

Performance Evaluation of Multi-protocol Label Switching-Traffic Engineering Schemes

Iflah Aijaz¹, Sheikh Mohammad Idrees^{2,*}

¹Department of Computer Science & Engineering, Jamia Hamdard, New-Delhi, India.

²Department of Computer Science (IDI), Norwegian University of Science and Technology, Norway.

Abstract

Generally, the priorities of traffic engineering are one of two groups. The first is traffic-related performance targets like reducing packet loss, reducing end-to-end delay etc. Additionally, there are efficiency-related goals, such as a balance of traffic allocation through usable bandwidth resources. The performance goals associated with traffic are set to reach the contracted level of services and offer customer's competitive services. All communication through this link is disrupted if a network connection is not established. Techniques to improve the effects of hardware-failure, networks have been used to replenish the traffic from the failed link to other working connections. The main theme of this paper is to develop methods and tools that study and evaluate Multiprotocol Label Switching (MPLS) and MPLS-Traffic Engineering schemes. These schemes are presented in order to improve the network performance in terms of resource utilization, delay and reliability. The simulations were performed in OPNET Modeler 14.5.

Keywords: Packet loss, end-to-end delay, traffic allocation, reliability, utilization, Multi-Protocol Label Switching, Traffic Engineering, OPNET Modeler 14.5.

Received on 10 August 2020, accepted on 25 September 2020, published on 08 October 2020

Copyright © 2020 Iflah Aijaz *et al.*, licensed to EAI. This is an open access article distributed under the terms of the [Creative Commons Attribution license](#), which permits unlimited use, distribution and reproduction in any medium so long as the original work is properly cited.

doi: 10.4108/eai.8-10-2020.166550

1. Introduction

MPLS (Multi-Protocol Label Switching) is one of the recent networking technologies used widely by most of the network service providers. Internet Engineering Task Force (IETF) came up with this idea originally in 1997 and since then has been popular for the routing efficiency and performance[1]. Internet Protocol (IP) uses IP switching, however, MPLS uses label switching. MPLS is a mechanism that forwards packets based on the information

present in the labels. MPLS label is a field of 32 bits with certain structure[2].

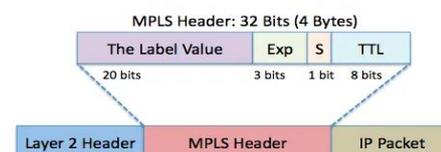


Figure 1 MPLS label

The label is comprised of following components:-

- 20-bit label value

*Corresponding author. Email: sheikh.idrees99@gmail.com

- 3-bit experimental bits for QoS (Quality of Service)
- 1-bit bottom of stack
- 8-bit Time-to-Live

MPLS has two major components[3]:

- a) Control Plane
- b) Data Plane

The control plane is the set of protocols that helps to set up the data of forwarding plane. Control plane includes routing protocols, the routing table and the other control or signaling protocols. Data plane also called as Forwarding Plane defines part of router architecture that decides what to do with the packet. It is the path of packet forwarding via a router or a switch. Data Plane consists of Forwarding Information Base and Label Forwarding Instance Base[2]. Unlike IP packets, MPLS labels are not forwarded on the basis of destination address. The labels are attached at the ingress router, swapped by intermediate routers and removed by egress router. These operations refer to push, pop and swap operation of MPLS labels in the label stack. IP lookup which is very complex is replaced with label lookup in Label Forwarding Information Base. One of the major benefits of MPLS is Traffic Engineering which uses the network infrastructure efficiently. The concept of Traffic Engineering is based on the concept to redirect the traffic through the link that are not utilized in IP routing since IP uses shortest path for forwarding packets. This shortest path gets utilized every time so congestion may result in case of traffic load.[4][5] However, MPLS traffic Engineering provides efficient spreading of traffic throughout the network avoiding under-utilized and over-utilized links. Traffic Engineering is also called Source Based Routing because the source router decides the path of the packets. Traffic Engineering is known to be one of the advantages of MPLS that efficiently uses the network infrastructures. The benefit of MPLS Traffic Engineering is Fast Re-Route which allows us to divert the traffic away from the link or node that has experienced a failure due to congestion[6]. It helps in identifying a substitute path that has the ability to overcome the link failure from source to destination node prior to this failure being resolved by Interior Gateway Protocol (IGP).

2. Literature Survey

The packet forwarding decision in a conventional IP network consists of three different processes: the routing protocols, the routing table and the process with the longest possible path. These three phases have been accompanied

by a forwarding decision and packets are switched from one router to another [7]. The shortest path becomes congested when all packets sent from various sources use only a shorter path between a pair of ingress and egress routers.[8]. Given the high cost of network infrastructure and the competitive nature of the provisioning of Internet services, service providers are involved in improving their networks' performance. Traffic management is one way to achieve this [9]. As the main technology for packet networks to improve packet forwarding efficiency, Multi-Protocol Label Switching (MPLS) has been recognized [10]. It also offers multiple services such as Traffic Engineering, Virtual Private Networks (VPN), etc. with QoS guarantees [11][12]. The MPLS system provides high-speed packet switching, routing and great scalability. MPLS TE consists of three steps. The first step is collection of information followed by monitoring and path signalling. [13] [14]. The authors in Paper [15] [16] primarily address the need for separate routing decisions on each incoming network for traditional IP networks. If a packet reaches a router, the router needs to check the next hop in the packet's IP header to find the packet target address in the routing table (longest match prefix lookup). That router runs BGP, OSPF etc. routing protocols for the creation of routing tables - router performs the same tasks, when a packet passes through the network, when determining the next step for the packet (i.e. router on the network conducts a routing search). The main problem with modern protocols for routing is addressed in [17] [18]. Such routing protocols do not take into account the capacities and traffic conditions as decisions are taken on routing. As a result, some network areas can get congested while other segments are under-utilized along alternative routes. Although the packets are dropped, even in the aspect of blocked links, the traditional routing protocol continues to transport traffic across these paths. In [19][20] these papers address traffic from TCP and UDP through MPLS networks, where TCP data flow started to decline very dramatically between source and ingress router as soon as UDP traffic starts to flow from the UDP source to the ingress router. But when MPLS-TE was introduced the throughput was recorded to an acceptable value. The TCP traffic did not have to reduce its traffic strength because it did not compete for network resources with UDP traffic. The reason is simple that TCP waits for the acknowledgement for every transmitted packet while as in UDP there is no such acknowledgement for the transmitted packet. Quality of Service (QoS) had also been implemented in order to achieve QoS routing for better network performance. Suhail Ahmad et al.[21] discuss the unmitigated deployment of QoS for traffic IPv6 in the backbone network MPLS in conjunction with the support of Differentiated Services, which has progressively evolved to the IPv4 Address Pool, and thus the development of the Internet Protocol (IP) continues to lead to the deployment of IPv6 QoS. This paper provides a QoS performance analysis with the help of MPLS in IPv4/IPv6 networks on certain applications like voice, video, mail and web via DiffServ. DiffServ and MPLS integration is

demonstrated and tested on the effectiveness of the DiffServ / IPv6 network. The ability to keep services running following link or node failure is one of the desired features of any network. This capacity has become a main service provider demand and is known as network resilience [22]. Resilient networks can recover from failure by automatically restoring them by moving traffic to another region of the network from the failed portion.

