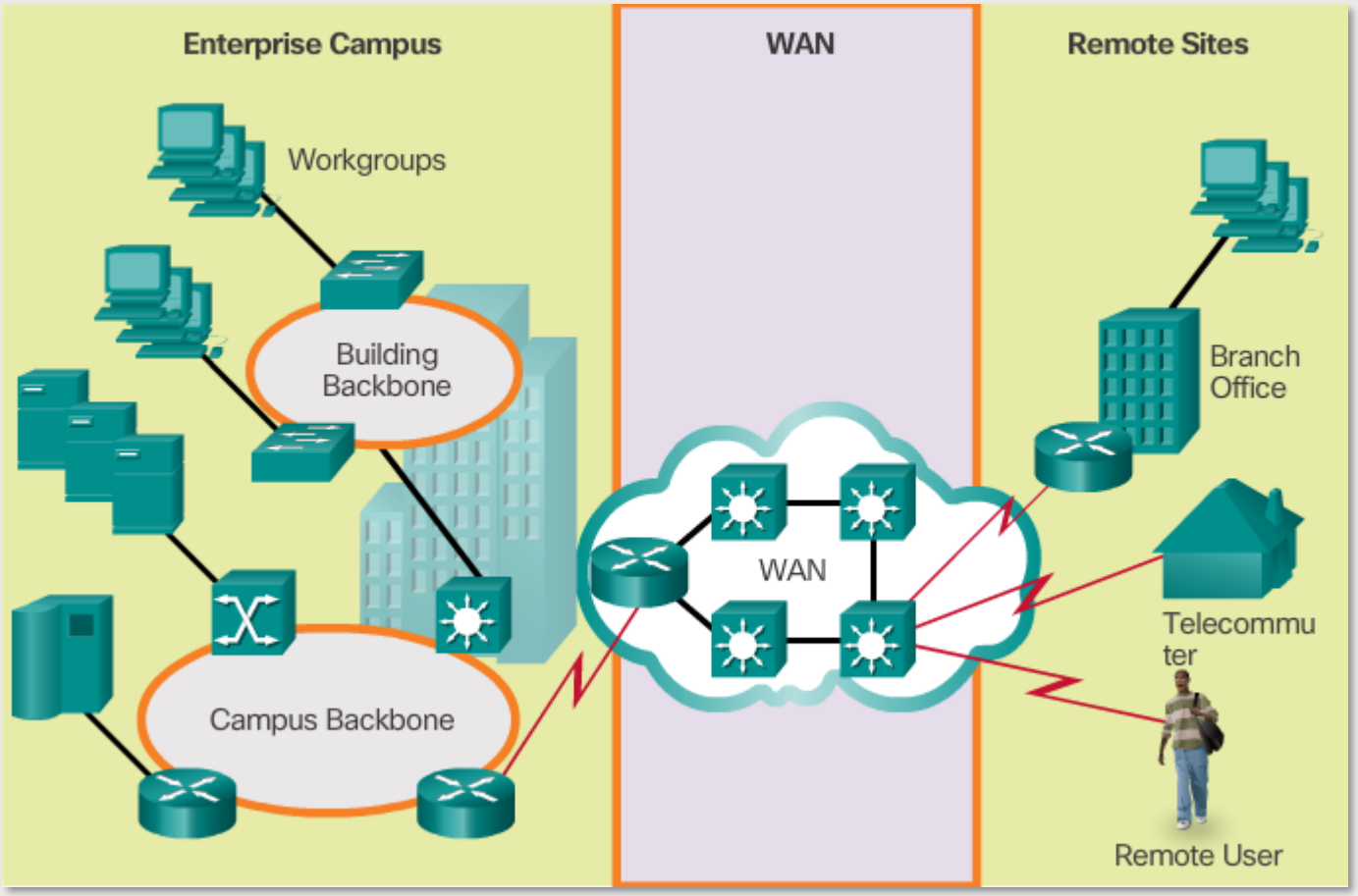
Lab 13

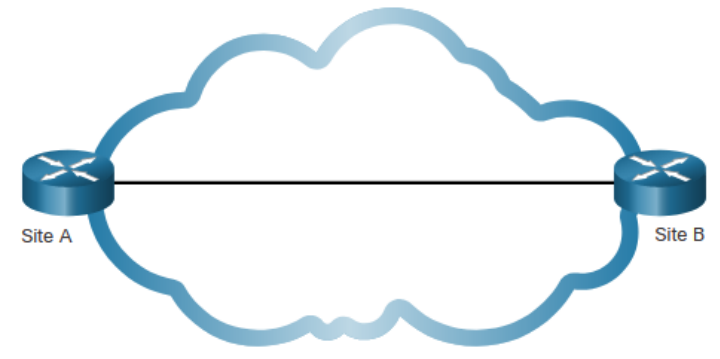
WAN technologies
Internet/Broadband VPNs

Wide Area Networks

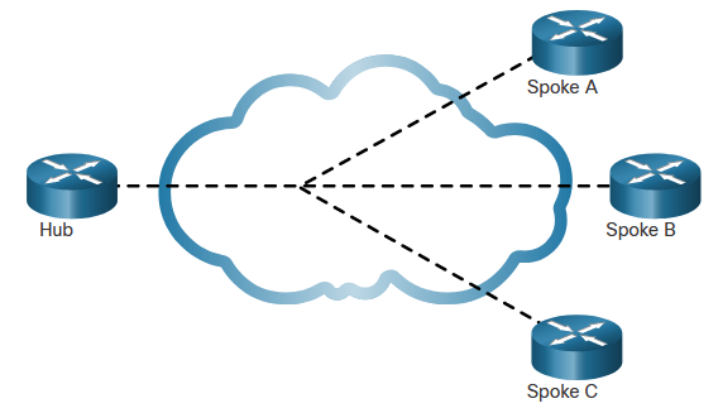
- A network that spans over a relatively large geographical area and is required to connect beyond the boundary of the LAN
- Operated by a telecommunication *provider*



