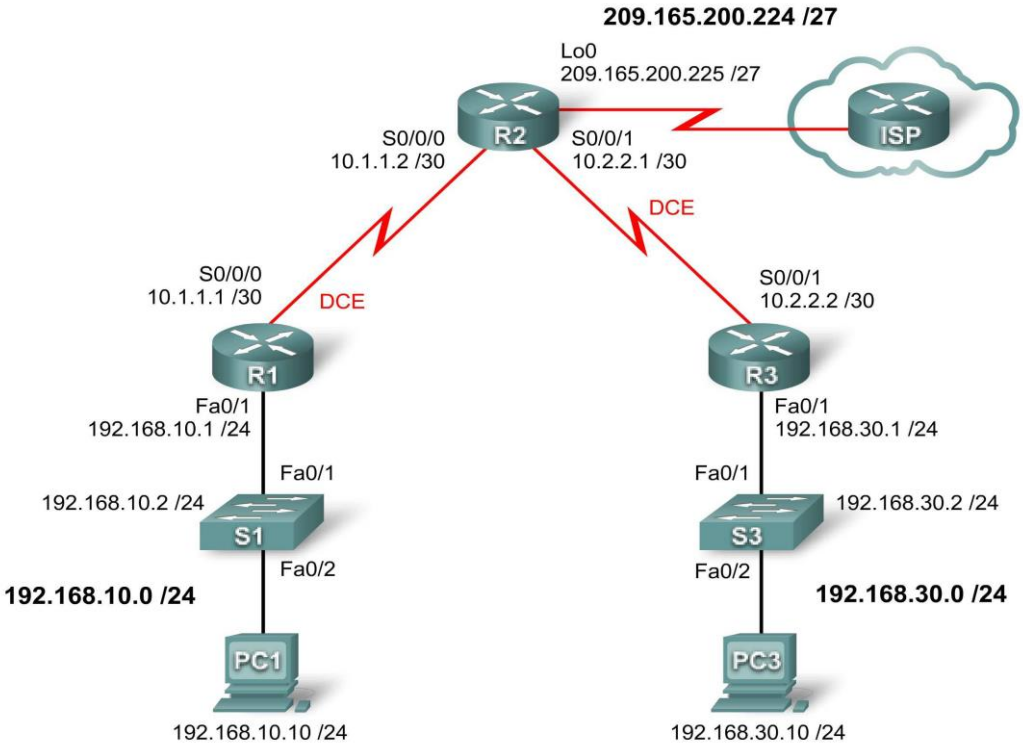
INDEX

Experiment – 1

Objective: Basic PPP Configuration Lab

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	192.168.10.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	Lo0	209.165.200.225	255.255.255.224	N/A
	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
R3	Fa0/1	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC3	NIC	192.168.30.10	255.255.255.0	192.168.30.1

Learning Objectives

1. Cable a network according to the topology diagram
2. Erase the startup configuration and reload a router to the default state

3. Perform basic configuration tasks on a router
4. Configure and activate interfaces
5. Configure OSPF routing on all routers
6. Configure PPP encapsulation on all serial interfaces
7. Learn about the **debug ppp negotiation** and **debug ppp packet** commands
8. Learn how to change the encapsulation on the serial interfaces from PPP to HDLC
9. Intentionally break and restore PPP encapsulation
10. Configure PPP PAP and CHAP authentication
11. Intentionally break and restore PPP PAP and CHAP authentication

Background / Scenario

In this lab, you will learn how to configure PPP encapsulation on serial links using the network shown in the topology diagram. You will also learn how to restore serial links to their default HDLC encapsulation. Pay special attention to what the output of the router looks like when you intentionally break PPP encapsulation. This will assist you in the Troubleshooting lab associated with this chapter. Finally, you will configure PPP PAP authentication and PPP CHAP authentication.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology diagram.

Note: If you use 1700, 2500, or 2600 routers, the router outputs and interface descriptions appear differently.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configuration

Configure the R1, R2, and R3 routers according to the following guidelines:

• Configure the router hostname.
• Disable DNS lookup.
• Configure an EXEC mode password.

CCNA Exploration

Accessing the WAN: PPP Lab 2.5.1: Basic PPP Configuration

• Configure a message-of-the-day banner.
• Configure a password for console connections.
• Configure synchronous logging.
• Configure a password for vty connections.

Task 3: Configure and Activate Serial and Ethernet Addresses

Step 1: Configure interfaces on R1, R2, and R3.

Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from the addressing table at the beginning of the lab. Be sure to include the clock rate on the serial DCE interfaces.

Step 2: Verify IP addressing and interfaces.

Use the **show ip interface brief** command to verify that the IP addressing is correct and that the interfaces are active. When you have finished, be sure to save the running configuration to the NVRAM of the router.

Step 3: Configure the Ethernet interfaces of PC1 and PC3.

Configure the Ethernet interfaces of PC1 and PC3 with the IP addresses and default gateways from the addressing table.

Step 4: Test the configuration by pinging the default gateway from the PC.

Task 4: Configure OSPF on the Routers

Step 1: Enable OSPF routing on R1, R2, and R3.

Use the **router ospf** command with a process ID of 1. Be sure to advertise the networks.

R1(config)#**router ospf 1**
R1(config-router)#**network 192.168.10.0 0.0.0.255 area 0**
R1(config-router)#**network 10.1.1.0 0.0.0.3 area 0**

R2(config)#**router ospf 1**
R2(config-router)#**network 10.1.1.0 0.0.0.3 area 0**
R2(config-router)#**network 10.2.2.0 0.0.0.3 area 0**
R2(config-router)#**network 209.165.200.224 0.0.0.31 area 0**

R3(config)#**router ospf 1**
R3(config-router)#**network 10.2.2.0 0.0.0.3 area 0**
R3(config-router)#network **192.168.30.0 0.0.0.255 area 0**

Step 2: Verify that you have full network connectivity.

Use the **show ip route** and **ping** commands to verify connectivity.

R1#**show ip route**
R1#**ping 192.168.30.1**

R2#**show ip route**
R2#**ping 192.168.30.1**
R2#**ping 192.168.10.1**

R3#**show ip route**
R3#**ping 209.165.200.225**
R3#**ping 192.168.10.1**

Task 5: Configure PPP Encapsulation on Serial Interfaces

Step 1: Use the show interface command to check whether HDLC is the default serial encapsulation.

R1#**show interface serial0/0/0**
R3#**show interface serial 0/0/1**

Step 2: Use debug commands on R1 and R2 to see the effects of configuring PPP.

R1#**debug ppp negotiation**
PPP protocol negotiation debugging is on
R1#**debug ppp packet**
PPP packet display debugging is on

R2#**debug ppp negotiation**
PPP protocol negotiation debugging is on
R2#**debug ppp packet**
PPP packet display debugging is on

Step 3: Change the encapsulation of the serial interfaces from HDLC to PPP.

Change the encapsulation type on the link between R1 and R2, and observe the effects. If you start to receive too much debug data, use the **undebug all** command to turn debugging off.

R1(config)#**interface serial 0/0/0**
R1(config-if)#**encapsulation ppp**
R2(config)#**interface serial 0/0/0**
R2(config-if)#**encapsulation ppp**

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

_____
_____
_____

What steps does PPP go through when the other end of the serial link on R2 is configured with PPP encapsulation?

_____
_____
_____
_____
_____
_____

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

_____
_____

Step 4: Turn off debugging.

Turn off debugging if you have not already used the **undebug all** command.

R1#**undebug all**
Port Statistics for unclassified packets is not turned on.
All possible debugging has been turned off

R2#**undebug all**
Port Statistics for unclassified packets is not turned on.
All possible debugging has been turned off

Step 5: Change the encapsulation from HDLC to PPP on both ends of the serial link between R2 and R3.

R2(config)#**interface serial0/0/1**
R2(config-if)#**encapsulation ppp**

When does the line protocol on the serial link come up and the OSPF adjacency is restored?

_____
_____

Step 7: Verify that PPP is now the encapsulation on the serial interfaces.

R1#**show interface serial0/0/0**
R2#**show interface serial 0/0/0**
R2#**show interface serial 0/0/1**
R3#**show interface serial 0/0/1**

Task 7: Break and Restore PPP Encapsulation

By intentionally breaking PPP encapsulation, you will learn about the error messages that are generated. This will help you later in the Troubleshooting lab.

Step 1: Return both serial interfaces on R2 to their default HDLC encapsulation.

R2(config)#**interface serial 0/0/0**
R2(config-if)#**encapsulation hdlc**

Why is it useful to intentionally break a configuration?

_____
_____
_____

Why do both serial interfaces go down, come back up, and then go back down?

_____
_____
_____

Can you think of another way to change the encapsulation of a serial interface from PPP to the default HDLC encapsulation other than using the **encapsulation hdlc** command? (Hint: It has to do with the **no** command.)

_____
_____
_____
_____

_____
_____

Step 2: Return both serial interfaces on R2 to PPP encapsulation.
R2(config)#**interface s0/0/0**
R2(config-if)#**encapsulation ppp**
R2(config-if)#**interface s0/0/1**
R2(config-if)#**encapsulation ppp**

Task 8: Configure PPP Authentication

Step 1: Configure PPP PAP authentication on the serial link between R1 and R2.
R1(config)#**username R1 password cisco**
R1(config)#**int s0/0/0**
R1(config-if)#**ppp authentication pap**
R1(config-if)#**ppp pap sent-username R2 password cisco**

What happens when PPP PAP authentication is only configured on one end of the serial link?

_____
_____

R2(config)#**username R2 password cisco**
R2(config)#**interface Serial0/0/0**
R2(config-if)#**ppp authentication pap**
R2(config-if)#**ppp pap sent-username R1 password cisco**

What happens when PPP PAP authentication is configured on both ends of the serial link?

_____
_____

Step 2: Configure PPP CHAP authentication on the serial link between R2 and R3.
In PAP authentication, the password is not encrypted. While this is certainly better than no authentication at all, it is still highly preferable to encrypt the password that is being sent across the link. CHAP encrypts the password.
R2(config)#**username R3 password cisco**
R2(config)#**int s0/0/1**
R2(config-if)#**ppp authentication chap**

R3(config)#**username R2 password cisco**
R3(config)#**int s0/0/1**
R3(config-if)#**ppp authentication chap**

Notice that the line protocol on interface serial 0/0/1 changes state to UP even before the interface is configured for CHAP authentication. Can you guess why this is the case?

