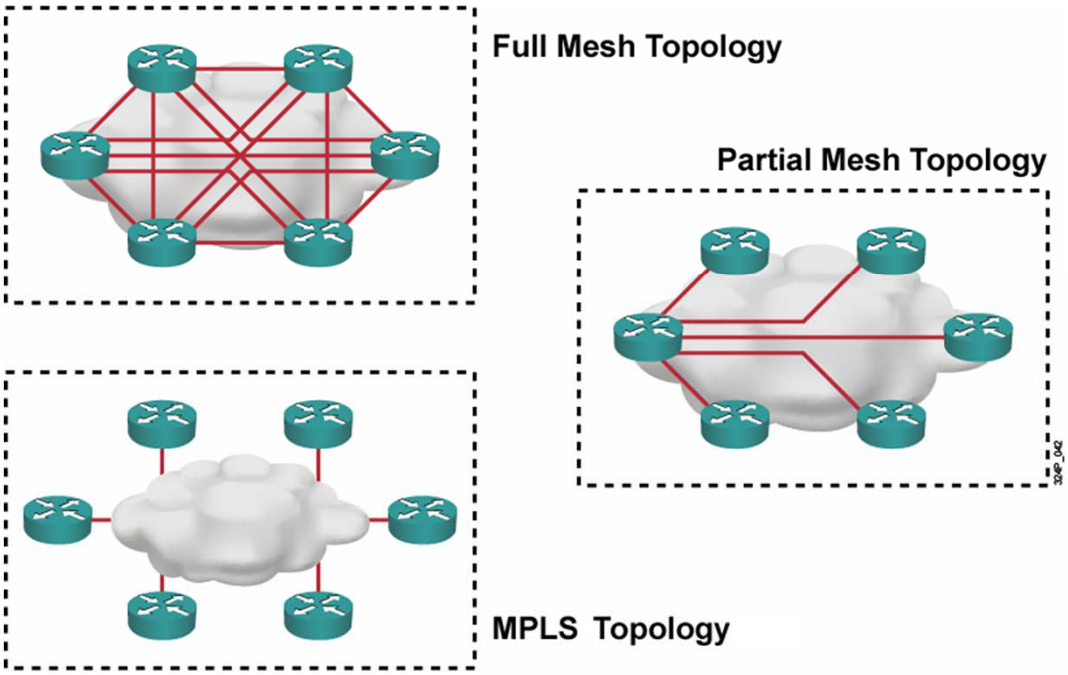
MPLS

WAN Topologies



- **a full mesh topology is required for optimal routing between the sites and provides a dedicated virtual circuit between any two customer edge (CE) routers in the network to support the best routing solution, but using the full mesh configuration is very expensive.**
- **A partial mesh topology or hub-and-spoke topology is a less expensive solution. These topologies use a central point to coordinate activities. these solutions do not provide optimal routing. Using the partial mesh topology reduces the number of virtual circuits to the minimum number of circuits that are needed to provide optimum transport between major sites.**
- **Multiprotocol Label Switching (MPLS) provides optimal routing between sites. A site requires only one connection to the MPLS Service Provider (SP). MPLS is a high-performance method for forwarding packets through a network. MPLS enables routers at the edge of a network to apply simple labels in the form of numbers to these packets. MPLS-enabled routers can then switch packets according to labels, incurring minimal overhead for routing lookup.**

Multiprotocol Label Switching (MPLS)

- IETF standard , RFC3031
- Basic idea was to combine IP routing protocols with a forwarding algoritm based on a header with fixed length label instead of the longest prefix match on the destination IP address in the IP header
- Label switching makes it possible to make forwarding decisions based on more complex criterias than IP dst address, but still keeping a simple lookup

- **Recursive route lookup - Occurs when the router has to perform multiple lookups in the routing table before forwarding a packet.**

Basic Multiprotocol Label Switching (MPLS) Features

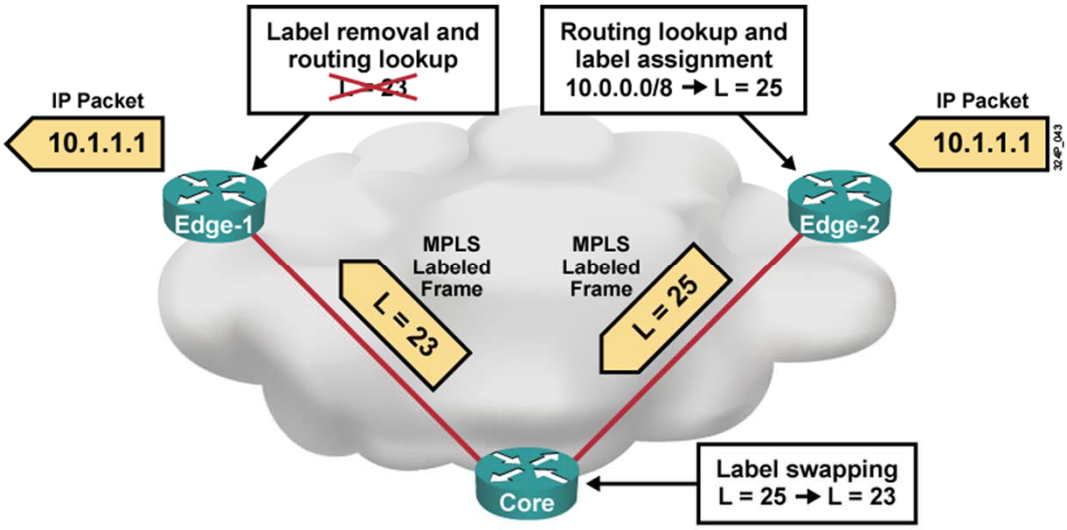
- MPLS reduces routing lookups.
- MPLS forwards packets based on labels.
- Labels usually correspond to IP destination networks (equal to traditional IP forwarding).
- Labels can also correspond to other parameters:
  - Layer 3 VPN destination
  - Layer 2 circuit
  - Outgoing interface on the egress router
  - QoS
  - Source address
- MPLS supports forwarding of all Layer 3 protocols, not just IP.

- **Recursive route lookup - Occurs when the router has to perform multiple lookups in the routing table before forwarding a packet.**

Application of MPLS

- Traffic engineering & Route control
- QoS
- VPNs MPLS

MPLS Operation



- Only edge routers must perform a routing lookup.
- Core routers switch packets based on simple label lookups and swap labels.

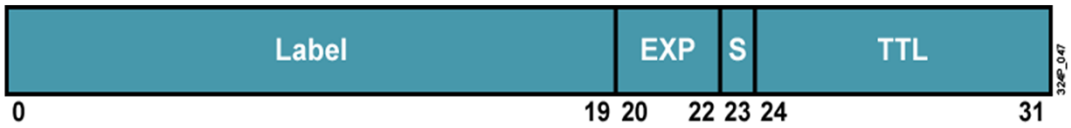
- **MPLS provides fast routing for large networks. Only the edge routers perform a routing lookup, and core routers forward packets based on the labels. These two functions mean faster forwarding of packets through the SP network.**
- **core router, does not have to perform a time-consuming routing lookup. core router y swaps label 25 with label 23. The core router then forwards the packet to the Edge-1 router based on receiving label 23 from the Edge-1 router.**
- **routing table tells the Edge-2 router that to reach the 10.1.1.1 network, the Edge-2 router should assign a label of 25 to the packet. The edge router then forwards the packet to the core router. The label tells the core router that when the core router receives a packet with label 25, the router should swap that label with label 23 and then forward the packet to the Edge-1 router. Later in the course, you will read about the actual method that is used to inform the routers of these label allocations.**
- **In larger networks, the result of MPLS labeling is that only the routers at the edge of an MPLS network perform a routing lookup. All the core MPLS routers forward packets based on labels.**

MPLS

- MPLS technology is intended to be used anywhere, regardless of Layer 1 media and Layer 2 protocol.

- MPLS uses a 32-bit label field that is inserted between Layer 2 and Layer 3 headers (frame mode MPLS).

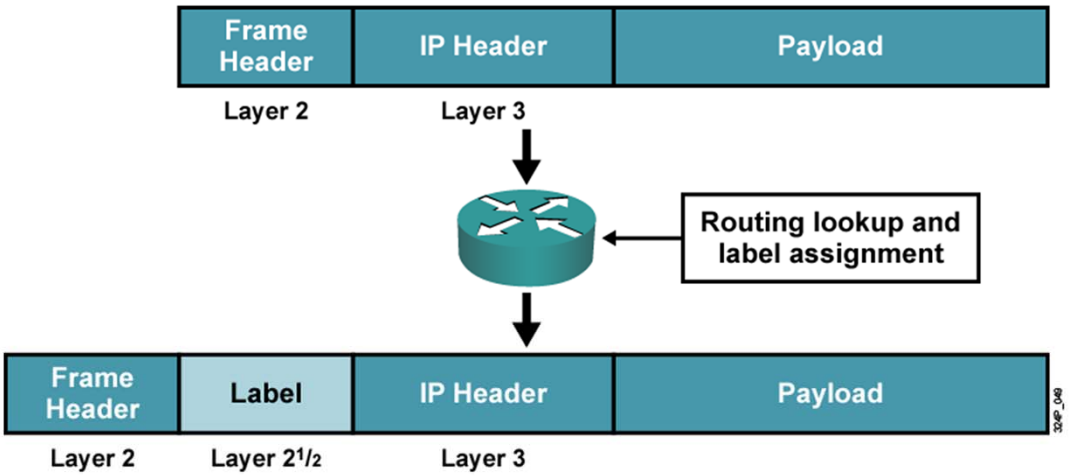
Label Format



Field	Description
20-bit label	The actual label. Values 0 to 15 are reserved.
3-bit experimental (EXP) field	Undefined in the RFC. Used by Cisco to define a class of service (CoS) (IP precedence).
1-bit bottom-of-stack indicator	MPLS allows multiple labels to be inserted. The bottom-of-stack bit determines if this label is the last label in the packet. If this bit is set (1), the setting indicates that this label is the last label.
8-bit Time to Live (TTL) field	Has the same purpose as the TTL field in the IP header.

- MPLS labels have a specific format and fields that assist in making forwarding decisions. The 32-bit MPLS label contains four fields.

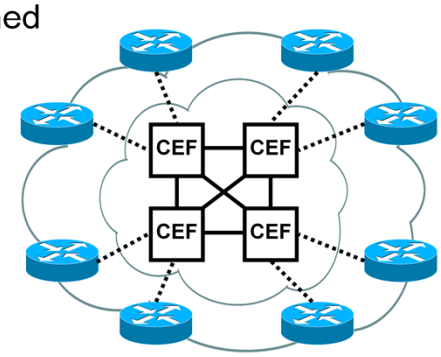
Frame Mode MPLS Operation



- This graphic shows an edge router that receives a normal IP packet. The MPLS label is often depicted as a new "shim layer" that has interposed itself between the network and data link layers. This layer is where the term "Layer 2.5 technology" comes from.

