Chapter 3: Branch Connections

Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 3

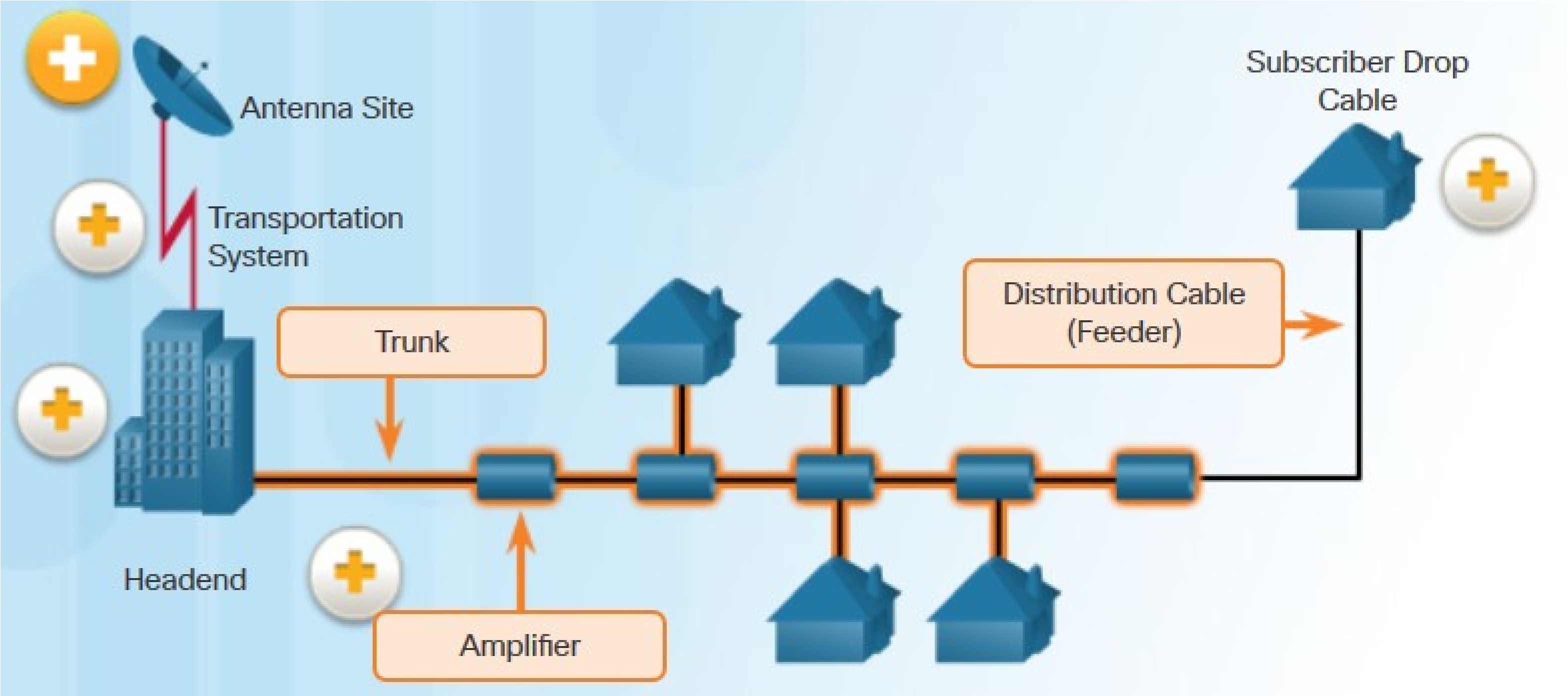
- 3.1 Remote Access Connections
- 3.2 PPPoE
- 3.3 VPNs
- 3.4 GRE
- 3.5 IPv6 Tunneling
- 3.6 eBGP

3.1 Remote Access Connections

Cisco | Networking Academy®
Mind Wide Open™

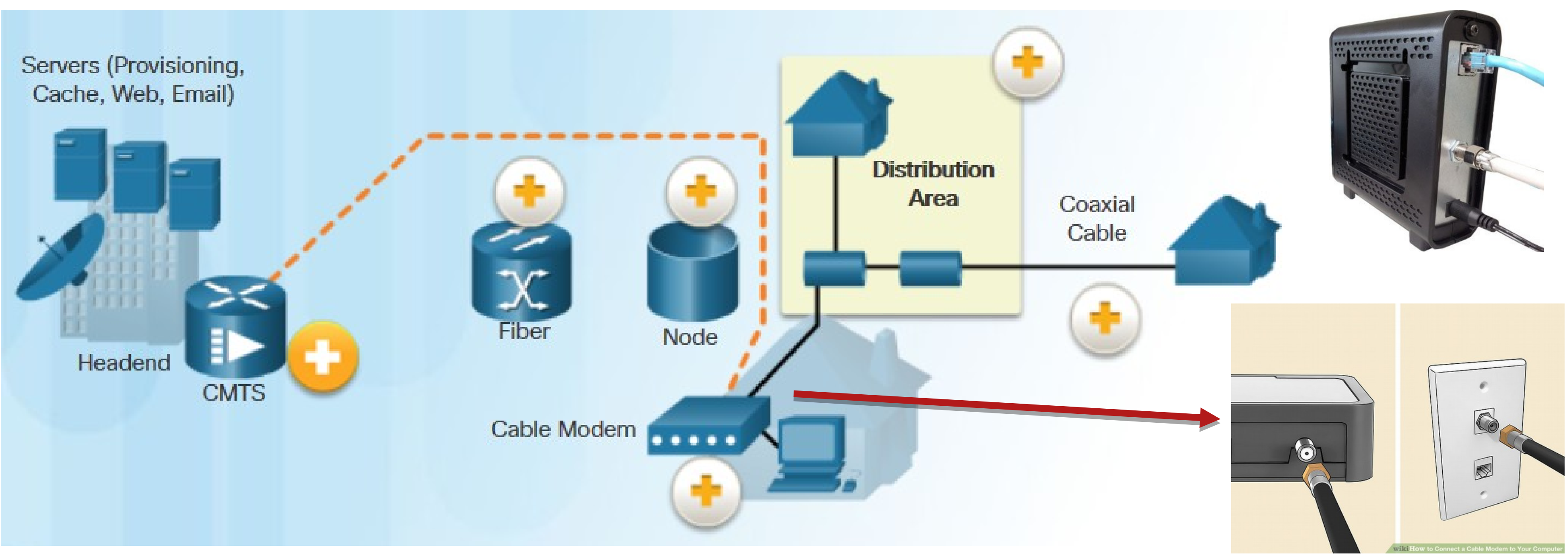
Cable System

- Cable system uses a coaxial cable that carries RF signal across the network.
- Based on CATV (Community Antenna Television) system developed in 1948
- Two-way communication between subscribers and the cable operator.
- Transmits Internet, TV, phone in different frequencies.
- Downstream frequencies 50-860 MHz, upstream frequencies: 5-42 MHz



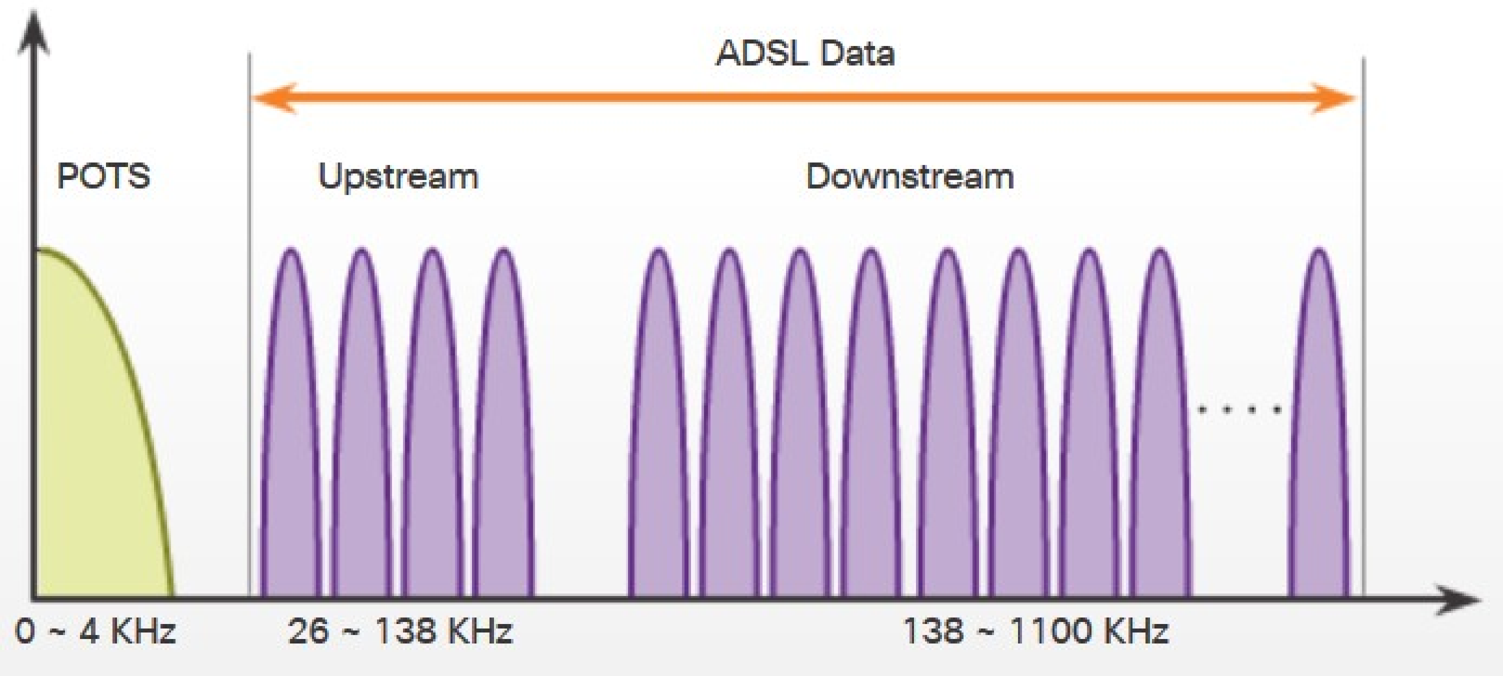
End-to-End Data Propagation Over Cable

- Operator equipment: Cable Modem Termination System (CMTS)
- Subscriber equipment: Cable modem (CM)
- Hybrid fiber-coaxial (HFC) networks: a mixed optical-coaxial network
  - 500 – 2000 subscribers per a shared segment
  - Bandwidth: up to 10 Bb/s downstream and up to 1 Bb/s upstream (DOCSIS 3.1)



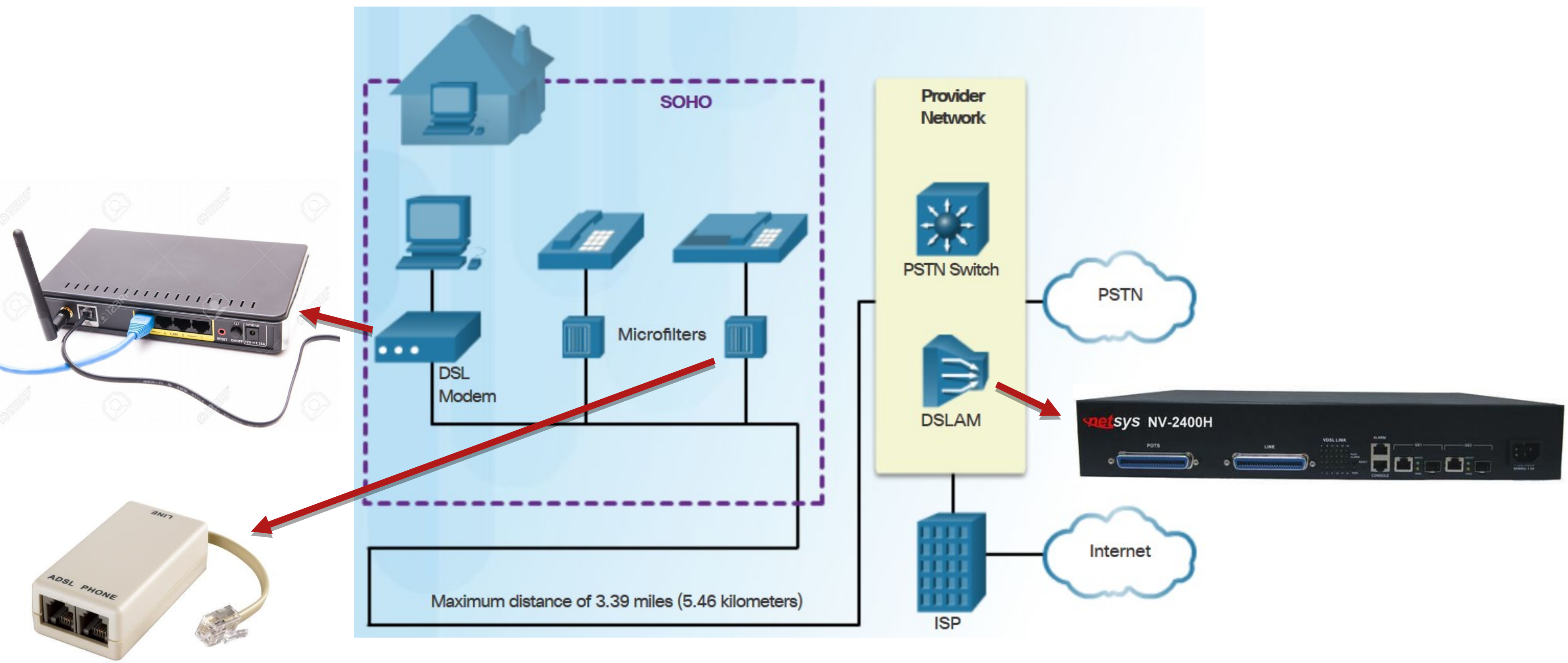
Digital Subscriber Line (DSL)

- DSL provides high-speed connections over installed copper wire system.
- Two basic types: asymmetric (ADSL) and symmetric (SDSL).
- ADSL uses a frequency range from approximately 20 kHz to 1 MHz.
- Bandwidth depends on the type of DSL: up to 40 Mb/s.
- Local loop must be less than approximately 3.39 miles (5.46 km) for ADSL.



