IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 5, May 2016.
www.ijiset.com
ISSN 2348 – 7968

Performance Analysis of IPv6 Over MPLS & MPLS-VPN for Sana’a University

Dr.Malek N. Algabri[1], Dr. Sharaf A. Alhomdy[2], Gamil Alselwi[3], Ameen A. Alowiri[4] &Dr. Naif Sharaby[5]

[1]Asst. Prof., Dept. of Comp. Science, Faculty of Computer and Information Technology, Sana'a University, Yemen.
Email: malekye@gmail.com
[2]Assoc. Prof., Dept. of IT, Faculty of Computer and Information Technology, Sana'a University, Yemen.
E-mail: sharafalhomdy@gmail.com
[3]M.Ss. student, Dept. of Comp. Science, Faculty of Computer and Information Technology, Sana'a University, Yemen.
E-mail: gamil.alsalwi@gmail.com
[4]B.E. Student, Dept. of CE, Faculty of Engineering, Sana'a University, Yemen.
[5]Asst. Prof., Computer Center, Amran University, Yemen. E-mail: sharabi28@hotmail.com

Abstract

With the explosive growth in communication and network technologies there is a need to data or voice to be communicated. In addition, recent years have seen an increasing deployment and usage of IPv6 with the recent IPv4 depletion, this increase is going faster and we expect to see more and more IPv6 networks in a near future. IPv6 is considered to be the next-generation Internet protocol. For that, there are many techniques that are used for communication such as frame relay, ATM network, VPN, MPLS etc.

Therefore, this paper gives the detailed description of the comprehensive and effective study of the MPLS & MPLS VPN network technology focused on a specific aspect of the IPv6 deployment. The researchers have considered the use ofIPv6 MPLS VPN for Sanaa University due to the unavailability of a network to connect all the colleges affiliated to the University. The descriptions show the network construction of Sana’a University as a main campus and its other campuses which are far away from it such as Arhab, Mahaweet, Khawlan, Medicine colleges and the Old University campus.

The simulation is set up and configured to obtain results based on OPNET simulator. The experiment includes two scenarios: The first scenario is IPv6 over MPLS and the second scenario is IPv6 over MPLS VPN. The result of the experiment was promising.

***Keyword*:** *MPLS, VPN, ATM, QoS, PACKET, DELAY*

1. Introduction

In the resent years, there has been an explosive growth in the area of communication and network technologies that is required a great demand of IPv6 addressing scheme. IPv6 is considered to be the next-generation Internet protocol. However, the development of IPv6 which removes the limitations imposed by IPv4 and provides the large number of address space. The Internet protocol architecture is designed for end to end connectionless packet services using IP Protocol. Furthermore, everyday this network goes larger and larger, sothe services become more needed by the costumers which are offered on the Internet. Such these services, MPLS based on IP that is a new WAN technology currently being standardized by IETF[1]. It specifies framework to manage traffic flows between different devices and/or applications to addresses key requirements of Internet Service Providers (ISP). ISPs can use MPLS mechanisms for improved traffic engineering and load balancing in their core Internet backbone. MPLS is a flexible tool that enables advanced services such as IP based VPNs.

In addition, MPLS is a protocol independent and allows for the mapping of IP addresses to MPLS labels, which are used to forward packets through the MPLS network. It supports a number of the standard routing protocols such as Enhance Border Gateway Protocol (EBGP), OSPF, and resource reservation protocol (RSVP) [1, 2]. It allows routers to reduce their processing overhead and provided new traffic engineering opportunities, it also supports tunnelling and new VPN technologies. Such this technology called MPLS-VPN, it is typically provided to an enterprise from a third party provider to create a secure connection between branch offices. With those definitions understood, an MPLS-VPN is a VPN that is built on top of an MPLS network, usually from a service provider, to deliver connectivity between enterprise office locations. Fig (1) illustrated the MPLS VPN [3].

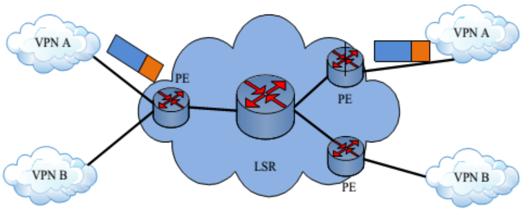

Fig (1): MPLS VPN

The primary focus of MPLS was to remove the overhead associated with route lookups. As frames enter an MPLS network, a look-up is performed at the edge of the network and a label is added to the frame as it is forwarded. All router decisions in the MPLS network are accomplished by comparing the incoming MPLS label with a label forwarding table that tells the router which port to send it out and with which new label to attach. The routers at the edge of an MPLS network known as Label Edge Routers (LER) are the only one that perform an IP address look-up, all other routers known as Label Switch Routers (LSR) make decisions based on the label-forwarding table [3-4].

