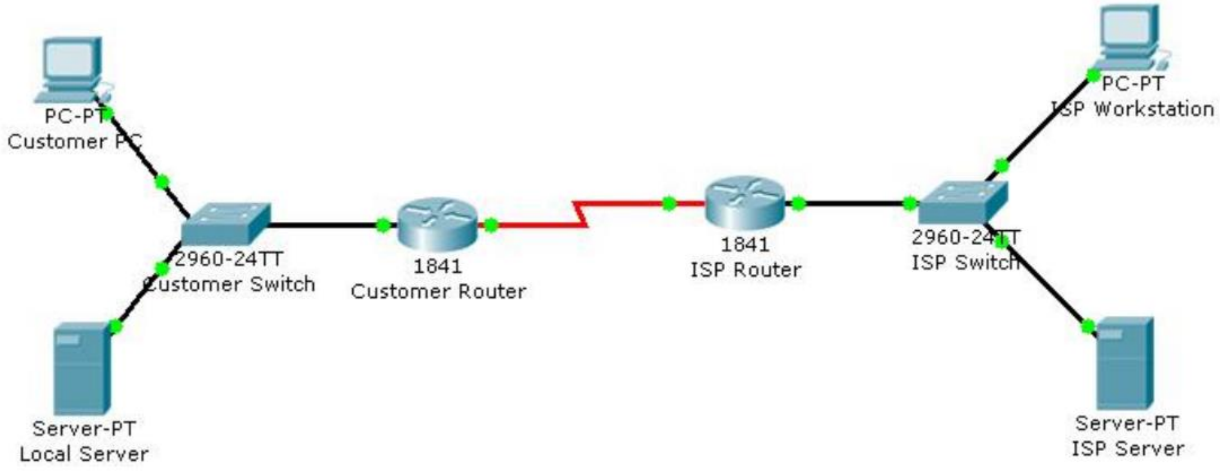
INDEX

Practical 1

Performing an Initial Switch Configuration

Topology



Step 1: Configure the switch host name.

- From the Customer PC, use a console cable and terminal emulation software to connect to the console of the customer Cisco Catalyst 2960 switch.
- Set the host name on the switch to CustomerSwitch using these commands.

```
Switch>enable
Switch#configure terminal
Switch(config)#hostname CustomerSwitch
```

Step 2: Configure the privileged mode password and secret.

- From global configuration mode, configure the password as cisco.
  `CustomerSwitch(config)#enable password cisco`
- From global configuration mode, configure the secret as cisco123.
  `CustomerSwitch(config)#enable secret cisco123`

Step 3: Configure the console password.

a. From global configuration mode, switch to configuration mode to configure the console line.

```
CustomerSwitch(config)#line console 0
```

b. From line configuration mode, set the password to cisco and require the password to be entered at login.

```
CustomerSwitch(config-line)#password cisco
CustomerSwitch(config-line)#login
CustomerSwitch(config-line)#exit
```

Step 4: Configure the vty password.

From global configuration mode, switch to the configuration mode for the vty lines 0 through 15.

```
CustomerSwitch(config)#line vty 0 15
```

From line configuration mode, set the password to cisco and require the password to be entered at login.

```
CustomerSwitch(config-line)#password cisco
CustomerSwitch(config-line)#login
CustomerSwitch(config-line)#exit
```

Step 5: Configure an IP address on interface VLAN1.

From global configuration mode, switch to interface configuration mode for VLAN1, and assign the IP address 192.168.1.5 with the subnet mask of 255.255.255.0.

```
CustomerSwitch(config)#interface vlan 1
CustomerSwitch(config-if)#ip address 192.168.1.5 255.255.255.0
CustomerSwitch(config-if)#no shutdown
CustomerSwitch(config-if)#exit
```

Step 6: Configure the default gateway.

- From global configuration mode, assign the default gateway to 192.168.1.1.

  ```
  CustomerSwitch(config)#ip default-gateway 192.168.1.1
  ```

- Click the Check Results button at the bottom of this instruction window to check your work.

Step 7: Verify the configuration.

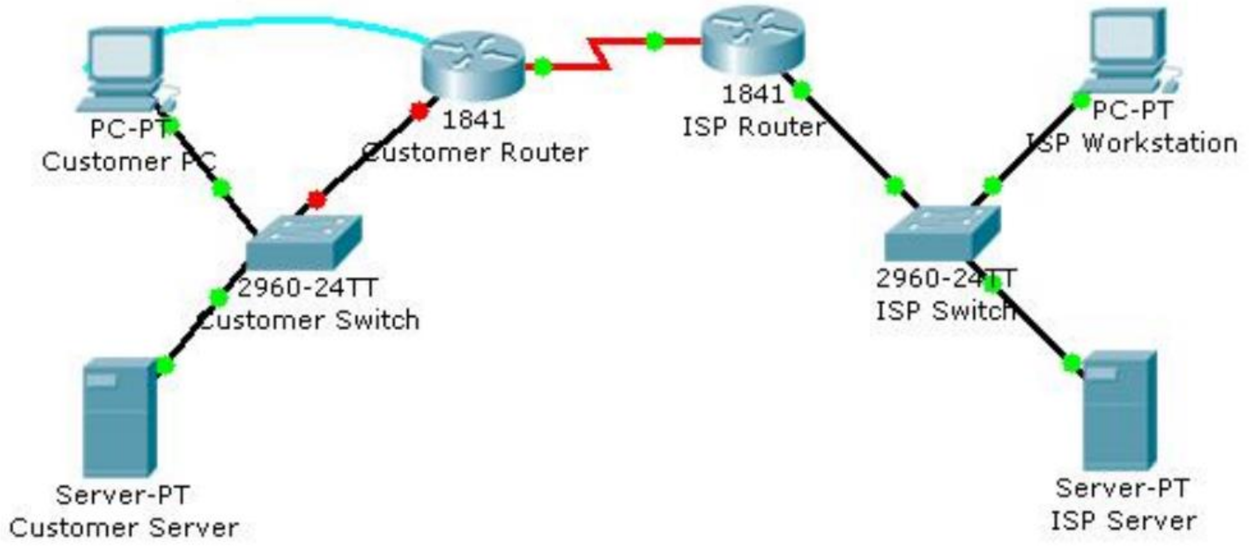
The Customer Switch should now be able to ping the ISP Server at 209.165.201.10. The first one or two pings may fail while ARP converges.

```
CustomerSwitch(config)#end
CustomerSwitch#ping 209.165.201.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.201.10, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 181/189/197 ms
CustomerSwitch#
```

Practical 2

Performing an Initial Router Configuration

Topology



Step 1: Configure the router host name.

On Customer PC, use the terminal emulation software to connect to the console of the customer Cisco 1841 ISR. Set the host name on the router to CustomerRouter by using these commands.

```
Router>enable
Router#configure terminal
Router(config)#hostname CustomerRouter
```

Step 2: Configure the privileged mode and secret passwords.

In global configuration mode, set the password to cisco.

```
CustomerRouter(config)#enable password cisco
```

Set an encrypted privileged password to cisco123 using the secret command.

```
CustomerRouter(config)#enable secret cisco123
```

Step 3: Configure the console password.

In global configuration mode, switch to line configuration mode to specify the console line.

```
CustomerRouter(config)#line console 0
```

Set the password to cisco123, require that the password be entered at login, and then exit line configuration mode.

```
CustomerRouter(config-line)#password cisco123
CustomerRouter(config-line)#login
CustomerRouter(config-line)#exit
CustomerRouter(config)#
```

Step 4: Configure the vty password to allow Telnet access to the router.

In global configuration mode, switch to line configuration mode to specify the vty lines.

```
CustomerRouter(config)#line vty 0 4
```

Set the password to cisco123, require that the password be entered at login, exit line configuration mode, and then exit the configuration session.

```
CustomerRouter(config-line)#password cisco123
CustomerRouter(config-line)#login
CustomerRouter(config-line)#exit
CustomerRouter(config)#
```

Step 5: Configure password encryption, a MOTD banner, and turn off domain server lookup.

