RESEARCH ARTICLE OPEN ACCESS

Comparative Analysis of MPLS Layer 2 VPN Techniques

Gurwinder Singh [1], Er. Manuraj Moudgil [2]
Department of Computer Science and Engineering [1]
Department of Information Technology and Engineering [2]
PTU/BGIET Institute of Engineering and Technology, Sangrur
Punjab – India

ABSTRACT

MPLS is a technology that is used for fast packet forwarding mechanism within service provider networks. 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. Layer 2 VPNs behave like the customer sites are connected using Layer 2 switches. There are different Layer 2 VPN techniques like Virtual Private LAN Services (VPLS), Virtual Private Wire Service (VPWS) and Ethernet Virtual Private Network (EVPN). As MPLS runs inside Service Provider Networks. Security is always one of the major objectives. This paper explains the security techniques that can be applied to make Layer 2 MPLS secure.

Keywords **:-** MPLS, LDP, Pseudowire, AToM, VPLS, L2VPN, LABELS

I. INTRODUCTION

1.1 MPLS: MPLS is a packet forwarding mechanism basically the uses labels to forward packets. Labels are attached to packets after that mapping of label is done from one provider edge of router to another provider edge of router. MPLS is used in Service Provider environments. In MPLS Label Distribution protocols are used to distribute the labels and exchange of labels from one router to other router. LDP is the most common and widely used protocol in MPLS for the distribution of label. In the Routing Information Base (RIB) we can assign the LDP only on the non-BGP routes.

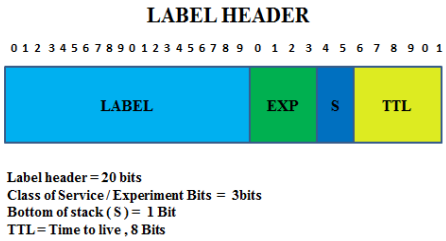

Fig. 1.1 Label Header

With its ability to forward traffic on the basis of labels instead of destination IP address, it eliminates the use of Border Gateway Protocol (BGP) protocol in the core service provider routers, but the greatest advantage of using MPLS is its ability to create Virtual Private Network.

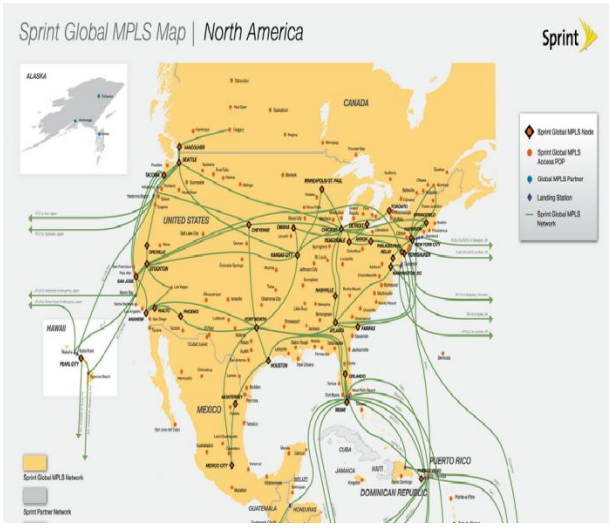

Fig. 1.2 Sprint Global MPLS Map | North America. http://1.bp.blogspot.com/-bW 377 zpwVKM/UHMA_E5PqI/ AAAAAAAAAW0/uwTSt1KC2h0/s1600/NorthAmerica-MPLS.png

MPLS is one of the big things happened to network industry in 21st century, and after around 14 years, since its first standard paper (IETF RFC 3031), it is still growing with BGP MPLS based Ethernet VPN

standard paper published in February 2015.MPLS is everywhere in networks with almost all of the service providers have their backbone network on MPLS, Datacenters are interconnected using L2 MPLS Technologies, Enterprises use MPLS services to connect their offices at remote locations.

II. MPLS LAYER 2 VPN

L2VPN (Layer2 VPNs) provides a transparent end-to-end layer2 connection to an enterprise over a SP's (Service Provider) MPLS or IP core. Client Sites behaves like they are connected via Switch. Traffic is forwarded from CE switch or router to PE switch in Layer 2 format. It is carried by MPLS over the service provider network and converted back to Layer 2 format at the receiving site.