3. Methodology

To get an insight into the performance of IP signalling protocol, adequate simulations were carried out in OPNET Modeler 14.5. To achieve this, a logical network as illustrated in Figure 2 was created using the following network elements: 15 ethernet4_slip8_gtwy Routers, 1 Host / Workstation, 1 Destination/ Server, PPP DS3 and Ethernet 100BaseT links are used for interconnection, IPv4 and IPv6 addressing is done. OSPF was selected as the routing protocol for the network. The network topology for MPLS is shown in Figure 3 and consists of following elements: 2 LERs, 13 LSRs, 1 Host / Workstation, Voice Sender, Video Sender, Database User, Email Client, 1 Destination/ Server, PPP DS3 and Ethernet 100BaseT links are used for interconnection, IPv4 and IPv6 addressing is done. OSPF is used as the routing protocol for the network.

3.1. Configured Applications

Applications (traffic types) were carefully selected so that the designed network would carry both *elastic* and *inelastic* traffic [23]. This helped in modelling the simulation network as close as possible to real life networks which carry diverse traffic types simultaneously. Traffic is termed *elastic* if it can adapt to appreciable changes in network characteristics such as delay, jitter and throughput. Examples of elastic traffic include; Hypertext transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP). If traffic demands consistent (without variations) network characteristics for acceptable service delivery, it is termed inelastic. Real time traffic such as voice and video conferencing are examples of inelastic traffic.

Table 1 Selected Applications and Examples of Their Uses

| Simulations | Situations where used |
|----------------------|---|
| Voice (IP telephony) | VOIP applications e.g. Skype |
| Video Conferencing | Remote news reporting and interviews e.g. CNN and BBC |
| Database(High Load) | Various database servers |
| E-mail (High Load) | Messaging |

E-mail_User and Database_User workstations were configured for E-mail and database respectively. Voice_Sender and Video_Sender were configured for voice and video conferencing respectively.

1. Two servers: Server_1 and Server_2 were configured to support the following services:

i) Server_1 :

Database applications service.

ii) Server_2 :

E-mail service.

Two destinations: Destination_1 and Destination_2 were configured to support the following services:

i) Destination_1 :

Voice application service.

ii) Destination_2 :

Video application service.

3.2. Configured Profiles

An OPNET profile specifies one or a group of applications configured in the application configuration object so that workstations and servers only have to support specific profiles specifying the applications running on them. The following profiles were configured in the network:

- i) Video_profile,
- ii) Voice_profile,
- iii) E-mail_profile and
- iv) Database_profile

3.3. Configured FEC's and LSP's (Traffic Engineering Part)

Four FEC were configured namely, Email_FEC, Data_FEC, Voice_FEC and Video_FEC. FECs specify grouping of traffic that should receive the same treatment in an MPLS network. In this work, all FECs were configured with respect to source IP address. The MPLS configuration object palette offers options for configuring FECs. Two static explicit routed LSPs were configured in the network.

3.4. Configured Traffic Trunks

Traffic trunks consist of configurable attributes that characterizes FECs in an MPLS network. Each FEC is associated with a specific traffic trunk. The attributes are: out of profile action, traffic profile and traffic class.

In the network, two traffic trunks were configured;

- i) Email_Data_Trunk and
- ii) Voice_Video_Trunk.

Configuration of traffic trunks is done in the MPLS configuration object.

3.5. Traffic Mapping Configuration

Traffic mapping configuration is done on the ingress LER. It is a process of associating interface(s) to a specific FEC which, in turn, is associated to a traffic trunk and an LSP. Traffic mapping configurations was thus performed on one LER.

3.6. Qos Attributes

i) Voice_Data_FEC

Table 2 Traffic Profile

| | |
|-----------------------|---------|
| Max Bit Rate | 64kbps |
| Max Burst Size | 32kbits |
| Average Bit Rate | 32kbits |
| Peak Burst Size | 32kbits |
| Out of profile action | Discard |
| Traffic class | AF21 |

ii) Email_Data_FEC

Table 3 Traffic Profile

| | |
|-----------------------|---------|
| Max Bit Rate | 128kbps |
| Max Burst Size | 32kbits |
| Average Bit Rate | 32kbits |
| Peak Burst Size | 32kbits |
| Out of profile action | Discard |
| Traffic class | AF21 |

4. Simulation Scenarios

Several scenarios were created to simulate different protocols so as to achieve the objective of this research. These scenarios include:

- Scenario 1:** IPv4 without MPLS
- Scenario 2:** IPv6 without MPLS
- Scenario 3:** IPv4 with MPLS
- Scenario 4:** IPv6 with MPLS
- Scenario 5:** IPv4 with MPLS and Link Failure
- Scenario 6:** IPv6 with MPLS and Link Failure

Scenario 7: IPv4 with MPLS and Node Failure

Scenario 8: IPv6 with MPLS and Node Failure

Scenario 9: IPv4 with MPLS and Traffic Engineering

Scenario 10: IPv6 with MPLS and Traffic Engineering

The description of these scenarios is given below:

Scenario 1, 2: These scenarios were created as a simple IP network with IPv4 and IPv6 as an addressing protocol, OSPF (and OSPFv3 in IPv6) as a routing protocol, TCP and UDP as a transport protocol. These scenarios actually highlight some of the shortest path routing principle characteristics. Under these scenarios, the performance of the network was very poor. There was no implementation of MPLS or Traffic Engineering in these scenarios. These scenarios are shown in figure 2.

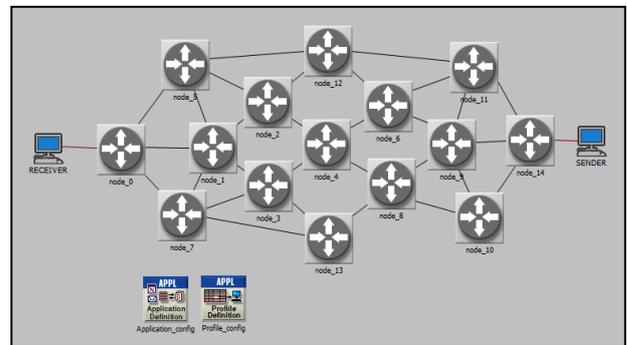


Figure 2 Scenario for Network Topology IPv4 and IPv6

Scenario 3, 4: In these scenarios MPLS was enabled in all LERs and LSRs routers so as to create an MPLS domain where the packets will get forwarded not on the basis of the destination address but on the basis of labels. In order to ensure the proper flow of packets on the basis of labels, another protocol called Label Distribution Protocol (LDP) was configured over these routers. These scenarios actually describe even though MPLS was implemented over the IPv4 network but there was no change in the congestion of the network that has been seen in scenario 1 and scenario. Thus, only implementation of MPLS over the IPv4 and IPv6 network does not solve the problem of over-utilization and under-utilization of the links in the network. These scenarios are shown in figure 3.