Currently, the line passwords and the enable password are shown in clear text when you show the running configuration. Verify this now by entering the show running-config command. To avoid the security risk of someone looking over your shoulder and reading the passwords, encrypt all clear text passwords.

```
CustomerRouter(config)#service password-encryption
```

Use the show running-config command again to verify that the passwords are encrypted. To provide a warning when someone attempts to log in to the router, configure a MOTD banner.

```
CustomerRouter(config)#banner motd $Authorized Access Only!$
```

Test the banner and passwords. Log out of the router by typing the exit command twice. The banner displays before the prompt for a password. Enter the password to log back into the router. You may have noticed that when you enter a command incorrectly at the user or privileged EXEC prompt, the router pauses while trying to locate an IP address for the mistyped word you entered. For example, this output shows what happens when the enable command is mistyped.

```
CustomerRouter>emable

Translating "emable"...domain server (255.255.255.255)
```

To prevent this from happening, use the following command to stop all DNS lookups from the router CLI.

```
CustomerRouter(config)#no ip domain-lookup
```

Save the running configuration to the startup configuration.

```
CustomerRouter(config)#end
CustomerRouter#copy run start
```

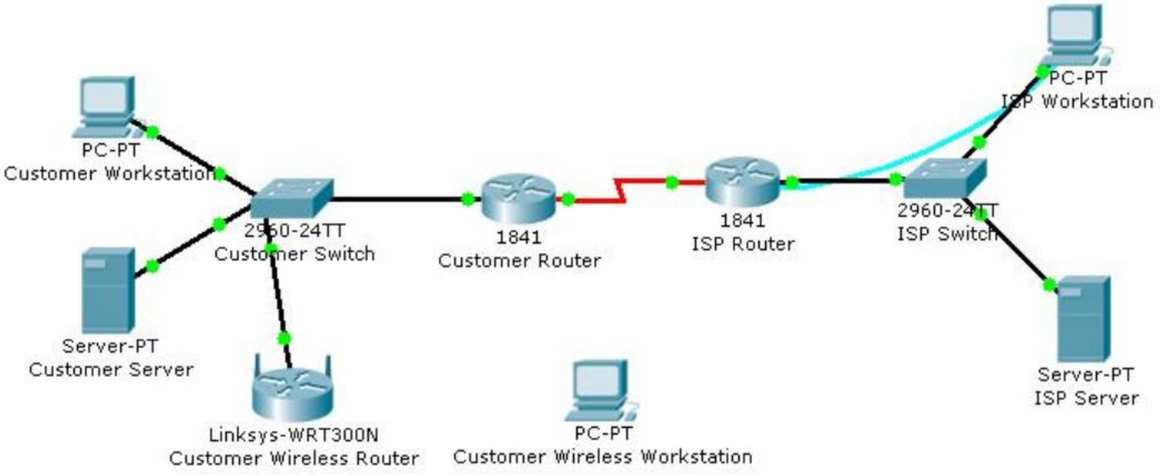
Step 6: Verify the configuration.

- Log out of your terminal session with the Cisco 1841 customer router.
- Log in to the Cisco 1841 Customer Router. Enter the console password when prompted.
- Navigate to privileged EXEC mode. Enter the privileged EXEC password when prompted.
- Click the Check Results button at the bottom of this instruction window to check your work.

Practical 3

Configuring WEP on a Wireless Router

Topology



Step 1: Configure the Linksys wireless router to require WEP.

1. **Click the Customer Wireless Router icon. Then, click the GUI tab to access the router web**
2. management interface.
3. Click the Wireless menu option and change the Network Name (SSID) from Default to
4. CustomerWireless. Leave the other settings with their default options.
5. Click the Save Settings button at the bottom of the Basic Wireless Settings window.
6. Click the Wireless Security submenu under the Wireless menu to display the current wireless
7. security parameters.
8. From the Security Mode drop-down menu, select WEP. f. In the Key1 text box, type 1a2b3c4d5e. This will be the new WEP pre-shared key to access the
9. wireless network.
10. Click the Save Settings button at the bottom of the Wireless Security window.

Step 2: Configure WEP on the customer wireless workstation.

1. Click the Customer Wireless Workstation. b. Click the Config tab.
2. Click the Wireless button to display the current wireless configuration settings on the workstation.
3. Change the SSID to CustomerWireless. e. Change the Security Mode to WEP. Enter 1a2b3c4d5e in the Key text box, and then close the window.

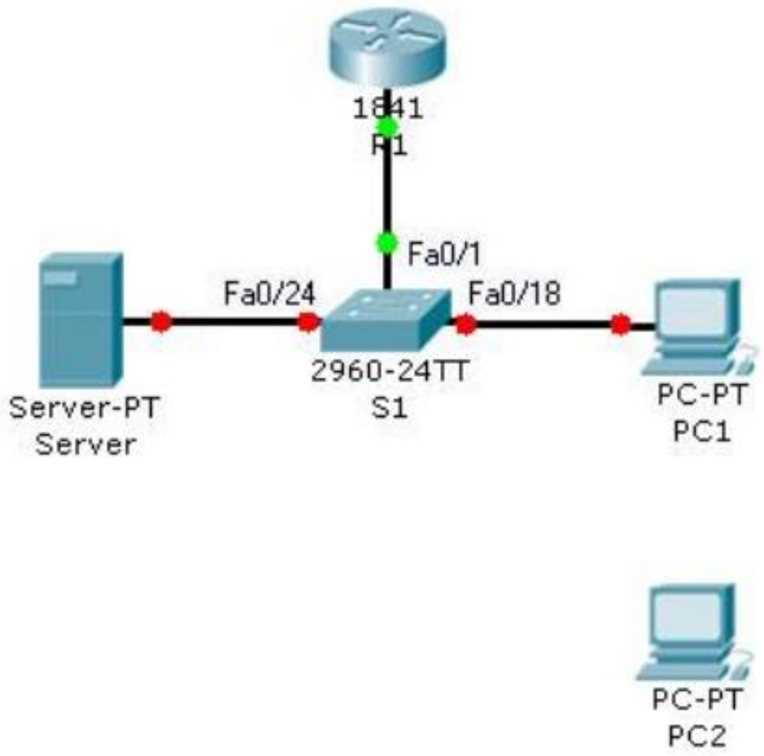
Step 3: Verify the configuration.

1. After you configure the correct WEP key and SSID on the customer wireless workstation, notice that there is a
2. wireless connection between the workstation and the wireless router.
3. Click the Customer Wireless Workstation.
4. Click the Desktop tab to view the applications that are available.
5. Click on the Command Prompt application to bring up the command prompt.
6. Type ipconfig /all and press Enter to view the current network configuration settings.
7. Type ping 192.168.2.1 to verify connectivity to the LAN interface of the customer wireless router.
8. Close the command prompt window.
9. Open a web browser.
10. In the address bar of the web browser window, type http://192.168.1.10. Press Enter. The Intranet web page that is running on the customer server appears. You have just verified that the customer wireless workstation has connectivity to the rest of the customer network.
11. Click the Check Results button at the bottom of this instruction window to check your work

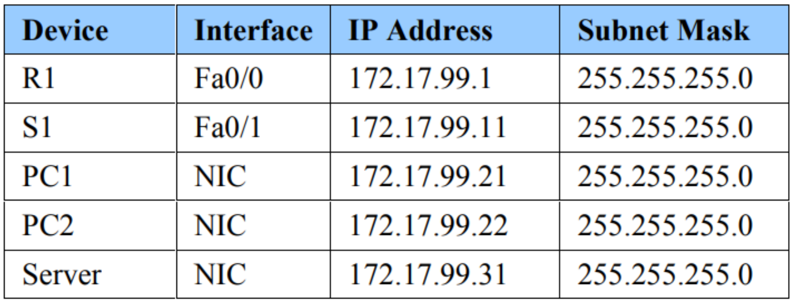
Practical 4

Configuring and Troubleshooting a Switched Network

Topology



Addressing Table



Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	172.17.99.1	255.255.255.0
S1	Fa0/1	172.17.99.11	255.255.255.0
PC1	NIC	172.17.99.21	255.255.255.0
PC2	NIC	172.17.99.22	255.255.255.0
Server	NIC	172.17.99.31	255.255.255.0

Step 1: Establish a console connection to a switch.

For this activity, direct access to the S1 Config and CLI tabs is disabled. You must establish a console session through PC1.

- Connect a console cable from PC1 to S1.
- From PC1, open a terminal window and use the default terminal configuration. You should now have access to the CLI for S1.
- Check results.

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

Step 2: Configure the host name and VLAN 1.

- Configure the switch host name as S1.
- Configure port Fa0/1. Set the mode on Fast Ethernet 0/1 to access mode.

i. S1(config)#interface fastethernet 0/1

ii. S1(config-if)#switchport mode access

- Configure IP connectivity on S1 using VLAN 1.

i. S1(config)#interface vlan 1

ii. S1(config-if)#ip address 172.17.99.11 255.255.255.0

iii. S1(config-if)#no shutdown

- Configure the default gateway for S1 and then test connectivity. S1 should be able to ping R1.
- Check results.

Your completion percentage should be 31%. If not, click Check Results to see which required components are not yet completed. Also, make sure that interface VLAN 1 is active.

Step 3: Configure the current time using Help.

- Configure the clock to the current time. At the privileged EXEC prompt, enter clock ?.
- Use Help to discover the steps required to set the current time.
- Use the show clock command to verify that the clock is now set to the current time. Packet Tracer may not correctly simulate the time you entered.
- Packet Tracer does not grade this command, so the completion percentage does not change.

Step 4: Configure passwords.

- Use the encrypted form of the privileged EXEC mode password and set the password to class.

- Configure the passwords for console and Telnet. Set both the console and vty password to cisco and require users to log in.
- View the current configuration on S1. Notice that the line passwords are shown in clear text. Enter the command to encrypt these passwords.
- Check results.

