ISSN 2277-3061
VOLUME 15 NUMBER 13
INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Efficient Data Forwarding Mechanism in Backbone Networks by Employing MPLS Technology

Walid Iltaf
FH Kärnten, Klagenfurt Austria
Walid.Iltaf@fh-kaernten.ac.at

Abstract

Multiprotocol Label Switching (MPLS) is a relatively new WAN technology that is attracting the networking professionals around the globe. Many ISPs have already deployed it in their network. Yet, some other ISPs are in the pipeline to deploy it. Nevertheless, it has caught the attention of professionals soon after it was developed. Instead of the IP address or MAC address, MPLS works on small labels. These labels are inserted between Data Link layer and Network layer of the OSI model. Forwarding decisions are based on these labels; instead of looking at complex routing tables. The MPLS network is configured, and tested under different conditions. A comparison is drawn between the IP and MPLS network. The obtained results show that MPLS has a lower end to end delay and less CPU utilization. Furthermore, MPLS has lesser processing delay as compared to the IP network. The performance difference is basically due to the intelligent forwarding mechanism of MPLS technology. It is also important to further investigate this topic in terms of security considerations. The labels values are not encrypted during transmission, and there is no authorization mechanism defined. It will be highly beneficial to have more sophisticated suite of security tools to encounter threats and vulnerabilities.

Keywords

MPLS, Backbone Network, End-to-end Delay, CPU utilization, Processing Delay

Introduction

MPLS technology is rapidly emerging as a core technology for the next generation networks (NGN), in particular optical networks and high speed backbones. MPLS is essentially a hybrid routing/forwarding strategy, streamlining the backbone switching of IP packets between layer 2 and layer 3 [1]. The forwarding decisions are based on small labels; instead of looking up complex IP tables. A label is inserted between Data Link layer (layer 2) and Network layer (layer 3) of the Open System Interconnection (OSI) model as shown in figure 1. It combines the advantages of Data Link and Network layers. Therefore, it is sometimes also defined as layer 2.5 technology [2]. It is backward compatible with the other legacy technologies like Asynchronous Transfer Mode (ATM), Frame Relay (FR) etc. This way of forwarding the data is not new. Previously FR and ATM adopted the same kind of mechanism, while forwarding the data. FR uses the frame of variable size, while the ATM has fixed cell size. The main similarity between these two technologies is that the “label” value in their header is changed from hop to hop [3]. Same mechanism is adapted by MPLS, where label is changed in each hop. This is altogether a different way, as compared to IP network, where destination IP address remains fixed during whole transmission in the network. The label is 32 bits in length. It consists of four fields as shown in figure 2 [4]. The first field is a 20 bit long label value. Labels are represented in decimal format. The second field is of experiment. These 3 bits are reserved for experiment. 1 bit long Set field (S) is kept 1 if it is the last label in number otherwise kept 0. Last field of Time to Live (TTL) comprises of 8 bits and is used to count the number of hops. It is used to detect the presence of loops in the network.

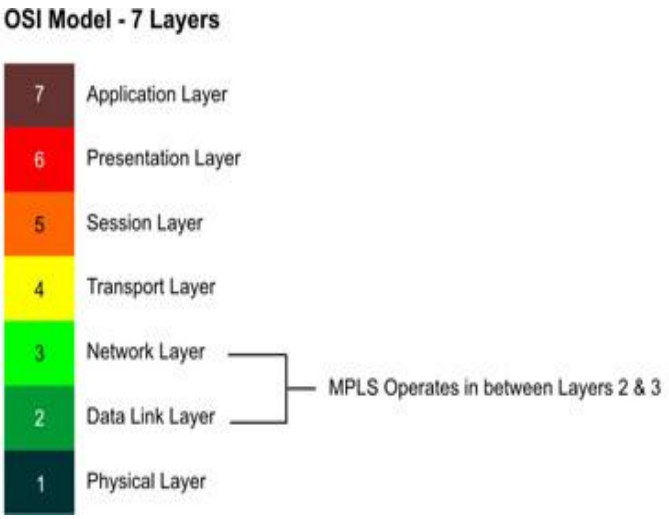

Figure 1: The MPLS label’s position in the OSI model [5]

The MPLS was developed by the Internet Engineering Task Force (IETF) in 2001. The standardized MPLS was described in Request for Comment (RFC) 3031 [6]. The terminologies related to the MPLS are also defined in the RFC 3031. The MPLS network consists of various devices and protocols. A simple MPLS network is shown in figure 3.