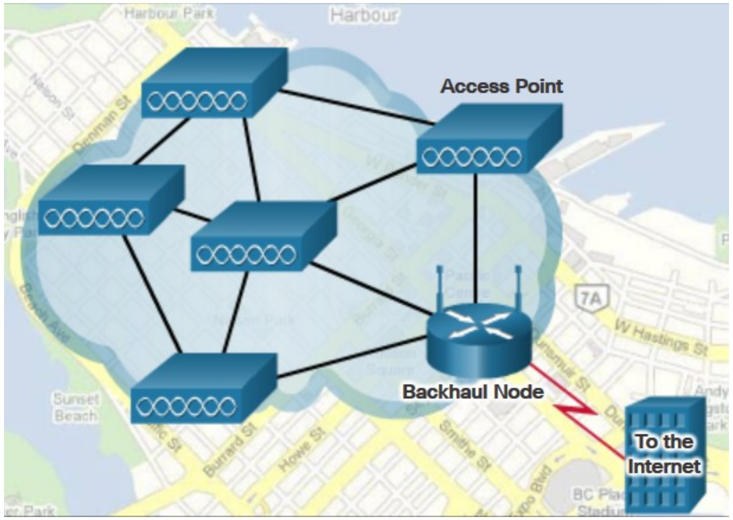
DSL Connections

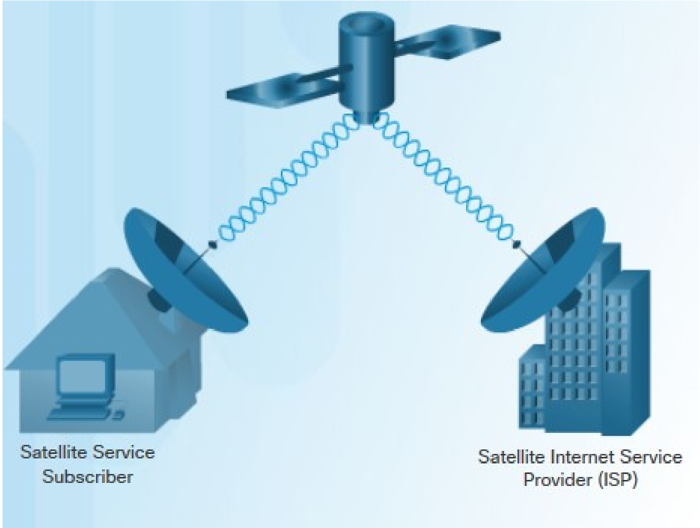
- **Transceiver** – connects the computer of the teleworker to the DSL.
- **DSL access multiplexer** (DSLAM) – combines individual DSL connections from users into one high-capacity link to an ISP.



Broadband Wireless Connection

- **Municipal Wi-Fi (Mesh)**
  - Wireless networks deployed over the city.
  - A mesh of interconnected APs.
- **Cellular/mobile Internet**
  - 2G: GSM, CDMA, TDMA
  - 3G: UMTS, CDMA2000, EDGE, HSPA+
  - 4G: Long-Term Evolution (LTE)
- **Satellite Internet**
  - one-way multicast
  - one-way terrestrial return
  - two-way satellite Internet





Comparing Broadband Solutions

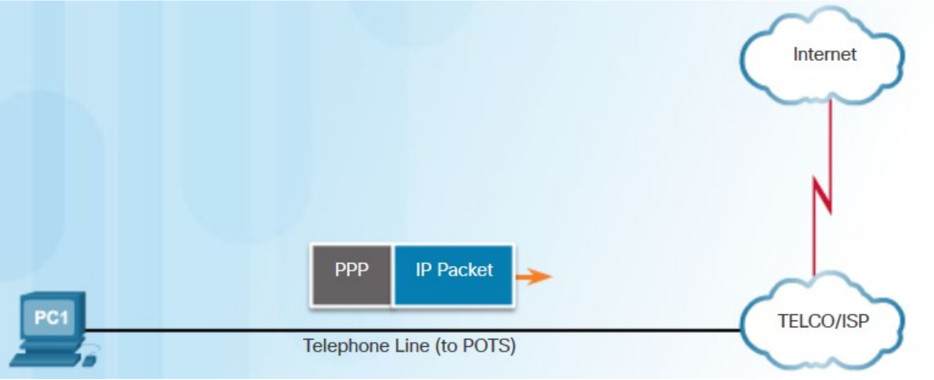
- **Cable**
  - Bandwidth is shared by many users.
  - Upstream rates can be slow due to high usage and oversubscription.
- **DSL**
  - Limited bandwidth that is distance-sensitive.
- **Fiber-to-the-Home**
  - Requires fiber-access network overlay.
- **Cellular/Mobile**
  - Coverage is often an issue, bandwidth relatively limited.
- **Wi-Fi Mesh**
  - Most municipalities do not have a mesh network deployed.
- **Satellite**
  - Expensive; limited capacity per subscriber.

3.2 PPPoE

Cisco | Networking Academy®
Mind Wide Open™

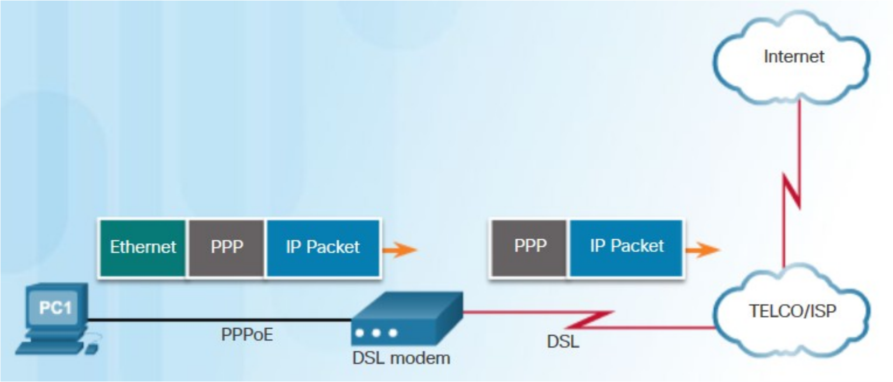
PPP Frames over an Ethernet (PPPoE)

- Most commonly used data link layer protocol by ISPs is PPP
  - Supported by analog modems, ISDN and DSL.
  - PPP supports CHAP authentication, IP address assignment, etc.
- Ethernet does not natively support PPP.
  - PPPoE allows the sending of PPP frames encapsulated inside Ethernet frames.

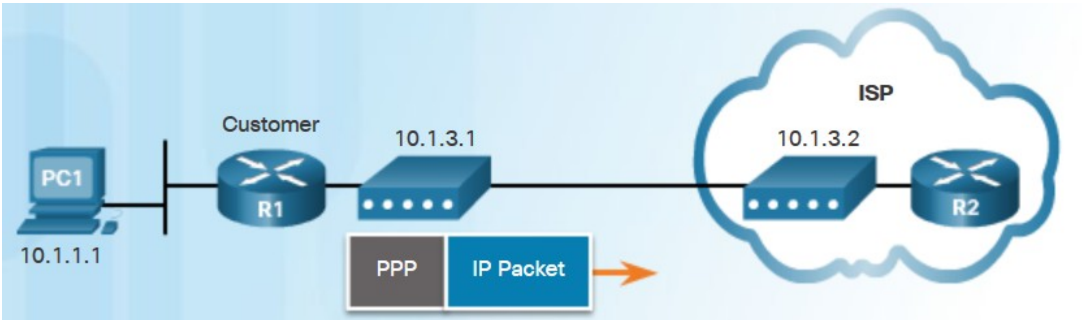


PPP Frames over Dialup Connection

PPP Frames over an Ethernet Connection

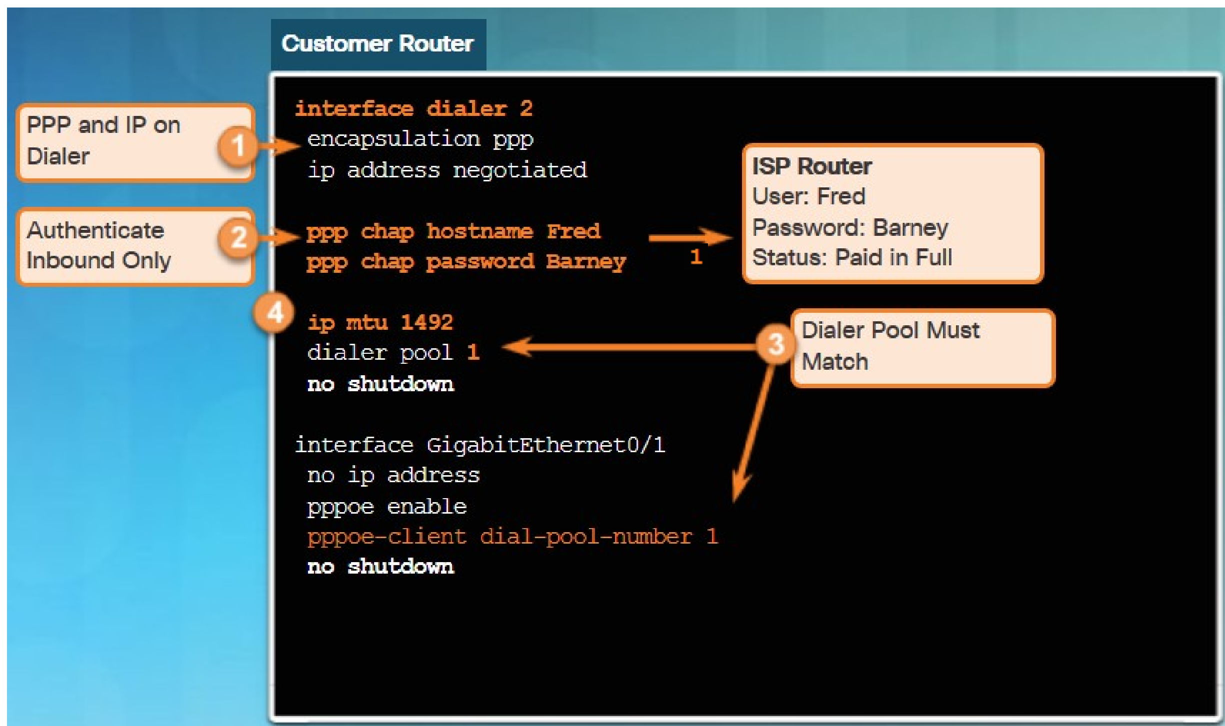


Tunneling PPP over Ethernet (PPPoE)

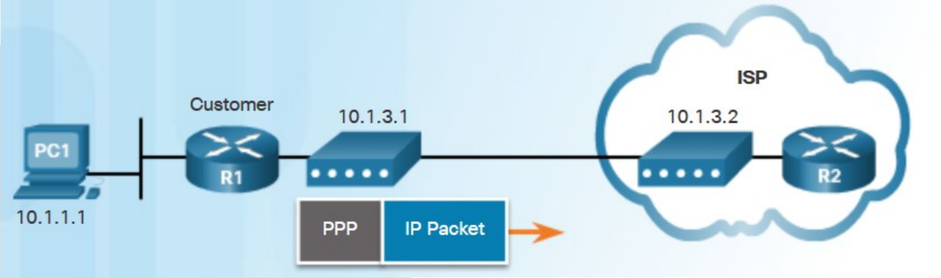


Configuring customer router:

1. Create a virtual dialer interface
2. Set PPP encapsulation and configure CHAP authentication
3. Enable PPPoE on a physical interface
4. Reduce MTU to 1492



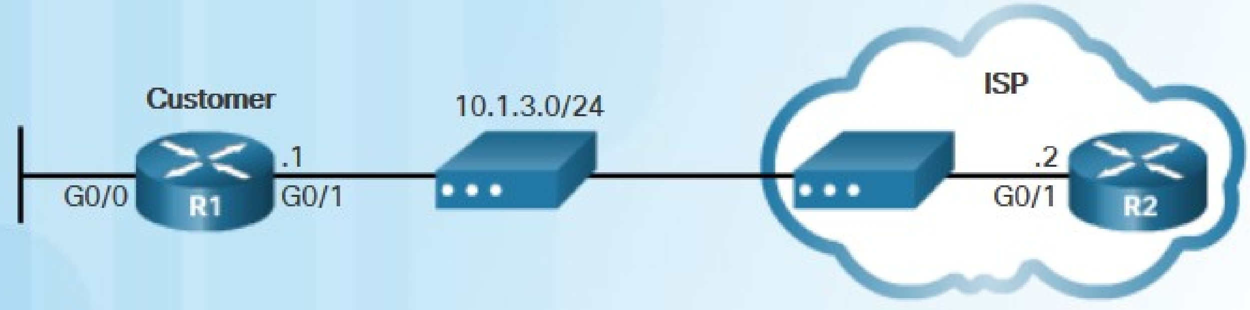
Tunneling PPP over Ethernet (PPPoE)



Configuring ISP router:

1. Create a local database
   - R2(conf)# username Fred password Barney
2. Create a pool of addresses for customers
   - R2(conf)# ip local pool PPPoE 10.1.3.1 10.1.3.50
3. Create the virtual template for customers
   - R2(conf)# interface virtual-template 1
   - R2(conf-if)# ip address 10.1.3.254 255.255.255.0
   - R2(conf-if)# mtu 1492
   - R2(conf-if)# peer default ip address pool PPPoE
   - R2(conf-if)# ppp authentication chap callin
4. Assign the template to the broadband aggregation group
   - R2(conf)# bba-group pppoe global
   - R2(conf-bba-group)# virtual-template 1
5. Associate the BBA with the physical interface
   - R2(conf)# interface g0/0
   - R2(conf)# pppoe enable group global
   - R2(conf)# no shutdown

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 ip interface brief

PPPoE Verification


```
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>
```

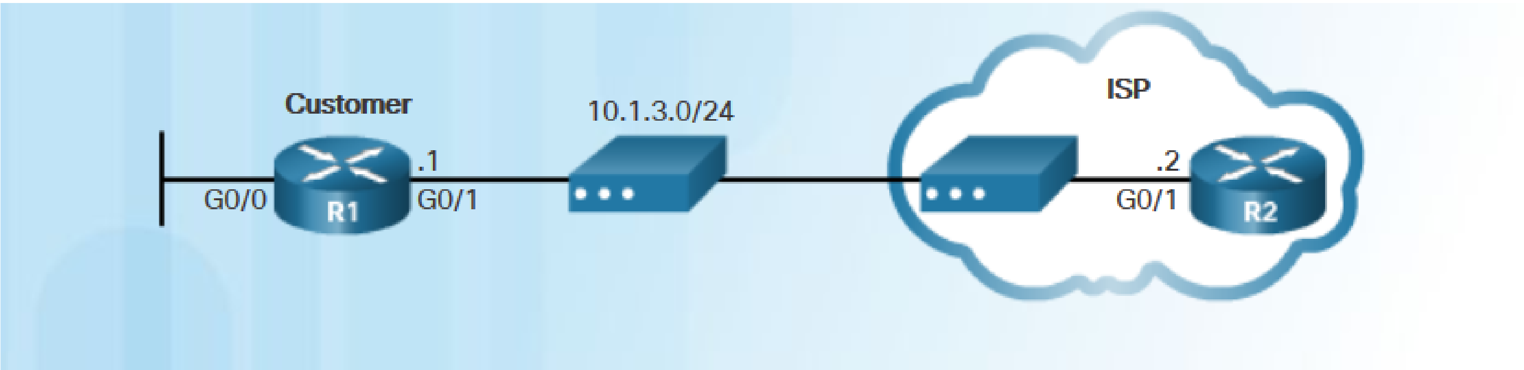
R1# show interface dialer <XX>

PPPoE Verification


```
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#
```

