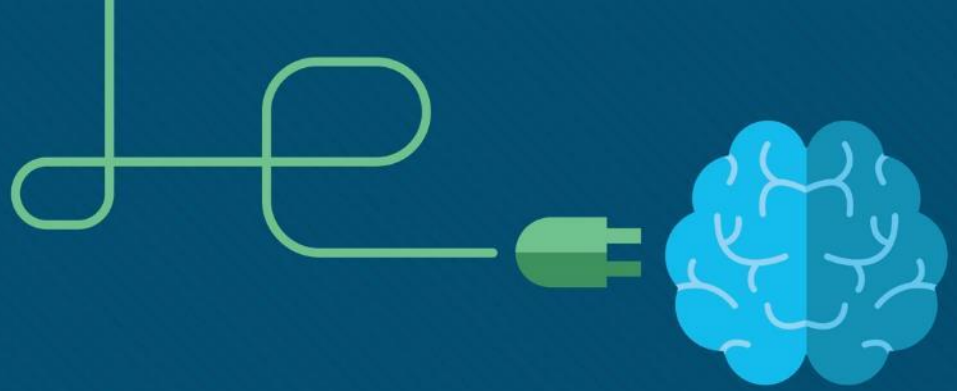


Branch Connections

CCNA Routing and Switching - Connecting Networks v6.0
Chapter 3: Branch Connections

Sections & Objectives

Remote Access Connections

- Select broadband remote access technologies to support business requirements.
  - Compare remote access broadband connection options for small to medium-sized businesses.
  - Select an appropriate broadband connection for a given network requirement.

PPPoE

- Configure a Cisco router with PPPoE.
  - Explain how PPPoE operates.
  - Implement a basic PPPoE connection on a client router.

Sections & Objectives (Cont.)

VPN

- Explain how VPN secure site-to-site and remote access connectivity.
  - Describe benefits of VPN technology.
  - Describe site-to-site and remote access VPN.

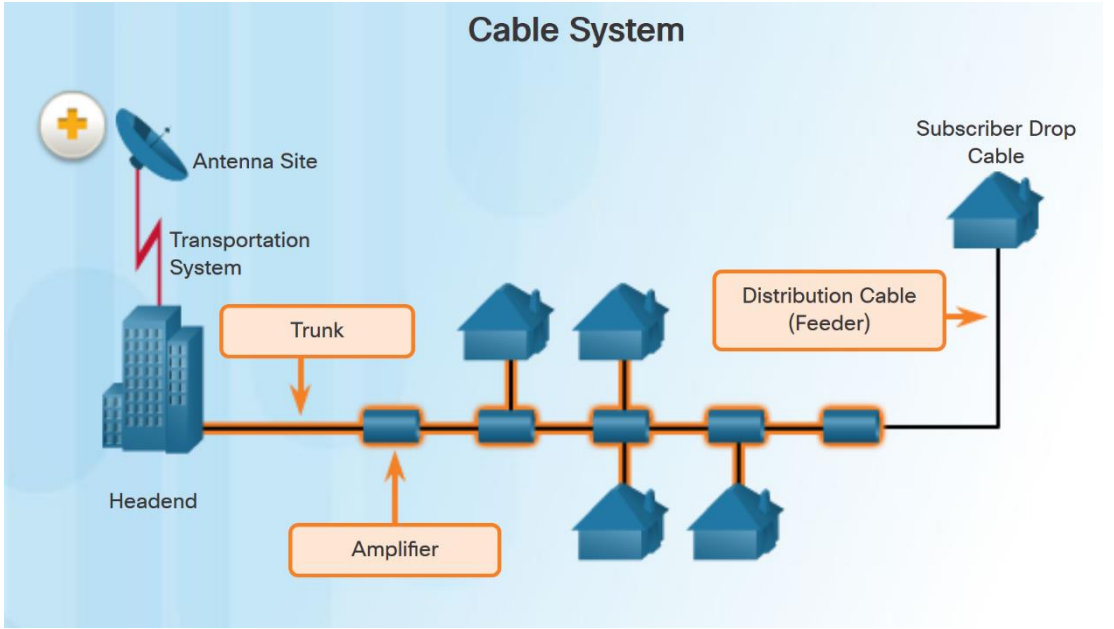
GRE

- Implement a GRE tunnel.
  - Explain the purpose and benefits of GRE tunnels.
  - Troubleshoot a site-to-site GRE tunnel.

Remote Access Connections

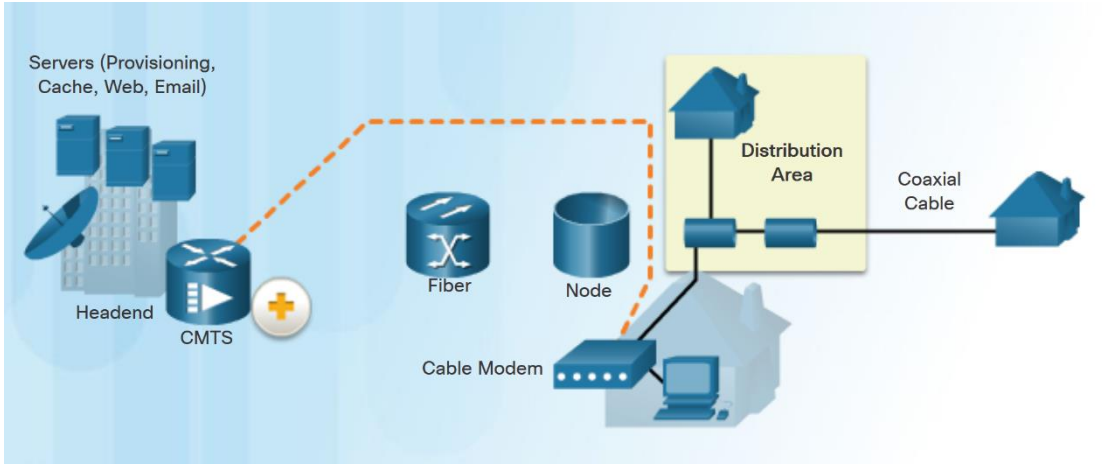
What is a Cable System?

- Cable system uses a coaxial cable that carries radio frequency (RF) signals across the network.
- Cable systems provide high-speed Internet access, digital cable television, and residential telephone service.
- Use hybrid fiber-coaxial (HFC) networks to enable high-speed transmission of data.