Cisco IOS Platform Switching Mechanisms

- Process switching, or routing table-driven switching:
  - Full lookup is performed at every packet
- Fast switching, or cache-driven switching:
  - Most recent destinations are entered in the cache
  - First packet is always process-switched
- Topology-driven switching:
  - CEF (prebuilt FIB table)



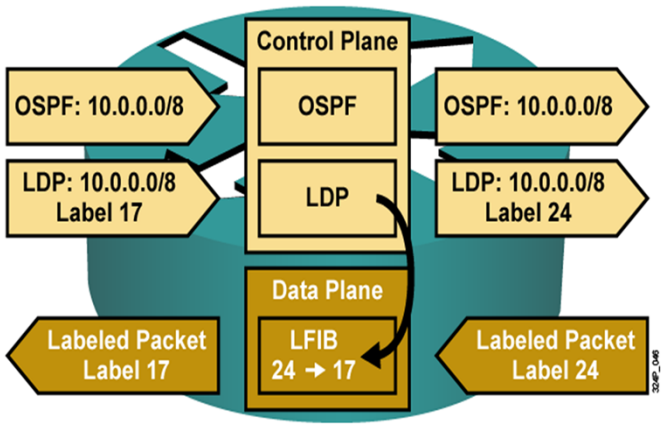
Cisco Express Forwarding

- **The original switching mechanism available on Cisco routers was process switching. Process switching is very slow because it must find a destination in the routing table. This process can possibly result in a recursive lookup. Process switching must also construct a new Layer 2 frame header for every packet. As a result, process switching is no longer widely used in modern networks.**
- **Cisco IOS platforms have the capability to overcome the slow performance of process switching. The platforms support several switching mechanisms that use a cache to store the most recently used destinations. A cache uses a faster searching mechanism than process switching does while storing the entire Layer 2 frame header to improve the encapsulation performance. In cache-driven switching, an entry is created in the cache when the first packet whose destination is not found in the fast-switching cache is process switched. The subsequent packets are switched in the interrupt code; this is how the cache improves performance.**
- **The most recent and preferred Cisco IOS platform switching mechanism is Cisco Express Forwarding (CEF), which incorporates the best of the previous switching mechanisms.**
- **One of the benefits of CEF is that this mechanism supports per-packet load balancing, which was previously supported only by process switching. CEF also supports per-source or per-destination load balancing, fast destination lookup, and many other features that are not supported by other switching mechanisms.**
- **CEF uses a Forwarding Information Base (FIB) to make IP destination prefix-based switching decisions. The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are reflected in the**

FIB. The FIB maintains next-hop address information based on the information in the IP routing table.

- **Because there is a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with switching paths such as fast switching and optimum switching.**

Major Components of MPLS Architecture



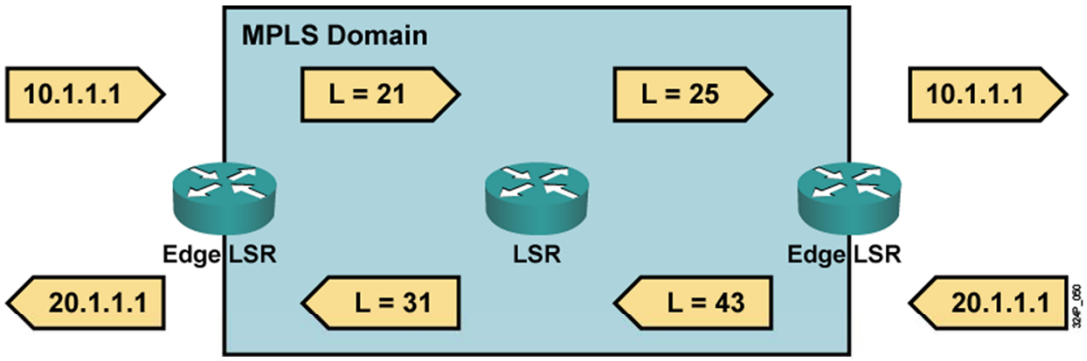
Control plane:
Exchanges routing information and labels
Contains complex mechanisms, such as OSPF, EIGRP, IS-IS, and BGP, to exchange routing information
Exchanges labels, such as LDP, BGP, and RSVP

Data plane:
Forwards packets based on labels
Has a simple forwarding engine

- Information from control plane is sent to the data plane.

- MPLS can implement destination-based forwarding using labels to make forwarding decisions.
- In the example shown, a Layer 3 routing protocol is needed to propagate Layer 3 routing information. A label exchange mechanism is simply an add-on mechanism that propagates labels that are used for Layer 3 destinations.
- The figure illustrates the two components of the control plane:
  - **OSPF:** Receives and forwards a routing update for IP network 10.0.0.0/8.
  - **LDP:** Receives label 17 to use for packets with destination address 10.x.x.x. A local label 24 is generated and sent to upstream neighbors when the packets are destined for 10.x.x.x. LDP inserts an entry into the LFIB table of the data plane, where an incoming label 24 is mapped to an outgoing label 17.
- The data plane then forwards all packets with label 24 through the appropriate interfaces after swapping label 24 for label 17.

Label Switch Routers (LSRs)



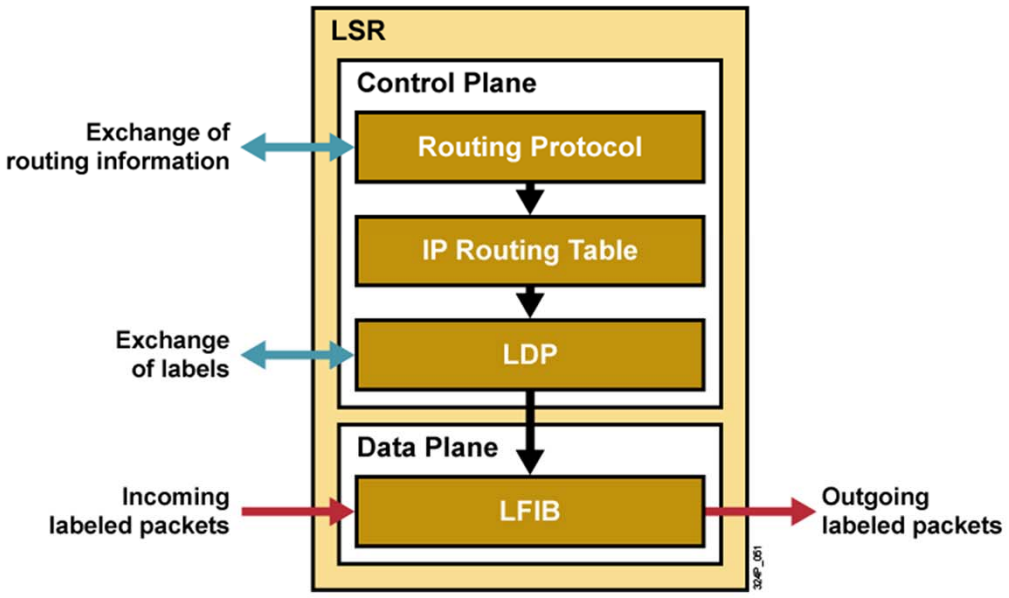
- LSR primarily forwards labeled packets (swap label).
- Edge LSR:

  Labels IP packets (impose label) and forwards them into the MPLS domain.

  Removes labels (pop label) and forwards IP packets out of the MPLS domain.

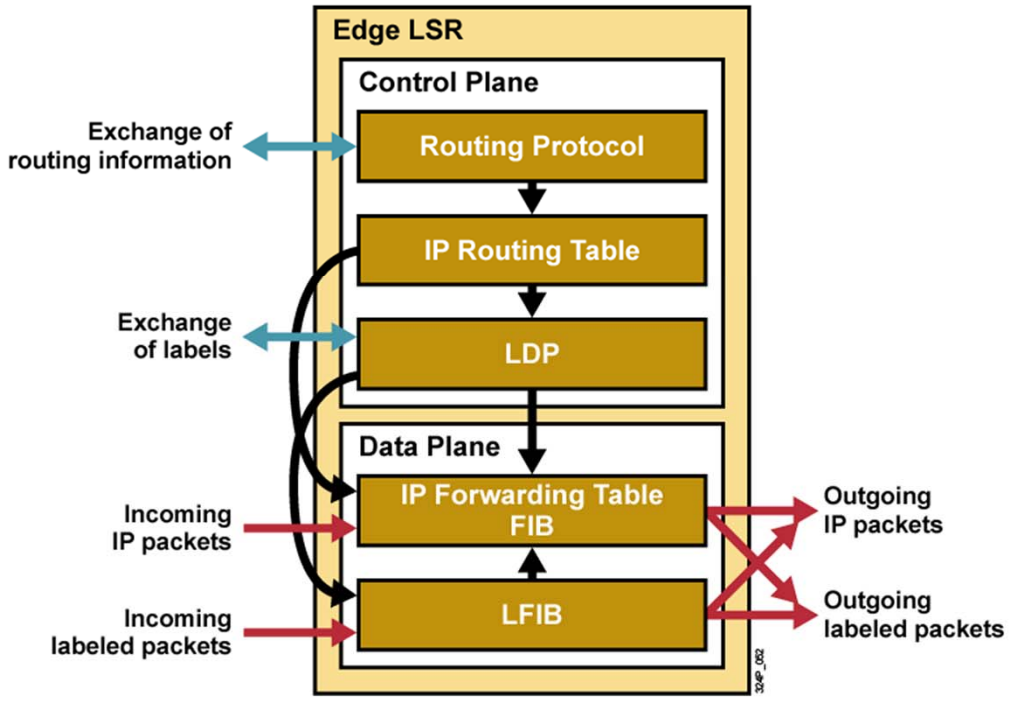
- When discussing MPLS, there are two commonly used terms:
  - **LSR:** A device that forwards packets primarily based on labels. Cisco calls this a provider router (P router).
  - **Edge LSR:** A device that primarily labels packets or removes labels. Cisco calls this a provider edge router (PE router).
- LSRs and Edge LSRs forward packets by making switching decisions based on the MPLS label. LSRs and Edge LSRs are usually capable of doing both label switching and IP routing. Their names are based on the router positions in an MPLS domain.
- Routers that have all interfaces enabled for MPLS are called LSRs because they mostly forward labeled packets. Routers that have some interfaces that are not enabled for MPLS are usually at the edge of an MPLS domain—autonomous systems (ASs). These routers also forward packets based on IP destination addresses and label the packets if the outgoing interface is enabled for MPLS.
- For example, an Edge LSR receives a packet for destination 10.1.1.1, imposes label 21, and forwards the frame to the LSR in the MPLS backbone. LSR swaps label 21 with label 25 and forwards the frame. The edge LSR removes label 25 and forwards the packet based on IP destination address 10.1.1.1.

Component Architecture of LSR



- This graphic shows the component architecture of an LSR.
- The primary function of an LSR is to forward labeled packets. To accomplish this, every LSR needs a Layer 3 routing protocol and a protocol to exchange labels.
- LDP populates the LFIB table in the data plane that is used to forward labeled packets.

Component Architecture of Edge LSR



- Edge LSRs also forward IP packets based on the IP destination addresses of the packet and, optionally, label the packets if a label exists.
  - •There are several possible combinations of forwarding and labeling packets:
  - •Forward the received IP packet based on the IP destination address and send as an IP packet
  - •Forward the received IP packet based on the IP destination address and send as a labeled packet
  - •Forward the received labeled packet based on the label, change (swap) the label, and send the labeled packet
  - •Forward the received labeled packet based on the label, remove the label, and send the IP packet
- These scenarios are possible if the network is not configured properly:
  - •A received labeled packet is dropped if the label is not found in the LFIB table, even if the IP destination exists in the IP forwarding table, also called the FIB.
  - •A received IP packet is dropped if the destination is not found in the IP forwarding table (FIB table), even if there is an MPLS label-switched path toward the destination.

