Wednesday, August 13, 2025 6:23 PM

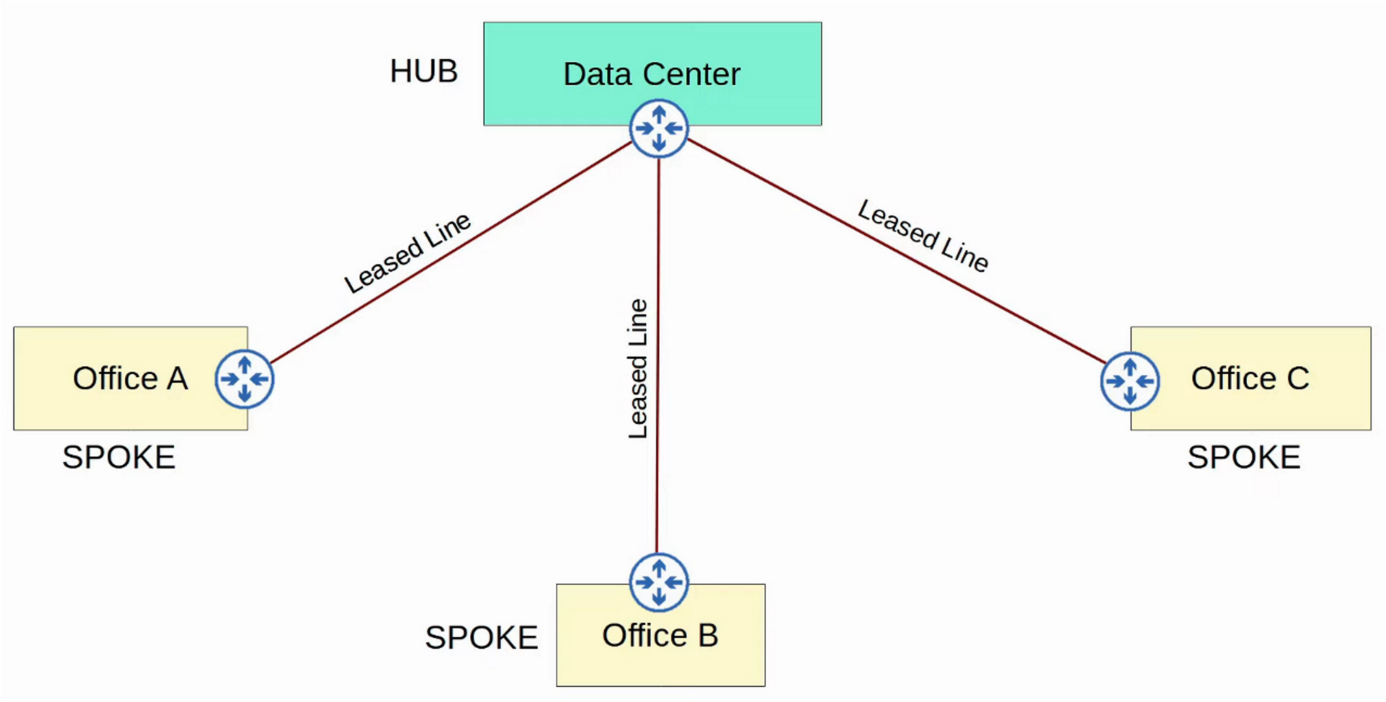
WAN ARCHITECTURES

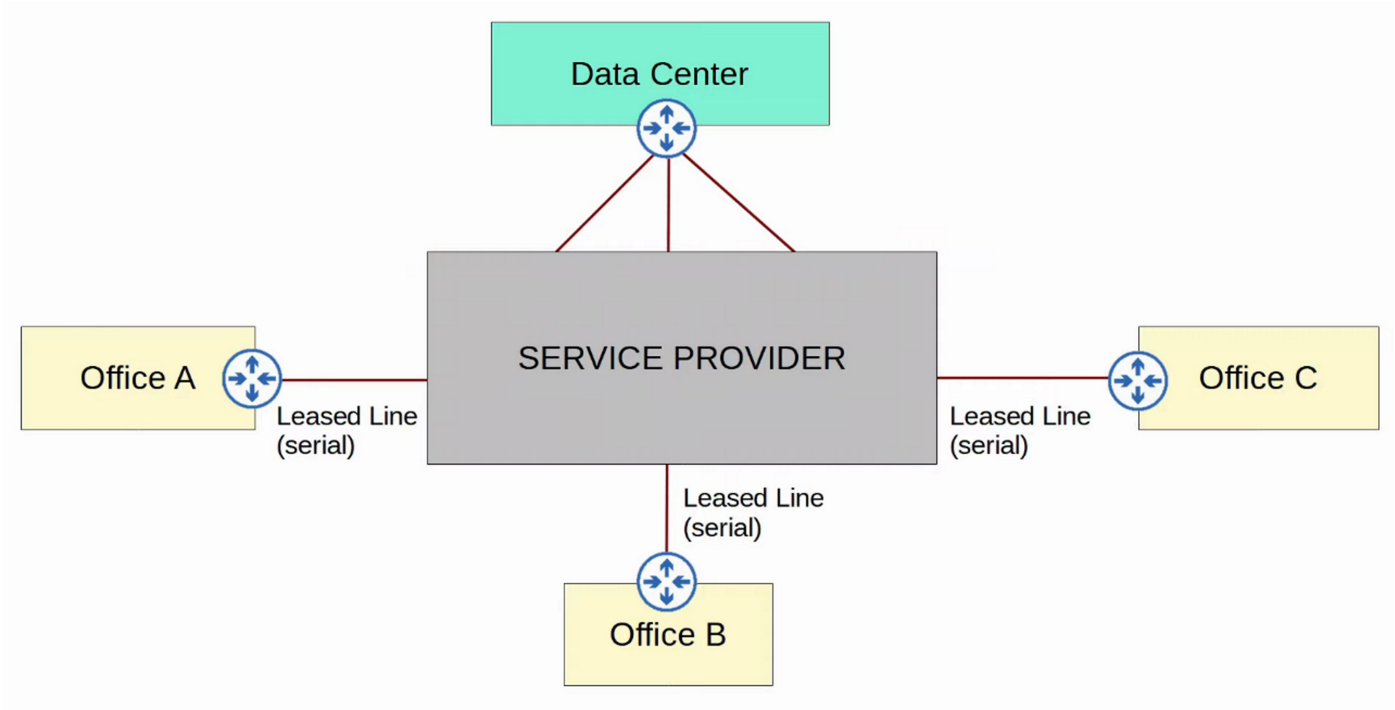
INTRODUCTION TO WANS

- WAN stands for WIDE AREA NETWORK
- A WAN is a NETWORK that extends over a large geographic area
- WANs are used to connect geographically separate LANs
- Although the Internet can be considered a WAN, the term “WAN” is typically used to refer to an enterprise’s private connections that connect their offices, data centers, and other sites together
- Over public/shared networks like the Internet, VPNs (Virtual Private Networks) can be used to create private WAN connections
- There have been many different WAN technologies over the years. Depending on the location, some will be available and some will not be
- Technologies which are considered “legacy” (old) in one country, might still be used in other countries

