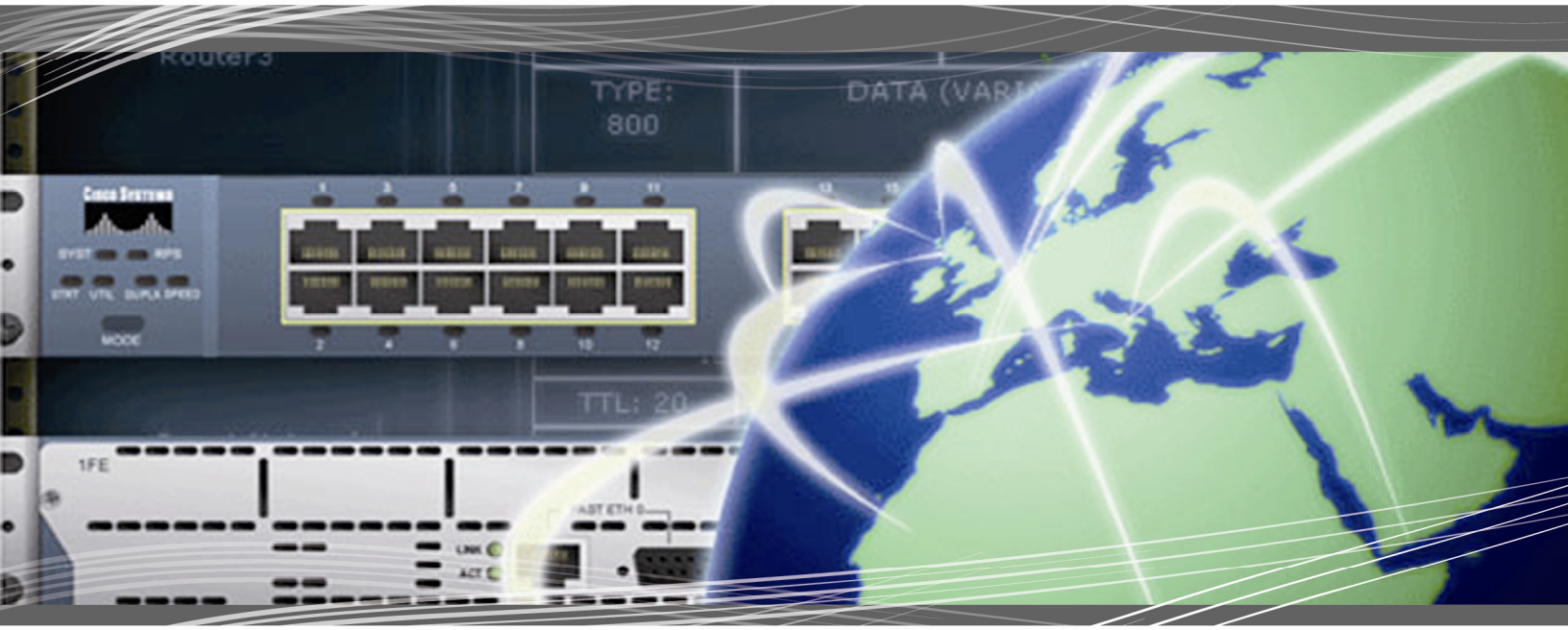
Cisco | Networking Academy®
Mind Wide Open™



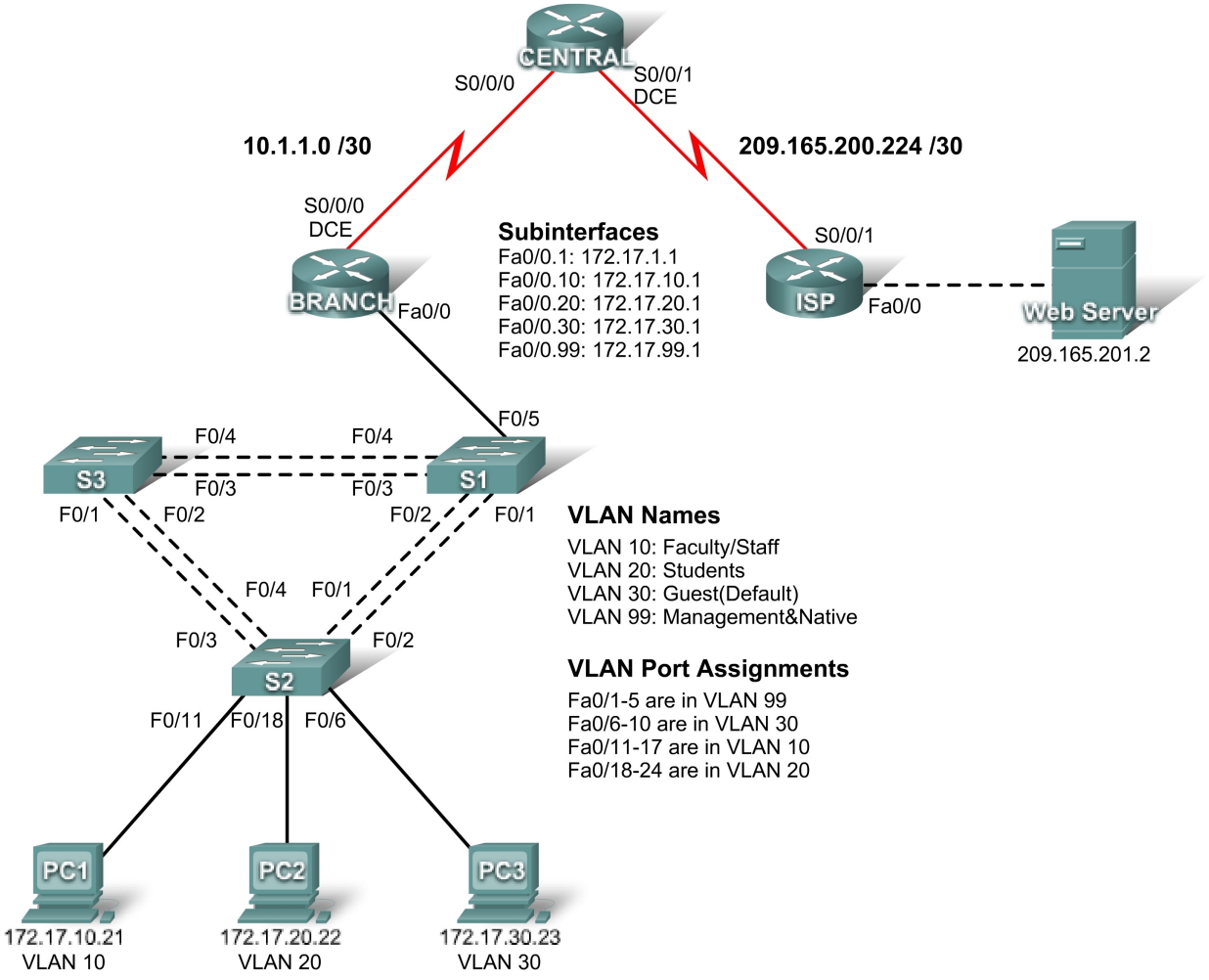
CCNA Exploration 4.0

Accessing the WAN

Instructor Packet Tracer Manual

PT Activity 1.5.1: Packet Tracer Skills Integration Challenge (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
ISP	**S0/0/1**	209.165.200.225	255.255.255.252	N/A
	Fa0/0	209.165.201.1	255.255.255.252	N/A
CENTRAL	**S0/0/0**	10.1.1.2	255.255.255.252	N/A
	S0/0/1	209.165.200.226	255.255.255.252	N/A
BRANCH	**S0/0/0**	10.1.1.1	255.255.255.252	N/A
	Fa0/0.1	172.17.1.1	255.255.255.0	N/A
	Fa0/0.10	172.17.10.1	255.255.255.0	N/A
	Fa0/0.20	172.17.20.1	255.255.255.0	N/A
	Fa0/0.30	172.17.30.1	255.255.255.0	N/A
	Fa0/0.99	172.17.99.1	255.255.255.0	N/A
S1	**VLAN 99**	172.17.99.11	255.255.255.0	172.17.99.1
S2	**VLAN 99**	172.17.99.12	255.255.255.0	172.17.99.1
S3	**VLAN 99**	172.17.99.13	255.255.255.0	172.17.99.1
PC1	**NIC**	172.17.10.21	255.255.255.0	172.17.10.1
PC2	**NIC**	172.17.20.22	255.255.255.0	172.17.20.1
PC3	**NIC**	172.17.30.23	255.255.255.0	172.17.30.1
Web Server	**NIC**	209.165.201.2	255.255.255.252	209.165.201.1

Learning Objectives

- Configure static and default routing
- Add and connect the BRANCH router
- Add and connect the switches
- Add and connect the PCs
- Perform basic device configuration
- Configure OSPF routing
- Configure STP
- Configure VTP
- Configure VLANs
- Verify end-to-end connectivity

Introduction

This activity covers many of the skills you acquired in the first three Exploration courses. Skills include building a network, applying an addressing scheme, configuring routing, VLANs, STP and VTP, and testing connectivity. You should review those skills before proceeding. In addition, this activity provides you an opportunity to review the basics of the Packet Tracer program. Packet Tracer is integrated

throughout this course. You must know how to navigate the Packet Tracer environment to complete this course. Use the tutorials if you need a review of Packet Tracer fundamentals. The tutorials are located in the Packet Tracer **Help** menu.

Note: There are over 150 assessed items in this activity. Therefore, you may not see the completion percentage increase every time you enter a command. The user EXEC password is **cisco** and the privileged EXEC password is **class**.

Task 1: Configure Static and Default Routing

Step 1. Configure static routing from ISP to CENTRAL.

Use the topology diagram to configure ISP with static routes to all networks. Each network is reachable via S0/0/1 from ISP. Use the exit interface parameter to configure static routes to the following networks:

- 10.1.1.0/30
- 172.17.1.0/24
- 172.17.10.0/24
- 172.17.20.0/24
- 172.17.30.0/24
- 172.17.99.0/24

Step 2. Configure default routing from CENTRAL to ISP.

Configure a default route on CENTRAL using the exit interface parameter to send all default traffic to ISP.

Step 3. Test connectivity to the Web Server.

CENTRAL should now be able to successfully ping the Web Server at 209.165.201.2.

Step 4. Check results.

Your completion percentage should be 4%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Add and Connect the BRANCH Router

Step 1. Add the BRANCH router.

Click **Custom Made Devices** and add an 1841 router to the topology. Use the **Config** tab to change the Display Name and Hostname to BRANCH. Display Names are case-sensitive.

Step 2. Connect BRANCH to CENTRAL.

- Connect BRANCH to CENTRAL.
- Configure the link between BRANCH and CENTRAL.
- Use a clock rate of **64000** bps

Step 3. Check results.

Your completion percentage should be 8%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Add and Connect the Switches

Refer to the topology for placement, switch names, and interfaces.

Step 1. Using the 2960 model, add the S1, S2, and S3 switches.

Step 2. Connect S1 to BRANCH.

Step 3. Connect S1 to S2.

Step 4. Connect S1 to S3.

Step 5. Connect S2 to S3.

Step 6. Check results.

Your completion percentage should be 28%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Add and Connect the PCs

Use the interfaces specified in the topology diagram and addressing table.

Step 1. Add PC1, PC2, and PC3.

Step 2. Connect PC1, PC2, and PC3 to S2.

Step 3. Configure PCs.

Step 4. Check results.

Your completion percentage should be 41%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Perform Basic Device Configuration

Step 1. Configure the basic commands on BRANCH, S1, S2, and S3.

Basic configuration commands should include the hostname, EXEC password, banner, console, and vty lines.

Step 2. Configure Fast Ethernet subinterfaces on BRANCH.

Remember to configure 802.1q encapsulation and VLAN settings for each subinterface. The third octet for each subinterface address corresponds to VLAN number. For example, subinterface Fa0/0.30 uses the IP address 172.17.**30**.1 and belongs to VLAN 30. VLAN 99 is the native VLAN.

Step 3. Configure the switches.

- Configure the VLAN 99 interface.
- Configure the default gateway.

Step 4. Check results.

Your completion percentage should be 60%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Configure OSPF Routing

Step 1. Configure OSPF on CENTRAL and propagate the default route.

- Configure OSPF using the process ID 1.
- Use OSPF Area 0.
- Add only the network shared with BRANCH.
- Propagate the default route to OSPF neighbors.

Step 2. Configure OSPF on BRANCH.

- Configure OSPF using the process ID 1.
- Use OSPF Area 0.
- Add all networks that BRANCH routes.

Step 3. Disable OSPF updates on the appropriate interfaces on both CENTRAL and BRANCH.

Disable OSPF updates on all LAN interfaces and to ISP.

Step 4. Test connectivity.

BRANCH should be able to successfully ping Web Server at 209.165.201.2

Step 5. Check results.

Your completion percentage should be 69%. If not, click **Check Results** to see which required components are not yet completed.

Task 7: Configure STP

Step 1: Ensure S1 is the root bridge.

Set priorities to 4096.

Step 2: Verify that S1 is the root bridge.

Step 3: Check results.

Your completion percentage should be 72%. If not, click **Check Results** to see which required components are not yet completed.

Task 8: Configure VTP

Step 1: Configure the VTP mode on all three switches.

Configure S1 as the server. Configure S2 and S3 as clients.

Step 2: Configure the VTP domain name on all three switches.

Use **CCNA** as the VTP domain name.

Step 3: Configure the VTP domain password on all three switches.

Use **cisco** as the VTP domain password.

Step 4: Check results.

Your completion percentage should be 77%. If not, click **Check Results** to see which required components are not yet completed.

Task 9: Configure Trunking

Step 1: Configure trunking on S1, S2, and S3.

Configure the appropriate interfaces in trunking mode and assign VLAN 99 as the native VLAN.

Step 2: Check results.

Your completion percentage should be 94%. If not, click **Check Results** to see which required components are not yet completed.

Task 10: Configure VLANs

Step 1. Configure S1 with VLANs.

VLAN names are case-sensitive. Add and name the four VLANs using the following specifications:

- VLAN 10 – **Faculty/Staff**
- VLAN 20 – **Students**
- VLAN 30 – **Guest(Default)**
- VLAN 99 – **Management&Native**

Step 2. Verify that S2 and S3 received VLAN configurations from S1.

Step 3. Configure the ports attached to PCs on S2 for access, and assign each port the appropriate VLAN.

Step 4. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

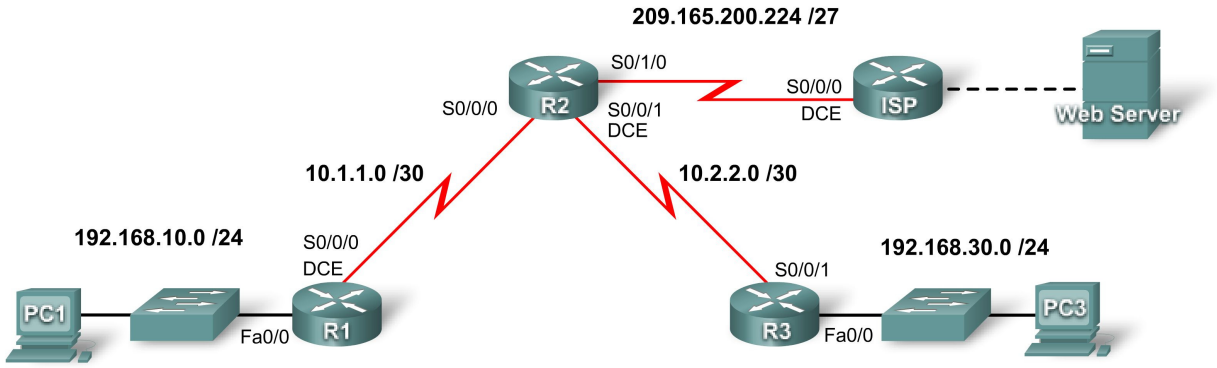
Task 11: Verify End-to-End Connectivity

Step 1. Verify that PC1, PC2, and PC3 can ping each other.

Step 2. Verify that PC1, PC2, and PC3 can ping the Web Server.

PT Activity 2.1.7: Troubleshooting a Serial Interface (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
R3	Fa0/0	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252
ISP	S0/0/0	209.165.200.226	255.255.255.224
	Fa0/0	209.165.200.1	255.255.255.252
Web Server	NIC	209.165.200.2	255.255.255.252
PC1	NIC	192.168.10.10	255.255.255.0
PC3	NIC	192.168.30.10	255.255.255.0

Learning Objectives

- Test connectivity
- Investigate connectivity problems by gathering data
- Implement the solution and test connectivity

Introduction

In this activity, you only have access to the command prompt on PC1 and PC3. To troubleshoot problems on the routers and implement solutions, you must telnet from either PC1 or PC3. The activity is complete when you achieve 100%, and PC1 can ping PC3.

Task 1: Test Connectivity

Step 1: Use ping to test end-to-end connectivity.

Wait for the link lights on S1 and S3 to transition from amber to green. Then, from the command prompt on PC1, ping PC3. This ping should fail.

Step 2: Use traceroute to discover where connectivity is failing.

From the command prompt on PC1, use the **tracert** command to find where the connection is failing.

```
Packet Tracer PC Command Line 1.0
PC>tracert 192.168.30.10
```

Use the key combination Ctrl-C to break out of the **tracert** command. What is the last router that responds to the **tracert**? _____ On the first pass, R1.

Step 3: Document the symptoms of the problem.

_____

_____

PC1 does not have access past its own default gateway.

Task 2: Gather Data on the Problem

Step 1: Access the last router that responded to the traceroute packet.

Telnet to the last router that responded to the **tracert**. Use **cisco** and **class** as the telnet and enable passwords, respectively.

Step 2: Use troubleshooting commands to investigate the reason this router may not be forwarding the trace to the next hop.

Use the following commands to isolate specific problems with the serial interface:

- **show ip interface brief**
- **show interface serial**
- **show controllers serial**

The **show ip interface brief** command indicates if an interface has been configured properly and whether it has been properly brought online with the **no shutdown** command.

The **show interface serial** command provides more information on the interface that is failing. It returns one of five possible states:

- 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 **show interface serial** command also shows which encapsulation is being used on the interface. For this activity, all routers should be using HDLC encapsulation.

The **show controllers serial** command indicates the state of the interface channels and whether a cable is attached to the interface.

You may also need to check the configuration on the connected router to detect the problem.

Step 3: Document the problem and suggest solutions.

What are some possible reasons for a serial link failing?

_____

_____

_____

On R1, the student should notice that the S0/0/0 is “up” and “down.” Attempting to bring it up with the no shutdown command has no effect because the interface is already physically “up.” Upon further investigation, the student sees that the encapsulation is set to PPP. The solution is to change it to HDLC with either the no encap ppp or encap hdlc command.

On R2, the student should notice that the s0/0/1 is “down” and “down.” Issuing the no shutdown command on the interface has no effect. The show interface se 0/0/1 command does not shed any light, but the show controllers se 0/0/1 command shows that a DCE cable is attached, but there is no clock set on the interface. The solution is to set the clock rate to 64000 bps.

On R3, the student should notice that the se0/0/1 is “administratively down” and “down.” The student should immediately know that the problem is likely a missing no shutdown command on the interface.

Task 3: Implement the Solution and Test Connectivity

Step 1: Make changes according to the suggested solutions in Task 2.

Step 2: Use ping to test end-to-end connectivity.

From the command line of the router or PC1, use the **ping** and **tracert** commands to test connectivity to PC3.

If the pings fail, return to Task 2 to continue troubleshooting. At some point, you may need to start your troubleshooting from PC3.

Step 3. Check results.

Click **Check Results**, **and** then **click** the **Connectivity Tests** tab. The Connectivity Test should now be successful.

Step 4. Summarize your findings.

Problem 1: _____

Solution 1: _____

Problem 2: _____

Solution 2: _____

Problem 3: _____

Solution 3: _____

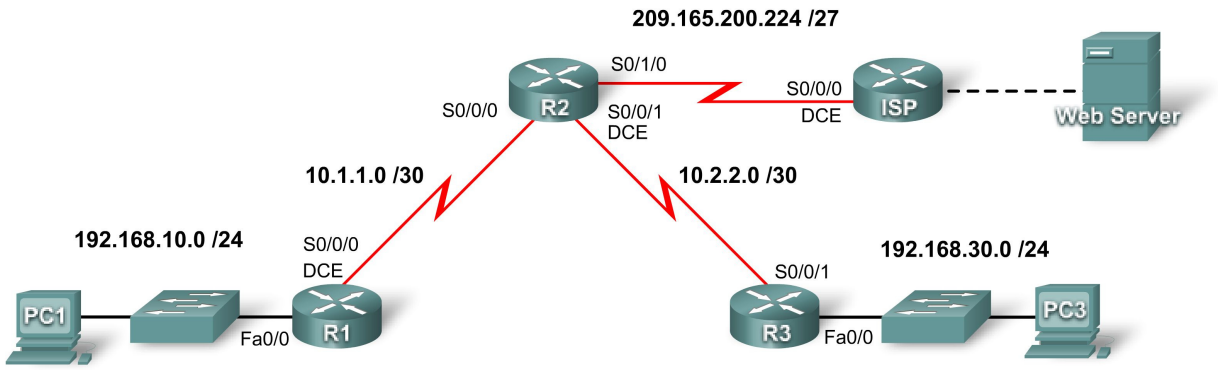
Problem 1: mismatched encapsulation on R1 serial 0/0/0 Solution: `encapsulation hdlc` on s0/0/0

Problem 2: clock rate missing on R2 serial 0/0/1 Solution: `clock rate 64000` on s0/0/1

Problem 3: R3 serial 0/0/1 shutdown Solution: `no shutdown` on s0/0/1

PT Activity 2.3.4: Configuring Point-to-Point Encapsulations (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/0	192.168.10.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
R2	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
R3	Fa0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
ISP	S0/0/0	209.165.200.226	255.255.255.252	N/A
	Fa0/0	209.165.200.1	255.255.255.252	N/A
Web Server	NIC	209.165.200.2	255.255.255.252	209.165.200.1
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

- Review routing configurations
- Configure PPP as the Encapsulation method
- Configure HDLC as the Encapsulation method

Task 1: Review Routing Configurations.

Step 1. View running configurations on all routers.

Note the routing configurations, both static and dynamic. You will be configuring both types of routing in the Packet Tracer Skills Integration Challenge Activity at the end of the chapter.

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

1. Open a command line from PC1.
2. Issue the command **ping 209.165.200.2**
3. Repeat with PC3.

Both **ping** commands should be successful. Remember to give enough time for STP and OSPF to converge.

Task 2: Configure PPP as the Encapsulation Method.

Step 1. Configure R1 to use PPP encapsulation with R2.

```
R1(config)#interface serial0/0/0
R1(config-if)#encapsulation ppp
```

Step 2. Configure R2 to use PPP encapsulation with R1 and R3.

Step 3. Configure R3 to use PPP encapsulation with R2.

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

Why does OSPF need to converge after the encapsulation change?

_____

_____

_____

When the encapsulation method on one side of the link changed, the link went down. After the dead interval, the router is marked as down and the router that stopped receiving the “Hellos” then floods the topology update to its neighbors. Routes are flushed from routing tables. So when connectivity is re-established with PPP, the routers must create new adjacencies and then send link-state updates.

Step 5. Check results.

Your completion percentage should be 67%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure HDLC as the Encapsulation Method.

Step 1. Configure ISP to use HDLC encapsulation with R2.

```
ISP(config)#interface serial0/0/0
ISP(config-if)#encapsulation hdlc
ISP(config-if)#no shutdown
```

Step 2. Configure R2 to use HDLC encapsulation with ISP.

```
R2(config)#interface serial0/1/0
R2(config-if)#encapsulation hdlc
```



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

Note: Although Check Results may show 100%, the Connectivity Tests will fail unless you configure the **no shutdown** command on R2 and ISP.

Step 3. Test connectivity between the PCs and the Web Server.

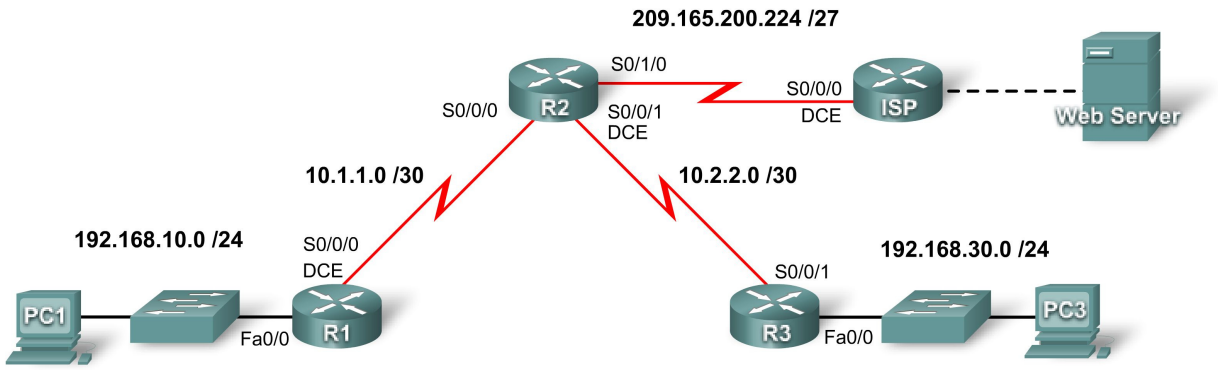
Use a Packet Tracer Simple PDU to check connectivity. It should be successful.

Step 4. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

PT Activity 2.4.6: Configuring PAP and CHAP Authentication (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.252
R3	Fa0/0	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252
ISP	S0/0/0	209.165.200.226	255.255.255.252
	Fa0/0	209.165.200.1	255.255.255.252
Web Server	NIC	209.165.200.2	255.255.255.252
PC1	NIC	192.168.10.10	255.255.255.0
PC3	NIC	192.168.30.10	255.255.255.0

Learning Objectives

- Configure OSPF routing
- Configure PAP authentication between R1 and R2
- Configure CHAP authentication between R3 and R2

Introduction

PPP encapsulation allows for two different types of authentication: PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). PAP uses a clear-text password, while CHAP invokes a one-way hash that provides more security than PAP. In this activity, you will configure both PAP and CHAP as well as review OSPF routing configuration.

Task 1: Configure OSPF Routing

Step 1: Enable OSPF on R1.

With a *process-ID* of **1**, use the **router ospf 1** command to enable OSPF routing.

Step 2: Configure network statements on R1.

In router configuration mode, add all the networks connected to R1 using the **network** command. The OSPF *area-id* parameter is **0** for all the **network** statements in this topology.

```
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
```

Step 3: Configure network statements on R2 and R3.

Repeat steps 1 and 2 for routers R2 and R3. Use the addressing table to determine the correct statements. On R2, do *not* advertise the 209.165.202.224/30 network. You will configure a default route in the next step.

Step 4: Establish and redistribute the OSPF default route.

- On R2, create a static default route to ISP with the command **ip route 0.0.0.0 0.0.0.0 s0/1/0**.
- At the router prompt, issue the **default-information originate** command to include the static route in OSPF updates sent from R2.

Step 5: Verify end-to-end connectivity.

At this point in your configuration, all devices should be able to ping all locations.

Click **Check Results**, and then click **Connectivity Tests**. The Status should be “Correct” for both tests**.** The routing tables for R1, R2, and R3 should be complete. R1 and R3 should have a default route as shown in the routing table for R1 below:

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
<output omitted>

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
O       10.2.2.0 [110/128] via 10.1.1.2, 00:03:59, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/0
O    192.168.30.0/24 [110/129] via 10.1.1.2, 00:02:19, Serial0/0/0
O*E2 0.0.0.0/0 [110/1] via 10.1.1.2, 00:02:19, Serial0/0/0
```


Step 6: Check results.

Your completion percentage should be 40%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure PAP Authentication

Step 1: Configure R1 to use PAP authentication with R2.

- On R1 in global configuration mode, type the command **username R2 password cisco123**. This command enables the remote router R2 to connect to R1 when using the password **cisco123**.
- Change the encapsulation type on the s0/0/0 interface of R1 to PPP using the **encapsulation ppp** command.
- While in the serial interface, configure PAP authentication with the **ppp authentication pap** command.
- Configure the username and password that will be sent to R2 with the **ppp pap sent-username R1 password cisco123** command. Although Packet Tracer does not grade the **ppp pap sent-username R1 password cisco123** command, the command is required to successfully configure PAP authentication.
- Return to the privileged exec mode and use the **show ip interface brief** command to observe that the link between R1 and R2 has gone down.

```
R1(config)#username R2 password cisco123
R1(config)#interface s0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R1 password cisco123
R1(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.10.1    YES manual up                    up
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/0/0            10.1.1.1        YES manual up                    down
Serial0/0/1            unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

Step 2: Configure R2 to use PAP authentication with R1.

Repeat Step 1 for R2, using the serial link to R1.

Remember, the name used in the command **username** *name* **password** *password* is always the name of the remote router, but in the **ppp pap sent-username** *name* **password** *password* command, the name is that of the originating router.

Note: Although Packet Tracer will bring the link up, on real equipment it is necessary to **shutdown** and then **no shutdown** the interface to force PAP to reauthenticate. You could also simply reload the routers.

Step 3: Test connectivity between the PC1 and the web server.

Use the **show ip interface brief** command to observe that the link between R1 and R2 is now up. Access to the web server from R1 should now be restored. Test this by sending a ping from PC1 to the web server.

```
R2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES manual administratively down down
FastEthernet0/1        unassigned      YES manual administratively down down
```



```
Serial0/0/0            10.1.1.2         YES manual up                    up
Serial0/0/1            10.2.2.1         YES manual up                    up
Serial0/1/0            209.165.200.225  YES manual up                    up
Serial0/1/1            unassigned       YES manual administratively down down
Vlan1                  unassigned       YES manual administratively down down
```

Step 4: Check results.

Your completion percentage should be 70%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure CHAP Authentication

Step 1: Configure R3 to use CHAP authentication with R2.

- In global configuration mode for R3, type **username R2 password cisco123**.
- On the s0/0/1 interface, issue the **encapsulation ppp** and **ppp authentication chap** commands, enabling PPP encapsulation and CHAP authentication.
- Use the **show ip interface brief** command to observe that the link between R2 and R3 has gone down.

```
R3(config)#username R2 password cisco123
R3(config)#interface s0/0/1
R3(config-if)#encapsulation ppp
R3(config-if)#ppp authentication chap
```

Step 2: Configure R2 to use CHAP authentication with R3.

Repeat Step 1 for R2, but change the username to R3**,** because R3 is the remote router.

Step 3: Test connectivity between PC3 and the web server.

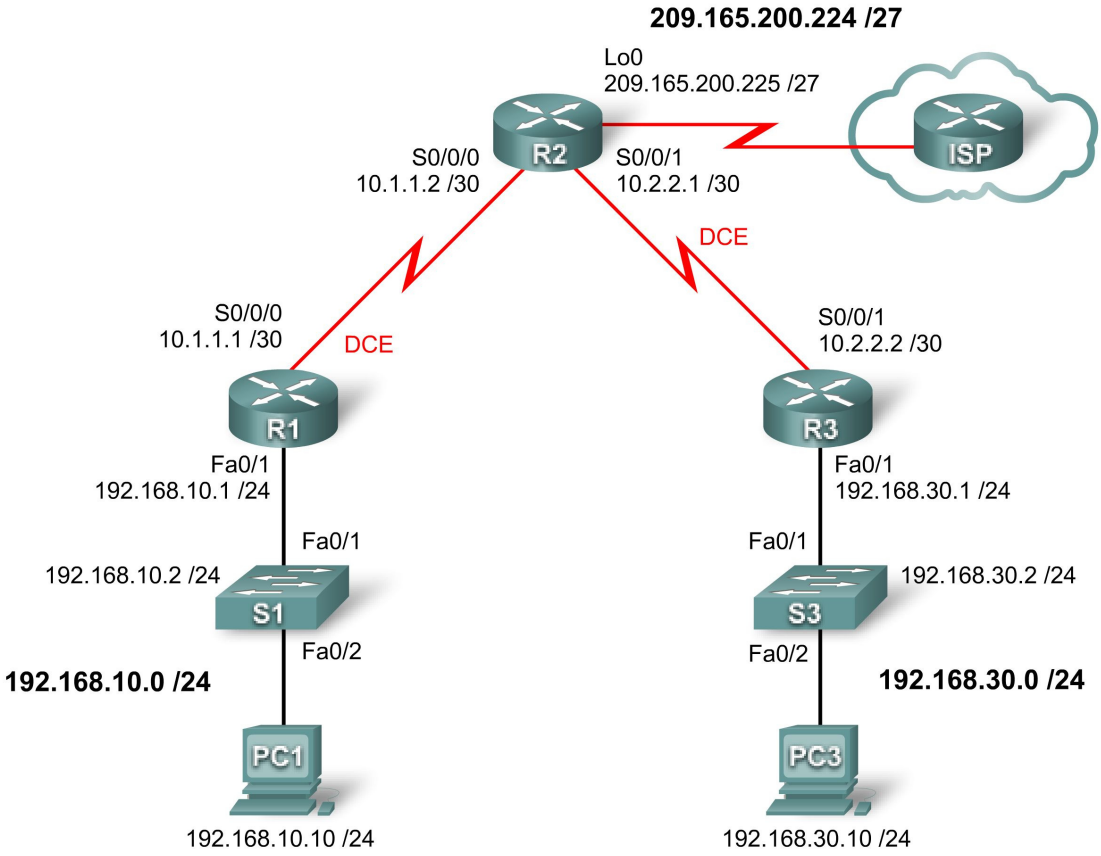
Using the **show ip interface brief** command, you should see that the link between R2 and R3 is now up, and PC3 can ping the web server.

Step 4: Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Activity 2.5.1: Basic PPP Configuration (Instructor Version)

Topology Diagram



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

- Configure OSPF routing on all routers
- Configure PPP encapsulation on all serial interfaces
- Intentionally break and restore PPP encapsulation
- Configure PPP PAP and CHAP authentication
- Intentionally break and restore PPP PAP and CHAP authentication

Introduction

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. Finally, you will configure PPP PAP authentication and PPP CHAP authentication.

Task 1: Configure OSPF on the Routers

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

Issue the **router ospf** command with a process ID of 1 to enter the router configuration prompt. For each router, advertise all the attached 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
R1(config-router)#

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
R2(config-router)#

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
R3(config-router)#
```

Step 2. Verify that you have full network connectivity.

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

```
R1#show ip route

<output omitted>

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
O       10.2.2.0 [110/128] via 10.1.1.2, 00:02:22, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/1
O    192.168.30.0/24 [110/129] via 10.1.1.2, 00:00:08, Serial0/0/0
     209.165.200.0/32 is subnetted, 1 subnets
O       209.165.200.225 [110/65] via 10.1.1.2, 00:02:22, Serial0/0/0

R1#ping 192.168.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
```



```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
R1#

R2#show ip route

<output omitted>

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
C       10.2.2.0 is directly connected, Serial0/0/1
O    192.168.10.0/24 [110/65] via 10.1.1.1, 00:02:31, Serial0/0/0
O    192.168.30.0/24 [110/65] via 10.2.2.2, 00:00:20, Serial0/0/1
     209.165.200.0/27 is subnetted, 1 subnets
C       209.165.200.224 is directly connected, Loopback0

R2#ping 192.168.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
R2#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
R2#

R3#show ip route

<output omitted>

     10.0.0.0/30 is subnetted, 2 subnets
O       10.1.1.0 [110/128] via 10.2.2.1, 00:00:34, Serial0/0/1
C       10.2.2.0 is directly connected, Serial0/0/1
O    192.168.10.0/24 [110/129] via 10.2.2.1, 00:00:34, Serial0/0/1
C    192.168.30.0/24 is directly connected, FastEthernet0/1
     209.165.200.0/32 is subnetted, 1 subnets
O       209.165.200.225 [110/65] via 10.2.2.1, 00:00:34, Serial0/0/1

R3#ping 209.165.200.225

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
R3#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
R3#
```


Task 2: Configure PPP Encapsulation on Serial Interfaces

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

The default serial encapsulation on Cisco routers is HDLC. Use the **show interface** command on any of the serial interfaces to view the current encapsulation.

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set

<output omitted>
```

If you check all the active serial interfaces, the encapsulation will be set to HDLC.

Step 2. 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.

```
R1(config)#interface serial 0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#
*Aug 17 19:02:53.412: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from F
ULL to DOWN, Neighbor Down: Interface down or detached
R1(config-if)#

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

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

Step 3. 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
R2(config-if)#
*Aug 17 20:02:08.080: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL
 to DOWN, Neighbor Down: Interface down or detached
*Aug 17 20:02:13.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to down
*Aug 17 20:02:58.564: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
*Aug 17 20:03:03.644: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOAD
ING to FULL, Loading Done
*Aug 17 20:03:46.988: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
```



```
 state to down
R3(config)#interface serial 0/0/1
R3(config-if)#encapsulation ppp
R3(config-if)#
*Aug 17 20:04:27.152: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
*Aug 17 20:04:30.952: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from L
OADING to FULL, Loading Done
```

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

Step 4. Verify that PPP is now the encapsulation on the serial interfaces.

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<output omitted>

R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<output omitted>

R2#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.2.2.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<output omitted>
R3#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.2.2.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<output omitted>
```


Task 3: Break and Restore PPP Encapsulation

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
R2(config-if)#
*Aug 17 20:36:48.432: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from FULL
 to DOWN, Neighbor Down: Interface down or detached
*Aug 17 20:36:49.432: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to down
R2(config-if)#
*Aug 17 20:36:51.432: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to up
R2(config-if)#interface serial 0/0/1
*Aug 17 20:37:14.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to down
R2(config-if)#encapsulation hdlc
R2(config-if)#
*Aug 17 20:37:17.368: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL
 to DOWN, Neighbor Down: Interface down or detached
*Aug 17 20:37:18.368: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to down
*Aug 17 20:37:20.368: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
*Aug 17 20:37:44.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to down
```

Why is it useful to intentionally break a configuration?

_____

_____

By seeing the ways in which you can intentionally break a protocol it will help you see the ways in which you could unintentionally break a protocol. You will find this very helpful when you have to solve the problems in the Troubleshooting lab.

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

_____

_____

The interfaces initially go down because they have mismatched encapsulation types. The interfaces then come back up so that they can seek to reestablish a connection. When the interfaces are unable to successfully re-establish a connection, they 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.)

_____

```
R2(config)#interface serial 0/0/0
R2(config-if)#no encapsulation ppp
R2(config-if)#interface serial 0/0/1
R2(config-if)#no encapsulation ppp
```

Step 2. Return both serial interfaces on R2 to PPP encapsulation.

```
R2(config)#interface s0/0/0
R2(config-if)#encapsulation ppp
*Aug 17 20:53:06.612: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to up
R2(config-if)#interface s0/0/1
*Aug 17 20:53:10.856: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOAD
ING to FULL, Loading Done
R2(config-if)#encapsulation ppp
*Aug 17 20:53:23.332: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
*Aug 17 20:53:24.916: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOAD
ING to FULL, Loading Done
R2(config-if)#
```

Task 4: 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)#
*Aug 22 18:58:57.367: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to down
*Aug 22 18:58:58.423: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from F
ULL to DOWN, Neighbor Down: Interface down or detached
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?

The line protocol on interface serial 0/0/0 goes down, and the OSPF adjacency goes into a DOWN state.

```
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
```

```
R2(config-if)#
*Aug 23 16:30:33.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
 state to up
*Aug 23 16:30:40.815: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOAD
ING to FULL, Loading Done
```

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

_____

The line protocol on interface serial 0/0/0 comes up, and the OSPF adjacency is established.

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
R2(config-if)#
*Aug 23 18:06:00.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to down
R2(config-if)#
*Aug 23 18:06:01.947: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL
 to DOWN, Neighbor Down: Interface down or detached
R2(config-if)#
R3(config)#username R2 password cisco
*Aug 23 18:07:13.074: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
R3(config)#int s0/0/1
R3(config-if)#
*Aug 23 18:07:22.174: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from L
OADING to FULL, Loading Done
R3(config-if)#ppp authentication chap
R3(config-if)#
```

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?

_____

_____

CHAP is able to do either one-way or two-way authentication. Therefore, as soon as the correct username and password are configured, the link comes up.

Task 5: 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#
*Aug 24 15:45:47.039: %SYS-5-CONFIG_I: Configured from console by console
R2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R2#reload
```

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

Yes. Verify that the protocol is down using the show ip interface brief command. If you do not reload the router, the line protocol stays up.

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
R2(config-if)#
*Aug 24 15:50:00.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
 state to up
R2(config-if)#
*Aug 24 15:50:07.467: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOAD
ING to FULL, Loading Done
R2(config-if)#
```

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#
*Aug 24 15:54:17.215: %SYS-5-CONFIG_I: Configured from console by console
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?

Down. Verify using the show ip interface brief command.

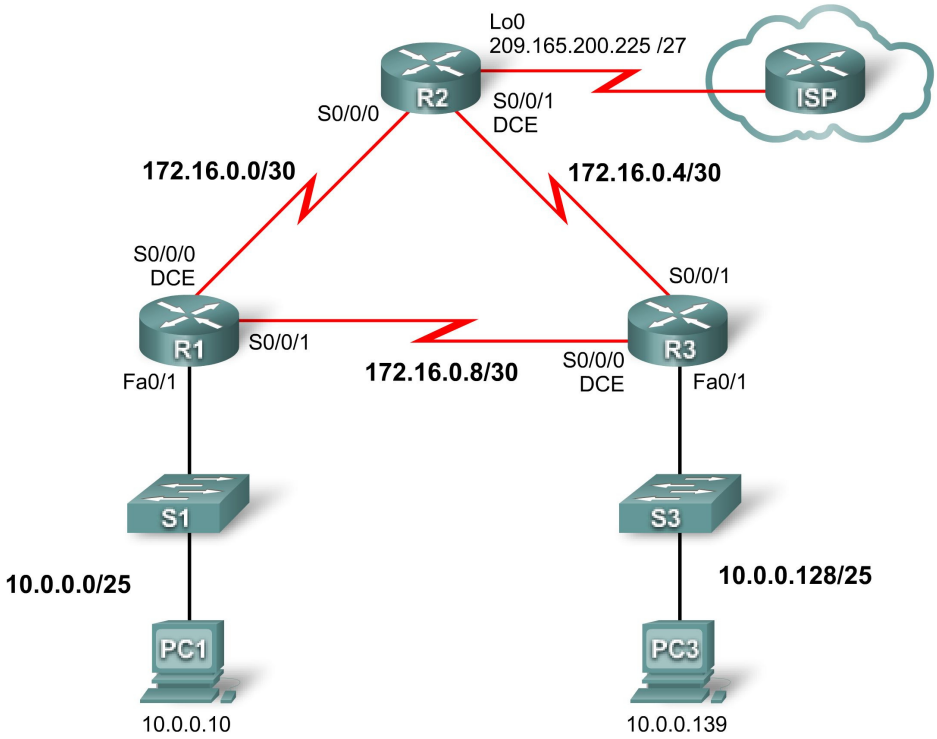
Step 4. Restore PPP CHAP authentication by changing the password on R3.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username R2 password cisco
R3(config)#
*Aug 24 16:11:10.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R3(config)#
*Aug 24 16:11:19.739: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
R3(config)#
```

Note that the link has come back up. Test connectivity by pinging from PC1 to PC3.

