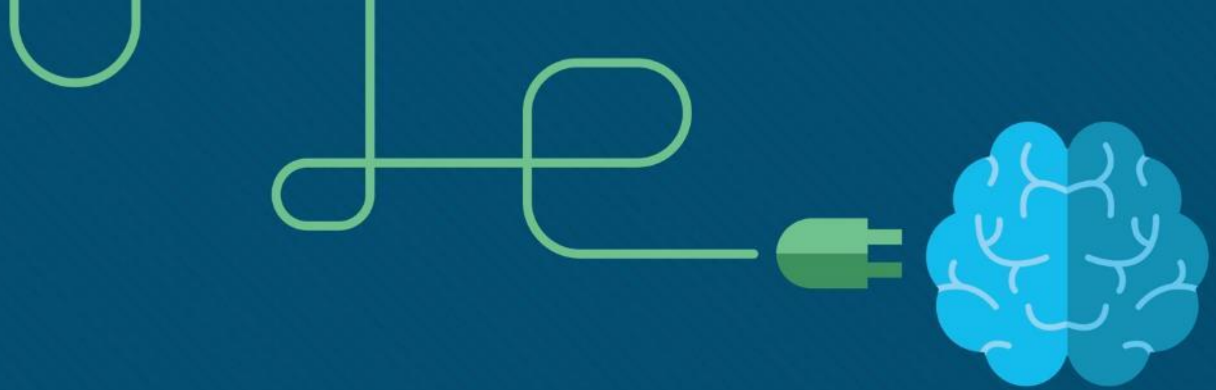


Chapter 3: Branch Connections

CCNA Routing and Switching

Connecting Networks v6.0

Chapter 3 - Sections & Objectives

- 3.1 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.
- 3.2 PPPoE
  - Configure a Cisco router with PPPoE.
    - Explain how PPPoE operates.
    - Implement a basic PPPoE connection on a client router.
- 3.3 VPNs
  - Explain how VPNs secure site-to-site and remote access connectivity.
    - Describe benefits of VPN technology.
    - Describe site-to-site and remote access VPNs.

Chapter 3 - Sections & Objectives (Cont.)

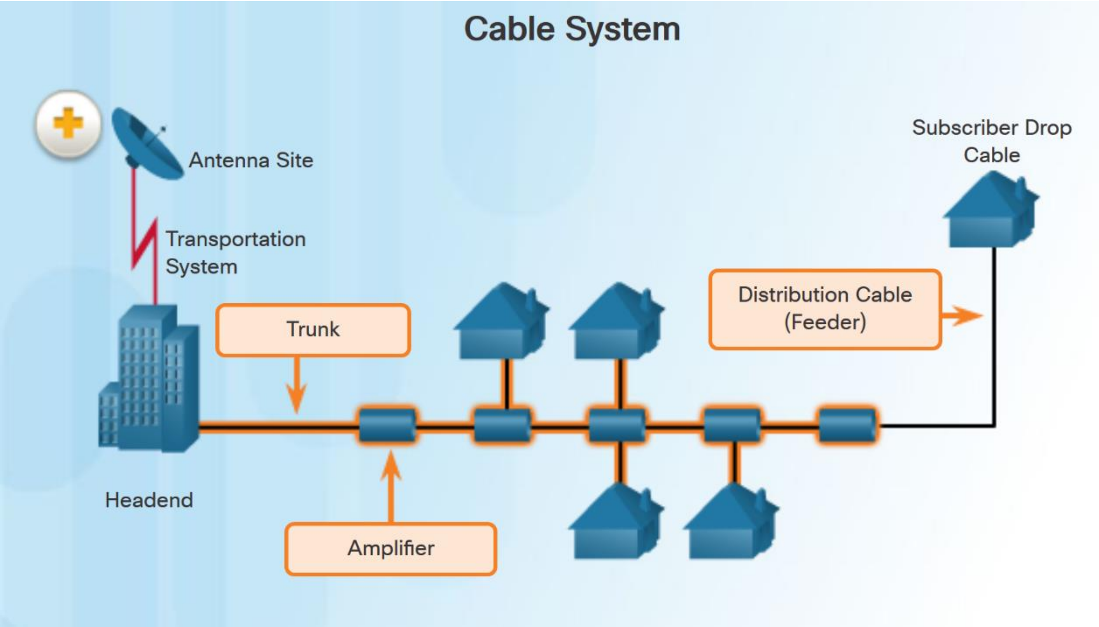
- 3.4 GRE
  - Implement a GRE tunnel.
    - Explain the purpose and benefits of GRE tunnels.
    - Troubleshoot a site-to-site GRE tunnel.
- 3.5 eBGP
  - Implement eBGP in a single-homed remote access network.
    - Describe basic BGP features.
    - Explain BGP design considerations.
    - Configure an eBGP branch connection.

3.1 Remote Access Connections

Broadband Connections

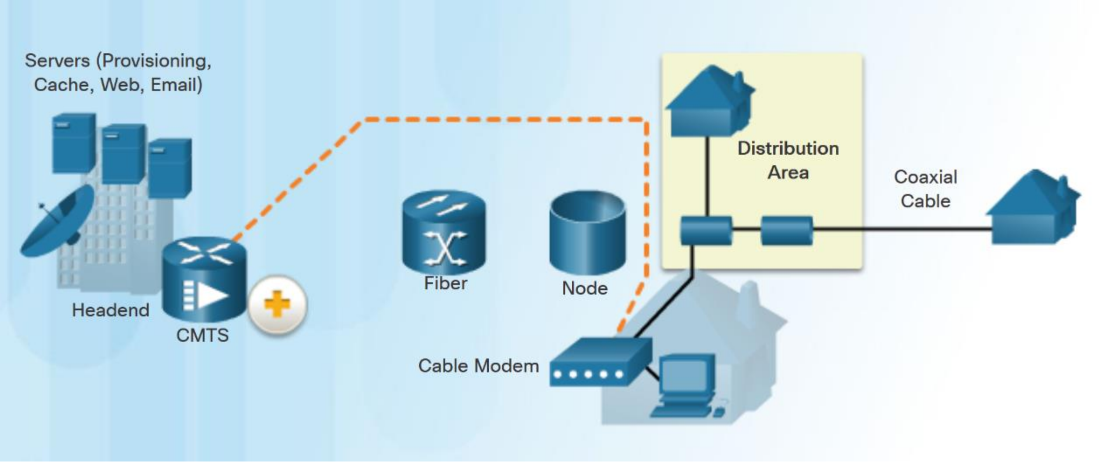
What is a Cable System?

- 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

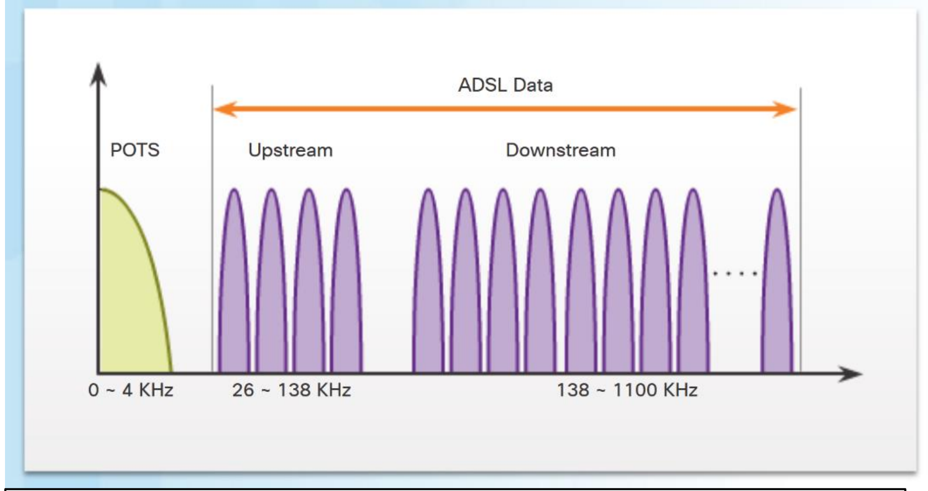
- Two types of equipment are required to send signals upstream and downstream on a cable system:
  - Cable Modem Termination System (CMTS) at the headend of the cable operator. The headend is a router with databases for providing Internet services to cable subscribers.
  - Cable Modem (CM) on the subscriber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



Broadband Connections

What is DSL?