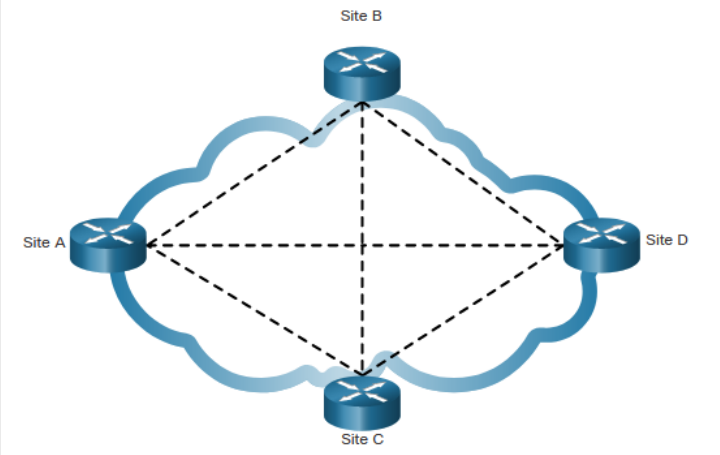
WAN topologies



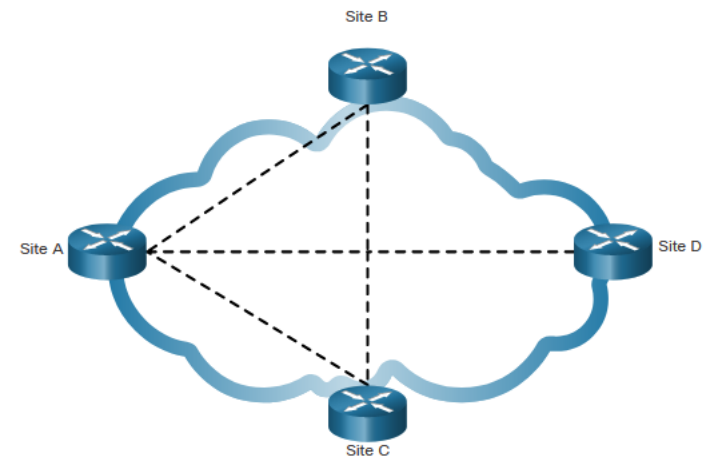
Point-to-Point Topology



Hub-and-Spoke Topology

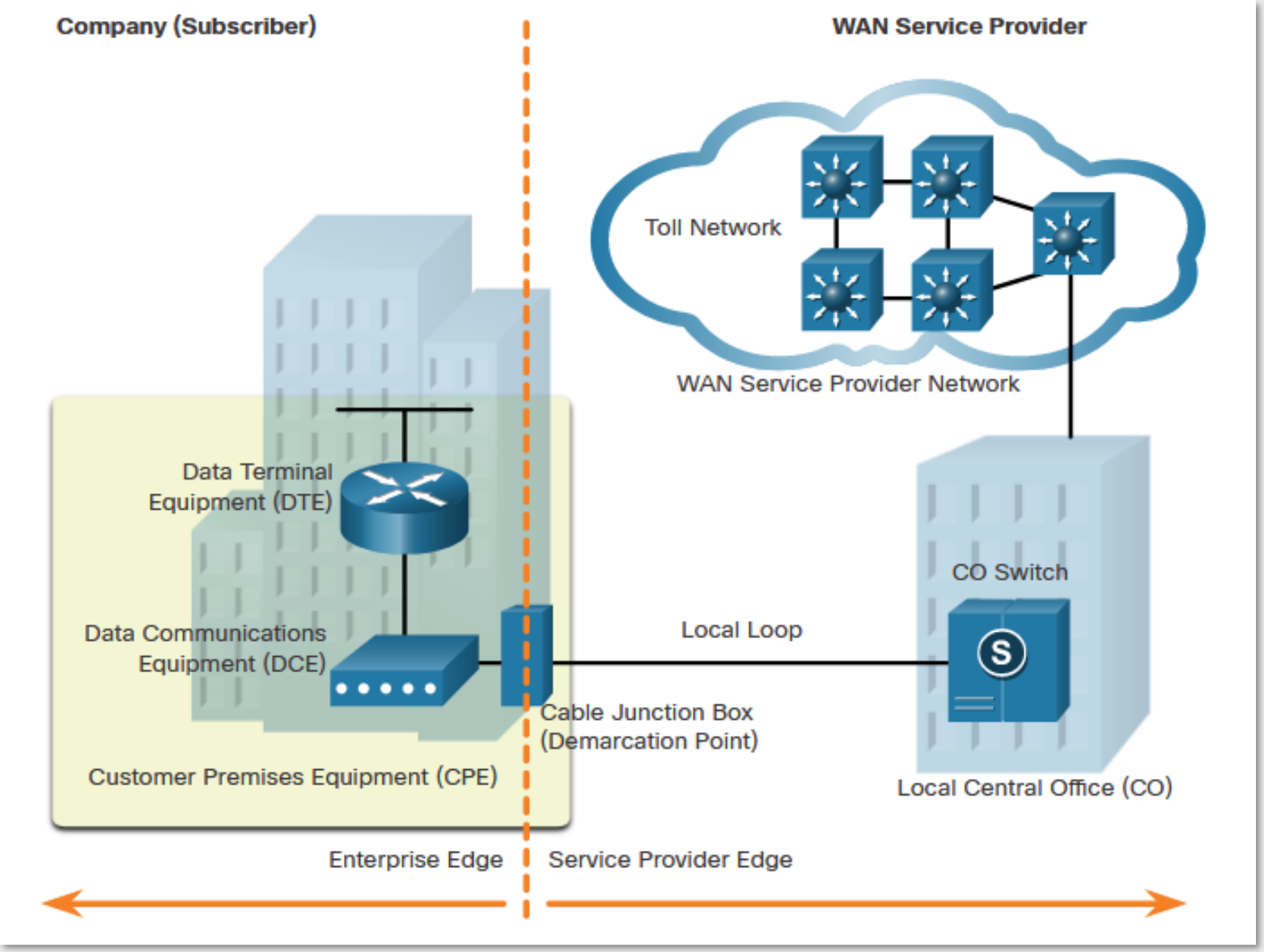


Full Mesh Topology

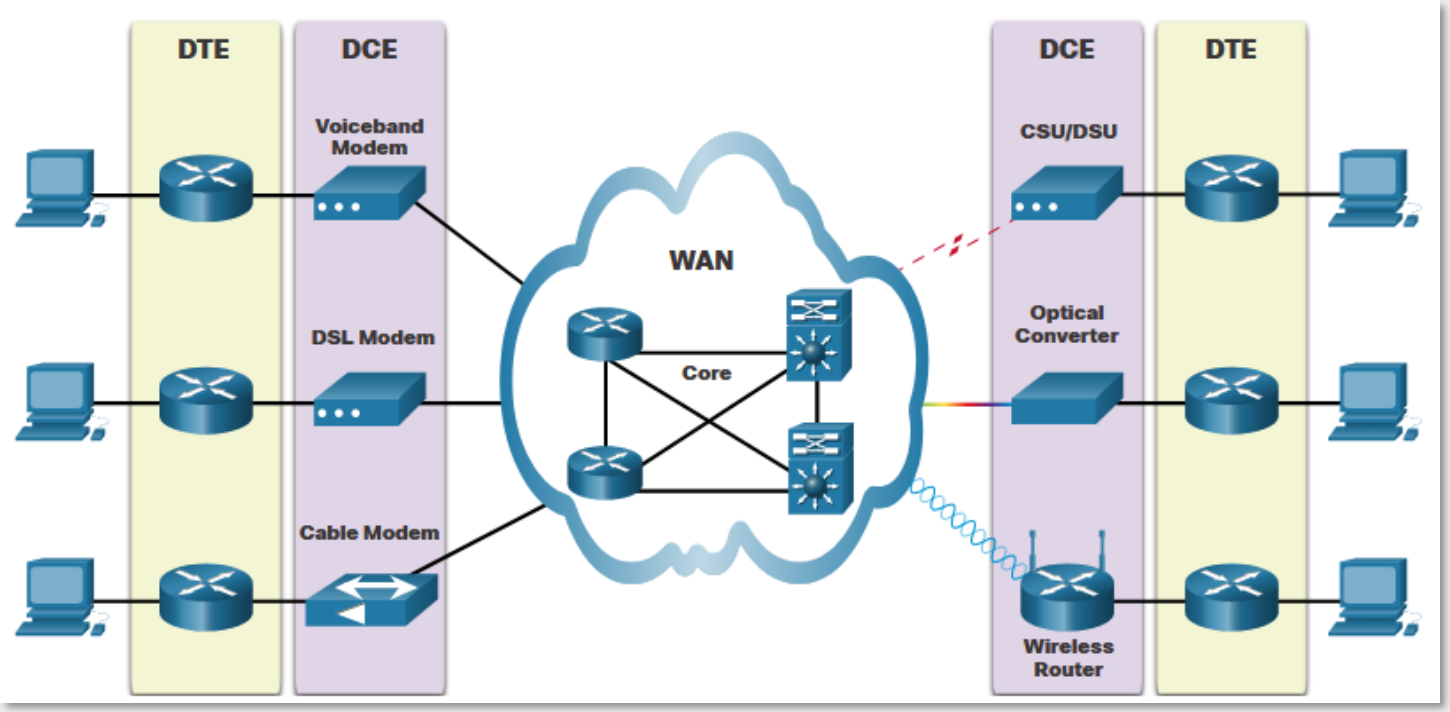


Partial Mesh Topology

WAN terminology

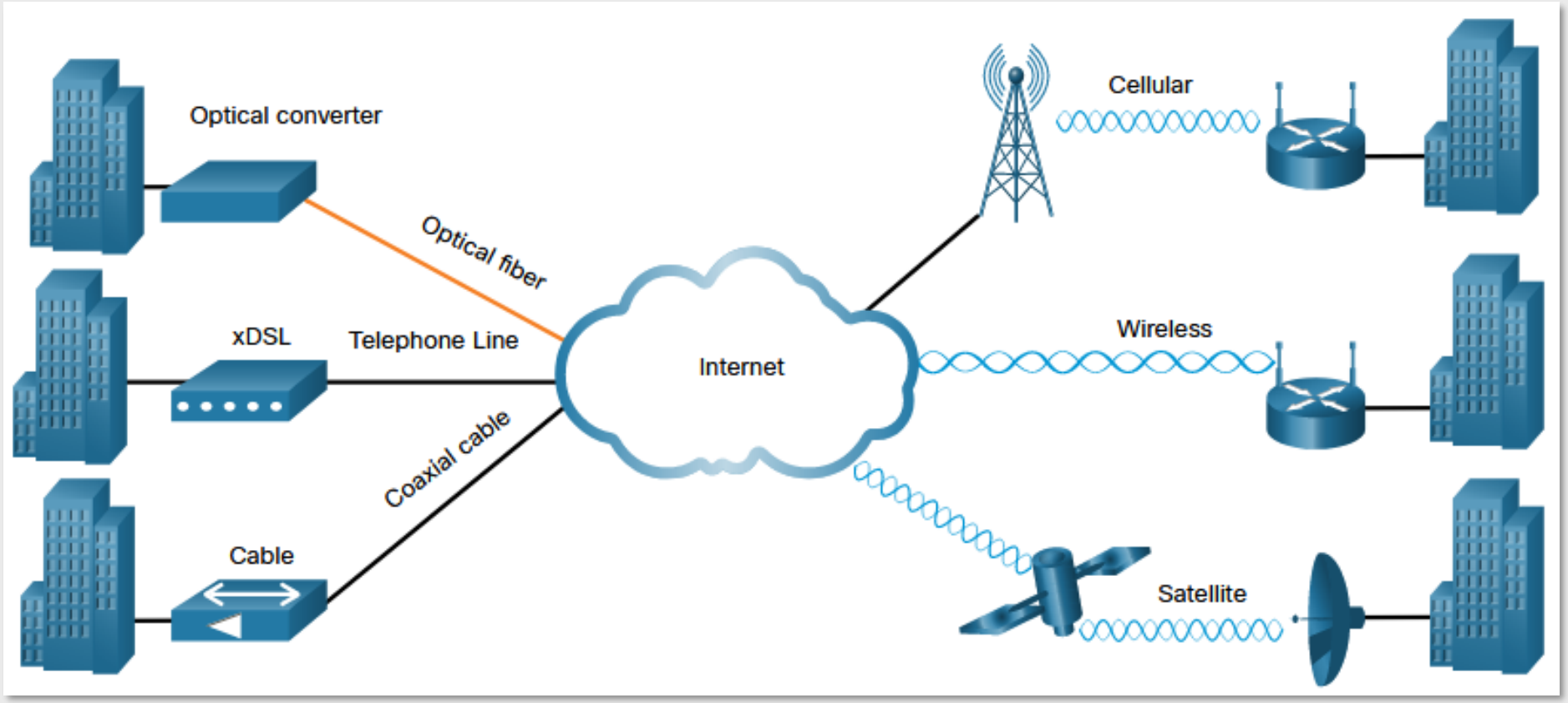


WAN devices

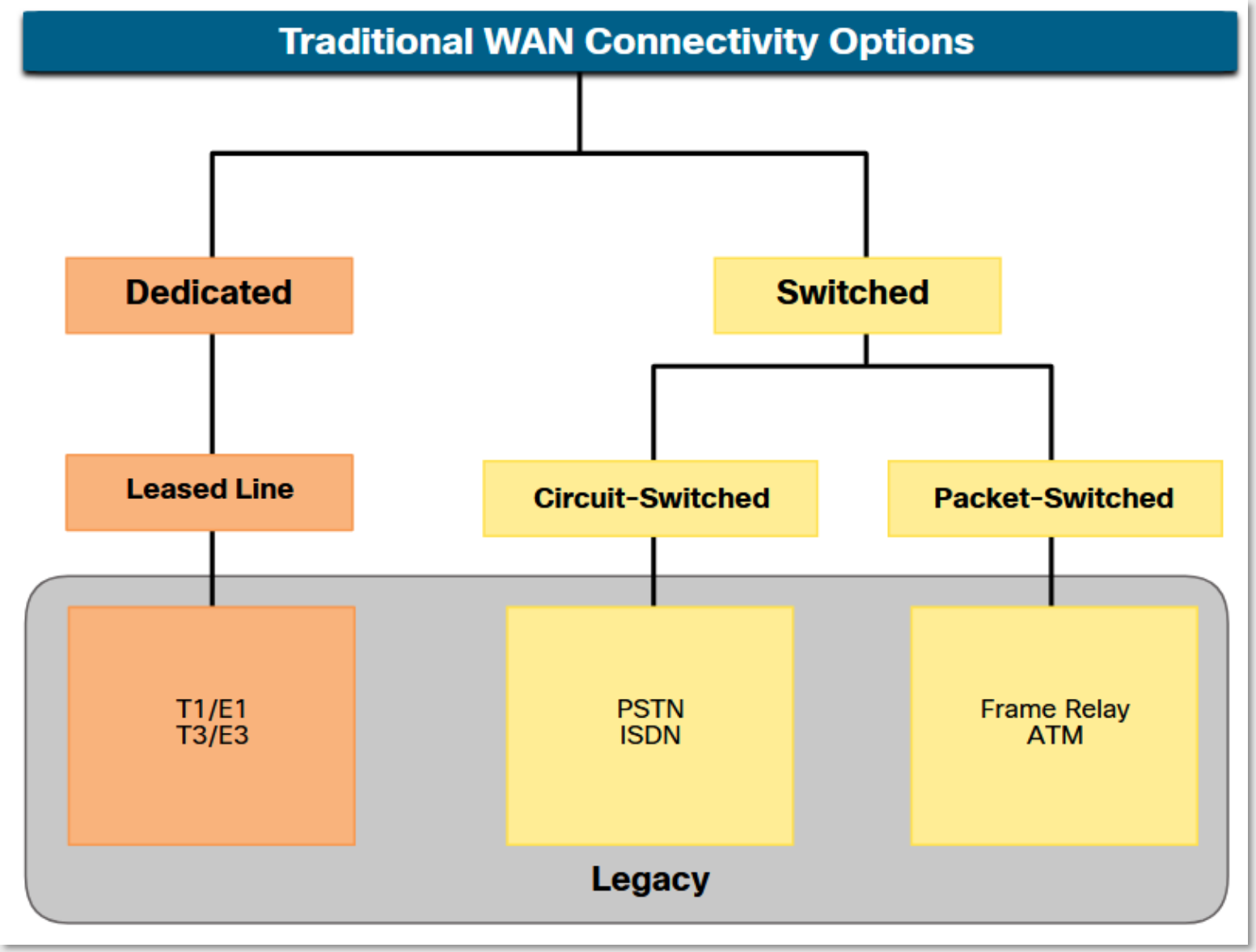


WAN Device	Description
Voiceband Modem	Dial-up modem – uses telephone lines Legacy device
DSL Modem / Cable Modem	Collectively known as broadband modems, these high-speed digital modems connect to the DTE router using Ethernet.
CSU/DSU	Digital-leased lines require a CSU and a DSU. It connects a digital device to a digital line.
Optical Converter	Connect fiber-optic media to copper media and convert optical signals to electronic pulses.
