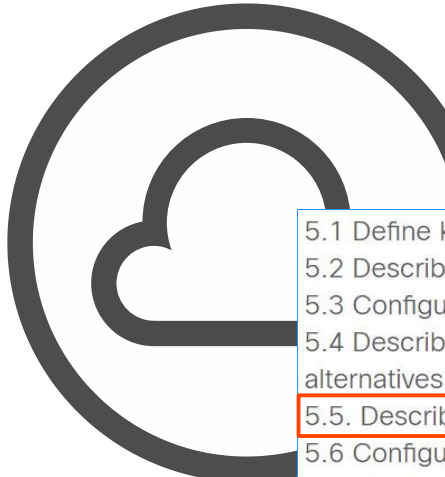


CCNA Day 53

WAN Architectures

1.2 Describe characteristics of network topology architectures

- 1.2.a 2 tier
- 1.2.b 3 tier
- 1.2.c Spine-leaf
- 1.2.d WAN
- 1.2.e Small office/home office (SOHO)
- 1.2.f On-premises and cloud

- 
- 
- 5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
 - 5.2 Describe security program elements (user awareness, training, and physical access control)
 - 5.3 Configure device access control using local passwords
 - 5.4 Describe security password policies elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
 - 5.5. Describe remote access and site-to-site VPNs
 - 5.6 Configure and verify access control lists
 - 5.7 Configure Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
 - 5.8 Differentiate authentication, authorization, and accounting concepts
 - 5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)
 - 5.10 Configure WLAN using WPA2 PSK using the GUI

Things we'll cover

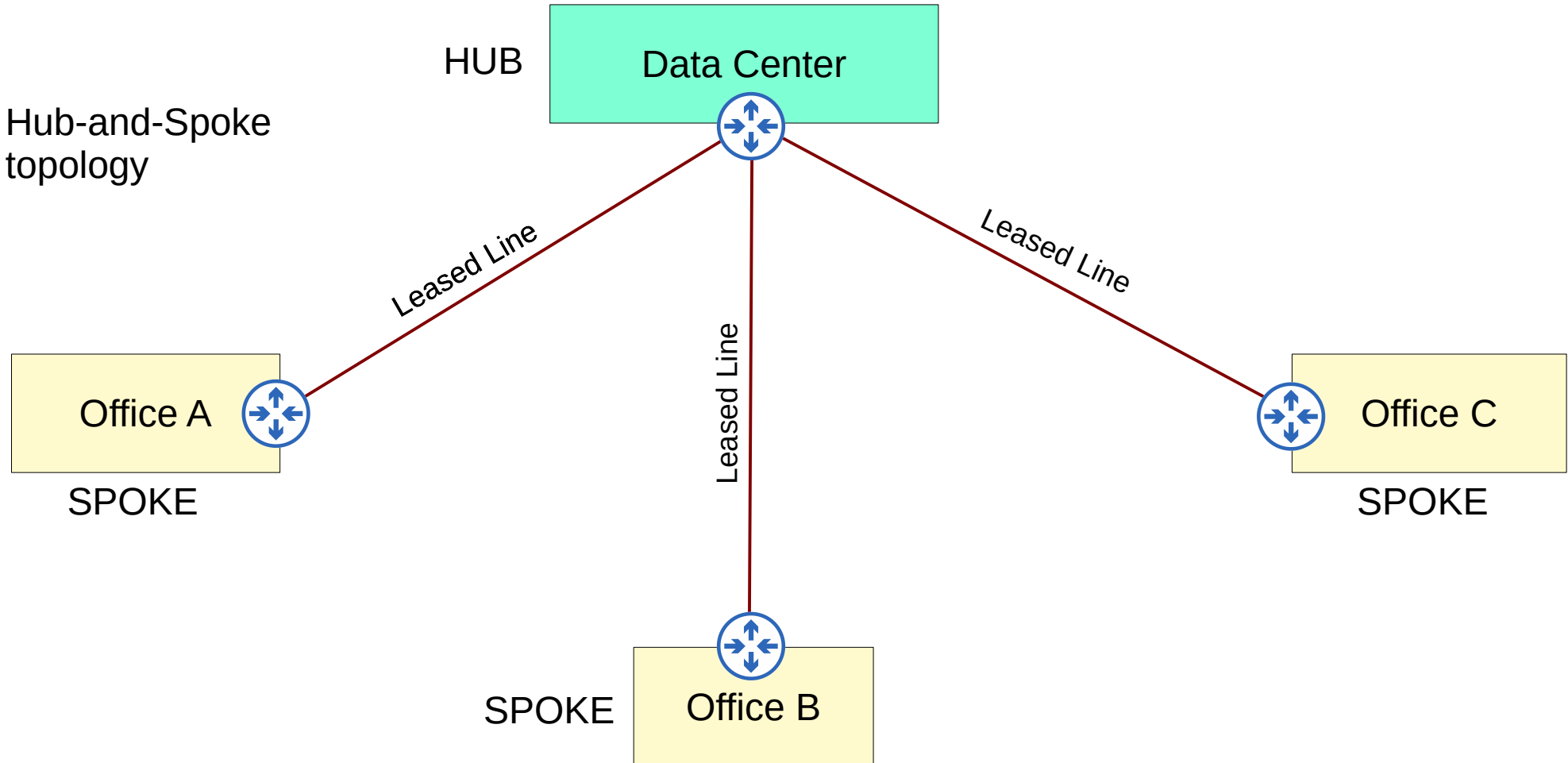
- Intro to WANs
- Leased Lines
- MPLS VPNs
- Internet connectivity
- Internet VPNs

