throughput in the MPLS network increased linearly with traffic work intensity (observation time) unlike Non-MPLS traffic which decreased. It was observed that the introduction of Resource Allocation/ Scheduling (RAS) and VLAN Traffic Engineering into the system, enhanced the efficient servicing of VPN traffic flow, thereby offering higher throughput in CBMV.

CBMV Delay Analysis

The traffic of both time-sensitive (voice and video) and best-effort (email) for MPLS and Non-MPLS is shown in **Fig. 7.** The graph shows that for a loaded MPLS-VPN scenario, delay deviations are relatively wide for time-sensitive (0.0027sec) 24.58% and best-effort traffic (0.0083sec) 75.42%. Though the deviation seems quite realistic, this signifies that the simulation results justify the real-life scenario. The lower the delay variation for time-sensitive

traffic, the better the performance of the network. With an excellent resource sharing and scheduling algorithm, the network delay profile was impacted.

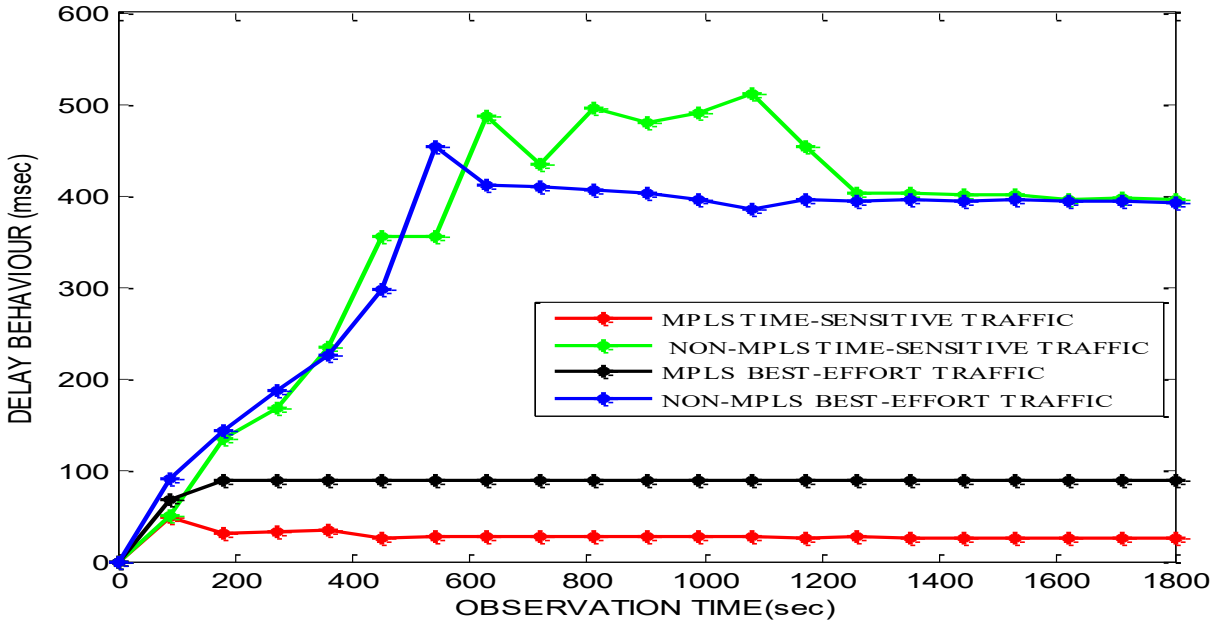
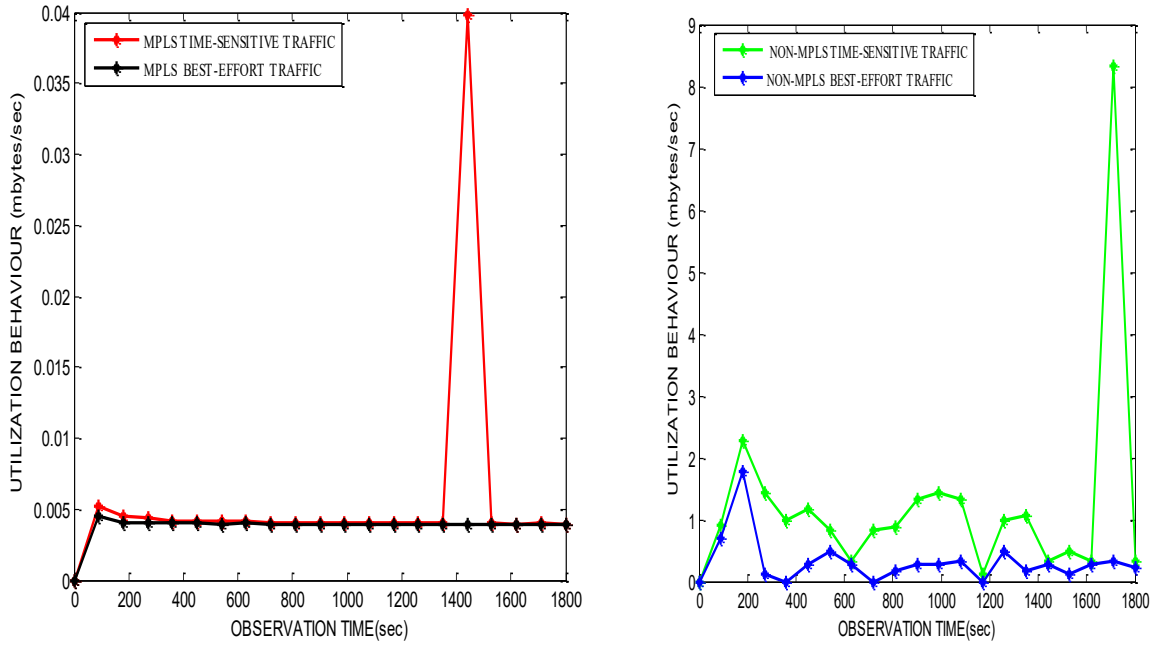