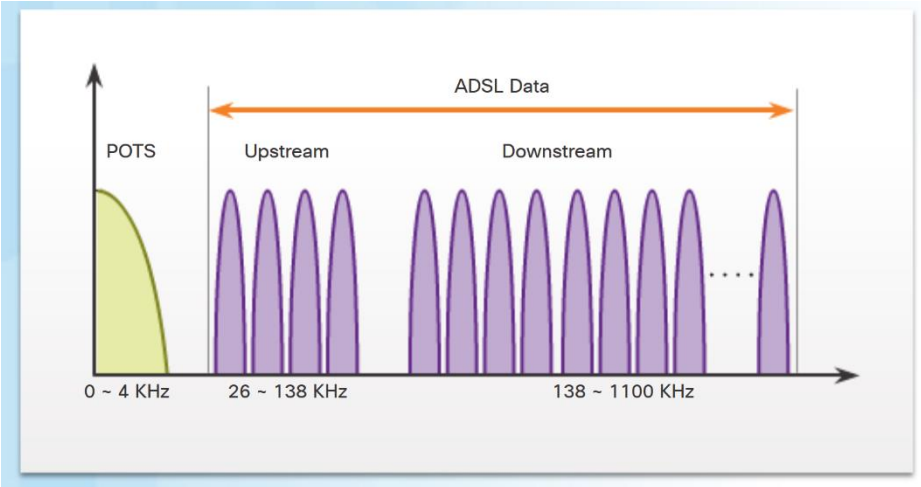
Cable Components

- Two types of equipment are required to send signals upstream and downstream on a cable system:
  - Cable Modem Termination System (CMTS) at the headend of the cable operator. The headend is a router with databases for providing Internet services to cable subscribers.
  - Cable Modem (CM) on the subscriber end.



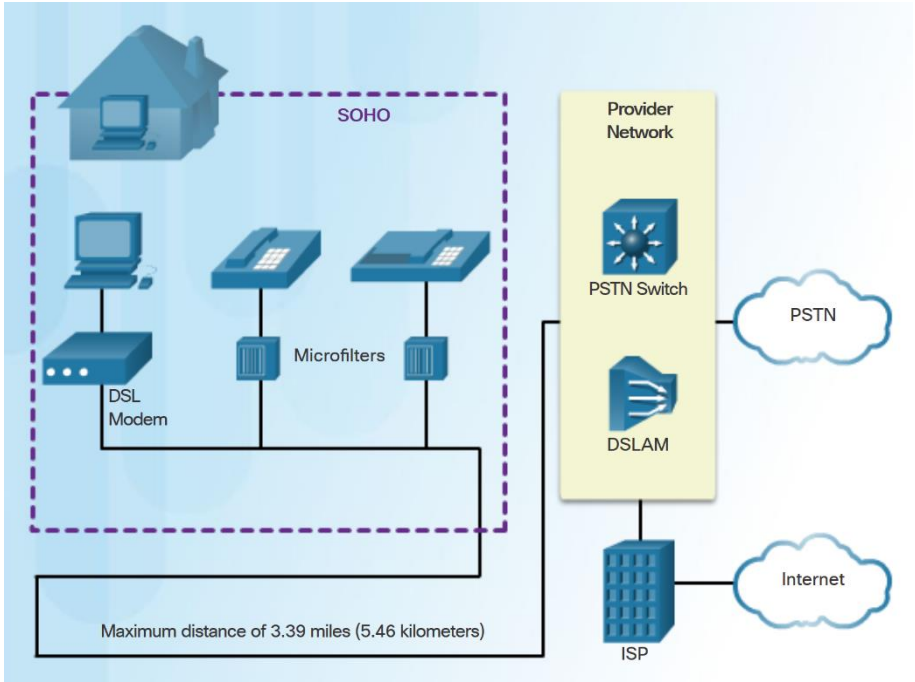
What is DSL?

- Digital Subscriber Line (DSL) is a means of providing high-speed connections over installed copper wires.
- Asymmetric DSL (ADSL) provides higher downstream bandwidth to the user than upload bandwidth.
- Symmetric DSL (SDSL) provides the same capacity in both directions.
- For satisfactory ADSL service, the local loop length must be less than 3.39 miles (5.46 km).



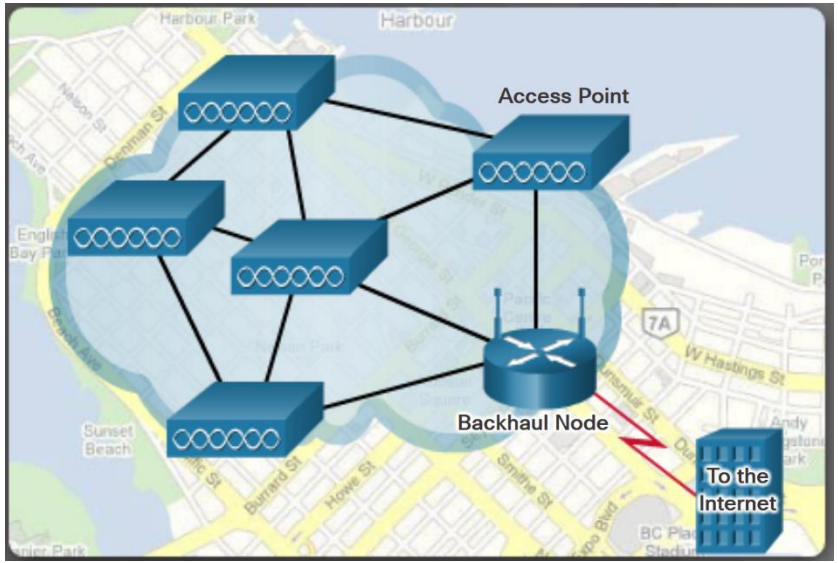
The figure shows a representation of bandwidth space allocation on a copper wire for ADSL. POTS (Plain Old Telephone System) identifies the frequency range used by the voice-grade telephone service. The area labeled ADSL represents the frequency space used by the upstream and downstream DSL signals.

DSL Connections



- The DSL connection is set up between the customer premises equipment (CPE) and the DSL access multiplexer (DSLAM) device located at the Central Office (CO).
- Key components in the DSL connection:
  - Transceiver - Usually a modem in a router which connects the computer of the teleworker to the DSL.
  - DSLAM - Located at the CO of the carrier, it combines individual DSL connections from users into one high-capacity link to an ISP.
- Advantage of DSL over cable technology is that DSL is not a shared medium. Each user has a separate direct connection to the DSLAM.

Wireless Connection



- Three main broadband wireless technologies:
  - **Municipal Wi-Fi** - Most municipal wireless networks use a mesh of interconnected access points as shown in figure.
  - **Cellular/mobile** - Mobile phones use radio waves to communicate through nearby cell towers. Cellular speeds continue to increase. LTE Category 10 supports up to 450 Mb/s download and 100 Mb/s upload. 5G Promises a theoretical maximum of 10 Gb/s.
  - **Satellite Internet** - Used in locations where land-based Internet access is not available. Primary installation requirement is for the antenna to have a clear view toward the equator.

Note: WiMAX has largely been replaced by LTE for mobile access, and cable or DSL for fixed access.

