Middle-East Journal of Scientific Research 20 (12): 2117-2127, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.20.12.21101

Mechanism of Multiprotocol Label Switching for Forwarding Packets & Performance in Virtual Private Network

Kashif Naseer Qureshi, Abdul Hanan Abdullah, Ahmed Nazar Hassan, Dalya Khalid Sheet and Raja Waseem Anwar

Faculty of Computing, University Teknologi Malaysia,
81310 Skudai, Johor Bahru, Malaysia

Abstract: Multiprotocol Label Switching (MPLS) is widely used and recognized as a tunneling technology that is used by many enterprises. This paper focuses on identifying the appropriate technology, which can be used by organizations as their core network technology for ensuring a consistent and protected communication across the WAN link. This technology provides a mechanism for forwarding packets for any network protocol and explores to overwhelm some of the IP based networks limitations. Because packet forwarding in MPLS is based only in label switching, it is faster than IP. In this paper we present a Multiprotocol Label Switching advantages, components, usage architecture. Further presents the Multiprotocol Label Switching services and compare MPLS with Frame relay in virtual private network through real experiment.

Key words: VPN (Virtual Private Network) · ATM(Asynchronous Transfer Mode) · IP(Internet protocol) · MPLS (Multiprotocol Label Switching)

INTRODUCTION

Information Technology has changed constantly over the past couple of decades. The concept of globalization has brought a revolution in the ICT (Information and Communication Technology) sector, resulting in an information era that provided new levels of global interconnectivity. The IETF(Internet Engineering Task Force) has proposed multiprotocol label switching (MPLS) as a new forwarding technology [1]. Multiprotocol Label Switching (MPLS) is a protocol broadly used in commercial operator networks to forward packets by matching link-specific labels in the packet header to outgoing links to a certain extent through standard IP longest prefix matching [2]. Many enterprise businesses today are looking for a suitable solution to their wide area networks spread over different locations which was possible by purchasing frame relay or ATM leased lines in the recent past. Multi-Protocol Label Switching (MPLS) provides a mechanism for forwarding a packet for any network protocol. MPLS support service creation (VPNs), traffic engineering, network convergence and increased resiliency. MPLS is an efficient and effective technique that forwards the packets across the network by using the contents of the labels attached to the IP packets [3]. MPLS is known to be a layer-2.5 technology because it supports both data link layer or layer-2 and network layer or layer-3. The use of MPLS as backbone networks has increased over the past few years as compared to traditional IP networks which were based on Iayer-2 technologies i.e. ATM and frame relay. MPLS has been around for more than a decade, in the last century, most of the customer, businesses and organizations are shifted to the Internet due to which Internet now plays an important role in our life and changed the whole infrastructure very rapidly and up to a large extent. Hasty growth in the Internet in terms of size of networks bandwidth requirements, geographical size and traffic volume, the demand for high-speed backbone networks has also increased. The basic idea behind MPLS was to improve the scalability of backbone In this paper, we discuss the MPLS according to the definitions mentioned below:

- "MPLS provides a mechanism for engineering network traffic patterns that is independent of routing tables" [4].

Corresponding Author: Kashif Naseer Qureshi, Faculty of Computing, University Teknologi Malaysia, 81310 Skudai, Johor Bahru, Malaysia.

- "MPLS is an improved method for forwarding packets through a network using information contained in labels attached to IP packets [3]".
- "Multi Protocol label Switching (MPLS) is a Core networking technology that operates between layers 2 and 3 of the OSI model [5]".

According to definition (b); the labels are inserted between the layer 3 (Network Layer) headers and the Layer 2 (Data-link Layer) in the case of frame-based layer 2 technologies and they are contained in the virtual path identifier (VPI) and virtual channel identifier (VCI) fields in the case of cell-based technologies such as ATM.

The labels are inserted between the layer 3 (Network Layer) header and the Layer 2 (Data-link Layer) in the case of frame-based layer 2 technologies and they are contained in the virtual path identifier (VPI) and virtual channel identifier (VCI) fields in the case of cell-based technologies such as ATM." [3].

Related Work: In past years several companies had begun to research for label switching. The label switching networks was to bring those connection oriented benefits into a non-connection oriented network; mainly IP. Original initiative of MPLS was based on IP over ATM. Multiprotocol Label Switching (MPLS) [6] is used in vehicular ad-hoc network (VANET) in the roadside backbone network. MPLS is a forwarding method and layer 2.5 technologies, used in Vehicular ad-hoc network (VANET) for gain better quality of services (QoS). Through simulation result, the author proved the MPLS performance in VANET as a back bone network specially urban areas. In vehicle 2 vehicle communication when data send to the nearest base station and then data sent via wired domain which is based on MPLS and have a higher reliability of end-to-end delay, packet loss and throughput. In this paper [7] the author selected the MPLS protocol for mobile ad-hoc networks (MANET). The MPLS enhances routing with respect to path and packet forwarding, further author simulated and analyzed the various effects of MPLS for MANET. The metrics of MPLS during simulation are discovery time, packet end-to-end delay and throughput showed the better and efficient performance of MPLS. In this work [8] author presented wireless mesh network (WMN) architecture based on label switching technology. Through this approach, the alternative data forwarding plane independently from existing routing protocol and orthogonal data and control planes built upon the MPLS technology. The paper [9] presented the Local Multipoint Distribution Service (LMDS) for a broadband wireless access (BWA) networking solution over MPLS (Multi-Protocol Label Switching) network for real-time multimedia applications is introduced. The author proposed a model and simulated the multimedia data samples voice, video and non critical traffic under varying load conditions. The LMDS over MPLS networking environment for real time multimedia applications studied.

