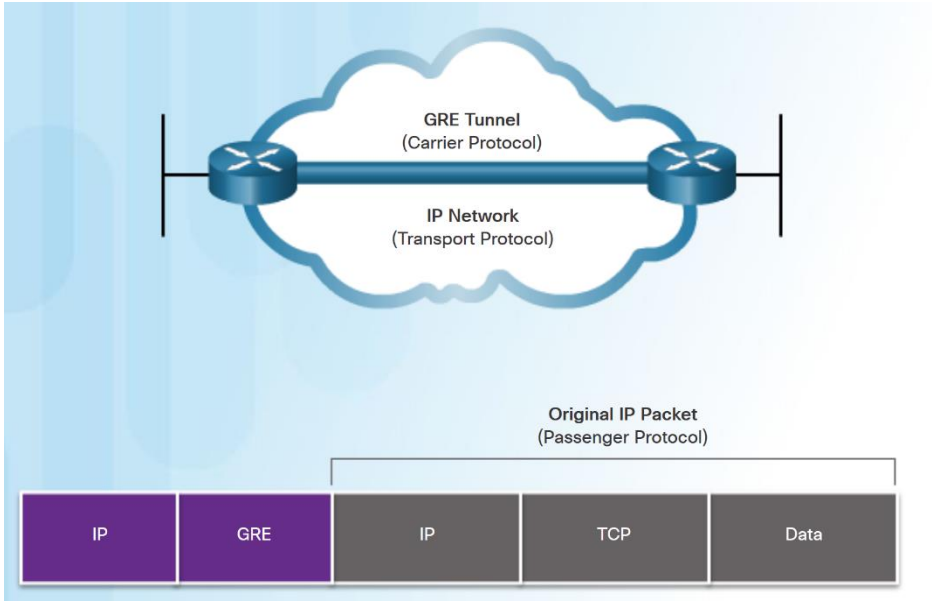
Chapter 3: Branch Connections

CCNA Routing and Switching

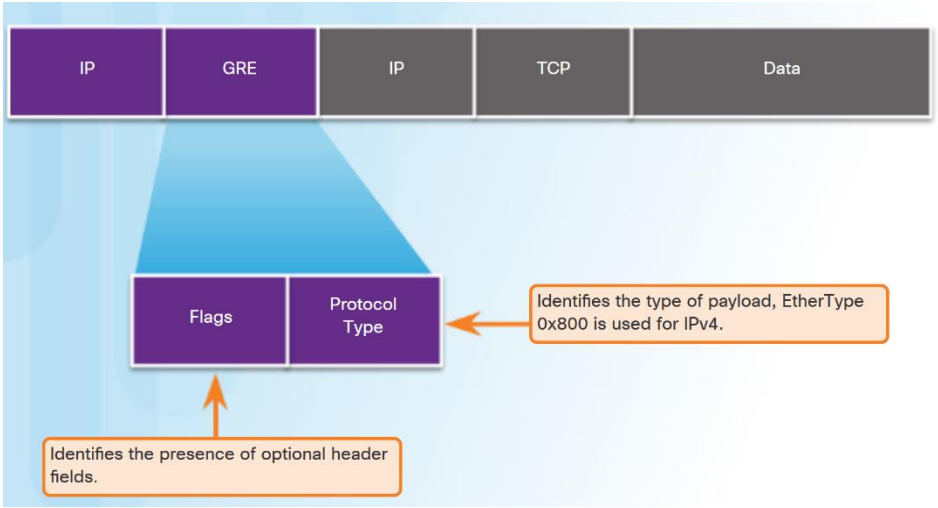
3.1 GRE

GRE Introduction



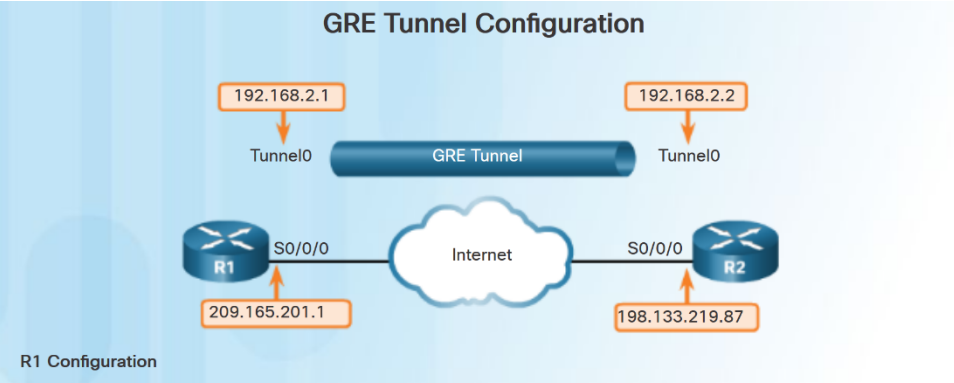
- Generic Routing Encapsulation (GRE) is a non-secure, site-to-site VPN tunneling protocol.