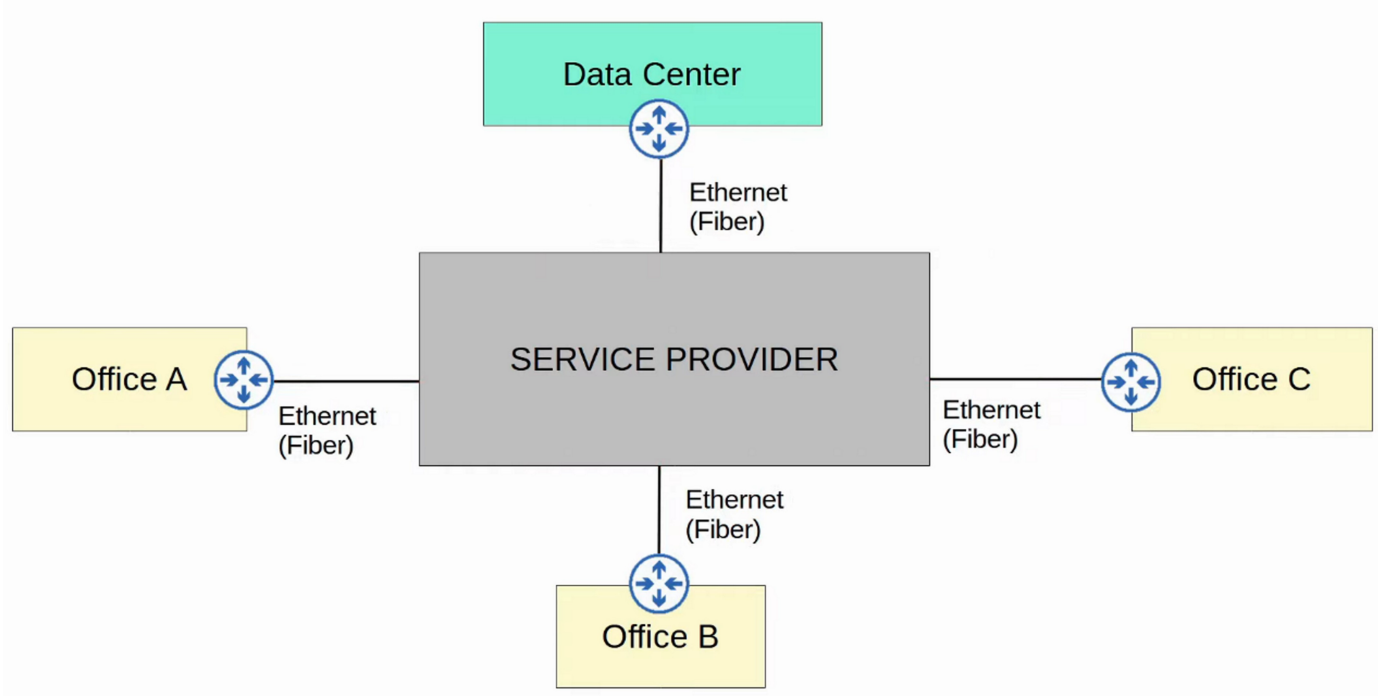
WAN OVER DEDICATED CONNECTION (LEASED LINE)

HUB-and-SPOKE topology

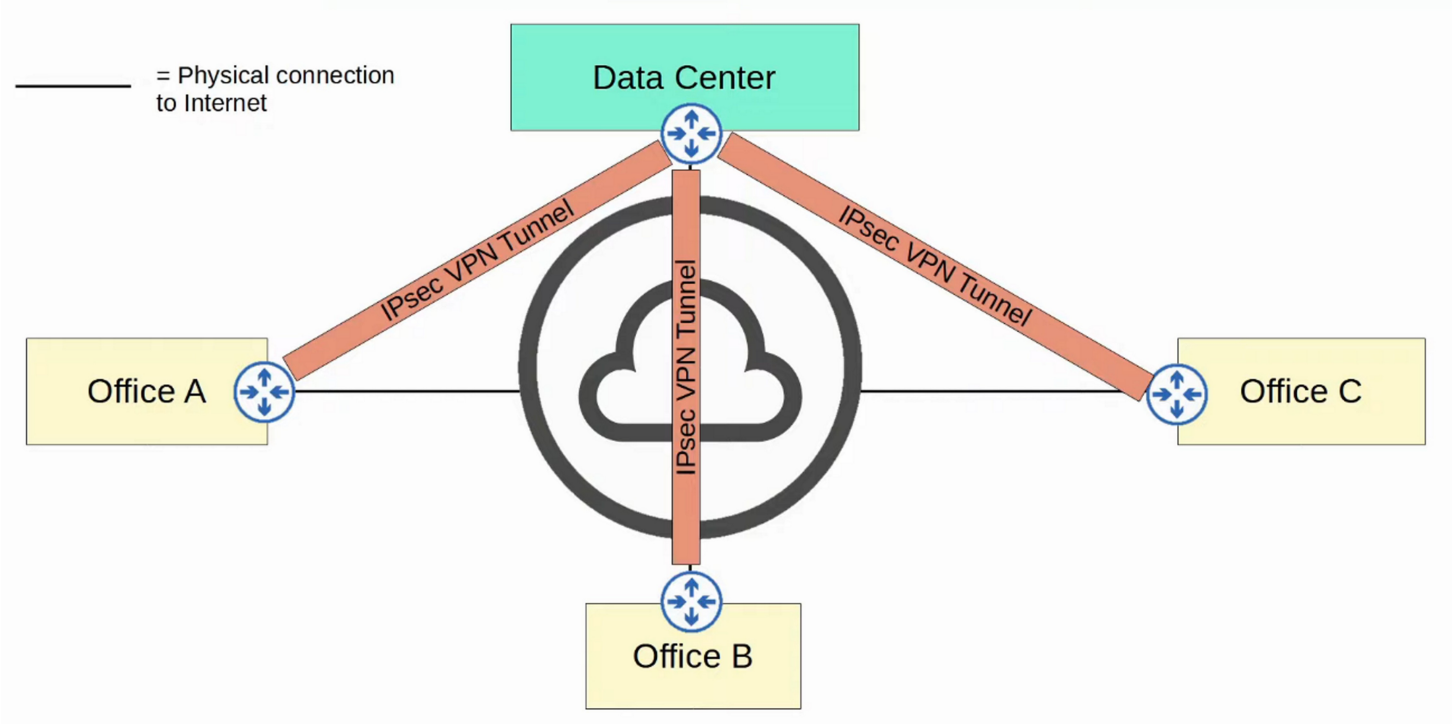




WAN CONNECTION VIA ETHERNET (FIBER)



