

## 5 MPLS VPN

### 5.1 LEARNING OBJECTIVE

This chapter covers the concept of MPLS. MPLS (Multi Protocol Label Switching) is a mechanism that switches traffic based on labels instead of routing traffic. MPLS VPN is a popular technique to build VPNs for customers over the MPLS provider network.

After reading the chapter the participants will be able to understand the concept of LSP, traffic engineering, and loop detection.

### 5.2 INTRODUCTION

Multi Protocol Label Switching (MPLS) is an efficient encapsulation mechanism that uses “Labels” appended to packets (IP packets, AAL5 frames) for transport of data. MPLS packets can run on other layer 2 technologies such as ATM, FR, PPP, POS, Ethernet. Other layer 2 technologies can be run over an MPLS network. Labels can be used as designators. For example—IP prefixes, ATM VC, or a bandwidth guaranteed path.

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 data-gram 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.

### 5.3 DRAWBACKS OF TRADITIONAL IP FORWARDING

- Routing protocols are used to distribute Layer 3 routing information and therefore every router may need full Internet routing information (more than 100,000 routes).
- Forwarding is based on the destination address only.
- Routing lookups are performed on every hop that slows down the forwarding operation.
- Packets can't be given priority. Though TOS field is there in IP packets through which priority can be given to packets but routers are designed to bypass the TOS field.
- Layer 2 devices have no knowledge of Layer 3 routing information —virtual circuits must be manually established.

### 5.4 MPLS ADVANTAGES

1. Specifies mechanisms to manage traffic flow of various granularities, such as flows between different hardware, machines, or even flows between different applications.

2. Create new services via flexible classification
3. Provides the ability to setup bandwidth guaranteed paths
4. Enable ATM switches to act as routers
5. 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.
6. Provides a means to map IP addresses to simple, fixed-length labels used by different packet-forwarding and packet-switching technologies
7. Interfaces to existing routing protocols such as resource reservation protocol (RSVP) and open shortest path first (OSPF).
8. Supports the IP, ATM, and frame- relay Layer-2 protocols.
9. MPLS gives network operators a great deal of flexibility to divert and route traffic around link failures, congestion, and bottlenecks.
10. From a Quality of Service (QoS) standpoint, ISPs will better be able to manage different kinds of data streams based on priority and service plan. For instance, those who subscribe to a premium service plan, or those who receive a lot of streaming media or high-bandwidth content can see minimal latency and packet loss.
11. Enable ATM switches to act as routers

## 5.5 MPLS HEADER

### 5.5.1 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.

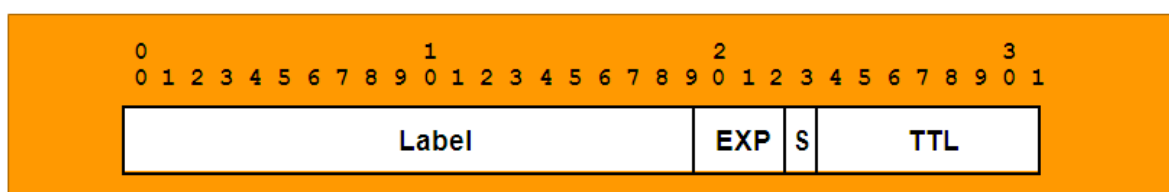


Fig:1 MPLS Header format

### 5.5.2 MPLS Label Stack

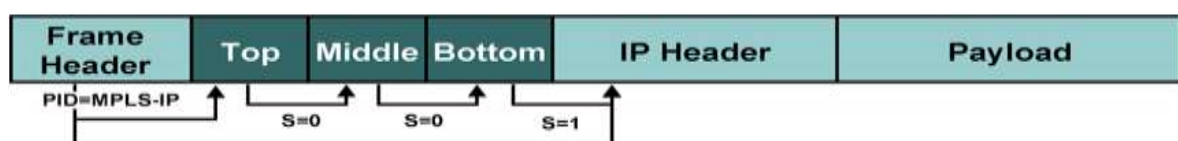


Fig:2 MPLS Label Stack

- Protocol identifier in a Layer 2 header specifies that the payload starts with a label (labels) and is followed by an IP header.
- Bottom-of-stack bit indicates whether the next header is another label or a Layer 3 header.
- Receiving router uses the top label only.
- Usually only one label is assigned to a packet.
- The following scenarios may produce more than one label:
  - MPLS VPNs (two labels: The top label points to the egress router and the second label identifies the VPN.)
  - MPLS TE (two or more labels: The top label points to the endpoint of the traffic engineering tunnel and the second label points to the destination.)
  - MPLS VPNs combined with MPLS TE (three or more labels.)

## 5.6 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 (built 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 known 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.

## 5.7. BASIC MPLS OPERATION

When packets enter a MPLS-based network, Label Edge Routers (LERs) give them one or more labels (identifiers). These labels not only contain information based on the routing table entry (i.e., destination, bandwidth, delay, and other metrics), but also refer to the IP header field (source IP address), Layer 4 socket number information, and differentiated service.

Once this classification is complete and mapped, different packets are assigned to corresponding Labeled Switch Paths (LSPs), where Label Switch Routers (LSRs) place outgoing labels on the packets. With these LSPs, network operators can divert and route traffic based on data-stream type and Internet-access customer