Your completion percentage should be 42%. If not, click Check Results to see which required components are not yet completed.

Step 5: Configure the login banner.

If you do not enter the banner text exactly as specified, Packet Tracer does not grade your command correctly.

These commands are case-sensitive. Also make sure that you do not include any spaces before or after the text.

- Configure the message-of-the-day banner on S1 to display as Authorized Access Only. (Do not include the period.)
- Check results.

Your completion percentage should be 46%. If not, click Check Results to see which required components are not yet completed.

Step 6: Configure the router.

Routers and switches share many of the same commands. Configure the router with the same basic commands you used on S1.

- Access the CLI for R1 by clicking the device.
- Do the following on R1:
    - Configure the hostname of the router as R1.
    - Configure the encrypted form of the privileged EXEC mode password and set the password to class.
    - Set the console and vty password to cisco and require users to log in.
    - Encrypt the console and vty passwords.
    - Configure the message-of-the-day as Authorized Access Only. (Do not include the period.)
- Check results.

Your completion percentage should be 65%. If not, click Check Results to see which required components are not yet completed.

Step 7: Solve a mismatch between duplex and speed.

PC1 and Server currently do not have access through S1 because the duplex and speed are mismatched.

Enter commands on S1 to solve this problem.

- Verify connectivity.
- Both PC1 and Server should now be able to ping S1, R1, and each other.
- Check results.

Your completion percentage should be 73%. If not, click Check Results to see which required components are not yet completed.

Step 8: Configure port security.

a. Use the following policy to establish port security on the port used by PC1: Enable port security

- Allow only one MAC address
- Configure the first learned MAC address to "stick" to the configuration

Note: Only enabling port security is graded by Packet Tracer and counted toward the completion percentage.

However, all the port security tasks listed above are required to complete this activity successfully.

b. Verify that port security is enabled for Fa0/18.

S1#show interface fa0/18

Step 9: Secure unused ports.

Disable all ports that are currently not used on S1. Packet Tracer grades the status of the following

ports: Fa0/2, Fa0/3, Fa0/4, Gig 1/1, and Gig 1/2.

Check results.

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

Step 10: Manage the switch configuration file.

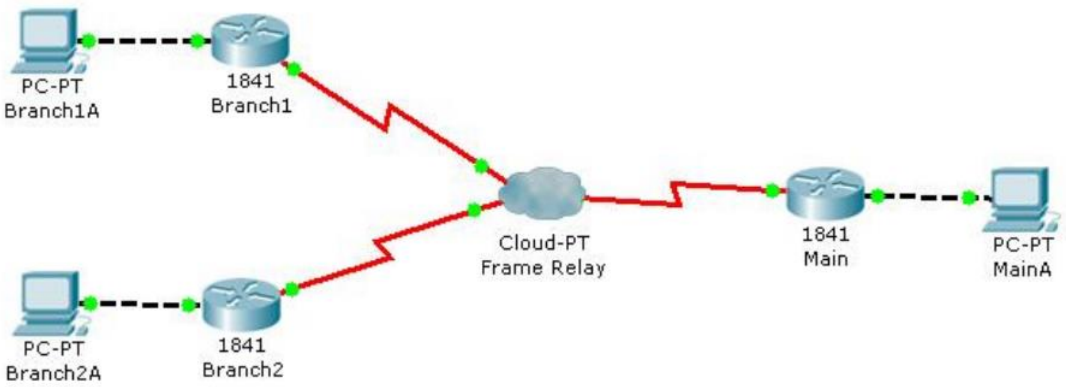
- Save the current configuration for S1 and R1 to NVRAM.
- Back up the startup configuration file on S1 and R1 by uploading them to Server. Verify that Server has the R1-confg and S1-confg files.
- Check results.

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

Practical 5

Examining WAN Connections

Topology



Step 1: Examine the configuration of Branch1 and Branch2.

- Click on Branch1 and use various show commands to view the connectivity to the network.
- Use the show running-configuration command to view the router configuration.
- Use the show ip interface brief command to view the status of the interfaces.
- Use the various show frame-relay map, show frame-relay pvc, and show frame-relay lmi commands to see the status of the Frame-relay circuit.
- Click on Branch 2 and use various show commands to view the connectivity to the network.
- Use the show running-configuration command to view the router configuration.
- Use the show ip interface brief command to view the status of the interfaces.
- Use the various show frame-relay map, show frame-relay pvc, and show frame-relay lmi commands to see the status of the Frame-relay circuit.

Step 2: Examine the configuration of Main.

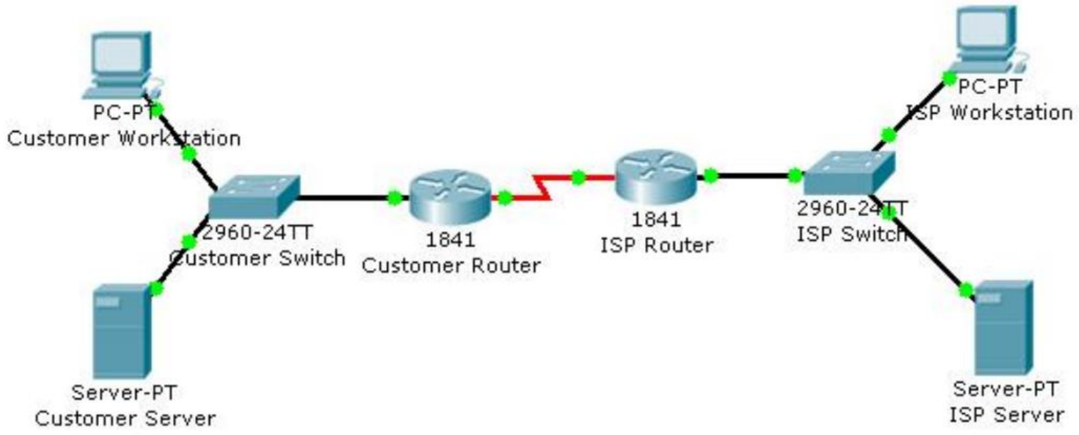
- Click on Main and use a variety of show commands to view the connectivity to the network.
- Use the show running-configuration command to view the router configuration.
- Use the show ip interface brief command to view the status of the interfaces.

To view the status of the frame-relay configurations use the show frame-relay lmi, show frame-relay map, and show frame-relay pvc commands.

Practical 6

Configuring a Cisco Router as a DHCP Server

Topology



you will continue to configure the Cisco 1841 ISR router for the customer network by configuring the DHCP service. The customer has several workstations that need to be automatically configured with IP addresses on the local subnet and appropriate DHCP options to allow access to the Internet. The DHCP pool will use the 192.168.1.0/24 network but the first 49 addresses are excluded. The default gateway and DNS server also need to be configured as 192.168.1.1 and 192.168.1.10.

Step 1: Configure the DHCP service.

- From the customer workstation, use a console cable and terminal emulation software to connect to the console of the customer Cisco1841 ISR.
- Log in to the console of the Cisco 1841 ISR and enter global configuration mode.
- Before creating a DHCP pool, configure the addresses that are excluded. The range is from 192.168.1.1 to 192.168.1.49.

```
CustomerRouter(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.49
```

- Create a DHCP pool called pool1.

```
CustomerRouter(config)#ip dhcp pool pool1
```

- Define the network address range for the DHCP pool.

```
CustomerRouter(dhcp-config)#network 192.168.1.0 255.255.255.0
```

- Define the DNS server as 192.168.1.10.

```
CustomerRouter(dhcp-config)#dns-server 192.168.1.10
```

- Define the default gateway as 192.168.1.1.

```
CustomerRouter(dhcp-config)#default-router 192.168.1.1
```

- Add an exclusion range of 192.168.1.1 to 192.168.1.49 to the DHCP pool.

```
CustomerRouter(dhcp-config)#exit
CustomerRouter(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.49
```

- Exit the terminal.

