CHAPTER 1

WAN Concepts

Wide-area networks (WANs) are used to connect remote LANs together. Various technologies are used to achieve this connection. This chapter reviews WAN technologies and the many WAN services available.

WAN Technologies Overview

WAN access options differ in technology, speed, and price. Each has advantages and disadvantages. Selecting the best technology depends largely on the network design.

Network Types and Their Evolving WAN Needs

The WAN needs of a network depend greatly on the size of the network. These network types run the spectrum from small offices that really need only a broadband connection to the Internet, all the way up to multinational enterprises that need a variety of WAN options to satisfy local, regional, and global restrictions.

In Table 1-1, indicate the network type that fits each of the descriptions. Some descriptions may apply to more than one network type.

Table 1-1 Identify the Network Type

Network Description	Small Office Network	Campus Network	Branch Network	Distributed Network
Outsourced IT support				
Very large-sized business				
Connectivity to the Internet				
Converged network and application services				
Hundreds of employees				
Home, branch, and regional offices, teleworkers, and a central office				
Limited number of employees				
In-house IT staff and network support				
Thousands of employees				
Several remote, branch, and regional offices (one central office)				
Small-sized business				
LAN focus of operations with broadband				
Small to medium-sized business				
Multiple campus LANs				
Medium-sized business				

WAN Operations and Terminology

WANs operate at which layers of the OSI model?

_____

Which organizations are responsible for WAN standards?

_____

_____

_____

What are some of the Layer 2 WAN technologies?

_____

Why is the Layer 2 address field not usually used in WAN services?

_____

Match the definition on the left with a term on the right. This exercise is a one-to-one matching.

Definitions

a. The boundary between customer equipment and service provider equipment

b. Devices inside the enterprise edge wiring closet that are owned or leased by the organization

c. Provider equipment that resides in the WAN backbone capable of supporting routing protocols

d. Digital modem used by DSL or cable Internet service providers

e. Dynamically establishes a dedicated circuit before communication starts

f. Provides an interface to connect subscribers to a WAN link

g. Splits traffic so that it can be routed over the shared network

h. Local service provider facility that connects the CPE to the provider network

i. Physical connection between the CPE and the CO

j. Required by digital leased lines to provide termination of the digital signal and convert into frames ready for transmission on the LAN

k. Consists of the all-digital, long-haul communications lines, switches, routers, and other equipment in the provider network

l. Customer device that provides internetworking and WAN access interface ports

m. Customer device that transmits data over the WAN link

n. Multiport device that sits at the service provider edge to switch traffic

o. Legacy technology device that converts digital signals into analog signals transmitted over telephone lines

p. Legacy technology device that can support hundreds of dial-in and dial-out users

Terms

___ Packet-switched network

___ WAN switch

___ Customer premises equipment (CPE)

___ Central office (CO)

___ Dialup modem

___ Access server

___ Data communications equipment (DCE)

___ Router

___ Data terminal equipment (DTE)

___ Local loop

___ CSU/DSU

___ Circuit-switched network

___ Demarcation point

___ Broadband modem

___ Toll network

___ Core multilayer switch

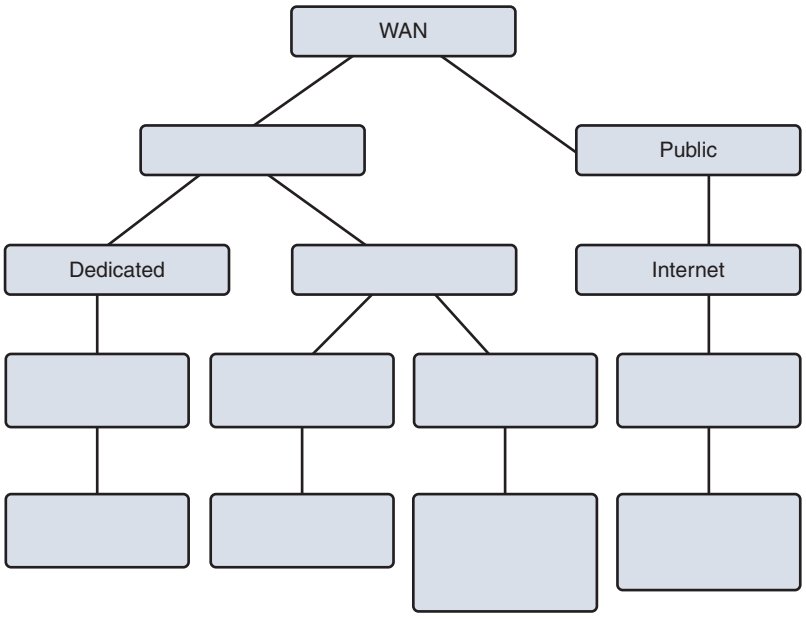
Selecting a WAN Technology

The WAN access connections your small to medium-sized business purchases could use a public or private WAN infrastructure—or a mix of both. Each type provides various WAN technologies. Understanding which WAN access connections and technologies are best suited to your situation is an important part of network design.

Varieties of WAN Link Connections

Your ISP can recommend several WAN link connection options based on your specific requirements. These options can be classified in various categories. Use the list of WAN access options to label Figure 1-1.

Figure 1-1 WAN Access Options Labels



T1/E1/T3/E3	ATM	Switched
Frame Relay	Circuit switched	Packet switched
Metro Ethernet	Cable	Wireless
MPLS	PSTN	DSL
VPN	Private	Broadband
ISDN	Leased lines	

Private and Public WAN Access Options

As shown in Figure 1-1, WAN access options can first be classified as either private or public. Table 1-2 lists descriptions for various private WAN access options. Indicate which one is described. Some options are described more than once.

Table 1-2 Private WAN Access Options

Private WAN Access Options	Leased Lines	MPLS	Metro Ethernet	ATM	ISDN	VSAT	Dialup	Frame Relay
Considered the most expensive of all WAN access technologies.								
Analog telephone lines are used to provide a switched WAN connection.								
A permanent, dedicated WAN connection that uses a T- or E-carrier system.								
Satellite to router communications for WAN connections.								
Delivers data using fixed 53-byte packet cells over permanent and switched virtual circuits.								
Service providers and short-path labeling are used for leased lines, Ethernet WANs, and Frame Relay WANs.								
Connects multiple sites using virtual circuits and data link connection identifiers.								
Includes MetroE, EoMPLS, and VPLS as WAN connection options.								
Converts analog to digital signals to provide a switched WAN connection over telephone lines.								
A popular replacement for traditional Frame Relay and ATM WAN access technologies.								

Match the definition on the left with a public WAN access option on the right. This exercise is a one-to-one matching.

Definitions

a. Radio and directional-antenna modem WAN access option provided to public organizations

b. WAN access option that uses telephone lines to transport data via multiplexed links

c. High-speed long-distance wireless connections through nearby special service provider towers

d. Cellular radio waves WAN access option used with smartphones and tablets

e. Dish and modem-based WAN access option for rural users where cable and DSL are not available

f. Secure Internet-based WAN access option used by teleworkers and extranet users

g. Entire networks connected together by using VPN routers, firewalls, and security appliances

h. A shared WAN access option that transports data using television-signal networks

Public WAN Access Options

___ 3G/4G Cellular

___ VPN Remote

___ WiMax

___ Satellite Internet

___ DSL

___ Cable

___ Municipal WiFi

___ VPN site-to-site

Labs and Activities

There are no Labs or Packet Tracer Activities in this chapter.

1.0.1.2 Class Activity–Branching Out

Objective

Describe WAN access technologies available to small-to-medium-sized business networks.

Scenario

Your medium-sized company is opening a new branch office to serve a wider, client-based network. This branch will focus on regular, day-to-day network operations, but will also provide TelePresence, web conferencing, IP telephony, video on demand, and wireless services.

Although you know that an ISP can provide WAN routers and switches to accommodate the branch office connectivity for the network, you prefer to use your own customer premises equipment (CPE). To ensure interoperability, Cisco devices have been used in all other branch-office WANs.

As the branch-office network administrator, it is your responsibility to research possible network devices for purchase and use over the WAN.

Resources

- World Wide Web
- Word processing software

Step 1. Visit the Cisco Branch-WAN Business Calculator site. Accept the agreement to use the calculator.

Step 2. Select the IT Infrastructure Requirements Tab.

Step 3. Input information to help the calculator determine a preferred router or ISR option for your branch and WAN (both).

Note: There is a slider tool within the calculator window that allows the choice of more service options for your branch office and WAN.

Step 4. The calculator will suggest a possible router or ISR device solution for your branch office and WAN. Use the tabs at the top of the calculator window to view the output.

Step 5. Create a matrix with three column headings and list some information provided by the output in each category:

- Return on investment (ROI)
- Total cost of ownership (TCO)
- Energy savings

Step 6. Discuss your research with a classmate, group, class, or your instructor. Include in your discussion:

- Specifics on the requirements of your network as used for calculator input
- Output information from your matrix
- Additional factors you would consider before purchasing a router or ISR for your new branch office

1.2.4.3 Lab–Researching WAN Technologies

Objectives

Part 1: Investigate Dedicated WAN Technologies and Providers

Part 2: Investigate a Dedicated Leased Line Service Provider in Your Area

Background/Scenario

Today's broadband Internet services are fast and affordable. With the use of VPN technology, the connection can also be secure. However, many companies still need a 24-hour dedicated connection to the Internet, or a dedicated point-to-point connection from one office location to another. In this lab, you will investigate the cost and availability of purchasing a dedicated T1 Internet connection for your home or business.

Required Resources

A device with Internet access.

Part 1: Investigate Dedicated WAN Technologies and Providers

In Step 1, you will research basic characteristics of dedicated WAN technologies, and in Step 2, you will discover providers that offer dedicated WAN services.

Step 1. Research WAN technology characteristics.

Use search engines and websites to research the following WAN technologies. Put your findings in the table below.

		Last Mile Media			
WAN Technology	**Dedicated Connection (yes/no)**	**Copper (yes/no)**	**Fiber (yes/no)**	**Wireless (yes/no)**	**Speed/Range**
T1/DS1					
T3/DS3					
OC3 (SONET)					
Frame Relay					
ATM					
MPLS					
EPL (Ethernet Private Line)					

Step 2. Discover dedicated WAN technology service providers.

Navigate to http://www.telarus.com/carriers.html. This web page lists the Internet service providers (also known as carriers) that partner with Telarus to provide automated real-time telecom pricing. Click the links to the various carrier partners and search for the dedicated WAN technologies that they provide. Complete the table below by identifying each service provider's dedicated WAN services, based on the information provided on the website. Use the extra lines provided in the table to record additional service providers.

Internet Service Provider	T1/DS1/PRI	T3/DS3	OC3 (SONET)	Frame Relay	ATM	MPLS	EPL Ethernet Private Line
Comcast							x
CenturyLink	x	x				x	
AT&T							
Earthlink							
Level 3 Communications							
XO Communications							
Verizon							

Part 2: Investigate a Dedicated Leased Line Service Provider in Your Area

In Part 2, you will research a local service provider that will provide a T1 dedicated leased line to the geographical area specified. This application requires a name, address, and phone number before the search can be performed. You may wish to use your current information or research an address locally where a business might be looking for a WAN connection.

Step 1. Navigate to http://www.telarus.com/geoquote.html to try GeoQuote.

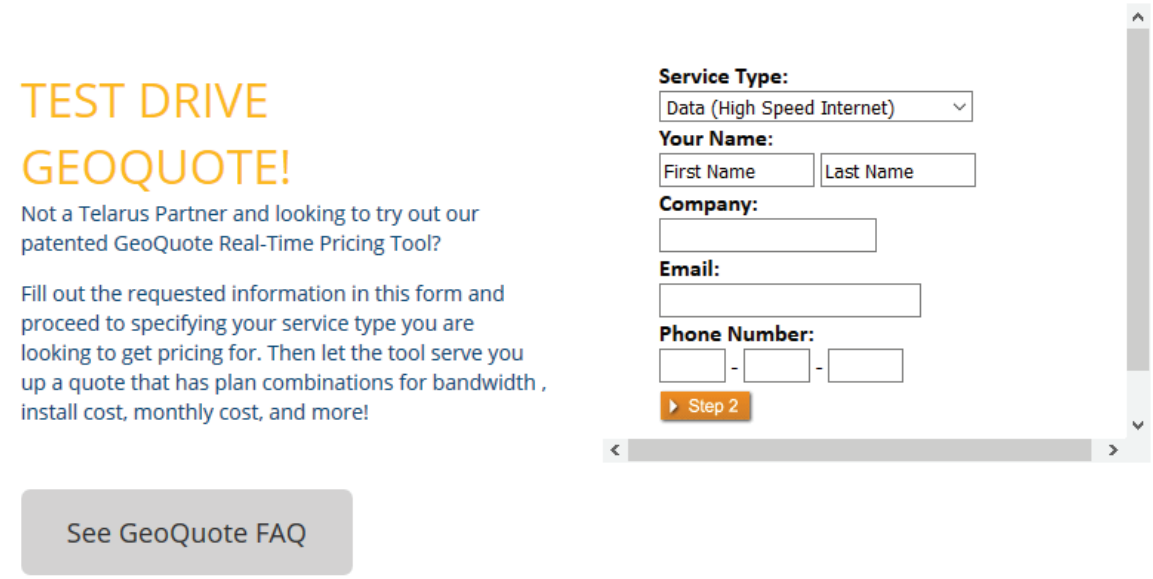
GeoQuote is a web application that automates the search for WAN technology service providers, and provides price quotes in real-time. Complete the required fields.

a. Click the **Service Type** drop-down list and select **Data (High Speed Internet)**.

b. Type your **First Name** and **Last Name**, your sample **Company**, and your **Email** address.

c. Type the **Phone Number** to connect to the WAN. This number should be a landline number.

d. Click the button marked **Step 2**.



Step 2. Provide Information.

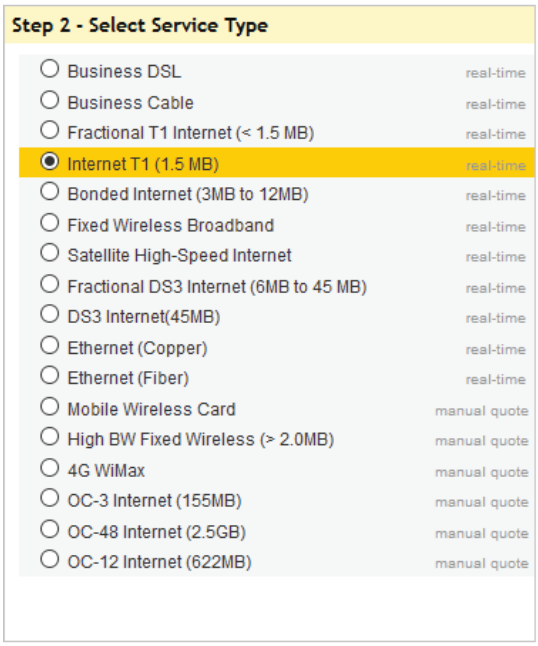
a. Choose **Internet T1 (1.5 MB)** in the GeoQuote Step 2 window (below).

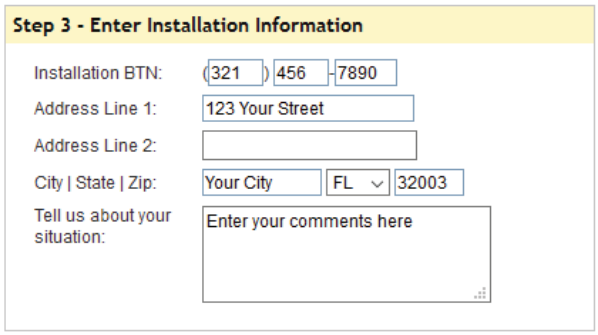
b. In the GeoQuote Step 3 window, in the **Installation BTN** field, enter your sample business telephone number.

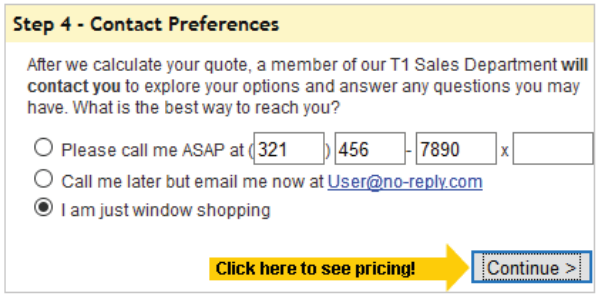
c. Enter your address, city, state, and zip code in the GeoQuote Step 3 window.

d. In the GeoQuote Step 4 window, click **I am just window shopping.**

e. Click **Continue** in the GeoQuote Step 4 window to display the results.







Step 3. Examine the results.

You should see a list of quotes showing the available pricing of a T1 connection to the location you specified. Was the pricing in the area you chose comparable to those pictured below?

_____

_____

What was the range of prices from your results?

_____

_____

Your Quote Results

Plan	Service Type	Bandwidth	Install	Rebate	Term	Router	Loop	Monthly Cost ↓	Order
1	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	3 Year	Yes	$161.00	$318.00	Order Now
2	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	2 Year	Yes	$161.00	$340.00	Order Now
3	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	3 Year	Yes	included	$352.90	Order Now
4	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	2 Year	Yes	included	$372.12	Order Now
5	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	1 Year	Yes	$231.00	$433.00	Order Now
6	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	3 Year	No	$310.81	$455.81	Order Now
7	Internet T1 (1.5 MB)	1.5M x 1.5M	$444.07	$0.00	1 Year	No	$318.83	$463.83	Order Now
8	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	2 Year	No	$327.66	$472.66	Order Now
9	Internet T1 (1.5 MB)	1.5M x 1.5M	$0.00	$0.00	3 Year	Yes	$310.81	$490.81	Order Now

Reflection

1. What are the disadvantages to using a T1 leased line for personal home use? What would be a better solution?

   _____

   _____

   _____

2. When might the use of a dedicated WAN connection, of any type, be a good connectivity solution for a business?

   _____

   _____

3. Describe other WAN technologies that provide high-speed, low-cost options that could be an alternative solution to a T1 connection.

   _____

   _____

1.3.1.1 Class Activity–WAN Device Modules

Objective

Select WAN access technologies to satisfy business requirements in a small-to-medium-sized business network.

Scenario

Your medium-sized company is upgrading its network. To make the most of the equipment currently in use, you decide to purchase WAN modules instead of new equipment.

All branch offices use either Cisco 1900 or 2911 series ISRs. You will be updating these routers in several locations. Each branch has its own ISP requirements to consider.

To update the devices, focus on the following WAN modules access types:

- Ethernet
- Broadband
- T1/E1 and ISDN PRI
- BRI
- Serial
- T1 and E1 Trunk Voice and WAN
- Wireless LANs and WANs

Resources

- World Wide Web
- Word processing software

Directions

Step 1. Visit Interfaces and Modules http://www.cisco.com/c/en/us/products/interfaces-modules/index.html. On this page, you will see many ISR interface modules options—remember that you currently own and use only the Cisco 1900 and 2900 series routers.

Note: If the above link is no longer valid, search the Cisco site for "Interfaces and Modules."

Step 2. Create a comparison matrix listing the following WAN access types for your branch networks:

- Ethernet
- Broadband
- T1/E1 and ISDN PRI
- BRI
- Serial WAN
- T1 and E1Trunk Voice and WAN
- Wireless LANs and WANs

Step 3. In the matrix, record the interface module type you need to purchase for your ISRs for upgrade purposes.

Step 4. Use the Internet to research pictures of the modules. Provide a screenshot of the module or a hyperlink to a picture of each module.

Step 5. Share your matrix with a classmate, group, class, or your instructor.

CHAPTER 2

Point-to-Point Connections

Point-to-point connections are the most common type of WAN connections. These connections are also called serial or leased lines. This chapter reviews the terms, technology, and protocols used in serial connections.

Serial Point-to-Point Overview

Understanding how point-to-point serial communication across a leased line works is important to an overall understanding of how WANs function.

Serial Communications

Briefly explain the difference between serial and parallel communications.

_____

_____

What is clock skew in parallel communications?

_____

WAN Protocols

Just like LANs, data is encapsulated into frames before transmission onto a WAN link. Various encapsulation protocols can be used to achieve the framing. In Table 2-1, indicate which protocol best fits the description.

Table 2-1 WAN Encapsulation Protocols

WAN Protocol Description	HDLC	PPP	SLIP	X.25/ LAPB	Frame Relay	ATM
Provides connections over synchronous and asynchronous circuits						
International standard for cell relay						
Predecessor to Frame Relay						
Default encapsulation on a serial link between two Cisco devices						
Eliminates the need for error correction and flow control						
Forms the basis for synchronous PPP						
Built-in security with PAP and CHAP						
Transfers data 53 bytes at a time so that processing can occur in hardware						
Next-generation protocol after X.25						
Largely replaced by PPP						
An ITU-T standard that defines connections between a DTE and DCE						

HDLC Encapsulation

What is the major difference between the ISO 13239 HDLC standard and Cisco's implementation of HDLC?

_____

In Figure 2-1, label the fields of Cisco HDLC frame.

Figure 2-1 Cisco HDLC Frame Format

List the three different formats of the Control field.

_____

_____

_____

HDLC Configuration and Troubleshooting

Although High-Level Data Link Control (HDLC) is the default encapsulation on Cisco synchronous serial lines, you may need to change the encapsulation back to HDLC. Record the commands, including the router prompt, to change the first serial interface on a 1900 series router to HDLC.

_____

_____

_____

Troubleshooting Serial Interfaces

Troubleshooting the cause of a serial interface issue usually begins by entering the **show interface serial** command. This command can return one of six possible statuses for the line. In Table 2-2, indicate what status would display for each of the conditions of the serial interface. Some statuses are used more than once.

Table 2-2 Line Conditions and Status Indicators

Condition of the Serial Interface	Serial X Is Up, Line Protocol Is Up	Serial X Is Down, Line Protocol Is Down	Serial X Is Up, Line Protocol Is Down	Serial X Is Up, Line Protocol Is Up (Looped)	Serial X Is Up, Line Protocol Is Down (Disabled)	Serial X Is Administratively Down, Line Protocol Is Down
A high error rate has occurred due to a WAN service provider problem.						
Keepalives are not being sent by the remote router.						

Condition of the Serial Interface	Serial X Is Up, Line Protocol Is Up	Serial X Is Down, Line Protocol Is Down	Serial X Is Up, Line Protocol Is Down	Serial X Is Up, Line Protocol Is Up (Looped)	Serial X Is Up, Line Protocol Is Down (Disabled)	Serial X Is Administratively Down, Line Protocol Is Down
The router configuration includes the **shutdown** interface configuration command.						
Cabling is faulty or incorrect.						
The **clockrate** command is not configured on the interface.						
This is the proper status line condition.						
The router is not sensing a carrier detect (CD) signal.						
The same random sequence number in the keepalive is returned over the link.						

What command will show whether a DTE or DCE cable is attached to the interface?

_____

PPP Operation

PPP encapsulation has been carefully designed to retain compatibility with most commonly used supporting hardware. PPP encapsulates data frames for transmission over Layer 2 physical links.

PPP Components

Briefly described the three main components of PPP.

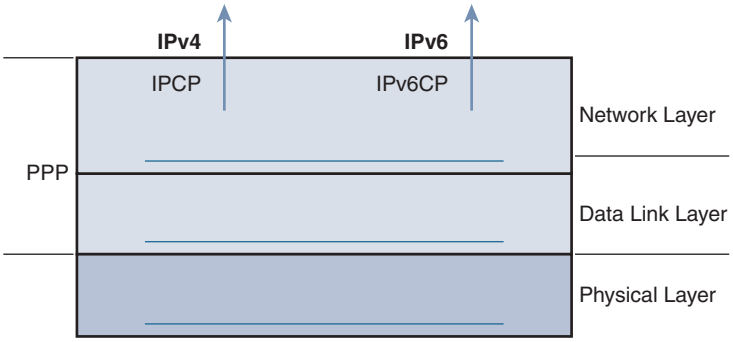
_____

_____

_____

In Figure 2-2, fill in the missing parts of the PPP layered architecture.

Figure 2-2 PPP Layered Architecture



List the type of physical interfaces supported by PPP.

What automatic configurations does the Link Control Protocol (LCP) provide at each end of the link?

Briefly describe how PPP uses Network Control Protocol (NCP).

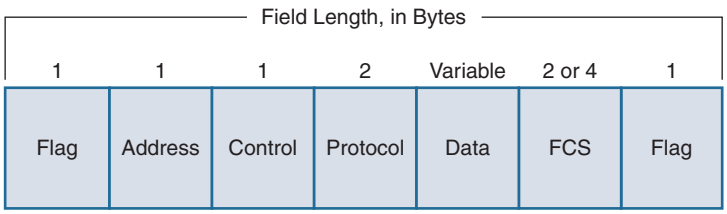
In Table 2-3, indicate whether each characteristic describes LCP or NCP.

Table 2-3 LCP and NCP Characteristics

Characteristic	LCP	NCP
Can configure authentication, compression, and error detection		
Bring network layer protocols up and down		
Encapsulate and negotiate options for IPv4 and IPv6		
Negotiate and set up control options on the WAN circuit		
Handle limits on packet size		
Establish, configure, and test the data link connection		
Use standardized codes to indicate the network layer protocol		
Determine if link is functioning properly		
Terminate the link		
Manage packets from several network layer protocols		

Figure 2-3 shows the PPP frame format. Answer the following questions about the specific features and purpose of each field.

Figure 2-3 PPP Frame Format



What is the bit pattern for the Flag field?

_____

Why is the Address field all 1s or 0xFF?

_____

What is the purpose of the Control field?

_____

_____

What is the purpose of the Protocol field?

_____

_____

What is the default size of the information stored in the Data field?

_____

What does FCS stand for and what is the purpose of this field?

_____

_____

PPP Sessions

What are the three phases for establishing a PPP session?

