Chapter 3: Branch Connections

Connecting Networks

Cisco | Networking Academy®
Mind Wide Open™

Chapter 3- Sections & Objectives

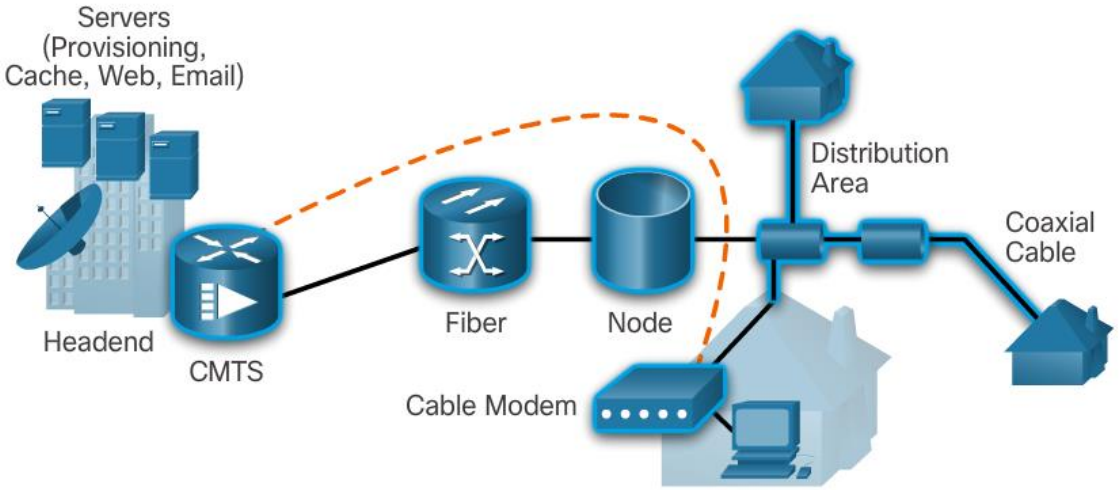
- 3.1 Remote Access Connections
  - Select broadband remote access technologies to support business requirements.
- 3.2 PPPoE
  - Configure a Cisco router with PPPoE.
- 3.3 VPNs
  - Explain how VPNs secure site-to-site and remote access connectivity.
- 3.4 GRE
  - Implement a GRE tunnel.
- 3.5 eBGP
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