WAN Architectures

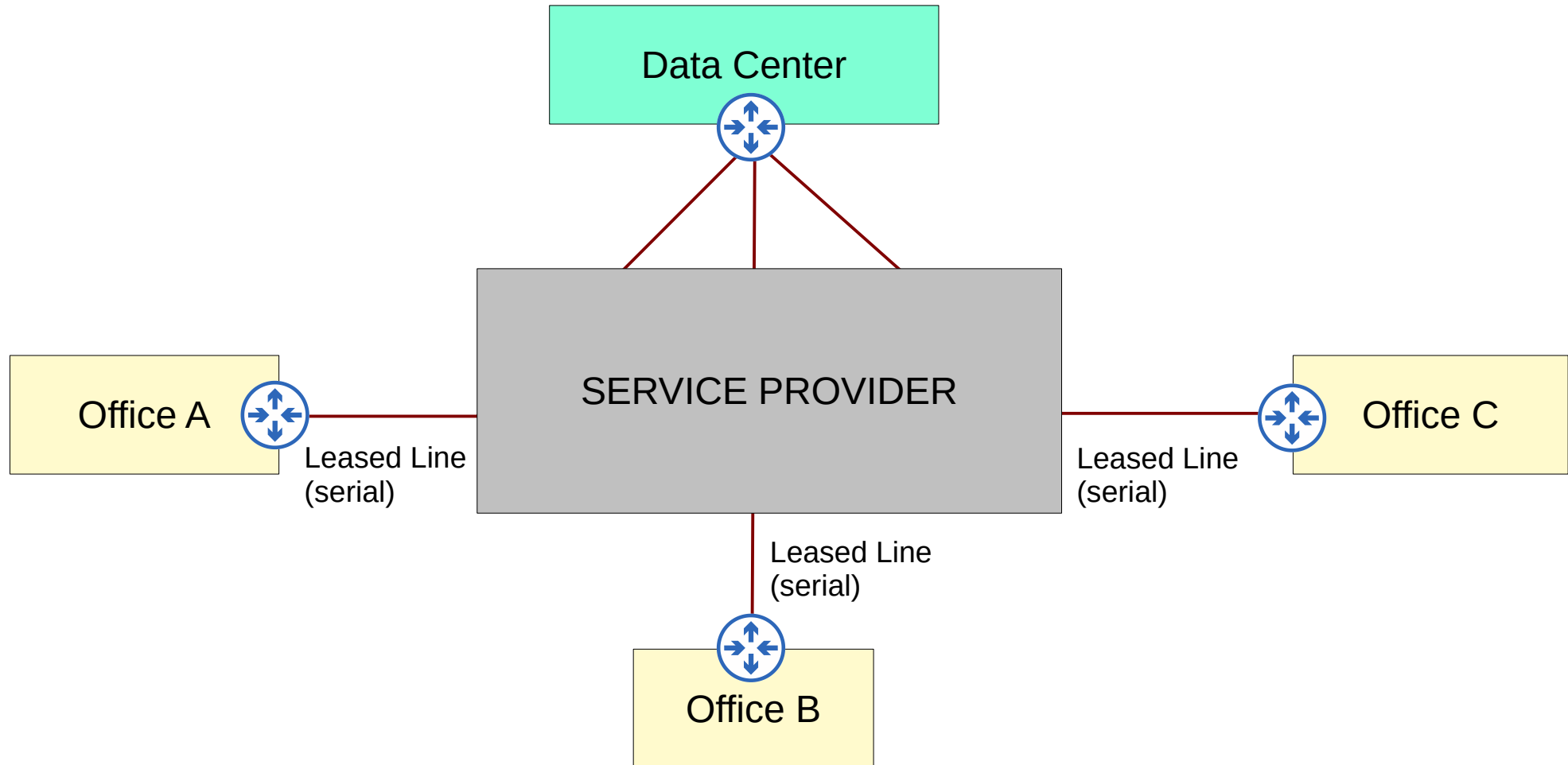
- WAN stands for Wide Area Network.
- A WAN is a network that extends over a large geographic area.
- WANs are used to connect geographically separate LANs.
- Although the Internet itself can be considered a WAN, the term WAN is typically used to refer to an enterprise's private connections that connect 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)