Fig. 7: Comparison of Delay on Time-sensitive and Best-effort Traffic for MPLS and Non-MPLS Network

CBMV Utilization Analysis

Recall that a virtualized Load Balancer with VLAN TE instantiations, Resource Allocation / Scheduling, all contribute to enhancing the overall network utilization by creating a uniform distribution of traffic throughout the network as well as minimizing congestion on any path to achieve the desired QoS. Comparative analysis of both time-sensitive and best-effort traffic for MPLS and Non-MPLS systems is tabulated in Table 2. Again, with a reduced network density and optimal traffic flow, resources can be assigned to user requests (traffic tasks) even under heavy VPN traffic tunneling. With the composite model for CBMV, load balancer, and hypervisor filtering schemes, efficient resource utilization was observed for both time-sensitive and best-effort traffic.



(a) MPLS Utilization (b) Non-MPLS Utilization

Fig. 8: Comparison of Utilization of Time-sensitive and Best-effort Traffic

The results were shown in Fig. 8. By employing system consolidation, the cloud-based MPLS network introduced into the individual network components' virtual machine instances (virtualization for the physical components) was highly useful in the CBMV LSRs' load balancers as well as the remote VPN site data centers. The implication was that both time-sensitive and best-effort traffic optimally utilized available scheduled resources. From Fig. 8(a), after the initial peak gradient, it was observed that the plot maintained a stable utilization pattern though having more resources drain on time-sensitive traffic (50.88%) compared with best-effort traffic (49.12%).

CBMV Packet Loss Analysis

The best-effort and time-sensitive packet loss response in MPLS and Non-MPLS scenarios is presented in this subsection. In MPLS-VPN, performance issues especially packet loss are a very serious problem. Link congestion resulting from queuing could result in packet discard. With bandwidth optimization using a hypervisor filtering scheme, Resource Allocation, and Scheduling (RAS), priority could be extended to time-sensitive traffic. Also, replacing a defective LSR, LER or even load balancer offered maximum throughput. It was observed from Fig. 9 that MPLS traffic applications had very negligible packet loss of less than 0.1 percent. This also shows that the traffic engineering efforts were significant in CBMV.