R1# show pppoe session

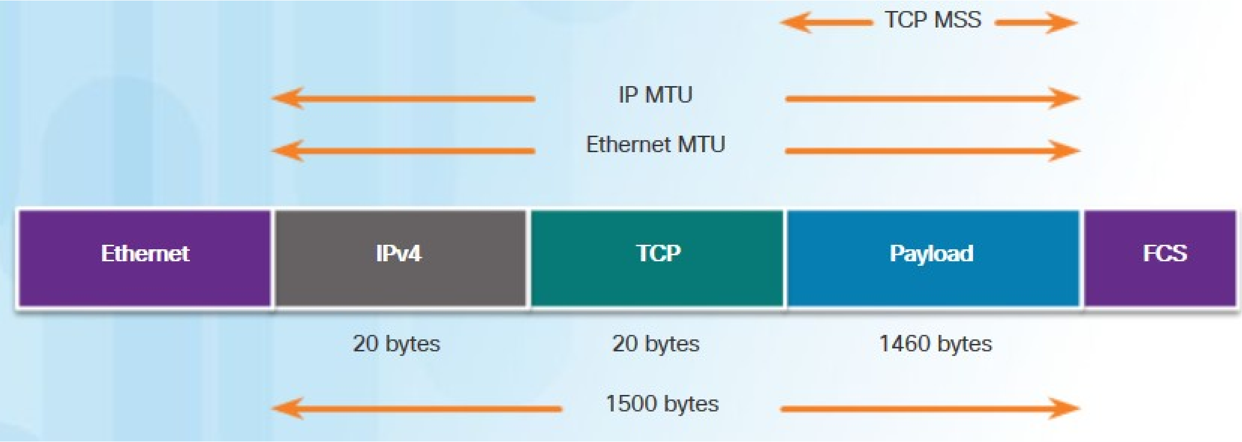
Debugging PPPoE Negotiation



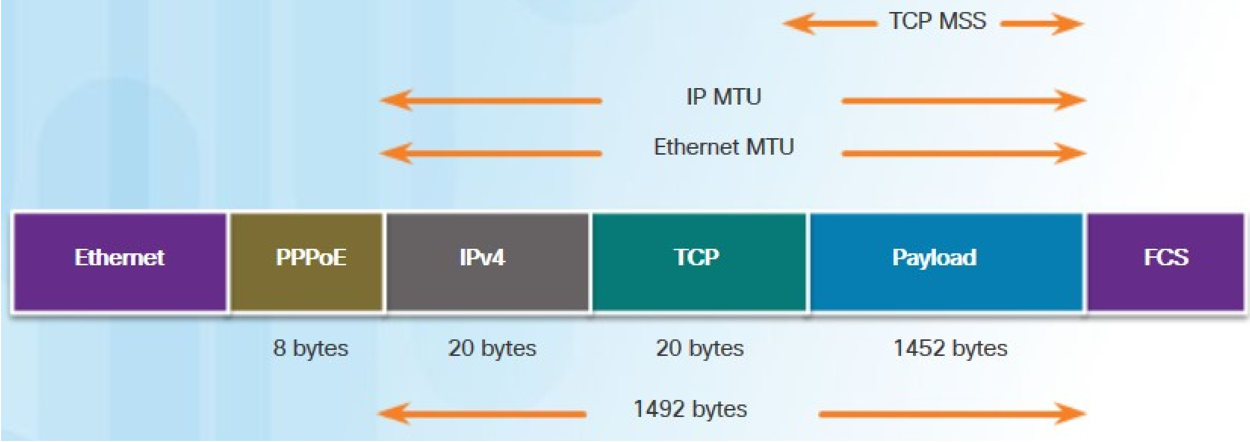

```
R1# debug ppp negotiation
*Sep 20 19:05:05.239: Vi2 PPP: Phase is AUTHENTICATING, by the peer
*Sep 20 19:05:05.239: Vi2 LCP: State is Open
 <output omitted>
*Sep 20 19:05:05.247: Vi2 CHAP: Using hostname from interface CHAP
*Sep 20 19:05:05.247: Vi2 CHAP: Using password from interface CHAP
*Sep 20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

R1# debug ppp negotiation

Adjusting MSS with PPPoE Header



TCP MSS computed using the default Ethernet MTU.



TCP MSS for PPPoE frames.

R1(conf)# interface g0/0

R1(conf-if)# ip tcp adjust-mss 1452

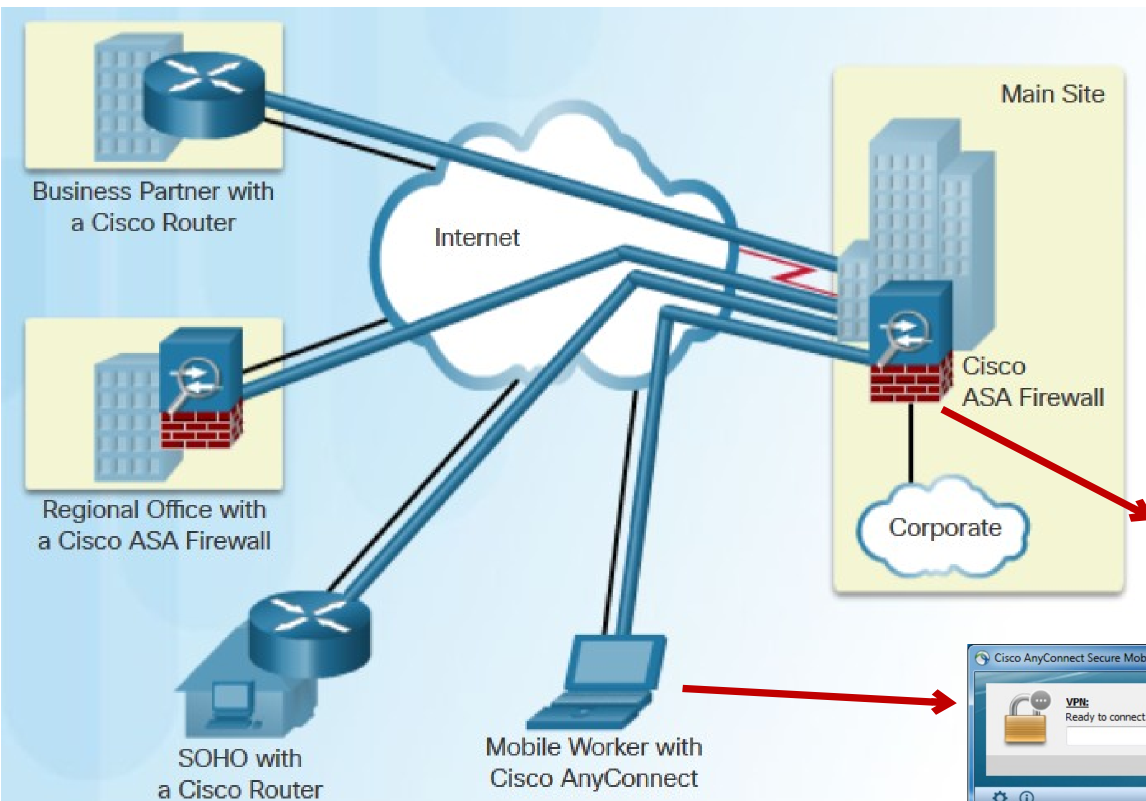
- The **ip tcp adjust-mss** *max-segment-size* interface command adjusts the MSS value during the TCP 3-way handshake.

3.3 VPNs

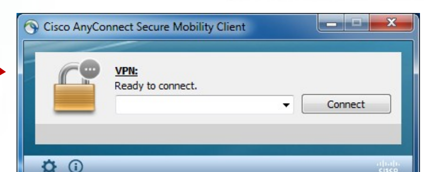
Cisco | Networking Academy®
Mind Wide Open™

Virtual Private Networks (VPNs)

- Virtual (logical) networks over public network infrastructure.
- Secure transmission of data using encryption and authentication.
- To implement VPNs, a VPN gateway is necessary:
  - A router, a firewall, or a Cisco Adaptive Security Appliance (ASA).

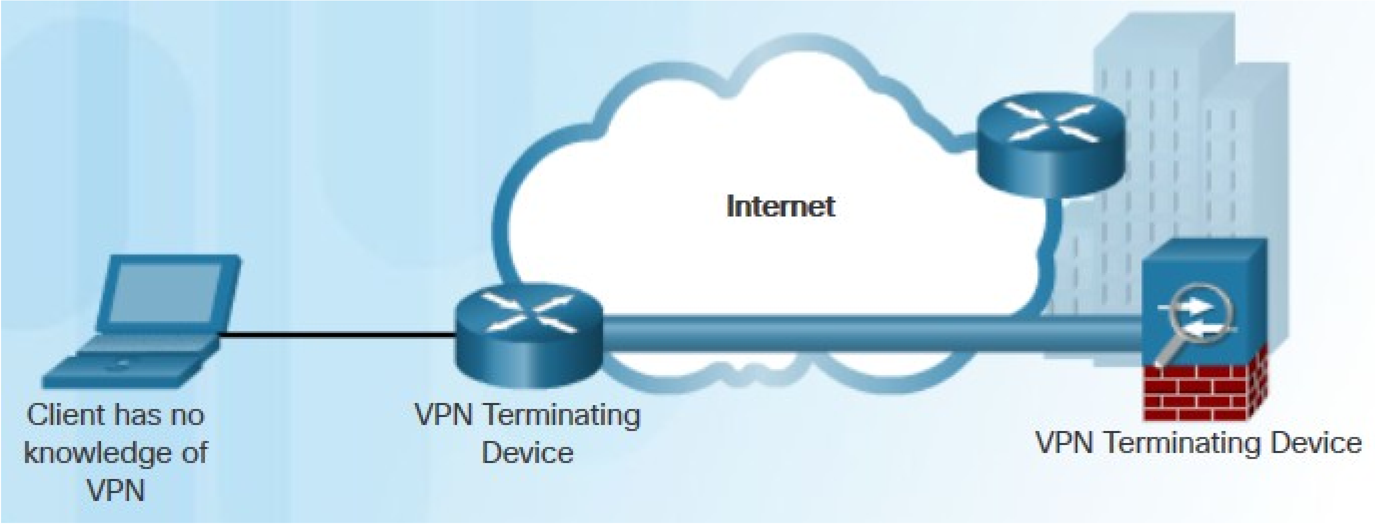


- Site-to-Site VPNs
- Remote Access VPNs
- Dynamic Multipoint VPNs (DMVPNs)



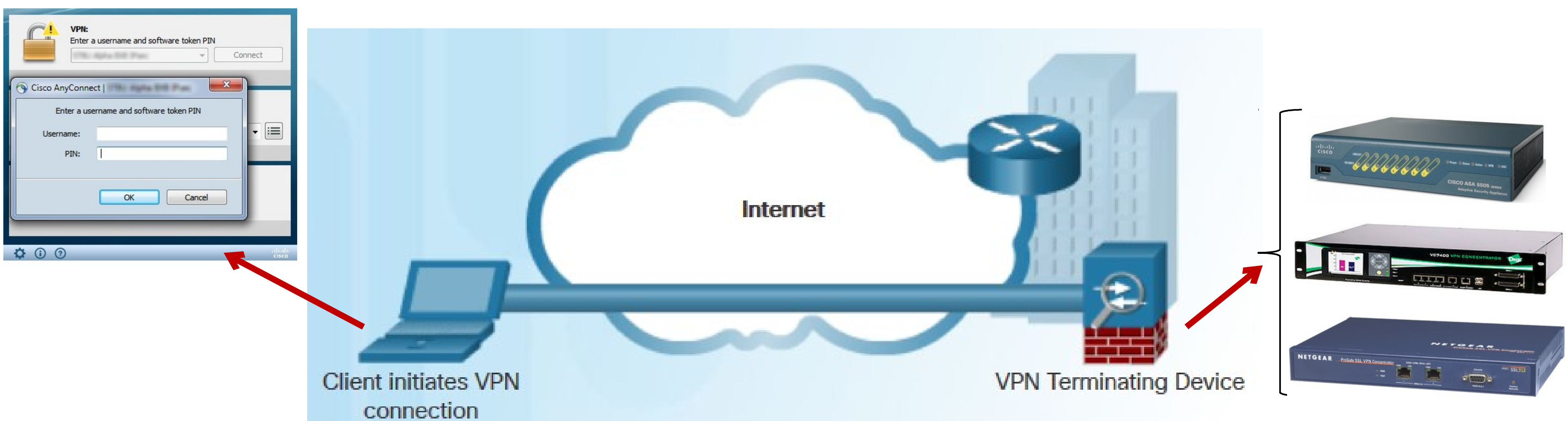
Site-to-Site VPNs

- Both sides of the VPN connection permanently configured in advance.
- Internal hosts have no knowledge that a VPN exists => transparent for users.
- End hosts send and receive normal TCP/IP traffic through a VPN gateway.
- VPN gateway responsible for encapsulating and encrypting outbound traffic.
- The VPN gateway sends data through a VPN tunnel over the Internet.
- The peer VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network.



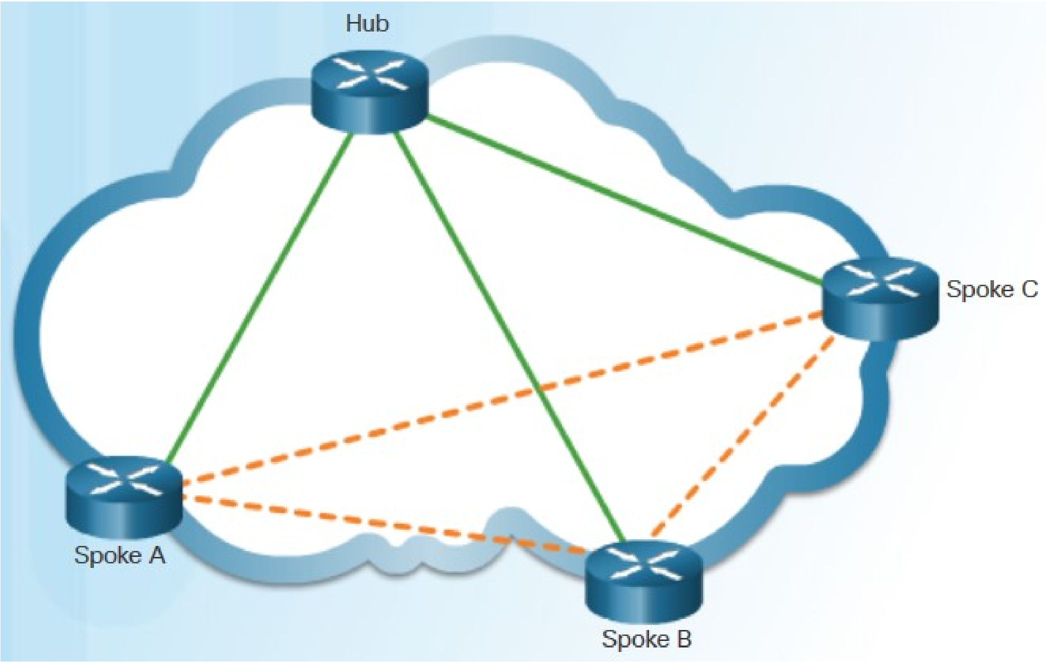
Remote Access VPNs

- For telecommuters, mobile users, and extranet, consumer-to-business traffic.
- Client/server architecture
  - VPN client (remote host) gains secure access to the enterprise network via a VPN server device at the network edge.