_____

_____

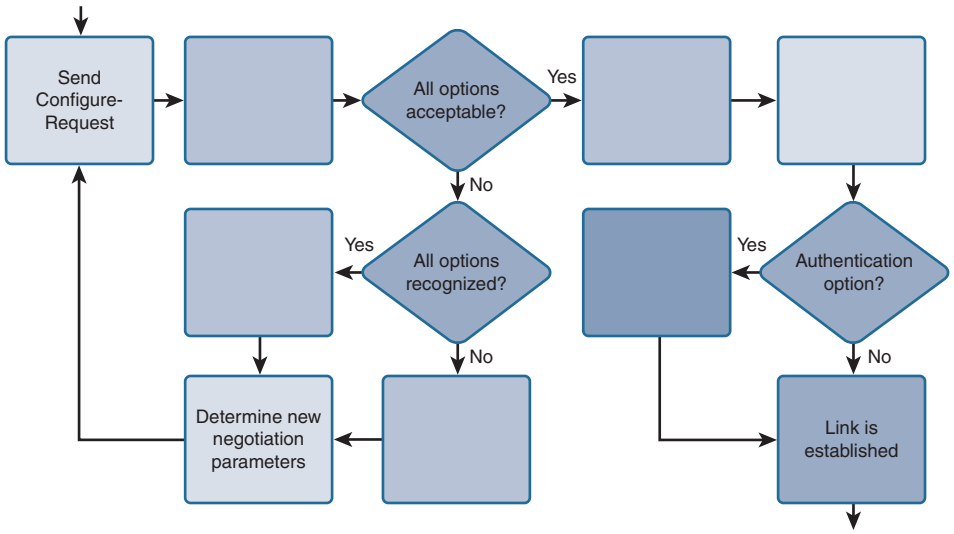
_____

Figure 2-4 shows a partially labeled flowchart for the LCP link negotiation process. Complete the flowchart by properly labeling it with the provided steps.

- Send Configure-Reject
- Receive Configure-Ack
- Process Configure-Request

- Send Configure-Ack
- Authentication Phase
- Send Configure-Nak

Figure 2-4 Steps in the LCP Link Negotiation Process



PPP can be configured to support optional functions, including the following:

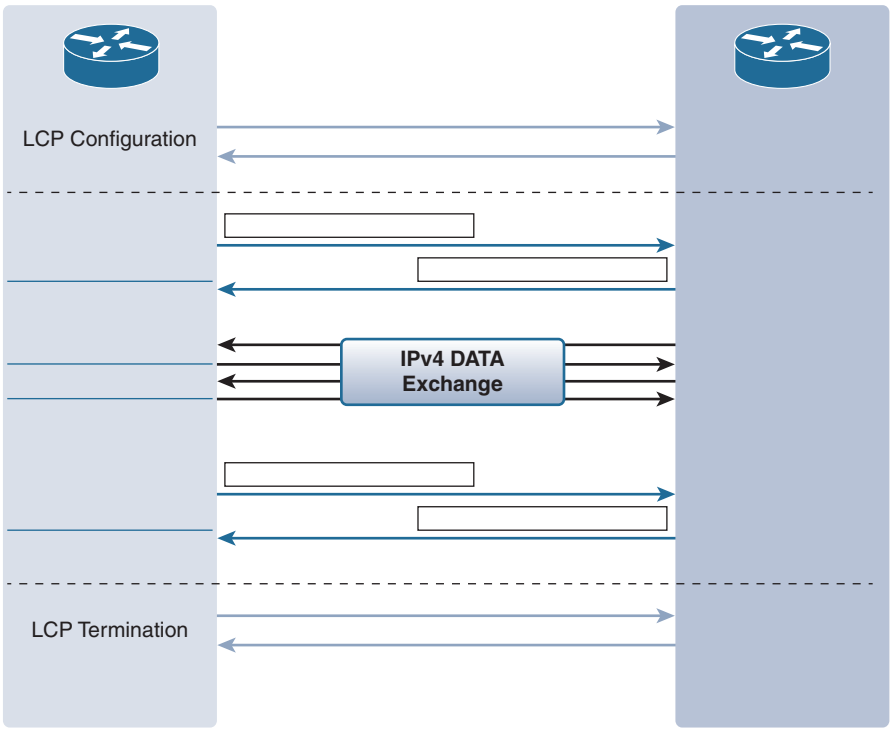
- _____ using either PAP or CHAP
- _____ using either Stacker or Predictor
- _____ that combines two or more channels to increase the WAN bandwidth

After the link is established, the LCP passes control to the appropriate NCP. Figure 2-5 shows the NCP process for IPv4. Complete the figure by properly labeling it with the provided phases and steps.

Missing Labels for Figure 2-5

- IPv4 Data Transfer
- NCP Termination
- IPCP Configure-Request
- IPCP Configure-Ack
- IPCP Terminate-Request
- LCP Maintenance
- IPCP Terminate-Ack
- NCP Configuration

Figure 2-5 The NCP Process



Configure PPP

PPP is a robust WAN protocol supporting multiple physical layer and network layer implementations. In addition, PPP has many optional features the network administrator can choose to implement.

Basic PPP Configuration with Options

Figure 2-6 shows the topology and Table 2-4 shows the addressing we will use for PPP configuration.

Figure 2-6 PPP Topology

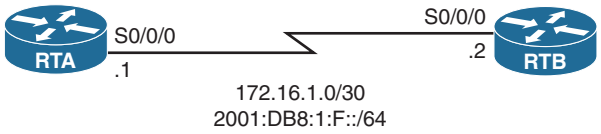


Table 2-4 Addressing Table for PPP

Device	Interface	IPv4 Address	Subnet Mask
		IPv6 Address/Prefix	
RTA	S0/0/0	172.16.1.1	255.255.255.252
		2001:DB8:1:F::1/64	
RTB	S0/0/0	172.16.1.2	255.255.255.252
		2001:DB8:1:F::2/64	

Assume that the router interfaces are already configured with IPv4 and IPv6 addressing. RTB is fully configured with PPP. Record the commands, including the router prompt, to configure RTA with a basic PPP configuration.

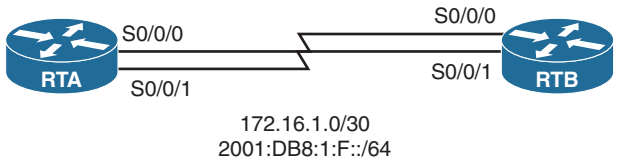
RTB is configured for software compression using the Stacker compression algorithm. What happens if RTA is not configured with compression?

Record the command, including the router prompt, to configure the same compression on RTA.

RTB is configured to take down the link if the quality falls below 70 percent. Record the command, including the router prompt, to configure the equivalent on RTA.

In Figure 2-7, RTA and RTB are now using two serial links to transfer data. RTB is already configured with PPP multilink to load balance the traffic to RTA. Record the commands, including the router prompt, to configure the RTA multilink interface including IPv4 and IPv6 addressing and the necessary commands for the serial interfaces. Use the addressing in Table 2-4 for the multilink interface rather than Serial 0/0/0.

Figure 2-7 PPP Multilink Topology



You can verify the operation of PPP using the following **show** commands. Record the commands used to generate the output on RTA.

```
RTA# _____________________________________________
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 172.16.1.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, IPV6CP, CCP, CDPCP, loopback not set
  Keepalive set (10 sec)
<output omitted>

RTA# _____________________________________________

Multilink1
  Bundle name: RTA
  Remote Endpoint Discriminator: [1] RTB
  Local Endpoint Discriminator: [1] RTA
  Bundle up for 00:01:20, total bandwidth 3088, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x2 received sequence, 0x2 sent sequence
  Member links: 2 active, 0 inactive (max 255, min not set)
    Se0/0/0, since 00:01:20
    Se0/0/1, since 00:01:06
No inactive multilink interfaces
```

PPP Authentication

Briefly explain the difference between PAP and CHAP.

_____

_____

_____

PAP is not interactive. When you configure an interface with the **ppp authentication pap** command, the username and password are sent as one LCP data package. You are not prompted for a username. The receiving node checks the username and password combination and either accepts or rejects the connection.

List three situations where PAP would be the appropriate choice for authentication.

_____

_____

_____

Once PAP authentication is established, the link is vulnerable to attack. Why?

_____

CHAP challenges periodically to make sure that the remote node still has a valid password. Complete the missing information in the following steps as RTA authenticates with RTB using CHAP.

Step 1. RTA initially negotiates the link connection using LCP with router RTB, and the two systems agree to use CHAP authentication during the PPP LCP negotiation.

Step 2. RTB generates an _____ and a _____ number, and sends that and its _____ as a CHAP challenge packet to RTA.

Step 3. RTA uses the _____ of the challenger (RTB) and cross references it with its local database to find its associated _____. RTA then generates a unique _____ number using the RTB's _____, _____, _____ number, and the shared _____.

Step 4. RTA then sends the challenge _____, the _____ value, and its _____ (RTA) to RTB.

Step 5. RTB generates its own _____ value using the _____, the shared _____, and the _____ number it originally sent to RTA.

Step 6. RTB compares its _____ value with the _____ value sent by RTA. If the values are the same, RTB sends a link established response to RTA.

When authentication is local (no AAA/TACACS+), what is the command syntax to configure PPP authentication on an interface?

_____

Assume that both PAP and CHAP are configured with the command **ppp authentication chap pap** on the interface. Explain how authentication will proceed.

_____

_____

PAP Configuration

In Figure 2-6, RTB is already configured with PAP authentication with the password cisco123. Record the commands to configure PAP on RTA.

_____

_____

_____

_____

CHAP Configuration

CHAP uses one less command than PAP. Now record the commands to remove PAP and configure RTA to use CHAP authentication.

_____

_____

_____

_____

Packet Tracer ☐ Activity

Packet Tracer Exercise 2-1: PPP Implementation

Now you are ready to use Packet Tracer to configure PPP with authentication. Download and open the file LSG04-0201.pka found at the companion website for this book. Refer to the Introduction of this book for specifics on accessing files.

Note: The following instructions are also contained within the Packet Tracer Exercise.

In this Packet Tracer activity, you will configure the RTA and RTB to use PPP with CHAP. You will then verify that RTA and RTB can ping each other using IPv4 and IPv6 addresses.

Requirements

Configure RTA and RTB with the following settings:

- The hostname is the username. Use **cisco123** as the password.
- Configure and activate the connected interfaces to use dual-stack IP addressing. Refer to the topology for addressing information.
- Configure PPP with CHAP authentication.
- Verify that the interfaces are up and that RTA and RTB can ping each other's IPv4 and IPv6 addresses.

Your completion percentage should be 100%. All the connectivity tests should show a status of "successful." If not, click **Check Results** to see which required components are not yet completed.

Troubleshoot WAN Connectivity

If you cannot ping across a PPP link and you have checked the physical and data link layer issues reviewed in the "Troubleshooting Serial Interfaces" section earlier, the issue is probably the PPP configuration. You can use the **debug** command to troubleshoot PPP issues using the **debug ppp** {*parameter*} syntax. Based on the descriptions in Table 2-5, fill in the corresponding parameter you would use with the **debug ppp** command.

Table 2-5 Parameters for the debug ppp Command

Parameter	Usage
	Displays issues associated with PPP connection negotiation and operation
	Displays information specific to the exchange of PPP connections using MPPC
	Displays PPP packets transmitted during PPP startup
	Displays PPP packets being sent and received
	Displays authentication protocol messages
	Displays protocol errors and statistics associated with PPP connection negotiations using MSCB

Labs and Activities

Command Reference

In Table 2-6, record the command, including the correct router prompt that fits the description. Fill in any blanks with the appropriate missing information.

Table 2-6 Commands for Chapter 2, Point-to-Point Connections

Command	Description
	Configure HDLC encapsulation.
	Display whether serial 0/0/0 is DCE or DTE.
	Configure PPP encapsulation.
	Configure PPP to use the predictor compression algorithm.
	Configure PPP to take down the link if the quality falls below 50 percent.
	Create a multilink interface with group number 1.
	Configure an interface to multilink.
	Configure an interface to belong to multilink group 1.
	Verify serial 0/0/0 is using PPP and that LCP and NCPs are open.
	Verify that multilink is operational.
	Configure RTA to use CHAP.
	Configure RTA to use PAP.
	Configure RTA to send the PAP username RTA and password cisco123.

2.0.1.2 Class Activity–PPP Persuasion

Objectives

Describe the benefits of using PPP over HDLC in a WAN.

This activity can be completed individually or in small groups of 2-3 students per group.

Scenario

Your network engineering supervisor recently attended a networking conference where Layer 2 protocols were discussed. He knows that you have Cisco equipment on the premises, but he would also like to offer security and advanced TCP/IP options and controls on that same equipment by using the Point-to-Point Protocol (PPP).

After researching the PPP protocol, you find it offers some advantages over the HDLC protocol, currently used on your network.

Create a matrix listing the advantages and disadvantages of using the HDLC vs. PPP protocols. When comparing the two protocols, include:

- Ease of configuration
- Adaptability to non-proprietary network equipment
- Security options
- Bandwidth usage and compression
- Bandwidth consolidation

Share your chart with another student or class. Justify whether or not you would suggest sharing the matrix with the network engineering supervisor to justify a change being made from HDLC to PPP for Layer 2 network connectivity.

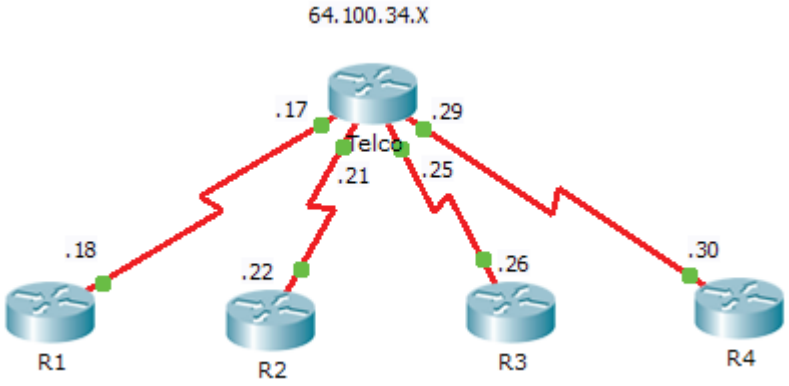
Resources

- Internet access to the World Wide Web
- Word processing or spreadsheet software

Packet Tracer
☐ Activity

2.1.2.5 Packet Tracer–Troubleshooting Serial Interfaces

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Route
Telco	S0/0/0 (DCE)	64.100.34.17	255.255.255.252	N/A
	S0/0/1 (DCE)	64.100.34.21	255.255.255.252	N/A
	S0/1/0 (DCE)	64.100.34.25	255.255.255.252	N/A
	S0/1/1 (DCE)	64.100.34.29	255.255.255.252	N/A
R1	S0/0/0	64.100.34.18	255.255.255.252	64.100.34.17
R2	S0/0/1	64.100.34.22	255.255.255.252	64.100.34.21
R3	S0/0/0	64.100.34.26	255.255.255.252	64.100.34.25
R4	S0/0/1	64.100.34.30	255.255.255.252	64.100.34.29

Objectives

Part 1: Diagnose and Repair the Physical Layer

Part 2: Diagnose and Repair the Data Link Layer

Part 3: Diagnose and Repair the Network Layer

Scenario

You have been asked to troubleshoot WAN connections for a local telephone company (**Telco**). The Telco router should communicate with four remote sites, but none of them are working. Use your knowledge of the OSI model and a few general rules to identify and repair the errors in the network.

Part 1: Diagnose and Repair the Physical Layer

Step 1. Diagnose and repair the cabling.

a. Examine the Addressing Table to determine the location of the DCE connections.

b. Each serial connection has a DCE and a DTE connection. To determine if each **Telco** interface is using the correct end of the cable look on the third line of output following the **show controllers** command.

```
Telco# show controllers [interface_type interface_num]
```

c. Reverse any cables that are incorrectly connected.

Note: In real network settings, the DCE (which sets the clock rate) is typically a CSU/DSU.

Step 2. Diagnose and repair incorrect port connections.

a. Examine the Addressing Table to match each router port with the correct **Telco** port.

b. Hold the mouse over each wire to ensure that the wires are connected as specified. If not, correct the connections.

Step 3. Diagnose and repair ports that are shut down.

a. Show a brief interface summary of each router. Ensure that all of the ports that should be working are not administratively down.

b. Enable the appropriate ports that are administratively down:

_____

_____

Part 2: Diagnose and Repair the Data Link Layer

Step 1. Examine and set clock rates on DCE equipment.

a. All of the DCE cables should be connected to **Telco**. Show the running configuration of **Telco** to verify that a clock rate has been set on each interface.

b. Set the clock rate of any serial interface that requires it:

_____

_____

_____

_____

Step 2. Examine the encapsulation on DCE equipment.

a. All of the serial interfaces should be using HDLC as the encapsulation type. Examine the protocol setting of the serial interfaces.

```
Telco# show interface [interface_type interface_num]
```

b. Change the encapsulation type to HDLC for any interface that is set otherwise:

_____

_____

Part 3: Diagnose and Repair the Network Layer

Step 1. Verify the IP addressing.

a. Show a brief interface summary of each router. Check the IP addresses against the Addressing Table and ensure that they are in the correct subnet with their connecting interface.

b. Correct any IP addresses that overlap, or are set to the host or broadcast address:

_____

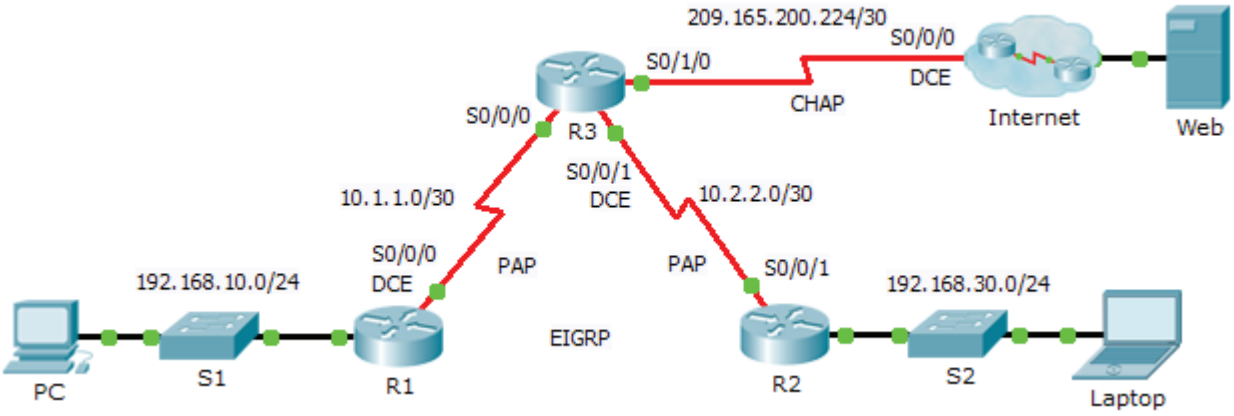
_____

Step 2. Verify connectivity between all routers.

Packet Tracer Activity

2.3.2.6 Packet Tracer–Configuring PAP and CHAP Authentication

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	G0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
R3	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	S0/1/0	209.165.200.225	255.255.255.252	N/A
ISP	S0/0/0	209.165.200.226	255.255.255.252	N/A
	G0/0	209.165.200.1	255.255.255.252	N/A
Web	NIC	209.165.200.2	255.255.255.252	209.165.200.1
PC	NIC	192.168.10.10	255.255.255.0	192.168.10.1
Laptop	NIC	192.168.30.10	255.255.255.0	192.168.30.1

Objectives

Part 1: Review Routing Configurations

Part 2: Configure PPP as the Encapsulation Method

Part 3: Configure PPP Authentication

Background

In this activity, you will practice configuring PPP encapsulation on serial links. You will also configure PPP PAP authentication and PPP CHAP authentication.

Part 1: Review Routing Configurations

Step 1. View running configurations on all routers.

While reviewing the router configurations, note the use of both static and dynamic routes in the topology.

Step 2. Test connectivity between computers and the Web Server.

From **PC** and **Laptop**, ping the Web Server at 209.165.200.2. Both **ping** commands should be successful. Remember to give enough time for STP and EIGRP to converge.

Part 2: Configure PPP as the Encapsulation Method

Step 1. Configure **R1** to use PPP encapsulation with **R3**.

Enter the following commands on **R1**:

```
R1(config)# interface s0/0/0
R1(config-if)# encapsulation ppp
```

Step 2. Configure **R2** to use PPP encapsulation with **R3**.

Enter the appropriate commands on **R2**:

_____

_____

Step 3. Configure **R3** to use PPP encapsulation with **R1**, **R2**, and **ISP**.

Enter the appropriate commands on **R3**:

_____

_____

_____

_____

_____

_____

Step 4. Configure **ISP** to use PPP encapsulation with **R3**.

a. Click the **Internet** cloud, then ISP. Enter the following commands:

```
Router(config)# interface s0/0/0
Router(config-if)# encapsulation ppp
```

b. Exit the **Internet** cloud by clicking **Back** in the upper left corner or by pressing **Alt+left arrow**.

Step 5. Test connectivity to the Web Server.

PC and **Laptop** should be able to ping the Web Server at 209.165.200.2. This may take some time as interfaces start working again and EIGRP reconverges.

Part 3: Configure PPP Authentication

Step 1. Configure PPP PAP authentication between **R1** and **R3**.

Note: Instead of using the keyword **password** as shown in the curriculum, you will use the keyword **secret** to provide a better encryption of the password.

a. Enter the following commands into **R1**:

```
R1(config)# username R3 secret class
R1(config)# interface s0/0/0
R1(config-if)# ppp authentication pap
R1(config-if)# ppp pap sent-username R1 password cisco
```

b. Enter the following commands into **R3**:

```
R3(config)# username R1 secret cisco
R3(config)# interface s0/0/0
R3(config-if)# ppp authentication pap
R3(config-if)# ppp pap sent-username R3 password class
```

Step 2. Configure PPP PAP authentication between **R2** and **R3**.

Repeat Step 1 to configure authentication between **R2** and **R3** changing the usernames as needed. Note that each password sent on each serial port matches the password expected by the opposite router.

Step 3. Configure PPP CHAP authentication between **R3** and **ISP**.

a. Enter the following commands into **ISP**. The hostname is sent as the username:

```
Router(config)# hostname ISP
ISP(config)# username R3 secret cisco
ISP(config)# interface s0/0/0
ISP(config-if)# ppp authentication chap
```

b. Enter the following commands into **R3**. The passwords must match for CHAP authentication:

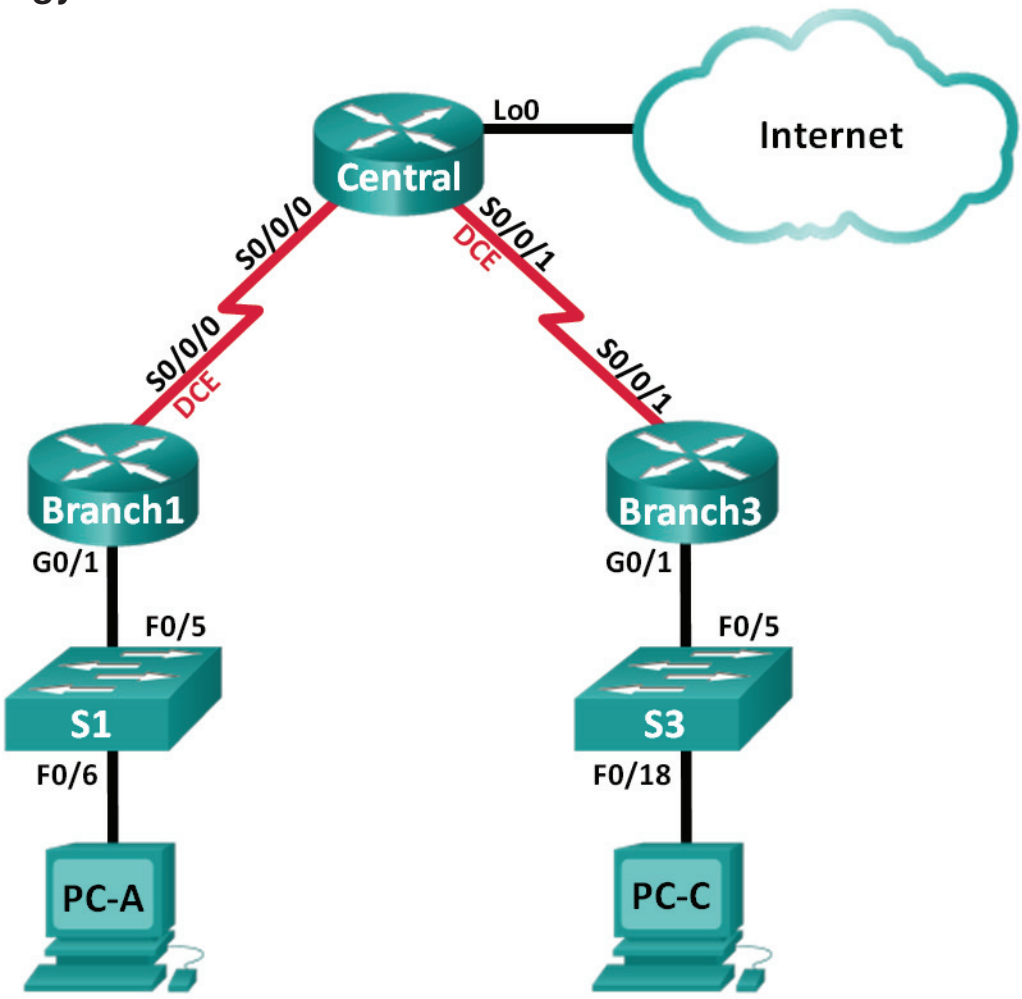
```
R3(config)# username ISP secret cisco
R3(config)# interface serial0/1/0
R3(config-if)# ppp authentication chap
```

Step 4. Test connectivity between computers and the Web Server.