Activity 2.5.2: Challenge PPP Configuration (Instructor Version)

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	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	Lo0	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	Fa0/1	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
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

Learning Objectives

- Configure and activate interfaces
- Configure OSPF routing on all routers
- Configure PPP encapsulation on all serial interfaces
- Configure PPP CHAP authentication

Introduction

In this activity, you will configure PPP encapsulation on serial links using the network shown in the topology diagram. You will also configure PPP CHAP authentication. If you need assistance, refer back to the Basic PPP Configuration lab or activity, but try to do as much on your own as possible.

Task 1: Configure and Activate Serial and Ethernet Addresses

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

The addressing scheme is listed on the topology and in the Addressing Table. Some interface addresses are provided, but for some interfaces only the network is provided. In the cases where you are only given the network address, you may use any valid address on the specified network in order to be graded correctly in Packet Tracer.

Configure the interfaces for R1, R2, and R3 according to the topology. On the DCE sides of the serial links, the clock rate is 64000 bits.

R1

```
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.255.255.128
 no shutdown
!

interface Serial0/0/0
 ip address 172.16.0.1 255.255.255.252
 no shutdown
 clock rate 64000
!
interface Serial0/0/1
 ip address 172.16.0.9 255.255.255.252
 no shutdown
```

R2

```
!
interface Loopback0
 ip address 209.165.200.161 255.255.255.224
!
!
interface Serial0/0/0
 ip address 172.16.0.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.5 255.255.255.252
 clock rate 64000
 no shutdown
```

R3

```
!
interface FastEthernet0/1
 ip address 10.0.0.129 255.255.255.128
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.10 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.6 255.255.255.252
 clock rate 64000
 no shutdown
```

Step 2. Verify IP addressing and interfaces.

Verify that all the interfaces are up at both the physical and data link layers. Directly connected routers should be able to ping each other.

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            unassigned      YES manual administratively down down
FastEthernet0/1            10.0.0.1        YES manual up                    up
Serial0/0/0                172.16.0.1      YES manual up                    up
Serial0/0/1                172.16.0.9      YES manual up                    up

R2#show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial0/0/0                172.16.0.2      YES manual up                    up
Serial0/0/1                172.16.0.5      YES manual up                    up
Loopback0                  209.165.200.161 YES manual up                    up

R3#show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            unassigned      YES unset  administratively down down
FastEthernet0/1            10.0.0.129      YES manual up                    up
Serial0/0/0                172.16.0.10     YES manual up                    up
Serial0/0/1                172.16.0.6      YES manual up                    up
```

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

For PC1, use any IP address between 10.0.0.2 and 10.0.0.126. For PC3, use any IP address between 10.0.0.128 and 10.0.0.254.

Step 4. Test connectivity between the PCs.

Should the PCs be able to ping each other at this point? Can they ping their default gateways?

Task 2: Configure OSPF on Routers

Step 1. Enable OSPF routing on the routers.

When configuring OSPF routing, use an area-id of 1.


```
R1
!
router ospf 1
 network 10.0.0.0 0.0.0.127 area 0
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
!
R2
!
router ospf 1
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 209.165.200.160 0.0.0.31 area 0
!
R3
!
router ospf 1
 network 10.0.0.128 0.0.0.127 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
!
```

Step 2. Verify that you have full network connectivity.

All routers should have routes to all networks and now be able to ping any device.

```
R1#show ip route

<output omitted>

     172.16.0.0/30 is subnetted, 3 subnets
C       172.16.0.8 is directly connected, Serial0/0/1
O       172.16.0.4 [110/1562] via 172.16.0.10, 00:09:11, Serial0/0/1
                   [110/1562] via 172.16.0.2, 00:09:11, Serial0/0/0
C       172.16.0.0 is directly connected, Serial0/0/0
     209.165.200.0/32 is subnetted, 1 subnets
O       209.165.200.161 [110/782] via 172.16.0.2, 00:09:11, Serial0/0/0
     10.0.0.0/25 is subnetted, 2 subnets
C       10.0.0.0 is directly connected, FastEthernet0/1
O       10.0.0.128 [110/782] via 172.16.0.10, 00:09:11, Serial0/0/1

R1#ping 209.165.200.161

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.161, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R1#ping 10.0.0.129

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R2#show ip route

<output omitted>

     172.16.0.0/30 is subnetted, 3 subnets
```

```
O       172.16.0.8 [110/1562] via 172.16.0.6, 00:12:42, Serial0/0/1
                   [110/1562] via 172.16.0.1, 00:12:42, Serial0/0/0
C       172.16.0.4 is directly connected, Serial0/0/1
C       172.16.0.0 is directly connected, Serial0/0/0
     209.165.200.0/27 is subnetted, 1 subnets
C       209.165.200.160 is directly connected, Loopback0
     10.0.0.0/25 is subnetted, 2 subnets
O       10.0.0.0 [110/782] via 172.16.0.1, 00:12:42, Serial0/0/0
O       10.0.0.128 [110/782] via 172.16.0.6, 00:12:42, Serial0/0/1

R2#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R2#ping 10.0.0.129

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms

R3#show ip route

<output omitted>

     172.16.0.0/30 is subnetted, 3 subnets
C       172.16.0.8 is directly connected, Serial0/0/0
C       172.16.0.4 is directly connected, Serial0/0/1
O       172.16.0.0 [110/1562] via 172.16.0.9, 00:14:14, Serial0/0/0
                   [110/1562] via 172.16.0.5, 00:14:14, Serial0/0/1
     209.165.200.0/32 is subnetted, 1 subnets
O       209.165.200.161 [110/782] via 172.16.0.5, 00:14:14, Serial0/0/1
     10.0.0.0/25 is subnetted, 2 subnets
O       10.0.0.0 [110/782] via 172.16.0.9, 00:14:14, Serial0/0/0
C       10.0.0.128 is directly connected, FastEthernet0/1

R3#ping 209.165.200.161

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.161, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R3#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
```

Task 3: Configure PPP Encapsulation on Serial Interfaces

Step 1. Configure PPP on the serial interfaces of all three routers.

Currently encapsulation is set to HDLC on all the serial links. In order to configure authentication later, encapsulation must be set to PPP.

R1

```
interface Serial0/0/0
 encapsulation ppp
!
interface Serial0/0/1
 encapsulation ppp
```

R2

```
interface Serial0/0/0
 encapsulation ppp
!
interface Serial0/0/1
 encapsulation ppp
```

R3

```
interface Serial0/0/0
 encapsulation ppp
!
interface Serial0/0/1
 encapsulation ppp
```

Step 2. Verify that all serial interfaces are using PPP encapsulation.

If connected serial interfaces have mismatched encapsulation, the link will go down. Make sure all interfaces are set to PPP encapsulation.

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

R1#show interface serial0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.9/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

R2

```
R2#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

```
R2#show interface serial0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.5/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

R3

```
R3#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.10/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

R3#show interface serial0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.6/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

Task 4: Configure PPP CHAP Authentication

The password for CHAP authentication is cisco.

Step 1. Configure PPP CHAP authentication on all serial links.

R1

```
username R2 password cisco
username R3 password cisco
interface serial0/0/0
 ppp authentication chap
interface serial0/0/1
 ppp authentication chap
```

R2

```
username R1 password cisco
username R3 password cisco
interface serial0/0/0
 ppp authentication chap
interface serial0/0/1
 ppp authentication chap
```

R3

```
username R1 password cisco
username R2 password cisco
```



```
interface serial0/0/0
 ppp authentication chap
interface serial0/0/1
 ppp authentication chap
```

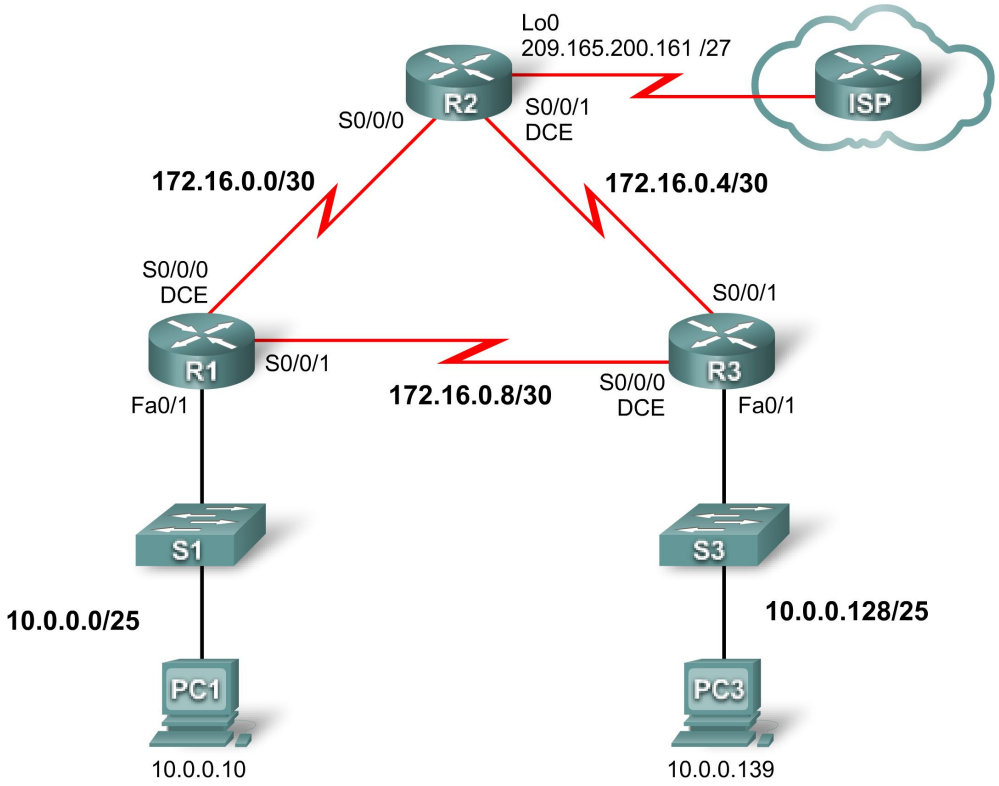
Step 2. Verify PPP CHAP authentication on all serial links.

Can all routers communicate with one another? Can the PC1 ping PC3?

The answer to both these questions should be yes.

Activity 2.5.3: Troubleshooting PPP Configuration (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Fa0/1	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	Lo0	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	Fa0/1	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
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

Learning Objectives

- Find and correct network errors
- Document the corrected network

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.

Task 1: Find and Correct Network Errors

- Use **64000** for all clock rates.
- Use **cisco** for all CHAP passwords.

Task 2: Document the Corrected Network

[Instructor Note: The following scripts show the correct configuration for each of the three routers.}
R1

```
R1#show run

!<output omitted>
!
hostname R1
!
!
enable secret cisco
!
!
no ip domain lookup
!
username R3 password 0 cisco
username R2 password 0 cisco
!
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.255.255.128
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.1 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.9 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
!
```

```
router ospf 1
 network 10.0.0.0 0.0.0.127 area 0
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
!
!
banner motd ^CCUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

R2

```
R2#show run

!<output omitted>
!
hostname R2
!
!
enable secret cisco
!
!
no ip domain lookup
!
username R1 password 0 cisco
username R3 password 0 cisco
!
!
!
interface Loopback0
 ip address 209.165.200.161 255.255.255.224
!
!
interface Serial0/0/0
 ip address 172.16.0.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.5 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
 no shutdown
!
```

```
!
router ospf 1
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 209.165.200.160 0.0.0.31 area 0
!
!
banner motd ^CCUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

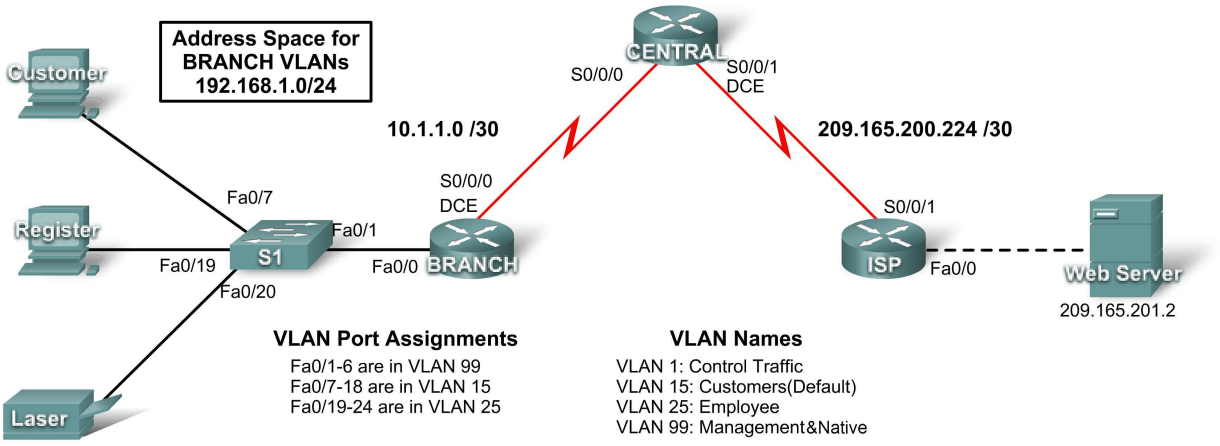
R3

```
R3#show run
!<output omitted>
!
hostname R3
!
!
enable secret cisco
!
!
no ip domain lookup
!
username R1 password 0 cisco
username R2 password 0 cisco
!
!
interface FastEthernet0/1
 ip address 10.0.0.129 255.255.255.128
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.10 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.6 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
router ospf 1
```

```
 network 10.0.0.128 0.0.0.127 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
!
!
banner motd ^CCUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

PT Activity 2.6.1: Packet Tracer Skills Integration Challenge (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
CENTRAL	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	209.165.200.226	255.255.255.252	N/A
ISP	S0/0/1	209.165.200.225	255.255.255.252	N/A
	Fa0/0	209.165.201.1	255.255.255.252	N/A
BRANCH	Fa0/0.1	192.168.1.193	255.255.255.224	N/A
	Fa0/0.15	192.168.1.1	255.255.255.128	N/A
	Fa0/0.25	192.168.1.129	255.255.255.192	N/A
	Fa0/0.99	192.168.1.225	255.255.255.224	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
S1	VLAN99	192.168.1.226	255.255.255.224	192.168.1.225
Customer	NIC	192.168.1.2	225.255.255.128	192.168.1.1
Register	NIC	192.168.1.130	225.255.255.192	192.168.1.129
Laser	NIC	192.168.1.190	225.255.255.192	192.168.1.129
Web Server	NIC	209.165.201.2	255.255.255.252	209.165.201.1

Learning Objectives

- Configure static and default routing
- Add and connect a router
- Design and document an addressing scheme
- Add and connect devices in an address space
- Configure basic device settings
- Configure PPP encapsulation with CHAP
- Configure OSPF routing
- Configure VLANs
- Verify connectivity

Task 1: Configure Static and Default Routing

Step 1. Configure static routing from ISP to CENTRAL.

Use the passwords **cisco** and **class** to access EXEC modes of the CLI for routers. Configure two static routes on ISP using the exit interface argument to the following networks:

- 10.1.1.0/30
- 192.168.1.0/24

Step 2. Configure default routing from CENTRAL to ISP.

Configure a default route on CENTRAL using the exit interface argument to send all default traffic to ISP.

Step 3. Test connectivity to Web Server.

CENTRAL should be able to successfully ping Web Server at 209.165.201.2

Step 4. Check results.

Your completion percentage should be 4%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Add and Connect a Router

Step 1. Add the BRANCH router.

Click Custom Made Devices and add an 1841 router to the topology. Use the Config tab to change the Display Name to BRANCH. Display names are case-sensitive. Do not change the hostname yet.

Step 2. Connect BRANCH to CENTRAL.

Choose the correct cable and connect BRANCH to CENTRAL according to the interfaces shown in the topology.

Step 3. Check results.

Your completion percentage should be 9%. If not, click **Check Results** to see which required components are not yet completed. If you changed the hostname in Step 2, then your percentage will be higher.

Task 3: Design and Document an Addressing Scheme

Step 1. Design an addressing scheme.

Using the topology and the following requirements, design an addressing scheme:

- Addressing is provided for all WAN links.
- For the VLANs attached to BRANCH, use the address space 192.168.1.0/24. Starting with the largest host requirement, assign subnets in the following order for all VLANs.
  - VLAN 15 needs space for 100 hosts _____ 192.168.1.0/25
  - VLAN 25 needs space for 50 hosts _____ 192.168.1.128/26
  - VLAN 1 needs space for 20 hosts _____ 192.168.1.192/27
  - VLAN 99 needs space for 20 hosts _____ 192.168.1.224/27

Step 2. Document the addressing scheme.

- Complete the addressing table using the following guidelines. You will add the remaining devices in the next task.
  - Assign the first address in each VLAN to the corresponding BRANCH subinterface. The subinterface numbers match the VLAN numbers.
  - Assign the second address in VLAN 99 to S1.
  - Assign the second address in VLAN 15 to the Customer PC.
  - Assign the second address in VLAN 25 to the Register PC.
  - Assign the last address in VLAN 25 to the laser printer.
- Be sure you record the appropriate subnet mask and default gateway for each address.

Task 4: Add and Connect the Devices in the Address Space

Step 1. Add S1, Customer PC, Register PC, and the laser printer in the 192.168.1.0/24 address space.

- S1 is a 2960 switch. Add it to the topology and change the display name to S1. Display names are case-sensitive. Do not change the hostname yet.
- The PCs and printer are listed under End Devices. Add two PCs and a printer. Change the display names of the PCs and printer according to the topology.

Step 2. Connect S1 to BRANCH.

Choose the correct cable and connect S1 to BRANCH according to the interfaces shown in the topology.

Step 3. Connect Customer PC, Register PC, and the laser printer to S1.

Choose the correct cable and connect the PCs and printer to S1 according to the interfaces shown in the topology.

Step 4. Check results.

Your completion percentage should be 22%. If not, click **Check Results** to see which required components are not yet completed. If you changed the hostname of S1 in Step 1, then your percentage will be higher.

Task 5: Configure Basic Device Settings

Step 1. Configure BRANCH and S1.

Using your documentation, set the basic configuration for BRANCH and S1, including addressing. Use **cisco** as the line password and **class** as the secret password. Use 64000 as the clock rate. Graded portions of the basic configuration include:

- Hostnames, which are case-sensitive.
- Interface addressing and activation. Set clocking to 64000 bps.
- For interface Fa0/0.99, configure VLAN 99 as the native VLAN.
- Interface VLAN 99 creation and addressing on S1. Activating VLAN 99 is done after the trunk is configured later in the activity.

Step 2. Configure remaining devices.

Using your documentation, configure the PCs and printer with the correct addressing.

Step 3. Test connectivity between BRANCH and CENTRAL.

CENTRAL should now be able to successfully ping BRANCH. S1 cannot ping until trunking is configured.

Step 4. Check results.

Your completion percentage should be 63%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Configure PPP Encapsulation with CHAP Authentication

Step 1. Configure CENTRAL to use PPP with CHAP for the link to BRANCH.

The password for CHAP authentication is **cisco123.** The link goes down.

Step 2. Configure BRANCH to use PPP with CHAP for the link to CENTRAL.

The password for CHAP authentication is **cisco123.** The link comes back up.

Step 3. Test Connectivity between BRANCH and CENTRAL.

It may take Packet Tracer a little longer than real equipment to bring the interfaces back up. Once the interfaces come up, CENTRAL should be able to successfully ping BRANCH.

Step 4. Check results.

Your completion percentage should be 71%. If not, click **Check Results** to see which required components are not yet completed.

Task 7: Configure OSPF Routing

Step 1. Configure OSPF on CENTRAL.

- Configure OSPF using the process ID 1.
- Add only the network shared with BRANCH.
- Propagate the default route to OSPF neighbors.
- Disable OSPF updates to ISP.

Step 2. Configure OSPF on BRANCH.

- Configure OSPF using the process ID 1.
- Add all active networks that BRANCH routes.
- Disable OSPF updates to the VLANs.

Step 3. Test connectivity to Web Server.

BRANCH should now be able to successfully ping Web Server at 209.165.201.2.

Step 4. Check results.

Your completion percentage should be 86%. If not, click **Check Results** to see which required components are not yet completed.

Task 8: Configure VLANs

Step 1. Add VLANs to S1.

VLAN names are case-sensitive. Add and name the four VLANs using the following specifications:

- VLAN 15; name is **Customers(Default)**
- VLAN 25; name is **Employee**
- VLAN 99; name is **Management&Native**

Step 2. Assign ports to the appropriate VLANs and activate interface VLAN 99.

- Using the VLAN Port Assignments shown in the topology diagram, configure the access ports attached to the end devices and assign each to the correct VLAN.
- Enable trunking on the Fa0/1 port and configure it to use VLAN 99 as the native VLAN.
- Activate interface VLAN 99, if necessary. It should already be up.

Step 3. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

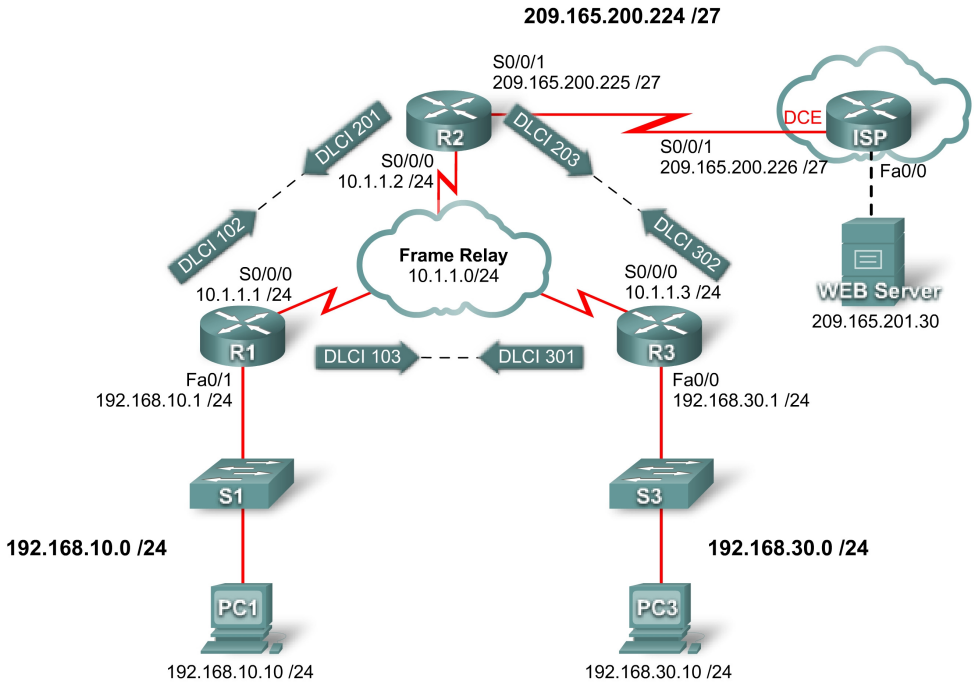
Task 9: Verify connectivity

Step 1. Verify that Customer PC, Register PC, and the laser printer can ping each other.

Step 2. Verify that Customer PC, Register PC, and laser printer can ping Web Server.

PT Activity 3.2.2: Configuring Basic Frame Relay with Static Maps (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	192.168.10.1	255.255.255.0
	S0/0/1	10.10.10.1	255.255.255.0
R2	S0/0/0	10.10.10.2	255.255.255.0
	S0/0/1	209.165.200.225	255.255.255.224
R3	Fa0/0	192.168.30.1	255.255.255.0
	S0/0/0	10.10.10.3	255.255.255.0
ISP	S0/0/1	209.165.200.226	255.255.255.224

Learning Objectives

- Configure Frame Relay
- Configure static Frame Relay maps
- Configure the Frame Relay LMI type

Introduction

In this activity, you will configure Frame Relay on the serial 0/0/0 interfaces of routers R1, R2, and R3. You will also configure two static Frame Relay maps on each router to reach the other two routers. Although the LMI type is autosensed on the routers, you will statically assign the type by manually configuring the LMI.

Routers R1, R2, and R3 have been preconfigured with hostnames and IP addresses on all interfaces. The Fast Ethernet interfaces on routers R1 and R3 are active, and the S0/0/1 interface of R2 is active.

Task 1: Configure Frame Relay

Step 1. Configure Frame Relay encapsulation on the serial 0/0/0 interface of R1.

```
R1(config)#interface serial0/0/0
R1(config-if)#encapsulation frame-relay
R1(config-if)#no shutdown
```

Step 2. Configure Frame Relay encapsulation on the serial 0/0/0 interfaces of R2 and R3.

Step 3. Test connectivity.

From the command line on PC1, verify connectivity to the PC3 host, located at 192.168.30.10, using the **ping** command.

The ping from PC1 to PC3 should fail since the R1 router does not know where the 192.168.30.0 network is. R1 must be configured with a Frame Relay map so that it can find the next hop destination to reach that network.

Step 4. Check results.

Your completion percentage should be 40%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure Static Frame Relay Maps

Note: Packet Tracer does not grade your map statements. However, you must still configure the commands.

Step 1. Configure static maps on R1, R2, and R3.

Each router requires two static maps to reach the other routers. The DLCIs to reach these routers are as follows:

Router R1:

- To reach router R2, use DLCI 102 located at IP address 10.10.10.2.
- To reach router R3, use DLCI 103 located at IP address 10.10.10.3.

Router R2:

- To reach router R1, use DLCI 201 located at IP address 10.10.10.1.
- To reach router R3, use DLCI 203 located at IP address 10.10.10.3.

Router R3:

- To reach router R1, use DLCI 301 located at IP address 10.10.10.1.
- To reach router R3, use DLCI 302 located at IP address 10.10.10.2.

The routers must also support RIP; therefore the **broadcast** keyword is required.

On router R1, configure the static Frame Relay maps as follows:

```
R1(config-if)#frame-relay map ip 10.10.10.2 102 broadcast
R1(config-if)#frame-relay map ip 10.10.10.3 103 broadcast
```

Configure routers R2 and R3 using the previously provided information.

Step 2. Check results.

Your completion percentage should be 80%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure the Frame Relay LMI Type

The Frame Relay cloud contains switches that are using ANSI as the LMI type. Therefore, all the Frame Relay links must be manually configured to use ANSI.

Step 1. Configure ANSI as the LMI type on R1, R2, and R3.

Enter the following command on the serial interface for each router.

```
R1(config-if)#interface s0/0/0
R1(config-if)#frame-relay lmi-type ansi
```

Step 2. Check results.

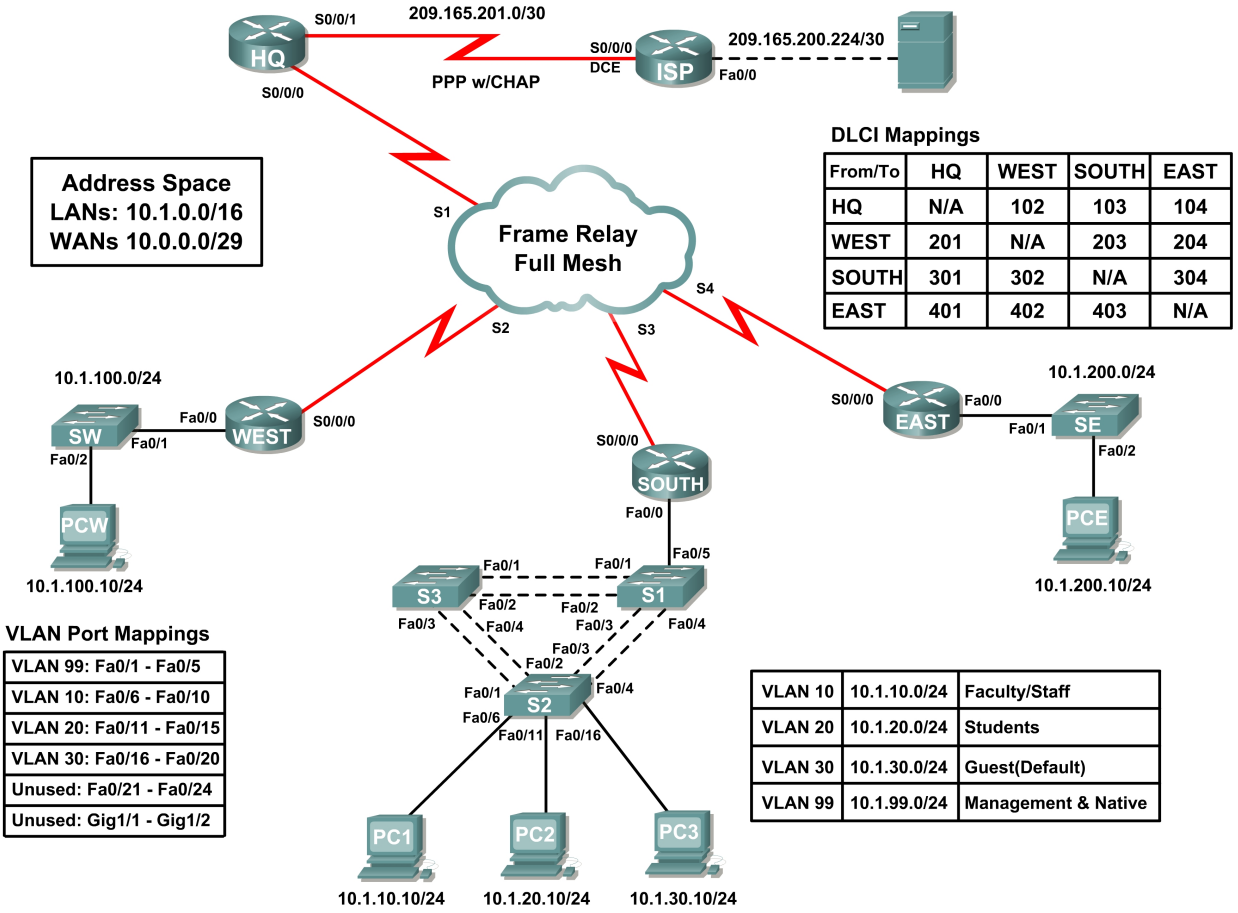
Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Step 3. Test connectivity.

It is possible to complete the activity with a 100%, yet still not have connectivity. PC1 and PC3 should now be able to successfully ping each other and the web server. If not, make sure that you entered all the commands exactly as specified in the previous steps.

PT Activity 3.6.1: Packet Tracer Skills Integration Challenge (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
HQ	**S0/0/1**	209.165.201.2	255.255.255.252
	S0/0/0	10.0.0.1	255.255.255.248
WEST	**S0/0/0**	10.0.0.2	255.255.255.248
	Fa0/0	10.1.100.1	255.255.255.0
SOUTH	**S0/0/0**	10.0.0.3	255.255.255.248
	Fa0/0.10	10.1.10.1	255.255.255.0
	Fa0/0.20	10.1.20.1	255.255.255.0
	Fa0/0.30	10.1.30.1	255.255.255.0
	Fa0/0.99	10.1.99.1	255.255.255.0
EAST	**S0/0/0**	10.0.0.4	255.255.255.248
	Fa0/0	10.1.200.1	255.255.255.0
ISP	**S0/0/0**	209.165.201.1	255.255.255.252
	Fa0/0	209.165.200.225	255.255.255.252
Web Server	**NIC**	209.165.200.226	255.255.255.252
S1	**VLAN99**	10.1.99.11	255.255.255.0
S2	**VLAN99**	10.1.99.12	255.255.255.0
S3	**VLAN99**	10.1.99.13	255.255.255.0

Learning Objectives

- Configure PPP with CHAP
- Configure full mesh Frame Relay
- Configure static and default routing
- Configure and test inter-VLAN routing
- Configure VTP and trunking on switches
- Configure VLANs on a switch
- Configure and verify interface VLAN 99
- Configure a switch as root for all spanning trees
- Assign ports to VLANS
- Test end-to-end connectivity

Introduction

This activity allows you to practice a variety of skills, including configuring Frame Relay, PPP with CHAP, static and default routing, VTP, and VLAN. Because there are close to 150 graded components in this activity, you may not see the completion percentage increase every time you configure a graded command. You can always click **Check Results** and **Assessment Items** to see if you correctly entered a graded command.

Task 1: Configure PPP with CHAP Between Devices

Step 1. Configure and activate serial 0/0/1 on HQ.

Step 2. Configure PPP encapsulation on HQ for the link shared with ISP.

Step 3. Configure CHAP authentication on HQ.

Use **cisco** as the password.

Step 4. Verify connectivity between HQ and ISP.

The link between HQ and ISP should now be up, and you should be able to ping ISP. However, the link may take a few minutes in Packet Tracer before it comes up. To speed up the process, switch between Simulation and Realtime mode three or four times.

Step 5. Check results.

Your completion percentage should be 4%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure Full Mesh Frame Relay

The above topology diagram and the table below both show the DLCI mappings used in this full mesh Frame Relay configuration. Read the table from left to right. For example, the DLCI mappings you will configure on HQ are: 102 to WEST; 103 to SOUTH; and 104 to EAST.

DLCI Mappings				
From/To	**HQ**	**WEST**	**SOUTH**	**EAST**
HQ	N/A	102	103	104
WEST	201	N/A	203	204
SOUTH	301	302	N/A	304
EAST	401	402	403	N/A

Note: HQ, WEST, and SOUTH are all using the default Frame Relay encapsulation **cisco**. However, EAST is using the encapsulation type IETF.

Step 1. Configure and activate the serial 0/0/0 interface on HQ.

Configure the interface with the following information:

- IP address
- Frame Relay encapsulation
- Mappings to WEST, SOUTH, and EAST (EAST uses IETF encapsulation)
- LMI type is ANSI

Step 2. Configure and activate the serial 0/0/0 interface on WEST.

Configure the interface with the following information:

- IP address
- Frame Relay encapsulation
- Mappings to HQ, SOUTH, and EAST (EAST uses IETF encapsulation)
- LMI type is ANSI

Step 3. Configure and activate the serial 0/0/0 interface on SOUTH.

Configure the interface with the following information:

- IP address
- Frame Relay encapsulation
- Mappings to HQ, WEST, and EAST (EAST uses IETF encapsulation)
- LMI type is ANSI

Step 4. Configure and activate the Serial 0/0/0 interface on EAST.

Configure the interface with the following information:

- IP address
- Frame Relay encapsulation using IETF
- Mappings to HQ, WEST and SOUTH
- LMI type is ANSI

Note: Packet Tracer does not grade your map statements. However, you must still configure the commands. You should now have full connectivity between the Frame Relay routers.

Step 5. Verify connectivity between Frame Relay routers.

The map on HQ should look like the following. Make sure all routers have full maps.

```
Serial0/0/0 (up): ip 10.0.0.2 dlci 102, static, broadcast, CISCO, status
defined, active
Serial0/0/0 (up): ip 10.0.0.3 dlci 103, static, broadcast, CISCO, status
defined, active
Serial0/0/0 (up): ip 10.0.0.4 dlci 104, static, broadcast, IETF, status
defined, active
```

Verify that HQ, WEST, SOUTH, and EAST can now ping each other.

Step 6. Check results.

Your completion percentage should be 28%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure Static and Default Routing

No routing protocol is used in this topology. All routing is done through static and default routing.

Step 1. Configure static and default routes on HQ.

- HQ needs six static routes to the six remote LANs in the topology. Use the *next-hop-ip* argument in the static route configuration.
- HQ also needs a default route. Use the *exit-interface* argument in the default route configuration.

Step 2. Configure static and default routes on WEST.

- WEST needs five static routes to the five remote LANs in the topology. Use the *next-hop-ip* argument in the static route configuration.
- WEST also needs a default route. Use the *next-hop-ip* argument in the default route configuration.

Step 3. Configure static and default routes on SOUTH.

- SOUTH needs two static routes to the two remote LANs in the topology. Use the *next-hop-ip* argument in the static route configuration.
- SOUTH needs a default route. Use the *next-hop-ip* argument in the default route configuration.

Step 4. Configure static and default routes on EAST.

- EAST needs five static routes to the five remote LANs in the topology. Use the *next-hop-ip* argument in the static route configuration.
- EAST needs a default route. Use the *next-hop-ip* argument in the default route configuration.

Step 5. Verify connectivity from EAST and WEST LANs to the Web Server.

- All routers should now be able to ping the Web Server.
- The WEST PC (PCW) and the EAST PC (PCE) should now be able to ping each other and the Web Server.

Step 6. Check results.

Your completion percentage should be 43%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure and Test Inter-VLAN Routing

Step 1. Configure inter-VLAN routing on SOUTH.

Using the addressing table, activate Fast Ethernet 0/0 on SOUTH and configure inter-VLAN routing. The subinterface number corresponds to the VLAN number. VLAN 99 is the native VLAN.

Step 2. Test inter-VLAN routing on SOUTH.

HQ, WEST, and EAST should now be able to ping each of the subinterfaces on SOUTH.

Step 3. Check results.

Your completion percentage should be 56%. If not, click **Check Results** to see which required components are not yet completed. The routers are now fully configured.

Task 5: Configure VTP and Trunking on the Switches

Step 1. Configure VTP settings on S1, S2, and S3.

- S1 is the server. S2 and S3 are clients.
- The domain name is **CCNA.**
- The password is **cisco.**

Step 2. Configure trunking on S1, S2, and S3.

Trunking ports for S1, S2, and S3 are all ports attached to another switch or router. Set all trunking ports to trunk mode, and assign VLAN 99 as the native VLAN.

Step 3. Check results.

Your completion percentage should be 81%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Configure VLANs on the Switch

Step 1. Create and name the VLANs.

Create and name the following VLANs on S1 only:

- VLAN 10, name = **Faculty/Staff**
- VLAN 20, name = **Students**
- VLAN 30, name = **Guest(Default)**
- VLAN 99, name = **Management&Native**

Step 2. Verify VLANs were sent S2 and S3.

What command displays the following output? _____ show vtp status

```
VTP Version                     : 2
Configuration Revision          : 8
Maximum VLANs supported locally : 64
Number of existing VLANs        : 9
VTP Operating Mode              : Client
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xF5 0x50 0x30 0xB6 0x91 0x74 0x95 0xD9
Configuration last modified by 0.0.0.0 at 3-1-93 00:12:30
```

What command displays the following output? _____ show vlan brief

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig1/1, Gig1/2
10   Faculty/Staff                     active
20   Students                          active
30   Guest(Default)                    active
99   Management&Native                 active
<output omitted>
```

Step 3. Check results.

Your completion percentage should be 84%. If not, click **Check Results** to see which required components are not yet completed.

Task 7: Configure and Verify VLAN 99

Step 1. On S1, S2, and S3 complete the following steps:

- Configure and activate VLAN 99
- Configure the default gateway
- Verify that S1, S2, and S3 can now ping SOUTH at 10.1.99.1

Step 2. Check results.

Your completion percentage should be 92%. If not, click **Check Results** to see which required components are not yet completed.

Task 8: Configure S1 as Root for All Spanning Trees

Step 1. Configure S1 as the root bridge for all spanning trees, including VLANs 1, 10, 20, 30, and 99.

Notice that S3 won the root war and is currently the root bridge for all spanning trees. Set the priority to 4096 on S1 for all spanning trees.

Step 2. Verify that S1 is now the root for all spanning trees.

Only the output for VLAN 1 is shown below. However, S1 should be the root for all spanning trees. What command displays the following output?

