RESEARCH ARTICLE OPEN ACCESS

Comparative Analysis of MPLS Layer 3vpn and MPLS Layer 2 VPN

Umar Bashir Sofi [1], Er. Rupinder Kaur Gurm [2]
Department of Computer Science and Engineering [1]
PTU/RIMT Institute of Engineering and Technology
Sirhind Side
Mandi Gobindgarh
Punjab – India

ABSTRACT

MPLS is the prime technology used in Service Provider Networks as fast packet forwarding mechanism. It is the technology used in service Provider networks to connect different remote sites. MPLS can be used to transport any kind of data whether it is layer 2 data such as frame relay, Ethernet, ATM data etc or layer 3 data such as IPV4, IPV6. MPLS creates two type of VPNs. One is Layer 3 MPLS VPN and other one is Layer 2 MPLS VPN. In Layer 3 MPLS VPN, customer forms IP neighbor ship with Service Provider device. In Layer 3 VPN routing is performed between customer edge device and Provider Edge device. Layer 2 VPNs behave like the customer sites are connected using a Layer 2 Switch. Various L2 MPLS VPN techniques are Virtual Private LAN Service (VPLS), Virtual Private Wire Service (VPWS), and Ethernet VPN. This paper gives an overview of all these L2 and L3 MPLS VPN technologies

Keywords:- MPLS, LDP, VRF, RD, RT, VPWS/AToM, VPLS, L3 MPLS VPN

I. INTRODUCTION

MPLS is a packet forwarding mechanism that uses labels to forward packets. Labels are attached to packets and a label mapping is done from one edge router of provider to other edge router of provider. MPLS is used in Service Provider environments. Label Distribution protocols are used for label distribution and exchange of labels from one router to other router. Different Label Distribution Protocols are Label Distribution Protocol (LDP) , Resource Reservation Protocol (RSVP), Multi-protocol BGP(MP-BGP). LDP is the default and most widely used protocol for label distribution. LDP labels can only be assigned to non-BGP routes in Routing Information Base(RIB). MP-BGP is used to distribute label bindings for BGP routes. RSVP is used to distribute labels for TrafficEngineering(TE).

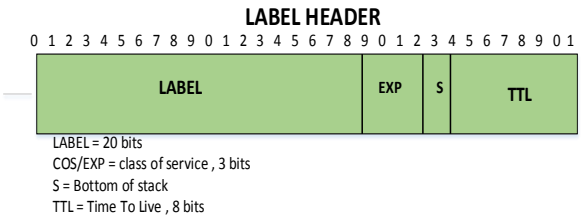

Fig. 1 Label Header

MPLS has the great ability to forward traffic on the basis of labels instead of destination IP address, which helps in elimination of using Border Gateway Protocol (BGP) in the core of Service Provider networks . This is a very big advantage. But the greatest advantage of using MPLS is to create Virtual Private Networks. MPLS has the ability to create both Layer 2 and Layer 3 MPLS VPNs. MPLS also provides many more benefits like Traffic Engineering, use of one unified network infrastructure, optimal traffic flow, better IP over ATM integration. MPLS is the technology used by all Internet Service Providers (ISPs) in their core or backbone networks for packet forwarding .it is still growing with Ethernet VPN paper published in February 2015.

Below is the figure showing Vodafone MPLS Network worldwide :

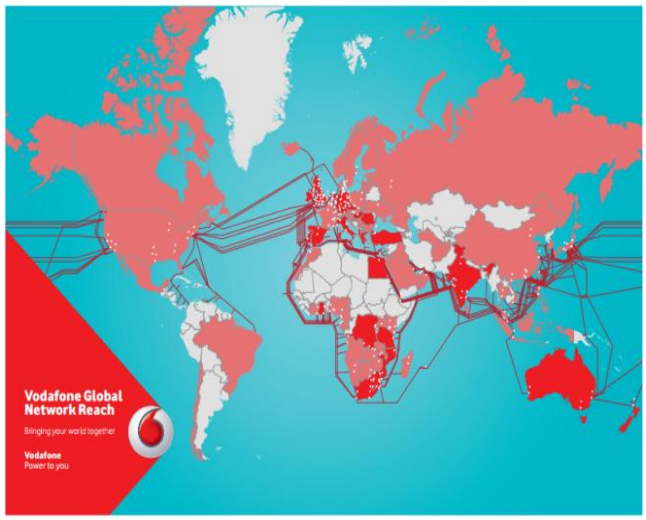

Fig. 2 - Vodafone Global MPLS Network Figure Source - http://globalnetworkmap.vodafone.com/#service-mpls

II. MPLS VPN Types

The greatest advantage of using MPLS is to create Virtual Private Networks (VPNs). MPLS has the ability to create both Layer 2 and Layer 3 MPLS VPNs. Both type of VPNs have their own merits and demerits.