  - VPN client software may need to be installed on the mobile user's end device (Cisco AnyConnect Secure Mobility Client).
- VPN Client encapsulates and encrypts this traffic and sends over the Internet to the VPN gateway at the edge of the target network.



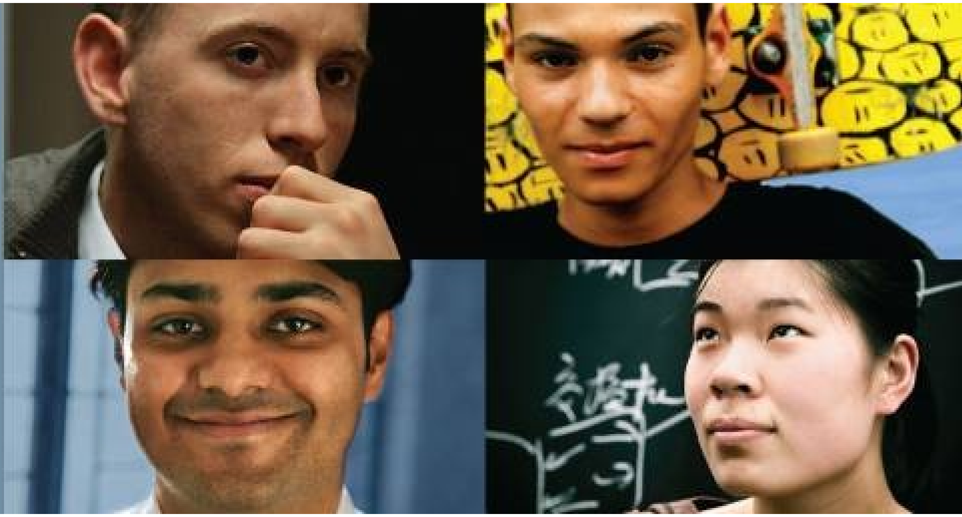
Dynamic Multipoint VPNs (DMVPNs)

- Hub-to-Spoke and Spoke-to-Spoke Tunnels
- DMVPN uses the following technologies
  - Next Hop Resolution Protocol (NHRP) – similar to ARP (mapping IP address to spokes)
  - Multipoint Generic Routing Encapsulation (mGRE) tunnels
    - GRE interface with multiple IPSec tunnels
  - IP Security (IPSec) encryption



- Easy
- Dynamic
- Scalable

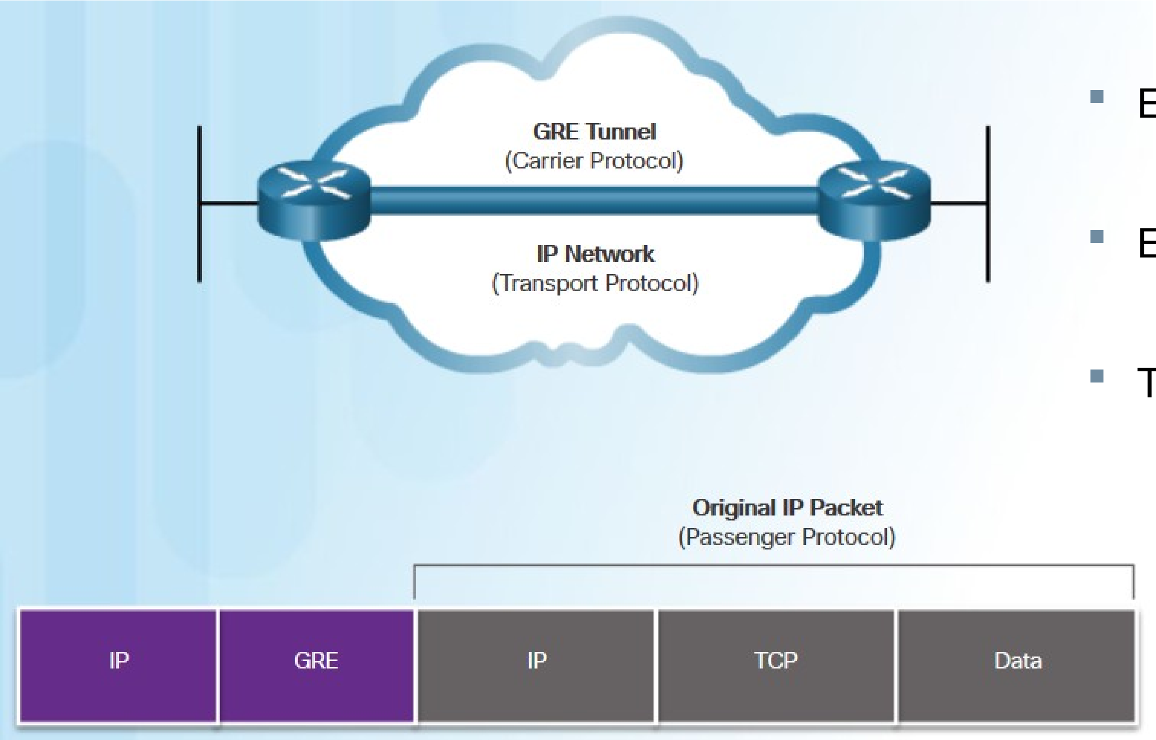
3.4 GRE



Cisco | Networking Academy®
Mind Wide Open™

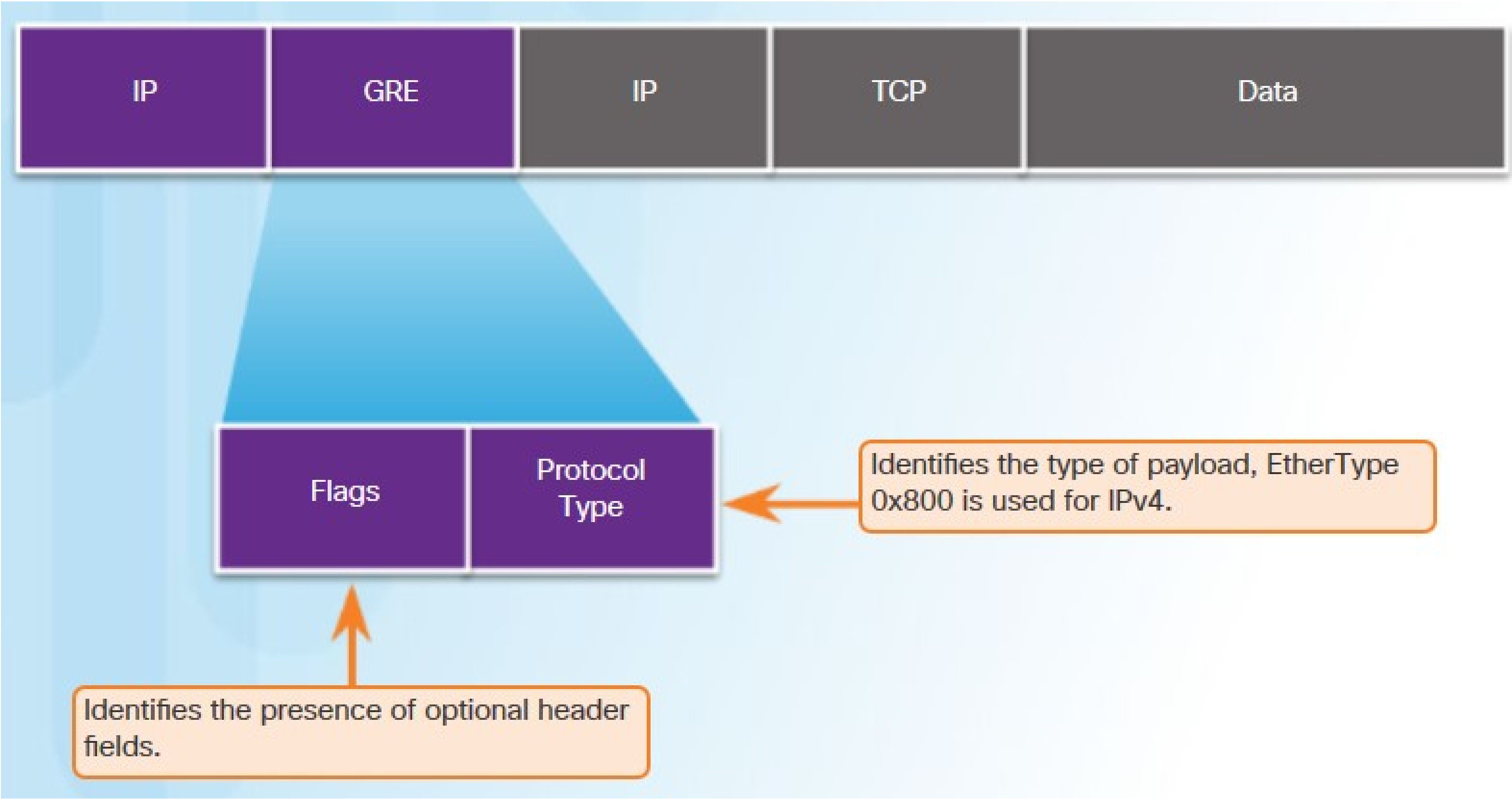
Generic Routing Encapsulation (GRE)

- Developed by Cisco, IETF standard RFC 2784 (2000)
- Basic, non-secure, site-to-site VPN tunneling protocol
  - Transportation of multiprotocol and IP multicast traffic between two sites
- Encapsulates a wide variety of protocol packet types inside IP tunnels
- Creates a virtual point-to-point link to remote routers over an IP internetwork



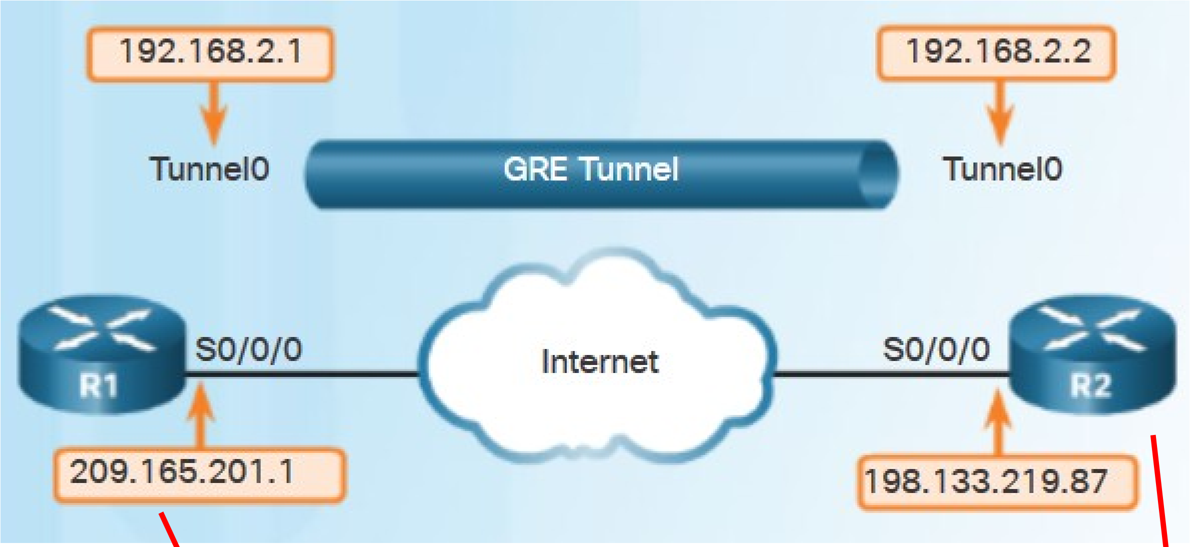
- Encapsulated (passenger) protocol
  - IPv4, IPv6, AppleTalk, IPX
- Encapsulation protocol (carrier)
  - GRE
- Transport delivery protocol
  - IP

GRE Encapsulated Packet Header



- IP protocol number for GRE- 47
- Stateless protocol, no flow control
- No encryption, no authentication

GRE Tunnel Configuration



1. Create a tunnel interface
2. Specify the tunnel source IP address
3. Specify the tunnel destination IP address
4. Configure an IP address for tunnel interface
5. Specify GRE tunnel mode (optional)

```
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
```

```
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
```

GRE Tunnel Verification

```
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
```

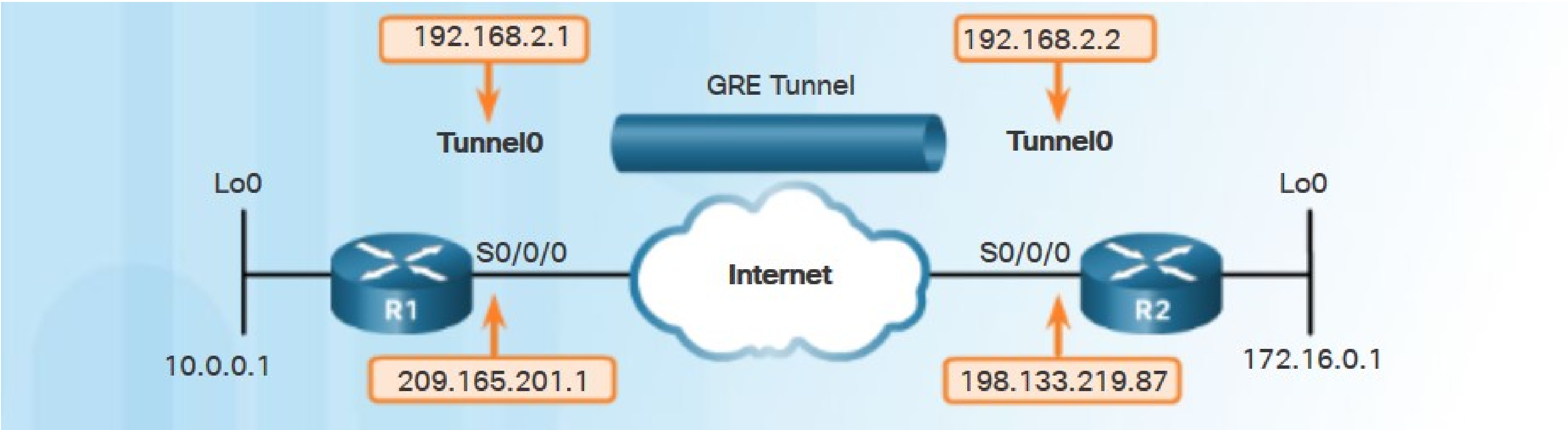
show ip interface brief

show interface Tunnel 0

show ip route

show ip ospf neighbor

GRE Tunnel Verification