_____ show spanning-tree vlan 1

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    4097
              Address     00D0.BC79.4B57
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    4097  (priority 4096 sys-id-ext 1)
              Address     00D0.BC79.4B57
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.3    Shr
Fa0/2            Desg FWD 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr
Fa0/5            Desg FWD 19        128.3    Shr
<output omitted>
```

Step 3. Check results.

Your completion percentage should be 96%. If not, click **Check Results** to see which required components are not yet completed.

Task 9: Assign Ports to VLANS

Step 1. Assign ports on S2 to VLANs.

Packet Tracer only grades the ports that are attached to PC1, PC2, and PC3.

- Configure the port for access mode
- Assign the port to its VLAN

The VLAN port mappings are as follows:

- VLAN 99: Fa0/1 – Fa0/5
- VLAN 10: Fa0/6 – Fa0/10
- VLAN 20: Fa0/11 – Fa0/15

- VLAN 30: Fa0/16 – Fa0/20
- Unused: Fa0/21 – Fa0/24; Gig1/1; Gig1/2

Unused ports should be shut down for security purposes.

Step 2. Verify VLAN port assignments.

What command was used to get the following output showing the VLAN assignments?

_____ show vlan brief

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig1/1, Gig1/2
10   Faculty/Staff                     active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10
20   Students                          active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15
30   Guest(Default)                    active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20
99   Management&Native                 active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Step 3. Check results.

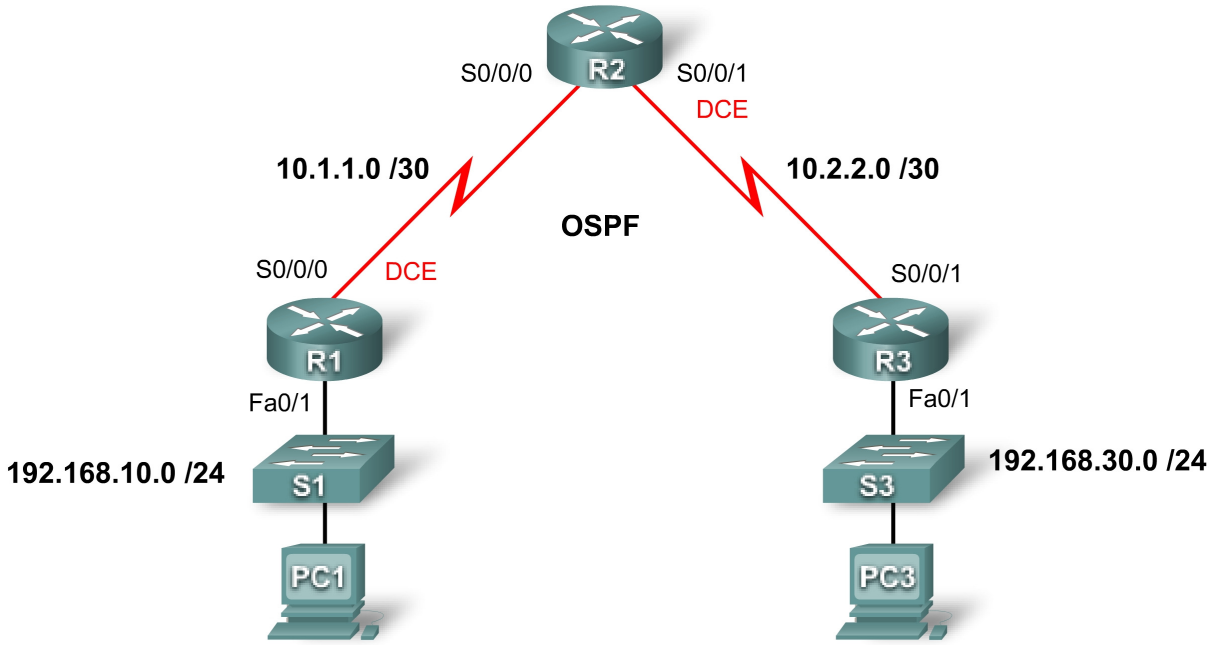
Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 10: Test End-to-End Connectivity

Although Packet Tracer may take some time to converge, pings will eventually succeed from PC1, PC2 and PC3. Test connectivity to PCW, PCE, and the Web Server. If necessary, switch between Simulation and Realtime mode to accelerate convergence.

PT Activity 4.3.2: Configuring OSPF Authentication (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	**S0/0/0**	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252
PC1	**NIC**	192.168.10.10	255.255.255.0
PC3	**NIC**	192.168.30.10	255.255.255.0

Learning Objectives

- Configure OSPF simple authentication
- Configure OSPF MD5 authentication
- Test connectivity

Introduction

This activity covers both OSPF simple authentication and OSPF MD5 (message digest 5) authentication. You can enable authentication in OSPF to exchange routing update information in a secure manner. With simple authentication, the password is sent in clear-text over the network. Simple authentication is used when devices within an area cannot support the more secure MD5 authentication. With MD5 authentication, the password does is sent over the network. MD5 is considered the most secure OSPF authentication mode. When you configure authentication, you must configure an entire area with the same type of authentication. In this activity, you will configure simple authentication between R1 and R2, and MD5 authentication between R2 and R3.

Task 1: Configure OSPF Simple Authentication

Step 1. Configure R1 with OSPF simple authentication.

To enable simple authentication on R1, enter router configuration mode using the **router ospf 1** command at the global configuration prompt. Then issue the **area 0 authentication** command to enable authentication.

```
R1(config)#router ospf 1
R1(config-router)#area 0 authentication
00:02:30: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Dead timer expired
00:02:30: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/0 from FULL to
Down: Interface down or detached
```

Eventually, you will see a console message that adjacency with R2 is down. R1 loses all OSPF routes from its routing table until it is able to authenticate routes with R2. Even though you have not yet configured a password, R1 is requiring any neighbors to use authentication in OSPF routing messages and updates.

The **area 0 authentication** command enables authentication for all the interfaces in area 0. Using only this command works for R1, because it does not have to support any other types of authentication.

To configure R1 will a simple authentication password, enter interface configuration mode for the link that connects to R2. Then issue the **ip ospf authentication-key cisco123** command. This command sets the authentication password to **cisco123**.

```
R1(config-router)#interface S0/0/0
R1(config-if)#ip ospf authentication-key cisco123
```

Step 2. Configure R2 with OSPF simple authentication.

You configured authentication on R1 for the entire area. Because R2 will support both simple and MD5 authentication, the commands are entered at the interface level.

Enter the interface configuration mode for S0/0/0. Specify that you are using simple authentication with the **ip ospf authentication** command. Then issue the **ip ospf authentication-key cisco123** command to set the authentication password to **cisco123**.

```
R2(config)#interface S0/0/0
R2(config-if)#ip ospf authentication
R2(config-if)#ip ospf authentication-key cisco123
00:07:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on Serial0/0/0 from
EXCHANGE to FULL, Exchange Done
```

When you have completed these configuration tasks, you should eventually see a console message indicating that adjacency is reestablished between R1 and R2. The OSPF routes are reinstalled into the routing table.

Step 3. Check results.

Your completion percentage should be 50%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure OSPF MD5 Authentication

Step 1. Configure R3 with OSPF MD5 authentication.

To enable MD5 authentication on R3, enter router configuration mode using the **router ospf 1** command at the global configuration prompt. Then issue the **area 0 authentication message-digest** command to enable authentication.

```
R3(config)#router ospf 1
R3(config-router)#area 0 authentication message-digest
00:10:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/1 from FULL to
DOWN, Neighbor Down: Dead timer expired
00:10:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/1 from FULL to
Down: Interface down or detached
```

Eventually, you will see a console message that adjacency with R2 is down. R3 loses all OSPF routes from its routing table until it is able to authenticate routes with R2.

To configure R3 will the MD5 authentication password, enter interface configuration mode for the link that connects to R2. Then issue the **ip ospf message-digest-key 1 md5 cisco123** command. This command sets the OSPF authentication password to **cisco123**, protected with the MD5 algorithm.

```
R3(config-router)#interface S0/0/1
R3(config-if)#ip ospf message-digest-key 1 md5 cisco123
```

Step 2. Configure R2 with OSPF MD5 authentication.

On R2, enter interface configuration mode for the link that connects to R3. Issue the **ip ospf authentication message-digest** command to enable MD5 authentication. This command is necessary on R2 because this router is using two types of authentication.

Then issue the **ip ospf message-digest-key 1 md5 cisco123** command to set up the authentication password.

```
R2(config)#interface S0/0/1
R2(config-if)#ip ospf authentication message-digest
R2(config-if)#ip ospf message-digest-key 1 md5 cisco123
00:13:51: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on Serial0/0/1 from
EXCHANGE to FULL, Exchange Done
```

After entering this command, give the routers a moment to converge. You should see a console message on both R2 and R3 indicating that neighbor adjacency is reestablished. You can confirm that R2 has reinstalled the OSPF routes and that R2 has R3 as an OSPF neighbor.

```
R2#show ip route
<output omitted>

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
C       10.2.2.0 is directly connected, Serial0/0/1
O    192.168.10.0/24 [110/65] via 10.1.1.1, 00:06:13, Serial0/0/0
O    192.168.30.0/24 [110/65] via 10.2.2.2, 00:00:07, Serial0/0/1
```



```
R2#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.10.1      1   FULL/-          00:00:32    10.1.1.1        Serial0/0/0
192.168.30.1      1   FULL/-          00:00:37    10.2.2.2        Serial0/0/1
```

Step 3. Check results.

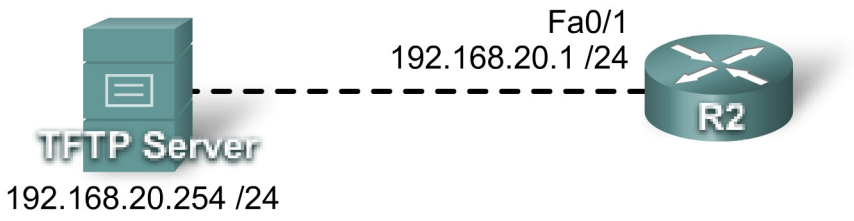
Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Test Connectivity

Authentication should now be configured correctly on all three routers, so PC1 should have no trouble pinging PC3. Click **Check Results**, and then **Connectivity Tests** to see if it is successful.

PT Activity 4.5.4: Using a TFTP Server to Upgrade a Cisco IOS Image (Instructor Version)

Topology Diagram



Learning Objectives

- Verify the current Cisco IOS image
- Configure access to the TFTP server
- Upload a new Cisco IOS image
- Configure the **boot system** command
- Test the new Cisco IOS image

Introduction

In this activity, you will configure access to a TFTP server and upload a newer, more advanced Cisco IOS image. Although Packet Tracer simulates upgrading the Cisco IOS image on a router, it does not simulate backing up a Cisco IOS image to the TFTP server. In addition, although the image you are upgrading to is more advanced, this Packet Tracer simulation will not reflect the upgrade by enabling more advanced commands. The same Packet Tracer command set will still be in effect.

Task 1: Verify the Current Cisco IOS Image

Step 1. Use the show version command to verify the image currently loaded in RAM.

```
R2#show version
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.3(14)T7,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 15-May-06 14:54 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-ipbase-mz.123-14.T7.bin"
<output omitted>
```

The image currently loaded in RAM does not support SSH or many other advanced features.

Step 2. Use the show flash command to verify any images currently available in flash.

```
R2#show flash

System flash directory:
File  Length   Name/status
  1   13832032 c1841-ipbase-mz.123-14.T7.bin
[13832032 bytes used, 18682016 available, 32514048 total]
32768K bytes of processor board System flash (Read/Write)
```

Only one Cisco IOS image is available. Before you can use SSH and additional security features, you must upgrade the image to a more advanced version.

Task 2: Configure Access to the TFTP Server

R2 needs to establish a connection to a TFTP server that has the Cisco IOS image you need.

Step 1. Connect R2 and the TFTP server.

Refer to the topology diagram for the correct interface.

Step 2. Configure R2 with an IP address.

Refer to the topology diagram for the correct IP addressing.

Step 3. Configure the TFTP server with IP addressing and a default gateway.

Refer to the topology diagram for the correct IP addressing.

Step 4. Test connectivity.

R2 should be able to successfully ping the TFTP server. If not, check your cabling and addressing.

Step 5. Check results.

Your completion percentage should be 80%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Upload a New Cisco IOS Image

Step 1. Check the TFTP server for Cisco IOS images.

Click TFTP Server and then the **Config** tab. Notice that there are several images available. You will upload the c1841-ipbasek9-mz.124-12.bin image to R2.

Step 2. Upload the c1841-ipbasek9-mz.124-12.bin image to R2.

- On R2, begin the upload process with the **copy tftp flash** command.
- Enter the IP address for TFTP Server.
- Enter the entire filename of the Cisco IOS image.

```
R2#copy tftp flash
Address or name of remote host []? 192.168.20.254
Source filename []? c1841-ipbasek9-mz.124-12.bin
Destination filename [c1841-ipbasek9-mz.124-12.bin]? Enter
Accessing tftp://192.168.20.254/c1841-ipbasek9-mz.124-12.bin...
Loading c1841-ipbasek9-mz.124-12.bin from 192.168.20.254:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```



```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!
[OK - 16599160 bytes]

16599160 bytes copied in 13.047 secs (284682 bytes/sec)
R2#
```

Step 3. Verify that the new image is now in flash.

```
R2#show flash

System flash directory:
File  Length   Name/status
  1   13832032 c1841-ipbase-mz.123-14.T7.bin
  2   16599160 c1841-ipbasek9-mz.124-12.bin
[30431192 bytes used, 2082856 available, 32514048 total]
32768K bytes of processor board System flash (Read/Write)

R2#
```

Step 4. Check results.

Your completion percentage should be 90%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure the boot system Command

By default, the router bootup sequence loads the first Cisco IOS image listed in flash. One way to make sure that the router loads the new image is to configure the **boot system flash** command. On R2, enter the following command:

```
R2(config)#boot system flash c1841-ipbasek9-mz.124-12.bin
```

This command is now part of the running configuration. However, the running configuration must also be saved to NVRAM; otherwise, the configuration is overwritten the next time you reload the router.

```
R2(config)#end
R2#copy running-config startup-config
```

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Test the New Image

Reload R2 and wait for it to reboot. When the router reloads, verify that the new image is in RAM with the **show version** command.

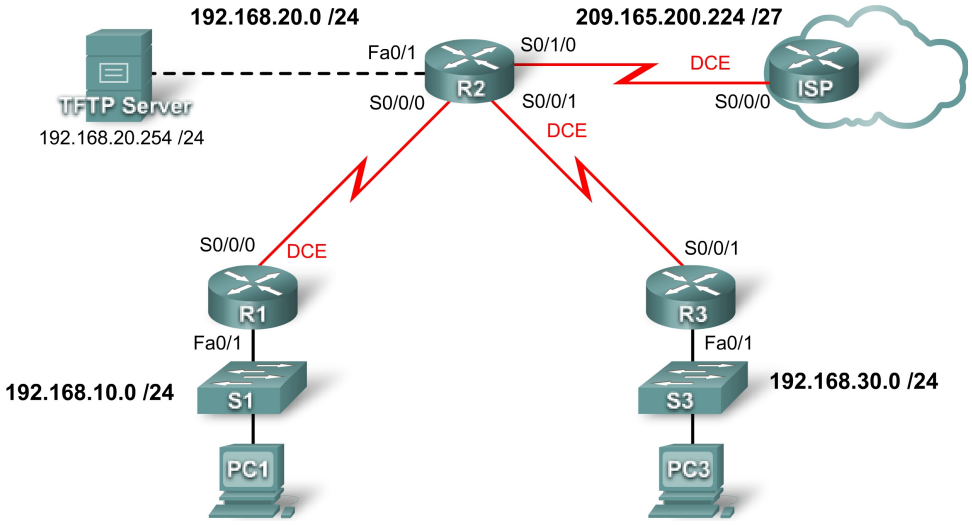
```
R2#reload
Proceed with reload? [confirm][Enter]

%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
<output omitted>

R2>show version
Cisco IOS Software, 1841 Software (C1841-IPBASEK9-M), Version 12.4(12),
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
```



```
Compiled Mon 15-May-06 14:54 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-ipbasek9-mz.124-12.bin"
<output omitted>
```


PT Activity 4.7.1: Packet Tracer Skills Integration Challenge (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
ISP	**S0/0/0**	209.165.200.226	255.255.255.252
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255255.255.252
R2	**Fa0/1**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.252
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252
PC1	**NIC**	192.168.10.10	255.255.255.0
PC3	**NIC**	192.168.30.10	255.255.255.0
TFTP Server	**NIC**	192.168.20.254	255.255.255.255

Learning Objectives

- Configure routing
- Configure OSPF authentication
- Upgrade the Cisco IOS image

Introduction

This activity is a cumulative review of the chapter covering OSPF routing, authentication, and upgrading the Cisco IOS image.

Task 1: Configure Routing

Step 1. Configure a default route to ISP.

On R2, use the exit interface argument to configure a default route to ISP.

Step 2. Configure OSPF routing between R1, R2, and R3.

Configure OSPF routing on all three routers. Use process ID 1. Disable OSPF updates on appropriate interfaces.

Step 3. Propagate the default route.

Step 4. Check results.

Your completion percentage should be 59%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure OSPF Authentication

Step 1. Configure MD5 authentication between R1, R2, and R3.

Configure OSPF MD5 authentication between R1, R2, and R3 using **1** as the key value and a **cisco123** as the password.

Step 2. Check results.

Your completion percentage should be 91%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Upgrade the Cisco IOS Image

Step 1. Copy a newer image from the TFTP server to flash on R2.

Look under the Config tab for the TFTP server to determine the name of the newer Cisco IOS image. Then copy the newer image to flash on R2.

Step 2. Configure R2 to boot with the new image.

Step 3. Save the configuration and reload.

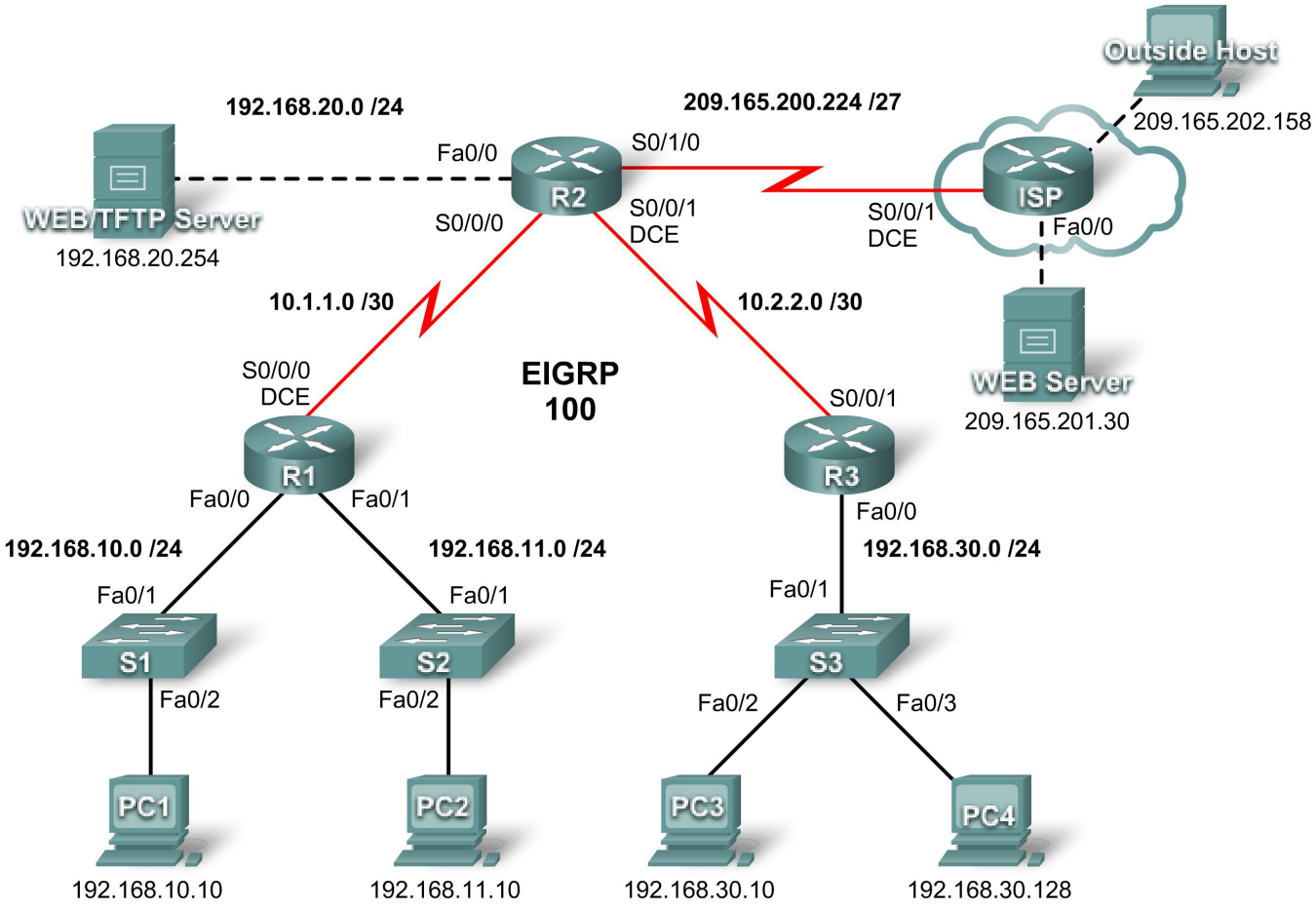
Verify that the new image is loaded in RAM.

Step 4. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

PT Activity 5.2.8: Configuring Standard ACLs (Instructor Version)

Topology Diagram



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	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/0	192.168.20.1	255.255.255.0
R3	S0/0/1	10.2.2.2	255.255.255.252
	Fa0/0	192.168.30.1	255.255.255.0
ISP	S0/0/1	209.165.200.226	255.255.255.224
	Fa0/0	209.165.201.1	255.255.255.224
	Fa0/1	209.165.202.129	255.255.255.224
PC1	NIC	192.168.10.10	255.255.255.0
PC2	NIC	192.168.11.10	255.255.255.0
PC3	NIC	192.168.30.10	255.255.255.0
PC4	NIC	192.168.30.128	255.255.255.0
WEB/TFTP Server	NIC	192.168.20.254	255.255.255.0
WEB Server	NIC	209.165.201.30	255.255.255.224
Outside Host	NIC	209.165.202.158	255.255.255.224

Learning Objectives

- Investigate the current network configuration
- Evaluate a network policy and plan an ACL implementation
- Configure numbered standard ACLs
- Configure named standard ACLs

Introduction

Standard ACLs are router configuration scripts that control whether a router permits or denies packets based on the source address. This activity focuses on defining filtering criteria, configuring standard ACLs, applying ACLs to router interfaces, and verifying and testing the ACL implementation. The routers are already configured, including IP addresses and EIGRP routing. The user EXEC password is **cisco,** and the privileged EXEC password is **class**.

Task 1: Investigate the Current Network Configuration

Step 1. View the running configuration on the routers.

View the running configurations on all three routers using the **show running-config** command while in privileged EXEC mode. Notice that the interfaces and routing are fully configured. Compare the IP address configurations to the Addressing Table above. There should not be any ACLs configured on the routers at this time.

The ISP router does not require any configuration during this exercise. Assume that the ISP router is not under your administration and is configured and maintained by the ISP administrator.

Step 2. Confirm that all devices can access all other locations.

Before applying any ACLs to a network, it is important to confirm that you have full connectivity. Without testing connectivity in your network prior to applying an ACL, troubleshooting may be more difficult.

One helpful step in testing connectivity is to view the routing tables on each device to ensure that each network is listed. On R1, R2, and R3, issue the **show ip route** command. You should see that each device has connected routes for attached networks, and dynamic routes to all other remote networks. All devices can access all other locations.

Although the routing table can be helpful in assessing the status of the network, you should still test connectivity using **ping**. Complete the following tests:

- From PC1, ping PC2.
- From PC2, ping Outside Host.
- From PC4, ping the Web/TFTP Server.

Each of these connectivity tests should be successful.

Task 2: Evaluate a Network Policy and Plan an ACL Implementation

Step 1. Evaluate the policy for the R1 LANs.

- The 192.168.10.0/24 network is allowed access to all locations, except the 192.168.11.0/24 network.
- The 192.168.11.0/24 network is allowed access to all destinations, except to any networks connected to the ISP.

Step 2. Plan the ACL implementation for the R1 LANs.

- Two ACLs fully implement the security policy for the R1 LANs.
- The first ACL on R1 denies traffic from the 192.168.10.0/24 network to the 192.168.11.0/24 network, but permits all other traffic.
- This first ACL, applied outbound on the Fa0/1 interface, monitors any traffic sent to the 192.168.11.0 network.
- The second ACL on R2 denies the 192.168.11.0/24 network access to the ISP, but permits all other traffic.
- Outbound traffic from the S0/1/0 interface is controlled.
- Place the ACL statements in the order of most specific to least specific. Denying the network traffic from accessing another network comes before permitting all other traffic.

Step 3. Evaluate the policy for the R3 LAN.

- The 192.168.30.0/10 network is allowed access to all destinations.
- Host 192.168.30.128 is not allowed access outside of the LAN.

Step 4. Plan the ACL implementation for the R3 LAN.

- One ACL fully implements the security policy for the R3 LAN.
- The ACL is placed on R3 and denies the 192.168.30.128 host access outside of the LAN, but permits traffic from all other hosts on the LAN.
- Applied inbound on the Fa0/0 interface, this ACL will monitor all traffic attempting to leave the 192.168.30.0/10 network.
- Place the ACL statements in the order of most specific to least specific. Denying the 192.168.30.128 host access comes before permitting all other traffic.

Task 3: Configure Numbered Standard ACLs

Step 1. Determine the wildcard mask.

The wildcard mask in an ACL statement determines how much of an IP source or destination address to check. A 0 bit means to match that value in the address, while a 1 bit ignores that value in the address. Remember that standard ACLs can only check source addresses.

- Since the ACL on R1 denies all 192.168.10.0/24 network traffic, any source IP that begins with 192.168.10 is denied. Since the last octet of the IP address can be ignored, the correct wildcard mask is 0.0.0.255. Each octet in this mask can be thought of as “check, check, check, ignore.”
- The ACL on R2 also denies 192.168.11.0/24 network traffic. The same wildcard mask can be applied, 0.0.0.255.

Step 2. Determine the statements.

- ACLs are configured in global configuration mode.
- For standard ACLs, use a number between 1 and 99. The number **10** is used for this list on R1 to help remember that this ACL is monitoring the 192.168.**10**.0 network.
- On R2, access list **11 will deny** traffic from the 192.168.**11**.0 network to any ISP networks, so the **deny** option is set with the network **192.168.11.0** and wildcard mask **0.0.0.255**.
- All other traffic must be permitted with the **permit** option because of the implicit “deny any” at the end of ACLs. The **any** option specifies any source host.

Configure the following on R1:

```
R1(config)#access-list 10 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 10 permit any
```

Note: Packet Tracer will not grade an ACL configuration until all statements are entered in the correct order.

Now create an ACL on R2 to deny the 192.168.11.0 network and permit all other networks. For this ACL, use the number **11**. Configure the following on R2:

```
R2(config)#access-list 11 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 11 permit any
```

Step 3. Apply the statements to the interfaces.

On R1, enter configuration mode for the Fa0/1 interface.

Issue the **ip access-group 10 out** command to apply the standard ACL outbound on the interface.

```
R1(config)#interface fa0/1
R1(config-if)#ip access-group 10 out
```

On R2, enter configuration mode for the S0/1/0 interface.

Issue the **ip access-group 11 out** command to apply the standard ACL outbound on the interface.

```
R2(config)#interface s0/1/0
R2(config-if)#ip access-group 11 out
```

Step 4. Verify and test ACLs.

With the ACLs configured and applied, PC1 (192.168.10.10) should not be able to ping PC2 (192.168.11.10), because ACL 10 is applied outbound on Fa0/1 on R1.

PC2 (192.168.11.10) should not be able to ping Web Server (209.165.201.30) or Outside Host (209.165.202.158), but should be able to ping everywhere else, because ACL 11 is applied outbound on S0/1/0 on R2. However, PC2 cannot ping PC1 because ACL 10 on R1 prevents the echo reply from PC1 to PC2.

Step 5. Check results.

Your completion percentage should be 67%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure a Named Standard ACL

Step 1. Determine the wildcard mask.

- The access policy for R3 states that the host at 192.168.30.128 should not be allowed any access outside the local LAN. All other hosts on the 192.168.30.0 network should be allowed access to all other locations.
- To check a single host, the entire IP address needs to be checked, which is accomplished using the **host** keyword.
- All packets that do not match the host statement are permitted.

Step 2. Determine the statements.

- On R3, enter global configuration mode.
- Create a named ACL called NO_ACCESS by issuing the **ip access-list standard NO_ACCESS** command. You will enter ACL configuration mode. All permit and deny statements are configured from this configuration mode.
- Deny traffic from the 192.168.30.128 host with the **host** option.
- Permit all other traffic with **permit any**.

Configure the following named ACL on R3:

```
R3(config)#ip access-list standard NO_ACCESS
R3(config-std-nacl)#deny host 192.168.30.128
R3(config-std-nacl)#permit any
```

Step 3. Apply the statements to the correct interface.

On R3, enter configuration mode for the Fa0/0 interface.

Issue the **ip access-group NO_ACCESS in** command to apply the named ACL inbound on the interface. This command causes all traffic entering the Fa0/0 interface from the 192.168.30.0/24 LAN to be checked against the ACL.

```
R3(config)#interface fa0/0
R3(config-if)#ip access-group NO_ACCESS in
```

Step 4. Verify and test ACLs.

Click **Check Results,** and then click **Connectivity Tests**. The following tests should fail:

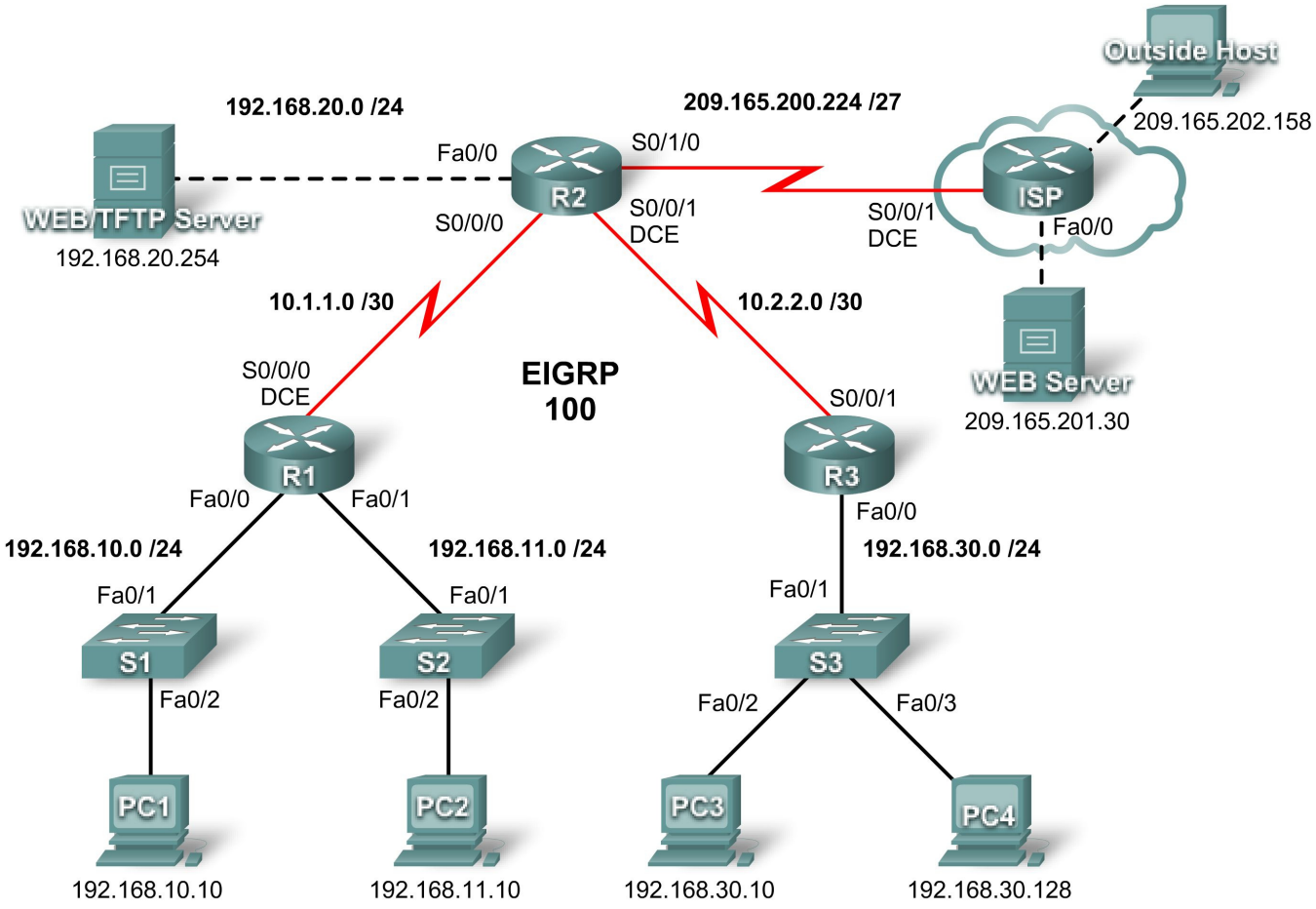
- PC1 to PC2
- PC2 to Outside Host
- PC2 to Web Server
- All pings from/to PC4 except between PC3 and PC4

Step 5. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

PT Activity 5.3.4: Configuring Extended ACLs (Instructor Version)

Topology Diagram



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	10.2.2.2	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/0	192.168.20.1	255.255.255.0
R3	S0/0/1	10.2.2.1	255.255.255.252
	Fa0/0	192.168.30.1	255.255.255.0
ISP	S0/0/1	209.165.200.226	255.255.255.224
	Fa0/0	209.165.201.1	255.255.255.224
	Fa0/1	209.165.202.129	255.255.255.224
PC1	NIC	192.168.10.10	255.255.255.0
PC2	NIC	192.168.11.10	255.255.255.0
PC3	NIC	192.168.30.10	255.255.255.0
PC4	NIC	192.168.30.128	255.255.255.0
WEB/TFTP Server	NIC	192.168.20.254	255.255.255.0
WEB Server	NIC	209.165.201.30	255.255.255.224
Outside Host	NIC	209.165.202.158	255.255.255.224

Learning Objectives

- Investigate the current network configuration
- Evaluate a network policy and plan an ACL implementation
- Configure numbered extended ACLs
- Configure named extended ACLs

Introduction

Extended ACLs are router configuration scripts that control whether a router permits or denies packets based on their source or destination address as well as protocols or ports. Extended ACLs provide more flexibility and granularity than standard ACLs. This activity focuses on defining filtering criteria, configuring extended ACLs, applying ACLs to router interfaces, and verifying and testing the ACL implementation. The routers are already configured, including IP addresses and EIGRP routing. The user EXEC password is **cisco,** and the privileged EXEC password is **class**.

Task 1: Investigate the Current Network Configuration

Step 1. View the running configuration on the routers.

View the running configurations on all three routers using the **show running-config** command while in privileged EXEC mode. Notice that the interfaces and routing are fully configured. Compare the IP address configurations to the Addressing Table above. There should not be any ACLs configured on the routers at this time.

The ISP router does not require any configuration during this exercise. It is assumed that the ISP router is not under your administration and is configured and maintained by the ISP administrator.

Step 2. Confirm that all devices can access all other locations.

Before applying any ACLs to a network, it is important to confirm that you have fully connectivity. Without testing connectivity in your network prior to applying an ACL, troubleshooting will be very difficult.

To ensure network-wide connectivity, use the **ping** and **tracert** commands between various network devices to verify connections.

Task 2: Evaluate a Network Policy and Plan an ACL Implementation

Step 1. Evaluate the policy for the R1 LANs.

- For the 192.168.10.0/24 network, block Telnet access to all locations and TFTP access to the corporate Web/TFTP server at 192.168.20.254. All other access is allowed.
- For the192.168.11.0/24 network, allow TFTP access and web access to the corporate Web/TFTP server at 192.168.20.254. Block all other traffic from the 192.168.11.0/24 network to the 192.168.20.0/24 network. All other access is allowed.

Step 2. Plan the ACL implementation for the R1 LANs.

- Two ACLs fully implement the security policy for the R1 LANs.
- The first ACL supports the first part of the policy and is configured on R1 and applied inbound to the Fast Ethernet 0/0 interface.
- The second ACL supports the second part of the policy and is configured on R1 and applied inbound to the Fast Ethernet 0/1 interface.

Step 3. Evaluate the policy for the R3 LAN.

- All IP addresses of the 192.168.30.0/24 network are blocked from accessing all IP addresses of the 192.168.20.0/24 network.
- The first half of 192.168.30.0/24 is allowed access to all other destinations.
- The second half of 192.168.30.0/24 network is allowed access to the 192.168.10.0/24 and 192.168.11.0/24 networks.
- The second half of 192.168.30.0/24 is allowed web and ICMP access to all remaining destinations.
- All other access is implicitly denied.

Step 4. Plan the ACL implementation for the R3 LAN.

This step requires one ACL configured on R3 and applied inbound to the Fast Ethernet 0/0 interface.

Step 5. Evaluate the policy for traffic coming from the Internet via the ISP.

- Outside hosts are allowed to establish a web session with the internal web server on port 80 only.
- Only established TCP sessions are allowed in.

- Only ping replies are allowed through R2.

Step 6. Plan the ACL implementations for traffic coming from the Internet via the ISP.

This step requires one ACL configured on R2 and applied inbound to the Serial 0/1/0 interface.

Task 3: Configure Numbered Extended ACLs

Step 1. Determine the wildcard masks.

Two ACLs are needed to enforce the access control policy on R1. Both ACLs will be designed to deny an entire Class C network. You will configure a wildcard mask that matches all hosts on each of these Class C networks.

For example, for the entire subnet of 192.168.10.0/24 to be matched, the wildcard mask is 0.0.0.255. This can be thought of as “check, check, check, ignore” and, in essence, matches the entire 192.168.10.0/24 network.

Step 2. Configure the first extended ACL for R1.

From global configuration mode, configure the first ACL with number 110. First, you want to block Telnet to any location for all IP addresses on the 192.168.10.0/24 network.

When writing the statement, make sure that you are currently in global configuration mode.

```
R1(config)#access-list 110 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
```

Next, block all IP addresses on the 192.168.10.0/24 network from TFTP access to the host at 192.168.20.254.

```
R1(config)#access-list 110 deny udp 192.168.10.0 0.0.0.255 host
192.168.20.254 eq tftp
```

Finally, permit all other traffic.

```
R1(config)#access-list 110 permit ip any any
```

Step 3. Configure the second extended ACL for R1.

Configure the second ACL with number 111. Permit WWW to the host at 192.168.20.254 for any IP addresses on the 192.168.11.0/24 network.

```
R1(config)#access-list 111 permit tcp 192.168.11.0 0.0.0.255 host
192.168.20.254 eq www
```

Next, permit TFTP to the host at 192.168.20.254 for any IP addresses on the 192.168.11.0/24 network.

```
R1(config)#access-list 111 permit udp 192.168.11.0 0.0.0.255 host
192.168.20.254 eq tftp
```

Block all other traffic from 192.168.11.0/24 network to the 192.168.20.0/24 network.

```
R1(config)#access-list 111 deny ip 192.168.11.0 0.0.0.255 192.168.20.0
0.0.0.255
```

Finally, permit any other traffic. This statement ensures that traffic from other networks is not blocked.

```
R1(config)#access-list 111 permit ip any any
```


Step 4. Verify the ACL configurations.

Confirm your configurations on R1 by issuing the **show access-lists** command. Your output should look like this:

```
R1#show access-lists
Extended IP access list 110
   deny tcp 192.168.10.0 0.0.0.255 any eq telnet
   deny udp 192.168.10.0 0.0.0.255 host 192.168.20.254 eq tftp
   permit ip any any
Extended IP access list 111
   permit tcp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq www
   permit udp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq tftp
   deny ip 192.168.11.0 0.0.0.255 192.168.20.0 0.0.0.255
   permit ip any any
```

Step 5. Apply the statements to the interfaces.

To apply an ACL to an interface, enter interface configuration mode for that interface. Configure the command **ip access-group** *access-list-number* {**in** | **out**} to apply the ACL to the interface.

Each ACL filters inbound traffic. Apply ACL 110 to Fast Ethernet 0/0 and ACL 111 to Fast Ethernet 0/1.

```
R1(config)#interface fa0/0
R1(config-if)#ip access-group 110 in
R1(config-if)#interface fa0/1
R1(config-if)#ip access-group 111 in
```

Confirm that the ACLs appear in the running configuration of R1 and that they have been applied to the correct interfaces.

Step 6. Test the ACLs configured on R1.

Now that ACLs have been configured and applied, it is very important to test that traffic is blocked or permitted as expected.

- From PC1, attempt to gain Telnet access to any device. This should be blocked.
- From PC1, attempt to access the corporate Web/TFTP server via HTTP. This should be allowed.
- From PC2, attempt to access the Web/TFTP server via HTTP. This should be allowed.
- From PC2, attempt to access the external Web server via HTTP. This should be allowed.

Based on your understanding of ACLs, try some other connectivity tests from PC1 and PC2.

Step 7. Check results.

Packet Tracer does not support testing TFTP access, so you will not be able to verify that policy. However, your completion percentage should be 50%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure a Numbered Extended ACL for R3

Step 1. Determine the wildcard mask.

The access policy for the lower half of the IP addresses on the 192.168.30.0/24 network requires:

- Deny access to the 192.168.20.0/24 network
- Allow access to all other destinations

The top half of the IP addresses in the 192.168.30.0/24 network has the following restrictions:

- Allow access to 192.168.10.0 and 192.168.11.0

- Deny access to 192.168.20.0
- Allow web and ICMP to all other locations

To determine the wildcard mask, consider which bits need to be checked for the ACL to match IP addresses 0–127 (lower half) or 128–255 (upper half).

Recall that one way to determine the wildcard mask is to subtract the normal network mask from 255.255.255.255. The normal mask for IP addresses 0–127 and 128–255 for a Class C address is 255.255.255.128. Using the subtraction method, here is the correct wildcard mask:

```
   255.255.255.255
 - 255.255.255.128
-----------------
     0.  0.  0.127
```

Step 2. Configure the extended ACL on R3.

On R3, enter global configuration mode and configure the ACL using 130 as the access list number.

The first statement blocks the 192.168.30.0/24 from accessing all addresses in the 192.168.30.0/24 network.

```
R3(config)#access-list 130 deny ip 192.168.30.0 0.0.0.255 192.168.20.0
0.0.0.255
```

The second statement allows the lower half of the 192.168.30.0/24 network access to any other destinations.

```
R3(config)#access-list 130 permit ip 192.168.30.0 0.0.0.127 any
```

The remaining statements explicitly permit the upper half of the 192.168.30.0/24 network access to those networks and services that the network policy allows.

```
R3(config)#access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.10.0
0.0.0.255
R3(config)# access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.11.0
0.0.0.255
R3(config)# access-list 130 permit tcp 192.168.30.128 0.0.0.127 any eq www
R3(config)# access-list 130 permit icmp 192.168.30.128 0.0.0.127 any
R3(config)# access-list 130 deny ip any any
```

Step 3. Apply the statement to the interface.

To apply an ACL to an interface, enter interface configuration mode for that interface. Configure the command **ip access-group** *access-list-number* {**in** | **out**} to apply the ACL to the interface.

```
R3(config)#interface fa0/0
R3(config-if)#ip access-group 130 in
```

Step 4. Verify and test ACLs.

Now that the ACL has been configured and applied, it is very important to test that traffic is blocked or permitted as expected.