Wireless Router / Access Point	Devices are used to wirelessly connect to a WAN provider.
WAN Core devices	WAN backbone consists of multiple high-speed routers and Layer 3 switches.

WAN connectivity

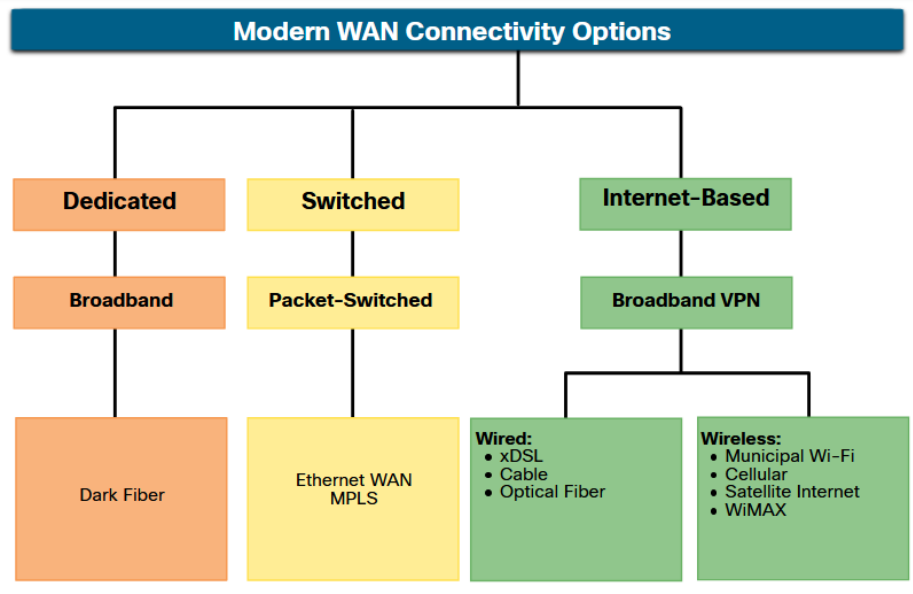


Traditional WAN services



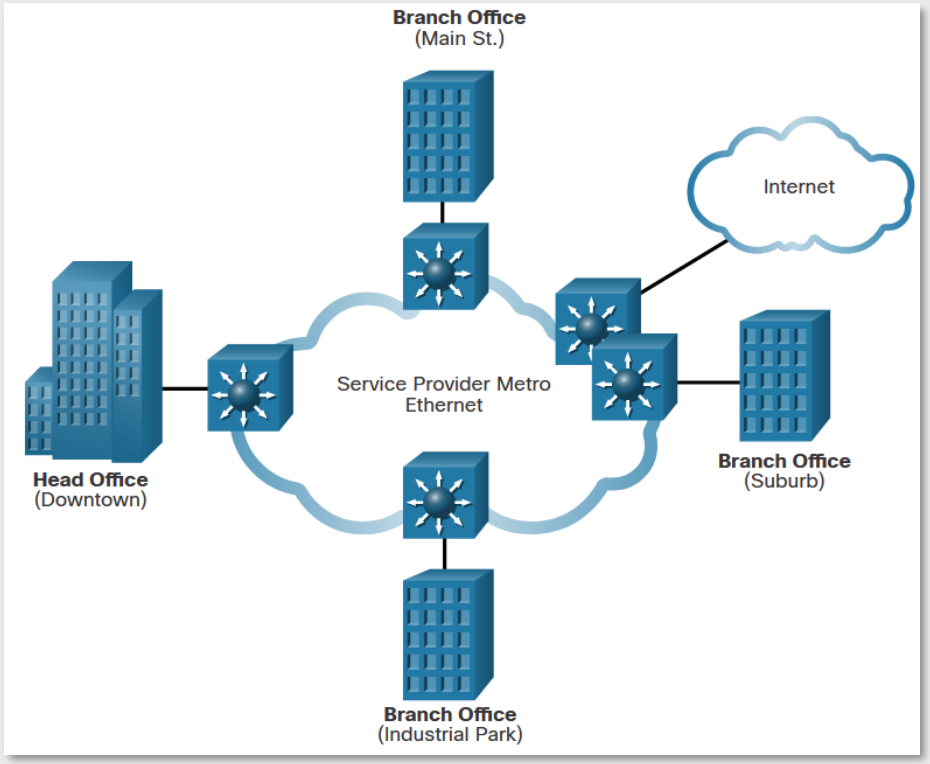
Modern WAN services

- **Dedicated broadband**
  - Fiber can be installed independently by an organization to connect remote locations directly together
  - Dark fiber can be leased or purchased from a supplier
- **Packet-switched**
  - Metro Ethernet – Replacing many traditional WAN options
  - MPLS – Enables sites to connect to the provider regardless of its access technologies
- **Internet-based broadband**
  - Organizations are now commonly using the global Internet infrastructure for WAN connectivity

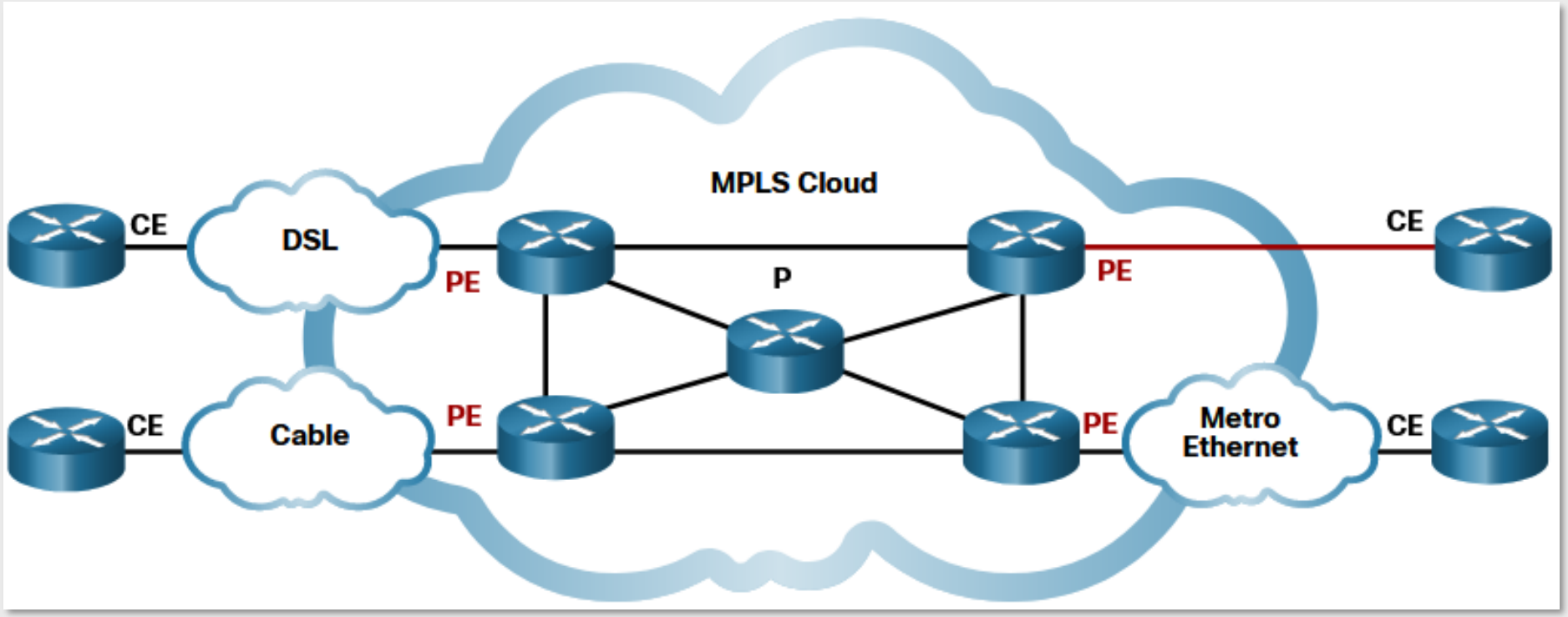


Ethernet WAN (L2VPN)