Comparing Broadband Solutions

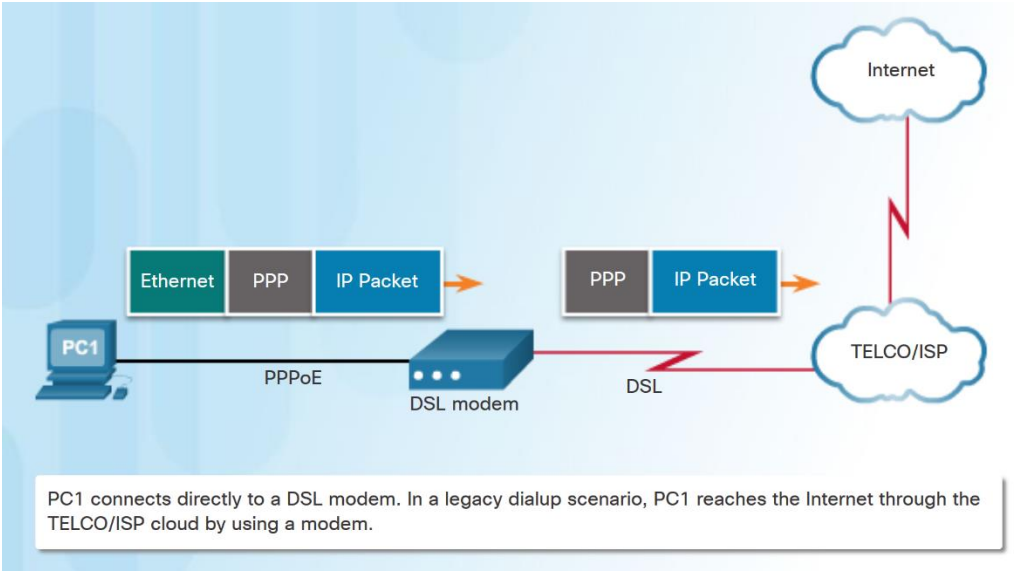
- Factors to consider in selecting a broadband solution:
  - **Cable -** Bandwidth shared by many users, slow data rates during high-usage hours.
  - **DSL** - Limited bandwidth that is distance sensitive (in relation to the ISP's central office).
  - **Fiber-to-the-Home** - Requires fiber installation directly to the home.
  - **Cellular/Mobile** - Coverage is often an issue.
  - **Wi-Fi Mesh** - Most municipalities do not have a mesh network deployed.
  - **Satellite** - Expensive, limited capacity per subscriber

PPP over Ethernet - PPPoE

PPPoE Motivation

- PPP can be used on all serial links including those links created with dial-up analog and ISDN modems.
- ISP often use PPP as the data link protocol over broadband connections.
  - ISPs can use PPP to assign each customer one public IPv4 address.
  - PPP supports CHAP authentication.
- Ethernet links do not natively support PPP.
  - PPP over Ethernet (PPPoE) provides a solution to this problem.

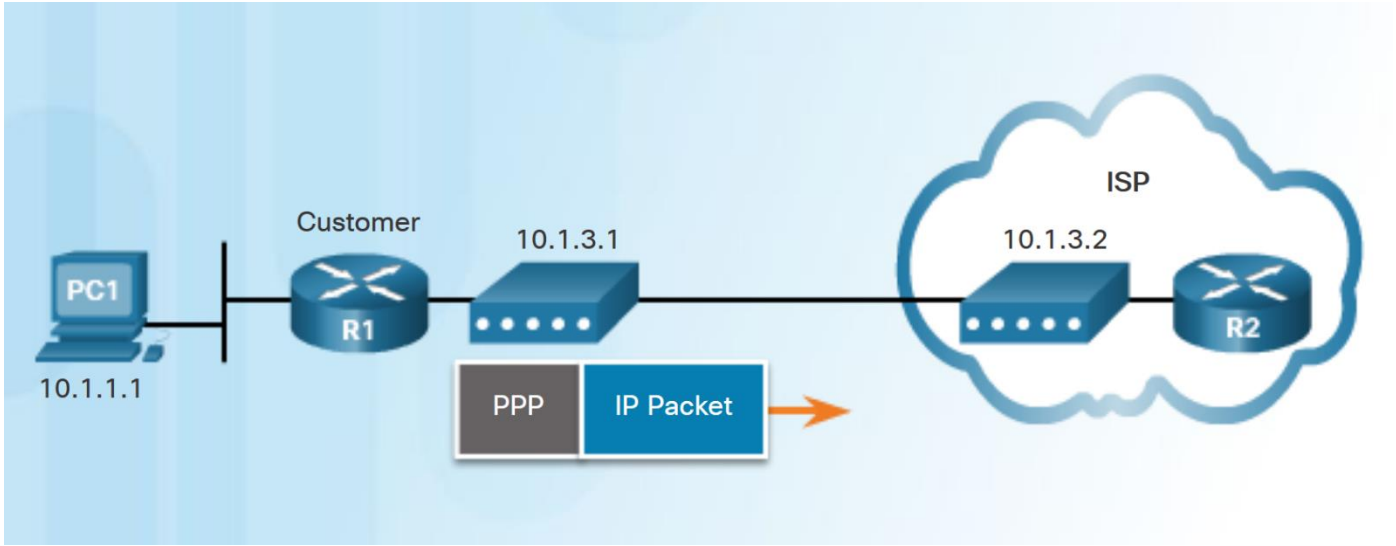
PPP Frames Over An Ethernet Connection



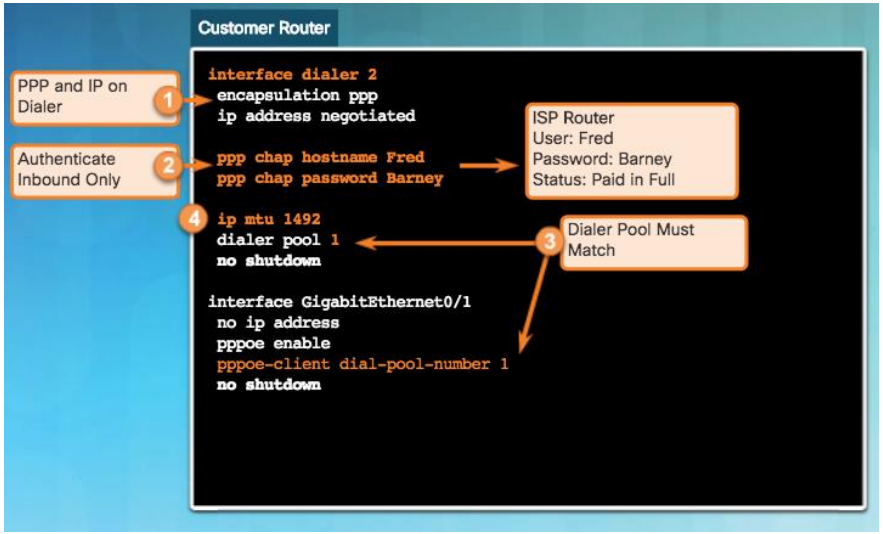
PC1 connects directly to a DSL modem. In a legacy dialup scenario, PC1 reaches the Internet through the TELCO/ISP cloud by using a modem.

PPPoE Concepts

- PPPoE creates a PPP tunnel over an Ethernet connection.
- This allows PPP frames to be sent across the Ethernet cable to the ISP from the customer's router.



PPPoE Configuration



- To create the PPP tunnel a dialer interface is configured.
  - Use **interface dialer** *number* command
- The PPP CHAP is then configured. Use **ppp chap hostname** *name* and **ppp chap password** *password.*
- The physical Ethernet interface connected to the DSL modem is enabled with the command **pppoe enable** interface configuration command.
- Dialer interface is linked to the Ethernet interface with the **dialer pool** and **pppoe-client** interface configuration commands.
- The MTU should be set to 1492 to accommodate PPPoE headers.