From **PC** and **Laptop**, ping the Web Server at 209.165.200.2. Both **ping** commands should be successful. Remember to give enough time for STP and EIGRP to converge.

2.3.2.7 Lab–Configuring Basic PPP with Authentication

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Branch1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
Central	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
Branch3	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure PPP Encapsulation

Part 3: Configure PPP CHAP Authentication

Background/Scenario

The Point-to-Point Protocol (PPP) is a very common Layer 2 WAN protocol. PPP can be used to connect from LANs to service provider WANs and for connection of LAN segments within an enterprise network.

In this lab, you will configure PPP encapsulation on dedicated serial links between the branch routers and a central router. You will configure PPP Challenge Handshake Authentication Protocol (CHAP) on the PPP serial links. You will also examine the effects of the encapsulation and authentication changes on the status of the serial link.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic router settings, such as the interface IP addresses, routing, device access, and passwords.

Step 1. Cable the network as shown in the topology.

Attach the devices as shown in the Topology, and cable as necessary.

Step 2. Initialize and reload the routers and switches.

Step 3. Configure basic settings for each router.

a. Disable DNS lookup.

b. Configure the device name.

c. Encrypt plaintext passwords.

d. Create a message of the day (MOTD) banner warning users that unauthorized access is prohibited.

e. Assign **class** as the encrypted privileged EXEC mode password.

f. Assign **cisco** as the console and vty password and enable login.

g. Set console logging to synchronous mode.

h. Apply the IP addresses to Serial and Gigabit Ethernet interfaces according to the Addressing Table and activate the physical interfaces.

i. Set the clock rate to **128000** for DCE serial interfaces.

j. Create **Loopback0** on the Central router to simulate access to the Internet and assign an IP address according to the Addressing Table.

Step 4. Configure routing.

a. Enable single-area OSPF on the routers and use a process ID of 1. Add all the networks, except 209.165.200.224/27 into the OSPF process.

b. Configure a default route to the simulated Internet on the Central router using Lo0 as the exit interface and redistribute this route into the OSPF process.

c. Issue the **show ip route ospf**, **show ip ospf interface brief**, and **show ip ospf neighbor** commands on all routers to verify that OSPF is configured correctly. Take note of the router ID for each router.

Step 5. Configure the PCs.

Assign IP addresses and default gateways to the PCs according to the Addressing Table.

Step 6. Verify end-to-end connectivity.

All devices should be able to ping other devices in the Topology. If not, troubleshoot until you can establish end-to-end connectivity.

Note: It may be necessary to disable the PC firewall to ping between PCs.

Step 7. Save your configurations.

Part 2: Configure PPP Encapsulation

Step 1. Display the default serial encapsulation.

On the routers, issue **show interfaces serial** *interface-id* to display the current serial encapsulation.

```
Branch1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:02, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
```

```
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
   1003 packets input, 78348 bytes, 0 no buffer
   Received 527 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   1090 packets output, 80262 bytes, 0 underruns
   0 output errors, 0 collisions, 3 interface resets
   0 unknown protocol drops
   0 output buffer failures, 0 output buffers swapped out
   2 carrier transitions
   DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

What is the default serial encapsulation for a Cisco router? _____

Step 2. Change the serial encapsulation to PPP.

a. Issue the **encapsulation ppp** command on the S0/0/0 interface for the Branch1 router to change the encapsulation from HDLC to PPP.

```
Branch1(config)# interface s0/0/0
Branch1(config-if)# encapsulation ppp
Branch1(config-if)#
Jun 19 06:02:33.687: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
Branch1(config-if)#
Jun 19 06:02:35.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
```

b. Issue the command to display the line status and line protocol for interface S0/0/0 on the Branch1 router. Document the command issued. What is the current interface status for S0/0/0?

_____

c. Issue the **encapsulation ppp** command on interface S0/0/0 for the Central router to correct the serial encapsulation mismatch.

```
Central(config)# interface s0/0/0
Central(config-if)# encapsulation ppp
Central(config-if)#
.Jun 19 06:03:41.186: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
.Jun 19 06:03:41.274: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done
```

d. Verify that interface S0/0/0 on both Branch1 and Central routers is up/up and is configured with PPP encapsulation.

What is the status of the PPP Link Control Protocol (LCP)? _____

Which Network Control Protocol (NCP) protocols have been negotiated?

_____

```
Branch1# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
```

```
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:03:58
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     77 packets input, 4636 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     117 packets output, 5800 bytes, 0 underruns
     0 output errors, 0 collisions, 8 interface resets
     22 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     18 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

Central# show interfaces s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 10.1.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, CDPCP, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:02, output 00:00:03, output hang never
  Last clearing of "show interface" counters 00:01:20
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     41 packets input, 2811 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     40 packets output, 2739 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

Step 3. Intentionally break the serial connection.

a. Issue the **debug ppp** commands to observe the effects of changing the PPP configuration on the Branch1 router and the Central router.

```
Branch1# debug ppp negotiation
PPP protocol negotiation debugging is on
Branch1# debug ppp packet
PPP packet display debugging is on

Central# debug ppp negotiation
PPP protocol negotiation debugging is on
Central# debug ppp packet
PPP packet display debugging is on
```

b. Observe the debug PPP messages when traffic is flowing on the serial link between the Branch1 and Central routers.

```
Branch1#
Jun 20 02:20:45.795: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 02:20:49.639: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
Jun 20 02:20:50.147: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic
0x73885AF2
Jun 20 02:20:50.147: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic
0x8CE1F65F
Jun 20 02:20:50.159: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic
0x8CE1F65F
Jun 20 02:20:50.159: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic
0x73885AF2
Jun 20 02:20:50.159: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up

Central#
Jun 20 02:20:49.636: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 02:20:50.148: Se0/0/0 LCP: O ECHOREQ [Open] id 45 len 12 magic
0x73885AF2
Jun 20 02:20:50.148: Se0/0/0 LCP-FS: I ECHOREP [Open] id 45 len 12 magic
0x8CE1F65F
Jun 20 02:20:50.148: Se0/0/0 LCP-FS: Received id 45, sent id 45, line up
Jun 20 02:20:50.160: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 45 len 12 magic
0x8CE1F65F
Jun 20 02:20:50.160: Se0/0/0 LCP-FS: O ECHOREP [Open] id 45 len 12 magic
0x73885AF2
Jun 20 02:20:55.552: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
```

c. Break the serial connection by returning the serial encapsulation to HDLC for interface S0/0/0 on the Branch1 router. Record the command used to change the encapsulation to HDLC.

_____

d. Observe the debug PPP messages on the Branch1 router. The serial connection has terminated, and the line protocol is down. The route to 10.1.1.2 (Central) has been removed from the routing table.

```
Jun 20 02:29:50.295: Se0/0/0 PPP DISC: Lower Layer disconnected
Jun 20 02:29:50.295: PPP: NET STOP send to AAA.
Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.299: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
```

```
Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.299: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.29
Branch1(config-if)#9: Se0/0/0 LCP: O TERMREQ [Open] id 7 len 4
Jun 20 02:29:50.299: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]
Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is TERMINATING
Jun 20 02:29:50.299: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0,
address 10.1.1.2
Jun 20 02:29:50.299: Se0/0/0 IPCP: Remove route to 10.1.1.2
Jun 20 02:29:50.299: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
Jun 20 02:29:50.299: Se0/0/0 PPP: Phase is DOWN
Branch1(config-if)#
Jun 20 02:30:17.083: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
Jun 20 02:30:17.083: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
```

e. Observe the debug PPP messages on the Central router. The Central router continues to attempt to establish a connection with Branch1 as indicated by the debug messages. When the interfaces are unable to establish a connection, the interfaces go back down again. Furthermore, OSPF cannot establish an adjacency with its neighbor due to the mismatched serial encapsulation.

```
Jun 20 02:29:50.296: Se0/0/0 PPP: Sending cstate DOWN notification
Jun 20 02:29:50.296: Se0/0/0 PPP: Processing CstateDown message
Jun 20 02:29:50.296: Se0/0/0 PPP DISC: Lower Layer disconnected
Jun 20 02:29:50.296: PPP: NET STOP send to AAA.
Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.296: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 02:29:50.296: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 02:29:50.296: Se0/0/0 LCP: O TERMREQ [Open] id 2 len 4
Jun 20 02:29:50.296: Se0/0/0 LCP: Event[CLOSE] State[Open to Closing]
Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is TERMINATING
Jun 20 02:29:50.296: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0,
address 10.1.1.1
Jun 20 02:29:50.296: Se0/0/0 IPCP: Remove route to 10.1.1.1
Jun 20 02:29:50.296: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 02:29:50.296: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
Jun 20 02:29:50.296: Se0/0/0 PPP: Phase is DOWN
Jun 20 02:29:52.296: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
.Jun 20 02:29:52.296: Se0/0/0 PPP: Sending cstate UP notification
.Jun 20 02:29:52.296: Se0/0/0 PPP: Processing CstateUp message
.Jun 20 02:29:52.296: PPP: Alloc Context [29F9F32C]
.Jun 20 02:29:52.296: ppp3 PPP: Phase is ESTABLISHING
.Jun 20 02:29:52.296: Se0/0/0 PPP: Using default call direction
.Jun 20 02:29:52.296: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:29:52.296: Se0/0/0 PPP: Session handle[60000003] Session id[3]
.Jun 20 02:29:52.296: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 02:29:52.296: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 02:29:52.296: Se0/0/0 LCP:    MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:29:52.296: Se0/0/0 LCP:Event[UP] State[Starting to REQsent]
```

```
.Jun 20 02:29:54.308: Se0/0/0 LCP: O CONFREQ [REQsent] id 2 len 10
.Jun 20 02:29:54.308: Se0/0/0 LCP:    MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:29:54.308: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:29:56.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24
link[illegal]
.Jun 20 02:29:56.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding
<output omitted>
.Jun 20 02:30:10.436: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10
.Jun 20 02:30:10.436: Se0/0/0 LCP:    MagicNumber 0x7397843B (0x05067397843B)
.Jun 20 02:30:10.436: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:30:12.452: Se0/0/0 PPP DISC: LCP failed to negotiate
.Jun 20 02:30:12.452: PPP: NET STOP send to AAA.
.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]
.Jun 20 02:30:12.452: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]
.Jun 20 02:30:12.452: Se0/0/0 PPP: Phase is DOWN
.Jun 20 02:30:14.452: PPP: Alloc Context [29F9F32C]
.Jun 20 02:30:14.452: ppp4 PPP: Phase is ESTABLISHING
.Jun 20 02:30:14.452: Se0/0/0 PPP: Using default call direction
.Jun 20 02:30:14.452: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:30:14.452: Se0/0/0 PPP: Session handle[6E000004] Session id[4]
.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 02:30:14.452: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 02:30:14.452: Se0/0/0 LCP:    MagicNumber 0x7397DADA (0x05067397DADA)
.Jun 20 02:30:14.452: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
.Jun 20 02:30:16.080: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24
link[illegal]
.Jun 20 02:30:16.080: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet, discarding
<output omitted>
.Jun 20 02:30:32.580: Se0/0/0 LCP: O CONFREQ [REQsent] id 10 len 10
.Jun 20 02:30:32.580: Se0/0/0 LCP:    MagicNumber 0x7397DADA (0x05067397DADA)
.Jun 20 02:30:32.580: Se0/0/0 LCP: Event[Timeout+] State[REQsent to REQsent]
.Jun 20 02:30:34.596: Se0/0/0 PPP DISC: LCP failed to negotiate
.Jun 20 02:30:34.596: PPP: NET STOP send to AAA.
.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[Timeout-] State[REQsent to Stopped]
.Jun 20 02:30:34.596: Se0/0/0 LCP: Event[DOWN] State[Stopped to Starting]
.Jun 20 02:30:34.596: Se0/0/0 PPP: Phase is DOWN
.Jun 20 02:30:36.080: Se0/0/0 PPP: I pkt type 0x008F, discarded, PPP not
running
.Jun 20 02:30:36.596: PPP: Alloc Context [29F9F32C]
.Jun 20 02:30:36.596: ppp5 PPP: Phase is ESTABLISHING
.Jun 20 02:30:36.596: Se0/0/0 PPP: Using default call direction
.Jun 20 02:30:36.596: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 02:30:36.596: Se0/0/0 PPP: Session handle[34000005] Session id[5]
.Jun 20 02:30:36.596: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
```

What happens when one end of the serial link is encapsulated with PPP and the other end of the link is encapsulated with HDLC?

_____

_____

_____

f. Issue the **encapsulation ppp** command on the S0/0/0 interface for the Branch1 router to correct mismatched encapsulation.

```
Branch1(config)# interface s0/0/0
Branch1(config-if)# encapsulation ppp
```

g. Observe the debug PPP messages from the Branch1 router as the Branch1 and Central routers establish a connection.

```
Branch1(config-if)#
Jun 20 03:01:57.399: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 03:01:59.399: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
Jun 20 03:01:59.399: Se0/0/0 PPP: Sending cstate UP notification
Jun 20 03:01:59.399: Se0/0/0 PPP: Processing CstateUp message
Jun 20 03:01:59.399: PPP: Alloc Context [30F8D4F0]
Jun 20 03:01:59.399: ppp9 PPP: Phase is ESTABLISHING
Jun 20 03:01:59.399: Se0/0/0 PPP: Using default call direction
Jun 20 03:01:59.399: Se0/0/0 PPP: Treating connection as a dedicated line
Jun 20 03:01:59.399: Se0/0/0 PPP: Session handle[BA000009] Session id[9]
Jun 20 03:01:59.399: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
Jun 20 03:01:59.399: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 10
Jun 20 03:01:59.399: Se0/0/0 LCP:    MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.399: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP:    MagicNumber 0x73B4F1AF (0x050673B4F1AF)
Jun 20 03:01:59.407: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP:    MagicNumber 0x73B4F1AF (0x050673B4F1AF)
Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to
ACKsent]
Jun 20 03:01:59.407: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.407: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 10
Jun 20 03:01:59.407: Se0/0/0 LCP:    MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.407: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to Open]
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
Jun 20 03:01:59.439: Se0/0/0 LCP: State is Open
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
Jun 20 03:01:59.439: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
Jun 20 03:01:59.439: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol
not up
Jun 20 03:01:59.439: Se0/0/0 PPP: Phase is UP
Jun 20 03:01:59.439: Se0/0/0 IPCP: Protocol configured, start CP.
state[Initial]
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]
Jun 20 03:01:59.439: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10
Jun 20 03:01:59.439: Se0/0/0 IPCP:    Address 10.1.1.1 (0x03060A010101)
Jun 20 03:01:59.439: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]
Jun 20 03:01:59.439: Se0/0/0 CDPCP: Protocol configured, start CP.
state[Initial]
<output omitted>
Jun 20 03:01:59.471: Se0/0/0 Added to neighbor route AVL tree: topoid 0,
address 10.1.1.2
```

```
Jun 20 03:01:59.471: Se0/0/0 IPCP: Install route to 10.1.1.2
Jun 20 03:01:59.471: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
Jun 20 03:01:59.479: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:01:59.479: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
Jun 20 03:01:59.483: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
Jun 20 03:01:59.483: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:01:59.491: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
Jun 20 03:01:59.491: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148
Jun 20 03:01:59.511: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
Jun 20 03:01:59.511: %OSPF-5-ADJCHG:Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from LOADING to FULL, Loading Done
Jun 20 03:01:59.511: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:01:59.519: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 60 link[ip]
```

h. Observe the debug PPP messages from the Central router as the Branch1 and Central routers establish a connection.

```
Jun 20 03:01:59.393: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14 link[ppp]
Jun 20 03:01:59.393: Se0/0/0 LCP: I CONFREQ [Open] id 1 len 10
Jun 20 03:01:59.393: Se0/0/0 LCP:    MagicNumber 0x8D0EAC44 (0x05068D0EAC44)
Jun 20 03:01:59.393: Se0/0/0 PPP DISC: PPP Renegotiating
Jun 20 03:01:59.393: PPP: NET STOP send to AAA.
Jun 20 03:01:59.393: Se0/0/0 LCP: Event[LCP Reneg] State[Open to Open]
Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: Se0/0/0 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: Se0/0/0 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 03:01:59.393: Se0/0/0 LCP: Event[DOWN] State[Open to Starting]
Jun 20 03:01:59.393: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
Jun 20 03:01:59.393: Se0/0/0 PPP: Outbound cdp packet dropped, NCP not negoti-
ated
.Jun 20 03:01:59.393: Se0/0/0 PPP: Phase is DOWN
.Jun 20 03:01:59.393: Se0/0/0 Deleted neighbor route from AVL tree: topoid 0,
address 10.1.1.1
.Jun 20 03:01:59.393: Se0/0/0 IPCP: Remove route to 10.1.1.1
.Jun 20 03:01:59.393: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Interface down or detached
.Jun 20 03:01:59.397: PPP: Alloc Context [29F9F32C]
.Jun 20 03:01:59.397: ppp38 PPP: Phase is ESTABLISHING
.Jun 20 03:01:59.397: Se0/0/0 PPP: Using default call direction
.Jun 20 03:01:59.397: Se0/0/0 PPP: Treating connection as a dedicated line
<output omitted>
.Jun 20 03:01:59.401: Se0/0/0 LCP:    MagicNumber 0x73B4F1AF (0x050673B4F1AF)
.Jun 20 03:01:59.401: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to
Open]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is FORWARDING, Attempting Forward
.Jun 20 03:01:59.433: Se0/0/0 LCP: State is Open
.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8021, datagramsize 14 link[ip]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Queue IPCP code[1] id[1]
.Jun 20 03:01:59.433: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Discarded CDPCP code[1] id[1]
.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
.Jun 20 03:01:59.433: %LINEPROTO-5-UPDOWN: Line protocol on Interface
```

```
Serial0/0/0, changed state to up
.Jun 20 03:01:59.433: Se0/0/0 PPP: Outbound cdp packet dropped, line protocol
not up
.Jun 20 03:01:59.433: Se0/0/0 PPP: Phase is UP
.Jun 20 03:01:59.433: Se0/0/0 IPCP: Protocol configured, start CP.
state[Initial]
.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[OPEN] State[Initial to Starting]
.Jun 20 03:01:59.433: Se0/0/0 IPCP: O CONFREQ [Starting] id 1 len 10
.Jun 20 03:01:59.433: Se0/0/0 IPCP:    Address 10.1.1.2 (0x03060A010102)
.Jun 20 03:01:59.433: Se0/0/0 IPCP: Event[UP] State[Starting to REQsent]
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Protocol configured, start CP.
state[Initial]
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[OPEN] State[Initial to Starting]
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: O CONFREQ [Starting] id 1 len 4
.Jun 20 03:01:59.433: Se0/0/0 CDPCP: Event[UP] State[Starting to REQsent]
<output omitted>
.Jun 20 03:01:59.465: Se0/0/0 IPCP: State is Open
.Jun 20 03:01:59.465: Se0/0/0 Added to neighbor route AVL tree: topoid 0,
address 10.1.1.1
.Jun 20 03:01:59.465: Se0/0/0 IPCP: Install route to 10.1.1.1
.Jun 20 03:01:59.465: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 03:01:59.465: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
.Jun 20 03:01:59.469: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 84
.Jun 20 03:01:59.477: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
.Jun 20 03:01:59.477: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 03:01:59.481: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 03:01:59.489: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
.Jun 20 03:01:59.493: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 148
.Jun 20 03:01:59.505: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 03:01:59.505: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 60
.Jun 20 03:01:59.517: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 88 link[ip]
.Jun 20 03:01:59.517: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on Serial0/0/0
from LOADING to FULL, Loading Done
.Jun 20 03:01:59.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 03:01:59.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:02:01.445: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8 link[cdp]
Jun 20 03:02:01.445: Se0/0/0 CDPCP: I CONFREQ [ACKrcvd] id 2 len 4
Jun 20 03:02:01.445: Se0/0/0 CDPCP: O CONFACK [ACKrcvd] id 2 len 4
Jun 20 03:02:01.445: Se0/0/0 CDPCP: Event[Receive ConfReq+] State[ACKrcvd to
Open]
Jun 20 03:02:01.449: Se0/0/0 CDPCP: State is Open
Jun 20 03:02:01.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
Jun 20 03:02:01.569: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
Jun 20 03:02:02.017: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 68
Jun 20 03:02:02.897: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 112 link[ip]
Jun 20 03:02:03.561: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
```

From the debug message, what phases does PPP go through when the other end of the serial link on the Central router is configured with PPP encapsulation?

_____

_____

What happens when PPP encapsulation is configured on each end of the serial link?

_____

i. Issue the **undebug all** (or **u all**) command on the Branch1 and Central routers to turn off all debugging on both routers.

j. Issue the **show ip interface brief** command on the Branch1 and Central routers after the network converges. What is the status for interface S0/0/0 on both routers?

_____

k. Verify that the interface S0/0/0 on both Branch1 and Central routers are configured for PPP encapsulation.

Record the command to verify the PPP encapsulation in the space provided below.

_____

_____

l. Change the serial encapsulation for the link between the Central and Branch3 routers to PPP encapsulation.

```
Central(config)# interface s0/0/1
Central(config-if)# encapsulation ppp
Central(config-if)#
Jun 20 03:17:15.933: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 03:17:17.933: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
Jun 20 03:17:23.741: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
Jun 20 03:17:23.825: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1
from LOADING to FULL, Loading Done

Branch3(config)# interface s0/0/1
Branch3(config-if)# encapsulation ppp
Branch3(config-if)#
Jun 20 03:17:21.744: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
Jun 20 03:17:21.948: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
.Jun 20 03:17:21.964: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
.Jun 20 03:17:23.812: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
```

m. Verify that end-to-end connectivity is restored before continuing to Part 3.

Part 3: Configure PPP CHAP Authentication

Step 1. Verify that PPP encapsulation is configured on all serial interfaces.

Record the command used to verify that PPP encapsulation is configured.

_____

Step 2. Configure PPP CHAP authentication for the link between the Central router and the Branch3 router.

a. Configure a username for CHAP authentication.

```
Central(config)# username Branch3 password cisco
Branch3(config)# username Central password cisco
```

b. Issue the **debug ppp** commands on the Branch3 router to observe the process, which is associated with authentication.

```
Branch3# debug ppp negotiation
PPP protocol negotiation debugging is on
Branch3# debug ppp packet
PPP packet display debugging is on
```

c. Configure the interface S0/0/1 on Branch3 for CHAP authentication.

```
Branch3(config)# interface s0/0/1
Branch3(config-if)# ppp authentication chap
```

d. Examine the debug PPP messages on the Branch3 router during the negotiation with the Central router.

```
Branch3(config-if)#
Jun 20 04:25:02.079: Se0/0/1 PPP DISC: Authentication configuration changed
Jun 20 04:25:02.079: PPP: NET STOP send to AAA.
Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[DOWN] State[Open to Starting]
Jun 20 04:25:02.079: Se0/0/1 IPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[DOWN] State[Open to Starting]
Jun 20 04:25:02.079: Se0/0/1 CDPCP: Event[CLOSE] State[Starting to Initial]
Jun 20 04:25:02.079: Se0/0/1 LCP: Event[DOWN] State[Open to Starting]
Jun 20 04:25:02.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
Jun 20 04:25:02.079: Se0/0/1 PPP: Outbound cdp packet dropped, NCP not
negotiated
.Jun 20 04:25:02.079: Se0/0/1 PPP: Phase is DOWN
.Jun 20 04:25:02.079: Se0/0/1 Deleted neighbor route from AVL tree: topoid 0,
address 10.2.2.2
.Jun 20 04:25:02.079: Se0/0/1 IPCP: Remove route to 10.2.2.2
.Jun 20 04:25:02.079: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
.Jun 20 04:25:02.083: PPP: Alloc Context [29F4DA8C]
.Jun 20 04:25:02.083: ppp73 PPP: Phase is ESTABLISHING
.Jun 20 04:25:02.083: Se0/0/1 PPP: Using default call direction
.Jun 20 04:25:02.083: Se0/0/1 PPP: Treating connection as a dedicated line
.Jun 20 04:25:02.083: Se0/0/1 PPP: Session handle[2700004D] Session id[73]
<output omitted>
.Jun 20 04:25:02.091: Se0/0/1 PPP: I pkt type 0xC021, datagramsize 19 link[ppp]
.Jun 20 04:25:02.091: Se0/0/1 LCP: I CONFACK [ACKsent] id 1 len 15
.Jun 20 04:25:02.091: Se0/0/1 LCP:    AuthProto CHAP (0x0305C22305)
.Jun 20 04:25:02.091: Se0/0/1 LCP:    MagicNumber 0xF7B20F10 (0x0506F7B20F10)
.Jun 20 04:25:02.091: Se0/0/1 LCP: Event[Receive ConfAck] State[ACKsent to
Open]
.Jun 20 04:25:02.123: Se0/0/1 PPP: Phase is AUTHENTICATING, by this end
.Jun 20 04:25:02.123: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Branch3"
.Jun 20 04:25:02.123: Se0/0/1 LCP: State is Open
.Jun 20 04:25:02.127: Se0/0/1 PPP: I pkt type 0xC223, datagramsize 32 link[ppp]
```

```
.Jun 20 04:25:02.127: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Central"
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is AUTHENTICATING, Unauthenticated
User
.Jun 20 04:25:02.127: Se0/0/1 PPP: Sent CHAP LOGIN Request
.Jun 20 04:25:02.127: Se0/0/1 PPP: Received LOGIN Response PASS
.Jun 20 04:25:02.127: Se0/0/1 IPCP: Authorizing CP
.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP stalled on event[Authorize CP]
.Jun 20 04:25:02.127: Se0/0/1 IPCP: CP unstall
.Jun 20 04:25:02.127: Se0/0/1 PPP: Phase is FORWARDING, Attempting Forward
.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is AUTHENTICATING, Authenticated User
.Jun 20 04:25:02.135: Se0/0/1 CHAP: O SUCCESS id 1 len 4
.Jun 20 04:25:02.135: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
.Jun 20 04:25:02.135: Se0/0/1 PPP: Outbound cdp packet dropped, line protocol
not up
.Jun 20 04:25:02.135: Se0/0/1 PPP: Phase is UP
.Jun 20 04:25:02.135: Se0/0/1 IPCP: Protocol configured, start CP.
state[Initial]
.Jun 20 04:25:02.135: Se0/0/1 IPCP: Event[OPEN] State[Initial to Starting]
.Jun 20 04:25:02.135: Se0/0/1 IPCP: O CONFREQ [Starting] id 1 len 10
<output omitted>
.Jun 20 04:25:02.143: Se0/0/1 CDPCP: I CONFACK [ACKsent] id 1 len 4
.Jun 20 04:25:02.143: Se0/0/1 CDPCP: Event[Receive ConfAck] State[ACKsent to
Open]
.Jun 20 04:25:02.155: Se0/0/1 IPCP: State is Open
.Jun 20 04:25:02.155: Se0/0/1 CDPCP: State is Open
.Jun 20 04:25:02.155: Se0/0/1 Added to neighbor route AVL tree: topoid 0,
address 10.2.2.2
.Jun 20 04:25:02.155: Se0/0/1 IPCP: Install route to 10.2.2.2
.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 04:25:02.155: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 80 link[ip]
.Jun 20 04:25:02.155: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 84
.Jun 20 04:25:02.167: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 84 link[ip]
.Jun 20 04:25:02.167: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 04:25:02.171: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 68 link[ip]
.Jun 20 04:25:02.171: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 148
.Jun 20 04:25:02.191: Se0/0/1 PPP: I pkt type 0x0021, datagramsize 148 link[ip]
.Jun 20 04:25:02.191: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
.Jun 20 04:25:02.191: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 68
.Jun 20 04:25:02.571: Se0/0/1 PPP: O pkt type 0x0021, datagramsize 80
.Jun 20 04:25:03.155: Se0/0/1 PPP: I pkt type 0x0207, datagramsize 333
link[cdp]
.Jun 20 04:25:03.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339
.Jun 20 04:25:04.155: Se0/0/1 PPP: O pkt type 0x0207, datagramsize 339
```

From the PPP debug messages, what phases did the Branch3 router go through before the link is up with the Central router?