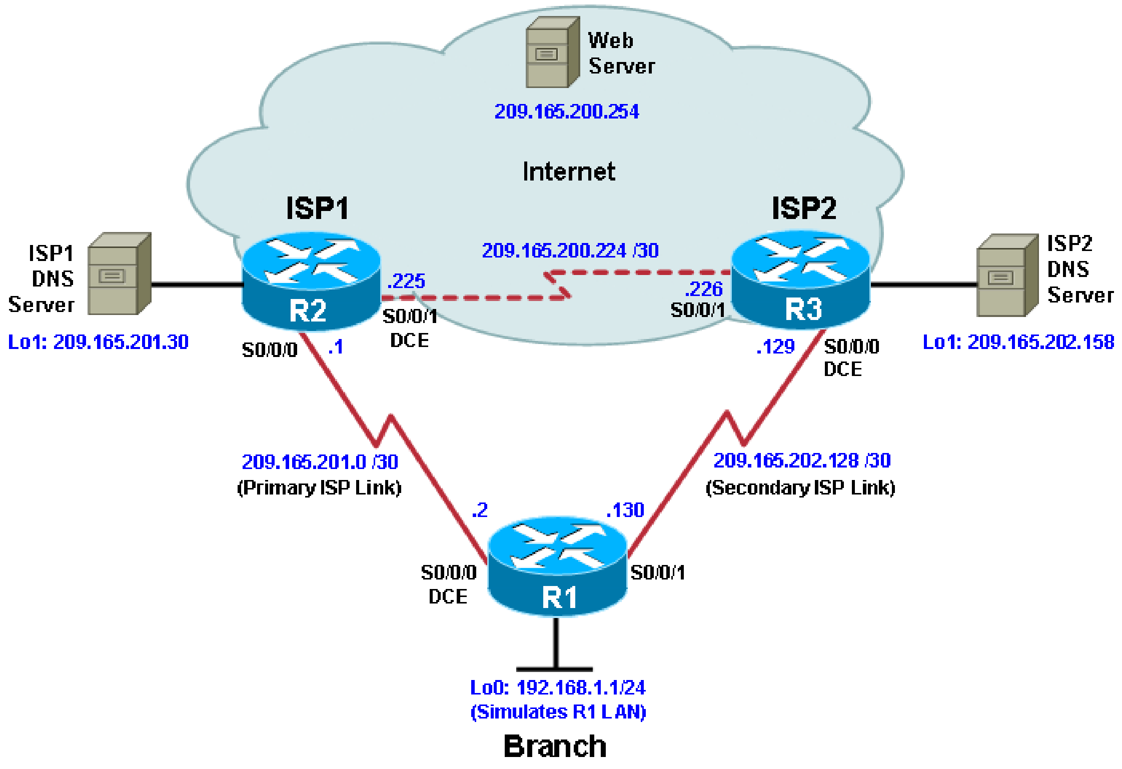
Step 2: Verify the DHCP configuration.

- From the customer workstation, open the Command Prompt window.
- Type ipconfig /release to release the current IP address.
- Type ipconfig /renew to request a new IP address on the local network.
- Verify that the IP address has been correctly assigned by pinging the LAN IP address of the Cisco 1841 ISR.
- Click the Check Results button at the bottom of this instruction window to check your work.

Practical 7

Configure IP SLA Tracking and Path Control

Topology



Required Resources

- 3 routers (Cisco IOS Release 15.2 or comparable)
- Serial and Ethernet cables

Step 1: Configure loopbacks and assign addresses.

Router R1

```
hostname R1

interface Loopback 0

description R1 LAN

ip address 192.168.1.1 255.255.255.0

interface Serial0/0/0

description R1 --> ISP1
```

```
ip address 209.165.201.2 255.255.255.252
clock rate 128000
bandwidth 128
no shutdown

interface Serial0/0/1
description R1 --> ISP2
 ip address 209.165.202.130 255.255.255.252
 bandwidth 128
 no shutdown
```

Router ISP1 (R2)

```
hostname ISP1
interface Loopback0
description Simulated Internet Web Server
ip address 209.165.200.254 255.255.255.255

interface Loopback1
description ISP1 DNS Server
ip address 209.165.201.30 255.255.255.255

interface Serial0/0/0
description ISP1 --> R1
ip address 209.165.201.1 255.255.255.252
bandwidth 128
no shutdown

interface Serial0/0/1
description ISP1 --> ISP2
```

```
ip address 209.165.200.225 255.255.255.252
clock rate 128000
bandwidth 128
no shutdown
```

Router ISP2 (R3)

```
hostname ISP2
interface Loopback0
description Simulated Internet Web Server
ip address 209.165.200.254 255.255.255.255

interface Loopback1
description ISP2 DNS Server
ip address 209.165.202.158 255.255.255.255

interface Serial0/0/0
description ISP2 --> R1
ip address 209.165.202.129 255.255.255.252
clock rate 128000
bandwidth 128
no shutdown

interface Serial0/0/1
description ISP2 --> ISP1
ip address 209.165.200.226 255.255.255.252
bandwidth 128
no shutdown
```

a. Verify the configuration by using the **show interfaces description** command. The output from router R1 is shown here as an example.

```
R1# show interfaces description | include up
```

```
R1#
```

All three interfaces should be active. Troubleshoot if necessary.

Step 2: Configure static routing.

Router R1

```
R1(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.1
R1(config)#
```

Router ISP1 (R2)

```
ISP1(config)# router eigrp 1
ISP1(config-router)# network 209.165.200.224 0.0.0.3
ISP1(config-router)# network 209.165.201.0 0.0.0.31
ISP1(config-router)# no auto-summary
ISP1(config-router)# exit
ISP1(config)#
ISP1(config-router)# ip route 192.168.1.0 255.255.255.0 209.165.201.2
ISP1(config)#
```

Router ISP2 (R3)

```
ISP2(config)# router eigrp 1
ISP2(config-router)# network 209.165.200.224 0.0.0.3
ISP2(config-router)# network 209.165.202.128 0.0.0.31
ISP2(config-router)# no auto-summary
ISP2(config-router)# exit
ISP2(config)#
ISP2(config)# ip route 192.168.1.0 255.255.255.0 209.165.202.130
ISP2(config)#
```

EIGRP neighbor relationship messages on ISP1 and ISP2 should be generated. Troubleshoot if necessary.

Before implementing the Cisco IOS SLA feature, you must verify reachability to the Internet servers. From router R1, ping the web server, ISP1 DNS server, and ISP2 DNS server to verify connectivity. You can copy the following Tcl script and paste it into R1.

```
foreach address {
209.165.200.254
209.165.201.30
209.165.202.158
} {
ping $address source 192.168.1.1
}
```

All pings should be successful. Troubleshoot if necessary.

b. Trace the path taken to the web server, ISP1 DNS server, and ISP2 DNS server. You can copy the following Tcl script and paste it into R1.

```
foreach address {
209.165.200.254
209.165.201.30
209.165.202.158
} {
trace $address source 192.168.1.1
}
```

Step 3: Configure IP SLA probes.

a. Create an ICMP echo probe on R1 to the primary DNS server on ISP1 using the **ip sla** command.

```
R1(config)# ip sla 11
R1(config-ip-sla)# icmp-echo 209.165.201.30
R1(config-ip-sla-echo)# frequency 10
R1(config-ip-sla-echo)# exit
R1(config)#
R1(config)# ip sla schedule 11 life forever start-time now
R1(config)#
```

b. Verify the IP SLAs configuration of operation 11 using the **show ip sla configuration 11** command.

```
R1# show ip sla configuration 11

R1#
```

c. Issue the **show ip sla statistics** command to display the number of successes, failures, and results of the latest operations.

```
R1# show ip sla statistics

R1#
```

You can see that operation 11 has already succeeded five times, has had no failures, and the last operation returned an OK result.

d. Although not actually required because IP SLA session 11 alone could provide the desired fault tolerance, create a second probe, 22, to test connectivity to the second DNS server located on router ISP2.

```
R1(config)# ip sla 22

R1(config-ip-sla)# icmp-echo 209.165.202.158

R1(config-ip-sla-echo)# frequency 10

R1(config-ip-sla-echo)# exit

R1(config)#

R1(config)# ip sla schedule 22 life forever start-time now

R1(config)# end

R1#
```

e. Verify the new probe using the **show ip sla configuration** and **show ip sla statistics** commands.

```
R1# show ip sla configuration 22

R1# show ip sla statistics 22

R1#
```

The output lists the details of the configuration of operation 22. The operation is an ICMP echo to 209.165.202.158, with a frequency of 10 seconds, and it has already started (the start time has already passed). The statistics also prove that operation 22 is active.

Step 4: Configure tracking options.

Although PBR could be used, you will configure a floating static route that appears or disappears depending on the success or failure of the IP SLA.

a. On R1, remove the current default route and replace it with a floating static route having an administrative distance of 5.

```
R1(config)# no ip route 0.0.0.0 0.0.0.0 209.165.201.1
```

```
R1(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.1 5

R1(config)# exit
```

b. Verify the routing table.

```
R1# show ip route | begin Gateway

R1#
```

c. From global configuration mode on R1, use the **track 1 ip sla 11 reachability** command to enter the config-track subconfiguration mode.

```
R1(config)# track 1 ip sla 11 reachability

R1(config-track)#
```

d. Specify the level of sensitivity to changes of tracked objects to 10 seconds of down delay and 1 second of up delay using the **delay down 10 up 1** command. The delay helps to alleviate the effect of flapping objects—objects that are going down and up rapidly. In this situation, if the DNS server fails momentarily and comes back up within 10 seconds, there is no impact.

```
R1(config-track)# delay down 10 up 1

R1(config-track)# exit

R1(config)#
```

e. To view routing table changes as they happen, first enable the **debug ip routing** command.

```
R1# debug ip routing

IP routing debugging is on

R1#
```

f. Configure the floating static route that will be implemented when tracking object 1 is active. Use the **ip route 0.0.0.0 0.0.0.0 209.165.201.1 2 track 1** command to create a floating static default route via 209.165.201.1 (ISP1). Notice that this command references the tracking object number 1, which in turn references IP SLA operation number 11.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.1 2 track 1

R1(config)#
```

Notice that the default route with an administrative distance of 5 has been immediately flushed because of a route with a better admin distance. It then adds the new default route with the admin distance of 2.

g. Repeat the steps for operation 22, track number 2, and assign the static route an admin distance higher than track 1 and lower than 5. On R1, copy the following configuration, which sets an admin distance of 3.