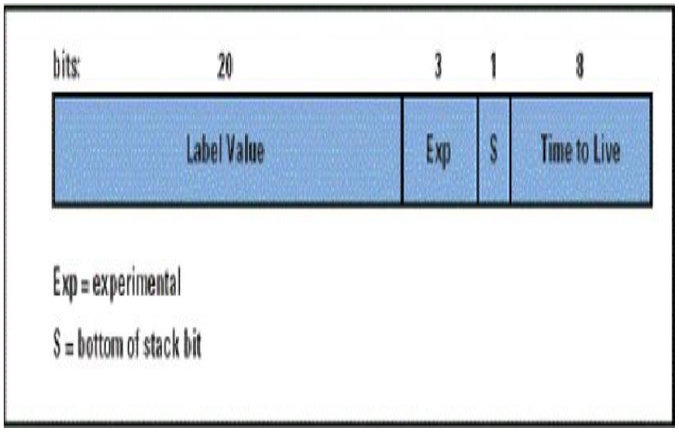

Figure 2: MPLS label format [7]

To understand the working methodology of MPLS, it is important to know the terms associated with it.

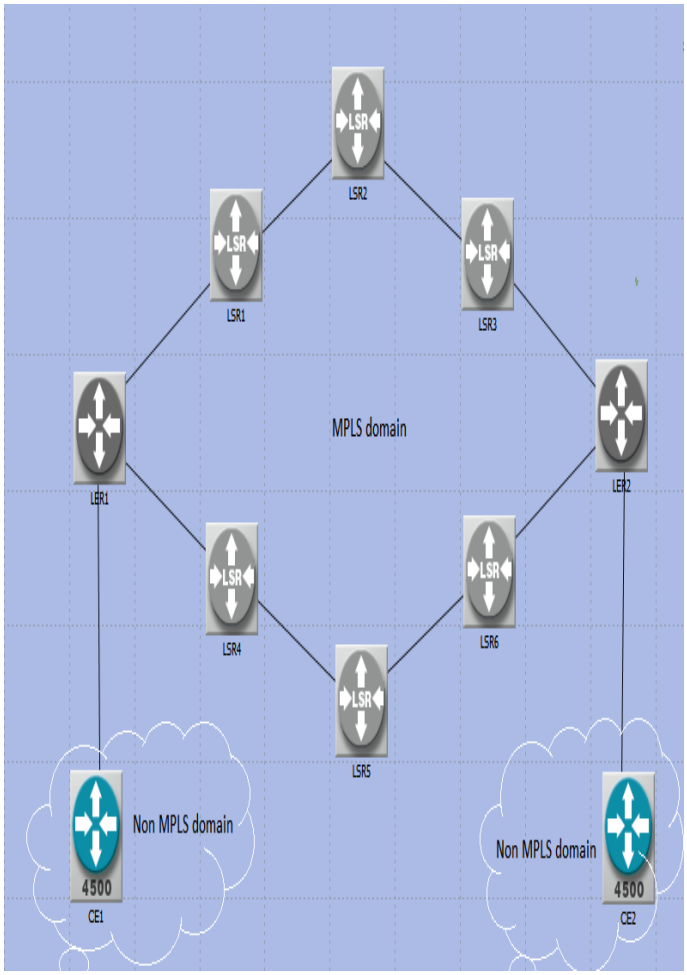

Figure 3: MPLS architecture

The terminology is described, so that the architecture of MPLS network can be defined conveniently. Moreover, these terms describe the roles of various network devices, which constitute the MPLS network.

Label Switch Router (LSR): It is a device in the MPLS domain, capable of inserting, swapping and removing MPLS labels. [8][9]. LSR has following types.

