E1-E2 (EB)

Chapter 2

MPLS VPN

Multi-Protocol Label Switching (MPLS VPN)

What is MPLS?

Multi Protocol Label Switching (MPLS) is a data-carrying mechanism in packet-switched networks. It operates at a layer that is generally considered to lie between traditional definitions of Layer 2 (data link layer) and Layer 3 (network layer or IP Layer), and thus MPLS is often referred to as a "Layer 2.5" protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients, which provide a datagram service model. It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, SONET, Frame relay and Ethernet frames. The IP network has emerged as the network for providing converged, differentiated classed of services to user with optimal use of resources and also to address the issues related to Class of service (CoS) and Quality of Service (QoS). MPLS is the technology that addresses all the issues in the most efficient manner. MPLS is a packet-forwarding technology that uses labels to make data forwarding decisions.

What is a MPLS header?

MPLS works by prefixing packets with an MPLS header, containing one or more 'labels'. This is called a label stack. Each label stack entry contains four fields:-

- 20-bit label value (This is MPLS Label)
- 3-bit Experimental field used normally for providing for QoS (Quality of Service)
- 1-bit bottom of stack flag. If this is 1, signifies that the current label is the last in the stack.
- 8-bit TTL (time to live) field.

Various Routing function units & Routers in MPLS

Routing function in MPLS can be described on the basis of some units which are defined as follows:

Label:

A label is an identifier which indicates the path a packet should traverse. Label is carried along with the packet. The receiving router examines the packet for its label content to determine the next hop. Once a packet has been labeled, the rest of the journey of the packet through the backbone is based on label switching. Since every intermediate router has to look in to the label for routing the decision making at the level of router becomes fast.

Label Creation:

Every entry in routing table (build by using any IGP protocol) is assigned a unique 20-bit label.

Swap:

Every incoming label is replaced by a new outgoing label (As per the path to be followed) and the packet is forwarded along the path associated with the new label.

Push:

A new label is pushed on top of the packet, effectively "encapsulating" the original IP packet in a layer of MPLS.

POP:

The label is removed from the packet effectively "de-encapsulating". If the popped label was the last on the label stack, the packet "leaves" the MPLS tunnel.

LER:

A router that operates at the edge of the access network and MPLS network LER performs the PUSH and POP functions and is also the interface between access and MPLS network, commonly know as Edge router.

LSR:

An LSR is a high-speed router device in the core of an MPLS network, normally called Core routers. These routers perform swapping functions and participate in the establishment of Label Switch Path (LSP)

Ingress / Egress Routers:

The routers receiving the incoming traffic or performing the first PUSH function are ingress routers and routers receiving the terminating traffic or performing the POP function are Egress routers. The same router performs both functionality i.e. Ingress and Egress. The routers performing these functions are LER.

FEC:

The forward equivalence class (FEC) is a representation of a group of packets that share the same requirements for their transport. All packets in such a group are provided the same treatment en route to the destination. As opposed to conventional IP forwarding, in MPLS, the assignment of a particular packet to a particular FEC is done just once, as the packet enters the network at the edge router.

MPLS functions:

MPLS performs following functions:-

- Specifies mechanisms to manage traffic flow of various granularities, such as flows between different hardware, machines, or even flows between different applications.
- MPLS remains independent of the Layer-2 & layer-3 protocols. Meaning thereby that label encapsulating the data packet does not depend upon layer 3 /layer 2 protocol of data. This justifies the name as multi protocol label switching.
- Provides a means to map IP addresses to simple, fixed-length labels used by different packet-forwarding and packet-switching technologies
- Interfaces to existing routing protocols such as resource reservation protocol (RSVP) and open shortest path first (OSPF).
- Supports the IP, ATM, and frame- relay Layer-2 protocols.

Label Distribution Protocol (LDP):

The LDP is a protocol for the distribution of label information to LSRs in a MPLS networks. It is used to map FECs to labels, which, in turn, create LSP. LDP sessions are established between LDP peers in the MPLS network (not necessarily adjacent).

MPLS Operation :

The following steps must be taken for a data packet to travel through an MPLS domain:

- Label creation and distribution
- Table creation at each router
- Label-switched path creation
- Label insertion/table lookup
- Packet forwarding.