```
R1(config)# track 2 ip sla 22 reachability

R1(config-track)# delay down 10 up 1

R1(config-track)# exit

R1(config)#

R1(config)# ip route 0.0.0.0 0.0.0.0 209.165.202.129 3 track 2

R1(config)#
```

h. Verify the routing table again.

```
R1#show ip route | begin Gateway

R1#
```

Although a new default route was entered, its administrative distance is not better than 2. Therefore, it does not replace the previously entered default route.

Step 5: Verify IP SLA operation.

In this step you observe and verify the dynamic operations and routing changes when tracked objects fail. The following summarizes the process:

- Disable the DNS loopback interface on ISP1 (R2).
- Observe the output of the **debug** command on R1.
- Verify the static route entries in the routing table and the IP SLA statistics of R1.
- Re-enable the loopback interface on ISP1 (R2) and again observe the operation of the IP SLA tracking feature.

a. On ISP1, disable the loopback interface 1.

```
ISP1(config-if)# int lo1

ISP1(config-if)# shutdown

ISP1(config-if)#
```

b. On R1, observe the **debug** output being generated. Recall that R1 will wait up to 10 seconds before initiating action therefore several seconds will elapse before the output is generated.

The tracking state of track 1 changes from up to down. This is the object that tracked reachability for IP SLA object 11, with an ICMP echo to the ISP1 DNS server at 209.165.201.30.

R1 then proceeds to delete the default route with the administrative distance of 2 and installs the next highest default route to ISP2 with the administrative distance of 3.

c. On R1, verify the routing table.

   R1# **show ip route | begin Gateway**

   R1#

   The new static route has an administrative distance of 3 and is being forwarded to ISP2 as it should.

d. Verify the IP SLA statistics.

   R1# **show ip sla statistics**

   R1#

   Notice that the latest return code is **Timeout** and there have been 45 failures on IP SLA object 11.

e. On R1, initiate a trace to the web server from the internal LAN IP address.

   R1# **trace 209.165.200.254 source 192.168.1.1**

   R1#

   This confirms that traffic is leaving router R1 and being forwarded to the ISP2 router.

f. On ISP1, re-enable the DNS address by issuing the **no shutdown** command on the loopback 1 interface to examine the routing behavior when connectivity to the ISP1 DNS is restored.

   ISP1(config-if)# **no shutdown**

   R1#

   Now the IP SLA 11 operation transitions back to an up state and reestablishes the default static route to ISP1 with an administrative distance of 2.

g. Again examine the IP SLA statistics.

   R1# **show ip sla statistics**

   R1#

   The IP SLA 11 operation is active again, as indicated by the OK return code, and the number of successes is incrementing.

h. Verify the routing table.

   R1# **show ip route | begin Gateway**

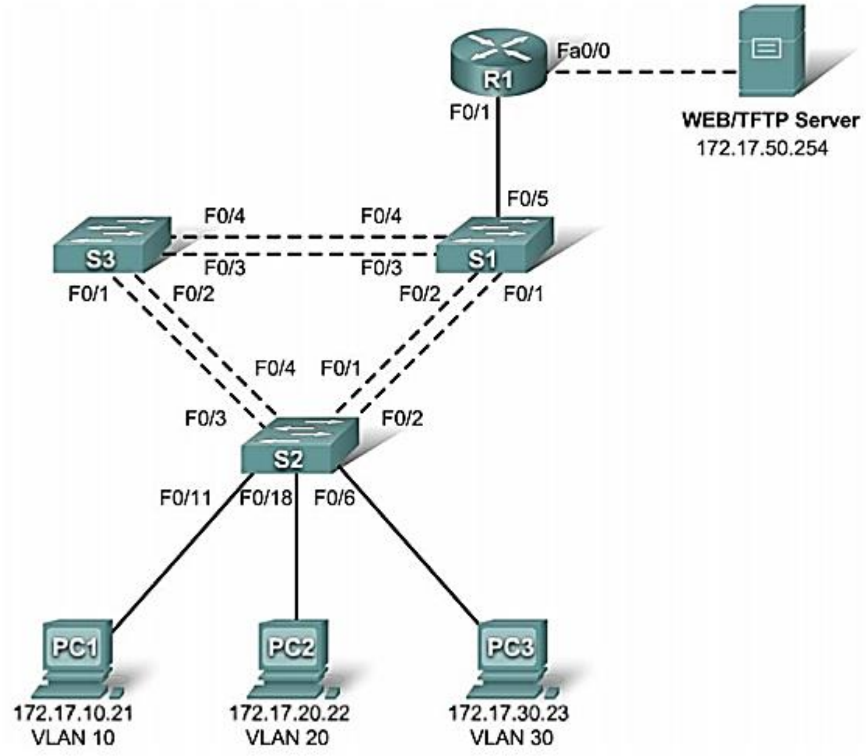
   R1#

   The default static through ISP1 with an administrative distance of 2 is reestablished.

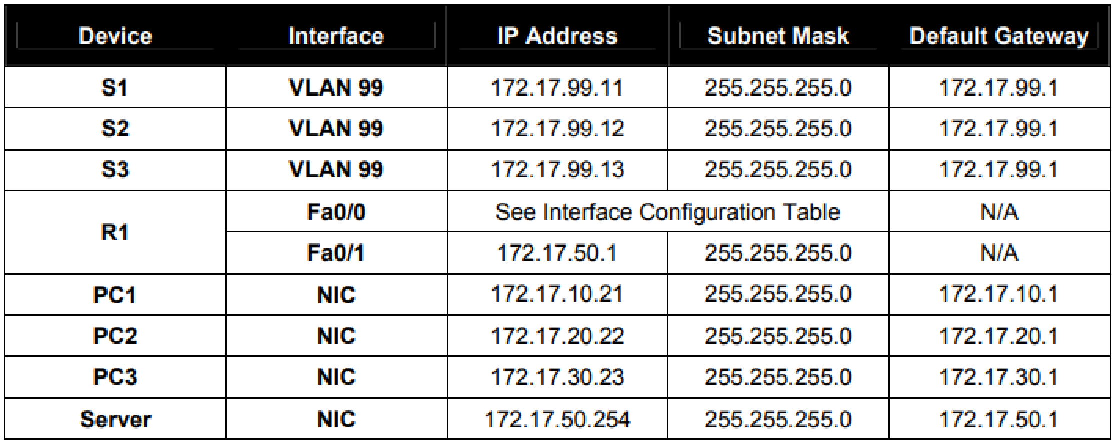
Practical 8

Basic Inter-VLAN Routing

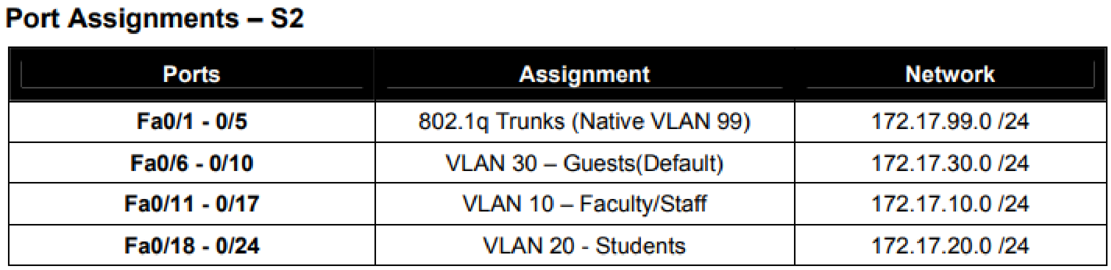
Topology Diagram



Addressing Table

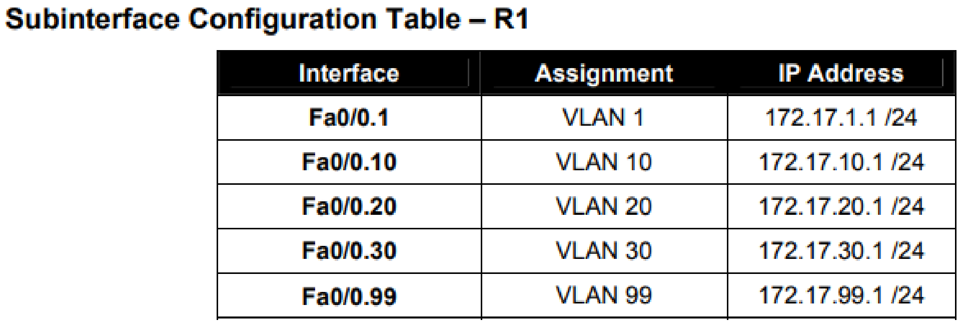


Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
S3	VLAN 99	172.17.99.13	255.255.255.0	172.17.99.1
R1	Fa0/0	See Interface Configuration Table		N/A
	Fa0/1	172.17.50.1	255.255.255.0	N/A
PC1	NIC	172.17.10.21	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
Server	NIC	172.17.50.254	255.255.255.0	172.17.50.1



Port Assignments – S2

Ports	Assignment	Network
Fa0/1 - 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 - 0/10	VLAN 30 – Guests(Default)	172.17.30.0 /24
Fa0/11 - 0/17	VLAN 10 – Faculty/Staff	172.17.10.0 /24
Fa0/18 - 0/24	VLAN 20 - Students	172.17.20.0 /24



Subinterface Configuration Table – R1

Interface	Assignment	IP Address
Fa0/0.1	VLAN 1	172.17.1.1 /24
Fa0/0.10	VLAN 10	172.17.10.1 /24
Fa0/0.20	VLAN 20	172.17.20.1 /24
Fa0/0.30	VLAN 30	172.17.30.1 /24
Fa0/0.99	VLAN 99	172.17.99.1 /24

Task 1: Perform Basic Switch Configurations

Configure the S1, S2, and S3 switches according to the addressing table and the following guidelines:

- Configure the switch hostname.
- Disable DNS lookup.
- Configure the default gateway.
- Configure an EXEC mode password of class.
- Configure a password of cisco for console connections.
- Configure a password of cisco for vty connections.
- Configure the default gateway on each switch.