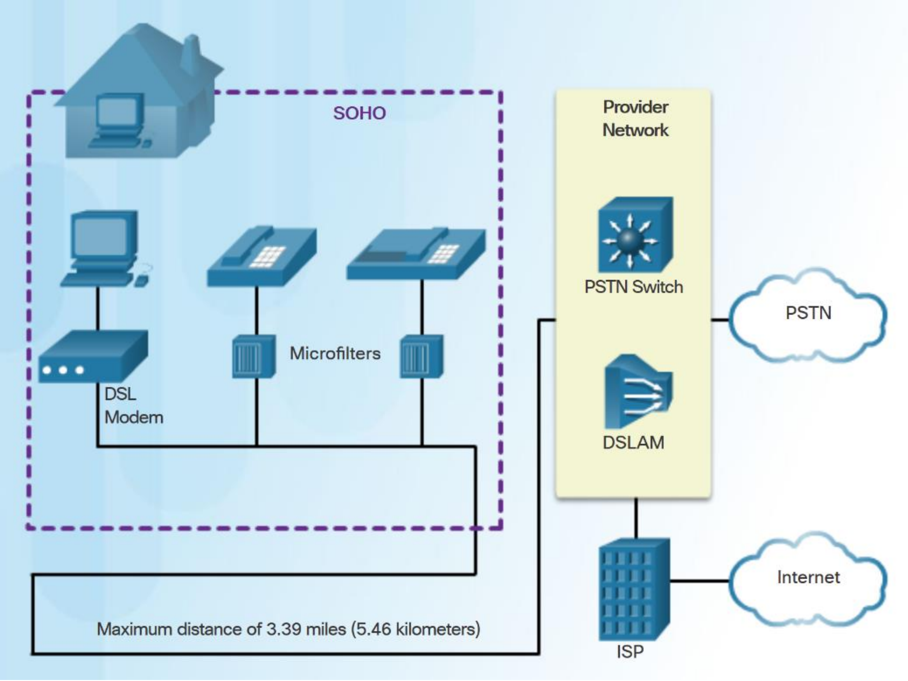
- Digital Subscriber Line (DSL) is a means of providing high-speed connections over installed copper wires.
- Asymmetric DSL (ADSL) provides higher downstream bandwidth to the user than upload bandwidth.
- Symmetric DSL (SDSL) provides the same capacity in both directions.
- For satisfactory ADSL service,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

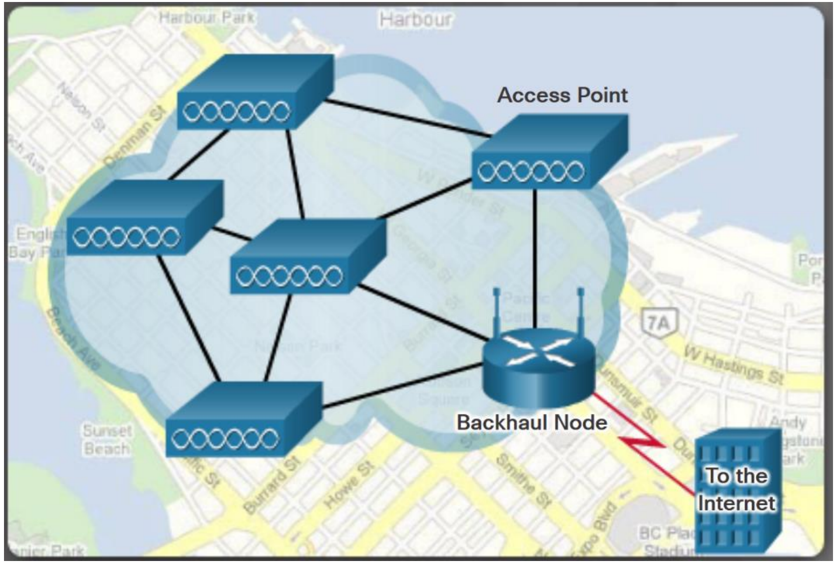
Broadband Connections

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.
  - **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

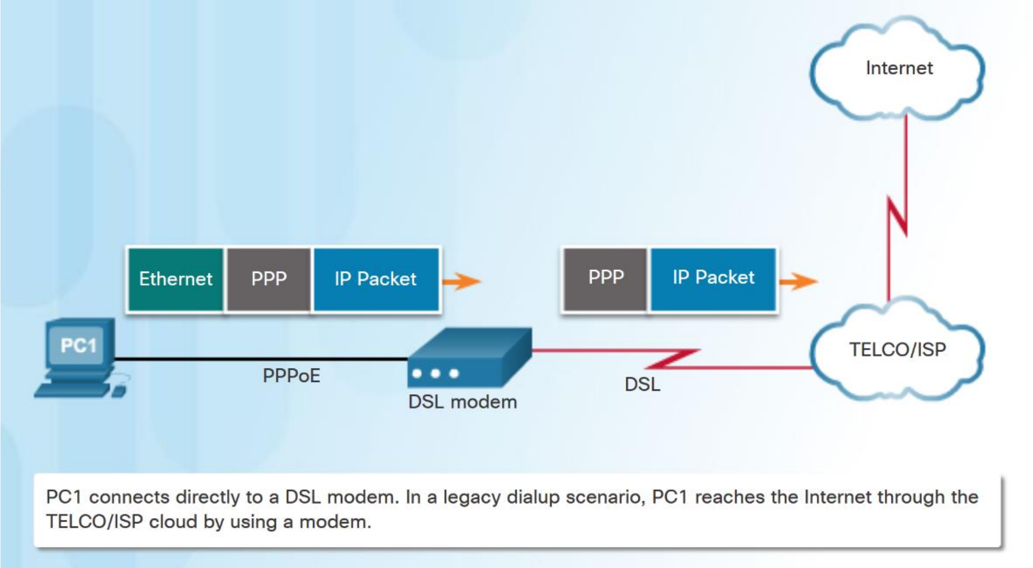
3.2 PPPoE

PPPoE Overview

PPPoE Motivation

- PPP can be used on all serial links including those links created with dial-up analog and ISDN modems.
- ISPs 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

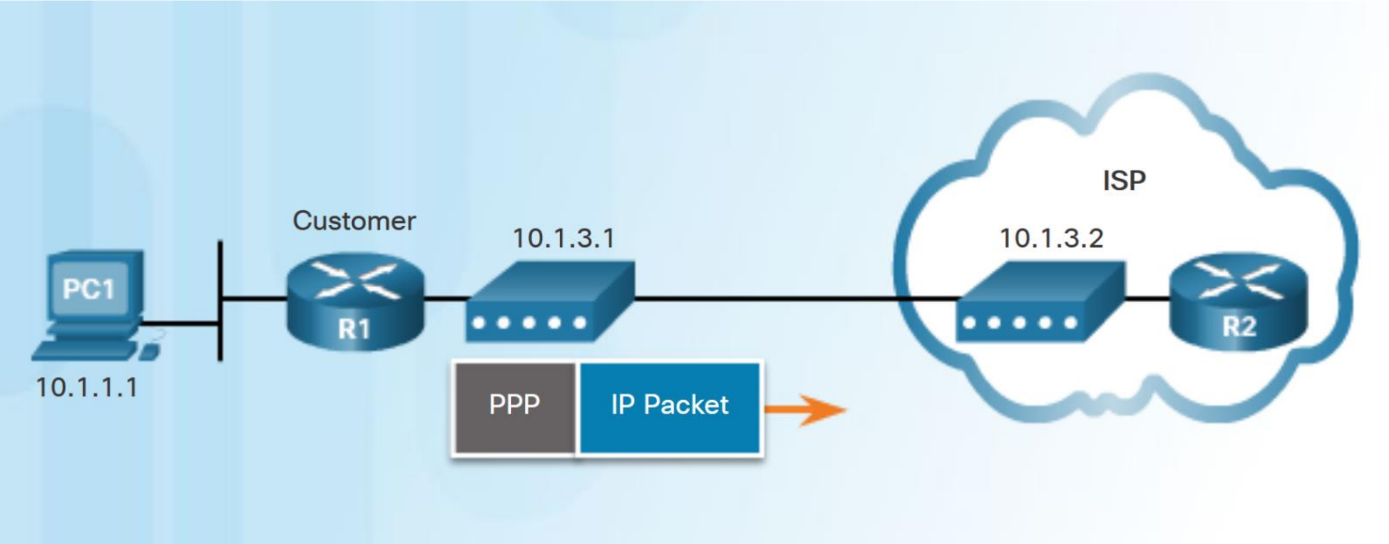


PC1 connects directly to a DSL modem. In a legacy dialup scenario, PC1 reaches the Internet through the TELCO/ISP cloud by using a modem.

PPPoE Overview

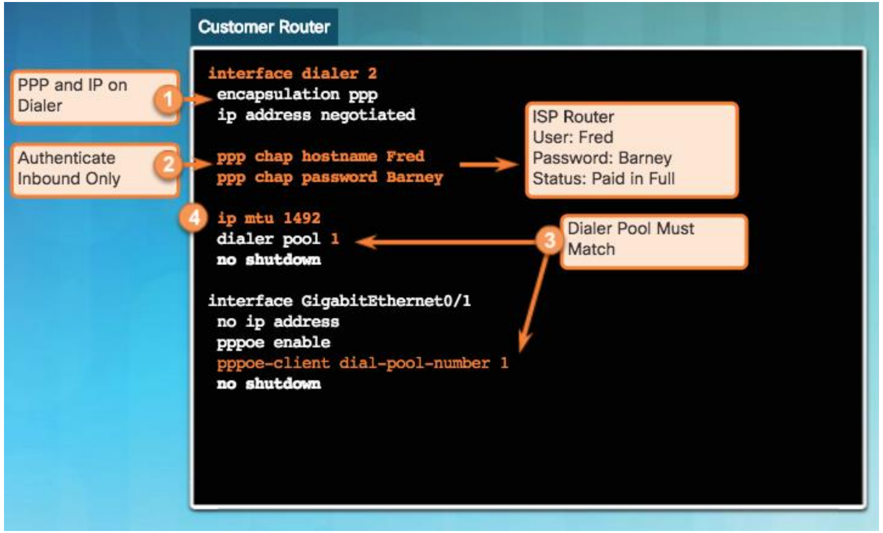
PPPoE Concepts

- 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.