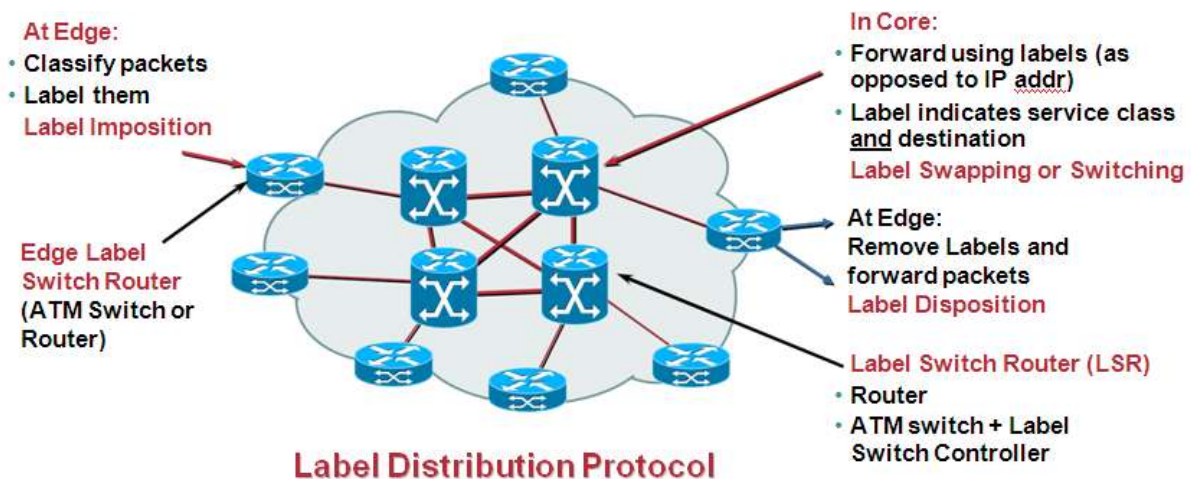
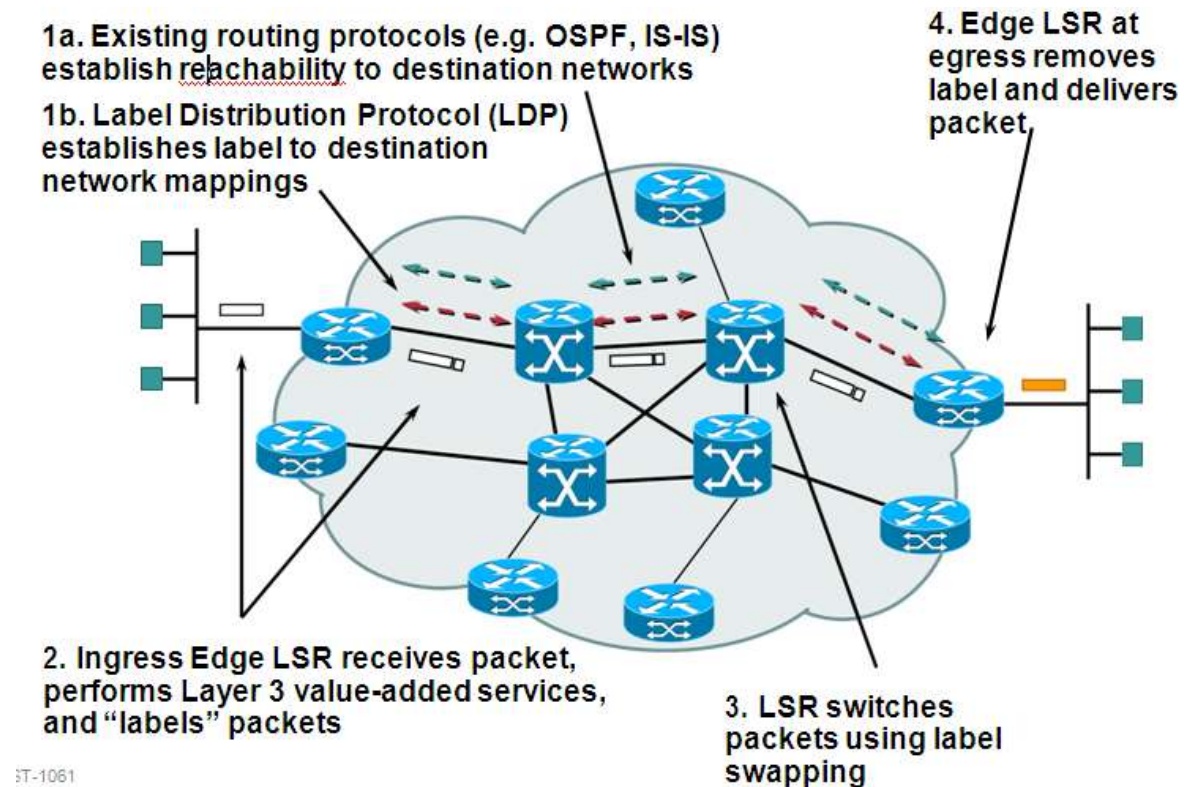


Fig. 3: LDP



**Fig: 4 Forwarding of Packets in MPLS network**

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

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

## 5.8. MPLS ROUTER FUNCTIONALITY

MPLS Router functionality is divided into two major parts

**5.8.1 Control plane:** Exchanges Layer 3 routing information and labels. Control plane contains complex mechanisms to exchange routing information, such as OSPF, EIGRP, IS-IS, and BGP, and to exchange labels, such as TDP, LDP, BGP, and RSVP.

