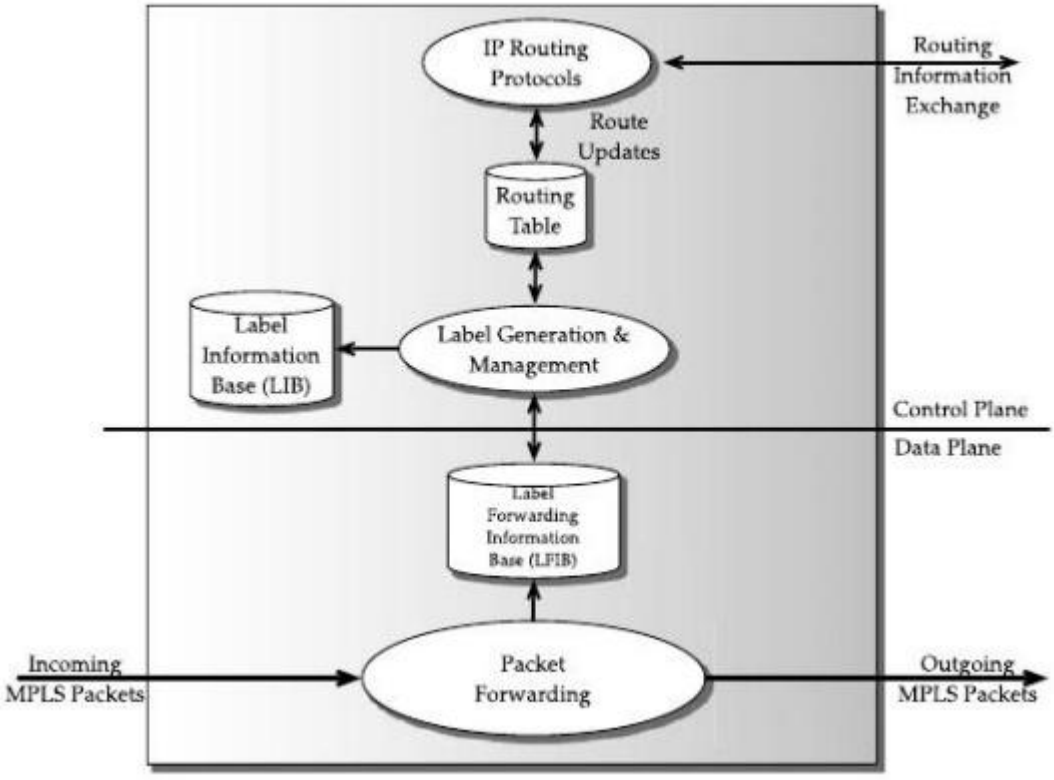
Nowdays, most network engineers/specialists consider MPLS (MultiProtocol Label Switching) one of the most promising transport technologies. Then, what is MPLS ? Multi Protocol Label Switching (MPLS) is a data-carrying mechanism to perform label switching that belongs to the family of packet-switched networks. MPLS operates at an OSI Model layer that is generally considered to lie between traditional definitions of Layer 2 (data link layer) and Layer 3 (network layer), and thus is often referred to as a "Layer 2.5" protocol. It combines the benefits of packet forwarding based on Layer 2 switching with the benefits of Layer 3 routing. Similar to Layer 2 networks (for example, Frame Relay or ATM), MPLS assigns labels to packets for transport across packet- or cell-based networks. The forwarding mechanism throughout the network is label swapping, in which units of data (for example, a packet or a cell) carry a short, fixed-length label that tells switching nodes along the packets path how to process and forward the data. And, 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.
Briefly, MPLS adds a label in front of a packet, i.e., as another header so that routers know how to act based on this label. To be able to act based on a label, routers must be label-switched routers (LSRs), and each LSR must maintain a valid mapping from the label of an incoming packet ("incoming label") to a label to be attached to the packet before being sent out ("output label"). This, in turn, means that LSRs maintain states in terms of input/output labels associated with a particular path, referred to as a label-switched path (LSP), which may be designated for a particular class of traffic flows. Note that an LSP must already be established between two routers so that packets can follow this path. To establish a path, a label distribution protocol is used. Certainly, the next question then is: how do we know this is the best path for the particular class of traffic flows ? This will depend on the traffic engineering requirements of the network, and on the service requirements of the traffic flow to be carried by the LSP.




