CCNP ENARSI Cram Notes

2.0 VPN Technologies

2.1 Describe MPLS operations (LSR, LDP, label switching, LSP)

Multiprotocol Label Switching (MPLS) is a networking technology that allows for the efficient forwarding of data across a network using labels instead of IP addresses. MPLS operates by creating a label-switched path (LSP) between two routers in a network, which is used to forward packets between them.

The key components of MPLS are Label Switching Routers (LSRs), Label Distribution Protocol (LDP), and label switching. LSRs are routers that operate at the network layer and are responsible for forwarding packets based on the labels they receive. LDP is the protocol used to distribute labels across the network, allowing LSRs to map labels to network layer destinations.

Label switching is the process of forwarding packets based on labels, rather than IP addresses. When a packet enters an MPLS network, the ingress router attaches a label to the packet and forwards it to the next hop router. Each subsequent router in the path then swaps the incoming label with a new label and forwards the packet to the next hop router until it reaches the egress router.

MPLS also allows for the creation of virtual private networks (VPNs) by using labels to distinguish between different VPNs. This is accomplished through the use of a VPN-specific label, which is attached to packets that are destined for a specific VPN. When these packets enter the MPLS network, the label is used to direct them to the appropriate VPN.

Overall, MPLS is a powerful technology that allows for the efficient forwarding of data across a network by using labels instead of IP addresses. MPLS also enables the creation of VPNs, which can be used to provide secure and scalable connectivity between different locations or organizations.

LDP is a protocol that automatically generates and exchanges labels between routers. Each router will locally generate labels for its prefixes and will then advertise the label values to its neighbors. LDP uses the Transmission Control Protocol (TCP) to transmit Session, Advertisement, and Notification messages to ensure reliable message transmission. LDP uses the User Datagram Protocol (UDP) only for transmitting Discovery messages.

Cisco Express Forwarding is an advanced layer 3 switching technology used mainly in large core networks or internet to enhance the overall network performance is mainly used to increase packet switching speed by reducing the overhead and delays introduced by other routing

techniques. CEF consists of two key components: The Forwarding Information Base (FIB) and adjacency.

LDP(Label Distribution Protocol):A protocol used between MPLS-enabled routers to generate and exchange labels that will be used to forward packets in the MPLS domain.

LSP(Label Switched Path): The cumulative labeled path (sequence of routers) that a labeled packet takes through the MPLS domain.

LFIB(Label Forwarding Information Base):A data plane table that is used to forward labeled packets.

LIB(Label Information Base): A control plane table that stores label information.

LSR(Label Switching Router):A router in an MPLS domain that forwards packets using label information.

1. MPLS PEs form a backbone area
2. Each PE-CE link can be any area.
3. MPLS uses MPBGP to redistribute routes
4. The Area 0 may exist in both customer premise as well as the Service providers (SP) network.

CE(Customer Edge):CE A CE router (Customer Edge router) is a router located on the customer premises that provides an Ethernet interface between the customer's LAN and the provider's core network. Customer Edge normally unaware of mpls labeling. Connects customer network to MPLS network

PE(Provider Edge): Provider edge is the egress and ingress for the mpls domain , it remove labels before sending them to CE and add labels to traffic received from CE

P(Provider): Provider , MPLS devices in the core of the MPLS domain , forward traffic based on labels

LSP (Label Switch path(): LSP is a predefined path that the packet takes during the transmission

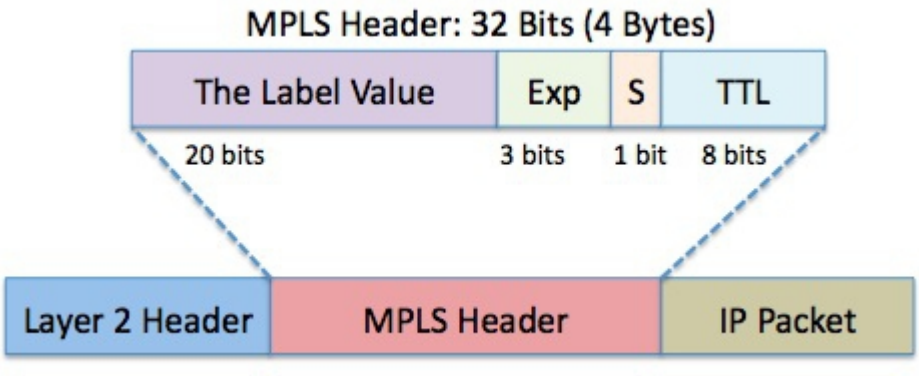
LSR(Label Switch Router) : MPLS network contains Label Switch Routers(LSR). These routers are capable of understanding MPLS labels and of receiving and transmitting the labeled packet.

ingress LSR:A router at the edge of the MPLS domain that adds labels to packets that are

entering the MPLS domain.

egress LSR: A router at the edge of the MPLS domain that removes labels from packets that are leaving the MPLS domain.

The MPLS header is of 32 bits. It contains the following information:-



1. **Label:** The label field is of 20 bits.
2. **Experimental(Exp)**:The three bits are reserved as experimental bits. They are used for Quality of Service(QoS).
3. **Bottom of Stack(BoS):** A network packet can have more than one MPLS labels which are stacked one over another. To ensure which MPLS label is at the bottom of stack we have a BoS field which is of 1 bit.
4. **Time to Live(TTL):** The last 8 bits are used for Time to Live(TTL).