The source sends its data to the destination. In an MPLS domain, not all of the source traffic is necessarily transported through the same path. Depending on the traffic characteristics, FEC s different LSP s could be created for packets with different CoS requirements.

In Figure 1, LER1 is the ingress and LER4 is the egress router.

LSP Creation & and Packet forwarding through an MPLS Domain

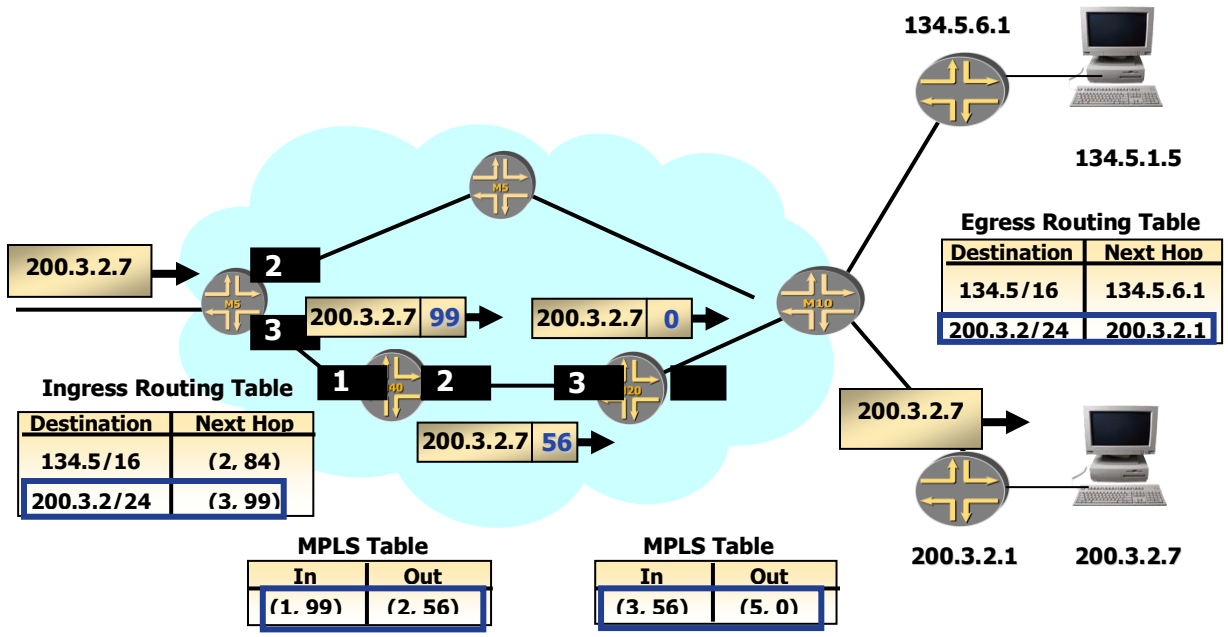

Figure-1

Tunnelling in MPLS

A unique feature of MPLS is that it can control the entire path of a packet without explicitly specifying the intermediate routers. It does this by creating tunnels through the intermediary routers that can span multiple segments. This concept is used for provisioning MPLS – based VPNs.(Figure-2)