Ingress LSR: It is the first device of MPLS domain. It has a direct link with the customer's network or non MPLS domain. This node is also called Label Edge Router (LER) or Provider Edge (PE) router. When traffic from the customer enters into this device (LER), a label is attached with it.

Egress LSR: This is the last node in the MPLS domain. This node handles the incoming MPLS traffic to forward it to non MPLS domain. The MPLS label is removed by this device.

Intermediate LSR: The functionality of this device is to swap the label, as MPLS label is changed by every device in the domain.

Label Switched Path (LSP): It contains all the LSRs through which traffic flows from the source to the destination in the MPLS network.

Customer Edge (CE): This is the end device in the customer domain. It has a direct link with the provider's network.

Customer's Network (C Network): This is a total customer controlled network. MPLS doesn't run in this network segment.

Provider's Network (P Network): This is the network of ISP. It is also called backbone network. MPLS runs in this network.

MPLS Working Methodology

There are two important challenges related to MPLS (Control plane & Data plane). The control plane is involved in exchanging routing information and exchange of labels [10]. This can be explained using figure 3. As, MPLS works in the provider's network only, the customer's network works like a normal IP network. The IP traffic from the customer's network enters into provider's network. At this point, MPLS comes into action. The question arises that how PE-1 in the figure knows that it has to forward the traffic of customer A1 to PE-2 instead of PE-3. The customer's routing information is forwarded to the connected PE routers using any routing protocol or static routing. This is also called PE-CE routing in MPLS VPN. This customer information is then stored in a Virtual Routing & Forwarding (VRF) instance, instead of router's main routing table. Labels are assigned to each customer, and route distinguishers (RD) are assigned to differentiate among the various customer sites connected with the same PE device. These routes are exchanged with the destination PE device with Interior gateway protocols like OSPF, RIP, and EIGRP etc. The labels are exchanged using Label Distribution Protocol (LDP). But, it is not true for all situations. When MPLS/BGP VPN is implemented, Multiprotocol BGP (MP-BGP) is used to carry both the routing and labels information to the destination PE. RSVP is another protocol used for signaling purposes in MPLS. It is important to note that label values are assigned based on the routing information.

Control plane problem explained how the routing information is exchanged in the MPLS network. Now, the question is about the data plane. It is about how actually data is transmitted from hop-to-hop in a MPLS network. It deals with the mechanism that which label is used for a particular customer, and swapping of labels as data moves in the network. The control plane and the data plane exchange information with each other as shown in figure 4. It is clear from the picture that data plane deals with the forwarding of IP or labeled packets received. It also communicates with the control plane to extract the routing and labeling information. The communication between both the planes is bi-directional.

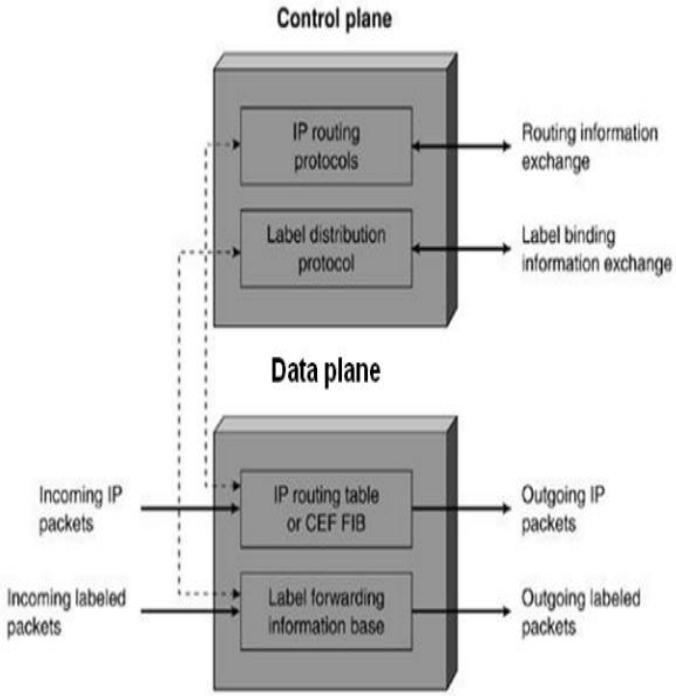

Figure 4: The control & data plane problem [10]

A. IP World Forwarding Technique

The routing & forwarding of traffic in the IP world is based on the destination IP address. Furthermore, every device in the network makes the forwarding decisions independently. The destination IP address in the IP header is matched with a same network address present in the routing table. A device in the backbone network has huge number of routing entries stored in the routing table. The router has to go through its complete routing table for the destination address match. This takes a lot of consumption power of the device and generates a higher processing delay. But, the irony is that the device has to perform the complete routing table lookup for every packet arriving at it.