Label Allocation in a Frame Mode MPLS Environment

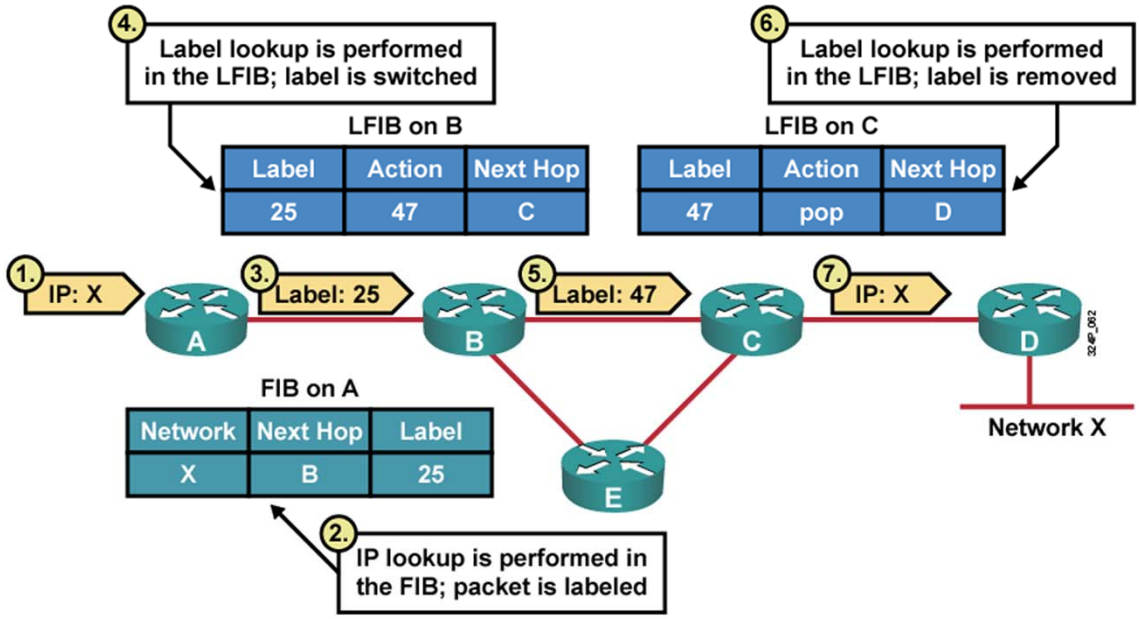
- Label allocation and distribution in a frame mode MPLS network follows these steps:
  1. IP routing protocols build the IP routing table.
  2. Each LSR independently assigns a label to every destination in the IP routing table.
  3. LSRs announce their assigned labels to all other LSRs.
  4. Every LSR builds LIB, LFIB, and FIB data structures based on the received labels.

Note: Label allocation, label imposing, label swapping, and label popping usually happen in the service provider network, not the customer (enterprise) network. Customer routers never see a label.

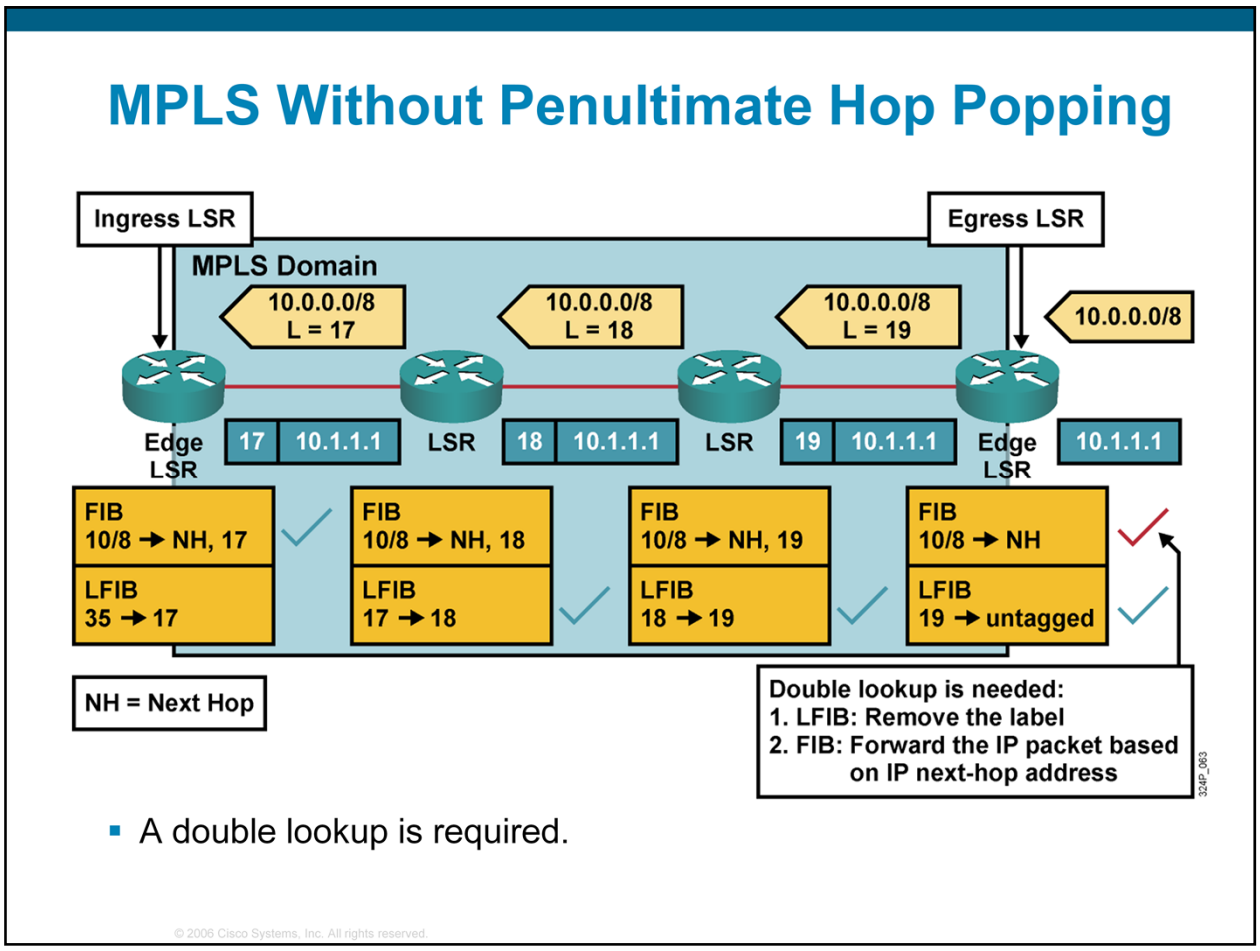
- There are four steps for label allocation and distribution in a Unicast IP routing network and MPLS functionality, including label allocation and distribution. The following steps detail what happens:
  1. The routers exchange information using standard or vendor-specific Interior Gateway Protocol (IGP), such as OSPF, IS-IS, and EIGRP.
  2. Local labels are generated. One locally unique label is assigned to each IP destination that is found in the main routing table and stored in the Label Information Base (LIB) table.
  3. Local labels are propagated to adjacent routers, where these labels might be used as next-hop labels (stored in the Forwarding Information Base [FIB] and LFIB tables to enable label switching).
  4. Every LSR builds its LIB, LFIB, and FIB data structures based on received labels.
- These data structures contain label information:
  - The LIB, in the control plane, is the database that LDP uses. This database is where an IP prefix is assigned a locally significant label that is mapped to a next-hop label that has been learned from a downstream neighbor.
  - The LFIB, in the data plane, is the database used to forward labeled packets. Local labels, previously advertised to upstream neighbors, are mapped to next-hop labels, previously received from downstream neighbors.
  - The FIB, in the data plane, is the database used to forward unlabeled IP packets. A forwarded packet is labeled if a next-hop label is available for

a specific destination IP network. Otherwise, a forwarded packet is not labeled.

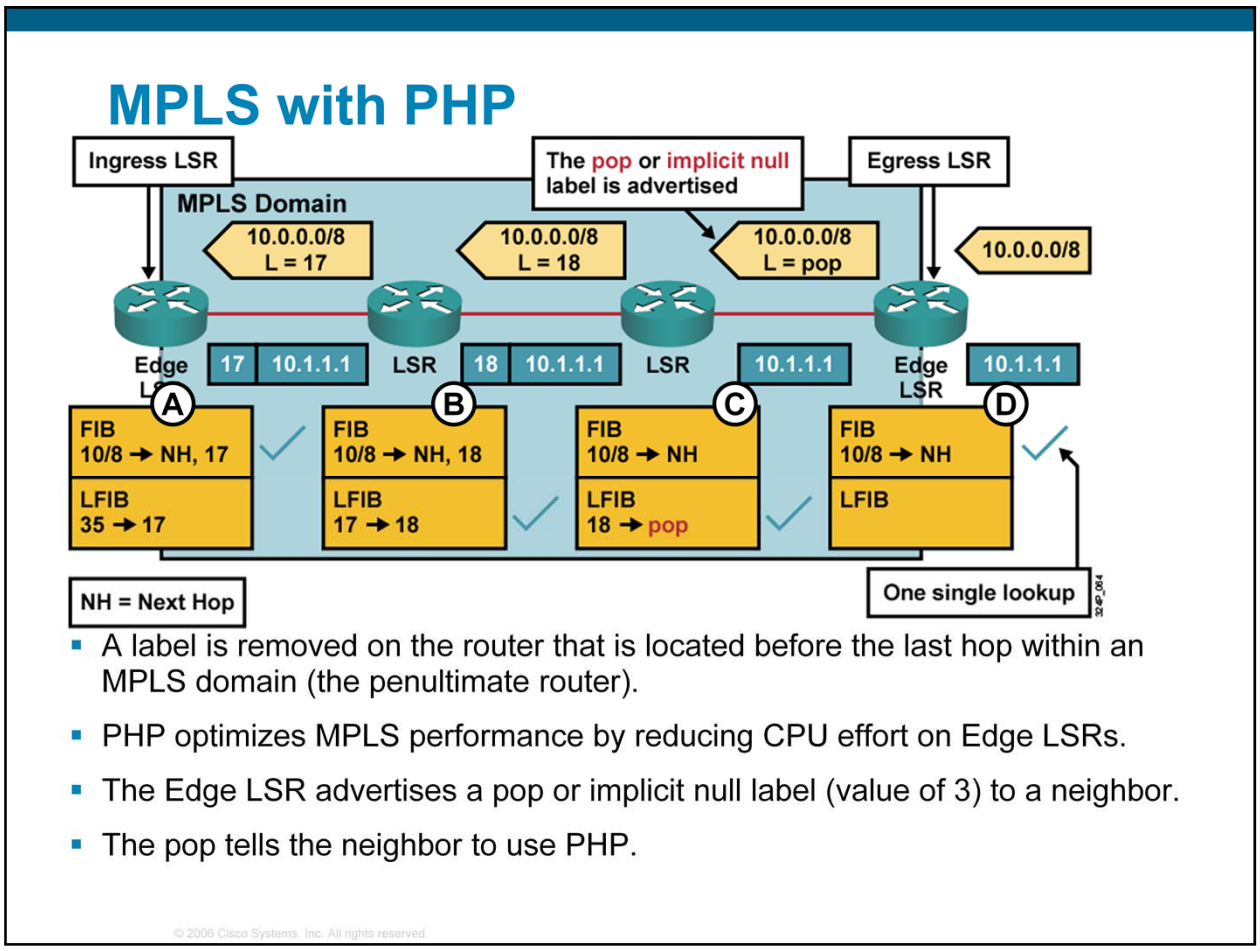
Packet Propagation Across an MPLS Network



