1.2.d WAN

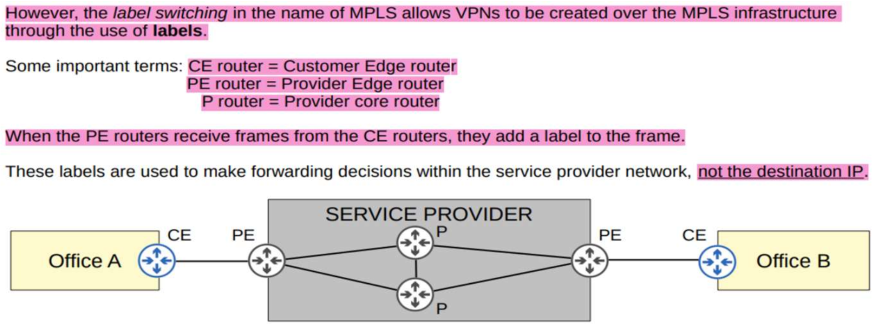
Wide Area Network (WAN) is a network that extends over a large geographic area and connects separate LANs.

The internet could be considered a WAN, WANs are more commonly used to enterprises' private connections between their sites.

There are two main types of WAN connection:

- **Leased Line: Point-to-point** serial link (High-level Data Link Control HDLC, or Point-to-Point PPP encapsulation) between offices over the Service Provider's network. There are standards provide different speeds:
  - In North America: T1 (1.544 Mbps), T2 (6.312 Mbps), T3 (44.736 Mbps).
  - In Europe: E1 (2.048 Mbps), E2 (8.448 Mbps), E3 (34.368 Mbps).

- Multiple Protocol Label Switching (**MPLS**): uses a **shared core infrastructure from the service provider**. Many different technologies can be used to connect to a service provider's MPLS network for WAN service (4G/5G, Cable TV, Serial, Ethernet/Fiber, etc.) When the Provider Edge (PE) router receives frames from the Customer Edge (CE) router, they add a label to the frame and these labels are used to make forwarding decisions over the service provider network, not the destination IP.



However, the *label switching* in the name of MPLS allows VPNs to be created over the MPLS infrastructure through the use of **labels**.

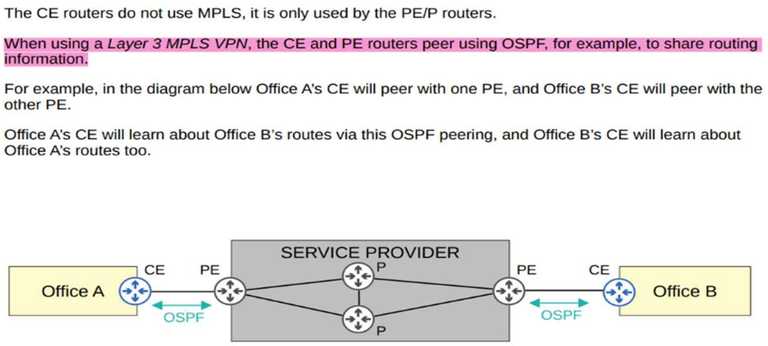
Some important terms: CE router = Customer Edge router
PE router = Provider Edge router
P router = Provider core router

When the PE routers receive frames from the CE routers, they add a label to the frame.

These labels are used to make forwarding decisions within the service provider network, not the destination IP.

Virtual Private Network (VPN) are often used with MPLS:

- **Layer 3 MPLS VPN**: The CE and PE routers peer using OSPF to share routing information. The provider's core routers are transparent to the customer.



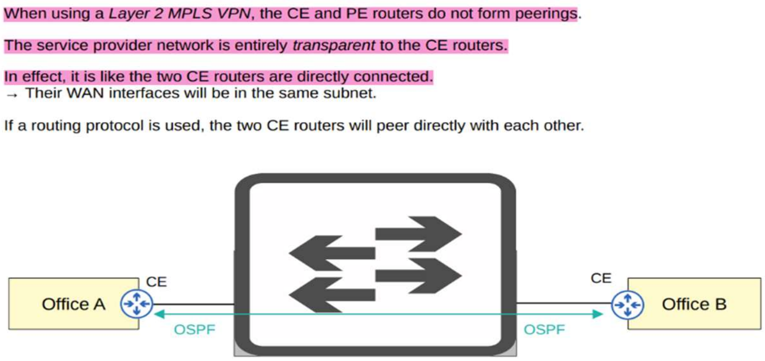
The CE routers do not use MPLS, it is only used by the PE/P routers.

When using a *Layer 3 MPLS VPN*, the CE and PE routers peer using OSPF, for example, to share routing information.

For example, in the diagram below Office A's CE will peer with one PE, and Office B's CE will peer with the other PE.

Office A's CE will learn about Office B's routes via this OSPF peering, and Office B's CE will learn about Office A's routes too.

- **Layer 2 MPLS VPN**: The service provider is transparent to the CE routers (all their network acts like a switch).



When using a *Layer 2 MPLS VPN*, the CE and PE routers do not form peerings.

The service provider network is entirely *transparent* to the CE routers.