A. MPLS Layer 3 VPN

MPLS Layer 3 VPN creates a peer-to-peer VPN with customer sites. It forms Layer 3 neighborship with service provider routers. Labels are added to customer IP routes when they enter from Customer Edge(CE) routers to Provider Edge(PE) routers. All forwarding is done using label switching with MPLS within service provider network and labels are removed when sending traffic from Provider Edge to Customer Edge routers. Some terms used in MPLS are listed below:

1) ***Label***
It is a 4 byte identifier which is attached to each packet when it enters the MPLS network. It is used by MPLS networks for label switching purposes. It is on the basis of this attached label that data is delivered from one provider router to another provider router.

2) ***LSR***
LSR stands for Label Switch Router. It is any router on which MPLS is running and is in use for label switching.

3) ***PE Router***
Provider Edge Router is an edge router in Provider network. It is a device where label is imposed and removed.

4) ***P Router***
Provider Router sometime is also called Core Router in Service Provider Networks. It is not an edge device. It is a router where Bgp is not running.

5) ***CE Router***
It stands for Customer Edge Router. It is an edge router in the customer site which is connected with the Provider Edge MPLS device.

6) ***Ingress PE Router***
It is an edge-LSR where the label is imposed to the packet coming from Customer Edge router to Provider Edge Router.

7) ***Egress PE Router***
It is the edge-LSR where the destination customer site is connected. This device receives labeled packets and disposes the labels attached to packets and forwards simple IP packets to customer.

8) ***VRF***
Virtual Routing and Forwarding (VRF) is used in Layer 3 MPLS VPNs which adds the capability in Service Provider Edge routers to have multiple routing tables with one routing table per customer and a global routing table. As every instance of routing table is different from other customers routing table, it provides an isolation between all the customers traffic on the same router even using the same IP address space. Each VRF instance creates a separate RIB(Routing Information Base), FIB(Forwarding Information Base), LFIB(Label Forwarding Information Base) table.

9) ***RD***
Route Distinguisher is a 64 bit value attached to client's IP address with VRF which uniquely identifies a route and produces a unique 96 bit VPNv4 address. VPN routes are transported over MPLS backbone with MP-BGP that needs transported routes to be unique.

10) ***RT***
Route-Target (RT) is a 64-bit extended BGP community attached to VPNv4 routes to indicate import and export routes. RTs can either be imported or exported.
Import RTs are used to select VPNv4 routes for insertion into matching VRF tables.
Export RTs are attached to a route when it is sent into VPNv4 routing table towards other end of the customer or its destination. It is used to identify VPN membership of routes. Figure below shows Route Propagation in Layer 3 MPLS VPN.

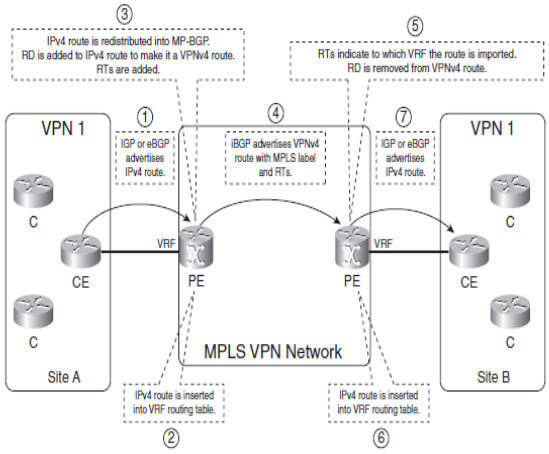

Fig. 3 Route Propagation in L3 MPLS VPN

B. MPLS Layer 2 VPN

1) Virtual Private Wire Service (VPWS) / Any transport over MPLS (AToM)

AToM is Cisco's implementation of VPWS in MPLS networks that provides Point-to-Point tunnel service from PE to PE. Two types of pseudowire technologies are used in VPWS, one is AToM, which targets MPLS networks and another is L2TPv3, which is a pseudowire technology for native IP networks. Both AToM and L2TPv3 supports the transport of ATM, HDLC, Frame-Relay and Ethernet traffic over an IP/MPLS network.