**5.8.2 Data plane:** Forwards packets based on labels. Data plane has a simple forwarding engine.

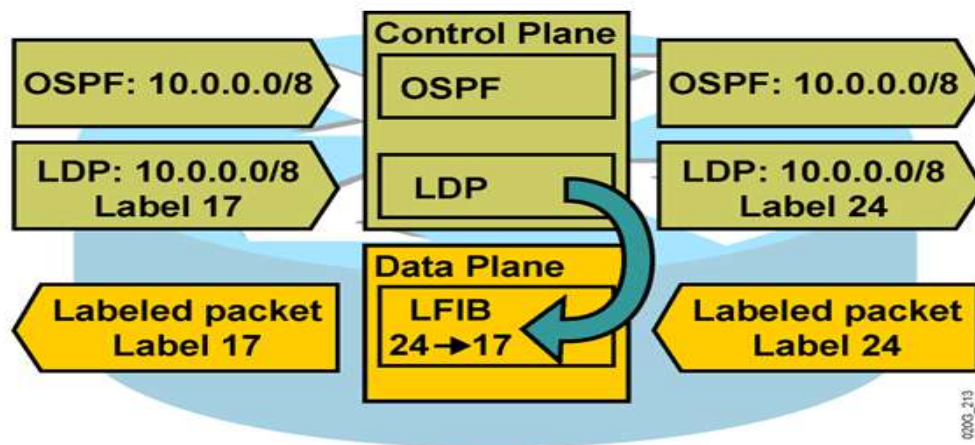


Fig:5 Control plane And Data plane

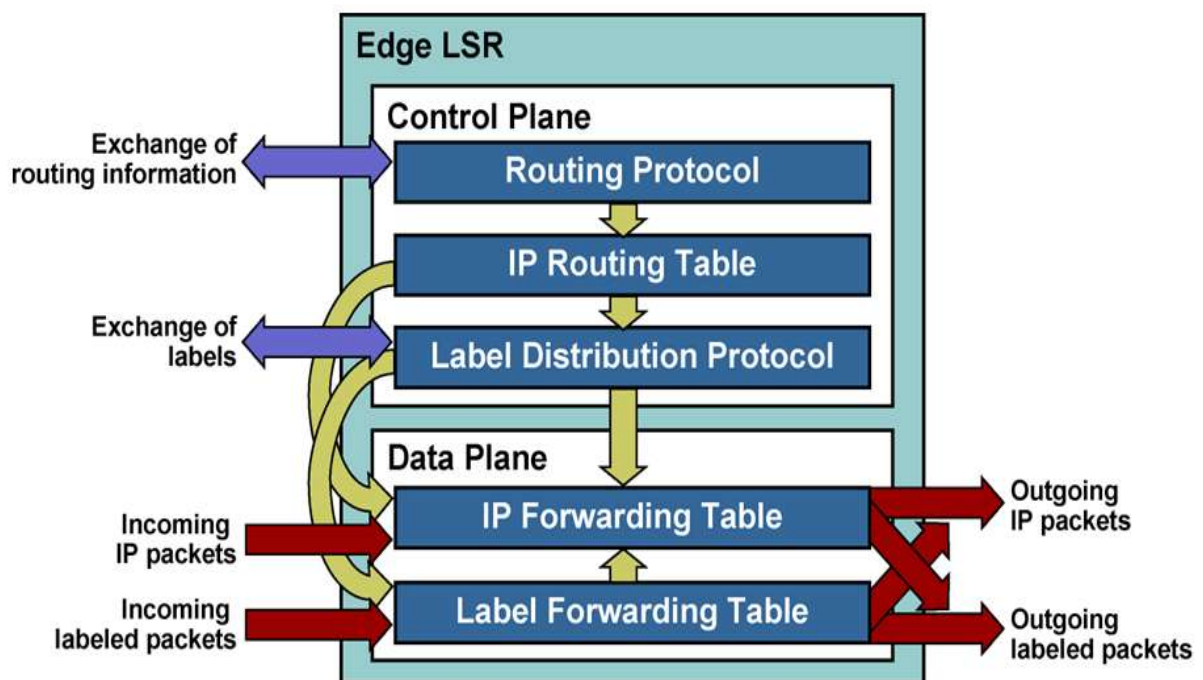


Fig:6 Architecture of LSR



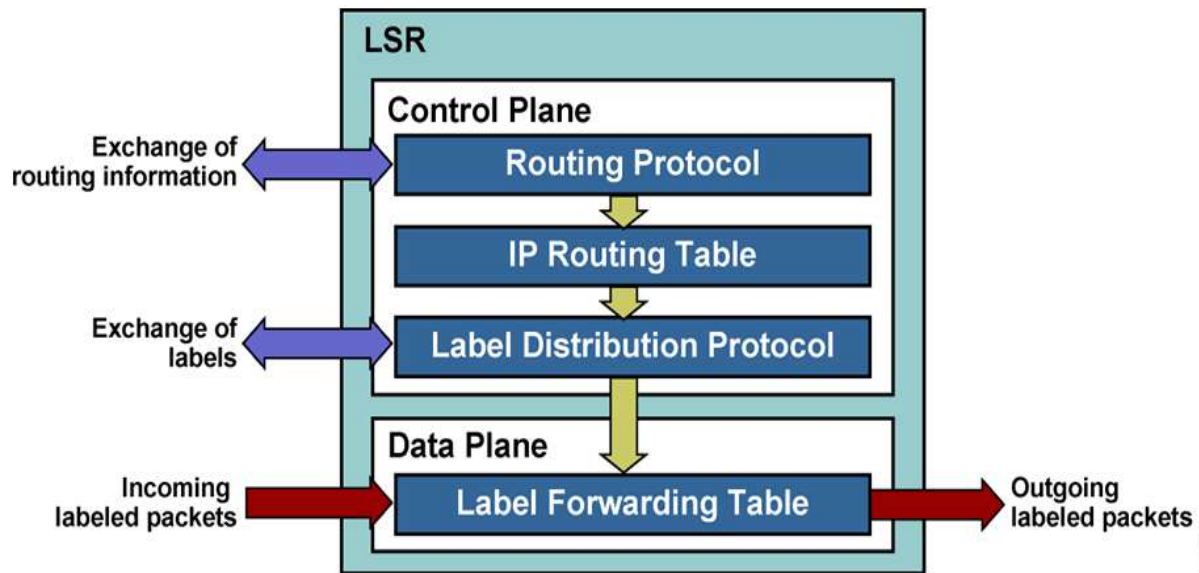


Fig:7 Label Switch Router

## 5.9. LABEL DISTRIBUTION AND FORWARDING OF PACKETS IN MPLS NETWORKS

- OSPF, IS-IS, BGP are needed in the network
- They provide reachability
- Label distribution protocols distribute labels for - prefixes advertised by unicast routing protocols using Either a dedicated Label Distribution Protocol (LDP, Extending existing protocols like BGP to distribute Labels
- Defined in RFC 3035 and 3036.
- It Used to distribute Labels in a MPLS network, Forwarding Equivalence Class( How packets are mapped to LSPs (Label Switched Paths)), Advertise Labels per FEC, Reach destination a.b.c.d with label x and Discovery