Implement PPPoE

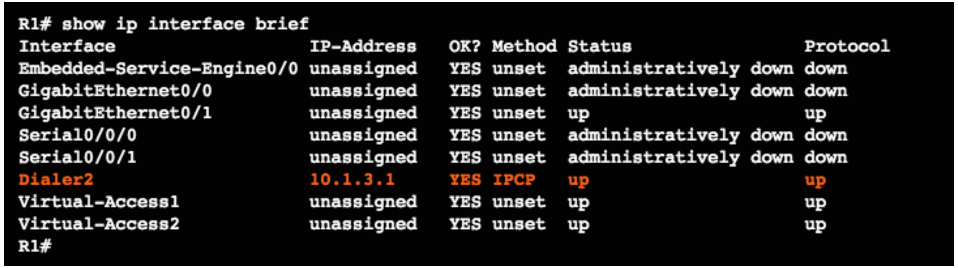
PPPoE Configuration



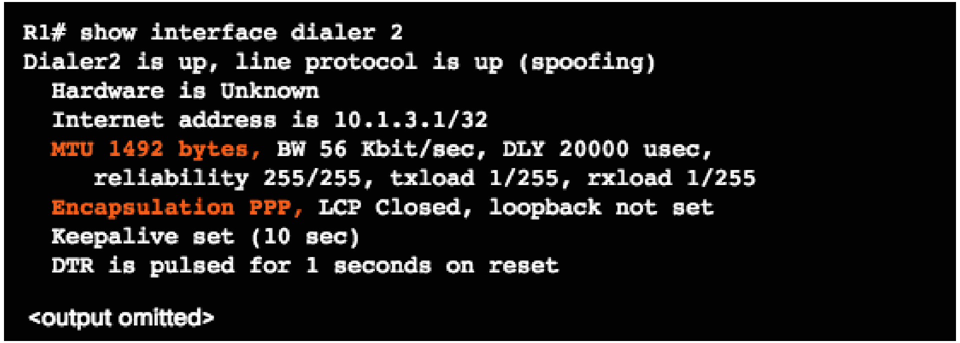
```
interface dialer 2
 encapsulation ppp
 ip address negotiated

 ppp chap hostname Fred
 ppp chap password Barney

 ip mtu 1492
 dialer pool 1
 no shutdown

interface GigabitEthernet0/1
 no ip address
 pppoe enable
 pppoe-client dial-pool-number 1
 no shutdown
```

- 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

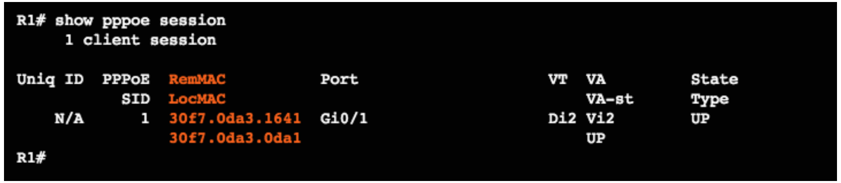


```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0         unassigned      YES unset  administratively down down
GigabitEthernet0/1         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#
```

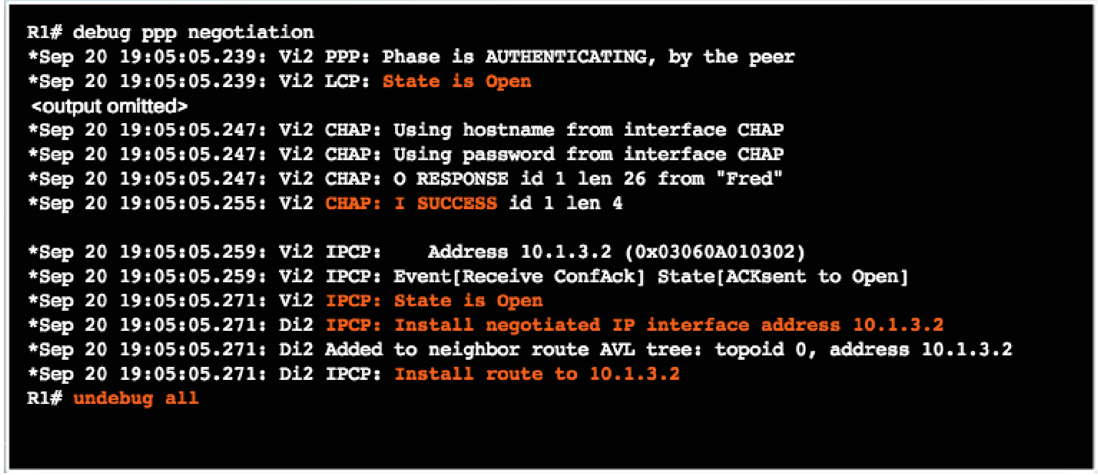
PPPoE Troubleshooting

- 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

Implement PPPoE

PPPoE Negotiation

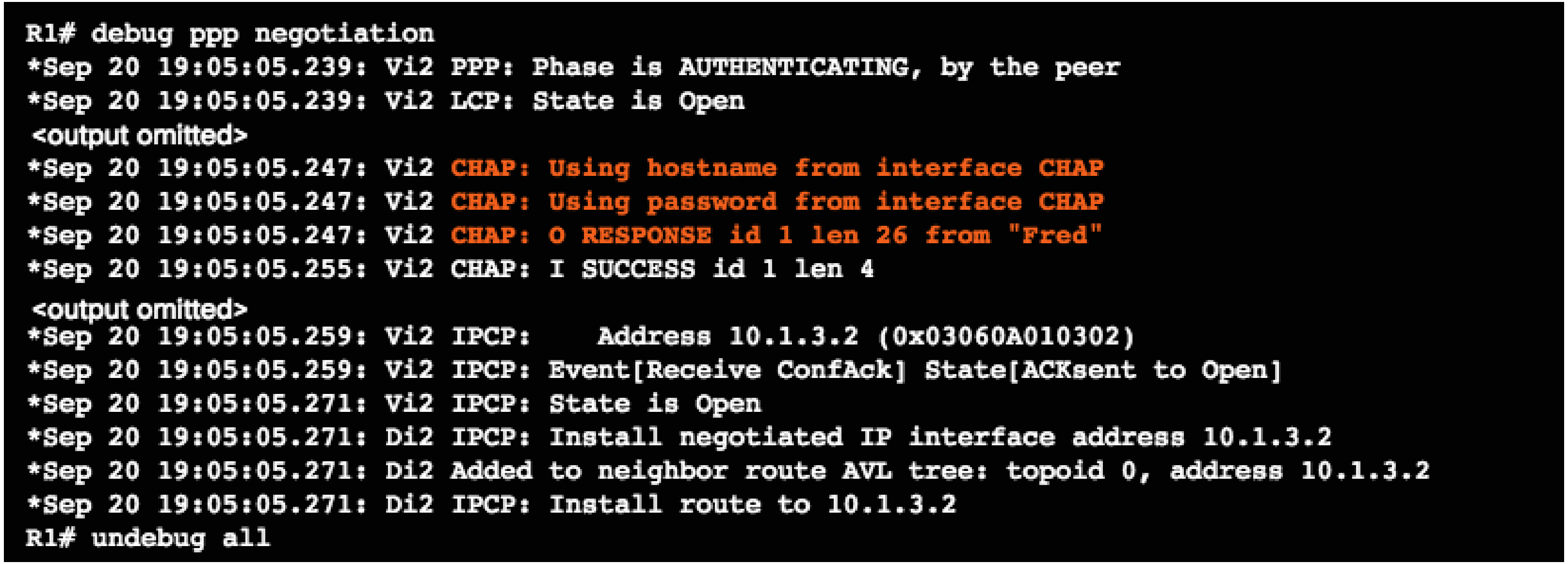
- Use the debug ppp negotiation command to verify PPP negotiation.
- Four possible points of failure in PPP negotiation:
  - No response from the remote device.
  - Link Control Protocol (LCP) not open.
  - Authentication failure.
  - IP Control Protocol (IPCP) failure.



```
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.

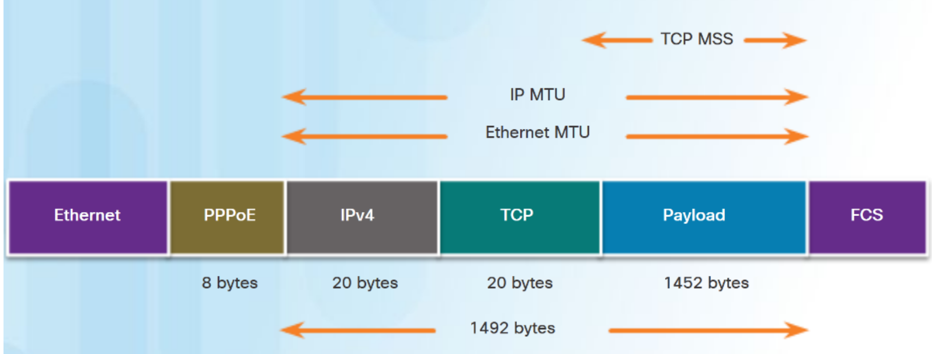


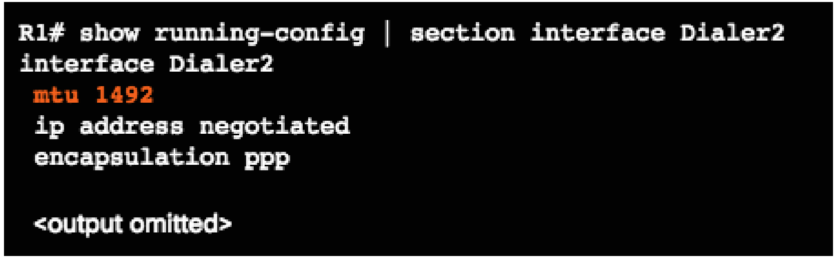
```
R1# debug ppp negotiation
*Sep 20 19:05:05.239: Vi2 PPP: Phase is AUTHENTICATING, by the peer
*Sep 20 19:05:05.239: Vi2 LCP: State is Open
 <output omitted>
*Sep 20 19:05:05.247: Vi2 CHAP: Using hostname from interface CHAP
*Sep 20 19:05:05.247: Vi2 CHAP: Using password from interface CHAP
*Sep 20 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