History of MPLS: The term MPLS was first used by IETF in 1997 after the formation of working group that was based on the global interest of label switching principle. The credit of practically implementing the concept of MPLS into hardware goes to Cisco when it released its first MPLS supported Cisco LOS 11.1(17) CT in 1998. The label was then called "tag" and "label switching" was known as "tag switching." The MPLS supported router was capable of assigning tags to networks and then attaching those tags to packets destined for those networks. Based on "tagging" mechanism a table called "Tag Forwarding Information Base" was built into the router. The table was then used to route packets using the "swap and forward" principle. If a tag of packet matches the tag in the TFIB of router, a new tag (outgoing) was added to the packet and forwarded to the next router unless otherwise discarded [10]. Some of the comparisons are shown below in the table, the changes in new and old MPLS tag/label switching terminologies.

In the beginning Label switching was considered to be used in shifting the features of data link layer switching to network layer switching. However, since the layer 3 switch with ASIC (Application Specific integrated circuit) technology was introduced to perform faster lookups with efficient speed and accuracy, MPLS was no longer considered to be used for the same benefits. MPLS was derived from many of its predecessors technologies such as ARIS (Aggregate Route- Based IP Switching) introduced by IBM, CSR (Cell Switched Router) manufactured by Toshiba, Cisco's Tag Switching and IP Navigator by Lucent. Many of MPLS features was originally incorporated from Cisco's Tag switching technology [3].

Operation of MPLS: In light of the above definitions quoted by different authors, MPLS is simply a framework for WAN that operates on the network and data link layer that belongs to packet switching family, because MPLS supports both link and network layer therefore, it is called layer 2.5 technique [11]. A tunneling technology based on the mechanism of tag switching/label swapping.

Table 1: Comparison of old and new switching terminologies [10]

Old Terminology	New Terminology
Tag Switching	Label switching
Tag	Label
TDP stands for (tag distribution protocol)	LDP short for (label distribution protocol)
TFIB short for (Tag forwarding information base)	LFIB short for (label forwarding information base)
TSR stands for (tag switch router)	LSR short for (label switch router)
TSC stands for (Tag switch controller)	LSC short for (label switch controller)
TSP stands for (tag switch path)	LSP short for (label switch path)

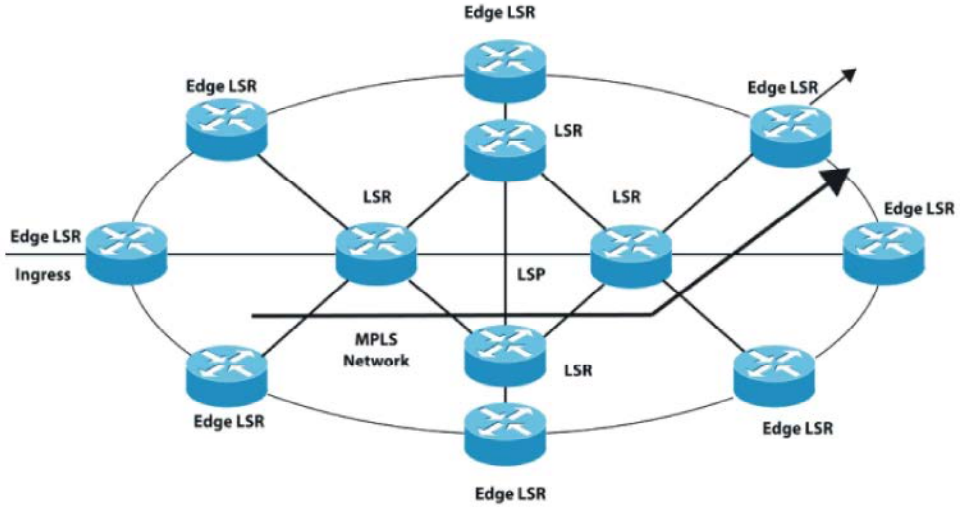

Fig. 1: Shows how packets entering the MPLS network and labeled to Edge router (Ingress)

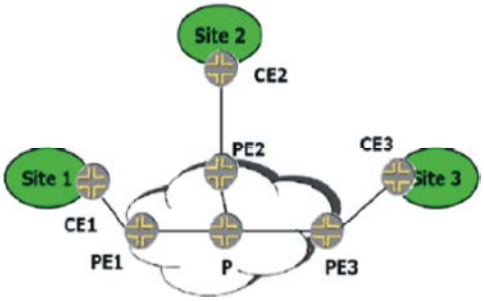

Fig. 6: Peer-to-Peer Network with MPLS tunneling [5]

MPLS defines architecture for high performance backbone network for service providers and enterprises. Multiprotocol Label Switching (MPLS) introduced to overcome the problems of traditional IP routing and the strange point and limitation of the predecessor technology like frame replay which is still used by service providers worldwide. The main reason for Multiprotocol Label Switching (MPLS) popularity is its flexible network-deployment nature as the term "Multiprotocol" indicates, the techniques can be applied to any protocol for network layer (Layer 3, OSI). This offers service providers to setup a high scale network providing high quality services with guaranteed reliability and security [12].