This paper describes the details of the comprehensive and effective simulation study of the MPLS & MPLS VPN network technology focused on a specific aspect of the IPv6 deployment. It focused on the IPv6 in MPLS &MPLS VPN for Sanaa University due to the unavailability of a network to connect all the colleges affiliated to the University that enhance the associated communication between the different colleges.

The paper has been organized in a flexible manner. Section II focuses on the background related to the previous work. Section III explains network design place for area of study. Section IV describes the network topology use in our simulation. In section V, a network scenarios & simulation parameters have been configured and built on the OPNET simulator. Analyzing the experimental result shown in section VI. Conclusionand future work assignments will be highlighted in section VII.

2. Background

MPLS is essentially a labelling system designed toaccommodate multiple protocols. It was originally presented as a way ofimproving the forwarding speed of routers. The MPLS technology is now emerging as a crucial standard technology that is being used by many ISPs. Traffic engineering and VPN support are examples of two key applications where MPLS is superior toany currently available IP technology.

There are several researches that have been concentrated on theMPLS network performance over thelast decade.Therefore, this sectionintroduces the reader to basic concept and terminology about MPLS and VPN.Awais[5], studied on an enable the traffic-engineering concept using IGP for delay sensitive traffic which performs better for delay sensitive traffic using MPLS. His proposed solution is validated using OPNET.

Akhilesh Kumar[6],had compared MPLS based network with conventional Internet Protocol based network. He comprised is made based on the metrics suchas packet end-to-end delay, packet send and received. The results and the practical implementations show that MPLS based network provide much better results than simple IP based network. Almandhari [7], focused on the performance evaluation of MPLS recovery mechanisms by developing a new generic modeling framework as a layered approach on top of OMNeT++ simulation tool. Ramadaa [8], proposed an algorithm which ensures real-time tunnel performance monitoring in MPLS networks with Traffic Engineering, giving the operator detailed insight into the network operation, and thus providing the ability to evaluate network performance and simplify troubleshooting.

Rozita[9], analyzes the performance of VoIP traffic in BGP-MPLS IPVPN between two interior routing protocols namely EIGRP and OSPF. The combination of MPLS and conventional routing improve the forwarding mechanism, scalability and overall network performance.Using OPNET to simulate both scenarios and metrics such as delay, jitter and mean opinion score value are measured. The simulation result shows OSPF and BGP-MPLS VPN provides better infrastructure for VoIP VPN application.

Luca[10], devoted to VPNs designed with MPLS, one of the most elusive protocols of the network stack. Saying that MPLS is “elusive” is not overemphasizing: starting from its arduous fitting within the ISO/OSI protocol stack, continuing with its entangled relationships with several other routing and forwarding protocols (IP, OSPF, MPLS-BGP, just to name a few), and ending with the complex technicalities involved in its configuration.

3. Network Design Place

Sana'a University was established in 1970 in the capital cityof the Republic of Yemen. Yemen is located in the Middle East. Sana'a University is the biggest &oldest Governmental University in the country. It includes many colleges and development centers.It contains about 70,000 students, 3000 professors& their assistants and 1500 employees.Therefore, this section describes Sana'a University campuses which are locatedin 6 different distant areas such as the old University campus, Medicine and the new campus in the capital city, and Khawlan, Arhab, and Almahweet in other Governorates which are far away from the main campus as seen in Fig.(2).

Fig (2) shows the outline of the network of the six areas for simulation study. Unfortunately, there is difficulty to connect all these areas due to difficult geographical nature in these areas. Therefore, this study describes the importance of using the MPLS-VPN to connect such areas. Moreover, each campus consists of a group of colleges that are close to each other which can easily be connected internally with either same technique. Table (1) shows a description of the areas, some of the colleges affiliated to the university.