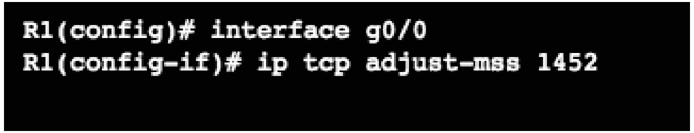
- PPPoE supports an MTU of only 1492 bytes in order to accommodate the additional 8-byte PPPoE header.
- Use **show running-config** command to verify PPPoE MTU.
- The **ip tcp adjust-mss** *max-segment-size* interface command prevents TCP sessions from being dropped by adjusting the MSS value during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

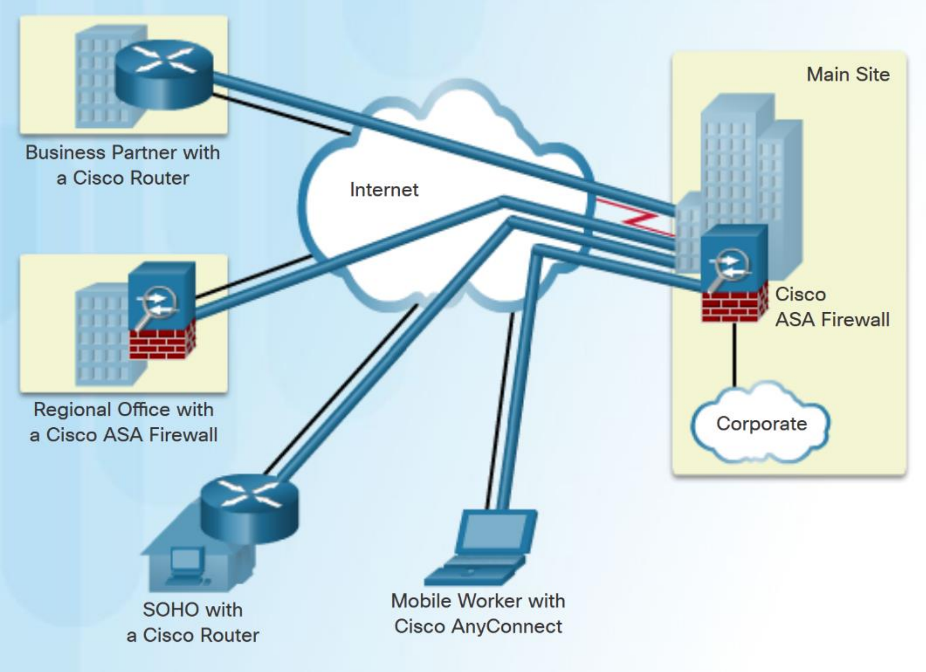
3.3 VPNs

Introducing VPNs

- A VPN is a private network created via tunneling over a public network, usually the Internet.

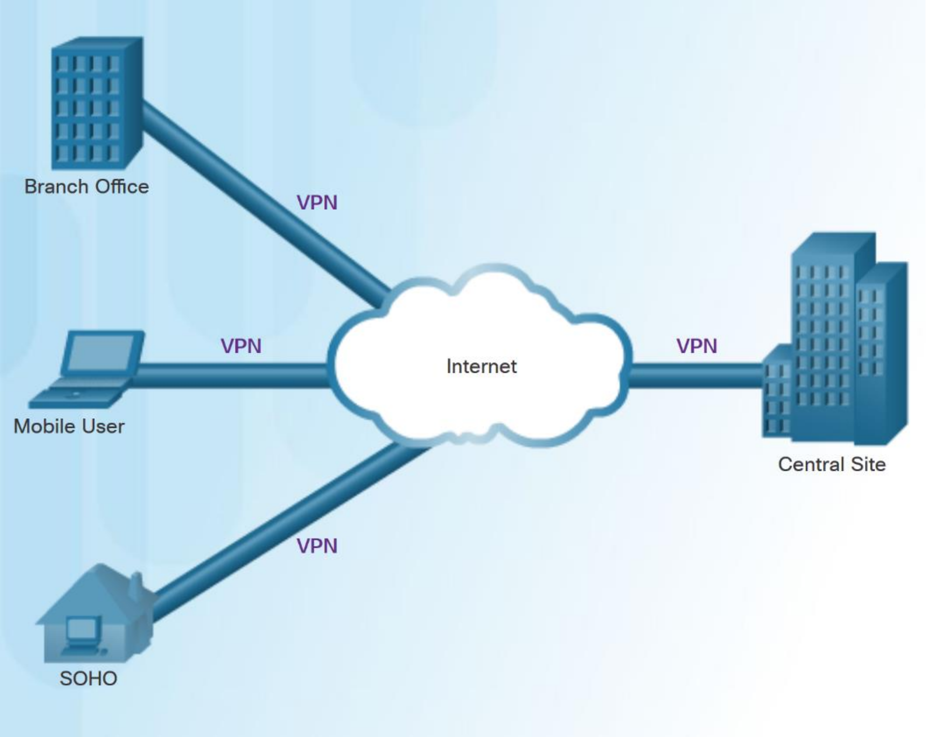
- A secure implementation of VPN with encryption, such as IPsec VPNs, is what is usually meant by virtual private networking.

- To implement VPNs, a VPN gateway is necessary - could be a router, a firewall, or a Cisco Adaptive Security Appliance (ASA).


Business Partner with a Cisco Router
Internet
Main Site
Cisco ASA Firewall
Corporate
Regional Office with a Cisco ASA Firewall
SOHO with a Cisco Router
Mobile Worker with Cisco AnyConnect

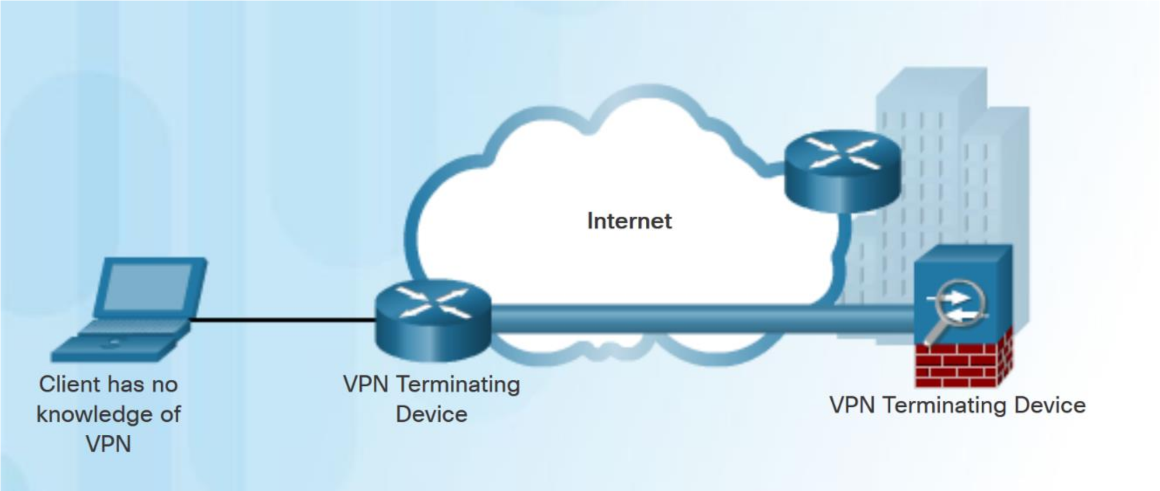
Benefits of VPNs

- The benefits of a VPN include the following:
  - **Cost savings** - VPNs 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** - VPNs can use advanced encryption and authentication protocols.



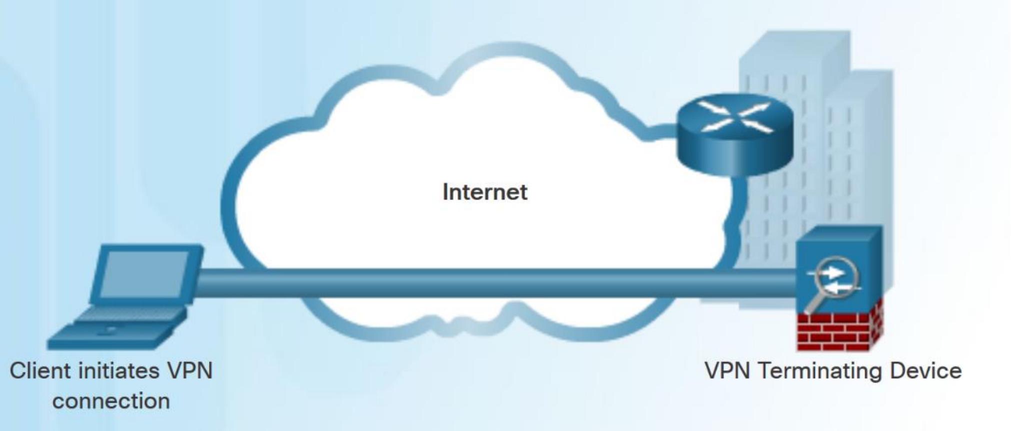
Site-to-Site VPNs

- Site-to-site VPNs 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.



