



CCNA Routing and Switching: Routing and Switching Essentials 6.0

Instructor Lab Manual

This document is exclusive property of Cisco Systems, Inc. Permission is granted to print and copy this document for non-commercial distribution and exclusive use by instructors in the CCNA Routing and Switching: Routing and Switching Essentials course as part of an official Cisco Networking Academy Program.



Do We Really Need a Map? (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Describe the primary functions and features of a router.

Routers send and receive information from networks they recognize. The routing table is a very important tool to supply the network administrator with information about how a network delivers data from source to destination between networks. This modeling activity focuses students' thoughts on how routing is mapped and documented.

Scenario

Using the Internet and Google Maps, located at <http://maps.google.com>, find a route between the capital city of your country and some other distant town, or between two places within your own city. Pay close attention to the driving or walking directions Google Maps suggests.

Notice that in many cases, Google Maps suggests more than one route between the two locations you chose. It also allows you to put additional constraints on the route, such as avoiding highways or tolls.

- Copy at least two route instructions supplied by Google Maps for this activity. Place your copies into a word processing document and save it for to use with the next step.
- Open the .pdf accompanying this modeling activity and complete it with a fellow student. Discuss the reflection questions listed on the .pdf and record your answers.

Be prepared to present your answers to the class.

Resources

- Internet connection
- Web browser
- Google Maps, <http://maps.google.com/>

Reflection

1. What do the individual driving, or walking based on your criteria you input, and non-highway directions look like? What exact information do they contain? How do they relate to IP routing?

Each suggested route has its overall length and duration indicated. The two sets of directions consist of detailed step-by-step instructions to reach the other destination. At each significant crossing, you are advised of the very next direction to take and of the distance to the next crossroad.

These instructions closely resemble information in routing tables of IP-based routers. Each crossing can be likened to a router on which the next path selection takes place. The overall length and duration of the route correspond to the route metric, or a measure of its usefulness, from the source to the destination. The advice on which next direction to take from a particular crossing resembles an entry in the particular router's routing table that contains information about the nearest next hop router on the path towards the destination. The distance to the next crossroad is similar to the so-called cost of an interface that is used by routing protocols to compute the resulting metric of a route.

2. If Google Maps offered a set of different routes, what makes this route different from the first? Why would you choose one route over another?

Multiple routes traverse different paths to them same destination. These paths may differ in various

Do We Really Need a Map?

characteristics, as some take longer to complete from source to destination and others are physically longer due to distance; therefore, when comparing this activity to network travel, distance and time can make a difference to the routes displayed.

3. What criteria can be used to evaluate the usefulness of a route?

Criteria could include:

- the number of different paths available from source to destination, such as direct connections, through other routers;
 - the time it takes to send data from source to destination, which can be based on bandwidth and delay;
 - the reliability of the route from source to destination, such as static vs. dynamic routes;
 - whether the route is the preferred route or a secondary route, such as static routes, default routes and other reported routes;
 - which speeds can be used to move packets from source to destination, such as the type of media/medium used to connect networks.
4. Is it sensible to expect that a single route can be “the best one”, i.e. meeting all various requirements? Justify your answer.

If the route given meets all the criteria requested, the single route can be the best route. Compare this to a default route or the only route available from source to destination.

5. As a network administrator or developer, how could you use a network map, or routing table, in your daily network activities?

Network maps or routing tables can be used to envision and document the best paths for data delivery on networks. They can also be used to structure a direct path, or direct paths, from one network to another.

Modeling Activity Graphic Representation (designs will vary)

Instructor Note: Listed below is representative output from the Google Maps site for Instructor use only.

Do We Really Need a Map?

The image displays two side-by-side screenshots of Google Maps. Both screenshots show the same route from Ashland, Virginia to Richmond, Virginia, but with different settings and details.

Left Screenshot (Default Settings):

- Start point: Ashland, Virginia (labeled A)
- End point: Richmond, Virginia (labeled B)
- Route: I-95 S (18.8 mi, 23 mins)
- Options: "Avoid highways" and "Avoid tolls" are unchecked.
- Buttons: "GET DIRECTIONS" and "miles / km" (km is selected).
- Driving directions to Richmond, VA:**
 - Head east on England St toward Maple St (1.0 mi)
 - Merge onto I-95 S via the ramp to Richmond (17.0 mi)
 - Take exit 74C to merge onto US-250 W/E Broad St toward US-33 (0.7 mi)
 - Turn left onto N 8th St (420 ft)
 - Take the 1st right onto E Grace St (190 ft)

Right Screenshot (Advanced Settings):