- From PC3, ping the Web/TFTP server. This should be blocked.
- From PC3, ping any other device. This should be allowed.
- From PC4, ping the Web/TFTP server. This should be blocked.
- From PC4, telnet to R1 at 192.168.10.1 or 192.168.11.1. This should be allowed.
- From PC4, ping PC1 and PC2. This should be allowed.
- From PC4, telnet to R2 at 10.2.2.2. This should be blocked.

After your tests have been conducted and yield the correct results, use the **show access-lists** privileged EXEC command on R3 to verify that the ACL statements have matches.

Based on your understanding of ACLs, conduct other tests to verify that each statement is matching the correct traffic.

Step 5. Check results.

Your completion percentage should be 75%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Configure a Named Extended ACL

Step 1. Configure a named extended ACL on R2.

Recall that the policy on R2 will be designed to filter Internet traffic. Since R2 has the connection to the ISP, this is the best placement for the ACL.

Configure a named ACL called FIREWALL on R2 using the **ip access-list extended** *name* command. This command puts the router into extended named ACL configuration mode. Note the changed router prompt.

```
R2(config)#ip access-list extended FIREWALL
R2(config-ext-nacl)#
```

In ACL configuration mode, add the statements to filter traffic as outlined in the policy:

- Outside hosts are allowed to establish a web session with the internal web server on port 80 only.
- Only established TCP sessions are allowed in.
- Ping replies are allowed through R2.

```
R2(config-ext-nacl)#permit tcp any host 192.168.20.254 eq www
R2(config-ext-nacl)#permit tcp any any established
R2(config-ext-nacl)#permit icmp any any echo-reply
R2(config-ext-nacl)#deny ip any any
```

After configuring the ACL on R2, use the **show access-lists** command to confirm that the ACL has the correct statements.

Step 2. Apply the statement to the interface.

Use the **ip access-group** *name* {**in** | **out**} command to apply the ACL inbound on the ISP facing interface of R2.

```
R3(config)#interface s0/1/0
R3(config-if)#ip access-group FIREWALL in
```

Step 3. Verify and test ACLs.

Conduct the following tests to ensure that the ACL is functioning as expected:

- From Outside Host, open a web page on the internal Web/TFTP server. This should be allowed.
- From Outside Host, ping the internal Web/TFTP server. This should be blocked.
- From Outside Host, ping PC1. This should be blocked.
- From PC1, ping the external Web Server at 209.165.201.30. This should be allowed.
- From PC1, open a web page on the external Web Server. This should be allowed.

After your tests have been conducted and yield the correct results, use the **show access-lists** privileged EXEC command on R2 to verify that the ACL statements have matches.

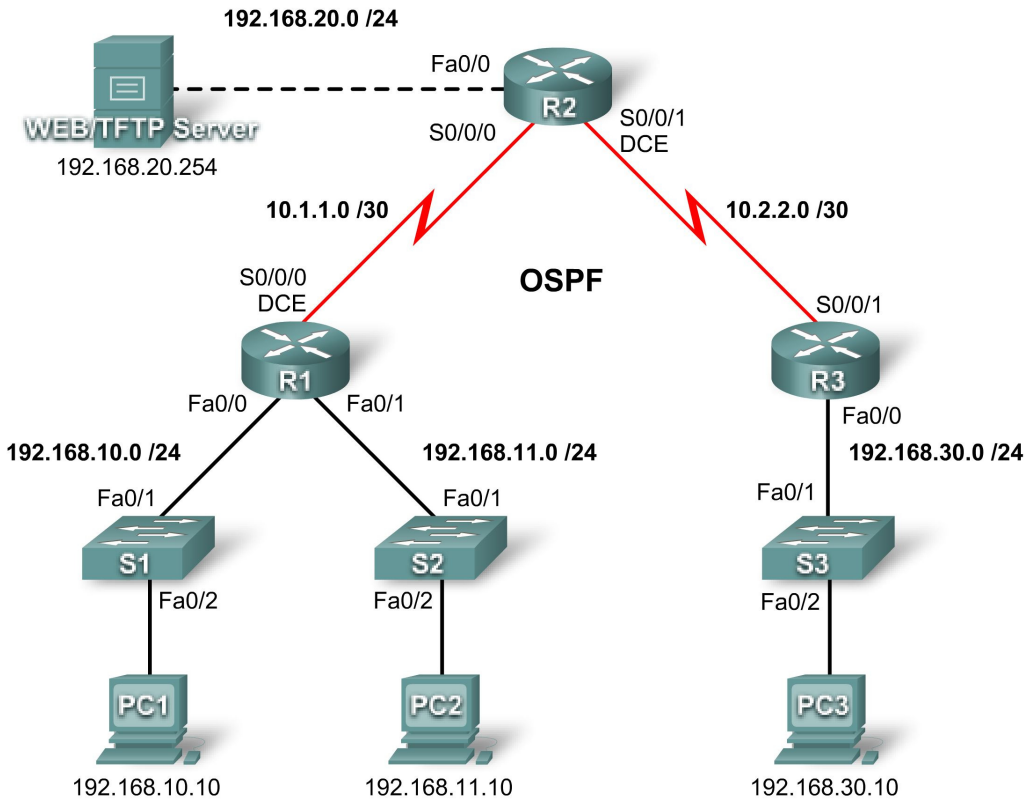
Based on your understanding of ACLs, conduct other tests to verify that each statement is matching the correct traffic.

Step 4. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

PT Activity 5.5.1: Basic Access Control Lists (Instructor Version)

Topology Diagram



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
R2	**Fa0/0**	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	N/A
R3	**Fa0/0**	192.168.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A

Addressing Table on the next page

Addressing Table continued

S1	**VLAN 1**	192.168.10.2	255.255.255.0	192.168.10.1
S2	**VLAN 1**	192.168.11.2	255.255.255.0	192.168.11.1
S3	**VLAN 1**	192.168.30.2	255.255.255.0	192.168.30.1
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
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1
Web Server	**NIC**	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

- Perform basic router and switch configurations
- Configuring a standard ACL
- Configuring an extended ACL
- Control access to the vty lines with a standard ACL
- Troubleshooting ACLs

Introduction

In this activity, you will design, apply, test and troubleshoot access list configurations.

Task 1: Perform Basic Router and Switch Configurations

Configure the R1, R2, R3, S1, S2, and S3 routers and switches according to the following guidelines:

- Configure hostnames to match the topology diagram.
- Disable DNS lookup.
- Configure an EXEC mode secret of **class**.
- Configure a **message-of-the-day** banner
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.
- Configure IP addresses and masks on all devices. Clock rate on **64000**.
- Enable OSPF using process ID 1 on all routers for all networks.
- Configure a loopback interface on R2.
- Configure IP addresses for the VLAN 1 interface on each switch.
- Configure each switch with the appropriate default gateway.
- Verify full IP connectivity using the **ping** command.

Task 2: Configuring a Standard ACL

Standard ACLs can filter traffic based on source IP address only. In this task, you are configuring a standard ACL that blocks traffic from the 192.168.11.0 /24 network. This ACL will be applied inbound on the R3 serial interface. Remember that every ACL has an implicit “deny all” that causes all traffic that has not matched a statement in the ACL to be blocked. For this reason, add the **permit any** statement to the end of the ACL.

Step 1. Create the ACL.

In global configuration mode, create a standard named ACL called **std-1**.

```
R3(config)#ip access-list standard std-1
```

In standard ACL configuration mode, add a statement that denies any packets with a source address of 192.168.11.0 /24 and prints a message to the console for each matched packet.

```
R3(config-std-nacl)#deny 192.168.11.0 0.0.0.255
```

Permit all other traffic.

```
R3(config-std-nacl)#permit any
```

Step 2. Apply the ACL.

Apply the ACL std-1 as a filter on packets entering R3 through serial interface 0/0/1.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group std-1 in
```

Step 3. Test the ACL.

Test the ACL by pinging from PC2 to PC3. Since the ACL is designed to block traffic with source addresses from the 192.168.11.0 /24 network, PC2 (192.168.11.10) should not be able to ping PC3.

In privileged EXEC mode on R3, issue the **show access-lists** command. You see output similar to the following. Each line of an ACL has an associated counter showing how many packets have matched the rule.

```
Standard IP access list std-1
    deny 192.168.11.0 0.0.0.255 (3 match(es))
    permit any
```

Task 3: Configuring an Extended ACL

When greater granularity is required, you should use an extended ACL. Extended ACLs can filter traffic based on more than just source address. Extended ACLs can filter on protocol, source, and destination IP addresses, and source and destination port numbers.

An additional policy for this network states that devices from the 192.168.10.0/24 LAN are only permitted to reach internal networks. Computers on this LAN are not permitted to access the Internet. Therefore, these users must be blocked from reaching the IP address 209.165.200.225. Because this requirement needs to enforce both source and destination, an extended ACL is needed.

In this task, you are configuring an extended ACL on R1 that blocks traffic originating from any device on the 192.168.10.0 /24 network to access the 209.165.200.255 host. This ACL will be applied outbound on the R1 Serial 0/0/0 interface.

Step 1. Configure a named extended ACL.

In global configuration mode, create a named extended ACL called **extend-1**.

```
R1(config)#ip access-list extended extend-1
```

Notice that the router prompt changes to indicate that you are now in extended ACL configuration mode. From this prompt, add the necessary statements to block traffic from the 192.168.10.0 /24 network to the host. Use the **host** keyword when defining the destination.

```
R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
```


Recall that the implicit “deny all” blocks all other traffic without the additional **permit** statement. Add the **permit** statement to ensure that other traffic is not blocked.

```
R1(config-ext-nacl)#permit ip any any
```

Step 2. Apply the ACL.

With standard ACLs, the best practice is to place the ACL as close to the destination as possible. Extended ACLs are typically placed close to the source. The **extend-1** ACL will be placed on the Serial interface, and will filter outbound traffic

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip access-group extend-1 out
```

Step 3. Test the ACL.

From PC1 or any other device on the 192.168.10.0 /24 network, ping the loopback interface on R2. These pings should fail, because all traffic from the 192.168.10.0 /24 network is filtered when the destination is 209.165.200.225. If the destination is any other address, the pings should succeed. Confirm this by pinging R3 from the 192.168.10.0 /24 network device.

You can further verify this by issuing the **show ip access-list** on R1 after pinging.

You should have matches for both rules of the ACL. This is because the ping from PC1 to R2s loopback interface was denied while the ping to R3 was permitted.

```
R1#show ip access-list
Extended IP access list extend-1
    deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 match(es))
    permit ip any any (4 match(es))
```

Task 4: Control Access to the vty Lines with a Standard ACL

It is good practice to restrict access to the router vty lines for remote administration. An ACL can be applied to the vty lines, allowing you to restrict access to specific hosts or networks. In this task, you will configure a standard ACL to permit hosts from two networks to access the vty lines. All other hosts are denied.

Verify that you can telnet to R2 from both R1 and R3.

Step 1. Configure the ACL.

Configure a named standard ACL on R2 that permits traffic from 10.2.2.0 /29 and 192.168.30.0 /24. Deny all other traffic. Call the ACL **Task-4**.

```
R2(config)#ip access-list standard Task-4
R2(config-std-nacl)#permit 10.2.2.0 0.0.0.3
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255
```

Step 2. Apply the ACL.

Enter line configuration mode for vty lines 0–4.

```
R2(config)#line vty 0 16
```

Use the **access-class** command to apply the ACL to the vty lines in the inbound direction. Note that this differs from the command used to apply ACLs to other interfaces.

```
R2(config-line)#access-class Task-4 in
```


Step 3. Test the ACL.

Telnet to R2 from R1. Note that R1 does not have IP addresses in the address range listed in the ACL Task-4 permit statements. Connection attempts should fail.

From R3, telnet to R2 or any device on the 192.168.30.0 /24 network. You will be presented with a prompt for the vty line password.

Why do connection attempts from other networks fail even though they are not specifically listed in the ACL?

_____

_____

All ACLs include an implicit deny all as a final statement. Any traffic not explicitly permitted is dropped.

Task 5: Troubleshooting ACLs

When an ACL is improperly configured or applied to the wrong interface or in the wrong direction, network traffic may be affected in an undesirable manner.

Step 1. Test the ACL.

In an earlier task, you created and applied a named standard ACL on R3. Use the **show running-config** command to view the ACL and its placement. You should see that an ACL named **std-1** was configured and applied inbound on Serial 0/0/1. Recall that this ACL was designed to block all network traffic with a source address from the 192.168.11.0 /24 network from accessing the LAN on R3.

To remove the ACL, go to interface configuration mode for Serial 0/0/1 on R3.

```
R3(config)#interface serial 0/0/1
```

Use the **no ip access-group std-1 in** command to remove the ACL from the interface.

```
R3(config-if)#no ip access-group std-1 in
```

Use the **show running-config** command to confirm that the ACL has been removed from Serial 0/0/1

Step 2. Apply ACL std-1 on S0/0/1 outbound.

To test the importance of ACL filtering direction, reapply the **std-1** ACL to the Serial 0/0/1 interface. This time the ACL will be filtering outbound traffic, rather than inbound traffic. Remember to use the **out** keyword when applying the ACL.

```
R3(config-if)#ip access-group std-1 out
```

Step 3. Test the ACL.

Test the ACL by pinging from PC2 to PC3. As an alternative, use an extended ping from R1. Notice that this time pings succeed, and the ACL counters are not incremented. Confirm this by issuing the **show ip access-list** command on R3.

Step 4. Restore the ACL to its original configuration.

Remove the ACL from the outbound direction and reapply it to the inbound direction.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group std-1 out
R3(config-if)#ip access-group std-1 in
```


Step 5. Apply Task-4 to the R2 serial 0/0/0 interface inbound.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group Task-4 in
```

Step 6. Test the ACL.

Attempt to communicate to any device connected to R2 or R3 from R1 or its attached networks. Notice that all communication is blocked, however, ACL counters are not incremented. This is because of the implicit “deny all” at the end of every ACL.

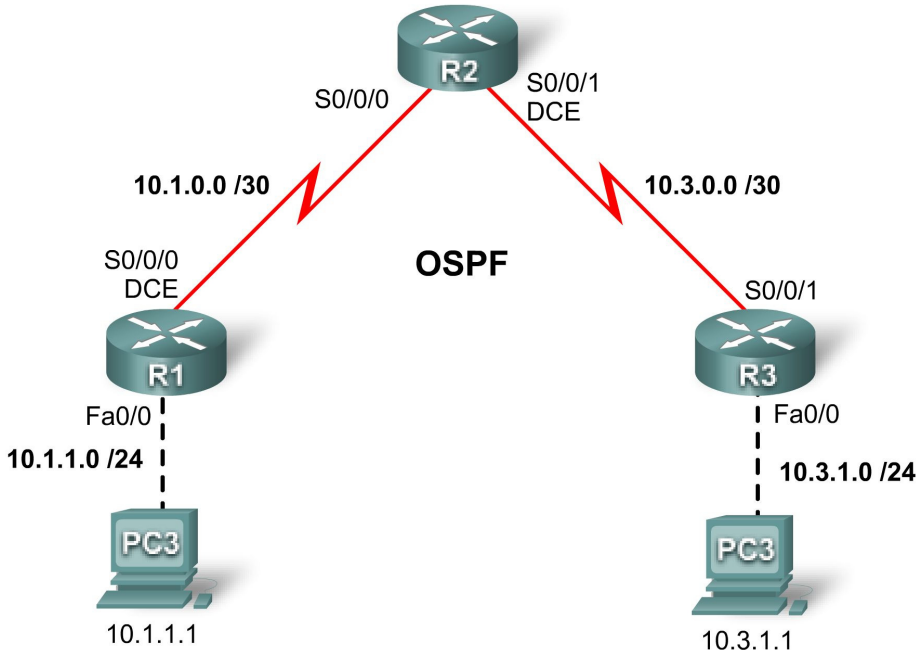
You should see messages similar to the following printed on the consoles of R1 and R2 after the OSPF dead timers expires:

```
*Sep  4 09:51:21.757: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

Remove ACL Task-4 from the interface.

PT Activity 5.5.2: Challenge Access Control Lists (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**S0/0/0**	10.1.0.1	255.255.255.252	N/A
	Fa0/0	10.1.1.254	255.255.255.0	N/A
R2	**S0/0/0**	10.1.0.2	255.255.255.252	N/A
	S0/0/1	10.3.0.1	255.255.255.252	N/A
R3	**S0/0/1**	10.3.0.2	255.255.255.252	N/A
	Fa0/0	10.3.1.254	255.255.255.0	N/A
PC1	**NIC**	10.1.1.1	255.255.255.0	10.1.1.254
PC2	**NIC**	10.3.1.1	255.255.255.0	10.3.1.254

Learning Objectives

- Perform basic router configurations
- Configuring standard ACLs
- Configuring extended ACLs
- Verifying ACLs

Introduction

In this activity, you will design, apply, test and troubleshoot access list configurations.

Task 1: Perform Basic Router Configurations

Configure all devices according to the following guidelines:

- Configure the router hostname.
- Disable DNS lookup.
- Configure an EXEC mode secret of **class**.
- Configure a **message-of-the-day** banner
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.
- Configure IP addresses and masks on all devices. Clock rate is **64000**.
- Enable OSPF with process ID 1 on all routers for all networks.
- Verify full IP connectivity using the **ping** command.

Task 2: Configuring Standard ACLs

Configure standard named ACLs on the R1 and R3 vty lines, permitting hosts connected directly to their Fast Ethernet subnets to gain Telnet access. Deny all other connection attempts. Name these standard ACLs **VTY-Local** and apply to all telnet lines. Document your ACL configuration.

_____

_____

_____

_____

_____

_____

_____

The following is configured on both R1 and R3. Only R1 is shown.

```
R1(config)#ip access-list standard VTY-Local
R1(config-std-nacl)#permit 10.1.1.0 0.0.0.255
R1(config-std-nacl)#deny any
R1(config-std-nacl)#line vty 0 4
R1(config-line)#access-class VTY-Local in
```

Task 3: Configuring Extended ACLs

Using extended ACLs on R2, complete the following requirements:

- Name the ACL block
- Prohibit traffic originating from the R1 connected subnets from reaching the R3 connected subnets.

- Prohibit traffic originating from the R3 connected subnets from reaching the R1 connected subnets.
- Permit all other traffic.

Document your ACL configuration

_____

_____

_____

_____

_____

_____

```
R2(config)#ip access-list extended block
R2(config-ext-nacl)#deny ip 10.1.1.0 0.0.0.255 10.3.1.0 0.0.0.255
R2(config-ext-nacl)#deny ip 10.3.1.0 0.0.0.255 10.1.0.0 0.0.0.255
R2(config-ext-nacl)#permit ip any any
R2(config-ext-nacl)#int s0/0/0
R2(config-if)#ip access-group block in
R2(config-if)#int s0/0/1
R2(config-if)#ip access-group block in
```

Task 4: Verifying ACLs

Step 1. Test telnet.

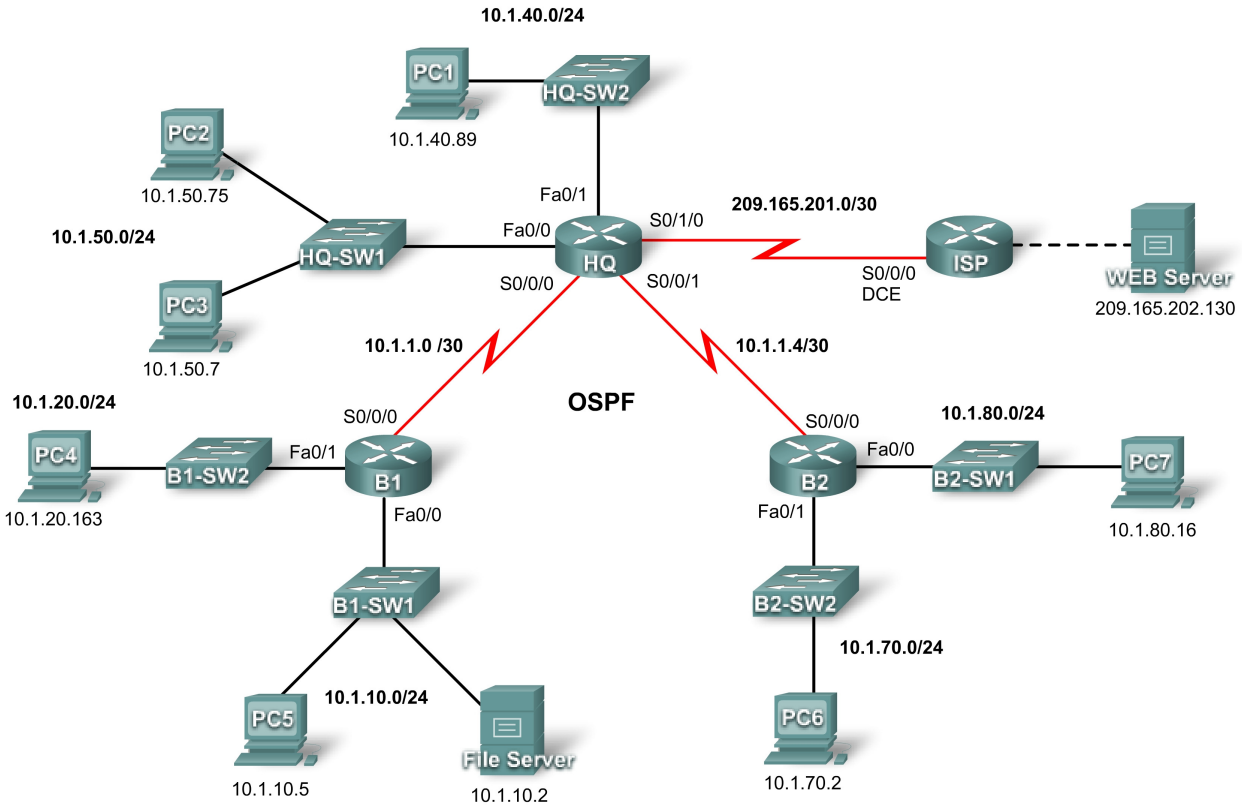
- PC1 should be able to telnet into R1
- PC3 should be able to telnet into R3
- R2 should be denied telnet access to R1 and R3

Step 2. Test traffic.

Pings between PC1 and PC3 should fail.

PT Activity 5.6.1: Packet Tracer Skills Integration Challenge (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
HQ	S0/0/0	10.1.1.1	255.255.255.252
	S0/0/1	10.1.1.5	255.255.255.252
	S0/1/0	209.165.201.2	255.255.255.252
	Fa0/0	10.1.50.1	255.255.255.0
	Fa0/1	10.1.40.1	255.255.255.0
B1	S0/0/0	10.1.1.2	255.255.255.252
	Fa0/0	10.1.10.1	255.255.255.0
	Fa0/1	10.1.20.1	255.255.255.0
B2	S0/0/0	10.1.1.6	255.255.255.252
	Fa0/0	10.1.80.1	255.255.255.0
	Fa0/1	10.1.70.1	255.255.255.0
ISP	S0/0/0	209.165.201.1	255.255.255.252
	Fa0/0	209.165.202.129	255.255.255.252
Web Server	NIC	209.165.202.130	255.255.255.252

Learning Objectives

- Configure PPP with CHAP authentication
- Configure default routing
- Configure OSPF routing
- Implement and verify multiple ACL security policies

Introduction

In this activity, you will demonstrate your ability to configure ACLs that enforce five security policies. In addition, you will configure PPP and OSPF routing. The devices are already configured with IP addressing. The user EXEC password is **cisco,** and the privileged EXEC password is **class**.

Task 1: Configure PPP with CHAP Authentication

Step 1. Configure the link between HQ and B1 to use PPP encapsulation with CHAP authentication.

The password for CHAP authentication is **cisco123**.

```
HQ(config)#username B1 password cisco123
HQ(config)#interface s0/0/0
HQ(config-if)#encapsulation ppp
HQ(config-if)#ppp authentication chap

B1(config)#username HQ password cisco123
B1(config)#interface s0/0/0
B1(config-if)#encapsulation ppp
```



```
B1(config-if)#ppp authentication chap
```

Step 2. Configure the link between HQ and B2 to use PPP encapsulation with CHAP authentication.

The password for CHAP authentication is **cisco123**.

```
HQ(config)#username B2 password cisco123
HQ(config)#interface s0/0/1
HQ(config-if)#encapsulation ppp
HQ(config-if)#ppp authentication chap

B2(config)#username HQ password cisco123
B2(config)#interface s0/0/0
B2(config-if)#encapsulation ppp
```

Step 3. Verify that connectivity is restored between the routers.

HQ should be able to ping both B1 and B2. The interfaces may take a few minutes to come back up. You can switch back and forth between Realtime and Simulation mode to speed up the process. Another possible workaround to this Packet Tracer behavior is to use the **shutdown** and **no shutdown** commands on the interfaces.

Note: The interfaces may go down at random points during the activity because of a Packet Tracer bug. The interface normally comes back up on its own if you wait a few seconds.

Step 4. Check results.

Your completion percentage should be 29%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure Default Routing

Step 1. Configure default routing from HQ to ISP.

Configure a default route on HQ using the *exit interface* argument to send all default traffic to ISP.

```
HQ(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0
```

Step 2. Test connectivity to Web Server.

HQ should be able to successfully ping Web Server at 209.165.202.130 as long as the ping is sourced from the Serial0/1/0 interface.

Step 3. Check results.

Your completion percentage should be 32%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure OSPF Routing

Step 1. Configure OSPF on HQ.

- Configure OSPF using the process ID 1.
- Advertise all subnets except the 209.165.201.0 network.
- Propagate the default route to OSPF neighbors.
- Disable OSPF updates to ISP and to the HQ LANs.


```
HQ(config)#router ospf 1
HQ(config-router)#network 10.1.1.0 0.0.0.3 area 0
HQ(config-router)#network 10.1.1.4 0.0.0.3 area 0
HQ(config-router)#network 10.1.40.0 0.0.0.255 area 0
HQ(config-router)#network 10.1.50.0 0.0.0.255 area 0
HQ(config-router)#default-information originate
HQ(config-router)#passive-interface fa0/0
HQ(config-router)#passive-interface fa0/1
HQ(config-router)#passive-interface s0/1/0
```

Step 2. Configure OSPF on B1 and B2.

- Configure OSPF using the process ID 1.
- On each router, configure the appropriate subnets.
- Disable OSPF updates to the LANs.

```
B1(config)#router ospf 1
B1(config-router)#network 10.1.1.0 0.0.0.3 area 0
B1(config-router)#network 10.1.10.0 0.0.0.255 area 0
B1(config-router)#network 10.1.20.0 0.0.0.255 area 0
B1(config-router)#passive-interface fa0/0
B1(config-router)#passive-interface fa0/1

B1(config)#router ospf 1
B1(config-router)#network 10.1.1.4 0.0.0.3 area 0
B1(config-router)#network 10.1.70.0 0.0.0.255 area 0
B1(config-router)#network 10.1.80.0 0.0.0.255 area 0
B1(config-router)#passive-interface fa0/0
B1(config-router)#passive-interface fa0/1
```

Step 3. Test connectivity throughout the network.

The network should now have full end-to-end connectivity. All devices should be able to successfully ping all other devices, including Web Server at 209.165.202.130.

Step 4. Check results.

Your completion percentage should be 76%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Implement Multiple ACL Security Policies

Step 1. Implement security policy number 1.

Block the 10.1.10.0 network from accessing the 10.1.40.0 network. All other access to 10.1.40.0 is allowed. Configure the ACL on HQ using ACL number 10.

- Use a standard or extended ACL? _____Standard
- Apply the ACL to which interface? _____Fa0/1
- Apply the ACL in which direction? _____Out


```
HQ(config)#access-list 10 deny 10.1.10.0 0.0.0.255
HQ(config)#access-list 10 permit any
HQ(config)#int fa0/1
HQ(config-if)#ip access-group 10 out
```

Step 2. Verify that security policy number 1 is implemented.

A ping from PC5 to PC1 should fail.

Step 3. Check results.

Your completion percentage should be 80%. If not, click **Check Results** to see which required components are not yet completed.

Step 4. Implement security policy number 2.

Host 10.1.10.5 is not allowed to access host 10.1.50.7. All other hosts are allowed to access 10.1.50.7. Configure the ACL on B1 using ACL number 115.

- Use a standard or extended ACL? _____Extended
- Apply the ACL to which interface? _____Fa0/0
- Apply the ACL in which direction? _____In

```
B1(config)#access-list 115 deny ip host 10.1.10.5 host 10.1.50.7
B1(config)#access-list 115 permit ip any any
B1(config)#int fa0/0
B1(config-if)#ip access-group 115 in
```

Step 5. Verify that security policy number 2 is implemented.

A ping from PC5 to PC3 should fail.

Step 6. Check results.

Your completion percentage should be 85%. If not, click **Check Results** to see which required components are not yet completed.

Step 7. Implement security policy number 3.

Hosts 10.1.50.1 through 10.1.50.63 are not allowed web access to Intranet server at 10.1.80.16. All other access is allowed. Configure the ACL on the appropriate router and use ACL number 101.

- Use a standard or extended ACL? _____Extended
- Configure the ACL on which router? _____HQ
- Apply the ACL to which interface? _____Fa0/0

- Apply the ACL in which direction? _____In

_____

_____

_____

_____

_____

```
HQ(config)#access-list 101 deny tcp 10.1.50.0 0.0.0.63 host 10.1.80.16 eq www
HQ(config)#access-list 101 permit ip any any
HQ(config)#interface fa0/0
HQ(config-if)#ip access-group 101 in
```

Step 8. Verify that security policy number 3 is implemented.

To test this policy, click PC3, then the **Desktop** tab, and then **Web Browser**. For the URL, type in the IP address for the Intranet server, 10.1.80.16, and press **Enter**. After a few seconds, you should receive a Request Timeout message. PC2 and any other PC in the network should be able to access the Intranet server.

Step 9. Check results.

Your completion percentage should be 90%. If not, click **Check Results** to see which required components are not yet completed.

Step 10. Implement security policy number 4.

Use the name **NO_FTP** to configure a named ACL that blocks the 10.1.70.0/24 network from accessing FTP services (port 21) on the file server at 10.1.10.2. All other access should be allowed.

Note: Names are case-sensitive.

- Use a standard or extended ACL? _____Extended
- Configure the ACL on which router? _____B2
- Apply the ACL to which interface? _____Fa0/1
- Apply the ACL in which direction? _____In

_____

_____

_____

_____

_____

```
B2(config)#ip access-list extended NO_FTP
B2(config-ext-nacl)#deny tcp 10.1.70.0 0.0.0.255 host 10.1.10.2 eq ftp
B2(config-ext-nacl)#permit ip any any
B2(config-ext-nacl)#interface fa0/1
B2(config-if)#ip access-group NO_FTP in
```


Step 11. Check results.

Packet Tracer does not support testing FTP access, so you will not be able to verify this policy. However, your completion percentage should be 95%. If not, click **Check Results** to see which required components are not yet completed.

Step 12. Implement security policy number 5.

Since ISP represents connectivity to the Internet, configure a named ACL called **FIREWALL** in the following order:

1. Allow only inbound ping replies from ISP and any source beyond ISP.
2. Allow only established TCP sessions from ISP and any source beyond ISP.
3. Explicitly block all other inbound access from ISP and any source beyond ISP.

- Use a standard or extended ACL? _____Extended
- Configure the ACL on which router? _____HQ
- Apply the ACL to which interface? _____S0/1/0
- Apply the ACL in which direction? _____In

_____

_____

_____

_____

_____

```
HQ(confi)#ip access-list extended FIREWALL
HQ(config-ext-nacl)#permit icmp any any echo-reply
HQ(config-ext-nacl)#permit tcp any any established
HQ(config-ext-nacl)#deny ip any any
HQ(config-ext-nacl)#interface s0/1/0
HQ(config-if)#ip access-group FIREWALL in
```

Step 13. Verify that security policy number 5 is implemented.

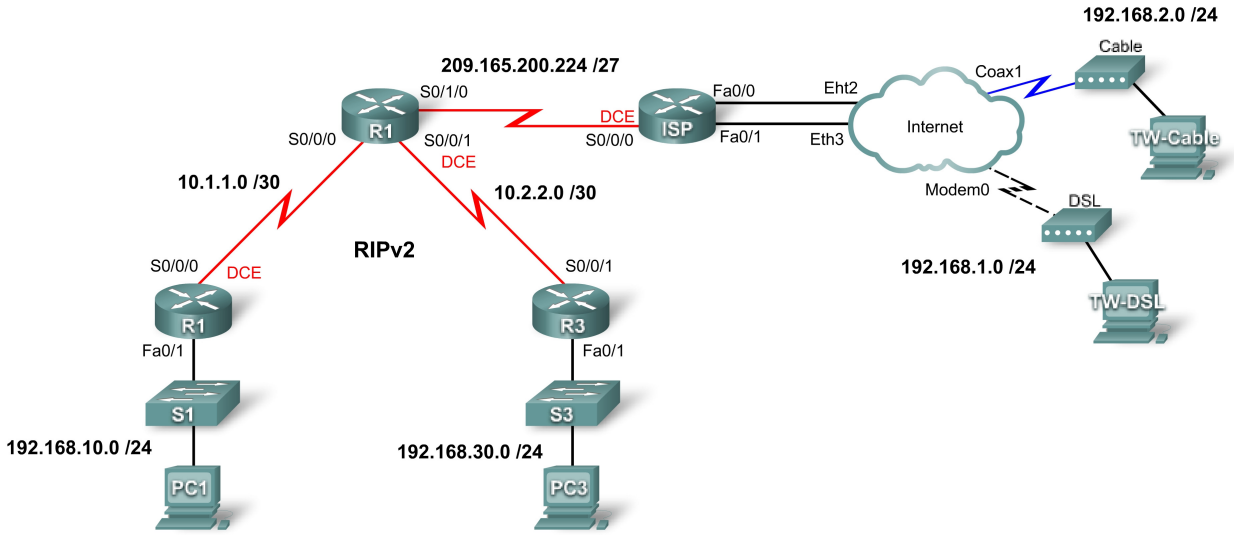
To test this policy, any PC should be able to ping ISP or Web Server. However, neither ISP nor Web Server should be able to ping HQ or any other device behind the ACL. **FIREWALL**

Step 14. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

PT Activity 6.2.4: Broadband Services (Instructor Version)

Topology Diagram



Learning Objectives

- Connect the ISP to the Internet cloud
- Add WAN devices
- Connect a WAN device to the Internet cloud
- Connect teleworker PCs to WAN devices
- Test connectivity

Introduction

In this activity, you will demonstrate your ability to add broadband devices and connections to Packet Tracer. Although you cannot configure DSL and cable modems, you can simulate end-to-end connectivity to teleworker devices.

Task 1: Connect the ISP to the Internet Cloud

Step 1. Make connections using the interfaces shown in the topology.

- Connect Fa0/0 on ISP to Eth2 on the Internet Cloud
- Connect Fa0/1 on ISP to Eth3 on the Internet Cloud

Step 2. Check results.

Your completion percentage should be 25%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Add WAN Devices

Step 1. Add DSL and cable devices.

The **DSL Modem** and **Cable Modem** devices are under the **WAN Emulation** menu. Place them as you would any other device.

Step 2. Name the WAN devices.

Use the Config tab to change the display name of each WAN device to **Cable** and **DSL,** respectively.

Task 3: Connect WAN Devices to the Internet Cloud

Step 1. Connect the cable modem to the Internet cloud.

Choose the **Coaxial** connection type from the **Connection** menu.

Step 2. Connect the DSL modem to the Internet cloud.

Choose the **Phone** connection type from the **Connection** menu.

Step 3. Check results

Your completion percentage should be 75%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Connect Teleworker PCs to WAN Devices

Step 1. Connect TW-Cable to Cable.

Step 2. Connect TW-DSL to DSL.

Step 3. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

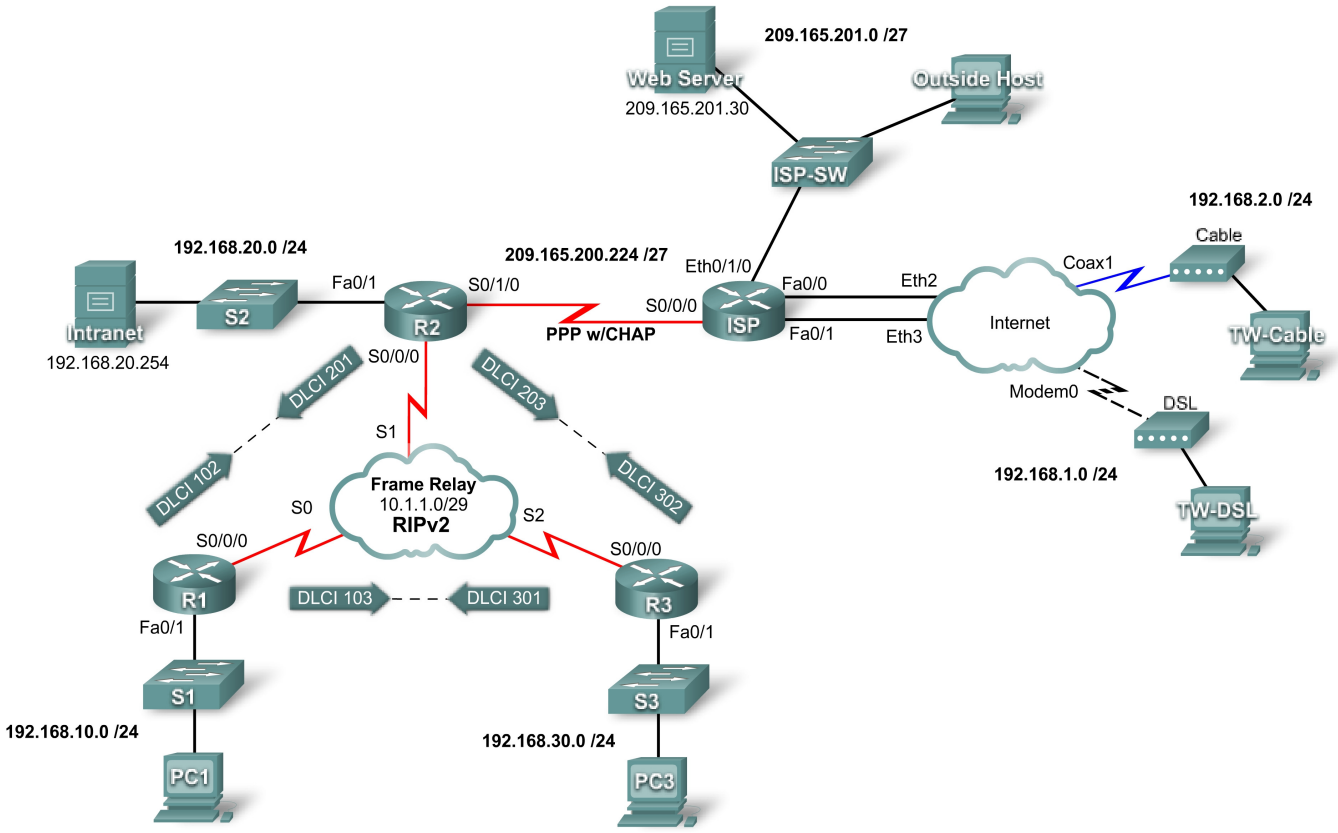
Task 5: Test Connectivity

Click **Check Results**, and then click the Connectivity Tests tab to verify that the Teleworker devices can communicate with the internal PCs.

Cisco | Networking Academy®
Mind Wide Open™

PT Activity 6.4.1: Packet Tracer Skills Integration Challenge (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	**Fa0/1**	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.248
R2	**Fa0/1**	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.248
	S0/1/0	209.165.200.225	255.255.255.224
R3	**Fa0/1**	192.168.30.1	255.255.255.0
	S0/0/0	10.1.1.3	255.255.255.248
ISP	**S0/0/0**	209.165.200.226	255.255.255.224
	Eth0/1/0	209.165.201.1	255.255.255.224
	Fa0/0	192.168.1.1	255.255.255.0
	Fa0/1	192.168.2.1	255.255.255.0
PC1	**NIC**	192.168.10.10	255.255.255.0
PC3	**NIC**	192.168.30.10	255.255.255.0
Intranet	**NIC**	192.168.20.254	255.255.255.0
TW-DSL	**NIC**	192.168.1.10	255.255.255.0
TW-Cable	**NIC**	192.168.2.10	255.255.255.0
Web Server	**NIC**	209.165.201.30	255.255.255.224
Outside Host	**NIC**	209.165.201.10	255.255.255.224

Learning Objectives

- Apply basic router configurations
- Configure dynamic and default routing
- Establish teleworker services
- Test connectivity before ACL configuration
- Apply ACL policies
- Test connectivity after ACL configuration

Introduction

This activity requires you to configure a default route as well as dynamic routing using RIP version 2. You will also add broadband devices to the network. Finally, you will set up ACLs on two routers to control network traffic. Because Packet Tracer is very specific in how it grades ACLs, you will need to configure the ACL rules in the order given.

Task 1: Apply Basic Router Configurations

Using the information in the topology diagram and addressing table, configure the basic device configurations on R1, R2, and R3. Hostnames are configured for you.

Include the following:

- Console and vty lines
- Banners
- Disable domain name lookup
- Interface descriptions

Task 2: Configure Dynamic and Default Routing

Step 1. Configure default routing.

R2 needs a default route. Use the *exit-interface* argument in the default route configuration.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0
```

Step 2. Configure dynamic routing.

Configure RIPv2 on R1, R2, and R3 for all available networks. R2 needs to pass its default network configuration to the other routers. Also, be sure to use the **passive-interface** command on all active interfaces not used for routing.