PPPoE Verification

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         unassigned      YES unset  up                    up
Serial0/0/0                unassigned      YES unset  administratively down down
Serial0/0/1                unassigned      YES unset  administratively down down
Dialer2                    10.1.3.1        YES IPCP   up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Virtual-Access2            unassigned      YES unset  up                    up
R1#
```

```
R1# show interface dialer 2
Dialer2 is up, line protocol is up (spoofing)
  Hardware is Unknown
  Internet address is 10.1.3.1/32
  MTU 1492 bytes, BW 56 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Closed, loopback not set
  Keepalive set (10 sec)
  DTR is pulsed for 1 seconds on reset

<output omitted>
```

- Use the following commands to verify PPPoE:
  - **show ip interface brief -** verify the IPv4 address automatically assigned.
  - **show interface dialer -** verifies the MTU and PPP encapsulation.
  - **show ip route**
  - **show pppoe session -** displays information about currently active PPPoE sessions.

```
R1# show pppoe session
     1 client session

Uniq ID  PPPoE  RemMAC          Port                 VT  VA         State
         SID    LocMAC                                   VA-st      Type
    N/A    1    30f7.0da3.1641  Gi0/1                Di2 Vi2        UP
                30f7.0da3.0da1                           UP
R1#
```

PPPoE Troubleshooting

- The following are possible causes of problems with PPPoE:
  - Failure in the PPP negotiation process
  - Failure in the PPP authentication process
  - Failure to adjust the TCP maximum segment size

PPPoE Negotiation

- Use the debug ppp negotiation command to verify PPP negotiation.
- Four possible points of failure in PPP negotiation:
  - No response from the remote device.
  - Link Control Protocol (LCP) not open.
  - Authentication failure.
  - IP Control Protocol (IPCP) failure.

```
R1# debug ppp negotiation
*Sep 20 19:05:05.239: Vi2 PPP: Phase is AUTHENTICATING, by the peer
*Sep 20 19:05:05.239: Vi2 LCP: State is Open
 <output omitted>
*Sep 20 19:05:05.247: Vi2 CHAP: Using hostname from interface CHAP
*Sep 20 19:05:05.247: Vi2 CHAP: Using password from interface CHAP
*Sep 20 19:05:05.247: Vi2 CHAP: O RESPONSE id 1 len 26 from "Fred"
*Sep 20 19:05:05.255: Vi2 CHAP: I SUCCESS id 1 len 4

*Sep 20 19:05:05.259: Vi2 IPCP:    Address 10.1.3.2 (0x03060A010302)
*Sep 20 19:05:05.259: Vi2 IPCP: Event[Receive ConfAck] State[ACKsent to Open]
*Sep 20 19:05:05.271: Vi2 IPCP: State is Open
*Sep 20 19:05:05.271: Di2 IPCP: Install negotiated IP interface address 10.1.3.2
*Sep 20 19:05:05.271: Di2 Added to neighbor route AVL tree: topoid 0, address 10.1.3.2
*Sep 20 19:05:05.271: Di2 IPCP: Install route to 10.1.3.2
R1# undebug all
```

PPPoE Authentication

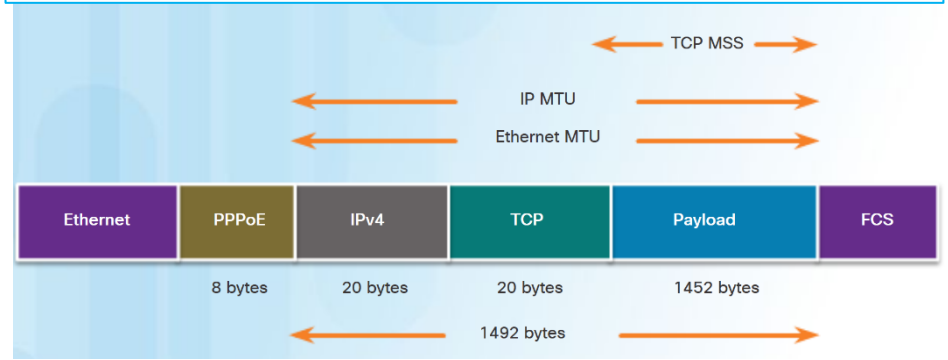
- Verify that the CHAP username and password are correct using **debug ppp negotiation** command.

```
R1# debug ppp negotiation
*Sep 20 19:05:05.239: Vi2 PPP: Phase is AUTHENTICATING, by the peer
*Sep 20 19:05:05.239: Vi2 LCP: State is Open
 <output omitted>
*Sep 20 19:05:05.247: Vi2 CHAP: Using hostname from interface CHAP
*Sep 20 19:05:05.247: Vi2 CHAP: Using password from interface CHAP
*Sep 20 19:05:05.247: Vi2 CHAP: O RESPONSE id 1 len 26 from "Fred"
*Sep 20 19:05:05.255: Vi2 CHAP: I SUCCESS id 1 len 4
 <output omitted>
*Sep 20 19:05:05.259: Vi2 IPCP:    Address 10.1.3.2 (0x03060A010302)
*Sep 20 19:05:05.259: Vi2 IPCP: Event[Receive ConfAck] State[ACKsent to Open]
*Sep 20 19:05:05.271: Vi2 IPCP: State is Open
*Sep 20 19:05:05.271: Di2 IPCP: Install negotiated IP interface address 10.1.3.2
*Sep 20 19:05:05.271: Di2 Added to neighbor route AVL tree: topoid 0, address 10.1.3.2
*Sep 20 19:05:05.271: Di2 IPCP: Install route to 10.1.3.2
R1# undebug all
```

PPPoE MTU Size

- PPPoE supports an MTU of only 1492 bytes in order to accommodate the additional 8-byte PPPoE header.
- Use **show running-config** command to verify PPPoE MTU.
- The **ip tcp adjust-mss** *max-segment-size* interface command prevents TCP sessions from being dropped by adjusting the MSS value during the TCP 3-way handshake.

Adjusted maximum segment size with PPPoE Header




```
R1# show running-config | section interface Dialer2
interface Dialer2
 mtu 1492
 ip address negotiated
 encapsulation ppp