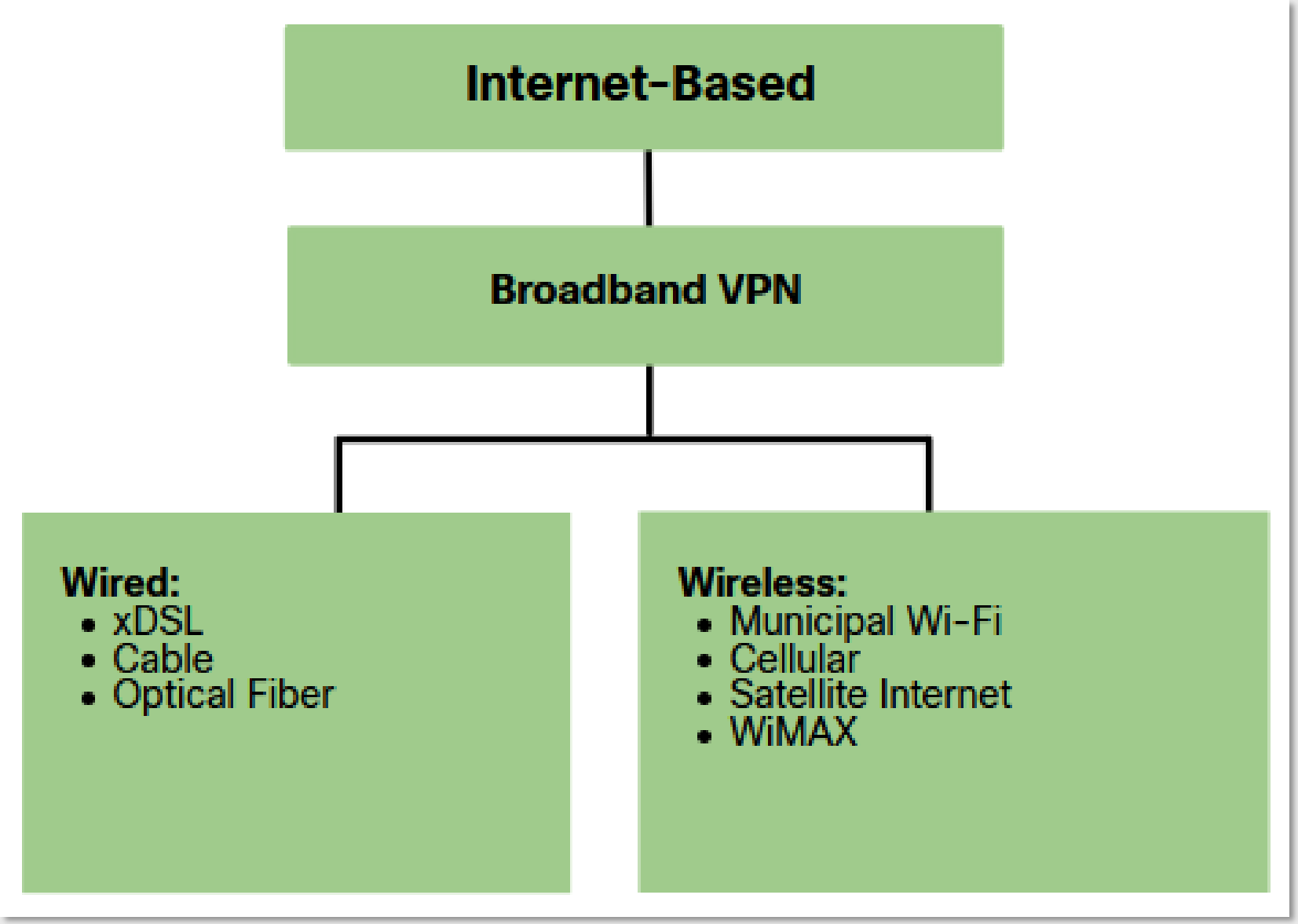
- Ethernet WAN service offered by providers based on fiber-optic cabling
  - Now commonly being used to replace the traditional serial point-to-point, Frame Relay and ATM WAN links
- Ethernet WAN service variants
  - Metro Ethernet (Metro E)
  - Ethernet over MPLS (EoMPLS)
  - Virtual Private LAN Service (VPLS)
- Benefits
  - Reduced expenses and administration
  - Easy integration with existing networks
  - Enhanced business productivity



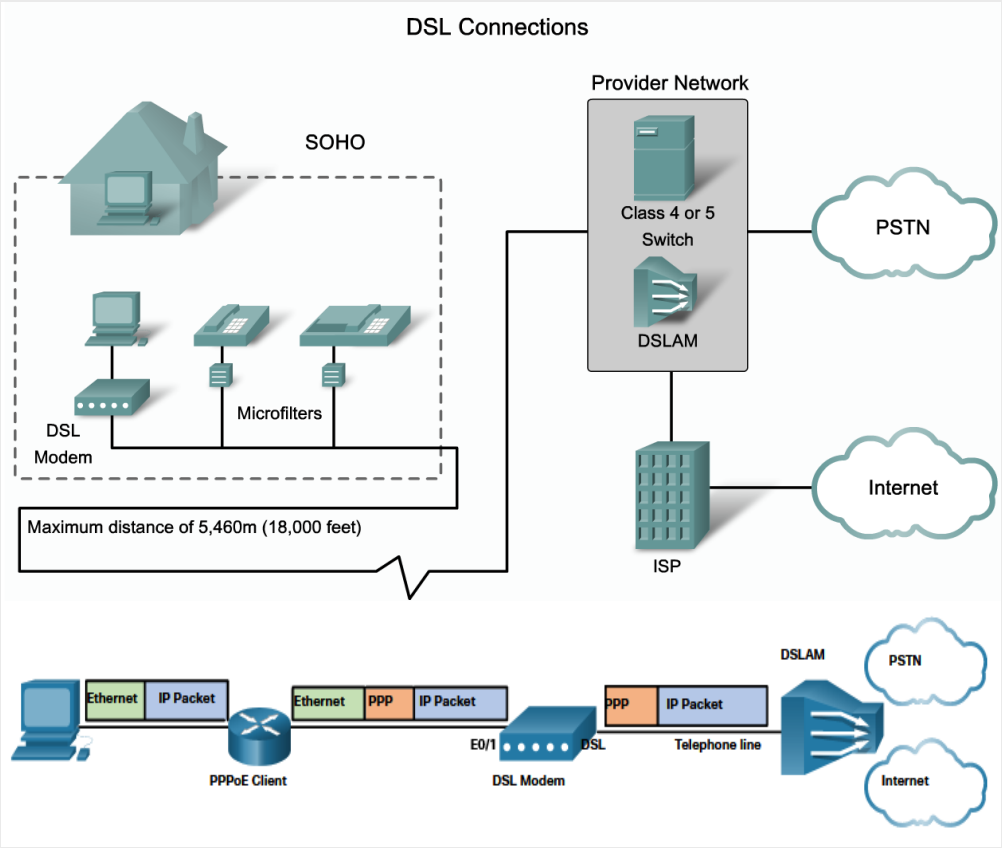
MPLS/BGP VPNs (L3VPN)

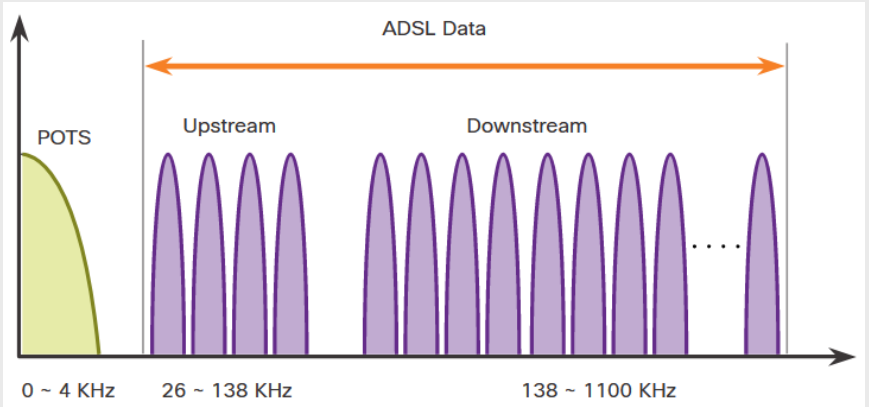


Internet-based connectivity



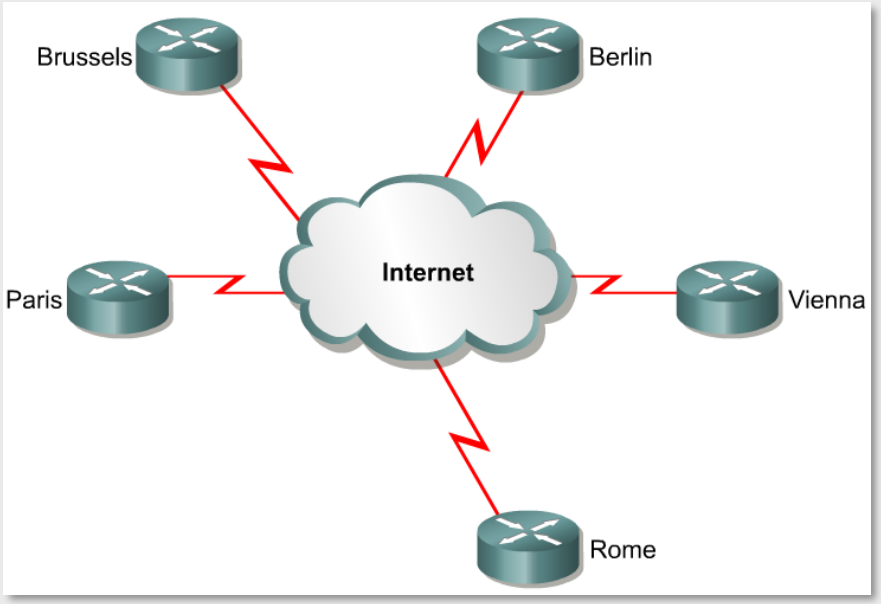
Digital Subscriber Line (xDSL)