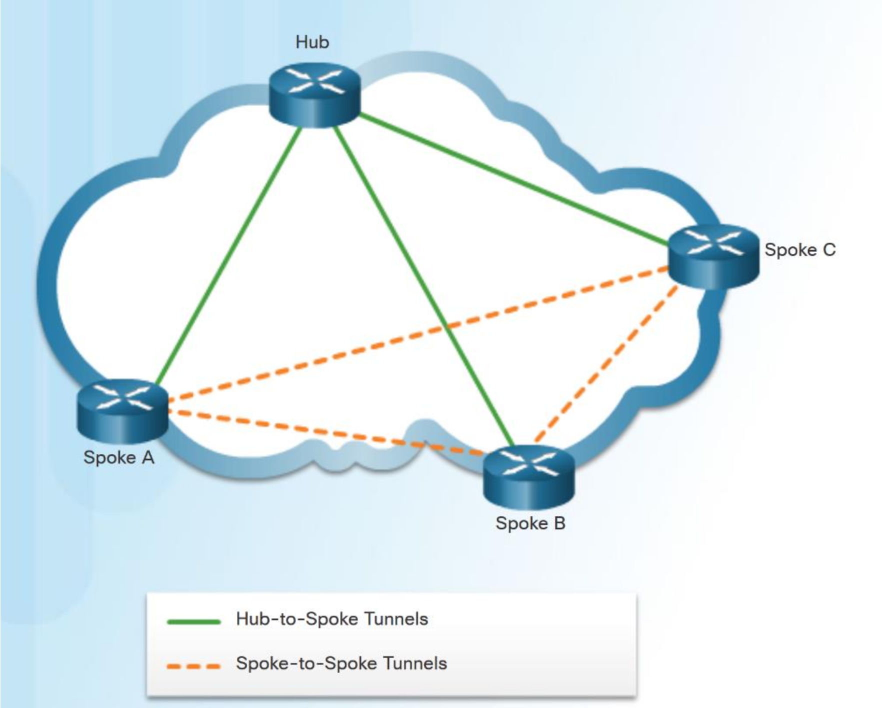
Remote Access VPNs

- 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.



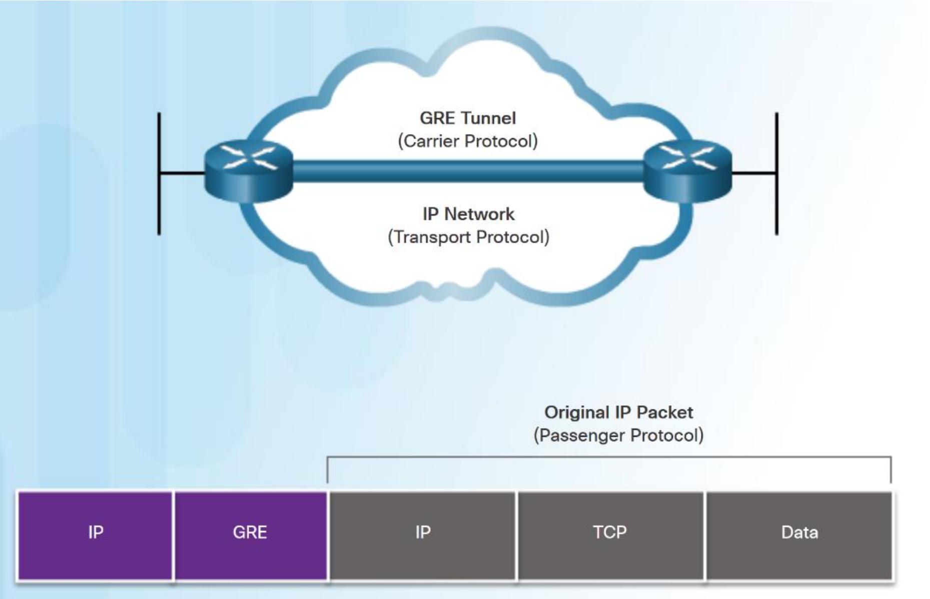
DMVPN

- Dynamic Multipoint VPN (DMVPN) is a Cisco software solution for building multiple VPNs.
- DMVPN is built using the following technologies:
  - **Next Hop Resolution Protocol (NHRP)** - NHRP creates a distributed mapping database of public IP addresses for all tunnel spokes.
  - **Multipoint Generic Routing Encapsulation (mGRE) tunnels** - An mGRE tunnel interface allows a single GRE interface to support multiple IPsec tunnels.
  - **IP Security (IPsec) encryption -** provides secure transport of private information over public networks.



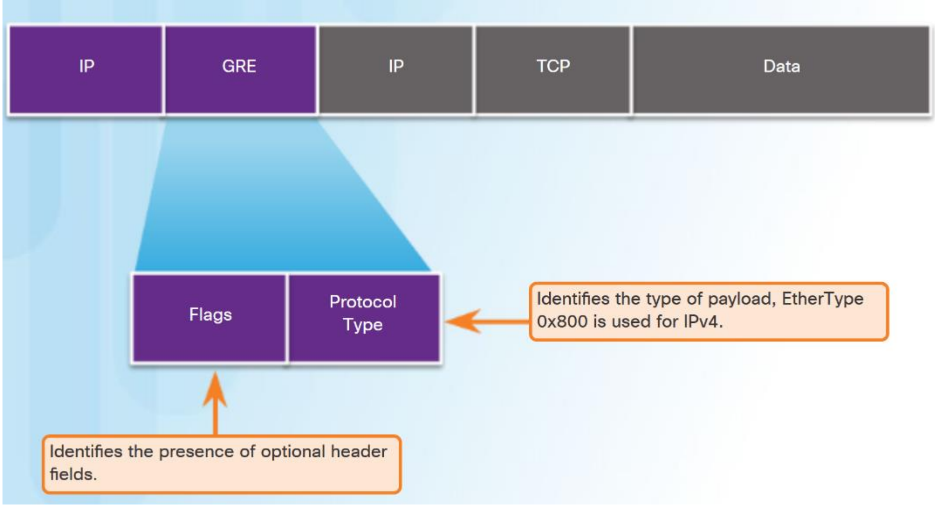
3.4 GRE

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



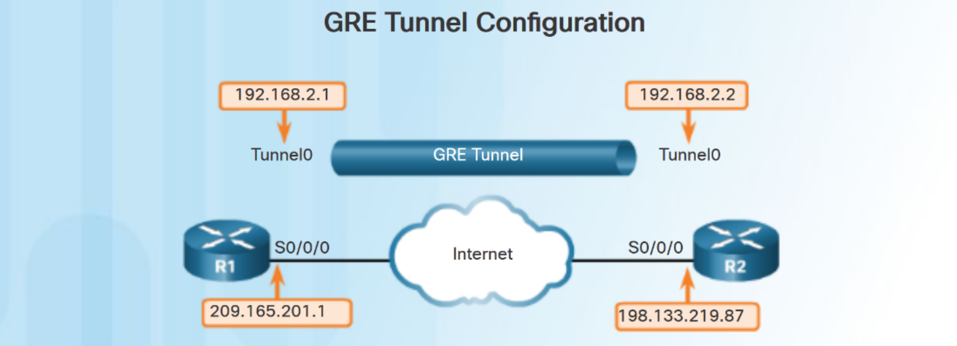
Identifies the type of payload, EtherType 0x800 is used for IPv4.

Identifies the presence of optional header fields.