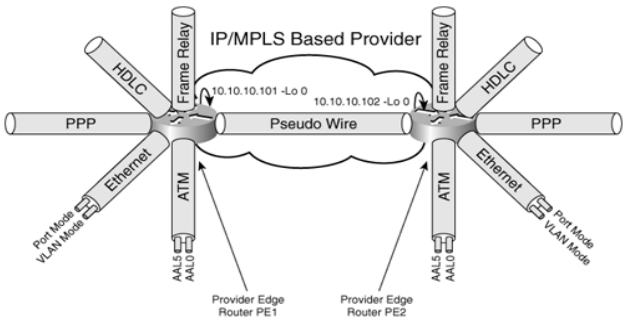

Fig. 4 Basic AToM Model

PE routers run LDP protocol between them in an AToM implementation of Layer 2 technology. Pseudowire or Tunnel is created between PE routers . This pseudowire is used to transfer data between provider edge routers. Two labels are associated with the data that travels from customer edge devices to provider edge device:

- Tunnel Label
- VC Label

The set of labels form the label stack. VC label is always the bottom label and Tunnel label is the top label in the label stack. The connection between PE router and the customer edge router is called Attachment Circuit (AC). VC label identifies to which attachment circuit the frame or data belongs. VC label identifies the remote customer to to which data has been sent. The Tunnel label identifies the pseudowire though data travels.

2) Virtual Private LAN Service (VPLS)

VPLS uses point-to-multipoint Ethernet based VPN that connects multiple customer sites over MAN or WAN. VPLS is designed for application that needs multipoint access. Service Provider network behaves like a switch with VPLS. VPLS can use either physical port or a pseudowire port. MAC addresses are learned dynamically when packets arrive at VPLS PE router just as in traditional Layer 2 Switching. Split horizon is used as a loop prevention mechanism. Layer 2 protocol tunneling is used to send Layer 2 protocols like CDP, STP, or VTP over a pseudowire.

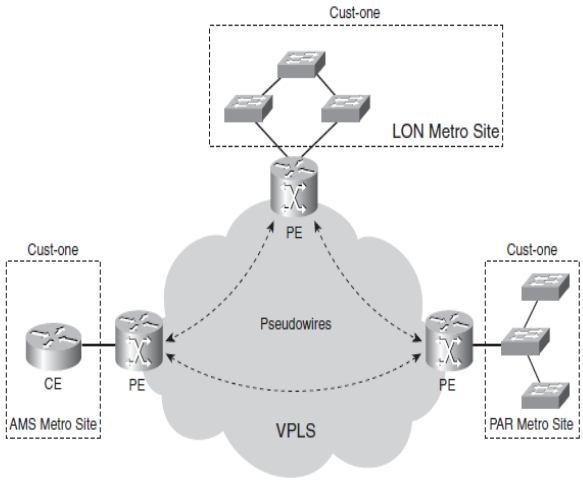

Fig. 5 VPLS Model

VPLS just like AToM maintains two labels viz VC Label and Tunnel Label for forwarding data across the MPLS backbone. VC Label identifies the attachment circuit i.e the customer to which data has been sent. Tunnel Label is the top label and is used to find how frame moves from ingress router to egress router.

III. BRIEF LITERATURE SURVEY

In May 2014[] Ezeh. G.N, Onyeakusi C.E, Adimonyemma T.M and Diala U.H. of Federal University of Technology carried out the Comparative Performance Evaluation of Multimedia Traffic over Multiprotocol Label Switching using VPN and traditional IP networks. Comparison is made on the basis(bits/seconds),end-to-enddelay(seconds)and utilization(tasks/sec).In this paper, results are analyzed and it shows that MPLS provides better performance in implementing the VoIP application.