_____
_____
_____

Step 3: Review the debug output.
To better understand the CHAP process, view the output of the **debug ppp authentication** command on R2 and R3. Then shut down interface serial 0/0/1 on R2, and issue the **no shutdown** command on interface serial 0/0/1 on R2.
R2#**debug ppp authentication**
PPP authentication debugging is on
R2#**conf t**
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#**int s0/0/1**
R2(config-if)#**shutdown**

R2(config-if)#**no shutdown**

R3#**debug ppp authentication**
PPP authentication debugging is on

Task 9: Intentionally Break and Restore PPP CHAP Authentication

Step 1: Break PPP CHAP authentication.

On the serial link between R2 and R3, change the authentication protocol on interface serial 0/0/1 to PAP.

R2#**conf t**
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#**int s0/0/1**
R2(config-if)#**ppp authentication pap**
R2(config-if)#**^Z**
R2#**reload**

Does changing the authentication protocol to PAP on interface serial 0/0/1 break authentication between R2 and R3?

_____
_____
_____

Step 2: Restore PPP CHAP authentication on the serial link.

Notice that it is not necessary to reload the router for this change to take effect.

R2#**conf t**
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#**int s0/0/1**
R2(config-if)#**ppp authentication chap**

Step 3: Intentionally Break PPP CHAP authentication by changing the password on R3.

R3#**conf t**
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#**username R2 password ciisco**
R3(config)#**^Z**
R3#**copy run start**
Destination filename [startup-config]?
Building configuration...
[OK]
R3#**reload**

After reloading, what is the status of the line protocol on serial 0/0/1?

_____
_____

Step 4: Restore PPP CHAP authentication by changing the password on R3.

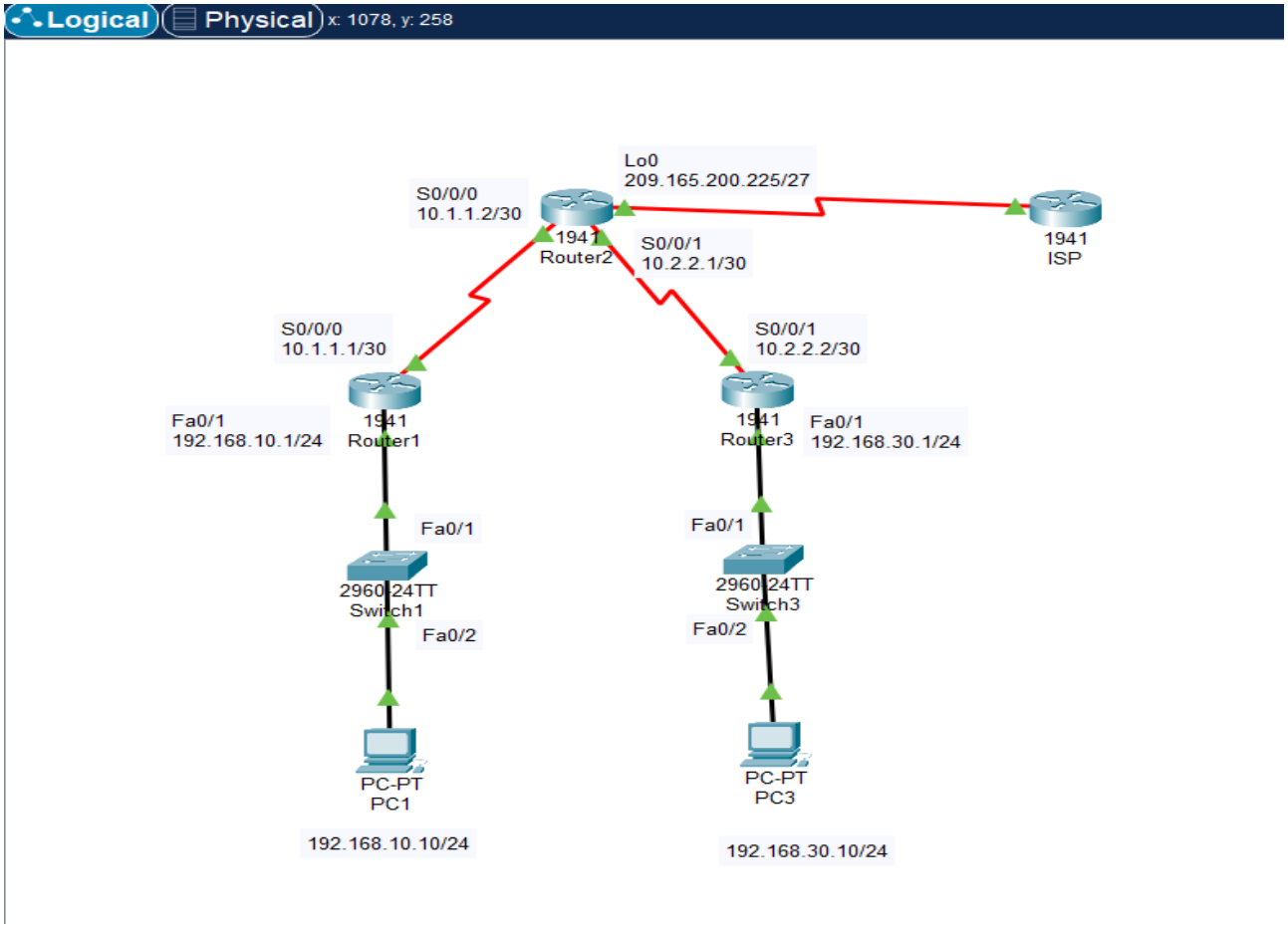
R3#**conf t**
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#**username R2 password cisco**

Task 10: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Router Interface Summary Table

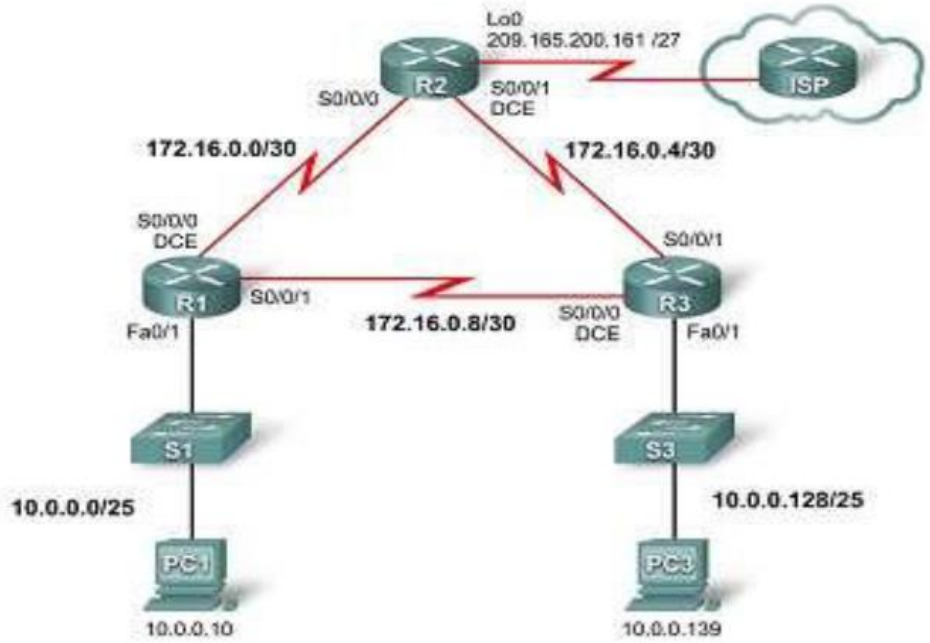
Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	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 parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				



Experiment – 2

Objective: Challenge PPP Configuration

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.

Branch1:

```
Branch1# show ip route ospf
Branch1# show ip ospf interface brief
Branch1# show ip ospf neighbor
```

Central:

```
Central# show ip route ospf
Central# show ip ospf interface brief
Central# show ip ospf neighbor
```

Branch3:

```
Branch3# show ip route ospf
Branch3# show ip ospf interface brief
Branch3# show ip ospf neighbor
```

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
```

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

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
```

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 current interface status for S0/0/0?

_____

Branch1# show ip interface brief

Line status is up, and line protocol is down.

```
Branch1# show ip interface brief
```

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
```

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)? _____ Open

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

_____

Internet Protocol Control Protocol (IPCP) and Cisco Discovery Protocol Control Protocol (CDPCP)

```
Branch1# show interfaces s0/0/0

Central# show interfaces s0/0/0
```

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.

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.

_____

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

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.

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

_____
___

_____
___

_____
___

The link goes down, and the OSPF adjacency is broken. PPP keeps trying to establish a connection with the opposite end of the link as indicated by the message “Phase is ESTABLISHING”. However, because it keeps receiving a non-NCP packet, LCP fails to negotiate and the link stays down.

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.

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

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?

_____
___

_____
___

PPP goes through the following phases: DOWN, ESTABLISHING, and UP.

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

_____
___

The link comes up, and the OSPF adjacency is restored.

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?

_____
___

Serial 0/0/0 has status up and protocol up.

```
Branch1# show ip interface brief
```

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.

_____
___

_____
___

Branch1# show interfaces s0/0/0

Central# show interfaces s0/0/0

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

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

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.

_____
___

show running-config with output modifiers or show interfaces *interface-id*

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.

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

_____
___

_____
___

PPP goes through the following phases: DOWN, ESTABLISHING, AUTHENTICATING, and UP.

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.

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

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

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?

_____
___

The interface S0/0/0 is going up and down.

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
```

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.

_____
___

_____
___

_____
___

The link terminated because the CHAP handshake cannot be completed without the correct user credential on Branch1.

Branch1(config)# username Central password cisco

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?

_____
___

Some of the indicators are: the network is no longer converged because some of the routes are removed and the line protocol for the link is down.

