ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 3; Issue 4; July-August-2015; Page No. 124-137

COMPARATIVE ANALYSIS OF MPLS LAYER 3 VPN AND LAYER 2 VPN

Umar Bashir Sofi[1], Er. Rupinder Kaur Gurm[2]

[1]Research Scholar, Department of CSE RIMT- IET, Punjab Technical University, Jalandhar India

umarbashir99@gmail.com

[2] Assistant Professor, Department of CSE RIMT- IET, Punjab Technical University, Jalandhar India

rupindergurm@gmail.com

Abstract

MPLS is the prime technology used in Service Provider Networks. It is used 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 types 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 occurs between customer edge device and Provider Edge device. Layer 2 VPNs behave like the customer sites are directly connected Layer 2 Switch between them. This paper gives an overview of all these L2 and L3 MPLS VPN technologies.

Key Words: MPLS, LDP VRF, RT, RD, Layer 2 MPLS VPN, Layer 3 MPLS VPN

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. MP-BGP is used to distribute label bindings for BGP routes. RSVP is used to distribute labels for Traffic Engineering (TE)

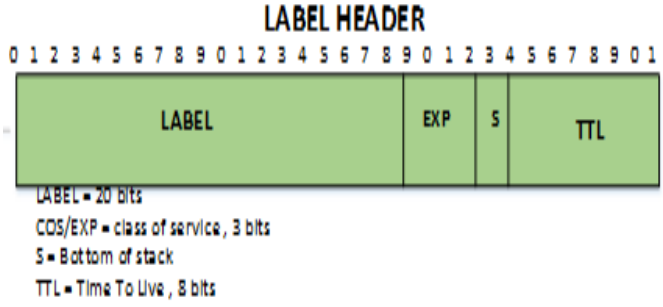

Figure 1 Label Header

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.

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 types 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 neighbor ship 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.

Corresponding author: Umar Bashir Sofi

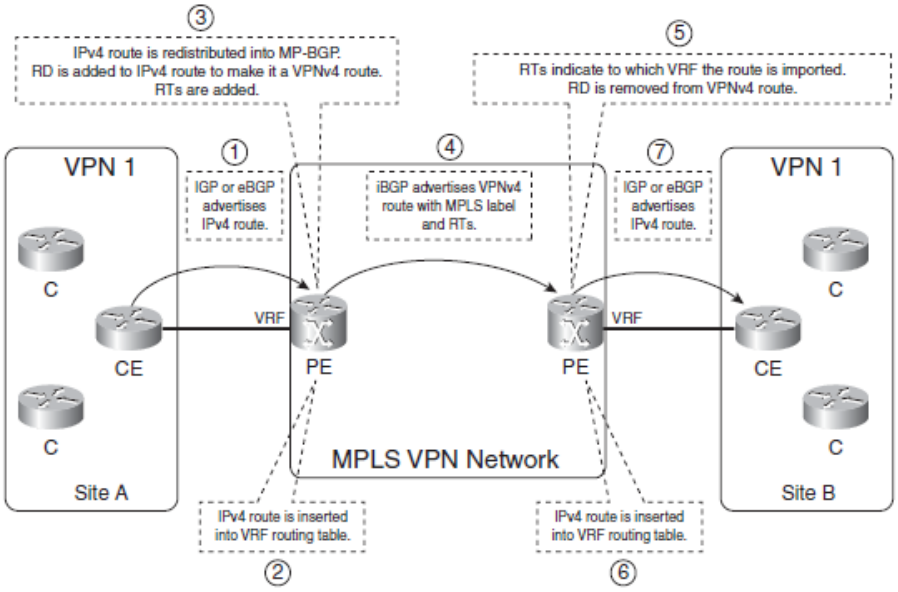

Figure 2: Route Propagation in L3 MPLS VPN

B. MPLS Layer 2 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.

PE routers run LDP protocol between them in an Layer 2 implementation. Pseudo wire or Tunnel is created between PE routers. This pseudo wire 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 pseudo wire though data travels.

1. 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-end delay (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.

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.

2. 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.

3. 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 Wire shark 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.

4. RESULTS AND DISCUSSIONS

Comparative Performance Analysis of MPLS Layer 3 and Layer 2 VPN based on parameters such as Convergence Time, Scalability and security Analysis 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 3:

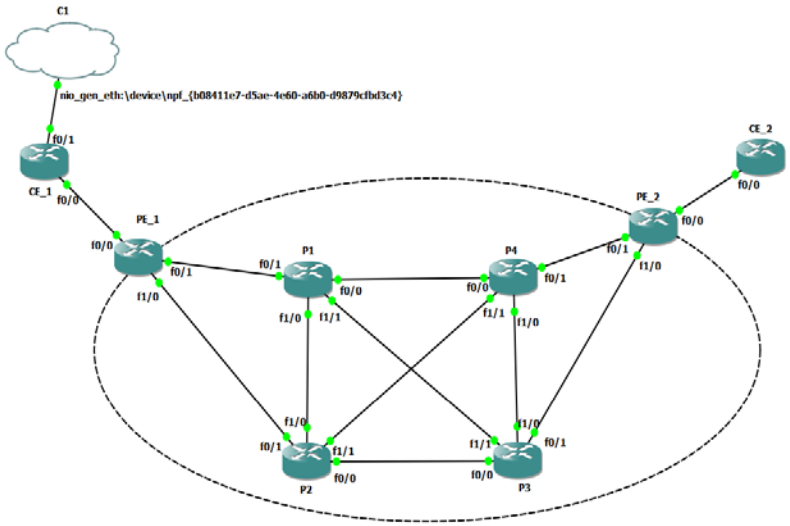

Figure: 3 MPLS L3 VPN topology

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:

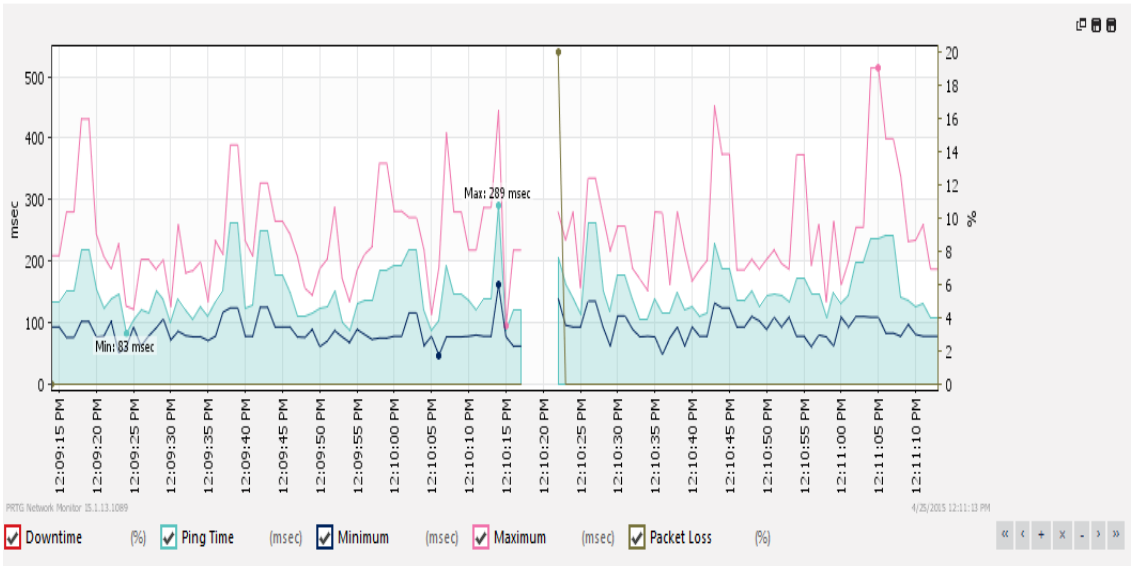

Figure 4: MPLS L3VPN Convergence Time Graph

Now as we see the graph in Fig 4, 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. Now after changing the SPF calculation timers inside an ISP network, it was possible to 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.

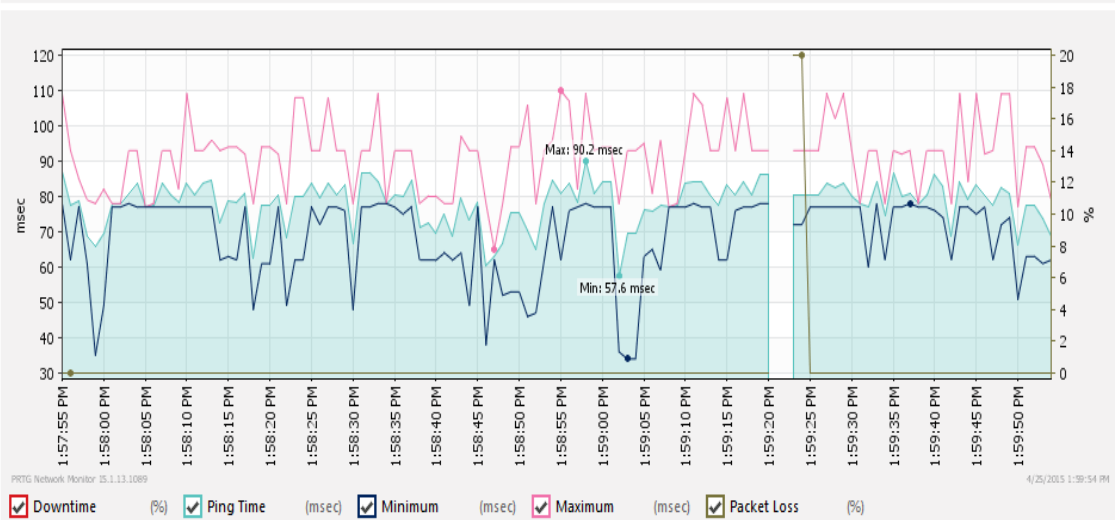

Figure 5 MPLS Layer 3 VPN convergence graph with OSPF SPF Calculation Timers tuned

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

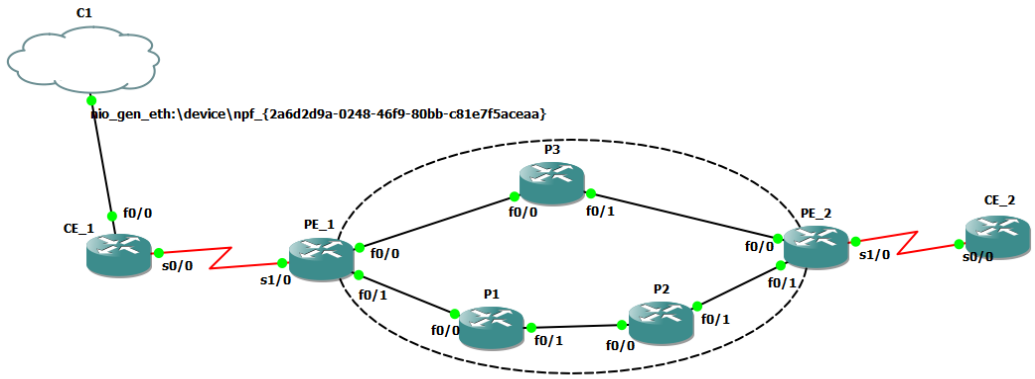

Figure 6 MPLS Layer 2 VPN (PPP over MPLS) Topology

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). 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 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, below is the graph showing Convergence time, minimum time for a ping reply and maximum time for a ping reply:

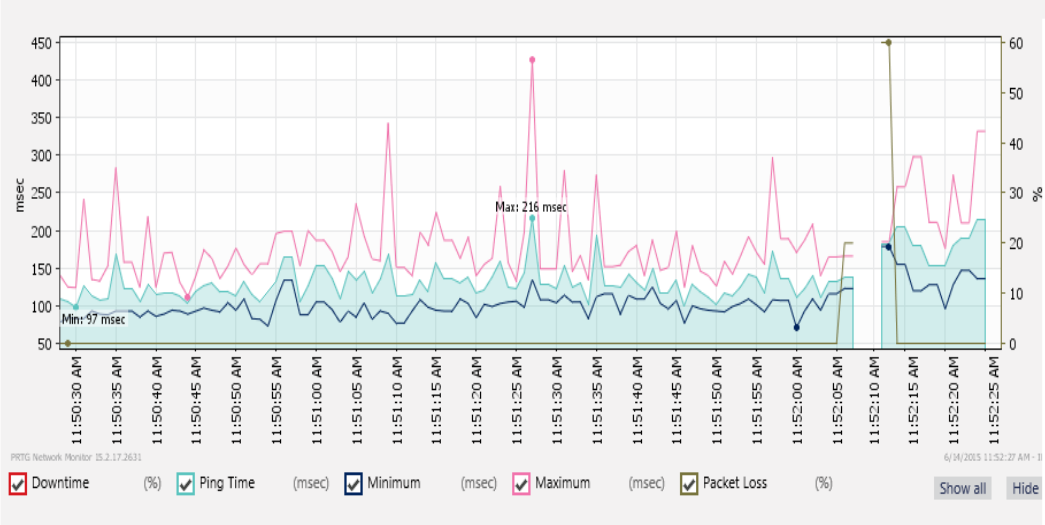

Figure 7 Layer 2 Graph showing convergence, minimum and maximum times

As shown above in the graph , 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 which is created after tuning the SPF calculation.

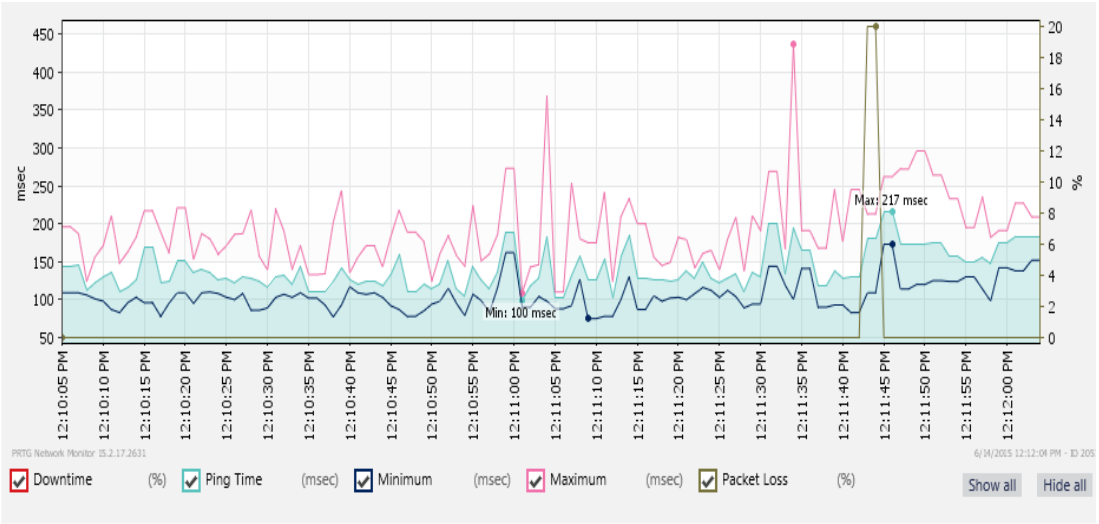

Figure 8 MPLS L2VPN convergence graph after tuning SPF calculation timers

Ethernet is the most popular Layer 2 technology and the most used Layer 2 technology in the world. When we use Layer 2 VPNs, most of the companies prefer using Ethernet over all other technologies as Ethernet is simple in implementation and to manage. I have used above topology for my Layer 2 VPN with Ethernet connecting customer edge with provider edge device.

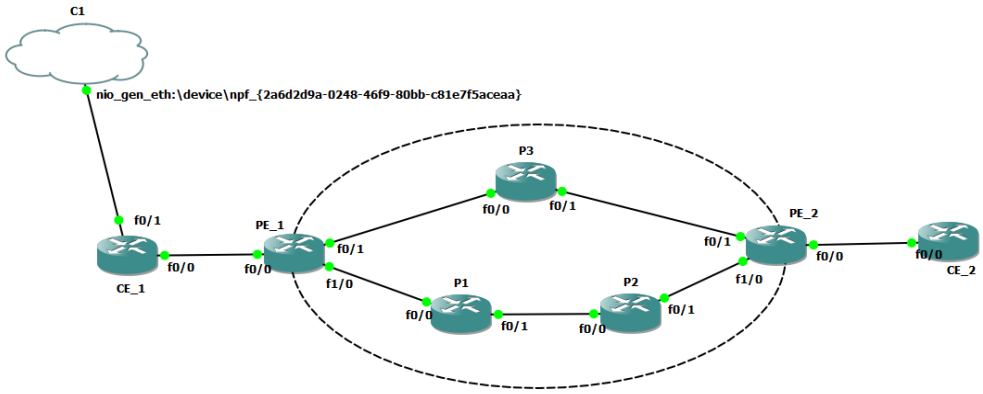

Figure 9 MPLS Layer 2 VPN (Ethernet over MPLS) Topology

Results for convergence time that I got are shown in the graph below:

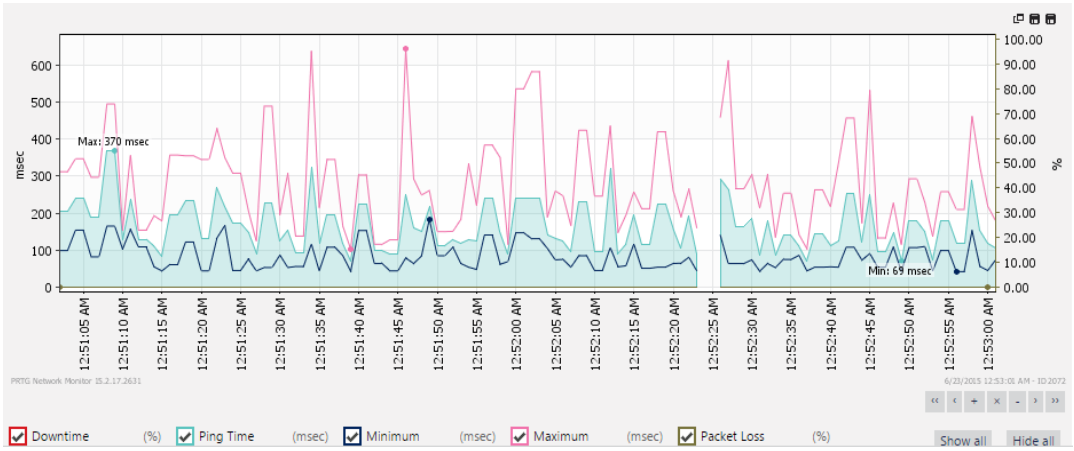

Figure 10 Layer 2 Graph showing convergence, minimum and maximum times

Above graph taken via PRTG shows the minimum and maximum time taken and also the convergence time in shifting the traffic from primary to backup link when link link fails. I also added the load on the link by playing the movie from CE_1 and the movie was located at CE_2, so that we can check if the delay can effect the movie streaming. Result shows that by default without any throttling, convergence time is around 2-2.5 seconds, which is not too much, but if we are using some UDP based connection like VoIP, then 2-2.5 seconds is a large number.
To reduce this convergence time, I throttled the SPF timers, and the result is:

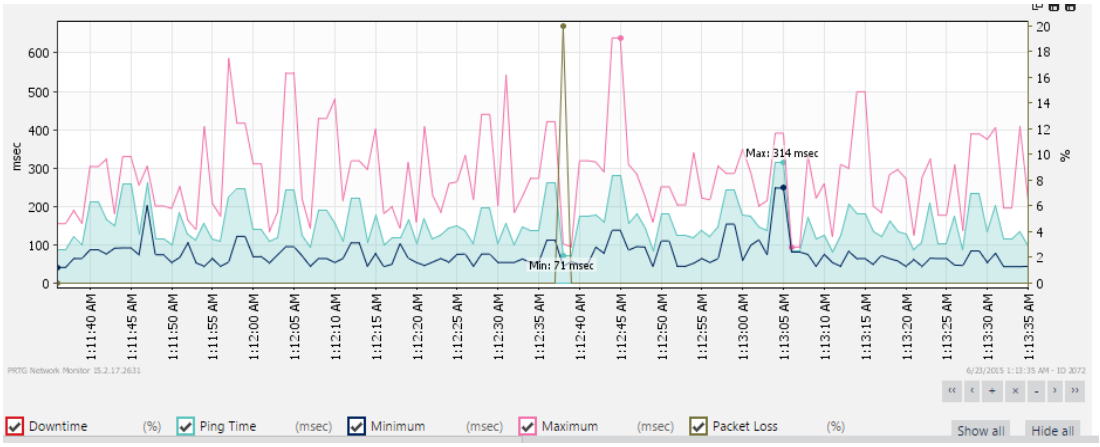

Figure 11 MPLS L2VPN convergence graph after tuning SPF calculation timers

Table below shows the summary for Default Convergence Time and Reduced Convergence Time in MPLS Layer 3 VPN and MPLS Layer 2 VPN.

Table 1: summary of default and reduced convergence time of MPLS L2 and L3 VPNs

MPLS VPN TYPE	Default Convergence Time	Reduced Convergence Time
Layer 3 VPN	5 – 5.5 seconds	2.5 – 3 seconds
Layer 2 VPN with ppp	4 – 4.5 seconds	Sub second
Layer 2 VPN with Ethernet	2 – 2.5 seconds	Sub second

C. Security Analysis of MPLS Layer 3 VPN

Security in MPLS can be achieved by using various methods. Security is important in MPLS networks. All the traffic like Voice, Data and Video traffic that transits from ISP for customer networks needs to be secure, as an insecure ISP network means Customer data will be insecure.

AUTHENTICATION

It means to check the legitimacy of source and destination of packets. We have to make sure that data or an update comes from legitimate source and also we need to prevent service provider devices to receive fraudulent data or route updates. MPLS networks can be made secure by using authentication feature between Label Distribution Protocol (LDP). It means MPLS neighbor ship can only be made if the passwords on the both ends of the neighbors match. This authentication ensures that a router receives reliable data or routing information from a trusted site. A security compromise could occur if an unfriendly party diverts or analyses our network traffic.

To prevent such attacks we used neighbor authentication to authenticate the source of each packet. Topology used where LDP authentication has been implemented is shown in Fig 12:

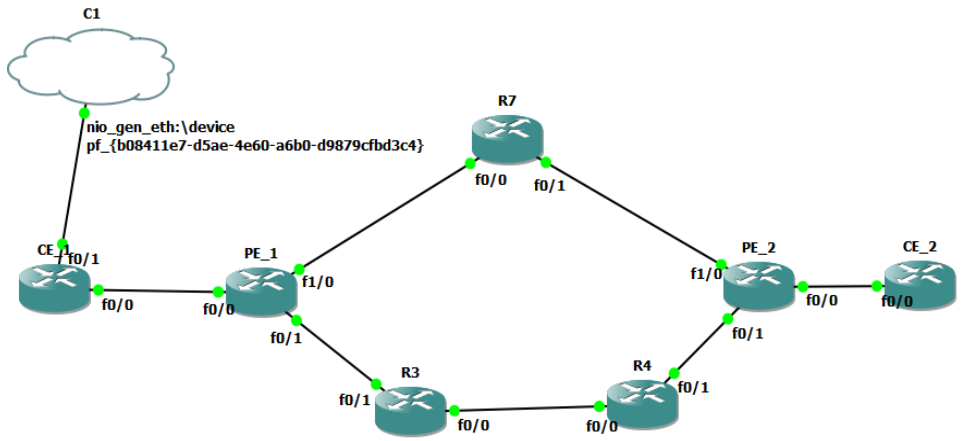

Figure 12 Topology used for LDP Authentication

In the topology above PE_1 with router – id 2.2.2.2 and R7 with router –id 7.7.7.7 will become neighbours only when their MD5 message digest matches. If R7 is not configured with MD5 Authentication and no password is given to it then PE_1 will get the notification message as shown in screenshot below:

```
*Mar  1 00:10:43.627: %TCP-6-BADAUTH: No MD5 digest from 7.7.7.7(59576) to 2.2.2
.2(646)
```

Figure 13 No Authentication Password Configured On R7

Now suppose the attacker tries to guess the password and if he fails to give the correct password then in this case PE_1 will get another notification message as an alert. The screenshot taken for this alert is shown below:

```
*Mar  1 00:14:15.751: %TCP-6-BADAUTH: Invalid MD5 digest from 7.7.7.7(36847) to 2.2.2.2(646)
 --More--
*Mar  1 00:14:22.287: %TCP-6-BADAUTH: Invalid MD5 digest from 7.7.7.7(39973) to 2.2.2.2(646)
```

Figure 14 Invalid Authentication Passwords

ENCRYPTION

The other security feature that can be implemented for securing MPLS Layer 3 VPNs is that we can use IPSec for securing our communication by encrypting the traffic at source and decrypting it at the destination. IPSec can be used in various scenarios which can be -

1.) Provider Edge to Provider Edge (PE-PE)

2.) Customer Edge to Customer Edge (CE-CE)

3.) Provider to Provider (P-P)

Best practice is to use CE-CE IPSec implementation, where traffic sourced from CE gets encrypted and decryption is done in CE site on the other end. I have used the MPLS Layer 3 design shown in Fig 15 for our MPLS Network Security Implementation.