- How a packet is forwarded depends on whether the packet is an IP packet or labeled packet. An incoming **IP packet** is forwarded by using the FIB table and can be sent out as an IP packet or as a labeled IP packet. An incoming **labeled** packet is forwarded by using the LFIB table and sent out as a labeled IP packet. If a router does not receive a label from the next-hop router, the label is removed and an unlabeled IP packet is sent.
- This graphic illustrates how IP packets are propagated across an MPLS domain. The steps are as follows:
    1. An IP packet destined for Network X arrives at Router A.
    2. Router A labels a packet destined for Network X by using the next-hop label 25 (CEF switching by using the FIB table).
    3. Router A sends the packet toward Network X with the MPLS label 25.
    4. Router B swaps label 25 with label 47 using the LFIB.
    5. Router B forwards the packet to Router C (label switching by using the LFIB table).
    6. Router C **removes (pops)** the label.
    7. Router C forwards the unlabeled packet to Router D (label removed by using the LFIB table).
- When a router receives an IP packet, the lookup done is an IP lookup. In Cisco IOS, this means that the packet is looked up in the CEF table. When a router receives a labeled packet, the lookup is done in the LFIB table of the router. The router knows that it receives a labeled packet or an IP packet by looking at the protocol field in the Layer 2 header. If a packet is forwarded by either Cisco Express Forwarding (CEF) (IP lookup) or by LFIB (label lookup), the packet can leave the router either labeled or unlabeled.



- This graphic shows how labels are propagated and used in a typical frame mode MPLS network without PHP enabled.
- The check marks show which tables are used on individual routers. The egress router in this example must perform a lookup in the LFIB table to determine whether the label must be removed and if a further lookup in the FIB table is required. PHP removes the requirement for a double lookup to be performed on egress LSRs.



- The term *pop* means to remove the top label in the MPLS label stack instead of swapping the top label with the next-hop label. When popping, the last router before the egress router removes the top label.
- This graphic shows how a predefined label pop, which corresponds to the pop action in the LFIB, is propagated on the first hop or the last hop, depending on the perspective. The following is a step-by-step explanation:
    1. IP packet enters the MPLS cloud at Router A, the Ingress LSR;
    2. A FIB lookup is performed and the packet is labeled with 17, the next hop;
    3. The pack travels to Router B an LFIB lookup is performed and the label is switched to Label: 18, which is the next hop to Router C;
    4. **Router C does an LFIB lookup and removes (that is, pops) the label;**
    5. **Router C sends the packet to router D, the Egress LSR.**
- PHP slightly optimizes MPLS performance by eliminating one LFIB lookup at the egress edge LSR.

Label Switched Path (LSP)

Two mechanisms to do path selection

Independet

- Hop-by- hop
- Regular routing protocol to select the path

Ordered

- Explicit routing
- Path completely specified by edge LSR

Label Distribution

Need to have signaling between LSRs and set up Label Switched Path (LSP)

- Label distributions

LDP (Label Distribution Protocol)

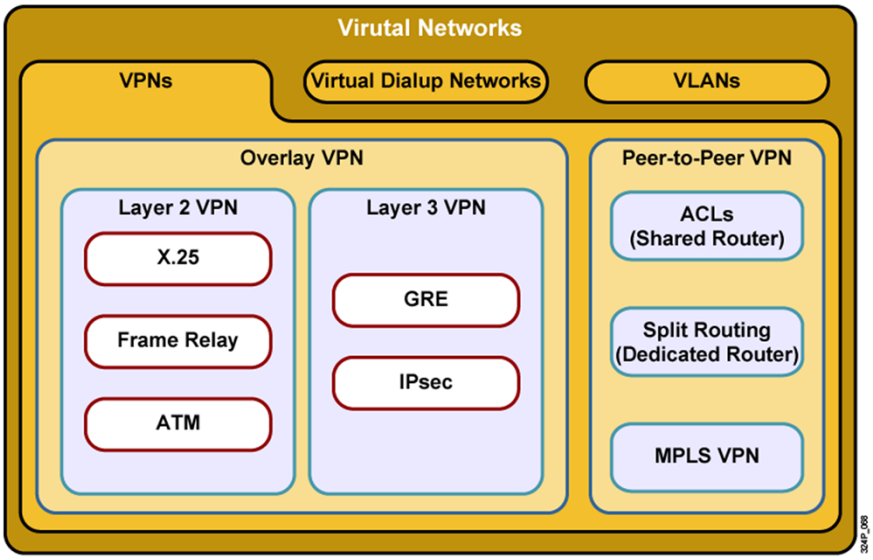
RSVP(Resourse Reservation Protocol)

BGP

MPLS Implementation MPLS VPN

Describing MPLS VPN Technology

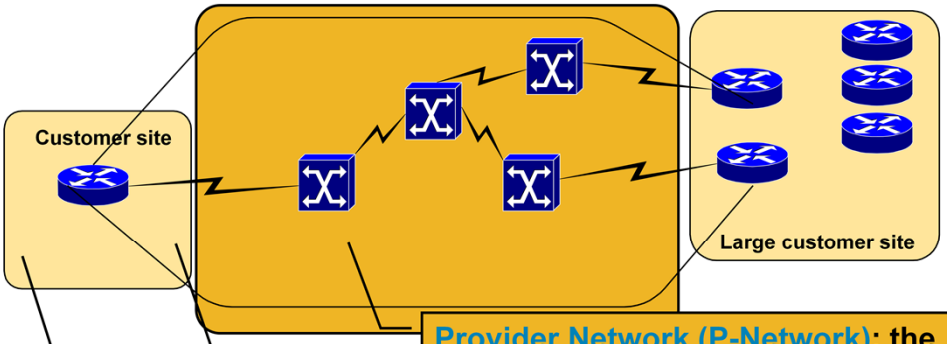
VPN Taxonomy



- Overlay VPNs—Service providers provide virtual point-to-point links.
- Peer-to-peer VPNs—Service providers participate in the customer routing.

- VLANs allow you to implement isolated LANs over a single physical infrastructure.
- Virtual private dialup networks (VPDNs) allow you to use the dial-in infrastructure of a SP for private dialup connections.
- VPNs allow you to use the shared infrastructure of a SP to implement your private networks. There are two implementation models:
  - **Overlay VPNs:** Includes technologies such as X.25, Frame Relay, ATM for Layer 2 Overlay VPN, and Generic Routing Encapsulation (GRE) and IPsec for Layer 3 Overlay VPN. With overlay VPNs, the SP provides virtual point-to-point links between customer sites.
  - **Peer-to-peer VPNs:** Implemented with routers and respective filters, with separate routers for each customer, or with the MPLS VPN technology. With peer-to-peer VPNs, the SP participates in customer routing.
- Some key VPN implementation technologies include the two major VPN models, overlay and peer-to-peer.

VPN Terminology

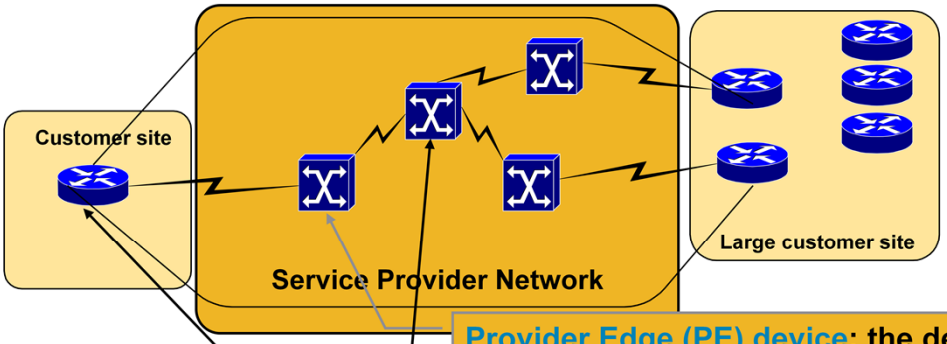


Provider Network (P-Network): the Service Provider infrastructure used to provide VPN services

Customer Network (C-Network): the part of the network still under customer control

Customer Site: a contiguous part of customer network (can encompass many physical locations)

VPN Terminology



Provider Edge (PE) device: the device in the P-network to which the CE-devices are connected

Provider core (P) device: the device in the P-network with no customer connectivity

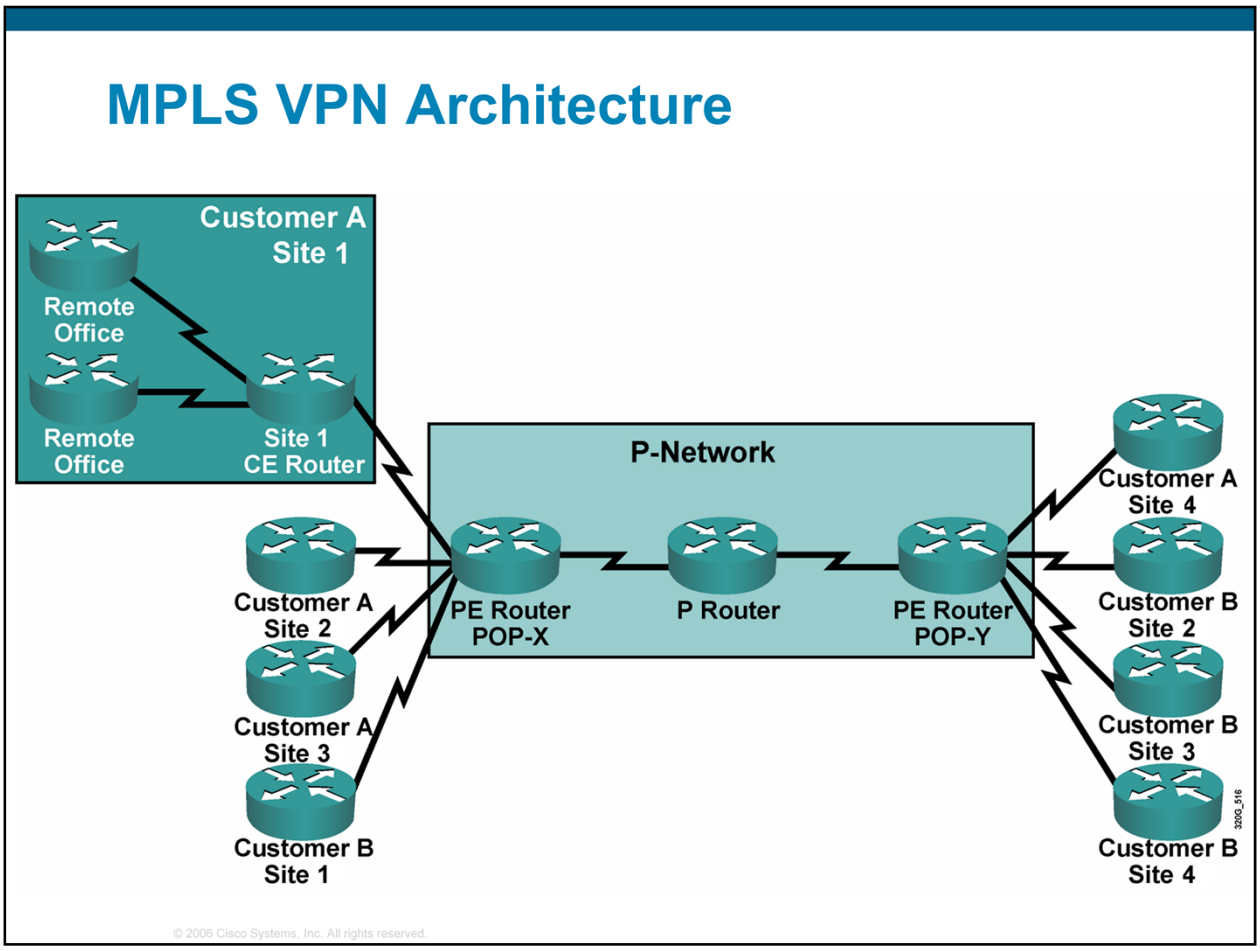
Customer Edge (CE) device: the device in the C-network with link into P-network. Also called **Customer Premises Equipment (CPE)**