Service	Download	Upload
ADSL	1.544 Mbps - 8.192 Mbps	16 kbps - 640 kbps
SDSL	1.544 Mbps - 2.048 Mbps	1.544 Mbps - 2.048 Mbps
HDSL	1.544 Mbps - 2.048 Mbps	1.544 Mbps - 2.048 Mbps
IDSL	144 kbps	144 kbps
RADSL	64 kbps - 8.192 Mbps	16 Mbps - 768 Mbps
CDSL	1 Mbps	16 kbps - 160 kbps

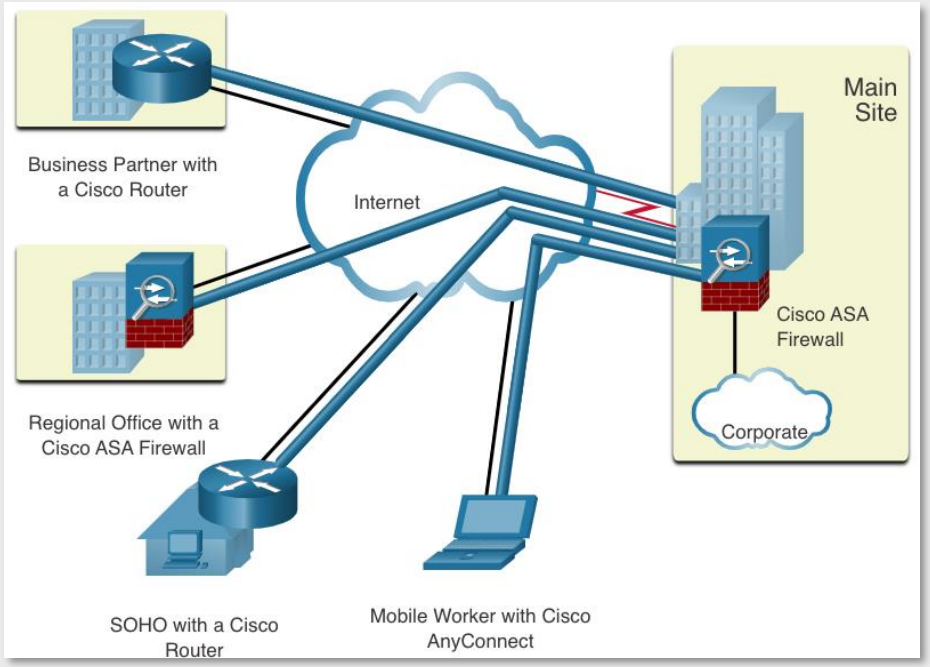
Connection to public Internet



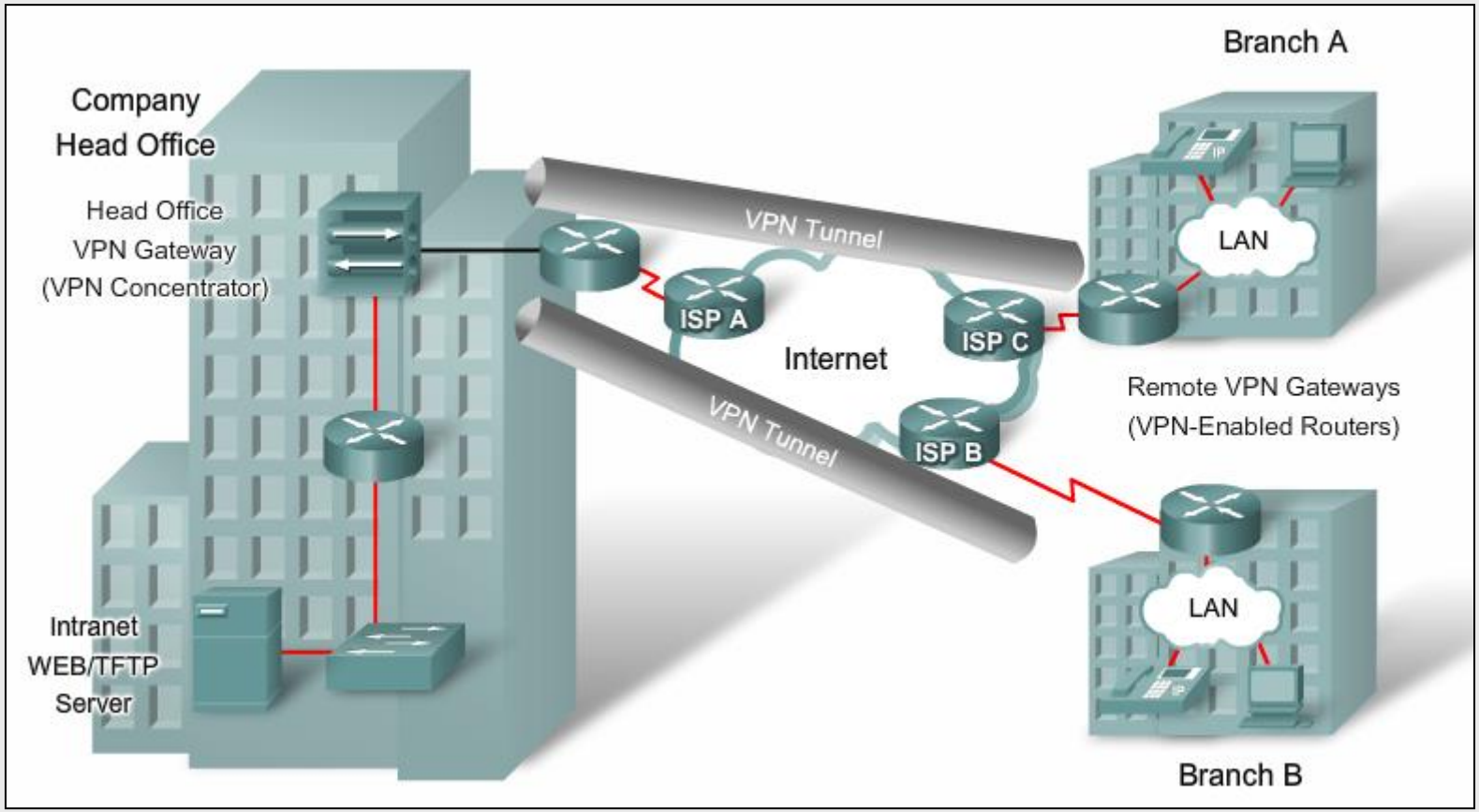
- Options
  - Each is connected to the closest ISP
    - Traffic to the Internet does not consume WAN link capacity
    - Multiple entry points for attacks
  - One router only is connected to the ISP
    - Single point of control
- The first option may be an alternative solution to provision WAN connectivity
  - Viable for limited WAN traffic with no requirements
  - Security is an issue

Enterprise VPNs

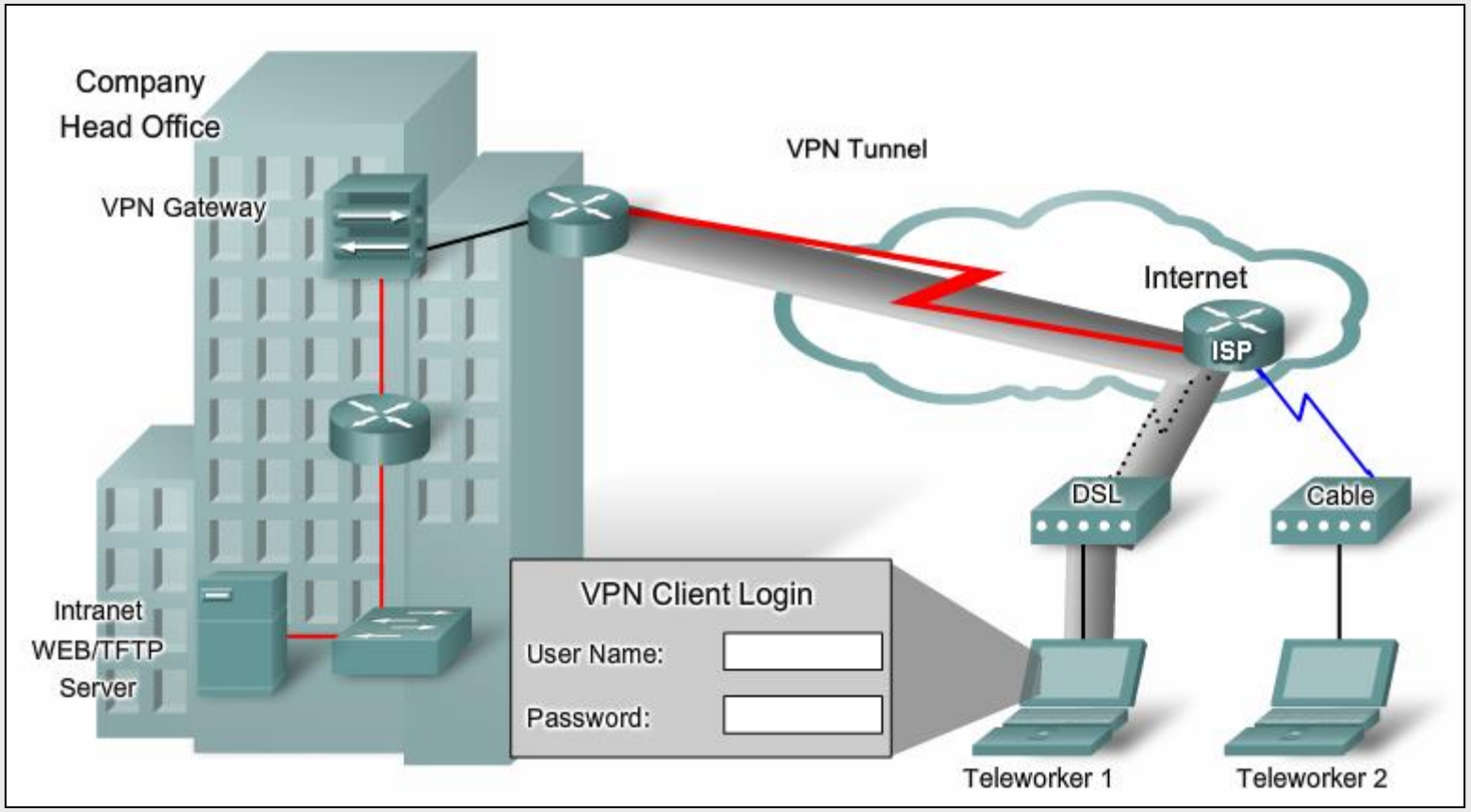
- Virtual Private Networks created and managed by the enterprise using secure end-to-end protocols (IPsec, SSL)
- Virtual: it carries information within a private network, but that information is actually transported over a public network
- Private: traffic is encrypted to keep the data confidential while it is transported across the public network
- Benefits
  - Cost savings
  - Security
  - Scalability