B. MPLS Forwarding Technique

The forwarding technique in the MPLS is altogether different from the IP world. Instead of destination based routing, source based routing is used. The MPLS router checks the incoming label and swaps it with a relevant outgoing label, by looking up in its LFIB table. The LFIB table is very small as compared to the routing table. Secondly, the labels agreement is already established among all the devices before the actual communication starts. Hence, the every device in the network is not free to choose the label value and make independent decisions.

Applications

MPLS is currently used in many applications. Originally, it was used to develop in the backbone networks and optimized VPN services. But, due to its outstanding advantages it was used in the wireless networks and MANETs as well. Following are the important applications of MPLS.

C. MPLS Layer 3 VPN

MPLS layer 3 VPN gained its popularity, as soon as MPLS was launched. In this method, the segregated networks are connected using an MPLS backbone network. This VPN type is in high demands because of its better performance, higher scalability and flexibility. The private traffic is entered into a tunnel at the PE router. This tunnel terminates at the destination PE router. Moreover, the routing information of customer is not stored in the global routing table. Instead, it is stored in separate Virtual Routing and Forwarding (VRF) instances. This separation of routing information is considered as a good security measure. However, by default no particular security algorithm is deployed as discussed in the earlier sections.

D. Any Transport over MPLS (AToM)

Any Transport over MPLS (AtoM) was developed after the success of MPLS VPN [11]. The MPLS doesn't only work with the IP protocol, but it was developed to work with the other layer 2 technologies. It made MPLS more flexible for the legacy technologies as well. It was also standardized by the IETF. Procedures were described to transport layer 2 frames over the MPLS enabled backbone network. The layer 2 technologies that are supported are Asynchronous Transfer Mode (ATM), Frame Relay (FR) and Ethernet. When the layer 2 frames of any of these technologies arrive at the PE router, they enter into a Pseudo Wire (PW). This PW is like an end to end tunnel, between the PE routers. These can be categorized as follow.

- Frame Relay over MPLS (FRoMPLS)
- Asynchronous Transfer Mode over MPLS (ATMoMPLS)
- Ethernet over MPLS (EoMPLS)

The EoMPLS is considered as a bright aspect of MPLS. But, it is mostly known by the name of Virtual Private LAN Service (VPLS). In this method, the Ethernet frames are transported across the network. The segregated parts of customers' network, virtually appear one single LAN.

E. Traffic Engineering

This is yet another charming feature of MPLS technology. The traffic is steered in a most optimum way. This way of finding the optimum path is more intelligent than IP, as it takes into consideration the parameters like available bandwidth of the link [3]. Furthermore, it offers a more robust way for the load balancing in the networks. It has also support for the QoS features as well.

F. Generalized MPLS (GMPLS)

Generalized MPLS (GMPLS) is a further extension to the original MPLS technology, to support further layer 2 and optical switching technologies. It was standardized by the IETF in the RFC 3495. It has support for the SONET/SDH, PDH, TDM and spatial switching techniques [11]. The GMPLS is used to allocate resources for these techniques, and provide mechanism for the restoration techniques in case of failures.

G. MPLS Transport Porfile (MPLS-TP)

It is a standard defined by IETF to enable the MPLS functionality in the transport networks [12]. Some attributes of MPLS are not used in this technique due to working methodology and architecture of these networks. The OAM plane of transport networks work differently, as the control plane of MPLS. However, MPLS is used to t converge the transport networks to a one infrastructure for reduce expenditures and ease of management.