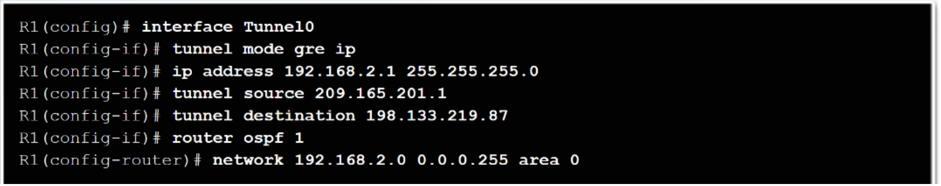
- GRE is defined as an IETF standard (RFC 2784).
- In the outer IP header, 47 is used in the protocol field.
- GRE encapsulation uses a protocol type field in the GRE header to support the encapsulation of any OSI Layer 3 protocol.
- GRE is stateless.
- GRE does not include any strong security mechanisms.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

Implement GRE

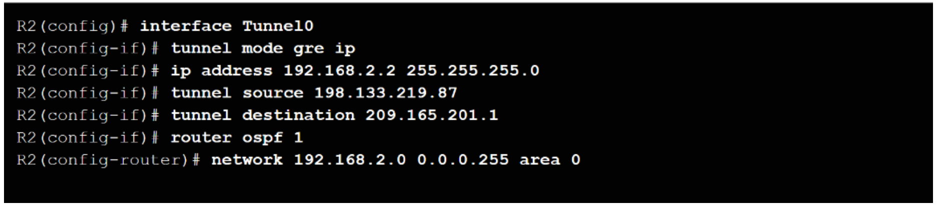
Configure GRE



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
```

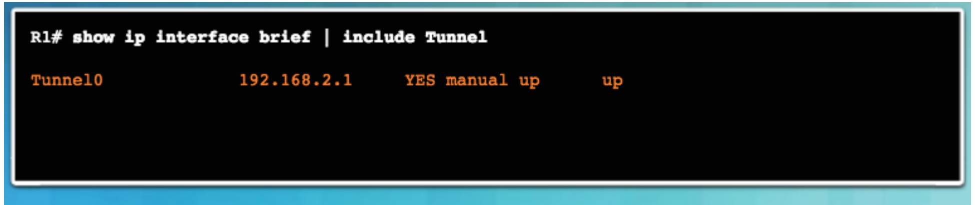
- Five steps to configuring a GRE tunnel:
  - Step 1. Create a tunnel interface using the **interface tunnel** *number* command.
  - Step 2. Configure an IP address for the tunnel interface. (Usually a private address)
  - Step3. Specify the tunnel source IP address.
  - Step 4. Specify the tunnel destination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

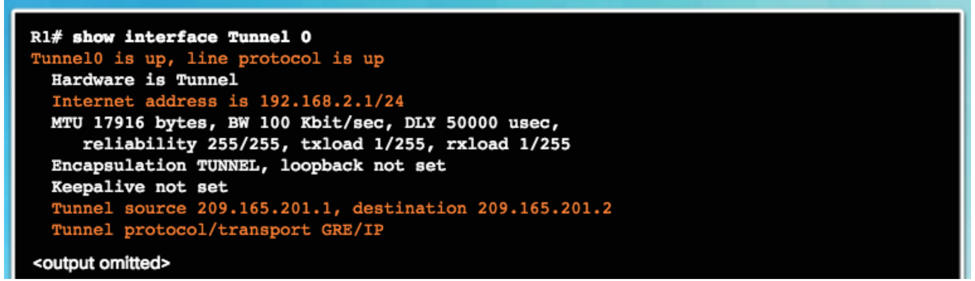
Implement GRE

Verify GRE

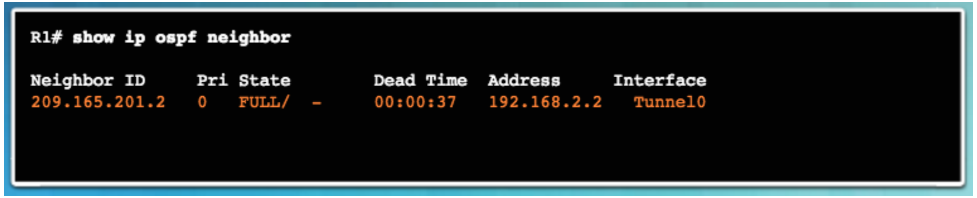
- Use the **show ip interface brief** command to verify that the tunnel interface is up.
- Use the **show interface tunnel** command to verify the state of the tunnel.
- Use the **show ip ospf neighbor** command to verify that an OSPF adjacency has been established over the tunnel interface.



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

Tunnel0              192.168.2.1     YES manual up       up
```



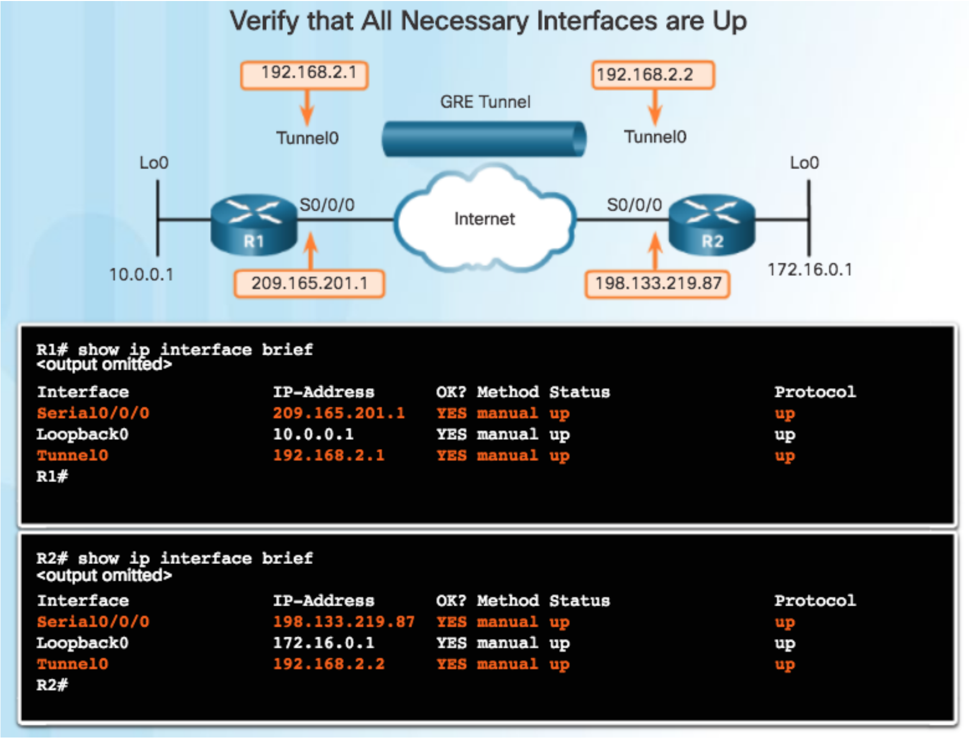
```
R1# show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 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.**



Verify that All Necessary Interfaces are Up

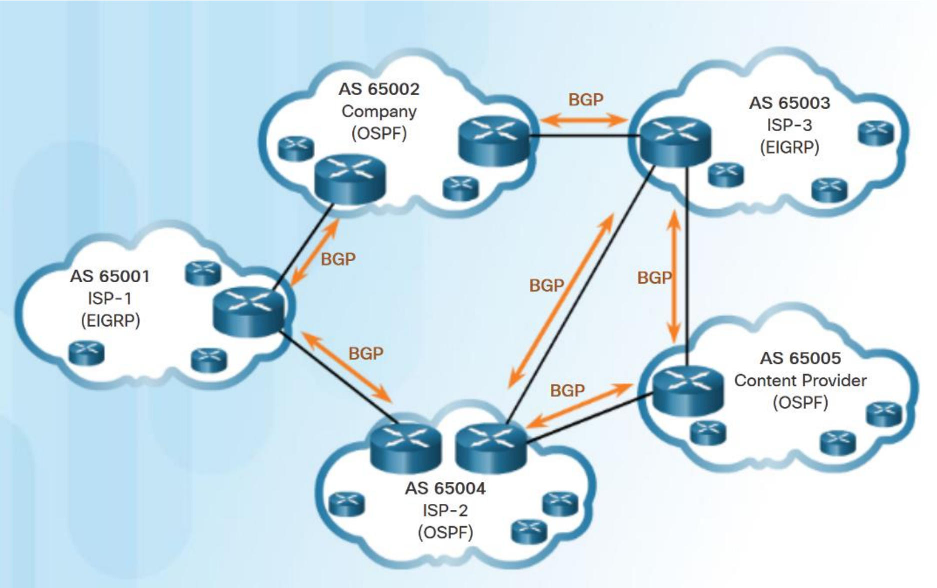
```
R1# show ip interface brief
<output omitted>
Interface              IP-Address      OK? Method Status                Protocol
Serial0/0/0            209.165.201.1   YES manual up                    up
Loopback0              10.0.0.1        YES manual up                    up
Tunnel0                192.168.2.1     YES manual up                    up
R1#
```

