QoS and Traffic Engineering in Multiprotocol Label Switched Backbone Networks

Umar Bashir Sofi
[1] *Research Scholar, Department of CSE RIMT- IET, Punjab Technical University, Jalandhar India*
(E-mail: umarbashir99@gmail.com)

Abstract— MPLS is a service provider technology and is used in the core of service providers to create virtual private networks. Data, Voice and Video traffic is increasing at a very rapid pace resulting in requirement of QOS and traffic engineering for critical VoIP traffic. In contrast to older algorithms in which traffic routing decision is taken on arrival at a node and selecting the best path available at that time, we can use traffic engineering and quality of service in MPLS and create tunnels for different types of traffic for a better traffic flow. Experimental bits are used in MPLS as Differentiated Services Code Points or IP Precedence in IP based networks to assign priority to different types of traffic types or to different tunnels. Using MPLS EXP bits also brings better jitter and packet delay variation in the network for low latency traffic like Voice over Internet Protocol(VoIP) or Cloud based Application Traffics. MPLS is and will be the primary technology used by the service providers because of its benefits that it provides, therefore MPLS has to have quality of service and MPLS traffic engineering enabled to make billions of bytes to data flow properly through the service provider with minimal packet loss or minimal delay. In this paper, MPLS is explained along with the different advantages that it provides in the service provider networks. It also includes the MPLS Traffic Engineering and Quality of Service Models which can be used for low latency traffic applications.

Keywords—*mpls; traffic engineering; quality of service; dscp; service provider network; vpn; experimental bits*

I. INTRODUCTION

Multiprotocol Label Switching or MPLS uses labels to forwards the packets within the Service Provider Networks, before MPLS, this process was done by using traditional packet forwarding using destination routing table lookups. With MPLS, Labels are embedded with the packets that enters from customer edge devices to the provider edge devices and all the forwarding in Service Provider is done hop by hop on the basis of the labels until the traffic reaches the egress port of the egress provider edge router. By default, when we enable MPLS, Label Distribution Protocol(LDP) is used for label distribution between the routers. Different Label Distribution protocols other than LDP are Resource Reservation Protocol(RSVP), Multi-Protocol BGP(MP-BGP). RSVP is mainly used for traffic engineering purposes while MP-BGP is used to distribute label bindings for BGP routes from one edge to other provider edge. Below is the figure of the Label Header :-

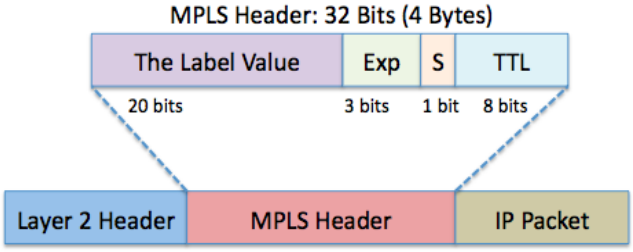

Figure 1.1 Label Header

With MPLS running in Service Providers, it also helps in having a BGP free core, as there is no need to run BGP in the core of Service Provider Network with all the decision making on packet forwarding can be done on the basis of labels and not on the destination routing table. The biggest advantage of using MPLS for Service Providers is that its ability to create both Layer 2 and Layer 3 VPNs so easily. Other important benefits of using MPLS is Traffic Engineering , use of one unified network infrastructure means that there's need not to buy extra infrastructure to run MPLS as it can run on Service Provider Routers and do not need any extra devices, MPLS also brings an optimal traffic flow. ISPs use MPLS at large extent to provider various applications or services to the customers. Below is the figure showing Vodafone MPLS Network worldwide :-

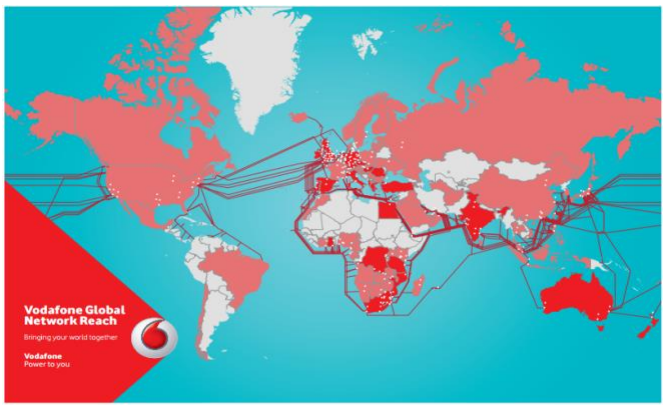

Figure 1.2 - Vodafone Global MPLS Network

2) MPLS Layer 3 VPN - MPLS Layer 3 VPN creates a peer-to-peer VPN network as customer edge shares the routing information with the provider edge device. With MPLS Layer

3 VPN, labels are added to simple IP traffic when it enters from CE device to the PE device, and all the forwarding within the MPLS Backbone network of Internet Service Provider is done using Label Switching, and labels are disposed when it goes out of Egress PE device. Routing Neighborship is made between PE and CE device.