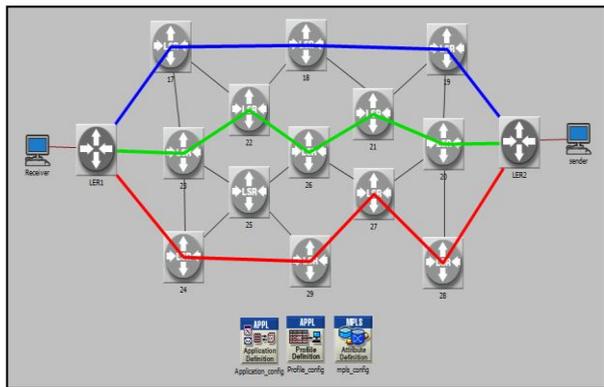


Figure 3 Scenario for Network Topology MPLS over IPv4 and IPv6

Scenario 5, 6: These scenarios illustrated in figure 4 were created to implement MPLS where the link between the routers node_17 and node_18 fails at 50 seconds and recovers at 200 seconds in both IPv4 and IPv6 network.

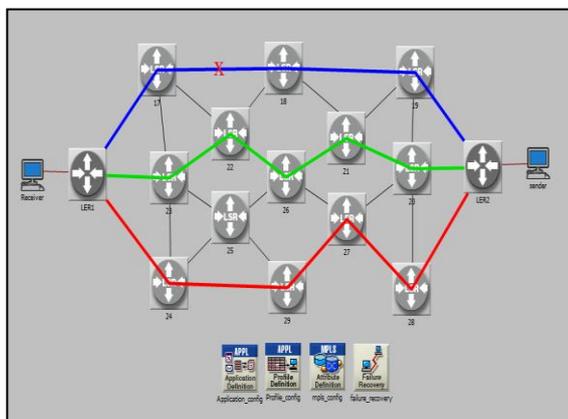


Figure 4 Scenario for Network Topology Link Failure

Scenario 7, 8: These scenarios illustrated in figure 5 were created to implement MPLS where the node_17 fails at 50 seconds and recovers at 200 seconds in both IPv4 and IPv6 network.

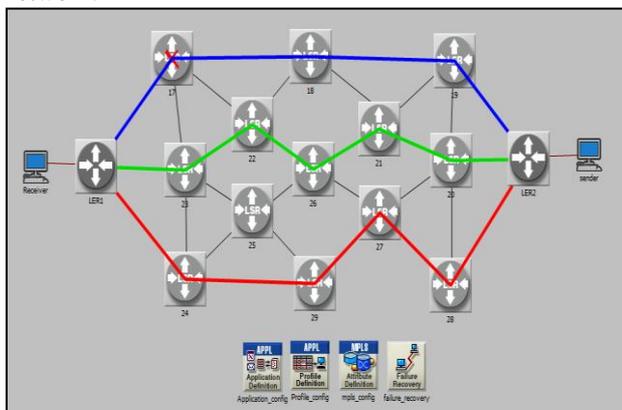


Figure 5 Scenario for Network Topology Node Failure

Scenario 9, 10: These scenarios illustrated in figure 6 were created to implement both MPLS and Traffic Engineering over IPv4 and IPv6 network. This scenario was used to overcome the problem of under-utilization and over utilization along the shortest path links in the network that were seen in scenario 1,2 and scenario 3,4. In order to fix this problem, one forwarding equivalence classes (FECs) for each data was created. A traffic trunk was also created for each traffic, one for UDP traffic and another for TCP traffic.

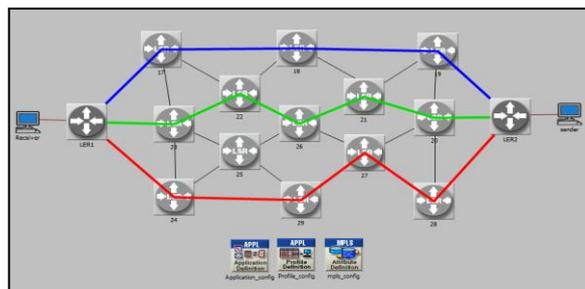


Figure 6 Scenario for Network Topology MPLS-TE

5. Results

After the simulation, the following parameters were evaluated to calculate the network's output under various scenarios.

- i) Throughput
- ii) Jitter
- iii) Queuing Delay
- iv) Link Utilization

5.1 Throughput

The throughput of a channel is a measure of amount of data that actually move through the channel while as bandwidth is the maximum number of data that can pass through a 'channel'. Both throughput and bandwidth are measured in bits per second (bps).[24]

5.1.1 Throughput along the Shortest Path

Throughput depends on the network infrastructure and the bandwidth of the links. As we can see from Figure 7 the throughput has shown improvement for IPv6 over MPLS as compared to simple IPv6 for Voice protocol. In Figure 8 we can see throughput is better in IPv4 over MPLS as compared to IPv4. In the case of IPv4, each packet must be initially processed and then a checksum generated. The route which manages the packet handles the optional field as well. However, in IPv6, the optional fields are put next to the IPv6 header along with other non-essential fields to the extension headers. The simulated results of "throughput" for 17 to 18 link in first four scenarios and scenario 9, 10 are obtained and compared in figure 9. It is

clear from the simulated results that in IP and MPLS based scenarios for both IPv4 and IPv6 the throughput over 17 to 18 link stays almost same. This is because all the traffic generated by clients follows the shortest path (LER1 to node 17 to node 18 to node 19 to LER2) from source to destination. But for “IPv4 MPLS-TE” and “IPv6 MPLS-TE” scenarios the throughput of same link goes down. This is due voice traffic generated by the voice clients had been forwarded through alternate path which was not being at all utilized before. Figure 10 illustrates the simulated results same scenarios for “link 18 to link 19” and the same explanation is also valid for this link because this link is also a part of shortest route.

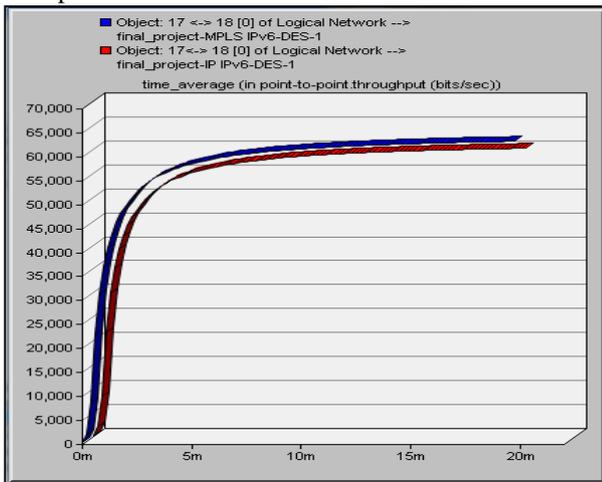


Figure 7 Average Throughput Comparison of IPv6 and MPLS IPv6 along 17 to 18 Link

5.1.2 Throughput along the Alternative Path

The simulated results of throughput for “24 to 29” link in first four scenarios and scenario 9, 10 are obtained and compared in figure 11. It is clear from the simulated results that in IP and MPLS based scenarios for both IPv4 and IPv6, the throughput over 24 to 29 link stays at zero. It is because the alternate paths available from source to destination in IP and MPLS were not utilized at all. But for “IPv4 MPLS-TE” and “IPv6 MPLS-TE” scenarios half of the traffic was passed through this alternate path by establishing a separate LSP for voice traffic and thus the throughput for those links in the alternate path had gone up. The same traffic then flows from 27 to 28 link and the same explanation is valid for this link. The figure 12 illustrates the throughput of the link 27 to 28 link for all these mentioned six scenarios. Thus, by MPLS-Traffic Engineering, over utilized links were offloaded by diverting some of the traffic through underutilized links in a network. This is achieved by making the use of RSVP protocol for MPLS-TE that establishes label switch paths (LSPs) or separate tunnels from ingress router to the egress router. In this way, the problems like congestion and under-utilization were efficiently addressed in an underlying network.