In 2013[4] S.Venkata Raju, P.Premchand, A.Govardhan evaluated the Routing Performance in Wide Area Networks using mpls , shows best performance of mpls in terms of throughput and end to end delay.

In 2011 Dr. Irfan Zafar and Faiz Ahmad carried out the analysis of Traffic engineering parameters using MPLS and Traditional IP Networks. They found MPLS is far better than traditional networks.

In 2011 Dr. Irfan Zafar and Faiz Ahmad carried out the analysis of Traffic engineering parameters using MPLS and Traditional IP Networks. They found MPLS is far better than traditional networks.

E. Rosen (2001) [4] describes Multiprotocol Label Switching Architecture of Cisco Systems, A. Viswanathan of Force10 Networks, and R. Callon [4] of Juniper Networks in Internet Engineering Task Force (IETF) RFC - 3031 specifies the architecture of Multiprotocol Label Switching(MPLS). It is the first standard document of Multiprotocol Label Switching by IETF MPLS Working Group. MPLS is described here as a technique that uses label switching at every hop or router to transfer datagrams between source and destination.

L. Andersson et. al. (2006) [5] describes framework for Layer 2 Virtual Private Networks (L2VPNs) Of Cisco Systems..This framework is intended to aid in standardizing protocols and mechanisms to support interoperable L2VPNs. This model also is a standard document for Virtual Private Wire Service (VPWS) and Virtual Private LAN Service (VPLS). With VPWS, a point-to-point connection can be made between different customer sites over service provider MPLS network and any type of datagram can be transported like Frame Relay, ATM, Ethernet, PPP etc. VPLS offers point-to-point and point-to-multipoint services. With Layer 2 VPN connections, neigborship between routing protocols are Customer Edge sites is done directly with Customer Edge sites at other end. All the customer sites of a single customer behaves like they are connected via a Layer 2 Switch.

L. Martini (2006) [6] describes pseudo wire Setup and Maintenance Using the Label Distribution Protocol (LDP) of Cisco Systems, N. El-Aawar of Level 3 Communications, T. Smith of Network Appliance and G. Heron [6] of Tellabs describes how layer 2 services like Frame Relay, Asynchronous Transfer Mode, and Ethernet can be emulated over a MPLS backbone by encapsulating the Layer 2 protocol units (PDU) and transmitting them over "pseudo wires". This document specifies a protocol for establishing and maintaining the pseudo wires, using extensions to LDP.

L. Martini (2006) [7] describes encapsulation Methods for Transport of Ethernet over MPLS Networks, Ed., E. Rosen [7] of Cisco Systems, N. El-Aawar [7] of Level 3 Communications and G. Heron of Tellabs describes an Ethernet pseudo wire(PW) is used to carry Ethernet/802.3 protocol data units(PDUs) over an MPLS network. Ethernet traffic can be transported over service provider MPLS network with VPWS or VPLS by creating a pseudowire between one provider edge to other provider edge.

K. Komepella (2007) [8] describes virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling, Ed. And Y. Rekhter [8], Ed of Juniper Networks describes BGP Auto Discovery and Signaling method for VPLS. It specifies a mechanism for signaling a VPLS, and rules for forwarding VPLS frames across a packet switched network.

M. Lasserre et. al. (2007) [9] describes virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling of Alcatel Lucent [9] in IETF RFC 4762 describes a Virtual Private LAN Service (VPLS) solution using pseudo wires, a service previously implemented over other tunneling technologies and known as Transparent LAN Services (TLS). A VPLS creates an emulated LAN segment for a given set of users; i.e., it creates a Layer 2 broadcast domain that is fully capable of learning and forwarding on Ethernet MAC addresses and that is closed to a given set of users. Multiple VPLS services can be supported from a single Provider Edge (PE) node.

N. Bitar (2014) [10] describes requirements for Ethernet VPN(EVPN) of Verizon, A. Sajassi [10] of Cisco Systems, R. Aggarwal [10] of Arktan, W. Henderickx [10] of Alcatel-Lucent, Aldrin Issac [10] of Bloomberg, J. Uttaro [10] of AT&T.

Grenville Armitage et. al. (2000) [11] describes MPLS: The Magic Behind the Myths [9] reviews the key differences between traditional IP Routing and the emerging MPLS approach, and identifies where MPLS adds value to IP networking.