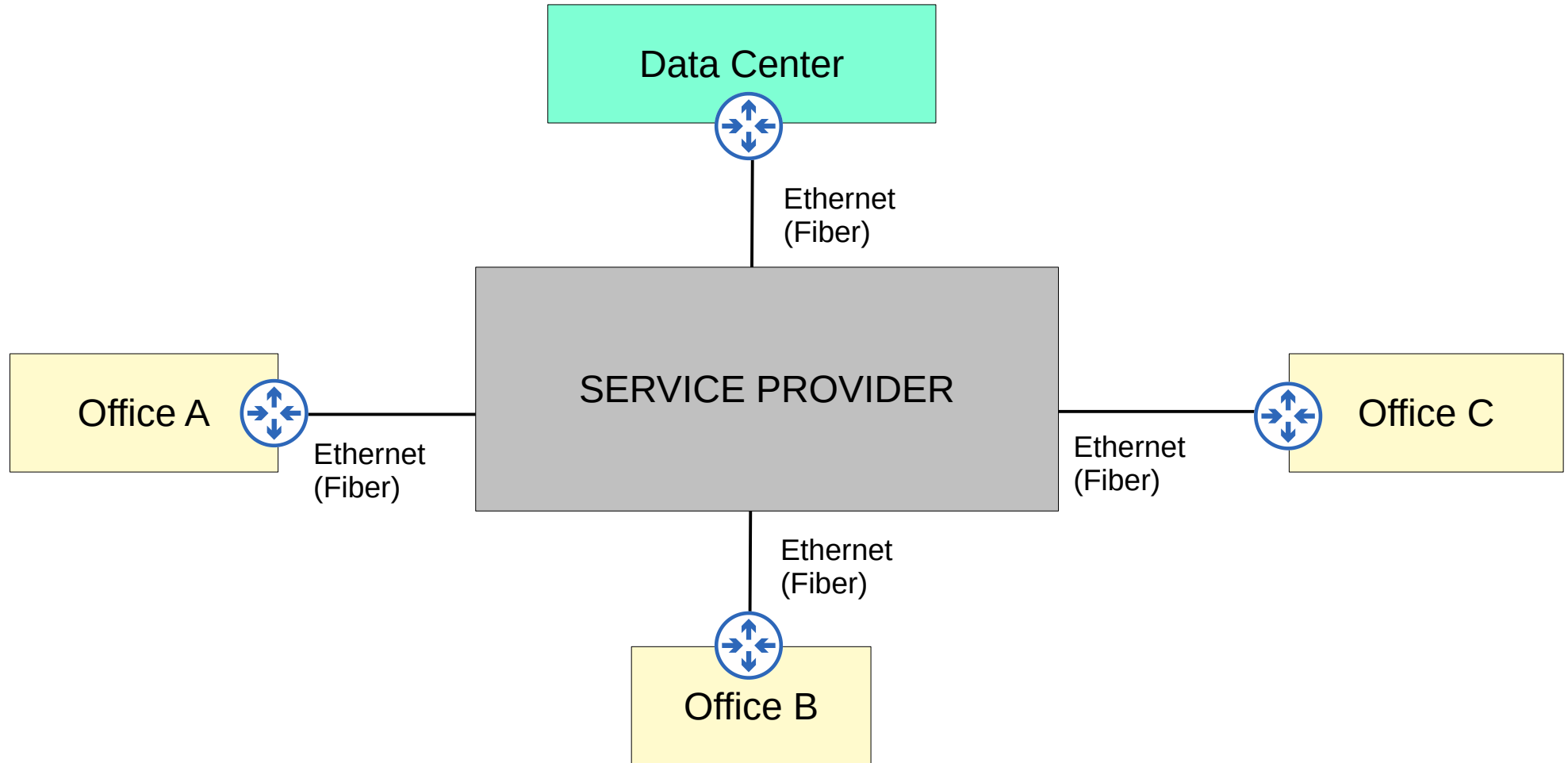
Hub-and-Spoke
topology



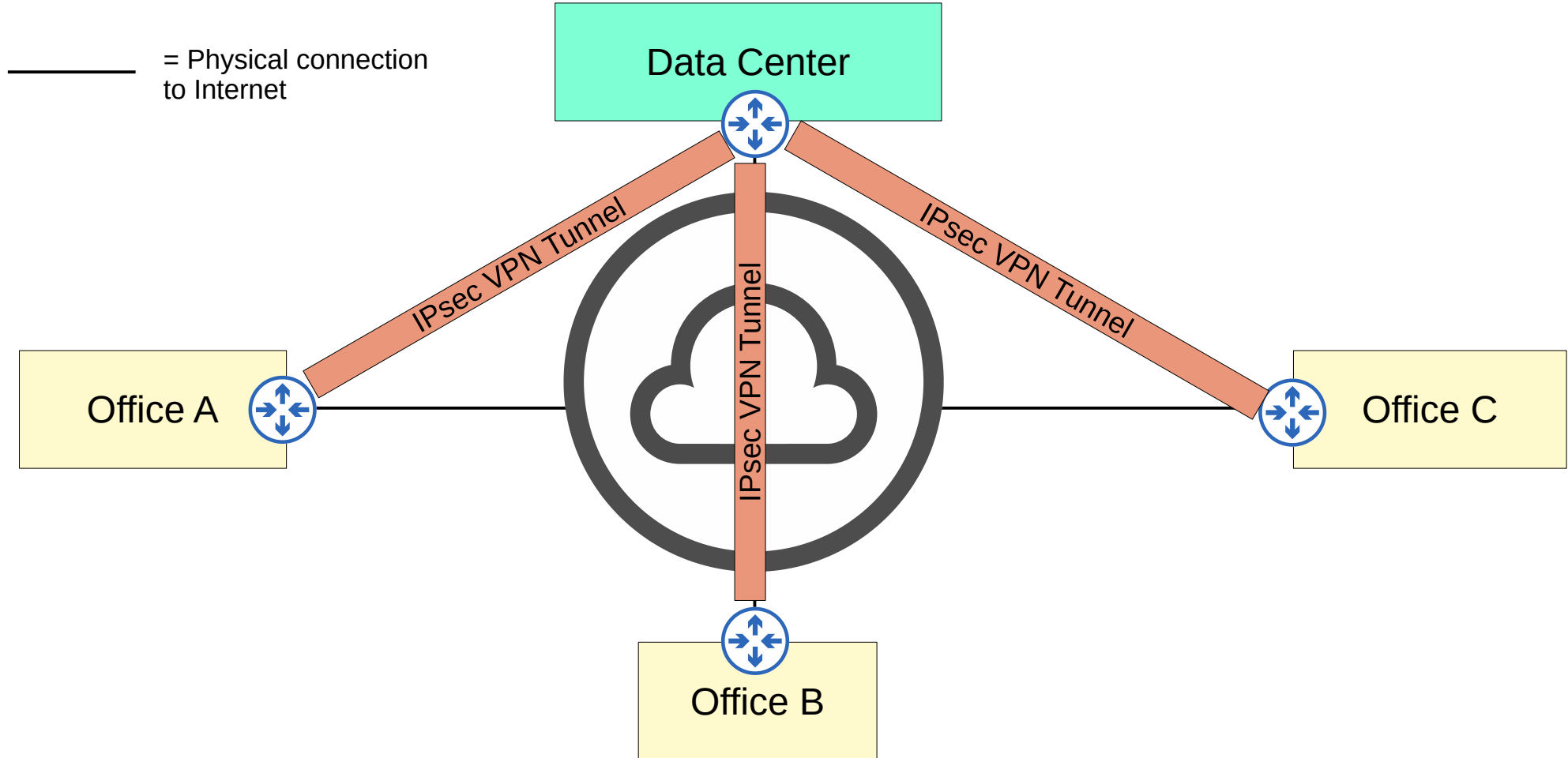
WAN over dedicated connection (Leased Line)



WAN connection via Ethernet (Fiber)



WAN over shared infrastructure (Internet VPN)



Leased Lines

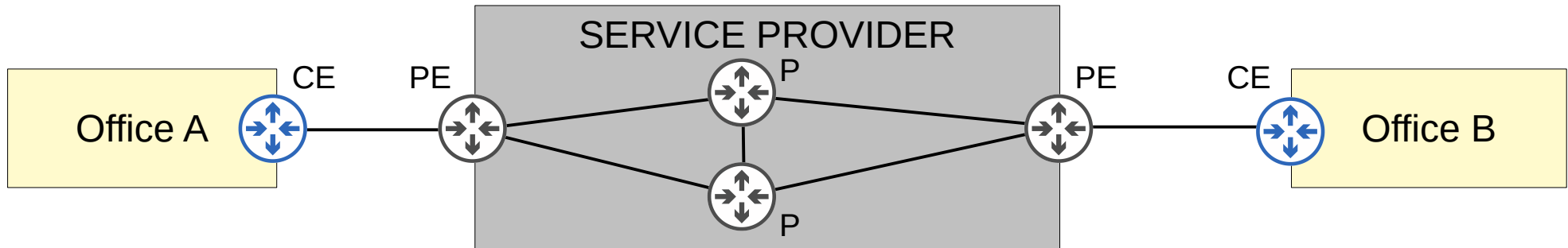
- A **leased line** is a dedicated physical link, typically connecting two sites.
- Leased lines use serial connections (PPP or HDLC encapsulation).
- There are various standards that provide different speeds, and different standards are available in different countries.

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'

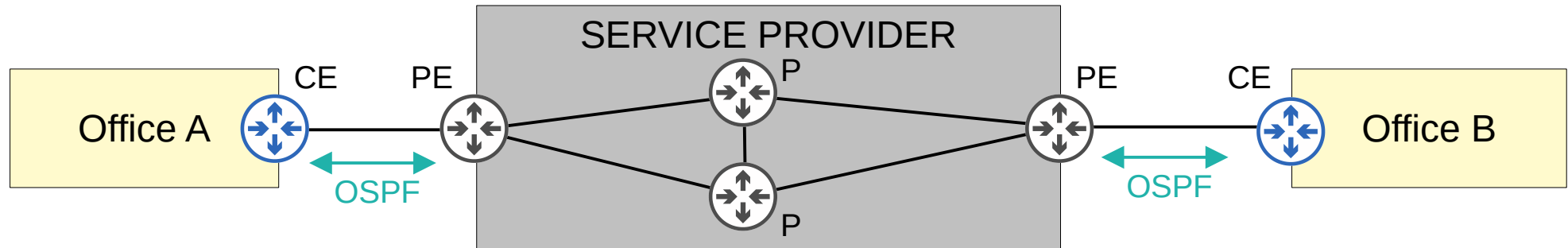
- Due to the higher cost, higher installation lead time, and slower speeds of leased lines, Ethernet WAN technologies are becoming more popular.