 <output omitted>
```

```
R1(config)# interface g0/0
R1(config-if)# ip tcp adjust-mss 1452
```

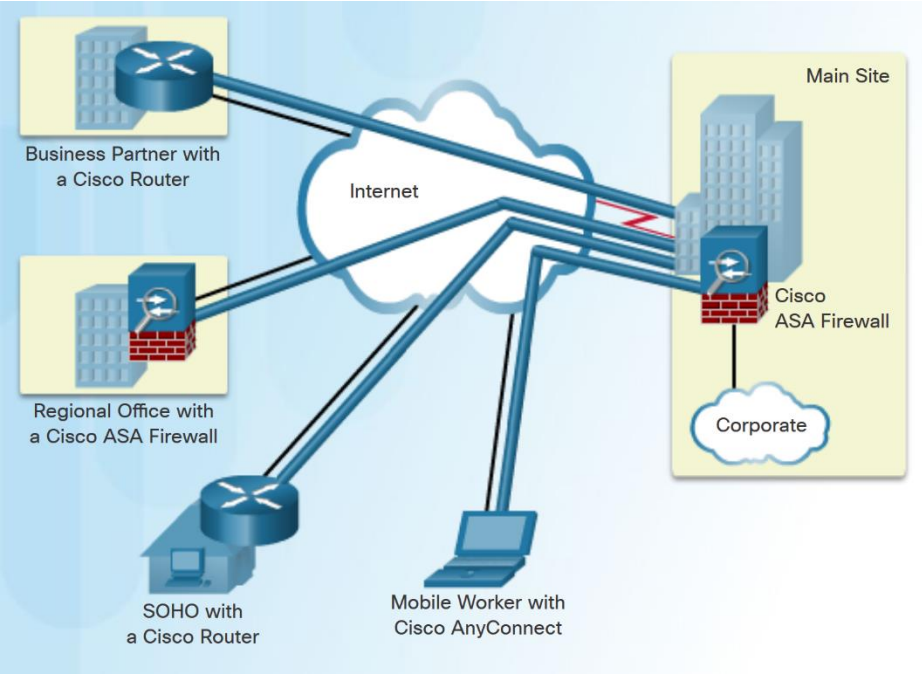
Virtual Private Networks - VPN

Introduction

- Security is a concern when using the public Internet to conduct business.
- Virtual Private Networks (VPN) are used to ensure the security of data across the Internet.
- A VPN is used to create a private tunnel over a public network.
- Data can be secured by using encryption in this tunnel through the Internet and by using authentication to protect data from unauthorized access.
- This section explains the concepts and processes related to VPN, as well as the benefits of VPN implementations, and the underlying protocols required to configure VPN.

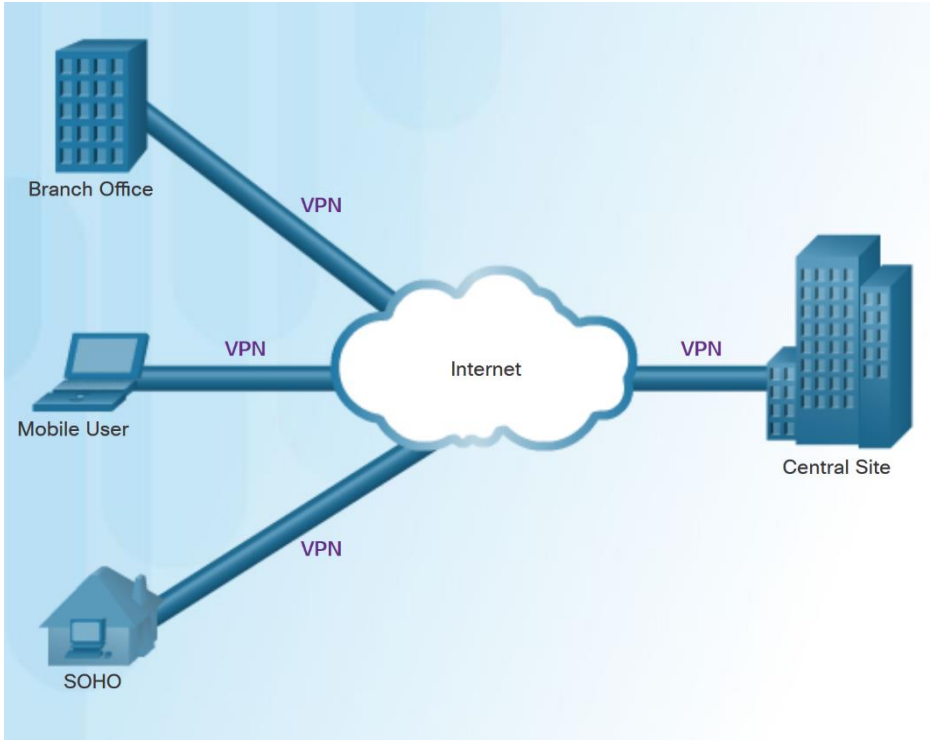
Introducing VPN

- A VPN is a private network created via tunneling over a public network, usually the Internet.
- A secure implementation of VPN with encryption, such as IPsec VPN, is what is usually meant by virtual private networking.
- To implement VPN, a VPN gateway is necessary - could be a router, a firewall, or a Cisco Adaptive Security Appliance (ASA).



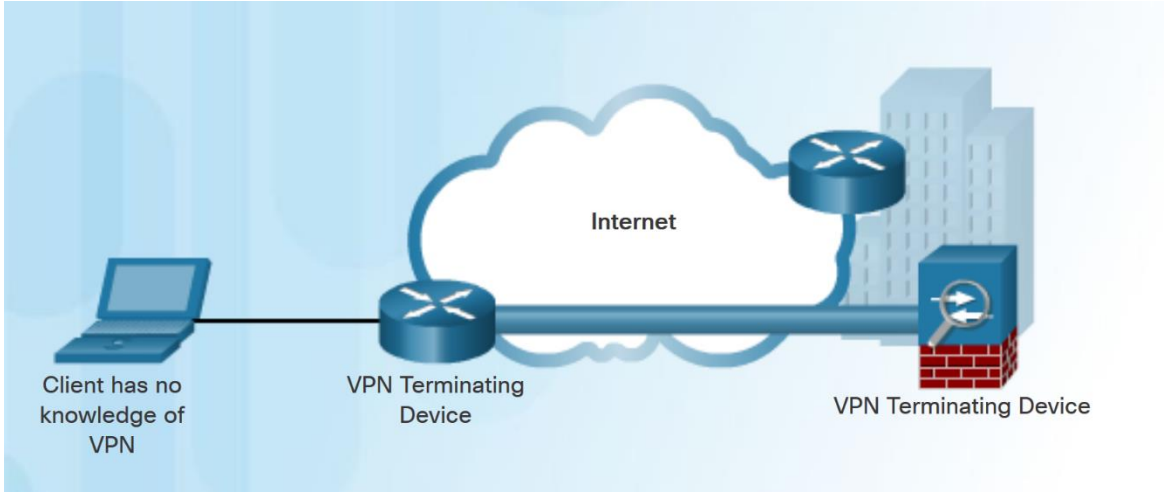
Benefits of VPN

- The benefits of a VPN include the following:
  - **Cost savings** - VPN enable organizations to use cost-effective, high-bandwidth technologies, such as DSL to connect remote offices and remote users to the main site.
  - **Scalability** - Organizations are able to add large amounts of capacity without adding significant infrastructure.
  - **Compatibility with broadband technology** - Allow mobile workers and telecommuters to take advantage of high-speed, broadband connectivity.
  - **Security** - VPN can use advanced encryption and authentication protocols.



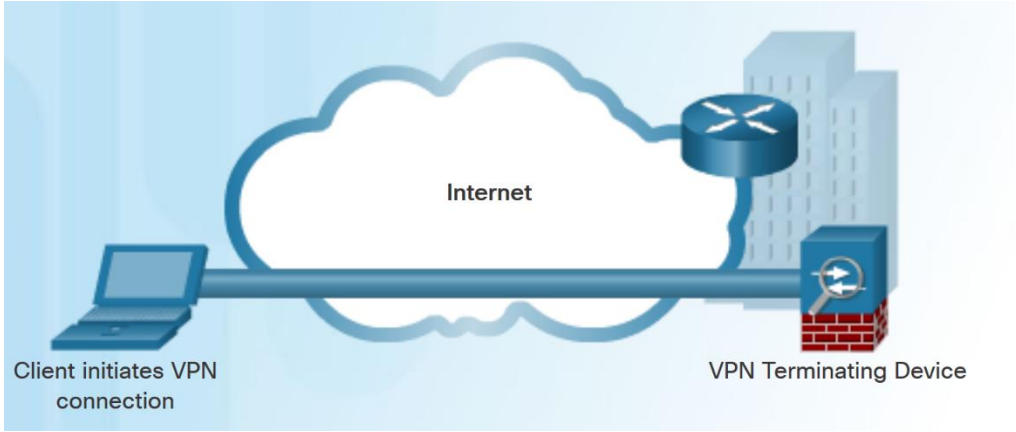
Site-to-Site VPN