In effect, it is like the two CE routers are directly connected.
→ Their WAN interfaces will be in the same subnet.

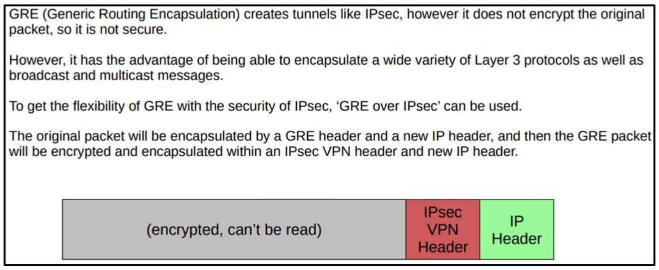
If a routing protocol is used, the two CE routers will peer directly with each other.

5.5 Describe IPsec remote access and site-to-site VPNs

There are two main VPN technologies used:

1. **Site-to-site VPN using IP security (IPsec)**: a VPN tunnel is created between two devices by encapsulating the encrypted original IP packet with a new VPN header and new IP header (original packet is encrypted before being encapsulated). A tunnel is formed only between two tunnel endpoints (for example, the two routers connected to the Internet). All other devices in each site don't need to create a VPN for themselves. They can send unencrypted data to their site's router, which will encrypt it and forward it in the tunnel as described above.

    a. GRE (Generic Routing Encapsulation) is able to encapsulate a wide variety of L3 protocols, as well as broadcast and multicast messages, therefore GRE over IPsec can be used. The original packet is encapsulated with GRE header, IP header then the GRE packet is encapsulated with an IPsec VPN header and another IP heade



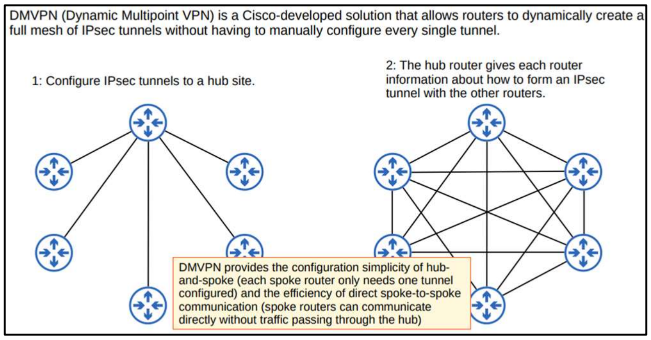
GRE (Generic Routing Encapsulation) creates tunnels like IPsec, however it does not encrypt the original packet, so it is not secure.

However, it has the advantage of being able to encapsulate a wide variety of Layer 3 protocols as well as broadcast and multicast messages.

To get the flexibility of GRE with the security of IPsec, 'GRE over IPsec' can be used.

The original packet will be encapsulated by a GRE header and a new IP header, and then the GRE packet will be encrypted and encapsulated within an IPsec VPN header and new IP header.

    b. DMVPN (Dynamic Multipoint VPN) is a Cisco-developed solution that allows routers to dynamically create a full mesh of IPsec tunnels without having to manually configure every single tunnel.



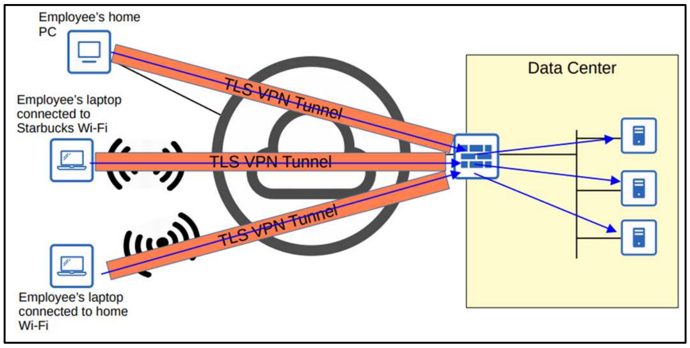
DMVPN (Dynamic Multipoint VPN) is a Cisco-developed solution that allows routers to dynamically create a full mesh of IPsec tunnels without having to manually configure every single tunnel.

1: Configure IPsec tunnels to a hub site.

2: The hub router gives each router information about how to form an IPsec tunnel with the other routers.

DMVPN provides the configuration simplicity of hub-and-spoke (each spoke router only needs one tunnel configured) and the efficiency of direct spoke-to-spoke communication (spoke routers can communicate directly without traffic passing through the hub)

2. **Remote-access VPNs** are used to allow end devices (PCs, mobile phones) to access the company's internal resources securely over the Internet. Remote-access VPNs typically use TLS (Transport Layer Security) VPN client software is installed on end devices, these end devices can then form secure tunnels to the company's router/firewalls acting as a TLS server



Employee's home PC
Employee's laptop connected to Starbucks Wi-Fi
Employee's laptop connected to home Wi-Fi
TLS VPN Tunnel
TLS VPN Tunnel
TLS VPN Tunnel
Data Center

	Remote Access	Site-to-Site
Typical security protocol	TLS	IPsec
Devices supported by one VPN (one or many)	One	Many
Typical use: on-demand or permanent	On-demand	Permanent