3.1 Remote Access Connections

Cisco | Networking Academy®
Mind Wide Open™

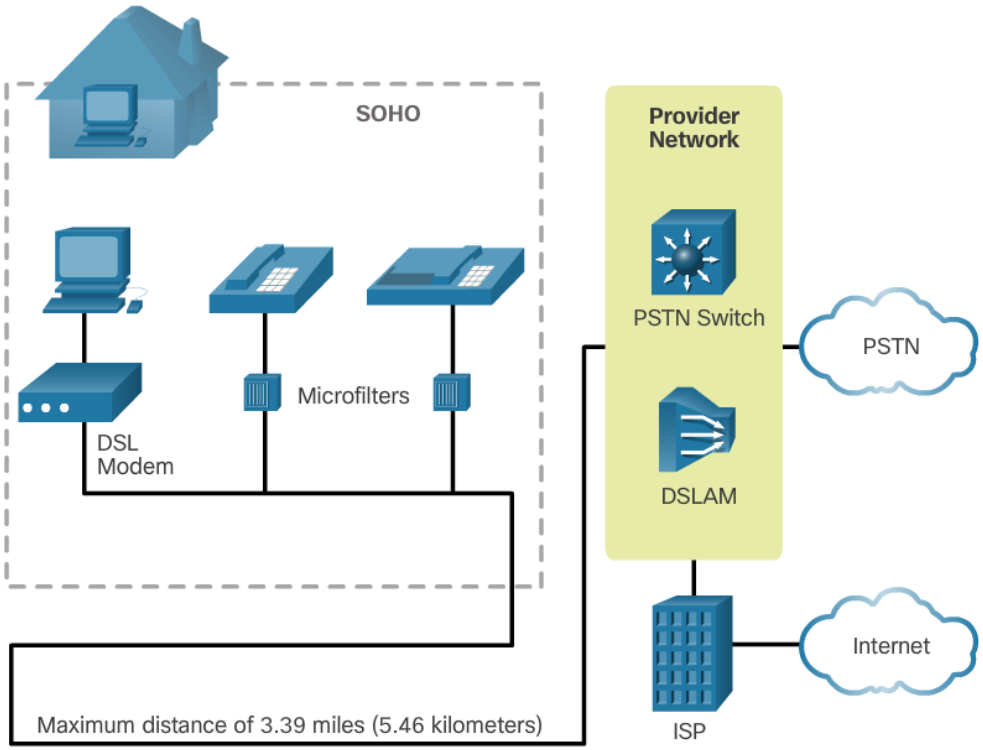
Broadband Connections

- The cable system uses a coaxial cable that carries radio frequency (RF) signals across the network.
- A headend CMTS communicates with CMs located in subscriber homes.
- The HFC network is a mixed optical-coaxial network in which optical fiber replaces the lower bandwidth coaxial cable.



Broadband Connections

- A Digital Subscriber Line (DSL) is a means of providing high-speed connections over installed copper wires.
- The two important components are the DSL transceiver and the DSLAM
- The advantage that DSL has over cable technology is that DSL is not a shared medium. Each user has a separate direct connection to the DSLAM.



Broadband Connections

- Developments in broadband wireless technology are increasing wireless availability through three main technologies:
  - **Municipal Wi-Fi** - Most municipal wireless networks use a mesh of interconnected access points. Each access point is in range and can communicate with at least two other access points. The mesh blankets a particular area with radio signals.
  - **Cellular/mobile** - Mobile phones use radio waves to communicate through nearby cell towers. Cellular/mobile broadband access consists of various standards.
  - **Satellite Internet** - Satellite Internet services are used in locations where land-based Internet access is not available, or for temporary installations that are mobile. Internet access using satellites is available worldwide.

Select a Broadband Connection

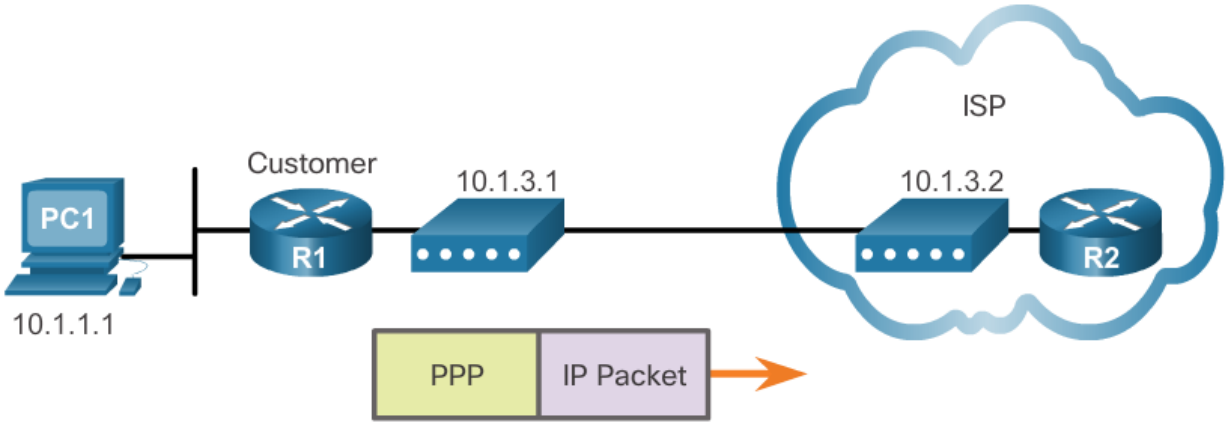
- Each broadband solution has advantages and disadvantages.
- Some factors to consider in making a decision include:
  - **Cable** - Bandwidth is shared by many users, upstream data rates are often slow during high-usage hours in areas with over-subscription.
  - **DSL** - Limited bandwidth that is distance sensitive (in relation to the ISP's central office), upstream rate is proportionally quite small compared to downstream rate.
  - **Fiber-to-the-Home** - Requires fiber installation directly to the home.
  - **Cellular/Mobile** - Coverage is often an issue, even within a SOHO where bandwidth is relatively limited.
  - **Wi-Fi Mesh** - Most municipalities do not have a mesh network deployed; if it is available and the SOHO is in range, then it is a viable option.
  - **Satellite** - Expensive, limited capacity per subscriber; often provides access where no other access is possible.

3.2 Varieties of Spanning Tree Protocols

Cisco | Networking Academy®
Mind Wide Open™

PPPoE Overview

- PPP can be used on all serial links including those links created with dial-up analog and ISDN modems.
  - PPP supports the ability to assign IP addresses to remote ends of a PPP link.
  - PPP supports CHAP authentication.
  - Ethernet links do not natively support PPP. PPP over Ethernet (PPPoE) provides a solution to this problem. PPPoE creates a PPP tunnel over an Ethernet connection.

