ISSN No:-2456-2165

Analysis of Multiprotocol Label Switching on Virtual Private Networks

Thet Zaw Aye
Faculty of Information and Communication Technology
University of Technology (Yatanarpon Cyber City)
Pyin Oo Lwin, Myanmar

Abstract:- Multiprotocol Label Switching (MPLS) is used in Service Provider Networks because of its fast packet forwarding mechanism. MPLS is a Wide Area Network (WAN) technology. This system concern about MPLS on Virtual Private Networks (VPN). MPLS creates two types of VPNs. One is Layer 3 MPLS VPN and other one is Layer 2 MPLS VPN. In this system, those two VPNs are configured in order to understand how MPLS VPNs work on different layers. And this system also focus on a performance analysis of Layer 2 MPLS VPN and Layer 3 MPLS VPN with performance parameters such as throughput and delay (end-to-end). Graphical Network Simulator-3 (GNS3) is used to configure Layer 2 MPLS VPN and Layer 3 MPLS VPN.

Keywords:- *MPLS; Layer 2 MPLS VPN; Layer 3 MPLS VPN.*

I. INTRODUCTION

Today, most of large enterprises and business companies are spread their offices on different locations. Computing networking and Internet are used to connect between their business branches and head office. In the past, company and organization are used various WAN technologies such as Frame Relay, ATM or T1 for Internet and WAN connections. But current network traffic and security concern, those technologies are not enough for the WAN connectivity. Multiprotocol label switching (MPLS) replaces other WAN technologies due to higher reliability and higher performance. To maintain security problems, layer2 VPN is used in a non-scalable enterprise network. MPLS VPN provides scalability to partition large companies into smaller networks. It becomes very useful in IT organizations that must provide isolated networks for their departments. Large companies are interested in MPLS VPN because it offers a new option for WAN connectivity.

II. MPLS

MPLS is an IP technology developed by the Internet Engineering Task Force (IETF) to overcome the weakness of traditional IP routing. MPLS technology is rapidly becoming a common technology of next-generation networks, especially optical networks and high-speed backbones used in service provider network. MPLS is essentially a hybrid routing/ forwarding strategy that simplifies the switching of the backbone network of IP packets between Layer 2 and Layer 3 [3]. MPLS used small label values for routing. The packets are forwarded according to the label and not the destination IP address. This way of forwarding data is not new. Previously, FR and ATM used the same mechanism when sending data. FR uses frames of variable size, while ATM has a fixed cell size. The main similarity between the two technologies is that the value of tag called label in the header changes from hop to hop [4]. MPLS uses the same mechanism like that in which the tags changed in each hop. This is altogether a different way of routing as compared to IP cloud, where the destination IP address remains fixed during the whole transmission in the network.

A. MPLS Operation

Multiprotocol label switching is a protocol that integrates layer 2 information, about network links (for example, bandwidth, latency, utilization) in Layer 3 (IP) within the network, which helps to improve and simplify the IP packets. The basic concept of MPLS is to accelerate packet delivery by assigning packets to a specific direct equivalence class (FEC). Here, the label edge router (LER) uses labels to label packets with the same destination. Multiprotocol BGP using the Label Distribution Protocol (LDP), the Resource Reservation Protocol (RSPP), the Restriction-based routing LDP (CR-LDP) and the Label Border Router (LSR) distribute the values of these labels to other LSR. In this paper, LDP is used to distribute labels in a network of service providers. Figure 1 shows the operation of MPLS.

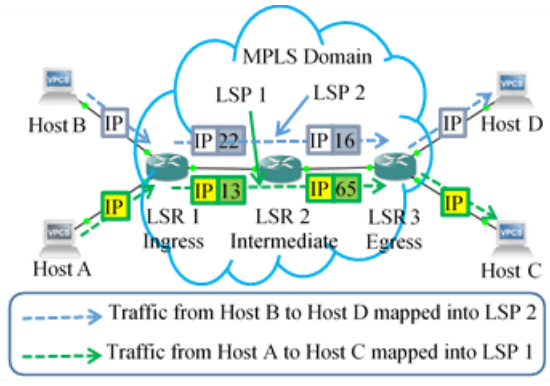

Fig 1:- MPLS Operation [5]

Before a packet enters the MPLS domain network, a label edge router (LER), also known as a label switch router (LSR), classifies IP packets into FEC. The FEC is identified by a fixed short-length value called a label. The Ingress LSR then assigns the MPLS header to the IP packet. Once the MPLS is assigned, the packet is routed through a predetermined Label Switching Path (LSP) through the

ISSN No:-2456-2165

intermediate LSR. Later routers use this label to forward packets. Therefore, subsequent routers do not require packet classification. The FEC table present in the router helps to identify the label of incoming packets. After identifying the package label, replace it with the outgoing label and transfer it to the next LSR. Due to the fixed length of the label, the forwarding operation is much faster than the IP forwarding that matches the longer prefix of the destination IP address. When the packet arrives at the destination router (ie Egress LSR), the label will be removed and forwarded as an IP packet to the destination address. [4].