WAN OVER SHARED INFRASTRUCTURE (INTERNET VPN)



LEASED LINES

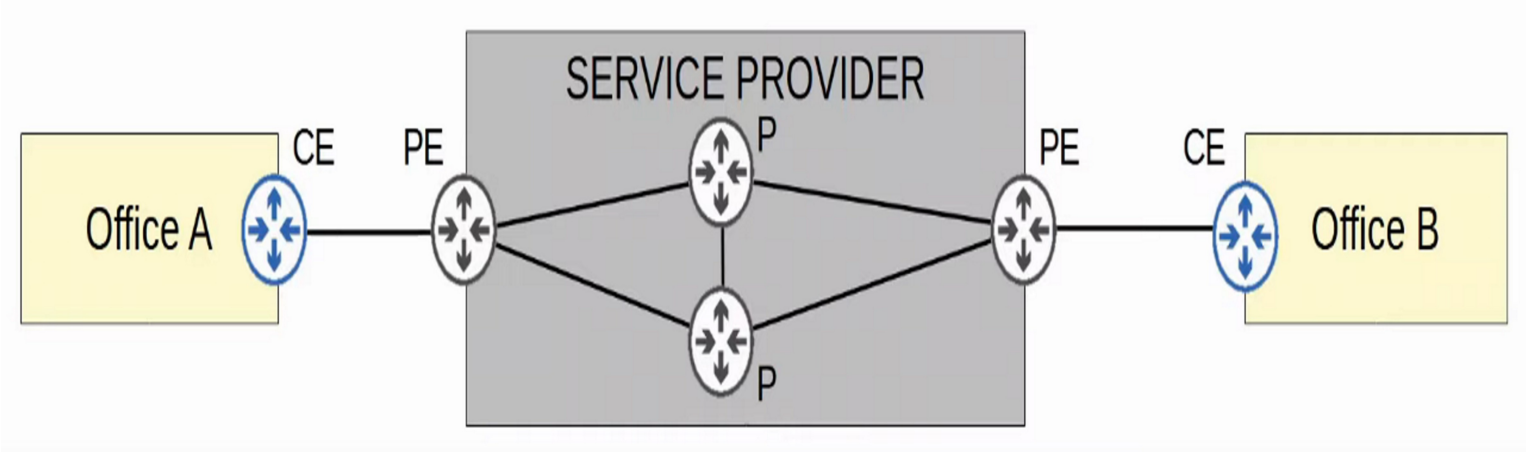
- A LEASED LINE is a dedicated physical link, typically connecting two sites
- LEASED LINES use serial connections (PPP or HDLC encapsulation)
- There are various standards that provide different speeds and different standards are available in different countries.
- Due to the HIGHER cost, HIGHER installation lead time, and SLOWER speeds of LEASED LINES, Ethernet WAN technologies are becoming MORE popular

System	North American	Japanese	European (CEPT)
Level zero (channel data rate)	64 kbit/s (DS0)	64 kbit/s	64 kbit/s
First level	1.544 Mbit/s (DS1) (24 user channels) (T1)	1.544 Mbit/s (24 user channels)	2.048 Mbit/s (32 user channels) (E1)
(Intermediate level, T-carrier hierarchy only)	3.152 Mbit/s (DS1C) (48 Ch.)	–	–
Second level	6.312 Mbit/s (DS2) (96 Ch.) (T2)	6.312 Mbit/s (96 Ch.), or 7.786 Mbit/s (120 Ch.)	8.448 Mbit/s (128 Ch.) (E2)
Third level	44.736 Mbit/s (DS3) (672 Ch.) (T3)	32.064 Mbit/s (480 Ch.)	34.368 Mbit/s (512 Ch.) (E3)
Fourth level	274.176 Mbit/s (DS4) (4032 Ch.)	97.728 Mbit/s (1440 Ch.)	139.264 Mbit/s (2048 Ch.) (E4)
Fifth level	400.352 Mbit/s (DS5) (5760 Ch.)	565.148 Mbit/s (8192 Ch.)	565.148 Mbit/s (8192 Ch.) (E5)

Wikipedia: 'Comparison of T-carrier and E-carrier systems'

MPLS VPNs

- MPLS stands for "Multi Protocol Label Switching"
- Similar to the Internet, service providers' MPLS NETWORKS are shared infrastructure because many customer enterprises connect to and share the same infrastructure to make WAN connections
- However, the "label switching" in the name of MPLS allows VPNs to be created over the MPLS infrastructure through the use of LABELS
- 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
- 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

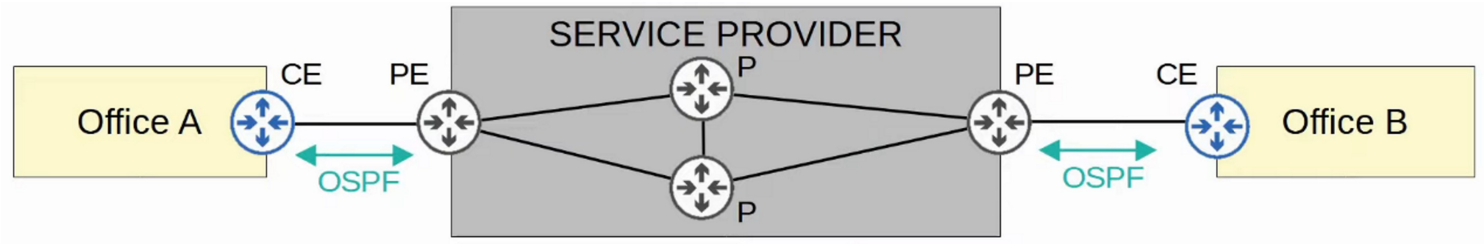
EXAMPLE:

OFFICE A's CE will peer with one PE

OFFICE B's CE will peer with the other PE

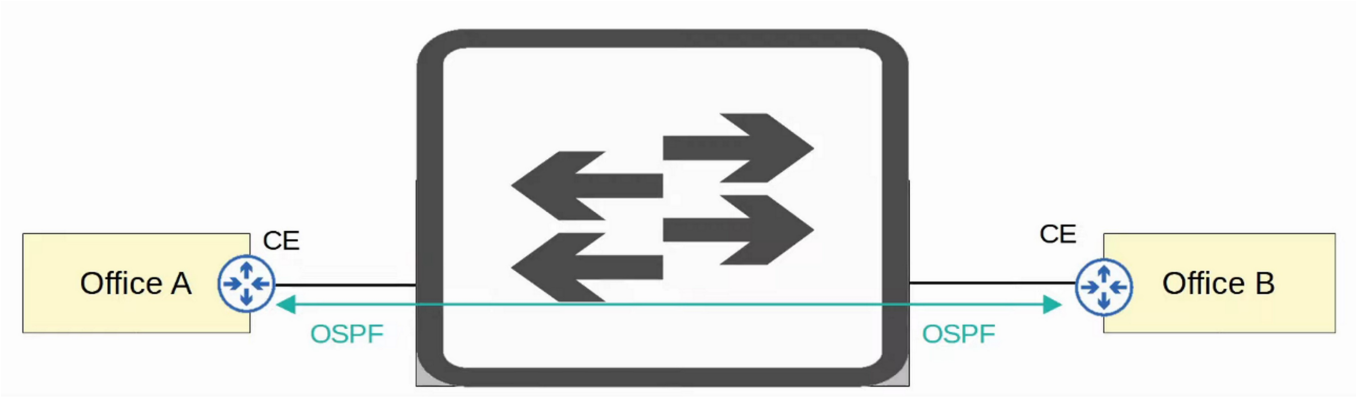
OFFICE A's CE will learn about OFFICE B's ROUTES via this OSPF peering

OFFICE B's CE will learn about OFFICE A's ROUTES as well



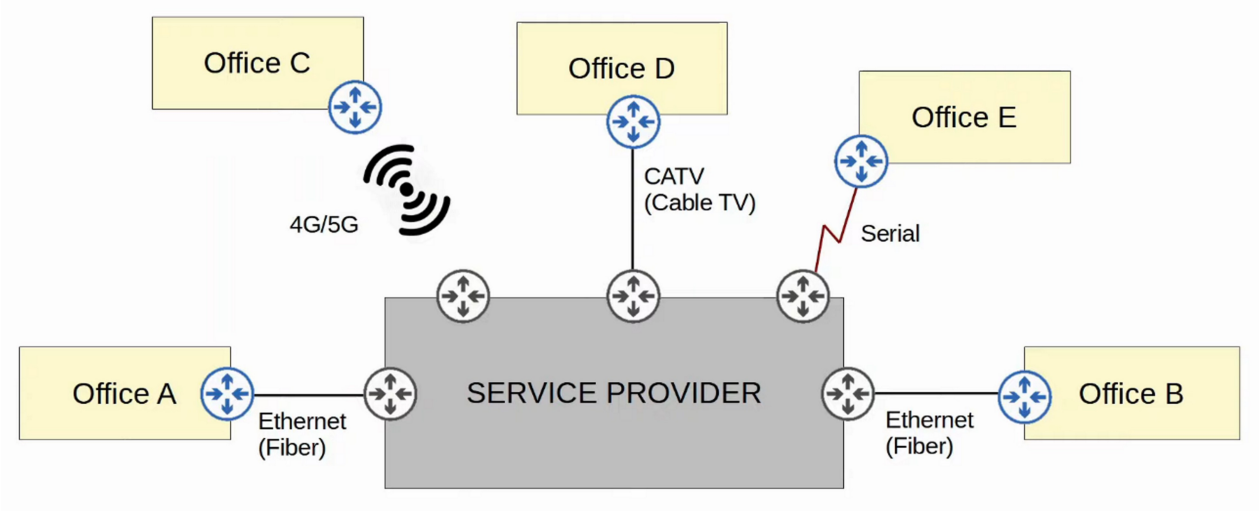
- When using a LAYER 2 MPLS VPN, the CE and PE ROUTERS do NOT form PEERINGS
- The SERVICE PROVIDER NETWORK is entirely *transparent* to the CE ROUTERS
- In effect, it is like the TWO CE ROUTERS are directly connected.
  - Their WAN INTERFACES will be in the SAME SUBNET
- If a ROUTING protocol is used, the TWO CE ROUTERS will peer directly with each other

CE ROUTERS connected via LAYER 2 MPLS VPN



MPLS

- Many different technologies can be used to connect to a SERVICE PROVIDER's MPLS NETWORK for WAN Service

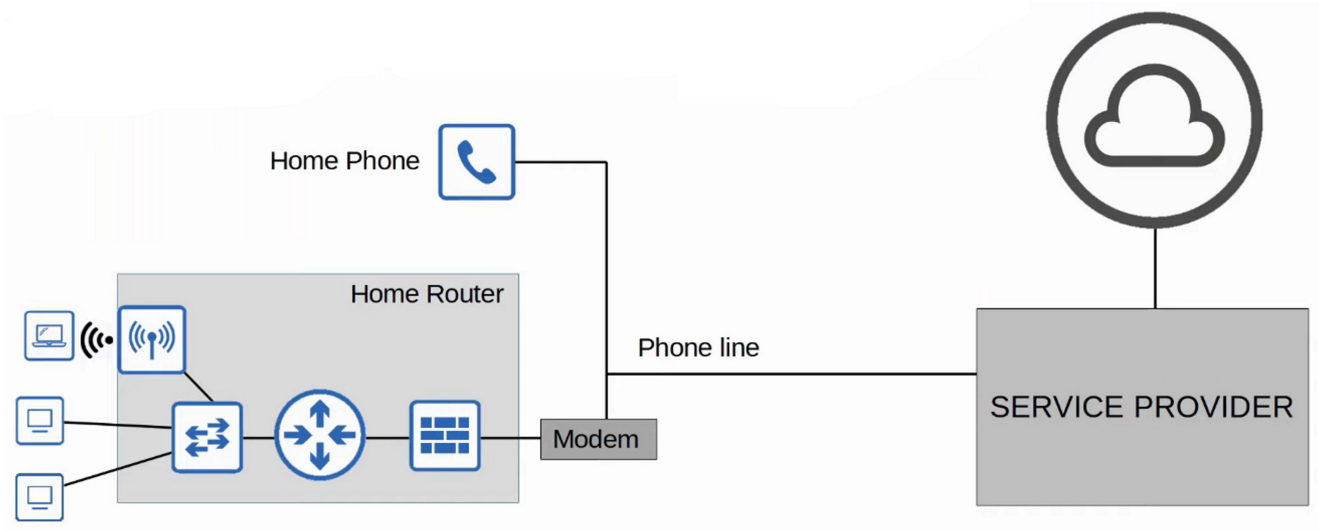


INTERNET CONNECTIVITY

- There are countless ways for an enterprise to connect to the INTERNET
- For example, PRIVATE WAN technologies such as LEASED LINES and MPLS VPNs can be used to connect to a SERVICE PROVIDER's INTERNET infrastructure
- In addition, technologies such as CATV and DSL commonly used by consumers (Home Internet Access) can also be used by an enterprise
- These days for both enterprise and consumer INTERNET access, FIBER OPTIC ETHERNET connections are growing in popularity due to high speeds they provide over long distances
- Let's briefly look at TWO INTERNET access technologies mentioned above:
  - CABLE (CATV)
  - DSL