Unlike L3VPNs where the SP takes part in the client routing, with L2VPNs the SP has no involvement in the client IP routing.

Client layer2 traffic is tunneled through the IP/MPLS core network, such that the CE routers appear to be directly connected.

A. Virtual Private Wire Service (VPWS) / Any Transport over Protocol (AToM)

Layer 2 traffic can be transported over MPLS backbone with the help of AToM/VPWS. AToM is Cisco's implementation of VPWS in MPLS networks. Layer 2 traffic is transparently carried across a MPLS backbone from one site to another with both the sites behaves like they are directly connected. Two pseudo wire technologies are used in VPWS, one is AToM, which is a pseudowire technology that targets MPLS networks and L2TPv3, a pseudo wire 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. Tunnel or pseudowire is create between the provider edge routers. Basically this type of pseudowires are used to transfer the data between the provider edges. A data that is travel from customer edge to provider edge identify by the two labels.

- Tunnel Label
- Virtual Circuit Label

Tunnel label is top label in the label stack and the VC label is always on the bottom in the stack. VC label always identify the remote customers which sent the data.

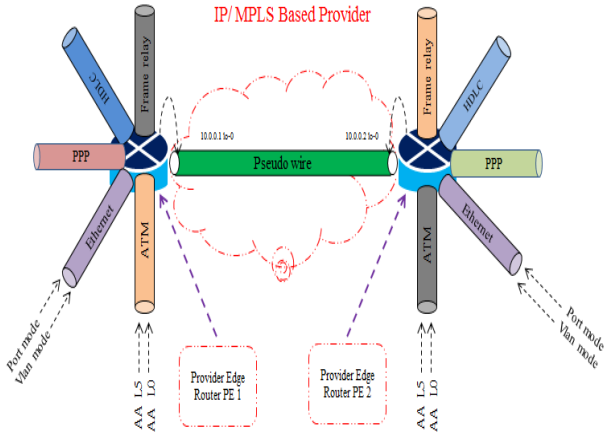

Fig. 2.1 AToM Model

B. Virtual Private LAN Services (VPLS)

VPLS uses Layer 2 architecture to offer multipoint Ethernet VPNs that connects multiple sites over Metropolitan-area-network(MAN) or Wide-Area-Network(WAN). VPLS is designed for those applications that requires multipoint access. VPLS emulates an Ethernet LAN. If a customer needs to connect his Ethernet segments from one site to another, VPLS service can emulate an Ethernet Switch that has ports leading to different Ethernet Sites. It can be a physical or a pseudowire port. MAC address learning takes place dynamically when packets arrive on a VPLS PE router, similar to traditional switch. Layer 2 loop prevention is done using split horizon forwarding. By default, layer2 control PDUs (VTP, STP, and CDP) are dropped at ingress VPLS PE routers. Layer2 protocol tunneling configured with "l2protocol - tunnel " allows VTP, STP or VTP to be sent across a pseudo wire. Enabling STP might be required in certain VPLS network designs to avoid downstream loops.

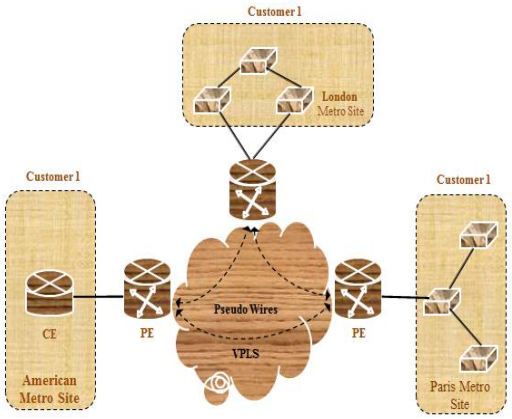

Fig.2.2 VPLS reference Model

c. Ethernet VPN & Provider Backbone Bridging-EVPN (EVPN & PBB- EVPN)

- EVPN and PBB-EVPN is designed to address various Datacenter and Servicer Provider requirements. It is a next-generation solution for Ethernet multipoint connectivity services. EVPN also gives you the capability to manage routing over a Virtual Private Network, providing complete control and security. EVPN uses BGP for distributing client's MAC addresses over the MPLS/IP network. EVPN advertises each of clients MAC address as BGP routes that add the capability of BGP policy control over MAC addresses. PBB-EVPN solution combines Ethernet PBB (IEEE 802.1ah) with EVPN, where PEs act as PBB Backbone Edge Bridge(BEB). PEs receives IEEE 802.1q Ethernet frames from their attachment circuits. These frames are encapsulated in the PBB header and forwarded over the IP/MPLS core. On the egress side, PBB header is removed and original dot1q frame is delivered to customer equipment.