### 5.9.1 Router Example: Forwarding Packets

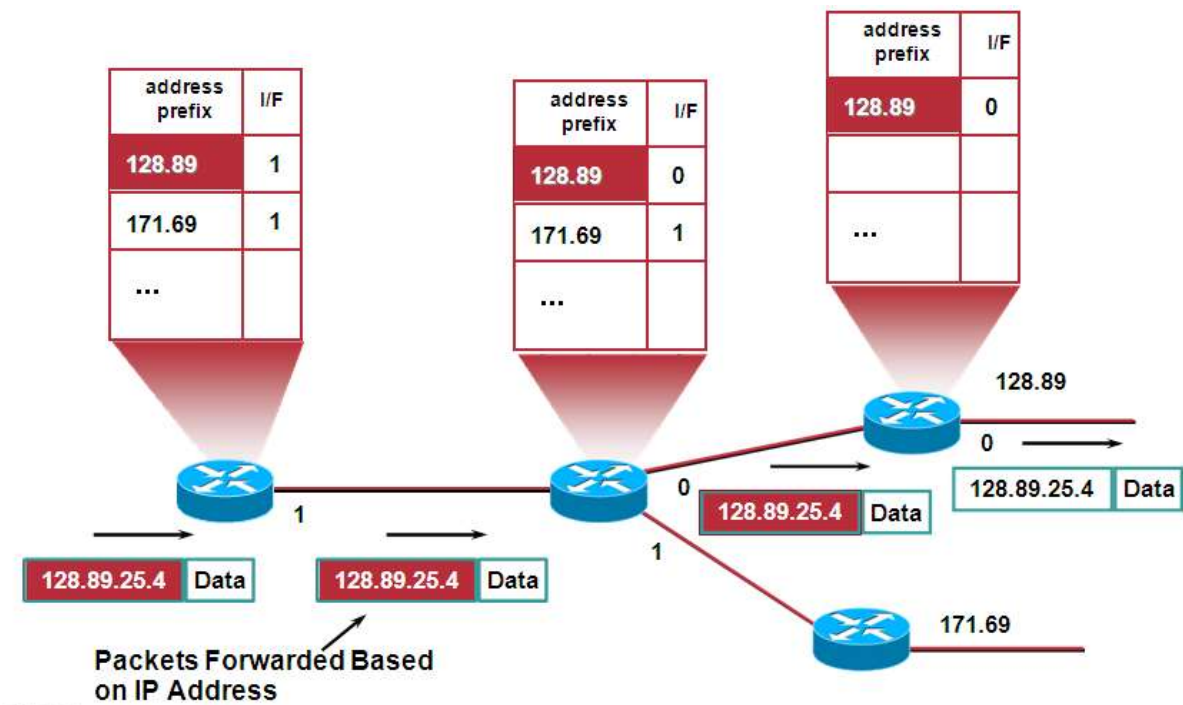


Fig:8 Packet Forwarding

### 5.9.2 MPLS Example: Routing Information

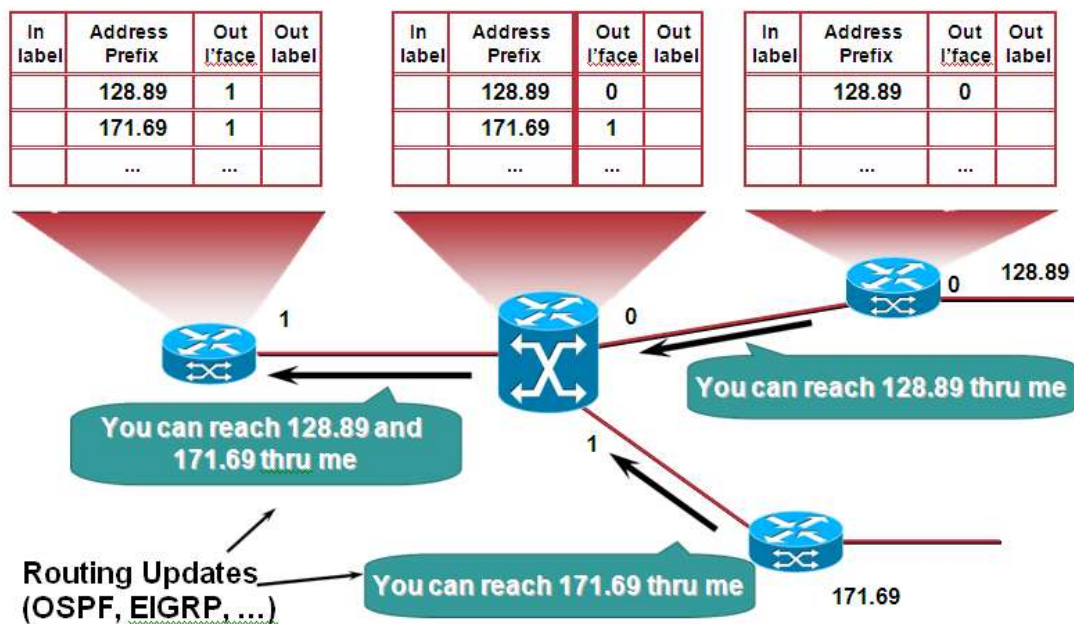


Fig:9 Routing Updates



### 5.9.3 MPLS Example: Assigning Labels

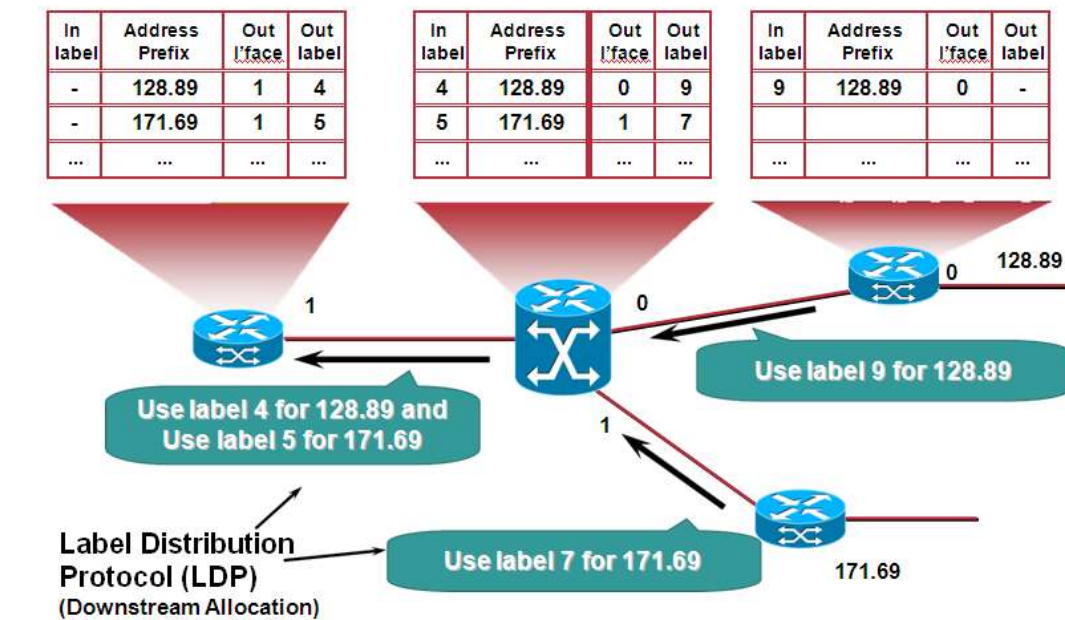


Fig:10 Lable Distribution

### 5.9.4 MPLS Example: Forwarding packets

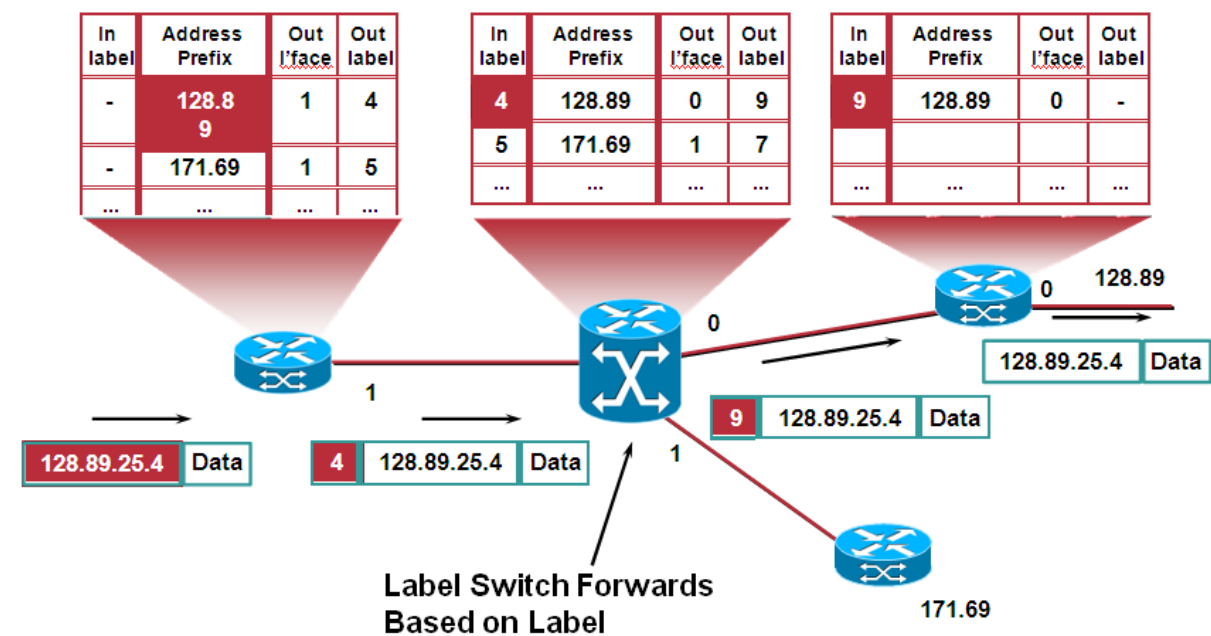


Fig:11 Labeled Packet Forwarding

## 5.10. MPLS LABEL DISTRIBUTION PROTOCOLS

MPLS architecture does not mandate a single method of signaling for label distribution. Existing routing protocols, such as the border gateway protocol (BGP), have been enhanced to piggyback the label information within the contents of the protocol. The RSVP has also been extended to support piggybacked exchange of labels. A summary of the various schemes for label exchange is as follows:

- **LDP**—maps unicast IP destinations into labels
- **RSVP, CR-LDP**—used for traffic engineering and resource reservation
- **protocol-independent multicast (PIM)**—used for multicast states label mapping
- **BGP**—external labels (VPN)

The Internet Engineering Task Force (IETF) has also defined a new protocol known as the label distribution protocol (LDP) for explicit signaling and management of the label space. Extensions to the base LDP protocol have also been defined to support explicit routing based on QoS and CoS requirements. These extensions are captured in the constraint-based routing (CR)–LDP protocol definition. It is used to map FECs to labels, which, in turn, create LSPs. LDP sessions are established between LDP peers in the MPLS network (not necessarily adjacent)

