MPLS Technology on IP Backbone Network

Gurpreet Kaur
Student, DAVIET
Jalandhar (144001), India

Dinesh Kumar
Assistant Professor, DAVIET,
Jalandhar (144001), India

ABSTRACT
Multiprotocol Label Switching is the protocol framework on which the attention of network service provider is focused as it provides privacy and unbreakable security to the users. So, it is used by ISP Backbone Network to form the MPLS Tunneling architecture like MPLS VPN which is discussed in this paper. Providers typically offer this type of service to large corporate customers that require IP connectivity of other remote sites. The main advantage is that MPLS is used over Layer 2 and Layer 3 protocols. It also discusses the concept of Traffic Engineering that utilizes Multiprotocol Label Switching and that also proves to be advantageous over IP based Routing. This Paper also discusses various Encryption Techniques which can be used for the security of MPLS Technology

Keywords
COS, LSP, LDP, LSR, TE, VRF, FEC and VFEC.

1. INTRODUCTION
MPLS stands for Multiprotocol Label Switching, is a technology proposed by Internet engineering Task Force (IETF) it was designed to facilitate several problems areas in the internet including routing performance and is increasingly being adopted by service providers in their core networks. MPLS solutions are to be used with Layer2 and Layer 3 Protocols. A label is a short fixed length identifier that is used to forward the packets. With MPLS, labels are attached to the packets at the ingress point to an MPLS network. Within the network the labels are used to route the packets without regard to the original packets header information, These labels can be stacked as a LIFO labels enabling MPLS to be combined for transport and distribution. MPLS header is 32 bits long [5]. The label field gives information needed to forward the packet and is the basis upon which MPLS switching operations occur. The COS bits affect the scheduling and or discard algorithms applied to the packet as it is transmitted through the network. These bits are not modified by the embedded implementation of MPLS. The Stack bit is set to 1 for the last entry in the label stack and 0 for all other label stack entries. The TTL field is decremented by 1 each time the packet passes through a router. The packet is discarded when the TTL reaches zero.

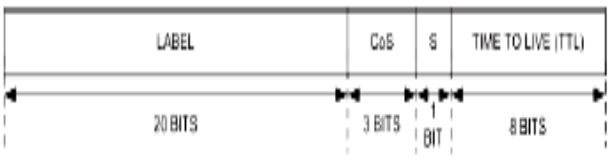

Figure 1 MPLS Label

2. MPLS ARCHITECTURE
Multiprotocol Label Switching (MPLS) is a tunneling technology used in many service provider networks [3]. The most popular MPLS-enabled application in use today is the MPLS virtual private network. MPLS VPNs were developed to operate over MPLS networks, but they can also run over native IP networks. This offers providers flexibility in network deployment choices, improved routing system scalability and greater reach to customers. The key element is the ability to encapsulate MPLS packets in IP tunnels. In an MPLS network, each LSP is created over the best path selected by the IGP, towards the destination network. An IGP (OSPF or IS-IS) is used to propagate routing information to all routers in an MPLS domain to determine the best path to specific destination networks. Each hop within the network core forwards packet based on the label, not IP information, until the final label switch is reached where the label is discarded and normal IP forwarding resumes.

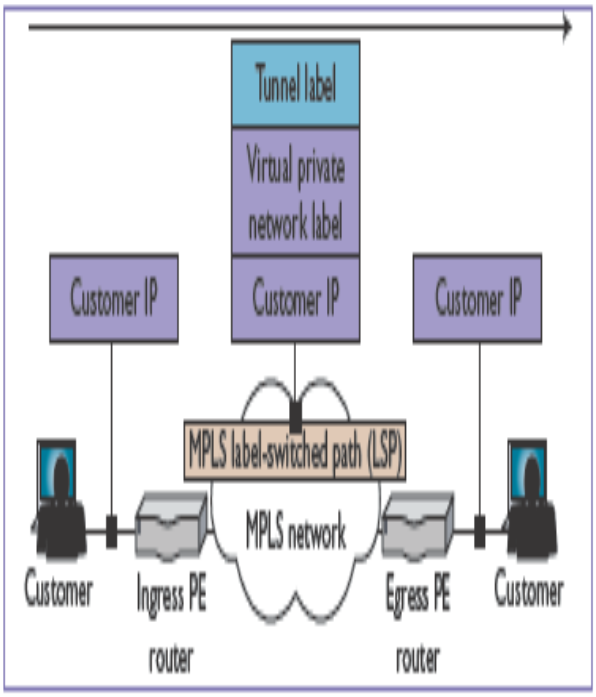

Figure 2 MPLS Tunneling Architecture

3. MPLS OPEARTION

In general, MPLS has two planes [6]:-

a) Control Plane: - The Control Plane is responsible for the routing information exchange and label distribution between adjacent devices. It uses standard routing protocols such OSPF routing, IS-IS and BGP to exchange information with other routers to build and IP forwarding table or label forwarding information base. It also needs label distribution protocols such as LDP.

b) Data Plane: - The Data Plane is responsible for forwarding packets according to the destination IP address or label using L-FIB managed by the control plane. The Data plane is a simple label based forwarding engine i.e independent of the type of routing protocol or label distribution protocol running on the control plane.