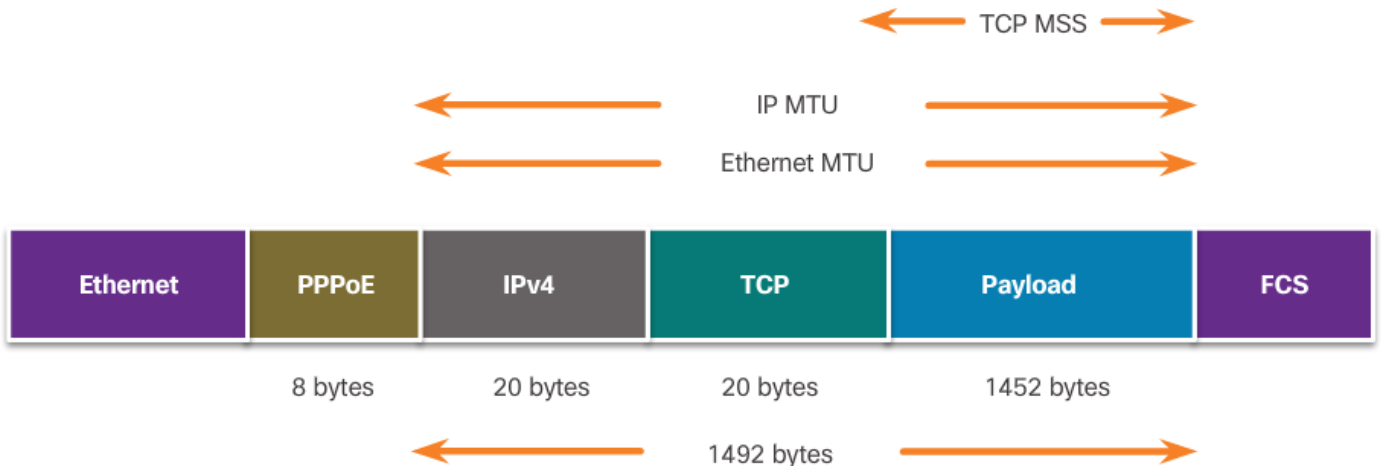


Implement PPPoE

- PPPoE Configuration
  - The dialer interface is created using the **interface dialer** *number* command.
  - The PPP CHAP configuration usually defines one-way authentication; therefore, the ISP authenticates the customer.
  - The physical Ethernet interface that connects to the DSL modem is then enabled with the command **pppoe enable**.
  - The dialer interface is linked to the Ethernet interface with the **dialer pool** and **pppoe-client** commands, using the same number.
  - The maximum transmission unit (MTU) should be set down to 1492, versus the default of 1500, to accommodate the PPPoE headers.
- PPPoE Verification
  - The **show ip interface brief** command is issued to verify the IPv4 address automatically assigned to the dialer interface by the ISP router.
  - The **show interface dialer** command verifies the MTU and PPP encapsulation configured on the dialer interface.
  - The **show pppoe session** command is used to display information about currently active PPPoE sessions.
  - The Ethernet MAC addresses can be verified by using the **show interfaces** command on each router.

Implement PPPoE

- PPPoE Troubleshooting
  - Verify PPP negotiation using the **debug ppp negotiation** command.
  - Re-examine the output of the **debug ppp negotiation** command.
  - PPPoE supports an MTU of only 1492 bytes in order to accommodate the additional 8-byte PPPoE header.
  - The **ip tcp adjust-mss** *max-segment-size* interface command adjusts the MSS value during the TCP 3-way handshake.



3.3 VPNs

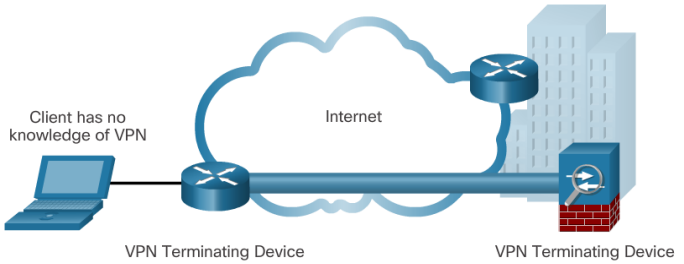
Cisco | Networking Academy®
Mind Wide Open™