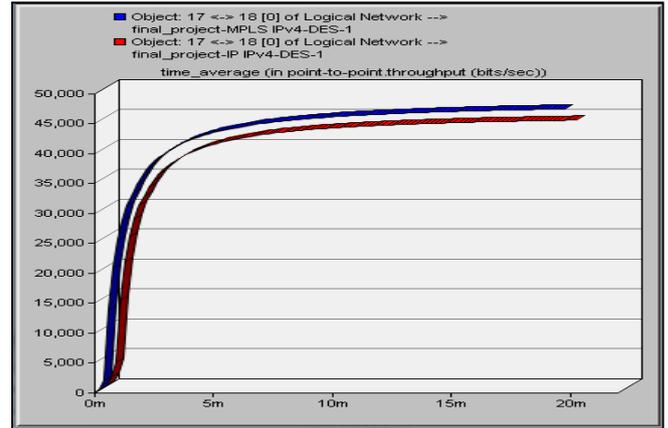


Figure 8 Average Throughput Comparison of IPv4 and MPLS IPv4 along 17 to 18 Link

5.1.3 Throughput Comparison for Link Failure in IPv4-MPLS and IPv6-MPLS Scenario

It is clear from the simulated results illustrated in Figure 13 that the throughput in IPv6 is higher than Ipv4. The link between node 17 and node 18 fails at 450 seconds and recovers at 750 seconds. The throughput performance in IPv6 is still better than IPv4 even if no repair techniques are used.

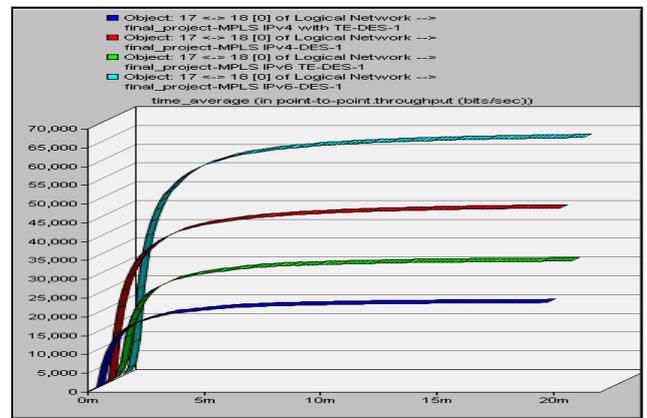


Figure 9 Throughput Comparison of IPv4 and IPv6 over MPLS and MPLS-TE along 17 to 18 Link

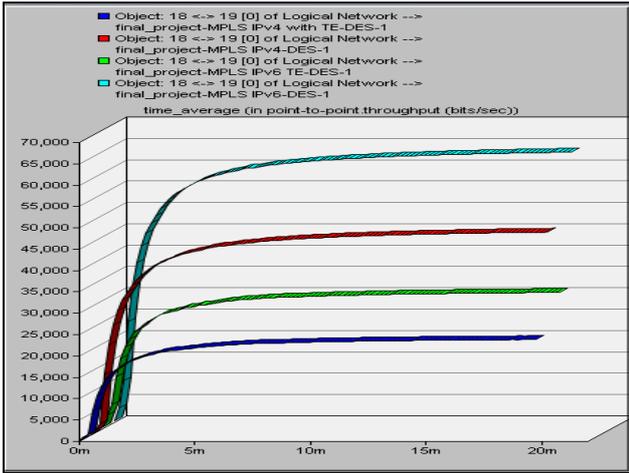


Figure 10 Throughput Comparison of IPv4 and IPv6 over MPLS and MPLS-TE along 18 to 19 link

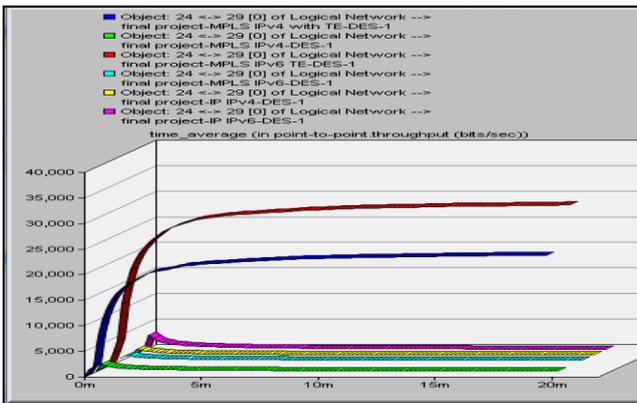


Figure 11 Average Throughput along 24 to 29 Link

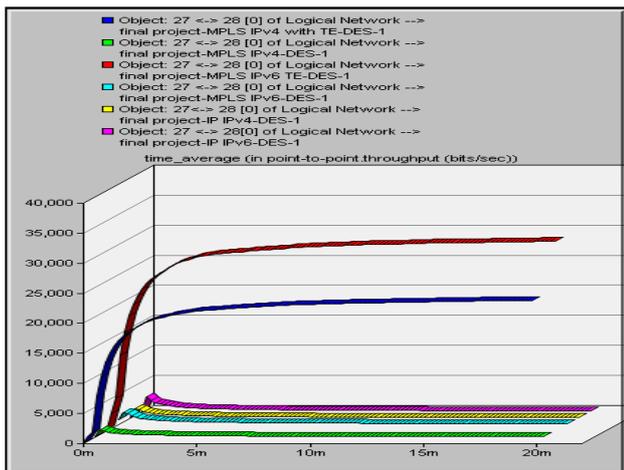


Figure 12 Average Throughput along 27 to 28 Link

5.1.4 Throughput Comparison for Node Failure in IPv4-MPLS and IPv6-MPLS Scenario

From the simulation results, as illustrated in Figure 14 it can be concluded if any node, say node 17 in our scenario fails at 450 seconds and recovers at 750 seconds, the throughput performance shown by IPv6 is better than IPv4. With regard to performance, the IPv6 Protocol offers better transmission efficiency and high output with the highest utilization per line.