Site-to-site VPN

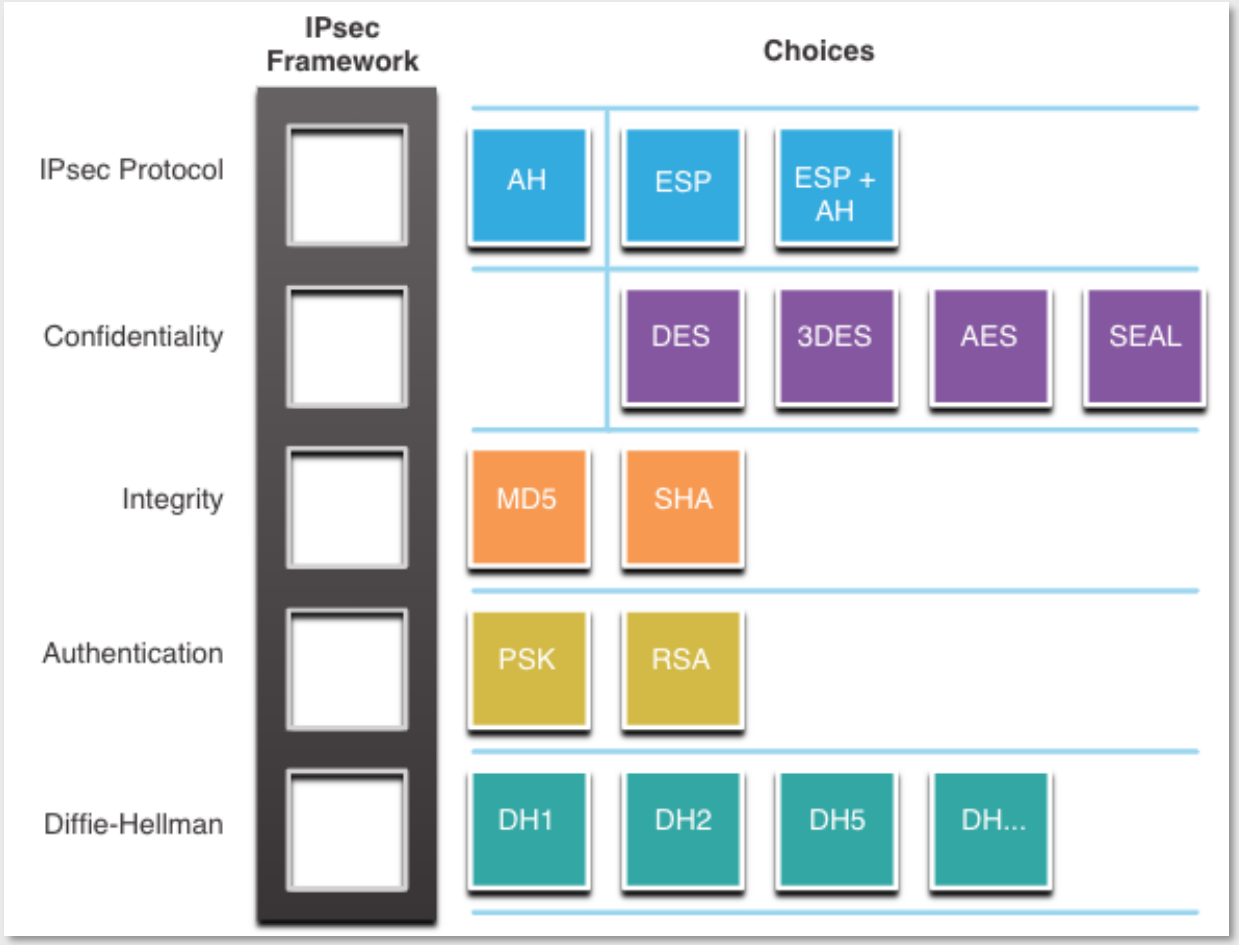


Remote access VPN



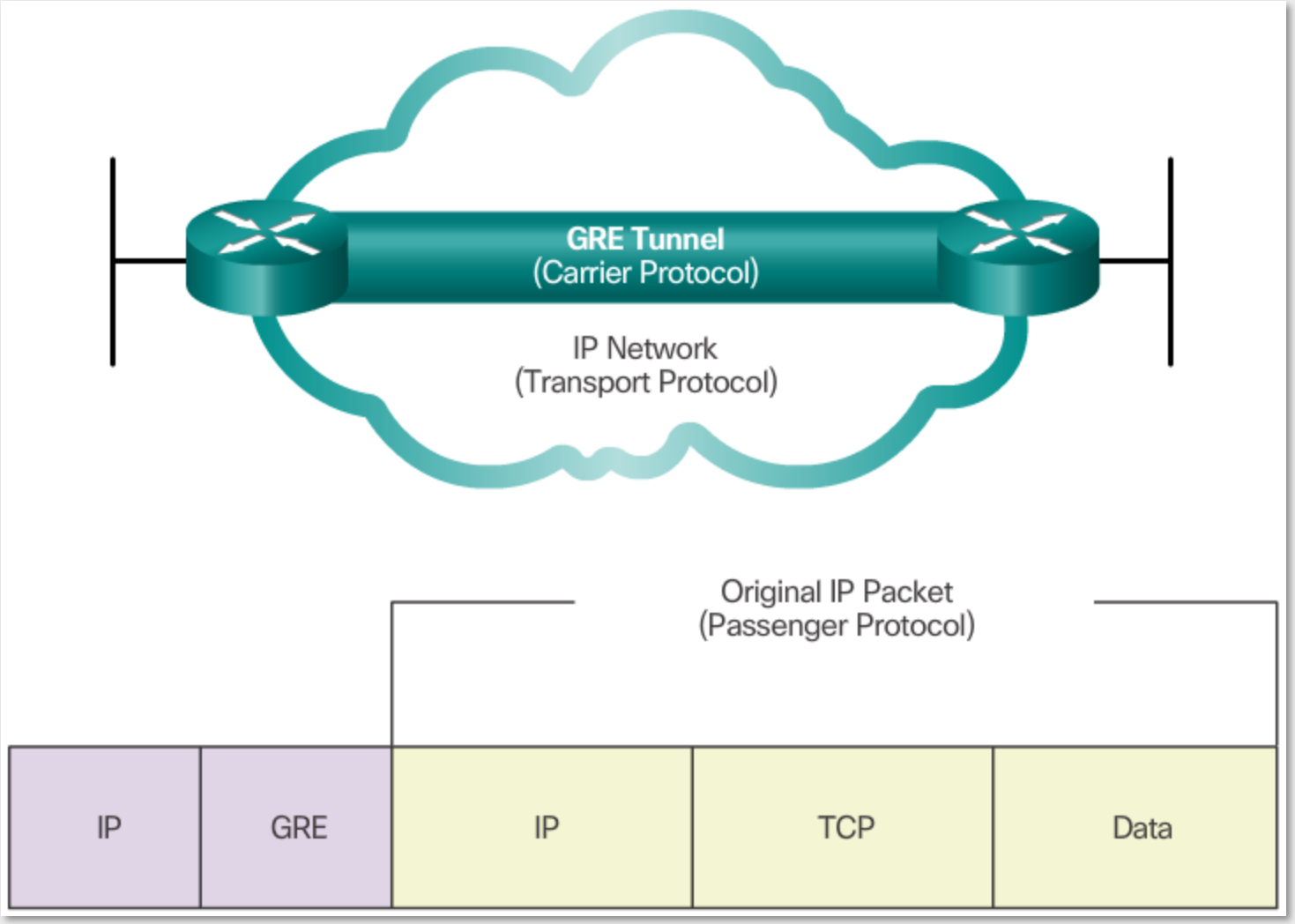
IPsec

- Authentication and encryption at IP layer
- Transparent to applications

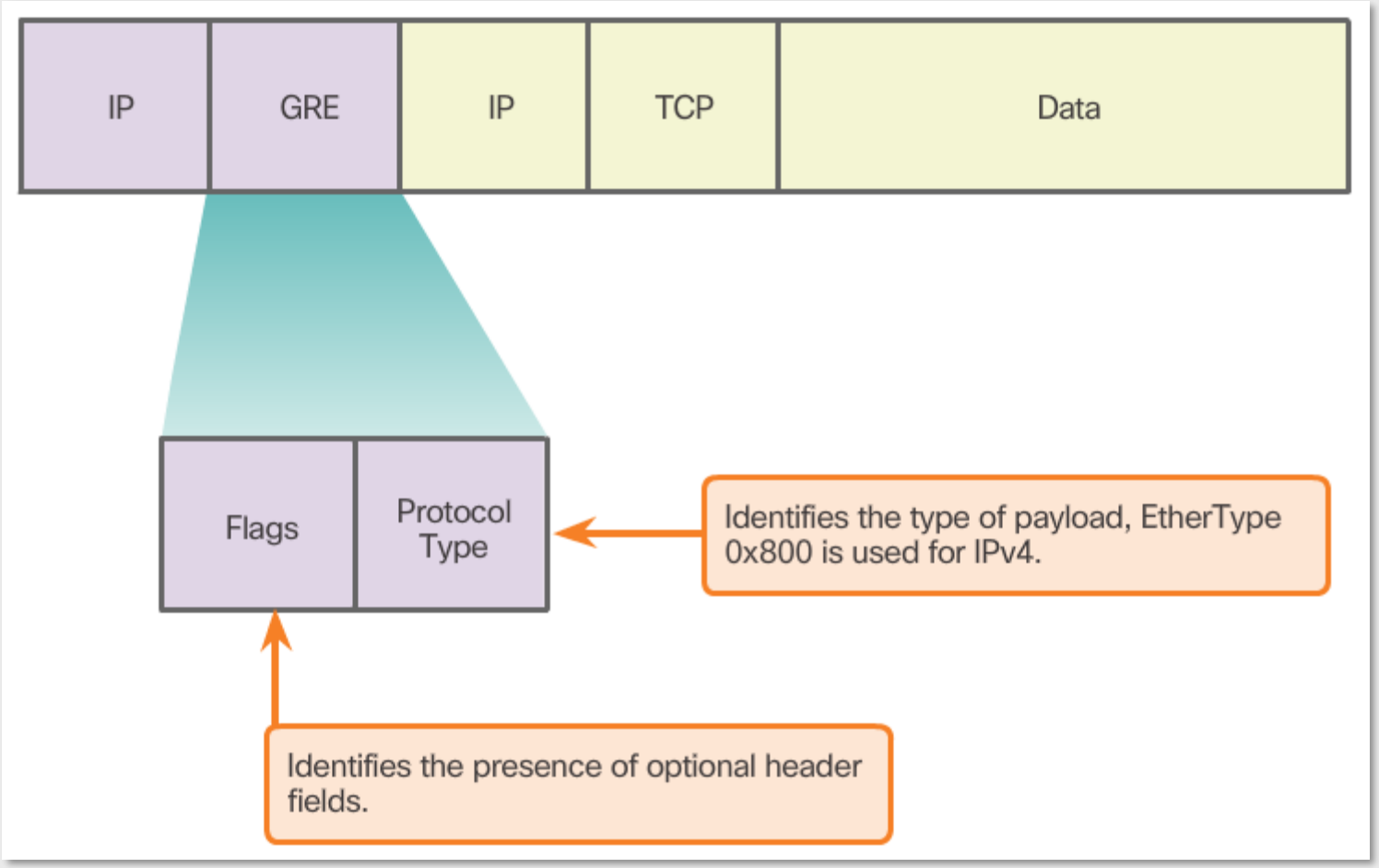


Generic Routing Encapsulation (GRE)

- RFC 2784 (March 2000), RFC 2890 (September 2000)

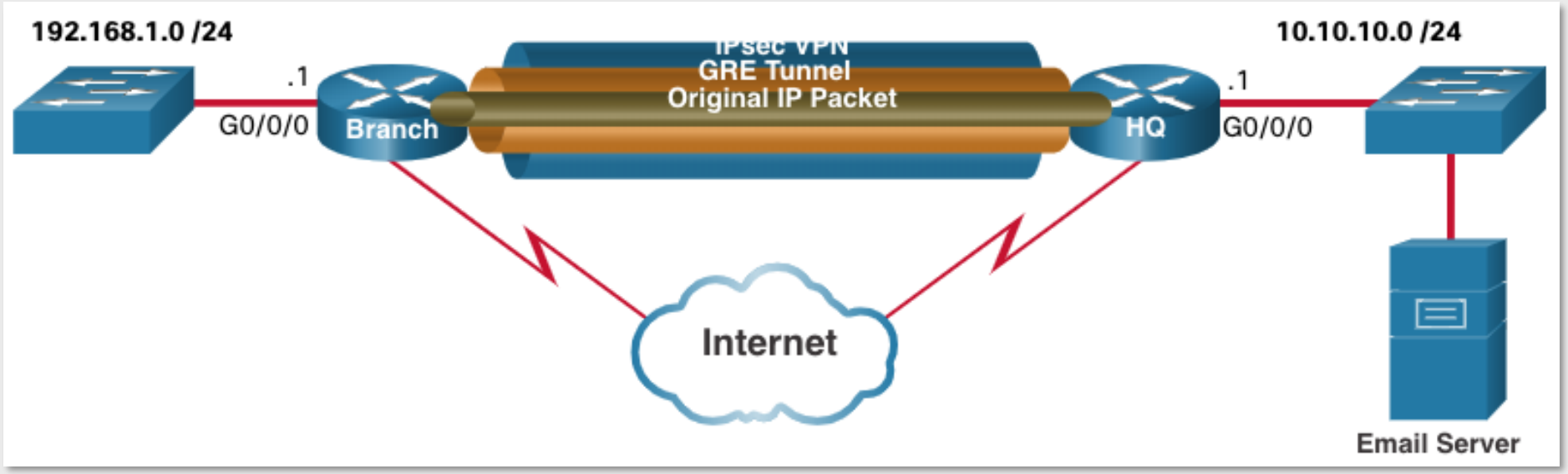


Generic Routing Encapsulation (GRE)