- Start point: Ashland, Virginia (labeled A)
- End point: Richmond, Virginia (labeled B)
- Route: U.S. 1 S (16.4 mi, 32 mins)
- Options: "Avoid highways" is checked, and "Avoid tolls" is unchecked.
- Buttons: "GET DIRECTIONS" and "miles / km" (miles is selected).
- Suggested routes:**
 - U.S. 1 S: 16.4 mi, 32 mins (In current traffic: 37 mins)
 - US-301 S: 21.2 mi, 40 mins (No traffic information)
 - U.S. 1 S and Wilkinson Rd: 20.2 mi, 41 mins (In current traffic: 46 mins)
- Driving directions to Richmond, VA:**
 - Head east on England St toward Maple St (0.5 mi)
 - Turn right onto U.S. 1 S (10.9 mi)
 - Turn left onto Azalea Ave (signs for US-1 S/Richmond) (0.2 mi)
 - Turn right onto Chamberlayne Ave (0.3 mi)
 - Continue onto N Belvidere St (0.4 mi)
 - Turn left onto W Broad St (0.9 mi)
 - Turn right onto N 8th St (377 ft)
 - Take the 1st right onto E Grace St (190 ft)

Identify elements of the model that map to IT-related content:

- Routes
- Routing Table
- Bandwidth
- Delay
- Cost
- Administrative Distance
- Default Route
- Static Route



Lab - Mapping the Internet (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Part 1: Determine Network Connectivity to a Destination Host

Part 2: Trace a Route to a Remote Server Using Tracert

Background / Scenario

Route tracing computer software lists the networks that data traverses from the user's originating end device to a distant destination device.

This network tool is typically executed at the command line as:

`tracert <destination network name or end device address>`

(Microsoft Windows systems)

or

`traceroute <destination network name or end device address>`

(UNIX, Linux systems, and Cisco devices, such as switches and routers)

Both **tracert** and **traceroute** determine the route taken by packets across an IP network.

The **tracert** (or **traceroute**) tool is often used for network troubleshooting. By showing a list of routers traversed, the user can identify the path taken to reach a particular destination on the network or across internetworks. Each router represents a point where one network connects to another network and through which the data packet was forwarded. The number of routers is known as the number of hops the data traveled from source to destination.

The displayed list can help identify data flow problems when trying to access a service such as a website. It can also be useful when performing tasks, such as downloading data. If there are multiple websites (mirrors) available for the same data file, one can trace each mirror to get a good idea of which mirror would be the fastest to use.

Command-line based route tracing tools are usually embedded with the operating system of the end device. This activity should be performed on a computer that has Internet access and access to a command line.

Instructor Note: Some institutions disable ICMP echo replies throughout the network. Before students begin this activity, make sure there are no local restrictions related to ICMP datagrams. This activity assumes that ICMP datagrams are not restricted by any local security policy.

Required Resources

PC with Internet access

Part 1: Determine Network Connectivity to a Destination Host

To trace the route to a distant network, the PC used must have a working connection to the Internet. Use the **ping** command to test whether a host is reachable. Packets of information are sent to the remote host with instructions to reply. Your local PC measures whether a response is received to each packet, and how long it takes for those packets to cross the network.

- a. At the command-line prompt, type **ping www.cisco.com** to determine if it is reachable.

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

- b. Now ping one of the Regional Internet Registry (RIR) websites located in different parts of the world to determine if it is reachable:

Africa: www.afrinic.net

Australia: www.apnic.net

South America: www.lacnic.net

North America: www.arin.net

Note: At the time of writing, the European RIR www.ripe.net does not reply to ICMP echo requests.

The website you selected will be used in Part 2 for use with the **tracert** command.

Part 2: Trace a Route to a Remote Server Using Tracert

After you determine if your chosen websites are reachable by using **ping**, you will use **tracert** to determine the path to reach the remote server. It is helpful to look more closely at each network segment that is crossed.

Each hop in the **tracert** results displays the routes that the packets take when traveling to the final destination. The PC sends three ICMP echo request packets to the remote host. Each router in the path decrements the time to live (TTL) value by 1 before passing it onto the next system. When the decremented TTL value reaches 0, the router sends an ICMP Time Exceeded message back to the source with its IP address and the current time. When the final destination is reached, an ICMP echo reply is sent to the source host.

For example, the source host sends three ICMP echo request packets to the first hop (192.168.1.1) with the TTL value of 1. When the router 192.168.1.1 receives the echo request packets, it decrements the TTL value to 0. The router sends an ICMP Time Exceeded message back to the source. This process continues until the source host sends the last three ICMP echo request packets with TTL values of 8 (hop number 8 in the output below), which is the final destination. After the ICMP echo request packets arrive at the final destination, the router responds to the source with ICMP echo replies.