```
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#
```

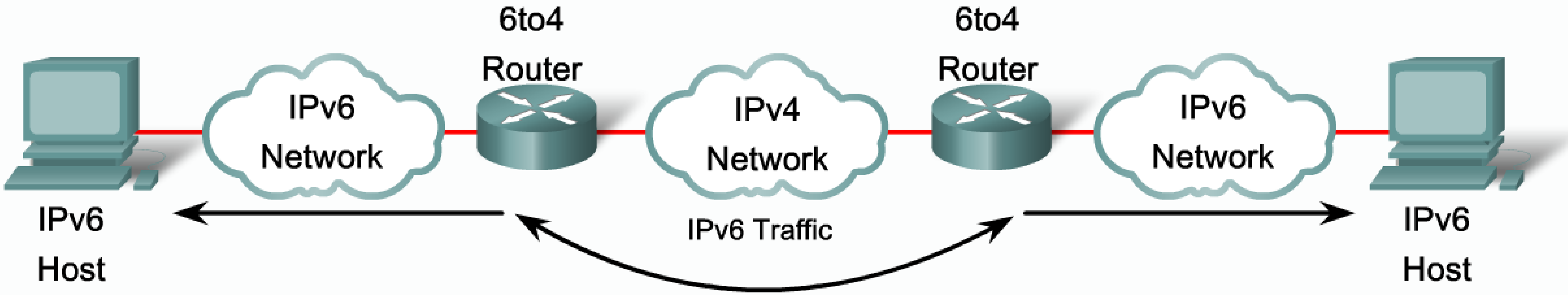
```
R2# show ip interface brief
<output omitted>
Interface              IP-Address      OK? Method Status                Protocol
Serial0/0/0            198.133.219.87  YES manual up                    up
Loopback0              172.16.0.1      YES manual up                    up
Tunnel0             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

3.5 IPv6 Tunneling

Cisco | Networking Academy®
Mind Wide Open™

IPv4 and IPv6 Coexistence

IPv6 Transition Strategies



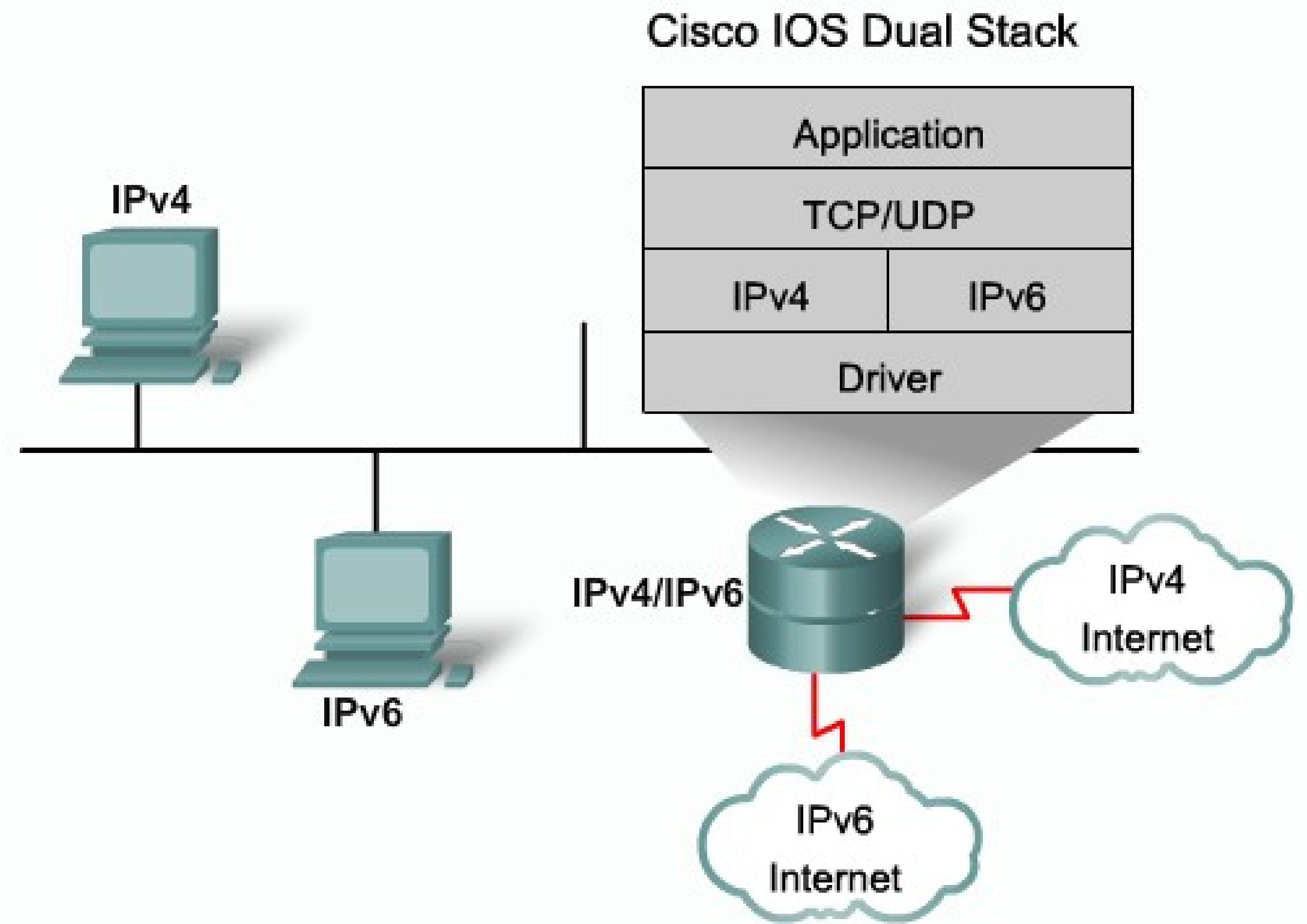
Different transition mechanisms are available:

- Dual stack
- Manual tunnel
- 6to4 tunnel
- ISATAP tunnel
- Teredo tunnel

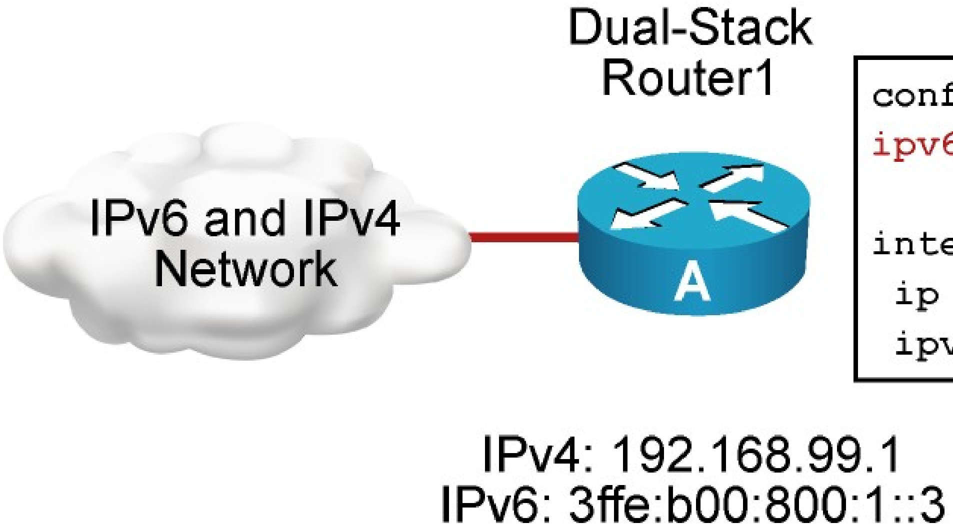
Different compatibility mechanisms:

- Proxying and translation (NAT-PT)

IPv4 and IPv6 Coexistence: Dual-stack



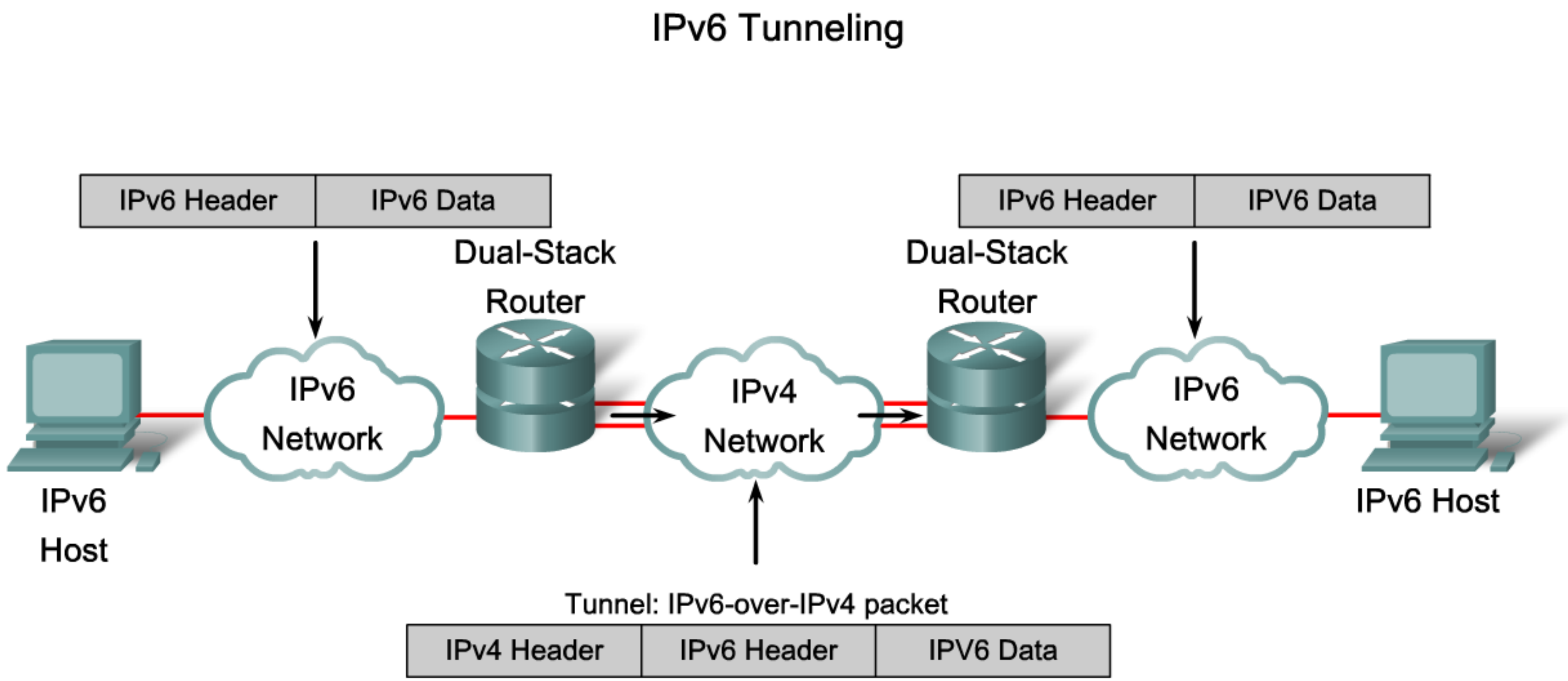
IPv4 and IPv6 Coexistence: Dual-stack




```
conf t
ipv6 unicast-routing

interface ethernet0
 ip address 192.168.99.1 255.255.255.0
 ipv6 address 3ffe:b00:c18:1::3/127
```

014G_013

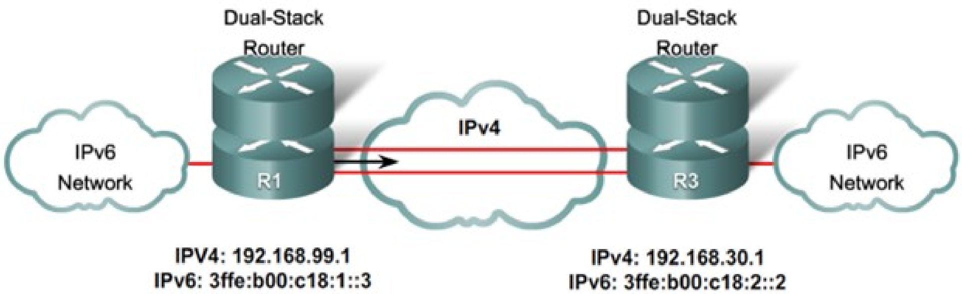
IPv4 and IPv6 Coexistence: Tunneling



Tunneling is an integration method in which an IPv6 packet is encapsulated within another protocol, such as IPv4. This method of encapsulation is IPv4:

- Includes a 20-byte IPv4 header with no options and an IPv6 header and payload
- Requires dual-stack routers