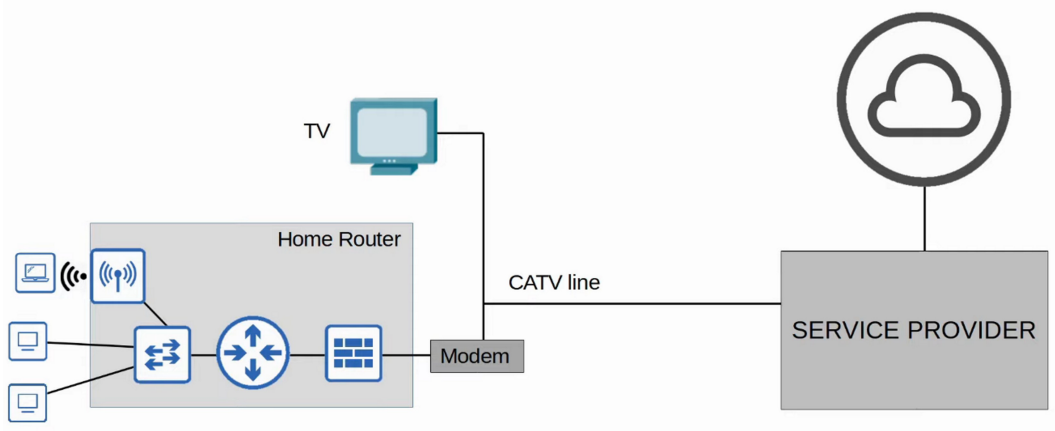
DIGITAL SUBSCRIBER LINE (DSL)

- DSL provides INTERNET connectivity to customers over phone lines and can share the same phone line that is already installed in most homes
- A DSL MODEM (Modulator / Demodulator) is required to convert DATA into a format suitable to be sent over the phone lines
  - The MODEM might be a separate DEVICE or it might be incorporated in to a "HOME ROUTER"

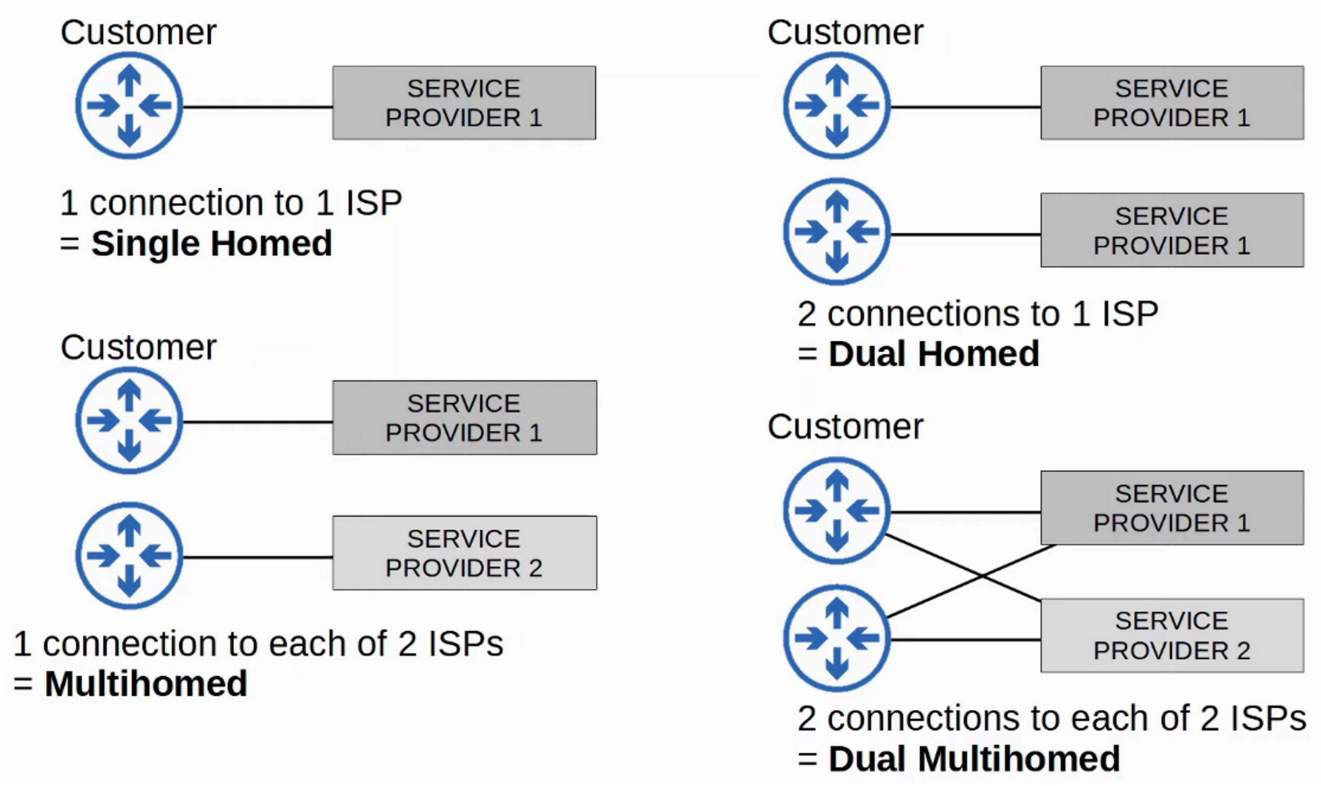


CABLE INTERNET

- CABLE INTERNET provides INTERNET ACCESS via the same CATV (Cable Television) lines used for TV service
- Like DLS, a CABLE MODEM is required to convert DATA into a format suitable to be sent over the CATV CABLES.
  - Like a DSL MODEM, this can be a separate device or built into the HOME ROUTER