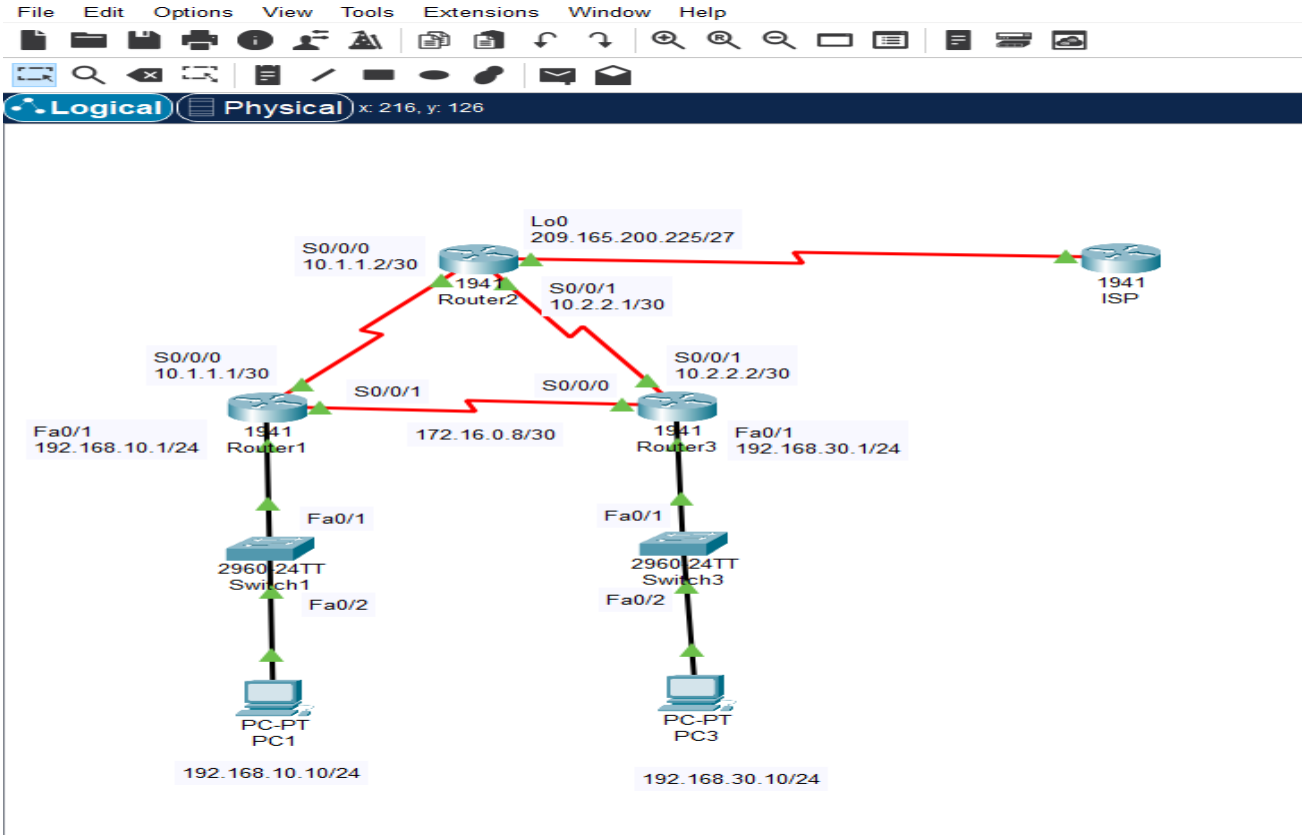
2. What are the indicators that you may have an authentication mismatch on a serial link?

_____
___

Some of the indicators are: the route is removed from the routing table and the line protocol goes up and down.

Router Interface Summary Table

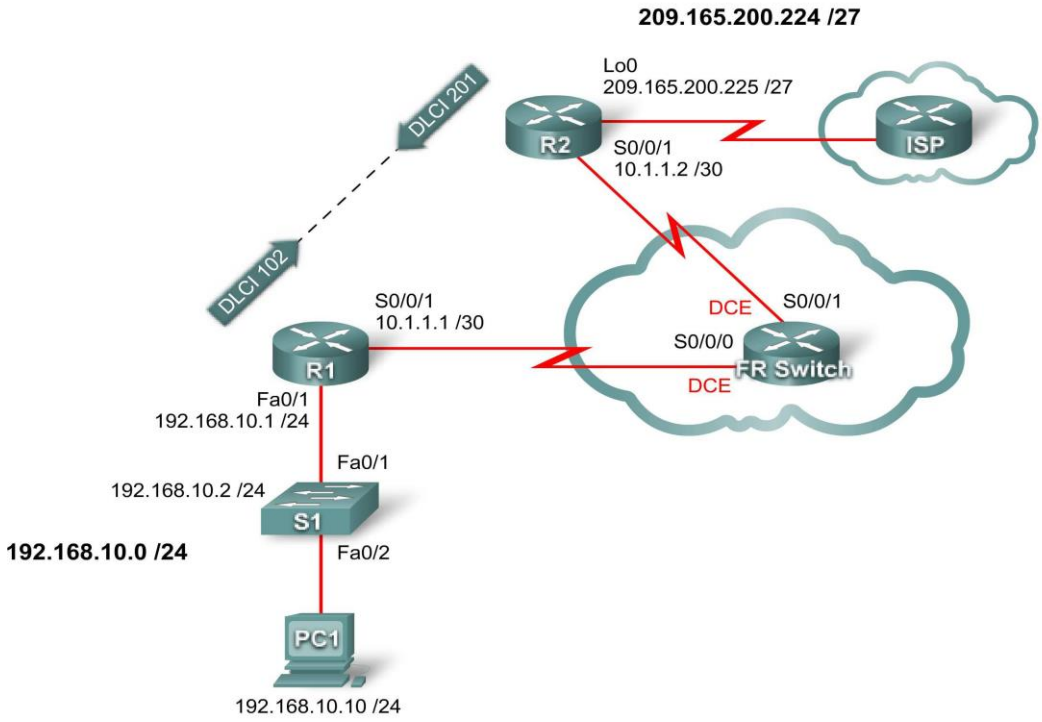
Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	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 parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				



Experiment – 3

Objective: Basic Frame Relay

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.10.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R2	S0/0/1	10.1.1.2	255.255.255.252	N/A
	Lo 0	209.165.200.225	255.255.255.224	N/A
S1	VLAN1	192.168.10.2	255.255.255.0	192.168.10.1
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1

Learning Objectives

Upon completion of this lab, you will be able to:

1. Cable a network according to the topology diagram
2. Erase the startup configuration and reload a router to the default state
3. Perform basic configuration tasks on a router
4. Configure and activate interfaces
5. Configure EIGRP routing on all routers
6. Configure Frame Relay encapsulation on all serial interfaces

7. Configure a router as a Frame Relay switch
8. Understand the output of the **show frame-relay** commands
9. Learn the effects of the **debug frame-relay lmi** command
10. Intentionally break and restore a Frame Relay link
11. Change the Frame Relay encapsulation type from the Cisco default to IETF
12. Change the Frame Relay LMI type from Cisco to ANSI
13. Configure a Frame Relay sub interface

Background / Scenario

In this lab, you will learn how to configure Frame Relay encapsulation on serial links using the network shown in the topology diagram. You will also learn how to configure a router as a Frame Relay switch. There are both Cisco standards and Open standards that apply to Frame Relay. You will learn both. Pay special attention in the lab section in which you intentionally break the Frame Relay configurations. This will help you in the Troubleshooting lab associated with this chapter.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

You can use any current router in your lab as long as it has the required interfaces shown in the topology. The Frame Relay labs, unlike any of the other labs in Exploration 4, have two DCE links on the same router. Be sure to change your cabling to reflect the topology diagram.
Note: If you use 1700, 2500, or 2600 routers, the router output and interface descriptions appear differently.

Step 2: Clear any existing configurations on the routers.

Task 2: Perform Basic Router Configuration

Configure the R1 and R2 routers and the S1 switch according to the following guidelines:
• Configure the router hostname.
• Disable DNS lookup.
• Configure an EXEC mode password.
• Configure a message-of-the-day banner.
• Configure a password for console connections.
• Configure a password for vty connections.
• Configure IP addresses on R1 and R2
Important: Leave serial interfaces shut down.
• Enable EIGRP AS 1 on R1 and R2 for all networks.

```
enable
configure terminal
no ip domain-lookup
enable secret class
banner motd ^CUnauthorized access strictly prohibited, violators
will be prosecuted to the full extent of the law^C
!
!
!
line console 0
logging synchronous
password cisco
login
!
line vty 0 4
password cisco
login
end
copy running-config startup-config
```

!R1

```
interface serial 0/0/1
ip address 10.1.1.1 255.255.255.252
shutdown
!The serial interfaces should remain shutdown until the Frame Relay
!switch is configured
interface fastethernet 0/0
ip address 192.168.10.1 255.255.255.0
no shutdown
router eigrp 1
no auto-summary
network 10.0.0.0
network 192.168.10.0
!
```

!R2

```
interface serial 0/0/1
ip address 10.1.1.2 255.255.255.252
shutdown
!The serial interfaces should remain shutdown until the Frame Relay
!switch is configured
interface loopback 0
ip address 209.165.200.225 255.255.255.224
router eigrp 1
no auto-summary
network 10.0.0.0
network 209.165.200.0
!
```

Task 3: Configure Frame Relay

You will now set up a basic point-to-point Frame Relay connection between routers 1 and 2. You first need to configure FR Switch as a Frame Relay switch and create DLCIs.

What does DLCI stand for?

_____

What is a DLCI used for?

_____

_____

What is a PVC and how is it used?

_____

_____

_____

Step 1: Configure FR Switch as a Frame Relay switch and create a PVC between R1 and R2.

This command enables Frame Relay switching globally on the router, allowing it to forward frames based on the incoming DLCI rather than on an IP address basis:

FR-Switch(config)#**frame-relay switching**

Change the interface encapsulation type to Frame Relay. Like HDLC or PPP, Frame Relay is a data link layer protocol that specifies the framing of Layer 2 traffic.

FR-Switch(config)#**interface serial 0/0/0**
FR-Switch(config)#**clock rate 64000**
FR-Switch(config-if)#**encapsulation frame-relay**

Changing the interface type to DCE tells the router to send LMI keepalives and allows Frame Relay route statements to be applied. You cannot set up PVCs using the **frame-relay route** command between two Frame Relay DTE interfaces.

FR-Switch(config-if)#**frame-relay intf-type dce**

Note: Frame Relay interface types do not need to match the underlying physical interface type. A physical DTE serial interface can act as a Frame Relay DCE interface, and a physical DCE interface can act as a logical Frame Relay DTE interface.

Configure the router to forward incoming traffic on interface serial 0/0/0 with DLCI 102 to serial 0/0/1 with an output DLCI of 201.
FR-Switch(config-if)#**frame-relay route 102 interface serial 0/0/1 201**
FR-Switch(config-if)#**no shutdown**
This configuration creates two PVCs: one from R1 to R2 (DLCI 102), and one from R2 to R1 (DLCI 201). You can verify the configuration using the **show frame-relay pvc** command.