_____

_____

e. Issue the **debug ppp authentication** command to observe the CHAP authentication messages on the Central router.

```
Central# debug ppp authentication
PPP authentication debugging is on
```

f. Configure CHAP authentication on S0/0/1 on the Central router.

_____

_____

g. Observe the debug PPP messages relating to CHAP authentication on the Central router.

```
Central(config-if)#
.Jun 20 05:05:16.057: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
.Jun 20 05:05:16.061: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1
from FULL to DOWN, Neighbor Down: Interface down or detached
.Jun 20 05:05:16.061: Se0/0/1 PPP: Using default call direction
.Jun 20 05:05:16.061: Se0/0/1 PPP: Treating connection as a dedicated line
.Jun 20 05:05:16.061: Se0/0/1 PPP: Session handle[12000078] Session id[112]
.Jun 20 05:05:16.081: Se0/0/1 CHAP: O CHALLENGE id 1 len 28 from "Central"
.Jun 20 05:05:16.089: Se0/0/1 CHAP: I CHALLENGE id 1 len 28 from "Branch3"
.Jun 20 05:05:16.089: Se0/0/1 PPP: Sent CHAP SENDAUTH Request
.Jun 20 05:05:16.089: Se0/0/1 PPP: Received SENDAUTH Response PASS
.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using hostname from configured hostname
.Jun 20 05:05:16.089: Se0/0/1 CHAP: Using password from AAA
.Jun 20 05:05:16.089: Se0/0/1 CHAP: O RESPONSE id 1 len 28 from "Central"
.Jun 20 05:05:16.093: Se0/0/1 CHAP: I RESPONSE id 1 len 28 from "Branch3"
.Jun 20 05:05:16.093: Se0/0/1 PPP: Sent CHAP LOGIN Request
.Jun 20 05:05:16.093: Se0/0/1 PPP: Received LOGIN Response PASS
.Jun 20 05:05:16.093: Se0/0/1 CHAP: O SUCCESS id 1 len 4
.Jun 20 05:05:16.097: Se0/0/1 CHAP: I SUCCESS id 1 len 4
.Jun 20 05:05:16.097: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
.Jun 20 05:05:16.165: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.3.1 on Serial0/0/1
from LOADING to FULL, Loading Done
```

h. Issue the **undebug all** (or **u all**) command on the Central and Branch3 routers to turn off all debugging.

```
Central# undebug all
All possible debugging has been turned off
```

Step 3. Intentionally break the serial link configured with authentication.

a. On the Central router, configure a username for use with Branch1. Assign **cisco** as the password.

```
Central(config)# username Branch1 password cisco
```

b. On the Central and Branch1 routers, configure CHAP authentication on interface S0/0/0. What is happening with the interface?

_____

Note: To speed up the process, shut down the interface and enable it again.

c. Use a **debug ppp negotiation** command to examine what is happening.

```
Central# debug ppp negotiation
PPP protocol negotiation debugging is on
Central(config-if)#
.Jun 20 05:25:26.229: Se0/0/0 PPP: Missed a Link-Up transition, starting PPP
.Jun 20 05:25:26.229: Se0/0/0 PPP: Processing FastStart message
.Jun 20 05:25:26.229: PPP: Alloc Context [29F9F32C]
.Jun 20 05:25:26.229: ppp145 PPP: Phase is ESTABLISHING
.Jun 20 05:25:26.229: Se0/0/0 PPP: Using default call direction
.Jun 20 05:25:26.229: Se0/0/0 PPP: Treating connection as a dedicated line
.Jun 20 05:25:26.229: Se0/0/0 PPP: Session handle[6000009C] Session id[145]
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[OPEN] State[Initial to Starting]
.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFREQ [Starting] id 1 len 15
.Jun 20 05:25:26.229: Se0/0/0 LCP:    AuthProto CHAP (0x0305C22305)
.Jun 20 05:25:26.229: Se0/0/0 LCP:    MagicNumber 0x74385C31 (0x050674385C31)
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[UP] State[Starting to REQsent]
.Jun 20 05:25:26.229: Se0/0/0 LCP: I CONFREQ [REQsent] id 1 len 10
.Jun 20 05:25:26.229: Se0/0/0 LCP:    MagicNumber 0x8D920101 (0x05068D920101)
.Jun 20 05:25:26.229: Se0/0/0 LCP: O CONFACK [REQsent] id 1 len 10
.Jun 20 05:25:26.229: Se0/0/0 LCP:    MagicNumber 0x8D920101 (0x05068D920101)
.Jun 20 05:25:26.229: Se0/0/0 LCP: Event[Receive ConfReq+] State[REQsent to
ACKsent]
.Jun 20 05:25:26.233: Se0/0/0 LCP: I CONFACK [ACKsent] id 1 len 15
.Jun 20 05:25:26.233: Se0/0/0 LCP:    AuthProto CHAP (0x0305C22305)
.Jun 20 05:25:26.233: Se0/0/0 LCP:    MagicNumber 0x74385C31 (0x050674385C31)
.Jun 20 05:25:26.233: Se0/0/0 LCP: Event[Receive ConfAck] State[ACKsent to
Open]
.Jun 20 05:25:26.261: Se0/0/0 PPP: Phase is AUTHENTICATING, by this end
.Jun 20 05:25:26.261: Se0/0/0 CHAP: O CHALLENGE id 1 len 28 from "Central"
.Jun 20 05:25:26.261: Se0/0/0 LCP: State is Open
.Jun 20 05:25:26.265: Se0/0/0 LCP: I TERMREQ [Open] id 2 len 4
.Jun 20 05:25:26.265: Se0/0/0 PPP DISC: Received LCP TERMREQ from peer
.Jun 20 05:25:26.265: PPP: NET STOP send to AAA.
.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is TERMINATING
.Jun 20 05:25:26.265: Se0/0/0 LCP: O TERMACK [Open] id 2 len 4
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[Receive TermReq] State[Open to
Stopping]
.Jun 20 05:25:26.265: Se0/0/0 PPP: Sending cstate DOWN notification
.Jun 20 05:25:26.265: Se0/0/0 PPP: Processing CstateDown message
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[CLOSE] State[Stopping to Closing]
.Jun 20 05:25:26.265: Se0/0/0 LCP: Event[DOWN] State[Closing to Initial]
.Jun 20 05:25:26.265: Se0/0/0 PPP: Phase is DOWN
```

Explain what is causing the link to terminate. Correct the issue and document the command issued to correct the issue in the space provided below.

_____

_____

_____

d. Issue the **undebug all** command on all routers to turn off debugging.

e. Verify end-to-end connectivity.

Reflection

1. What are the indicators that you may have a serial encapsulation mismatch on a serial link?

_____

2. What are the indicators that you may have an authentication mismatch on a serial link?

_____

Router Interface Summary Table

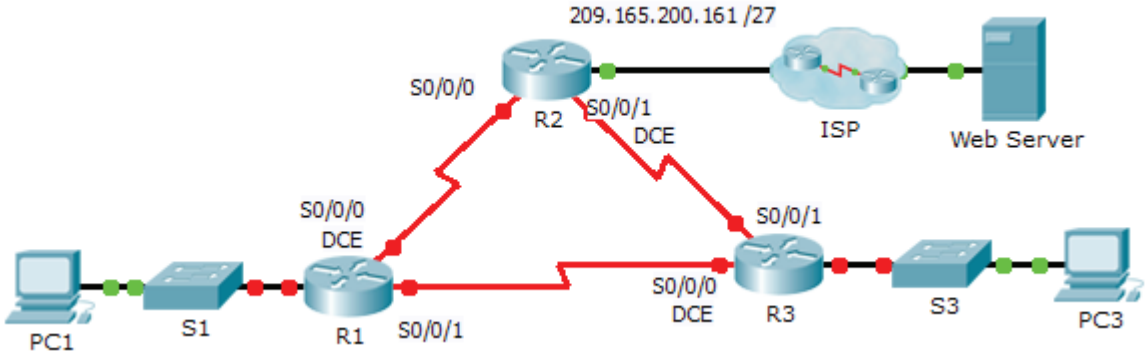
Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parentheses is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Packet Tracer Activity

2.4.1.4 Packet Tracer–Troubleshooting PPP with Authentication

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	10.0.0.1	255.255.255.128	N/A
	S0/0/0	172.16.0.1	255.255.255.252	N/A
	S0/0/1	172.16.0.9	255.255.255.252	N/A
R2	G0/1	209.165.200.161	255.255.255.224	N/A
	S0/0/0	172.16.0.2	255.255.255.252	N/A
	S0/0/1	172.16.0.5	255.255.255.252	N/A
R3	G0/1	10.0.0.129	255.255.255.128	N/A
	S0/0/0	172.16.0.10	255.255.255.252	N/A
	S0/0/1	172.16.0.6	255.255.255.252	N/A
ISP	G0/1	209.165.200.162	255.255.255.224	N/A
PC1	NIC	10.0.0.10	255.255.255.128	10.0.0.1
PC3	NIC	10.0.0.139	255.255.255.128	10.0.0.129
Web Server	NIC	209.165.200.2	255.255.255.252	209.165.200.1

Objectives

Part 1: Diagnose and Repair the Physical Layer

Part 2: Diagnose and Repair the Data Link Layer

Part 3: Diagnose and Repair the Network Layer

Scenario

The routers at your company were configured by an inexperienced network engineer. Several errors in the configuration have resulted in connectivity issues. Your boss has asked you to troubleshoot and correct the configuration errors and document your work. Using your knowledge of PPP and standard testing methods, find and correct the errors. Make sure that all of the serial links use PPP CHAP authentication, and that all of the networks are reachable. The passwords are **cisco** and **class**.

Part 1: Diagnose and Repair the Physical Layer

Step 1. Diagnose and repair the cabling.

a. Examine the **Addressing Table** to determine the location of all the connections.

b. Verify cables are connected as specified.

c. Diagnose and repair any inactive interfaces.

Part 2: Diagnose and Repair the Data Link Layer

Step 1. Examine and set clock rates on the DCE equipment.

Examine the configuration of each router to verify that a clock rate has been set on appropriate interfaces. Set the clock rate of any serial interface that requires it.

Step 2. Examine the encapsulation on the DCE equipment.

All of the serial interfaces should be using PPP as the encapsulation type. Change the encapsulation type to PPP for any interface that is set otherwise.

Step 3. Examine and set CHAP usernames and passwords.

Examine each link to verify that routers are logging into each other correctly. All CHAP passwords are set to **cisco**. Use the **debug ppp authentication** command if needed. Correct or set any usernames and passwords that need it.

Part 3: Diagnose and Repair the Network Layer

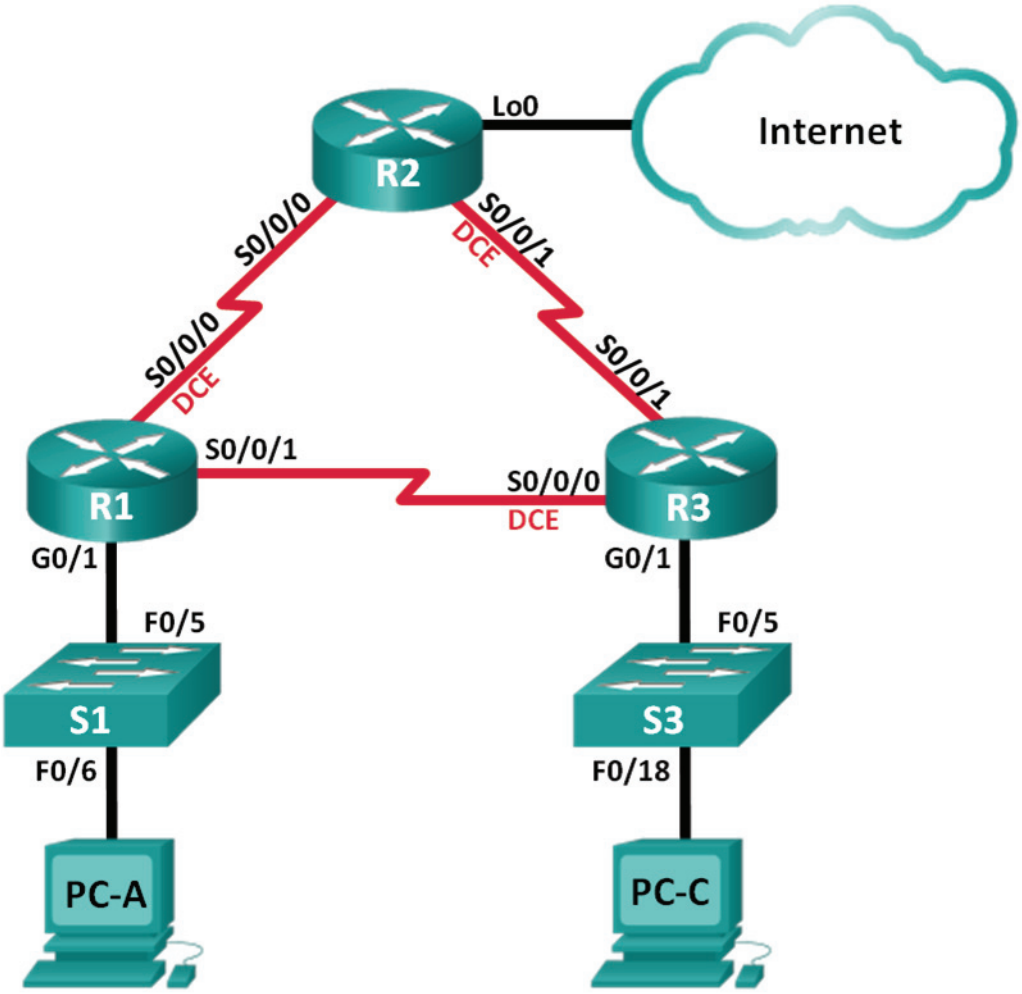
Step 1. Verify the IP addressing.

Check IP addresses against the Addressing Table and ensure that they are in the correct subnet with their connecting interface. Correct any IP addresses that overlap, are on the wrong interface, have the wrong subnet address, or are set to the host or broadcast address.

Step 2. Verify full connectivity by tracing a path from **PC1** and **PC3** to the Web Server.

2.4.1.5 Lab–Troubleshooting Basic PPP with Authentication

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.12.1	255.255.255.252	N/A
	S0/0/1	192.168.13.1	255.255.255.252	N/A
R2	Lo0	209.165.200.225	255.255.255.252	N/A
	S0/0/0	192.168.12.2	255.255.255.252	N/A
	S0/0/1 (DCE)	192.168.23.1	255.255.255.252	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.13.2	255.255.255.252	N/A
	S0/0/1	192.168.23.2	255.255.255.252	N/A

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objectives

Part 1: Build the Network and Load Device Configurations

Part 2: Troubleshoot the Data Link Layer

Part 3: Troubleshoot the Network Layer

Background/Scenario

The routers at your company were configured by an inexperienced network engineer. Several errors in the configuration have resulted in connectivity issues. Your manager has asked you to troubleshoot and correct the configuration errors and document your work. Using your knowledge of PPP and standard testing methods, find and correct the errors. Ensure that all of the serial links use PPP CHAP authentication, and that all of the networks are reachable.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows with a terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Load Device Configurations

In Part 1, you will set up the network topology, configure basic settings on the PC hosts, and load configurations on the routers.

Step 1. Cable the network as shown in the topology.

Step 2. Configure the PC hosts.

Step 3. Load router configurations.

Load the following configurations into the appropriate router. All routers have the same passwords. The privileged EXEC mode password is **class**. The password for console and vty access is **cisco**. All serial interfaces should be configured with PPP encapsulation and authenticated with CHAP using the password of **chap123**.

Router R1 Configuration:

```
hostname R1
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R2 password chap123
username R3 password chap123
interface g0/1
 ip address 192.168.1.1 255.255.255.0
 no shutdown
interface s0/0/0
 ip address 192.168.12.1 255.255.255.252
 clock rate 128000
 encapsulation ppp
 ppp authentication chap
interface s0/0/1
 ip address 192.168.31.1 255.255.255.252
 encapsulation ppp
 ppp authentication pap
exit
router ospf 1
 router-id 1.1.1.1
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.13.0 0.0.0.3 area 0
 passive-interface g0/1
 exit
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
```

Router R2 Configuration:

```
hostname R2
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R1 password chap123
username r3 password chap123
```

```
interface lo0
 ip address 209.165.200.225 255.255.255.252
interface s0/0/0
 ip address 192.168.12.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
interface s0/0/1
 ip address 192.168.23.1 255.255.255.252
 clock rate 128000
 no shutdown
 exit
router ospf 1
 router-id 2.2.2.2
 network 192.168.12.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
 default-information originate
 exit
ip route 0.0.0.0 0.0.0.0 loopback0
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
```

Router R3 Configuration:

```
hostname R3
enable secret class
no ip domain lookup
banner motd #Unauthorized Access is Prohibited!#
username R2 password chap123
username R3 password chap123
interface g0/1
 ip address 192.168.3.1 255.255.255.0
 no shutdown
interface s0/0/0
 ip address 192.168.13.2 255.255.255.252
 clock rate 128000
 encapsulation ppp
 ppp authentication chap
 no shutdown
interface s0/0/1
 ip address 192.168.23.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
 exit
router ospf 1
 router-id 3.3.3.3
```

```
 network 192.168.13.0 0.0.0.3 area 0
 network 192.168.23.0 0.0.0.3 area 0
 passive-interface g0/1
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
```

Step 4. Save your running configuration.

Part 2: Troubleshoot the Data Link Layer

In Part 2, you will use **show** commands to troubleshoot data link layer issues. Be sure to verify settings, such as clock rate, encapsulation, CHAP, and usernames/passwords.

Step 1. Examine the R1 configuration.

a. Use the **show interfaces** command to determine whether PPP has been established on both serial links.

From the **show interfaces** results for S0/0/0 and S0/0/1, what are possible issues with the PPP links?

_____

_____

_____

b. Use the **debug ppp authentication** command to view real-time PPP authentication output during troubleshooting.

```
R1# debug ppp authentication
PPP authentication debugging is on
```

c. Use the **show run interface s0/0/0** command to examine the settings on S0/0/0.

Resolve all problems found for S0/0/0. Record the commands used to correct the configuration.

_____

_____

After correcting the issue, what information does the debug output provide?

_____

_____

d. Use the **show run interface s0/0/1** command to examine the settings on S0/0/1.

Resolve all problems found for S0/0/1. Record the commands used to correct the configuration.

_____

_____

_____

After correcting the issue, what information does the debug output provide?

_____

_____

_____

e. Use the **no debug ppp authentication** or **undebug all** command to turn off the debug PPP output.

f. Use the **show running-config | include username** command to verify the correct username and password configurations.

Resolve all problems found. Record the commands used to correct the configuration.

_____

Step 2. Examine the R2 configuration.

a. Use the **show interfaces** command to determine if PPP has been established on both serial links.

Have all links been established? _____

If the answer is no, which links need to be examined? What are the possible issues?

_____

_____

_____

b. Use the **show run interface** command to examine links that have not been established.

Resolve all problems found for the interfaces. Record the commands used to correct the configuration.

_____

_____

_____

c. Use the **show running-config | include username** command to verify the correct username and password configurations.

Resolve all problems found. Record the commands used to correct the configuration.

_____

_____

d. Use the **show ppp interface serial** command for the serial interface that you are troubleshooting.

Has the link been established? _____

Step 3. Examine the R3 configuration.

a. Use the **show interfaces** command to determine whether PPP has been established on both serial links.

Have all links been established? _____

If the answer is no, which links need to be examined? What are the possible issues?

_____

_____

b. Use the **show run interface** command to examine any serial link that has not been established.

Resolve all problems found on the interfaces. Record the commands used to correct the configuration.

_____

_____

c. Use the **show running-config | include username** command to verify the correct username and password configurations.

Resolve all problems found. Record the commands used to correct the configuration.

_____

_____

d. Use the **show interface** command to verify that serial links have been established.

e. Have all PPP links been established?_____

f. Can PC-A ping Lo0? _____

g. Can PC-A ping PC-C? _____

Note: It may be necessary to disable the PC firewall for pings between the PCs to succeed.

Part 3: Troubleshoot the Network Layer

In Part 3, you will verify that Layer 3 connectivity is established on all interfaces by examining IPv4 and OSPF configurations.

Step 1. Verify that the interfaces listed in the Addressing Table are active and configured with the correct IP address information.

Issue the **show ip interface brief** command on all routers to verify that the interfaces are in an up/up state.

Resolve all problems found. Record the commands used to correct the configuration.

_____

_____

Step 2. Verify OSPF Routing

Issue the **show ip protocols** command to verify that OSPF is running and that all networks are advertised.

Resolve all problems found. Record the commands used to correct the configuration.

_____

_____

Can PC-A ping PC-C? _____

If connectivity does not exist between all hosts, then continue troubleshooting to resolve any remaining issues.

Note: It may be necessary to disable the PC firewall for pings between the PCs to succeed.

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parentheses is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

2.5.1.1 Class Activity–PPP Validation

Objective

Use **show** and **debug** commands to troubleshoot PPP.

Scenario

Three friends who are enrolled in the Cisco Networking Academy want to check their knowledge of PPP network configuration.

They set up a contest where each person will be tested on configuring PPP with defined PPP scenario requirements and varying options. Each person devises a different configuration scenario.

Below are some suggested scenarios:

Scenario 1

- Address the topology using IPv4.
- Configure PPP encapsulation with CHAP.
- Configure OSPF routing.
- Configure the clock to read today's date.
- Change the OSPF router priorities on both serial interfaces.

Scenario 2

- Address the topology using IPv6.
- Configure PPP encapsulation with PAP.
- Configure EIGRP routing.
- Configure the clock to read the current time.
- Place a description on both connected serial interfaces.

Scenario 3

- Address the topology using IPv6.
- Configure a Message of the Day.
- Configure PPP with CHAP.
- Configure OSPF routing.
- Configure the clock to read today's time and date.

Resources

- Packet Tracer software
- Stopwatch or timer

Step 1. Open Packet Tracer.

- **a.** Create a two-router topology with a serial connection.
- **b.** Include one PC and switch attached to each router.

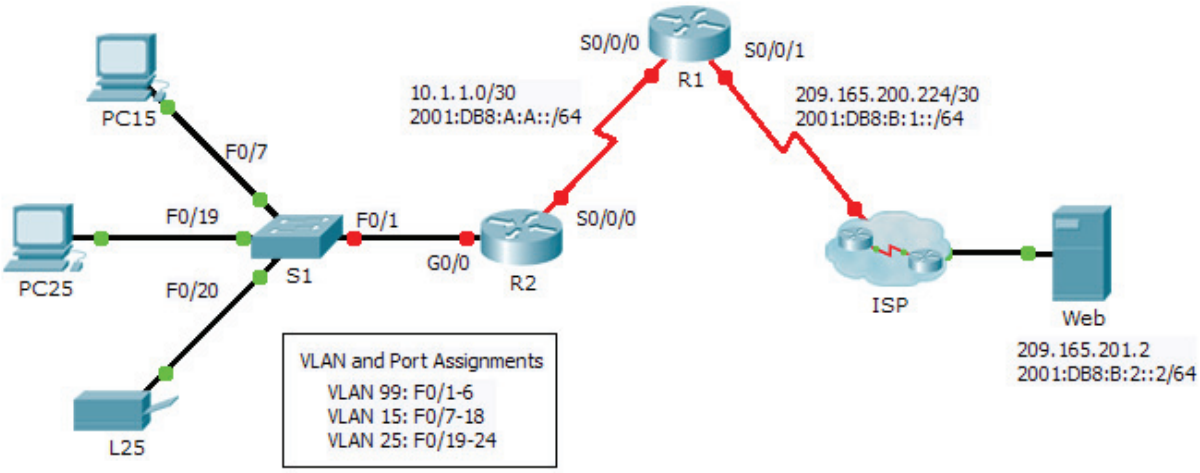
Step 2. Complete the first scenario.