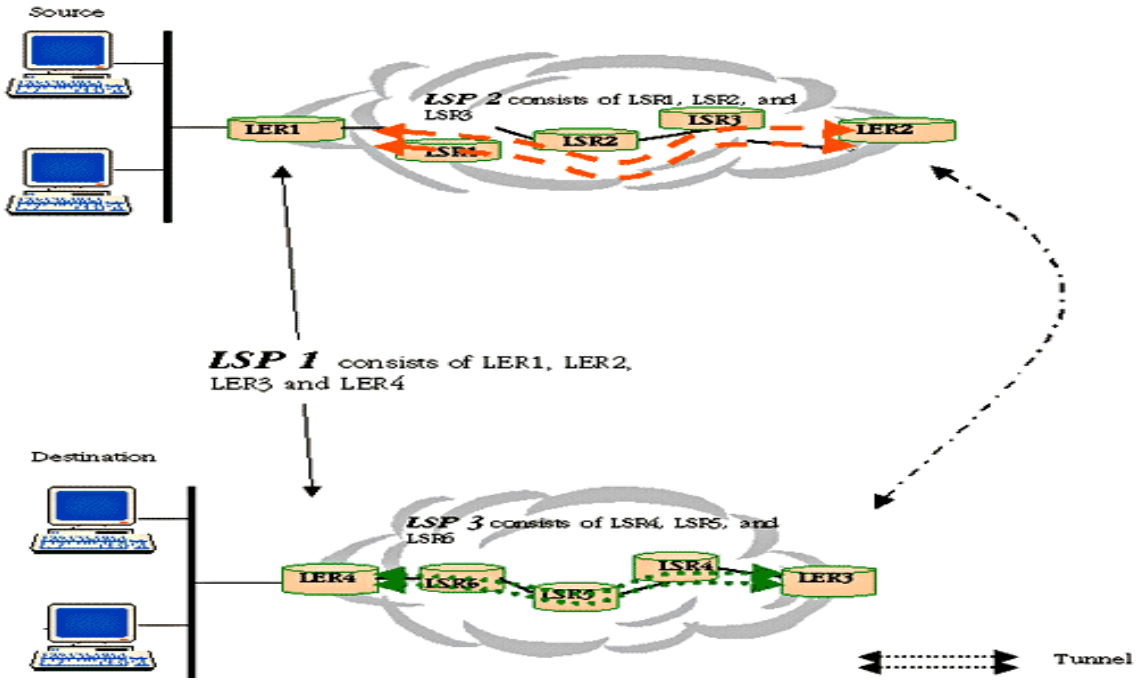

Figure-2

MPLS Applications

MPLS addresses today's network backbone requirements effectively by providing a standards-based solution that accomplishes the following:

- Improves packet-forwarding performance in the network.
- MPLS enhances and simplifies packet forwarding through routers using Layer-2 switching paradigms.
- MPLS is simple which allows for easy implementation.
- MPLS increases network performance because it enables routing by switching at wire line speeds.
- Supports QoS and CoS for service differentiation.
- MPLS uses traffic-engineered path setup and helps achieve service-level guarantees.
- MPLS incorporates provisions for constraint-based and explicit path setup.
- Supports network scalability.
- MPLS can reuse existing router/ATM switch hardware, effectively joining the two disparate networks.
- Builds interoperable networks
- MPLS is a standards-based solution.
- MPLS helps build scalable VPNs with traffic-engineering capability.

MPLS VPN

MPLS technology is being widely adopted by service providers worldwide to implement VPNs to connect geographically separated customer sites. VPNs were originally introduced to enable service providers to use common physical infrastructure to implement emulated point-to-point links between customer sites. A customer network implemented with any VPN technology would contain distinct regions under the customer's control called the *customer sites* connected to each other via the *service provider (SP)* network. In traditional router-based networks, different sites belonging to the same customer were connected to each other using dedicated point-to-point links. The cost of implementation depended on the number of customer sites to be connected with these dedicated links. A full mesh of connected sites would consequently imply an exponential increase in the cost associated. Frame Relay and ATM were the first technologies widely adopted to implement VPNs.

These networks consisted of various devices, belonging to either the customer or the service provider, that were components of the VPN solution. Generically, the VPN realm would consist of the following regions:

Customer network:

Consisted of the routers at the various customer sites. The routers connecting individual customers' sites to the service provider network were called *customer edge (CE)* routers.

Provider network:

Used by the service provider to offer dedicated point-to-point links over infrastructure owned by the service provider. Service provider devices to which the CE routers were directly attached were called *provider edge (PE)* routers. In addition, the service provider network might consist of devices used for forwarding data in the backbone called *provider (P)* routers.

Classification of VPN Implementations

Depending on the service provider's participation in customer routing, the VPN implementations can be classified broadly into one of the following:

- Overlay model
- Peer-to-peer model

Overlay model

- Service provider doesn't participate in customers routing, only provides transport to customer data using virtual point-to-point links. As a result, the service provider would only provide customers with virtual circuit connectivity at Layer 2.
- If the virtual circuit was permanent or available for use by the customer at all times, it was called a permanent virtual circuit (PVC).
- If the circuit was established by the provider on-demand, it was called a switched virtual circuit (SVC).
- The primary drawback of an Overlay model was the full mesh of virtual circuits between all customer sites for optimal connectivity. It resembles the physical mesh connectivity in case of leased lines. Overlay VPNs were initially implemented by the SP by providing either Layer 1 (physical layer) connectivity or a Layer 2 transport circuit between customer sites.