- 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**.
- 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.

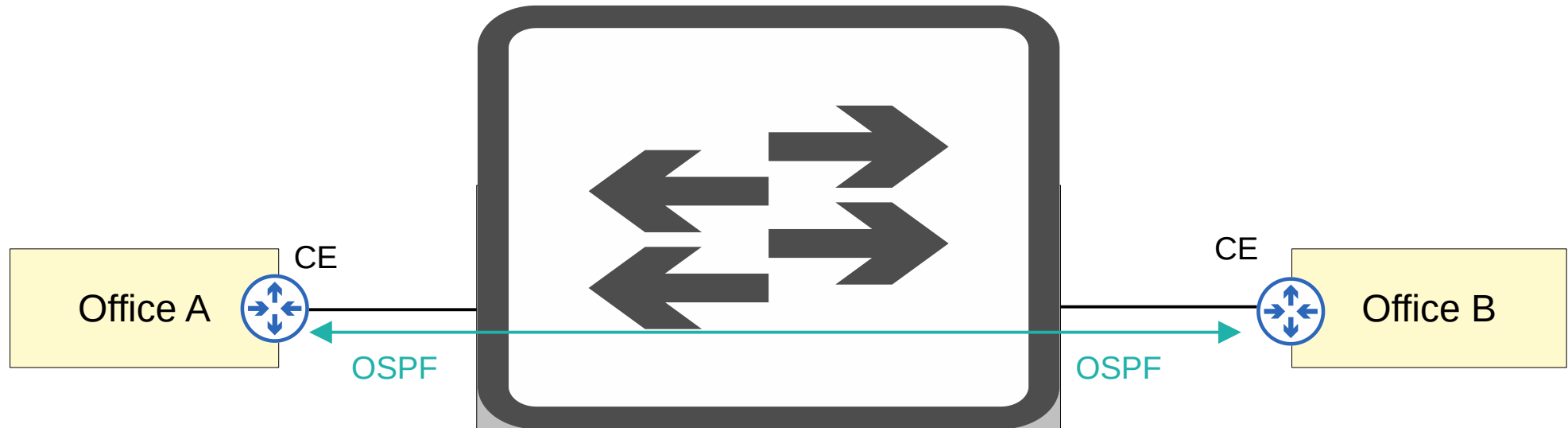


MPLS

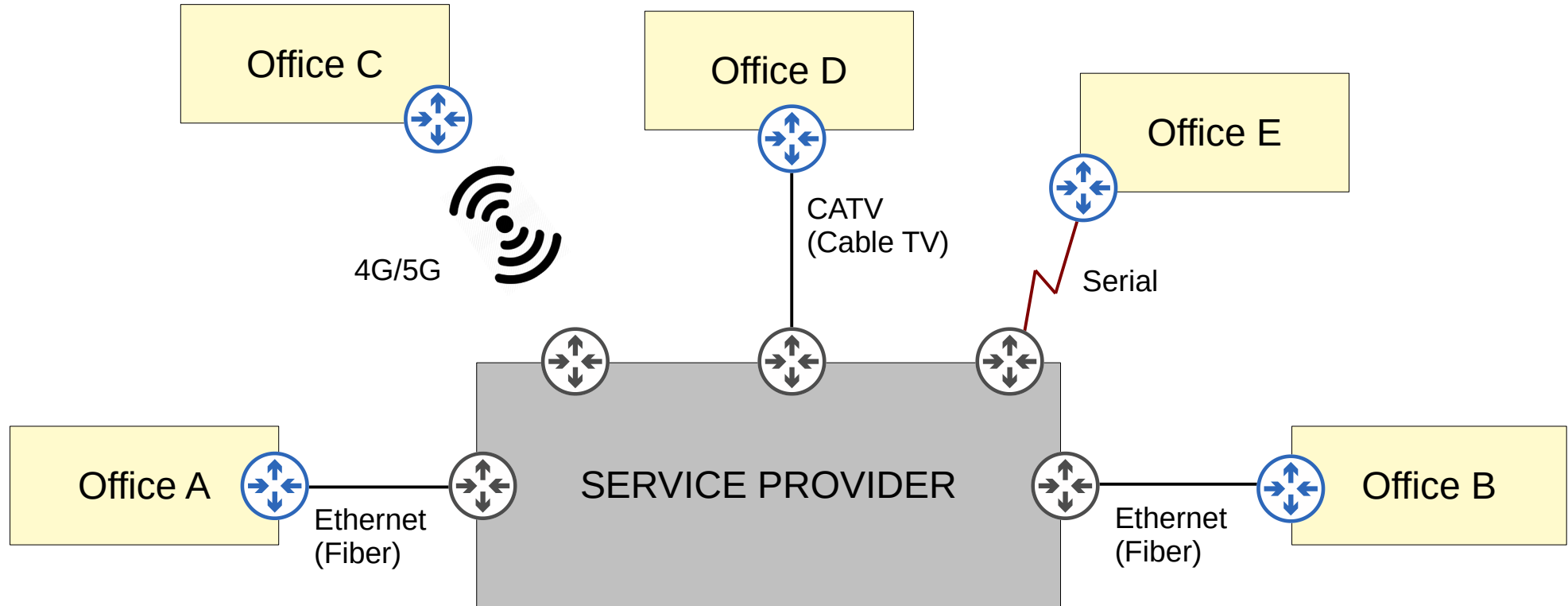
- The CE routers do not use MPLS, it is only used by the PE/P routers.
- When using a *Layer 3 MPLS VPN*, the CE and PE routers peer using OSPF, for example, to share routing information.
- For example, in the diagram below Office A's CE will peer with one PE, and Office B's CE will peer with the other 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.



- 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.



- Many different technologies can be used to connect to a service provider's MPLS network for WAN service.