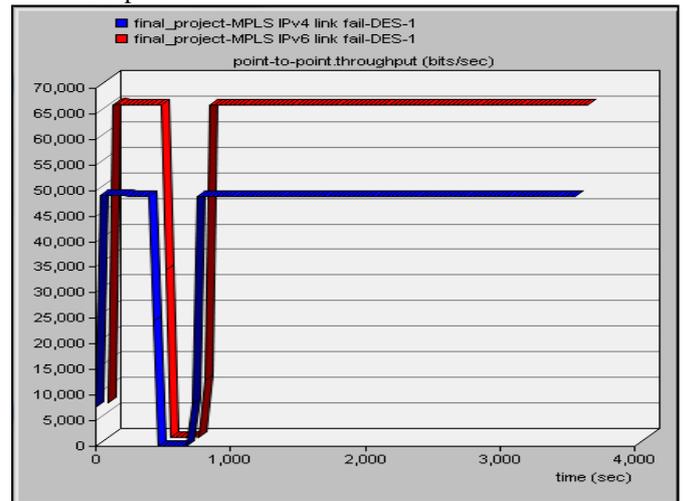


Figure 13 Link failure

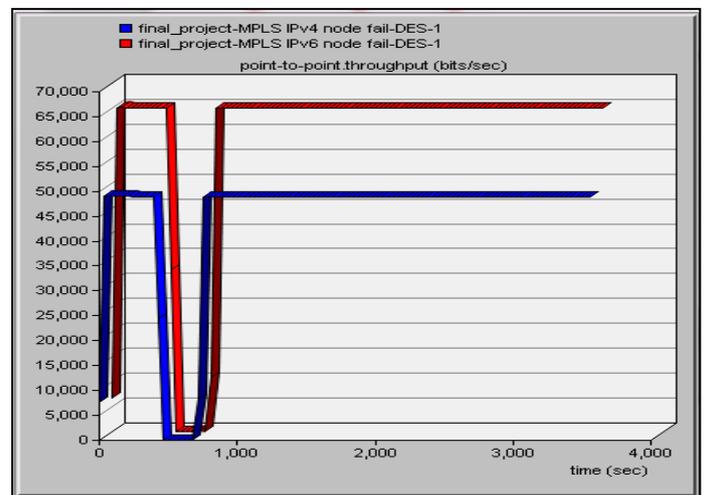


Figure 14 Node failure

5.2 Jitter

Electromagnetic interference can cause jitter in the network and crosstalk with other signal carriers. This causes undesirable effects in audio signal and data loss between network devices. Jitter is the rate of change of delay. As illustrated in Figure 15, Figure 16 and Figure 17, latency is more extensive in IPv6 over the MPLS network than in

IPv4 over the MPLS network, therefore Jitter is more extreme in IPv6 over MPLS.

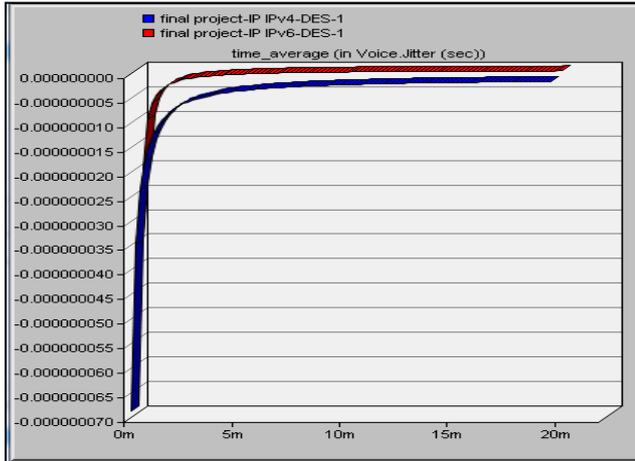


Figure 15 Jitter comparison of IPv4 and IPv6 network

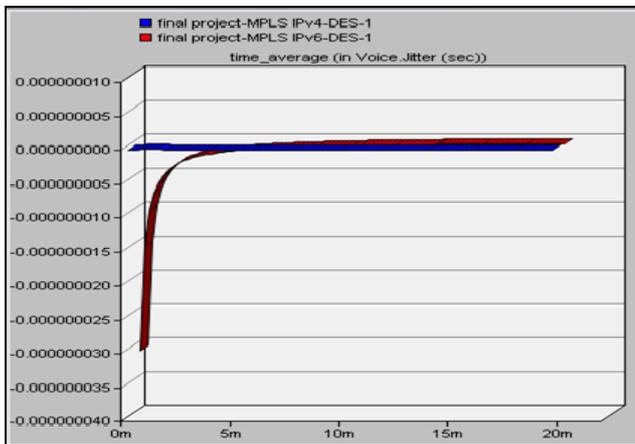


Figure 16 Jitter Comparison of IPv4 and IPv6 over MPLS

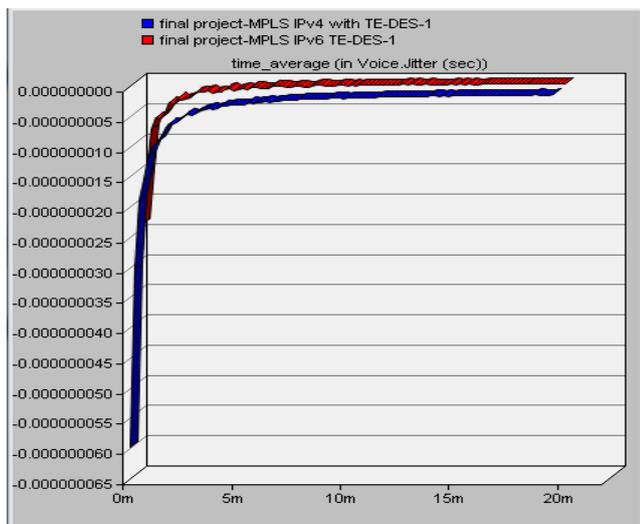


Figure 17 Jitter comparison of IPv4 and IPv6 over MPLS-TE

5.3 Queuing Delay

The time that a packet is waiting in a queue is an important feature of a network design and its performance and it is measured as the time it takes for a job to take place. The amount of delays that a packet faces between entry to a network and transmission time to addresses is summarized in the packet switched network. Queues are generally formed by the delays produced at the originating devices like switches, routers etc.

5.3.1 Queuing Delay of Shortest Path (LER1 to 17 to 18 to 19 to LER2 Link)

The simulated results of queuing delay over 17 to 18 link under six scenarios are obtained and compared in figure 18 and figure 19. It is clear from the graph that the average queuing delay for IP and MPLS based scenarios are high while as the queuing delay for Traffic Engineering based scenarios is almost zero seconds for both IPv4 and IPv6. The main reason behind it is that in IP and MPLS based scenarios all the packets follow the shortest path route from source to destination. This shortest path route becomes jammed and packets need to wait at each and every router which results the higher queuing delay along the shortest path. While as in MPLS based scenarios for both IPv4 and IPv6 half of the traffic (i.e. the traffic from voice client) was steered through the alternate route. This results the free flow of the packets through the shortest route and thus not a single packet needs to wait at any router. Thus, the queuing delay for the packets that follow the shortest route from source to destination in Traffic Engineering is zero.