IPv4 and IPv6 Coexistence: Tunneling



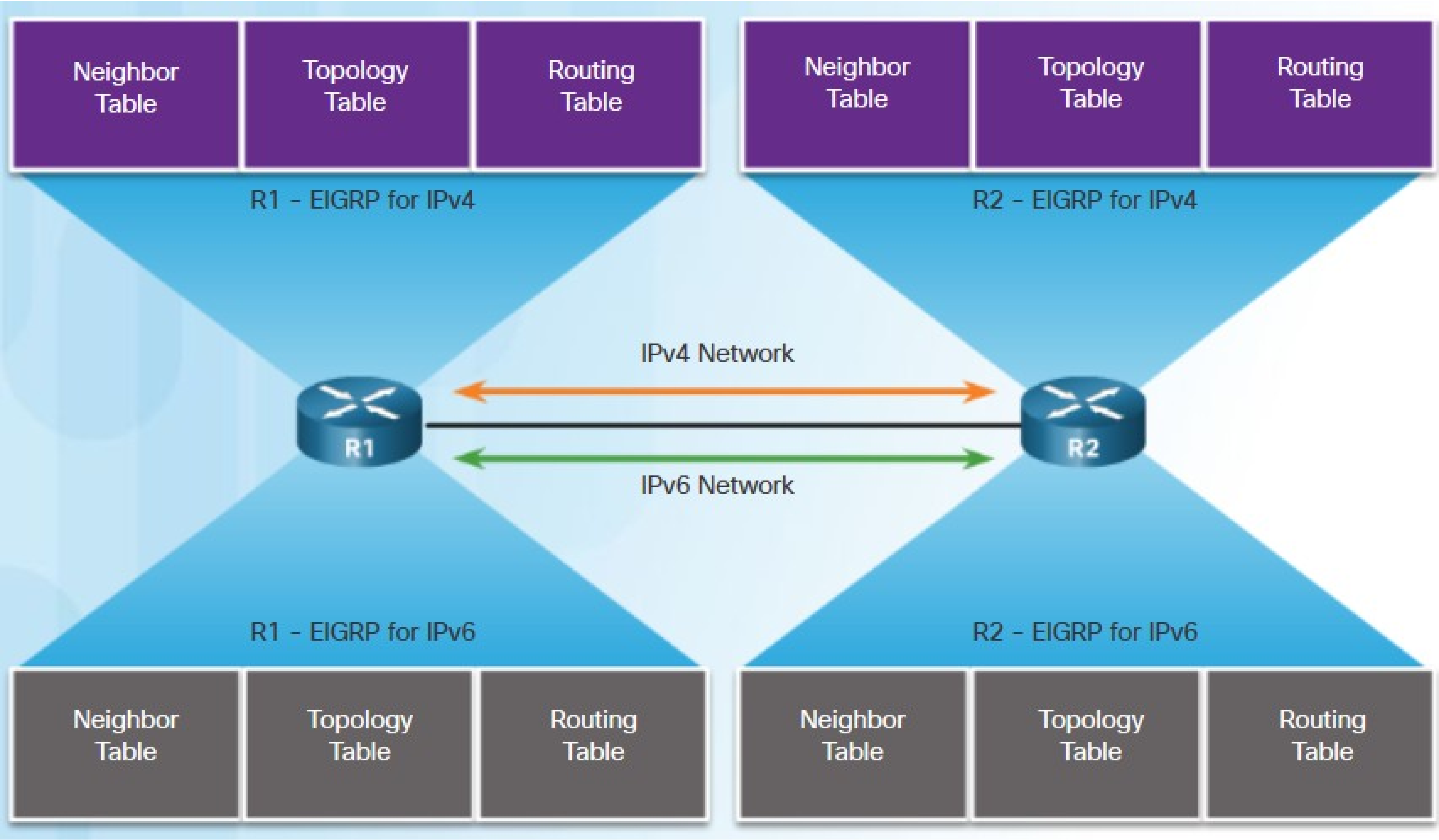
Router R1

```
interface ethernet 0
  ip address 192.168.99.1 255.255.255.0

interface tunnel 0
  ipv6 address 3ffe:b00:c18:1::3/127
  tunnel source ethernet 0
  tunnel destination 192.168.30.1
  tunnel mode ipv6ip
```

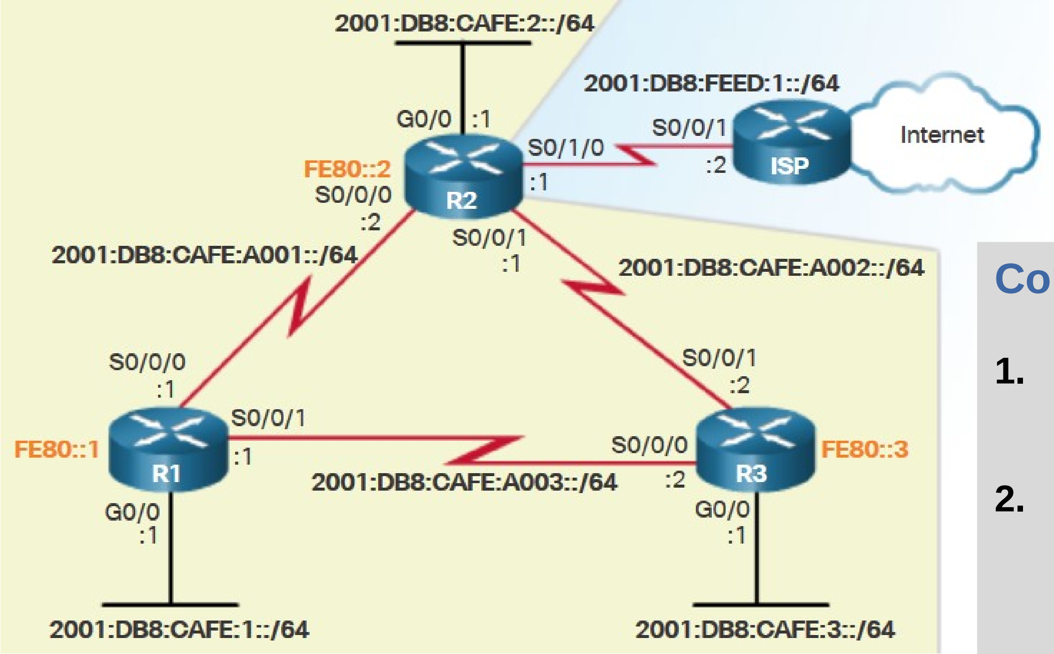
Router R2

```
interface ethernet 0
  ip address 192.168.30.1 255.255.255.0

interface tunnel 0
  ipv6 address 3ffe:b00:c18:1::2/127
  tunnel source ethernet 0
  tunnel destination 192.168.99.1
  tunnel mode ipv6ip
```

IPv6 Routing Using EIGRP



IPv6 Routing Using EIGRP




```
R2(config)# ipv6 unicast-routing
R2(config)# ipv6 router eigrp 2
R2(config-rtr)# eigrp router-id 2.0.0.0
R2(config-rtr)# no shutdown
R2(config-rtr)#
```

```
R2(config)# interface g 0/0
R2(config-if)# ipv6 eigrp 2
R2(config-if)# exit
R2(config)# interface s 0/0/0
R2(config-if)# ipv6 eigrp 2
R2(config-if)# exit
%DUAL-5-NBRCHANGE: EIGRP-IPv6 2: Neighbor FE80::1
 (Serial0/0/0) is up: new adjacency
```

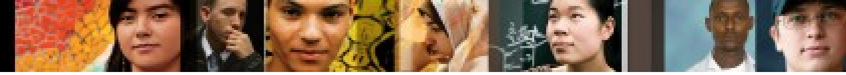
Configuring EIGRP routing for IPv6

1. **Enable IPv6 routing**
   Router(conf)# ipv6 unicast-routing

2. **Configure EIGRP routing process**
   Router(conf)# ipv6 router eigrp <AS>
   Router(conf-rtr)# eigrp router-id <router-ID>
   Router(conf-rtr)# no shutdown

3. **Enable EIGRP for IPv6 on the interface**
   Router(conf)# interface <interface-id>
   Router(conf-if)# ipv6 eigrp <AS>
   Router(conf-rtr)# no shutdown

4. **Verify EIGRP routing**
   Router# show ipv6 eigrp neighbors
   Router# show ipv6 route
   Router# show ipv6 protocols



IPv6 Routing Using RIPng

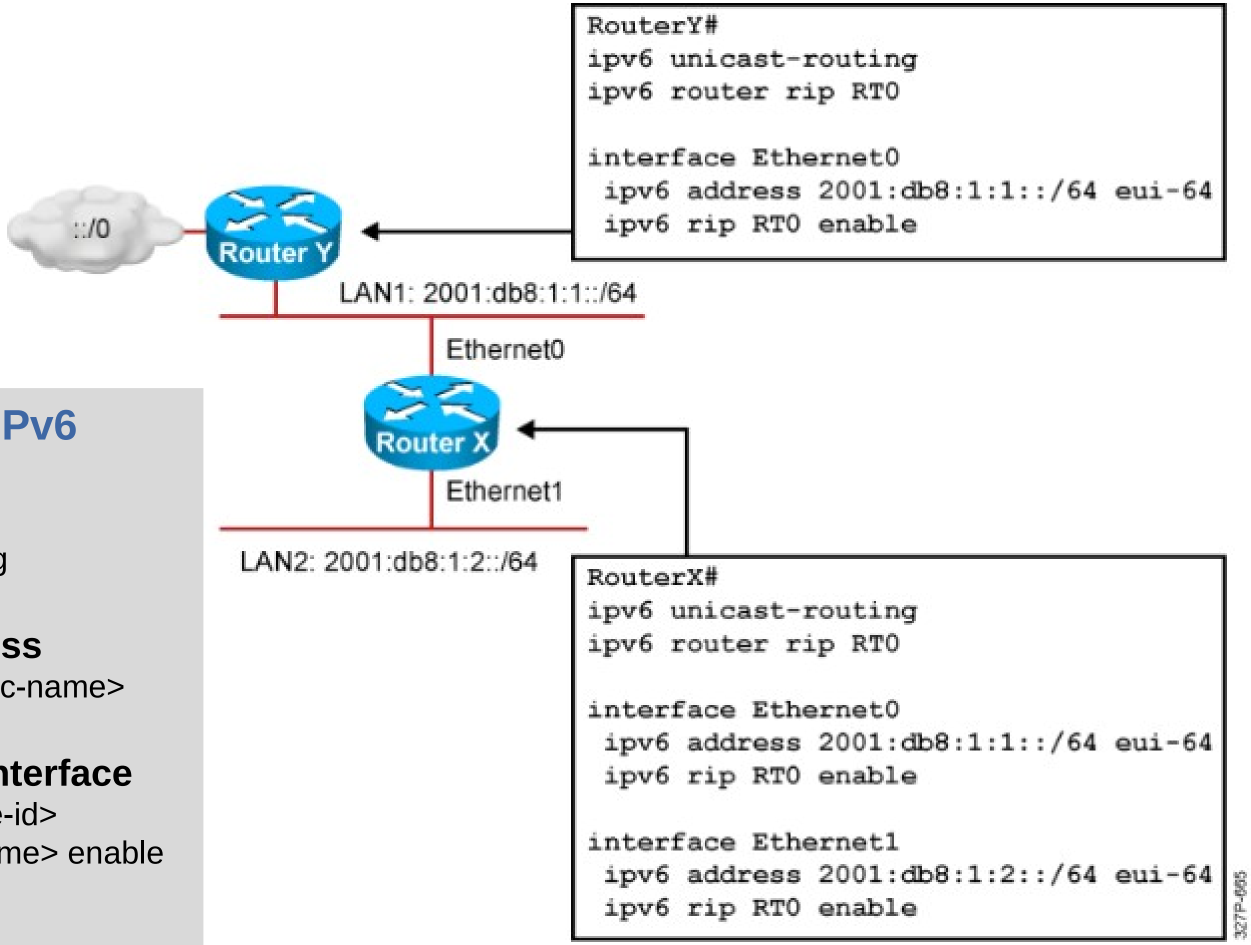
Configuring RIP routing for IPv6

1. **Enable IPv6 routing**
   Router(conf)# ipv6 unicast-routing

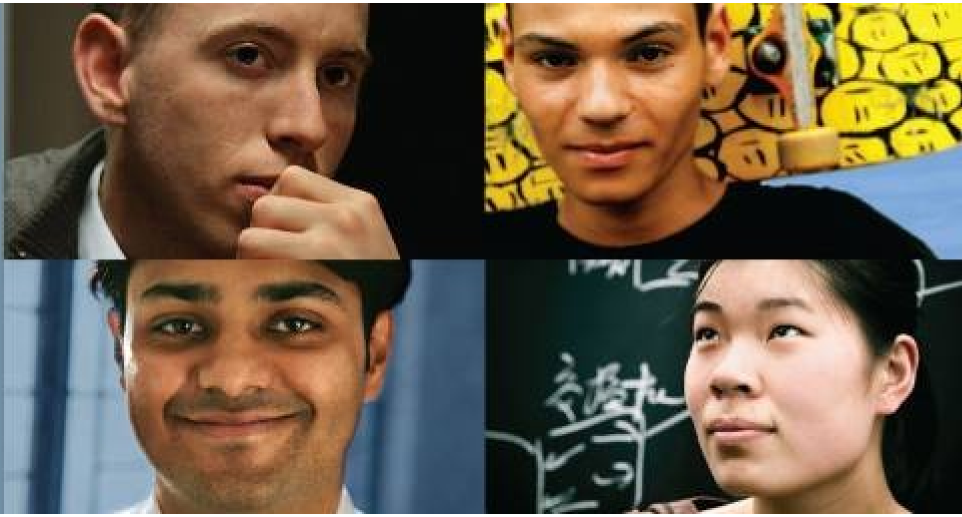
2. **Configure RIP routing process**
   Router(conf)# ipv6 router rip <proc-name>

3. **Enable RIP for IPv6 on the interface**
   Router(conf)# interface <interface-id>
   Router(conf-if)# ipv6 rip <proc-name> enable

4. **Verify EIGRP routing**
   Router# show ipv6 rip database
   Router# show ipv6 route
   Router# show ipv6 protocols