- **a.** Start the assigned scenario.
- **b.** The instructor calls the time when the scenario is completed; all students and groups must stop their configuration work at that time.
- **c.** The instructor checks the validity of the completed scenario configuration.
  - **1)** The devices must be able to successfully ping from one end of the topology to the other.
  - **2)** All scenario options requested must be present in the final topology.
  - **3)** The instructor may ask you to prove your work by choosing different **show** and **debug** commands to display the configuration output.
- **d.** Begin the same process for the second scenario assigned by the instructor.
  - **1)** Delete the configurations from the first scenario, but you can re-use the same configurations.
  - **2)** Complete Steps 1 and 2 again using the next scenario's requirements.

Packet Tracer ☐ Activity

2.5.1.2 Packet Tracer–Skills Integration Challenge

Topology



Addressing Table

Device	Interface	IPv4 Address	Subnet Mask	IPv4 and IPv6 Default Gateway
		IPv6 Address/Prefix		
R1	S0/0/0	10.1.1.2	255.255.255.252	N/A
		2001:DB8:A:A::2/64		FE80::1
	S0/0/1	209.165.200.226	255.255.255.252	N/A
		2001:DB8:B:1::2/64		FE80::1
R2	G0/0.1	192.168.1.193	255.255.255.224	N/A
		2001:DB8:A:1::1/64		FE80::2
	G0/0.15	192.168.1.1	255.255.255.128	N/A
		2001:DB8:A:15::1/64		FE80::2
	G0/0.25			N/A
		2001:DB8:A:25::1/64		FE80::2
	G0/0.99	192.168.1.225	255.255.255.224	N/A
		2001:DB8:A:99::1/64		FE80::2
	S0/0/0	10.1.1.1	255.255.255.252	N/A
		2001:DB8:A:A::1/64		FE80::2
S1	VLAN 99	192.168.1.226	255.255.255.224	192.168.1.225
PC15	NIC	192.168.1.2	255.255.255.128	192.168.1.1
		2001:DB8:A:15::2/64		FE80::2
PC25	NIC			
		2001:DB8:A:25::2/64		FE80::2
L25	NIC			
		2001:DB8:A:25::A/64		FE80::2

Background

This activity allows you to practice a variety of skills including configuring VLANs, PPP with CHAP, static and default routing, using IPv4 and IPv6. Due to the sheer number of graded elements, you can click **Check Results** and **Assessment Items** to see if you correctly entered a graded command. Use the **cisco** and **class** passwords to access privileged EXEC modes of the CLI for routers and switches.

Requirements

Addressing

- The addressing scheme uses the 192.168.1.0/24 address space. Additional address space is available between VLAN 15 and VLAN 1. VLAN 25 needs enough addresses for 50 hosts. Determine the subnet and complete the subnet table below.

VLAN	IPv4 Subnet Address	Subnet Mask	Hosts
1	192.168.1.192	255.255.255.224	20
15	192.168.1.0	255.255.255.128	100
25			50
99	192.168.1.224	255.255.255.224	20

- Complete the **Addressing Table** by assigning the following addresses to VLAN 25:
  - **R2 G0/0.25** - First IPv4 address
  - **PC25** - 2nd IPv4 address
  - **L25** - Last IPv4 address
- Configure IPv4 addressing on the necessary end devices.
- On **R2**, create and apply IPv4 and IPv6 addressing to the G0/0.25 subinterface.

VLANs

- On **S1**, create VLAN 86 and name it **BlackHole**.
- Configure **S1** ports in static mode with the following requirements:
  - **F0/1** is the native trunk for VLAN 99.
  - **F0/7 - F0/18** as access ports in VLAN 15.
  - **F0/19 - F0/24** as access ports in VLAN 25.
  - **G0/1 - 2** and **F0/2 - F0/6** are unused. They should be properly secured and assigned to the **BlackHole** VLAN.
- On **R2**, configure inter-VLAN routing. VLAN 99 is the native VLAN.

PPP

- Configure **R1** and **R2** to use PPP with CHAP for the shared link. The password for CHAP is **cisco**.

Routing

- On **R1**, configure IPv4 and IPv6 default routes using the appropriate exit interface.
- On **R2**, configure an IPv6 default route using the appropriate exit interface.
- Configure IPv4 OSPF using the following requirements:
  - Use process ID 1.
  - Routers **R1** and **R2** are in area 0.
  - **R1** uses router ID 1.1.1.1.
  - **R2** uses router ID 2.2.2.2.
  - Advertise specific subnets.
  - On **R1**, propagate the IPv4 default route created.
- Configure IPv6 OSPF using the following requirements:
  - Use process ID 1.
  - Routers **R1** and **R2** are in area 0.
  - Configure OSPF on appropriate interfaces on **R1** and **R2**.
  - **R1** uses router ID 1.1.1.1.
  - **R2** uses router ID 2.2.2.2.

Connectivity

- All devices should be able to ping the Web Server.

CHAPTER 3

Branch Connections

With the advent of broadband technologies like digital subscriber line (DSL) and cable, working from home has become a popular option for both employees and companies alike. Virtual private networks (VPN) allow workers to securely connect to the business from remote locations. There are several factors to consider when choosing a broadband solution. This chapter reviews DSL, cable, wireless, VPN, and the factors to consider when implementing broadband solutions. In addition, the protocols Generic Routing Encapsulation (GRE) and Border Gateway Protocol (BGP) are reviewed.

Broadband Connections

Depending on the location of the teleworker, connecting to the corporate network can be done in one of three ways: cable, DSL, or broadband wireless.

Cable

Cable broadband uses a coaxial cable that carries _____ signals across the network. What portion of the electromagnetic spectrum do these signals occupy?

_____

Traditionally, cable communication was one way. Modern cable systems now provide two-way communication. What three main telecommunication services are offered by today's cable companies?

_____

Two-way communications occur downstream in the 50- to 860-MHz range and upstream in the 5- to 42-MHz range.

The _____ is the international standard developed by CableLabs that cable operators use to provide Internet access over their existing _____ infrastructure.

What two types of equipment are required to send digital modem signals upstream and downstream on a cable system?

_____

_____

Match the definition on the left with a term on the right. Terms are only used once.

Definitions

a. Combining both fiber-optic and coax cabling together into a hybrid cabling infrastructure

b. Defines the communications and operation support interface that permits the addition of high-speed data transfer to a traditional cable TV system

c. The direction of a signal transmission from the headend to subscribers

d. Located in the headend (and communicates with CMs located in subscriber homes)

e. The rate at which current (voltage) cycles (computed as the number of waves per second)

f. The direction of a signal transmission from subscribers to the headend

Terms

___ CMTS

___ DOCSIS

___ Downstream

___ Frequency

___ HFC

___ Upstream

DSL

Digital subscriber line (DSL) technology takes advantage of the additional bandwidth available in telephone networks between 3 KHz and 1 MHz.

Briefly describe the two main types of DSL.

_____

_____

The local loop connection to the CO must be less than 3.39 miles (5.46 km).

What two components are required to provide a DSL connection to the teleworker?

_____

_____

_____

The analog voice and ADSL signals must be separated to avoid interference. What two devices can separate the signals?

_____

_____

Match the definition on the left with a term on the right. Terms are only used once.

Definitions

a. Located at the CO, a device that combines individual DSL connections from subscribers into one high-capacity link to an ISP

b. Sometimes referred to as the DSL modem, a device that connects the subscriber to the DSL network

c. The category of DSL technology that provides high-speed downstream data capacity value with a lower upstream capacity value

d. Device with one end connecting to a telephone device and the other end connecting to the telephony wall jack

e. Category of DSL technology that provides equal high-speed downstream and upstream data capacities

f. A means of providing high-speed connections over pre-existing installed copper wire infrastructure

Terms

___ ADSL
___ DSL
___ DSLAM
___ Microfilter
___ SDSL
___ Transceiver

Broadband Wireless

Of the three broadband technologies, wireless offers the largest variety of ways to connect. Whether from your laptop or from a smartphone, urban or rural, broadband wireless has a solution.

Match the definition on the left with a term on the right. Terms are only used once.

Definitions

a. Uses a point-to-multipoint topology to provide wireless cellular broadband access at speeds up to 1 Gbps

b. Newer and faster technology for high-speed cellular data (considered to be part of 4G)

c. Cellular broadband access that gets faster with each generation

d. Employs a mesh network with an access point at each node for 802.11 connections

e. A general term for Internet service from a mobile phone or any other mobile device that uses the same technology

f. Two-way satellite Internet using IP multicasting technology

Terms

___ 3G/4G Wireless
___ LTE
___ Municipal WiFi
___ VSAT
___ WiMAX
___ Wireless Internet

Select a Broadband Solution Connection

Ideally, a teleworker would have a fiber-optic cable directly connected to the home office. When selecting the broadband solution that is right for you, you want to consider several factors. In Table 3-1, indicate the factors for each broadband solution.

Table 3-1 Broadband Solutions: Factors to Consider

Factor to Consider	Cable	DSL	Fiber-to-the-Home	Cellular/ Mobile	Wi-Fi Mesh	WiMAX	Satellite
Requires fiber installation directly to the home.							
Coverage is often an issue, bandwidth is limited, and data may not be unlimited.							
Bit rate is limited to 2 Mbps per subscriber, cell size is 1 to 2 km (1.25 mi).							
Bandwidth is shared by many users, and upstream data rates are often slow.							
Limited bandwidth that is distance sensitive, and the upstream rate is proportionally quite small compared to downstream rate.							
Expensive, limited capacity per subscriber; often provides access where no other access is possible.							
Most municipalities do not have a mesh network deployed; if it is available and the SOHO is in range, it is a viable option.							

PPPoE

The underlying data link protocol commonly used by Internet service providers (ISPs) to send and receive data across DSL links is PPP over Ethernet (PPPoE).

PPPoE Overview

For the ISP, what are the benefits of using PPP?

_____

_____

What are the three stages of evolution in teleworker connections from the home that use PPP?

_____

Configuring PPPoE

Although PPPoE configuration is beyond the scope of the course, understanding how PPPoE is implemented will help solidify your skills in configuring PPP.

The two steps to configure PPPoE are as follows:

Step 1. Create a PPP tunnel using dialer interface with the following settings:

- Encapsulation is PPP.
- IP address is negotiated.
- MTU size is set to 1492. Why?

_____

_____

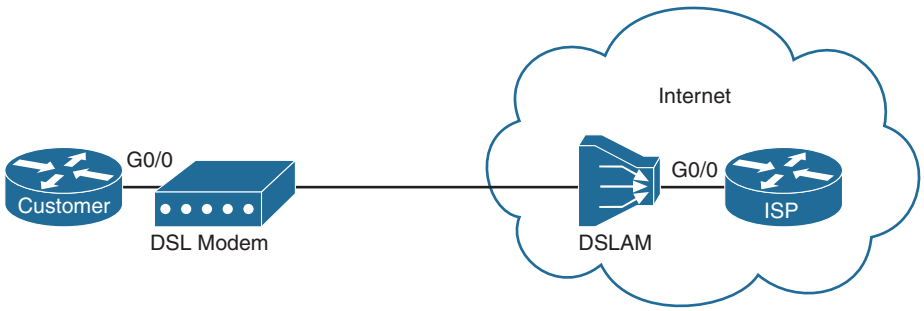
- Dialer interface is assigned a pool.
- CHAP authentication with username and password assigned by ISP.

Step 2. Enable PPPoE on the interface attached to the DSL modem and assign it as a PPPoE client using the dialer pool defined in Step 1.

You can verify the dialer interface was assigned an IP address with the **show ip interface brief** command.

In Figure 3-1, the ISP router is already configured. Record the commands to configure the Customer router using the following CHAP information:

Figure 3-1 PPPoE Configuration Topology



- Username is CustomerBob.
- Password is Bob$connect.

_____

_____

_____

_____

_____

_____

_____

If you want to configure this on lab equipment, connect two routers through a switch or with a cross-over cable and use the following configuration for ISP:

```
username CustomerBob password Bob$connect
!
bba-group pppoe global
 virtual-template 1
!
interface GigabitEthernet0/0
 no ip address
 pppoe enable group global
 no shutdown
!
interface Virtual-Template1
 mtu 1492
 ip address 64.100.1.254 255.255.255.0
 peer default ip address pool CUSTOMER_POOL
 ppp authentication chap callin
!
ip local pool CUSTOMER_POOL 64.100.1.1 64.100.1.253
```

VPNs

With the proper implementation at that central site, VPNs provide the flexibility of having safe and secure connections regardless of the underlying access technology. This is increasingly important as more users need or want access to their corporate networks no matter their current location.

Fundamentals of VPNs

VPNs are used to create a private tunnel over the Internet regardless of the WAN access option used to make the connection.

Briefly describe three different scenarios in which VPNs are a viable solution.

What is the difference between VPN and secure VPN?

To implement a VPN, a VPN gateway is needed. List three devices that can serve as a VPN gateway.

Briefly describe four benefits to using VPNs.

Types of VPNs

There are two main types of VPN networks. Site-to-site VPNs support connections where the two locations are permanent and contain more than one user. For example, a branch site or a business partner site most likely would benefit from a site-to-site VPN. Remote-access VPNs are best used for single user connection needs such as teleworkers and mobile users.

In Table 3-2, indicate the type of VPN described by each characteristic.

Table 3-2 Comparing Site-to-Site and Remote-Access VPNs

Characteristic	Site-to-Site VPN	Remote-Access VPNs
VPN is dynamically enabled when needed.		
Most likely uses VPN client software to establish VPN connection and encrypt data.		
Users have no knowledge of the VPN.		
Connects networks together through peer VPN gateways.		
Uses a client/server model.		
Connects teleworkers and mobile users.		
VPN connection is static.		

Dynamic Multipoint VPN (DMVPN) is a Cisco software solution for building multiple VPNs in an easy, dynamic, and scalable manner. Multiple branch VPNs can be connected easily to the central office in a hub-and-spoke topology. Spoke-to-spoke VPNs can be dynamically created as needed when branches offices need to communicate directly.

List and define the three main technologies that are used to create DMVPNs:

GRE

Generic routing encapsulation (GRE) is a site-to-site VPN tunneling protocol developed by Cisco. GRE can encapsulate a wide variety of protocol packet types inside IP tunnels.

Fundamentals of Generic Routing Encapsulation

List three protocols that GRE can encapsulate.

_____

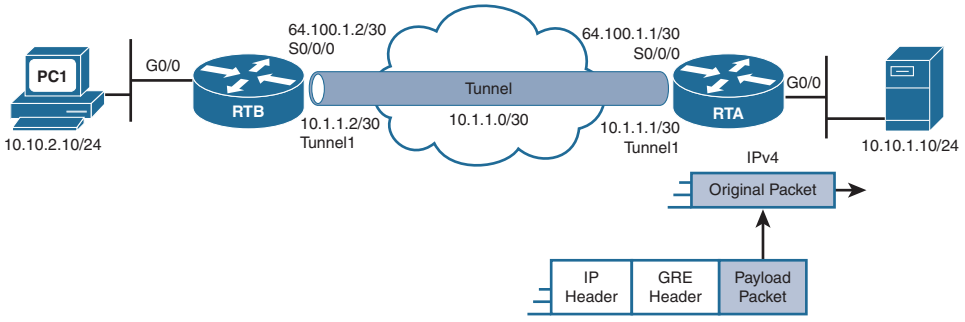
Figure 3-2 shows the basic fields in a GRE encapsulated packet.

Figure 3-2 GRE Encapsulated Packet

Figure 3-3 shows the topology we will use to configure GRE later in this section. Notice how the protocol packet, IP, is encapsulated with GRE, then encapsulated in an IP packet for transport across the Internet. The inside IP packet is using private addressing and the outside IP packet is using public addressing.

Note: The public addressing is on the same subnet. This is uncommon on real networks. However, we are doing it here so that you can easily attach to routers and use this configuration for practice.

Figure 3-3 GRE Topology



GRE is defined by IETF RFC _____. In the outer IP header, _____ is used in the Protocol field to indicate that a GRE header follows. In the GRE header, a Protocol _____ field specifies the OSI Layer 3 protocol that is encapsulated (IP in Figure 3-3). GRE is _____, meaning that it does not include any flow-control mechanisms. Also, GRE does not include any _____ mechanisms to protect the payload. The GRE header and additional IP header create at least _____ bytes of additional overhead for tunneled packets.

Configuring GRE Tunnels

In Figure 3-3 shown earlier, assume the physical interfaces on RTA and RTB are configured and active. Also assume that RTA is already configured with a GRE tunnel and OSPF routing. To configure GRE on RTB, complete the following steps:

Step 1. Create a tunnel interface using the **interface tunnel** *number* command. The interface numbers do not have to match between RTA and RTB.

Step 2. Configure an IP address for the tunnel interface. The two routers on the tunnel should use addresses from the same subnet. In our topology, the subnet is 10.1.1.0/30.

Step 3. Specify the tunnel's source IP address in the public part of the network with the **tunnel source** *ip-address* command. The IP address must match the other side's configuration for **tunnel destination** *ip-address*. For RTB, this address is the 64.100.1.2 IP address configured on its S0/0/0 interface.

Step 4. Specify the tunnel's destination IP address in the public part of the network with the **tunnel destination** *ip-address* command. The IP address must match the other side's **tunnel source** *ip-address*. For RTB, this address is the 64.100.1.1 IP address configured on RTA's S0/0/0.

Step 5. Configure routing to use the tunnel to advertise the private LANs at each site.

Note: These steps do not include configuring the **tunnel mode** command because the default, GRE IP, is what is needed here. However, in the future, the GRE tunnel will most likely be IPv6.

Using these steps, record the commands including the router prompt to configure RTB with a GRE tunnel to RTA.

_____

_____

_____

_____

_____

_____

_____

A number of commands can be used to verify the GRE tunnel is operational. Of course, the ultimate test is that PC1 should now be able to ping the server attached to the RTA LAN. If connectivity fails, use the following commands to troubleshoot the issue.

Record the commands and command filtering used to generate the following output.

```
RTB# _____________________________________________________

Neighbor ID     Pri   State           Dead Time   Address         Interface
64.100.1.1        0   FULL/  -        00:00:34    10.1.1.1        Tunnel1
RTB# _____________________________________________________
Tunnel1                    10.1.1.2        YES manual up                    up
RTB# _____________________________________________________
Gateway of last resort is not set
```

```
      10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
O        10.10.1.0/24 [110/1001] via 10.1.1.1, 00:23:49, Tunnel1
RTB# _____________________________________________________
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 10.1.1.2/30
  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 64.100.1.2, destination 64.100.1.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255, Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
<output omitted>
RTB#
```

In the output from the last command shown, why is the maximum transmission unit (MTU) set at 1476 bytes?

_____

_____

List three common GRE misconfiguration issues.

_____

_____

_____

_____

_____

Packet Tracer ☐ Activity

Packet Tracer Exercise 3-1: GRE Implementation

Download and open the file LSG04-0301.pka found at the companion website for this book. Refer to the Introduction of this book for specifics on accessing files.

Note: The following instructions are also contained within the Packet Tracer Exercise.

In this Packet Tracer activity, you will configure the RTA and RTB routers to pass OSPF updates over a GRE tunnel.

Requirements

- Use OSPF process ID 1 to configure the routers to advertise the LAN and tunnel networks. Do not advertise the 64.100.1.0/30 network.

- Configure a GRE tunnel with the following:
  - Configure the tunnel interfaces according to the topology.
  - The mode is IP.
  - The tunnel source is the outbound interface number. Packet Tracer does support configuring the IP address as the tunnel source.

After OSPF converges, PC1 should be able to ping the Server. Your completion percentage should be 100%. All the connectivity tests should show a status of "successful." If not, click **Check Results** to see which required components are not yet completed.

eBGP

Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) used for the exchange of routing information between autonomous systems, such as ISPs, companies, and content providers.

BGP Overview

BGP exchanges routing information with another router, called a BGP _____ or BGP _____, which are routers in other companies, not routers in the same company. This distinguishes BGP from interior gateway protocols (IGP) such as OSPF and EIGRP that exchange routing information with routers in the same company.

BGP updates are encapsulated over TCP on port _____. Therefore, BGP inherits the connection-oriented properties of TCP, which ensures that BGP updates are transmitted reliably.

Describe the two types of BGP:

- **eBGP:** _____
- **iBGP:** _____

eBGP Branch Configuration

To implement eBGP for this course, you will need to complete the following tasks:

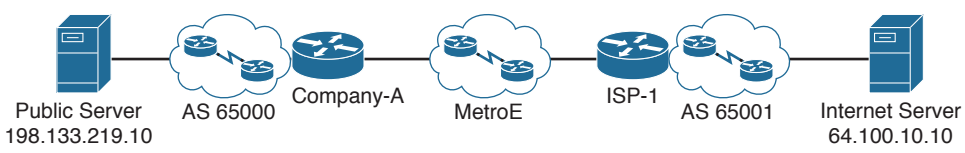
Step 1. Enable BGP routing.

Step 2. Configure BGP neighbor(s) (peering).

Step 3. Advertise network(s) originating from this AS.

Figure 3-4 shows the BGP configuration topology.

Figure 3-4 BGP Topology



List the commands to configure the Company-A router for single-homed BGP. ISP-1 is at 209.165.201.1. Advertise the 198.133.219.0/24 network to ISP-1.

_____

_____

_____

Record the commands to generate the following output.

```
Company-A# _____________________________________________________
B*   0.0.0.0 [20/0] via 209.165.201.1, 00:25:09

Company-A# _____________________________________________________
BGP table version is 4, 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
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0/32        209.165.201.1            0     0      0 65001 i
*> 198.133.219.0/24  0.0.0.0                  0     0 32768 i

Company-A# _____________________________________________________
BGP router identifier 209.165.201.2, local AS number 65000
BGP table version is 4, main routing table version 6
2 network entries using 264 bytes of memory
2 path entries using 104 bytes of memory
1/1 BGP path/bestpath attribute entries using 184 bytes of memory
2 BGP AS-PATH entries using 48 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
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 632 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      30      28        4    0    0 00:23:08        4
```

Packet Tracer ☐ Activity

Packet Tracer Exercise 3-2: BGP Branch Configuration

Download and open the file LSG04-0302.pka found at the companion website for this book. Refer to the Introduction of this book for specifics on accessing files.

Note: The following instructions are also contained within the Packet Tracer Exercise.

In this Packet Tracer activity, you will configure the Company-A router to send BGP updates to the ISP-1 router.

Requirements

- Use AS 65000.
- Configure the **neighbor** command.
- Advertise the 198.133.219.0/24 network.

After BGP converges, the Public Server should be able to ping the Internet Server. Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Labs and Activities

Command Reference

In Table 3-3, record the command, including the correct router prompt, that fits the description. Fill in any blanks with the appropriate missing information.

Table 3-3 Commands for Chapter 3, Branch Connections

Command	Description
	Configure a dialer interface to use an MTU of 1492.
	Configure an interface to use PPPoE.
	Configure an interface as a PPPoE client mapped to dialer pool 1.
	Create Tunnel 1.
	Configure a tunnel to use s0/0/0 as the source.
	Configure a tunnel to use the destination address 64.100.1.1.
	Enter the command to verify a tunnel interface.
	Configure a router with a BGP peer 64.100.1.1 that belongs to AS 65001.
	Configure a router to advertise 192.0.2.0/24 to its BGP peer.

3.0.1.2 Class Activity–Broadband Varieties

Objective

Select broadband solutions to support remote connectivity in a small- to medium-sized business network.

Scenario

Telework employment opportunities are expanding in your local area every day. You have been offered employment as a teleworker for a major corporation. The new employer requires teleworkers to have access to the Internet to fulfill their job responsibilities.

Research the following broadband Internet connection types that are available in your geographic area:

- DSL
- Cable
- Satellite

Consider the advantages and disadvantages of each broadband variation as you notate your research, which may include cost, speed, security, and ease of implementation or installation.

Resources

- World Wide Web access
- Word processing software

Step 1. Research three major types of broadband Internet connections:

- DSL
- Cable
- Satellite

Step 2. Decide which broadband options would be important to you as a teleworker in your small or home office:

- Cost
- Speed
- Security
- Ease of implementation
- Reliability

Step 3. Using the options from Step 2, create a matrix that lists the advantages and disadvantages of each broadband type.

Step 4. Share your research with the class or another group.

3.1.2.2 Lab–Researching Broadband Internet Access Technologies

Objectives

Part 1: Investigate Broadband Distribution

Part 2: Research Broadband Access Options for Specific Scenarios

Background/Scenario

Although broadband Internet access options have increased dramatically in recent years, broadband access varies greatly depending on location. In this lab, you will investigate current broadband distribution and research broadband access options for specific scenarios.

Required Resources

Device with Internet access

Part 1: Investigate Broadband Distribution

In Part 1, you will research broadband distribution in a geographical location.

Step 1. Research broadband distribution.

Use the Internet to research the following questions:

a. For the country in which you reside, what percentage of the population has broadband Internet subscriptions?

_____

b. What percentage of the population is without broadband Internet options?

_____

Step 2. Research broadband distribution in the United States.

Navigate to the website www.broadbandmap.gov. The National Broadband Map allows users to search and map broadband availability across the United States.

Note: For access options and ISPs for locations outside the United States, perform an Internet search using the keywords "broadband access XYZ," where XYZ is the name of the country.

---

a. Enter your zip code, city, and country that you would like to explore and click **Find Broadband**. List the zip code or city in the space provided.