MPLS L3 VPN Terminology

- **Label -** Label is a 4 byte identifier used by MPLS for label switching purposes.
- **LSR -** Label Switch Router is any router on which MPLS is running.
- **P -** Provider router that runs MPLS and is not a edge router connecting with CE device.
- **PE Router -** Provider Edge Router is an edge router in the Service Provider, labels are imposed and disposed.
- **CE Router -** Customer Edge Router is an edge router in the customer network which is connected directly with the provider edge router.
- **Ingress PE Router -** In this edge router, labels are imposed to the normal IP Packet.
- **Egress PE Router -** It is the edge-LSR device, and the destination CE is connected directly with this device. This device receives the labeled packet and dispose the label and sends a normal IP Packet to the customer edge device.
- **VRF -** Virtual Routing and Forwarding is used in Layer 3 MPLS VPNs to create different routing tables for different customers. VRF is implemented at PE routers and is integrated with the PE interfaces connected with CE interfaces. Every VRF interface has a different Routing Information Base(RIB), Forwarding Information Base(FIB), Label Information Base(LIB), Label Forwarding Information Base(LFIB) table.
- **Route Distinguisher(RD) -** RD is a very important part of the VRF. Route Distinguisher is a 64 bit value which is attached to the client's IP address and helps in uniquely identify a route by producing a unique 96 bit VPNv4 address. These VPNv4 routes are then taken from one PE to other PE via Multi-Protocol BGP(MP-BGP).
- **Route Target(RT) -** RT is a 64 bit community value which is attached to the VPNv4 routes and are used to import and export routes. RTs can either be imported or exported. We can also use "both" keyword to indicate export and import together. Import RTs are used to fetch the VPNv4 routes and add them to their specific VRF routing tables. Export Route Tags are embedded to the route when it is sent into VPNv4 Routing Table towards the other end of the customer. Below is the figure showing Route Propagation in Layer 3 MPLS VPN :-

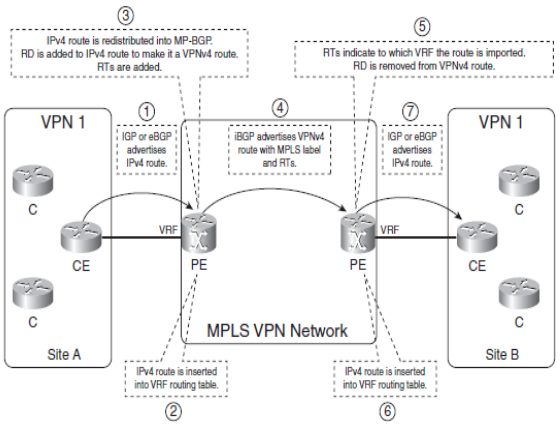

Figure 2.2 - MPLS Layer 3 Route Propagation

3.) MPLS Traffic Engineering

MPLS Traffic Engineering is used to utilize network resources and all the paths in a more efficient manner than with MPLS without traffic engineering. Protocol that we can use with MPLS traffic engineering is RSVP-TE. We can reserve explicit paths also which are not the best paths to reach destination according to Interior Gateway Routing Protocols like OSPF(Open Shortest Path First) or IS-IS(Intermediate-System to Intermediate-System) . The best thing about traffic engineering is that underutilized links can also be used, therefore load can be balanced in a much better manner. Fast Rerouting is another traffic engineering feature that helps in fast failover in case of primary Label Switch Path failure from one PE to other PE.In MPLS, Traffic engineering is solely based on Experimental bits and bandwidth can be reserved by using RSVP TE mechanisms. Below is the figure that displays the RSVP Path Reservation message flow:

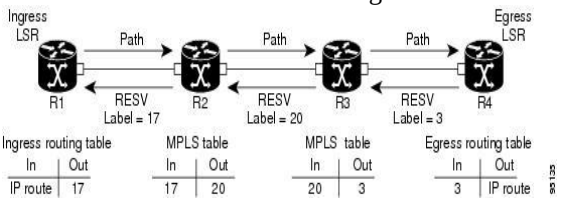

Figure 3.1 – RSVP Path Reservation

One of the reasons why MPLS is so much popular in Internet Service Provider industry and has overcome all the traditional ISP technologies like Frame Relay and ATM etc is traffic engineering options that MPLS provides to the Service Provider. MPLS Fast Reroute makes the MPLS convergence as faster as 50ms in case the link is converged from primary to backup link. Using MPLS FRR, multiple tunnels can be created between the PE routers and primary and backup tunnels are assigned to the traffic and in case the primary tunnel goes down, the backup tunnel comes up in around 50 ms. Below is the illustration in the figure that displays the MPLS FRR:

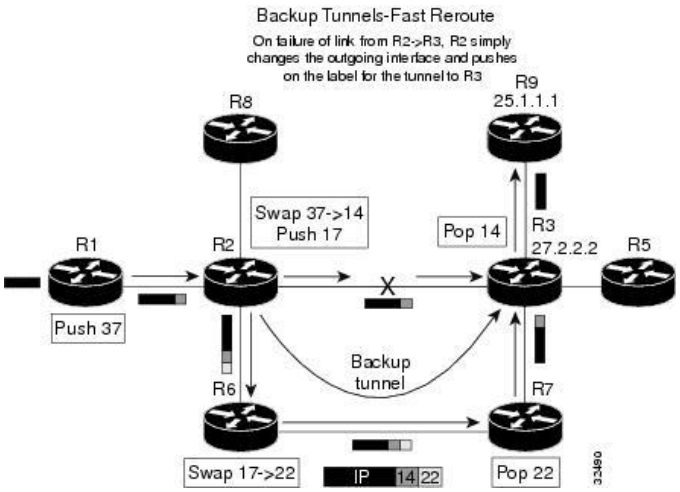

Figure 3.2 – MPLS FRR

MPLS QOS

Currently three models are used for implementing quality of services in MPLS that are explained as under:

QOS Models in MPLS

- **PIPE MODEL**

In this mode, ingress Provider edge router defines its MPLS Experimental bits. This mode is defined by Service Provider. When the traffic reaches egress Provider Edge router, then the forwarding is done on the basis of EXP bits.
It can be used when Core and Customer networks have a total different QOS policy. QOS policy followed in MPLS core is same for every customer.

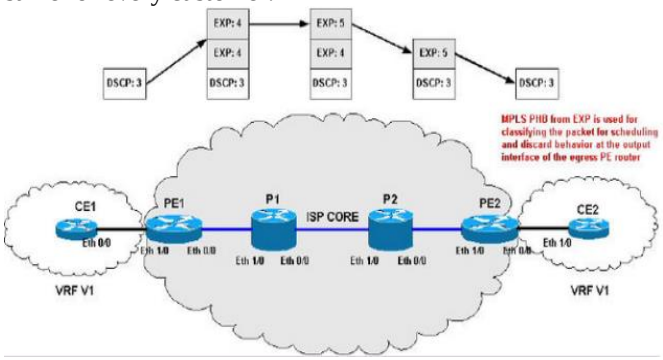

Figure 3.3 – MPLS QoS Pipe Model

- **SHORT PIPE MODEL**

In this mode Service Provider defines MPLS Experimental Bits on Ingress Provider Edge. Forwarding is done on the basis of DSCP on egress router. Here one can define different QOS for each customer in Egress PE. It is mainly used when the MPLS core and the customer networks have difference QoS Policy, and when SP wants to honor customer DSCP marking on egress PE to CE link.

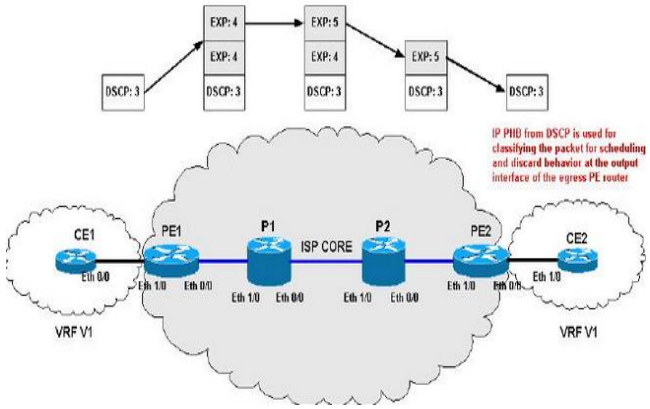

Figure 3.4 - MPLS QOS Policy - Short Pipe Model

- **UNIFORM MODEL**

In the Uniform Model, Experimental Bits on every LSP and tunnel labels are copied from Customer IP precedence across MPLS networks. If there is any change in the Outer EXP, then its not copied to the DSCP. But if there exists a change of EXP in MPLS, then in that case it will be copied to all labels and DSCP. It is used where customer and ISP shares the same QOS policy for some large enterprise that has its own MPLS core. This model is mainly used for large scale customers who have multiple types of traffic and they want their different types of traffic to be tagged and prioritized in same manner as the traffic is originated on to the path towards destination.