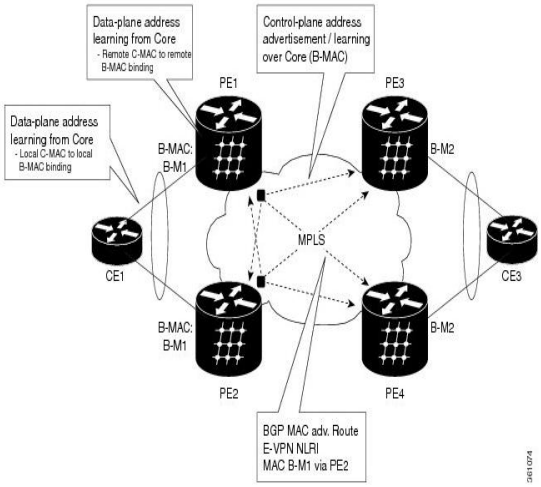

Fig. 2.3 PBB-EVPN Network [www.cisco.com - ASR 9000 Series L2VPN and Ethernet Services Configuration Guide]

III. BRIEF LITERATURE REVIEW

Multiprotocol Label Switching Architecture [1] by E. Rosen of Cisco Systems, A. Viswanathan of Force10 Networks, and R. Callon 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.

Framework for Layer 2 Virtual Private Networks (L2VPNs) [2] by L. Andersson, Ed. , Acreo AB, E. Rosen, Ed. Of Cisco Systems provides a framework for Layer 2 provider provisioned Virtual Private Networks (L2VPNs). 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 Virtal Private LAN Service(VPLS).

Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP) [3] by L. Martini, E. Rosen of Cisco Systems, N. Eul-Aawar of Level 3 Communications, T. Smith of Network Appliance and G. Heron 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 "pseudowires". This ducument specifies a protocol for establishing

and maintaining the pseudowires, using extensions to LDP.

Encapsulation Methods for Transport of Ethernet over MPLS Networks [4] by L. Martini, Ed. , E. Rosen of Cisco Systems, N. El-Aawar of Level 3 Communications and G. Heron of Tellabs describes an ethernet pseudowire(PW) is used to carry Ethernet/802.3 protocol data units(PDUs) over an MPLS network.

Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling [5] by K. Komepella, Ed. And Y. Rekhter, Ed of Juniper Networks describes BGP Auto Discovery and Signalling method for VPLS. It specifies a mechanism for signaling a VPLS, and rules for forwarding VPLS frames across a packet switched network.

Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling [6] by M. Lasserre, Ed. , V. Kompella, Ed. of Alcatel Lucent in IETF RFC 4762 describes a Virtual Private LAN Service (VPLS) solution using pseudowires, 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.

Requirements for Ethernet VPN(EVPN) [8] by N. Bitar of Verizon, A. Sajassi of Cisco Systems, R. Aggarwal of Arktan, W. Henderickx of Alcatel-Lucent, Aldrin Issac of Bloomberg, J. Uttaro of AT&T

MPLS: The Magic Behind the Myths [9] by Grenville Armitage, Bell Labs Research, Silicon Valley, Lucent Technologies reviews the key differences between traditional IP Routing and the emerging MPLS approach, and identifies where MPLS adds value to IP networking.

IV. OBJECTIVES

Comparative analysis of different MPLS L2 VPN technologies on the basis of :

- Performance
- Scalability
- Security

To determine which is the best L2 VPN option for Large Enterprise Networks?

To determine which is the best L2 VPN option for Inter-AS Service Providers?

V. METHODOLOGY/PLANNING OF WORK

1) To study various Layer 2 MPLS Standard documents which are used by different vendors while developing their devices and network operating systems.

2) Implementing Layer 2 MPLS VPN technologies in simulation environment, and draw conclusions based on the various parameters.

3) Implementation of Layer 2 VPN on Real Cisco Devices and a conclusion will be drawn from the output

4) A deep packet comparison will be made by comparing the headers of all the Layer 2 MPLS protocols using Wireshark Traffic Analyzer.