Conceptual

architecture of an MPLS label-switched router
The MPLS architecture is split into two separate components: the control component (also called the control plane) and the forwarding component (also called the data plane). The control component/control plane is responsible for creating and maintaining label-forwarding information (referred to as bindings) among a group of interconnected label switches, which IP routing protocols can exchange routing information, and another component manages label distribution and binding. It also maintains a label information base (LIB), and creates a label forwarding information base (LFIB). The forwarding component/data plane uses a label-forwarding database maintained by a label switch to perform the forwarding of data packets based on labels carried by packets, which packet arriving on the data plane consults the LFIB for proper forwarding in an outgoing direction.
It may be noted that the establishment of an LSP is a connection-oriented functionality--that is, a path must be set up before traffic can use this path. An established LSP may or may not have any packet traffic flow on it; furthermore, the packet traffic flow rate on an LSP can vary from one instant of time to another. Many traffic flows may be combined on a specific LSP; usually, such a flow aggregation is based on some affinity, such as a traffic class. The aggregated flow constructed on some affinity basis is referred to as a traffic trunk. Typically, a traffic trunk is defined on an ingress/egress LSR pair basis and is carried on an LSP. Note that all traffic between the same two ingress/egress LSRs may be split into multiple traffic trunks; each traffic trunk is then mapped into an LSP. Thus, a traffic trunk is a logical entity, while an LSP is a transport manifestation of this logical entity.
And, in briefly we can conclude the benefits of running MPLS in your network, these benefits include the following:

- The use of one unified network infrastructure
- Better IP over ATM integration
- Border Gateway Protocol (BGP)-free core
- The peer-to-peer model for MPLS VPN
- Optimal traffic flow
- Traffic engineering

Then, let's define VPN, Virtual Private Network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits which emulates a private network over a common infrastructure. The VPN might provide communication at OSI Layer 2 or 3. The link-layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features. A VPN may have best-effort performance, or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point.

**MPLS-based Virtual Private Network (MPLS VPN)**

The VPN usually belongs to one company and has several sites interconnected across the common service provider infrastructure. The private network requires that all customer sites are able to interconnect and are completely separate from other VPNs. That is the minimum connectivity requirement. However, VPN models at the IP layer might require more than that. They can provide connectivity between different VPNs when that is wanted and even provide connectivity to the Internet. MPLS VPN offers all of this. MPLS VPNs are made possible because the service provider runs MPLS in the backbone network, which supplies a decoupling of forwarding plane and control plane that IP does not.

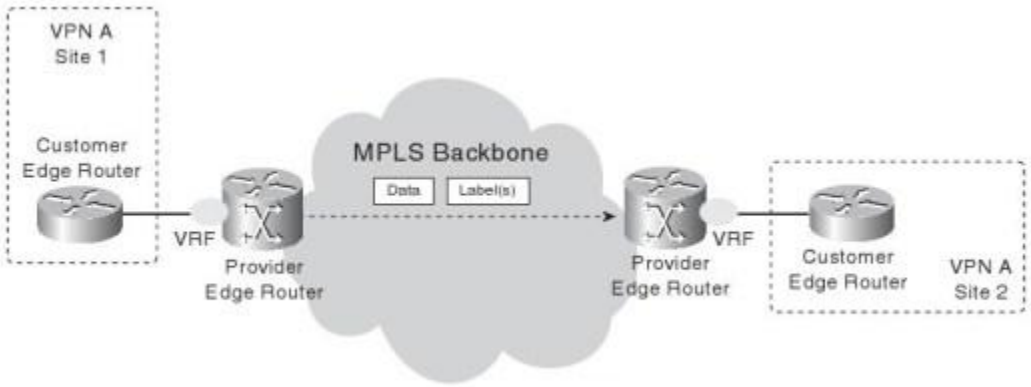
Basically, every VPN's client wants a VPN service provider to connect its networks and ensure that the resulting internet is isolated from the networks of other clients. Then, MPLS VPN technology rise to serve the paradox of ensuring isolation while preserving the connectivity, which is the solution came quite elegant: by automatically filtering routing advertisements and using MPLS tunnels for transmitting client traffic through the internal network of the provider.