REDUNDANT INTERNET CONNECTIONS

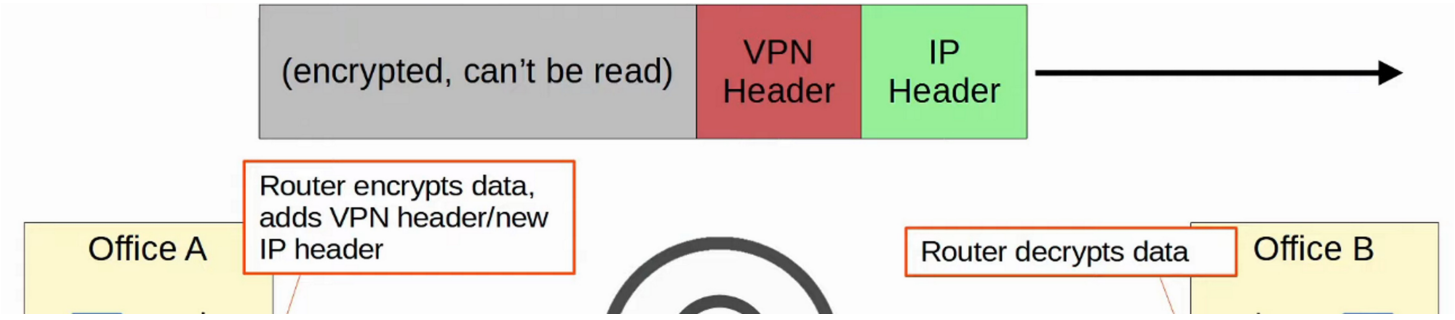


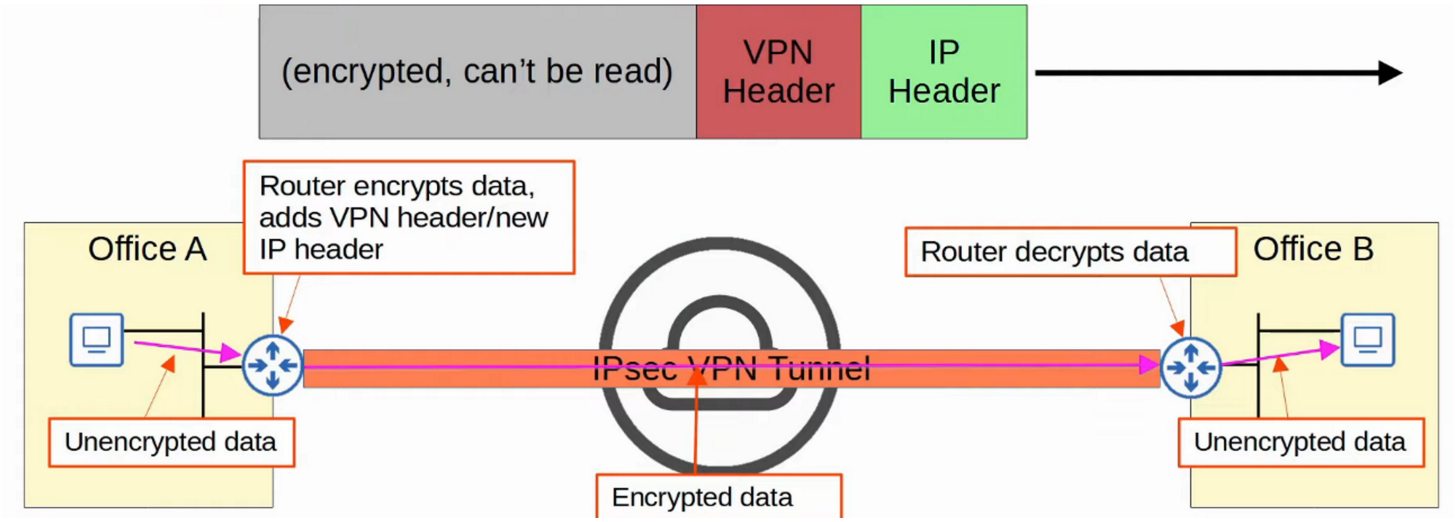
INTERNET VPNs

- PRIVATE WAN SERVICES such as LEASED LINES and MPLS provide security because each customer's TRAFFIC is separated by using dedicated physical connections (LEASED LINE) or by MPLS TAGS
- When using the INTERNET as a WAN to connect SITES together, there is no built-in security by DEFAULT
- To provide secure communications over the Internet, VPNs (Virtual Private Networks) are used
- We will cover two kinds of Internet VPNs:
  - SITE-TO-SITE VPNS using IPSec
  - REMOTE-ACCESS VPNs using TLS

SITE-TO-SITE VPNs (IPSec)

- A "SITE-TO-SITE" VPN is a VPN between two DEVICES and is used to connect TWO SITES together over the INTERNET
- A VPN "TUNNEL" is created between the TWO DEVICES by ENCAPSULATING the original IP PACKET with a VPN HEADER and a new IP HEADER
  - When using IPSec, the original PACKET is encrypted before its ENCAPSULATED with the new HEADER





Internet Protocol Security (IPSec) configured in tunnel mode encrypts the entire packet. IPSec is a suite of protocols that can be used to encrypt Generic Routing Encapsulation (GRE) tunnel traffic, such as over a virtual private network (VPN). IPSec supports two modes: transport and tunnel. In tunnel mode, IPSec encrypts the entire Internet Protocol (IP) packet, including the header.

IPSec configured in tunnel mode does require an additional header. This is because the entire packet is encrypted. Layer 3 forwarding devices are not capable of decrypting the encrypted packet. Therefore, a new unencrypted IP header encapsulates the encrypted packet for routing.

IPSec configured in transport mode, not tunnel mode, does not encrypt the IP header. In transport mode, only the IP packet's payload is encrypted by IPSec, which means that the IP packet's header remains intact.

IPSec tunnel mode is not required for Network Address Translation (NAT) traversal. However, IPSec tunnel mode is more compatible with NAT than IPSec transport mode. IPSec in tunnel mode encrypts the entire packet, including both the header and payload. The encrypted packet is then encapsulated in a new IP packet that includes a new IP header, which can be used by NAT. Transport mode, on the other hand, creates complications for NAT if Authentication Header (AH) is used. It is possible to use IPSec in transport mode when NAT is deployed. However, it requires the use of a NAT Traversal (NAT-T) solution as described in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 3947.

PROCESS SUMMARY:

1. The SENDING DEVICE combines the original PACKET and SESSION KEY (ENCRYPTION KEY) and runs them through an ENCRYPTION FORMULA
2. The SENDING DEVICE encapsulates the ENCRYPTED PACKET with a VPN HEADER and a new IP HEADER
3. The SENDING DEVICE sends the NEW PACKET to the DEVICE on the other side of the TUNNEL
4. The RECEIVING DEVICE decrypts the DATA to get the original PACKET and then forwards the original PACKET to it's DESTINATION

- In a "SITE-TO-SITE" VPN, a TUNNEL is formed only between TWO TUNNEL ENDPOINTS (for example, the TWO ROUTERS connected to the INTERNET)
- All OTHER DEVICES in each site DO NOT 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.

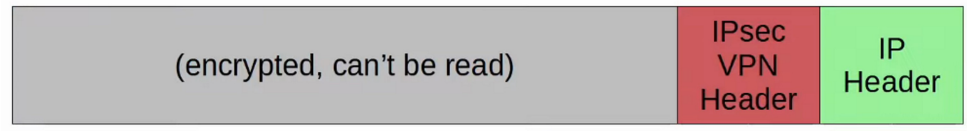
LIMITATIONS OF STANDARD IPSec

1. IPSec doesn't support BROADCAST or MULTICAST TRAFFIC, only UNICAST.
- This means that ROUTING PROTOCOLS such as OSPF cannot be used over the TUNNELS because they rely on MULTICAST TRAFFIC
  - This can be SOLVED with "GRE over IPSec"
2. Configuring a full mesh of TUNNELS between many sites is a labor-intensive task

Let's look at each of the above SOLUTIONS

GRE over IPSec

- **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 a 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 a NEW IP HEADER



After a sending host on a site-to-site virtual private network (VPN) that is constructed by using Generic Routing Encapsulation (GRE) with Internet Protocol Security (IPSec) for transport adds a VPN header and an Internet Protocol (IP) header to the packet, the sending host sends the packet to the destination. The addition of the VPN header and IP header to the packet is a process known as encapsulation.