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

6) A 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

Security Analysis of MPLS Layer 2 VPN

Layer 2 traffic mainly consists of Ethernet or PPP etc protocols, with ethernet as the most widely used standard worldwide. I also did a security analysis on

MPLS layer 2 VPN. In Layer 2 VPN, all the IP traffic is not shared with the Service Provider and it acts as a Overlay VPN as compared with MPLS Layer 3 VPNs, where customer's routing table is shared with the Service Provider Edge Routers. Security is one the major concerns in the network industry as insecure delivery of data or unauthorized access of data can be very harmful for both customers and Service Providers. Imagine what happens if there is a insecure Service Provider, how can its clients be secure, or insecure customer devices which can cause every bit of damage to Service Provider, if they do not implement best security practices. In the very first security practice, i checked how harmful a loop can be in a layer 2 network, as there is no Time-To-Live value in Layer 2 networks. I created an environment where a Customer has two offices connected using Layer 2 MPLS VPN. Spanning-Tree Protocol is used by default in order to prevent loops in the switches as Customer Edge. A loop can be created due to some misconfigurations happened at the customer-edge devices or because of some problem in the media like one end not able to receive, but can send frames. Topology that we used for our Layer 2 MPLS VPN Security Analysis is shown below :

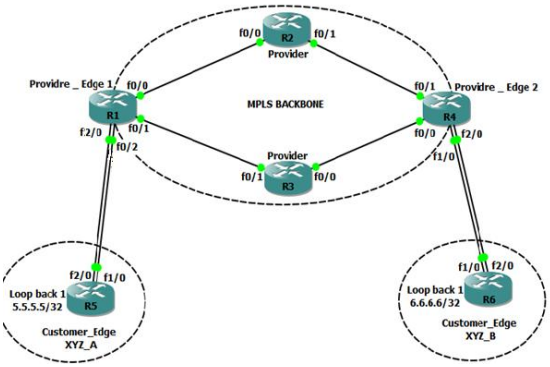

Figure. 6.1 - L2VPN topology used in the security analysis

In the above topology shown in Figure 1.1, Provider ABC has a customer named XYZ, who has two sites located at different parts of the country and needs to connect them using Layer 2 MPLS VPN. Both the customer-edge devices are connected with Provider-Edge devices using redundant connections, and with spanning-tree protocol running between Customer-Edges and Provider-Edges, there can be a blocking port between two customers, but if due to some misconfiguration, or some media issue, a loop generates, that can be very severe, A graph taken from PRTG Monitoring Tool when a loop occur between the different customer sites connected using L2 MPLS VPN is shown below :

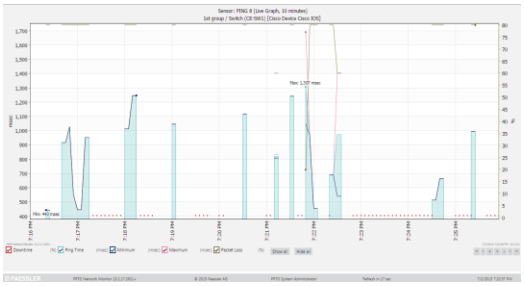

Figure 6.2 - Loop effect on traffic over L2MPLS VPN

Above graph taken from PRTG Monitoring Tool shows how the traffic gets dropped when the loop is in effect. Minimum time taken for a ping reply packet from on CE to other CE takes 443 msec and Maximum time taken is 1307 msec and rest you can also see that around 80 percent of traffic is unable to reach from one CE to other CE.

A loop can be very devastating to a network, which can be service provider or its customer network, I have misconfigured in my switch and created a loop in my network to check the effect of a layer 2 loop on the network. I am using Fastethernet ports in my network from Customer Edge to Provider Edge and after creation of loop, i sent 4 ping packets from source CE to remote CE, which inturns create a massive loop between CE-CE. Below is the output of the show command taken from Cisco Switch that shows how a loop can generate a broadcast storm in the network :