IV. OBJECTIVES

The major objectives of thesis could be summarized as below:

1) To evaluate the Performance of MPLS layer 2 VPN and MPLS layer 3 VPN based on the parameters such as convergence time , delay and scalability. The performance of these two technologies will be checked with topologies of different sizes.

2) Security analysis will be performed on both MPLS Layer 3 VPNs and MPLS Layer 2 VPNs. It will be analyzed which one is easily vulnerable to attacks and study will be carried out on how to prevent such attacks.

3) Business evaluation is also done as of which one of the services returns more on investment. It will be done both on ISP and customer basis.

V. METHODOLOGY

This research work is proposed to be completed in various stages as described below:

1) The 1st step will be to study various Layer 2 and Layer 3 MPLS Standard documents which are used by different vendors while developing their devices and network operating systems.

2) The 2nd step will be to Implement Layer 2 and Layer 3 MPLS VPN technologies in simulation environment, and draw conclusions based on the various parameters.

3) The 3rd step will be to Implement Layer 2 and Layer 3 MPLS VPN on Real Cisco Devices and a conclusion will be drawn from the output.

4) In 4th step deep packet comparison will be made by comparing the headers of all the Layer 3 and Layer 2 MPLS protocols using Wireshark Traffic Analyzer.

5) In 5thstep,for monitoring purposes, Simple Network Management Protocol(SNMP) will be used between Network Monitoring Tool and Routers/Switches.

6) Finally monitoring tool like Paessler Router Traffic Grapher(PRTG) will be used to draw output graphs that will help us comparing different outputs.

VI. RESULTS AND DISCUSSIONS

Comparative Performance Analysis of MPLS Layer 3 and Layer 2 VPN based on parameters such as Convergence Time , with different topologies has been done in this Chapter.

A. Performance Analysis Of MPLS Layer 3 VPN

For performance analysis, convergence time is used to check, how much time MPLS layer 3 VPN takes when primary link in MPLS backbone network goes down, Topology used is shown below in figure

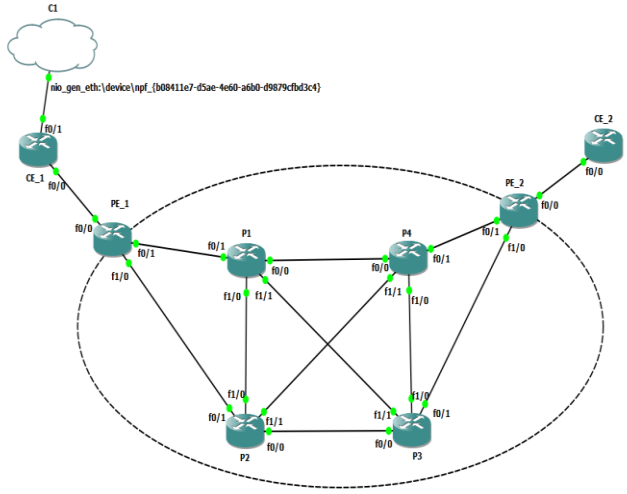

Fig. 6 MPLS L3 VPN topology used in Thesis

Clearly from the topology shown above, it is shown that CE_1 is a customer of Internet Service Provider ABC, Customer 1 has a site at distant location that is connected with the help of MPLS Layer 3 based VPN. Customer , when transfers data, voice or video traffic from CE_1 to CE_2, has two paths in the core network of Internet Service Provider ABC via P1 and P2. Traffic mainly moves towards P1 which is acting as a primary path and P2 is in use only when P1 goes down. When P1 goes down, convergence time taken with default timers by MPLS L3 VPN is shown in the graph below :

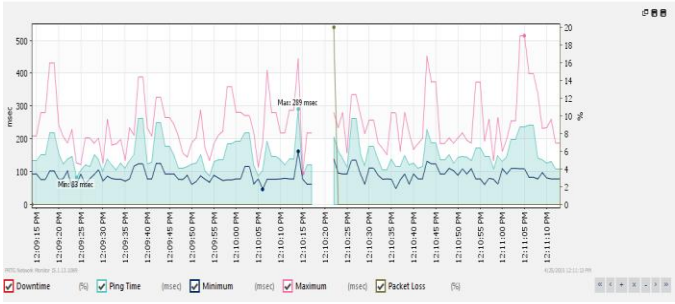

Fig.7 MPLS L3VPN Convergence Time Graph taken from PRTG

Now as we see the graph in Figure 7, it shows that there is a delay of around 5 seconds when traffic from primary link shifts to backup link in case of primary link failure in the MPLS Backbone network. Five seconds is a large amount of time when we talk about network convergence in today's world where Voice and Video based traffic is a kind of necessity with Video Conferencing solutions, Voice Mails, voice messaging solutions etc.