III. MPLS VPN

Today, most service providers use MPLS VPN as a replacement for Frame Relay and ATM services. In a short period of time, the popularity of MPLS VPN has been very high, because it is cheaper, more flexible, simpler and easier to manage for companies and service providers. There are two types of MPLS VPN, Layer 2 MPLS VPN and Layer 3 MPLS VPN [4].

A. Layer 2 MPLS VPN

Layer 2 VPNs provides a transparent end-to-end layer 2 connection to an enterprise over a Service Provider Network with Customer Sites behaving like they are connected via a Switch. It appears that customer devices are directly connected to each other. Layer 3 neigborship is created between Customer Edge devices. Traffic from Customer Edge is carried over MPLS network and is converted back to Layer 2 format at the receiving site. Different MPLS Layer 2 VPN techniques are including AToM, VPLS and EVPN.

In service provider domain, the Provider Edge (PE) routers use LDP protocol between them to form a Layer 2 connection. Pseudo Wire (PW) or Tunnel is created between PE routers. This PW is used to transfer data between PE routers. Two labels are associated with the data that travels from Customer Edge (CE) routers to PE routers:

- *Tunnel Label*
- *VC Label*

These labels become a form of label stack. In the bottom of the stack, the VC label exists. The Tunnel label always set on the upper of the VC label. To become a path between PE routers and CE routers, a circuit needs to be established with these labels. The circuit is mostly known as Attachment Circuit (AC). By setting the VC label, the routers can determine which frame or data belongs to which circuit. The tunnel label describes the PW which will carry the frame or data. [2]. In this system, point-to-point Layer 2 MPLS VPN (VPWs) is described to analyze MPLS VPN. The operation of Layer 2 MPLS VPN is shown in Fig. 2.

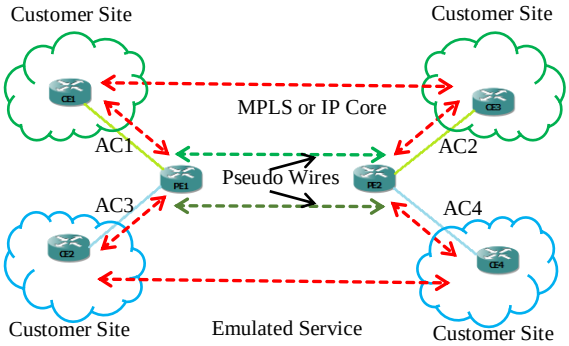

Fig 2:- Layer 2 MPLS VPN [6]

B. Layer 3 MPLS VPN

A layer 3 MPLS VPN is generally referred to as an MPLS VPN. It is a peer-to-peer model that Border Gateway Protocol (BGP) uses to distribute information related to VPN. In the peer-to-peer model, the PE device is a router, PE-router that directly exchanges routing information with the CE router. The service provider's routers becomes the core of the WAN network when MPLS Layer 3 VPN service is used. The companies or customers need to share their internal routing information to their MPLS service providers. It is highly scalable and provide to reduction the operational complexity of the companies or customers. Fig. 3 is the operation of Layer 3 MPLS VPN [4].

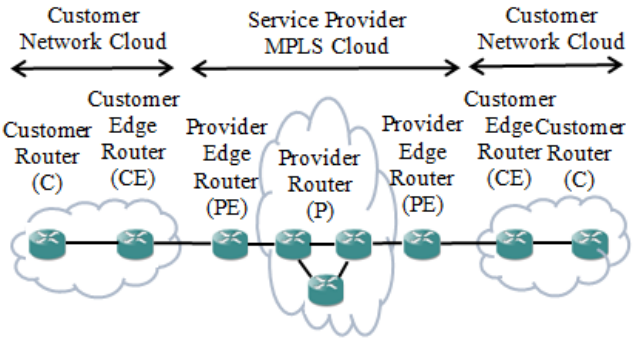

Fig 3:- Layer 3 MPLS VPN

IV. EXPERIMENTAL SETUP

The simulation environment employed in this paper is based on GNS 3.0 simulator. The simulations were setup using a Layer 2 MPLS VPN and a Layer 3 MPLS VPN network are implemented. The results from these simulations are used for comparison between the two networks. Both simulations are based on the common topology as shown in Fig. 4. The devices used in this system are as follows:

- *7 Routers*
- *4 Multilayer Switches*
- *4 Personal Computers (PCs)*
- *10 Fast Ethernet Cables*

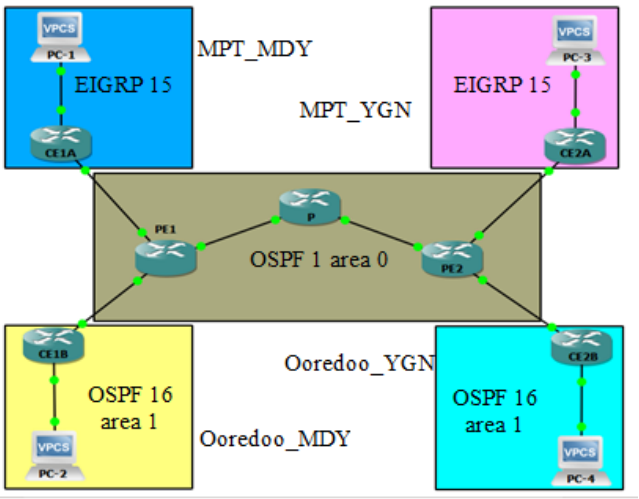

Fig 4:- System Design

In this experimental test, the head office and branches office of two companies which located at Yangon and Mandalay are connected by using MPLS VPN across the service provider network. Each of the simulation are as follow.

A. Configuring Layer 2 MPLS VPN

Fig. 5 shows the detail network design to test for Layer 2 MPLS VPN. Three c7200 routers (P, PE1 and PE2) are service provider routers. And four c3725 multilayer switches (CE1A, CE2A, CE1B and CE2B) are used for customer edge router. In this simulation, only service provider routers are used to configure MPLS features. The network with those three routers is called MPLS backbone. Layer 2 MPLS VPN is configured using Pseudowire (PWs). It is also called Any Transport over MPLS (AToM). This will allow service providers to connect layer 2 networks of customers transparently by using their MPLS backbone. Packets are transferred via PWs from logical interface of one customer site to another site. In this simulation, there are four customer sites to share data from one site to another. The system uses dynamic routing protocols: OSPF for two customer sites and EIGRP for another two sites.

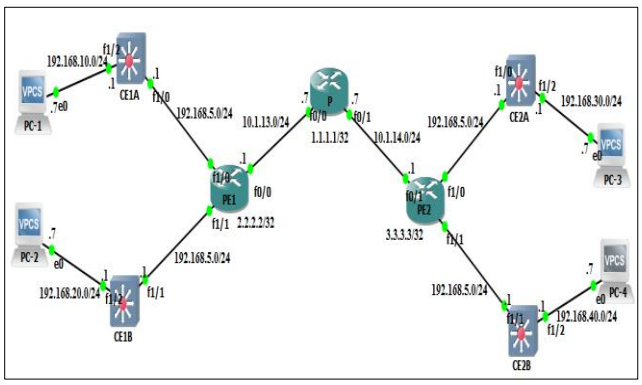

Fig 5:- Design for Layer 2 MPLS VPN

After finishing all the configuration on PE routers and CE switches, the customer site can see to the other customer router as the following.

```
CE1A#sh cdp nei
CE1A#sh cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
CE2A             Fas 1/0           102          S I       3725      Fas 1/0
CE1A#
```

Fig 6:- CDP Neighbor

Fig. 7 shows the ping test result of Layer 2 MPLS VPN on customer sites.

```
CE1A#ping 192.168.5.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 128/210/288 ms
CE1A#
```

Fig 7:- Ping Test from CE1A to CE2A

B. Configuring Layer 3 MPLS VPN

The system uses seven c7200 routers to implement Layer 3 MPLS VPN in GNS3 as shown in Fig. 8. Like Layer 2, the system need to configure MPLS features only on three routers.

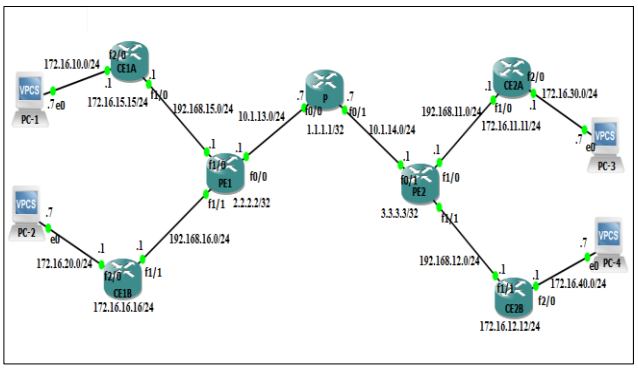

Fig 8:- Design for Layer 3 MPLS VPN

In Layer 3 MPLS VPN simulation, there are four customer sites to share data from one site to another as like in Layer 2 MPLS VPN. The system uses the same routing protocols, OSPF and EIGRP for customer sites. In this Layer 3 MPLS VPN, the ISP is running eBGP between the CE and PE routers to exchange prefixes. And then all internal (P, PE) routers of the ISP is configure iBGP (OSPF), so that PE1 and PE2 are able to reach each other. Some loopback interfaces on the ISP routers that will be advertised as well are added.