FR-Switch(config-if)#**interface serial 0/0/1**
FR-Switch(config)#**clock rate 64000**
FR-Switch(config-if)#**encapsulation frame-relay**
FR-Switch(config-if)#**frame-relay intf-type dce**
FR-Switch(config-if)#**frame-relay route 201 interface serial 0/0/0 102**
FR-Switch(config-if)#**no shutdown**
FR-Switch#**show frame-relay pvc**

The PVC you have created does not have any endpoints
configured. The Frame Relay switch knows this and has marked the PVC as Inactive.

Issue the **show frame-relay route** command. This command shows any existing Frame Relay routes, their interfaces, DLCIs, and status. This is the Layer 2 route that Frame Relay traffic takes through the network. Do not confuse this with Layer 3 IP routing.
FR-Switch#**show frame-relay route**

Step 2: Configure R1 for Frame Relay.
Inverse ARP allows distant ends of a Frame Relay link to dynamically discover each other and provides a dynamic method of mapping IP addresses to DLCIs. Although Inverse ARP is useful, it is not always reliable. The best practice is to statically map IP addresses to DLCIs and to disable inverse-arp.
R1(config)#**interface serial 0/0/1**
R1(config-if)#**encapsulation frame-relay**
R1(config-if)#**no frame-relay inverse-arp**
Why would you want to map an IP address to a DLCI?
_____
_____
_____
_____
The command **frame-relay map** statically maps an IP address to a DLCI. In addition to mapping IP to a DLCI, Cisco IOS software allows several other Layer 3 protocol addresses to mapped. The **broadcast** keyword in the following command sends any multicast or broadcast traffic destined for this link over the DLCI. Most routing protocols require the **broadcast** keyword to properly function over Frame Relay. You can use the **broadcast** keyword on multiple DLCIs on the same interface. The traffic is replicated to all PVCs.
R1(config-if)#**frame-relay map ip 10.1.1.2 102 broadcast**
Is the DLCI mapped to the local IP address or the IP address at the other end of the PVC?
_____
R1(config-if)#**no shutdown**

Why is the **no shutdown** command used after the **no frame-relay inverse-arp** command?
_____
_____
_____
_____
Step 3: Configure R2 for Frame Relay.
R2(config)#**interface serial 0/0/1**
R2(config-if)#**encapsulation frame-relay**
R2(config-if)#**no frame-relay inverse-arp**

R2(config-if)#**frame-relay map ip 10.1.1.1 201 broadcast**
R2(config-if)#**no shutdown**
At this point, you receive messages indicating that the interfaces have come up and that EIGRP neighbor adjacency has been established.

The **show ip route** command shows complete routing tables.

R1#**show ip route**

R2#**show ip route**

Task 4: Verify the Configuration

You should now be able to ping from R1 to R2. It may take several seconds after bringing up the interfaces for the PVC to become active. You can also see EIGRP routes for each router.

Step 1: Ping R1 and R2.

Ensure that you can ping router R2 from router R1.
R1#**ping 10.1.1.2**
R2#**ping 10.1.1.1**

Step 2: Get PVC information.

The **show frame-relay pvc** command displays information on all PVCs configured on the router. The output also includes the associated DLCI.
R1#**show frame-relay pvc**
R2#**show frame-relay pvc**
FR-Switch#**show frame-relay pvc**

Step 3: Verify Frame Relay mappings.

The **show frame-relay map** command displays information on the static and dynamic mappings of Layer 3 addresses to DLCIs. Because Inverse ARP has been turned off, there are only static maps.
R1#**show frame-relay map**
R2#**show frame-relay map**
FR Switch:
FR Switch acts as a Layer 2 device, so there is no need to map Layer 3 addresses to Layer 2 DLCIs.

Step 4: Debug the Frame Relay LMI.

What purpose does the LMI serve in a Frame Relay network?

_____
_____
_____
_____

What are the three different types of LMI?

_____

What DLCI does the LMI operate on?

_____

Issue the **debug frame-relay lmi** command. The output gives detailed information on all LMI data. Keepalives are sent every 10 seconds, so you may have to wait until you see any output. The debug output shows two LMI packets: the first outgoing, the second incoming.
R1#**debug frame-relay lmi**
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
R1#**undebug all**

Task 4: Troubleshooting Frame Relay.

A variety of tools are available for troubleshooting Frame Relay connectivity issues. To learn about troubleshooting, you will break the Frame Relay connection established earlier and then reestablish it.

Step 1: Remove the frame map from R1.
R1#**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#**interface serial0/0/1**
R1(config-if)#**encapsulation frame-relay**
R1(config-if)#**no frame-relay map ip 10.1.1.2 102 broadcast**

Now that you have removed the frame map statement from R1, try to ping router R1 from router R2. You will get no response.

R2#**ping 10.1.1.1**

Issue the **debug ip icmp** command on R1:
R1#**debug ip icmp**
ICMP packet debugging is on
Now ping the serial interface of R1 again. The following debug message appears on R1:
R2#**ping 10.1.1.1**

Why does the ping fail?

_____
_____

Issuing the **show frame-relay map** command returns a blank line.
R1#**show frame-relay map**
Turn off all debugging with the **undebug all** command, and re-apply the **frame-relay map ip** command but without using the **broadcast** keyword.
R1#**undebug all**
Port Statistics for unclassified packets is not turned on.
All possible debugging has been turned off
R1#**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#**interface serial0/0/1**
R1(config-if)#**encapsulation frame-relay**
R1(config-if)#**frame-relay map ip 10.1.1.2 102**
R2#**ping 10.1.1.1**
Type escape sequence to abort.
Why does the EIGRP adjacency continue to flap?

_____
_____

Replace the Frame Relay map statement and include the **broadcast** keyword this time. Verify that the full routing table is restored and that you have full end-to-end connectivity.
R1#**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#**interface serial0/0/1**
R1(config-if)#**encapsulation frame-relay**
R1(config-if)#**frame-relay map ip 10.1.1.2 102 broadcast**
R1#**show ip route**

Step 2: Change the Frame Relay encapsulation type.
Cisco IOS software supports two types of Frame Relay encapsulation: the default Cisco encapsulation and the standards-based IETF encapsulation. Change the Frame Relay encapsulation on serial0/0/1 on R2 to IETF.
R2(config-if)#**encapsulation frame-relay ietf**

Notice that the interface does not go down. You might be surprised by this. Cisco routers can correctly interpret Frame Relay frames that use either the default Cisco Frame Relay encapsulation or the IETF standard Frame Relay encapsulation. If your network is composed entirely of Cisco routers, then it does not make any difference whether you use the default Cisco Frame Relay encapsulation or the IETF standard. Cisco routers understand both types of incoming frames. However, if you have routers from different vendors using Frame Relay, then the IETF standard must be used. The command **encapsulation frame-relay ietf** forces the Cisco router to encapsulate its outgoing frames using the IETF standard. This

standard can be correctly understood by the router of another vendor.

R2#**show interface serial 0/0/1**
FR-Switch#**show int s0/0/0**

Step 3: Change the LMI type.
On R2, change the LMI type to ANSI.
R2#**configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#**interface serial 0/0/1**
R2(config-if)#**encapsulation frame-relay**
R2(config-if)#**frame-relay lmi-type ansi**
R2(config-if)#**^Z**
R2#**copy run start**
Destination filename [startup-config]?
Building configuration...
[OK]

R2#**show interface serial 0/0/1**
Serial0/0/1 is up, line protocol is down
R2#**show frame-relay lmi**

If you continue issuing the **show frame-relay lmi** command, you will notice the highlighted times incrementing. When 60 seconds have passed, the interface changes its state to Up Down, because R2 and FR Switch are no longer exchanging keepalives or any other link-state information.
Issue the **debug frame-relay lmi** command. Notice that LMI packets are no longer showing up in pairs. While all outgoing LMI messages are logged, no incoming messages are shown. This is because R2 is expecting ANSI LMI, and FR Switch is sending Cisco LMI.

R2#**debug frame-relay lmi**
R2(config-if)#**frame-relay lmi-type cisco**

As you can see, the LMI sequence number has been reset to 1, and R2 began to understand the LMI messages coming in from FR Switch. After FR Switch and R2 had successfully exchanged LMI messages, the interface changed state to Up.

Task 5: Configure a Frame Relay Sub-interface
Frame Relay supports two types of sub-interfaces: point-to-point and point-to-multipoint. Point-tomultipoint sub-interfaces support non-broadcast multi-access topologies. For example, a hub and spoke topology would use a point-to-multipoint sub-interface. In this lab, you will create a point-topoint sub-interface.

Step 1: On FR Switch, create a new PVC between R1 and R2.
FR-Switch(config)#**interface serial 0/0/0**
FR-Switch(config-if)#**frame-relay route 112 interface serial 0/0/1 212**
FR-Switch(config-if)#**interface serial 0/0/1**
FR-Switch(config-if)#**frame-relay route 212 interface serial 0/0/0 112**

Step 2: Create and configure a point-to-point sub-interface on R1.
Create subinterface 112 as a point-to-point interface. Frame Relay encapsulation must be specified on the physical interface before subinterfaces can be created.
R1(config)#**interface serial 0/0/1.112 point-to-point**
R1(config-subif)#**ip address 10.1.1.5 255.255.255.252**
R1(config-subif)#**frame-relay interface-dlci 112**

Step 3: Create and configure a point-to-point sub-interface on R2.
R2(config)#**interface serial 0/0/1.212 point-to-point**
R2(config-subif)#**ip address 10.1.1.6 255.255.255.252**

R2(config-subif)#**frame-relay interface-dlci 212**

Step 4: Verify connectivity.
You should be able to ping across the new PVC.
R1#**ping 10.1.1.6**
R2#**ping 10.1.1.5**

You can also verify the configuration using the **show frame-relay pvc** and **show frame-relay map** commands in Task 4.