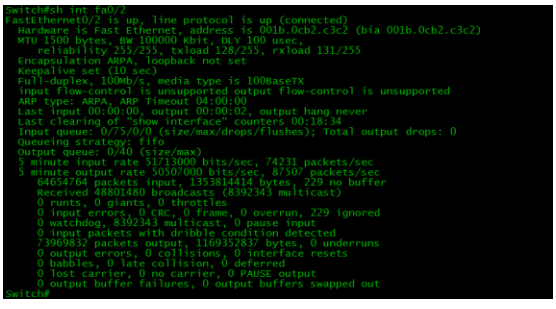

Figure 6.3 - 4 packet loop effect on L2MPLSVPN topology

As shown in the output above from a Cisco Switch, over 64 million packets are sent/received between the Customer-Edge devices at the rate of 75000 approx packets per second, A total of 1353814414 bytes of data or 1291 Mb of data is received in around 14 minutes, and all that happened is just with a Layer 2 Loop and 4 ping packets. Now this is tested in a lab environment, one can suppose the effect of a Layer 2 Loop when its in production network with IP Phones calling all the time, data transfer, Video Conferences etc. In around 14 minutes, 50 percent of 100Mbps line is in use and that is achieved with just 4 packets. To prevent this type of traffic storm, a feature known as Storm-Control can be used which can provide a rising and falling threshold packets-per-second(pps) limit on the interface regarding broadcast/unicast/multicast storm. I have implemented this feature on my lab's CE devices whose ports are connected with PE devices. These CE switchports are taking part in the Spanning-Tree. I have configured storm-control on these two ports, configuration is shown on the page below :

```
Switch(config-if)#storm-control broadcast level pps 100 80
Switch(config-if)#storm-control unicast level pps 100 80
Switch(config-if)#storm-control multicast level pps 100 80
```

Figure. 6.4 - Storm Control Configuration

```
Switch#sh storm-control
Interface  Filter State   Trap State     Upper     Lower    Current  Traps Sent
---------  -------------  -------------  --------  -------  -------  ----------
Fa0/1      Forwarding     Below rising   100 pps   80 pps   0 pps    0
Fa0/2      Forwarding     inactive        10 pps    8 pps   0 pps    0
Fa0/3      inactive       inactive       100.00%  100.00%   N/A      0
Fa0/4      inactive       inactive       100.00%  100.00%   N/A      0
Fa0/5      inactive       inactive       100.00%  100.00%   N/A      0
Fa0/6      Forwarding     inactive        10 pps    8 pps   0 pps    0
Fa0/7      inactive       inactive       100.00%  100.00%   N/A      0
Fa0/8      inactive       inactive       100.00%  100.00%   N/A      0
```

Figure 6.5 - output of storm-control configuration

Above configuration done shows that we have configured rising and falling threshold of 100 and 80 packets per second. Storm Control can help when loop occurs even after applying all other conditions like LoopGuard or Unidirectional Link Detection(UDLD). Storm Control provides a maximum threshold that can be configured on any interface in the form of bits or packets per second. We can also assign percentage of the interface bandwidth.If interface traffic exceeds the specified threshold, traffic is blocked until the traffic rate drops below the falling threshold level. A graph below illustrates Storm Control's Rising and Falling Threshold :

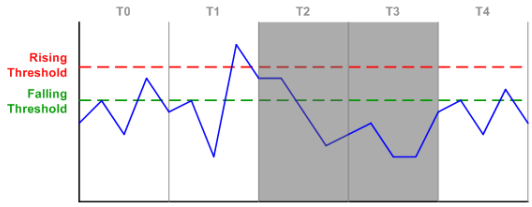

Figure 6.6- Storm Control Basic Model with Falling and Rising Thresholds

In the configuration, the maximum threshold that i gave to interface is 100 and the falling threshold is 80, action that can be taken when rising threshold limit is exceeded is to shutdown the port, therefore whenever the traffic goes beyond 100 packets per second, the port automatically goes into shutdown state. I intentionally sent the traffic storm over the port which was configured with storm control, and the result is shown below :

```
Switch(config-if)#
00:06:01: %STORM_CONTROL-2-SHUTDOWN: Storm control shut down FastEthernet0/24
```