We can use various methods to fasten the convergence time with Bidirectional Forwarding Detection or by decreasing the Interior Gateway Protocol timers. IGPs used in Service provider network can be either be Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS), as only Link State routing protocols are preferred in Internet Service Provider (ISP). Both these protocols use Dijkstra Shortest Path First Algorithm(SPF). We can shorten the timers between SPF calculations or other IGP timers to reduce the convergence time. How this will help is whenever a primary link goes down, SPF calculations can be done for backup link in much faster time than by using default timers. After changing the default hello timer and dead timer interval in OSPF which is used as IGP inside the ISP network for internal routing, the results that i got are shown below in a graph taken with the help of PRTF Traffic Analyzer :

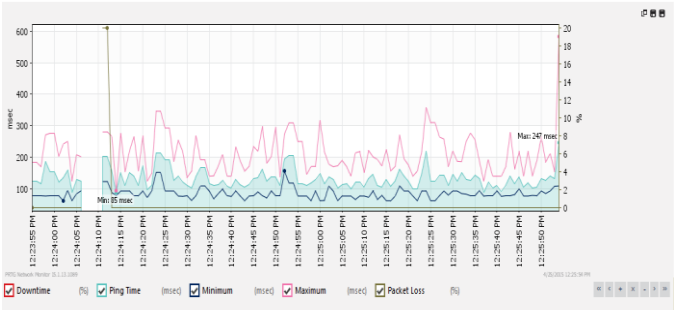

Fig.8 MPLS Layer 3 Convergence Graph with OSPF Timers Tuned.

In the above graph, the result shows that there is not much difference that can be made by tuning Hello or Dead Timers of IGP that can be used inside an ISP internal network. Now let's try to change the SPF calculation timers inside an ISP network. We will reduce the timers of SPF calculations that can be done in the case of some link failure so that backup path SPF calculation can be done in much fast manner. One PE is connected with other PE using an IGP protocol, so it will definitely make a difference in our MPLS network. Graph below shows the convergence time between Primary Link

failure and traffic shifting from primary link towards backup link.

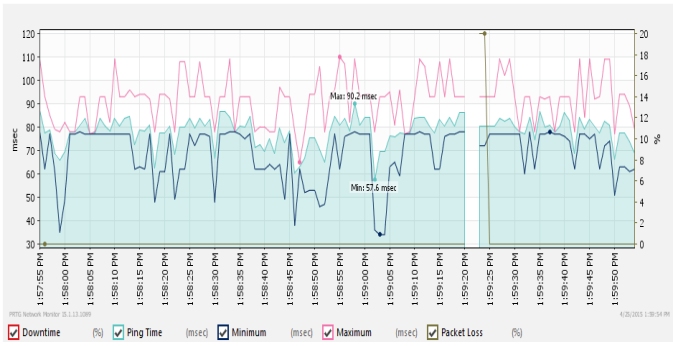

Fig. 9 MPLS Layer 3 VPN convergence graph with OSPF SPF Calculation Timers tuned

As we can see, convergence time is reduced from 5-5.5 seconds to 2.5 - 3 seconds which is much better than the normal results.