_____

b. Click **Show Wired** and **Expand All**. What, if any, wired broadband Internet connections are available at this location? Complete the table below.

_____

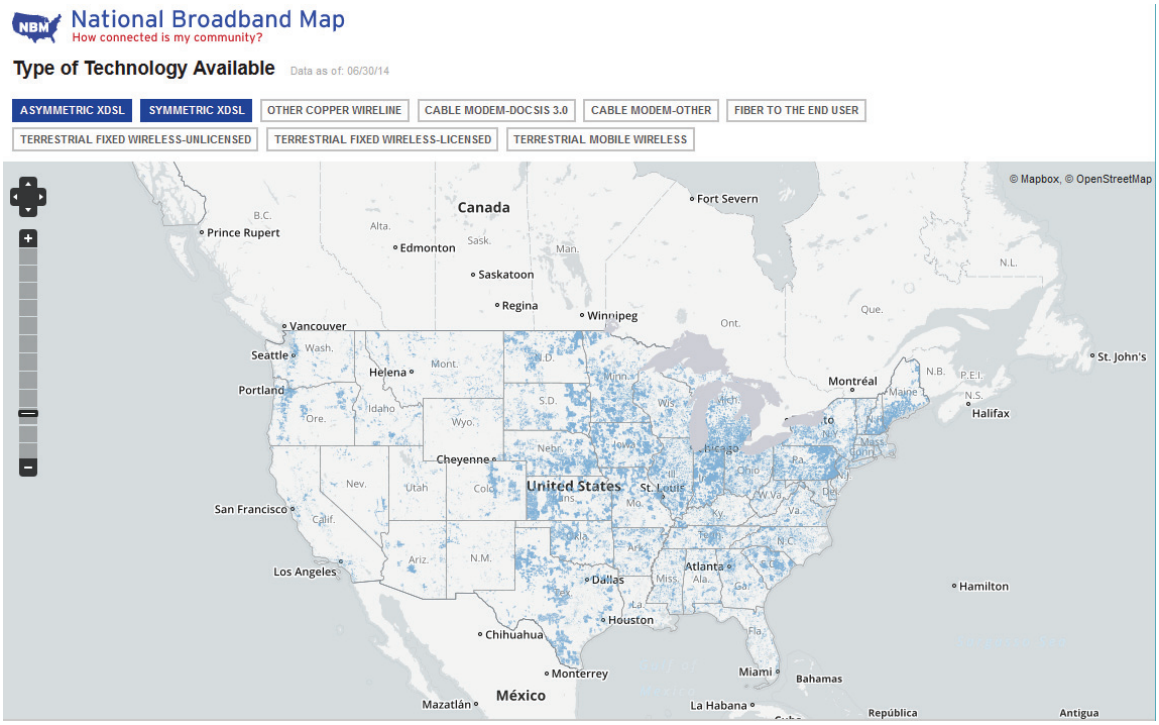
ISP	Connection Type	Download Speed

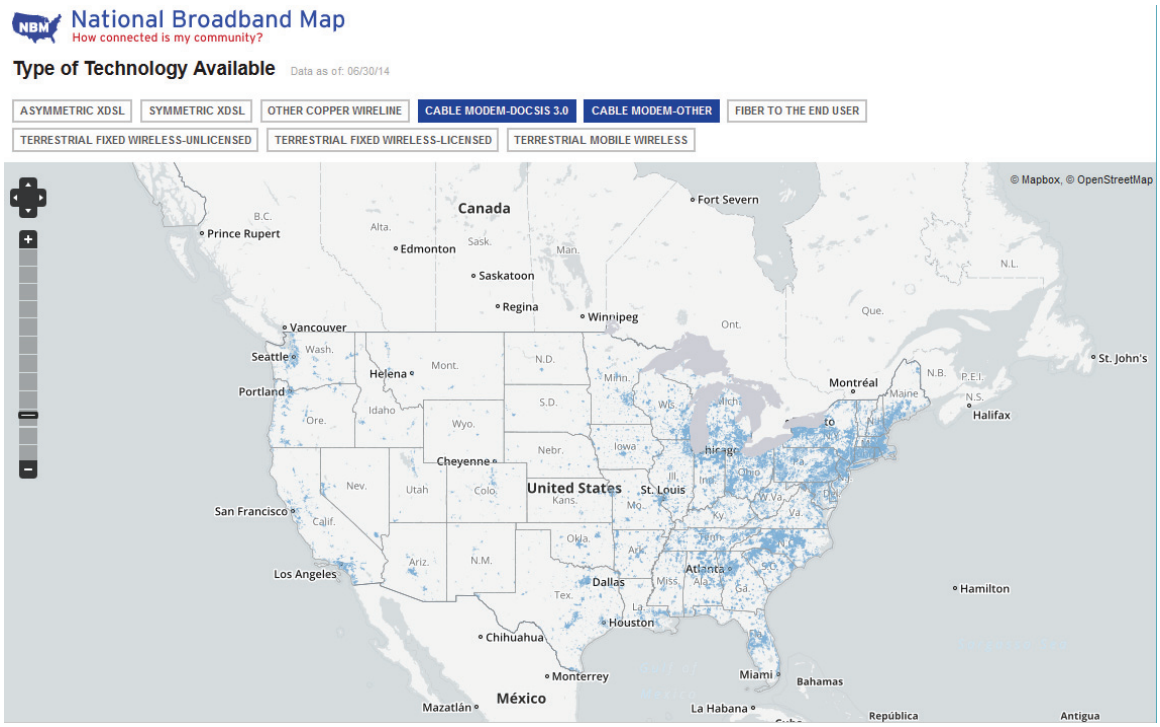
c. Click **Show Wireless** and **Expand All**. What, if any, wireless broadband Internet connections are available in this location? Complete the table below.

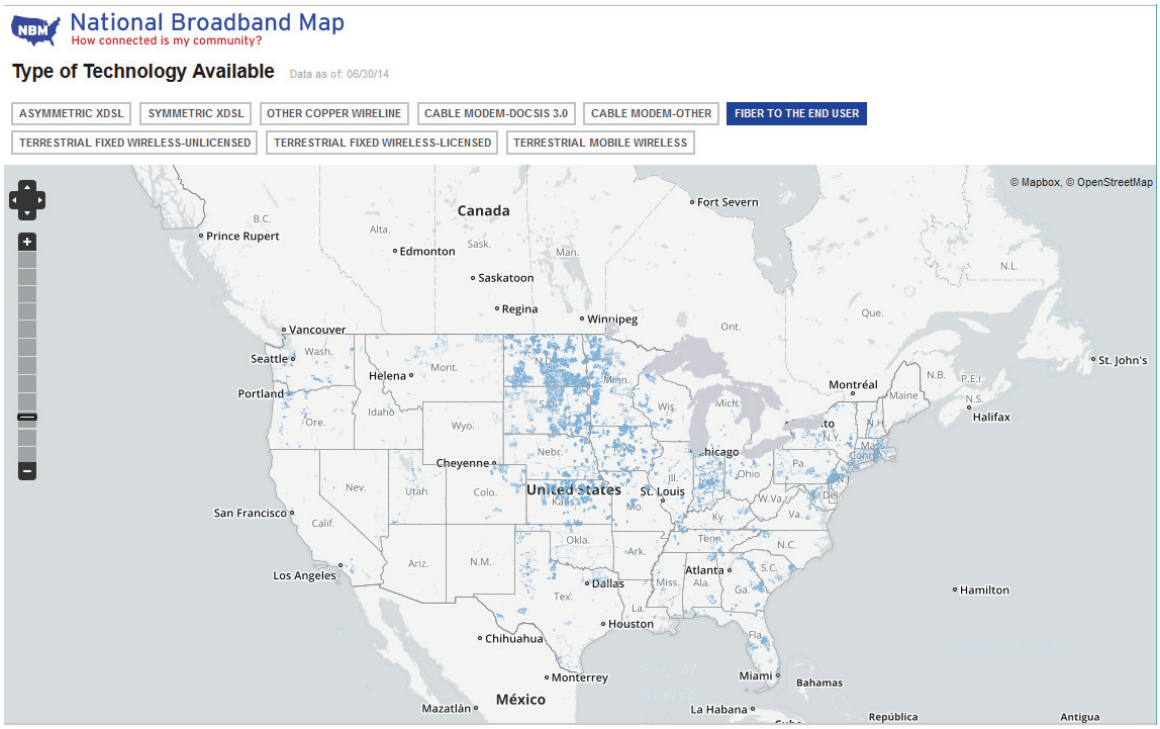
ISP	Connection Type	Download Speed

d. Return to the home page and click **Explore the Maps**. The interactive map allows you to explore the geographical availability of a number of broadband Internet options.

e. Highlight each of the wired connections independently (DSL, cable, and fiber). Selections are highlighted in dark blue.



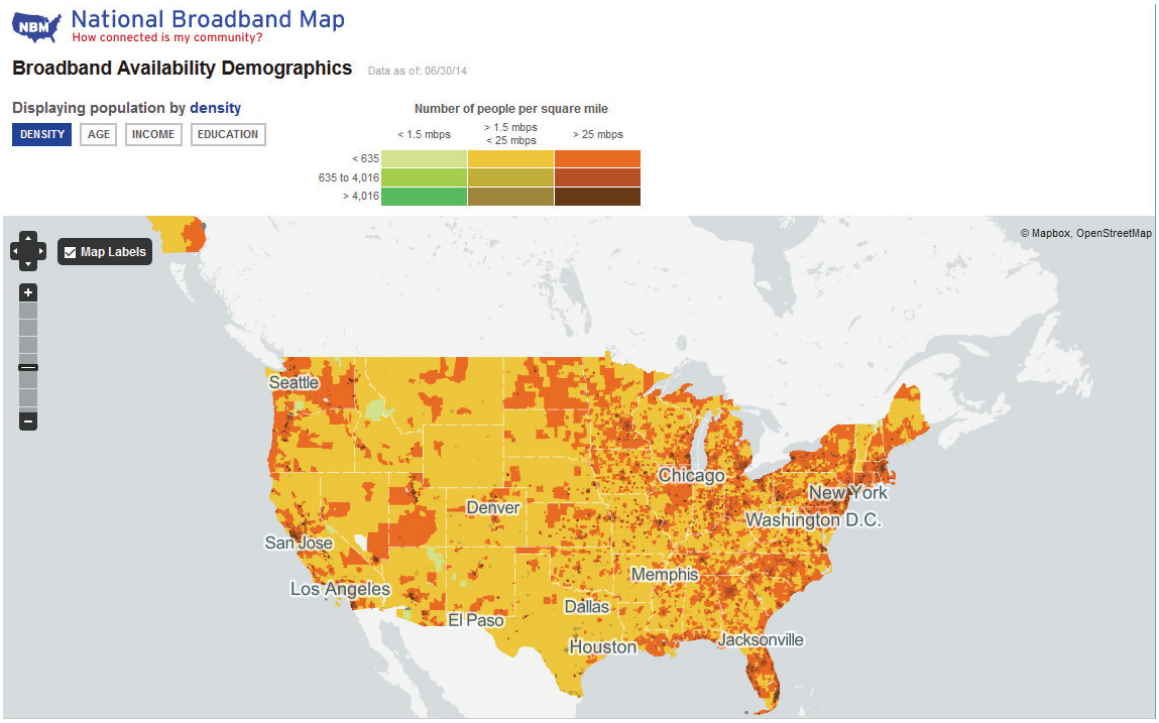




For wired connections, order the wired broadband connections from least to greatest in terms of geographical area covered. List your answer in the space provided.

_____

f. In the gallery of maps at the bottom of the web page, select **Broadband Availability Demographics**. Display the population by **density** and compare the broadband connection to the population distribution of the United States. What correlations can be drawn?



Part 2: Research Broadband Access Options for Specific Scenarios

In Part 2, you will research and detail broadband options for the following scenarios and select the best last-mile technology to meet the needs of the consumer. You can use the http://www.broadbandmap.gov site as a starting point for your research.

Scenario 1: You are moving to Kansas City, Missouri and are exploring home Internet connections. Research and detail two Internet connections from which you can select in this metropolitan area.

ISP	Connection Type	Cost per Month	Download Speed

Choose one from the list of local ISPs that you selected. Give the reasons why you chose that particular ISP.

_____

_____

_____

Scenario 2: You are moving to an area outside of Billings, Montana and are exploring home Internet connections. You will be beyond the reach of cable or DSL connections. Research and detail two Internet connections from which you can select in this area.

ISP	Connection Type	Cost per Month	Download Speed

Choose one from the list of local ISPs that you selected. Give the reasons why you chose that particular ISP.

_____

_____

_____

Scenario 3: You are moving to New York City and your job requires you to have 24 hours anytime/anywhere access. Research and detail two Internet connections from which you can select in this area.

ISP	Connection Type	Cost per Month	Download Speed

Choose one from the list of local ISPs that you selected. Give the reasons why you chose that particular ISP.

_____

_____

_____

Scenario 4: You are a small business owner with 10 employees who telecommute in the Fargo, North Dakota area. The teleworkers live beyond the reach of cable Internet connections. Research and detail two Internet connections from which you can select in this area.

ISP	Connection Type	Cost per Month	Download Speed

Choose one from the list of local ISPs that you selected. Give the reasons why you chose that particular ISP.

_____

_____

_____

Scenario 5: Your business in Washington, D.C. is expanding to 25 employees and you will need to upgrade your broadband access to include equipment colocation and web hosting. Research and detail two Internet connections from which you can select in this area.

ISP	Connection Type	Cost per Month	Download Speed

Choose one from the list of local ISPs that you selected. Give the reasons why you chose that particular ISP.

_____

_____

_____

Reflection

How do you think broadband Internet access will change in the future?

_____

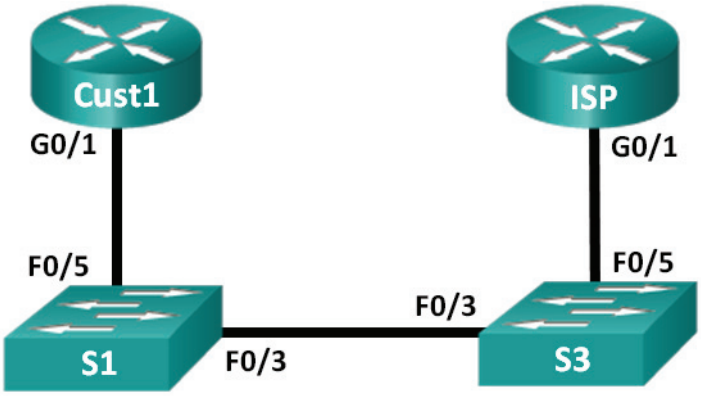
_____

_____

_____

3.2.2.7 Lab–Configuring a Router as a PPPoE Client for DSL Connectivity

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Cust1	G0/1	Learned via PPP	Learned via PPP	Learned via PPP
ISP	G0/1	N/A	N/A	N/A

Objectives

Part 1: Build the Network

Part 2: Configure the ISP Router

Part 3: Configure the Cust1 Router

Background/Scenario

ISPs often use Point-to-Point Protocol over Ethernet (PPPoE) on DSL links to their customers. PPP supports the assignment of IP address information to a device at the remote end of a PPP link. More importantly, PPP supports CHAP authentication. ISPs can check accounting records to see if a customer's bill has been paid, before letting them connect to the Internet.

In this lab, you will configure both the client and ISP side of the connection to set up PPPoE. Typically, you would only configure the client end.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Ensure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network

Step 1. Cable the network as shown in the topology.

Step 2. Initialize and reload the routers and switches.

Step 3. Configure basic settings for each router.

a. Disable DNS lookup.

b. Configure device name as shown in the topology.

c. Encrypt plaintext passwords.

d. Create a message of the day (MOTD) banner warning users that unauthorized access is prohibited.

e. Assign **class** as the encrypted privileged EXEC mode password.

f. Assign **cisco** as the console and vty password and enable login.

g. Set console logging to synchronous mode.

h. Save your configuration.

Part 2: Configure the ISP Router

In Part 2, you configure the ISP router with PPPoE parameters for connection from the Cust1 router.

Note: Many of the ISP router PPPoE configuration commands are beyond the scope of the course; however, they are necessary for completion of the lab. They can be copied and pasted into the ISP router at the global configuration mode prompt.

a. Create a local database username **Cust1** with a password of **ciscopppoe**.

```
ISP(config)# username Cust1 password ciscopppoe
```

b. Create a pool of addresses that will be assigned to customers.

```
ISP(config)# ip local pool PPPoEPOOL 10.0.0.1 10.0.0.10
```

c. Create the Virtual Template and associate the IP address of G0/1 with it. Associate the Virtual Template with the pool of addresses. Configure CHAP to authenticate customers.

```
ISP(config)# interface virtual-template 1
ISP(config-if)# ip address 10.0.0.254 255.255.255.0
ISP(config-if)# mtu 1492
```

```
ISP(config-if)# peer default ip address pool PPPoEPOOL
ISP(config-if)# ppp authentication chap callin
ISP(config-if)# exit
```

d. Assign the template to the PPPoE group.

```
ISP(config)# bba-group pppoe global
ISP(config-bba-group)# virtual-template 1
ISP(config-bba-group)# exit
```

e. Associate the bba-group with the G0/1 physical interface.

```
ISP(config)# interface g0/1
ISP(config-if# pppoe enable group global
ISP(config-if)# no shutdown
```

Part 3: Configure the Cust1 Router

In Part 3, you will configure the Cust1 router with PPPoE parameters.

a. Configure G0/1 interface for PPPoE connectivity.

```
Cust1(config)# interface g0/1
Cust1(config-if)# pppoe enable
Cust1(config-if)# pppoe-client dial-pool-number 1
Cust1(config-if)# exit
```

b. Associate the G0/1 interface with a dialer interface. Use the username **Cust1** and password **ciscopppoe** configured in Part 2.

```
Cust1(config)# interface dialer 1
Cust1(config-if)# mtu 1492
Cust1(config-if)# ip address negotiated
Cust1(config-if)# encapsulation ppp
Cust1(config-if)# dialer pool 1
Cust1(config-if)# ppp authentication chap callin
Cust1(config-if)# ppp chap hostname Cust1
Cust1(config-if)# ppp chap password ciscopppoe
Cust1(config-if)# exit
```

c. Set up a static default route pointing to the Dialer interface.

```
Cust1(config)# ip route 0.0.0.0 0.0.0.0 dialer 1
```

d. Set up debugging on the Cust1 router to display PPP and PPPoE negotiation.

```
Cust1# debug ppp authentication
Cust1# debug pppoe events
```

e. Enable the G0/1 interface on the Cust1 router and observe the debug output as the PPPoE dialer session is established and CHAP authentication takes place.

```
*Jul 30 19:28:42.427: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed
state to down
*Jul 30 19:28:46.175: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed
state to up
*Jul 30 19:28:47.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
*Jul 30 19:29:03.839:  padi timer expired
*Jul 30 19:29:03.839:  Sending PADI: Interface = GigabitEthernet0/1
*Jul 30 19:29:03.839: PPPoE 0: I PADO  R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1
*Jul 30 19:29:05.887:  PPPOE: we've got our pado and the pado timer went off
```

```
*Jul 30 19:29:05.887: OUT PADR from PPPoE Session
*Jul 30 19:29:05.895: PPPoE 1: I PADS  R:30f7.0da3.0b01 L:30f7.0da3.0bc1 Gi0/1
*Jul 30 19:29:05.895: IN PADS from PPPoE Session
*Jul 30 19:29:05.899: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Jul 30 19:29:05.899: PPPoE: Virtual Access interface obtained.
*Jul 30 19:29:05.899: PPPoE : encap string prepared
*Jul 30 19:29:05.899: [0]PPPoE 1: data path set to PPPoE Client
*Jul 30 19:29:05.903: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state
to up
*Jul 30 19:29:05.911: Vi2 PPP: Using dialer call direction
*Jul 30 19:29:05.911: Vi2 PPP: Treating connection as a callout
*Jul 30 19:29:05.911: Vi2 PPP: Session handle[C6000001] Session id[1]
*Jul 30 19:29:05.919: Vi2 PPP: No authorization without authentication
*Jul 30 19:29:05.939: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"
*Jul 30 19:29:05.939: Vi2 PPP: Sent CHAP SENDAUTH Request
*Jul 30 19:29:05.939: Vi2 PPP: Received SENDAUTH Response FAIL
*Jul 30 19:29:05.939: Vi2 CHAP: Using hostname from interface CHAP
*Jul 30 19:29:05.939: Vi2 CHAP: Using password from interface CHAP
*Jul 30 19:29:05.939: Vi2 CHAP: O RESPONSE id 1 len 26 from "Cust1"
*Jul 30 19:29:05.955: Vi2 CHAP: I SUCCESS id 1 len 4
*Jul 30 19:29:05.955: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-
Access2, changed state to up
*Jul 30 19:29:05.983: PPPoE : ipfib_encapstr  prepared
*Jul 30 19:29:05.983: PPPoE : ipfib_encapstr  prepared
```

f. Issue a **show ip interface brief** command on the Cust1 router to display the IP address assigned by the ISP router. Sample output is shown below. By what method was the IP address obtained? _____

```
Cust1# 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
Dialer1                    10.0.0.1   YES IPCP   up                    up
Virtual-Access1            unassigned YES unset  up                    up
Virtual-Access2            unassigned YES unset  up                    up
```

g. Issue a **show ip route** command on the Cust1 router. Sample output is shown below.

```
Cust1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0
```

```
S*    0.0.0.0/0 is directly connected, Dialer1
      10.0.0.0/32 is subnetted, 2 subnets
C        10.0.0.1 is directly connected, Dialer1
C        10.0.0.254 is directly connected, Dialer1
```

h. Issue a **show pppoe session** on Cust1 router. Sample output is shown below.

```
Cust1# show pppoe session
     1 client session

Uniq ID  PPPoE  RemMAC          Port                    VT  VA          State
           SID  LocMAC                                      VA-st       Type
    N/A      1  30f7.0da3.0b01  Gi0/1                   Di1 Vi2         UP
                30f7.0da3.0bc1                              UP
```

i. Issue a ping to 10.0.0.254 from the Cust1 router. The ping should be successful. If not, troubleshoot until you have connectivity.

```
Cust1# ping 10.0.0.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Reflection

Why do ISPs who use DSL primarily use PPPoE with their customers?

_____

_____

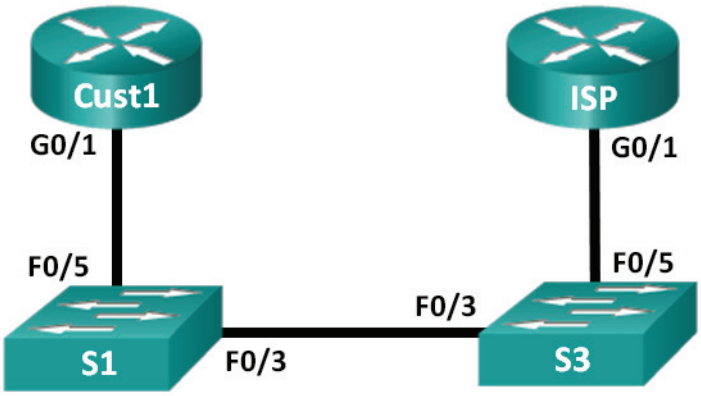
Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parentheses is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

3.2.2.8 Lab–Troubleshoot PPPoE

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Cust1	G0/1	Learned via PPP	Learned via PPP	Learned via PPP
ISP	G0/1	N/A	N/A	N/A

Objectives

Part 1: Build the Network

Part 2: Troubleshoot PPPoE on Cust1

Background/Scenario

ISPs sometimes use Point-to-Point Protocol over Ethernet (PPPoE) on DSL links to their customers. PPP supports the assignment of IP address information to a device at the remote end of a PPP link. More importantly, PPP supports CHAP authentication. ISPs can check accounting records to see if a customer's bill has been paid, before letting them connect to the Internet.

In this lab, you will troubleshoot the Cust1 router for PPPoE configuration problems.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Ensure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network

Step 1. Cable the network as shown in the topology.

Step 2. Initialize and reload the routers and switches.

Step 3. Copy the configurations on to routers.

a. Copy and paste the Cust1 configuration to the Cust1 router.

```
hostname Cust1
enable secret class
no aaa new-model
no ip domain lookup
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 pppoe enable group global
 pppoe-client dial-pool-number 1
 no shut
interface Dialer1
 mtu 1492
 ip address negotiated
 encapsulation ppp
 dialer pool 1
 ppp authentication chap callin
 ppp chap hostname Cust1
 ppp chap password 0 ciscoppp
ip route 0.0.0.0 0.0.0.0 Dialer1
banner motd ^C
Unauthorized Access Prohibited.
^C
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
end
```

b. Copy and paste the ISP configuration to the ISP router.

```
hostname ISP
enable secret class
username Cust1 password 0 ciscopppoe
bba-group pppoe global
 virtual-template 1
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 pppoe enable group global
 no shut
interface Virtual-Template1
 ip address 10.0.0.254 255.255.255.0
 mtu 1492
 peer default ip address pool PPPoEPOOL
 ppp authentication chap callin
ip local pool PPPoEPOOL 10.0.0.1 10.0.0.10
ip forward-protocol nd
banner motd ^C
Unauthorized Access Prohibited.
^C
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
end
```

Note: Many of the ISP router PPPoE configuration commands are beyond the scope of the course.

c. Save the router configurations.

Part 2: Troubleshoot PPPoE on Cust1

In Part 2, you will troubleshoot PPPoE on the Cust 1 router. The privileged EXEC mode password is **class**, and console and vty passwords are **cisco**. The ISP has provided a username of **Cust1** and a password of **ciscopppoe** for PPPoE CHAP authentication.

The following log messages should be appearing on your console session to Cust1:

```
Cust1#
*Nov  5 22:53:46.999: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Nov  5 22:53:47.003: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to up
*Nov  5 22:53:47.035: %DIALER-6-UNBIND: Interface Vi2 unbound from profile Di1
*Nov  5 22:53:47.039: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state to down
Cust1#
```

Step 1. Verify that IPv4 Address is assigned to the Cust1 Dialer interface.

The Dialer virtual interface did not receive an IP address.