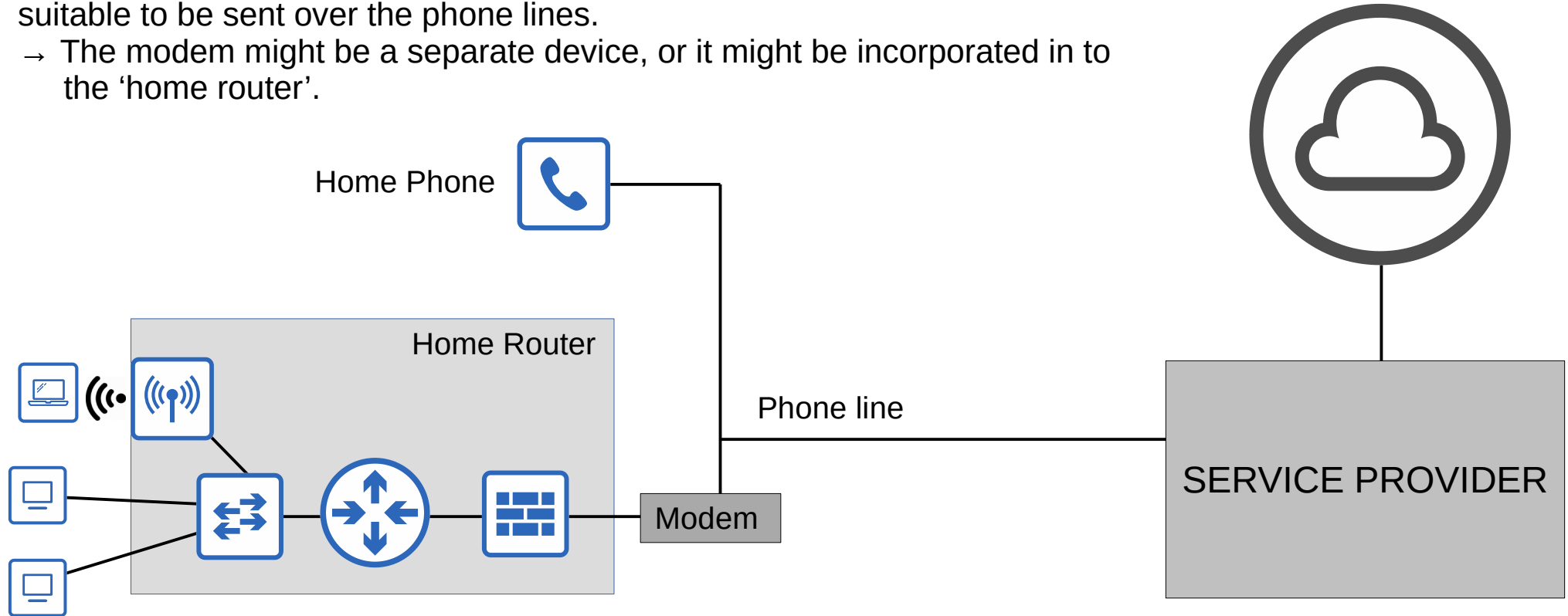


Internet Connections

- 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 the high speeds they provide over long distances.
- Let's briefly look at two Internet access technologies mentioned above: cable (CATV) and DSL.

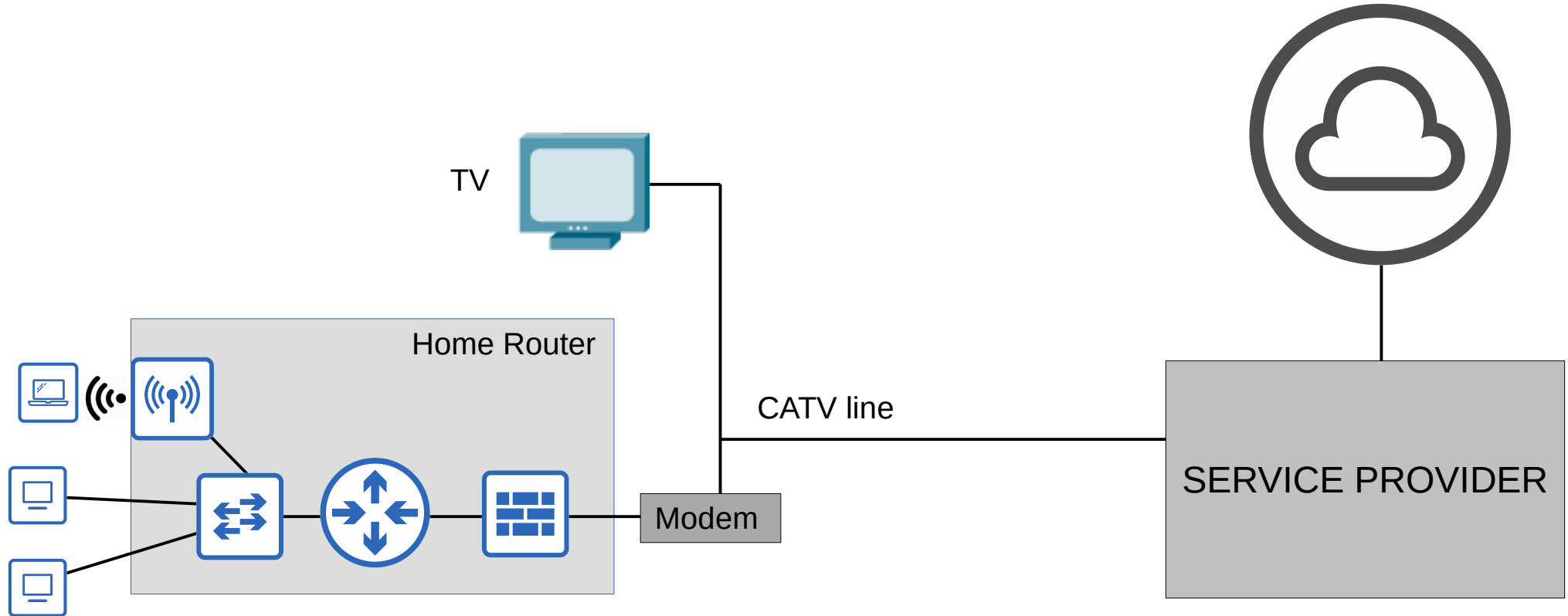
Digital Subscriber Line (DSL)

- 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 the 'home router'.



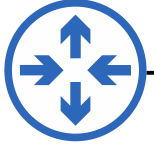
Cable Internet

- Cable Internet provides Internet access via the same CATV (Cable Television) lines used for TV service.
- Like DSL, 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.