Commonly, there are two types of MPLS VPN:

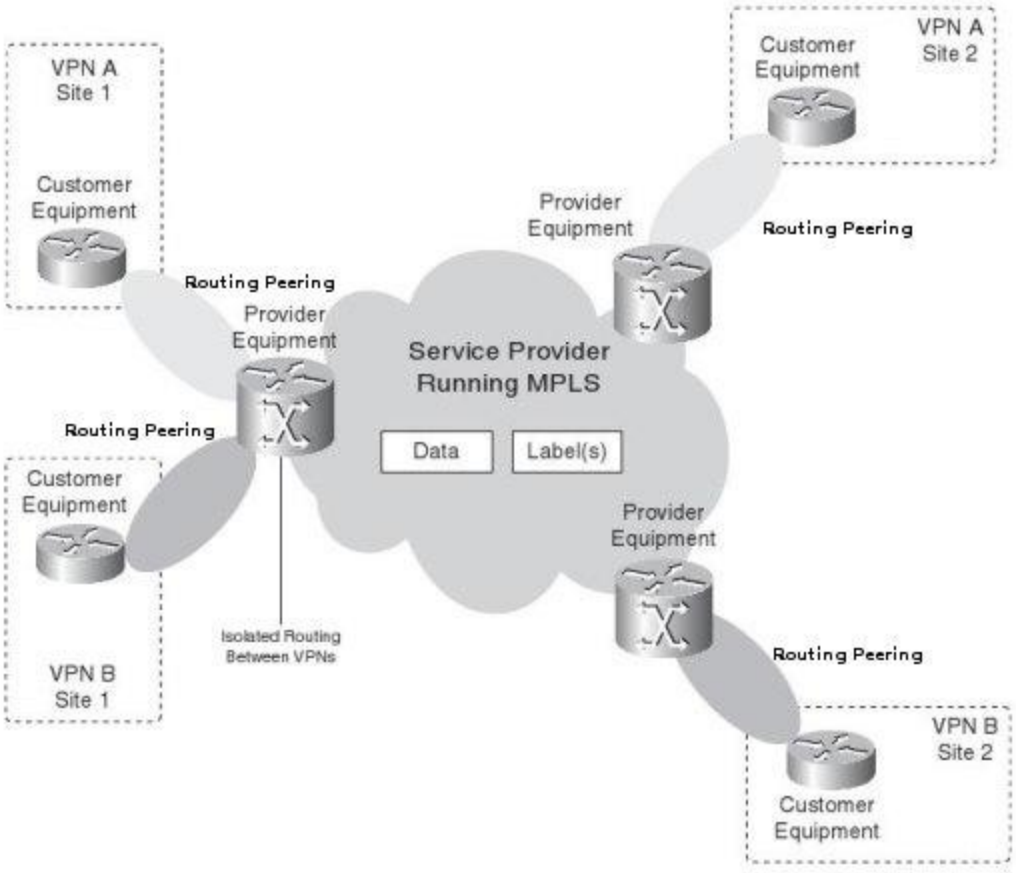
1. MPLS L3VPN, where traffic delivery from client to the boundary device of the provider network is carried out using IP technology (layer 3).2. MPLS L2VPN, where client traffic is transmitted into the provider network using any of the layer 2 technologies, for example, Ethernet, Frame Relay or ATM.

In both cases, transmission ofthe client traffic within the provider network is carried out using MPLS technology. And in the real world, MPLS L3VPN implementation is more dominant than MPLS L2VPN deployed by provider networks because its maturity and reliability.

MPLS VPN architecture using peer-to-peer VPN model (in the peer-to-peer VPN model, the service provider routers not only carry the customer data across the network, but they also participate in the customer routing. In other words, the service provider routers peer directly with the customer routers at Layer 3. The result is that one routing protocol neighborship or adjacency exists between the customer and the service provider router) less time and effort. With MPLS VPN, one customer router, called the customer edge (CE) router, peers at the IP Layer with at least one service provider router, called the provider edge (PE) router. The privateness in MPLS VPN networks is achieved by using the concept of virtual routing forwarding (VRF) and the fact that the data is forwarded in the backbone as labeled packets. The VRFs ensure that the routing information from the different customers is kept separate, and the MPLS in the backbone ensures that the packets are forwarding based on the label information and not the information in the IP header. Picture below shows the concept of VRFs and forwarding labeled packets in the backbone of a network that is running MPLS VPN.