LSR (Label Switched Router) swaps the label as the packet travels along the Labeled-switched path (LSP) [13]. The forwarding mechanism depends on the information contained inside the label. Layer 3(IP) routing is based on destination IP address means the packet will be delivered to the end node by looking at the destination address. Model of MPLS describe packet forwarding in a same manner as used in ATM for cells and in Frame relay for frame forwarding. A different label is attaché to packet every time it passes through an LSR. Which guides the next router about the route to the destination? The label is removed when the packet reaches the edge (ingress) router then forwarded to the destination.

Advantages of MPLS: The best feature of MPLS is that it uses a peer model to connect different sites with minimum cost of implementation using reduced virtual links between customer and provider's equipments. The figure shows a typical MPLS peer-to-peer model.

The above figure illustrates a typical peer-to-peer VPN based on MPLS. The devices shown in the figure explains below:

- Site l, 2 & 3 are customer networks using VPN
- PE 1, 2 & 3 are provider edge routers connected to the core MPLS network through router P
- CE 1, 2 & 3 are customer edge routers connected together through a VPN.

Quality of Service (QOS): Majority of the people would accept the fact that information technology has a great deal of concern in our personal and social lives. Almost every aspect of our life has been affected due to constant changes in the internet and rich multimedia applications. One reason of its popularity is that Internet is accessible globally [3].

Q0S is a measure to determine the performance of a network that provided with service level agreement (a.k.a SLA). The policies considered in SLA to determine the QOS involves loss of packet, reduced bandwidth, jitter (a.k.a variable delay) and latency. There are many mission critical applications, which have very tough requirements for high bandwidth and availability of services. These applications include, voice conference, video streaming sites, rich multimedia web applications and traffic for VoIP calls, banking and finance online applications. All of these have different requirements for different factors. All of the above factors are critical to every service provider to provide all of these at the same time with high level of availability and performance [3].

Every network designed with the intention to provide a scalable, highly secure, manageable and robust network to meet the end customer requirements. Therefore, the responsibility of service providers is to take care when providing time sensitive services such voice and video streaming and video conferencing. Voice and video being the most sensitive as these applications cannot bear any delay more than l5Oms, latency, or jitter while transmission. The quality of the services provided may be suffered if these time critical applications are set to lower priority [5]. In short, Q0S is a method of giving preference to important data traffic over least important with high assurance of availability. The IETF has introduced two different ways to deploy quality of service in an MPLS based network i.e. lntServ and DiffSrv.

Comparison of MPLS with Traditional IP/Routing: The traditional IP routing has make independent routing decision for each incoming packet. Router has consulted our routing table for find the next hop on the base of destination address or IP header. Open shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS), Border Gateway Protocol (BGP) etc IP routing protocols build routing tables. When the packet traverses, each router performs the same steps for finding the next hop. The problem with this routing is that they are not capacity constraints and traffic characteristics into account when they take decision. The outcomes are some segments of a network along alternative routes become under utilized. IP routing will continue traffic forwarding until packets are dropped. IP packet forwarding is limited due to limited capability for deal with addressing data.

Table 3: Comparison of IP and MPLS routing

	MPLS	IP
No of Packets Received	867	812
Throughput (Mbps)	0.7202	0.6832
BW Utilization (%)	74.03	62.32
End to End Delay (s)	0.035	0.048
Average Jitter (s)	$0.3*10^{-2}$	$0.37*10^{-4}$

On the other hand the MPLS technology is highly interactive for flowing, it is low delay and packet loss threshold and efficiently utilize the available network resources. MPLS supports new features and applications.

In MPLS the short fixed-length labels are assigned to packets at the edge of the MPLS domain. These pre assigned labels are used rather than the original packet headers to forward packets on pre-routed paths. In MPLS, the route the packet is forwarded through the MPLS domain and it is assigned only once for example when the packet enters the domain. Before a router forwards a packet, it changes the label in the packet to a label that is used for forwarding by the next router in the path.

We simulate the both technologies in real lab environment and show the performance of traditional IP and MPLS Routing below.

MPLS Performance in Virtual Private Network (VPN): The best example of a network using MPLS services today is the VPN network. VPNs are the practical implementation of MPLS, which provide the services by using the best features of MPLS. Similarly, the process of forwarding data packets is fast and simple, as the tasks have been divided between devices with different capabilities. Such as the responsibility of the core layer is in perform the label switching function while provider edge routers perform label forwarding using look-up tables [5].

Virtual Private Network (VPN): Virtual private networks (VPN) offer a secure data exchange over public networks [14]. A VPN is an enterprise network which traverses a shared or public infrastructure. For example the internet

establishes Private and secure connections over an un trusted network, with geographically dispersed users, customers and business partners. Now a days the Virtual private network using ‘‘layer 2’’ (Frame Relay or, in a broad interpretation of layer 2, ATM and MPLS) and layer 3 technologies (IP over IP, GRE, IPSEC) [15]. A VPN have various characteristics such as a private network that offers protection from data modification, data interception or disclosure and denial of service while operating on a public network [16]. Virtual Private Networks (VPNs) are built on top of an Internet Service Provider’s (ISP) public infrastructure to establish secure and reliable connections with guaranteed Quality of Service (QoS) [17]. In VPN networks, the two main functions performed by MPLS are packet forwarding and route distribution.

Performance Evaluations: In this section we present the implementation of a Virtual Private Network (VPN) using a Multi-Protocol Label switching (MPLS) protocol, because this protocol is very promising, economically and technologically”. The environment that we have create or topology that we have build to test results i.e. to configure and test the result of VPN over MPLS and VPN over frame relay. The first topology is MPLS based VPN topology and the second one is VPN over Frame relay topology.