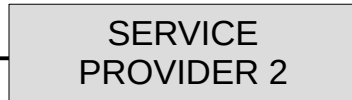
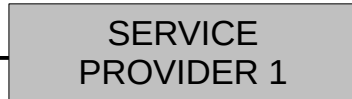
Redundant Internet Connections

Customer



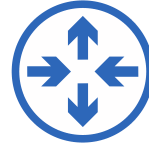
1 connection to 1 ISP
= **Single Homed**

Customer



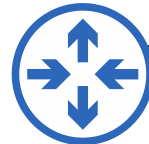
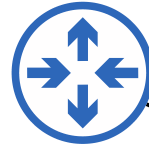
1 connection to each of 2 ISPs
= **Multihomed**

Customer



2 connections to 1 ISP
= **Dual Homed**

Customer



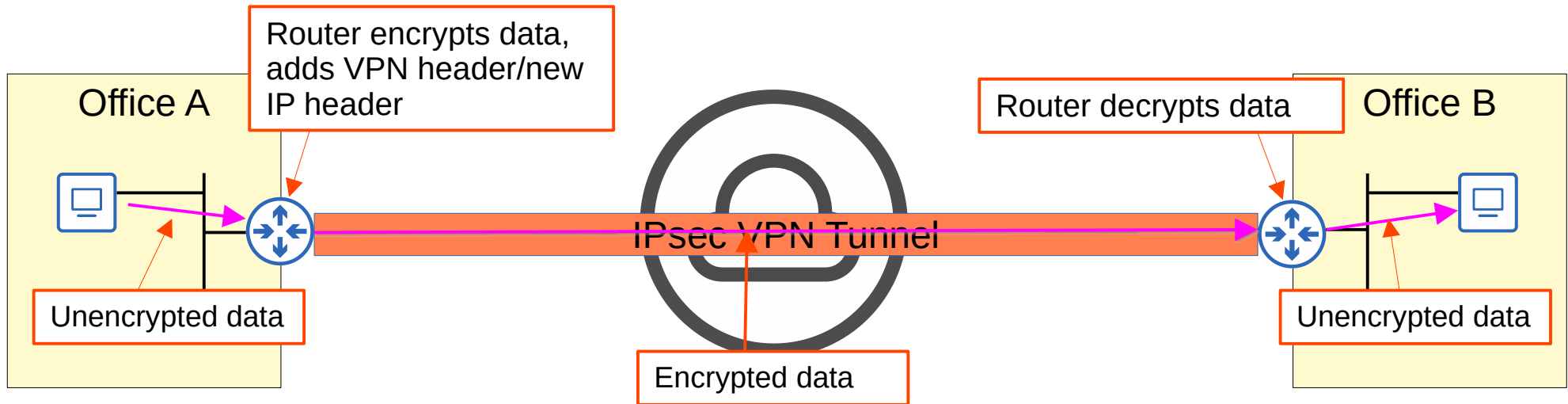
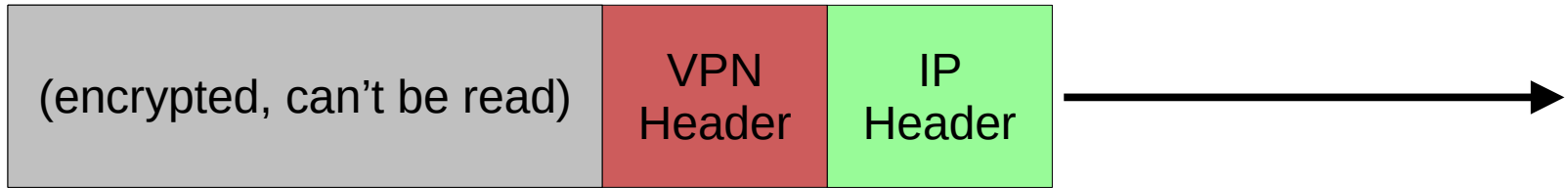
2 connections to each of 2 ISPs
= **Dual Multihomed**

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:
 - 1) Site-to-Site VPNs using IPsec
 - 2) 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 being encapsulated with the new header.



Site-to-Site VPNs (IPsec)

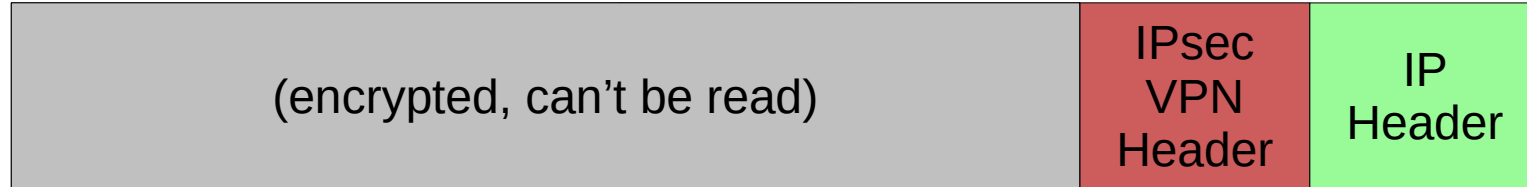
- Let's summarize that process:
 - 1) The sending device combines the original packet and session key (encryption key) and runs them through an encryption formula.
 - 2) The sending device encapsulates the encrypted packet with a VPN header and a new IP header.
 - 3) The sending device sends the new 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 its 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 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.

Site-to-Site VPNs (IPsec)

- There are some limitations to standard IPsec:
 - 1) IPsec doesn't support broadcast and multicast traffic, only unicast. This means that routing protocols such as OSPF can't 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.
 - This can be solved with Cisco's DMVPN.
- Let's look at each of the above solutions.

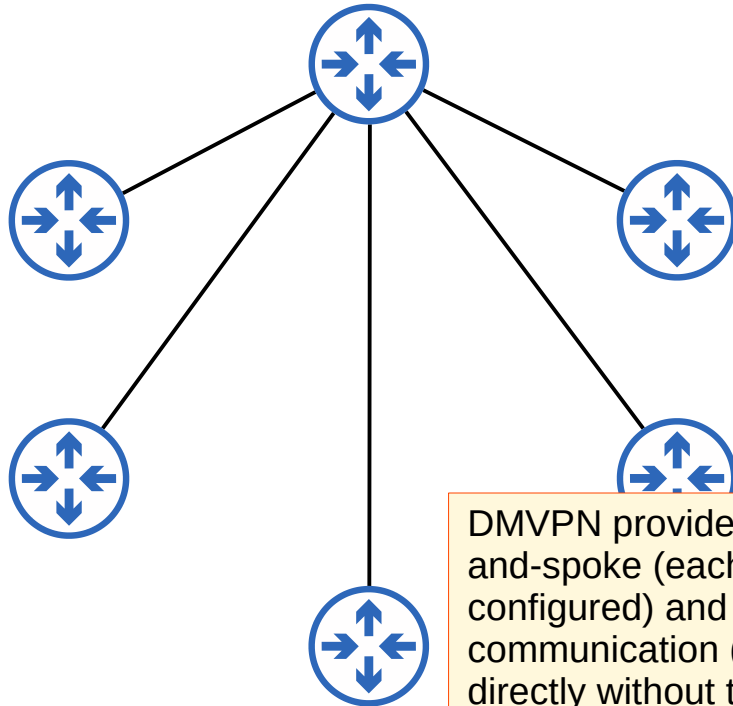
GRE over IPsec

- 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 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.