A site-to-site VPN uses IPSec to transport information across a tunnel that is established between two hosts. A typical site-to-site VPN uses GRE with confidentiality, integrity, and antireplay protection provided by IPSec. There are four steps in the site-to-site VPN IPSec encryption process. By contrast, a remote access VPN uses client software to encrypt traffic between a remote user and internal company resources.

First, the sending device combines a session key, which is also known as an encryption key or a shared key, with the data that is to be transported over the tunnel. It then uses the session key to encrypt both the data and the key.

Second, the sending device encapsulates the encrypted data and session key into a packet with a VPN header and a new IP header. These headers contain the source and destination information that is used to transport the encrypted data and session key over the tunnel.

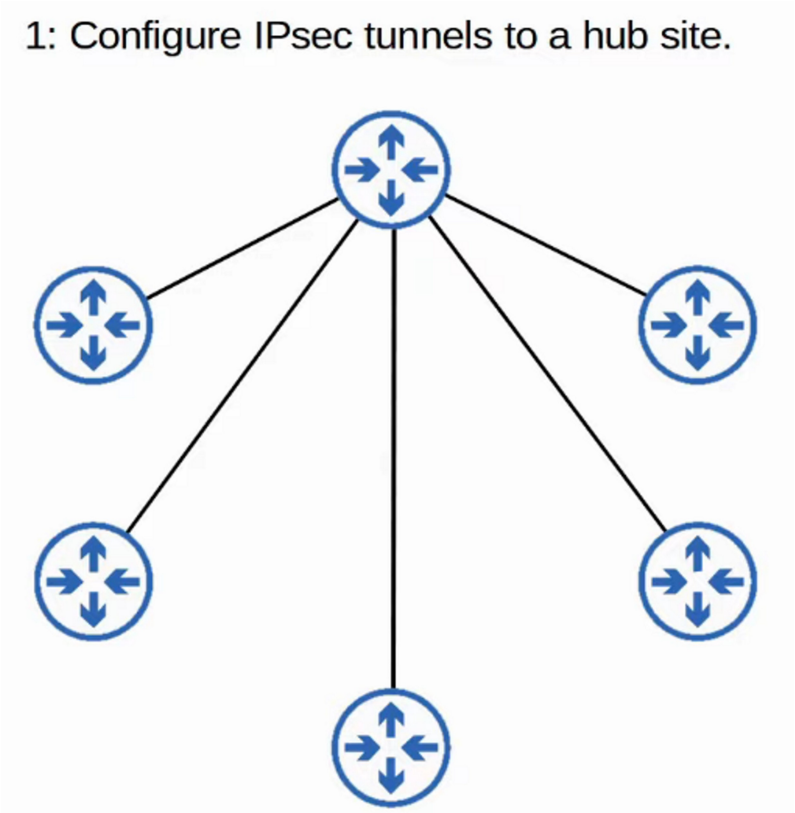
Third, the sending device sends the completed packet to the destination device at the other end of the tunnel, or site-to-site VPN.

Fourth and finally, the destination device, or receiving device, uses the same session key that the sending device used for encryption to decrypt the encrypted packet and session key.

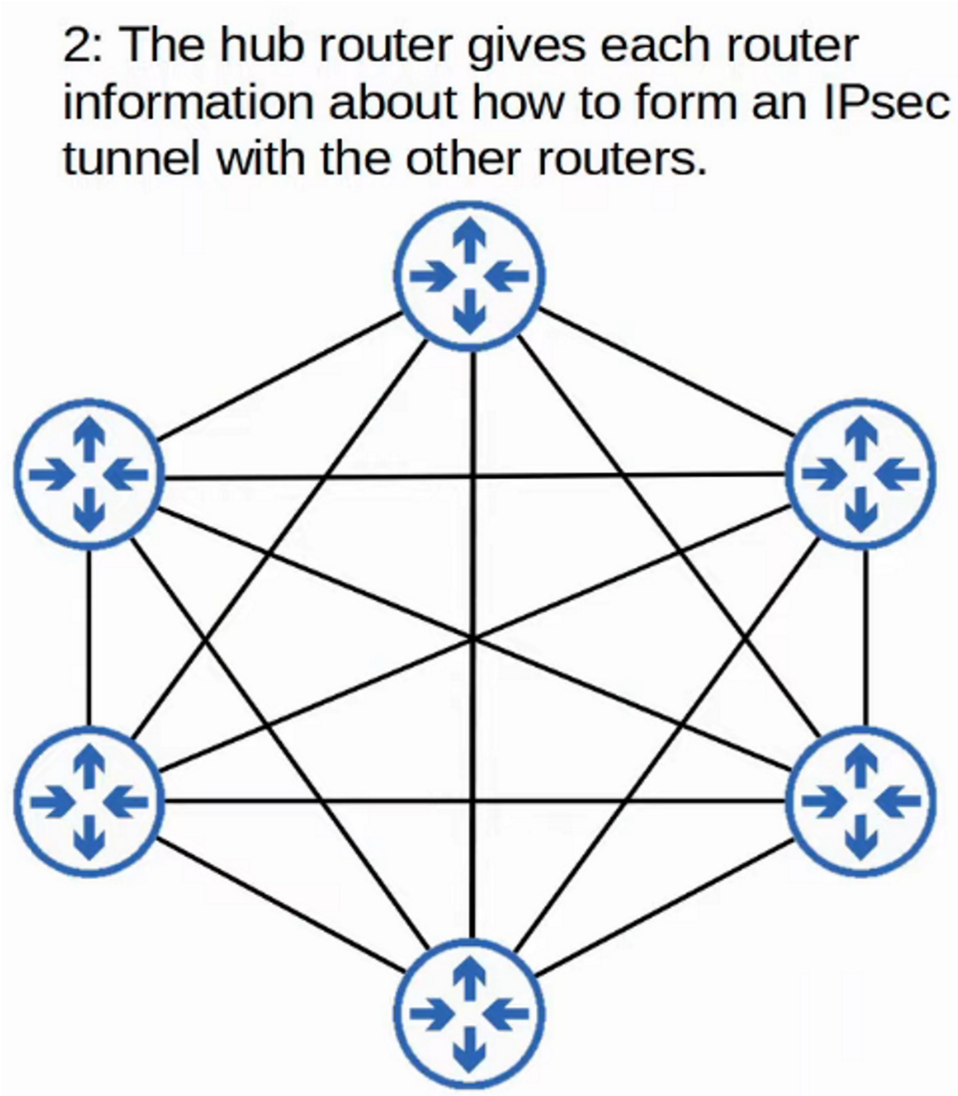
DMVPN

- **DMVPN (Dynamic Multipoint VPN) i**s 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