MPLS VPN with VRF

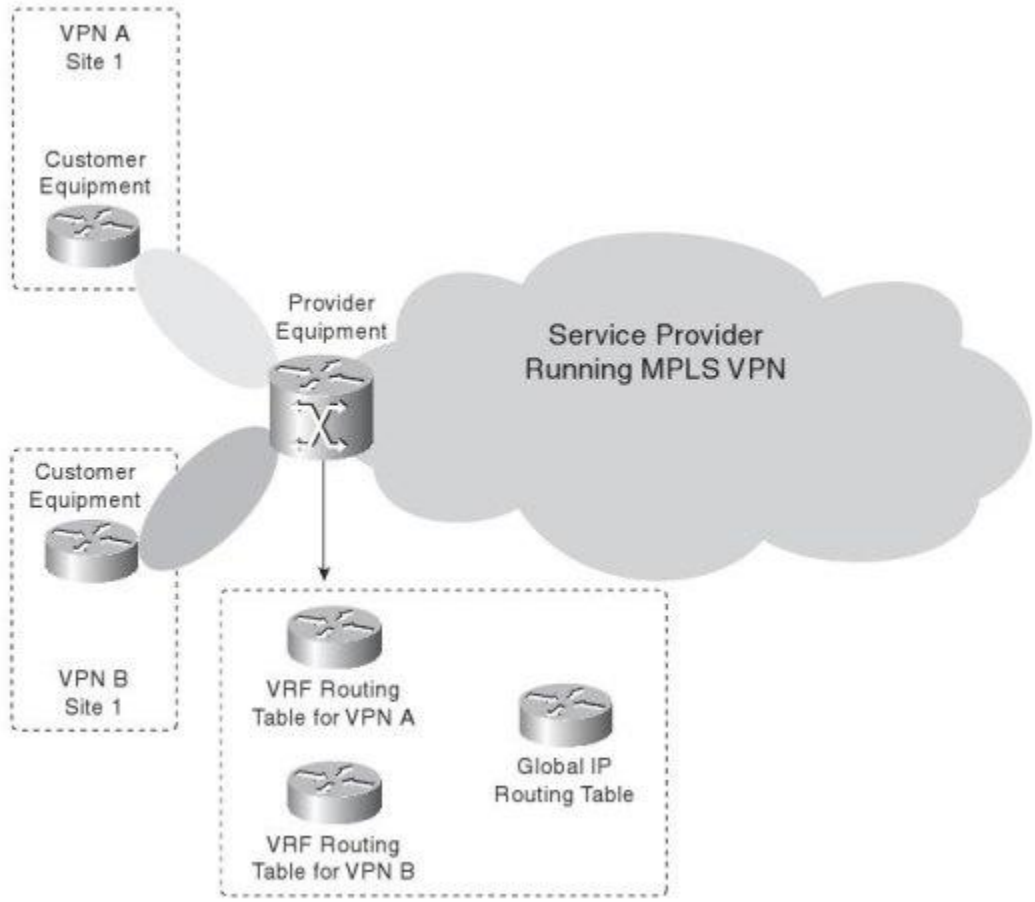



Peer-to-Peer MPLS VPN Model

To achieve MPLS VPN, it need some basic building blocks on the PE routers. These building blocks are the following: VRF, route distinguisher (RD), route targets (RT), route propagation through MP-BGP, and forwarding of labeled packets.

**- Virtual Routing Forwarding (VRF)**

A PE router has a VRF instance for each attached VPN. PE router holds the global IP routing table, but also a VRF routing table per VPN connected to the PE. Because the routing should be separate and private for each customer (VPN) on a PE router, each VPN should have its own routing table. This private routing table is called the VRF routing table. The interface on the PE router toward the CE router can belong to only one VRF, as such, all IP packets received on the VRF interface are unambiguously identified as belonging to that VRF.