H. MPLS in Wireless & AdHoc Networks

With the rapid growth of traffic in mobile networks, the higher performance in the backbone is required. Operators are now using the MPLS in the mobile backhaul for optimized results. Furthermore, it is also used in the MANETs for the increased performance.

SEcurity Aspects in mpls

The possible security vulnerabilities are discussed in [13]. Generally, the LDP communication is not encrypted in the MPLS infrastructure. Secondly, this mechanism is also not authorized, as any device even from outside the MPLS core can send the labeled packets. This may create a situation where a number of possible hacking attacks can becarried out. The possible situations are discussed in the subsequent sections.

I. LDP Information Hacking

As, the LDP communication is neither encrypted, nor authorized in the MPLS core. If this LDP information is somehow stole, may result into number of possible attacks. For example, this may lead to rogue destination, or rough path switching. It means that it reaches the destination, for which the packet was not intended. Secondly, a particular LSP is followed in MPLS, which can be manipulated using this information. A new rough path can be set up.

J. Labels Brute Force Attack

Another possible situation is, when the MPLS core accepts the labeled packets from outside the core. A brute force attack is possible, by attempting all possible label values for the specific destination. After a reply message is transmitted back, the actual label distribution in the network can be retrieved. If MPLS core accepts labeled packets form outside, there is possibility that Label Information Base (LIB) can be manipulated because the LDP sessions are not authenticated. Poisonous information can be installed in the LIB, and can be used for injurious purposes. For example, it can be manipulated in such a way that time sensitive traffic is forwarded on the congested paths, resulting into an inefficient network performance.

SIMULATIONS

A simple network is shown in the figure 5. The baseline simulations are carried out using OPNET. The network is tested by transmitting voice traffic among the end devices. The network consists of MPLS routes (Ingress_R1, LSR_R1 to LSR_R6, and Egress_R6). The IP routers (R1 and R2) are Cisco 4000. R1 and R2 are CE edge routers and provide a direct connectivity with the PE router (Ingress_R1). The MPLS working starts working from this device. The voice traffic is sent by the devices PC1-PC6. To compare the end-to-end delay in both networks, the MPLS routes are replaced by the IP routers (Cisco 4000) and performance parameters are compared in the section VI. The theoretically important parameters like CPU utilization, end-to-end delay, processing delay are compared and discussed in the subsequent section.

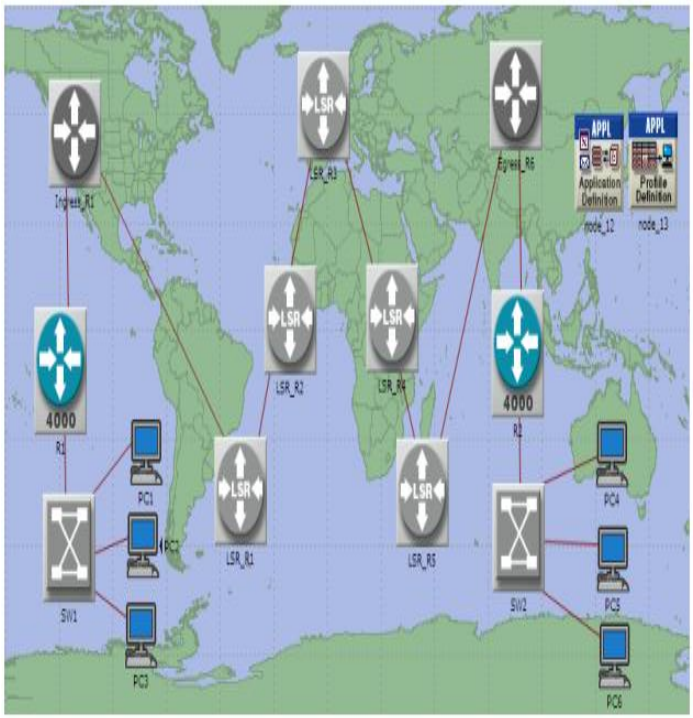

Figure 5: The network topology for the simulations

RESULTS

The important results obtained are discussed in this section. The CPU utilization of different devices is shown in the figure 6 below.