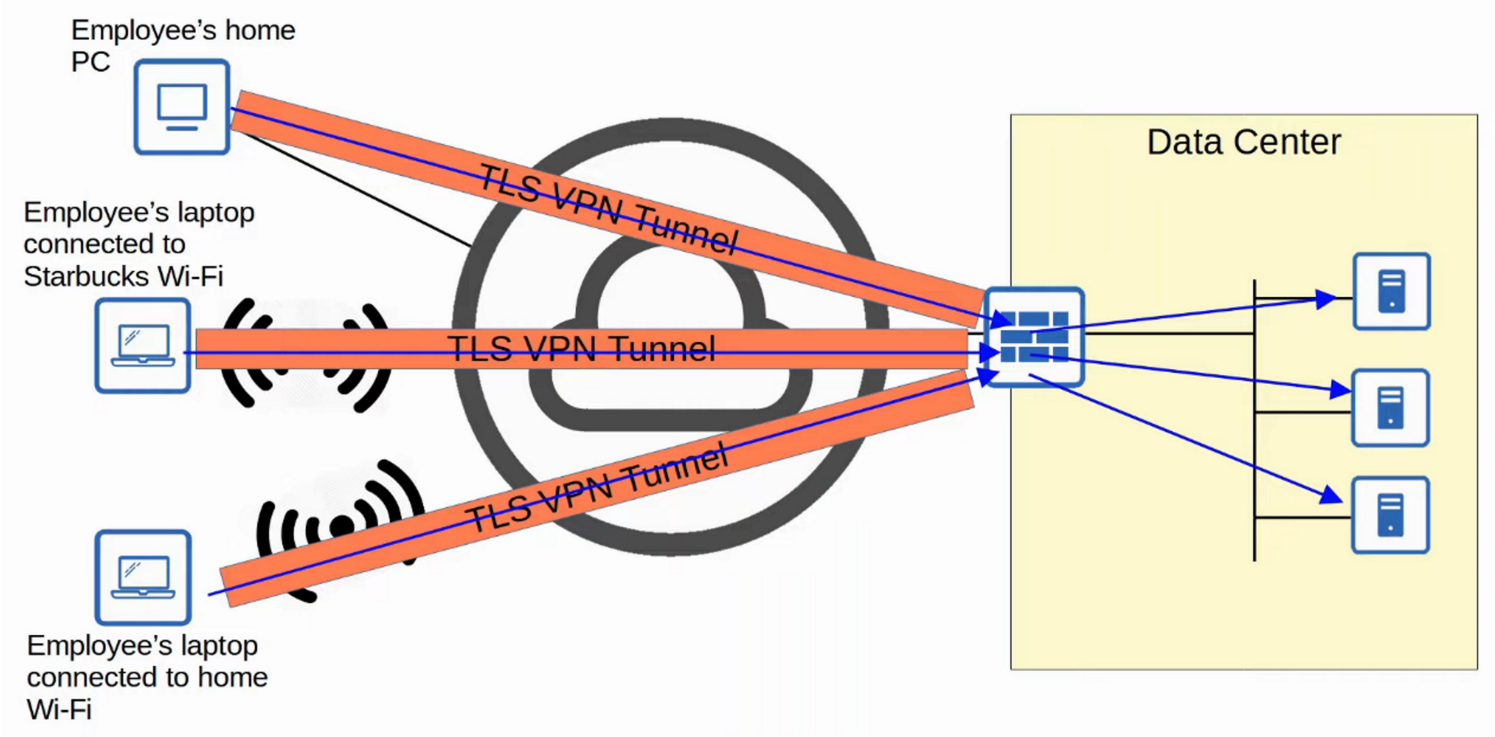
2. The HUB ROUTER gives each ROUTER information about HOW to form an IPSec TUNNEL with the OTHER ROUTERS



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)

REMOTE-ACCESS VPNs

- Whereas SITE-TO-SITE VPNs are used to make a POINT-TO-POINT connection between TWO SITES over the INTERNET, REMOTE-ACCESS VPNs are used to allow END DEVICES (PCs, Mobile Phone) to ACCESS the company's internal resources securely over the INTERNET
- REMOTE-ACCESS VPNs typically use TLS (TRANSPORT LAYER SECURITY)
  - TLS is also what provides security for HTTPS (HTTP SECURE)
  - TLS was formerly known as SSL (Secure Socket Layer) and developed by Netscape, but it was renamed to TLS when it was standardized by the IETF
- VPN client software (for example Cisco AnyConnect) is installed on END DEVICES (for example company-provided laptops that employees use to work from home)
- These END DEVICES then form SECURE TUNNELS to one of the company's ROUTERS / FIREWALLS acting as a TLS SERVER
- This allows the END USERS to securely access RESOURCES on the company's INTERNAL NETWORK without being directly connected to the company NETWORK



SITE-TO-SITE versus REMOTE-ACCESS VPN

- SITE-TO-SITE VPNs typically use IPSec
- REMOTE-ACCESS VPNs typically use TLS
- SITE-TO-SITE VPNs provide SERVICE to many DEVICES within the SITES they are connecting
- REMOTE-ACCESS VPNs provide SERVICE to the ONE END DEVICE the VPN CLIENT SOFTWARE is installed on
- SITE-TO-SITE VPNs are typically used to permanently connect TWO SITES over the INTERNET
- REMOTE-ACCESS VPNs are typically used to provide ON-DEMAND ACCESS for END DEVICES that want to securely ACCESS company resources while connected to a NETWORK which is not SECURE

LAB COMMANDS

Create the Tunnel interface

R1(config)#int tunnel <tunnel number>

This changes the mode to the Tunnel Interface

The exit interface for the tunnel

tunnel source <interface>

IP of the Tunnel Destination Interface

tunnel destination <destination ip address>

Set the IP of the Source Tunnel Interface (from step 1)

ip address <tunnel IP> <netmask>

Configure a Default Route to the Service Provider Network

R1(config)#ip route 0.0.0.0 0.0.0.0 <next hop interface>

This will now bring the Tunnel Interface Administratively Up / Up

==========

Now you need to set up the TUNNEL ROUTERS as OSPF Neighbors for the Service Provider Network so they can share routes

R1(config)router ospf <ospf process ID>

This switches to the OSPF Router configuration mode

network <tunnel interface IP> <wildcard mask> area <area #>

Since the tunnel is a single HOST, you would use 0.0.0.0 for the Wildcard Mask

network <router gateway IP> <wildcard mask> area <area #>

Since the router gateway is also a single HOST, you would use 0.0.0.0 for the Wildcard Mask

passive-interface <router gateway IP interface>