B. Performance Analysis Of MPLS Layer 2 VPN

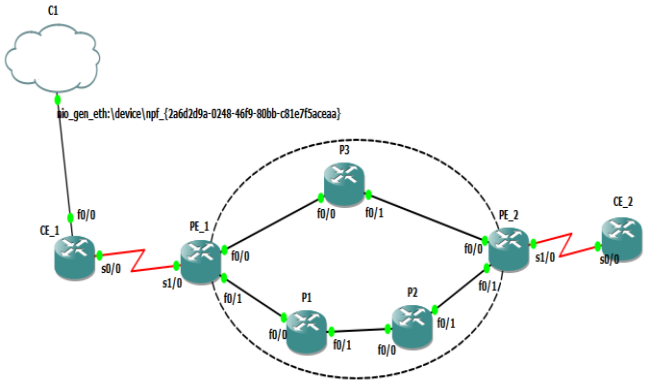

Fig. 10 MPLS Layer 2 (PPP over MPLS) Topology

In MPLS Layer 2 VPN topology used above, we have two customer sites at CE-1 and CE-2 at distant locations connected using MPLS L2 VPN technology. CEs at both end are connected with Provider Edge routers using serial links running Point-to-Point protocol(PPP). PPP has an advantage over other Layer 2 encapsulation methods like HDLC as PPP can be used in multi-vendor deployments. For example, if CE is using Juniper device and PE with which it is connected is using Cisco device, then HDLC cannot work as HDLC only works at Cisco Devices, therefore PPP can always be a better option, also PPP provides other features like Authentication with methods like Password Authentication Protocol(PAP) and Challenge Handshake Authentication Protocol(CHAP). Also it provides features like PPP Multilink, with which multiple physical links can be integrated to form a single Logical link. In the topology used for PPP over MPLS or Any Transport Over MPLS, CE_1 is connected with PE_1 and CE_2 is connected with PE_2, PE_1 has two paths to reach PE_2, one via P3 and other one via P1 and P2, the link via P3 is the link via P3 is the primary link and the link via P1 and P2 is the backup link.

As PPP is a Layer 2 technology, I have used PPP in my thesis work for Layer 2 connectivity. What I have done is, when the traffic was flowing from CE_1 to CE_2 via PE_1 to P3 to PE_2 link, then I intentionally terminated the link between PE1 and P3, so that I can calculate the convergence time that happens between Primary to backup link failure. Result that I got after termination of primary link is way better than MPLS layer 3 VPN results, the graph shows that MPLS Layer 2 VPN with PPP used between CE and PE has a sub-second convergence in case of primary link failure and time taken in shifting traffic from Primary to backup link is very small. Below is the graph showing Convergence time, minimum time for a ping reply and maximum time for a ping reply :

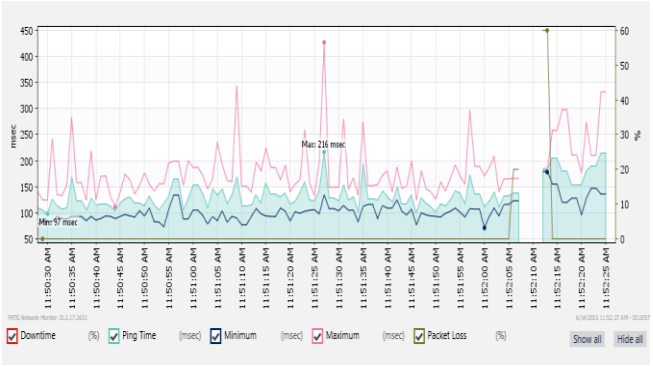

Fig.11 Layer 2 Graph showing convergence, minimum and maximum times

Table 1

PPP over MPLS	Minimum Time	Maximum Time	Convergence Time
	97 msec	216 msec	4-4.5 sec

As shown above in the graph and table 1, for MPLS Layer 2 VPN with PPP used between Customer Edge and Provider Edge devices with default parameters ,the minimum time is 97 msec and the maximum time is 216 msec , while the convergence time between primary to backup link is 4-4.5 seconds. This convergence time can further be decreased by using SPF calculation between the Service Provider Interior Gateway Routing Protocol. Below is the graph and table which is created after tuning the SPF calculation.