- Developed by Cisco.
- GRE manages the transportation of multiprotocol and IP multicast traffic between two or more sites
- A tunnel interface supports a header for each of the following:
  - An encapsulated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

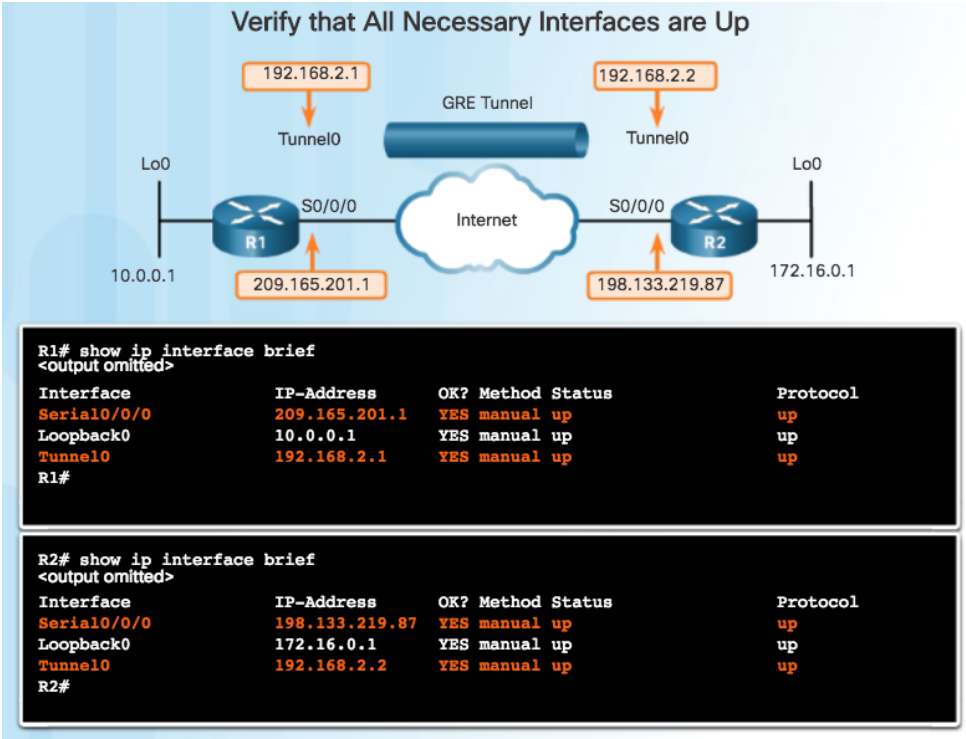
```
R1# show interface Tunnel 0
Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 192.168.2.1/24
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source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

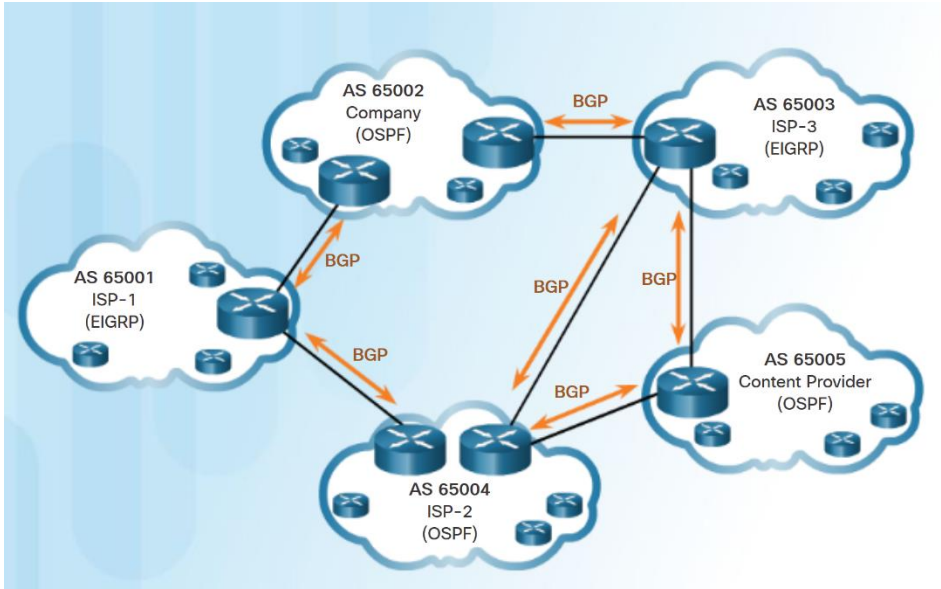
- Issues with GRE are usually due to one or more of the following:
  - The tunnel interface IP addresses are not on the same network or the subnet masks do not match. Use the **show ip interface brief** command.