MPLS Based VPN Topology: In this topology MPLS based VPN is evaluated in a real environment. Here one site was consider as an End-User which is connected to another side of the network over MPLS backbone and on the other side few server arc connected to the LAN of the HQ (Head Quarter). The MPLS backbone is comprises of three (Cisco routers namely SP-l (Service Provider), SP-2 and SP-3. The two routers SP-1 and SP-3 acts as PE (Provider Edge) routers while SP-2 is called P-router (provider router). The purpose of the PE routers is to acts as a Ingress router or Egress router that depends on the flow of data. If data comes from end user and enter the MPLS domain so SP-l will acts as a Ingress router and will assign label to the IP packets known as PUSH label and will forward the traffic to the MPLS domain where the P-router will perform two major duties i.e. it will swap the label and forward to the correct next node which is SP-3 which then remove the label know as POP label and allow the packets as an IP packets to send out of the MPLS domain. The routers at the user’s side are known as CE (Customer Edge) routers.

VPN over Frame Relay Topology: In this topology VPN over Frame Relay is evaluated in a real environment. Two sites are connected here over frame relay link called customer-A and customer-B. Customer-A includes few users who are trying to access different data server across the link on the other side. Two routers are connected using Frame Relay Switch which is at the service provider side. After configuring the links and establishing the circuits we configured VPN over this frame relay link and check few parameters to find out how this layer-2 technology behaves.

Performance Comparison of Frame Relay and MPLS in VPN: We analyze the data that we have capture from the lab real environment. The analysis is done keeping in view different parameters namely bit rate, data rate. Throughput, average end-to-end delay and packet control overhead to find out which technology perform well. The results shows that MPLS based VPN have low average end-to-end delay, less packet control overhead and high data rate and high throughput ". Following are the comparison of the summaries of the communication port (Network Interface Card) on which the traffic was captured in both environment i.e. VPN over frame relay and IPLS based VPN. The parameters that are under observation in these two topologies are:

I. Bit Rate:

- To find whether the network provides Constant Data Rate, Variable Data Rate or is of Bursty Nature.

Data Rate:

- Peak Data Rate
- Average Data Rate
- Throughput
- End-to-End Delay
- Protocol Control Overhead

Number of Packets Processed: The following graph clearly shows the behavior of packets processing in both environments. We have take the following data for several times for a variable period of time and the average: number of packets processed in frame relay environment was 10000 packets while in MPLS based VPN it was noted that total of 18597 packets was processed.