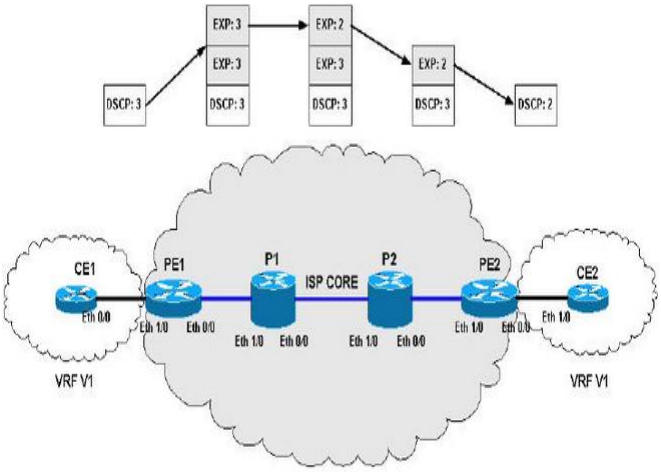

Figure 3.5 - MPLS QOS Policy - Uniform Model

CONCLUSION

MPLS is the core technology used in service provider networks and is also known as backbone of ISPs. It provides plethora of advantages with the like of BGP free core, Layer 2 and Layer 3 VPNs. Service Providers have clients using different types of traffic like Data, Voice, Video, Cloud etc. which traverse through the ISP MPLS backbone. QoS and

Traffic Engineering are very much required in the MPLS backbone for better flow of traffic and better network convergence. There are three QoS models in MPLS and can be used for different types of traffic and in different network environments. MPLS EXP bits and QoS only runs inside the MPLS backbone and IP based network uses DSCP or IP Precedence. MPLS FRR is used for faster convergence and provides millisecond convergence in case of multiple links from one PE to another PE. MPLS as a technology has been around for two decades and is still improving with new researches going on in this technology.

ACKNOWLEDGMENT

This paper has been made possible through the constant encouragement and help from my colleagues and parents. I would like to thank them for their generous guidance, help and useful suggestions.

REFERENCES

[1] HESAM HOSEINZADEH (2015)"Path Selection Analysis in MPLS Network Based on QOS" under science journal (CSJ), Vol. 36, No: 6 Special Issue(2015) ISSN:1300-1449.

[2] Jyoti Aggarwal and Akansha dhall (2015)"Simulation Based Comparative Analysis of Voice over Internet Protocol over MPLS and Traditional IP Network" under International science journal ,Engineering and Technology Research (IJSER), Volume 4, Issue 6 (june 2015) ISSN:2278-7798.

[3] Ezeh G.N, Oneakusi C.E, Adimonyemma TM and Diala U.H (2014) "Comparative Performance Evaluation of Multimedia Traffic over Multiprotocol Label Switching using VPN and traditional IP networks" under IJETR-ISSN(E):2347-5900 ISSN(P): 2347-6079

[3] Rosen E ,Viswanathan A , and Callon. R.(2001) "MPLS Architecture"
[4] Andersson Loa , and Rosen E. (2006)"Framework for layer 2 virtual private networks(L2VPNs)" RFC 4664.
[5] Martini and Luca. (2006) "Pseudowire Setup and Maintenance Using the Label Distribution Protocol(LDP)"
[6] Martini L (2006) " Encapsulation methods for transport of Ethernet over MPLS networks" .RFC4448.
[7] Kompella , Kireeti , and akov Rekhter(2007). "Virtual private LAN service (VPLS) using BGP for auto-discovery and signaling".
[8] Lassere , Marc , and VachKompella(2007). "Virtual private LAN service (VPLS) using label distribution protocol(LDP) signaling". RFC 4762.
[9] Isaac and Aldrin(2014) " Requirements for Ethernet VPN (EVPN) ".
[10] Armitage and Grenville (2000) " MPLS: the magic behind myths [multiprotocol label switching]. "Communications Magazine , IEEE 38.1(2000) : 124-131.
[11] Press , Cisco. " MPLS fundamentals . " Page 438, (2007).
[12] 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
[13] Sajassi , Ali , e 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.