Figure 6.7 - Storm Control prevents the traffic storm by shutting down the port

Another security threat can be Dynamic Trunking Protocol(DTP) being enabled on the switchports where some PC or server is installed. It can be very dangerous. Let's see an example - Suppose you have a company named ABC, your company has a MPLS L2VPN connection from one Branch office to other. A guest came into your office who is the friend of the Network Head and says that he needs to have internet for 30 minutes and he forget his smartphone and has no device to connect with the internet and you ask him for the his Laptop for 10 minutes, as a good friend, he agrees to give you laptop and suddenly the network head got a call thet a client has come to office to meet him, he left the place to meet the client and said his friend that he will come within 30 minutes, until then he can use his Laptop and Internet. Network Head's Laptop is connected with Lan with which the CE device is connected. Now we can say that the guy(Network Head's Friend) is the network head for the next 30 minutes. Now the profile of this guy is that he is a network security analyst in some other company. He saw lots of networking software1s and packet sniffers on Network Head's Laptop. He intentionally opens

GNS3 and add a switch in the working space and connects that with local lan and assigning it lowest priority to make the GNS3 switch as root bridge, which can make this GNS3 switch as the main switch or main authority of the entire CE-CE L2VPN. All the topology gets redesigned automatically within few seconds and almost all the data gets through his simulated switch in GNS3 which he can sniff easily using Wireshark Packet Analyzer. To stop this kind of attacks, first precaution measure is that never give your office device control to anyone , even if you trust them. Other security practice that we can make all the host connected ports as "access-ports" and also with a "different vlan other than default-vlan 1", if we have configured all the switchports that are connected with the hosts as "access", then the simulated switch can never create a trunk link as it did when DTP is configured on the switchports. There can never be a trunk link if trunk is configured at one end and access at other end. Also if the local lan has a different vlan configured then also simulated switch cannot be able to access any traffic with default vlan 1 configured on simulated switch.

The best security that we can apply to this problem is BPDUGurad, switches share their information using Bridge Protocol Data Units(BPDU) after every two seconds in the case of Spanning Tree Protocol. If switch is connected with some PC like we have in our example, with Network Head's PC is connected with CE Switch, host machines cannot send BPDUs and doesn't understand BPDUs, so on the switchport where a host machine is connected, with BPDUguard, we can apply a filter which can disable the port if a BPDU is received on a port using a Host Machine. BPDUGuard configuration is done of the port that is connected with the host machines. Following is the configuration that i did on a Cisco Switch :

```
UPPER-SW(config-if)#spanning-tree bpduguard enable
```

Figure 6.8 – BPDU Guard Configuration on a Cisco Switchport

With BPDU Guard configured on the Switch port, if switch port on which BPDU Guard is configured receives any BPDU, then it will straightway goes into error-disabled state. Therefore if friend of Network Head in our example if intentionally or unintentionally tries to become Root Bridge using Network Head's PC, then he will be blocked. Following is the output that is shown when a switchport with BDUGuard enabled receives a BPDU:

Figure 6.9 - Port goes into error disabled state after receiving BPDU on a BPDUGuard enabled port

This switchport can act normal or we can say that this port can get out of error-disabled state with two methods, either by "shut down and again no shut" on the switchport manually or by using error-disable recovery mechanism for BPDUGuard.

Another Security Best practice that we can implement is Switchport Port Security. Switchport Port Security is used to harden the switchport to use a specific number of Mac addresses or we can also harden the MAC address that can be used. This method helps in prevention of CAM table overflow attacks also known as MAC Overflow attacks. Switch can use various options if more than the defined number of MAC address received at the switchport. There are mainly three options :

1.) Protect Mode - Switchport will drop the packets that come from the unknown source MAC address and it will carry on dropping the packets until we remove some secure MAC address which will help in dropping down the maximum value of MAC addresses on the switchport.

2.) Restrict Mode - It will also drop the packets from the unknown source MAC address and can also let the traffic go through if the certain number of secure MAC address are removed in order to drop the level below the maximum value. Also it will let the security violation counter to increment.

3.) Shutdown Mode - This mode is used by default. It brings the port into error-disabled state, which can only be in enabled state again, by "manually shutting down the port and then again no shut", or we can use error-disable recovery mechanism.

Configuration that we have done for switchport security is given below :

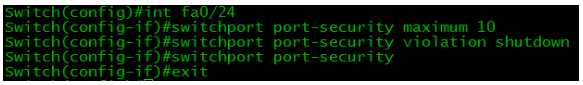

Figure 6.10 - Switchport Port Security Configuration with maximum number of MAC set to 10

In the above configuration that we have done, the maximum number of MAC addresses that we have tell the switchport to receive is 10, and the violation mode that is used is Shutdown Mode. So, if the switch receives more than 10 Mac addresses on the switchport than the switchport will gets into error-disabled state.