```
Cust1# 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
Dialer1                    unassigned      YES manual up                    up
Virtual-Access1            unassigned      YES unset  up                    up
Virtual-Access2            unassigned      YES unset  down                  down
```

Step 2. Debug PPP to determine if the problem is with authentication.

a. Turn on debug for PPP authentication.

```
Cust1# debug ppp authentication
PPP authentication debugging is on
Cust1#
*Nov  5 23:09:00.283: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Nov  5 23:09:00.287: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state
to up
*Nov  5 23:09:00.287: Vi2 PPP: Using dialer call direction
*Nov  5 23:09:00.287: Vi2 PPP: Treating connection as a callout
*Nov  5 23:09:00.287: Vi2 PPP: Session handle[8A000036] Session id[54]
*Nov  5 23:09:00.315: Vi2 PPP: No authorization without authentication
*Nov  5 23:09:00.315: Vi2 CHAP: I CHALLENGE id 1 len 24 from "ISP"
*Nov  5 23:0
Cust1#9:00.315: Vi2 PPP: Sent CHAP SENDAUTH Request
*Nov  5 23:09:00.315: Vi2 PPP: Received SENDAUTH Response FAIL
*Nov  5 23:09:00.315: Vi2 CHAP: Using hostname from interface CHAP
*Nov  5 23:09:00.315: Vi2 CHAP: Using password from interface CHAP
*Nov  5 23:09:00.315: Vi2 CHAP: O RESPONSE id 1 len 26 from "Cust1"
*Nov  5 23:09:00.315: Vi2 CHAP: I FAILURE id 1 len 25 msg is "Authentication
failed"
*Nov  5 23:09:00.315: %DIALER-6-UNBIND: Interface Vi2 unbound from profile Di1
*Nov  5 23:09:00.319: %LINK-3
Cust1#-UPDOWN: Interface Virtual-Access2, changed state to down
Cust1#
```

b. End debug mode.

```
Cust1# u all
All possible debugging has been turned off
Cust1#
```

Step 3. Verify that the PPPoE username and password matches what was given by the ISP.

a. Display the running configuration; apply a filter to display only the Dialer section. Verify that the username and password matches what was provided by the ISP.

```
Cust1# show run | section Dialer
interface Dialer1
 mtu 1492
 ip address negotiated
```

```
 encapsulation ppp
 dialer pool 1
 ppp authentication chap callin
 ppp chap hostname Cust1
 ppp chap password 0 ciscoppp
ip route 0.0.0.0 0.0.0.0 Dialer1
```

b. The problem appears to be with the password. Enter global configuration mode and fix the ppp password.

```
Cust1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Cust1(config)# interface Dialer1
Cust1(config-if)# ppp chap password ciscopppoe
Cust1(config-if)# end
Cust1#
*Nov  5 23:42:07.343: %SYS-5-CONFIG_I: Configured from console by console
Cust1#
*Nov  5 23:42:25.039: %DIALER-6-BIND: Interface Vi2 bound to profile Di1
*Nov  5 23:42:25.043: %LINK-3-UPDOWN: Interface Virtual-Access2, changed state
to up
Cust1#
*Nov  5 23:42:25.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-
Access2, changed state to up
```

Step 4. Verify PPPoE connectivity.

a. Verify that this change resolved the problem and that an IP address has been assigned to the Dialer1 interface.

```
Cust1# 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
Dialer1                    10.0.0.1   YES IPCP   up                    up
Virtual-Access1            unassigned YES unset  up                    up
Virtual-Access2            unassigned YES unset  up                    up
```

b. Display the routing table to verify a route to the ISP router.

```
Cust1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0
```

```
S*    0.0.0.0/0 is directly connected, Dialer1
      10.0.0.0/32 is subnetted, 2 subnets
C        10.0.0.1 is directly connected, Dialer1
C        10.0.0.254 is directly connected, Dialer1
```

c. Display information about the active PPPoE sessions.

```
Cust1# 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                   Di1 Vi2         UP
                30f7.0da3.0da1                              UP
```

Step 5. Adjust the maximum segment size on the physical interface.

The PPPoE header adds an additional 8 bytes to each segment. To prevent TCP sessions from being dropped, the maximum segment size (MSS) needs to be adjusted to its optimum value on the physical interface.

a. Display G0/1s configuration setting to see if the MSS has been adjusted.

```
Cust1# show run interface g0/1
Building configuration...

Current configuration : 136 bytes
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 pppoe enable group global
 pppoe-client dial-pool-number 1
end
```

b. Adjust the MSS to its optimum value of 1452 bytes.

```
Cust1(config)# interface g0/1
Cust1(config-if)# ip tcp adjust-mss 1452
Cust1(config-if)# end
```

Reflection

Explain why the TCP segment size needs to be adjusted for PPPoE.

_____

_____

_____

_____

Router Interface Summary Table

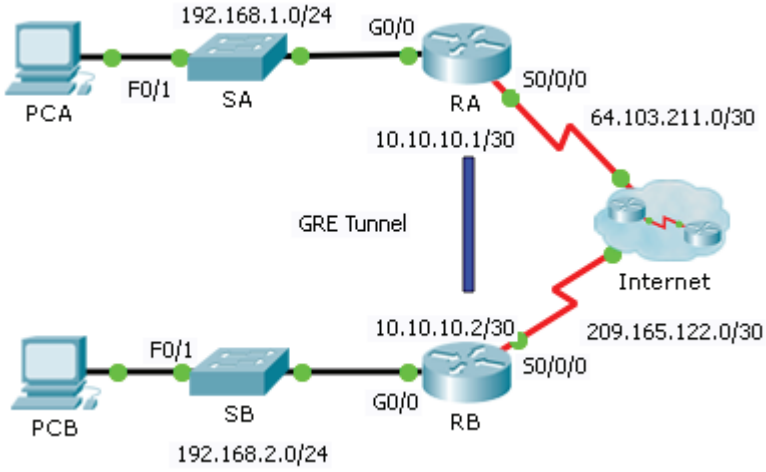
Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parentheses is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Packet Tracer Activity

3.4.2.4 Packet Tracer–Configuring GRE

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
RA	G0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	64.103.211.2	255.255.255.252	N/A
	Tunnel 0	10.10.10.1	255.255.255.252	N/A
RB	G0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	209.165.122.2	255.255.255.252	N/A
	Tunnel 0	10.10.10.2	255.255.255.252	N/A
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.2.2	255.255.255.0	192.168.2.1

Objectives

Part 1: Verify Router Connectivity

Part 2: Configure GRE Tunnels

Part 3: Verify PC Connectivity

Scenario

You are the network administrator for a company that wants to set up a GRE tunnel to a remote office. Both networks are locally configured, and need only the tunnel configured.

Part 1: Verify Router Connectivity

Step 1. Ping **RA** from **RB**.

a. Use the **show ip interface brief** command on **RA** to determine the IP address of the S0/0/0 port.

b. From **RB** ping the IP S0/0/0 address of **RA.**

Step 2. Ping **PCA** from **PCB**.

Attempt to ping the IP address of **PCA** from **PCB**. We will repeat this test after configuring the GRE tunnel. What were the ping results? Why?

_____

Part 2: Configure GRE Tunnels

Step 1. Configure the Tunnel 0 interface of RA.

a. Enter into the configuration mode for **RA** Tunnel 0.

```
RA(config)# interface tunnel 0
```

b. Set the IP address as indicated in the Addressing Table.

```
RA(config-if)# ip address 10.10.10.1 255.255.255.252
```

c. Set the source and destination for the endpoints of Tunnel 0.

```
RA(config-if)# tunnel source s0/0/0
RA(config-if)# tunnel destination 209.165.122.2
```

d. Configure Tunnel 0 to convey IP traffic over GRE.

```
RA(config-if)# tunnel mode gre ip
```

e. The Tunnel 0 interface should already be active. In the event that it is not, treat it like any other interface.

```
RA(config-if)# no shutdown
```

Step 2. Configure the Tunnel 0 interface of **RB**.

Repeat Steps 1 a – e with **RB**. Be sure to change the IP addressing as appropriate.

_____

_____

_____

_____

_____

_____

Step 3. Configure a route for private IP traffic.

Establish a route between the 192.168.X.X networks using the 10.10.10.0/30 network as the destination.

```
RA(config)# ip route 192.168.2.0 255.255.255.0 10.10.10.2
RB(config)# ip route 192.168.1.0 255.255.255.0 10.10.10.1
```

Part 3: Verify Router Connectivity

Step 1. Ping **PCA** from **PCB**.

Attempt to ping the IP address of **PCA** from **PCB**. The ping should be successful.

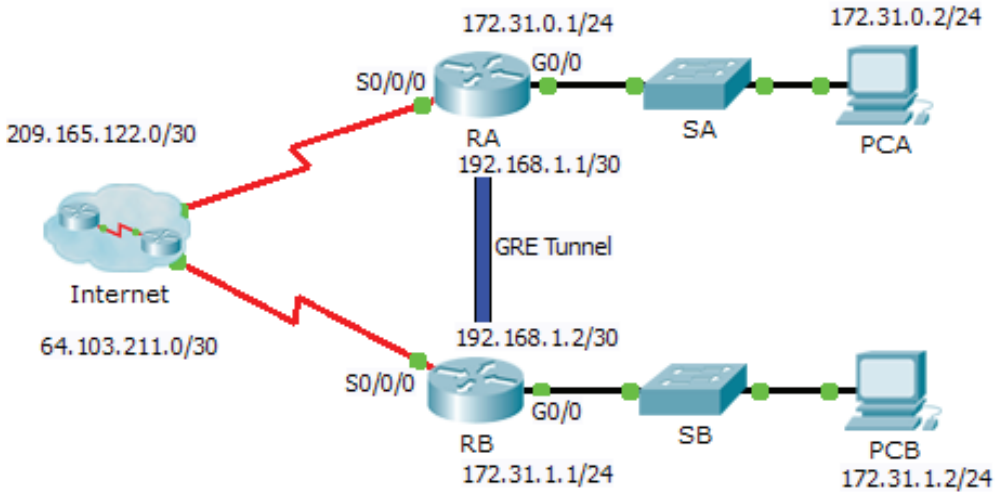
Step 2. Trace the path from **PCA** to **PCB**.

Attempt to trace the path from **PCA** to **PCB**. Note the lack of public IP addresses in the output.

Packet Tracer
Activity

3.4.2.5 Packet Tracer–Troubleshooting GRE

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
RA	G0/0	172.31.0.1	255.255.255.0	N/A
	S0/0/0	209.165.122.2	255.255.255.252	N/A
	Tunnel 0	192.168.1.1	255.255.255.252	N/A
RB	G0/0	172.31.1.1	255.255.255.0	N/A
	S0/0/0	64.103.211.2	255.255.255.252	N/A
	Tunnel 0	192.168.1.2	255.255.255.252	N/A
PC-A	NIC	172.31.0.2	255.255.255.0	172.31.0.1
PC-C	NIC	172.31.1.2	255.255.255.0	172.31.1.1

Objectives

- Find and Correct All Network Errors
- Verify Connectivity

Scenario

A junior network administrator was hired to set up a GRE tunnel between two sites and was unable to complete the task. You have been asked to correct configuration errors in the company network.

Part 1: Find and Correct All Network Errors

Device	Error	Correction

Part 2: Verify Connectivity

Step 1. Ping **PCA** from **PCB**.

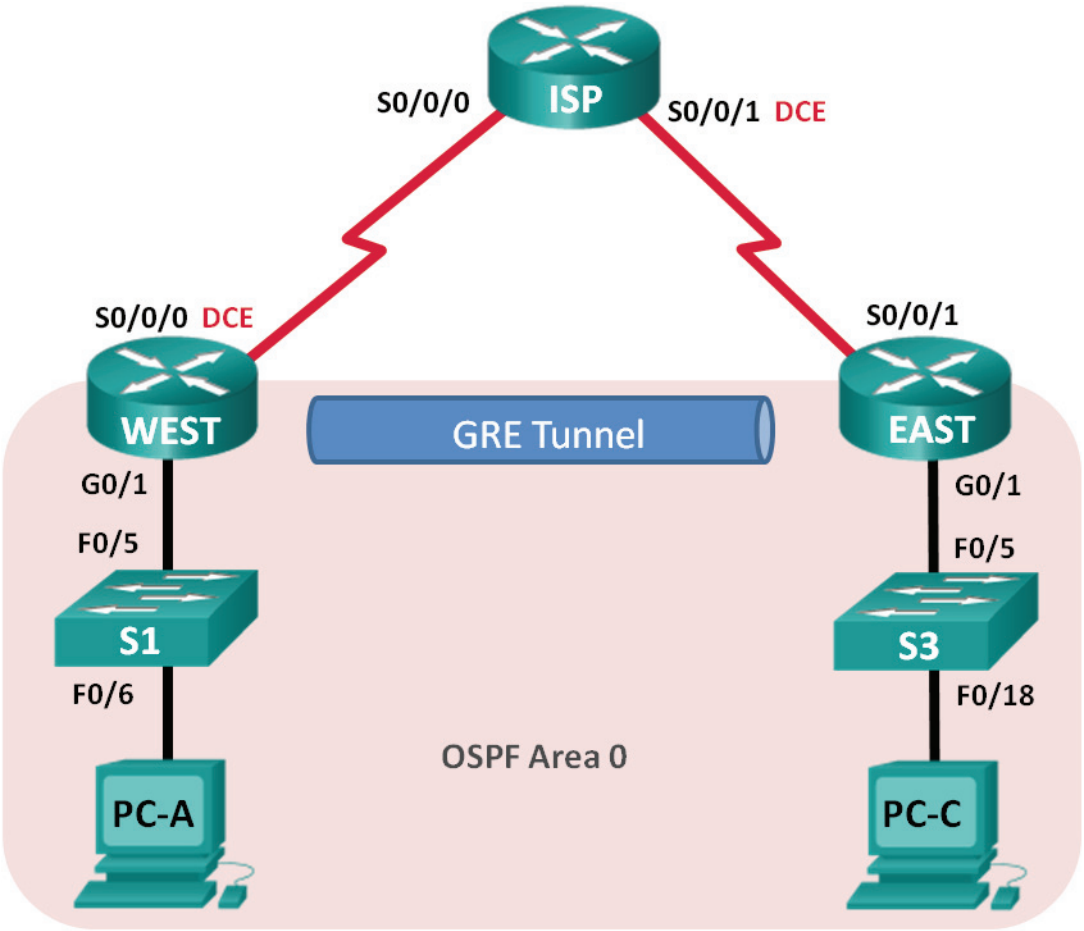
Attempt to ping the IP address of **PCA** from **PCB**. The ping should be successful.

Step 2. Trace the path from **PCA** to **PCB**.

Attempt to trace the path from **PCA** to **PCB**. Note the lack of public IP addresses in the output.

3.4.2.6 Lab–Configuring a Point-to-Point GRE VPN Tunnel

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
WEST	G0/1	172.16.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
	Tunnel0	172.16.12.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
EAST	G0/1	172.16.2.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
	Tunnel0	172.16.12.2	255.255.255.252	N/A
PC-A	NIC	172.16.1.3	255.255.255.0	172.16.1.1
PC-C	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure a GRE Tunnel

Part 3: Enable Routing over the GRE Tunnel

Background/Scenario

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a variety of network layer protocols between two locations over a public network, such as the Internet.

GRE can be used with:

- Connecting IPv6 networks over IPv4 networks
- Multicast packets, such as OSPF, EIGRP, and streaming applications

In this lab, you will configure an unencrypted point-to-point GRE VPN tunnel and verify that network traffic is using the tunnel. You will also configure the OSPF routing protocol inside the GRE VPN tunnel. The GRE tunnel is between the WEST and EAST routers in OSPF area 0. The ISP has no knowledge of the GRE tunnel. Communication between the WEST and EAST routers and the ISP is accomplished using default static routes.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic router settings, such as the interface IP addresses, routing, device access, and passwords.

Step 1. Cable the network as shown in the topology.

Step 2. Initialize and reload the routers and switches.

Step 3. Configure basic settings for each router.

- **a.** Disable DNS lookup.
- **b.** Configure the device names.
- **c.** Encrypt plain text passwords.
- **d.** Create a message of the day (MOTD) banner warning users that unauthorized access is prohibited.
- **e.** Assign **class** as the encrypted privileged EXEC mode password.
- **f.** Assign **cisco** as the console and vty password and enable login.
- **g.** Set console logging to synchronous mode.
- **h.** Apply IP addresses to Serial and Gigabit Ethernet interfaces according to the Addressing Table and activate the physical interfaces. Do NOT configure the Tunnel0 interfaces at this time.
- **i.** Set the clock rate to **128000** for DCE serial interfaces.

Step 4. Configure default routes to the ISP router.

```
WEST(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2

EAST(config)# ip route 0.0.0.0 0.0.0.0 10.2.2.2
```

Step 5. Configure the PCs.

Assign IP addresses and default gateways to the PCs according to the Addressing Table.

Step 6. Verify connectivity.

At this point, the PCs are unable to ping each other. Each PC should be able to ping its default gateway. The routers are able to ping the serial interfaces of the other routers in the topology. If not, troubleshoot until you can verify connectivity.

Step 7. Save your running configuration.

Part 2: Configure a GRE Tunnel

In Part 2, you will configure a GRE tunnel between the WEST and EAST routers.

Step 1. Configure the GRE tunnel interface.

- **a.** Configure the tunnel interface on the WEST router. Use S0/0/0 on WEST as the tunnel source interface and 10.2.2.1 as the tunnel destination on the EAST router.

```
WEST(config)# interface tunnel 0
WEST(config-if)# ip address 172.16.12.1 255.255.255.252
WEST(config-if)# tunnel source s0/0/0
WEST(config-if)# tunnel destination 10.2.2.1
```

- **b.** Configure the tunnel interface on the EAST router. Use S0/0/1 on EAST as the tunnel source interface and 10.1.1.1 as the tunnel destination on the WEST router.

```
EAST(config)# interface tunnel 0
EAST(config-if)# ip address 172.16.12.2 255.255.255.252
```

```
EAST(config-if)# tunnel source 10.2.2.1
EAST(config-if)# tunnel destination 10.1.1.1
```

Note: For the **tunnel source** command, either the interface name or the IP address can be used as the source.

Step 2. Verify that the GRE tunnel is functional.

a. Verify the status of the tunnel interface on the WEST and EAST routers.

```
WEST# 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         172.16.1.1  YES manual up                    up
Serial0/0/0                10.1.1.1    YES manual up                    up
Serial0/0/1                unassigned  YES unset  administratively down down
Tunnel0                    172.16.12.1 YES manual up                    up
```

```
EAST# 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         172.16.2.1  YES manual up                    up
Serial0/0/0                unassigned  YES unset  administratively down down
Serial0/0/1                10.2.2.1    YES manual up                    up
Tunnel0                    172.16.12.2 YES manual up                    up
```

b. Issue the **show interfaces tunnel 0** command to verify the tunneling protocol, tunnel source, and tunnel destination used in this tunnel.

What is the tunneling protocol used? What are the tunnel source and destination IP addresses associated with GRE tunnel on each router?

_____

_____

c. Ping across the tunnel from the WEST router to the EAST router using the IP address of the tunnel interface.

```
WEST# ping 172.16.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/34/36 ms
```

d. Use the **traceroute** command on the WEST to determine the path to the tunnel interface on the EAST router. What is the path to the EAST router? _____

_____

e. Ping and trace the route across the tunnel from the EAST router to the WEST router using the IP address of the tunnel interface.

What is the path to the WEST router from the EAST router? _____

_____

With which interfaces are these IP addresses associated? Explain.

_____

_____

f. The **ping** and **traceroute** commands should be successful. If not, troubleshoot before continuing to the next part.

Part 3: Enable Routing over the GRE Tunnel

In Part 3, you will configure OSPF routing so that the LANs on the WEST and EAST routers can communicate using the GRE tunnel.

After the GRE tunnel is set up, the routing protocol can be implemented. For GRE tunneling, a network statement will include the IP network of the tunnel, instead of the network associated with the serial interface. just like you would with other interfaces, such as Serial and Ethernet. Remember that the ISP router is not participating in this routing process.

Step 1. Configure OSPF routing for area 0 over the tunnel.

a. Configure OSPF process ID 1 using area 0 on the WEST router for the 172.16.1.0/24 and 172.16.12.0/24 networks.

```
WEST(config)# router ospf 1
WEST(config-router)# network 172.16.1.0 0.0.0.255 area 0
WEST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

b. Configure OSPF process ID 1 using area 0 on the EAST router for the 172.16.2.0/24 and 172.16.12.0/24 networks.

```
EAST(config)# router ospf 1
EAST(config-router)# network 172.16.2.0 0.0.0.255 area 0
EAST(config-router)# network 172.16.12.0 0.0.0.3 area 0
```

Step 2. Verify OSPF routing.

a. From the WEST router, issue the **show ip route** command to verify the route to 172.16.2.0/24 LAN on the EAST router.

```
WEST# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.1.1.2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/1
```

```
L        172.16.1.1/32 is directly connected, GigabitEthernet0/1
O        172.16.2.0/24 [110/1001] via 172.16.12.2, 00:00:07, Tunnel0
C        172.16.12.0/30 is directly connected, Tunnel0
L        172.16.12.1/32 is directly connected, Tunnel0
```

What is the exit interface and IP address to reach the 172.16.2.0/24 network?

_____

b. From the EAST router issue the command to verify the route to 172.16.1.0/24 LAN on the WEST router.

What is the exit interface and IP address to reach the 172.16.1.0/24 network?

_____

Step 3. Verify end-to-end connectivity.

a. Ping from PC-A to PC-C. It should be successful. If not, troubleshoot until you have end-to-end connectivity.

Note: It may be necessary to disable the PC firewall to ping between PCs.

b. Traceroute from PC-A to PC-C. What is the path from PC-A to PC-C?

_____

Reflection

1. What other configurations are needed to create a secured GRE tunnel?

_____

2. If you added more LANs to the WEST or EAST router, what would you need to do so that the network will use the GRE tunnel for traffic?

_____

Router Interface Summary Table

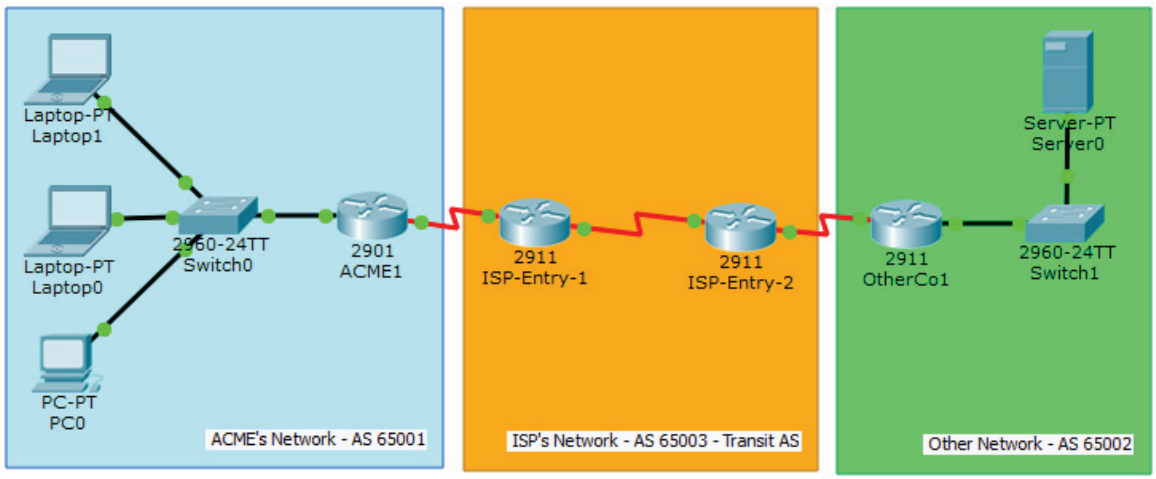
Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parentheses is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Packet Tracer ☐ Activity

3.5.3.5 Packet Tracer–Configure and Verify eBGP

Topology



Objectives

Configure and verify eBGP between two autonomous systems.

Background/Scenario

In this activity, you will configure and verify the operation of eBGP between autonomous systems 65001 and 65002. ACME Inc. is a company that has a partnership with Other Company and must exchange routes. Both companies have their own autonomous systems and will use ISP as the transit AS to reach each other.

Note: Only companies with very large networks can afford their own autonomous system.

Address Table

Device	Interface	IPv4 Address	Subnet Mask	Default Gateway
ACME1	G0/0	192.168.0.1	255.255.255.0	N/A
	S0/0/0	1.1.1.2	255.255.255.252	N/A
OtherCo1	G/0/0	172.16.10.1	255.255.255.0	N/A
	S0/0/0	1.1.1.10	255.255.255.252	N/A
ISP1	S0/0/0	1.1.1.1	255.255.255.252	
	S0/0/1	1.1.1.5	255.255.255.252	
ISP2	S0/0/0	1.1.1.9	255.255.255.252	
	S0/0/1	1.1.1.6	255.255.255.252	
PC0	NIC		DHCP	192.168.0.1
Laptop0	NIC		DHCP	192.168.0.1
Laptop1	NIC		DHCP	192.168.0.1
Server	NIC	172.16.10.2	255.255.255.0	172.16.10.1

Step 1. Configure eBGP in ACME Inc.