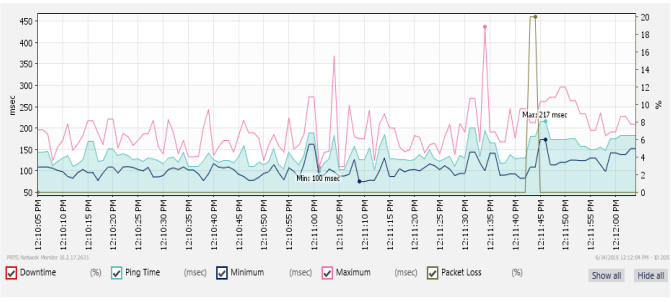

Fig.12 MPLS L2VPN convergence graph after tuning SPF calculation timers

TABLE 2

PPP over MPLS	Minimum Time	Maximum Time	Convergence Time
	100 msec	**217 msec**	**Sub-Second**

VII. CONCLUSION

MPLS is a label switching technology used mainly in Internet Service Provider(ISP) for label switching and VPN purposes. MPLS provides great performance with its label switching method. It also has the ability to create VPNs at both Layer 2 and Layer 3. In Layer 3 MPLS VPN, CE shares the routing table information with the PE router, while in Layer 2 MPLS VPN, ISP acts like a Layer 2 Switch and is used just to forward the packets from one CE to other. By default Layer 3 MPLS VPN has a convergence time of 5-5.5 seconds, which can e reduced to 2.5 to 3 seconds when we fasten the SPF calculation of Link State IGP used in the core of ISP. Layer 2 MPLS VPN provides the convergence time of 4-4.5 seconds , which can be reduced to sub-second after tuning SPF calculation of Link State IGP used in the core of the ISP. So, the end result is that performance of Layer 2 MPLS VPN is much better when compared to Layer 3 MPLS VPN.

ACKNOWLEDGMENT

This paper has been made possible through the constant encouragement and help from my parents and guide. I would like to thank Assistant Prof. Er. Rupinder Kaur Gurm, , for her generous guidance, help and useful suggestions.

REFERENCES

[1] Ciscopress MPLS and Next Generation Networks,"Foundations for NGN and EnterpriseVirtualization",http://ptgmedia.pearsoncmg.com/images/chap3_9781587201202/elementLinks/md100302.gif" ISBN-10:1-58720-120-8

[2] Comparative Performance Evaluation of Multimedia Traffic over Multiprotocol Label Switching using VPN and traditional IP networks by Ezeh. G.N, Onyeakusi C.E, Adimonyemma T.M and Diala U.H. of Federal University of Technology, Owerri, Nigeria in April, 2014 under IJETR – ISSN(E):2347-5900 ISSN(P): 2347-6079

[3] Rosen, Eric, Arun Viswanathan, and Ross Callon. "Multiprotocol label switching architecture." (2001).

[4] Andersson, Loa, and E. Rosen. Framework for layer 2 virtual private networks (L2VPNs). RFC 4664, September, 2006.

[5] Martini, Luca. "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)." (2006).

[6] Martini, Luca, et al. "Encapsulation methods for transport of Ethernet over MPLS networks." RFC4448, April (2006).

[7] Kompella, Kireeti, and Yakov Rekhter. "Virtual private LAN service (VPLS) using BGP for auto-discovery and signaling." (2007).

[8] Lasserre, Marc, and Vach Kompella. Virtual private LAN service (VPLS) using label distribution protocol (LDP) signaling. RFC 4762, January, 2007.

[9] Isaac, Aldrin, et al. "Requirements for Ethernet VPN (EVPN)." (2014).

[10] Armitage, Grenville. "MPLS: the magic behind the myths [multiprotocol label switching]." Communications Magazine, IEEE 38.1 (2000): 124-131.

[11] Cisco press MPLS Configuration on Cisco IOS Software http://flylib.com/books/2/686/1/html/2/images/1587051990/graphics/11fig01.gif

[12] Press, Cisco. "MPLS fundamentals." Page 438, (2007).

[13] Cisco," ASR 9000 Series L2VPN and Ethernet Services Configuration Guide",http://www.cisco.com/c/dam/en/us/td/i/300001400000/360001370000/361000362000/361074.eps/_jcr_content/renditions/361074.jpg

[14] Sajassi, Ali, et al. "BGP MPLS Based Ethernet VPN." (2011).

[15] Press, Cisco. "MPLS fundamentals." (2007).

[16] Luo, Wei, et al. Layer 2 VPN architectures. Pearson Education, 2004.

[17] Darukhanawalla, Nash, et al. Interconnecting data centers using VPLS. Cisco Press, 2009.

[18] Zhang, Lixia, et al. "Resource Reservation protocol (RSVP)--version 1 functional specification." Resource (1997).

[19] Press, Cisco. "MPLS fundamentals." (2007).