R1#**show frame-relay pvc**
R2#**show frame-relay pvc**
FR-Switch#**show frame-relay pvc**

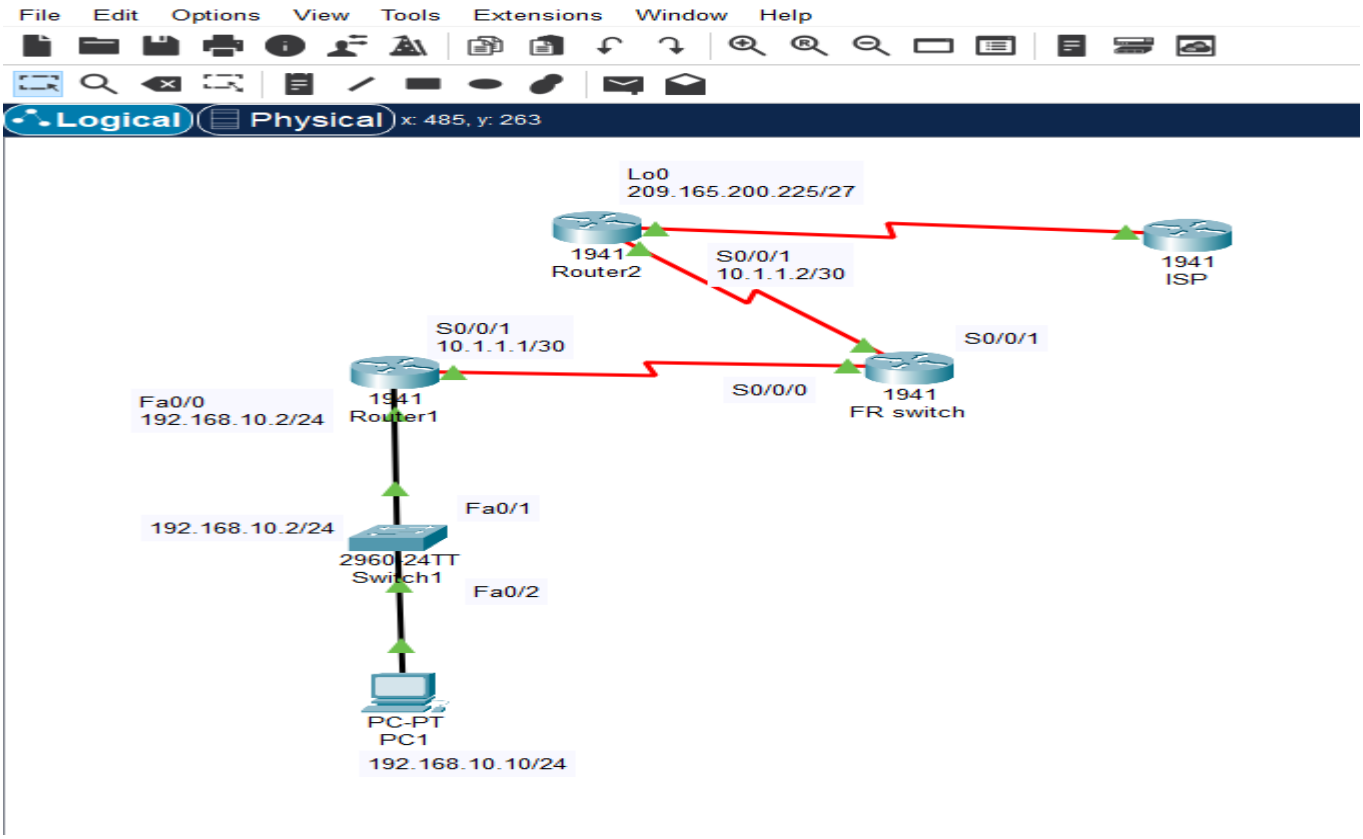
R1#**show frame-relay map**
R2#**show frame-relay map**
FR-Switch#**show frame-relay route**

R1#**debug frame-relay lmi**
Note that two DLCIs are listed in the LMI message from FR Switch to R1.
R2#**debug frame-relay lmi**

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)

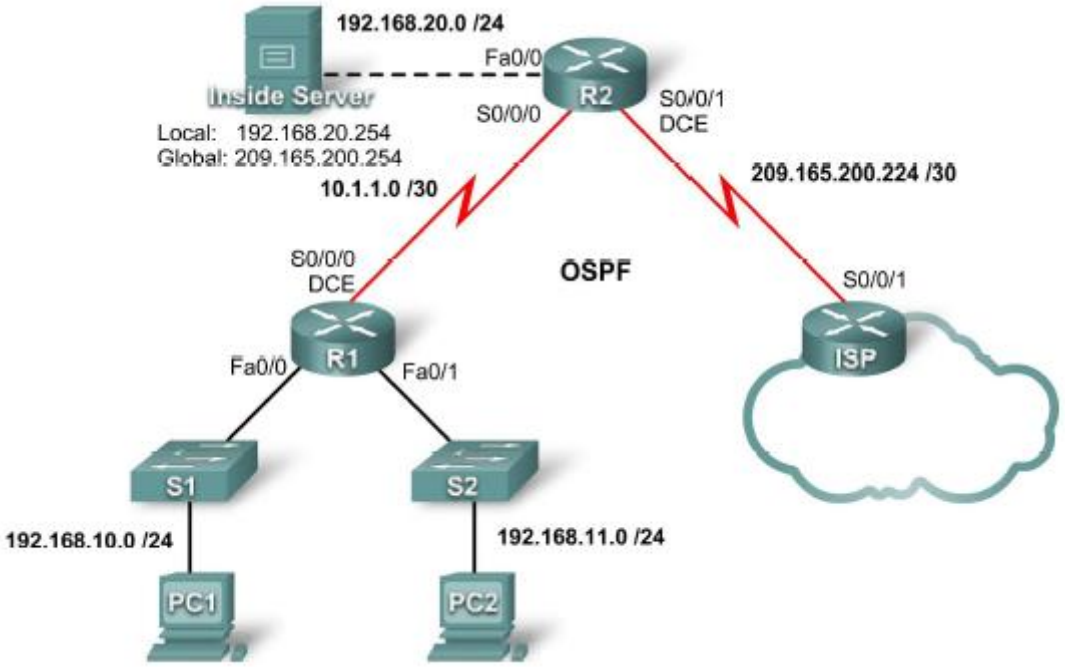
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations 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 parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.


File Edit Options View Tools Extensions Window Help
Logical
Physical
x: 485, y: 263
Lo0
209.165.200.225/27
1941
Router2
S0/0/1
10.1.1.2/30
1941
ISP
S0/0/1
10.1.1.1/30
S0/0/1
S0/0/0
1941
Router1
1941
FR switch
Fa0/0
192.168.10.2/24
192.168.10.2/24
Fa0/1
2960-24TT
Switch1
Fa0/2
PC-PT
PC1
192.168.10.10/24

Experiment – 4

Objective: Basic DHCP and NAT Configuration

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	209.165.200.225	255.255.255.252
	Fa0/0	192.168.20.254	255.255.255.0
ISP	S0/0/1	209.165.200.226	255.255.255.252

Background / Scenario

In this lab, you will configure the DHCP and NAT IP services. One router is the DHCP server. The other router forwards DHCP requests to the server. You will also configure both static and dynamic NAT configurations, including NAT overload. When you have completed the configurations, verify the connectivity between the inside and outside addresses.

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear all existing configurations on the routers.

Task 2: Perform Basic Router Configurations

Configure the R1, R2, and ISP routers according to the following guidelines:
• Configure the device hostname.
• Disable DNS lookup.
• Configure a privileged EXEC mode password.
• Configure a message-of-the-day banner.
• Configure a password for the console connections.
• Configure a password for all vty connections.
• Configure IP addresses on all routers. The PCs receive IP addressing from DHCP later in the lab.
• Enable OSPF with process ID 1 on R1 and R2. Do not advertise the 209.165.200.224/27 network.
Note: Instead of attaching a server to R2, you can configure a loopback interface on R2 to use the IP address 192.168.20.254/24. If you do this, you do not need to configure the Fast Ethernet interface.

Task 3: Configure PC1 and PC2 to receive an IP address through DHCP

On a Windows PC go to **Start** -> **Control Panel** -> **Network Connections** -> **Local Area Connection**.
Right mouse click on the **Local Area Connection** and select **Properties**.
Make sure the button is selected that says **Obtain an IP address automatically**.
Once this has been done on both PC1 and PC2, they are ready to receive an IP address from a DHCP server.

Task 4: Configure a Cisco IOS DHCP Server

Cisco IOS software supports a DHCP server configuration called Easy IP. The goal for this lab is to have devices on the networks 192.168.10.0/24 and 192.168.11.0/24 request IP addresses via DHCP from R2.

Step 1: Exclude statically assigned addresses.

The DHCP server assumes that all IP addresses in a DHCP address pool subnet are available for assigning to DHCP clients. You must specify the IP addresses that the DHCP server should not assign to clients. These IP addresses are usually static addresses reserved for the router interface, switch management IP address, servers, and local network printer. The **ip dhcp excluded-address** command prevents the router from assigning IP addresses within the configured range. The following commands exclude the first 10 IP addresses from each pool for the LANs attached to R1. These addresses will not be assigned to any DHCP clients.

R2(config)#**ip dhcp excluded-address 192.168.10.1 192.168.10.10**
R2(config)#**ip dhcp excluded-address 192.168.11.1 192.168.11.10**

Step 2: Configure the pool.

Create the DHCP pool using the **ip dhcp pool** command and name it **R1Fa0**.
R2(config)#**ip dhcp pool R1Fa0**

Specify the subnet to use when assigning IP addresses. DHCP pools automatically associate with an interface based on the network statement. The router now acts as a DHCP server, handing out addresses in the 192.168.10.0/24 subnet starting with 192.168.10.1.
R2(dhcp-config)#**network 192.168.10.0 255.255.255.0**

Configure the default router and domain name server for the network. Clients receive these settings via DHCP, along with an IP address.
R2(dhcp-config)#**dns-server 192.168.11.5**
R2(dhcp-config)#**default-router 192.168.10.1**

Note: There is not a DNS server at 192.168.11.5. You are configuring the command for practice only. Because devices from the network 192.168.11.0/24 also request addresses from R2, a separate pool must be created to serve devices on that network. The commands are similar to the commands shown above:
R2(config)#**ip dhcp pool R1Fa1**
R2(dhcp-config)#**network 192.168.11.0 255.255.255.0**
R2(dhcp-config)#**dns-server 192.168.11.5**
R2(dhcp-config)#**default-router 192.168.11.1**

Step 3: Test DHCP
On PC1 and PC2 test whether each has received an IP address automatically. On each PC go to **Start** -> **Run** -> **cmd** -> **ipconfig -all**
What are the results of your test? _____
Why are these the results? _____

Step 4: Configure a helper address.
Network services such as DHCP rely on Layer 2 broadcasts to function. When the devices providing these services exist on a different subnet than the clients, they cannot receive the broadcast packets. Because the DHCP server and the DHCP clients are not on the same subnet, configure R1 to forward DHCP broadcasts to R2, which is the DHCP server, using the **ip helper-address** interface configuration command.
Notice that **ip helper-address** must be configured on each interface involved.
R1(config)#**interface fa0/0**
R1(config-if)#**ip helper-address 10.1.1.2**
R1(config)#**interface fa0/1**
R1(config-if)#**ip helper-address 10.1.1.2**

Step 5: Release and Renew the IP addresses on PC1 and PC2
Depending upon whether your PCs have been used in a different lab, or connected to the internet, they may already have learned an IP address automatically from a different DHCP server. We need to clear this IP address using the **ipconfig /release** and **ipconfig /renew** commands.