  - The interfaces for the tunnel source and/or destination are not configured with the correct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



3.2 eBGP

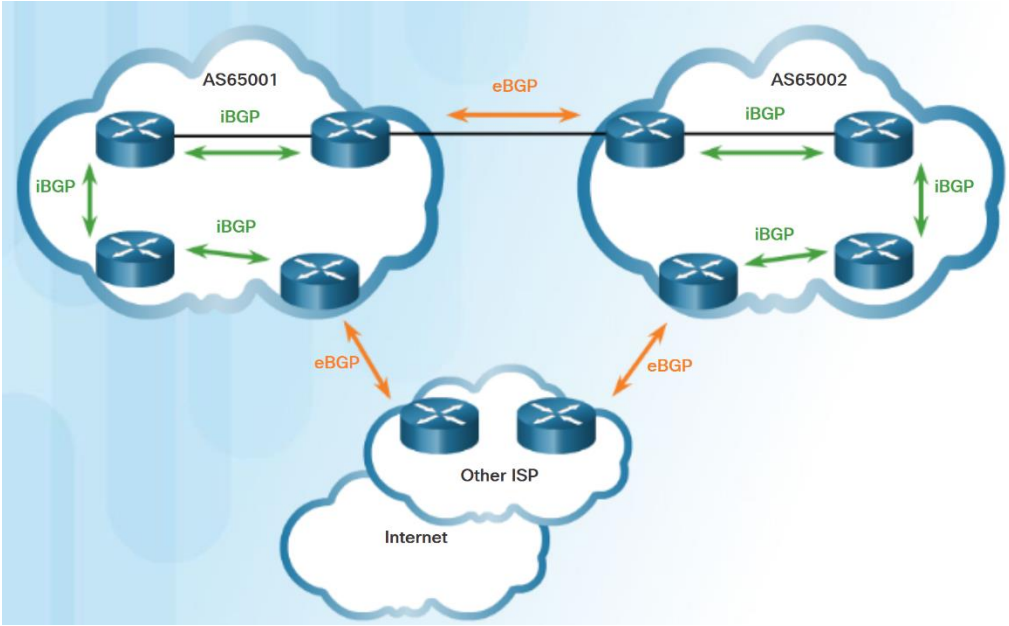
IGP and EGP Routing Protocols

- 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.