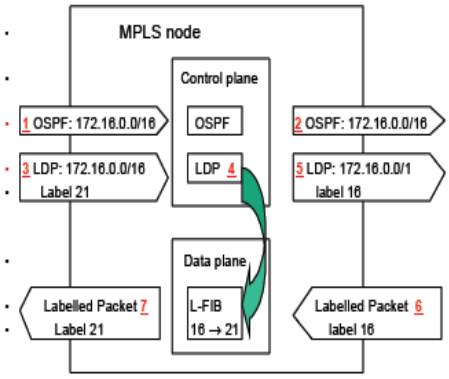

Figure 3 Functionality of Control and Data Plane

3.1 LDP Principle

MPLS network after establishing LSPs. For a given flow the LER acting as a entry point is called "Ingress LER" and the LER acting as exit point is referred as "Egress LER". A label in its simplest form identifies the path a packet should traverse. A label is carried or encapsulated in a layer-2 header along with the packet. The receiving router examines the packet for its label content to determine the next hop. On receiving a packet from non-MPLS domain the LER first analyzes the network layer header and decides "Forward Equivalence Class (FEC)" to which the packet belongs to and assigns one label to it. The FEC is a representation of a group of packets that share the same requirements for their transport.

4. IMPORTANCE OF MPLS OVER IP-BASED ROUTING

a) Congestion Awareness: COS support on the basis of Traffic or user is not possible in IP which eventually results in congested routes but MPLS overcomes this problem with FEC support also the possible solution provided by IP to overcome this problem is termed as load balancing but due to its simple criteria of dividing the traffic it suffers from scalability problem.

b) Scalability: IP routing has encountered the scalability issue due to routing mechanism .MPLS addresses enhances the shortcoming of load balancing in IP networks by introducing the concept of FEC which divides the different types of Traffic according to their requirement.

c) IP Route Recovery: When a link goes down in IP network its recovery speed depends upon 3 factors 1.Time taken by router to detect a link failure 2.Distributon of this information across the whole network 3.Calculation of new routing tables by all routers and finding alternate route for traffic **.**But MPLS route recovery is much more proficient than IP since it introduces the concept of Label stack.

d) MPLS based traffic engineering architecture: MPLS forms the packet forwarding component of the traffic engineering architecture. It directs a flow of IP packets along a pre-determined path across a network that is called label switched path (LSP). LSPs are simplex in nature. The creation of an LSP is accomplished by concatenation of one or more label switched hops. This allows a packet to traverse one label switching router (LSR) to another LSR in the MPLS domain. This type of LSR packet forwarding is based on label swapping. In label swapping, the label of an incoming packet is examined which is then used as an index in the MPLS forwarding table. Then the detailed knowledge of network topology and network loading is required to make traffic engineering decisions. Then finally, path selection is done. This path can either be strict or loose explicit route. An explicit route refers to the preconfigured sequence of LSRs that should be a part of the physical path of LSP. If all the LSRs are specified by the ingress LSR, the LSP is identified by a strict explicit route. If only some of the LSRs are specified, the LSP is described by a loose route.

5. WHY MPLS FOR TE

MPLS is seen as a hybrid solution, which encompasses the features of IP. The most telling feature of MPLS is its ability to separate Control and Data Plane. This effectively means that TE is entirely controlled by IP without any support of Layer 2 technologies, which contributes to its simplicity. MPLS plays an important role in the introduction of Next Generation Network (NGN). It helps in Intelligent Routing decisions. Unlike IP routing, which is based on the shortest path and destination IP addresses, techniques used by MPLS for routing are much sensible. Configuration of LSR/LER can be static or dynamic and during configuration traffic and path constraints are taken into account. In IP routing there are signaling protocols (OSPF, IS-IS), which distribute path information without considering path and traffic constraints. MPLS also needs an efficient signaling mechanism to share label information among all LSRs. MPLS supports different protocols for distributing constraint information across all LSRs. MPLS implementation of route recovery is much more proficient than IP [9].