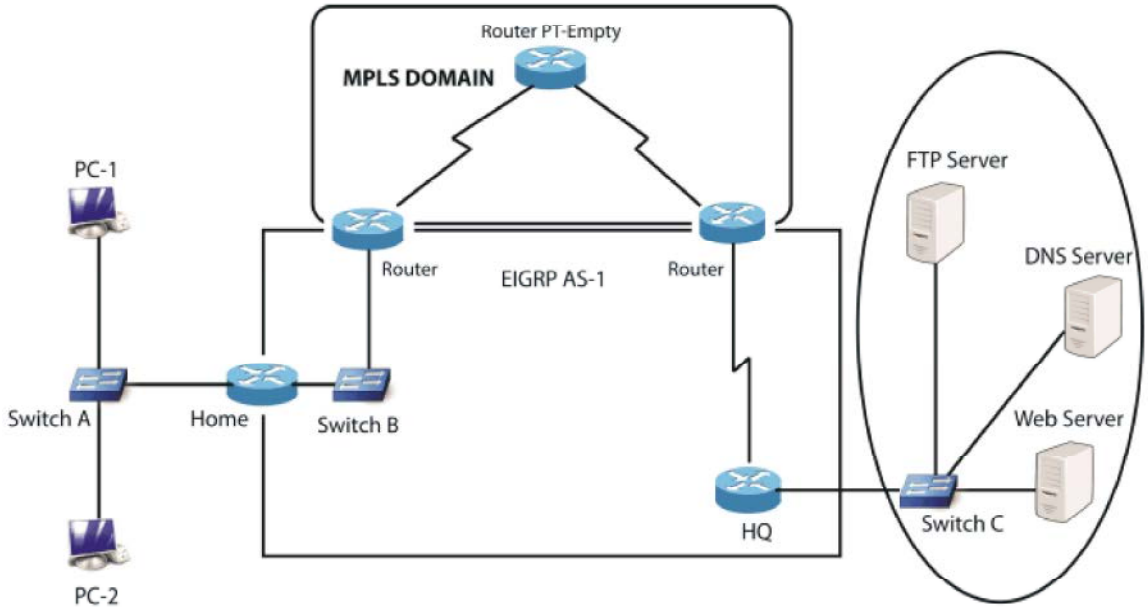

Fig. 7: VPN over MPLS

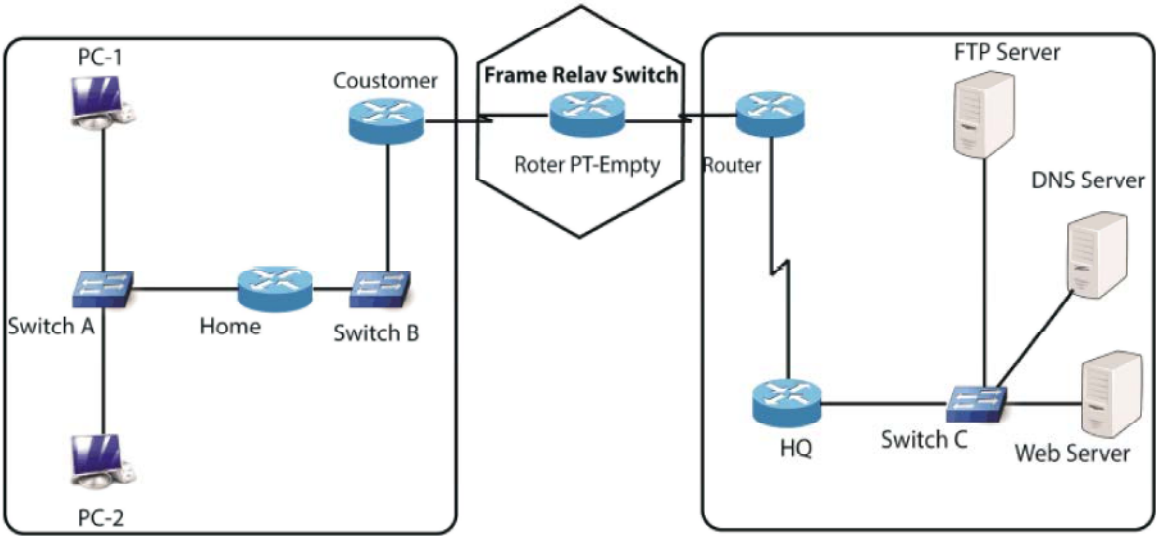

Fig. 8: VPN over Frame Relay

Number of Average Packets Processed/Sec: The following graph clearly shows the average packets per second in both environments. We have take the following data for many times for a variable period of time and the average number of packets processed per second in frame relay environment was 11.383 packets while in MPLS based VPN the number of packets per second is 11.491.

Total Bytes Processed: In this graph the total number of bytes processed has been matched. A total of 6415570 bytes has been processed in VPN over frame relay while total of 14033966 bytes has been processed in MPLS based VPN. The graph clearly shows the better behavior of MPLS.

Average Bytes/Sec: In this graph the average bytes/sec processed bytes has been compared where VPN over frame relay process 7384.741 bytes/sec and a total of 7870.872 bytes/sec are processed by MPLS based VPN.

The overall analysis of the IP traffic, FTP Traffic, FTP-Data traffic has been captured. It is clearly noted that in case of VPN over frame relay traffic (packets) has been