```
Switch>enable
Switch#config term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#ip default-gateway 172.17.99.1
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
```

```
Destination filename [startup-config]? [enter]
Building configuration...
```

Task 2: Configure the Ethernet Interfaces on the Host PCs

Configure the Ethernet interfaces of PC1, PC2 and PC3 with the IP addresses from the addressing table.

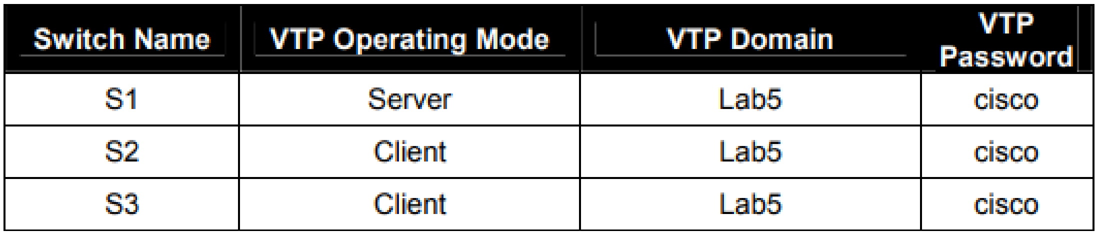
Task 3: Configure VTP on the Switches

Step 1. Enable the user ports on S2 in access mode.

```
S2(config)#interface fa0/6
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/11
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
S2(config-if)#interface fa0/18
S2(config-if)#switchport mode access
S2(config-if)#no shutdown
```

Step 2. Configure VTP.

Configure VTP on the three switches using the following table. Remember that VTP domain names and passwords are case-sensitive.



Switch Name	VTP Operating Mode	VTP Domain	VTP Password
S1	Server	Lab5	cisco
S2	Client	Lab5	cisco
S3	Client	Lab5	cisco

```
S1(config)#vtp mode server
S1(config)#vtp domain Lab6
S1(config)#vtp password cisco
S1(config)#end
S2(config)#vtp mode client
S2(config)#vtp domain Lab6
S2(config)#vtp password cisco
S2(config)#end
S3(config)#vtp mode client
S3(config)#vtp domain Lab6
S3(config)#vtp password cisco
```

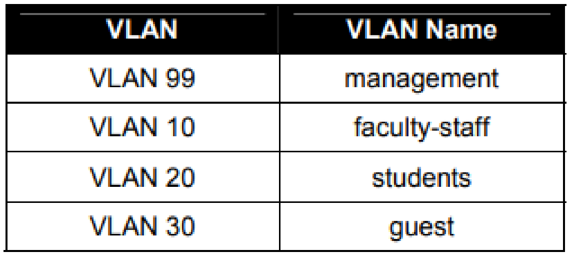
```
S3(config)#end
```

Step 3. Configure trunking ports and designate the native VLAN for the trunks.

Configure Fa0/1 through Fa0/5 as trunking ports, and designate VLAN 99 as the native VLAN for these trunks. When this activity was started, these ports were disabled and must be re-enabled now using the no shutdown command.
Only the commands for the FastEthernet0/1 interface on each switch are shown, but the commands should be applied up to the FastEthernet0/5 interface.

```
S1(config)#interface fa0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#no shutdown
S1(config)#end
S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 99
S2(config-if)#no shutdown
S2(config-if)#end
S3(config)#interface fa0/1
S3(config-if#switchport mode trunk
S3(config-if)#switchport trunk native vlan 99
S3(config-if)#no shutdown
S3(config-if-#end
```

Step 4. Configure the VTP server with VLANs.
Configure the following VLANS on the VTP server:



VLAN	VLAN Name
VLAN 99	management
VLAN 10	faculty-staff
VLAN 20	students
VLAN 30	guest

```
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config)#vlan 10
S1(config-vlan)#name faculty-staff
S1(config)#vlan 20
S1(config-vlan)#name students
S1(config)#vlan 30
```

```
S1(config-vlan)#name guest
S1(config-vlan)#end
```

Verify that the VLANs have been created on S1 with the show vlan brief command.

Step 5. Verify that the VLANs created on S1 have been distributed to S2 and S3.

Use the show vlan brief command on S2 and S3 to verify that all four VLANs have been distributed to the client switches.

```
S2#show vlan brief
S3#show vlan brief
```

Step 6. Configure the management interface address on all three switches.

```
S1(config)#interface vlan99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S2(config)#interface vlan99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S3(config)#interface vlan99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
```

Verify that the switches are correctly configured by pinging between them. From S1, ping the management interface on S2 and S3. From S2, ping the management interface on S3.

Step 7. Assign switch ports to VLANs on S2.

Port assignments are listed in the table at the beginning of the activity. However, since Packet Tracer 4.11 does not support the interface range command, only assign the first port from each range.

```
S2(config)#interface fa0/6
S2(config-if)#switchport access vlan 30
S2(config-if)#interface fa0/11
S2(config-if)#switchport access vlan 10
S2(config-if)#interface fa0/18
S2(config-if)#switchport access vlan 20
S2(config-if)#end
S2#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
S2#
```

Task 4: Configure the Router and the Remote Server LAN

Step 1. Create a basic configuration on the router.

- Configure the router with hostname R1.
- Disable DNS lookup.
- Configure an EXEC mode password of class.
- Configure a password of cisco for console connections.
- Configure a password of cisco for vty connections.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#no shutdown
R1(config-if)#interface fastethernet 0/0.1
R1(config-subif)#encapsulation dot1q 1
R1(config-subif)#ip address 172.17.1.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 172.17.10.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 172.17.20.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 172.17.30.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.99
R1(config-subif)#encapsulation dot1q 99 native
R1(config-subif)#ip address 172.17.99.1 255.255.255.0
```

Step 3. Configure the server LAN interface on R1.

```
R1(config)#interface FastEthernet0/1
R1(config-if)#ip address 172.17.50.1 255.255.255.0
R1(config-if)#description server interface
R1(config-if)#no shutdown
R1(config-if)#end
```

There are now six networks configured. Verify that you can route packets to all six by checking the routing table on R1.