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.10.0
R1(config-router)#network 10.0.0.0
R1(config-router)#passive-interface fa0/1

R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 192.168.20.0
R2(config-router)#network 10.0.0.0
R2(config-router)#default-information originate
R2(config-router)#passive-interface fa0/1
R2(config-router)#passive-interface s0/1/0

R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#no auto-summary
R3(config-router)#network 192.168.30.0
R3(config-router)#network 10.0.0.0
R3(config-router)#passive-interface fa0/1
```

Step 3. Check results.

Your completion percentage should be 59%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Establish Teleworker Services

Step 1. Add WAN devices.

Add one DSL and one cable modem according to the topology diagram.

Step 2. Name the WAN devices.

Use the **Config** tab to change the display name of each WAN device to **Cable** and **DSL,** respectively.

Step 3. Connect the WAN devices.

Connect the WAN devices to their PCs and the Internet using the appropriate cables and interfaces.

Step 4. Check results.

Your completion percentage should be 86%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Test Connectivity Before ACL Configuration

At this point, all branches of the topology should have connectivity. Switching between Simulation mode and Realtime mode can speed up convergence.

Task 5: Apply ACL Policies

Step 1. Create and apply security policy number 1.

Implement the following ACL rules using ACL number 101:

1. Allow hosts on the 192.168.30.0/24 network web access to any destination
2. Allow hosts on the 192.168.30.0/24 network ping access to any destination.
3. Deny any other access originating from the network.

```
R3(config)#access-list 101 permit tcp 192.168.30.0 0.0.0.255 any eq www
R3(config)#access-list 101 permit icmp 192.168.30.0 0.0.0.255 any
R3(config)#access-list 101 deny ip any any
R3(config)#interface fa0/1
R3(config-if)#ip access-group 101 in
```

Step 2. Create and apply security policy number 2.

Because ISP represents connectivity to the Internet, configure a named ACL called **FIREWALL** in the following order:

1. Allow TW-DSL web access to the Intranet server.
2. Allow TW-Cable web access to the Intranet server.
3. Allow only inbound ping replies from ISP and any source beyond ISP.
4. Allow only established TCP sessions from ISP and any source beyond ISP.
5. Explicitly block all other inbound access from ISP and any source beyond ISP.

```
R2(config)#ip access-list extended FIREWALL
R2(config-ext-nacl)#permit tcp host 192.168.1.10 host 192.168.20.254 eq www
R2(config-ext-nacl)#permit tcp host 192.168.2.10 host 192.168.20.254 eq www
R2(config-ext-nacl)#permit icmp any any echo-reply
R2(config-ext-nacl)#permit tcp any any established
R2(config-ext-nacl)#deny ip any any
R2(config-ext-nacl)#interface s0/1/0
R2(config-if)#ip access-group FIREWALL in
```

Step 3. Check results.

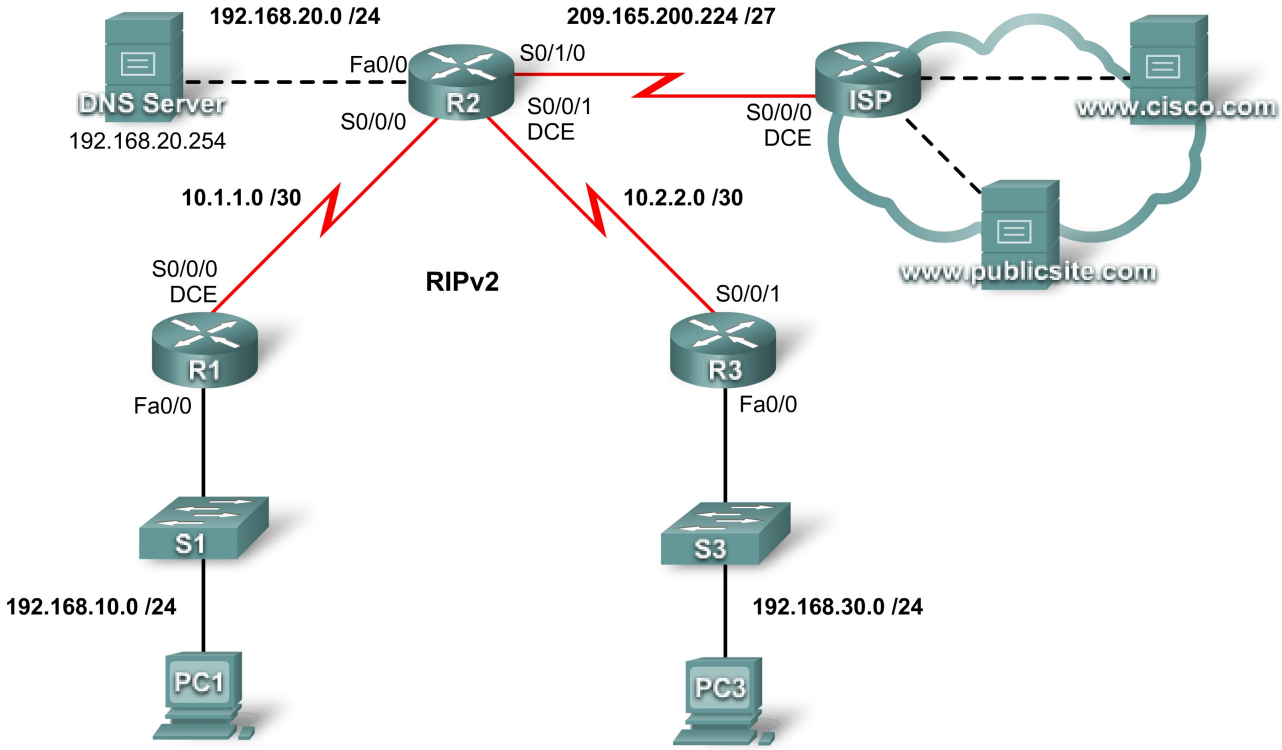
Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Test Connectivity After ACL Configuration

Teleworkers should not be able to ping the Intranet Server, but should be able to access its HTTP server via the web browser. Included in the activity are three PDUs, two of which should fail and one should succeed. Check the **Connectivity Tests** in the **Check Results** menu to be sure that the completion results are 100%.

PT Activity 7.1.8: Configuring DHCP Using Easy IP (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	Fa0/1	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	Fa0/0	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	225.255.255.224
R3	Fa0/1	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252

Learning Objectives

- Configure routers with Easy IP
- Verify that PCs are automatically configured with addressing details
- Configure a DNS server with DNS entries
- Test PC connectivity to domain names

Introduction

DHCP assigns IP addresses and other important network configuration information dynamically. Cisco routers can use the Cisco IOS feature set, Easy IP, as an optional, full-featured DHCP server. Easy IP leases configurations for 24 hours by default. In this activity, you will configure DHCP services on two routers and test your configuration.

Task 1: Configure Routers with Easy IP

Step 1. Configure the excluded addresses for R1 and R3.

Define a set of addresses that are reserved for hosts that need static addresses, such as servers, routers, and printers. These addresses are not included in the pool of addresses that are available for assigning to DHCP clients. For R1 and R3, exclude the first nine addresses from the DHCP pool.

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)#

R3(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.9
R3(config)#
```

Step 2. Configure the address pool for R1.

Define the pool of addresses from which DHCP assigns addresses to DHCP clients on the R1 LAN. The available addresses are all addresses on the 192.168.10.0 network, except for those excluded in Step 1.

On R1, name the address pool R1LAN. Specify the address pool, default gateway, and DNS server that are assigned to each client device requesting DHCP service.

```
R1(config)#ip dhcp pool R1LAN
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#dns-server 192.168.20.254
```

Step 3. Configure the address pool for R3 .

On R3, name the address pool R3LAN. Specify the address pool, default gateway, and DNS server that are assigned to each client device requesting DHCP service.

```
R3(config)#ip dhcp pool R3LAN
R3(dhcp-config)#network 192.168.30.0 255.255.255.0
R3(dhcp-config)#default-router 192.168.30.1
R3(dhcp-config)#dns-server 192.168.20.254
```

Step 4. Check results.

Your completion percentage should be 43%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Verify that the PCs Are Automatically Configured

Step 1. Configure PC1 and PC3 for DHCP configuration.

In the **Desktop** tab of each PC, click **IP Configuration**, and then select **DHCP**. The IP configuration information should be immediately updated.

Step 2. Check the DHCP operation on the routers.

To verify DHCP operation on the routers, issue the **show ip dhcp binding** command. The results should show one IP address bound on each of the routers.

Step 3. Check results.

Your completion percentage should be 86%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure a DNS Server with DNS Entries

Step 1. Configure the DNS server.

To configure DNS on the DNS server, click the **DNS** button in the **Config** tab.

Make sure that DNS is turned on, and enter the following DNS entries:

- www.cisco.com 209.165.201.30
- www.publicsite.com 209.165.202.158

Step 2. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Test PC Connectivity to Domain Names

Step 1. Verify that PC1 can connect to servers using the domain name.

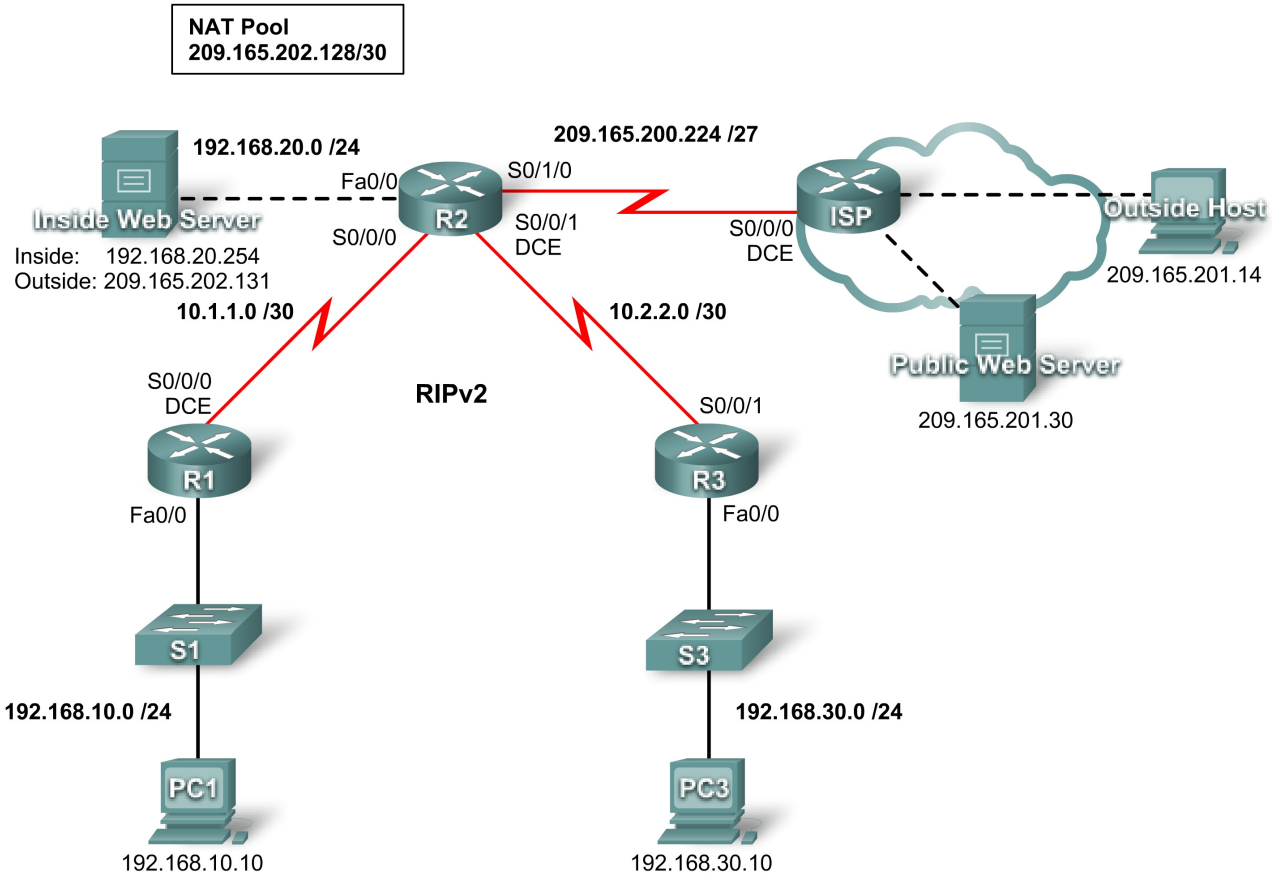
On PC1, open the web browser and enter **www.cisco.com** in the address line. The web page should appear.

Step 2. Verify that PC3 can connect to servers using domain name.

On PC3, open the web browser and enter **www.publicsite.com** in the address line. The web page should appear.

PT Activity 7.2.8: Scaling Networks with NAT (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	Fa0/1	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	Fa0/0	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
R3	Fa0/1	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252

Addressing Table continued on next page

Addressing Table continued

Inside Web Server	**NIC**	Local: 192.168.20.254	255.255.255.252
	NIC	Global: 209.165.202.131	255.255.255.252
PC1	**NIC**	192.168.10.10	255.255.255.0
PC3	**NIC**	192.168.30.10	255.255.255.0
Outside Host	**NIC**	209.165.201.14	255.255.255.240
Public Web Server	**NIC**	209.265.201.30	255.255.255.240

Learning Objectives

- Configure an ACL to permit NAT
- Configure static NAT
- Configure dynamic NAT Overload
- Configure the ISP router with static route
- Test connectivity

Introduction

NAT translates non-routable private, internal addresses into routable, public addresses. NAT has an added benefit of providing a degree of privacy and security to a network because it hides internal IP addresses from outside networks. In this activity, you will configure dynamic and static NAT.

Task 1: Configure an ACL to Permit NAT

Step 1. Create a named standard ACL.

To define the internal addresses that are translated to public addresses in the NAT process, create a named standard ACL called R2NAT. This list is used in the NAT configuration steps that follow.

```
R2(config)#ip access-list standard R2NAT
R2(config-std-nacl)# permit 192.168.10.0 0.0.0.255
R2(config-std-nacl)# permit 192.168.20.0 0.0.0.255
R2(config-std-nacl)# permit 192.168.30.0 0.0.0.255
```

Step 2. Check results.

Your completion percentage should be 11%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure Static NAT

Step 1. Configure static NAT for an inside web server.

The Inside Web Server needs to have a public IP address that never changes so that it can be accessed from outside the network. Configuring a static NAT address allows the web server to be configured with a private internal address. The NAT process then always maps packets using the public address of the server to the private address.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.202.131
```


Step 2. Check results.

Your completion percentage should be 22%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure Dynamic NAT Overload

In addition to the public IP address assigned to Inside Web Server, the ISP has assigned three public addresses for your use. These addresses are mapped to all other internal hosts that access the Internet.

To allow more than three internal hosts to access the Internet at the same time, configure NAT with overload to accommodate the additional hosts. NAT overload, also called Port Address Translation (PAT), uses port numbers to distinguish packets from different hosts that are assigned the same public IP address.

Step 1. Define the address pool and configure dynamic NAT.

Enter the following commands to configure the pool of public addresses that are dynamically mapped to the internal hosts.

The first command defines the pool of three public addresses that are mapped to internal addresses.

The second command instructs the NAT process to map the addresses in the pool to the addresses defined in the access list you created in Task 1.

```
R2(config)#ip nat pool R2POOL 209.165.202.128 209.165.202.130 netmask
255.255.255.252
R2(config)#ip nat inside source list R2NAT pool R2POOL overload
```

Step 2. Configure the interfaces on R2 to apply NAT.

In interface configuration mode on R2, configure each of the interfaces using the **ip nat** {**inside** | **outside**} command. Because the internal addresses are on networks connected to the Fa0/0, Serial 0/0/0, and Serial0/0/1 interfaces, use the **ip nat inside** command in configuring these interfaces. The Internet is connected to Serial0/1/0, so use the **ip nat outside** command on this interface.

Step 3. Check results.

Your completion percentage should be 89%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure the ISP with a Static Route

Step 1. Configure ISP with a static route to R2.

ISP needs a static route to the public addresses of R2. Use the following command to configure this route.

```
ISP(config)#ip route 209.165.202.128 255.255.255.224 serial0/0/0
```

Step 2. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Test Connectivity

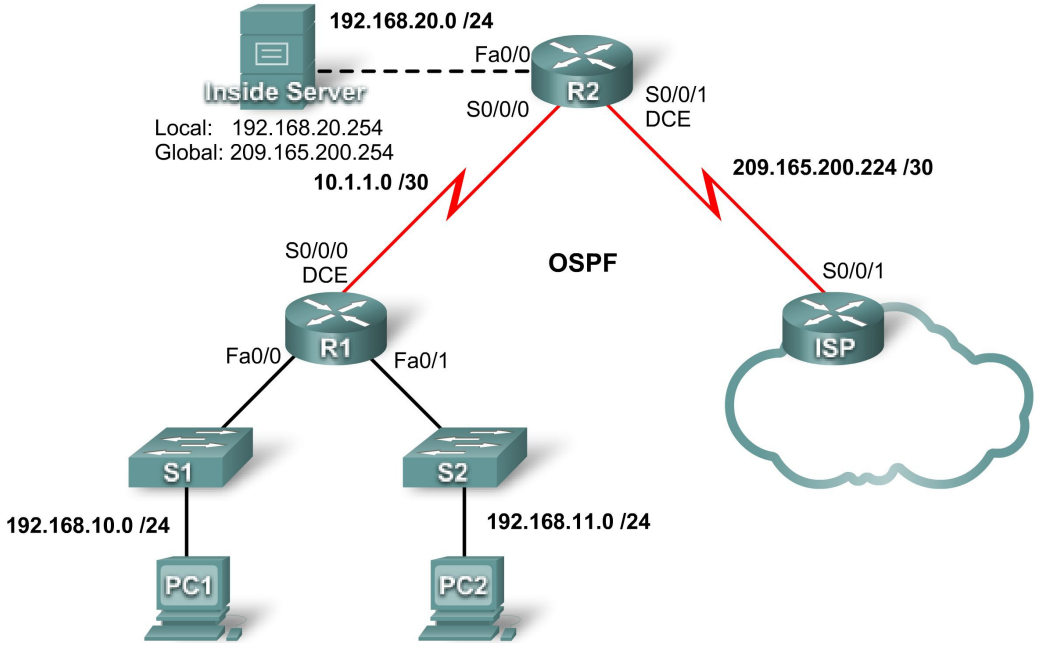
You should now be able to ping from any inside host to Outside Host or Public Web Server.

To see the effects of NAT on a specific packet, enter Simulation mode and observe the packet that originates from PC1.

Click the colored information box associated with that packet as it is passed from R1 to R2. By clicking **Inbound PDU Details**, you should see that the source address is 192.168.10.10. By clicking **Outbound PDU Details**, you should see that the source address has been translated to a 209.165.x.x address.

Activity 7.4.1: Basic DHCP and NAT Configuration (Instructor)

Topology Diagram



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	192.168.20.1	255.255.255.0
ISP	**S0/0/1**	209.165.200.226	255.255.255.252

Learning Objectives

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

- Prepare the network
- Perform basic router configurations
- Configure a Cisco IOS DHCP server
- Configure static and default routing
- Configure static NAT
- Configure dynamic NAT with a pool of addresses

- Configure NAT overload

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: 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 activity.
- Enable OSPF with process ID 1 on R1 and R2. Do not advertise the 209.165.200.224/27 network.

For all devices:

```
enable
conf t
no ip domain-lookup
enable secret class
banner motd $Authorized Access Only!$
!
line con 0
logging synchronous
 password cisco
 login
!
line vty 0 4
 password cisco
 login
end
copy run start
```

R1:

```
hostname R1
int fa0/0
 ip address 192.168.10.1 255.255.255.0
 no shut
int fa0/1
 ip address 192.168.11.1 255.255.255.0
 no shut
int s0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 125000
 no shut
```



```
!
router ospf 1
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
 network 10.1.1.0 0.0.0.3 area 0
```

R2:

```
hostname R2
int fa0/0
 ip address 192.168.20.1 255.255.255.0
 no shut
int s0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shut
int s0/0/1
 ip address 209.165.200.225 255.255.255.252
 clock rate 125000
 no shut
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
```

ISP:

```
hostname ISP
int s0/0/1
 ip address 209.165.200.226 255.255.255.252
 no shut
!
```

Task 2: Configure a Cisco IOS DHCP Server

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 address 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.

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R1(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**.

```
R1(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.

```
R1(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.

```
R1(dhcp-config)#dns-server 192.168.11.5
R1(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.

```
R1(config)#ip dhcp pool R1Fa1
R1(dhcp-config)#network 192.168.11.0 255.255.255.0
R1(dhcp-config)#dns-server 192.168.11.5
R1(dhcp-config)#default-router 192.168.11.1
```

Step 3: Verify the DHCP configuration.

You can verify the DHCP server configuration in several different ways. The most basic way is to configure a host on the subnet to receive an IP address via DHCP. 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 pm.

```
R1#show ip dhcp binding
IP address Client-ID/ Lease expiration Type
Hardware address
192.168.10.11 0007.EC66.8752 -- Automatic
192.168.11.11 00E0.F724.8EDA -- Automatic
```

Task 3: 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 R2 (209.165.200.225). The pings should be successful. Troubleshoot if the pings fail.

Task 4: 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
```

Step 3: Verify the static NAT configuration.

From ISP, ping the public IP address 209.165.200.254.

Task 5: 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 a standard access control list to identify which inside addresses are translated.

```
R2(config)#ip access-list extended NAT
R2(config-std-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-std-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 and PC2. Then use the **show ip nat translations** command on R2 to verify NAT.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.241   192.168.10.11      ---                ---
---  209.165.200.242   192.168.11.11      ---                ---
---  209.165.200.254   192.168.20.254     ---                ---
```


Task 6: 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 pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL
```

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 and PC2. Then use the **show ip nat translations** command on R2 to verify NAT.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.225:3 192.168.10.11:3    209.165.200.226:3
209.165.200.226:3
icmp 209.165.200.225:1024192.168.11.11:3    209.165.200.226:3
209.165.200.226:1024
---  209.165.200.254   192.168.20.254     ---                ---
```

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 7: Document the Network

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

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.

Note: If you use a 1700, 2500, or 2600 series router, the router outputs and interface descriptions may look different.

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 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. 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 4. Verify the DHCP configuration.

You can verify the DHCP server configuration in several different ways. The most basic way is to configure a host on the subnet to receive an IP address via DHCP. 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
Bindings from all pools not associated with VRF:
IP address        Client-ID/            Lease expiration        Type
                  Hardware address/
                  User name
192.168.10.11     0063.6973.636f.2d30.  Sep 14 2007 07:33 PM    Automatic
                  3031.632e.3537.6563.
                  2e30.3634.302d.566c.
                  31
```

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
Pool R1Fa0 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range                    Leased addresses
 192.168.10.12        192.168.10.1     - 192.168.10.254    1
```

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

```
*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER:
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80b01010000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: Seeing if there is an internally specified pool
class:
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80b01010000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: there is no address pool for 192.168.11.1.
*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER:
R1#
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80a01000000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: Seeing if there is an internally specified pool
class:
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80a01000000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
R1#
*Sep 13 21:04:20.072: DHCPD: Adding binding to radix tree (192.168.10.12)
*Sep 13 21:04:20.072: DHCPD: Adding binding to hash tree
*Sep 13 21:04:20.072: DHCPD: assigned IP address 192.168.10.12 to client
0063.6973.636f.2d30.3031.632e.3537.6563.2e30.3634.302d.566c.31.
*Sep 13 21:04:20.072: DHCPD: Sending notification of ASSIGNMENT:
*Sep 13 21:04:20.072:   DHCPD: address 192.168.10.12 mask 255.255.255.0
*Sep 13 21:04:20.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:20.072:   DHCPD: lease time remaining (secs) = 86400
*Sep 13 21:04:20.076: DHCPD: Sending notification of ASSIGNMENT:
*Sep 13 21:04:20.076:   DHCPD: address 192.168.10.12 mask 255.255.255.0
R1#
*Sep 13 21:04:20.076:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:20.076:   DHCPD: lease time remaining (secs) = 86400
```

Task 4: 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 0.0.0.0 209.165.200.225
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 R2 (209.165.200.226). The pings should be successful. Troubleshoot if the pings fail.

Task 5: 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 6: 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
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.241:4 192.168.10.1:4     209.165.200.226:4  209.165.200.226:4
--- 209.165.200.241    192.168.10.1       ---                ---
--- 209.165.200.254    192.168.20.254     ---                ---

R2#show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 0 extended)
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0, Loopback0
Hits: 23  Misses: 3
CEF Translated packets: 18, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NAT pool MY-NAT-POOL refcount 1
 pool MY-NAT-POOL: netmask 255.255.255.248
        start 209.165.200.241 end 209.165.200.246
        type generic, total addresses 6, allocated 1 (16%), misses 0
Queued Packets: 0
```

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
IP NAT debugging is on
R2#
*Sep 13 21:15:02.215: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [25]
*Sep 13 21:15:02.231: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [25]
*Sep 13 21:15:02.247: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [26]
*Sep 13 21:15:02.263: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [26]
*Sep 13 21:15:02.275: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [27]
*Sep 13 21:15:02.291: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [27]
*Sep 13 21:15:02.307: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [28]
*Sep 13 21:15:02.323: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [28]
*Sep 13 21:15:02.335: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [29]
*Sep 13 21:15:02.351: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [29]
```



```
R2#
```

Task 7: Configure NAT Overload

In the previous example, what would happen if you needed more than the six public IP addresses that the pool allows?

_____

The seventh and subsequent users would not be able to access destinations beyond R2.

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 pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL
```

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
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:6 192.168.10.11:6    209.165.200.226:6  209.165.200.226:6
--- 209.165.200.254    192.168.20.254     ---                ---

R2#show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0, Loopback0
Hits: 48  Misses: 6
CEF Translated packets: 46, CEF Punted packets: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
```



```
[Id: 2] access-list NAT interface Serial0/0/1 refcount 1
Queued Packets: 0
```

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 8: Document the Network

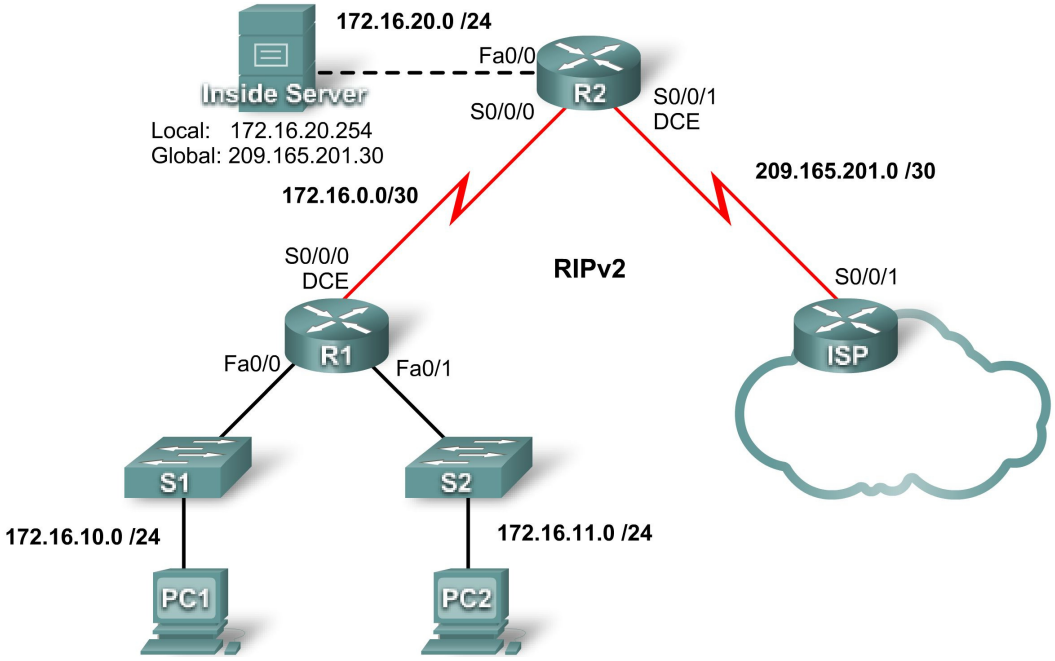
On each router, issue the **show run** command and capture the configurations.

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.

Activity 7.4.2: Challenge DHCP and NAT Configuration (Instructor)

Topology Diagram



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

Learning Objectives

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

- Prepare the network
- Perform basic router configurations
- Configure a Cisco IOS DHCP server
- Configure static and default routing
- Configure static NAT

- Configure dynamic NAT with a pool of addresses
- Configure NAT overload

Scenario

In this lab, configure the IP address services using the network shown in the topology diagram. If you need assistance, refer back to the basic DHCP and NAT configuration lab. However, try to do as much on your own as possible.

Task 1: 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 RIPv2 on R1 and R2. Do not advertise the 209.165.200.224/27 network.

For all devices:

```
enable
conf t
no ip domain-lookup
enable secret class
banner motd $Authorized Access Only!$
!
line con 0
logging synchronous
 password cisco
 login
!
line vty 0 4
 password cisco
 login
end
copy run start
```

R1:

```
hostname R1
int fa0/0
 ip address 172.16.10.1 255.255.255.0
 no shut
int fa0/1
 ip address 172.16.11.1 255.255.255.0
 no shut
int s0/0/0
 ip address 172.16.0.1 255.255.255.252
 clock rate 125000
 no shut
!
router rip
```



```
 version 2
 network 172.16.0.0
 no auto-summary
```

R2:

```
hostname R2
int fa0/0
 ip address 172.16.20.1 255.255.255.0
 no shut
int s0/0/0
 ip address 172.16.0.2 255.255.255.252
 no shut
int s0/0/1
 ip address 209.165.201.1 255.255.255.252
 clock rate 125000
 no shut
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
```

ISP:

```
hostname ISP
int s0/0/1
 ip address 209.165.201.2 255.255.255.252
 no shut
!
```

Task 2: Configure a Cisco IOS DHCP Server

Configure R1 as the DHCP server for the two directly attached LANs.

Step 1. Exclude statically assigned addresses.

Exclude the first three addresses from each pool.

```
R1(config)#ip dhcp excluded-address 172.16.10.1 172.16.10.3
R1(config)#ip dhcp excluded-address 172.16.11.1 172.16.11.3
```

Step 2. Configure the DHCP pool.

- Create two DHCP pools. Name one of them **R1_LAN10** for the 172.16.10.0/24 network, and name the other **R1_LAN11** for the 172.16.11.0/24 network.
- Configure each pool with a default gateway and a simulated DNS at 172.16.20.254.

```
R1(config)#ip dhcp pool R1_LAN10
R1(dhcp-config)#network 172.16.10.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.10.1
R1(dhcp-config)#dns-server 172.16.20.254
R1(dhcp-config)#ip dhcp pool R1_LAN11
R1(dhcp-config)#network 172.16.11.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.11.1
R1(dhcp-config)#dns-server 172.16.20.254
```


Step 3. Verify the DHCP configuration.

```
R1#show ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
172.16.10.4      00E0.F70C.7E1E           --                     Automatic
172.16.11.4      0009.7CB0.39E6           --                     Automatic
```

Task 3: Configure Static and Default Routing

- Configure ISP with a static route for the 209.165.201.0/27 network. Use the exit interface as an argument.

```
ISP(config)#ip route 209.165.201.0 255.255.255.224 serial 0/0/1
```

- Configure a default route on R2 and propagate the route in OSPF. Use the next-hop IP address as an argument.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
R2(config)#router rip
R2(config-router)#default-information originate
```

Task 4: Configure Static NAT

Step 1. Statically map a public IP address to a private IP address.

Statically map the inside server IP address to the public address 209.165.201.30.

```
R2(config)#ip nat inside source static 172.16.20.254 209.165.201.30
```

Step 2. Specify inside and outside NAT interfaces.

```
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
```

Step 3. Verify the static NAT configuration.

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.201.30    172.16.20.254      ---                ---
```

Task 5: Configure Dynamic NAT with a Pool of Addresses

Step 1. Define a pool of global addresses.

Create a pool named **NAT_POOL** for the IP addresses 209.165.201.9 through 209.165.201.14 using a /29 subnet mask.

```
R2(config)#ip nat pool NAT_POOL 209.165.201.9 209.165.201.14 netmask
255.255.255.248
```

Step 2. Create a standard named access control list to identify which inside addresses are translated.

Use the name **NAT_ACL** and allow all hosts attached to the two LANs on R1.

Note: The **.10** LAN must be configured first, then the **.11** LAN. Otherwise, Packet Tracer will not grade the ACL as correct.

```
R2(config)#ip access-list standard NAT_ACL
R2(config-std-nacl)#permit 172.16.10.0 0.0.0.255
R2(config-std-nacl)#permit 172.16.11.0 0.0.0.255
```

Step 3. Establish dynamic source translation.

Bind the NAT pool to the ACL and allow NAT overloading.