ISSN 2348 – 7968

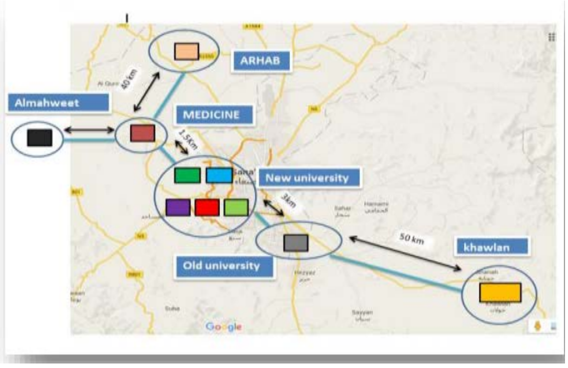

Fig (2): Sana'a University Outline

Table (1): Sana'a University Collages

Area No.	Area Name	College Affiliated
1	New University (Main campus)	- College of Engineering - College of Computer & IT - College of Agriculture - College of Language - College of Information - College of Education - College of Commerce - College of Law - Centers - Administrations Building
2	old university	- College of ART - College of Science
3	Faculty of Medicines	- College of Medicines - College of Pharmacy - College of Dental
4	Faculty of Khawlan	- Education - Arts - Science
5	Faculty of Arhab	- Education - Arts - Science
6	Faculty of Almahweet	- Education - Arts - Science

4. Network Topology

This section describes the network topology used in our simulation for Sana'a University which has many campuses, some of them located in remote areas from the main campus, namely, Khawlan, Almahweet and Arhab as shown in Fig. (2) &Table (1).Such areashave difficult geographical nature.Thus, it is not easy to connect them. Therefore, in this case, the solution can be made by using MPLS VPN through Internet connection that allowsto access to all thecollegesaffiliated to Sana'a University according to the nature of the network. The server leads the voice, video applications, Internet access and other services.Therefore, two suggested networks topology modulethat will be simulated namelyIPv6 MPLS &IPv6 MPLS VPN show in Fig (3) & Fig (4) respectively.

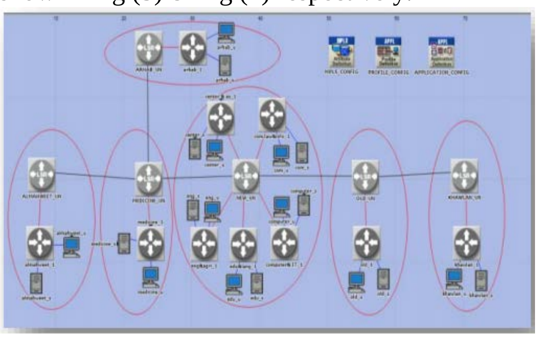
Fig (3): Scenario IPv6 MPLS

5. Network Scenarios & Simulation Parameters

This section describes two scenarios that have been employed in the network simulator (OPNET Module 14.5).These scenarios are prototyped as follows:

- Scenario 1: IPv6 over MPLS backbone.
- Scenario2:IPv6 over MPLS VPNbackbone.

In both scenarios the center area consists of 6 LER, 1 LSR routers. These routers are connected with point-to-point DS3 cables of data rate 44.736 Mbps. The end nodes are connected to LER with 100baseT cables of data rate 100 Mbps. These elements are the following:

- 6 LSR routers.
- 10 PPP workstations
- 10 PPP servers
- 10 LER routers
- DS3 links between LSRs routers
- 100baseT links between LERs and workstations and servers.

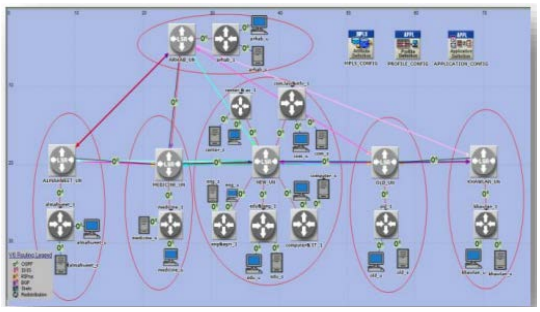
Fig (4): Scenario IPv6 MPLS VPN

Fig. (3) illustrates the first scenario, it shows that the routers installtheLSRand associatedto routers of typeof LERsuch as each LSRrepresents for each area. In addition, the LER represents thecollegeorcollectionofthe colleges.On the other hand, Fig (4) shows the second scenario which adds the VPN to the MPLS network as a new service thatwill be used across the Internet instead of using cabling between these colleges. The addresses for each network components added to the simulation. The OSPF protocol uses routing process. The link of type DS3 of 100BaseT between the routers is added to each router.

In the profile we define services that have been installed in the applications of this network. A new object known as MPLS VPN configuration will be defined and control the network components. After all the operations, the Traffic-Engineering is installing to the network to define the path or the Label Switching Path (LSP). The used communication environments are known as delay and data traffic (either sent or received).