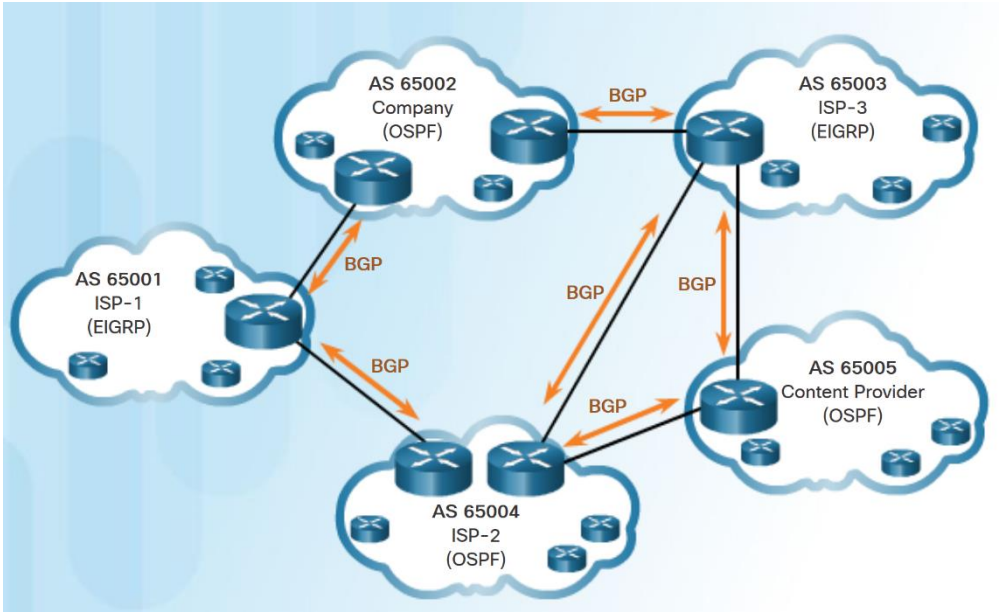
eBGP and iBGP

- **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

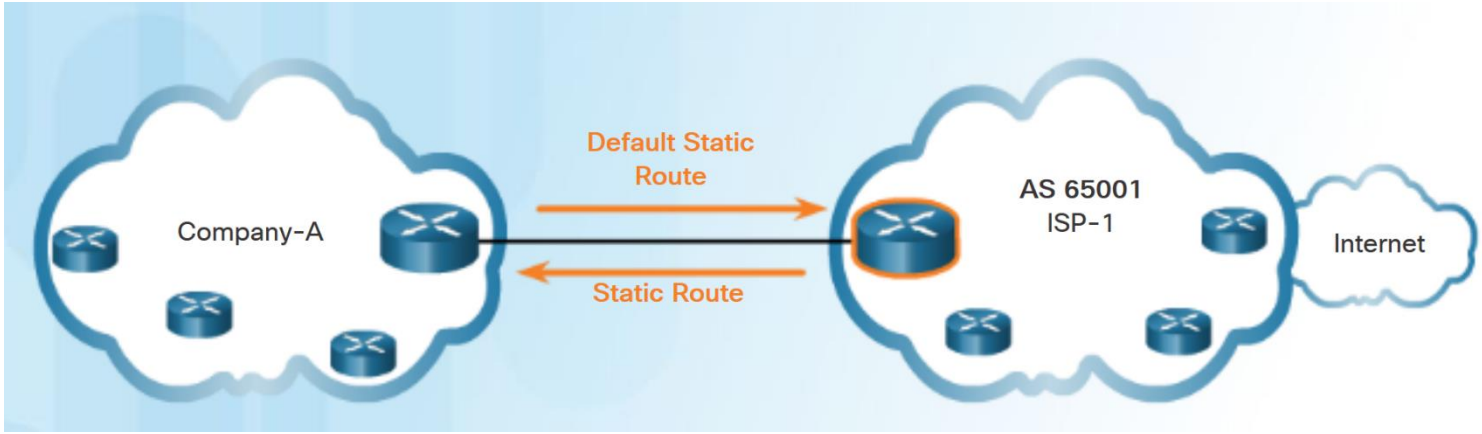
- BGP is used when an AS has connections to multiple autonomous systems. This is known as multi-homed.
- A misconfiguration of a BGP router could have negative effects throughout the Internet.