In the Layer 1 implementation, the SP would provide physical layer connectivity between customer sites, and the customer was responsible for all other layers. In the Layer 2 implementation, the SP was responsible for transportation of Layer 2 frames (or cells) between customer sites, which was traditionally implemented using either Frame Relay or ATM switches as PE devices. Therefore, the service provider was not aware of customer routing or routes.

Later, overlay VPNs were also implemented using VPN services over IP (Layer 3) with tunneling protocols like L2TP, GRE, and IPSec to interconnect customer sites. In all cases, the SP network was transparent to the customer, and the routing protocols were run directly between customer routers.

Peer-to-peer model

The peer-to-peer model was developed to overcome the drawbacks of the Overlay model and provide customers with optimal data transport via the SP backbone. Hence, the service provider would actively participate in customer routing. In the peer-to-peer model, routing information is exchanged between the customer routers and the service provider routers, and customer data is transported across the service provider's core, optimally. Customer routing information is carried between routers in the provider network (P and PE routers) and customer network (CE routers). The peer-to-peer model, consequently, does not require the creation of virtual circuits. The CE routers exchange routes with the connected PE routers in the SP domain. Customer routing information is propagated across the SP backbone between PE and P routers and identifies the optimal path from one customer site to another.

Dial VPN Service

Mobile users of a corporate customer need to access their Corporate Network from remote sites. Dial VPN service enables to provide secure remote access to the mobile users of the Corporate. Dial VPN service, eliminates the burden of owning and maintaining remote access servers, modems, and phone lines at the Corporate Customer side. Currently accessible from PSTN (127233) & ISDN (27225) also from Broadband.

MPLS VPN Architecture and Terminology

In the MPLS VPN architecture, the edge routers carry customer routing information, providing optimal routing for traffic belonging to the customer for inter-site traffic. The MPLS-based VPN model also accommodates customers using overlapping address spaces, unlike the traditional peer-to-peer model in which optimal routing of customer traffic required the provider to assign IP addresses to each of its customers (or the customer to implement NAT) to avoid overlapping address spaces. MPLS VPN is an implementation of the peer-to-peer model; the MPLS VPN backbone and customer sites exchange Layer 3 customer routing information, and data is forwarded between customer sites using the MPLS-enabled SP IP backbone.

The MPLS VPN domain, like the traditional VPN, consists of the customer network and the provider network. The MPLS VPN model is very similar to the dedicated PE router model in a peer-to-peer VPN implementation. However, instead of deploying a dedicated PE router per customer, customer traffic is isolated on the same PE router that provides connectivity into the

service provider's network for multiple customers. The components of an MPLS VPN shown in Figure are highlighted next.

Figure-3 MPLS VPN Network Architecture

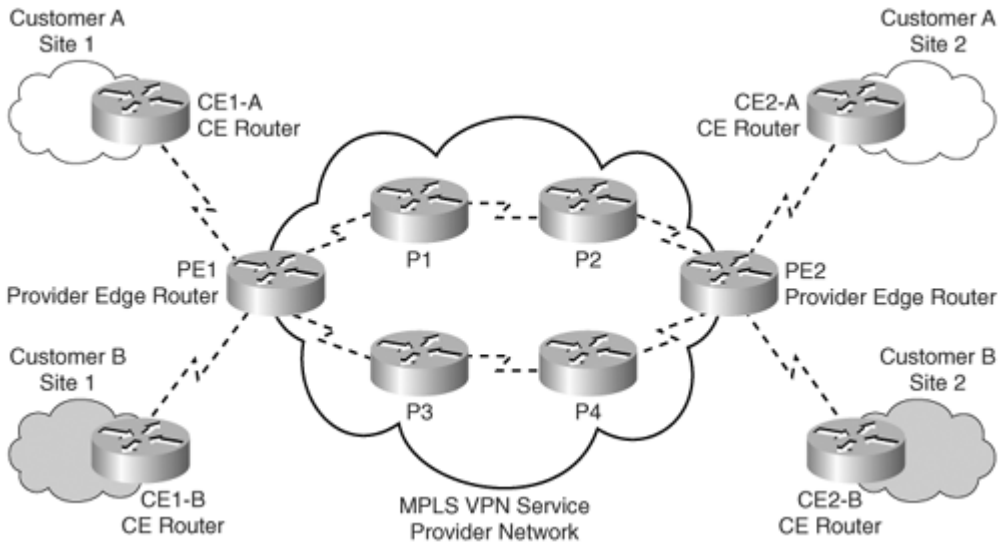

Figure-3

The main components of MPLS VPN architecture are:

Customer network:

which is usually a customer-controlled domain consisting of devices or routers spanning multiple sites belonging to the customer. In Figure, the customer network for Customer A consists of the routers CE1-A and CE2-A along with devices in the Customer A sites 1 and 2.

CE routers:

which are routers in the customer network that interface with the service provider network. In Figure , the CE routers for Customer A are CE1-A and CE2-A, and the CE routers for Customer B are CE1-B and CE2-B. Provider network, which is the provider controlled domain consisting of provider edge and provider core routers that connect sites belonging to the customer on a shared infrastructure. The provider network controls the traffic routing between sites belonging to a customer along with customer traffic isolation.

In Figure, the provider network consists of the routers PE1, PE2, P1, P2, P3, and P4.

PE routers:

which are routers in the provider network that interface or connect to the customer edge routers in the customer network. PE1 and PE2 are the provider edge routers in the MPLS VPN domain for customers A and B. P routers, which are routers in the core of the provider network that interface with either other provider core routers or provider edge routers. Routers P1, P2, P3, and P4 are the provider routers.

Advantages of MPLS over other technologies

BSNL's primary objectives in setting up the BGP/MPLS VPN network are:

- Provide a diversified range of services (Layer 2, Layer 3 and Dial up VPNs) to meet the requirements of the entire spectrum of customers from Small and Medium to Large business enterprises and financial institutions.
- Make the service very simple for customers to use even if they lack experience in IP routing.
- Make the service very scalable and flexible to facilitate large-scale deployment.
- Provide a reliable and amenable service.
- Offering SLA to customers.
- Capable of meeting a wide range of customer requirements, including security, quality of Service (QOS) and any-to-any connectivity.
- Capable of offering fully managed services to customers.
- Allow BSNL to introduce additional services such as bandwidth on demand etc over the same network.

MPLS Tariff

TARIFF OF MPLS BASED IP-VPN SERVICE

http://bsnl.co.in/service/mplsvpn_tariff.htm

Tariff of MPLS VPN and IP VPN Services in Rs. :

Particular	64 Kbps	128 Kbps	192 Kbps	256 Kbps	384 Kbps	512 Kbps
Gold	63000	105000	138000	178000	221000	301000
Silver	52000	88000	116000	149000	185000	249000
Bronze	43000	72000	95000	122000	162000	219000
IP VPN	35000	60000	79000	102000	137000	186000

Particular	768 Kbps	1 Mbps	2 Mbps	8 Mbps	34 Mbps	45 Mbps
Gold	368000	423000	610000	2134000	3902000	4389000
Silver	306000	353000	487000	1706000	3119000	3509000
Bronze	267000	305000	355000	1242000	2272000	2556000
IP VPN	229000	263000	294000	1028000	1880000	2115000

Tariff for higher bandwidth i.e 100Mbps, STM1, 1 Gbps and 2.5Gbps

Particular	100mbps	STM1 (155 Mbps)	1 Gbps	2.5Gbps
Gold	8079500	11770000	56496000	101222000
Silver	6459500	9410000	45168000	80926000
Bronze	4705000	6854000	32899200	58944400
Best Effort	3893500	5672000	27225600	48779200

- Committed Data Rate in Bronze category - The bandwidth of Bronze category would be restricted to 50% of bandwidth. However, the minimum B/W of 25% B/W will be committed to Bronze customers.
- Discount on MPLS VPN ports - It has been decided to give multiple port discounts on the total number of ports hired across the country as given below. **It may be noted that multiple ports are not required to be located in a city for offering this discount:**