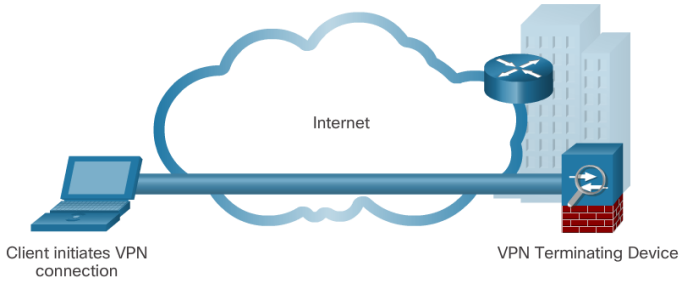
Fundamentals of VPNs

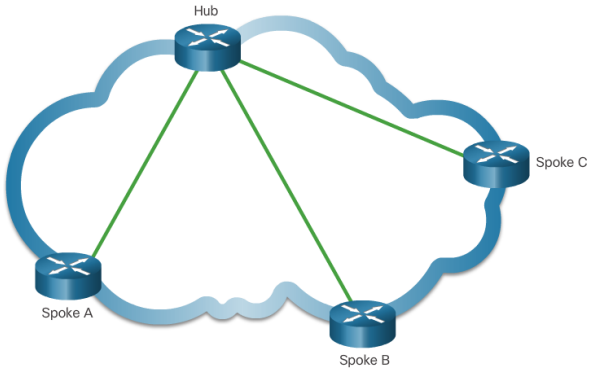
- Introducing VPNs
  - Organizations use VPNs to create an end-to-end private network connection over third-party networks, such as the Internet.
  - Today, a secure implementation of VPN with encryption, such as IPsec VPNs, is what is usually meant by virtual private networking.
  - To implement VPNs, a VPN gateway is necessary. The VPN gateway could be a router, a firewall, or a Cisco Adaptive Security Appliance (ASA).
- Benefits of VPNs
  - Cost savings
  - Scalability
  - Compatibility with broadband technology
  - Security

Types of VPNs

- Site-to-Site
  - Site-to-site VPNs connect entire networks to each other, for example, they can connect a branch office network to a company headquarters network.
- Remote Access
  - Remote-access VPNs are used to connect individual hosts that must access their company network securely over the Internet.
- DMVPN
  - Dynamic Multipoint VPN (DMVPN) is a Cisco software solution for building multiple VPNs in an easy, dynamic, and scalable manner.







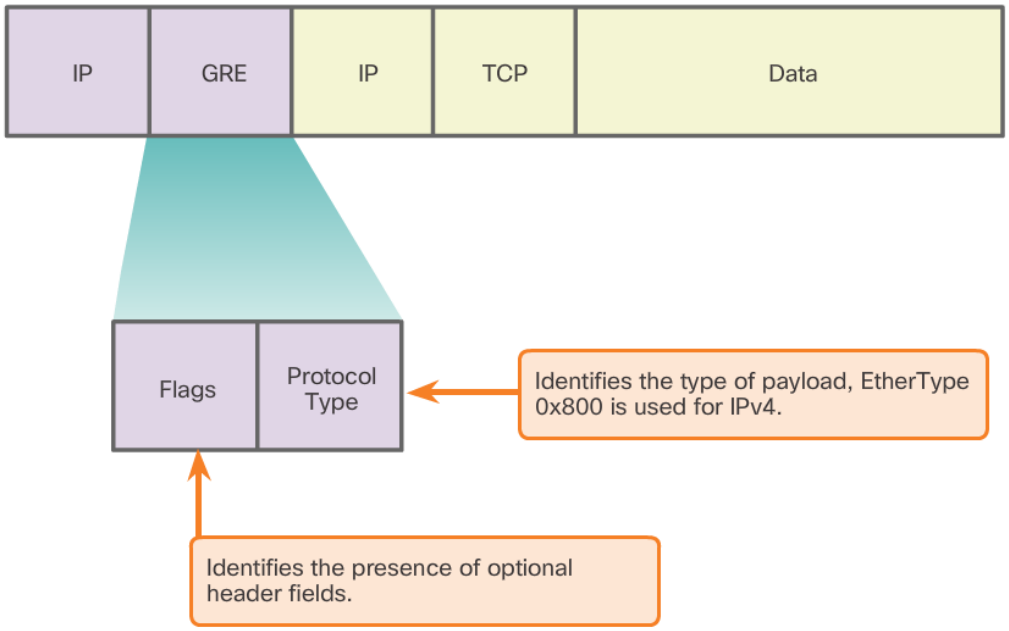
3.4 GRE

Cisco | Networking Academy®
Mind Wide Open™

GRE Overview

- GRE Introduction
  - Generic Routing Encapsulation (GRE) is designed to manage the transportation of multiprotocol and IP multicast traffic between two or more sites, that may only have IP connectivity.