Further, the traffic such as voice and video conferencing will be generated. The video and voice can be controlled in term of start, end, and repeatability. Tables (2 & 3) show the parameters environment for the voice & video setting. The application traffic priority through Type of Service (ToS) attribute which is configured as DSCP uses assured forwarding G.711. The encoder scheme used in voice/video is framed per packet attribute. The number of encoded voice frames is grouped into a voice packet before being sent by the application to the lower layers. The ToS represents a session attribute which allows for packets to be processed faster in IPv6 queues which compresses delay and decompressing a voice packet.

Table (2): Voice Environment Parameters

Voice application		
PCM Quality Speech		
Silence Length	Incoming Length	Exponential (0.65)
	Outgoing Length	Exponential (0.65)
Encoder Scheme		G.711
Voice Frames / Packet		10
ToS		Interactive (voice(6))
Compression Delay (s)		0.02
Decompression Delay		0.02

Table (3) : Video Environment Parameters

Video application	
High resolution video	
Frame interval time information	30 frames / s
Frame size information(bytes)	352*240 pixel
ToS	Streaming multimedia(4)

6. Result Analysis

This section describes the simulation studies to capture the network trace. The simulation studies were performed by exploiting the OPNET Module of 14.5 simulator. The results show that the running time of the voice and video conferencing is 15 & 30 minutes when using different parameters of two scenarios as mentioned in the previous section. These parameters are described as follows:

6.1 Packet Delay Variation

This statistic gives the average packet delay variation (jitter) for traffic through the MPLS & MPLS-VPN. This delay variation is measured as the time elapsed during the transmission of packets from the source to destination in the network under constant load. Fig. (5) & (6) show the average packet delay for two different running times 15& 30 m respectively. We note that, in the voice application the delay is 0.15699ms in first scenario while it is 0.05599ms in second scenario. The delay of the video application is 2.246635ms in first scenarios, whereas it is 1.34169ms in the second scenario. Hence, the results shown that second scenario has performed lesser delay variation as compared to first scenario.

6.2 Packet End To End Delay

When the packets have transmitted from source to destination, the end to end delay time would be considered. If the packet takes too much time to arrive, it will cause delay in the whole process. Therefore this delay has a critical effect on the performance of a communication network. Thus, if the end to end delay is long, the packet can be efficiently destroyed. Fig (7) & (8) show that the results in the second scenario has performed lesser end to end delay as compared to the first scenario in terms of different running times that are 15 & 30m

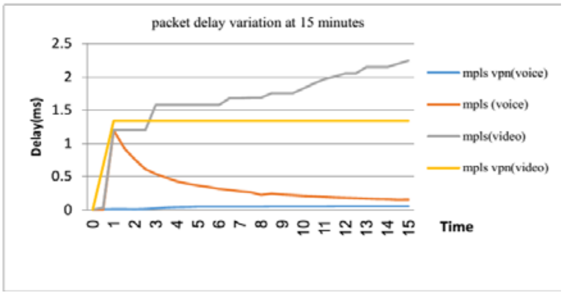

Fig (5): Packet delay Variation at 15 minutes

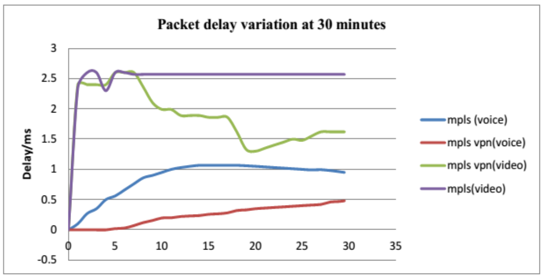

Fig (6): Packet Delay Variation at 30 minutes

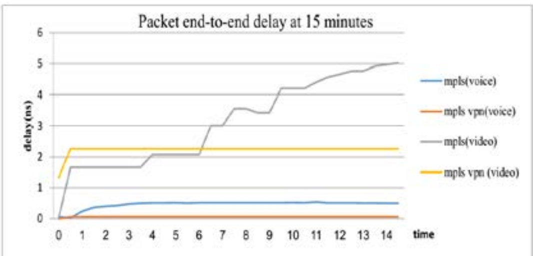

Fig (7): Packet End-to-End Delay at 15 minutes

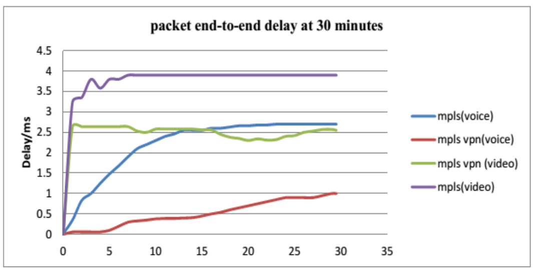

Fig (8): Packet End-to-End Delay at 30 minutes

6.3 Traffic Send (Packet/Sec)

The average sent and received voice/video traffic are presented in Fig. (9) & (10) for different running times that are 15 & 30ms. We note that the more the amount of time is increased, the more the number of packets per second are sent and received. The result shows that the performance of sent and received packets of IPv6 MPLS VPN is better than those of IPv6 MPLS.