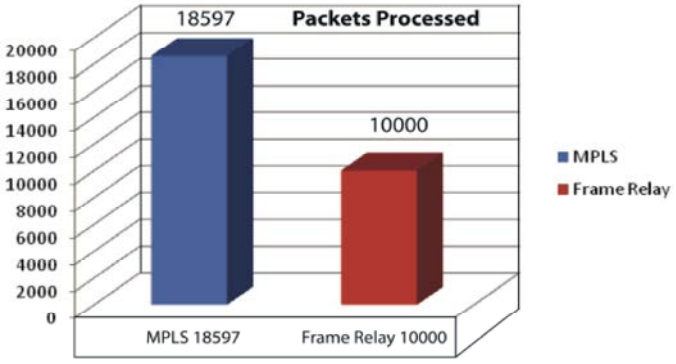

Fig. 5.1: Packets Processed

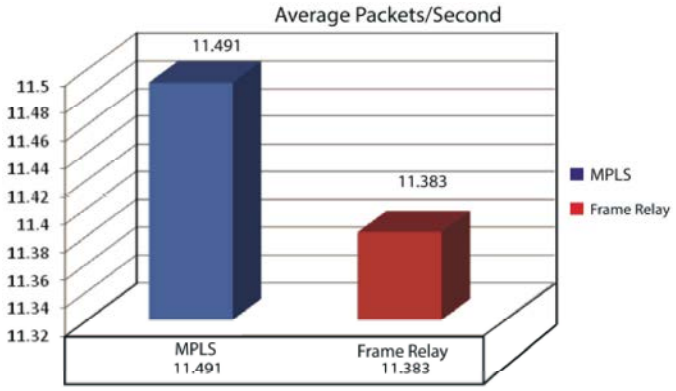

Fig. 5.2: Average Packets/Sec

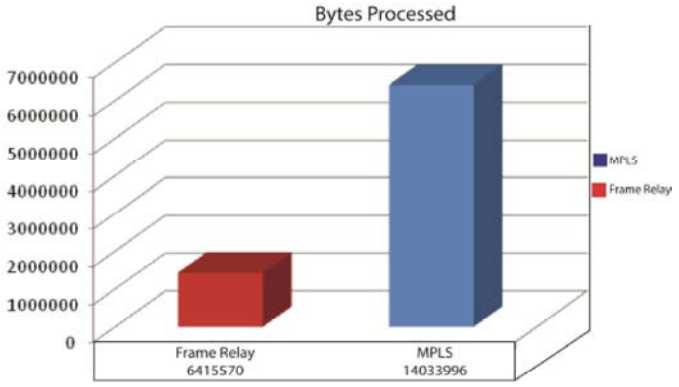

Fig. 5.3: Total Bytes Processed

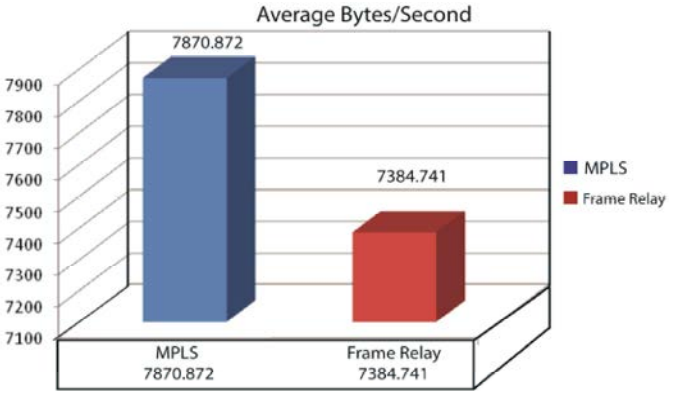

Fig. 5.4: Average Bytes/Sec

lost. In case of MPLS based VPN no packet lost has been detected and also the IP and FTP-DATA traffic are passing constantly. The traffic is captured after getting the traffic for many times for long time spam.

Data Rate

Average Data Rate: The following graph shows the average data rate of traffic which passes through VPN over Frame Relay and MPLS based VPN. The average data rate was noticed during the communication process in VPN over Frame Relay is 2144 bytes/sec while in MPLS based VPN the average data rate noticed is 2685.8884 bytes/sec. A lot of variation is also noticed in the data rate of VPN over frame relay while a constant data rate is noticed when VPN are working on MPLS. When packets were passing through the network in frame relay so the data rate is seen constant for the 30-seconds while there is seen a variation in the data rate when heavy traffic is sent which is not seen in the MPLS based VPN. The minimum average data rate noted in frame relay is 141.1318947451 bytes/sec while maximum goes to 3840.7079646018 bytes/sec and minimum average data rate noticed in MPLS based VPN is 2655.8540 bytes/sec while maximum is 2838.7898 bytes/sec. All of the above facts and figure show the better performance of Virtual Private Network (VPN) in MPLS domain then on Frame Relay.

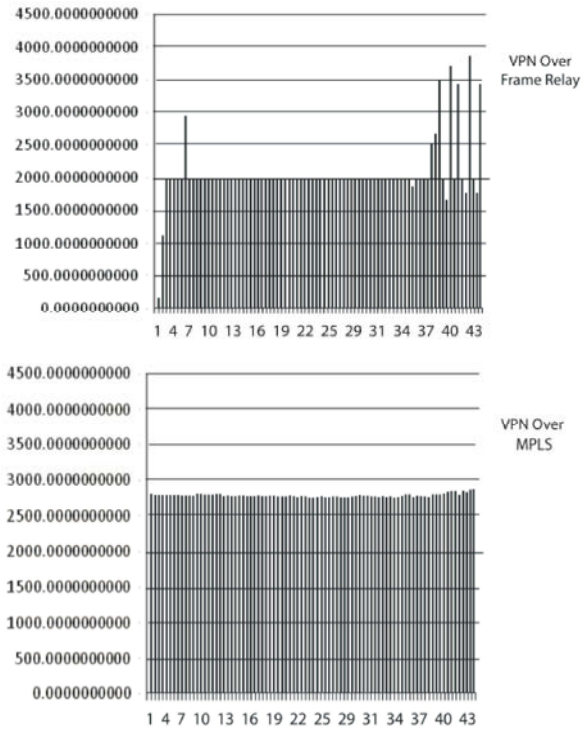

Fig. 5.6: Average Data Rate Analysis (VPN over FR and MPLS)

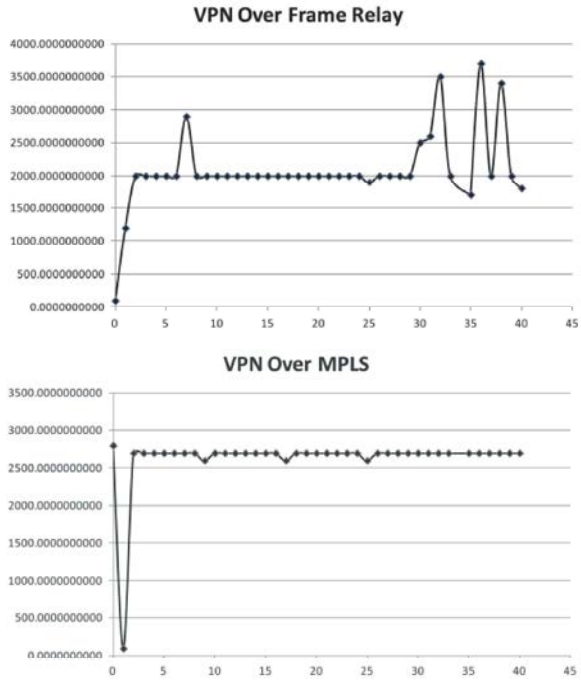

Fig. 5.7: Peak Data Rate Analysis (VPN over FR and MPLS)

Peak Data Rate: The main purpose of the Peak data rate is to find the maximum rate the data can achieve so that we can set the maximum bandwidth according to that rate. It is clear from the graph below and the behavior of both the technologies, the peak rate for VPN over frame relay is bursty means we cannot judge the average near peak rate as it goes up to maximum of 3840.7079646018 bytes/see but for very short span of time then again goes down and then again up, on the other hand the average peak data rate of VPN in MPLS domain is 2838.7898 bytes/sec which goes constant for the test of communication that take place over the MPLS domain. This graph again shows the constant nature of MPLS which results in better performance.