```
R2(config)#ip nat inside source list NAT_ACL pool NAT_POOL overload
```

Step 4. Specify the inside and outside NAT interfaces.

Verify that the inside and outside interfaces are all correctly specified.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```

Step 5. Verify the dynamic NAT configuration by pinging from PC1 and PC2 to ISP.

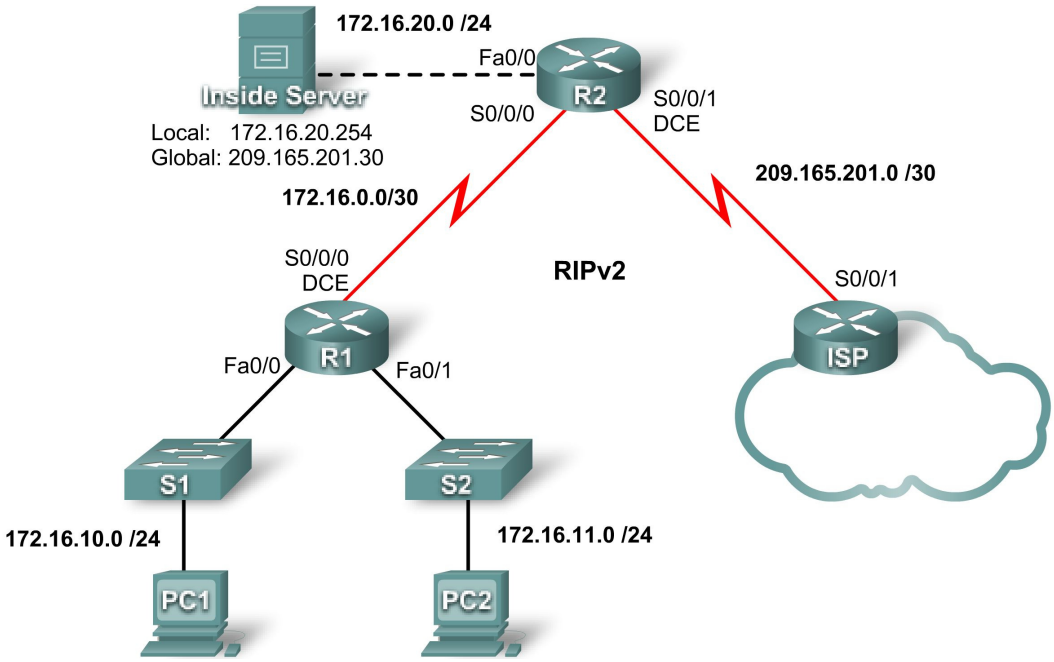
```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.201.9:2   172.16.10.4:2      209.165.201.2:2    209.165.201.2:2
icmp 209.165.201.9:1024172.16.11.4:2      209.165.201.2:2    209.165.201.2:1024
---  209.165.201.30    172.16.20.254      ---                ---
```

Task 6: Document the Network

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

PT Activity 7.4.3: Troubleshooting DHCP and NAT (Instructor)

Topology Diagram



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

Learning Objectives

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

- Find and correct network errors
- Document the corrected network

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 DHCP, NAT, and standard testing methods, find and correct the errors. Make sure all clients have full connectivity.

Task 1: Find and Correct Network Errors

Use troubleshooting commands to discover errors and then correct them. When all errors are corrected, you should be able to ping from PC1 and PC2 to ISP. ISP should be able to ping the inside web server at its public IP address.

The following errors are in the activity:

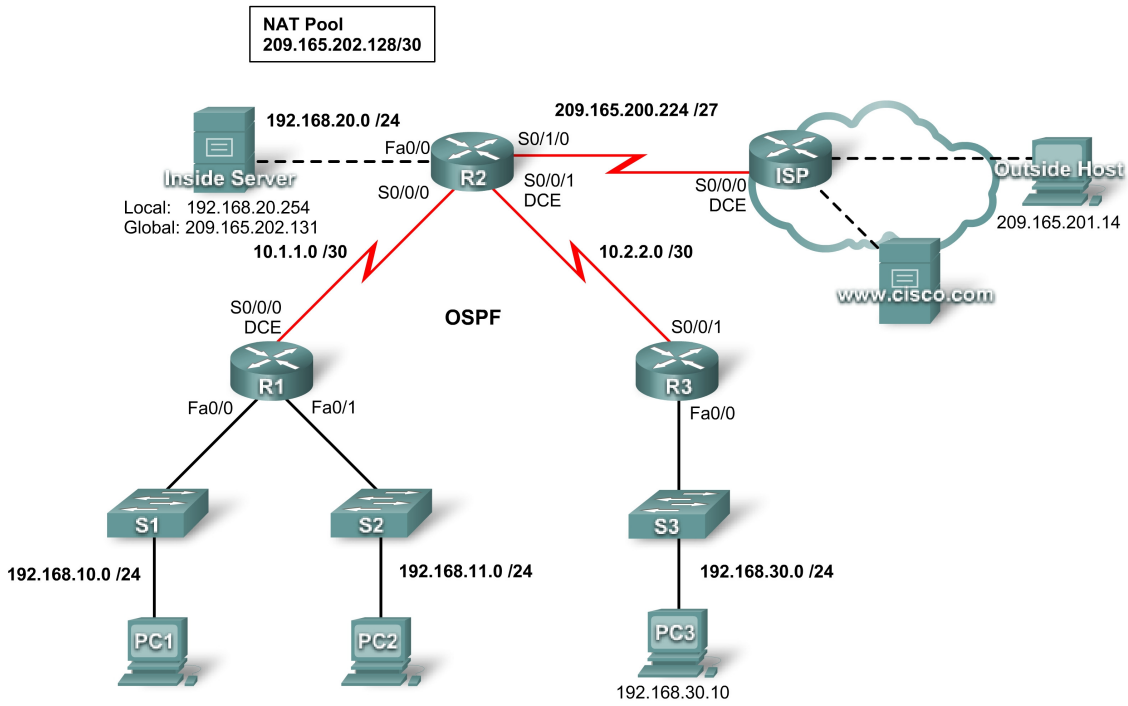
- R1 is missing the **no shutdown** command on the serial 0/0/0 interface.
- The ACL on R2 is missing a permit statement for the .11 network.
- R2 is missing the **ip nat inside** command on the serial 0/0/0 interface.
- R2 is missing the **default-information originate** command in the RIP configuration.

Task 2: Document the Corrected Network

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

PT Activity 7.5.1: Packet Tracer Skills Integration Challenge (Instructor Version)

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	Fa0/0	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	225.255.255.224
R3	Fa0/1	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252
Inside Server	NIC	Local: 192.168.20.254	255.255.255.0
	NIC	Global: 209.165.202.131	255.255.255.252
Outside Host	NIC	209.165.201.14	255.255.255.240

Learning Objectives

- Apply basic configurations
- Configure PPP encapsulation with CHAP
- Configure dynamic and default routing
- Configure routers with Easy IP
- Verify PCs are automatically configured with addressing details
- Configure a DNS server with DNS entries
- Configure an ACL to permit NAT
- Configure static NAT
- Configure dynamic NAT with overload
- Configure the ISP router with a static route
- Test connectivity

Introduction

In this culminating activity, you will configure PPP, OSPF, DHCP, NAT and default routing to ISP. You will then verify your configuration.

Task 1: Apply Basic Configurations

Step 1. Configure R1, R2, and R3 with the basic global configuration.

- Hostname as listed in the addressing table
- Console line for login with password **cisco**
- vtys 0–4 for login with password **cisco**
- Secret password **class**
- Banner of “AUTHORIZED ACCESS ONLY!”

Only the hostname and banner are graded.

Step 2. Configure the interfaces on R1, R2, and R3.

Use the addressing table to determine the interface addresses. Use the topology diagram to determine which interfaces are DCE interfaces. Configure the DCE interfaces for a clock rate of 64000.

Step 3. Check results.

Your completion percentage should be 38%. If not, click **Check Results** to see which required components are not yet completed.

Task 2: Configure PPP Encapsulation with CHAP

Step 1. Configure the link between R1 and R2 to use PPP encapsulation with CHAP authentication.

The password for CHAP authentication is **cisco123**.

Step 2. Configure the link between R2 and R3 to use PPP encapsulation with CHAP authentication.

The password for CHAP authentication is **cisco123**.

Step 3. Verify that connectivity is restored between the routers.

R2 should be able to ping both R1 and R3. The interfaces may take a few minutes to come back up. You can switch back and forth between Realtime and Simulation modes to speed up the process. Another possible workaround to this Packet Tracer behavior is to use the **shutdown** and **no shutdown** commands on the interfaces.

Note: The interfaces may go down at random points during the activity because of a Packet Tracer bug. The interface normally comes back up on its own if you wait a few seconds.

Step 4. Check results.

Your completion percentage should be 51%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure Dynamic and Default Routing

Step 1. Configure R1, R2, and R3 to use the OSPF routing protocol.

- Use a process ID of 1 when configuring OSPF on the routers.
- Advertise all networks connected to R1 and R3, but do not send routing updates out the LAN interfaces.
- On R2, do not advertise the 209.165.200.224 network, and do not send routing updates out the Fa0/0 or the Serial0/1/0 interfaces.

Step 2. Configure a default route on R2.

Configure a default route to ISP, specifying the outgoing interface on R2 as the next-hop address.

Step 3. Configure OSPF to advertise the default route.

On R2, enter the command to advertise the default route to R1 and R3 via OSPF.

Step 4. Check results.

Your completion percentage should be 66%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure Routers with Easy IP

Step 1. Configure R1 to act as a DHCP server for the 192.168.10.0 and 192.68.11.0 networks.

- Name the DHCP pool for the 192.168.10.0 network **R1LAN1**. For the 192.168.11.0 network, use the name **R1LAN2**.
- Exclude the first nine addresses on each network from dynamic assignment.
- In addition to the IP address and subnet mask, assign the default gateway and DNS server addresses.

Step 2. Configure R3 to act as a DHCP server for the 192.168.30.0 network.

- Name the DHCP pool for the 192.168.30.0 network **R3LAN**.
- Exclude the first nine addresses on each network from dynamic assignment.
- In addition to the IP address and subnet mask, assign the default gateway and DNS server addresses.

Step 3. Check results.

Your completion percentage should be 75%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Verify that PCs Are Automatically Configured with Addressing Details

Step 1. Configure PC1, PC2, and PC3 for automatic IP configuration using DHCP.

Step 2. Verify that each PC has an address assigned from the correct DHCP pool.

Step 3. Check results.

Your completion percentage should be 88%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Configure a DNS Server with DNS Entries

Step 1. Configure the DNS server.

To configure DNS on the Inside Server, click the **DNS** button in the **Config** tab.

Make sure that DNS is turned on, and enter the following DNS entry:

- www.cisco.com 209.165.201.30

Step 2. Check results.

You will not be able to ping the **www.cisco.com** server by domain name until you configure the static route in Task 10. Your completion percentage should be 90%. If not, click **Check Results** to see which required components are not yet completed.

Task 7: Configure an ACL to Permit NAT

Step 1. Create a standard named ACL.

Create the standard named ACL, **R2NAT**, which permits all the internal networks to be mapped by NAT.

Note: For Packet Tracer to grade this task correctly, you must enter the permitted networks in the following order:

- 192.168.10.0
- 192.168.20.0
- 192.168.30.0
- 192.168.11.0

Step 2. Check results.

Your completion percentage should be 91%. If not, click **Check Results** to see which required components are not yet completed.

Task 8: Configure Static NAT

Step 1. Configure static NAT for an inside web server.

Configure static NAT to map the local IP address and global IP addresses for Inside Server. Use the addresses listed in the addressing table.

Step 2. Check results.

Your completion percentage should be 92%. If not, click **Check Results** to see which required components are not yet completed.

Task 9: Configure Dynamic NAT with Overload

Step 1. Configure the dynamic NAT pool.

Configure a dynamic NAT address pool using the Nat Pool specified in the topology diagram. Name the address pool **R2POOL**.

Step 2. Configure the dynamic NAT mapping.

Map the addresses in R2POOL to the networks defined above in R2NAT.

Step 3. Apply NAT to the internal and external interfaces of R2.

Step 4. Check results.

Your completion percentage should be 99%. If not, click **Check Results** to see which required components are not yet completed.

Task 10: Configure the ISP Router with a Static Route

Step 1. Configure a static route to the global IP addresses of R2.

This is the 209.165.202.128/27 network. Use the serial interface of ISP as the next-hop address.

Step 2. Check results.

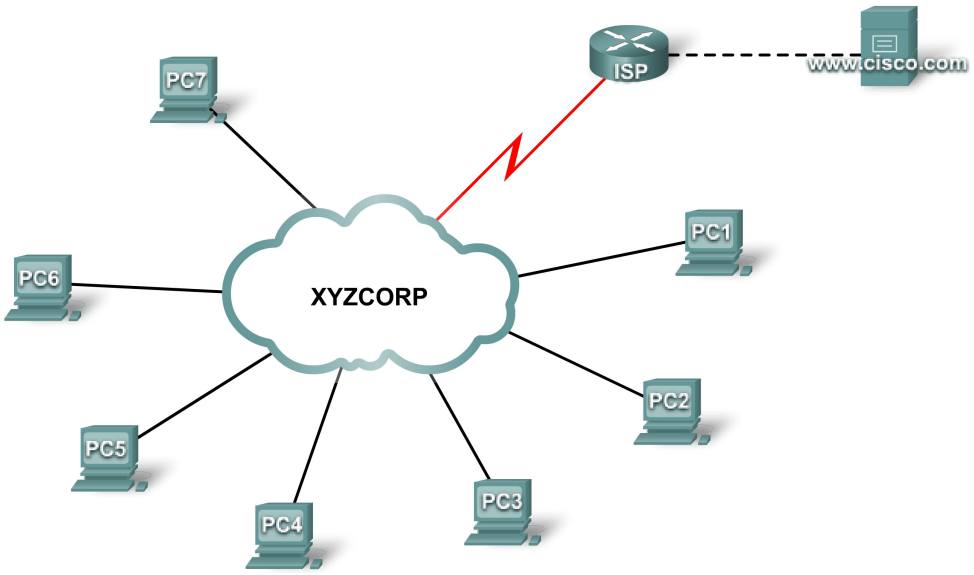
Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 11: Test Connectivity

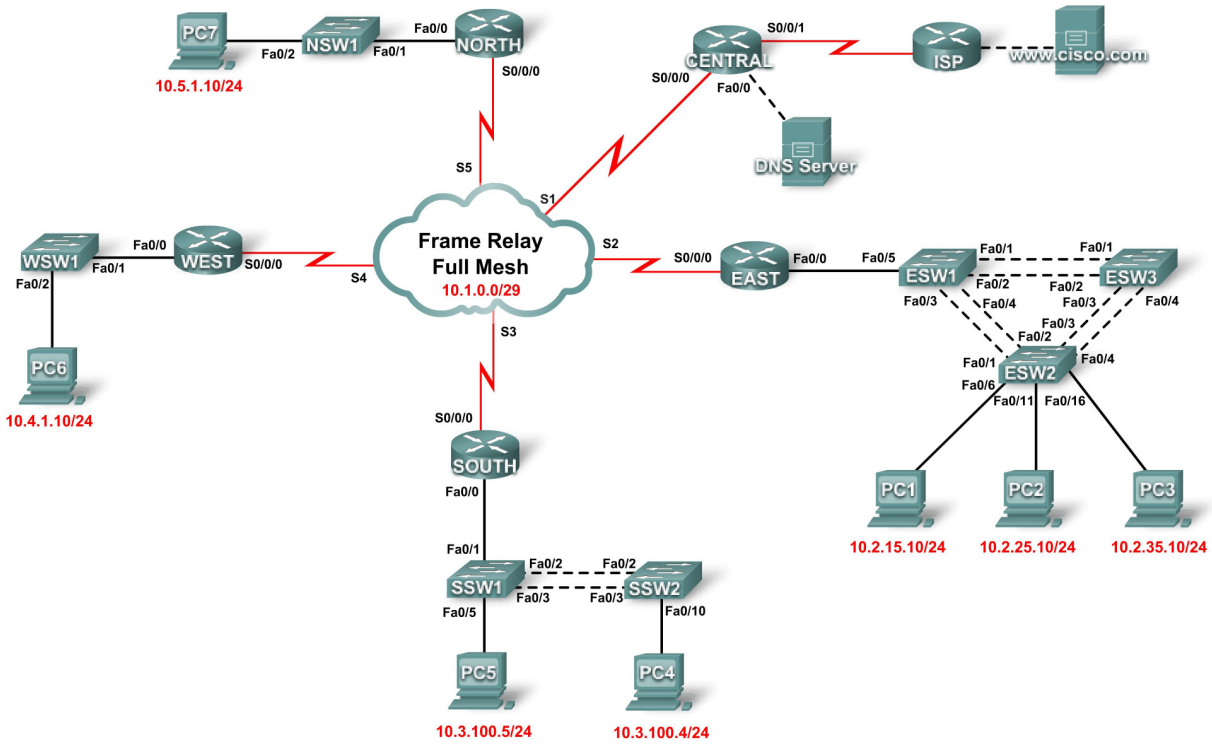
- Inside hosts should be able to ping Outside Host.
- Inside hosts should be able to ping www.cisco.com.
- Outside Host should be able to ping Inside Server by its global IP address.

PT Activity 8.1.2: Network Discovery and Documentation (Instructor Version)

Topology Diagram



Topology Diagram (Instructor only)



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10.2.15.10	255.255.255.0	10.2.15.1
PC2	NIC	10.2.25.10	255.255.255.0	10.2.25.1
PC3	NIC	10.2.35.10	255.255.255.0	10.2.35.1
PC4	NIC	10.3.100.4	255.255.255.0	10.3.100.1
PC5	NIC	10.3.100.5	255.255.255.0	10.3.100.1
PC6	NIC	10.4.1.10	255.255.255.0	10.4.1.1
PC7	NIC	10.5.1.10	255.255.255.0	10.5.1.1
DNS Server	NIC	10.1.100.2	255.255.255.0	10.1.100.1
CENTRAL	S0/0/0	10.1.0.1	255.255.255.248	N/A
CENTRAL	S0/0/1	209.165.201.2	255.255.255.252	N/A
CENTRAL	Fa0/0	10.1.100.1	255.255.255.0	N/A
EAST	S0/0/0	10.1.0.2	255.255.255.248	N/A
EAST	Fa0/0.5	10.2.5.1	255.255.255.0	N/A
EAST	Fa0/0.15	10.2.15.1	255.255.255.0	N/A
EAST	Fa0/0.25	10.2.25.1	255.255.255.0	N/A
EAST	Fa0/0.35	10.2.35.1	255.255.255.0	N/A
ESW1	VLAN 5	10.2.5.21	255.255.255.0	10.2.5.1
ESW2	VLAN 5	10.2.5.22	255.255.255.0	10.2.5.1
ESW3	VLAN 5	10.2.5.23	255.255.255.0	10.2.5.1
SOUTH	S0/0/0	10.1.0.3	255.255.255.248	N/A
SOUTH	Fa0/0.100	10.3.100.1	255.255.255.0	N/A
SOUTH	Fa0/0.105	10.3.105.1	255.255.255.0	N/A
SSW1	VLAN 105	10.3.105.21	255.255.255.0	10.3.105.1
SSW2	VLAN 105	10.3.105.22	255.255.255.0	10.3.105.1
WEST	S0/0/0	10.1.0.4	255.255.255.248	N/A
WEST	Fa0/0	10.4.1.1	255.255.255.0	N/A
WSW1	None	None	None	None
NORTH	S0/0/0	10.1.0.5	255.255.255.248	N/A
NORTH	Fa0/0	10.5.1.1	255.255.255.0	N/A
NSW1	None	None	None	None

Learning Objectives

- Test connectivity

- Discover PC configuration information
- Discover the configuration information of the default gateway
- Discover routes and neighbors in the network
- Draw the network topology

Introduction

This activity covers the steps to take to discover a network using primarily the **telnet**, **show cdp neighbors detail**, and **show ip route** commands. This is Part I of a two-part activity.

The topology you see when you open the Packet Tracer activity does not reveal all of the details of the network. The details have been hidden using the cluster function of Packet Tracer. The network infrastructure has been collapsed, and the topology in the file shows only the end devices. Your task is to use your knowledge of networking and discovery commands to learn about the full network topology and document it.

Task 1: Test Connectivity

Step 1. Converge and test the network.

Packet Tracer needs a little help to converge the network. Ping between the PCs and between the PCs and the www.cisco.com server to speed up convergence and to test the network. All PCs should be able to ping one another as well as the server. Remember it may take a few pings before they are successful.

Task 2: Discover PC Configuration Information

Step 1. Access the PC1 command prompt.

Click **PC1**, the **Desktop** tab, and then **Command Prompt**.

Step 2. Determine the addressing information for PC1.

To determine the current IP addressing configuration, enter the **ipconfig /all** command.

Note: In Packet Tracer, you must enter a space between **ipconfig** and /**all**.

Step 3. Document the information for PC1 in the addressing table.

Step 4. Repeat for the other PCs.

Repeat steps 1-3 for PCs 2-7.

Task 3: Discover the Configuration Information of the Default Gateway

Step 1. Test connectivity between PC1 and its default gateway.

From PC1, ping the default gateway to ensure you have connectivity.

Step 2. Telnet to the default gateway.

Use the **telnet** *ip-address* command. The IP address is that of the default gateway. When prompted for the password, type **cisco**.

Step 3. View current interface configurations.

Use both the **show ip interface brief** and **show protocols** command to determine the current interface configurations.

What is the difference between these two commands?

_____

The show protocols command shows the subnet mask information.

Step 4. Document the hostname and interface configuration in the addressing table.

Use the following space to sketch a rough draft of the topology.

Topology Rough Draft

Task 4: Discover Routes and Neighbors in the Network

Step 1. On the same router, display the routing table.

Display the routing table with the **show ip route** command. You should see five connected routes and six routes learned through RIP, one of which is a default route.

In addition to the routes, what other useful information does the routing table provide to help you further discover and document the network?

There are four IP addresses you can telnet to continue discovering the network.

Step 2. Discover directly connected Cisco devices.

On the same router, use the **show cdp neighbors detail** command to discover other directly connected Cisco devices.

Step 3. Document the neighbor information and test connectivity.

The **show cdp neighbors detail** command lists information for one neighbor, including its IP address. Document the hostname and IP address of the neighbor. Then ping the IP address to test connectivity. The first two or three pings fail while ARP resolves the MAC address.

Step 4. Telnet to the neighbor and discover directly connected Cisco devices.

Telnet to the neighbor and use the **show cdp neighbors detail** command to discover other directly connected Cisco devices.

You should see three devices listed this time. Why is the router listed more than once?

The EAST router is listed once for each subinterface.

Step 5. Document the hostnames and IP addresses of the neighbors and test connectivity.

Document and ping the new neighbors you have discovered. Remember, the first two or three pings fail while ARP resolves MAC addresses.

Step 6. Telnet to each neighbor and check for additional Cisco devices.

Telnet to each of the new neighbors you have discovered, and use the **show cdp neighbors detail** command to check for any additional Cisco devices. The access password is **cisco**.

Step 7. Continue discovering and documenting the network.

Exit the telnet sessions to return to the default gateway router for PC1. From this router, telnet to other routers in the network to continue discovering and documenting the network. Remember to use the **show ip route** and **show ip cdp neighbors** commands to discover IP addresses you can use for Telnet.

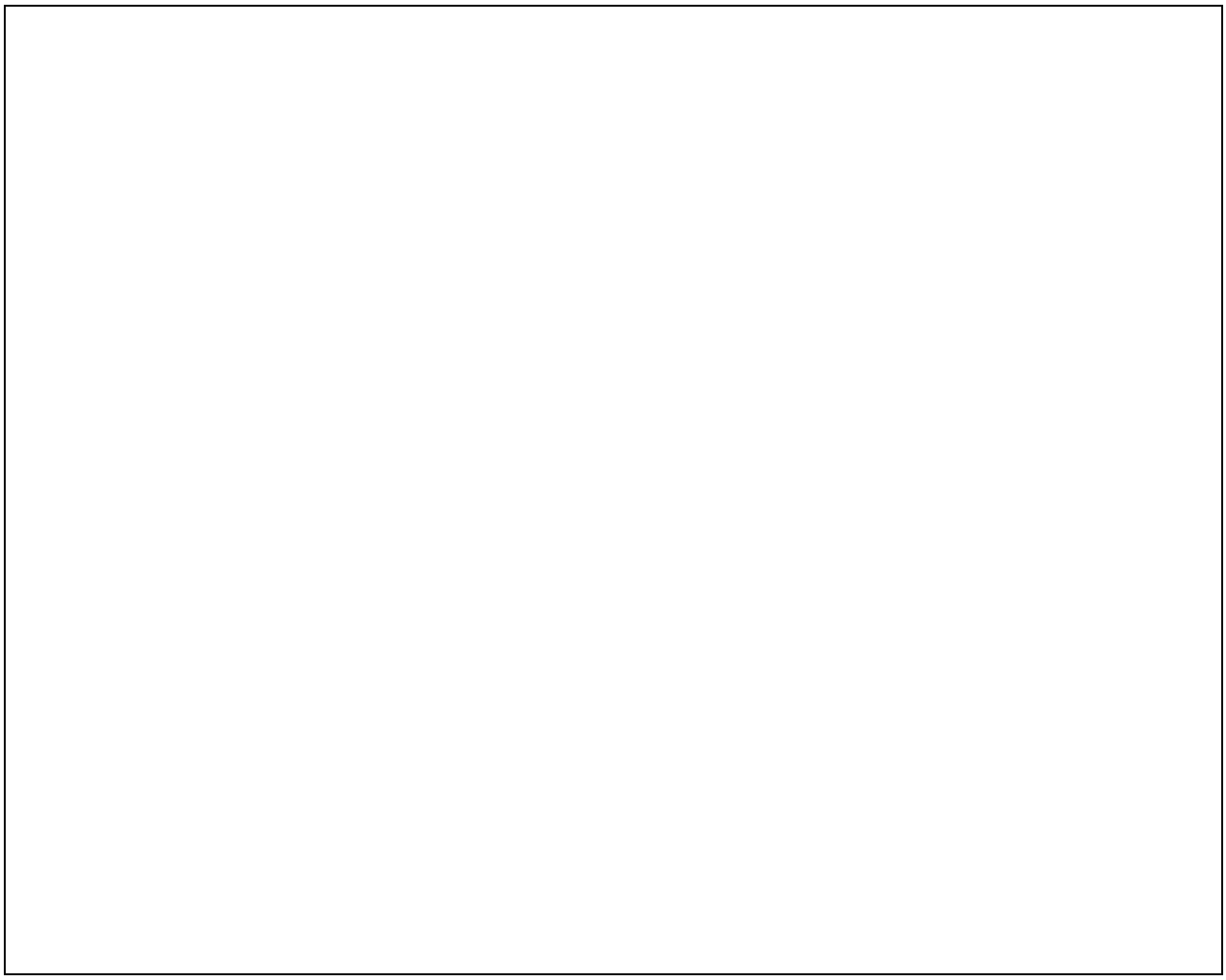
Task 5: Draw the Network Topology

Step 1. Draw a topology.

Now that you have discovered all the network devices and documented their addresses, use the addressing table and your sketch of the topology to draw a final version of the topology.

Hint: There is a Frame Relay cloud in the middle of the network.

Final Topology Diagram

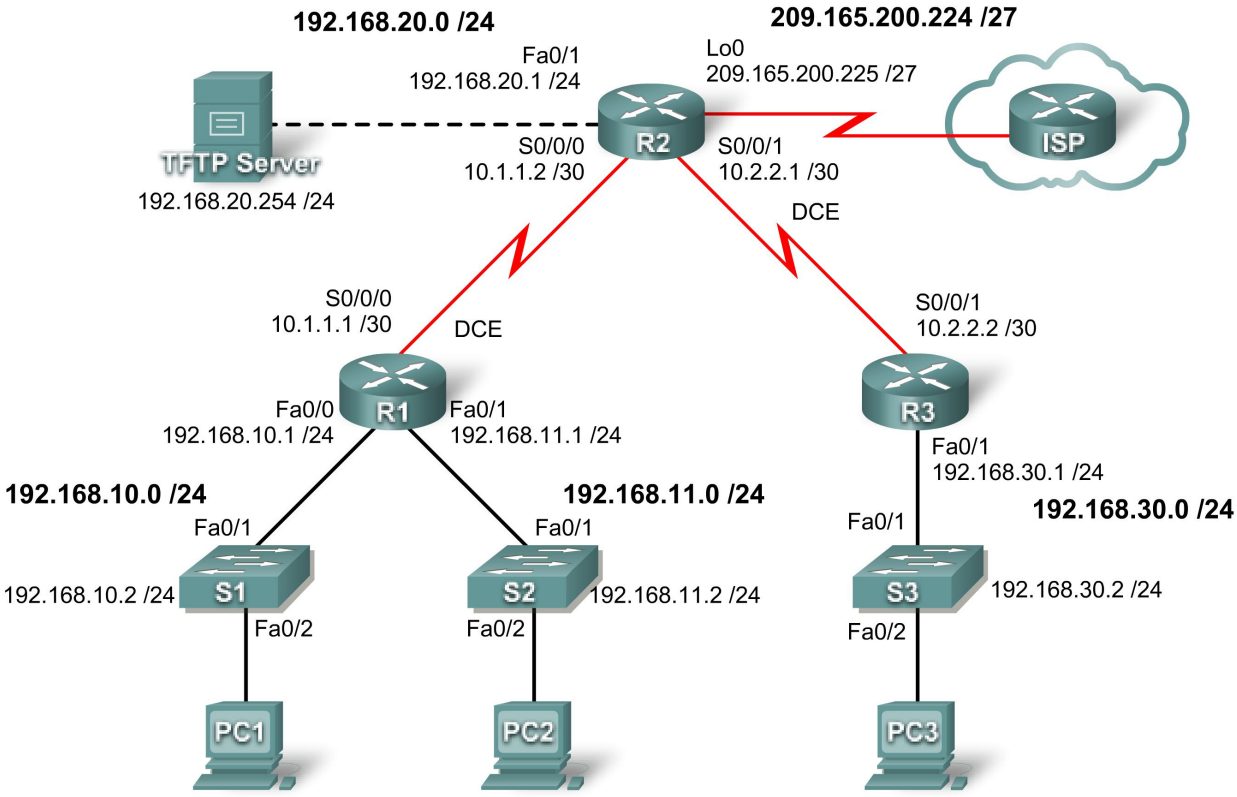


Step 2. Keep this documentation.

Your topology diagram and addressing table is needed for the next activity, 8.4.6 Troubleshooting Network Problems.

Activity 8.3.7: Troubleshooting Role Play (Instructor Version)

Topology Diagram



Learning Objectives

- Build a network
- Test a network
- Break a network
- Troubleshoot a problem
- Gather symptoms
- Correct the problem
- Document the problem and solution

Scenario

In this activity, you and another student will build the network displayed in the topology diagram. You will configure NAT, DHCP, and OSPF, and then verify connectivity. When the network is fully operational, one student will introduce several errors. Then the other student will use troubleshooting skills to isolate and solve the problem. Then the students will reverse roles and repeat the process. This activity can be done on real equipment or with Packet Tracer.

Task 1: Build the Network

Step 1: Cable and configure devices according to the topology diagram.

Step 2: Configure NAT, DHCP, and OSPF

Task 2: Test the Network

Step 1: Ensure that you have connectivity from end to end.

Step 2: Verify that DHCP and NAT are working correctly.

Step 3: Become familiar with every device using show and debug commands.

Task 3: Break the Network

One student leaves the room, if necessary, while the other student breaks the configuration. The break should only be one problem. The idea is to help each other develop troubleshooting skills. Creating multiple problems magnifies the scope of the work, which is not the goal of the lab. The goal is to help you become aware of the various changes that can occur in the network from just one problem.

Task 4: Troubleshoot the Problem

The student returns and questions the other student about the symptoms of the problem. Begin with general questions and attempt to narrow the scope of the problem. When the student being questioned feels that enough information has been provided, the questioning can stop.

Task 5: Gather Symptoms from Suspect Devices

Begins gathering symptoms using various **show** and **debug** commands. Use the **show running-config** command as the very last option.

Task 6: Correct the Problem

Correct the configuration and test the solution.

Task 7: Document the problem and solution.

Both students should enter the problem in their journal and document the solution.

Task 8: Reverse the roles and start over.

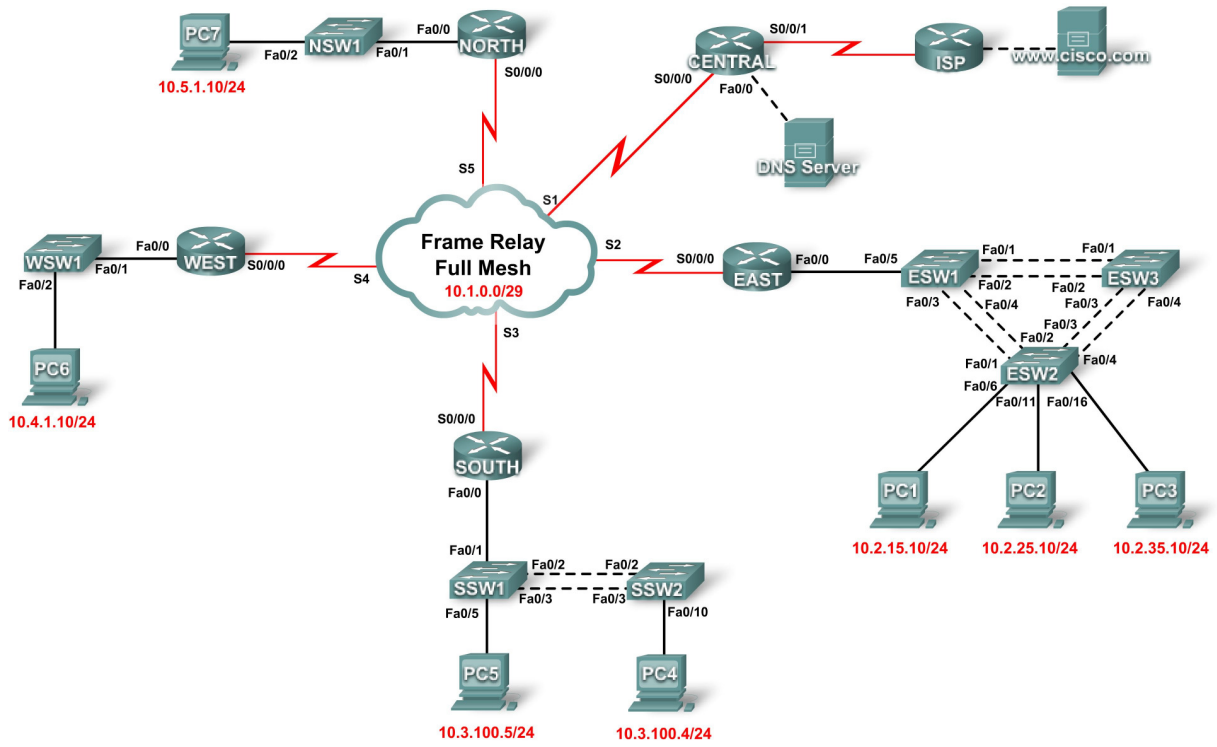
The students should now switch roles and start the process over.

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 to the Internet, reconnect the appropriate cabling and restore the TCP/IP settings.

PT Activity 8.4.6: Troubleshooting Network Problems (Instructor Version)

Topology Diagram (Instructor only)



Addressing Table (Instructor only)

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC1	NIC	10.2.15.10	255.255.255.0	10.2.15.1
PC2	NIC	10.2.25.10	255.255.255.0	10.2.25.1
PC3	NIC	10.2.35.10	255.255.255.0	10.2.35.1
PC4	NIC	10.3.100.4	255.255.255.0	10.3.100.1
PC5	NIC	10.3.100.5	255.255.255.0	10.3.100.1
PC6	NIC	10.4.1.10	255.255.255.0	10.4.1.1
PC7	NIC	10.5.1.10	255.255.255.0	10.5.1.1
DNS Server	NIC	10.1.100.2	255.255.255.0	10.1.100.1
CENTRAL	S0/0/0	10.1.0.1	255.255.255.0	N/A
CENTRAL	S0/0/1	209.165.201.2	255.255.255.252	N/A
CENTRAL	Fa0/0	10.1.100.1	255.255.255.0	N/A

Device	Interface	IP Address	Subnet Mask	Default Gateway
EAST	**S0/0/0**	10.1.0.2	255.255.255.0	N/A
EAST	**Fa0/0.5**	10.2.5.1	255.255.255.0	N/A
EAST	**Fa0/0.15**	10.2.15.1	255.255.255.0	N/A
EAST	**Fa0/0.25**	10.2.25.1	255.255.255.0	N/A
EAST	**Fa0/0.35**	10.2.35.1	255.255.255.0	N/A
ESW1	**VLAN 5**	10.2.5.21	255.255.255.0	10.2.5.1
ESW2	**VLAN 5**	10.2.5.22	255.255.255.0	10.2.5.1
ESW3	**VLAN 5**	10.2.5.23	255.255.255.0	10.2.5.1
SOUTH	**S0/0/0**	10.1.0.3	255.255.255.0	N/A
SOUTH	**Fa0/0.100**	10.3.100.1	255.255.255.0	N/A
SOUTH	**Fa0/0.105**	10.3.105.1	255.255.255.0	N/A
SSW1	**VLAN 105**	10.3.105.21	255.255.255.0	10.3.105.1
SSW2	**VLAN 105**	10.3.105.22	255.255.255.0	10.3.105.1
WEST	**S0/0/0**	10.1.0.4	255.255.255.0	N/A
WEST	**Fa0/0**	10.4.1.1	255.255.255.0	N/A
WSW1	**None**	None	None	None
NORTH	**S0/0/0**	10.1.0.5	255.255.255.0	N/A
NORTH	**Fa0/0**	10.5.1.1	255.255.255.0	N/A
NSW1	**None**	None	None	None

Learning Objectives

- Gather network documentation
- Test connectivity
- Gather data and implement solutions
- Test connectivity

Introduction

In this activity, you will troubleshoot connectivity issues between PCs routed through XYZCORP. The activity is complete when you achieve 100% and all the PCs can ping each other and the www.cisco.com server. Any solution you implement must conform to the topology diagram.

Task 1: Gather Network Documentation

To successfully complete this activity, you need your final documentation for the PT Activity 8.1.2: Network Discovery and Documentation you completed previously in this chapter. This documentation should have an accurate topology diagram and addressing table. If you do not have this documentation, then ask your Instructor for accurate versions.

Task 2: Test Connectivity

At the end of this activity, there should be full connectivity between all PCs and between PCs and the www.cisco.com server. To begin troubleshooting connectivity failures, ping the following:

- PCs to www.cisco.com server
- PC to PC
- PC to default gateway

Were any of the pings successful? Which failed?

_____

_____

_____

_____

_____

None of the PCs can ping another PC or the www.cisco.com server. Only PC4, PC5, PC6, and PC7 can ping their respective default gateways.

Task 3: Gather Data and Implement Solutions

Step 1. Choose a PC to begin gathering data.

Choose any PC and begin gathering data by testing connectivity to the default gateway. You can also use **traceroute** to see where connectivity fails.

Step 2. Telnet to the default gateway and continue gathering data.

If the PC you chose does not have connectivity to its default gateway, choose another PC to approach the problem from a different direction.

When you established connectivity through a default gateway, the login password is **cisco**.

Step 3. Use troubleshooting tools to verify the configuration.

At the default gateway router, use troubleshooting tools to verify the configuration with your own documentation. Remember to check switches in addition to the routers. Be sure to verify the following:

- Addressing information
- Interface activation
- Encapsulation
- Routing
- VLAN configuration
- Duplex or speed mismatches
- VTP operation

As you discover symptoms of the PC connectivity issue, document them in the space provided in the next step.

Step 4. Document network symptoms and possible solutions.

_____

_____

Instructor Note: The following is only one way the student might progress through this activity. The student can start from PC4, PC6, or PC7. For this sample answer, we started at PC4.
PC1, PC2, PC3 and PC5 cannot access the default gateway, therefore, troubleshooting the connectivity problems of those PCs must come from another direction.

Problem 1: From PC4, you can access the default gateway, SOUTH. Telnet to SOUTH and verify the routing table. SOUTH only has directly connected routes, so verify the current interface configuration using the **show protocols** or **show ip interface brief** command. Careful examination of the IP addresses reveals that the S0/0/0 address is transposed. It should be 10.1.0.3 instead of 10.0.1.3. The **show ip protocols** command reveals no problems with the RIP configuration on SOUTH.
Solution 1: Configure the correct IP address for the S0/0/0 interface on SOUTH.
Problem 2: When RIP converges on SOUTH, use the **show ip route** command to gather further information about possible problems. SOUTH has directly connected routes but only has two RIP routes. Missing routes include the four VLANs for EAST, the WEST LAN, and the NORTH LAN. Pinging EAST is successful, so telnet to EAST. Because SOUTH is not receiving routes from EAST, check the RIP configuration on EAST with the **show ip protocols** command. EAST is sending and receiving RIP updates and is advertising the correct network. However, automatic networks summarization is in effect. Therefore, EAST is only sending the classful 10.0.0.0/8 network in RIP periodic updates.
Solution 2: Configure EAST with the **no auto-summary** command.
Problem 3: While on EAST, investigate the connectivity problems between PC1, PC2, and PC3. Use the **show ip interface brief** and **show protocols** commands to verify the IP configuration for the VLAN subinterface. No problems are found, so ping ESW1 and then telnet to ESW1. Because ESW1 is not an access layer switch, check the VLAN configuration (**show vlan brief**) and VTP status (**show vtp status**). All VLANs are there as they should be. This switch is correctly configured as the VTP server for the XYZCORP domain. The command **show vtp password** reveals that ESW1 is using the correct password, which is **eastbranch**. First ping and then telnet to ESW2. Check the interfaces for any Layer 1 or Layer 2 problems with the **show ip interface brief** command. The interfaces that PC1, PC2, and PC3 are attached to are all “up” and “up”. Check the VLAN configuration and VTP status. ESW2 does not have all the correct VLANs, and the VTP status shows that ESW2 belongs to the Null domain. ESW2 is using the correct VTP password.
Solution 3: Configure ESW2 for the correct VTP domain name, XYZCORP. After STP converges, PC1, PC2, and PC3 should be able to ping each other.
Problem 4: Exit back to EAST and check the routing table. Routes are missing for the WEST and NORTH LANs. Test connectivity to WEST and NORTH by pinging the serial interfaces for those routers. Pings to WEST fail but succeed to NORTH. Telnet to NORTH. On NORTH, display the routing table. NORTH has no RIP routes, so use the **show ip protocols** command to verify RIP routing. The command generates no output, so RIP is either not configured at all or not configured correctly. Use the **show run** command to check the RIP commands. RIP is missing the network command.
Solution 4: Configure NORTH with the RIP command **network 10.0.0.0**
Problem 5: After RIP converges, check the NORTH routing table. The WEST LAN is still missing. Because pings to WEST fail, access WEST from PC6. First, ping the default gateway address and then telnet to WEST. Display the routing table. Notice that only the Fa0/0 network is in the routing table. Check the interface configuration with the **show ip interface brief** command. The S0/0/0 interface is physically “up” but the data link layer is “down”. Further investigate S0/0/0 with the **show interface** command. The encapsulation is set to HDLC instead of Frame Relay.
Solution 5: Change the S0/0/0 interface encapsulation from HCLC to Frame Relay with the **encapsulation frame-relay** command. All PCs should now be able to ping each other
Problem 6: PCs still cannot ping the www.cisco.com server. From any device, test connectivity and then telnet to CENTRAL. Investigate the interface status with the **show ip interface brief** command. The S0/0/1 interface is administratively down.
Solution 6: Activate the S0/0/1 interface on CENTRAL with the **no shutdown** command.
Problem 7: PCs still cannot ping the www.cisco.com server. However, PCs can ping the DNS server. The problem is either with the CENTRAL configuration or the ISP configuration. Because you do not have access to the ISP router, check the configuration on CENTRAL. The **show run** command reveals that CENTRAL is using NAT. The configuration is missing the NAT statement that binds the NAT pool to the access list.

Solution 7: Configure CENTRAL with the **ip nat inside source list 1 pool XYZCORP overload** command.

Step 5. Make changes based on your solutions from the previous step.

Task 4: Test Connectivity

Step 1. Test PC connectivity.

All PCs should now be able to ping each other and the www.cisco.com server. If you changed any IP configurations, create new pings because the prior pings use the old IP address.

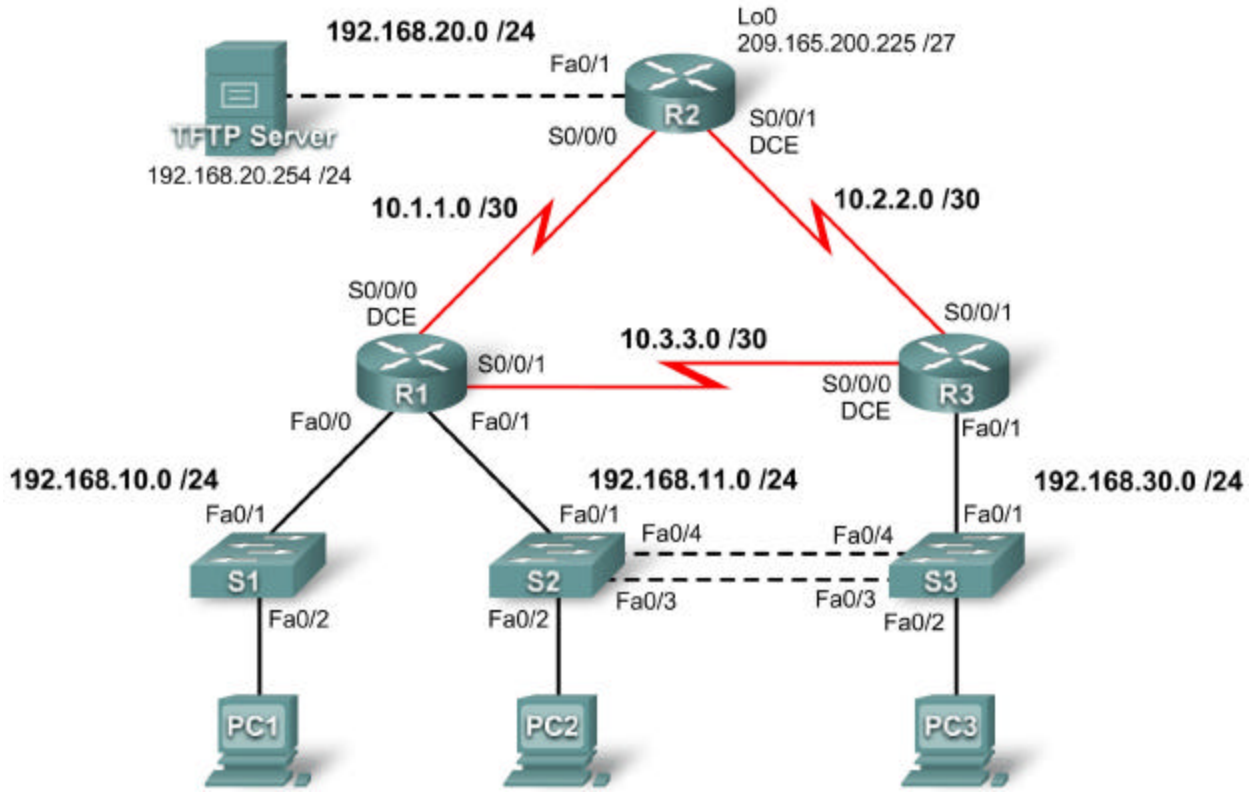
If there are still connectivity issues between PCs or PC to server, return to Task 3 and continue troubleshooting.

Step 2. Check results.

Your completion percentage should be 100%. If not, return to Task 3 and continue to troubleshoot and implement your suggested solutions. You will not be able to click **Check Results** and see which required components are not yet completed.

PT Activity 8.5.1: Troubleshooting Enterprise Networks 1 (Instructor Version)

Topology Diagram



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

Addressing Tabled continued on next page

Addressing Table continued

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**	DHCP	DHCP	DHCP
PC2	**NIC**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	**NIC**	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

- Find and correct all network errors
- Verify that requirements are fully met
- Document the corrected network

Scenario

You have been asked to correct configuration errors in the company network. For this activity, 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 activity is cumulative, you will be using all the knowledge and troubleshooting techniques that you have acquired from the previous material to successfully complete this activity.

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 uses PPP.
- 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.
- 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 0/0.
- 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.
- All addresses shown in the diagram must be reachable from every device.

Task 1: Find and Correct All Network Errors

```
R1
!
router rip
 no passive-interface FastEthernet0/0
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
!

R2
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 frame-relay map ip 10.1.1.2 201
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252

S2
!
vtp mode client
!

S3
!
vtp domain CCNA_Troubleshooting
!
vlan 11
vlan 30
!
interface FastEthernet0/1
 switchport trunk allowed vlan 11,30
!
interface FastEthernet0/2
 switchport access vlan 30
!
```

Task 2: 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).

This is intentionally left vague because there are many ways to verify the requirements. Below is an example for requirement 1.