```
R2# show ip interface brief
<output omitted>
Interface              IP-Address      OK? Method Status                Protocol
Serial0/0/0            198.133.219.87  YES manual up                    up
Loopback0              172.16.0.1      YES manual up                    up
Tunnel0                192.168.2.2     YES manual up                    up
R2#
```

3.5 eBGP

IGP and EGP Routing Protocols

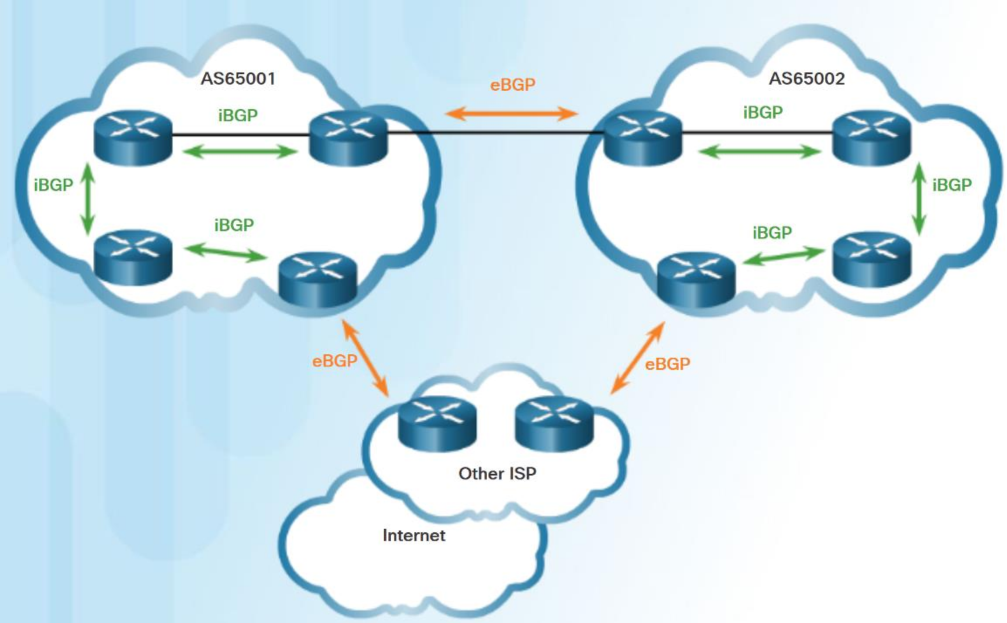
- IGPs are used to exchange routing information within a company network or an autonomous system (AS).
- An Exterior Gateway Protocol (EGP) is used for the exchange of routing information between autonomous systems, such as ISPs.
- Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP).
  - Every AS is assigned a unique 16-bit or 32-bit AS number which uniquely identifies it on the Internet.



BGP Overview

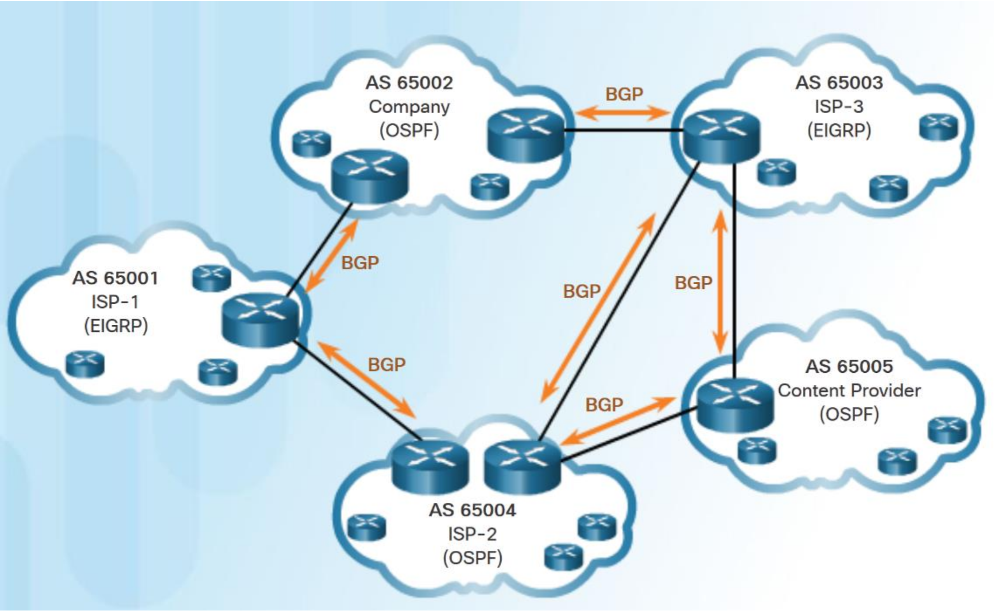
eBGP and iBGP

- **External BGP (eBGP)** – External BGP is the routing protocol used between routers in different autonomous systems.
- **Internal BGP (iBGP)** - Internal BGP is the routing protocol used between routers in the same AS.
- Two routers exchanging BGP routing information are known as BGP peers



When to use BGP

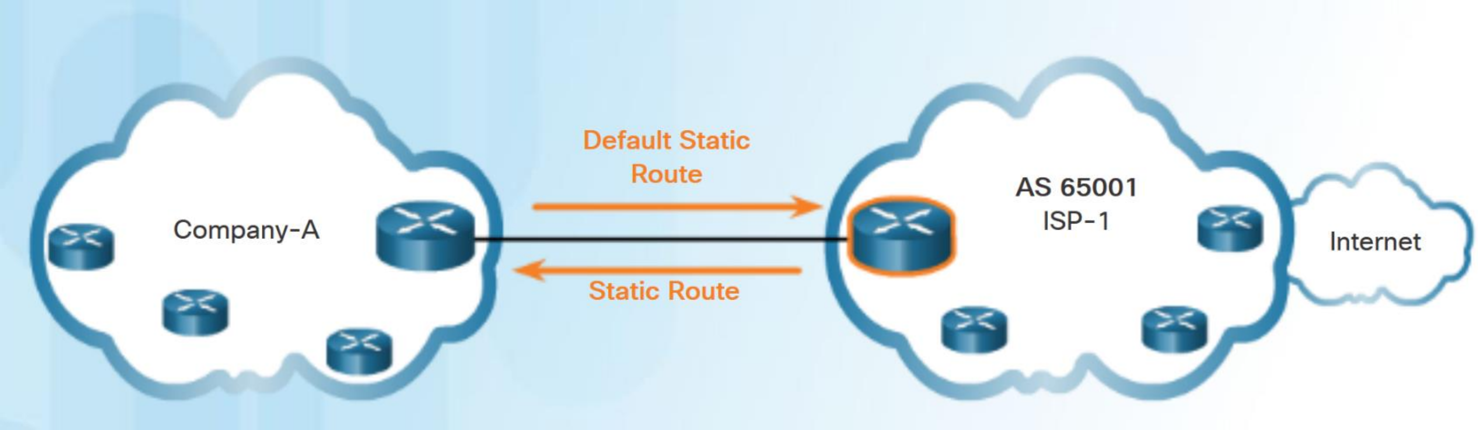
- BGP is used when an AS has connections to multiple autonomous systems. This is known as multi-homed.
- A misconfiguration of a BGP router could have negative effects throughout the Internet.



When not to use BGP

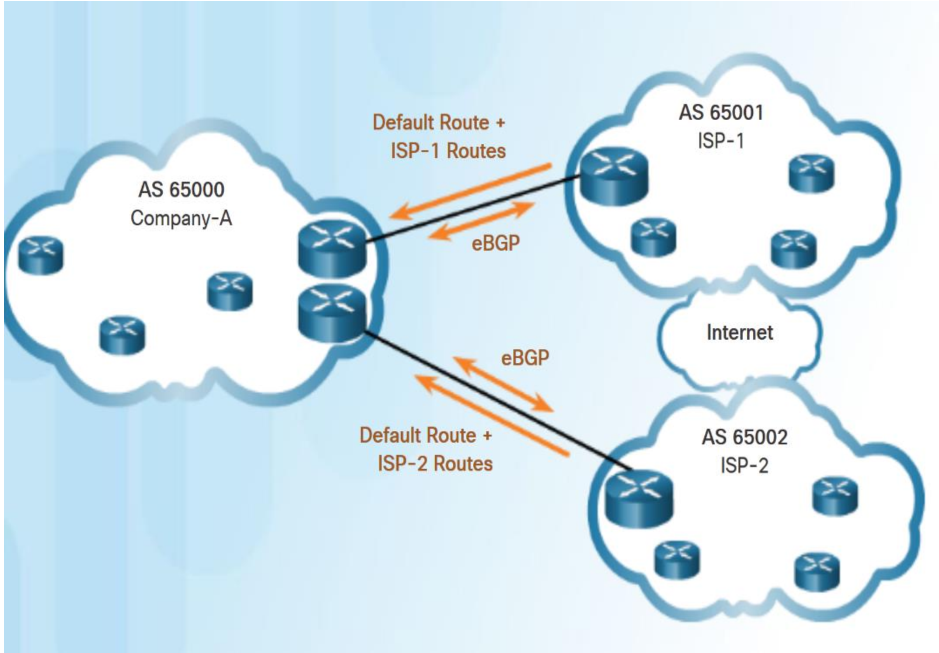
- BGP should not be used when one of the following conditions exist:
  - There is a single connection to the Internet or another AS. Known as single-homed.
  - When there is a limited understanding of BGP.

Note: Although it is recommended only in unusual situations, for the purposes of this course, you will configure single-homed BGP.



BGP Options

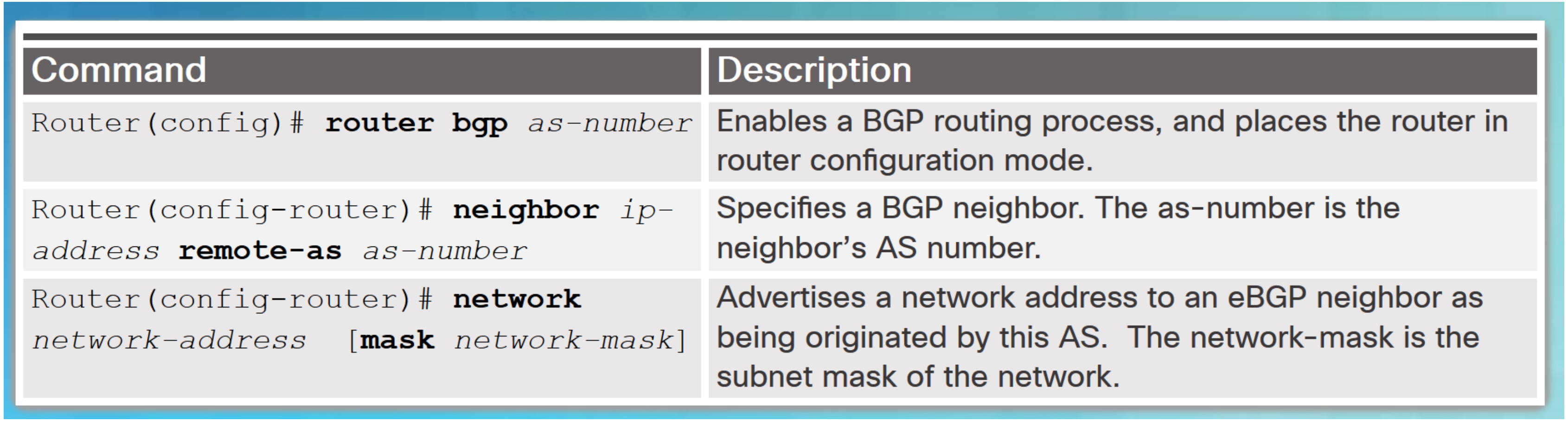
- Three common ways an organization can implement BGP in a multi-homed environment:
  - Default Route Only
  - Default Route and ISP Routes
  - All Internet Routes (this would include routes to over 550,000 networks)



eBGP Branch Configuration

Steps to Configure eBGP

- To implement eBGP:
  - Enable BGP routing.
  - Configure BGP neighbor(s) (peering)
  - Advertise network(s) originating from this AS.

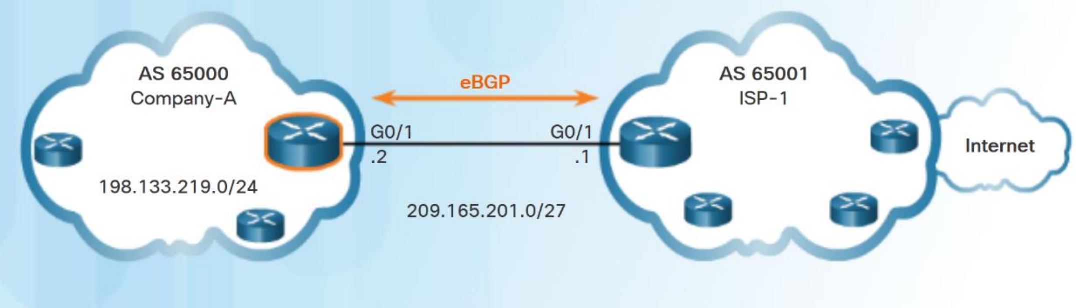


Command	Description
Router(config)# **router bgp** *as-number*	Enables a BGP routing process, and places the router in router configuration mode.
Router(config-router)# **neighbor** *ip-address* **remote-as** *as-number*	Specifies a BGP neighbor. The as-number is the neighbor's AS number.
Router(config-router)# **network** *network-address* [**mask** *network-mask*]	Advertises a network address to an eBGP neighbor as being originated by this AS. The network-mask is the subnet mask of the network.

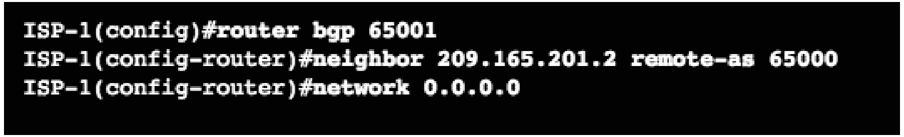
BGP Sample Configuration

- The **router bgp** *as-number* global configuration command enables BGP and identifies the AS number.
- The **neighbor** *ip-address* **remote-as** *as-number* router configuration command identifies the BGP peer and its AS number.
- The **network** *network-address* [**mask** *network-mask*] router configuration command enters the network-address into the local BGP table.

Note: The network-address used in the network command does not have to be a directly connected network.

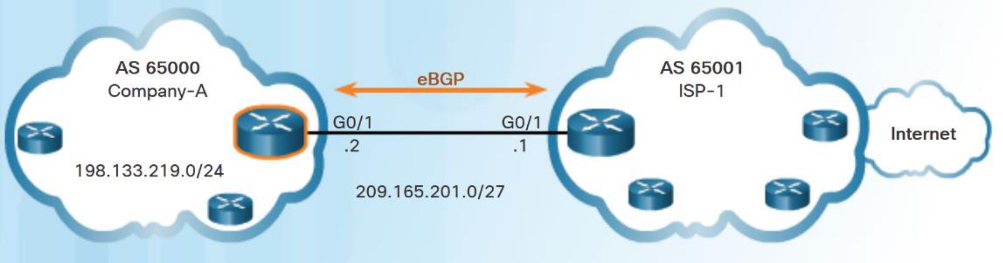