### 5.10.1 LDP (Label Distribution Protocol)

LDP Protocol has the following functions:

- Neighbor discovery  
Discover directly attached Neighbors—pt-to-pt links (including Ethernet)  
Establish a session  
Exchange prefix/FEC and label information
- Extended Neighbor Discovery  
Establish peer relationship with another router that is not a neighbor  
Exchange FEC and label information  
May be needed to exchange service labels

### 5.10.2 TDP (Tag Distribution Protocol)

Tag Distribution Protocol—Cisco proprietary  
Pre-cursor to LDP  
Used for Cisco Tag Switching

- TDP and LDP supported on the same device  
Per neighbor/link basis  
Per target basis  
LDP is a superset of TDP  
Uses the same label/TAG  
Has different message formats

### 5.10.3 Other Label Distribution Protocol – BGP

- Used in the context of MPLS VPNs
- Need multiprotocol extensions to BGP
- Routers need to be BGP peers
- 

The peersexchange the following types of LDP messages:

- **discovery messages**—announce and maintain the presence of an LSR in a network
- **session messages**—establish, maintain, and terminate sessions between LDP peers
- **advertisement messages**—create, change, and delete label mappings for FECs
- **notification messages**—provide advisory information and signal error information

## 5.11. SETTING UP LABEL-SWITCHED PATHS (LSPS)

MPLS provides the following two options to set up an LSP:

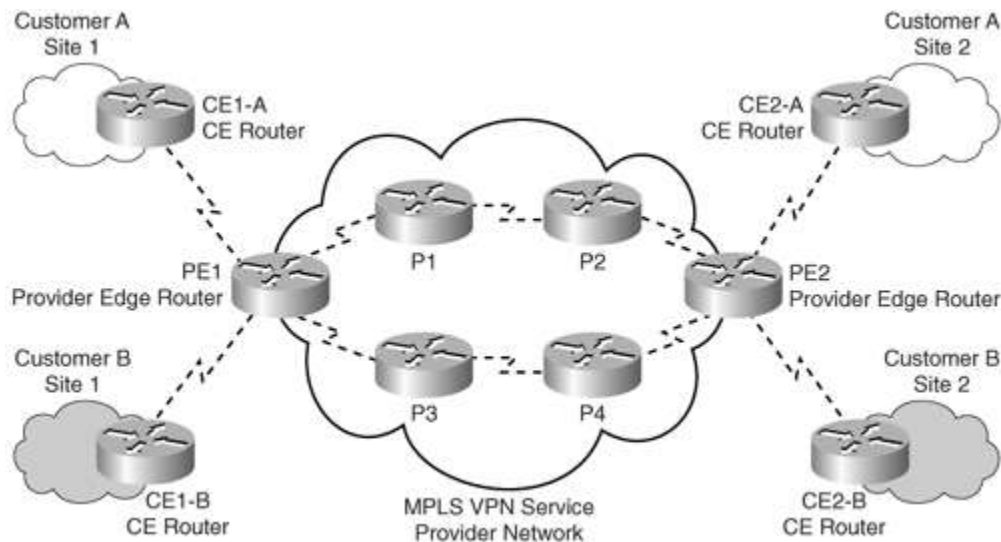
- **hop-by-hop routing**—Each LSR independently selects the next hop for a given FEC. This methodology is similar to that currently used in IP networks. The LSR uses any available routing protocols, such as OSPF, ATM private network-to-network interface(PNNI), etc.
- **explicit routing**—Explicit routing is similar to source routing. The ingress LSR (i.e., the LSR where the data flow to the network first starts) specifies the list of nodes through which the ER–LSP traverses. The path specified could be non-optimal, as well. Along the path, the resources may be reserved to ensure QoS to the data traffic. This eases traffic engineering throughout the network, and differentiated services can be provided using flows based on policies or network management methods.

The LSP setup for an FEC is unidirectional in nature. The return traffic must take another LSP.

## MPLS VPNs

### 5.12. WHAT IS A VPN:

- VPN is a set of sites which are allowed to communicate with each other
- VPN is defined by a set of administrative policies
  - Policies determine both connectivity and QoS among sites
  - Policies established by VPN customers
  - Policies could be implemented completely by VPN Service Providers
  - Using BGP/MPLS VPN mechanisms
- Flexible inter-site connectivity ranging from complete to partial mesh
- Sites may be either within the same or in different organizations (VPN can be either intranet or extranet)
- Site may be in more than one VPN (VPNs may overlap)
- Not all sites have to be connected to the same service provider (VPN can span multiple providers)



**Fig: 12 MPLS VPN Architectures**

**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.

## 5.14. CLASSIFICATION OF VPN IMPLEMENTATION

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

### 5.14.1 OVERLAY MODEL

1. 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.

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).

3. If the circuit was established by the provider on-demand, it was called a switched virtual circuit (SVC).

4. 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

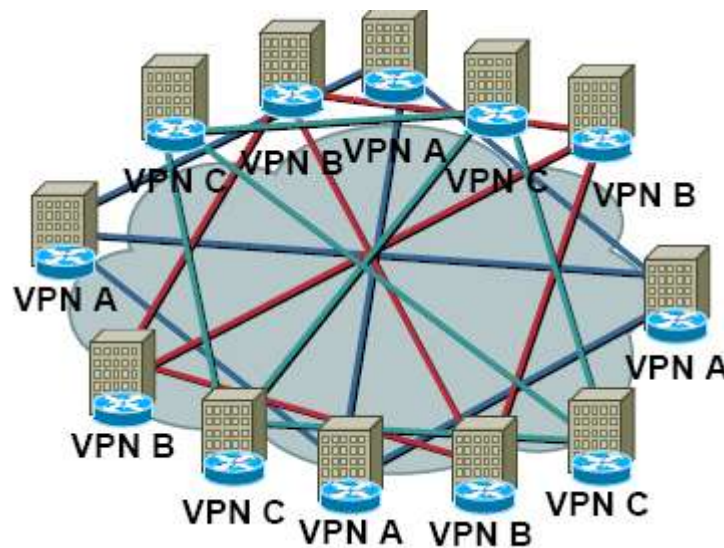
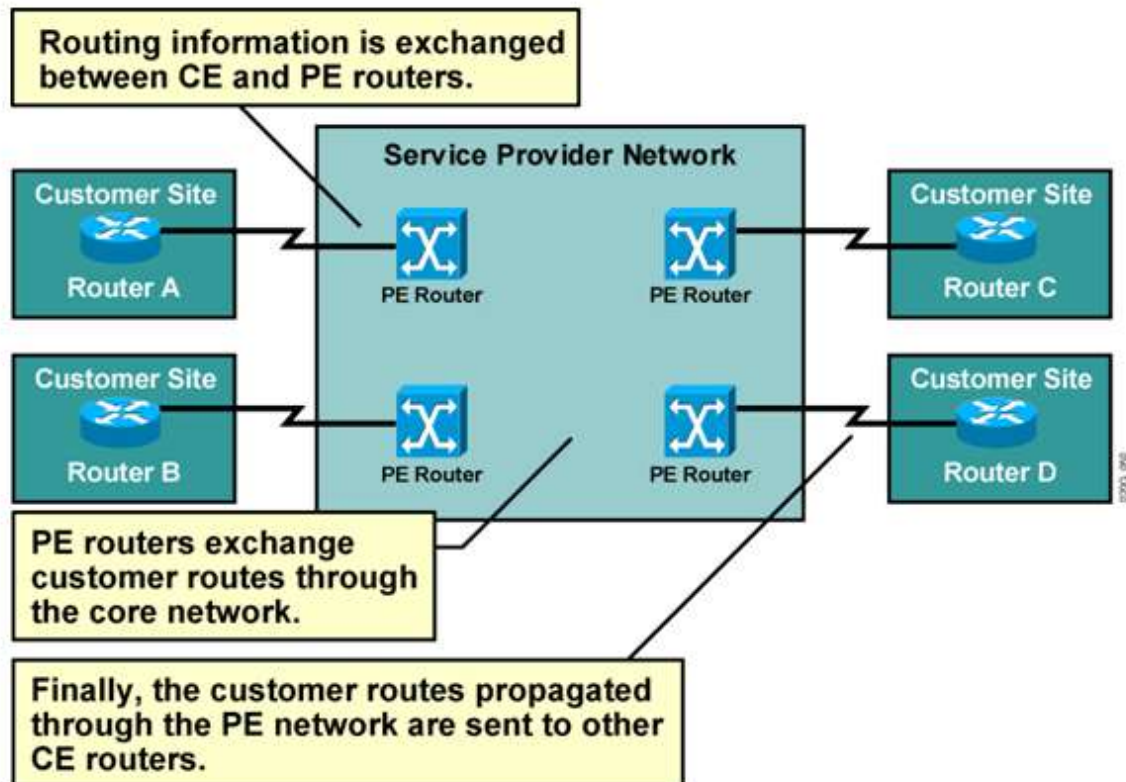