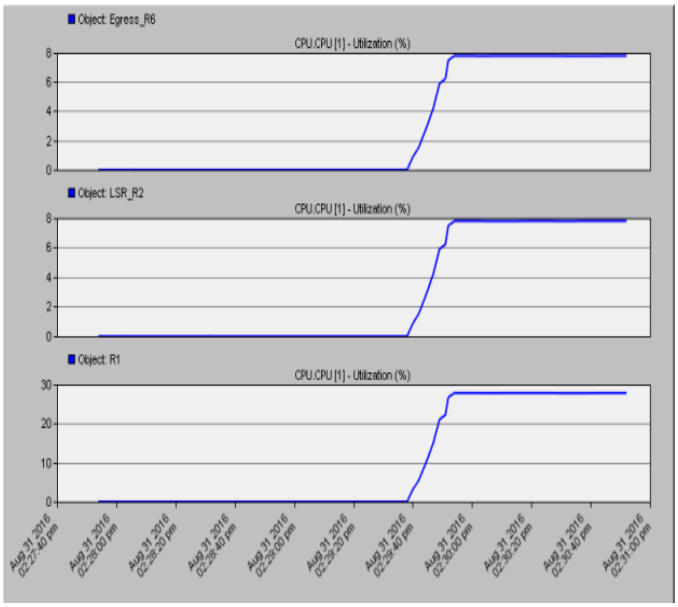

Figure 6: CPU utilization of different devices

The figure shows that MPLS router has low CPU utilization (8%). While, in the same network the IP router's utilization is on the higher side (30%). This significant difference of processing consumption is due to the difference in the forwarding methodology of both technologies. The IP router has lookup its complete routing table for destination address entry. It has to repeat this task for every incoming packet at the device. This resulted into higher processing consumption. On the other hand, the LFIB table of MPLS router is quite small as compared to the IP router. This resulted into a low value of CPU utilization. The higher CPU consumption may lead to higher value of mean time between failures (MTBF) of the IP routers, which may result into increased expenditures. The value of CPU utilization can be higher in real backbone networks due to the presence of huge amount of routing entries in the routing table and LFIB. But, in this case result was obtained for a relatively small network. Even with the bigger network, the output pattern will show the similar difference between the two technologies.

Another important result is the end-to-end delay in the network. Figure 7 and 8 shows the delay in both types of networks.

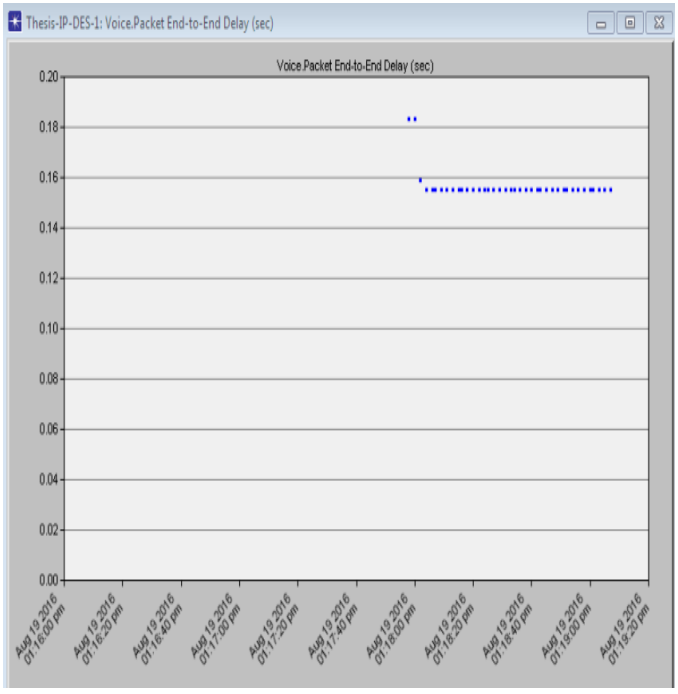

Figure 7: End-to-end delay in IP network

It can be seen that end-to-end delay in the IP network is almost 156 mille seconds (ms). This amount of delay is considered very high in the context of Voice over IP (VoIP) traffic. VoIP is a time sensitive, and maximum possible delay for smooth communication is 150 ms, which is exceeded in this case. However, by employing MPLS the end-to-end delay is reduced to 140 ms, as seen in figure 7. This reduction in the delay is due to efficient forwarding mechanism employed by the MPLS technology. The same is true not only for the voice networks, but also other kinds of traffic carried by the network. The lesser delay results into improved throughput, and lower values of dropped packets. This parameter yields into overall improved performance in the backbone network.