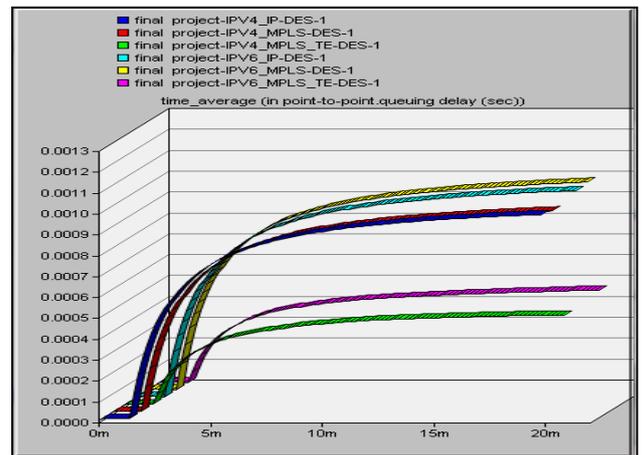


Figure 18 Average Queuing Delay Comparison along shortest path

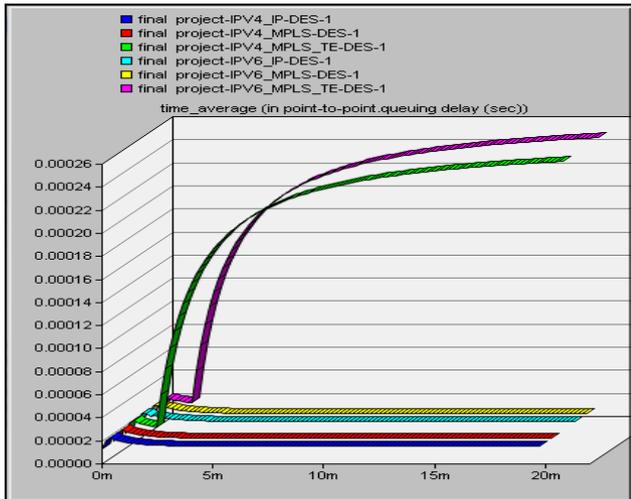


Figure 19 Average Queuing Delay Comparison along alternate path

5.4 Utilization

The utilization of a link is the percentage of the bandwidth currently used by network traffic and the constant high use that is more than 50 percent which suggests network congestion or failure points in the network and the need for network infrastructure enhancements.

In order to exploit the limitations of the routing protocol like OSPF, each traffic generating client (voice client and video client) generates 386 packets per second (each packet of 2000 bits) destined for voice server and video server respectively. Once these packets reach to the core of the network, all the packets from these traffic generating clients were forwarded through the shortest path of the network towards their destinations. Even though there were multiple paths available in the network for the traffic flow but only a specific route were utilized for forwarding the traffic. This is due to because all the IP routing protocols works on the least cost principle. Due to this reason the shortest path links were utilized by more than 90% while as the other paths were not utilized at all (i.e. underutilized).

5.4.1 Utilization of 17 to 18 Link

The simulated results of the point to point link utilization (17 to 18 link) in first four scenarios and scenario 9, 10 are illustrated in Figure 20, Figure 21, Figure 22. It is clear from the graph that link utilization stays at high for both IPv4 and IPv6 MPLS and without MPLS based scenarios. This is due to because “without MPLS scenarios” follows the least cost principle of the routing protocol like OSPF and in MPLS based scenarios an MPLS core is actually being made in which the packets are being forwarded on the basis of labels rather than destination address but the traffic generated by the traffic generating clients follows the same route from source to destination. It is to be noted

here that in IP networks, routing look ups are performed by each and every router as packets get forwarded from source to destination.

While as in MPLS based scenarios, these routing look ups are not performed as the packets get forwarded on the basis of labels and thus save a lot of time while forwarding the packets. But in Traffic Engineering based scenarios for both IPv4 and IPv6, the utilization of 17 to 18 link had come down from 90% to 45% (i.e. the over utilization problem of 17 to 18 link got resolved). This is due to half of the traffic from the traffic generating clients was steered through the other links that were not used before in the network. Earlier in MPLS and without MPLS based scenarios entire traffic from the traffic generating clients was forwarded through shortest path in the network and thus the utilization of 17 to 18 link was about 90% but in traffic engineering based scenarios, voice traffic has been steered through other path and video traffic flows the same shortest path. Steering of traffic via alternate paths in the network is achieved by making the use of RSVP protocol which actually establishes the tunnels (called LSPs) for each traffic flow. Thus, implementation of Traffic Engineering in the network addresses the problem of congestion that was seen in IP and MPLS based scenarios for both IPv4 and IPv6.

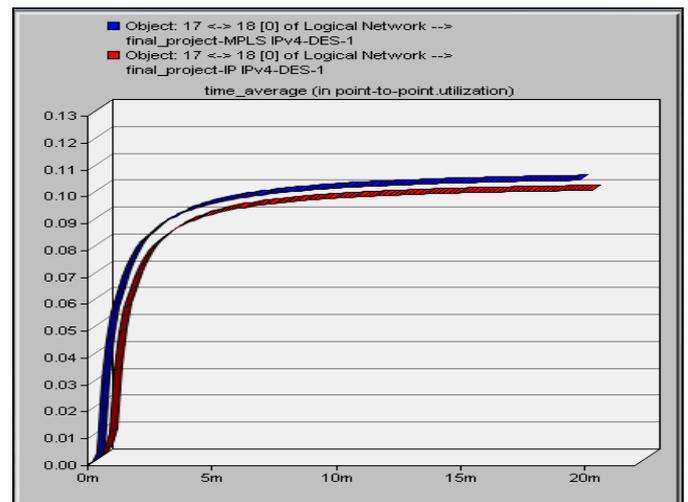


Figure 20 Link Utilization Comparison of IPv4 and MPLS IPv4 along 17 to 18 Link

5.4.2 Utilization of 18 to 19 Link

The simulated results of the point to point link utilization (18 to 19 link) under six scenarios are illustrated in Figure 23, Figure 24 and Figure 25. It is clear from the graph that link utilization stays at 90% for both IPv4 and IPv6 MPLS and without MPLS based scenarios. But for Traffic Engineering based scenarios for both IPv4 and IPv6 the utilization of the same link (i.e. 18 to 19 link) had come down from 90% to 45%. The explanation is given in above section. Thus, it is clear the shortest path route that was

earlier congested in IP and MPLS based scenarios had become congestion free in Traffic Engineering case.

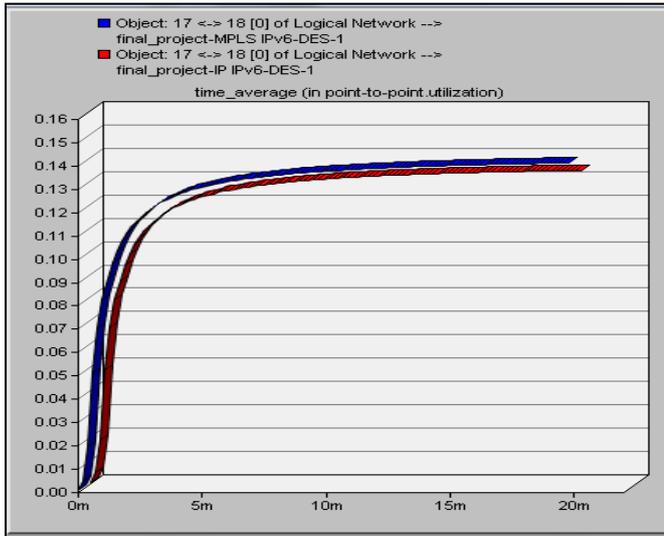


Figure 21 Link Utilization Comparison of IPv6 and MPLS IPv6 along 18 to 19 Link

5.4.3 Utilization of 24 to 29 Link

The simulated results of the point to point utilization of 24 to 29 link under six scenarios are obtained and compared in Figure 26. It is clear from the graph that link utilization stays at 0% for both IPv4 and IPv6 MPLS and without MPLS based scenarios. This is due to because entire traffic from traffic generating clients was forwarded through the shortest path and not a single packet got forwarded through the available alternate path in the network. Thus, the utilization of this link during IP and MPLS based scenarios for both IPv4 and IPv6 stays at 0%. But simulated results from the Traffic Engineering based scenarios for both IPv4 and IPv6 shows that utilization of this link has gone up from 0% to 45%. This is due to because the voice traffic gets forwarded through this link. This is achieved by using the RSVP protocol for Traffic Engineering that establishes a separate tunnel for each application.