Step 6: Verify the DHCP configuration.
You can verify the DHCP server configuration in several different ways. Issue the command **ipconfig** on PC1 and PC2 to verify that they have now received an IP address dynamically. You can then issue commands on the router to get more information. The **show ip dhcp binding** command provides information on all currently assigned DHCP addresses. For instance, the following output shows that the IP address 192.168.10.11 has been assigned to MAC address 3031.632e.3537.6563. The IP lease expires on September 14, 2007 at 7:33 p.m.
R1#**show ip dhcp binding**

The **show ip dhcp pool** command displays information on all currently configured DHCP pools on the router. In this output, the pool **R1Fa0** is configured on R1. One address has been leased from this pool. The next client to request an address will receive 192.168.10.12.
R2#**show ip dhcp pool**

The **debug ip dhcp server events** command can be extremely useful when troubleshooting DHCP leases with a Cisco IOS DHCP server. The following is the debug output on R1 after connecting a host. Notice that the highlighted portion shows DHCP giving the client an address of 192.168.10.12 and mask of 255.255.255.0

Task 5: Configure Static and Default Routing
ISP uses static routing to reach all networks beyond R2. However, R2 translates private addresses into public addresses before sending traffic to ISP. Therefore, ISP must be configured with the public addresses that are part of the NAT configuration on R2. Enter the following static route on ISP:
ISP(config)#**ip route 209.165.200.240 255.255.255.240 serial 0/0/1**
This static route includes all addresses assigned to R2 for public use.
Configure a default route on R2 and propagate the route in OSPF.
R2(config)#**ip route 0.0.0.0 0.0.0.0 209.165.200.226**
R2(config)#**router ospf 1**
R2(config-router)#**default-information originate**
Allow a few seconds for R1 to learn the default route from R2 and then check the R1 routing table. Alternatively, you can clear the routing table with the **clear ip route** * command. A default route pointing to R2 should appear in the R1 routing table. From R1, ping the serial 0/0/1 interface on ISP (209.165.200.226). The pings should be successful. Troubleshoot if the pings fail.

Task 6: Configure Static NAT

Step 1: Statically map a public IP address to a private IP address.
The inside server attached to R2 is accessible by outside hosts beyond ISP. Statically assign the public IP address 209.165.200.254 as the address for NAT to use to map packets to the private IP address of the inside server at 192.168.20.254.
R2(config)#**ip nat inside source static 192.168.20.254 209.165.200.254**

Step 2: Specify inside and outside NAT interfaces.
Before NAT can work, you must specify which interfaces are inside and which interfaces are outside.
R2(config)#**interface serial 0/0/1**
R2(config-if)#**ip nat outside**
R2(config-if)#**interface fa0/0**
R2(config-if)#**ip nat inside**
Note: If using a simulated inside server, assign the **ip nat inside** command to the loopback interface.

Step 3: Verify the static NAT configuration.
From ISP, ping the public IP address 209.165.200.254.

Task 7: Configure Dynamic NAT with a Pool of Addresses
While static NAT provides a permanent mapping between an internal address and a specific public address, dynamic NAT maps private IP addresses to public addresses. These public IP addresses come from a NAT pool.

Step 1: Define a pool of global addresses.
Create a pool of addresses to which matched source addresses are translated. The following command creates a pool named MY-NAT-POOL that translates matched addresses to an available IP address in the 209.165.200.241–209.165.200.246 range.
R2(config)#**ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask 255.255.255.248**

Step 2: Create an extended access control list to identify which inside addresses are translated.
R2(config)#**ip access-list extended NAT**
R2(config-ext-nacl)#**permit ip 192.168.10.0 0.0.0.255 any**
R2(config-ext-nacl)#**permit ip 192.168.11.0 0.0.0.255 any**

Step 3: Establish dynamic source translation by binding the pool with the access control list.
A router can have more than one NAT pool and more than one ACL. The following command tells the router which address pool to use to translate hosts that are allowed by the ACL.
R2(config)#**ip nat inside source list NAT pool MY-NAT-POOL**

Step 4: Specify inside and outside NAT interfaces.
You have already specified the inside and outside interfaces for your static NAT configuration. Now add the serial interface linked to R1 as an inside interface.
R2(config)#**interface serial 0/0/0**
R2(config-if)#**ip nat inside**

Step 5: Verify the configuration.
Ping ISP from PC1 or the Fast Ethernet interface on R1 using extended **ping**. Then use the **show ip nat translations** and **show ip nat statistics** commands on R2 to verify NAT.
R2#**show ip nat translations**
R2#**show ip nat statistics**

To troubleshoot issues with NAT, you can use the **debug ip nat** command. Turn on NAT debugging and repeat the ping from PC1.
R2#**debug ip nat**

Task 8: Configure NAT Overload
In the previous example, what would happen if you needed more than the six public IP addresses that the pool allows?

By tracking port numbers, NAT overloading allows multiple inside users to reuse a public IP address. In this task, you will remove the pool and mapping statement configured in the previous task. Then you will configure NAT overload on R2 so that all internal IP addresses are translated to the R2 S0/0/1 address when connecting to any outside device.

Step 1: Remove the NAT pool and mapping statement.
Use the following commands to remove the NAT pool and the map to the NAT ACL.
R2(config)#**no ip nat inside source list NAT pool MY-NAT-POOL**
R2(config)#**no ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask 255.255.255.248**
If you receive the following message, clear your NAT translations.
%Pool MY-NAT-POOL in use, cannot destroy
R2#**clear ip nat translation ***

Step 2: Configure PAT on R2 using the serial 0/0/1 interface public IP address.
The configuration is similar to dynamic NAT, except that instead of a pool of addresses, the **interface** keyword is used to identify the outside IP address. Therefore, no NAT pool is defined. The **overload** keyword enables the addition of the port number to the translation.
Because you already configured an ACL to identify which inside IP addresses to translate as well as which interfaces are inside and outside, you only need to configure the following:
R2(config)#**ip nat inside source list NAT interface S0/0/1 overload**

Step 3: Verify the configuration.
Ping ISP from PC1 or the Fast Ethernet interface on R1 using extended **ping**. Then use the **show ip nat translations** and **show ip nat statistics** commands on R2 to verify NAT.
R2#**show ip nat translations**

Note: In the previous task, you could have added the keyword **overload** to the **ip nat inside source list NAT pool MY-NAT-POOL** command to allow for more than six concurrent users.

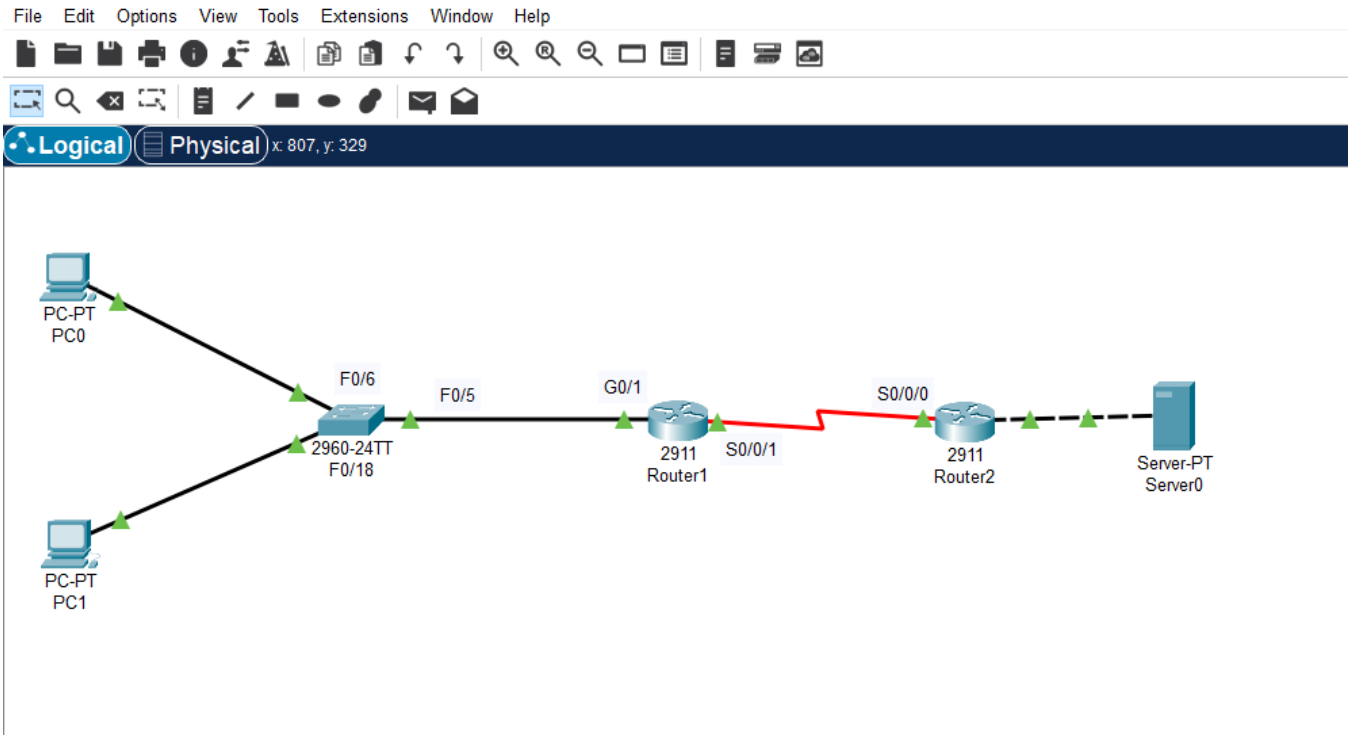
Task 9: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