LDP is used within the service provider network and then it will use the address as the transport address for the TCP connection. Fig. 9 shows checking the LDP neighbor and Fig. 10 shows MPLS forwarding table on some interfaces of PE1, P, and PE2.

```
P#sh mpls ldp nei | include Peer
P#sh mpls ldp neighbor | include Peer
    Peer LDP Ident: 2.2.2.2:0; Local LDP Ident 1.1.1.1:0
    Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 1.1.1.1:0
P#
```

Fig 9:- LDP Neighbor Table

ISSN No:-2456-2165

```
PE1#sh mpls forwarding-table
Local      Outgoing   Prefix          Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id    Switched      interface
16         Pop Label  1.1.1.1/32      0             Fa0/0      10.1.13.7
17         17         3.3.3.3/32      0             Fa0/0      10.1.13.7
18         Pop Label  10.1.14.0/24    0             Fa0/0      10.1.13.7
PE1#
```

Fig 10:- MPLS Forwarding Table of Layer 3 VPN

Layer 3 MPLS VPN is done by using VRFs. Each VRF has its own Route Distinguisher (RD) unit. The RD is to make sure that all prefixes are unique. The customer prefix + RD together are a VPNv4 route. And then assign the created VRF on the interface. Fig. 11 shows the connection between provider router and customer is done with IPv4 address and each connection is sent with VRF.

```
PE1
PE1#
*Nov 15 15:07:33.347: %SYS-5-CONFIG_I: Configured from console by console
PE1#
PE1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
PE1(config)#router eigrp 1
PE1(config-router)#address-family ipv4 vrf MM
PE1(config-router-af)#network 192.168.15.0 0.0.0.255
PE1(config-router-af)#no auto-summary
PE1(config-router-af)#autonomous-system 15
PE1(config-router-af)#exit-address-family
PE1(config-router)#!
PE1(config-router)#router ospf 16 vrf OM
PE1(config-router)#network 192.168.16.0 0.0.0.255 area 1
PE1(config-router)#!
PE1(config-router)#end
PE1#
```

Fig 11:- Configuration with IPv4 address on VRF

V. OUTPUT OF THE SYSTEM

Performance will be measured using parameters: throughput and end-to-end delay. Throughput is the amount of data moved successfully from one place to another across a network and is typically measured with kilobits per second. Delay (end-to-end) is the amount of time taken by a packet to reach from one destination to another.

In this system, performance can be done by transferring different types of packets and different size of packets from one customer site to another. FTP server is created on one site of customer and stored different types and different size of packets on that FTP server. The other customer site will be client. After approval of connection between two sites, client can get any files stored on that FTP server. The result of throughput and delay by transferring packets from one customer site to another are shown in the following tables. The result is the average value got by transferring packets six times. Table 1 is the average value of throughput and delay measure between customer sites, CE1A to CE2A, with Layer 2 MPLS VPN. Table 2 describes the result from Layer 3 MPLS VPN between the same sites.

File Name	File Size (Bytes)	Throughput (kbps)	Delay (sec)
Mplsvpn.txt	10391	26.74	3.11
Ch3f.docx	105264	140.68	5.99
Project.pkt	637502	218.56	23.34
Smallmario.png	1764904	235.7	59.91
Winrar-x64-560.exe	3180248	241.06	105.54
Mplsguide.pdf	6465096	243.98	212.01
Lovemyself.mp3	10123270	246.68	328.12
Magicshop.mp4	12558379	246.9	406.92

Table 1:- Performance of L2 MPLS VPN from CE1A to CE2A

File Name	File Size (Bytes)	Throughput (kbps)	Delay (sec)
Mplsvpn.txt	10391	453.82	0.36
Ch3f.docx	105264	1531.06	0.55
Project.pkt	637502	4691.58	1.1
Smallmario.png	1764904	4553.68	3.19
Winrar-x64-560.exe	3180248	6012.66	4.24
Mplsguide.pdf	6465096	5982.66	8.65
Lovemyself.mp3	10123270	6258.64	12.94
Magicshop.mp4	12558379	6283.52	15.99