No. of Ports	Existed discount on VPN Ports on Graded basis	Revised discount on VPN Ports on Non-graded basis
1 to 4 ports	0%	0%
5 to 25 ports	10%	5%

26 to 50 ports	15%	10%
51 to 100 ports	20%	10%
101 to 150 ports	20%	15%
More than 150 ports	20%	20%

- Volume based discount on MPLS VPN Service - Annual volume based discount on graded basis may be given to all customers as under:

Annual Revenue(in Rs.) on MPLS VPN Service per annum	Volume based Discount on Graded basis
Upto Rs.50 lakhs	No discount
Rs.50 lakhs to 1 Crore	5%
Rs.1 Crore to 2 Crore	7.5%
Rs.2 Crore to 5 Crore	10%
More than Rs.5 Crore	15%

- Shifting charges of MPLS VPN & IP VPN Port - Rs.2000/- per port.
- Minimum hiring period for MPLS VPN and IP VPN ports - One year.
- Upgradation of port to higher Bandwidth – No charges to be levied for upgradation to higher bandwidth. The rent for the lower BW port to be adjusted on pro-rata basis.
- Provision of last mile on R&G/ Special construction basis - The charges to be levied as per prevalent R&G/ Special construction terms.

- Local Lead charges : Included in Port Charges, if these are within Local Area of Telephone system of a City/Town (Virtual Nodes).
- All charges are exclusive of Service Tax.

Tariff for Postpaid dial-up VPN Service from MPLS VPN customers(w.e.f 1st May, 2007):

I. Duration Based Plans:

Particulars	Number of Dial-in Users				
	5 Users	25 Users	50 Users	100 Users	250 users
Security Deposit (Rs.)	10,000	50,000	1,00,000	2,00,000	5,00,000
Activation charges(one time) Rs.	500	2,500	5,000	10,000	10,000
Monthly fixed charges(Rs.)	6,000	30,000	60,000	1,20,000	3,00,000
Monthly free usages (equivalent to Rs.)	6,000	30,000	60,000	1,20,000	3,00,000
Credit Limit (Rs.)	10,000	50,000	1,00,000	2,00,000	5,00,000
Usage Charges (Rs. per hour)					
PSTN	16	16	14	12	10
ISDN (64K)	20	20	18	16	14
Other Charges per User per month (Rs.)					

CLI Restriction Deactivation	10	10	10	10	10
Time of Day access Restriction	10	10	10	10	10
Details of child usages	5	5	5	5	5
Source NAP restriction activation	5	5	5	5	5

II. Volume Based Plans:

Particulars	Number of Dial-in Users				
	5 Users	25 Users	50 Users	100 Users	250 users
Security Deposit (Rs.)	10,000	50,000	1,00,000	2,00,000	5,00,000
Activation charges(one time) Rs.	500	2,500	5,000	10,000	10,000
Monthly fixed charges(Rs.)	6,000	30,000	60,000	1,20,000	3,00,000
Monthly free usages (equivalent to Rs.)	6,000	30,000	60,000	1,20,000	3,00,000
Credit Limit (Rs.)	10,000	50,000	1,00,000	2,00,000	5,00,000
Usage Charges (Rs. per MB)					
PSTN	1.00	1.00	0.80	0.70	0.60

ISDN (64K)	0.75	0.75	0.65	0.55	0.50
Other Charges per User per month (Rs.)					
CLI Restriction Deactivation	10	10	10	10	10
Time of Day access Restriction	10	10	10	10	10
Details of child usages	5	5	5	5	5
Source NAP restriction activation	5	5	5	5	5

Other terms and conditions :

- Monthly Fixed charges are payable in advance;
- Minimum 10 MPLS leased line ports should be in VPN before Postpaid dial-up facility is allowed;
- Account will be deactivated once credit limit is crossed and fresh Action Charge will be payable ;
- PSTN/ ISDN rentals and access charges will be extra;
- Service Tax will be extra.

FAQ's Regarding BSNL MPLS VPN can be seen at

- http://bsnl.co.in/faq/mplsvpn_faq.htm
- http://www.iec.org/online/tutorials/

Questions

1) Write MPLS header format
2) Write the two models of VPN
3) Write the advantages of MPLS VPN
4) Write the advantages of MPLS
5) Write some applications of MPLS