Fig:13

### 5.15 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.





**Fig:14 Peer – to – Peer VPN**

### 5.15.1 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.

### 5.16. LAYER 2 AND LAYER 3 VPNS

#### ➤ Layer 2 VPNS

- Customer End points (CPE) connected via layer 2 such as Frame Relay DLCI, ATM VC or point to point connection
- If it connects IP routers then peering or routing relationship is between the end points
- Multiple logical connections (one with each end point)

#### ➤ Layer 3 VPNS

- Customer end points peer with provider routers Single peering relationship
- No mesh of connections
- Provider network responsible for
- Distributing routing information to VPN sites
- Separation of routing tables from one VPN to another

## 5.17 MPLS VPN WORKING

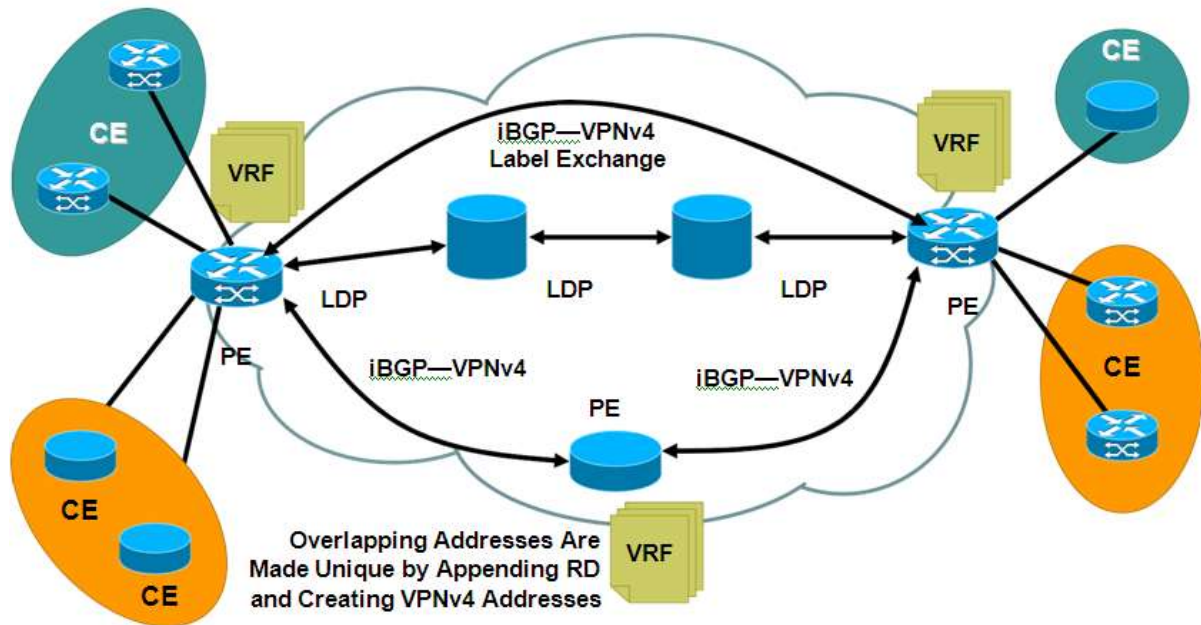


Fig: 15 MPLS VPN WORKING

### 5.17.1 MPLS LER ARCHITECTURE

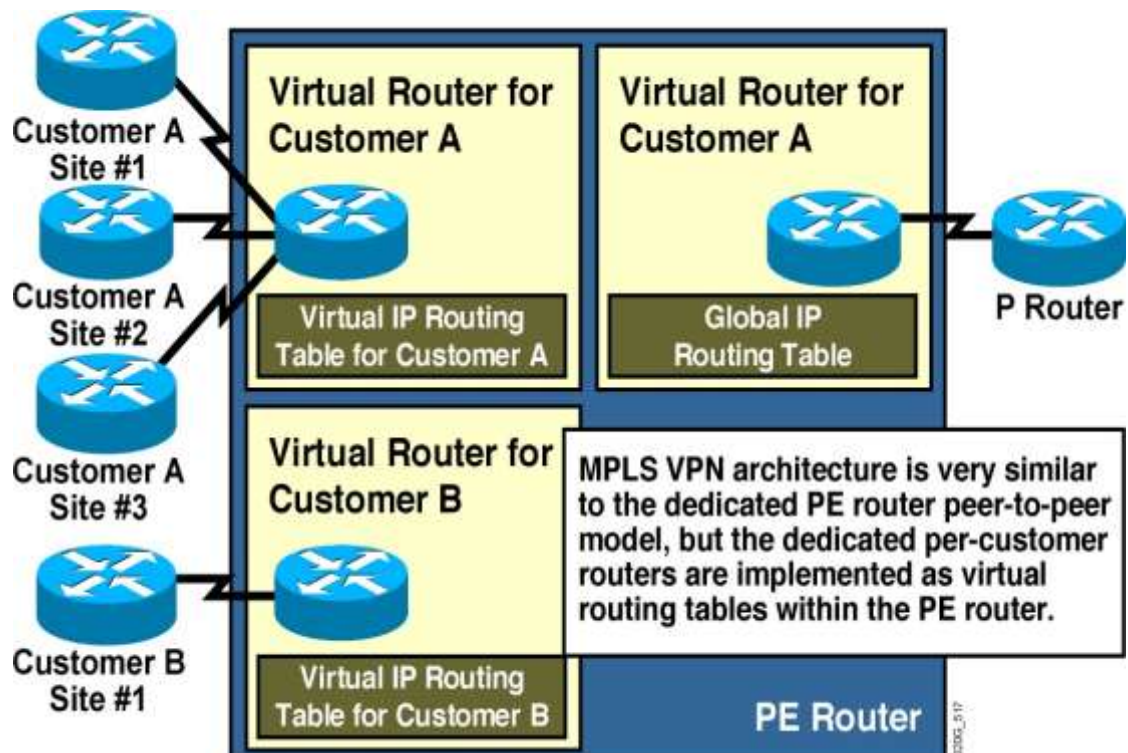


Fig:16 MPLS LER ARCHITECTURE

### 5.17.2 MPLS Control Plane Path:

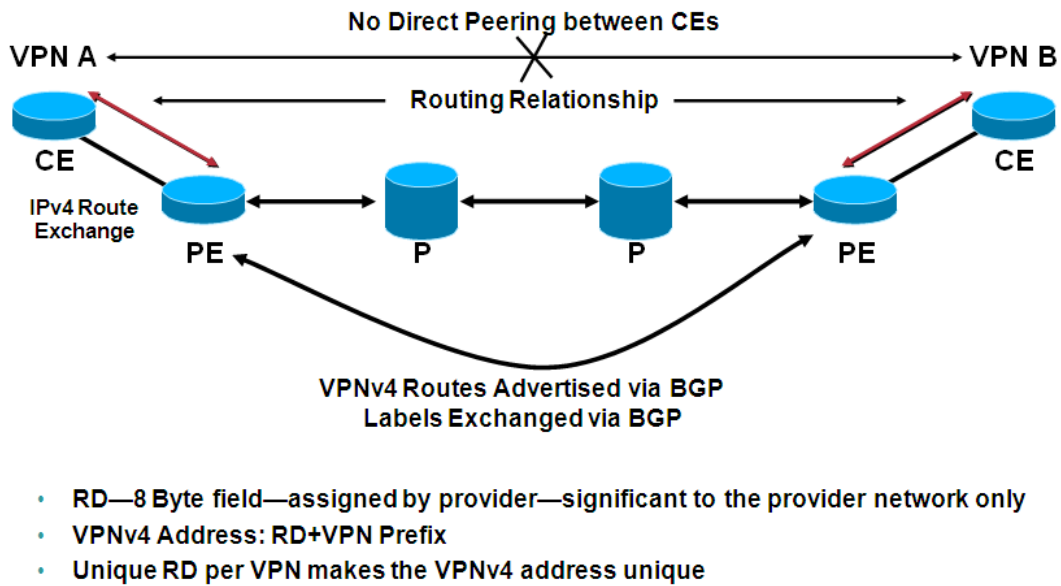
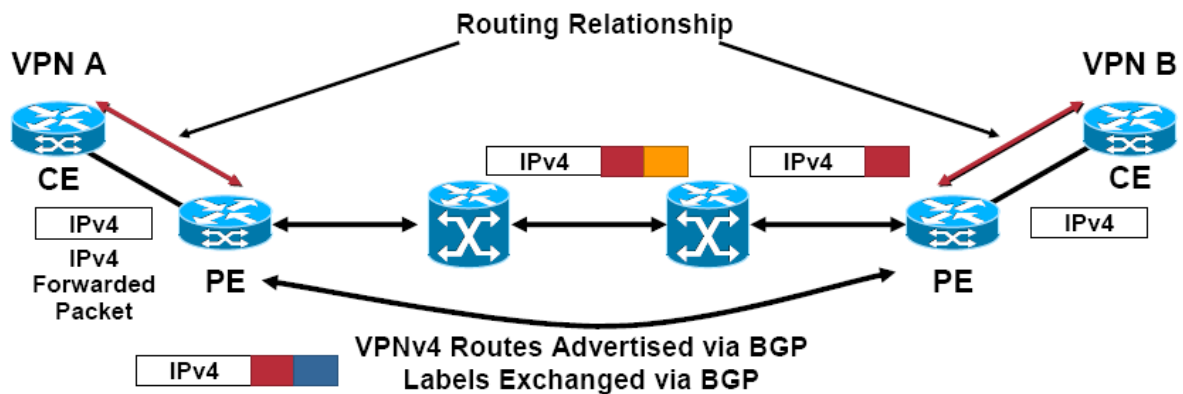


Fig:17 MPLS CONTROL PLANE PATH

### 5.17.3 MPLS DATA PLANE PATH:



- Ingress PE is imposing 2 labels

Fig:18 MPLS DATA PLANE PATH

## 5.18. ADVANTAGES OF MPLS VPNS OVER OTHER TECHNOLOGIES

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

1. 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.
2. Make the service very simple for customers to use even if they lack experience in IP routing.
3. Make the service very scalable and flexible to facilitate large-scale deployment.
4. Provide a reliable and amenable service.
5. Offering SLA to customers.
6. Capable of meeting a wide range of customer requirements, including security, quality of Service (QOS) and any-to-any connectivity.
7. Capable of offering fully managed services to customers.
8. Allow BSNL to introduce additional services such as bandwidth on demand etc over the same network.

## **5.19 CONCLUSION**

MPLS VPN is a popular technique to build VPNs for customers over the MPLS provider network. The better understanding of MPLS – VPN facilitates the participants to better handle the O and M of MPLS network in real time scenario.