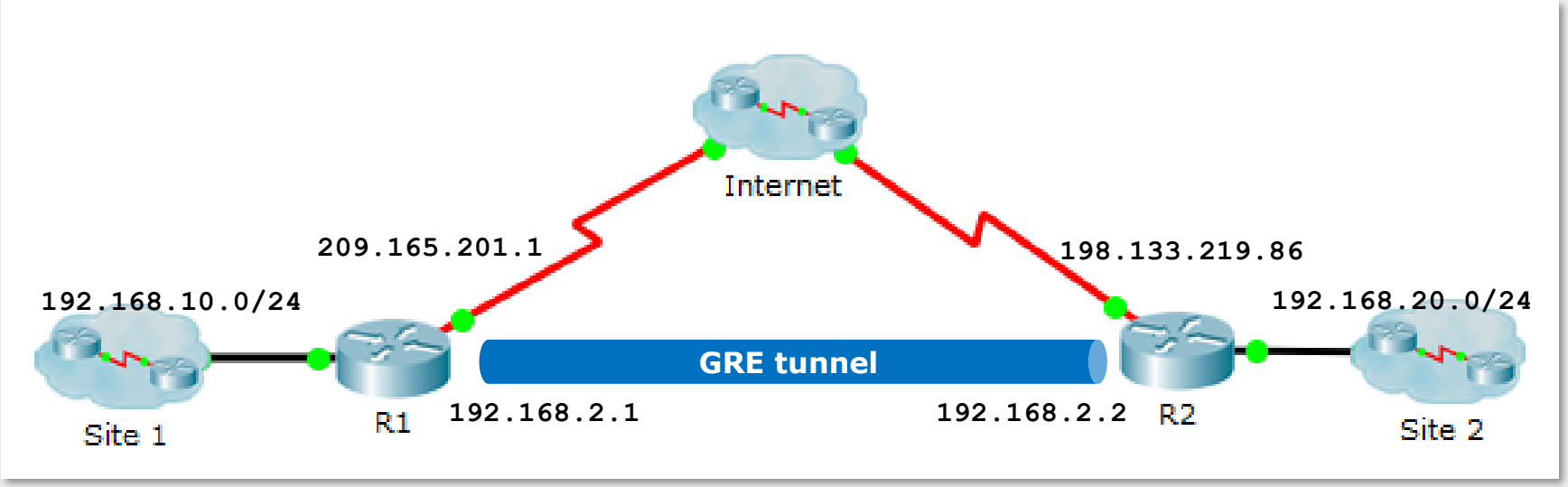


GRE over IPsec

- Allows to support routing protocol traffic over the IPsec VPNs



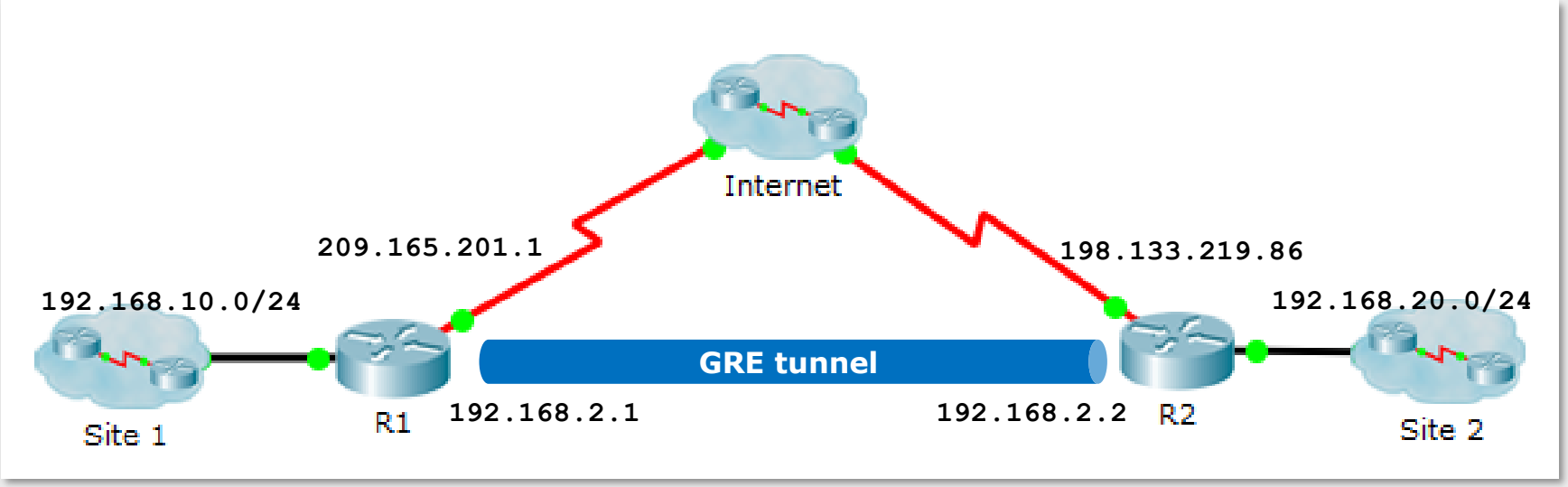
GRE configuration




```
R1(config)#interface Tunnel0
R1(config-if)#tunnel mode gre ip
R1(config-if)#ip address 192.168.2.1 255.255.255.252
R1(config-if)#tunnel source Serial0/0/0
R1(config-if)#tunnel destination 198.133.219.86
```