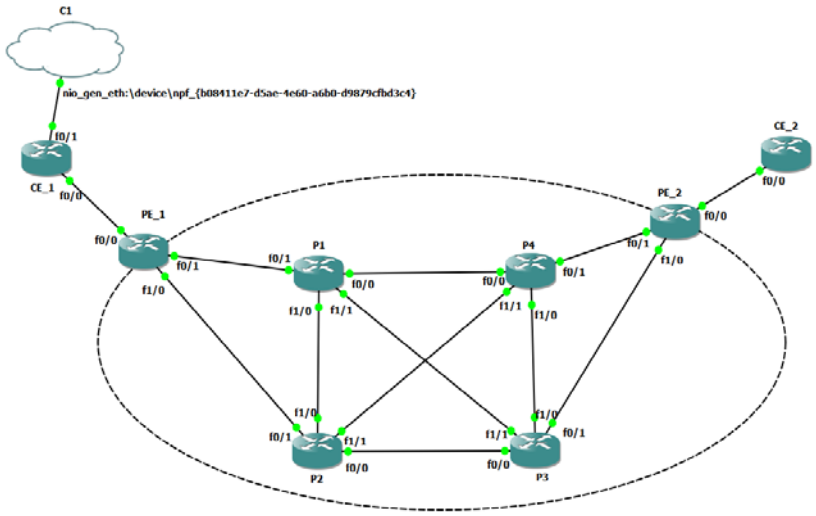

Figure 15 IPSEC IMPLEMENTED

I used IPSec for traffic between 1.1.1.1 which is on CE_1 and 8.8.8.8 on CE_2 and after creating a secure IPSEC tunnel between CE_1 and CE_2, we are able to access R8 via R1 as shown in the fig. 16:

```
R1#ping 8.8.8.8 source 1.1.1.1 repeat 999999

Type escape sequence to abort.
Sending 999999, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 1.1.1.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Figure 16 R1 checking reachability with R8 by issuing ping command sourced from 1.1.1.1

After sending the traffic from CE_1 (R1) to CE_2 (R8) by using ping command on R1, I issued the **debug crypto engine packet** command on R8 to check whether the incoming traffic from R1 is coming in encrypted form or not. Result is shown in the fig. 17 :

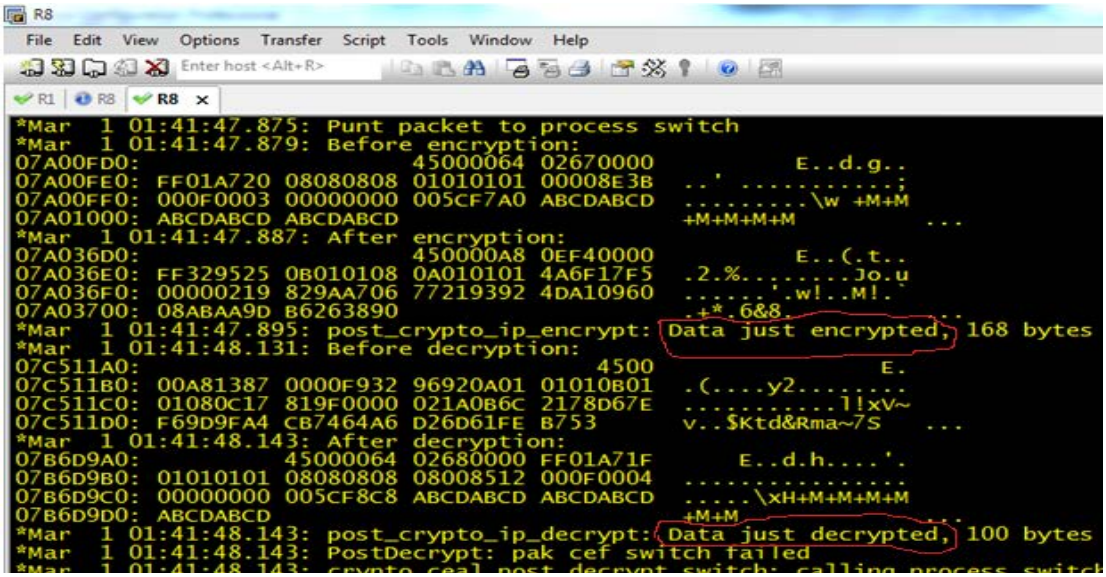

Figure 17 Output of debug crypto engine command showing encrypted and decrypted traffic on R8

As we can see data travels in the encrypted form and at the same time data gets decrypted at the destination. We also have to make sure that source and destination addresses of packets should not be visible. These addresses should be hidden so that attacker may not be able to divert the traffic to some unknown location by changing the destination address in the packet header. This has been done by using Tunnel mode of IPSEC.

To get into more detail, I have also used Wire shark Packet analyzer to sniff data that is going over Service Provider Network. Below is the capture taken from Wireshark:

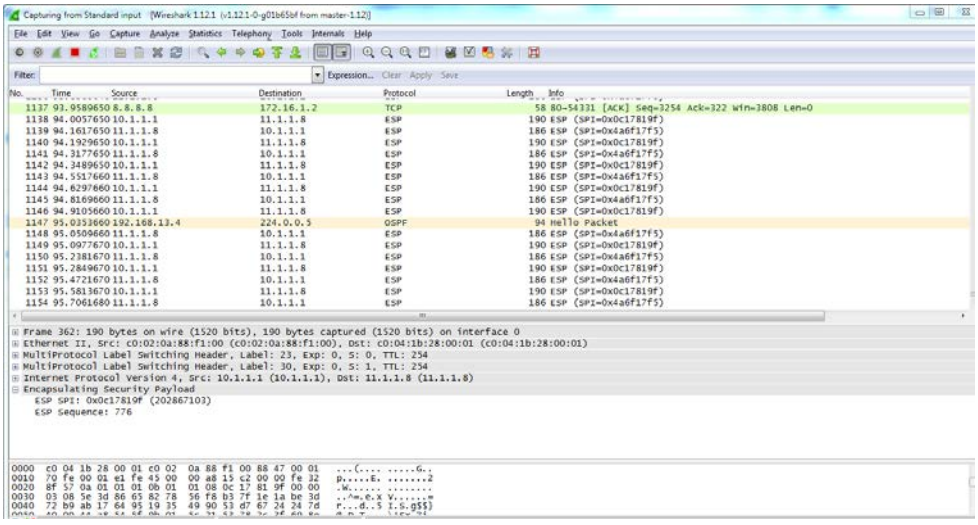

Figure 18 Wireshark capture showing traffic from 1.1.1.1 to 8.8.8.8 using ESP.

Above capture from Wireshark shows that Source and Destination IP addresses are hidden because we are using Tunnel Mode in IPSec. With Tunnel Mode, original IP address gets hidden and Tunnel's Source and Destination IP addresses are used which is a add-on to the network security.

Now after encryption and decryption of packets we have to be sure that number of packets that have been encrypted at the source should be equal in number of packets that have been decrypted. We have to make sure that no packet has been lost.

A graph showing Encrypted and Decrypted traffic between Source IP Address 1.1.1.1 and Destination 8.8.8.8 is shown in Fig 19:

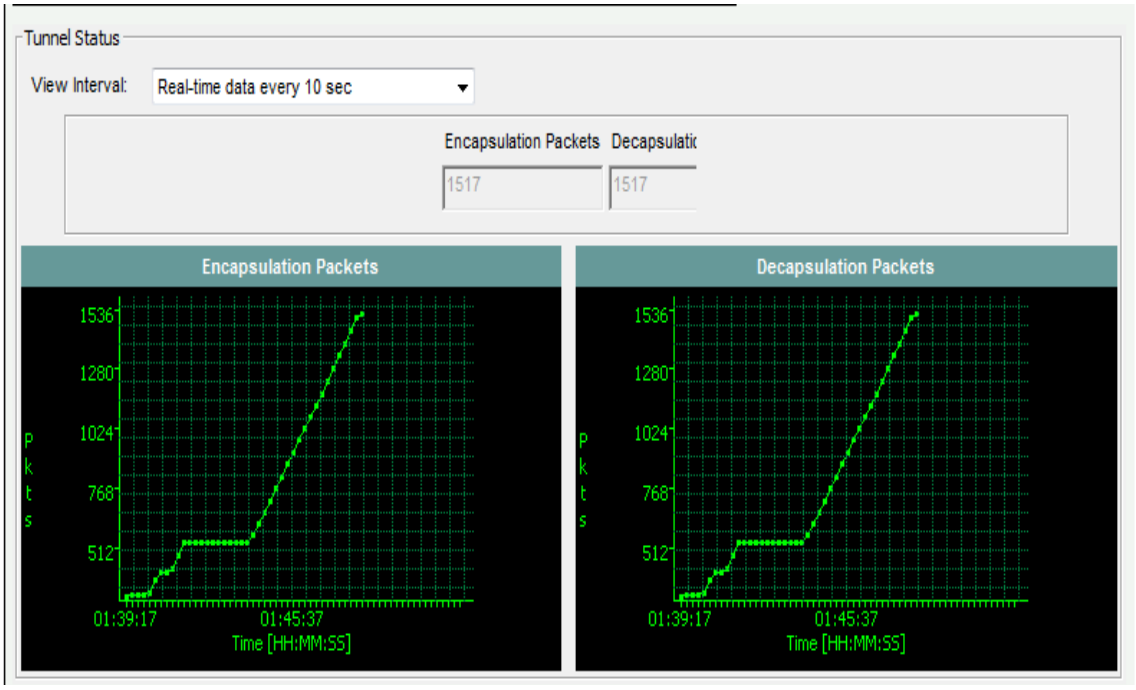

Figure 19 Graph showing encrypted and decrypted packets using IPSec.

Above graph created using Cisco Configuration Professional shows that 1517 packets have been encrypted using IPSec and same number of packets have been decrypted.

D. Security Analysis Of MPLS Layer 2 VPN

Denial of Service

It prevents authorized users to use specific network service or resource such as website. Recently Indian Telecom Regulators website was down due to Denial Of Service attack. We need to prevent such attacks as these cause so much damage to organization.

For Layer 2 MPLS VPN mainly Layer 2 Ethernet traffic travel from One Customer Edge towards other Customer Edge device at the other end. All the decision making on the path selection is done on the basis of the destination Mac address in the mac address table instead of routing table. In Layer 2 Environments, the major problem that can make our network unworkable and even can crash our devices is LOOPS. Now why loops can be so dangerous is that in Layer 2, there is no Time-To-Live value as we have in IP Packet. So a layer 2 loop is always endless and can create mess of our network within seconds. If a loop is created then it will always be endless as it has no life as mentioned before. It will behave like a broadcast packet which never stops. So for preventing DDOS attacks and loops, I have used a topology of two switches shown below for my thesis work.

Figure 20 Basic Layer 2 topology