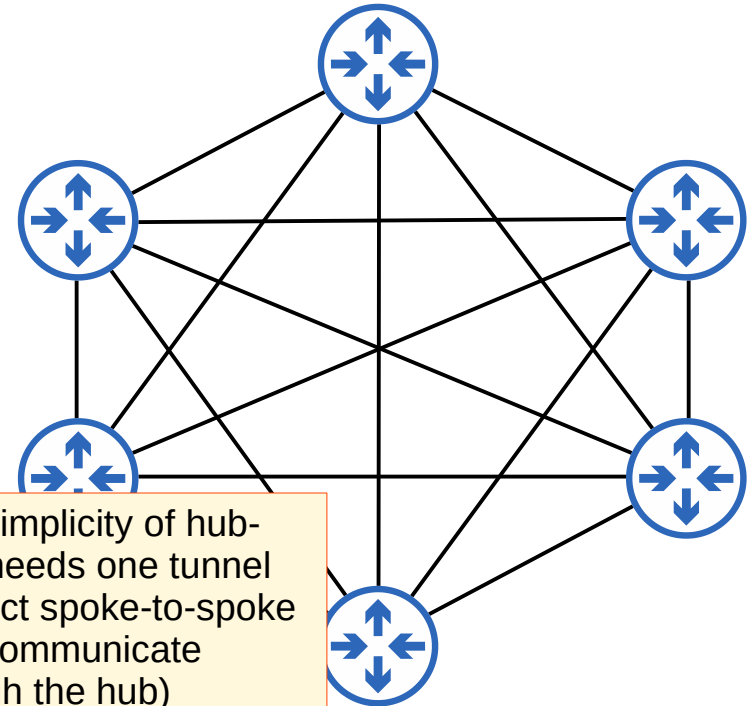


- DMVPN (Dynamic Multipoint VPN) is a Cisco-developed solution that allows routers to dynamically create a full mesh of IPsec tunnels without having to manually configure every single tunnel.

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.

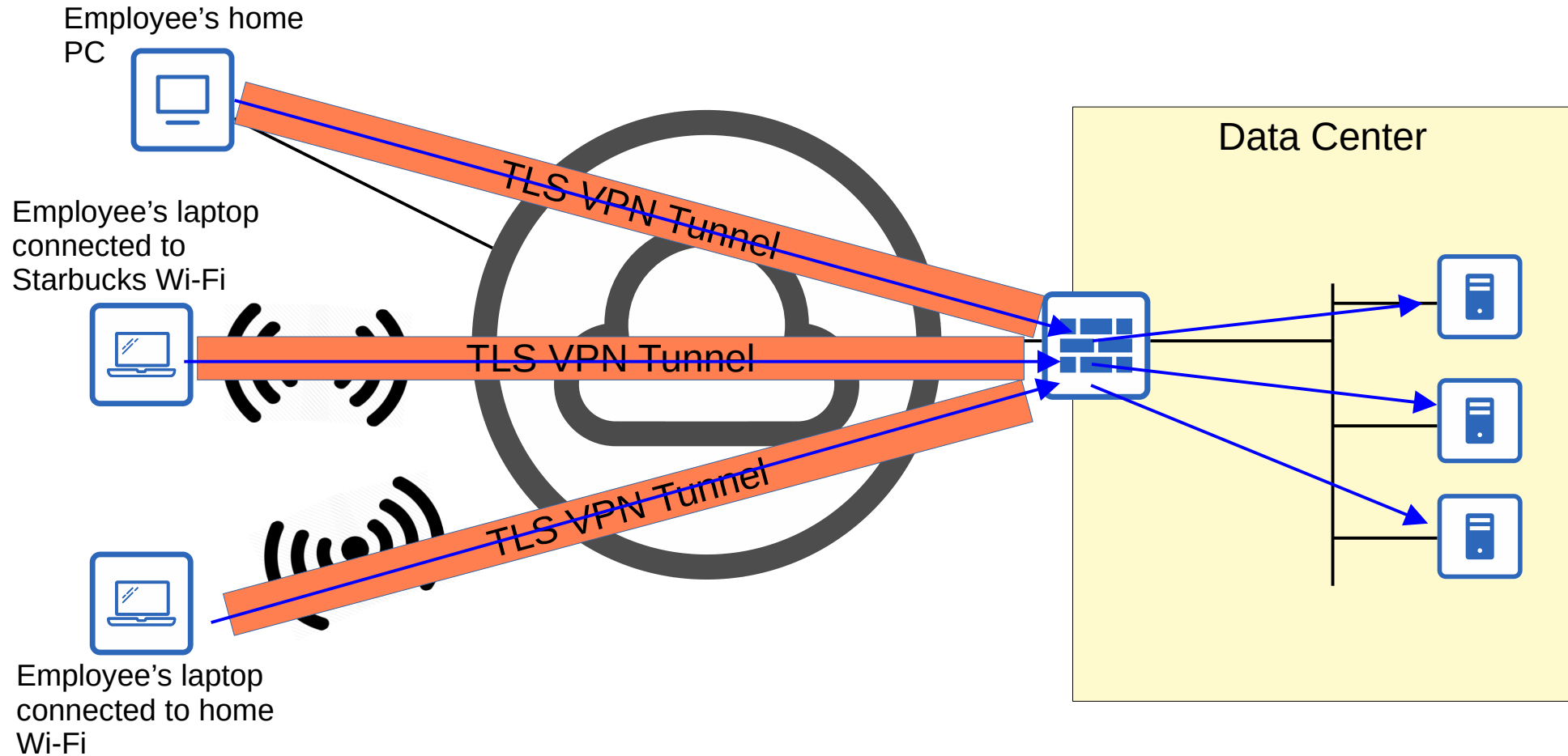


DMVPN provides the configuration simplicity of hub-and-spoke (each spoke router only needs one tunnel configured) and the efficiency of direct spoke-to-spoke communication (spoke routers can communicate directly without traffic passing through the hub)

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 phones) 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 Sockets 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.

Remote-Access VPNs



Site-to-Site vs 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.