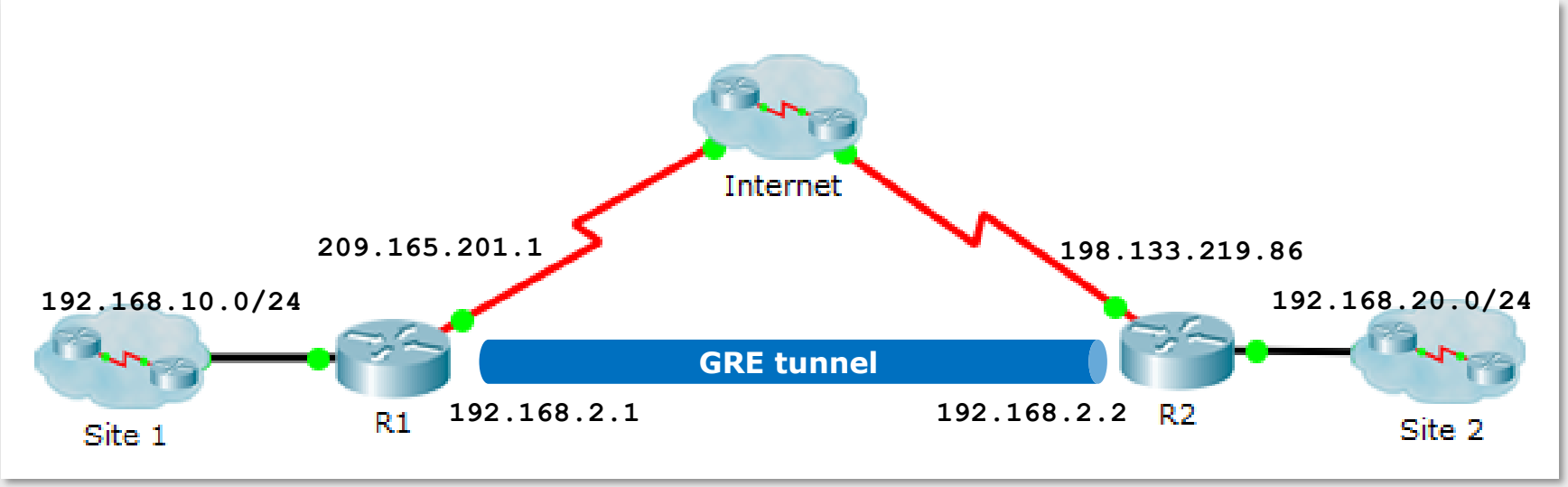
```
R2(config)#interface Tunnel0
R2(config-if)#tunnel mode gre ip
R2(config-if)#ip address 192.168.2.2 255.255.255.252
R2(config-if)#tunnel source Serial0/0/0
R2(config-if)#tunnel destination 209.165.201.1
```

GRE configuration




```
R1#show interfaces Tunnel 0
Tunnel0 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 192.168.2.1/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.201.1 (Serial0/0/0), destination 198.133.219.86
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  …
```

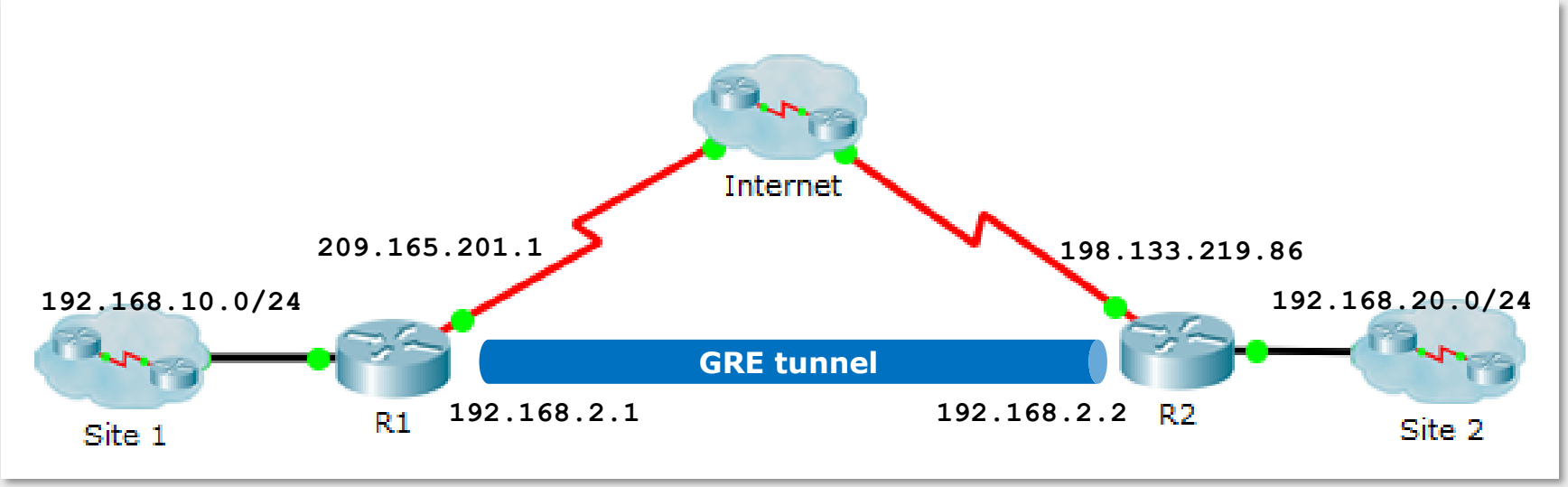
GRE configuration




```
R1(config)#router ospf 1
R1(config-router)#network 192.168.2.0 0.0.0.3 area 0
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
```

```
R2(config)#router ospf 1
R2(config-router)#network 192.168.2.0 0.0.0.3 area 0
R2(config-router)#network 192.168.20.0 0.0.0.255 area 0
```

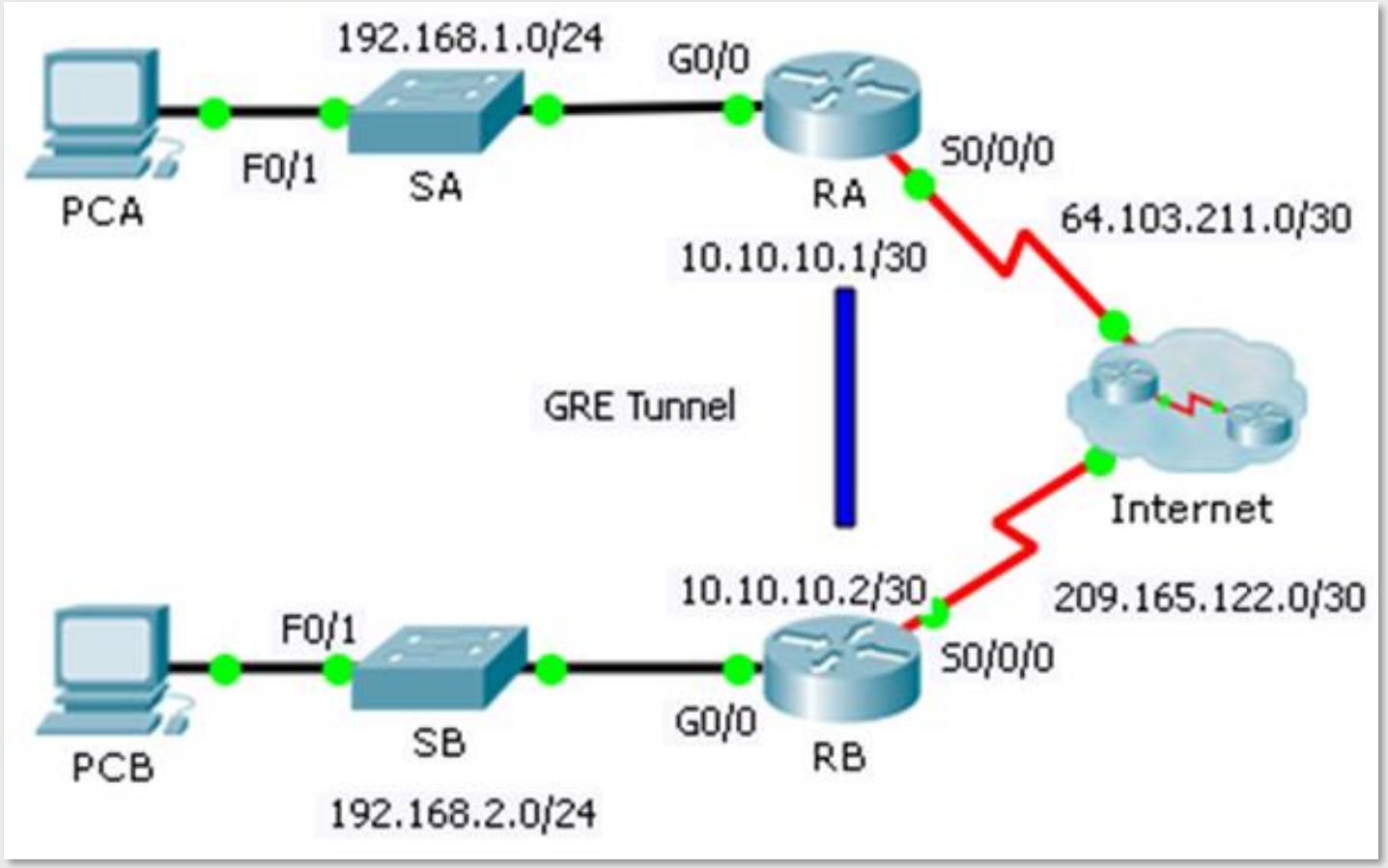
GRE configuration




```
R1#show ip route
…
Gateway of last resort is 209.165.201.2 to network 0.0.0.0

     192.168.2.0/30 is subnetted, 1 subnets
C       192.168.2.0 is directly connected, Tunnel0
C    192.168.10.0/24 is directly connected, FastEthernet0/0
O    192.168.20.0/24 [110/1001] via 192.168.2.2, 00:12:54, Tunnel0
     209.165.201.0/30 is subnetted, 1 subnets
C       209.165.201.0 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.201.2
```

Lab activity



Lab activity