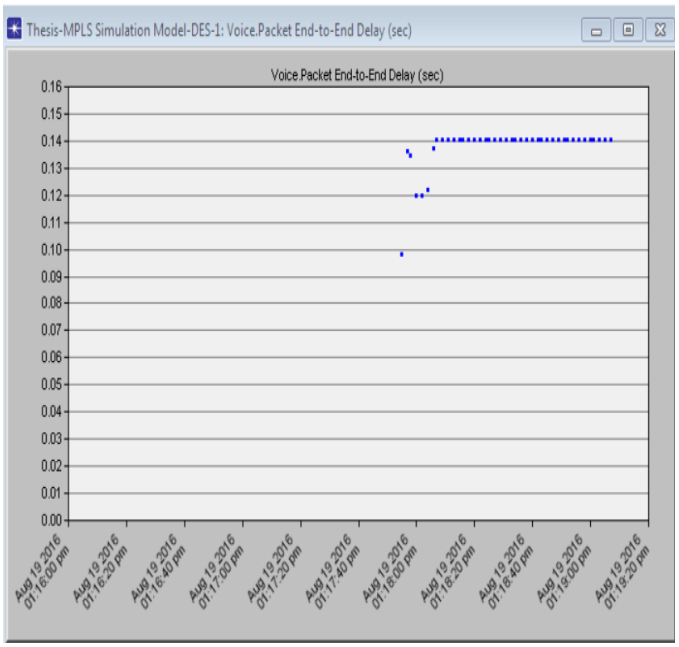

Figure 8: End-to-end delay in MPLS network

The time spent by a router to processes a packet is also important. A quick processing will yield better network performance. A processing delay of the IP and MPLS router is shown in the figure 9.

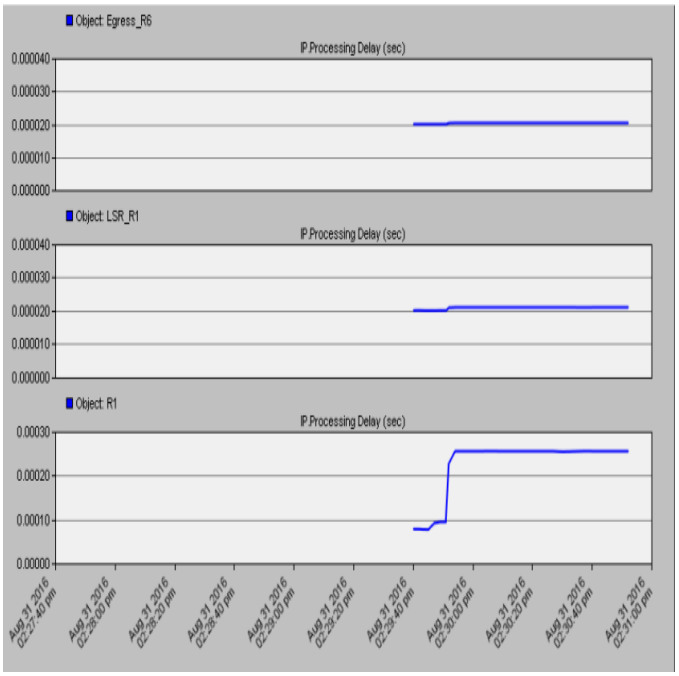

Figure 8: Processing delay in IP & MPLS routers

It can be seen that the processing delay in IP router (R1) is 250 micro seconds (us). While, the processing delay for the MPLS router is only 20 us, which is comparatively low. This delay is increased by many times as in a backbone network, a huge amount of packets are flowing. The lower value in the MPLS outperforms the IP network, and proves its credibility. The higher delay in the IP network is due to its lookup in a long IP table.