```
S2#show spanning-tree

VLAN0011
  Spanning tree enabled protocol ieee
  Root ID    Priority    24587
```



```
             Address     00E0.A380.CD1C
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    24587  (priority 24576 sys-id-ext 11)
             Address     00E0.A380.CD1C
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/1            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr
Fa0/2            Desg FWD 19        128.3    Shr
```

Task 3: Document the Corrected Network

```
R1
!
hostname R1
!
!
enable secret ciscoccna
!
username R3 password 0 ciscoccna
username ccna password 0 ciscoccna
!
no ip domain-lookup
!
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 201
 frame-relay map ip 10.1.1.2 201 broadcast
 no keepalive
 clock rate 4000000
!
interface Serial0/0/1
 ip address 10.3.3.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
interface Vlan1
 no ip address
 shutdown
!
router rip
```



```
 version 2
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.10.0
 network 192.168.11.0
 no auto-summary
!
ip classless
!
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
!
!
ip dhcp pool Access1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
!
line con 0
line vty 0 4
 access-class VTY in
 login
!
!
end


R2
!
hostname R2
!
!
enable secret ciscoccna
!
username ccna password 0 ciscoccna
!
no ip domain-lookup
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
```



```
 ip access-group Anti-spoofing in
 ip access-group TFTP out
 ip nat outside
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 201 broadcast
 frame-relay map ip 10.1.1.2 201
 no keepalive
 ip nat inside
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 ip access-group R3-telnet in
 ip nat inside
 clock rate 4000000
!
interface Loopback0
 ip address 209.165.200.245 255.255.255.224
 ip access-group private in
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.20.0
 default-information originate
 no auto-summary
!
ip nat inside source list NAT interface FastEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
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 host 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
line vty 0 4
 login
!
!
end


R3
!
hostname R3
!
!
enable secret 5 $1$mERr$NY2X7xBCS5tAN/W1NAs2c1
!
username R1 password 0 ciscoccna
username ccna password 0 ciscoccna
!
no ip domain-lookup
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.11
 encapsulation dot1Q 11
 ip address 192.168.11.3 255.255.255.0
!
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
 ppp authentication chap
 clock rate 4000000
!
interface Serial0/0/1
```



```
 ip address 10.2.2.2 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 no passive-interface FastEthernet0/1.11
 no passive-interface FastEthernet0/1.30
 network 10.0.0.0
 network 192.168.11.0
 network 192.168.30.0
 no auto-summary
!
ip classless
!
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
line vty 0 4
 login
!
!
end


S1
!
hostname S1
!
enable secret ciscoccna
!
no ip domain-lookup
!
vtp domain CCNA_Troubleshooting
vtp mode transparent
vtp password ciscoccna
!
!
vlan 10
!
interface FastEthernet0/1
 switchport access vlan 10
```



```
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address dhcp
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

```
S2
!
hostname S2
!
enable secret ciscoccna
!
no ip domain-lookup
!
spanning-tree vlan 11 priority 24576
spanning-tree vlan 30 priority 28672
!
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 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 Vlan1
 no ip address
 shutdown
```



```
!
interface Vlan11
 ip address 192.168.11.2 255.255.255.0
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

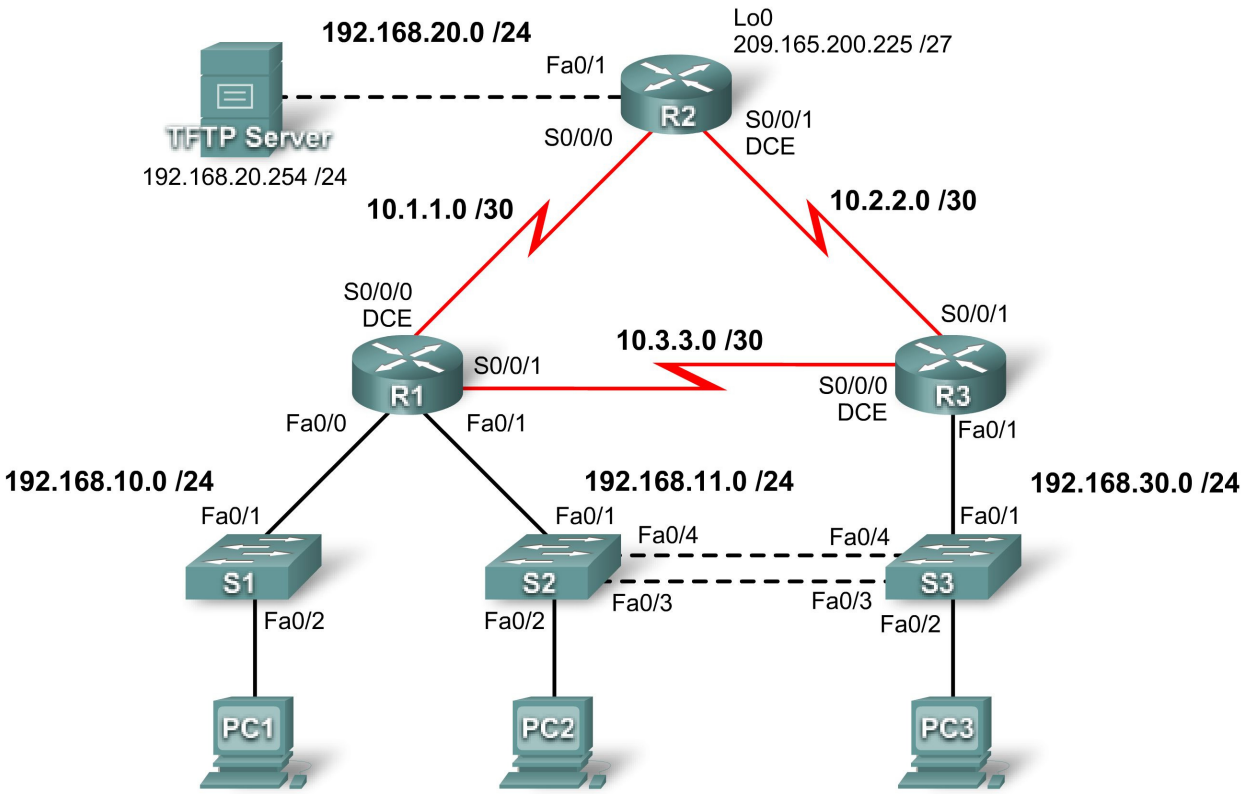
```
S3
!
hostname S3
!
enable secret ciscoccna
!
no ip domain-lookup
!
spanning-tree vlan 11 priority 28672
spanning-tree vlan 30 priority 24576
!
interface FastEthernet0/1
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode 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 Vlan1
 no ip address
 shutdown
!
interface Vlan30
 ip address 192.168.30.2 255.255.255.0
!
ip default-gateway 192.168.30.1
!
line con 0
!
line vty 0 4
```



```
 login
line vty 5 15
 login
!
!
end
```


PT Activity 8.5.2: Troubleshooting Enterprise Networks 2 (Instructor Version)

Topology Diagram



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

Addressing Table continued on the next page

Addressing Table continued

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**	DHCP	DHCP	DHCP
PC2	**NIC**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	**NIC**	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

- Find and correct all network errors
- Verify that requirements are fully met
- Document the corrected network

Scenario

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

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

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. EIGRP 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: Find and Correct All Network Errors

Use a clock rate of **4000000** and VLAN priority of **24576** where needed.

```
R1
!
no username R2
username R3 password ciscoccna
! A typo in the username will prevent R3 from authenticating with CHAP.
!
interface FastEthernet0/0
 no ip access-group Anti-spoofing out
 ip access-group Anti-spoofing in
! The access list was applied in the wrong direction. This common
! mistake prevents all traffic from exiting the interface.
!
interface Serial0/0/1
 ip address 10.3.3.1 255.255.255.252
! The subnet was misconfigured most likely due to wide use of the /24
! subnet.
!

R2
!
interface Serial0/0/1
 ip access-group R3-telnet in
! It is common for an access list to be created but not applied to an
! interface, which is required for the ACL to function.

R3
!
interface Serial0/0/0
 clock rate 4000000
! The clock rate was forgotten on the DCE interface.
 ppp authentication chap
! PAP was mistakenly misconfigured instead of CHAP.
!
router eigrp 10
 no passive-interface FastEthernet0/1.11
 no passive-interface FastEthernet0/1.30
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
! These commands were forgotten, so EIGRP is sent on all interfaces.
!
ip route 0.0.0.0 0.0.0.0 10.2.2.1
! The default route to the Internet gateway was forgotten, preventing
! this device from reaching it.
!
interface FastEthernet0/1.30
 ip access-group Anti-spoofing in
! The access list was mistyped. It now references a nonexistent ACL,
```



```
! so traffic is dropped because of the implicit deny all at the end of !
every ACL.
!

S3
!
spanning-tree vlan 30 priority 24576
!
```

Task 2: 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).

This is intentionally left vague because there are many ways to verify the requirements. Below is an example for requirement 1.

```
S2#show spanning-tree

VLAN0011
  Spanning tree enabled protocol ieee
  Root ID     Priority    24587
              Address     00E0.A380.CD1C
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    24587  (priority 24576 sys-id-ext 11)
              Address     00E0.A380.CD1C
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.3    Shr
Fa0/1            Desg FWD 19        128.3    Shr
Fa0/2            Desg FWD 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr

S3#show spanning-tree
<output omitted>

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID     Priority    24606
              Address     0050.0FCE.8E14
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    24606  (priority 24576 sys-id-ext 30)
              Address     0050.0FCE.8E14
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Desg FWD 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/1            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr
```


Task 3: Document the Corrected Network

```
R1
!
hostname R1
!
!
enable secret ciscoccna
!
username R3 password ciscoccna
username ccna password ciscoccna
!
no ip domain-lookup
!
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip access-group Anti-spoofing in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 201
 frame-relay map ip 10.1.1.2 201 broadcast
 no keepalive
 clock rate 4000000
!
interface Serial0/0/1
 ip address 10.3.3.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 10
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.1.1.0 0.0.0.255
 network 10.3.3.0 0.0.0.255
 network 192.168.10.0
 network 192.168.11.0
 network 10.1.1.0 0.0.0.3
 network 10.3.3.0 0.0.0.3
 no auto-summary
!
```



```
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
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
!
!
ip dhcp pool Access1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
!
line con 0
line vty 0 4
 access-class VTY in
 login
!
!
end
```

R2

```
!
hostname R2
!
!
enable secret ciscoccna
!
username ccna password ciscoccna
!
no ip domain-lookup
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 ip access-group Anti-spoofing in
 ip access-group TFTP out
 ip nat outside
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 201 broadcast
 frame-relay map ip 10.1.1.2 201
```



```
 no keepalive
 ip nat inside
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 ip access-group R3-telnet in
 ip nat inside
 clock rate 4000000
!
interface Loopback0
 ip address 209.165.200.245 255.255.255.224
 ip access-group private in
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 10
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.1.1.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 network 192.168.20.0
 no auto-summary
!
ip nat inside source list NAT interface FastEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
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 host 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
line vty 0 4
 login
!
```



```
!
end
```

R3

```
!
hostname R3
!
!
enable secret ciscoccna
!
username R1 password ciscoccna
username ccna password ciscoccna
!
no ip domain-lookup
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.11
 encapsulation dot1Q 11
 ip address 192.168.11.3 255.255.255.0
!
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
 ppp authentication chap
 clock rate 4000000
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 10
 network 10.3.3.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 network 192.168.11.0
 network 192.168.30.0
 no auto-summary
!
```



```
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.2.1
!
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
line vty 0 4
 login
!
!
end
```

S1

```
!
hostname S1
!
enable secret ciscoccna
!
no ip domain-lookup
!
vtp domain CCNA_Troubleshooting
vtp mode transparent
vtp password ciscoccna
!
!
vlan 10
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address dhcp
!
line con 0
!
line vty 0 4
 login
line vty 5 15
```



```
 login
!
!
end
```

S2

```
!
hostname S2
!
enable secret ciscoccna
!
no ip domain-lookup
!
spanning-tree vlan 11 priority 24576
spanning-tree vlan 30 priority 28672
!
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 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 Vlan1
 no ip address
 shutdown
!
interface Vlan11
 ip address 192.168.11.2 255.255.255.0
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

S3

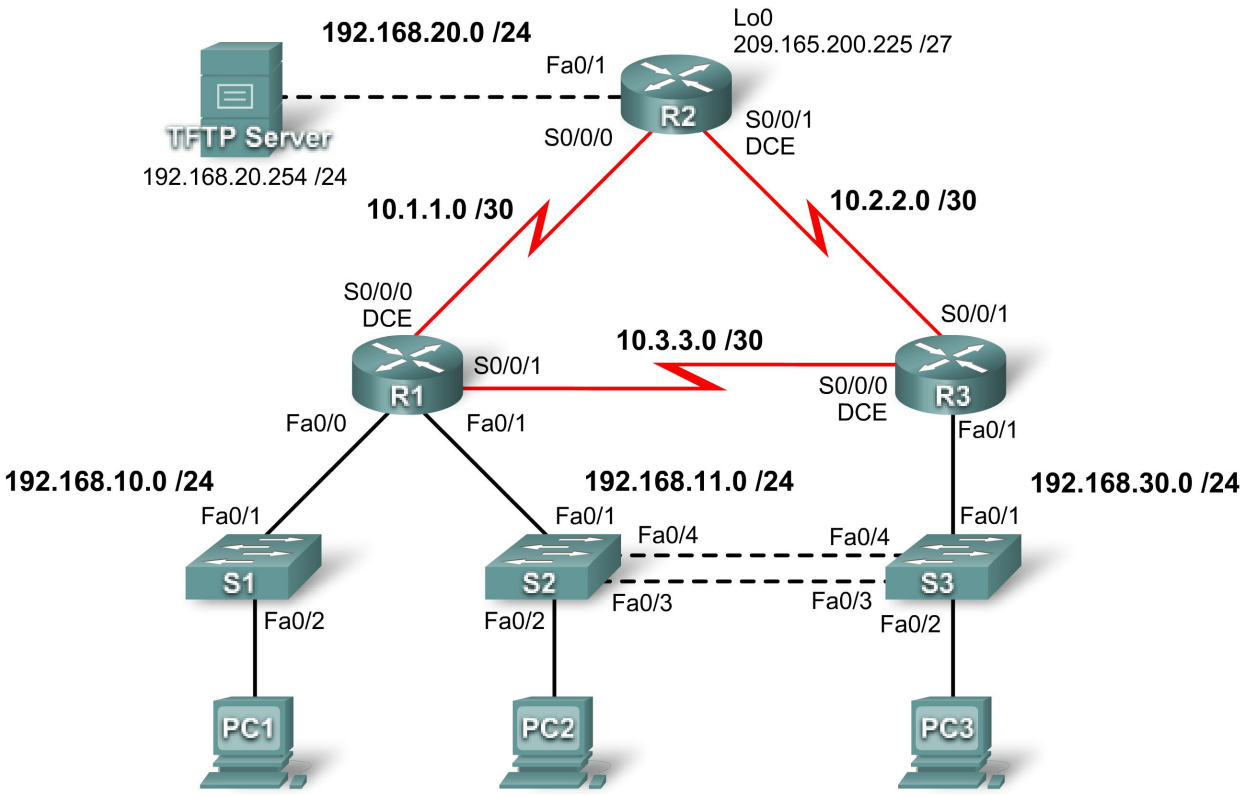
```
!
hostname S3
!
```



```
enable secret ciscoccna
!
no ip domain-lookup
!
spanning-tree vlan 11 priority 28672
spanning-tree vlan 30 priority 24576
!
interface FastEthernet0/1
 switchport trunk allowed vlan 11,30
 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 Vlan1
 no ip address
 shutdown
!
interface Vlan30
 ip address 192.168.30.2 255.255.255.0
!
ip default-gateway 192.168.30.1
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```


PT Activity 8.5.3: Troubleshooting Enterprise Networks 3 (Instructor Version)

Topology Diagram



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

Addressing Table continued on the next page

Addressing Table continued

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**	DHCP	DHCP	DHCP
PC2	**NIC**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1
TFTP Server	**NIC**	192.168.20.254	255.255.255.0	192.168.20.1

Learning Objectives

- Find and correct all network errors
- Verify that requirements are fully met
- Document the corrected network

Scenario

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

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

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: Find and Correct All Network Errors

Use a clock rate of **4000000** and VLAN priority of **24576** where needed.

R1

```
!
router ospf 1
 network 10.3.3.0 0.0.0.3 area 0
!
```

R2

```
interface FastEthernet0/1
 ip nat outside
 no shutdown
!
interface Serial0/0/0
 ip nat inside
 no shutdown
!
interface Serial0/0/1
 clock rate 4000000
 ip nat inside
 no shutdown
!
router ospf 1
 network 192.168.20.0 0.0.0.255 area 0
 default-information originate
!
ip nat inside source list NAT interface FastEthernet0/1 overload
!
```

R3

```
!
interface FastEthernet0/1.11
 encapsulation dot1Q 11
! The VLAN was mistyped, which puts the subnet on the wrong VLAN.
```

S2

```
!
interface FastEthernet0/3
 switchport trunk native vlan 99
interface FastEthernet0/4
 switchport trunk native vlan 99
! The native VLAN was changed on S3 but was then forgotten. This native
! VLAN mismatch will produce errors while trunking.
```

S3

```
!
vlan 11
! VLAN 11 must exist for it to be in the active management domain and
! for traffic to traverse it.
```


Task 2: 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).

This is intentionally left vague because there are many ways to verify the requirements. Below is an example for requirement 1.

```
S2#show spanning-tree

VLAN0011
  Spanning tree enabled protocol ieee
  Root ID     Priority    24587
              Address     00E0.A380.CD1C
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    24587  (priority 24576 sys-id-ext 11)
              Address     00E0.A380.CD1C
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/2            Desg FWD 19        128.3    Shr
Fa0/1            Desg FWD 19        128.3    Shr

S3#show spanning-tree
<output omitted>

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID     Priority    24606
              Address     0050.0FCE.8E14
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    24606  (priority 24576 sys-id-ext 30)
              Address     0050.0FCE.8E14
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.3    Shr
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/2            Desg FWD 19        128.3    Shr
Fa0/1            Desg FWD 19        128.3    Shr
```

Task 3: Document the Corrected Network

```
R1
!
hostname R1
!
!
enable secret ciscoccna
!
```



```
username R3 password ciscoccna
username ccna password ciscoccna
!
no ip domain-lookup
!
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 201
 frame-relay map ip 10.1.1.2 201 broadcast
 no keepalive
 clock rate 4000000
!
interface Serial0/0/1
 ip address 10.3.3.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/0
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
 network 10.3.3.0 0.0.0.3 area 0
 default-information originate
!
ip classless
!
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
!
!
ip dhcp pool Access1
 network 192.168.10.0 255.255.255.0
```



```
 default-router 192.168.10.1
!
line con 0
line vty 0 4
 access-class VTY in
 login
!
!
end
```

R2

```
!
hostname R2
!
!
enable secret ciscoccna
!
username ccna password ciscoccna
!
no ip domain-lookup
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 ip access-group Anti-spoofing in
 ip access-group TFTP out
 ip nat outside
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 201 broadcast
 frame-relay map ip 10.1.1.2 201
 no keepalive
 ip nat inside
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 ip access-group R3-telnet in
 ip nat inside
 clock rate 4000000
!
interface Loopback0
 ip address 209.165.200.245 255.255.255.224
 ip access-group private in
!
interface Vlan1
 no ip address
 shutdown
```



```
!
router ospf 1
 log-adjacency-changes
 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
 network 192.168.20.0 0.0.0.255 area 0
 default-information originate
!
ip nat inside source list NAT interface FastEthernet0/1 overload
ip nat inside source list nat interface FastEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
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 host 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
line vty 0 4
 login
!
!
end
```

R3

```
!
hostname R3
!
!
enable secret 5 $1$mERr$NY2X7xBCS5tAN/W1NAs2c1
!
username R1 password 0 ciscoccna
username ccna password 0 ciscoccna
!
no ip domain-lookup
```



```
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.11
 encapsulation dot1Q 11
 no ip address
!
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
 ppp authentication chap
 clock rate 4000000
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/1.30
 network 10.2.2.0 0.0.0.3 area 0
 network 10.3.3.0 0.0.0.3 area 0
 network 192.168.11.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
ip classless
!
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
line vty 0 4
 login
!
!
end
```

S1

```
!
hostname S1
!
enable secret ciscoccna
!
no ip domain-lookup
!
vtp domain CCNA_Troubleshooting
vtp mode transparent
vtp password ciscoccna
!
!
vlan 10
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address dhcp
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

S2

```
!
hostname S2
!
enable secret ciscoccna
!
no ip domain-lookup
!
spanning-tree vlan 11 priority 24576
spanning-tree vlan 30 priority 28672
```



```
!
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 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 Vlan1
 no ip address
 shutdown
!
interface Vlan11
 ip address 192.168.11.2 255.255.255.0
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```

S3

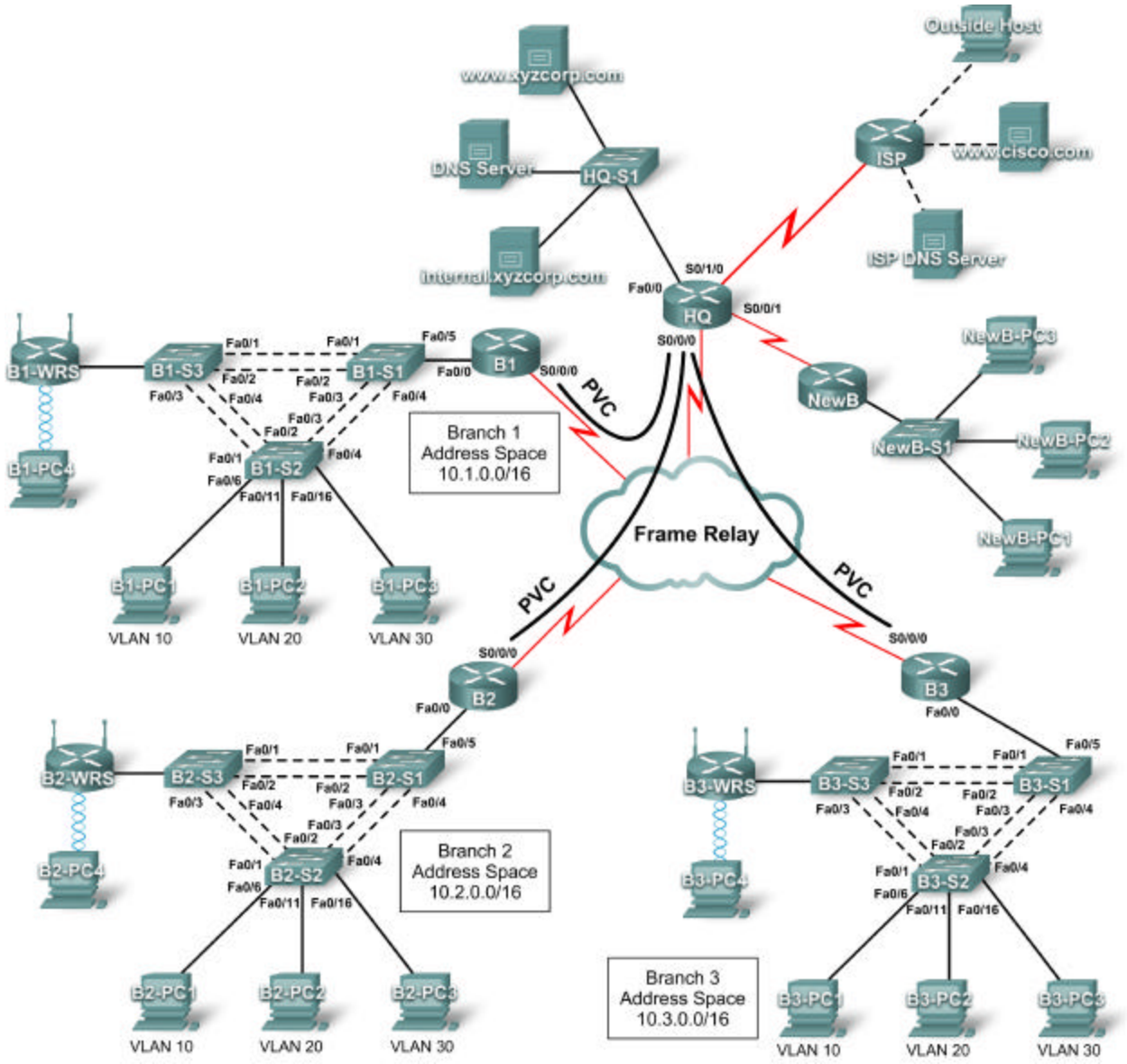
```
!
hostname S3
!
enable secret ciscoccna
!
no ip domain-lookup
!
spanning-tree vlan 11 priority 28672
spanning-tree vlan 30 priority 24576
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/3
 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 Vlan1
 no ip address
 shutdown
!
interface Vlan30
 ip address 192.168.30.2 255.255.255.0
!
ip default-gateway 192.168.30.1
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
end
```


PT Activity 8.6.1: CCNA Skills Integration Challenge (Instructor Version)

Topology Diagram



Addressing Table for HQ

Device	Interface	IP Address	Subnet Mask	DLCI Mappings
HQ	Fa0/0	10.0.1.1	255.255.255.0	N/A
	S0/0/0.41	10.255.255.1	255.255.255.252	DLCI 41 to B1
	S0/0/0.42	10.255.255.5	255.255.255.252	DLCI 42 to B2
	S0/0/0.43	10.255.255.9	255.255.255.252	DLCI 43 to B3
	S0/0/1	10.255.255.253	255.255.255.252	N/A
	S0/1/0	209.165.201.1	255.255.255.252	N/A

Addressing Table for Branch Routers

Device	Interface	IP Address	Subnet Mask
BX	Fa0/0.10	10.X.10.1	255.255.255.0
	Fa0/0.20	10.X.20.1	255.255.255.0
	Fa0/0.30	10.X.30.1	255.255.255.0
	Fa0/0.88	10.X.88.1	255.255.255.0
	Fa0/0.99	10.X.99.1	255.255.255.0
	S0/0/0	2nd address	255.255.255.252
BX-S1	VLAN 99	10.X.99.21	255.255.255.0
BX-S2	VLAN 99	10.X.99.22	255.255.255.0
BX-S3	VLAN 99	10.X.99.23	255.255.255.0
BX-WRS	VLAN 1	10.X.40.1	255.255.255.0

- Replace “X” with the Branch router number (B1, B2, or B3).
- The point-to-point PVCs with HQ use the second address in the subnet. HQ is using the first address.
- The WRT300N routers get the Internet address through DHCP from the Branch router.

VLAN Configuration and Port Mappings

VLAN Number	Network Address	VLAN Name	Port Mappings
10	10.X.10.0/24	Admin	BX-S2, Fa0/6
20	10.X.20.0/24	Sales	BX-S2, Fa0/11
30	10.X.30.0/24	Production	BX-S2, Fa0/16
88	10.X.88.0/24	Wireless	BX-S3, Fa0/7
99	10.X.99.0/24	Mgmt&Native	All trunks

Learning Objectives

- Configure Frame Relay in a hub-and-spoke topology
- Configure PPP with CHAP and PAP authentication
- Configure static and dynamic NAT
- Configure static and default routing

Introduction

In this comprehensive CCNA skills activity, the XYZ Corporation uses a combination of Frame Relay and PPP for WAN connections. The HQ router provides access to the server farm and the Internet through NAT. HQ also uses a basic firewall ACL to filter inbound traffic. Each Branch router is configured for inter-VLAN routing and DHCP. Routing is achieved through EIGRP as well as static and default routes. The VLANs, VTP, and STP are configured on each of the switched networks. Port security is enabled and wireless access is provided. Your job is to successfully implement all of these technologies, leveraging what you have learned over the four Exploration courses leading up to this culminating activity.

You are responsible for configuring HQ and the Branch routers, B1, B2, and B3. In addition, you are responsible for configuring every device that attaches to the network through a Branch router. The NewB router represents a new Branch office acquired through a merger with a smaller company. You do not have access to the NewB router. However, you will establish a link between HQ and NewB to provide this new Branch office with access to the internal network and the Internet.

Routers and switches under your administration have no configuration. None of the basic configurations like hostname, passwords, banners, and other general maintenance commands are graded by Packet Tracer and will not be part of the task specification. However, you are expected to configure them, and your instructor may choose to grade these commands.

Because this activity uses such a large network with close to 500 required components under the assessment items, you will not necessarily see your completion percentage increase each time you enter a command. In addition, you will not be given a specific percentage that should be complete at the end of each task. Instead, you use connectivity tests to verify each task's configurations. However, at any time you can click **Check Results** to see if a particular component is graded and if you configured it correctly.

Because the Branch routers (B1, B2, and B3) and switches are designed with scalability in mind, you can reuse scripts. For example, your configurations for B1, B1-S1, B1-S2, and B1-S3 can be directly applied to the B2 devices with only minor adjustments.

Note: This CCNA Skills Integration Challenge is also available in an open-ended version where you can choose the addressing scheme and technologies that you want to implement. You verify your configuration by testing end-to-end connectivity.

Task 1: Configure Frame Relay in a Hub-and-Spoke Topology

Step 1. Configure the Frame Relay core.

Use the addressing tables and the following requirements.

HQ is the hub router. B1, B2, and B3 are the spokes.

- HQ uses a point-to-point subinterface for each of the Branch routers.
- B3 must be manually configured to use IETF encapsulation.
- The LMI type must be manually configured as q933a for HQ, B1, and B2. B3 uses ANSI.

```
!------------
!HQ
!------------
```



```
enable
configure terminal
host HQ
enable secret class
banner motd $AUTHORIZED ACCESS ONLY!$
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
service password-encryption
!
interface Serial0/0/0
 no ip address
 encapsulation frame-relay
 frame-relay lmi-type q933a
 no shutdown
!
interface Serial0/0/0.41 point-to-point
 ip address 10.255.255.1 255.255.255.252
 frame-relay interface-dlci 41
!
interface Serial0/0/0.42 point-to-point
 ip address 10.255.255.5 255.255.255.252
 frame-relay interface-dlci 42
!
interface Serial0/0/0.43 point-to-point
 ip address 10.255.255.9 255.255.255.252
 frame-relay interface-dlci 43
end
wr

!-----------
!B1
!-----------
enable
configure terminal
host B1
enable secret class
banner motd $AUTHORIZED ACCESS ONLY!$
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
service password-encryption
!
interface Serial0/0/0
 ip address 10.255.255.2 255.255.255.252
 encapsulation frame-relay
 frame-relay lmi-type q933a
 no shutdown
end
wr
```



```
!-----------
!B2
!-----------
enable
configure terminal
host B2
enable secret class
banner motd $AUTHORIZED ACCESS ONLY!$
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
service password-encryption
!
interface Serial0/0/0
 ip address 10.255.255.6 255.255.255.252
 encapsulation frame-relay
 frame-relay lmi-type q933a
 no shutdown
end
wr

!-----------
!B3
!-----------
enable
configure terminal
host B3
enable secret class
banner motd $AUTHORIZED ACCESS ONLY!$
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
service password-encryption
!
interface Serial0/0/0
 ip address 10.255.255.10 255.255.255.252
 encapsulation frame-relay ietf
 frame-relay lmi-type ansi
 no shutdown
end
wr
```

Step 2. Configure the LAN interface on HQ.

```
!
interface FastEthernet0/0
 description Server Farm
 ip address 10.0.1.1 255.255.255.0
 no shutdown
!
```


Step 3. Verify that HQ can ping each of the Branch routers.

```
HQ#ping 10.255.255.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.255.255.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/71/89 ms

HQ#ping 10.255.255.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.255.255.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 35/60/69 ms

HQ#ping 10.255.255.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.255.255.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 23/58/87 ms
```

Task 2: Configure PPP with CHAP and PAP Authentication

Step 1. Configure the WAN link from HQ to ISP using PPP encapsulation and CHAP authentication.

The CHAP password is **ciscochap**.

```
username ISP password ciscochap
interface Serial0/1/0
 description Link to ISP
 ip address 209.165.201.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
```

Step 2. Configure the WAN link from HQ to NewB using PPP encapsulation and PAP authentication.

You need to connect a cable to the correct interfaces. HQ is the DCE side of the link. You choose the clock rate. The PAP password is **ciscopap**.

```
username NewB password ciscopap
interface Serial0/0/1
 description Link to B4
 ip address 10.255.255.253 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username HQ password 0 ciscopap
 clock rate 64000
 no shutdown
```

Step 3. Verify that HQ can ping ISP and NewB.

```
HQ#ping 209.165.201.2

Type escape sequence to abort.
```



```
Sending 5, 100-byte ICMP Echos to 209.165.201.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 17/30/38 ms

HQ#ping 10.255.255.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.255.255.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/29/47 ms
```

Task 3: Configure Static and Dynamic NAT on HQ

Step 1. Configure NAT.

Use the following requirements:

- Allow all addresses for the 10.0.0.0/8 address space to be translated.
- XYZ Corporation owns the 209.165.200.240/29 address space. The pool, XYZCORP, uses addresses .241 through .245 with a /29 mask.
- The www.xyzcorp.com website at 10.0.1.2 is registered with the public DNS system at IP address 209.165.200.246.

```
ip access-list standard NAT_LIST
 permit 10.0.0.0 0.255.255.255
!
ip nat pool XYZCORP 209.165.200.241 209.165.200.245 netmask 255.255.255.248
ip nat inside source list NAT_LIST pool XYZCORP overload
ip nat inside source static 10.0.1.2 209.165.200.246
!
interface fa0/0
 ip nat inside
interface s0/0/0.41 point-to-point
 ip nat inside
interface s0/0/0.42 point-to-point
 ip nat inside
interface s0/0/0.43 point-to-point
 ip nat inside
interface s0/0/1
 ip nat inside
interface s0/1/0
 ip nat outside
```

Step 2. Verify NAT is operating by using extended ping.

From HQ, ping the serial 0/0/0 interface on ISP using the HQ LAN interface as the source address. This ping should succeed.

```
HQ#ping
Protocol [ip]:
Target IP address: 209.165.201.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.0.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
```



```
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.2, timeout is 2 seconds:
Packet sent with a source address of 10.0.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/34/42 ms
```

Verify that NAT translated the ping with the **show ip nat translations** command.

```
HQ#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.241:3510.0.1.1:35        209.165.201.2:35   209.165.201.2:35
icmp 209.165.200.241:3610.0.1.1:36        209.165.201.2:36   209.165.201.2:36
icmp 209.165.200.241:3710.0.1.1:37        209.165.201.2:37   209.165.201.2:37
icmp 209.165.200.241:3810.0.1.1:38        209.165.201.2:38   209.165.201.2:38
icmp 209.165.200.241:3910.0.1.1:39        209.165.201.2:39   209.165.201.2:39
---  209.165.200.246   10.0.1.2           ---                ---
```

Task 4: Configure Static and Default Routing

Step 1. Configure HQ with a default route to ISP and a static route to the NewB LAN.

Use the exit interface as an argument.

```
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
ip route 10.4.5.0 255.255.255.0 Serial0/0/1
```

Step 2. Configure the Branch routers with a default route to HQ.

Use the next-hop IP address as an argument.

```
!B1
ip route 0.0.0.0 0.0.0.0 10.255.255.1

!B2
ip route 0.0.0.0 0.0.0.0 10.255.255.5

!B3
ip route 0.0.0.0 0.0.0.0 10.255.255.9
```

Step 3. Verify connectivity beyond ISP.

All three NewB PCs and the NetAdmin PC should be able to ping the www.cisco.com web server.

```
!From NewB-PC1

Packet Tracer PC Command Line 1.0
PC>ping www.cisco.com

Pinging 209.165.202.134 with 32 bytes of data:

Request timed out.
Reply from 209.165.202.134: bytes=32 time=10ms TTL=125
Reply from 209.165.202.134: bytes=32 time=10ms TTL=125
Reply from 209.165.202.134: bytes=32 time=10ms TTL=125

Ping statistics for 209.165.202.134:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
```



```
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms

PC>

!From NetAdmin

Packet Tracer PC Command Line 1.0
PC>ping www.cisco.com

Pinging 209.165.202.134 with 32 bytes of data:

Reply from 209.165.202.134: bytes=32 time=12ms TTL=126
Reply from 209.165.202.134: bytes=32 time=188ms TTL=126
Reply from 209.165.202.134: bytes=32 time=8ms TTL=126
Reply from 209.165.202.134: bytes=32 time=8ms TTL=126

Ping statistics for 209.165.202.134:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 188ms, Average = 54ms

PC>
```

Task 5: Configure Inter-VLAN Routing

Step 1. Configure each Branch router for inter-VLAN routing.

Using the addressing table for Branch routers, configure and activate the LAN interface for inter-VLAN routing. VLAN 99 is the native VLAN.

```
!-----------------
!Branch Routers
!-----------------
!Replace the X with the router number.

interface FastEthernet0/0
 no shutdown
!
interface FastEthernet0/0.10
 description Admin VLAN 10
 encapsulation dot1Q 10
 ip address 10.X.10.1 255.255.255.0
!
interface FastEthernet0/0.20
 description Sales VLAN 20
 encapsulation dot1Q 20
 ip address 10.X.20.1 255.255.255.0
!
interface FastEthernet0/0.30
 description Production VLAN 30
 encapsulation dot1Q 30
 ip address 10.X.30.1 255.255.255.0
!
interface FastEthernet0/0.88
 description Wireless VLAN 88
 encapsulation dot1Q 88
```



```
 ip address 10.X.88.1 255.255.255.0
!
interface FastEthernet0/0.99
 description Mgmt&Native VLAN 99
 encapsulation dot1Q 99 native
 ip address 10.X.99.1 255.255.255.0
!
```

Step 2. Verify routing tables.

Each Branch router should now have six directly connected networks and one static default route.

```
B1#show ip route
<output omitted>

Gateway of last resort is 10.255.255.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.1.10.0/24 is directly connected, FastEthernet0/0.10
C       10.1.20.0/24 is directly connected, FastEthernet0/0.20
C       10.1.30.0/24 is directly connected, FastEthernet0/0.30
C       10.1.88.0/24 is directly connected, FastEthernet0/0.88
C       10.1.99.0/24 is directly connected, FastEthernet0/0.99
C       10.255.255.0/30 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 10.255.255.1
```

Task 6: Configure and Optimize EIGRP Routing

Step 1. Configure HQ, B1, B2, and B3 with EIGRP.

- Use AS 100.
- Disable EIGRP updates on appropriate interfaces.
- Manually summarize EIGRP routes so that each Branch router only advertises the 10.X.0.0/16 address space to HQ.

Note: Packet Tracer does not accurately simulate the benefit of EIGRP summary routes. Routing tables will still show all subnets, even though you correctly configured the manual summary.

```
!-----------------
!HQ Router
!-----------------

router eigrp 100
 passive-interface FastEthernet0/0
 passive-interface Serial0/0/1
 passive-interface Serial0/1/0
 network 10.0.0.0
 no auto-summary
!

!-----------------
!Branch Routers
!-----------------

!
router eigrp 100
 passive-interface FastEthernet0/0.10
 passive-interface FastEthernet0/0.20
 passive-interface FastEthernet0/0.30
```



```
 passive-interface FastEthernet0/0.99
 network 10.0.0.0
 no auto-summary
!
!
!Replace the X with the router number
!
interface serial 0/0/0
 ip summary-address eigrp 100 10.X.0.0 255.255.0.0
```

Step 2. Verify routing tables and connectivity.

HQ and the Branch routers should now have complete routing tables.

```
HQ#sh ip route
<output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 21 subnets, 2 masks
C       10.0.1.0/24 is directly connected, FastEthernet0/0
D       10.1.10.0/24 [90/2172416] via 10.255.255.2, 00:00:14, Serial0/0/0.41
D       10.1.20.0/24 [90/2172416] via 10.255.255.2, 00:00:14, Serial0/0/0.41
D       10.1.30.0/24 [90/2172416] via 10.255.255.2, 00:00:14, Serial0/0/0.41
D       10.1.88.0/24 [90/2172416] via 10.255.255.2, 00:00:14, Serial0/0/0.41
D       10.1.99.0/24 [90/2172416] via 10.255.255.2, 00:00:14, Serial0/0/0.41
D       10.2.10.0/24 [90/2172416] via 10.255.255.6, 00:00:07, Serial0/0/0.42
D       10.2.20.0/24 [90/2172416] via 10.255.255.6, 00:00:07, Serial0/0/0.42
D       10.2.30.0/24 [90/2172416] via 10.255.255.6, 00:00:07, Serial0/0/0.42
D       10.2.88.0/24 [90/2172416] via 10.255.255.6, 00:00:07, Serial0/0/0.42
D       10.2.99.0/24 [90/2172416] via 10.255.255.6, 00:00:07, Serial0/0/0.42
D       10.3.10.0/24 [90/2172416] via 10.255.255.10, 00:00:04, Serial0/0/0.43
D       10.3.20.0/24 [90/2172416] via 10.255.255.10, 00:00:04, Serial0/0/0.43
D       10.3.30.0/24 [90/2172416] via 10.255.255.10, 00:00:04, Serial0/0/0.43
D       10.3.88.0/24 [90/2172416] via 10.255.255.10, 00:00:04, Serial0/0/0.43
D       10.3.99.0/24 [90/2172416] via 10.255.255.10, 00:00:04, Serial0/0/0.43
S       10.4.5.0/24 is directly connected, Serial0/0/1
C       10.255.255.0/30 is directly connected, Serial0/0/0.41
C       10.255.255.4/30 is directly connected, Serial0/0/0.42
C       10.255.255.8/30 is directly connected, Serial0/0/0.43
C       10.255.255.252/30 is directly connected, Serial0/0/1
     209.165.201.0/30 is subnetted, 1 subnets
C       209.165.201.0 is directly connected, Serial0/1/0
S*   0.0.0.0/0 is directly connected, Serial0/1/0
```

The NetAdmin PC should now be able to ping each VLAN subinterface on each Branch router.

```
!From NetAdmin PC

Packet Tracer PC Command Line 1.0
PC>ping 10.1.10.1

Pinging 10.1.10.1 with 32 bytes of data:

Reply from 10.1.10.1: bytes=32 time=104ms TTL=254
Reply from 10.1.10.1: bytes=32 time=104ms TTL=254
Reply from 10.1.10.1: bytes=32 time=100ms TTL=254
Reply from 10.1.10.1: bytes=32 time=132ms TTL=254
```



```
Ping statistics for 10.1.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 100ms, Maximum = 132ms, Average = 110ms

PC>ping 10.2.20.1

Pinging 10.2.20.1 with 32 bytes of data:

Reply from 10.2.20.1: bytes=32 time=83ms TTL=254
Reply from 10.2.20.1: bytes=32 time=152ms TTL=254
Reply from 10.2.20.1: bytes=32 time=118ms TTL=254
Reply from 10.2.20.1: bytes=32 time=103ms TTL=254

Ping statistics for 10.2.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 83ms, Maximum = 152ms, Average = 114ms

PC>ping 10.3.30.1

Pinging 10.3.30.1 with 32 bytes of data:

Reply from 10.3.30.1: bytes=32 time=114ms TTL=254
Reply from 10.3.30.1: bytes=32 time=99ms TTL=254
Reply from 10.3.30.1: bytes=32 time=108ms TTL=254
Reply from 10.3.30.1: bytes=32 time=153ms TTL=254

Ping statistics for 10.3.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 99ms, Maximum = 153ms, Average = 118ms
```

Task 7: Configure VTP, Trunking, the VLAN Interface, and VLANs

The following requirements apply to all three Branches. Configure one set of three switches. Then use the scripts for those switches on the other two sets of switches.

Step 1. Configure Branch switches with VTP.

- BX-S1 is the VTP server. BX-S2 and BX-S3 are VTP clients.
- The domain name is **XYZCORP**.
- The password is **xyzvtp**.

Step 2. Configure trunking on BX-S1, BX-S2, and BX-S3.

Configure the appropriate interfaces in trunking mode and assign VLAN 99 as the native VLAN.

Step 3. Configure the VLAN interface and default gateway on BX-S1, BX-S2, and BX-S3.

Step 4. Create the VLANs on BX-S1.

Create and name the VLANs listed in the VLAN Configuration and Port Mappings table on BX-S1 only. VTP advertises the new VLANs to BX-S2.