MPLS VPN Architecture

- RFC 4364

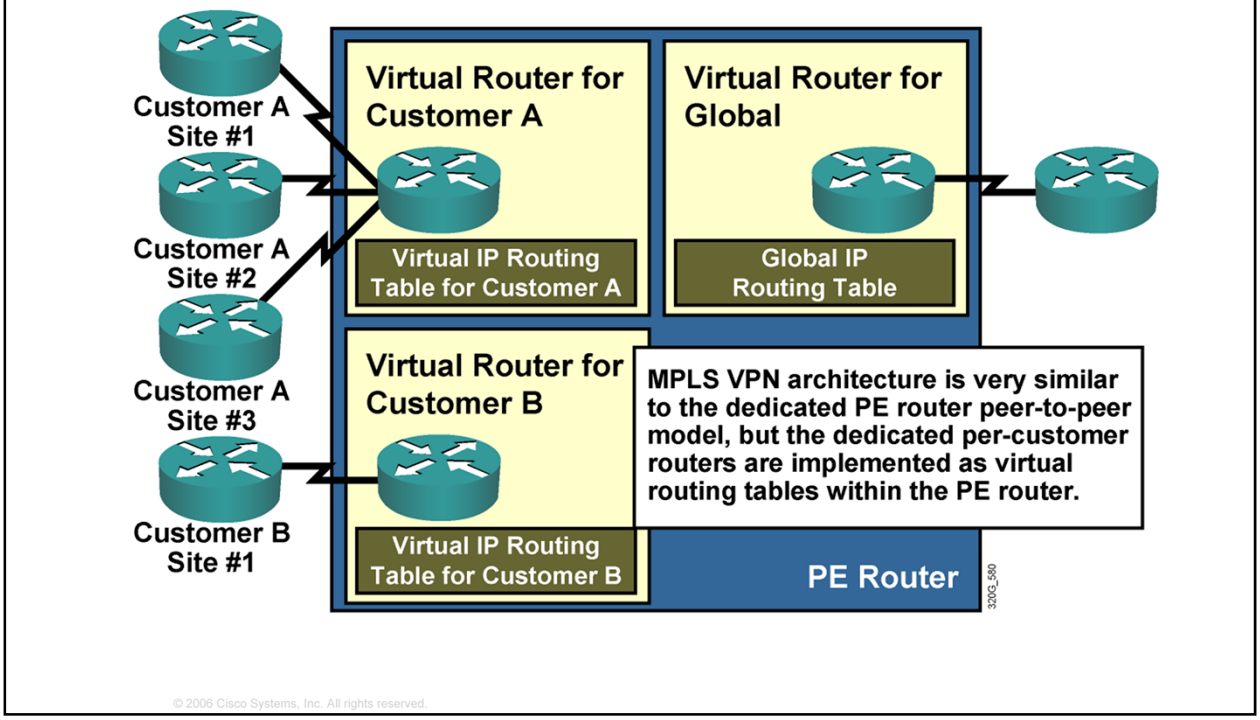
- An MPLS VPN combines the best features of overlay VPN and a peer-to-peer VPN models:
  - PE routers participate in customer routing, guaranteeing optimum routing between sites and easy provisioning.
  - PE routers carry a separate set of routes for each customer (similar to the dedicated PE router approach).
  - Customers can use overlapping addresses.

- The MPLS VPN architecture offers SPs a peer-to-peer VPN architecture that combines the best features of overlay VPNs (support for overlapping customer address spaces) with the best features of peer-to-peer VPNs.
- There are three such features:
  - •PE routers participate in customer routing, guaranteeing optimum routing between customer sites.
  - •PE routers use a separate virtual routing table for each customer, resulting in perfect isolation between customers.
  - •Customers can use overlapping addresses.

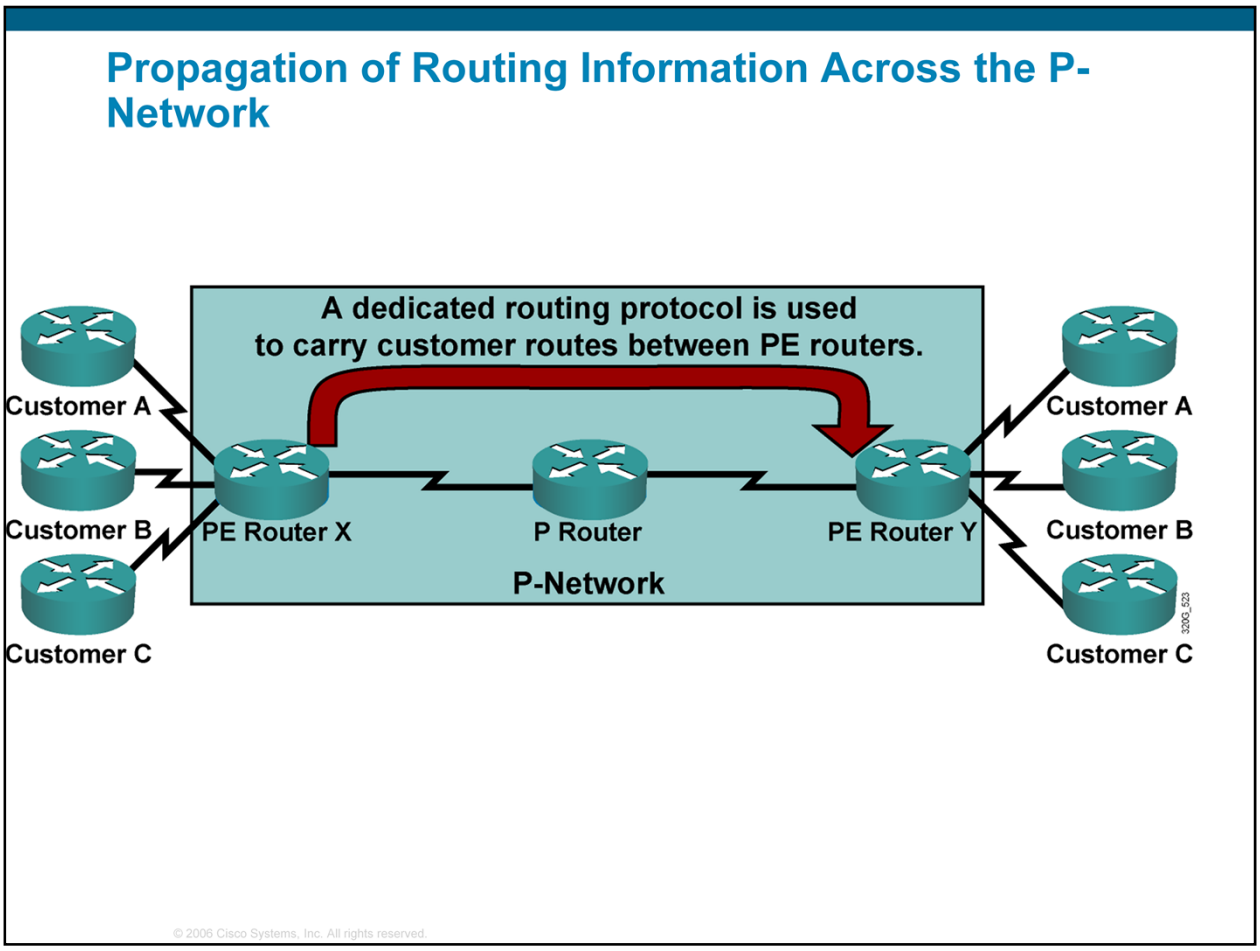


- For the sake of understanding terms, this graphic illustrates a simple MPLS VPN:
  - •There are two parts of the network: a customer-controlled part (the C-network) and a provider-controlled part (the P-network).
  - •Contiguous portions of the C-network are called sites and are linked with the P-network via CE routers (Customer A Site 2, Customer A Site 3, and so on). The CE routers connect to the PE routers that serve as the edge devices of the P-network. The core devices in the P-network that are the provider routers provide transport across the provider backbone and do not carry customer routes.

PE Router Architecture

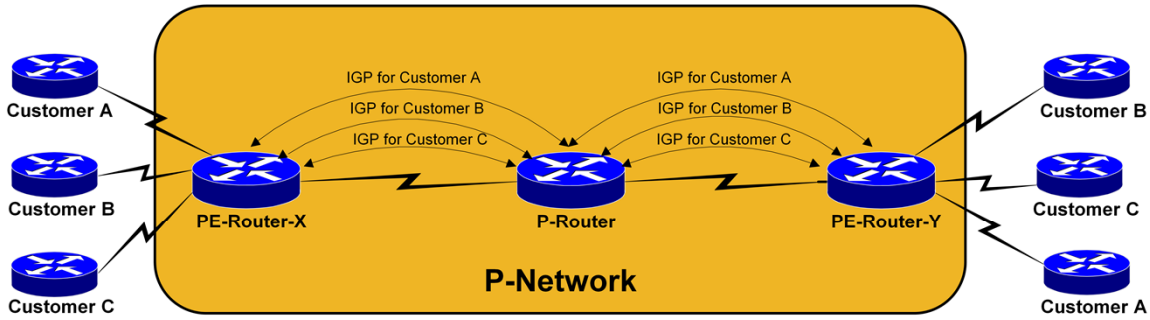


- The architecture of a PE router in an MPLS VPN is very similar to the architecture of a POP in the dedicated PE router peer-to-peer model. The only difference is that the whole PE router architecture is condensed into one physical device.
- Each customer is assigned an independent routing table, or virtual routing and forwarding (VRF) table. This routing table corresponds to the dedicated PE router in the traditional peer-to-peer model. Routing across the provider backbone is performed by another routing process that uses a global IP routing table.
- The MPLS VPN architecture offers the best features of both overlay VPNs and peer-to-peer VPNs. The next topic describes propagation of routing information across the P-Network.