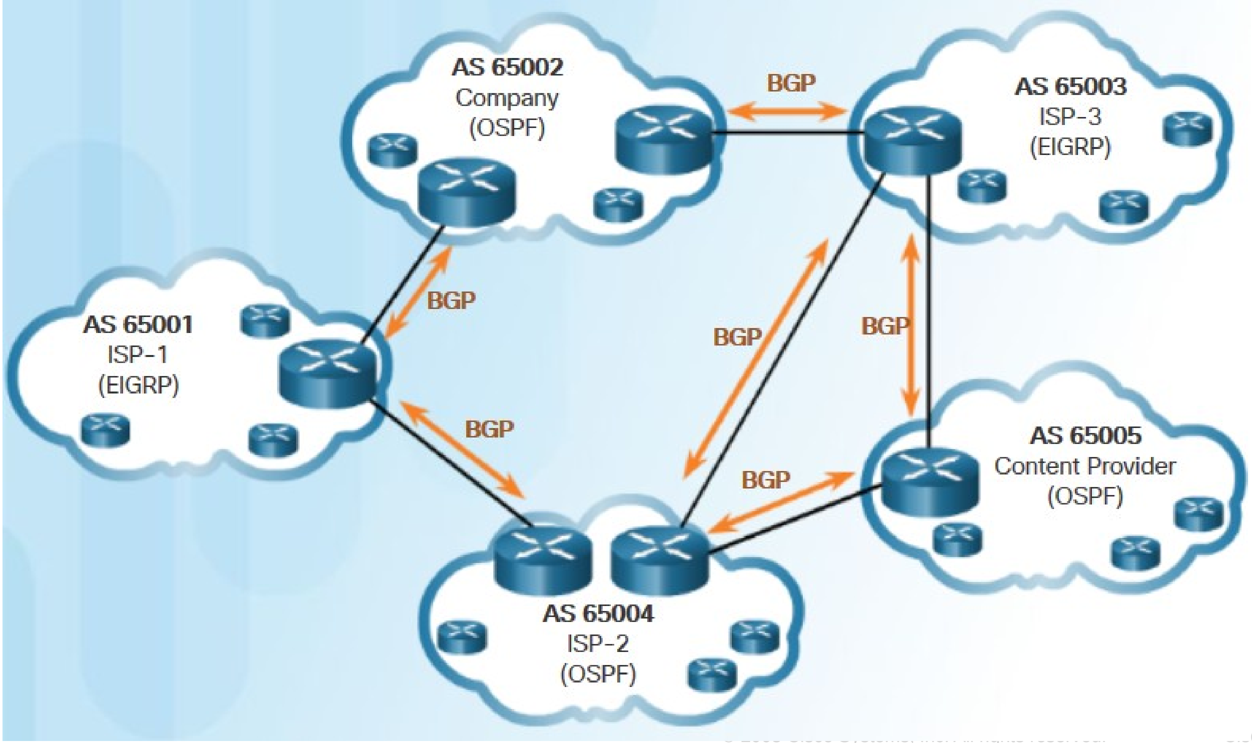


3.6 eBGP



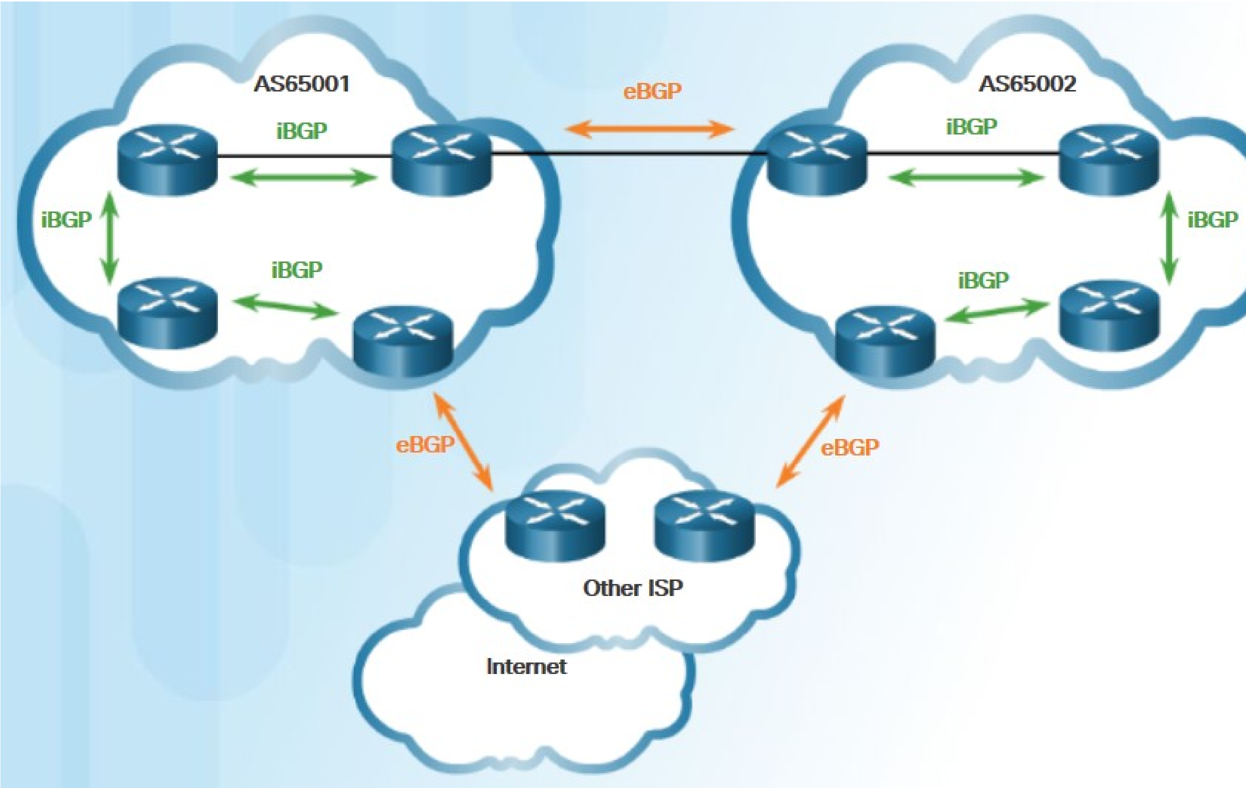
IGP and EGP Routing Protocols

- Interior Gateway Protocols (IGPs)
  - Used to exchange routing information within a company network or an autonomous system (AS).
- Exterior Gateway Protocols (EGPs)
  - Used for the exchange of routing information between autonomous systems.



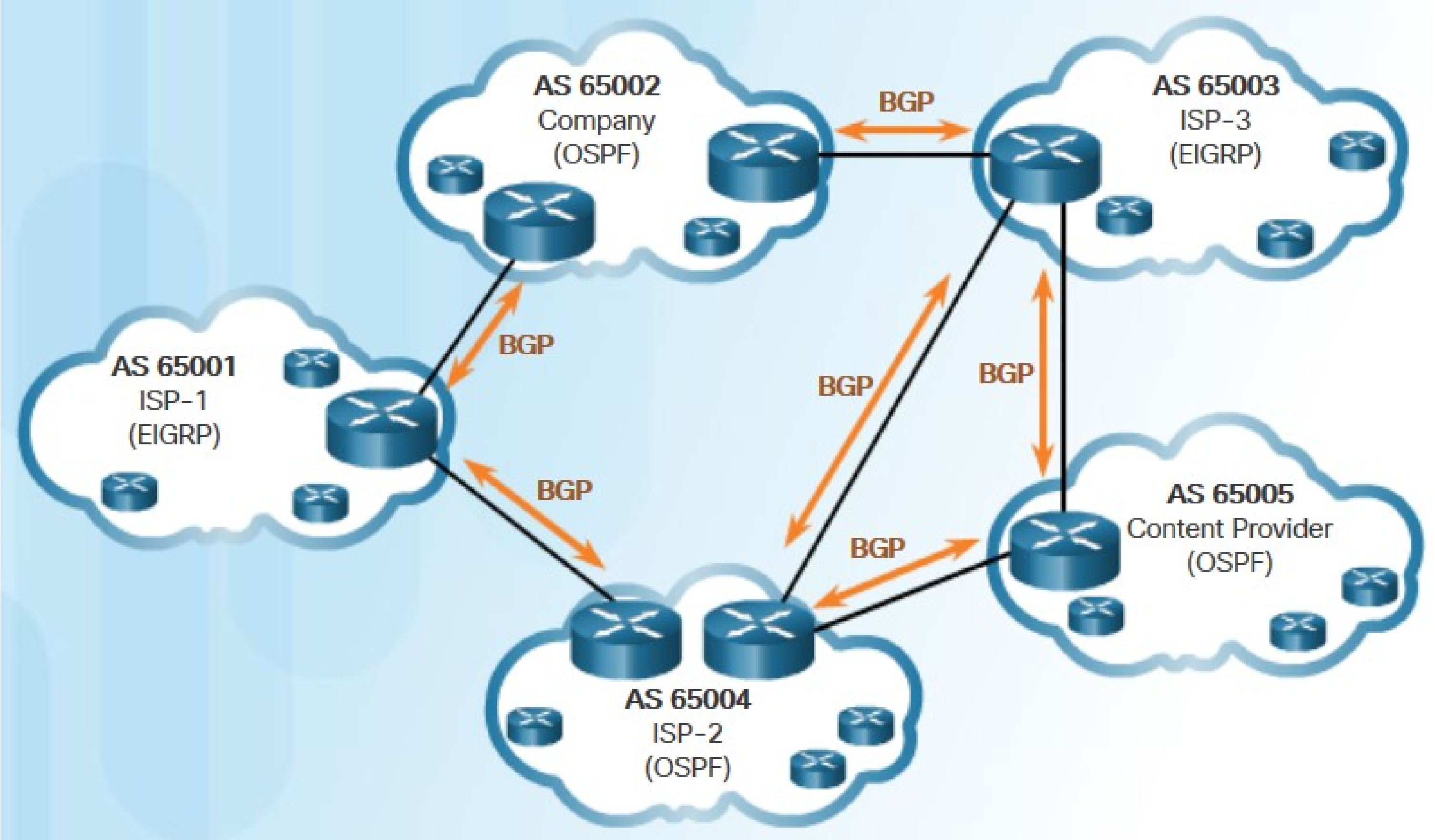
eBGP and iBGP Routing Protocols

- External BGP (eBGP)
  - Routing protocol used between routers in different autonomous systems.
- Internal BGP (iBGP)
  - Routing protocol used between routers in the same AS.



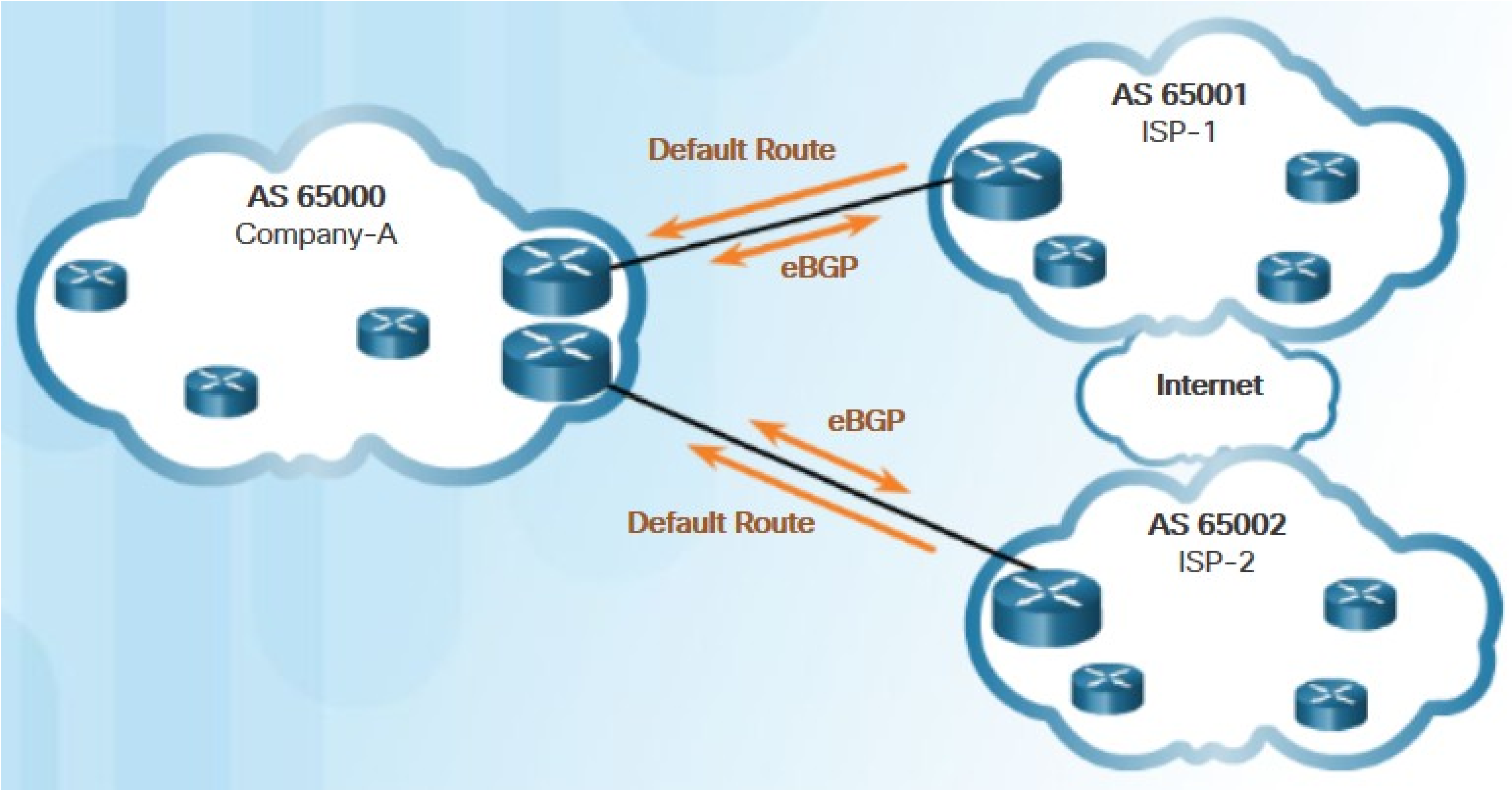
Multi-Homed Connection

- An AS is connected to multiple autonomous systems.
  - Single-homed connection: static route applied.



BPG in multi-homed environment

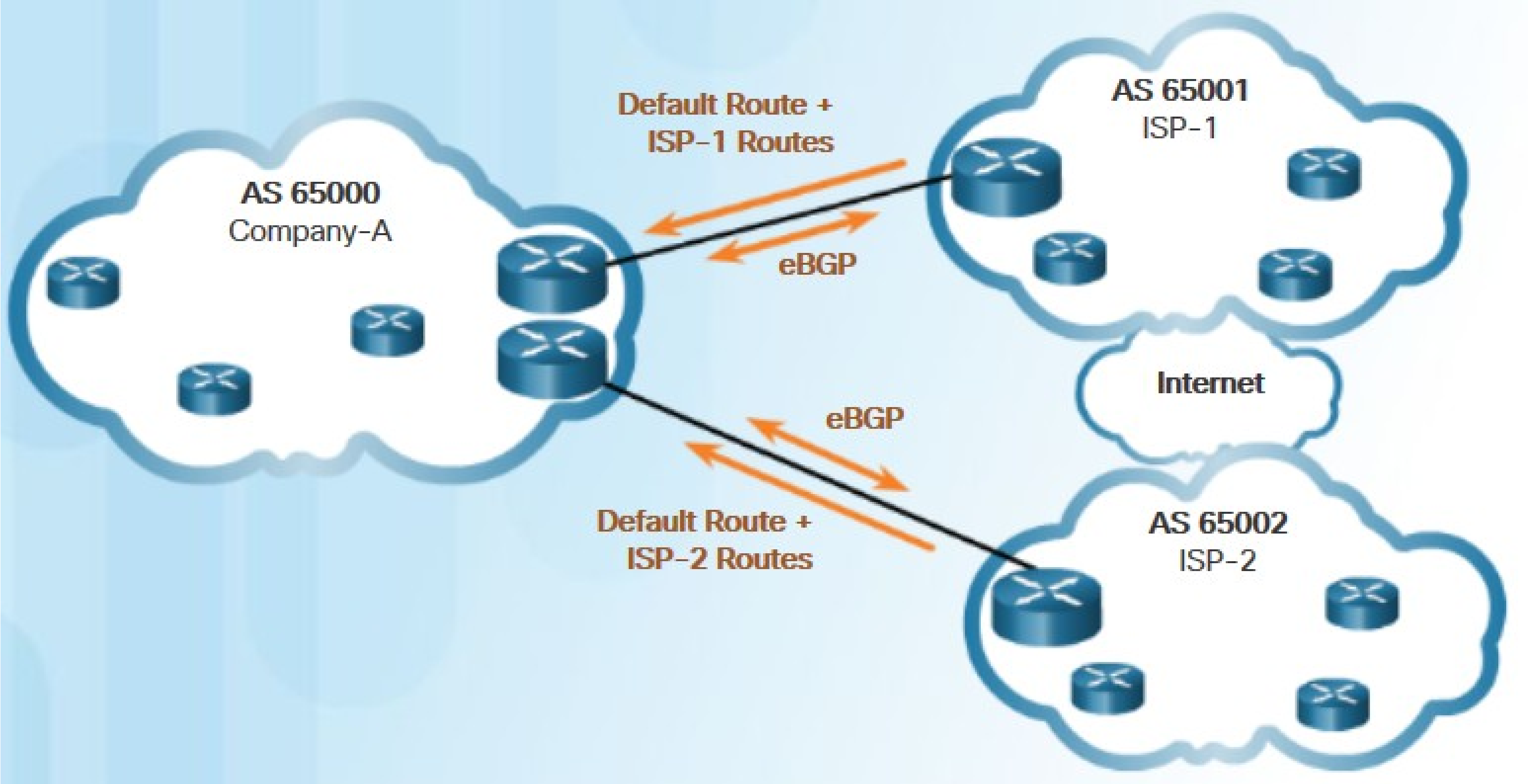
1. **Default Route Only (impractical)**
   - ISPs advertise a default route to a customer.
   - Customer chooses sub-optimal routing.