For hops 2 and 3, these IP addresses are private addresses. These routers are the typical setup for point-of-presence (POP) of ISP. The POP devices connect users to an ISP network.

A web-based whois tool is found at <http://whois.domaintools.com/>. It is used to determine the domains traveled from the source to destination.

- a. At the command-line prompt, trace the route to www.cisco.com. Save the **tracert** output in a text file.
Alternatively, you can redirect the output to a text file by using **>** or **>>**.

```
C:\Users\User1> tracert www.cisco.com
```

or

Lab - Mapping the Internet

```
C:\Users\User1> tracert www.cisco.com > tracert-cisco.txt

Tracing route to e144.dscb.akamaiedge.net [23.67.208.170]
over a maximum of 30 hops:

 1      1 ms     <1 ms     <1 ms  192.168.1.1
 2     14 ms      7 ms      7 ms  10.39.0.1
 3     10 ms      8 ms      7 ms  172.21.0.118
 4     11 ms     11 ms     11 ms  70.169.73.196
 5     10 ms      9 ms     11 ms  70.169.75.157
 6     60 ms     49 ms      *   68.1.2.109
 7     43 ms     39 ms     38 ms  Equinix-DFW2.netarch.akamai.com [206.223.118.102]
 8     33 ms     35 ms     33 ms  a23-67-208-170.deploy.akamaitechnologies.com
[23.67.208.170]
```

Trace complete.

- b. The web-based tool at <http://whois.domaintools.com/> can be used to determine the owners of both the resulting IP address and domain names shown in the tracert tools output. Now perform a **tracert** to one of RIR web sites from Part 1 and save the results.

Africa: **www.afrinic.net**

Australia: **www.apnic.net**

Europe: **www.ripe.net**

South America: **www.lacnic.net**

North America: **www.arin.net**

List the domains below from your tracert results using the web-based whois tool.

Answers will vary. cox.net, level3.com, registro.br

- c. Compare the lists of domains crossed to reach the final destinations.

Reflection

What can affect **tracert** results?

Answer will vary but could include network outages, high traffic loads, firewall blocking ICMP packets, ACL on intermediary devices prevents ICMP packets and asymmetric forwarding paths.

Lab – Configuring Basic Router Settings with IOS CLI (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

- Cable equipment to match the network topology.
- Initialize and restart the router and switch.

Part 2: Configure Devices and Verify Connectivity

- Assign static IPv4 information to the PC interfaces.
- Configure basic router settings.
- Verify network connectivity.
- Configure the router for SSH.

Part 3: Display Router Information

- Retrieve hardware and software information from the router.
- Interpret the output from the startup configuration.
- Interpret the output from the routing table.
- Verify the status of the interfaces.

Part 4: Configure IPv6 and Verify Connectivity

Background / Scenario

This is a comprehensive lab to review previously covered IOS router commands. In Parts 1 and 2, you will cable the equipment and complete basic configurations and IPv4 interface settings on the router.

Lab – Configuring Basic Router Settings with IOS CLI

In Part 3, you will use SSH to connect to the router remotely and utilize IOS commands to retrieve information from the device to answer questions about the router. In Part 4, you will configure IPv6 on the router so that PC-B can acquire an IP address and then verify connectivity.

For review purposes, this lab provides the commands necessary for specific router configurations.

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

Note: Make sure that the router and switch have been erased and have no startup configurations. Refer to Appendix A for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Gigabit Ethernet interfaces on Cisco 1941 ISRs are autosensing and an Ethernet straight-through cable can be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

Part 1: Set Up the Topology and Initialize Devices

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

- a. Attach the devices as shown in the topology diagram, and cable as necessary.
- b. Power on all the devices in the topology.

Step 2: Initialize and reload the router and switch.

Note: Appendix A details the steps to initialize and reload the devices.

Part 2: Configure Devices and Verify Connectivity

Step 1: Configure the PC interfaces.

- a. Configure the IP address, subnet mask, and default gateway settings on PC-A.
- b. Configure the IP address, subnet mask, and default gateway settings on PC-B.

Step 2: Configure the router.

- a. Console into the router and enable privileged EXEC mode.
Router> **enable**
Router#
b. Enter into global configuration mode.

Lab – Configuring Basic Router Settings with IOS CLI

```
Router# config terminal  
Router(config)#
```

- c. Assign a device name to the router.

```
Router(config)# hostname R1
```

- d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.

```
R1(config)# no ip domain-lookup
```

- e. Require that a minimum of 10 characters be used for all passwords.

```
R1(config)# security passwords min-length 10
```

Besides setting a minimum length, list other ways to strengthen passwords.