Throughput: The following graph clearly shows the throughput of both technologies, the throughput of VPN traffic over frame relay is variable. It is noted from the graph that for first 30-sec there is a slight variation in the throughput but after 30-sec when heavy traffic is sent so a lot of variation is noticed which not the case when VPN traffic goes across. MPLS domain. The total number of packets arc 1422 that passes through the frame relay link which result in average throughout of 25 packets/sec while the total number of packets that cross MPLS domain is 1729 which results in the average

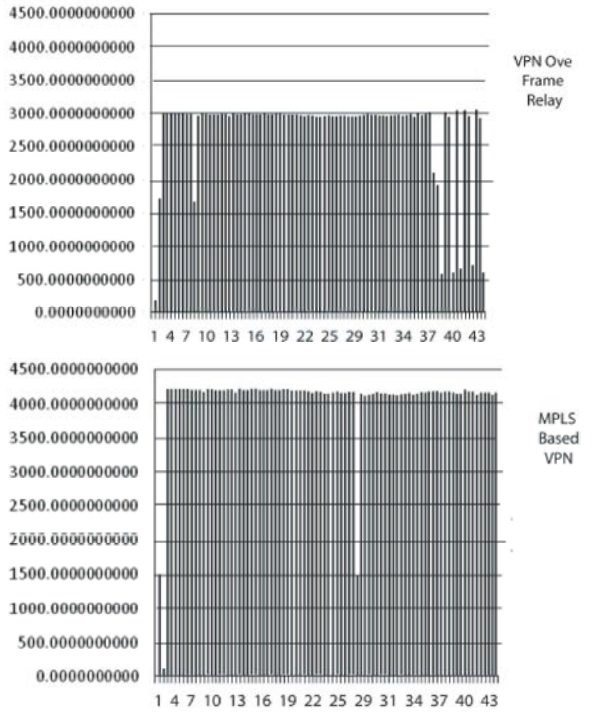

Fig. 5.8: Throughput (VPN over Frame Relay & MPLS)

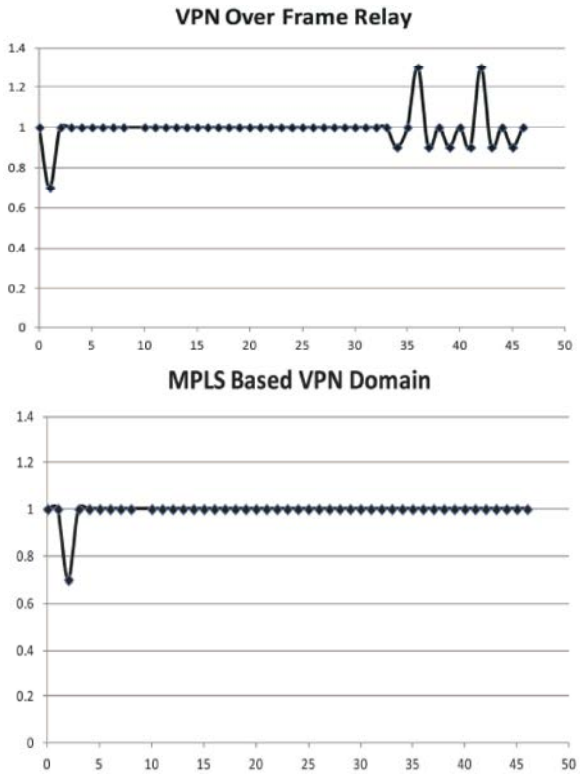

Fig. 5.9: Average End-to-End Delay (VPN over Frame Relay & MPLS)

throughput of 39 packets/sec. The throughput of both technologies shows the correct choice through which we can send our VPN which is MPLS.

End-to-End Delay: It is clear from the graph given below that VPN over frame relay and MPLS perform differently. The nature of VPN over frame relay shows that a variable pattern of delay occurred which will affect the performance of the flow of the traffic in terms of end-to-end delay. In frame relay delay is small at the start of communication that is 1 sec; while it suddenly drops down to 0.7 sec then again jump up to 1-sec which remains constant till 30-sec. In case heavy traffic is sent, the delay goes up to a maximum of 1.333333 sec and then changes very quickly. While in case of VPN over MPLS, the performance clearly shows that the delay is small at the start of communication; that is 0.68 sec. while it goes up to a maximum of 1-sec which then remains constant for remaining communication. The uniform nature of MPLS VPN make it better option an VPN over Frame Relay which shows variation and more delay.

The results shows that MPLS based VPN faced 54.55 msec/packet delays while VPN over Frame Relay faced 106.67 msec/packet. This can conclude that if 100.0% is the delay in MPLS based VPN so 195.52% will be the delay in VPN over Frame Relay which is almost double of the delay in MPLS based VPN.

Protocol Control Overhead: The graph illustrates that frame relay VPN has low routing overhead throughout the communication. The routing traffic that is sent across the frame relay is 4093.947 bits/sec against the data traffic that is received which are 267662.44 bits/see while in MPLS based VPN the routing traffic that is sent is 568.4768 bits/sec against the data traffic received 398365.69 bits/sec. As noted the routing overhead increases in frame relay as compare to MPLS while at the same time the number of packets processed is more in case of MPLS. From these facts and figures it is clear that VPN over MPLS domain works better than VPN over frame relay.This is why we say that VPN over MPLS domain perform well in Protocol Control Overhead and also in other parameters also namely constant data rate, low delay and consistent nature and high data traffic rate.