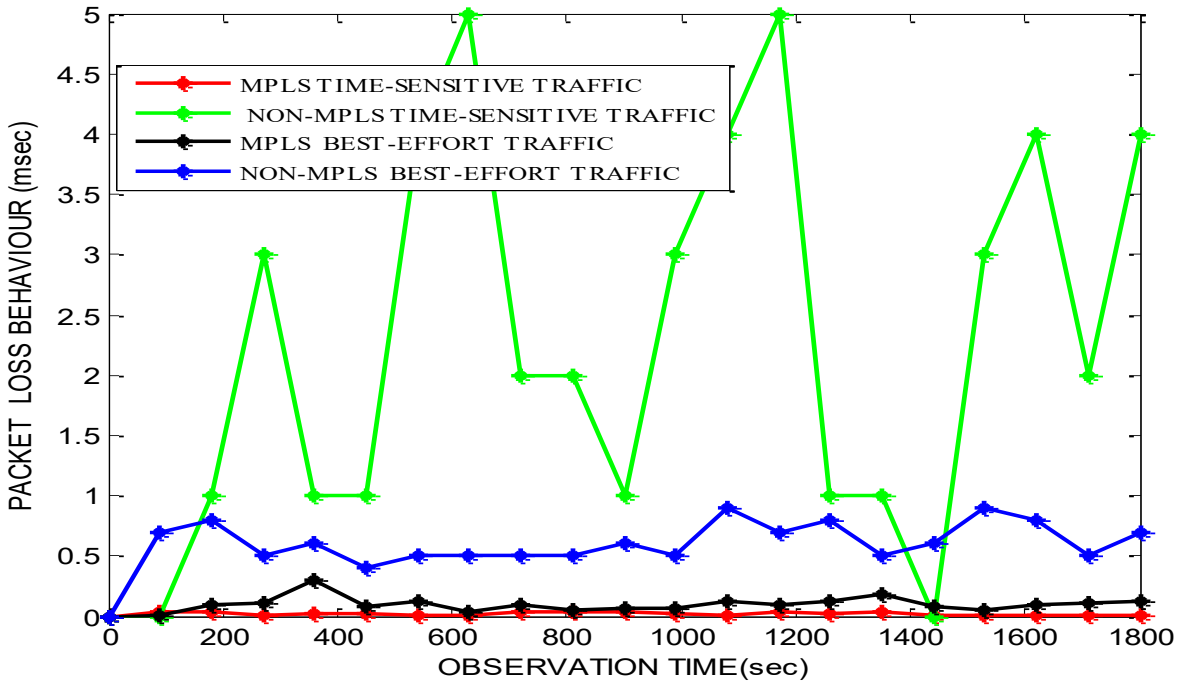


Fig. 9: Comparison of Percentage Packet Loss on Time-sensitive and Best-effort Traffic for MPLS

Conclusion

The main aim of this paper is based on the performance evaluation of MPLS networks for time-sensitive and best-effort applications. Analysis of the results related to network metrics such as throughput, delay, packet loss, and utilization within the nodes in the MPLS network shows significant performance in time-sensitive than best-effort applications. It was concluded from the simulation results that the evaluation of MPLD technology is necessary for the improvement of the performance of time-sensitive applications.

References

Ahmad, A.S., Alatky, T., & Jafar, M. (2015). Performance Analysis DifferServ based Quality of Service in MPLS Networks. *International Journal of Scientific & Engineering Research*, 6(9), 15-23.

Ahmed, M., & Basit, A. (2014). Implementation of Traffic Engineering and Addressing QOS in MPLS_-VPN based IP backbone. *International Journal of Computer Science & Telecommunication*, 5(6), 9-14.

Almfory, N.H., Moustafa, H.S., & Zaki, F.W. (2013). Scalability Aspects in BGP/ MPLS-VPN. *International Journal of Modern Engineering Science*, 2(2), 17-27.

Banu, F.J., & Ramachandran, V. (2013). Study of QoS Management Techniques for Voice Applications. *International Journal of Computer Science and Electronics Engineering*, 1(1), 80-84.

Efendi, R. (2012). A Simulation Analysis of Latency and Packet Loss on Virtual Private Network through Multi- Virtual Routing and Forwarding. *International Journal of Computer Applications*, 60(19), 50-56.

Eze, G.N., Onyeakusi, C.E., Adimonyemma, T.M., & Dial, U.H. (2014). Comparative Performance Evaluation of Multimedia Traffic over Multi-Protocol Label Switching using Virtual Private Network Internet Cloud and Traditional IP Networks. *International Journal of Emerging Technology & Research*, 1(3), 130-143.

Kaur, G., & Kumar, D. (2010). MPLS Technology on IP Backbone Network. *International Journal of Computer Applications*, 5(1), 13-16.

Khan, A., & Babar, I.K. (2015). Implementing Virtual Private Network over MPLS. *International Organization of Scientific Research Journal of Electronics and Communications Engineering*, 10(3), 48-53.

Nenghai, Y., Qiong, S., Yahnui, G., & Yuzhong, C. (2004). A Novel Approach to Improve the Performance of MPLS-VPN. 8th Korea-Russia International Symposium on Science and Technology, KO-RUS, pp. 35-39.

Ogbu, M.N., Onoh, G.N., & Okafor, K.C. (2017). Cloud-based Virtual Private Network using IP tunneling for Remote Site Interfaces. IEEE NIGERCOM 3rd International Conference on Electro-Technology for National Development, pp. 106-108.