CONCLUSION

The results show that forwarding strategy employed by the IP is not intelligent. It causes delay in the network and higher values of CPU utilization. The problems in the IP world can be addressed by enabling MPLS in the backbone networks. The efficient way of forwarding the traffic in MPLS results into lower values of delays (end-to-end, and processing) in the network. Another, improved parameter in the MPLS is CPU utilization. The MPLS takes very less processing power, while the IP forwarding is highly processing intensive.

The better network parameters results and its backward compatibility with the other legacy technologies, and Ipv6 addressing scheme make MPLS a popular technology to be used in the backbone networks. However due to its efficient features, it has numerous popular applications like MPLS/BGP VPN, VPLS and deployment in mobile backhaul networks. The usage in transport networks and MANETs is also increasing due to its labels based forwarding mechanism. However, security techniques used by MPLS are not highly reliable. There is no by default security standard employed by MPLS.

Furtuer work

More and more intelligent networks attacks are carried out by hackers, and need for a higher level of security is required more than ever. MPLS has to be studies in depth, in terms of security matters and possible loop holes must be addressed.

Furthermore, the standardization of LDP for the Ipv6 addressing scheme is in pipeline. It is important to investigate the label distribution mechanism and find out its efficiency and possible vulnerabilities. Moreover, the original MPLS protocol was updated in the RFC 3945. This Generalized MPLS (GMPLS) is defined to support other switching technologies like TDM. This protocol can be further studied, as it may require new updates or possible deficiencies can be spotted out. It is also interesting that many wireless networks use the IP protocol for their backbone network for example, UMTS, LTE, WiMax etc. MPLS works on the bases of IP protocol, MPLS can be deployed in wireless networks for efficient performance. The topic of wireless MPLS (WMPLS) is highly valued in recent times.

REFRENCES

[1] Francesco Palmieri “VPN scalability over High Performance Backbones Evaluating MPLS VPN Against Traditional Approaches” Eighth IEEE International Symposium on Computers and Communication (ISCC’03), 2003

[2] Rohit Mishra, Hifzan Ahmad “Comparative Analysis of Conventional IP Network and MPLS Network over VoIP Application” International Journal of Computer Sciences and Information Technologies Vol 5(3), 2014

[3] Luc De Ghein “MPLS Fundamentals”, Cisco Press USA 2006

[4] Rissal Efendi “A Simulation Analysis of Latency and Packet Loss on Virtual Private Network through Multi Virtual Routing and Forwarding”, International Journal of Computer Applications Volume 60-No.19, 2012

[5] What is MPLS? Available online: http://mplsinfo.org/ last accessed, 18 October, 2016

[6] Muhmmad Ahsan Chishti and Ajaz Hussain Mir “Performance Analysis of Traffic Engineering (TE) in IPv6 with IPv4 over Multi Protocol Label Switching (MPLS)” International Journal of Computing and Network Technology, January 2015

[7] MPLS label format (http://www.cisco.com/c/dam/en_us/about/ac123/ac147/images/ipj/ipj_4-3/figure3.gif), last accessed 18 October, 2016

[8] E. Rosen, A. Viswanathan, R. Callon “Multiprotocol Label Switching Architecture” RFC 3031, January 2001

[9] Edmira Xhaferra “A Review Paper: Analysis of OSPF & RIPv2 over MPLS VPN with OPNET Simulation” Imperial Journal of Interdisciplinary Research (IJIR), vol-2, issue-2, 2016

[10] Vivek Alwayn, “Advanced MPLS design and Implementation”, Cisco Systems, Cisco press USA, 2001

[11] Tran Cong Hung, Le Quoc Cuong, Tran Tahi Thuy Mui “A Study on Any Transport over MPLS (AToM)”, ICACT 2010

[12] Understanding MPLS-TP and Its Benefits, Cisco Press 2009, Available online: http://www.cisco.com/en/US/technologies/tk436/tk428/white_paper_c11-562013.pdf last accessed 18 October, 2016

[13] Thorsten Fischer, “MPLS Security Overview” Information Risk Management London, December 2007