- GRE Characteristics
  - IP tunneling using GRE enables network expansion across a single-protocol backbone environment.



Implement GRE

- There are 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. This is normally a private IP address.
  - **Step 3.** 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.

Command	Description
`tunnel mode gre ip`	Specifies that the mode of the tunnel interface is GRE over IP.
`tunnel source` *ip_address*	Specifies the tunnel source address.
`tunnel destination` *ip_address*	Specifies the tunnel destination address.
`ip address` *ip_address mask*	Specifies the IP address of the tunnel interface.

Implement GRE

- Verify GRE
  - To determine whether the tunnel interface is up or down, use the **show ip interface brief** command.
  - To verify the state of a GRE tunnel, use the **show interface tunnel** command.
  - Verify that an OSPF adjacency has been established over the tunnel interface using the **show ip ospf neighbor** command.
- Troubleshoot GRE
  - Use the **show ip interface brief** command on both routers to verify that the tunnel interface is up and configured with the correct IP addresses for the physical interface and the tunnel interface.
  - Use the **show ip ospf neighbor** command to verify neighbor adjacency.
  - Use **show ip route** to verify that networks are being passed between the two routers

3.5 eBGP

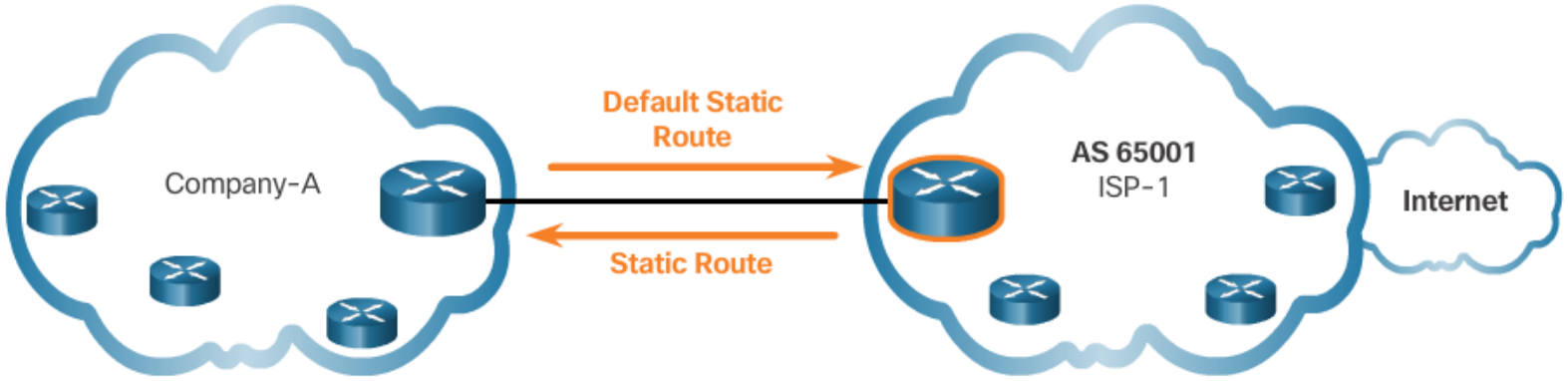
Cisco | Networking Academy®
Mind Wide Open™

BGP Overview

- IGP and EGP
  - Interior Gateway Protocols (IGPs) are used to exchange routing information within a company network or an autonomous system (AS).
  - Exterior Gateway Protocols (EGPs) are used for the exchange of routing information between autonomous systems.
- eBGP and iBGP
  - External BGP (eBGP) is the routing protocol used between routers in different autonomous systems.
  - Internal BGP (iBGP) is the routing protocol used between routers in the same AS.
- This course focuses on eBGP only.

BGP Design Considerations

- When to use BGP
  - The use of BGP is most appropriate when an AS has connections to multiple autonomous systems.
  - BGP should not be used when at least one of the following conditions exist:
    - There is a single connection to the Internet or another AS. This is known as single-homed.
    - When there is a limited understanding of BGP.