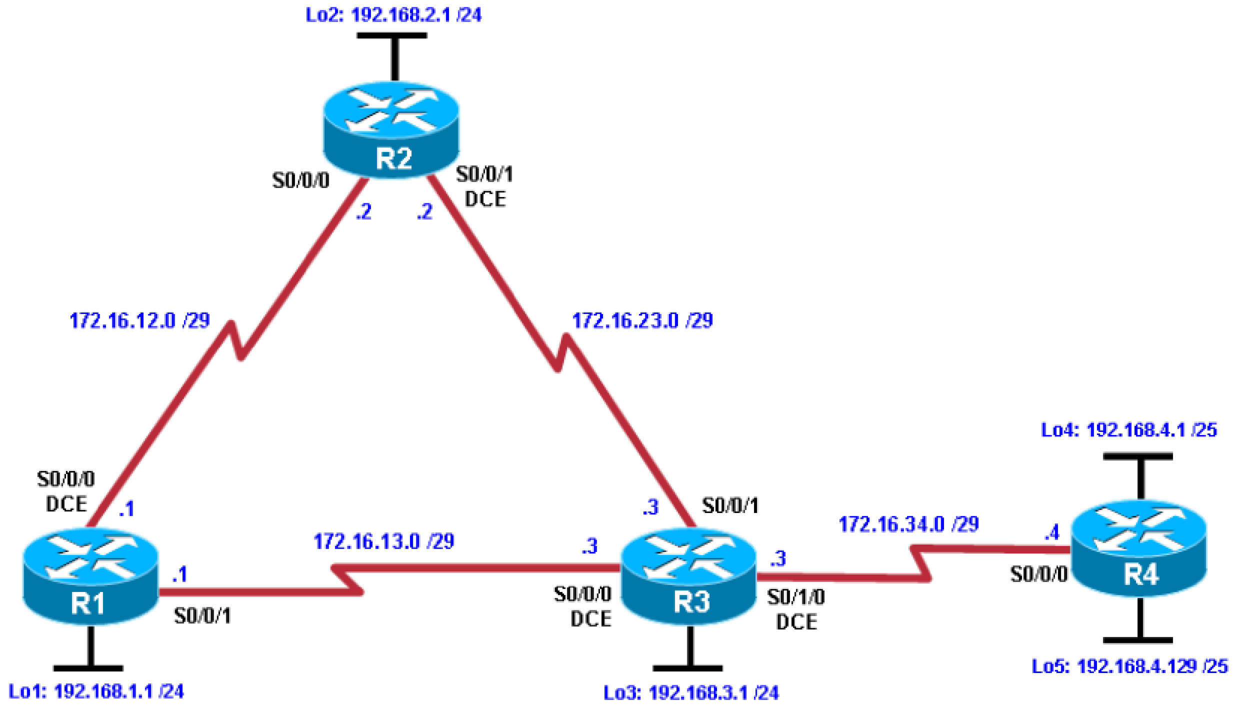
```
R1#show ip route
```

If your routing table does not show all six networks, troubleshoot your configuration and resolve the problem before proceeding.

Practical 9

Configure and Verify Path Control Using PBR

Topology



Required Resources

- 4 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Services or comparable)
- Serial and console cables

Step 1: Prepare the routers for the lab.

Cable the network as shown in the topology diagram. Erase the startup configuration, and reload each router to clear previous configurations.

Step 2: Configure router hostname and interface addresses.

Router R1

```
hostname R1
!
interface Lo1
description R1 LAN
ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0/0
description R1 --> R2
ip address 172.16.12.1 255.255.255.248
clock rate 128000
bandwidth 128
no shutdown
```

```
!
interface Serial0/0/1
description R1 --> R3
ip address 172.16.13.1 255.255.255.248
bandwidth 64
no shutdown
!
end
```

Router R2

```
hostname R2
!
interface Lo2
description R2 LAN
ip address 192.168.2.1 255.255.255.0
!
interface Serial0/0/0
description R2 --> R1
ip address 172.16.12.2 255.255.255.248
bandwidth 128
no shutdown
interface Serial0/0/1
description R2 --> R3
ip address 172.16.23.2 255.255.255.248
clock rate 128000
bandwidth 128
no shutdown
!
end
```

Router R3

```
hostname R3
!
interface Lo3
description R3 LAN
ip address 192.168.3.1 255.255.255.0
!
interface Serial0/0/0
description R3 --> R1
ip address 172.16.13.3 255.255.255.248
clock rate 64000
bandwidth 64
no shutdown
!
interface Serial0/0/1
description R3 --> R2
```

```
ip address 172.16.23.3 255.255.255.248
bandwidth 128
no shutdown
!
interface Serial0/1/0
description R3 --> R4
ip address 172.16.34.3 255.255.255.248
clock rate 64000
bandwidth 64
no shutdown
!
end
```

Router R4

```
hostname R4
!
interface Lo4
description R4 LAN A
ip address 192.168.4.1 255.255.255.128
!
interface Lo5
description R4 LAN B
ip address 192.168.4.129 255.255.255.128
!
interface Serial0/0/0
description R4 --> R3
ip address 172.16.34.4 255.255.255.248
bandwidth 64
no shutdown
!
end
```

Verify the configuration with the show ip interface brief, show protocols, and show interfaces description commands. The output from router R3 is shown here as an example.

```
R3# show ip interface brief
R3# show protocols
R3# show interfaces description
```

Step 3: Configure basic EIGRP

Router R1

```
router eigrp 1
network 192.168.1.0
network 172.16.12.0 0.0.0.7
network 172.16.13.0 0.0.0.7
```

```
no auto-summary
```

Router R2

```
router eigrp 1
network 192.168.2.0
network 172.16.12.0 0.0.0.7
network 172.16.23.0 0.0.0.7
no auto-summary
```

Router R3

```
router eigrp 1
network 192.168.3.0
network 172.16.13.0 0.0.0.7
network 172.16.23.0 0.0.0.7
network 172.16.34.0 0.0.0.7
no auto-summary
```

Router R4

```
router eigrp 1
network 192.168.4.0
network 172.16.34.0 0.0.0.7
no auto-summary
```

You should see EIGRP neighbor relationship messages being generated.

Step 4: Verify EIGRP connectivity

```
R1# show ip eigrp neighbors
R2# show ip eigrp neighbors
R3# show ip eigrp neighbors
R4# show ip eigrp neighbors
```

Run the following Tcl script on all routers to verify full connectivity.

```
R1# tclsh
foreach address {
172.16.12.1
172.16.12.2
172.16.13.1
172.16.13.3
172.16.23.2
172.16.23.3
172.16.34.3
172.16.34.4
192.168.1.1
192.168.2.1
192.168.3.1
192.168.4.1
192.168.4.129
} { ping $address }
```

You should get ICMP echo replies for every address pinged. Make sure to run the Tcl script on each
router.

Step 5: Verify the current path

```
R1# show ip route
R4# traceroute 192.168.1.1 source 192.168.4.1
R4# traceroute 192.168.1.1 source 192.168.4.129
R3# show ip route
R3# show interfaces s0/0/0
R3# show interfaces s0/0/1
R3# show ip eigrp topology 192.168.1.0
```

Step 6: Configure PBR to provide path control

On router R3, create a standard access list called PBR-ACL to identify the R4 LAN B network.

```
R3(config)# ip access-list standard PBR-ACL
R3(config-std-nacl)# remark ACL matches R4 LAN B traffic
R3(config-std-nacl)# permit 192.168.4.128 0.0.0.127
R3(config-std-nacl)# exit
```

Create a route map called R3-to-R1 that matches PBR-ACL and sets the next-hop interface to the R1 serial 0/0/1 interface.

```
R3(config)# route-map R3-to-R1 permit
R3(config-route-map)# match ip address PBR-ACL
R3(config-route-map)# set ip next-hop 172.16.13.1
R3(config-route-map)# exit
```

Apply the R3-to-R1 route map to the serial interface on R3 that receives the traffic from R4. Use the ip policy route-map command on interface S0/1/0.

```
R3(config)# interface s0/1/0
R3(config-if)# ip policy route-map R3-to-R1
R3(config-if)# end
```

On R3, display the policy and matches using the show route-map command.

```
R3# show route-map
```

Step 7: Test the policy.

On R3, create a standard ACL which identifies all of the R4 LANs.

```
R3# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)# access-list 1 permit 192.168.4.0 0.0.0.255
R3(config)# exit
```

Enable PBR debugging only for traffic that matches the R4 LANs.

```
R3# debug ip policy ?
R3# debug ip policy 1
Policy routing debugging is on for access list 1
```

Test the policy from R4 with the traceroute command, using R4 LAN A as the source network.

```
R4# traceroute 192.168.1.1 source 192.168.4.1
```

Test the policy from R4 with the traceroute command, using R4 LAN B as the source network.

```
R4# traceroute 192.168.1.1 source 192.168.4.129
```

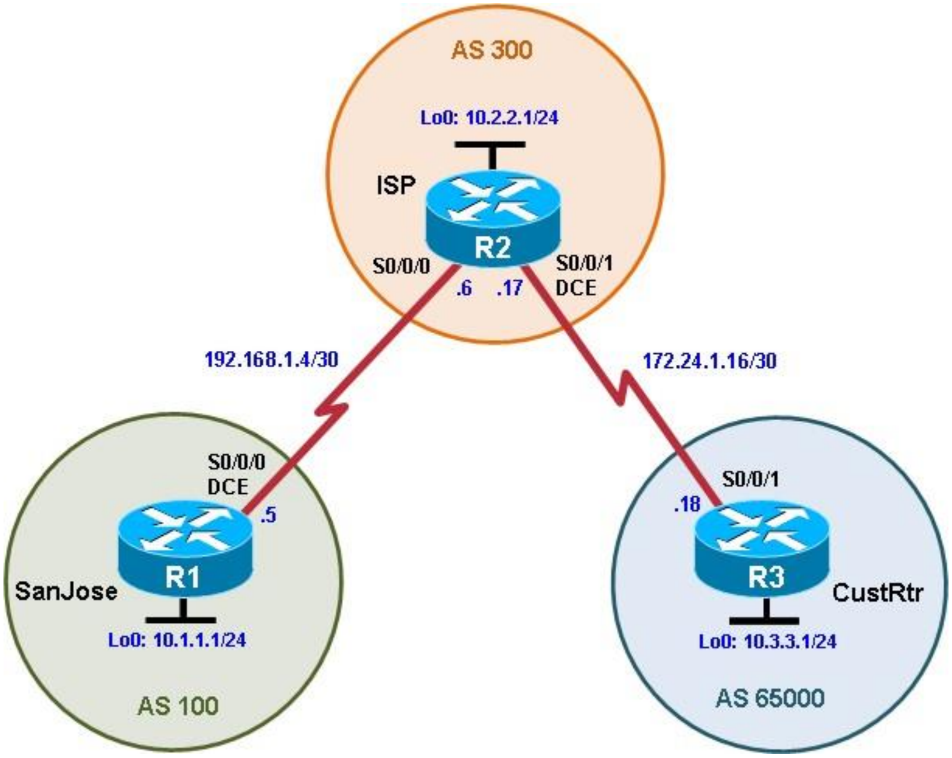
On R3, display the policy and matches using the show route-map command.

```
R3# show route-map
```