VRFs on a PE Router

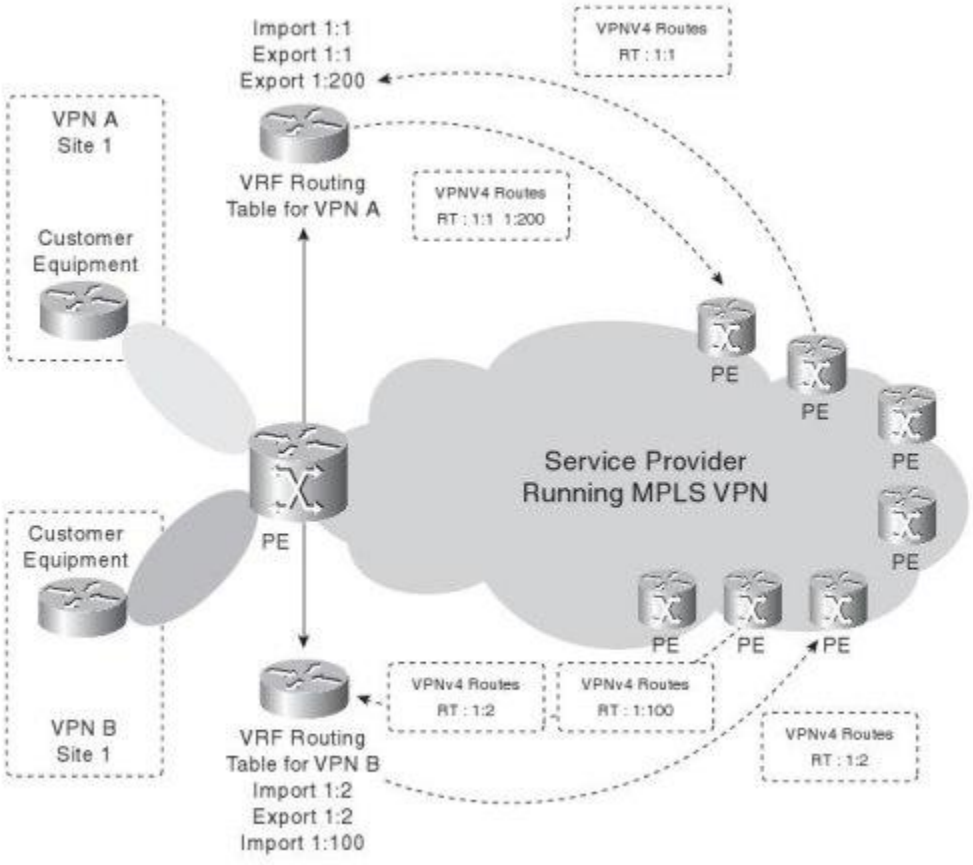
**- Route Distinguisher (RD)**

The VPN prefixes are propagated across the MPLS VPN network by Multiprotocol BGP (MP-BGP). The problem is that when BGP carries these IPv4 prefixes across the service provider network, they must be unique. If the customers had overlapping IP addressing, the routing would be wrong. To solve this problem, the concept of RDs was conceived to make IPv4 prefixes unique. The basic idea is that each prefix from each customer receives a unique identifier (the RD) to distinguish the same prefix from different customers. A prefix derived from the combination of the IPv4 prefix and the RD is called a vpnv4 prefix. MP-BGP needs to carry these vpnv4 prefixes between the PE routers.

An RD is a 64-bit field used to make the VRF prefixes unique when MP-BGP carries them. The RD does not indicate which VRF the prefix belongs to. The function of the RD is not that of a VPN identifier, because some more complex VPN scenarios might require more than one RD per VPN. Each VRF instance on the PE router must have one RD assigned to it. This 64-bit value can have two formats: ASN:nn or IP-address:nn, where nn represents a number. The most commonly used format is ASN:nn, where ASN stands for autonomous system number. Usually, the service provider uses ASN:nn, where ASN is the autonomous system number that the Internet Assigned Numbers Authority (IANA) assigns to the service provider and nn is the number that the service provider uniquely assigns to the VRF. The RD does not impose semantics; it is just used to uniquely identify the VPN routes. This is needed because the IPv4 routes from one customer might be overlapping with the IPv4 routes from another. The combination of the RD with the IPv4 prefix provides a vpnv4 prefix, of which the address is 96 bits long. The mask is 32 bits long, just as it is for an IPv4 prefix. If you take an IPv4 prefix 10.1.1.0/24 and an RD 1:1, the vpnv4 prefix becomes 1:1:10.1.1.0/24.
One customer might use different RDs for the same IPv4 route. When a VPN site is connected to two PE routers, routes from the VPN site might get two different RDs, depending on which PE router the routes are received. Each IPv4 route would get two different RDs assigned and would have two completely different vpnv4 routes. This would allow BGP to see them as different routes and apply a different policy to the routes.