- Although VRFs provide isolation between customers, the data from these routing tables still needs to be exchanged between PE routers to enable data transfer between sites that are attached to different PE routers. Therefore, you must choose a routing protocol that will transport all customer routes across the P-network, while maintaining the independence of individual customer address spaces.
- The best solution to the customer route propagation issue is to run a single routing protocol between PE routers that will exchange all customer routes without the involvement of the P routers.
- This solution is scalable. There are benefits to this approach:
    - The number of routing protocols running between PE routers does not increase with an increasing number of customers.
    - The P routers do not carry customer routes.
- The next design decision is the choice of the routing protocol running between PE routers. Because the total number of customer routes is expected to be very large, the only well-known protocol with the required scalability is Border Gateway Protocol (BGP). Therefore, BGP is used in MPLS VPN architecture to transport customer routes directly between PE routers.

Routing Information Propagation Across P-Network



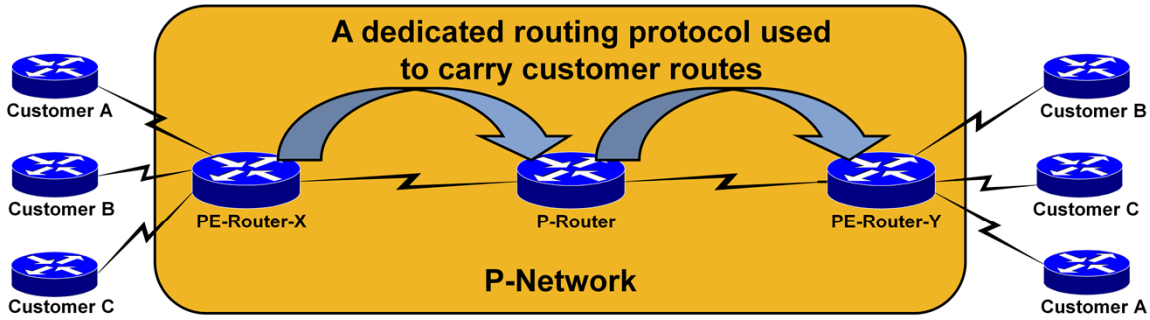
Q: How will PE routers exchange customer routing information?

A1: Run a dedicated IGP for each customer across P-network.

Wrong answer:

- **The solution does not scale.**
- **P-routers carry all customer routers.**

Routing Information Propagation Across P-Network



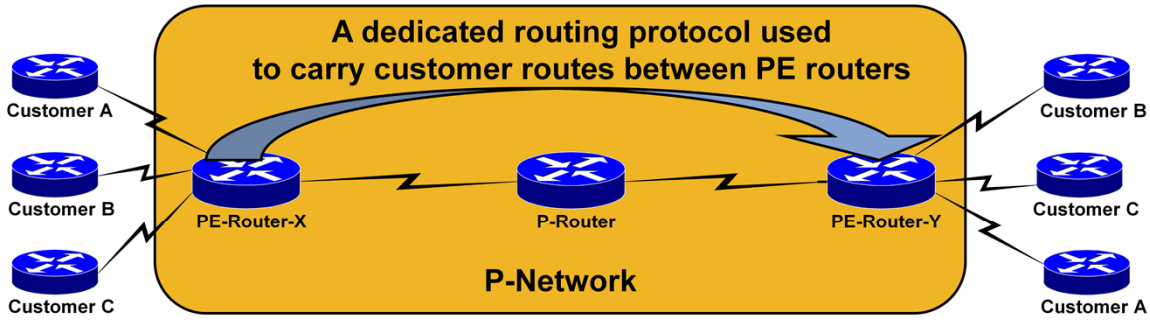
Q: How will PE routers exchange customer routing information?

A2: Run a single routing protocol that will carry all customer routes inside the provider backbone.

Better answer, but still not good enough

- P-routers carry all customer routers.

Routing Information Propagation Across P-Network



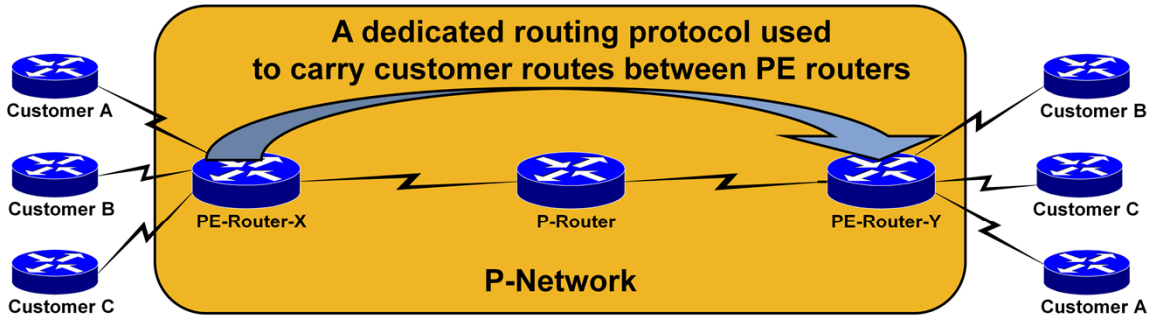
Q: How will PE routers exchange customer routing information?

A3: Run a single routing protocol that will carry all customer routes between PE routers. Use MPLS labels to exchange packets between PE routers.

The best answer

- P-routers do not carry customer routes, the solution is scalable.

Routing Information Propagation Across P-Network



Q: Which protocol can be used to carry customer routes between PE-routers?

A: The number of customer routes can be very large. BGP is the only routing protocol that can scale to a very large number of routes.

Conclusion:

BGP is used to exchange customer routes directly between PE routers.

Route Distinguishers

Question?	**How will information about the overlapping subnetworks of two customers be propagated via a single routing protocol?**
Answer:	**Extend the customer addresses to make them unique.**

- The 64-bit RD is prepended to an IPv4 address to make the address globally unique.
- The resulting address is a VPNv4 address.
- VPNv4 addresses are exchanged between PE routers via BGP.
- BGP that supports address families other than IPv4 addresses is called multiprotocol BGP (MPBGP).

- MPLS VPN architecture differs from traditional peer-to-peer VPN solutions in the support of overlapping customer address spaces. By deploying the BGP single routing protocol to exchange all customer routes between PE routers, an important question arises. How can BGP propagate several identical prefixes belonging to different customers between PE routers?
- The only solution to this dilemma is the expansion of customer IP prefixes with a unique prefix that makes the addresses unique even if the addresses had previously overlapped. MPLS VPNs use a 64-bit prefix called the route distinguisher (RD) to convert non-unique 32-bit customer IPv4 addresses into 96-bit unique addresses that can be transported between PE routers.
- The RD is used only to transform non-unique 32-bit customer IPv4 addresses into unique 96-bit VPN version 4 (VPNv4) addresses. These addresses are also called VPN IPv4 addresses.
- VPNv4 addresses are exchanged only between PE routers; the addresses are never used between CE routers. The BGP session between PE routers must therefore support the exchange of traditional IPv4 prefixes and the exchange of VPNv4 prefixes. A BGP session between PE routers must support multiple protocols, so an MPBGP session is established.

VPNV4 address

- BGP uses VPNv4 address to carry MPLS-VPN routers to IPv4 networks

- VPNv4 address =

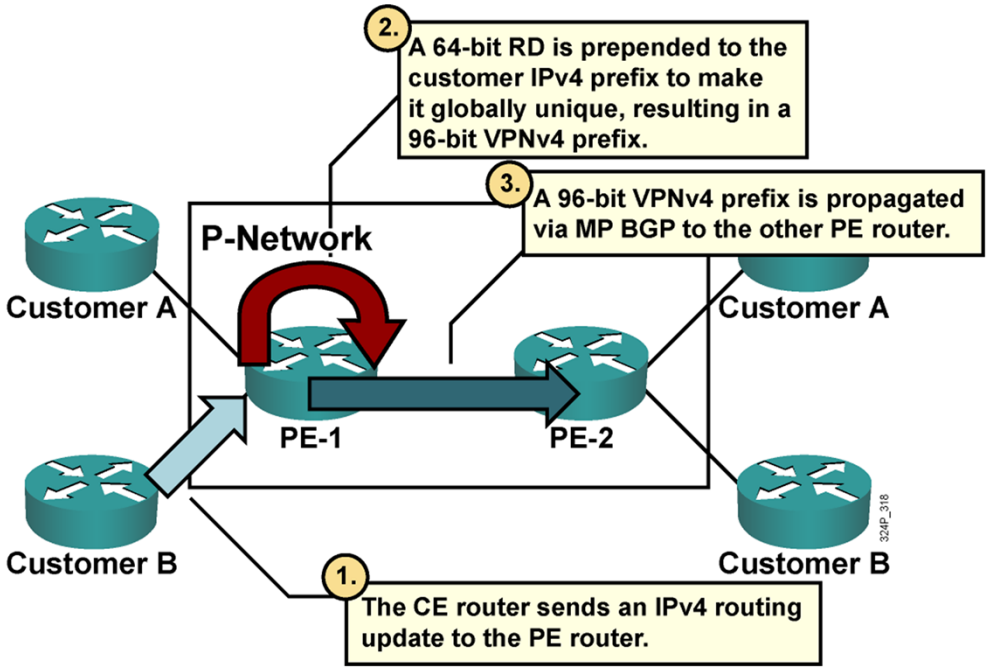
12 byte route distinguisher + 4 byte IPv4 address

RD represents ASN:nn

R1(config)#ip vrf customer

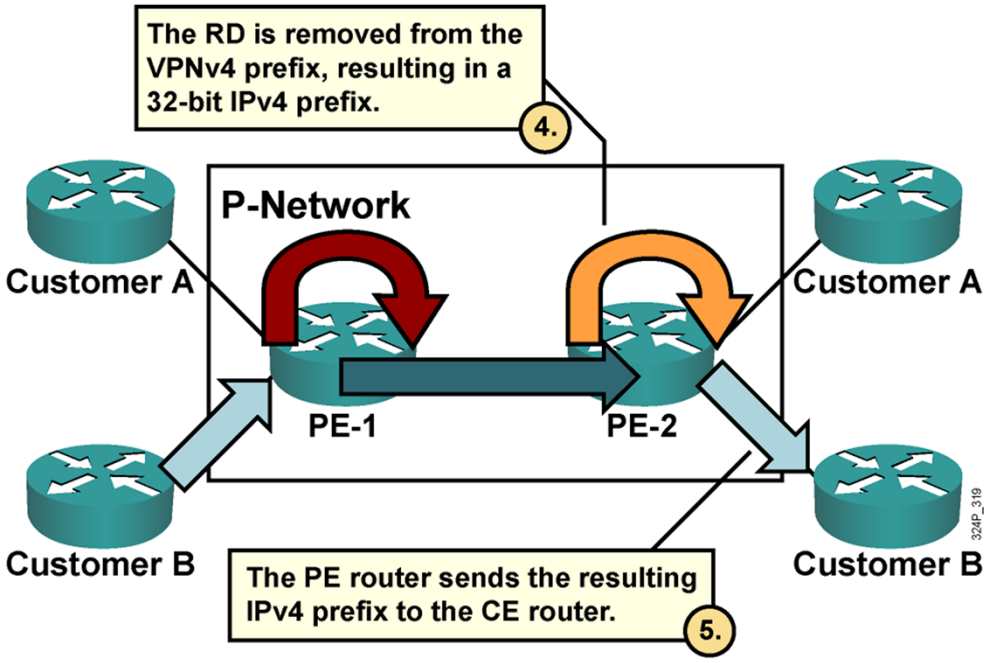
R1(config-vrf)#rd 100:1

Distinguishing Routes: Steps 1, 2, and 3



- The first three steps for customer route propagation across an MPLS VPN network:
  1. The CE router sends an IPv4 routing update to the PE router.
  2. The PE router prepends a 64-bit RD to the IPv4 routing update, resulting in a globally unique 96-bit VPNv4 prefix.
  3. The VPNv4 prefix is propagated via an MPBGP session to other PE routers.