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)

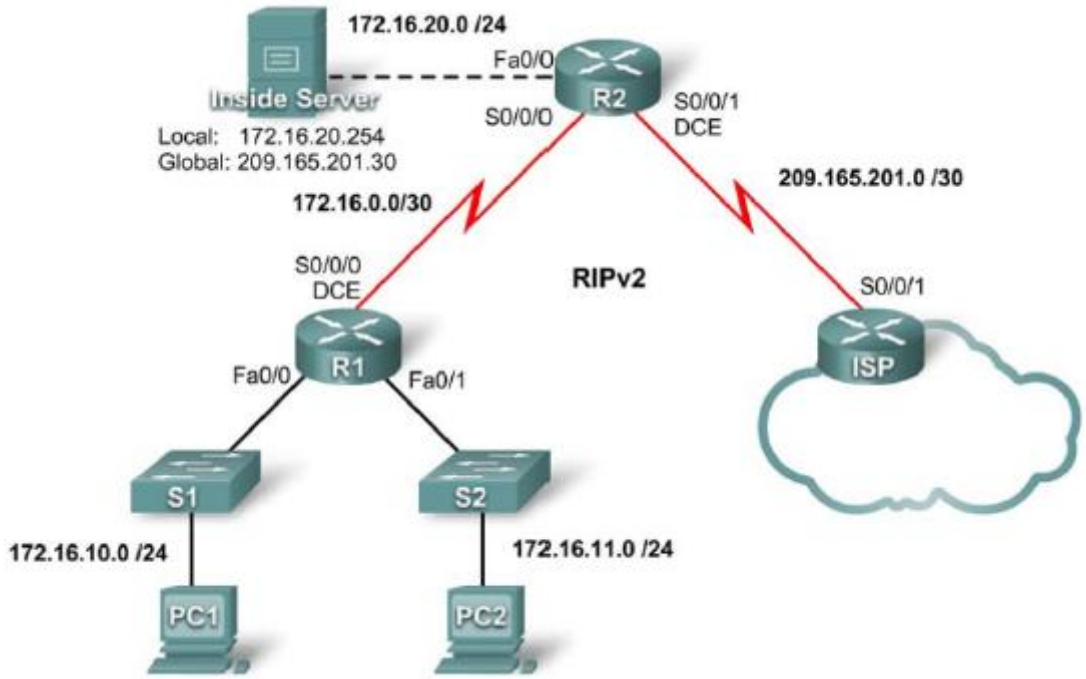
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations 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 parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.



Experiment – 5

Objective: Troubleshooting DHCP and NAT

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	S0/0/0	172.16.0.1	255.255.255.252
	Fa0/0	172.16.10.1	255.255.255.0
	Fa0/1	172.16.11.1	255.255.255.0
R2	S0/0/0	172.16.0.2	255.255.255.252
	S0/0/1	209.165.201.1	255.255.255.252
	Fa0/0	172.16.20.1	255.255.255.0
ISP	S0/0/1	209.165.201.2	255.255.255.252

Scenario

The routers, R1 and R2, 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 DHCP, NAT, and standard testing methods, find and correct the errors. Make sure all clients have full connectivity. The ISP has been configured correctly.

Ensure that the network supports the following:

1. The router R2 should serve as the DHCP server for the 172.16.10.0/24 and 172.16.11.0/24 networks connected to R1.
2. All PCs connected to R1 should receive an IP address in the correct network via DHCP.
3. Traffic from the R1 LANs entering the Serial 0/0/0 interface on R2 and exiting the Serial 0/0/1 interface on R2 should receive NAT translation with a pool of addresses provided by the ISP.
4. The Inside Server should be reachable from outside networks using IP address 209.165.201.30, and to inside networks using IP address 172.16.20.254

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Step 2: Clear all existing configurations on the routers.

Step 3: Import the configurations below.

R1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 172.16.10.1 255.255.255.0
 ip helper-address 172.16.0.2
 no shutdown
!
interface FastEthernet0/1
 ip address 172.16.11.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.1 255.255.255.252
 clock rate 125000
 no shutdown
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
banner motd $AUTHORIZED ACCESS ONLY$
!
```

```
line con 0
password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end
```

R2

```
hostname R2
!
enable secret class
!
ip dhcp excluded-address 172.16.10.1 172.16.10.3
ip dhcp excluded-address 172.16.11.1 172.16.11.3
!
ip dhcp pool R1_LAN10
   network 172.16.10.0 255.255.255.0
   dns-server 172.16.20.254
!
ip dhcp pool R1_LAN11
   network 172.16.11.0 255.255.255.0
   dns-server 172.16.20.254
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 172.16.20.1 255.255.255.0
 ip nat inside
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 209.165.201.1 255.255.255.252
 ip nat outside
 clock rate 125000
 no shutdown
!
router rip
 version 2
 network 172.16.0.0
 default-information originate
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.201.2
!
ip nat pool NAT_POOL 209.165.201.9 209.165.201.14 netmask 255.255.255.248
ip nat inside source list NAT_ACL pool NATPOOL overload

!
```

```
ip access-list standard NAT_ACL
 permit 172.16.10.0 0.0.0.255
!
banner motd $AUTHORIZED ACCESS ONLY$
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end
```

ISP

```
hostname ISP
!
enable secret class
!
interface Serial0/0/1
 ip address 209.165.201.2 255.255.255.252
 no shutdown
!
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
banner motd $AUTHORIZED ACCESS ONLY$
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end
```

Task 2: Find and Correct Network Errors

When the network is configured correctly:

- PC1 and PC2 should be able to receive IP addresses from the correct DHCP pool as evidenced by an ipconfig on the PCs. Additionally; a `show ip dhcp bindings` on R2 should show that both PCs have received IP addresses.
- Test pings from PC1 and PC2 to the ISP should receive NAT overload translation as evidenced by a `show ip nat translations` on R2.
- Test pings from the Inside Server to ISP should receive the static NAT translation indicated on the topology. Use the `show ip nat translations` command to verify this.
- A ping from the ISP to the global address of the Inside Server should be successful.

- Test pings from ISP to R1 should not receive NAT translation as evidenced by a `show ip nat translations` or a `debug ip nat` on R2.

Task 3: Document the Router Configurations

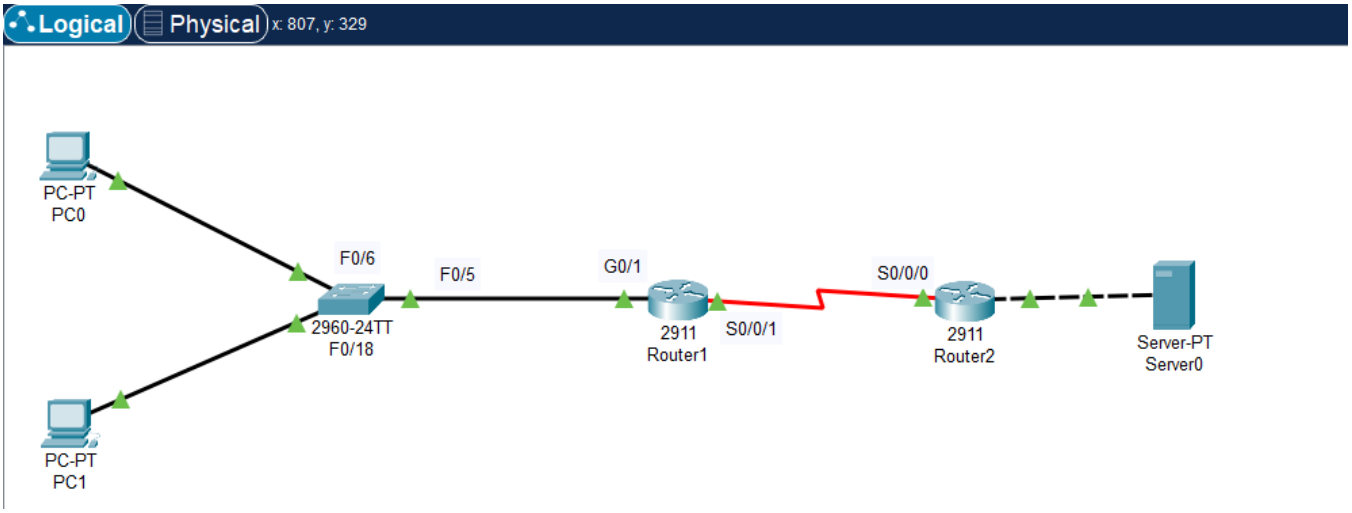
On each router, issue the **show run** command and capture the configurations.

Task 4: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks, such as the school LAN or to the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

Router Interface Summary Table

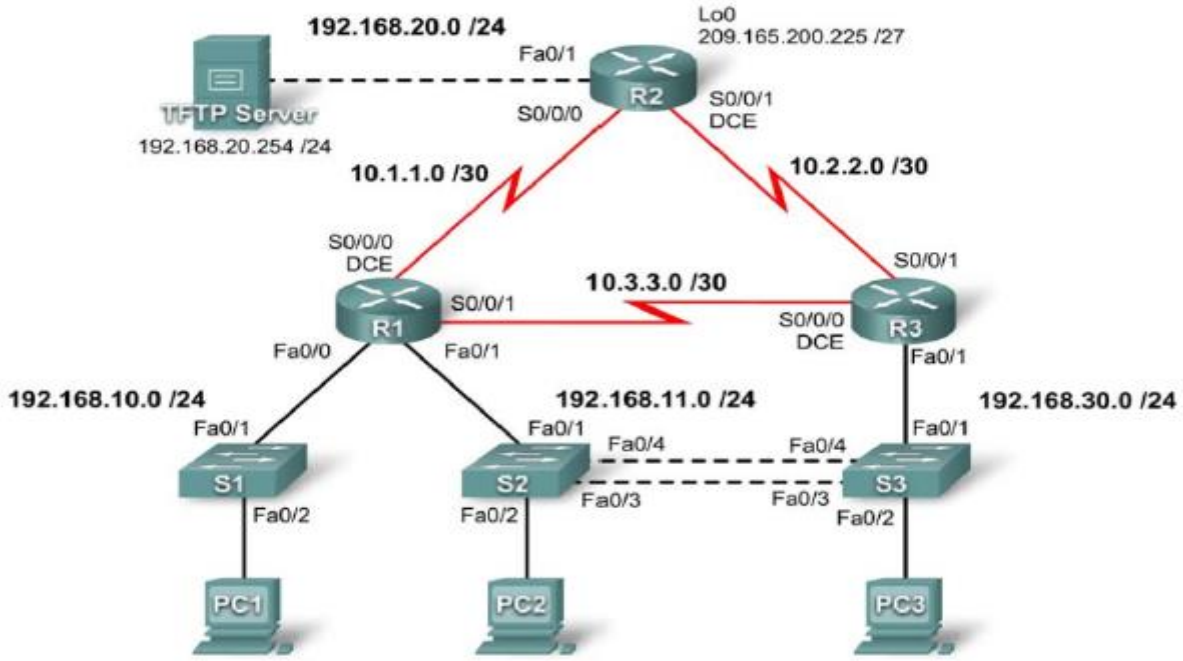
Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	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 parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				



Experiment – 6

Objective: Troubleshooting Enterprise Networks 1

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.10.1	255.255.255.0	N/A
	Fa0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	Fa0/1	192.168.20.1	255.255.255.0	N/A
	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
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226
R3	Fa0/1	N/A	N/A	N/A
	Fa0/1.11	192.168.11.3	255.255.255.0	N/A
	Fa0/1.30	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
S1	VLAN10	DHCP	255.255.255.0	N/A
S2	VLAN11	192.168.11.2	255.255.255.0	N/A
S3	VLAN30	192.168.30.2	255.255.255.0	N/A
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC2	NIC	192.168.11.10	255.255.255.0	192.168.11.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable a network according to the topology diagram
- Erase the startup configuration and reload a router to the default state
- Load the routers and switches with supplied scripts
- Find and correct all network errors
- Document the corrected network

Scenario

For this lab do not use login or password protection on any console lines to prevent accidental lockout. Use **ciscoccna** for all passwords in this scenario.

Note: Because this lab is cumulative, you will be using all the knowledge and troubleshooting techniques that you have acquired from the previous material to successfully complete this lab.

Requirements

- S2 is the spanning-tree root for VLAN 11, and S3 is the spanning-tree root for VLAN 30.
- S3 is a VTP server with S2 as a client.
- The serial link between R1 and R2 is Frame Relay.
- The serial link between R2 and R3 uses HDLC encapsulation.
- The serial link between R1 and R3 is authenticated using CHAP.
- R2 must have secure login procedures because it is the Internet edge router.
- All vty lines, except those belonging to R2, allow connections only from the subnets shown in the topology diagram, excluding the public address.
- Source IP address spoofing should be prevented on all links that do not connect to other routers.
- Routing protocols must be used securely. OSPF is used in this scenario.
- R3 must not be able to telnet to R2 through the directly connected serial link.
- R3 has access to both VLAN 11 and 30 via its Fast Ethernet port 0/1.
- The TFTP server should not get any traffic that has a source address outside the subnet. All devices have access to the TFTP server.
- All devices on the 192.168.10.0 subnet must be able to get their IP addresses from DHCP on R1. This includes S1.
- All addresses shown in diagram must be reachable from every device.

Task 1: Load Routers with the Supplied Scripts