5.1 MPLS traffic engineering forwarding and VFEC Forwarding

MPLS-TE forwarding strategy is totally different. With the same destination address but different source address, MPLS-TE will divide these two flows into different paths. Traditional single FEC forwarding and MPLS-TE all aims at a specific label which chooses a unique LSP path which is shown as follows:

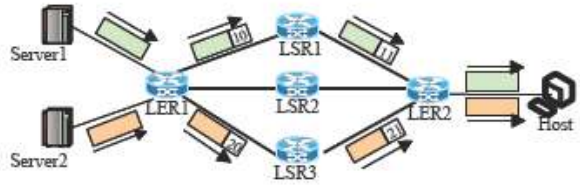

Figure 4 MPLS traffic engineering forwarding

So, there is another class of FEC which is called VFEC, stands for Variable Forwarding Equivalence Class that splits the same FEC into different available paths according to the current performance of various links [7]. It is assumed in the fig. below that the traffic from server 2 is very large. After the process of VFEC, packet with label 20 from server 2 is forwarded into two links: LER1-LSR2-LER2 and LER1-LSR3-LER2. The VFEC is not a variable label but a variable forwarding scheme for the same label. So, the same label is transmitted into two LSP paths concurrently.

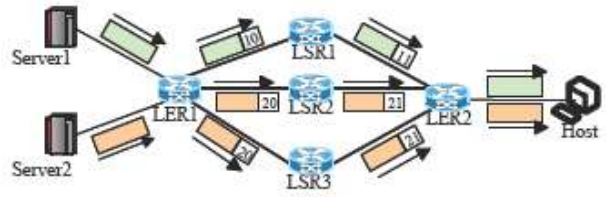

Figure 5 VFEC forwarding

5.2 Inter Service Provider: MPLS-VPN

MPLS VPNs are classified as network based IP VPNs. Customers exchange per site routing information by connecting to the nearest local provider edge router. The provider then uses the Multiprotocol Border Gateway Protocol (MP-BGP) to advertise these customer routes and associated labels called VPN labels to other PE routers attached to other customer sites within the same VPN. The customer routes, VPN labels and advertising PE router's IP address are stored on the receiving PE routers in separate per customer virtual routing and forwarding tables (VRFs). When a customer IP packet arrives, the ingress or local PE performs a lookup in the VRF table to determine the destination customer network. This yields a VPN label that represents the destination customer network and another label called the tunnel label that represents the LSP leading to the egress or remote PE router [2].

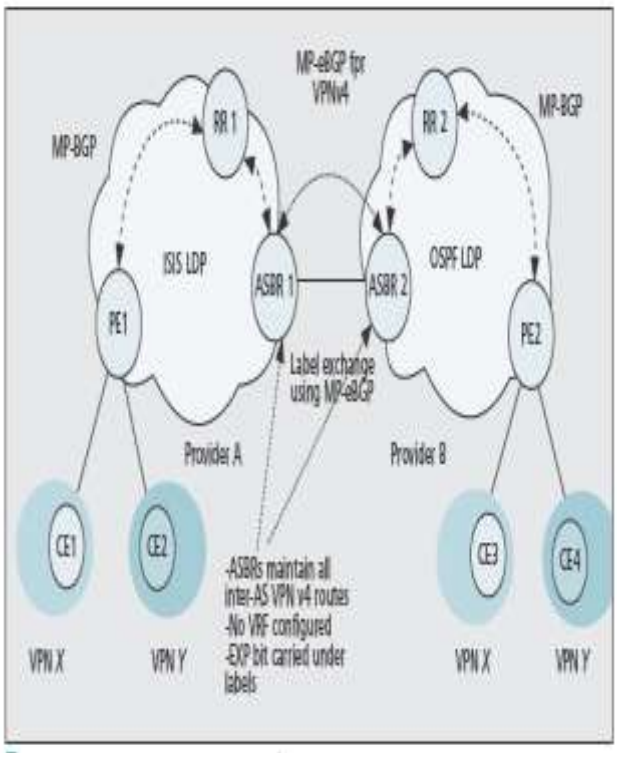

Figure 6 BGP/MPLS VPN inter-AS

This shows that upon receiving the packet the egress PE router removes the VPN label and forwards the native IP packet to its destination. A PE uses iBGP to redistribute labeled VPN routes to ASBRs directly or via a route reflector (RR). Each ASBR(Autonomous System Border Router) then uses eBGP to redistribute the routes to the peering ASBR in another AS, which will in turn redistribute the routes to the PEs in that AS. Each ASBR needs to maintain all VPN routes it has connections to. No VRF is required in this option. Multiprotocol eBGP (MP-eBGP) connectivity is shown in the figure above.