**- Route Target (RT)**

If RDs were just used to indicate the VPN, communication between sites of different VPNs would be problematic. A site of Company A would not be able to talk to a site of Company B because the RDs would not match. The concept of having sites of Company A being able to talk to sites of Company B is called extranet VPN. The simple case of communication between sites of the same company--the same VPN--is called intranet. The communication between sites is controlled by another MPLS VPN feature called RTs.
An RT is a BGP extended community that indicates which routes should be imported from MP-BGP into the VRF. Exporting an RT means that the exported vpnv4 route receives an additional BGP extended community--this is the RT--as configured under ip vrf on the PE router, when the route is redistributed from the VRF routing table into MP-BGP. Importing an RT means that the received vpnv4 route from MP-BGP is checked for a matching extended community--this is the route target--with the ones in the configuration. If the result is a match, the prefix is put into the VRF routing table as an IPv4 route. If a match does not occur, the prefix is rejected.
Picture below shows that the RTs control which routes are imported into which VRFs from the remote PE routers and with which RTs the vpnv4 routes are exported toward the remote PE routers. More than one RT might be attached to the vpnv4 route. For the import into the VRF to be permitted, only one RT from the vpnv4 route needs to be matched with the configuration of the imported RTs under the ip vrf section on the PE router.




RTs

**- Route Propagation**

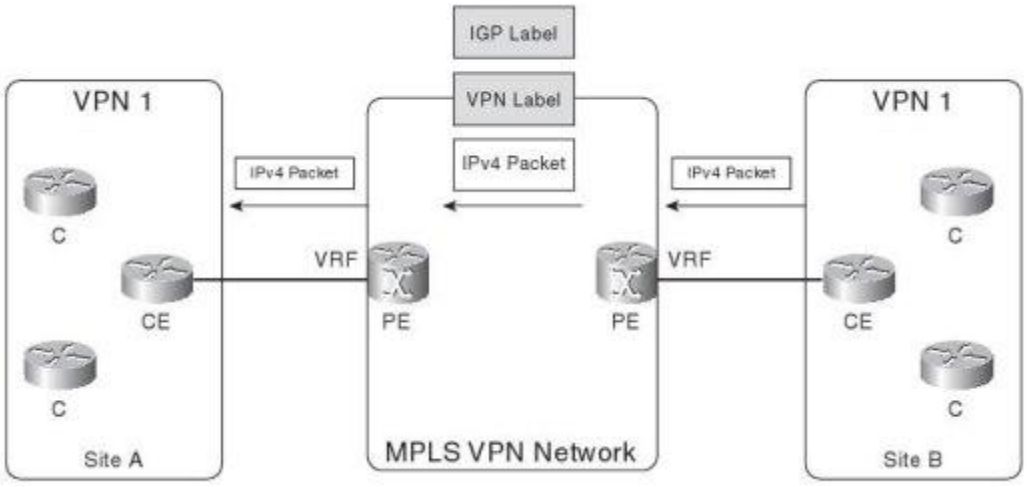
The VRF separates the customer routes on the PE routers, but how are the prefixes transported across the service provider network ? The answer is using Multiprotocol BGP (MP-BGP), because potentially, numerous routes--perhaps hundred of thousands--could be transported, BGP is the ideal candidate because it is a proven and stable routing protocol for carrying that many routes. Just realize that BGP is the standard routing protocol for carrying the complete Internet routing table. Because the customer VPN routes are made unique by adding the RD to each IPv4 route--turning them into vpnv4 routes--all customer routes can safely be transported across the MPLS VPN network.

**- Forwarding of Labeled Packets**

The provider core routers cannot forward the packets as pure IP packets between sites, because they do not have the VRF information from each site. MPLS can solve this problem by labeling the packets. The provider core routers must then have only the correct forwarding information for the label to forward the packets. The most common way is to configure Label Distribution

Protocol (LDP) between all provider core and PE routers so that all IP traffic is label-switched between them. The IP packets are then label-forwarded with one label from ingress PE router to egress PE router. A provider core router never has to perform a lookup of the destination IP address. This is the way the packets are switched between the ingress PE and egress PE router. This label is called the IGP label, because it is the label that is bound to an IPv4 prefix in the global routing table of the P and PE router, and the IGP of the service provider network advertises it.

Picture below shows the packet forwarding in an MPLS VPN network. The packet enters the PE router on the VRF interface as an IPv4 packet. It is forwarded throughout the MPLS VPN network with two labels. Provider core routers forward the packet by looking at the top label. The top label is swapped at each Provider core router. The labels are stripped off at the egress PE router and the packet is forwarded as an IPv4 packet onto the VRF interface toward the CE router. The correct CE router is found by looking at the VPN label.




Packet Forwarding in an MPLS VPN Network