When not to use BGP

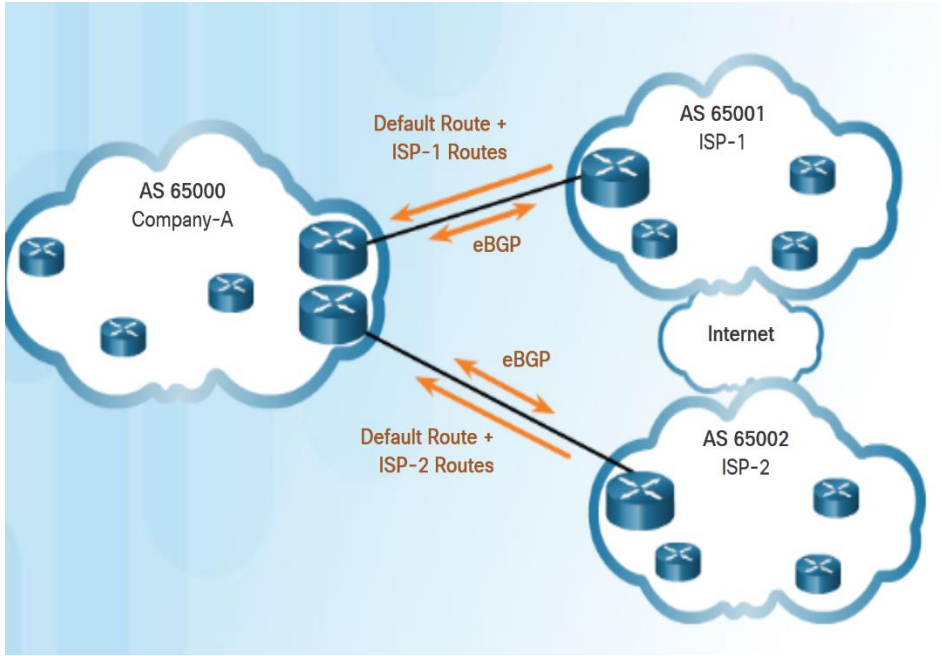
- BGP should not be used when one of the following conditions exist:
  - There is a single connection to the Internet or another AS. Known as single-homed.
  - When there is a limited understanding of BGP.

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)



Steps to Configure eBGP

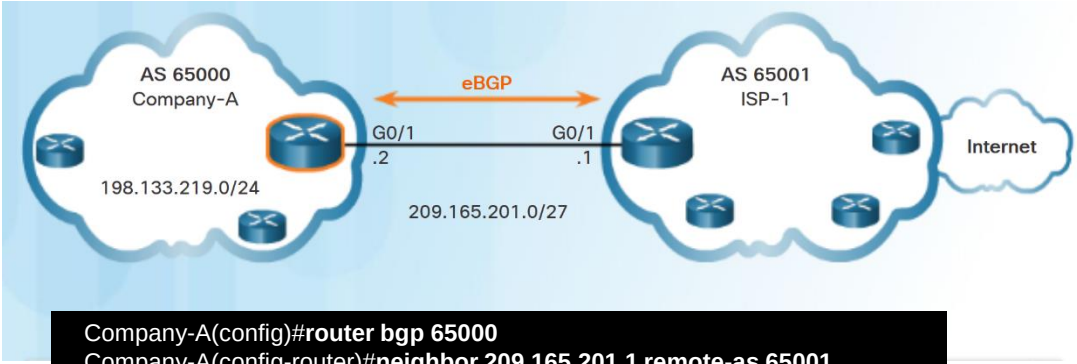
- To implement eBGP:
  - Enable BGP routing.
  - Configure BGP neighbor(s) (peering)
  - Advertise network(s) originating from this AS.

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.

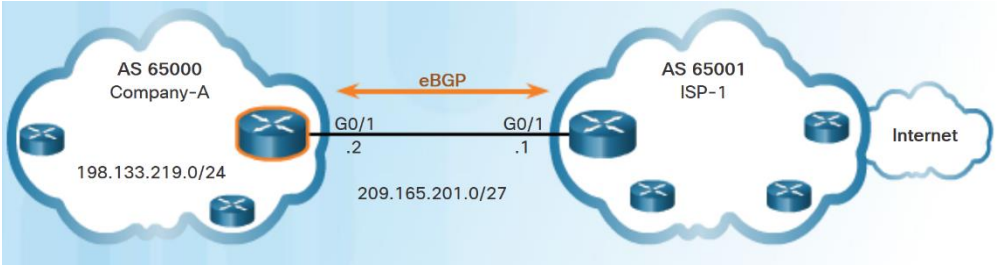
Note: The network-address used in the network command does not have to be a directly connected network.




```
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#
```


CISCO