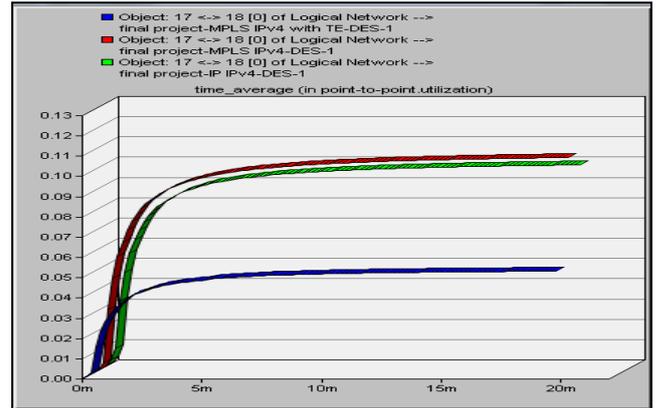


Figure22 Link Utilization Comparison of IPv4, IPv4 over MPLS and IPv4 over MPLS-TE along 18 to 19 Link

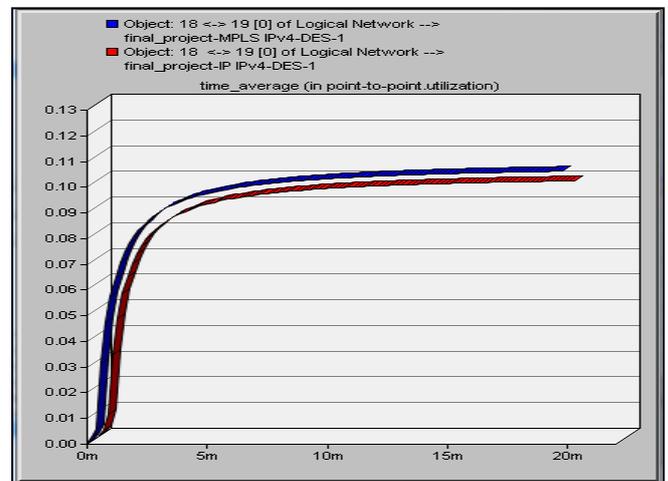


Figure 23 Link Utilization Comparison of IPv4 and MPLS IPv4 along 18 to 19 Link

5.4.4 Utilization of 27 to 28 Link

The simulated results of the point to point utilization of 27 to 28 link in all six scenarios are obtained and compared in figure 27. It is clear from the graph that link utilization stays at 0% for both IPv4 and IPv6 MPLS and without MPLS based scenarios. But simulated results from the Traffic Engineering based scenarios for both IPv4 and IPv6 shows that utilization of this link has gone up from 0% to 45%. The reason is already explained in above section.

It is clear that the shortest path links which were over utilized (90% utilization) in the IP and MPLS based scenarios have become congestion free (only 45% utilization) in Traffic Engineering scenarios and the alternate paths that were not used at all (0% utilization) in IP and MPLS scenarios had now been utilized (45% utilization).

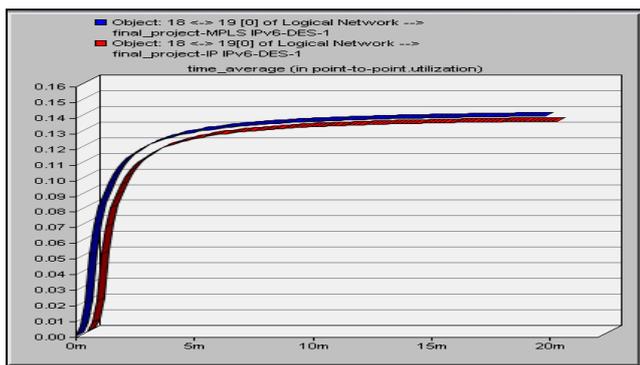


Figure 24 Link Utilization Comparison of IPv6 and MPLS IPv6 along 18 to 19 Link

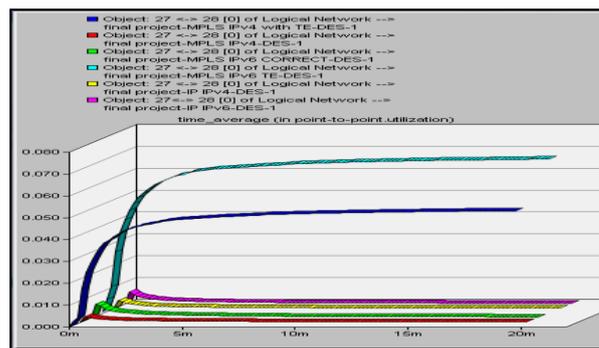


Figure 27 Link Utilization Comparison of 27 to 28 link

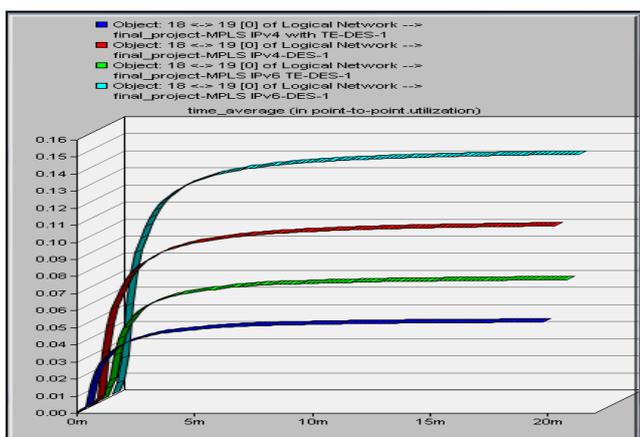


Figure 25 Link Utilization Comparison of IPv4, IPv4 over MPLS and IPv4 over MPLS-TE along 18 to 19 Link

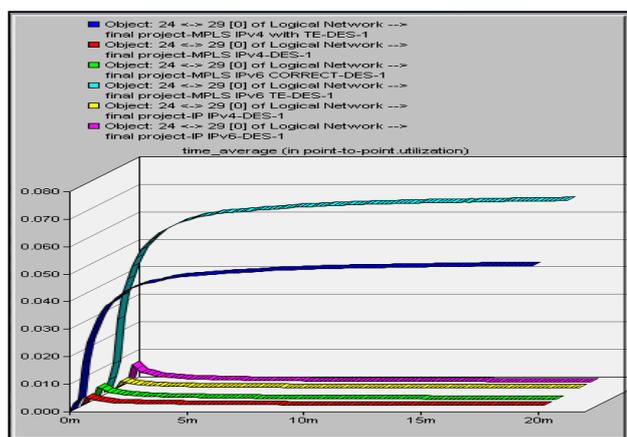


Figure 26 Link Utilization Comparison of 24 to 29 Link

6. Conclusion

All Business organizations are constantly being flooded with an enormous amount of data [25]. Due to the huge Internet traffic due to increased demand for heavy audio / video content and other real-time services, it is now necessary to integrate bandwidth-optimized technologies such as MPLS with Traffic Engineering. In this study, traffic engineering performance evaluation with MPLS was conducted in various scenarios involving IPv4 and IPv6 addressing protocols. Traffic engineering has made better use of the connections by reducing the use of overused links to zero, 90 to 45. It was found that network resources could be used well if most of the underutilized links were put to use. The reduction was almost the same for both IPv4 and IPv6 scenarios. With respect to Queuing latency, both the IPv4 and IPv6 MPLS situations involving Traffic Engineering were less. Because of the traffic engineering reduced traffic over LSPs, it was seen that packet drop in MPLS-TE scenarios was also reduced. Nevertheless, it has been observed that average packet drop in traffic engineered networks based on IPv6 MPLS is nearly double that of traffic engineered networks based on IPv4 MPLS. Finally, it was found that average LSP delays in both IPv4 and IPv6 traffic-engineered scenarios were lower than those in which traffic-engineering was not used. Therefore, the simulations carried out demonstrated the applicability of the traffic engineering carried on IPv6 over MPLS.