BPG in multi-homed environment

2. Default Route and ISP Routes

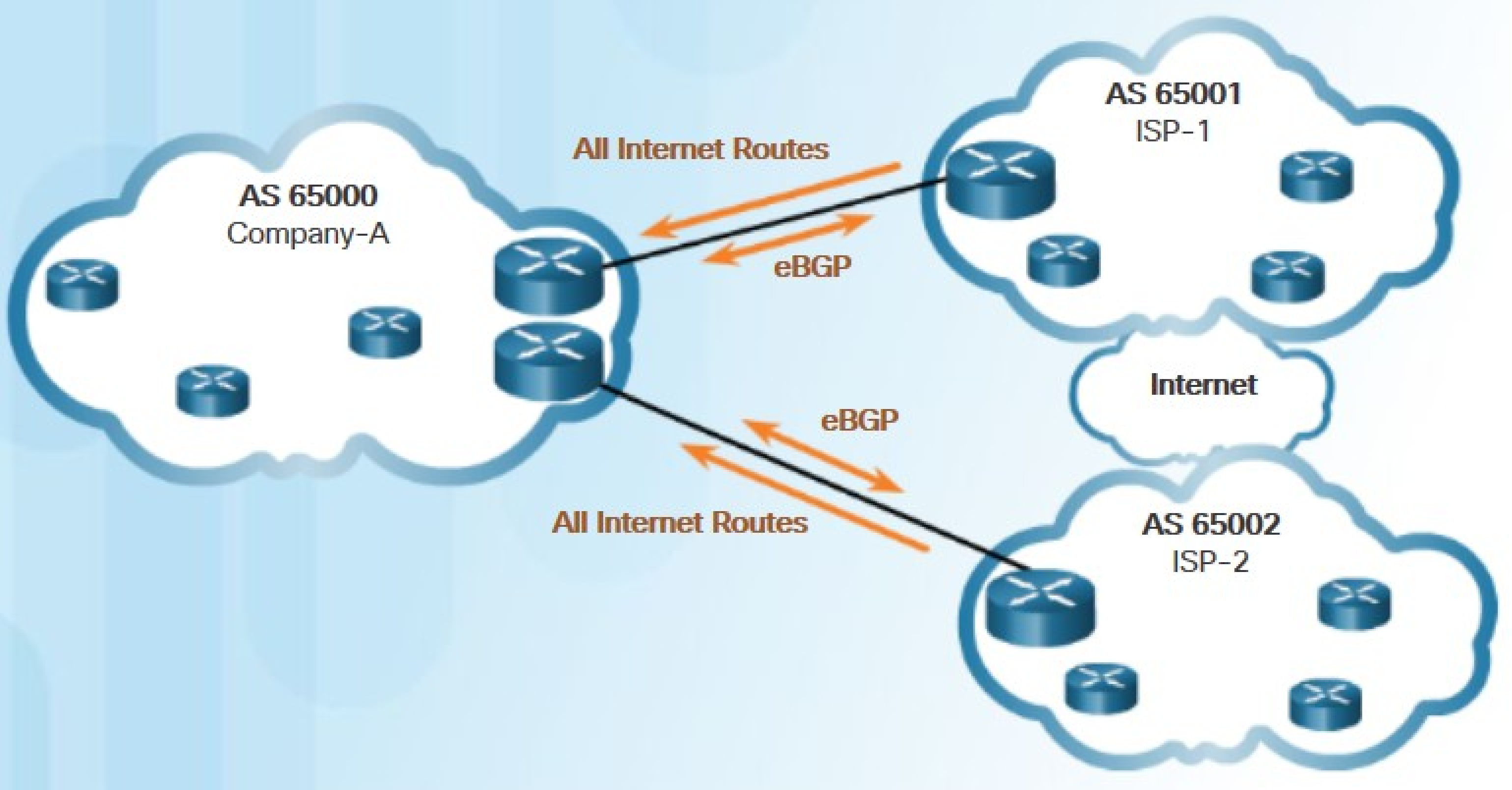
- ISPs advertise a default route and its own networks to a customer.
- For all other networks, customer chooses one of the default networks.



BPG in multi-homed environment

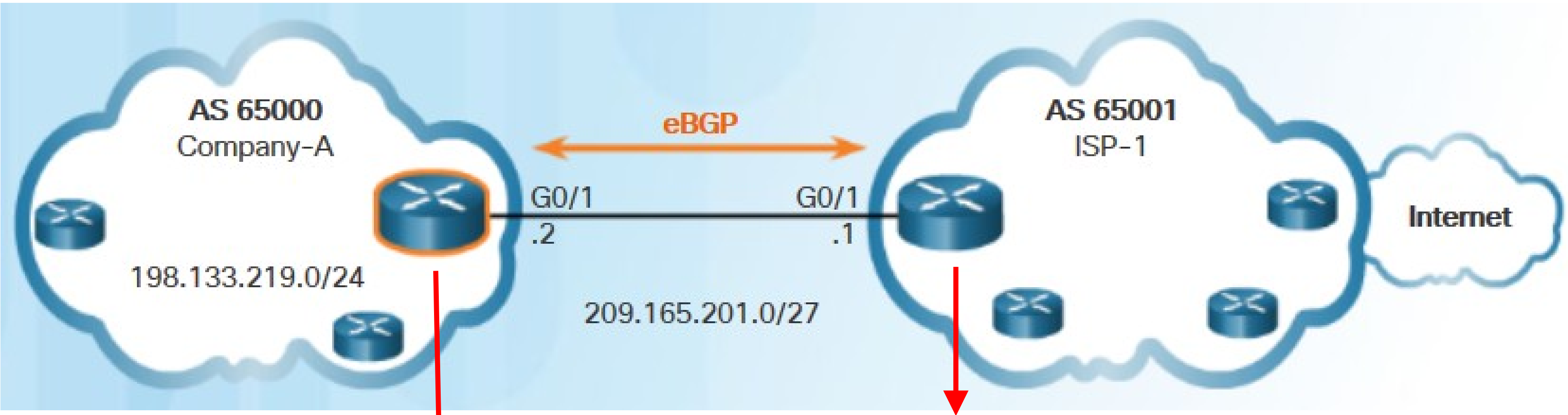
3. All Internet Routes

- ISPs advertise all Internet routes to a customer.
- The customer chooses the best route based on the metric.



BGP Configuration

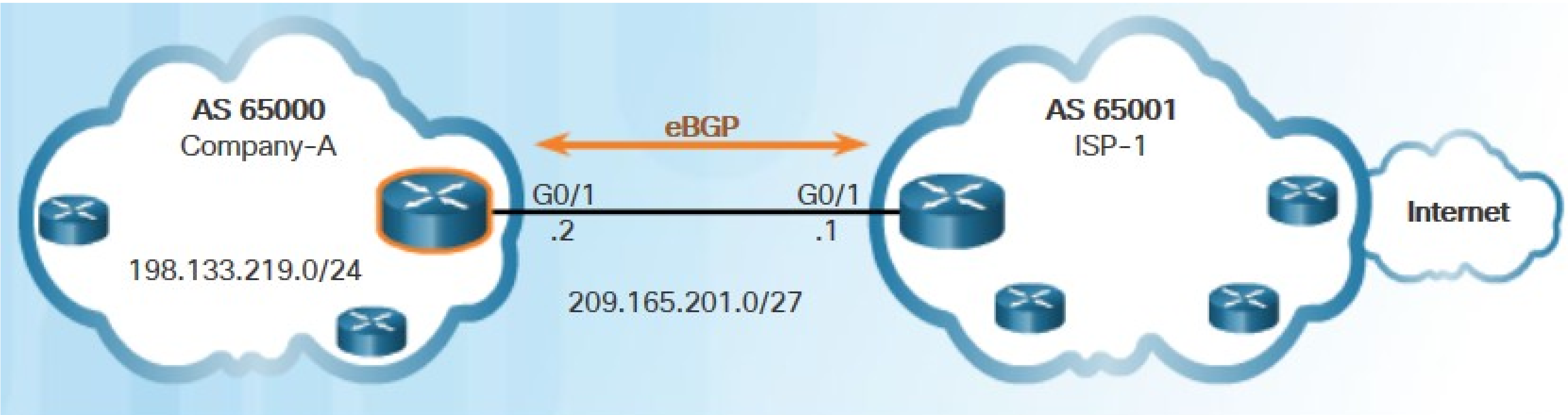
- **Step 1**: Enable BGP routing. # router bgp *AS_NUM*
- **Step 2**: Configure BGP neighbor(s) (peering). # neighbor *IPADDR* remote-as *AS_NUM*
- **Step 3**: Advertise network(s) originating from this AS. # network *IPADDR* mask *MASK*




```
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
```

```
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
```

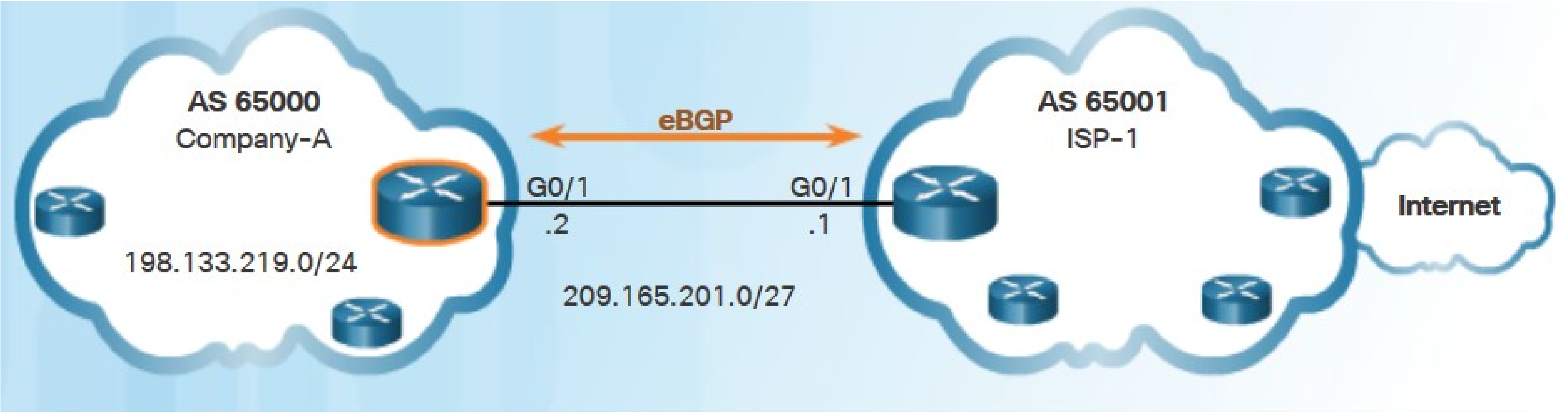
Verify eBGP Configuration




```
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#
```

Show IPv4 routing table: # show ip route

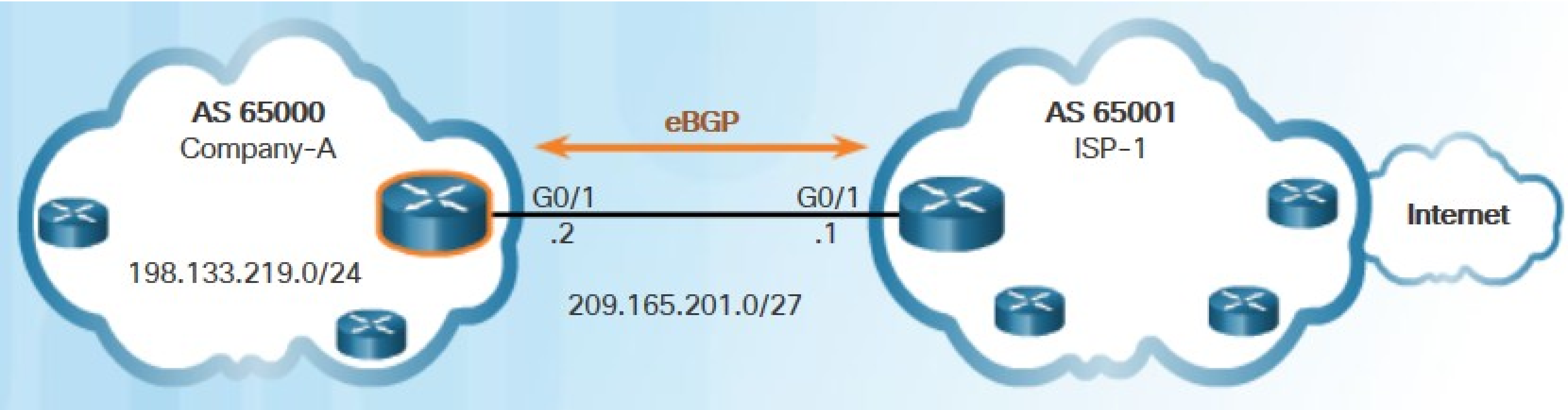
Verify eBGP Configuration




```
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#
```

Show BGP table: # show ip bgp

Verify eBGP Configuration




```
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
```

Show BGP connections: # show ip bgp summary