In the above topology, I have created a Layer 2 Loop between switch 1 and switch 2, in which traffic loops between SW1 and SW2 and the packet rate goes around 40000-50000 frames per second. Switch used in the topology are Cisco 2950 Layer 2 Switch, Screenshot below is taken at the time of loop creation from one of the switch.

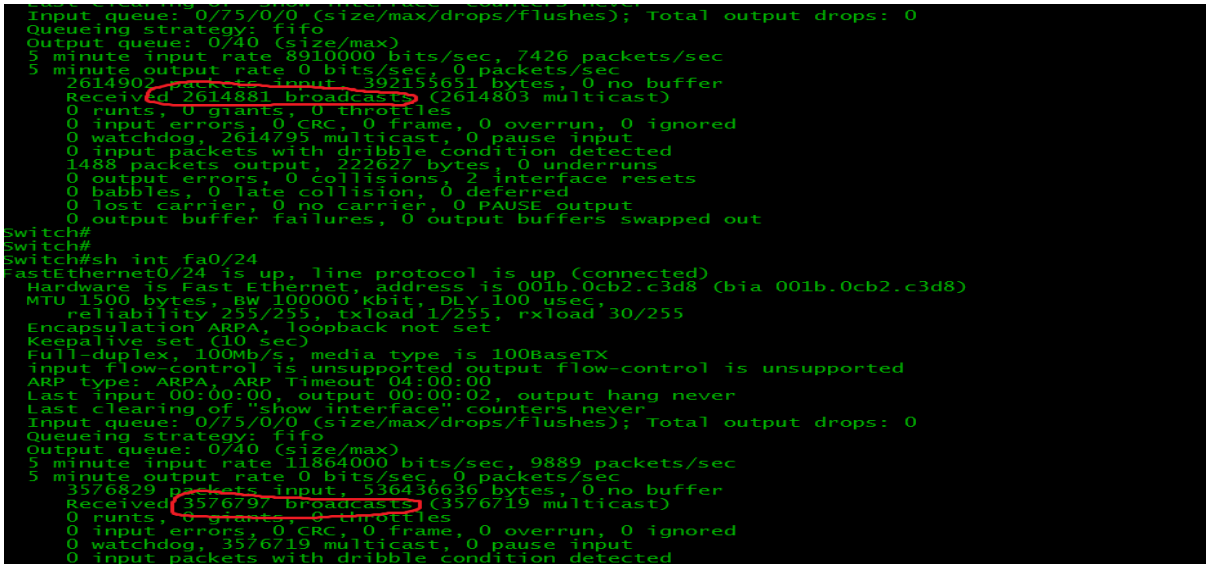

Figure 21 Switchport shows broadcasts that it receives

Above figure shows the number of broadcasts that a switchport receives. In my topology, Fastethernet 0/24 receives around 40000-50000 broadcast frames per second. This broadcast storm is created with just one single ping request and that single ping request of 32 bytes now uses 11864000 bits/second of the link. Suppose what could it be if it was a real network with 1000 employees are using the network. In the above screenshot, I used the command "show interface fastethernet 0/24" two times with the time gap of around 20 seconds, and the "received broadcast" counters increased from 2614881 to 3576797, which means a total of 961916 broadcast frames are sent at an average of 48095 broadcast frames sent every second. And this all started with just a single 32 byte ping request.

This broadcast storm or DDOS attacks can be stopped by using Loop Prevention mechanisms like Loopguard, Unidirectional Link Failure (UDLD), but one feature that can help us most in such situation is "Storm Control". With Storm Control, a maximum threshold can be configured on any interface in the form of bits or packets per second, or we can give a percentage of the interface bandwidth. If incoming traffic exceeds the specified threshold, traffic is blocked until the incoming traffic rate drops below the configured falling threshold interval.

Storm Control is a method with which we can create a limit on number of broadcast packets that we can receive per second. I have configured Storm Control on my Switch at Interface Fast Ethernet 0/24 using the following configuration:

Figure 22 Storm Control Configurations

In the above configuration I have configured maximum packets per second to be 10, if more than 10 packets are received at Interface Fast Ethernet 0/24 in a single second, then the port goes into shutdown state automatically as the action taken is selected as Shutdown state, the falling threshold is configured as 8 packets, if the packets per second drop to 8 or lesser, than the port can again starts working properly.

Now after configuring Storm Control, I once again created a loop and the result is shown below:

Figure 23 STORM CONTROL shuts down port in case of reaching rising threshold limit of 10 packets.

Another security threat in Layer 2 MPLS VPN can be Content Addressable Memory(CAM) table overflow attacks. In this attack, excessive traffic can be generated using different source mac-addresses in Layer 2 Network which can make the mac-address-table to be full and can also make our switch stop working properly or our switchport will get stuck in hang mode. Now if we know the maximum number of mac addresses that we can receive on a single port, we can also apply "switchport port security" methods on them, which can secure the layer 2 network from CAM overflow attacks. With Switchport Port security configuration, we can tell a switchport the maximum number of mac addresses than it can receive and also the action that needs to be taken if the maximum limit of mac addresses reaches. In my topology, I have simply used a maximum value of 1 Mac address , with a violation action of "Shutdown" on my Switch's interface Fastethernet 0/24. If the maximum limit of mac adresses is breached, then the port gets into "error-disable" state, in which port has stopped working.Below is the screenshot taken from the switch that receives more than one mac address on a port with maximum mac address limit is set to 1 :

a.) Before Security Violation , the security violation count is 0.