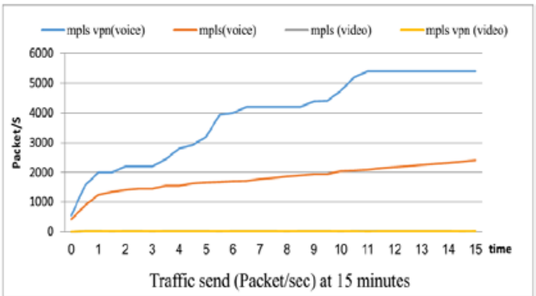

Fig (9): Traffic Sent (Packet/s) at 15minutes

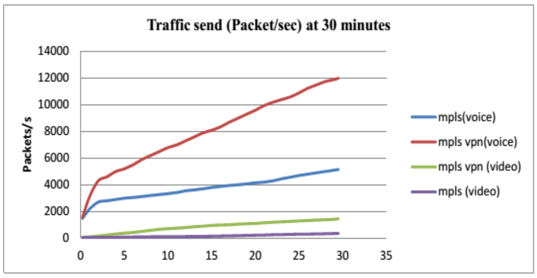

Fig (10): Traffic Sent (Packet/s) at 30 minutes

7. Conclusion & Future Work

In this paper, we have presented a comparative analysis, using Opnet module 14.5, the behavior of MPLS connection base on IPv6 VPN tunnel for connecting all colleges affiliated to Sana'a University.The comparative analysis has been done in the two scenarios: The first scenario is IPv6 over MPLS and the second scenario is IPv6 over MPLS VPN.Performance has been measured on the basis of some parameters that aimed to figure out the effects of IPv6 on the MPLS backbone. The simulation run time were 15 & 30 m. The result of the experiments was promising.It shows that MPLS VPN is better than MPLS.

Thus, we recommend using the MPLS VPN for connecting all colleges in different sites affiliated to Sana'a University.The main benefits of this technique are; safety, low-cost, all of this is done via the Internet connection which is available to use. So, it will be able to send, receive, processing and analysis data. Further, wethenutilized a networktraffic generatorto create typicaldomain name queries, file service including voice & video and Internet destined email & web traffic fordifferent sites.In future, a research work can be done on theexplicit features to connect the different Universities in Yemen with Ministry of Higher Education.

Reference

1. DivyaSharma& et al. (2015), "A Detail Review on Multiprotocol Label Switching (MPLS)", International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015 India.
2. Firdous A. Khan, et al. (2014) "Performance Analysis of IPv4 & IPv6 over MPLS", International Journal of Computing and Network Technology, Vol. 2, Issue 3, India.
3. Md. Tariq Aziz & et al. (2012) "Effect of Packet Delay Variation on Video/Voice OverDiffserv-MPLS in IPv4/IPv6 networks", International Journal of Distributed and Parallel Systems (IJDPS) Vol. 3, No.1.
4. Mahmoud M. Al-Quzwini, Sarmad K. Ibrahim, (2012), "Performance Evaluation of Traffic Engineering Signal Protocols in IPv6 MPLS Networks",Communications and Network, Vol. 4 No. 4, 2012, pp. 298-305
5. AwaisQasim, et al. (2015)"Traffic Engineering Using Multi-protocol Label Switching (MPLS) for Delay Sensitive Traffic." Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference on IEEE.
6. KumarAkhilesh, et al. (2015), "Performance evaluation of IP network and MPLS network using NS2 simulator." Futuristic Trends on Computational Analysis and Knowledge Management (ABLAZE), 2015 International Conference on. IEEE, 2015.
7. Almandhari, et al. (2015) "A performance study framework for Multi-Protocol Label Switching (MPLS) networks." GCC Conference and Exhibition (GCCCE), 2015 IEEE 8th. IEEE, 2015.
8. Ramadaa, et al. (2015) "Network performance monitoring within MPLS traffic engineering enabled networks." Software, Telecommunications and Computer Networks (SoftCOM), 2015 23rd International Conference on IEEE.
9. Yunos, et al. (2013),"Analysis of routing protocols of VoIP VPN over MPLS network." Systems, Process & Control (ICSPC), IEEE Conference.
10. Cittadini, Luca et al. (2012) "MPLS virtual private networks." Recent Advances in Networking.