References

- [1] Rosen E. and Viswanathan A., A Proposed Architecture for MPLS /draft-ietf-mpls-arch-00.txt, February 1998
- [2] L. De Ghein, *MPLS Fundamentals*. 2006. Retrieved from <https://doc.lagout.org/network/Cisco/CCIE/CCIE SP/CiscoPress - MPLS Fundamentals.pdf>
- [3] M. A. Panhwar, K. A. Memon, A. Abro, D. Zhongliang, S. A. Khuhro, and Z. Ali, "Efficient approach for optimization in traffic engineering for multiprotocol label switching," *ICEIEC 2019 - Proceedings of 2019 IEEE 9th International Conference on Electronics Information and Emergency Communication.*, pp. 9–15, 2019, doi: 10.1109/ICEIEC.2019.8784486.
- [4] F. Bensalah and N. El Kamoun, "Novel software-defined network approach of flexible network adaptive for VPN

- MPLS traffic engineering,” *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 4, pp. 280–284, 2019, doi: 10.14569/ijacsa.2019.0100433.
- [5] T. Settawatcharawanit, Y. H. Chiang, V. Suppakitpaisarn, and Y. Ji, “A Computation-Efficient Approach for Segment Routing Traffic Engineering,” *IEEE Access*, vol. 7, pp. 160408–160417, 2019, doi: 10.1109/ACCESS.2019.2951163.
- [6] K. Qiu, J. Zhao, X. Wang, X. Fu, and S. Secci, “Efficient Recovery Path Computation for Fast Reroute in Large-Scale Software-Defined Networks,” *IEEE Journal on Selected Areas in Communications*, vol. 37, no. 8, pp. 1755–1768, 2019, doi: 10.1109/JSAC.2019.2927098.
- [7] Cisco, “Route Selection in Cisco Routers - Cisco,” 8651, pp. 1–7, 2008.
- [8] [8] H. Wang and M. R. Ito, “Dynamics of load-sensitive adaptive routing,” *IEEE International Conference on Communications*, vol. 1, no. C, pp. 213–217, 2005, doi: 10.1109/icc.2005.1494349.
- [9] A. Mishra, A. Sahoo, B. Dalvi, and T. Zhu, “WOSPF: A traffic engineering solution for OSPF networks,” *2016 IEEE Global Communications Conference, GLOBECOM 2016 Proc.*, pp. 1845–1849, 2016, doi: 10.1109/GLOCOM.2016.7842393.
- [10] A. Durrezi, M. Durrezi, L. Barolli, and F. Xhafa, “MPLS traffic engineering in satellite networks,” *First International Conference on Complex, Intelligent and Software Intensive Systems*, pp. 19–24, 2007, doi: 10.1109/CISIS.2007.39.
- [11] M. Tatipamula, F. Le Faucheur, T. Otani, and H. Esaki, “Implementation of IPv6 services over a GMPLS-based IP/optical network,” *IEEE Communications Magazine* vol. 43, no. 5, pp. 114–122, 2005, doi: 10.1109/MCOM.2005.1453432.
- [12] F. Solano, R. Fabregat, and J. L. Marzo, “On optimal computation of MPLS label binding for multipoint-to-point connections,” *IEEE Transactions on Communications*, vol. 56, no. 7, pp. 1056–1059, 2008, doi: 10.1109/TCOMM.2008.050601.
- [13] J. M. Chung, E. Marroun, H. Sandhu, and S. C. Kim, “VoIP over MPLS networking requirements,” *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2094, pp. 735–744, 2001, doi: 10.1007/3-540-47734-9_73.
- [14] M. Spainhower, J. Butts, D. Guernsey, and S. Shenoi, “Security analysis of RSVP-TE signaling in MPLS networks,” *International Journal of Critical Infrastructure Protection*, vol. 1, no. C, pp. 68–74, 2008, doi: 10.1016/j.ijcip.2008.08.005.
- [15] A. Ghanwani, B. Jamoussi, D. Fedyk, P. Ashwood-Smith, L. Li, and N. Feldman, “Traffic engineering standards in IP networks using MPLS,” *IEEE Communications Magazine* vol. 37, no. 12, pp. 49–53, 1999, doi: 10.1109/35.809384.
- [16] B. Fortz and M. Thorup, “Internet traffic engineering by optimizing OSPF weights,” *Proceedings - IEEE INFOCOM*, vol. 2, pp. 519–528, 2000, doi: 10.1109/infcom.2000.832225.
- [17] T. Li and G. Swallow, “2/21/2020 www.awduche.com/papers/papers99/draft-li-mpls-igp-te-00.txt,” no. August 1999, pp. 1–7, 2020.
- [18] B. Fortz, J. Rexford, and M. Thorup, “Traffic engineering with traditional IP routing protocols,” *IEEE Communications Magazine*, vol. 40, no. 10, pp. 118–124, 2002, doi: 10.1109/MCOM.2002.1039866.
- [19] “Ina Minei, “MPLS enabled applications: emerging deve,” p. 2020, 2020.
- [20] T. A. Al-Radaei and Z. A. Zukarnain, “Comparison study of transmission control protocol and user datagram protocol behavior over multi-protocol label switching networks in case of failures,” *Journal of Computer Science*, vol. 5, no. 12, pp. 1042–1047, 2009, doi: 10.3844/jcssp.2009.1042.1047.
- [21] S. Ahmad, W. Ali, and M. Hassan, “Performance Evaluation of IPv4 and IPv6 over MPLS using OPNET,” *International Journal of Computer Applications*, vol. 125, no. 3, pp. 34–38, 2015, doi: 10.5120/ijca2015905869.
- [22] S. N. S. V. Kumar, “MPLS Traffic Engineering ? Fast Reroute,” *International Journal of Science and Research*, vol. 3, no. 5, pp. 1796–1801, 2014.
- [23] Adarshpal S. Sethi Vasil Y. Hnatyshin, *The Practical OPNET User Guide for Computer Network Simulation*, CRC Press.
- [24] Forouzan B.A, *Data Networks*, no. 1–2. 1981.
- [25] Idrees, S. M., Alam, M. A., Agarwal, P., & Ansari, L. (2019, April). Effective Predictive Analytics and Modeling Based on Historical Data. In *International Conference on Advances in Computing and Data Sciences* (pp. 552-564). Springer, Singapore.