ACME Inc. hired an ISP to connect to a partner company called Other Company. The ISP has established network reachability within its network and to Other Company. You must connect ACME to the ISP so that ACME and Other Company can communicate. Because ISP is using BGP as the routing protocol, you must configure ACME1, ACME's border router, to establish a BGP neighbor connection with ISP1, the ISP border router that faces ACME.

a. Verify that the ISP has provided IP reachability through its network by pinging 1.1.1.9, the IP address assigned to ISP2's Serial 0/0/0.

b. From any device inside ACME's network, ping the Other Company's server 172.16.10.2. The pings should fail as no BGP routing is configured at this time.

c. Configure ACME1 to become an eBGP peer with ISP1. ACME's AS number is 65001, while the ISP is using AS number 65003. Use 1.1.1.1 as the neighbor IP address and make sure to add ACME's internal network 192.168.0.0/24 to BGP.

From any device inside ACME's network, ping the Other Company internal server again. Does it work?

Step 2. Configure eBGP in Other Company Inc.

The network administrator at Other Company is not familiar with BGP and could not configure their side of the link. You must also configure their end of the connection.

Configure OtherCo1 to form an eBGP adjacency with ISP2, the ISP border router facing OtherCo1. Other Company is under AS 65002 while ISP is under AS 65003. Use 1.1.1.9 as the neighbor IP address of ISP2 and make sure to add Other Company's internal network 172.16.10.0/24 to BGP.

Step 3. eBGP Verification

a. Verify that ACME1 has properly formed an eBGP adjacency with ISP1. The **show ip bgp summary** command is very useful here.

b. Use the **show ip bgp summary** command to verify all the routes ACME1 has learned via eBGP and their status.

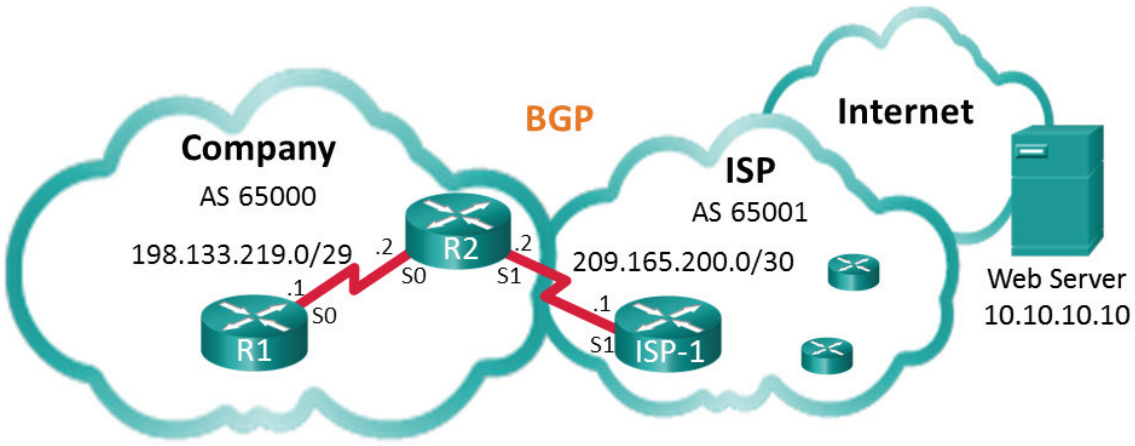
c. Look at the routing tables on ACME1 and OtherCo1. ACME1 should have routes learned about Other Company's route 172.16.10.0/24. Similarly, OtherCo1 should now know about ACME's route 192.168.0.0/24.

d. Open a web browser in any ACME Inc. end devices and navigate to Other Company's server by entering its IP address 172.16.10.2

e. From any ACME Inc. device, ping the Other Company's server at 172.16.10.2.

3.5.3.5 Lab–Configure and Verify eBGP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	S0/0/0 (DCE)	198.133.219.1	255.255.255.248
R2	S0/0/0	198.133.219.2	255.255.255.248
	S0/0/1 (DCE)	209.165.200.2	255.255.255.252
ISP-1	S0/0/1	209.165.200.1	255.255.255.252
Web Server		10.10.10.10	255.255.255.255

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure eBGP on R1

Part 3: Verify eBGP Configuration

Background/Scenario

In this lab you will configure eBGP for the Company. The ISP will provide the default route to the Internet. Once configuration is complete you will use various **show** commands to verify that the eBGP configuration is working as expected.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- Console cables to configure the Cisco IOS devices via the console ports
- Serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on R1 and R2 routers. You will also copy the provided configuration for ISP-1 on to that router.

Step 1. Cable the network as shown in the topology.

Step 2. Initialize and reload the network devices as necessary.

Step 3. Configure basic settings on R1 and R2.

- **a.** Disable DNS lookup to prevent the routers from attempting to translate incorrectly entered commands as though they were host names.
- **b.** Configure the hostnames according to the topology.
- **c.** Configure interfaces according to the Addressing Table.
- **d.** Save the running configuration to the startup configuration file.

Step 4. Copy configuration to ISP-1.

Copy and paste the following configuration to ISP-1.

```
hostname ISP-1
no ip domain-lookup
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
interface Serial0/0/1
 ip address 209.165.200.1 255.255.255.252
 no shut
ip route 0.0.0.0 0.0.0.0 lo0
router bgp 65001
 bgp log-neighbor-changes
 network 0.0.0.0
 neighbor 209.165.200.2 remote-as 65000
end
```

Part 2: Configure eBGP on R2

Configure R2 to become an eBGP peer with ISP-1. Refer to the Topology for BGP AS number information.

Step 1. Enable BGP and identify the AS number for the Company.

```
R2(config)# router bgp 65000
```

Step 2. Use the neighbor command to identify ISP-1 as the BGP peer.

```
R2(config-router)# neighbor 209.165.200.1 remote-as 65001
```

Step 3. Add the Company's network to the BGP table so it is advertised to ISP-1.

```
R2(config-router)# network 198.133.219.0 mask 255.255.255.248
```

Part 3: Verify eBGP Configuration

In Part 3, use the BGP verification commands to verify that the BGP configuration is working as expected.

Step 1. Display the IPv4 routing table on R2.

```
R2# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 209.165.200.1 to network 0.0.0.0

B*    0.0.0.0/0 [20/0] via 209.165.200.1, 00:00:07
      198.133.219.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.133.219.0/29 is directly connected, Serial0/0/0
L        198.133.219.2/32 is directly connected, Serial0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.0/30 is directly connected, Serial0/0/1
L        209.165.200.2/32 is directly connected, Serial0/0/1
```

Step 2. Display the BGP table on R2.

```
R2# show ip bgp
BGP table version is 4, local router ID is 209.165.200.2
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          209.165.200.1            0             0 65001 i
 *>  198.133.219.0/29 0.0.0.0                  0         32768 i
```

Step 3. Display the BGP connection status on R2.

```
R2# show ip bgp summary
BGP router identifier 209.165.200.2, local AS number 65000
BGP table version is 4, main routing table version 4
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
209.165.200.1   4        65001      12      11        4    0    0 00:06:56        1
```

Step 4. Display the IPv4 routing table on ISP-1.

Verify that the 198.133.218.0/29 network is being advertised to the ISP-1 router.

```
ISP-1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S*    0.0.0.0/0 is directly connected, Loopback0
      10.0.0.0/32 is subnetted, 1 subnets
C        10.10.10.10 is directly connected, Loopback0
      198.133.219.0/29 is subnetted, 1 subnets
B        198.133.219.0 [20/0] via 209.165.200.2, 00:00:25
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.0/30 is directly connected, Serial0/0/1
L        209.165.200.1/32 is directly connected, Serial0/0/1
```

Ping the Web Server from R1. Were the pings successful?

_____

Reflection

The topology used in this lab was created to demonstrate how to configure the BGP routing protocol. However, the BGP protocol would not normally be configured for a topology like this in the real world. Explain.

_____

_____

_____

_____

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parentheses is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

3.6.1.1 Class Activity–VPN Planning Design

Objective

Explain the use of VPNs in securing site-to-site connectivity in a small- to medium-sized business network.

Scenario

Your small- to medium-sized business has received quite a few new contracts lately. This has increased the need for teleworkers and workload outsourcing. The new contract vendors and clients will also need access to your network as the projects progress.

As network administrator for the business, you recognize that VPNs must be incorporated as a part of your network strategy to support secure access by the teleworkers, employees, and vendors or clients.

To prepare for implementation of VPNs on the network, you devise a planning checklist to bring to the next department meeting for discussion.

Resources

- World Wide Web access
- Packet Tracer software
- Word processing software

Step 1. Visit the VPN Discovery Tool, http://help.mysonicwall.com/sw/eng/4201/ui2/23600/VPN/VPN_Policy.htm, or any other Internet site with VPN-implementation or planning checklist examples.

Step 2. Use Packet Tracer to draw the current topology for your network; no device configurations are necessary. Include:

- Two branch offices: the Internet cloud and one headquarters location
- Current network devices: servers, switches, routers/core routers, broadband ISR devices, and local user workstations

Step 3. On the Packet Tracer topology, indicate:

a. Where would you implement VPNs?

b. What types of VPNs would be needed?

1) Site to site

2) Remote access

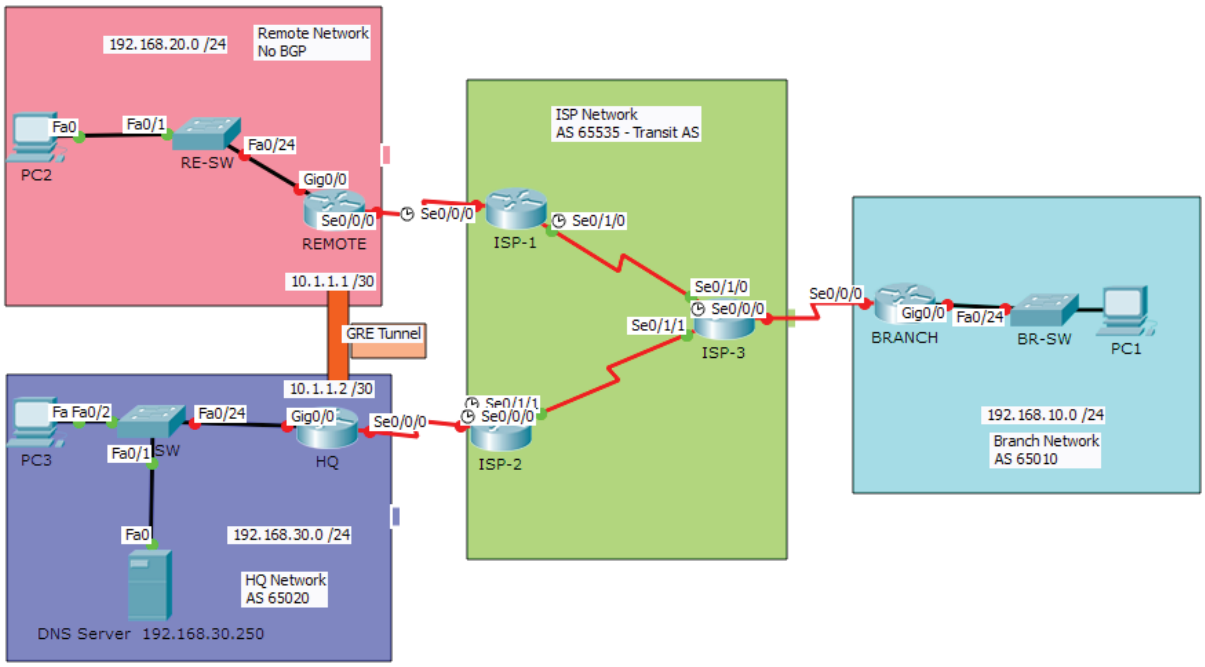
Step 4. Using a word processing software program, create a small VPN planning checklist based on your research from Step 1.

Step 5. Share your work with the class, another group, or your instructor.

Packet Tracer
Activity

3.6.1.2 Packet Tracer–Skills Integration Challenge

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
ISP-1	S0/0/0	209.165.201.1	255.255.255.252	N/A
	S0/1/0	209.165.201.9	255.255.255.252	N/A
ISP-2	S0/0/0	209.165.201.17	255.255.255.252	N/A
	S0/1/1	209.165.201.13	255.255.255.252	N/A
ISP-3	S0/0/0	209.165.201.21	255.255.255.252	N/A
	S0/1/0	209.165.201.10	255.255.255.252	N/A
	S0/1/1	209.165.201.14	255.255.255.252	N/A
REMOTE	S0/0/0	209.165.201.2	255.255.255.252	N/A
	G0/0	192.168.20.1	255.255.255.0	N/A
	Tunnel 10	10.1.1.1	255.255.255.252	N/A
HQ	S0/0/0	209.165.201.18	255.255.255.252	N/A
	G0/0	192.168.30.1	255.255.255.0	N/A
	Tunnel 10	10.1.1.2	255.255.255.252	N/A
BRANCH	S0/0/0	209.165.201.22	255.255.255.252	N/A
	G0/0	192.168.10.1	255.255.255.0	N/A
PC1	NIC	DHCP		192.168.10.1
PC2	NIC	192.168.20.10	255.255.255.0	192.168.20.1
PC3	NIC	DHCP		192.168.30.1
DNS Server	NIC	192.168.30.250	255.255.255.0	192.168.30.1

Background/Scenario

In this skills integration challenge, the XYZ Corporation uses a combination of eBGP, PPP, and GRE WAN connections. Other technologies include DHCP, default routing, OSPF for IPv4, and SSH configurations.

Requirements

Note: The user EXEC password is **cisco** and the privileged EXEC password is **class**.

Interface Addressing

- Configure interface addressing as needed on appropriate devices.
  - Use the topology table to implement addressing on routers REMOTE, HQ, and BRANCH.
  - Configure **PC1** and **PC3** to use DHCP.

SSH

- Configure **HQ** to use SSH for remote access.
  - Set the modulus to **2048**. The domain name is **CISCO.com**.
  - The username is **admin** and the password is **secureaccess**.
  - Only SSH should be allowed on the VTY lines.
  - Modify the SSH defaults: version 2; 60-second timeout; two retries.

PPP

- Configure the WAN link from **BRANCH** to the **ISP-3** router using PPP encapsulation and CHAP authentication.
  - Create a user **ISP-3** with the password of **cisco**.
- Configure the WAN link from **HQ** to the **ISP-2** router using PPP encapsulation and CHAP authentication.
  - Create a user **ISP-2** with the password of **cisco**.

DHCP

- On **BRANCH**, configure a DHCP pool for the BRANCH LAN using the following requirements:
  - Exclude the first 5 IP addresses in the range.
  - The case-sensitive pool name is **LAN**.
  - Include the DNS server attached to the **HQ** LAN as part of the DHCP configuration.
- Configure PC1 to use DHCP.
- On **HQ**, configure a DHCP pool for the HQ LAN using the following requirements:
  - Exclude the first 10 IP addresses in the range.
  - The case-sensitive pool name is **LAN**.
  - Include the DNS server attached to the **HQ** LAN as part of the DHCP configuration.
- Configure PC3 to use DHCP.

Default Routing

- Configure **REMOTE** with a default route to the **ISP-1** router. Use the Next-Hop IP as an argument.

eBGP Routing

- Configure **BRANCH** with eBGP routing.
  - Configure **BRANCH** to peer with **ISP-3**.
  - Add **BRANCH's** internal network to BGP.
- Configure **HQ** with eBGP routing.
  - Configure **HQ** to peer with **ISP-2**.
  - Add **HQ's** internal network to BGP.

GRE Tunneling

- Configure **REMOTE** with a tunnel interface to send IP traffic over GRE to **HQ**.
  - Configure **Tunnel 10** with appropriate addressing information.
  - Configure the tunnel source with the local exit interface.
  - Configure the tunnel destination with the appropriate endpoint IP address.
- Configure **HQ** with a tunnel interface to send IP traffic over GRE to **REMOTE**.
  - Configure **Tunnel 10** with appropriate addressing information.
  - Configure the tunnel source with the local exit interface.
  - Configure the tunnel destination with the appropriate endpoint IP address.

OSPF Routing

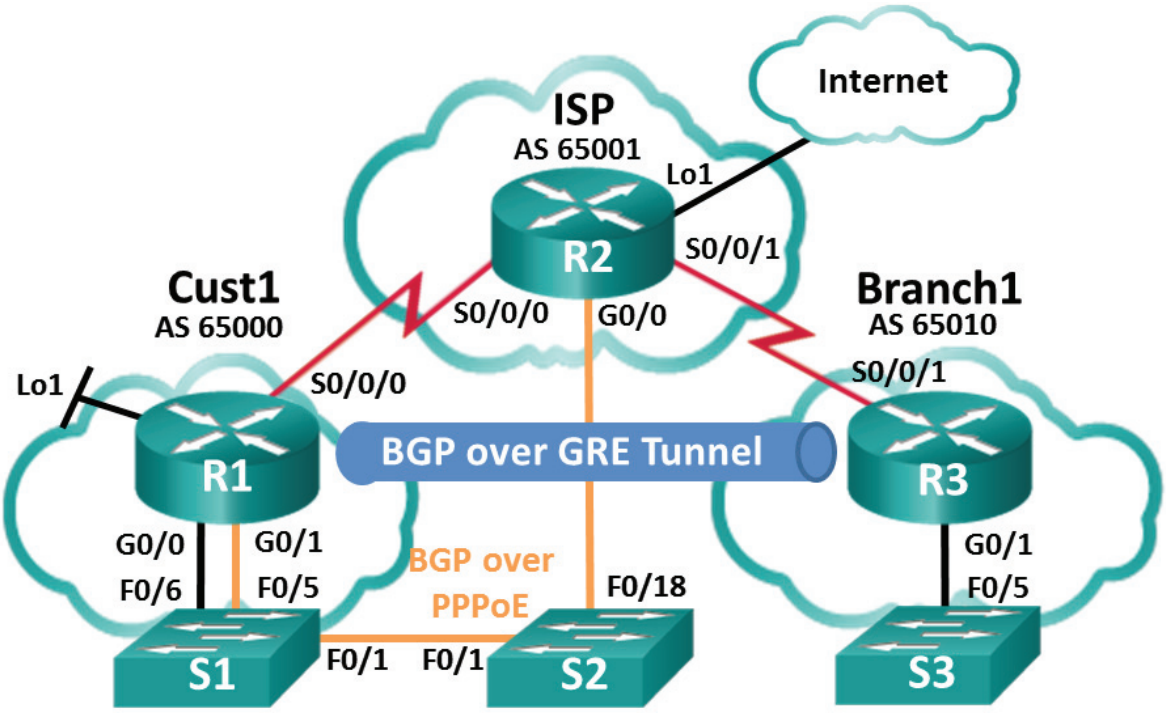
- Because the **REMOTE** LAN should have connectivity to the **HQ** LAN, configure OSPF across the GRE tunnel.
  - Configure OSPF process 100 on the **REMOTE** router.
  - **REMOTE** should advertise the LAN network via OSPF.
  - **REMOTE** should be configured to form an adjacency with **HQ** over the GRE tunnel.
  - Disable OSPF updates on appropriate interfaces.
- Because the **HQ** LAN should have connectivity to the **REMOTE** LAN, configure OSPF across the GRE tunnel.
  - Configure OSPF process 100 on the **HQ** router.
  - **HQ** should advertise the LAN network via OSPF.
  - **HQ** should be configured to form an adjacency with **REMOTE** over the GRE tunnel.
  - Disable OSPF updates on appropriate interfaces.

Connectivity

- Verify full connectivity from **PC2** to the **DNS Server**.
- Verify full connectivity from **PC1** to the **DNS Server**.

3.6.1.3 Lab–Configure a Branch Connection

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	G0/0	192.168.1.1	255.255.255.0
	G0/1	PPPoE Client	
	Lo1	209.165.200.49	255.255.255.240
	S0/0/0 (DCE)	209.165.200.81	255.255.255.252
R2	G0/0	PPPoE Provider	
	Lo1	209.165.200.65	255.255.255.240
	S0/0/0	209.165.200.82	255.255.255.252
	S0/0/1 (DCE)	209.165.200.85	255.255.255.252
R3	G0/1	192.168.3.1	255.255.255.0
	S0/0/1 (DCE)	209.165.200.86	255.255.255.252

Objectives

Part 1: Build the Network and Load Device Configurations

Part 2: Configure a PPPoE Client Connection

Part 3: Configure a GRE Tunnel

Part 4: Configure BGP over PPPoE and BGP over a GRE Tunnel

Background/Scenario

In this lab, you will configure two separate WAN connections, a BGP route over a PPPoE connection, and a BGP route over a GRE tunnel. This lab is a test case scenario and does not represent a realistic BGP implementation.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS, Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Ensure that the routers have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 3 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables and Serial cables as shown in the topology

Part 1: Build the Network and Load Device Configurations

Step 1. Cable the network as shown in the topology.

Step 2. Load router configurations.

Copy and paste the following configurations into the appropriate routers and switch.

Cust 1 (R1) Configuration:

```
conf t
hostname Cust1
no cdp run
interface Loopback1
 ip address 209.165.200.49 255.255.255.240
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 no shut
interface Serial0/0/0
 ip address 209.165.200.81 255.255.255.252
 no shut
ip route 0.0.0.0 0.0.0.0 s0/0/0 25
end
```

Note: In the Cust1 configuration above, CDP is disabled with the **no cdp run** command. The static default route with an administrative distance is manually configured to 25 instead of the default 1. The significance of these configurations will be explained later in the lab.

ISP (R2) Configuration:

```
conf t
hostname ISP
username Cust1 password 0 ciscopppoe
bba-group pppoe global
 virtual-template 1
interface Loopback 1
 ip address 209.165.200.65 255.255.255.240
interface GigabitEthernet0/0
 ip tcp adjust-mss 1452
 pppoe enable group global
 no shut
interface Serial0/0/0
 ip address 209.165.200.82 255.255.255.252
 no shut
interface Serial0/0/1
 ip address 209.165.200.85 255.255.255.252
 no shut
interface Virtual-Template1
 mtu 1492
 ip address 209.165.200.30 255.255.255.224
 peer default ip address pool PPPoEPOOL
 ppp authentication chap callin
router bgp 65001
 network 0.0.0.0
 neighbor 209.165.200.1 remote-as 65000
ip local pool PPPoEPOOL 209.165.200.1 209.165.200.20
ip route 0.0.0.0 0.0.0.0 Loopback1
end
```

Branch1 (R3) Configuration:

```
conf t
hostname Branch1
interface GigabitEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 no shut
interface Serial0/0/1
 ip address 209.165.200.86 255.255.255.252
 no shut
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
end
```

S1 Configuration:

```
conf t
hostname S1
vlan 111
interface f0/6
```

```
switchport mode access
switchport access vlan 111
    end
```

Note: Because S1 connects to two separate networks, G0/0 and G0/1 on Cust1, it is necessary to segment the switch into two separate VLANs, in this case VLAN111 and VLAN1.

Step 3. Save the configuration on all configured routers and switches.

Part 2: Configure a PPPoE Client Connection

In Part 2, following the PPPoE requirements listed below, you will configure Cust1 as the PPPoE client. The ISP router configuration is already complete.

PPPoE requirements for the Cust1 router:

- Configure an **interface Dialer1** with the following settings:
  - **a negotiated ip address**
  - **mtu 1492**
  - **ppp encapsulation**
  - **dialer pool 1**
  - **ppp chap callin authentication**
  - **ppp chap hostname Cust1**
  - **ppp chap password ciscopppoe (unencrypted)**
- Configure **G0/1** with the following settings:
  - **enable global pppoe**
  - **adjust the TCP maximum segment size to 1452**
  - **set the pppoe-client to dialer pool 1**

List the commands used to configure Cust1 as the PPPoE Client:

If the Cust1 router is configured correctly, it should receive an IP address from the ISP router. What IP address did Cust1 receive and on what interface? What command did you use to check for the IP address and interface?

_____

_____

Note: If Cust1 had CDP running on interface dialer1, it could produce the following repeating log message: *PPP: Outbound cdp packet dropped, NCP not negotiated*. To prevent this, CDP was globally turned off.

Part 3: Configure a GRE Tunnel

In Part 3, following the GRE requirements listed below, you will configure a GRE tunnel between Cust1 and Branch1.

GRE tunnel requirements:

- On Cust1 and Branch1, configure **interface Tunnel 0** with the following settings:
  - **IP address 192.168.2.1/24 and 192.168.2.2/24 respectively**
  - **Tunnel mode GRE over IP**
  - **Tunnel source interface and destination address using serial interfaces**

List the commands used to configure a GRE tunnel between Cust1 and Branch1:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

How can you tell if the tunnel was created successfully? What command could you use to test the tunnel?

_____

_____

What would happen if Cust1 did not have a static default route? Test it by removing the static default route. What was the result? Make sure to replace the static default route, as shown in the Cust1 configuration in Part 1 Step 2, before moving on.

_____

_____

Part 4: Configure BGP over PPPoE and BGP over a GRE Tunnel

In Part 4, following the BGP requirements listed below, you will configure BGP on Cust1 and Branch1. The ISP router configuration is already complete.

BGP requirements:

- On Cust1:
  - **Create a BGP routing process AS 65000**
  - **Advertise networks attached to Loopback 1 and G0/0**
  - **Configure BGP neighbors to the ISP and Branch1 routers**
- On Branch1:
  - **Create a BGP routing process AS 65010**
  - **Advertise the network attached to G0/1**
  - **Configure BGP neighbor to Cust1 only**

List the commands used to configure BGP on Cust1 and Branch1:

_____

_____

_____

_____

_____

_____

_____

On Cust1, did you receive console messages regarding BGP neighbor relationships to ISP and Branch1?

_____

On Cust1, can you ping the ISP at 209.165.200.30 over PPPoE? Can you ping the Branch1 local network at 192.168.3.1?

_____

Check the routing table of Cust1. What routes were learned by BGP? There should be a route learned from both ISP and Branch1.

_____

_____

Examine the two routes learned by BGP in the Cust1 routing table. What do they show about routes in the network now?

_____

_____

_____

_____

_____

Router Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parentheses is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.