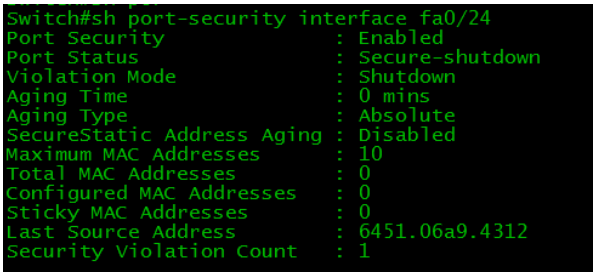

Figure 6.11 - show command in cisco showing all the configured parameters on Port-Security

I have intentionally sent more than 10 MAC addresses on the switchport as the source addresses, and the resulted output is given below :

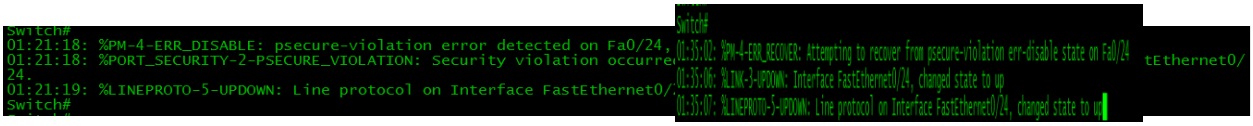

Figure 6.12- Port gets into error disabled state after violated against Port security violation

Now as the port gets into error-disabled state, it can get out of error-disabled state with two methods :

1. Manual recovery mode : We can shut down the port first then use "no shutdown" command on the switchport manually. Manual method is shown in the following screenshots :

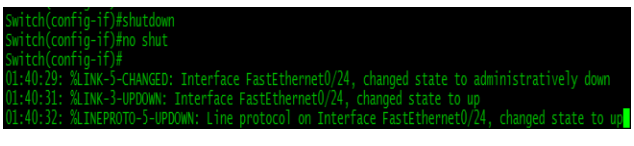

Figure 6.13 - Switchport recovering from error-disable state using manual recovery method

2.) Auto Recovery - Other method is with error-disable auto-recovery method, with which switchport is insructed to recover automatically after a specific period of time, default time is 300 seconds, when we enable auto-recovery, but we don't assign the time. Configuration, and outputs are shown below :

Figure 6.14 - Portsecurity error-disable auto recovery configuration with interval 60 seconds

Figure 6.15 - show command shows that 13 seconds are left for auto-recovery

Figure 6.16 - Switchport successfully attempted to recover from port-security error-disabled state

Apart from the above security best practices, following are some of the security implementation, which can help network become much more secure :

- Always apply secure password for console/aux/vty access
- Ensure VTP is configured in Transparent Mode
- Establish broadcast controls on interfaces
- Shut Down all unused ports
- Use allowed list and remove unused from it.
- Hardcode physical port attributes
- Establish error reporting, use Syslog Server
- Disable Dynamic Trunkking Protocol(DTP) and Cisco Discovery Protocol(CDP)

VII. CONCLUSION

MPLS is a prime technology used mainly in Internet Service Provider (ISP) for label switching and VPN purposes. Some of the techniques that are used for security purpose one of them is Storm Control that is used to control the loops, unknown unicast, and broadcast storms. A total of 1291 mb of data or 64 million packets have travelled between CE and PE device by sending just a single ping in a looped network. Storm control is used to control such kind of bursts traffic attack. UDLD and Loop guard is used for loop prevention in case of unidirectional links failure. BPDU Guard can be used in case if BPDU are received on port where switch is not used and someone tries to send the BPDUs over it for authorized access or to become the ROOT BRIDGE. Switch port security is used in order to limit the MAC address that can be received on PE port connected with CE, which can helps in preventions of Denial – of – service attack. To secure the MPLS, above techniques are a necessary in order to service L2 MPLS VPN.

ACKNOWLEDGEMENT

This paper has been made possible through the constant encouragement and help from my parents and guide. I would like to thank Head of Department of Information Technology Er. Manuraj Moudgil, for her generous guidance, help and useful suggestions.

REFERENCES

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

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

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

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

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

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

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

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

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

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

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