Practical 10

Using the AS_PATH Attribute

Topology



The International Travel Agency's ISP has been assigned an AS number of 300. This provider uses BGP to exchange routing information with several customer networks. Each customer network is assigned an AS number from the private range, such as AS 65000. Configure the ISP router to remove the private AS numbers from the AS Path information of CustRtr. In addition, the ISP would like to prevent its customer networks from receiving route information from International Travel Agency's AS 100. Use the AS_PATH attribute to implement this policy.

Note: This lab uses Cisco 1841 routers with Cisco IOS Release 12.4(24)T1 and the Advanced IP Services image c1841-advipservicesk9-mz.124-24.T1.bin. You can use other routers (such as 2801 or 2811) and Cisco IOS Software versions, if they have comparable capabilities and features. Depending on the router model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(24)T1 Advanced IP Services or comparable)
- Serial and console cables

Step 1: Prepare the routers for the lab.

Cable the network as shown in the topology diagram. Erase the startup configuration and reload each router to clear previous configurations.

Step 2: Configure the hostname and interface addresses.

You can copy and paste the following configurations into your routers to begin.

Router R1 (hostname SanJose)

```
hostname SanJose
!
interface Loopback0
ip address 10.1.1.1 255.255.255.0
!
interface Serial0/0/0
ip address 192.168.1.5 255.255.255.252
clock rate 128000 no shutdown
```

Router R2 (hostname ISP)

```
hostname ISP
!
interface Loopback0
ip address 10.2.2.1 255.255.255.0
!
interface Serial0/0/0
ip address 192.168.1.6 255.255.255.252
no shutdown
!
```

```
interface Serial0/0/1

ip address 172.24.1.17 255.255.255.252

clock rate 128000 no shutdown
```

Router R3 (hostname CustRtr)

```
hostname CustRtr

!

interface Loopback0

ip address 10.3.3.1 255.255.255.0

!

interface Serial0/0/1

ip address 172.24.1.18 255.255.255.252

no shutdown
```

Use **ping** to test the connectivity between the directly connected routers.

Note: SanJose will not be able to reach either ISP's loopback (10.2.2.1) or CustRtr's loopback (10.3.3.1), nor will it be able to reach either end of the link joining ISP to CustRtr (172.24.1.17 and 172.24.1.18).

Step 3: Configure BGP.

Configure BGP for normal operation. Enter the appropriate BGP commands on each router so that they identify their BGP neighbors and advertise their loopback networks.

```
SanJose(config)# router bgp 100

SanJose(config-router)# neighbor 192.168.1.6 remote-as 300

SanJose(config-router)# network 10.1.1.0 mask 255.255.255.0

ISP(config)# router bgp 300

ISP(config-router)# neighbor 192.168.1.5 remote-as 100

ISP(config-router)# neighbor 172.24.1.18 remote-as 65000

ISP(config-router)# network 10.2.2.0 mask 255.255.255.0

CustRtr(config)# router bgp 65000

CustRtr(config-router)# neighbor 172.24.1.17 remote-as 300
CustRtr(config-router)# network 10.3.3.0 mask 255.255.255.0
```

Verify that these routers have established the appropriate neighbor relationships by issuing the **show ip bgp neighbors** command on each router.

```
ISP# show ip bgp neighbors

BGP neighbor is 172.24.1.18, remote AS 65000, external link BGP version 4, remote router ID 10.3.3.1

BGP state = Established, up for 00:02:05

<output omitted>

BGP neighbor is 192.168.1.5, remote AS 100, external link BGP version 4, remote router ID 10.1.1.1

BGP state = Established, up for 00:04:19

<output omitted>
```

Step 4: Remove the private AS.

Display the SanJose routing table using the **show ip route** command. SanJose should have a route to both 10.2.2.0 and 10.3.3.0. Troubleshoot if necessary.

```
SanJose# show ip route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 3 subnets

B       10.3.3.0 [20/0] via 192.168.1.6, 00:01:11

B       10.2.2.0 [20/0] via 192.168.1.6, 00:02:16

C               10.1.1.0 is directly connected, Loopback0 192.168.1.0/30 is subnetted, 1 subnets

C       192.168.1.4 is directly connected, Serial0/0/0
```

Ping, this time as an extended ping, sourcing from the Loopback0 interface address.

```
SanJose# ping

Protocol [ip]:

Target IP address: 10.3.3.1

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:
```

```
Extended commands [n]: y
Source address or interface: 10.1.1.1
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 10.3.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/64/68 ms
```

Note: You can bypass extended ping mode and specify a source address using one of these commands:

```
SanJose# ping 10.3.3.1 source 10.1.1.1
```

or

```
SanJose# ping 10.3.3.1 source Lo0
```

Check the BGP table from SanJose by using the **show ip bgp** command. Note the AS path for the 10.3.3.0 network. The AS 65000 should be listed in the path to 10.3.3.0.

```
SanJose# show ip bgp
```

Configure ISP to strip the private AS numbers from BGP routes exchanged with SanJose using the following commands.

```
ISP(config)# router bgp 300
ISP(config-router)# neighbor 192.168.1.5 remove-private-as
```

After issuing these commands, use the **clear ip bgp *** command on ISP to reestablish the BGP relationship between the three routers. Wait several seconds and then return to SanJose to check its routing table.

Note: The **clear ip bgp * soft** command can also be used to force each router to resend its BGP table.

SanJose should be able to ping 10.3.3.1 using its loopback 0 interface as the source of the ping.

```
SanJose# ping 10.3.3.1 source lo0
```

```
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.3.3.1, timeout is 2 seconds: Packet sent with a source address of 10.1.1.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
```

Now check the BGP table on SanJose. The AS_ PATH to the 10.3.3.0 network should be AS 300. It no longer has the private AS in the path.

```
SanJose# show ip bgp
```

Step 5: Use the AS_PATH attribute to filter routes.

As a final configuration, use the AS_PATH attribute to filter routes based on their origin. In a complex environment, you can use this attribute to enforce routing policy. In this case, the provider router, ISP, must be configured so that it does not propagate routes that originate from AS 100 to the customer router CustRtr.

Configure a special kind of access list to match BGP routes with an AS_PATH attribute that both begins and ends with the number 100. Enter the following commands on ISP.

```
ISP(config)# ip as-path access-list 1 deny ^100$

ISP(config)# ip as-path access-list 1 permit .*
```

Apply the configured access list using the **neighbor** command with the **filter-list** option.

```
ISP(config)# router bgp 300

ISP(config-router)# neighbor 172.24.1.18 filter-list 1 out
```

The **out** keyword specifies that the list is applied to routing information sent to this neighbor.

Use the **clear ip bgp *** command to reset the routing information. Wait several seconds and then check the routing table for ISP. The route to 10.1.1.0 should be in the routing table.

```
ISP# show ip route
```

Check the routing table for CustRtr. It should not have a route to 10.1.1.0 in its routing table.

```
CustRtr# show ip route
```

Return to ISP and verify that the filter is working as intended. Issue the **show ip bgp regexp ^100$**

command.

```
ISP# show ip bgp regexp ^100$
```

The output of this command shows all matches for the regular expressions that were used in the access list. The path to 10.1.1.0 matches the access list and is filtered from updates to CustRtr.

Run the following Tcl script on all routers to verify whether there is connectivity. All pings from ISP should be successful. SanJose should not be able to ping the CustRtr loopback 10.3.3.1 or the WAN link

172.24.1.16/30. CustRtr should not be able to ping the SanJose loopback 10.1.1.1 or the WAN link 192.168.1.4/30.

```
ISP# tclsh

foreach address { 10.1.1.1

10.2.2.1

10.3.3.1

192.168.1.5

192.168.1.6

172.24.1.17

172.24.1.18

} {

ping $address }
```