Distinguishing Routes: Steps 4 and 5

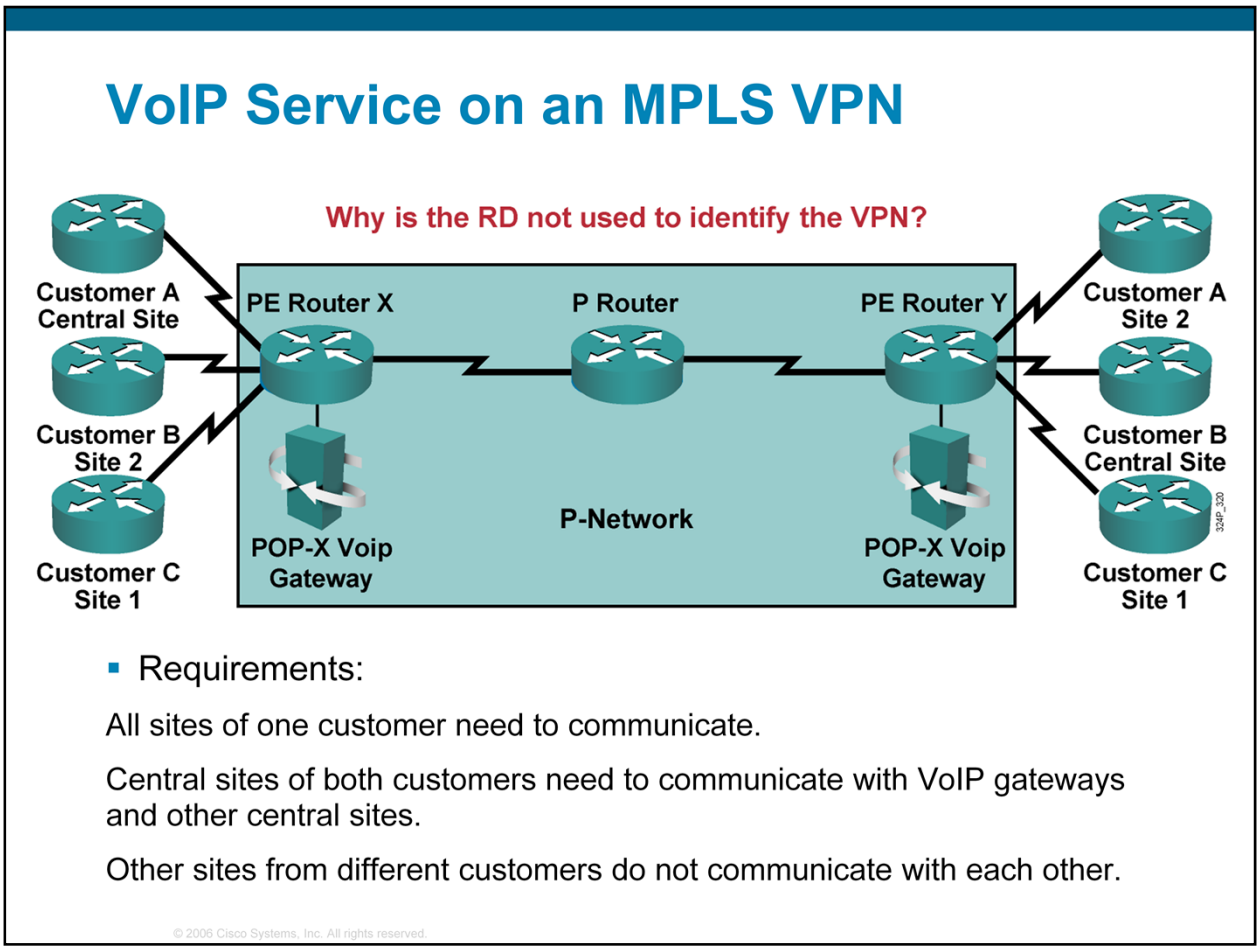


- The next two steps:
  4. The receiving PE routers strip the RD from the VPNv4 prefix, resulting in an IPv4 prefix.
  5. The IPv4 prefix is forwarded to other CE routers within an IPv4 routing update

Using RDs in an MPLS VPN

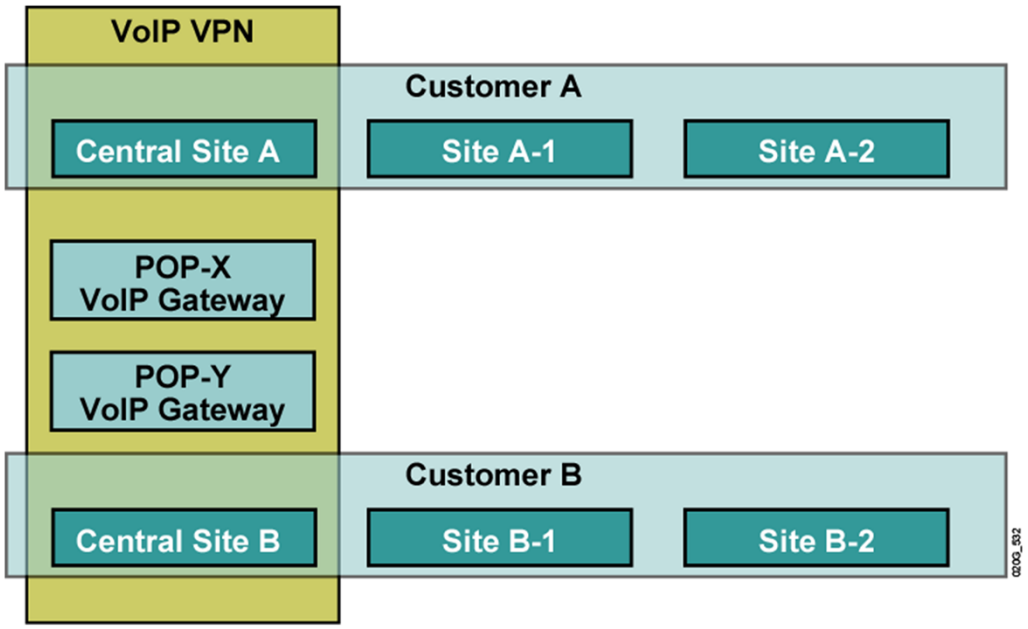
- The RD has no special meaning or role in MPLS VPN architecture.
- The RD is used only to make potentially overlapping IPv4 addresses globally unique.
- This design cannot support all topologies that are required by the customer.

- The RD has no special meaning or role in MPLS VPN architecture. The only function of the RD is to make overlapping IPv4 addresses globally unique.
- The RD is configured at the PE router as part of the setup of the VPN site. The RD is not configured on the CE and is not visible to the customer.
- Simple VPN topologies require only one RD per customer. This requirement makes it possible for the RD to serve as a VPN identifier. This design, however, would not allow for the implementation of more complex VPN topologies, such as when a customer site belongs to multiple VPNs.



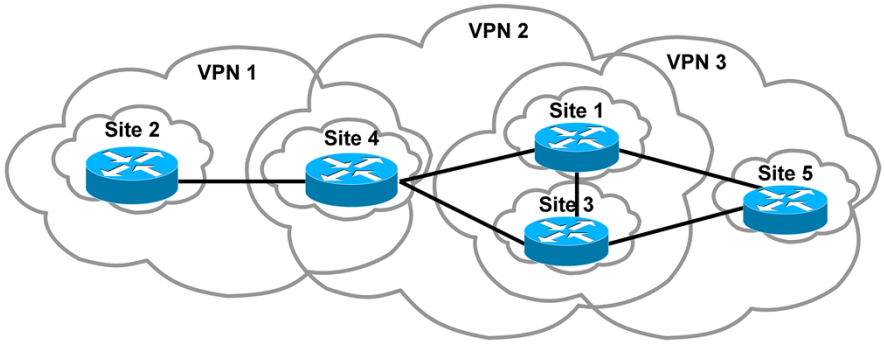
- To illustrate the need for a more versatile VPN indicator than the RD, consider the VoIP service. This topology illustrates the need for a more versatile VPN indicator than the RD. There are two connectivity requirements of the VoIP service:
  - •All sites of a single customer need to communicate.
  - •The central sites of different customers who subscribe to the VoIP service need to communicate with the VoIP gateways to originate and receive calls in the public voice network. The sites also need to communicate with other central sites to exchange inter-company voice calls.

Connectivity Requirements for VoIP Service



- This graphic illustrates the connectivity requirements of the VoIP service. Three VPNs are needed to implement the desired connectivity: two customer VPNs (Customer A and Customer B) and a shared VoIP VPN. These sites are related as follows:
  - •Central site A participates in the Customer A VPN and in the VoIP VPN.
  - •Central site B participates in the Customer B VPN and in the VoIP VPN.
  - •Customer sites A-1 and A-2 participate in Customer A VPN.
  - •Customer sites B-1 and B-2 participate in Customer B VPN.

Route Targets



- Some sites participate in more than one VPN.
- The RD cannot identify participation in more than one VPN.
- RTs were introduced in the MPLS VPN architecture to support complex VPN topologies.
- RTs are additional attributes that attach to VPNv4 BGP routes to indicate VPN membership.

- In this example there are five customer sites that are communicating within three VPNs. The VPNs can communicate with the following sites: VPN1 with Sites 2 and 4 VPN2 with Sites 1, 3, and 4 VPN3 with Sites 1,3, and 5
- Each VPN contains customer devices that are attached to the CE routers. These customer devices use VPNs to exchange information between devices. Only the PE routers are aware of the VPNs.
- Each VPN is associated with one or more VPN routing-forwarding instances (VRFs). A VRF defines the VPN membership of a customer site that is attached to a PE router. A VRF consists of an IP routing table, a derived CEF table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table.
- A one-to-one relationship does not necessarily exist between customer sites and VPNs. A given site can be a member of multiple VPNs. However, a site can only associate with one VRF. A customer site's VRF contains all the routes available to the site from the VPNs of which that site is a member.
- At this point, you may ask that since there is no one-to-one mapping between VPN and VRF, how does the router know which routes need to be inserted into which VRF? The introduction of another concept in the MPLS/VPN architecture, the route target, solves this dilemma. Every VPN route is tagged with one or more route targets when it is exported from a VRF (to be offered to other VRFs). You can also associate a set of route targets with a VRF, and all routes tagged with at least one of those route targets will be inserted into the VRF.
- Packet forwarding information is stored in the IP routing table and the CEF table for each VRF. A separate set of routing and CEF tables is maintained for each VRF. These tables prevent information from being forwarded outside a VPN and also prevent packets that

are outside a VPN from being forwarded to a router within the VPN.