- Site-to-site VPN connect entire networks to each other, for example, connecting a branch office network to a company headquarters network.
- In a site-to-site VPN, end hosts send and receive normal TCP/IP traffic through a VPN “gateway”.
- The VPN gateway is responsible for encapsulating and encrypting outbound traffic.



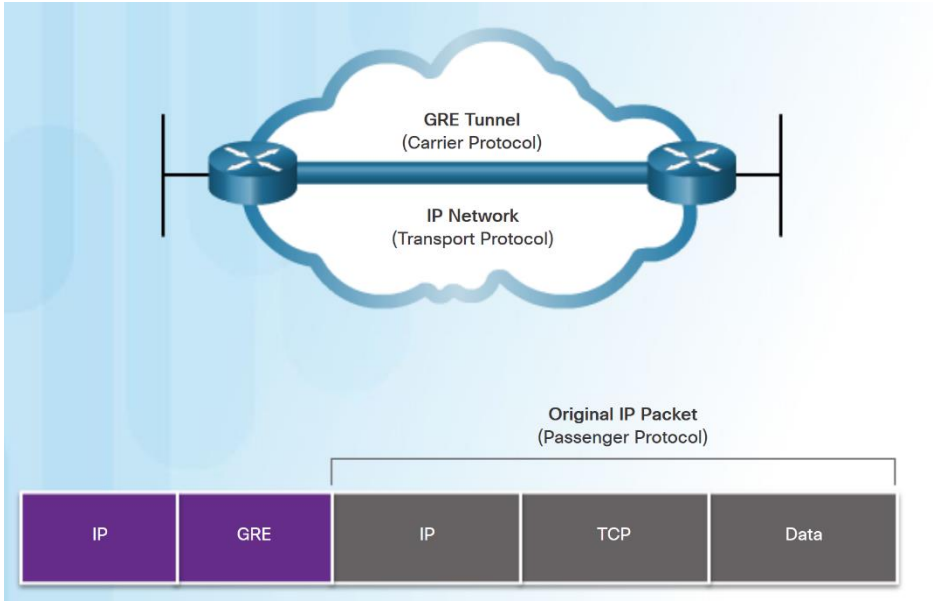
Remote Access VPN

- A remote-access VPN supports the needs of telecommuters, mobile users, and extranet traffic.
- Allows for dynamically changing information, and can be enabled and disabled.
- Used to connect individual hosts that must access their company network securely over the Internet.
- VPN client software may need to be installed on the mobile user's end device.



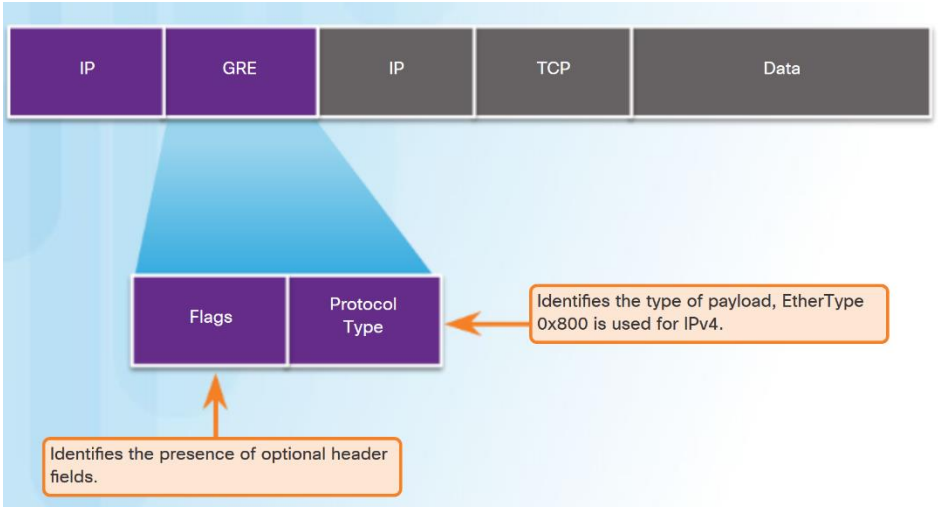
Generic Routing Encapsulation - GRE

GRE Introduction



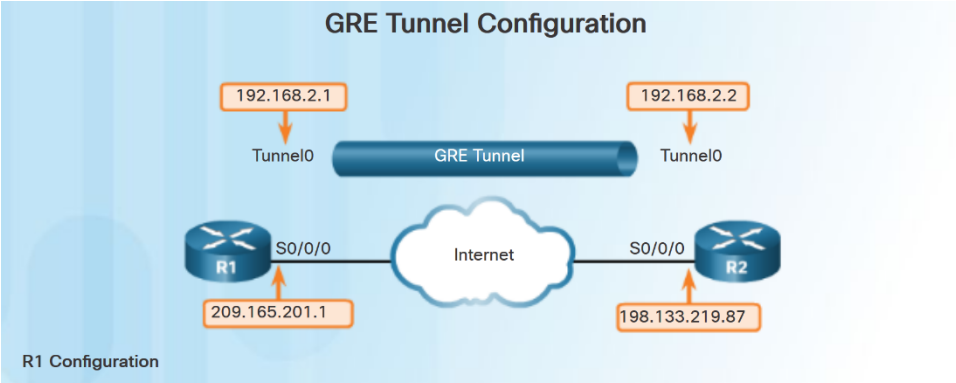
- Generic Routing Encapsulation (GRE) is a non-secure, site-to-site VPN tunneling protocol.
- Developed by Cisco.
- GRE manages the transportation of multiprotocol and IP multicast traffic between two or more sites
- A tunnel interface supports a header for each of the following:
  - An encapsulated protocol - or passenger protocol, such as IPv4, IPv6.
  - An encapsulation protocol - or carrier protocol, such as GRE.
  - A transport delivery protocol, such as IP.

GRE Characteristics



- GRE is defined as an IETF standard (RFC 2784).
- In the outer IP header, 47 is used in the protocol field.
- GRE encapsulation uses a protocol type field in the GRE header to support the encapsulation of any OSI Layer 3 protocol.
- GRE is stateless.
- GRE does not include any strong security mechanisms.
- GRE header, together with the tunneling IP header, creates at least 24 bytes of additional overhead for tunneled packets.

Configure GRE



R1 Configuration