```
Switch#sh port-security interface fastEthernet 0/24
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address        : 0024.8137.148b
Security Violation Count   : 0
```

Figure 24 Before Security Violation Count 0

b.) After Security Violation, the security Violation Count sets to 1

```
00:30:37: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/24, putting Fa0/24 in err-disable state
00:30:37: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0024.8137.148b on port FastEthernet0/
24.
Switch#sh port-security interface fastEthernet 0/24
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address        : 0024.8137.148b
Security Violation Count   : 1
```

Figure 25 Security Violation Count 1

E. Business Evaluation: Layer 2 or Layer 3?

Various factors like service supply, budgets and application requirements are taken into account by various enterprises to make the decision about which type of MPLS VPN Service (Layer 2 or Layer 3) to use in connecting various remote sites. This decision needs to be taken carefully as choosing wrong technology can effect the enterprise as a whole in terms of budget , time etc. At the same time they want the service that is within their budgetary limits and the one that does not cause financial issues in the organization. Selection of Layer 3 or Layer 2 VPN service also depends on issues like need to control routing decisions, maintenance of network and outsourcing control.

Enterprises that prefer Layer 2 VPN services can be generalized to have following characteristics:

- These enterprises usually have lesser than 20 remote locations.
- For most of these remote locations bandwidth requirement is more than 10 Mbps.
- These enterprises have well developed IT infrastructure. These maintain their networks and make routing decisions themselves. This approach enables them to make decisions between various remote sites without involving service provider and thus provide more

security as decisions remain within the enterprise level. Also this allows to make changes faster.

Enterprises that prefer Layer 3 VPN services can be generalized to have following characteristics:

- These enterprises usually have more than 20 remote locations.
- For most of the remote locations bandwidth requirement is less than 10 Mbps. These usually require high bandwidth links between their head office, data centre and disaster recovery locations.
- These enterprises have the IT departments that outsource the maintenance of their networking and routing decisions.

If we decide on cost parameters, then service provider charge more for Layer 2 MPLS VPN than a Layer 3 MPLS VPN and the reason for that is with the L2 MPLS VPN, customer can send any type of traffic without any restriction and Service provider is mainly used just for Forwarding the traffic, while in L3 MPLS VPN, routing is shared with the customers and service provider can do restrict some traffic as it is under their authorization.

5. 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.The Performance of MPLS Layer 2 VPN is much better compared to MPLS Layer 3 VPN as by default Layer 3 MPLS VPN has a convergence time of 5-5.5 seconds, which can be reduced to 2.5 to 3 seconds. While by default Layer 2 MPLS VPN has a convergence time of 2-2.5 seconds, which can be reduced to sub-second after tuning SPF calculation. Cost for implementing Layer 2 VPN is more as compared to Layer 3 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. 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
2. Rosen, Eric, Arun Viswanathan, and Ross Callon. "Multiprotocol label switching architecture." (2001).
3. Andersson, Loa, and E. Rosen. Framework for layer 2 virtual private networks (L2VPNs). RFC 4664, September, 2006.
4. Martini, Luca. "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)." (2006).
5. Martini, Luca, et al. "Encapsulation methods for transport of Ethernet over MPLS networks." RFC4448, April (2006).
6. Kompella, Kireeti, and Yakov Rekhter. "Virtual private LAN service (VPLS) using BGP for auto-discovery and signaling." (2007).
7. Lasserre, Marc, and Vach Kompella. Virtual private LAN service (VPLS) using labels distribution protocol (LDP) signaling. RFC 4762, January, 2007.
8. Isaac, Aldrin, et al. "Requirements for Ethernet VPN (EVPN)." (2014).
9. Armitage, Grenville. "MPLS: the magic behind the myths [multiprotocol label switching]." Communications Magazine, IEEE 38.1 (2000): 124-131.
10. Cisco press MPLS Configuration on Cisco IOS Software http://flylib.com/books/2/686/1/html/2/images/1587051990/graphics/11fig01.gif
11. Press, Cisco. "MPLS fundamentals." Page 438, (2007).
12. Cisco," ASR 9000 Series L2VPN and Ethernet Services ConfigurationGuide",http://www.cisco.com/c/dam/en/us/td/i/300001400000/360001370000/361000362000/361074.eps/_jcr_content/renditions/361074.jpg
13. Sajassi, Ali, et al. "BGP MPLS Based Ethernet VPN." (2011).
14. Press, Cisco. "MPLS fundamentals." (2007).
15. Luo, Wei, et al. Layer 2 VPN architectures. Pearson Education, 2004.
16. Darukhanawalla, Nash, et al. interconnecting data centers using VPLS. Cisco Press, 2009.
17. Zhang, Lixia, et al. "Resource Reservation protocol (RSVP)--version 1 functional specification." Resource (1997).
18. Press, Cisco. "MPLS fundamentals." (2007).