5.3 Benefits of the MPLS VPN

a) Scalability: A well executed MPLS based VPN deployment is capable of supporting tens of thousands of VPNs over the same network. MPLS based VPNs scale well because they do not require the full mesh, end to end site peering across the network.

b) Traffic Engineering: By deploying traffic engineering in the core, services provider network engineers can implement policies to help ensure the optimal traffic distribution and improve the over all network utilization. MPLS enables traffic engineering by allowing traffic to be directed through a specific path based on least cost routing, link utilization, latency, jitter and other factors.

6. GAP IN MPLS TECHNOLOGY: SECURITY

An attack on the control plane of a network is a doorway to attacking the data plane or even completely disabling the data plane traffic. It could also result in loss of user confidentiality

and prevention of new services. Varieties of Security Encryption Techniques are used for securing MPLS technology. There are various attacks which can break the MPLS technology. For example a brute force attack is a strategy used to break the encryption of data in MPLS Technology. It involves traversing the search space of possible keys until the correct key is found. The selection of an appropriate key length depends on the practical feasibility of performing a brute force attack. So Encryption Algorithms like AES , DES, TDES which is a part of IPSec are used to secure MPLS technology against various attacks. The AES standard comprises three block ciphers : AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael**.** Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The DES is a block cipher which is a form of shared secret encryption made up of 56 bit key size. Triple DES is simply another mode of DES operation. It takes three 64-bit keys for an overall key length of 192 bits.

7. CONCLUSION AND FUTURE WORK

The rapidly increasing volume of Internet traffic has forced ISPs to find the ways to increase the capacity of their networks. Those ISPs that have kept pace with time by transitioning to new backbone technologies have been successful in increasing their market share. So, for this MPLS is an emerging technology and by no means a perfect solution to current IP network problems. It provides much better Traffic Engineering capability than the other networks. MPLS operates in coordination with IP Routing and its main objective is to provide the speed of switching to Layer 3. Introduction of labels provides an effective alternative and evades the need of large routing table lookups and results in fast routing. However, the telling factor of MPLS is its ability to manage and classify the traffic in order to provide better utilization of resources. Hence, this technology is used to effectively resolve integration and traffic engineering issues in carrier networks. MPLS VPN provides benefits that service providers need urgently in their networks, such as scalability, manageability and reliability. But Security is the major issue in this Technology.

So, in the future work, we are targeting to implement some of the IPSec Encryption standards like AES, DES and Triple DES on the MPLS network in order to Overcome Security Gap Analysis of this Technology.

8. REFERENCES

[1] Khan. F., "Traffic Engineering with Multipoint Label Switching". E.Tech, 04 pp. 61-67, July 2004.

[2] Fang L.; Bita N.; Le R.; Miles J., "Interprovider IP- MPLS services: requirements, implementations, and Challenges". Communications Magazine, IEEE , vol.43, no.6, pp.119-128,June 2005.

[3] Daugherty B.; Metz C.," Multiprotocol label Switching and IP, Part1: MPLS VPNs over IP Tunnels". IEEE Internet Computing, pp. 68-72, May-June 2005.

[4] Azher I.; Aurengzeb M.; Masood K.," Virtual Private Network Implementation over Multiprotocol Label Switching". Engineering Sciences and Technology, pp. 1-5, Aug 2005.

[5] Peterkin R.; Ionescu D.,"A Hardware/Software Co-Design for RSVP-TE MPLS". Electrical and Computer Engineering, Canadian Conference on, pp.1409-1412, May 2006.

[6] Liwen He; Botham, P.," Pure MPLS Technology". Availability, Reliability and Security, ARES 08, Third International Conference on , pp.253-259, 4-7 March 2008.

[7] Han L.; Wang J.; Wang C.; Cai L.,"A Variable Forwarding Equivalence Class for MPLS Networks". Multimedia Information Networking and Security, MINES '09. International Conference on , pp.273-276, 18-20 Nov. 2009.

[8] Ramakrishnan, V.; Wargo, C.; John, S.,"GMPLS Network Security: Gap Analysis". ICNS Conference, 2008 IEEE Systems, pp. 1-7, 5-7 May 2008.

[9] Shah. S. A. A.; Ahmed. L.,"MPLS Feasibility for General & Core IP Networks using Open Source System". Second International on Electrical Engineering, pp. 1-6, March 2008.