```
R1(config)# interface Tunnel0
R1(config-if)# tunnel mode gre ip
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# tunnel source 209.165.201.1
R1(config-if)# tunnel destination 198.133.219.87
R1(config-if)# router ospf 1
R1(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

```
R2(config)# interface Tunnel0
R2(config-if)# tunnel mode gre ip
R2(config-if)# ip address 192.168.2.2 255.255.255.0
R2(config-if)# tunnel source 198.133.219.87
R2(config-if)# tunnel destination 209.165.201.1
R2(config-if)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
```

- Five steps to configuring a GRE tunnel:
  - Step 1. Create a tunnel interface using the **interface tunnel** *number* command.
  - Step 2. Configure an IP address for the tunnel interface. (Usually a private address)
  - Step3. Specify the tunnel source IP address.
  - Step 4. Specify the tunnel destination IP address.
  - Step 5. (Optional) Specify GRE tunnel mode as the tunnel interface mode.

Note: The tunnel source and tunnel destination commands reference the IP addresses of the preconfigured physical interfaces.

Verify GRE

- Use the **show ip interface brief** command to verify that the tunnel interface is up.
- Use the **show interface tunnel** command to verify the state of the tunnel.
- Use the **show ip ospf neighbor** command to verify that an OSPF adjacency has been established over the tunnel interface.

```
R1# show ip interface brief | include Tunnel

Tunnel0            192.168.2.1     YES manual up      up
```

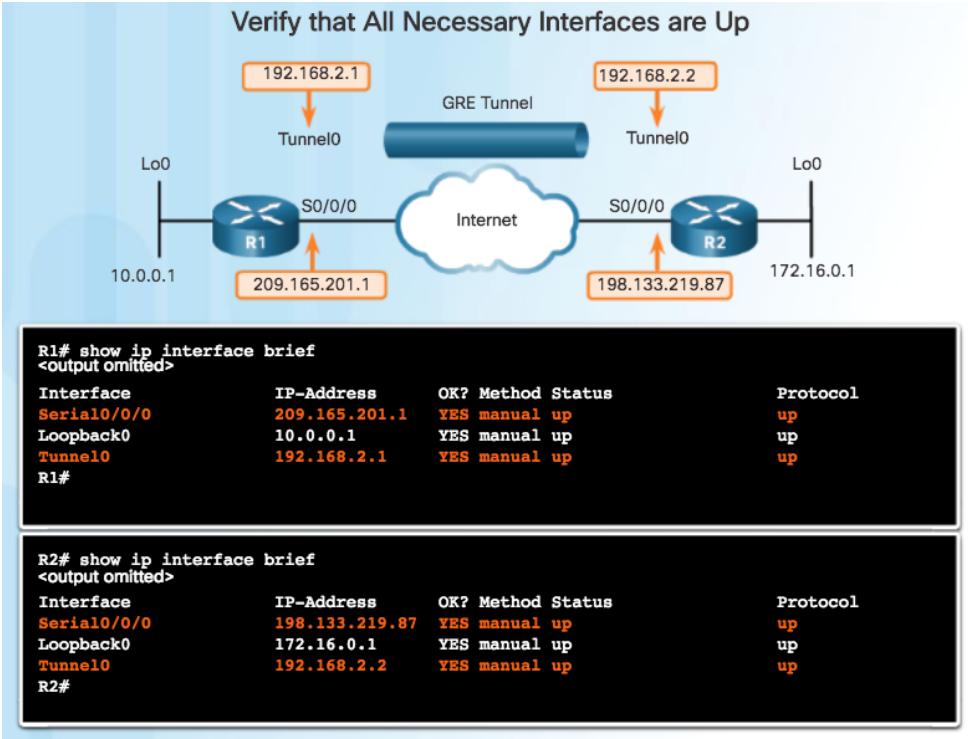
```
R1# show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.201.1, destination 209.165.201.2
  Tunnel protocol/transport GRE/IP
<output omitted>
```

```
R1# show ip ospf neighbor

Neighbor ID     Pri State        Dead Time  Address      Interface
209.165.201.2   0   FULL/  -     00:00:37   192.168.2.2  Tunnel0
```

Troubleshoot GRE

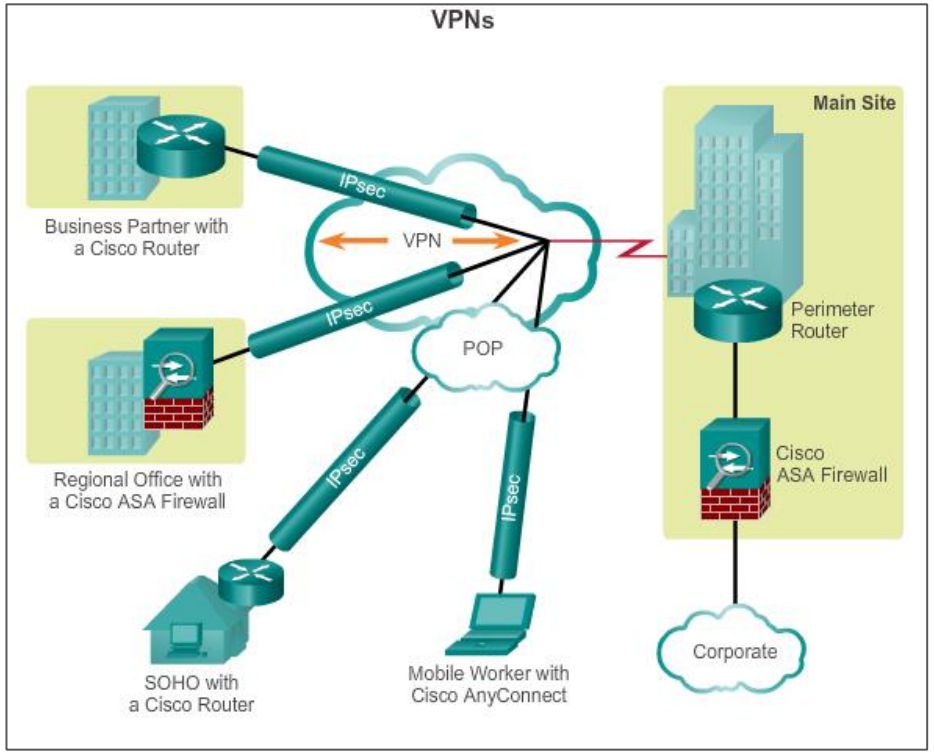
- Issues with GRE are usually due to one or more of the following:
  - The tunnel interface IP addresses are not on the same network or the subnet masks do not match. Use the **show ip interface brief** command.
  - The interfaces for the tunnel source and/or destination are not configured with the correct IP address or are down. Use the **show ip interface brief** command.
  - Static or dynamic routing is not properly configured. Use **show ip route** or **show ip ospf neighbor.**



Introducing IPSec

IPsec VPN

- Information from a private network is securely transported over a public network.
- Forms a virtual network instead of using a dedicated Layer 2 connection.
- To remain private, the traffic is encrypted to keep the data confidential.