```
!
!Replace the "X" in the following scripts with the Branch number
!
```



```
!-----------
!S1
!-----------
enable
configure terminal
host BX-S1
enable secret class
banner motd $AUTHORIZED ACCESS ONLY!$
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
service password-encryption
!
vtp mode server
vtp domain xyzcorp
vtp password xyzvtp
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk native vlan 99
 switchport mode trunk
!
interface vlan 99
 ip address 10.X.99.21 255.255.255.0
 no shut
ip default-gateway 10.X.99.1
!
vlan 10
 name Admin
vlan 20
 name Sales
vlan 30
 name Production
vlan 88
 name Wireless
vlan 99
 name Mgmt&Native
end
wr
```



```
!-----------
!S2
!-----------
enable
configure terminal
host BX-S2
enable secret class
banner motd $AUTHORIZED ACCESS ONLY!$
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
service password-encryption
!
vtp mode client
vtp domain xyzcorp
vtp password xyzvtp
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface vlan 99
 ip address 10.X.99.22 255.255.255.0
 no shut
ip default-gateway 10.X.99.1
!
end
wr

!-----------
!S3
!-----------
enable
configure terminal
host BX-S3
enable secret class
banner motd $AUTHORIZED ACCESS ONLY!$
line con 0
pass cisco
login
line vty 0 4
```



```
pass cisco
login
service password-encryption
!
vtp mode client
vtp domain xyzcorp
vtp password xyzvtp
!
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport mode trunk
!
interface vlan 99
 ip address 10.X.99.23 255.255.255.0
 no shut
ip default-gateway 10.X.99.1
!
end
wr
```

Step 5. Verify that VLANs have been sent to BX-S2 and BX-S3.

Use the appropriate commands to verify that S2 and S3 now have the VLANs you created on S1. It may take a few minutes for Packet Tracer to simulate the VTP advertisements. A quick way to force the sending of VTP advertisements is to change one of the client switches to transparent mode and then back to client mode.

```
!All switches will have similar output. VTP operating mode is server
!for all BX-S1 switches.

B2-S2#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 64
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : xyzcorp
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xCD 0xBF 0xDE 0x4E 0x0F 0x79 0x7D 0x3E
Configuration last modified by 10.2.99.21 at 3-1-93 00:43:41

B2-S2#show vlan brief

VLAN Name                              Status    Ports
```



```
---- -------------------------------- --------- -------------------------------
1    default                          active  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                              Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                              Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                              Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                              Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig1/1, Gig1/2
10   Admin                            active
20   Sales                            active
30   Production                       active
88   Wireless                         active
99   Mgmt&Native                      active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Task 8: Assign VLANs and Configure Port Security

Step 1. Assign VLANs to access ports.

Use the VLAN Configuration and Port Mappings table to complete the following requirements:

- Configure access ports
- Assign VLANs to the access ports

Step 2. Configure port security.

Use the following policy to establish port security on the BX-S2 access ports:

- Allow only one MAC address
- Configure the first learned MAC address to “stick” to the configuration
- Set the port to shut down if there is a security violation

```
!-----------
!BX-S3
!-----------
!
interface FastEthernet0/7
 switchport access vlan 88
 switchport mode access

!-----------
!BX-S2
!-----------

!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 1
 switchport port-security mac-address sticky
 switchport port-security violation shutdown
!
interface FastEthernet0/11
 switchport access vlan 20
 switchport mode access
 switchport port-security
```



```
 switchport port-security maximum 1
 switchport port-security mac-address sticky
 switchport port-security violation shutdown
!
interface FastEthernet0/16
 switchport access vlan 30
 switchport mode access
 switchport port-security
 switchport port-security maximum 1
 switchport port-security mac-address sticky
 switchport port-security violation shutdown
!
```

Step 3. Verify VLAN assignments and port security.

Use the appropriate commands to verify that access VLANs are correctly assigned and that the port security policy has been enabled.

```
B1-S2#show vlan brief

VLAN Name                              Status  Ports
---- --------------------------------- ------- -------------------------------
1    default                           active  Fa0/5, Fa0/7, Fa0/8, Fa0/9
                                               Fa0/10, Fa0/12, Fa0/13, Fa0/14
                                               Fa0/15, Fa0/17, Fa0/18, Fa0/19
                                               Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                               Fa0/24, Gig1/1, Gig1/2
10   Admin                             active  Fa0/6
20   Sales                             active  Fa0/11
30   Production                        active  Fa0/16
88   Wireless                          active
99   Mgmt&Native                       active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active

B1-S2#show port-security interface fa0/6
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Task 9: Configure STP

Step 1. Configure BX-S1 as the root bridge.

Set the priority level to 4096 on BX-S1 so that these switches are always the root bridge for all VLANs.

```
!-----------
!BX-S1
```



```
!-----------
!
spanning-tree vlan 1 priority 4096
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 4096
spanning-tree vlan 30 priority 4096
spanning-tree vlan 88 priority 4096
spanning-tree vlan 99 priority 4096
!
```

Step 2. Configure BX-S3 as the backup root bridge.

Set the priority level to 8192 on BX-S3 so that these switches are always the backup root bridge for all VLANs.

```
!-----------
!BX-S3
!-----------
!
spanning-tree vlan 1 priority 8192
spanning-tree vlan 10 priority 8192
spanning-tree vlan 20 priority 8192
spanning-tree vlan 30 priority 8192
spanning-tree vlan 88 priority 8192
spanning-tree vlan 99 priority 8192
!
```

Step 3. Verify that BX-S1 is the root bridge.

```
!Output should be similar for all VLANs on all switches.
!
B1-S1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority    4106
             Address     00D0.BA3D.2C94
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    4106  (priority 4116 sys-id-ext 10)
             Address     00D0.BA3D.2C94
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/3            Desg FWD 19        128.3    Shr
Fa0/1            Desg FWD 19        128.3    Shr
Fa0/2            Desg FWD 19        128.3    Shr
Fa0/5            Desg FWD 19        128.3    Shr
Fa0/4            Desg FWD 19        128.3    Shr
```

Task 10: Configure DHCP

Step 1. Configure DHCP pools for each VLAN.

On the Branch routers, configure DHCP pools for each VLAN using the following requirements:

- Exclude the first 10 IP addresses in each pool for the LANs.

- Exclude the first 24 IP addresses in each pool for the wireless LANs.
- The pool name is **BX_VLAN##** where **X** is the router number and ## is the VLAN number.
- Include the DNS server attached to the HQ server farm as part of the DHCP configuration.

```
!-----------
!B1
!-----------
!
ip dhcp excluded-address 10.1.10.1 10.1.10.10
ip dhcp excluded-address 10.1.20.1 10.1.20.10
ip dhcp excluded-address 10.1.30.1 10.1.30.10
ip dhcp excluded-address 10.1.88.1 10.1.88.24
!
ip dhcp pool B1_VLAN10
 network 10.1.10.0 255.255.255.0
 default-router 10.1.10.1
 dns-server 10.0.1.4
ip dhcp pool B1_VLAN20
 network 10.1.20.0 255.255.255.0
 default-router 10.1.20.1
 dns-server 10.0.1.4
ip dhcp pool B1_VLAN30
 network 10.1.30.0 255.255.255.0
 default-router 10.1.30.1
 dns-server 10.0.1.4
ip dhcp pool B1_VLAN88
 network 10.1.88.0 255.255.255.0
 default-router 10.1.88.1
 dns-server 10.0.1.4

!-----------
!B2
!-----------
!
ip dhcp excluded-address 10.2.10.1 10.2.10.10
ip dhcp excluded-address 10.2.20.1 10.2.20.10
ip dhcp excluded-address 10.2.30.1 10.2.30.10
ip dhcp excluded-address 10.2.88.1 10.2.88.24
!
ip dhcp pool B2_VLAN10
 network 10.2.10.0 255.255.255.0
 default-router 10.2.10.1
 dns-server 10.0.1.4
ip dhcp pool B2_VLAN20
 network 10.2.20.0 255.255.255.0
 default-router 10.2.20.1
 dns-server 10.0.1.4
ip dhcp pool B2_VLAN30
 network 10.2.30.0 255.255.255.0
 default-router 10.2.30.1
 dns-server 10.0.1.4
ip dhcp pool B2_VLAN88
 network 10.2.88.0 255.255.255.0
 default-router 10.2.88.1
 dns-server 10.0.1.4

!-----------
```



```
!B3
!-----------
!
ip dhcp excluded-address 10.3.10.1 10.3.10.10
ip dhcp excluded-address 10.3.20.1 10.3.20.10
ip dhcp excluded-address 10.3.30.1 10.3.30.10
ip dhcp excluded-address 10.3.88.1 10.3.88.24
!
ip dhcp pool B3_VLAN10
 network 10.3.10.0 255.255.255.0
 default-router 10.3.10.1
 dns-server 10.0.1.4
ip dhcp pool B3_VLAN20
 network 10.3.20.0 255.255.255.0
 default-router 10.3.20.1
 dns-server 10.0.1.4
ip dhcp pool B3_VLAN30
 network 10.3.30.0 255.255.255.0
 default-router 10.3.30.1
 dns-server 10.0.1.4
ip dhcp pool B3_VLAN88
 network 10.3.88.0 255.255.255.0
 default-router 10.3.88.1
 dns-server 10.0.1.4
```

Step 2. Configure the PCs to use DHCP.

Currently, the PCs are configured to use static IP addresses. Change this configuration to DHCP.

Step 3. Verify that the PCs and wireless routers have an IP address.

Step 4. Verify connectivity.

All PCs physically attached to the network should be able to ping the www.cisco.com web server.

```
!From B1-PC1

Packet Tracer PC Command Line 1.0
PC>ping www.cisco.com

Pinging 209.165.202.134 with 32 bytes of data:

Reply from 209.165.202.134: bytes=32 time=234ms TTL=125
Reply from 209.165.202.134: bytes=32 time=184ms TTL=125
Reply from 209.165.202.134: bytes=32 time=230ms TTL=125
Reply from 209.165.202.134: bytes=32 time=228ms TTL=125

Ping statistics for 209.165.202.134:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 184ms, Maximum = 234ms, Average = 219ms

PC>
```


Task 11: Configure a Firewall ACL

Step 1. Verify connectivity from Outside Host.

The Outside Host PC should be able to ping the server at www.xyzcorp.com.

```
!-----------
!Outside Host
!-----------
!
Packet Tracer PC Command Line 1.0
PC>ping www.xyzcorp.com

Pinging 209.165.200.246 with 32 bytes of data:

Reply from 209.165.200.246: bytes=32 time=45ms TTL=126
Reply from 209.165.200.246: bytes=32 time=115ms TTL=126
Reply from 209.165.200.246: bytes=32 time=124ms TTL=126
Reply from 209.165.200.246: bytes=32 time=101ms TTL=126

Ping statistics for 209.165.200.246:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 45ms, Maximum = 124ms, Average = 96ms

PC>
```

Step 2. Implement a basic firewall ACL.

Because ISP represents connectivity to the Internet, configure a named ACL called **FIREWALL** in the following order:

1. Allow inbound HTTP requests to the www.xyzcorp.com server.
2. Allow only established TCP sessions from ISP and any source beyond ISP.
3. Allow only inbound ping replies from ISP and any source beyond ISP.
4. Explicitly block all other inbound access from ISP and any source beyond ISP.

```
!-----------
!HQ
!-----------

ip access-list extended FIREWALL
 permit tcp any host 209.165.200.244 eq www
 permit tcp any any established
 permit icmp any any echo-reply
 deny ip any any
!
interface Serial0/1/0
 ip access-group FIREWALL in
```

Step 3. Verify connectivity from Outside Host.

The Outside Host PC should not be able to ping the server at www.xyzcorp.com. However, the Outside Host PC should be able to request a web page.

```
!-----------
!Outside Host
!-----------
!
PC>ping www.xyzcorp.com
```



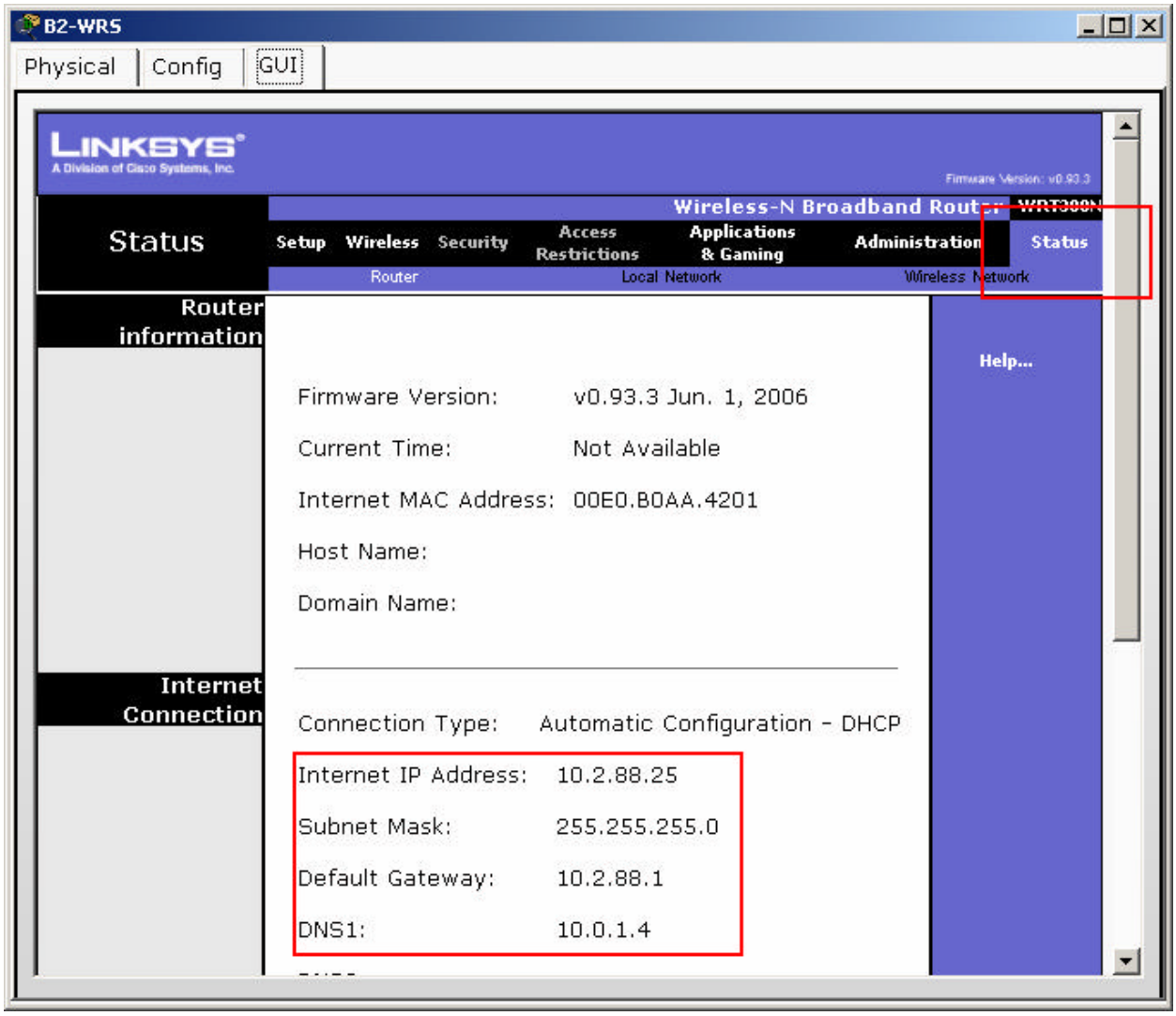
```
Pinging 209.165.200.246 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 209.165.200.246:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
```

Task 12: Configure Wireless Connectivity

Step 1. Verify the DHCP configuration.

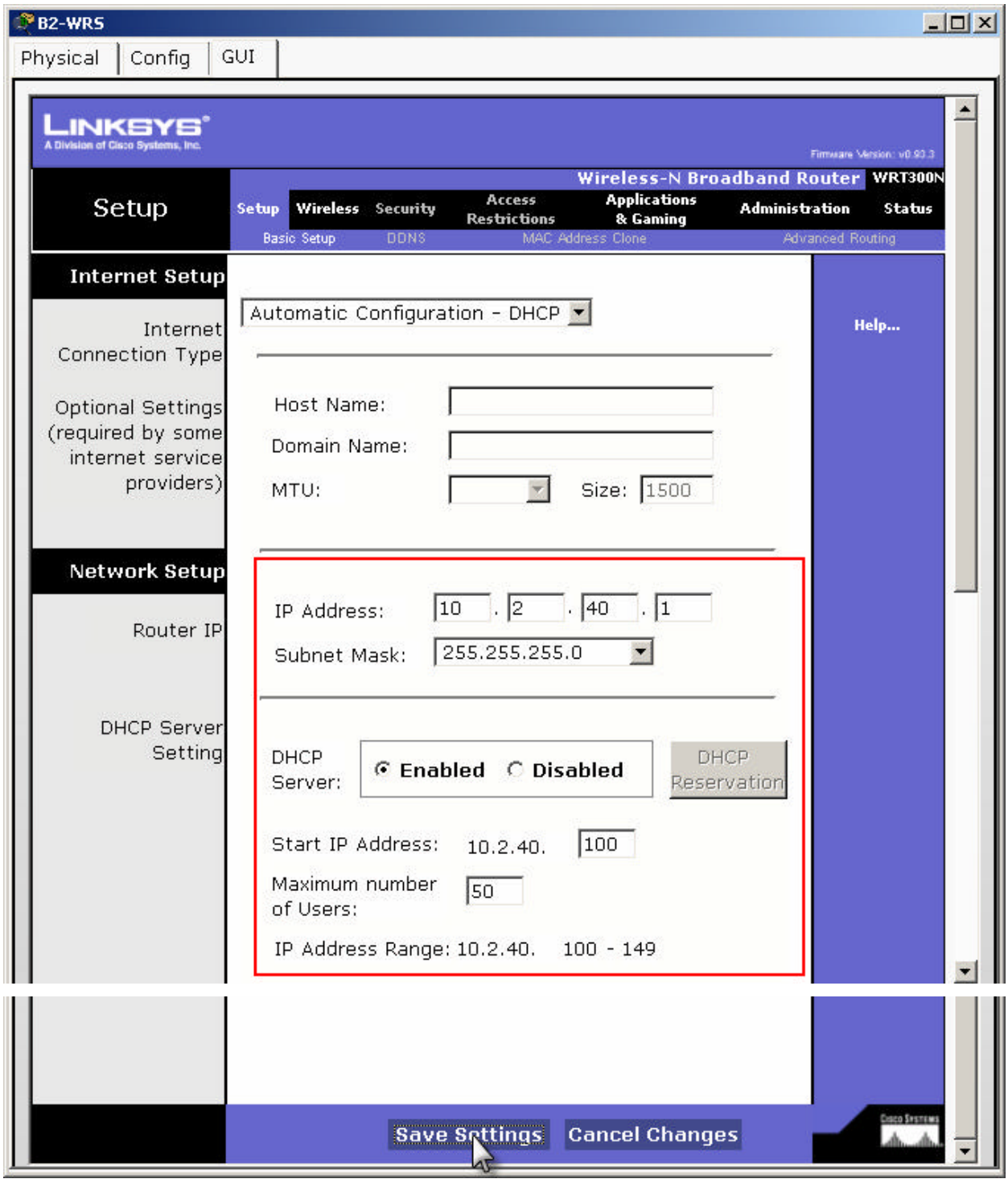
Each BX-WRS router should already have IP addressing from the DHCP of the BX router for VLAN 88.

Graphics in this task are for the Instructor version only



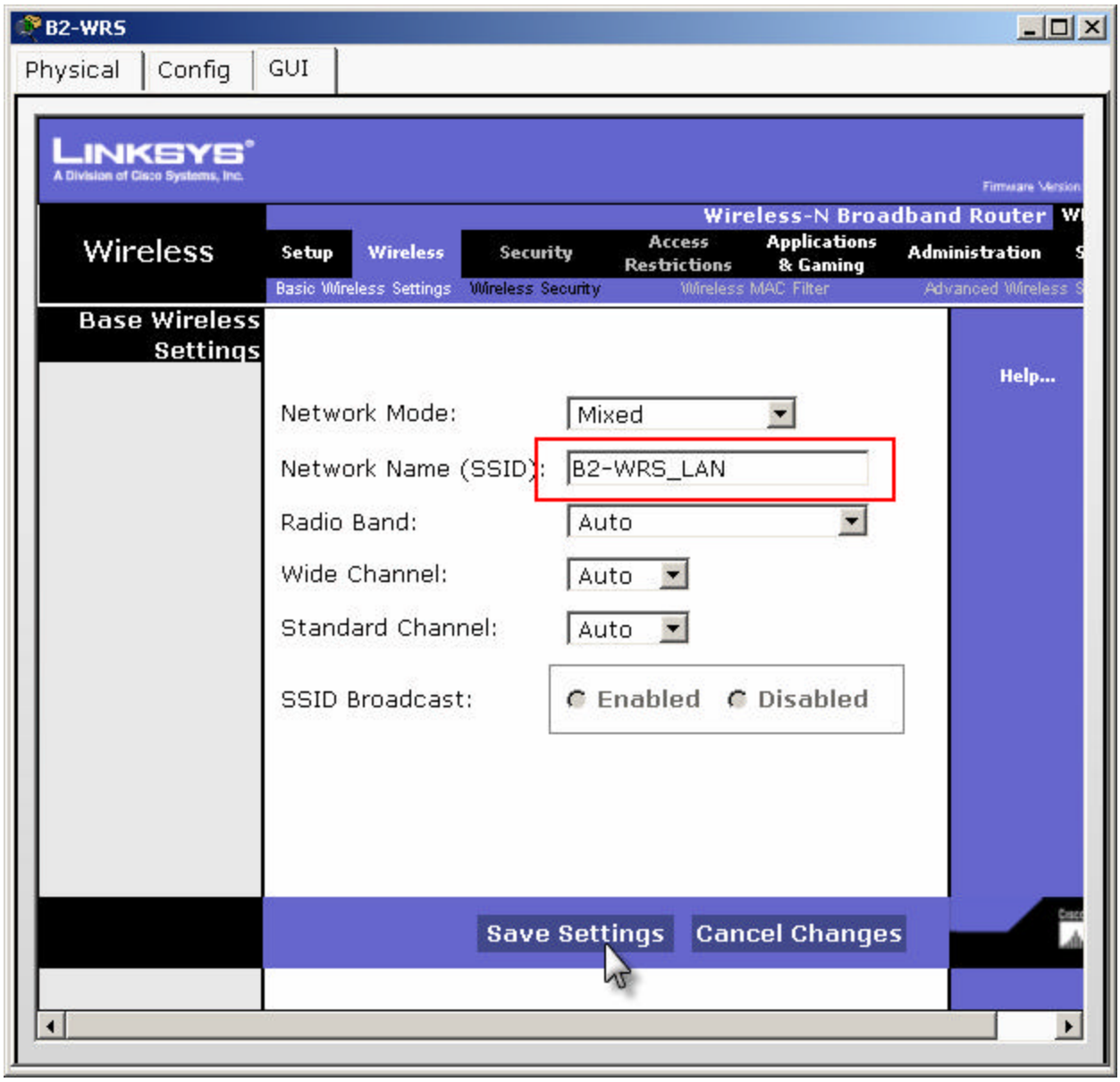
Step 2. Configure the Network Setup/LAN settings.

The “Router IP” on the **Status** page in the GUI tab should be the first IP of the 10.X.40.0 /24 subnet. Leave all other settings at the default.

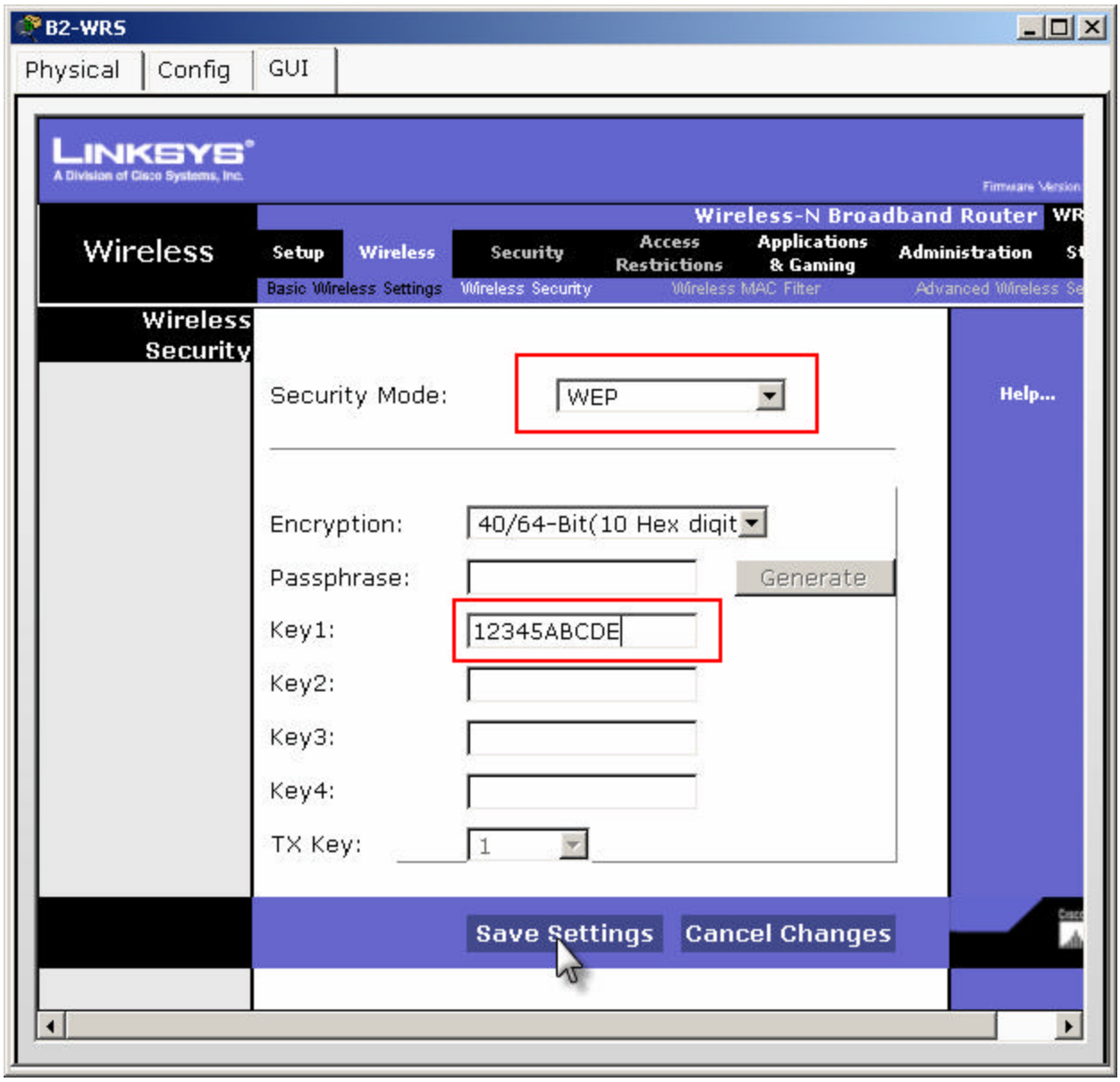


Step 3. Configure the wireless network settings.

The SSIDs for the routers are **BX-WRS_LAN** where the **X** is the Branch router number.

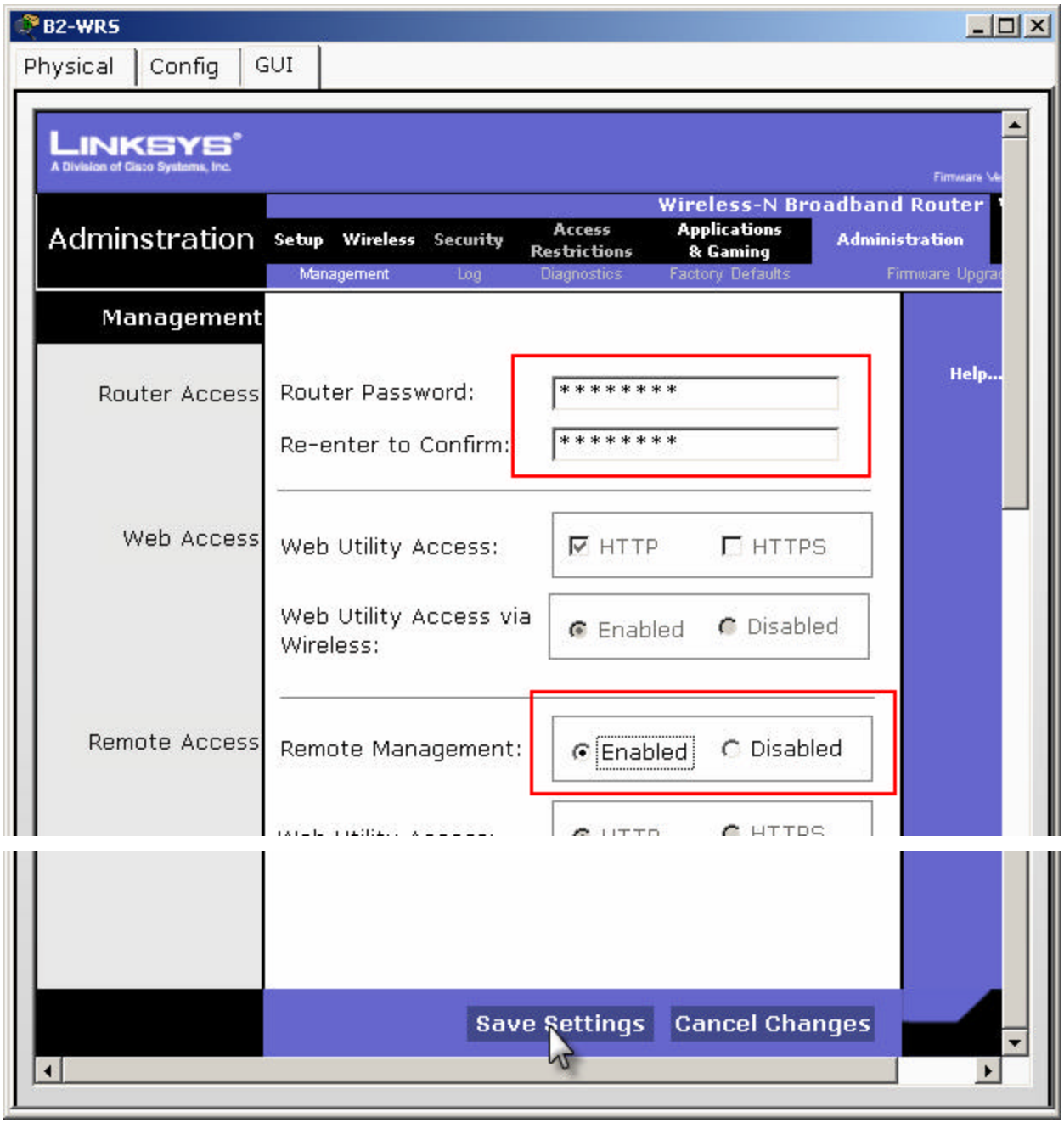


The WEP key is **12345ABCDE**

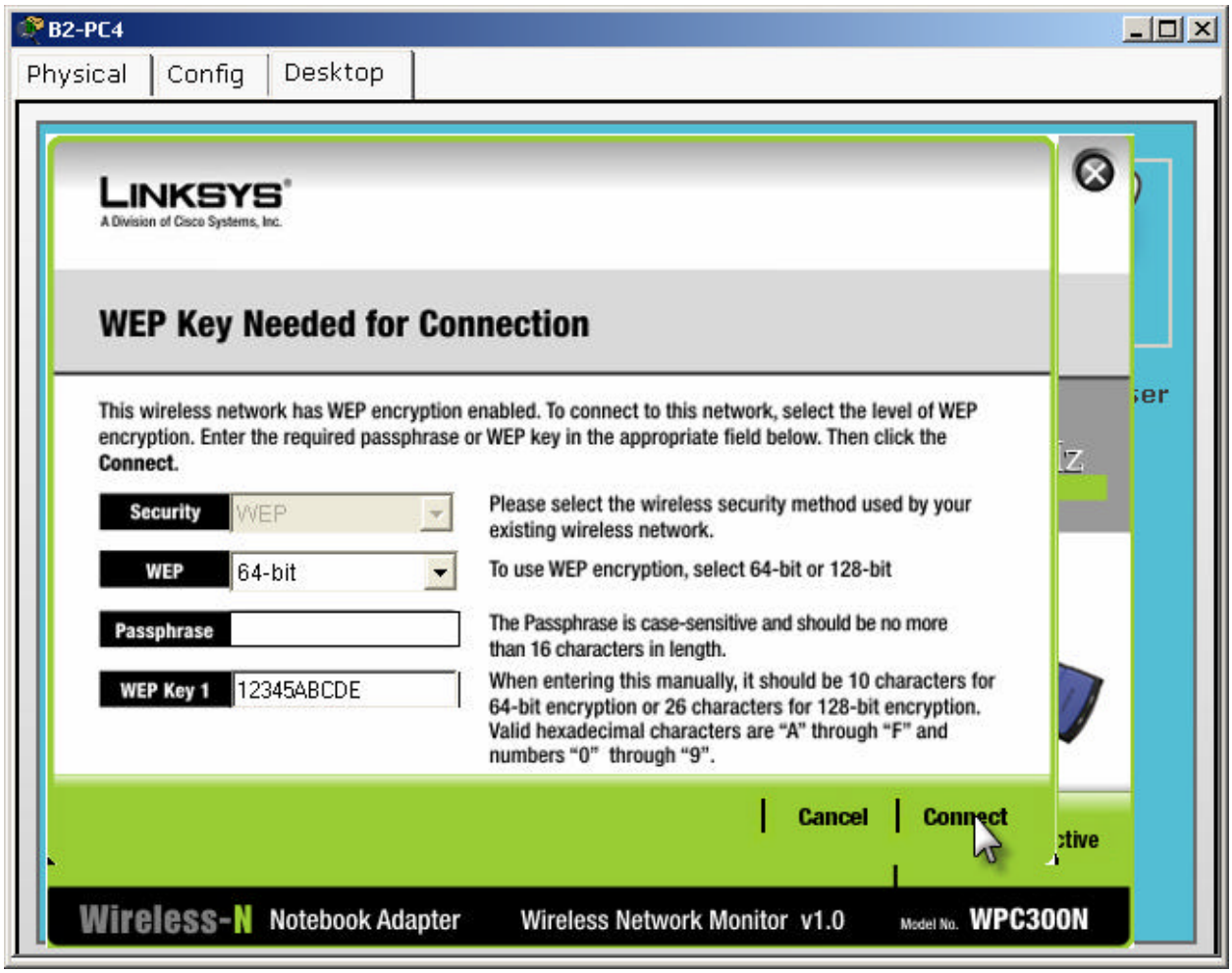


Step 4. Configure the wireless routers for remote access.

Configure the administration password as **cisco123** and enable remote management.

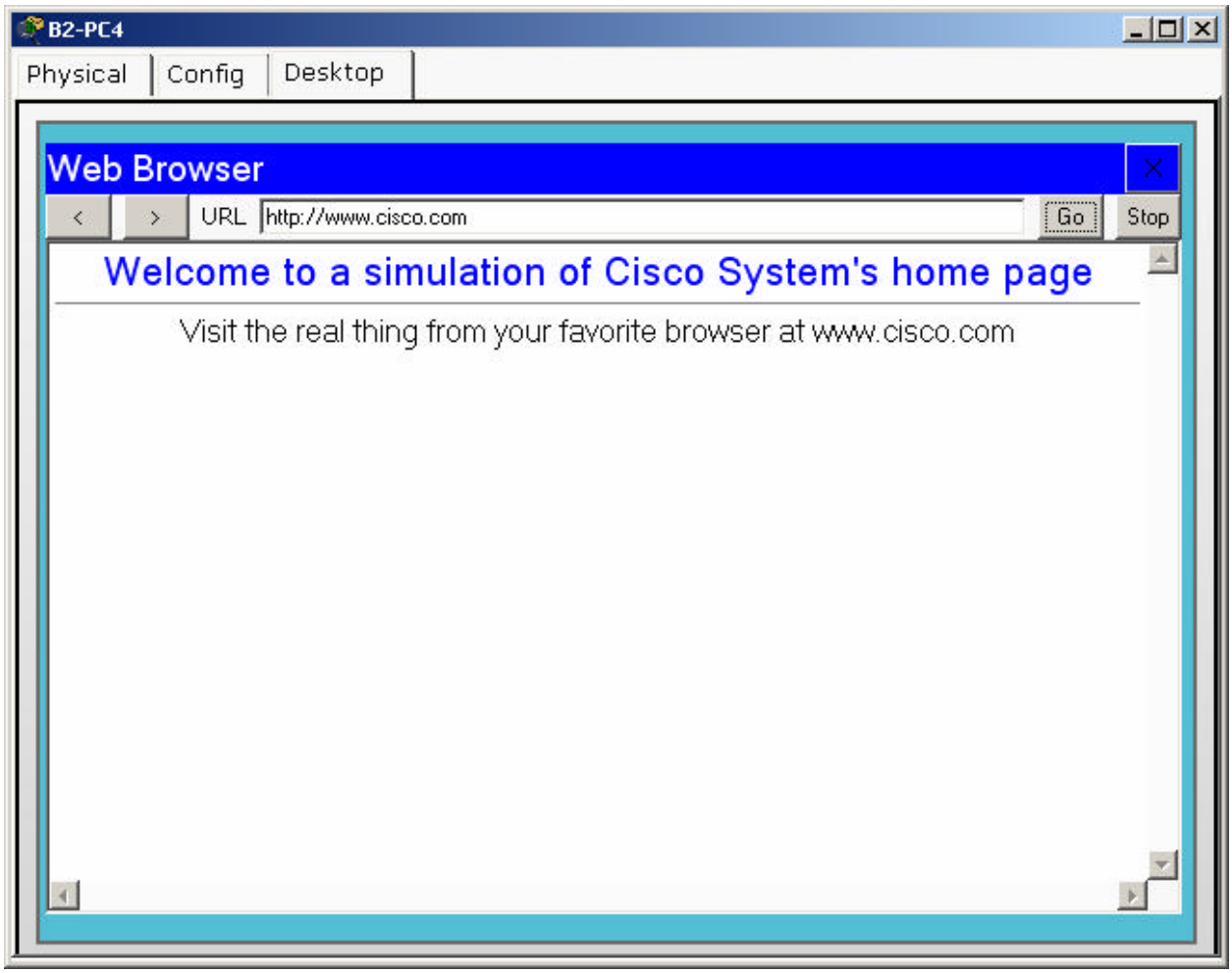


Step 5. Configure the BX-PC4 PCs to access the wireless network using DHCP.

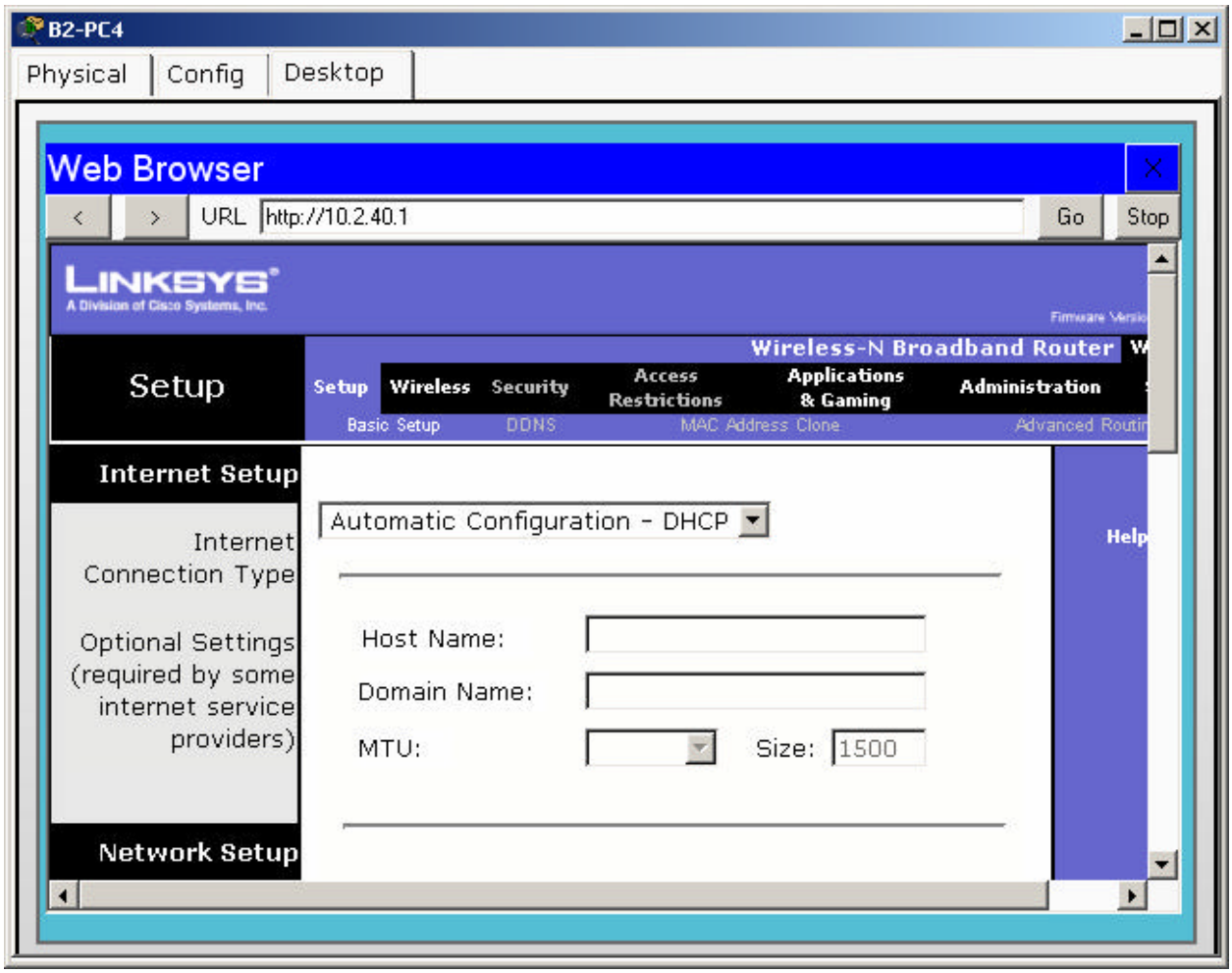


Step 6. Verify connectivity and remote management capability.

Each wireless PC should be able to access the www.cisco.com web server.



Verify remote management capability by accessing the wireless router through the web browser.



Task 13: Network Troubleshooting

Step 1. Break the network.

One student leaves the room, if necessary, while another student breaks the configuration.

Step 2. Troubleshoot the problem.

The student returns and uses troubleshooting techniques to isolate and solve the problem.

Step 3. Break the network again.

The students switch roles and repeat steps 1 and 2.