```
!----------------------------------------
!                  R1
!----------------------------------------
no service password-encryption
!
hostname R1
!
```

```
boot-start-marker
boot-end-marker
!
security passwords min-length 6
enable secret ciscoccna
!
ip cef
!
ip dhcp pool Access1
   network 192.168.11.0 255.255.255.0
   default-router 192.168.10.1
!
no ip domain lookup
!
ip dhcp excluded-address 192.168.10.2 192.168.10.254
!
frame-relay switching
!
username R3 password 0 ciscoccna
username ccna password 0 ciscoccna
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 duplex auto
 speed auto
no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
 no keepalive
 clockrate 128000
 frame-relay map ip 10.1.1.1 201
 frame-relay map ip 10.1.1.2 201 broadcast
 no frame-relay inverse-arp
 frame-relay intf-type dce
 no shutdown
!
interface Serial0/0/1
 ip address 10.3.3.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
interface Serial0/1/0
 no ip address
 shutdown
 clockrate 2000000
!
interface Serial0/1/1
```

```
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/0
 network 10.1.1.0 0.0.0.255 area 0
 network 10.2.2.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
ip http server
!
ip access-list standard Anti-spoofing
 permit 192.168.10.0 0.0.0.255
 deny   any
ip access-list standard VTY
 permit 10.0.0.0 0.255.255.255
 permit 192.168.10.0 0.0.0.255
 permit 192.168.11.0 0.0.0.255
 permit 192.168.20.0 0.0.0.255
 permit 192.168.30.0 0.0.0.255
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
line vty 0 4
 access-class VTY in
 login local
!
end
!----------------------------------------
!                  R2
!----------------------------------------
no service password-encryption
!
hostname R2
!
security passwords min-length 6
enable secret ciscoccna
!
aaa new-model
!
aaa authentication login local_auth local
aaa session-id common
!
ip cef
!
no ip domain lookup
!
username ccna password 0 ciscoccna
!
interface Loopback0
 ip address 209.165.200.245 255.255.255.224
 ip access-group private in
```

```
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 ip access-group TFTP out
 ip access-group Anti-spoofing in
 ip nat inside
 duplex auto
 speed auto
!
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 ip nat outside
 encapsulation frame-relay
 no keepalive
 frame-relay map ip 10.1.1.1 201 broadcast
 frame-relay map ip 10.1.1.2 201
 no frame-relay inverse-arp
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 ip access-group R3-telnet in
 ip nat outside
!
!
router ospf 1
 passive-interface FastEthernet0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
no ip http server
ip nat inside source list nat interface FastEthernet0/0
!
ip access-list standard Anti-spoofing
 permit 192.168.20.0 0.0.0.255
 deny   any
ip access-list standard NAT
 permit 10.0.0.0 0.255.255.255
 permit 192.168.0.0 0.0.255.255
ip access-list standard private
 deny   127.0.0.1
 deny   10.0.0.0 0.255.255.255
 deny   172.0.0.0 0.31.255.255
 deny   192.168.0.0 0.0.255.255
 permit any
!
ip access-list extended R3-telnet
 deny   tcp host 10.2.2.2 host 10.2.2.1 eq telnet
 deny   tcp host 10.3.3.2 host 10.2.2.1 eq telnet
 deny   tcp host 192.168.11.3 host 10.2.2.1 eq telnet
 deny   tcp host 192.168.30.1 host 10.2.2.1 eq telnet
 permit ip any any
!
```

```
ip access-list standard TFTP
 permit 192.168.20.0 0.0.0.255
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport output telnet
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport input telnet
!
end
!-----------------------------------------
!                  R3
!-----------------------------------------
no service password-encryption
!
hostname R3
!
security passwords min-length 6
enable secret ciscoccna
!
no aaa new-model
!
ip cef
!
no ip domain lookup
!
username R1 password ciscoccna
username ccna password ciscoccna
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1.11
 encapsulation dot1Q 12
ip address 192.168.11.3 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip access-group Anti-spoofing in
!
!
interface Serial0/0/0
 ip address 10.3.3.2 255.255.255.252
```

```
 encapsulation ppp
 clockrate 125000
 ppp authentication chap
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 encapsulation lapb
 no shutdown
!
router ospf 1
 passive-interface FastEthernet0/1.30
 network 10.2.2.0 0.0.0.3 area 1
 network 10.3.3.0 0.0.0.3 area 1
 network 192.168.11.0 0.0.0.255 area 1
 network 192.168.30.0 0.0.0.255 area 1
!
ip classless
!
ip http server
!
ip access-list standard Anti-spoofing
 permit 192.168.30.0 0.0.0.255
 deny   any
ip access-list standard VTY
 permit 10.0.0.0 0.255.255.255
 permit 192.168.10.0 0.0.0.255
 permit 192.168.11.0 0.0.0.255
 permit 192.168.20.0 0.0.0.255
 permit 192.168.30.0 0.0.0.255
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
 exec-timeout 15 0
 logging synchronous
line vty 0 4
 access-class VTY in
 exec-timeout 15 0
 logging synchronous
 login local
!
end
!----------------------------------------
!               S1
!----------------------------------------
no service password-encryption
!
hostname S1
!
security passwords min-length 6
enable secret ciscoccna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
```

```
vtp mode transparent
vtp password ciscoccna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 10
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface range FastEthernet0/3-24
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan10
 ip address dhcp
 no ip route-cache
!
ip default-gateway 192.168.10.1
ip http server
!
line con 0
 exec-timeout 5 0
 logging synchronous
line vty 0 4
 password ciscoccna
 login
line vty 5 15
 no login
!
end
!----------------------------------------
!                S2
!----------------------------------------
no service pad
service timestamps debug uptime
```

```
service timestamps log uptime
no service password-encryption
!
hostname S2
!
security passwords min-length 6
enable secret ciscoccna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
vtp mode client
vtp password ciscoccna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 11 priority 24576
spanning-tree vlan 30 priority 28672
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport access vlan 11
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 11
 switchport mode access
!
interface FastEthernet0/3
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface range FastEthernet0/5-24
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan11
 ip address 192.168.11.2 255.255.255.0
```

```
 no ip route-cache
!
ip http server
!
line con 0
 exec-timeout 5 0
 logging synchronous
line vty 0 4
 password ciscoccna
 login
line vty 5 15
 no login
!
end
!----------------------------------------
!                S3
!----------------------------------------
no service password-encryption
!
hostname S3
!
security passwords min-length 6
enable secret ciscoccna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
vtp mode Server
vtp password ciscoccna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 11 priority 28672
spanning-tree vlan 30 priority 24576
!
vlan internal allocation policy ascending
!
vlan 30
!
interface FastEthernet0/1
 switchport trunk allowed vlan 11
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
```

```
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface range FastEthernet0/5-24
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan30
 ip address 192.168.30.2 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.30.1
ip http server
!
line con 0
 exec-timeout 5 0
 logging synchronous
line vty 0 4
 password ciscoccna
 login
line vty 5 15
 no login
!
end
```

Task 2: Find and Correct All Network Errors

Task 3: Verify that Requirements Are Fully Met

Because time constraints prevent troubleshooting a problem on each topic, only a select number of topics have problems. However, to reinforce and strengthen troubleshooting skills, you should verify that each requirement is met. To do this, present an example of each requirement (for example a **show** or **debug** command).

Task 4: Document the Corrected Network

Task 4: Clean Up

Erase the configurations and reload the routers. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

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 parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.