IPsec Functions

- Defines how a VPN can be configured in a secure manner using IP.
- Framework of open standards that spells out the rules for secure communications.
- Not bound to any specific encryption, authentication, security algorithms, or keying technology.
- Relies on existing algorithms to implement secure communications.
- Works at the network layer, protecting and authenticating IP packets between participating IPsec devices.
- Secures a path between a pair of gateways, a pair of hosts, or a gateway and host.
- All implementations of IPsec have a plaintext Layer 3 header, so there are no issues with routing.
- Functions over all Layer 2 protocols, such as Ethernet, ATM, or Frame Relay.

IPsec Characteristics

- IPsec characteristics can be summarized as follows:
- IPsec is a framework of open standards that is algorithm-independent.
- IPsec provides data confidentiality, data integrity, and origin authentication.
- IPsec acts at the network layer, protecting and authenticating IP packets.

IPsec Security Services

- **Confidentiality (encryption)** – encrypt the data before transmitting across the network
- **Data integrity** – verify that data has not been changed while in transit, if tampering is detected, the packet is dropped
- **Authentication** – verify the identity of the source of the data that is sent, ensures that the connection is made with the desired communication partner, IPsec uses Internet Key Exchange (IKE) to authenticate users and devices that can carry out communication independently.
- **Anti-Replay Protection** – detect and reject replayed packets and helps prevent spoofing

CIA: confidentiality, integrity, and authentication

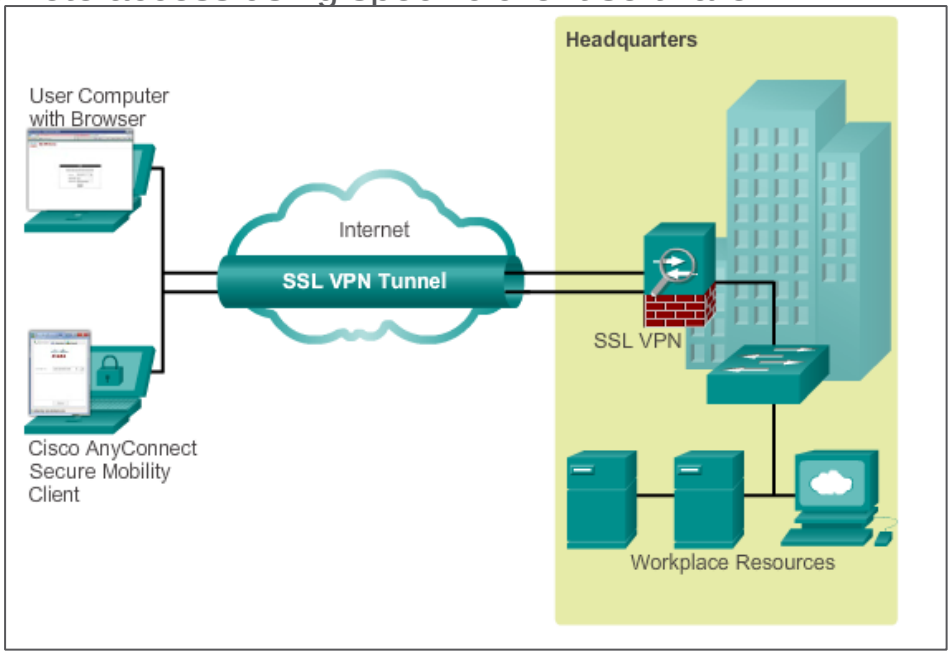
Remote Access

Types of Remote Access VPN

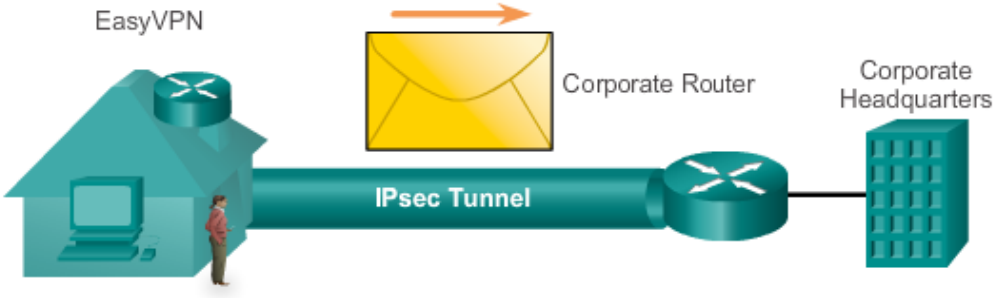
- There are two primary methods for deploying remote access VPN:
  - Secure Sockets Layer (SSL)
  - IP Security (IPsec)
- Type of VPN method based on the access requirements of the users and the organization's IT processes.
- Both types offer access to virtually any network application or resource.

SSL VPN

- Provides remote access by using a web browser and the web browser's native SSL encryption.
- Can provide remote access using specific client software



IPsec Remote Access



Cisco Easy VPN

- Negotiates tunnel parameters
- Establishes tunnels according to set parameters
- Authenticates users by usernames, group names, and passwords
- Manages security keys for encryption and decryption
- Authenticates, encrypts, and decrypts data through the tunnel

Chapter Summary

Summary

Branch Connections

- Several options to remote access broadband connection are available for small to medium-sized businesses.
  - An issue is selecting the appropriate broadband connection for a given network requirement.
- PPPoE is the main solution to connect on a client router to the company infrastructure over a third-party network, such as the Internet
- VPNs are used to create a secure end-to-end private network connection over a third-party network.
  - A site-to-site VPN uses a VPN gateway device at the edge of both sites.
    - The end hosts are unaware of the VPN and have no additional supporting software.
    - IPSec is the main used technology
  - A remote access VPN requires software to be installed on the individual host device that accesses the network from a remote location.
    - The two types of remote access VPNs are SSL and IPsec.
    - SSL technology can provide remote access using a client's web browser and the browser's native SSL encryption.

Summary

Branch Connections

- GRE is a basic, non-secure site-to-site VPN tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, thus allowing an organization to deliver other protocols through an IP-based WAN.
  - Today, it is primarily used to deliver IP multicast traffic or IPv6 traffic over an IPv4 unicast-only connection.

New Terms and Commands

- PPP over Ethernet (PPPoE)
- Internet Protocol Security (IPsec)
- Border Gateway Protocol (BGP)
- radio frequency (RF)
- hybrid fiber-coaxial (HFC)
- Data over Cable Service Interface Specification (DOCSIS)
- Antenna Site
- Transportation Network
- distribution network
- central office (co)
- Amplifier
- Subscriber Drop
- Node
- downstream
- upstream
- Asymmetric DSL (ADSL)
- symmetric DSL (SDSL)
- DSL Transceiver
- DSL micro filter
- Cellular/mobile
- dialer interface
- maximum transmission unit (MTU)
- maximum segment size (MSS)
- VPN gateway
- VPN client software
- Transport protocol
- Secure Sockets Layer (SSL)
- Dynamic Multipoint VPN (DMVPN)
- Next Hop Resolution Protocol (NHRP)


CISCO