- The distribution of VPN routing information is controlled using VPN route target communities, implemented by BGP extended communities. Distribution of VPN routing information follows two steps:
- When a VPN route that is learned from a CE router is injected into BGP, a list of VPN route target (RT) extended community attributes are associated with the route. Typically, the list of route target community values is set from an export list of route targets that are associated with the VRF that the route was learned from.
- An import list of route target extended communities is associated with each VRF. The import list defines the route target extended community attributes that a route must have for the route to be imported into the VRF. For example, if the import list for a particular VRF includes route target communities A, B, and C, then any VPN route that carries any of those route target extended communities—A, B, or C—is imported into the VRF.
- RTs in the MPLS VPN architecture support the requirements for multi-VPN membership. RTs are attributes that are attached to a VPNv4 BGP route to indicate the route's VPN membership.
- The RD (a single entity prepended to an IPv4 route) cannot indicate that a site participates in more than one VPN. We need a method in which a set of VPN identifiers can be attached to a route to indicate the site's membership in several VPNs.

MPLS VPN Routing Criteria

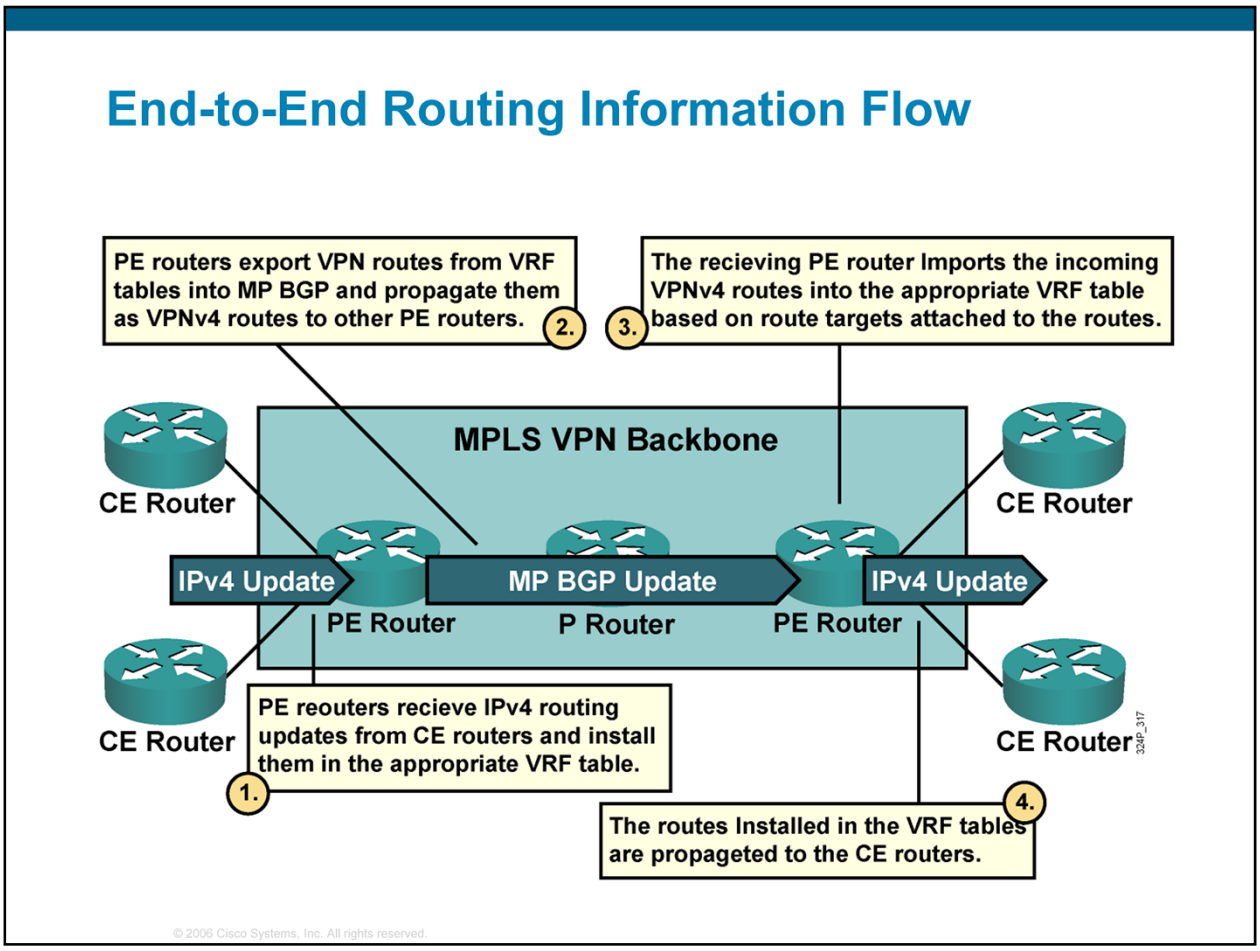
- Designers imposed these criteria on MPLS VPNs:

  CE routers can only run standard IP routing software.

  Only PE routers need to support MPLS VPN services and Internet routing.

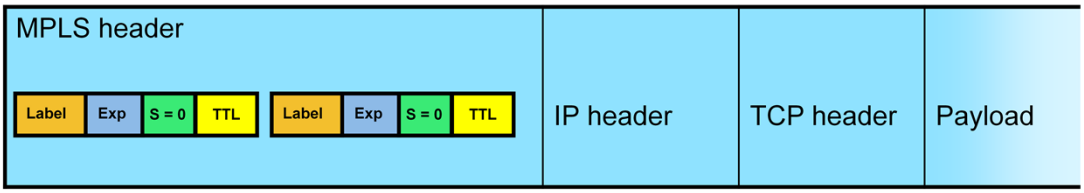
  P routers have no VPN routes.

- The designers of MPLS VPN technology aimed to meet these criteria:
  - •CE routers should not be MPLS VPN-aware; they should run standard IP routing software.
  - •PE routers must support MPLS VPN services and traditional Internet services.
  - •To make the MPLS VPN solution scalable, P routers must not carry VPN routes.



- These steps describe the stages of routing information flow. The flow goes from the IPv4 routing updates entering the MPLS VPN backbone through their propagation as VPNv4 routes across the backbone:
    1. PE routers receive IPv4 routing updates from the CE routers and install the updates in the appropriate VRF table.
    2. The customer routes from VRF tables are exported as VPNv4 routes into MPBGP and propagated to other PE routers.
    3. The PE routers receiving MPBGP updates import the incoming VPNv4 routes into their VRF tables based on RTs that are attached to the incoming routes and on import RTs that are configured in the VRF tables.
    4. The VPNv4 routes that are installed in the VRF tables are converted to IPv4 routes and then propagated to the CE routers.
- The CE routers, PE routers, and P routers have specific requirements for end-to-end routing information flow.

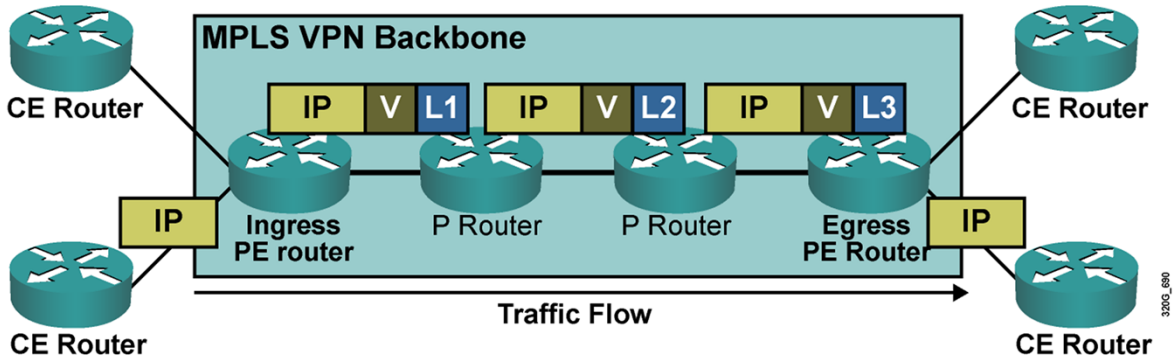
MPLS Label Stack



- Each Label entry contains four fields:
  - Label: A 20-bit label value
  - Exp: A 3-bit field for QoS priority
  - S = 0: A 1-bit bottom of stack flag to signify whether the label is at the bottom of the stack
  - TTL: An 8-bit TTL field

- MPLS works by prepending packets with an MPLS header, containing one or more “labels.” This is called a label stack. You can use an MPLS label stack to tell the egress PE router what to do with the VPN packet. The ingress PE router labels each VPN packet with a label uniquely identifying the egress PE router. The PE router sends the VPN packet across the network and all the routers in the network subsequently switch labels without having to look into the packet itself.
- The graphic represents an MPLS label with two labels in the stack.

MPLS VPNs and Packet Forwarding



- The PE routers label the VPN packets with a label stack, as follows:
  - Using the LDP label for the egress PE router as the top label
  - Using the VPN label that is assigned by the egress PE router as the second label in the stack

- When using the label stack, the ingress PE router labels the incoming IP packet with two labels:
- The **top label in the stack is the LDP label for normal frame forwarding in the MPLS network**. This label guarantees that the packet will traverse the MPLS VPN backbone and arrive at the egress PE router.
- The **second label in the stack identifies the egress PE router**. This label tells the router **how** to forward the incoming VPN packet. The second label can point directly toward an outgoing interface. In this case, the egress PE router performs label lookup only on the VPN packet. The second label can also point to a VRF table. For this case, the egress PE router first performs a label lookup to find the target VRF table and then performs an IP lookup within the VRF table.
- **When you are implementing MPLS VPN, you need to increase the MTU size to allow for two labels**.
- The second label in the stack points toward an outgoing interface whenever the CE router is the next hop of the VPN route. **The second label in the stack points to the VRF table for aggregate VPN routes**, VPN routes pointing to a null interface, and routes for directly connected VPN interfaces.
- The two-level MPLS label stack satisfies these MPLS VPN forwarding requirements:
- **The P routers perform label switching on the LDP-assigned label toward the egress PE router**.
- The **egress PE router performs label switching on the second label** (which the router has previously assigned), and either forwards the IP packet toward the CE router or performs another IP lookup in the VRF table that the second label in the stack points to.

Summary

- VPNs allow you to use the shared infrastructure of a SP to implement your private networks. There are two implementation models: overlay and peer-to-peer.
- The MPLS VPN architecture offers SPs a peer-to-peer VPN architecture that combines the best features of overlay VPNs with the best features of peer-to-peer VPNs.
- MPLS VPNs use a 64-bit prefix called the route distinguisher (RD) to convert non-unique 32-bit customer IPv4 addresses into 96-bit unique addresses that can be transported.
- MPLS works by prepending packets with an MPLS header, containing one or more “labels.” This is called a label stack.