```
Company-A(config)#router bgp 65000
Company-A(config-router)#neighbor 209.165.201.1 remote-as 65001
Company-A(config-router)#network 198.133.219.0 mask 255.255.255.0
```

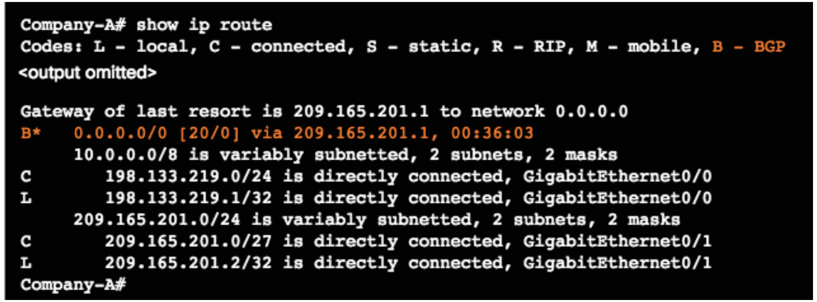


```
ISP-1(config)#router bgp 65001
ISP-1(config-router)#neighbor 209.165.201.2 remote-as 65000
ISP-1(config-router)#network 0.0.0.0
```

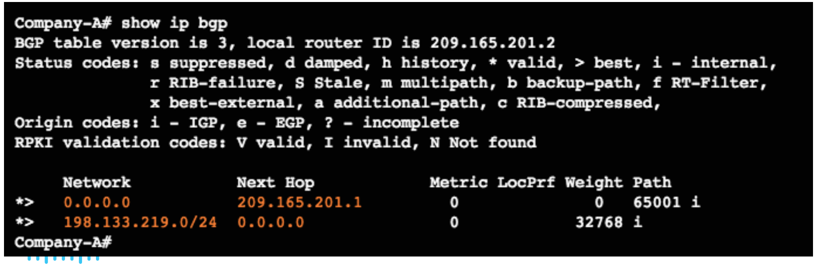
Verify eBGP



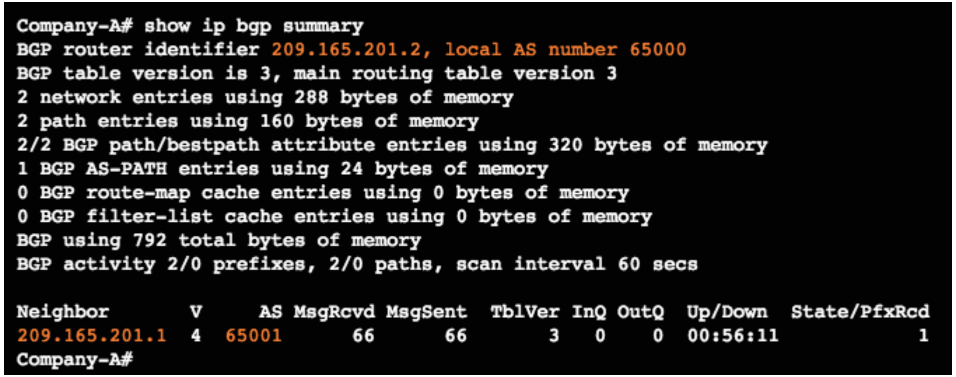
- Three commands to verify eBGP:
  - **show ip route**
  - **show ip bgp**
  - **show ip bgp summary**



```
Company-A# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
<output omitted>

Gateway of last resort is 209.165.201.1 to network 0.0.0.0
B*    0.0.0.0/0 [20/0] via 209.165.201.1, 00:36:03
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        198.133.219.0/24 is directly connected, GigabitEthernet0/0
L        198.133.219.1/32 is directly connected, GigabitEthernet0/0
      209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.201.0/27 is directly connected, GigabitEthernet0/1
L        209.165.201.2/32 is directly connected, GigabitEthernet0/1
Company-A#
```



```
Company-A# show ip bgp
BGP table version is 3, local router ID is 209.165.201.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
*>   0.0.0.0          209.165.201.1            0             0 65001 i
*>   198.133.219.0/24 0.0.0.0                  0         32768 i
Company-A#
```



```
Company-A# show ip bgp summary
BGP router identifier 209.165.201.2, local AS number 65000
BGP table version is 3, main routing table version 3
2 network entries using 288 bytes of memory
2 path entries using 160 bytes of memory
2/2 BGP path/bestpath attribute entries using 320 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 792 total bytes of memory
BGP activity 2/0 prefixes, 2/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
209.165.201.1   4 65001      66      66        3    0    0 00:56:11            1
Company-A#
```

3.6 Chapter Summary

Conclusion

Chapter 3: Branch Connections

- Select broadband remote access technologies to support business requirements.
- Configure a Cisco router with PPPoE.
- Explain how VPNs secure site-to-site and remote access connectivity.
- Implement a GRE tunnel.
- Implement eBGP in a single-homed remote access network.