2.2 Describe MPLS Layer 3 VPN

MPLS Layer 3 VPN (Virtual Private Network) is a type of VPN that uses MPLS technology to create a secure and scalable connection between different locations or organizations. Layer 3 VPN is also referred to as an MPLS VPN.

In a Layer 3 VPN, the customer's traffic is encapsulated in MPLS packets by the provider's network and is transported across the provider's network to the destination site. The traffic is carried over a separate virtual routing and forwarding (VRF) instance, which allows the VPN traffic to be isolated from other traffic in the network.

At the provider edge (PE) router, the MPLS packets are assigned to a particular VPN using labels. The customer edge (CE) router, which is located at the customer's site, sends and

receives traffic through the PE router using the assigned label. This label allows the PE router to forward the traffic to the appropriate destination site, and to ensure that the traffic is kept separate from other VPN traffic.

MPLS Layer 3 VPN provides several benefits, including:

1. Scalability: MPLS Layer 3 VPNs can support a large number of sites and users, making them ideal for organizations that need to connect multiple locations.

2. Security: MPLS Layer 3 VPNs provide a high level of security by using encryption and access control mechanisms to protect the traffic.

3. Quality of Service: MPLS Layer 3 VPNs support quality of service (QoS) mechanisms, which ensure that critical traffic is given priority over less important traffic.

Overall, MPLS Layer 3 VPN is a powerful and flexible technology that allows organizations to connect multiple sites securely and efficiently, and to manage their network traffic effectively.

For the MPLS domain to forward traffic, a label stack is required. Specifically, two labels are required for traffic to be successfully forwarded through the MPLS domain. The first label that is attached to the packet is a VPN label, and the second label that is attached is the LDP label.

The control plane functions include the system configuration,management, and exchange of routing table information. These are performed relatively infrequently. The route controller exchanges the topology information with other routers and constructs a routing table based on a routing protocol, for example,

RIP (Routing Information Protocol), OSPF (Open Shortest Path Forwarding), or BGP (Border Gateway Protocol). It can also create a forwarding table for the forwarding engine. Since the control functions are not performed on each arriving individual packet, they do not have a strict speed constraint and are implemented in software in general. The Control plane feeds the forwarding/data plane with what it needs to create its forwarding tables and updates topology changes as they occur. A list of functions performed in traditional routing engines/route processors are the following:

Allocates resources to the forwarding engine/plane.
Routing state
ARP handling is always processed by general purpose processor located in the routing engine.
Security functions to secure the control plane access. Telnet, SSH, AAA etc.
Establishes and maintains management sessions, such as Telnet connections
Routing state to neighboring network elements.

Vendor and platform specific stacking, clustering, pairing etc.

1. A CE router forms a neighbor relationship with the PE router on the other end of the access link.

2. A CE router cannot form a neighbor relationship with other CE routers.
3. The MPLS network advertises the customer's routes between the various PE routers.
4. The MPLS network uses route redistribution to advertise CE routes among other CE routers.
5. It is possible that the PE routers use different layer-3 protocols to connect to the MPLS network.

Multiprotocol Label Switching (MPLS) is a protocol for speeding up and shaping network traffic flows. MPLS allows most packets to be forwarded at Layer 2 (the switching level) rather than having to be passed up to Layer 3 (the routing level). Each packet gets labeled on entry into the service provider's network by the ingress router. All the subsequent routing switches perform packet forwarding based only on those labels - they never look as far as the IP header. Finally, the egress router removes the label(s) and forwards the original IP packet toward its final destination.

MPLS is an IETF initiative that integrates Layer 2 information about network links (e.g. bandwidth, latency, utilization) into Layer 3 (IP) within a particular autonomous system, or ISP, in order to simplify and improve IP packet exchange. MPLS gives network operators a great deal of flexibility to divert and route traffic around link failures, congestion, and bottlenecks.

MPLS Layer 3 VPNs provide peer-to-peer connectivity between private customer sites across a shared network. Customer isolation is achieved on the PE (Provider Edge) router by the use of virtual routing tables or instances, also called virtual routing and forwarding tables/instances (VRFs). VRF is a technology for creating separate virtual routers on a single physical router.

A Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) consists of a set of sites that are interconnected by means of an MPLS provider core network. At each site, there are one or more customer edge (CE) devices, which attach to one or more provider edge (PE) devices. PEs use the Multiprotocol-Border Gateway Protocol (MP-BGP) to dynamically communicate with each other.

Advantages of using MPLS:

1. The label-switching technology offers QoS capabilities.
2. MPLS VPNs are available in Layer-2 as well as Layer-3 designs. Layer-2 typically uses Metro Ethernet, where as Layer-3 connectivity may use a variety of L3 technologies such as EIGRP, OSPF, RIPv2, etc., depending on what the SP could provide.
3. By keeping your traffic on a single vendor using MPLS VPNs gives the vendor the ability to

offer your company service-level agreements (SLAs) for network performance.
4. MPLS supports many types of access links such as Metro Ethernet, Serial (TDM), ATM, and Frame Relay.

Some of the disadvantages are given below:

1. Your routing protocol choice might be limited.