BGP Design Considerations

- BGP Options
  - There are three common ways an organization can choose to implement BGP in a multi-homed environment:
    - Default Route Only - This is the simplest method to implement BGP. However, because the company only receives a default route from both ISPs, sub-optimal routing may occur.
    - Default Route and ISP Routes - This option allows Company-A to forward traffic to the appropriate ISP for networks advertised by that ISP.
    - All Internet Routes - Because Company-A receives all Internet routes from both ISPs, Company-A can determine which ISP to use as the best path to forward traffic for any network. Although this solves the issue of sub-optimal routing, the Company-A's BGP router must contain all Internet routes.

BGP Branch Configuration

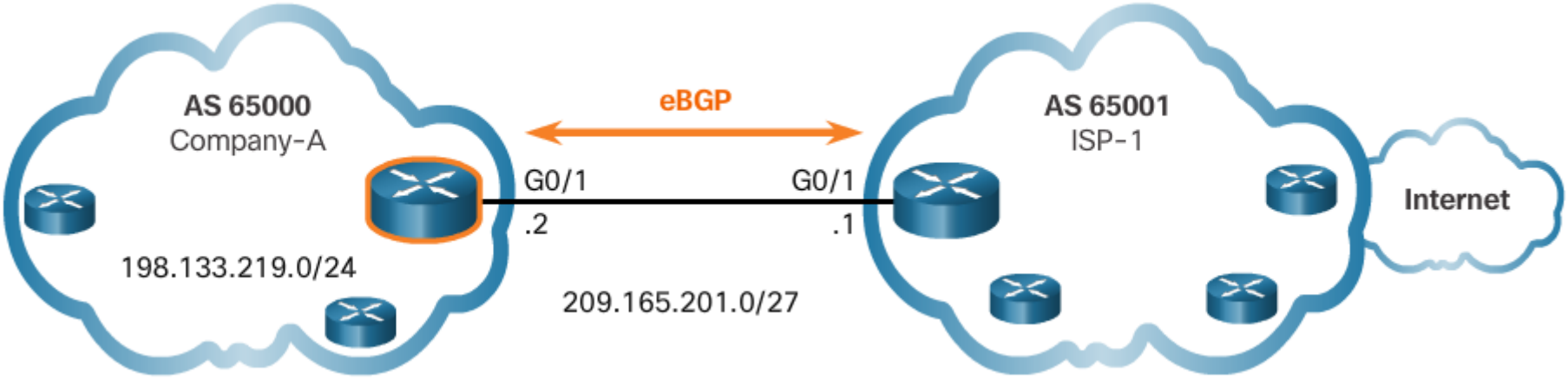
- BGP Configuration Commands
  - There are three steps to implement eBGP:
    - **Step 1**: Enable BGP routing.
    - **Step 2**: Configure BGP neighbor(s) (peering).
    - **Step 3**: Advertise network(s) originating from this AS.

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 Branch Configuration

- Verify eBGP
  - Three commands can be used to verify eBGP

Command	Description
`Router# show ip route`	Verify routes advertised by the BGP neighbor are present in the IPv4 routing table.
`Router# show ip bgp`	Verify that received and advertised IPv4 networks are in the BGP table.
`Router# show ip bgp summary`	Verify IPv4 BGP neighbors and other BGP information.



3.6 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

Summary

- Broadband transmission is provided by a wide range of technologies, including DSL, fiber-to-the-home, coaxial cable systems, wireless, and satellite. This transmission requires additional components at the home end and at the corporate end. Broadband wireless solutions include municipal Wi-Fi, cellular/mobile, and satellite Internet. Municipal Wi-Fi mesh networks are not widely deployed. Cellular/mobile coverage can be limited and bandwidth can be an issue. Satellite Internet is relatively expensive and limited, but it may be the only method to provide access.
- If multiple broadband connections are available to a particular location, a cost-benefit analysis should be performed to determine the best solution. The best solution may be to connect to multiple service providers to provide redundancy and reliability.
- PPPoE is a popular data link protocol for connecting remote networks to their ISPs. PPPoE provides the flexibility of PPP and the convenience of Ethernet.

Summary Continued

- VPNs are used to create a secure end-to-end private network connection over a third party network, such as the Internet. 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.
- BGP is the routing protocol implemented between autonomous systems. Three basic design options for eBGP are as follows:
- The ISP advertises a default route only to the customer
- The ISP advertises a default route and all of its routes to the customer.
- The ISP advertises all Internet routes to the customer.
- Implementing eBGP in a single-homed network only requires a few commands.