Table 2:- Performance of L3 MPLS VPN From CE1A To CE2A

ISSN No:-2456-2165

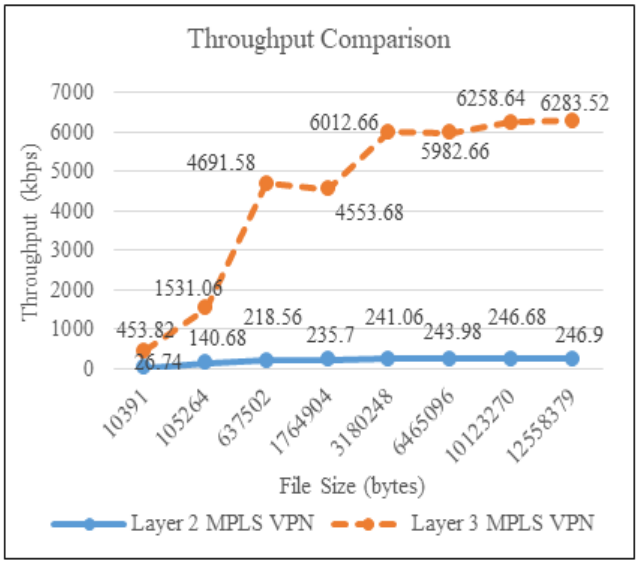

Fig 12:- Throughput Comparison of Layer 2 and Layer 3 MPLS VPN

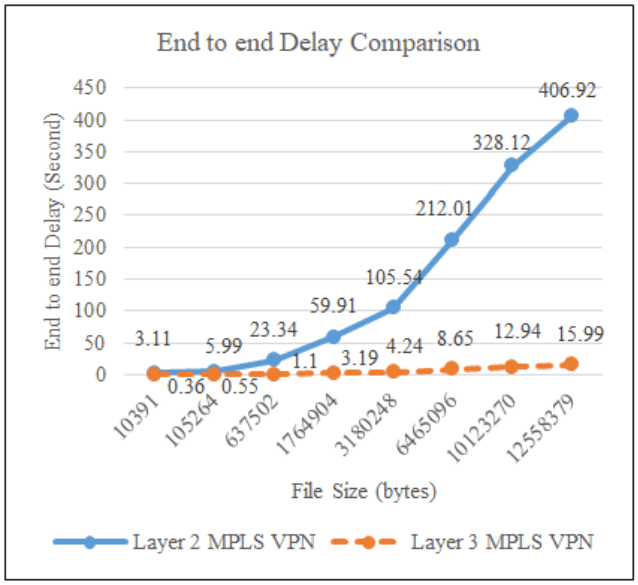

Fig 13:- End to end Delay Comparison of Layer 2 and Layer 3 MPLS VPN

After performance comparison of Layer 2 MPLS VPN and Layer 3 MPLS VPN, throughput result of Layer 3 MPLS VPN is more than 10 times faster than that of Layer 2 MPLS VPN. Moreover, Layer 2 MPLS VPN takes more delay time than Layer 3 MPLS VPN. In general, in this system, the bigger the file size, the faster the throughput is. Moreover, L2 MPLS VPN configured in this system is point-to-point and it can transfer data only one customer site to only one other customer site. So Layer 2 MPLS VPN is not suitable for large networks which demand point to multipoint connections.

VI. CONCLUSION

The system is about how MPLS works on VPNs. Layer 2 MPLS VPN and Layer 3 MPLS VPN are implemented in order to concern about MPLS VPN and its performance. In this paper, performance is analyzed using parameters such as throughput and delay (end-to-end). By comparing performance of Layer 2 and Layer 3 MPLS VPNs in this system, the fact that which MPLS VPN is more suitable to use is known. Layer 2 MPLS VPN is suitable in small networks. Layer 3 MPLS VPN is scalable and it is faster than Layer 2 MPLS VPN. So Layer 3 MPLS VPN is suitable to use in corporate networks.

REFERENCES

[1]. Molenaar R., “Introduction to MPLS”, 2015.
[2]. Press, Cisco, “L2VPN and Carrier Ethernet Concepts”, 2007.
[3]. Guan Chye Tan, “A Performance Analysis of BGP/MPLS VPN Failover Functionality”, 2006.
[4]. Sanjib Gurung, “Implementation of MPLS VPN”.
[5]. http://www.slideshare.net/ameliakot/fyp-presentation-15100528
[6]. http://www.ciscotr.com/l2-transport-ve-l2vpn.ht