Things we covered

- Intro to WANs
- Leased Lines
- MPLS VPNs
- Internet connectivity
- Internet VPNs

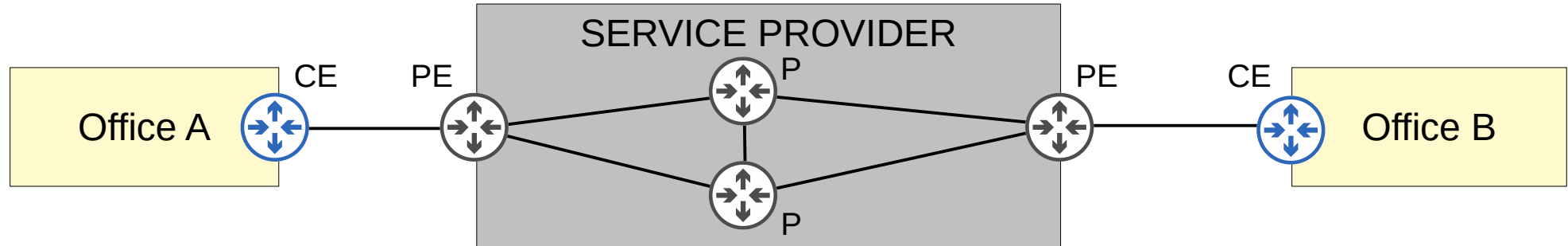
Which of the following leased line standards provides 1.544 Mbps of bandwidth?

- a) E1
- b) T1
- c) E2
- d) T2

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)

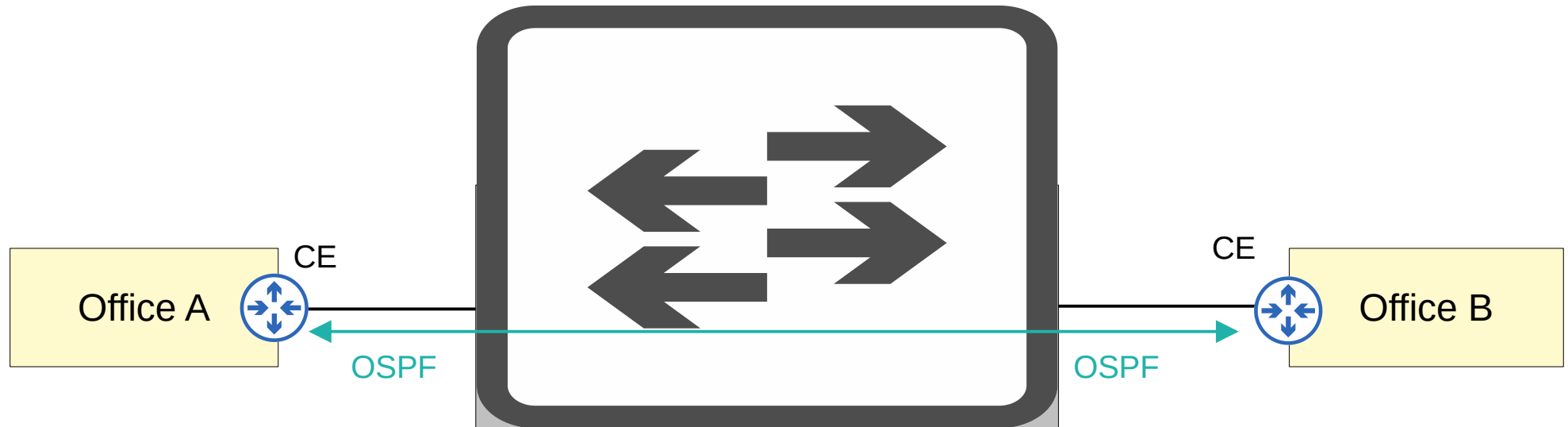
Jeremy's IT Lab Professional IT Training Inc. uses an MPLS VPN to connect its various offices together. Which of the following routers does NOT run MPLS?

- a) PE
- b) P
- c) CE



Which of the following MPLS VPN types allows CE routers to directly form OSPF peerings with each other?

- a) Layer 2 MPLS VPN
- b) Layer 2.5 MPLS VPN
- c) Layer 3 MPLS VPN



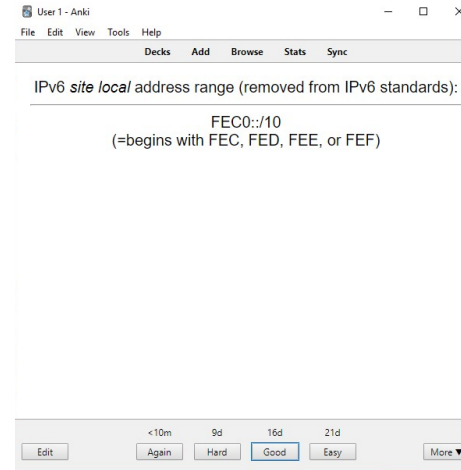
Which of the following Internet access technologies takes advantage of already-installed phone lines?

- a) Cable Internet
- b) DSL
- c) Fiber
- d) MPLS

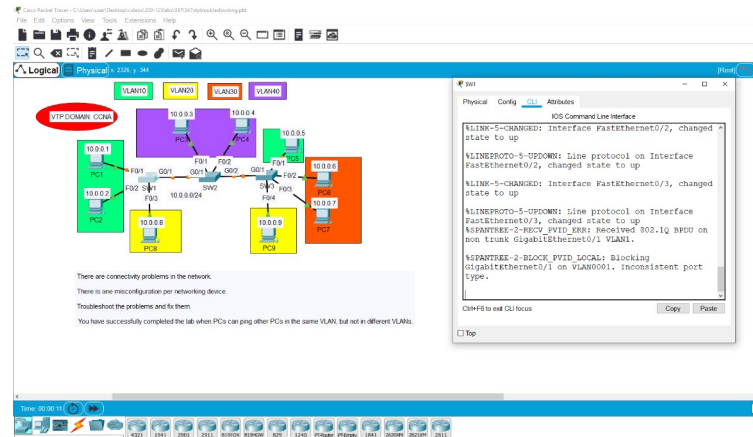
Which of the following protocols can be used in combination with IPsec to provide more flexibility by allowing multicast traffic to be forwarded in the tunnel?

- a) TLS
- b) Site-to-Site VPN
- c) GRE
- d) Remote-Access VPN






































- Review flash cards
(link in the description)



- Packet Tracer lab



JCNP-Level Channel Members

 Joseph Chase	 Samil Cañas	 Serge Romeo Kwedi Ek...	 kone fine	 john goff
 Khoa Dang	 Scott Corbitt	 Njoku Valentine	 Donald Sabusap	 funnydart
 Dragos Hirnea	 Martin Keilaus	 Viktor Balogh	 Gustavo BR	 velvijaykum
 tanvir Khan	 Tebogo Kgoloane	 Suki Ghuman	 Prakaash Rajan	Channel has been deleted
 Charlesetta Estelle	 Anand Karandikar	 Kenneth Williams	 Nasir Chowdhury	 Boson Software
 Gerrard Baker	 Павел M	 Seamus Mooney	 Erlison Santos	 Devin Sukhu
 Tom Oakes	 Abraham Yeiah	 Brandon Byers	 Marko Barbaric	 Yonatan Makara
		 Marcel Lord	 Ed Velez	 Vance Simmons

*as of July 19th, 2021