If we refer to the packet control overhead values so VPN over Frame Relay shows a 1.53% packet control overhead while MPLS based VPN shows 0.14% which is very low as compare to VPN over Frame Relay.

VPN and VPN over Frame relay have been configured and study in a live environment, the capture data is then analyze and we have at the conclusion that MPLS effect VPN in a good and positive manner i.e. if an application

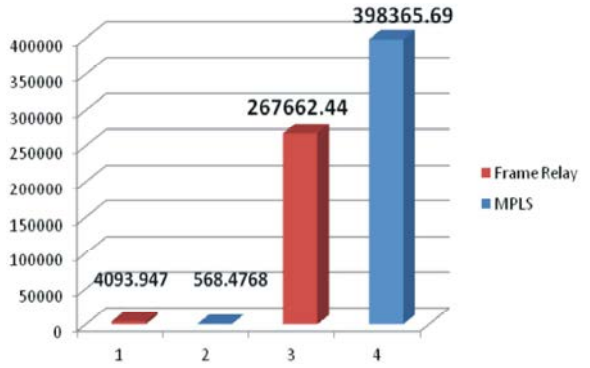

Fig. 5.10: Protocol Control Overhead (VPN over Frame Relay & MPLS)

works well in a frame relay, it will work better using MPLS, if an application not perform adequately on VPN over frame relay and results in packet loss or delay, MPLS will be right solution.

CONCLUSION

The basic purpose of a network begins with initial design and architecture, with provider provision services of voice, video and data with high level of availability is the requirement of an enterprise business customer. "A layer-2 protocol e.g. MPLS or the Ethernet protocol is used to optimally map IP traffic on the physical infrastructure and to implement value-added network features and services e.g. Q0S" and "Quality of Service is used as Umbrella term to cover network performance characteristics". Every enterprise has certain basic critical application and service which should be running properly and smoothly for which we need a reliable technology that we should configured in our network. Another important need of an organization is that the communication should take place securely over the network and for that many business and office have configured VPN and the important application of MPLS is MPLS based VPN and many small and medium business organizations rely on VPNs on a shared network. Infrastructure based on MPLS technology. In order to achieve optimal results and successful business operations providers must adopt efficient and cost-effective policies. "Multiprotocol Label Switch virtual private network (VPN) service emerged as a Value added cost effective VPN based service and its market opportunity is tremendous for network service providers.(NSP)".

REFERENCES

1. Lin, J.W. and H.Y. Liu, 2010. Redirection based recovery for MPLS network systems. Journal of Systems and Software, 83(4): 609-620.
2. Kempf, J., *et al*., 2011. OpenFlow MPLS and the open source label switched router. in Teletraffic Congress (ITC), 2011 23rd International.
3. Alwayn, V., 2001. Advanced MPLS design and implementation. Cisco Systems.
4. Subash Babu Asokan, B.G., Brian Wesley Simmons, Fran Singer, Megha Shaseendran, Krupa Chandrashekar, Namrata Mehta, Pallavi Madhusudhan, Chander Aima, Poornima Goswami, Hema Priya J, Sairam Venugopalan, MPLS Overview, B. Mann, 2010, Juniper Networks, Inc.
5. Kaimal., J., 2010. MPLS Based VPN, in Technical Report Series. Nov 2010, George Mason University: Fairfax, Virginia.
6. Fathy, M., S. GholamalitabarFirouzjaee and K. Raahemifar, Improving QoS in VANET Using MPLS. Procedia Computer Science, 10(0): 1018-1025.
7. Kiani, H.S. and M.H. Baig, 2010. Performance Evaluation of MANET Using MPLS., MS thesis, Bleking Institute of Technology, Sweden.
8. Bisti, L., *et al*., 2011. Improved network resilience of wireless mesh networks using MPLS and Fast Re-Routing techniques. Ad Hoc Networks, 9(8): 1448-1460.
9. Koçak, C., I. Erturk and H. Ekiz, 2011. A Real-time Multimedia Application Study in Lmds Networks Using Mpls. e-Journal of New World Sciences Academy, 6(1): 1A0153.
10. De Ghein, L., 2007. MPLS Fundamentals. Cisco Press.
11. Bush, R. and T.G. Griffin, 2003. Integrity for virtual private routed networks. in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies.
12. Daugherty, B. and C. Metz, 2005. Multiprotocol label switching and IP. Part I. MPLS VPNs over IP tunnels. Internet Computing, IEEE, 9(3): 68-72.
13. Akar, N. and M.A. Toksöz, 2011. MPLS automatic bandwidth allocation via adaptive hysteresis. Computer Networks, 55(5): 1181-1196.
14. Rossberg, M. and G. Schaefer, 2011. A survey on automatic configuration of virtual private networks. Computer Networks, 55(8): 1684-1699.

15. Bolla, R., R. Bruschi and F. Davoli, 2006. Capacity planning in IP Virtual Private Networks under mixed traffic. Computer Networks, 50(8): 1069-1085.
16. Gallaher, R., 2003. Chapter 7 - Virtual Private Networks and MPLS, in Rick Gallahers MPLS Training Guide., Syngress: Rockland, pp: 141-185.
17. Robert, J.M., *et al*., 2012. A distributed resource management model for Virtual Private Networks: Tit-for-Tat strategies. Computer Networks, 56(2): 927-939.