Use capital letters, numbers, and special characters in passwords.

- f. Assign **cisco12345** as the privileged EXEC encrypted password.

```
R1(config)# enable secret cisco12345
```

- g. Assign **ciscoconpass** as the console password, establish a timeout, enable login, and add the **logging synchronous** command. The **logging synchronous** command synchronizes debug and Cisco IOS software output and prevents these messages from interrupting your keyboard input.

```
R1(config)# line con 0  
R1(config-line)# password ciscoconpass  
R1(config-line)# exec-timeout 5 0  
R1(config-line)# login  
R1(config-line)# logging synchronous  
R1(config-line)# exit  
R1(config)#
```

For the **exec-timeout** command, what do the **5** and **0** represent?

The session will timeout in 5 minutes and 0 seconds.

- h. Assign **ciscovtypass** as the vty password, establish a timeout, enable login, and add the **logging synchronous** command.

```
R1(config)# line vty 0 4  
R1(config-line)# password ciscovtypass  
R1(config-line)# exec-timeout 5 0  
R1(config-line)# login  
R1(config-line)# logging synchronous  
R1(config-line)# exit  
R1(config)#
```

- i. Encrypt the clear text passwords.

```
R1(config)# service password-encryption
```

- j. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.

```
R1(config)# banner motd #Unauthorized access prohibited!#
```

- k. Configure an IP address and interface description. Activate both interfaces on the router.

```
R1(config)# int g0/0
R1(config-if)# description Connection to PC-B
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# int g0/1
R1(config-if)# description Connection to S1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# exit
R1#
```

- I. Set the clock on the router; for example:

```
R1# clock set 17:00:00 18 Feb 2013
```

- m. Save the running configuration to the startup configuration file.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

What would be the result of reloading the router prior to completing the **copy running-config startup-config** command?

The contents of the running configuration would be erased. In this lab, the router would have no startup configuration. Upon a reboot, a user would be asked if they would like to enter initial configuration dialog.

Step 3: Verify network connectivity.

- a. Ping PC-B from a command prompt on PC-A.

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

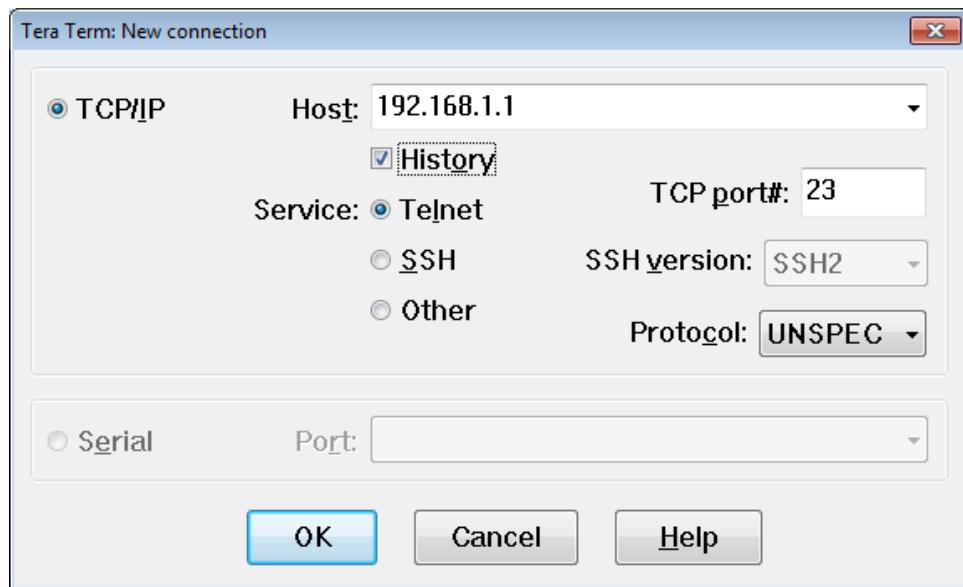
Were the pings successful? _____ Yes

After completing this series of commands, what type of remote access could be used to access R1?

Telnet

- b. Remotely access R1 from PC-A using the Tera Term Telnet client.

Open Tera Term and enter the G0/1 interface IP address of R1 in the Host: field of the Tera Term: New Connection window. Ensure that the **Telnet** radio button is selected and then click **OK** to connect to the router.



Was remote access successful? _____ Yes

Why is the Telnet protocol considered to be a security risk?

A Telnet session can be seen in clear text. It is not encrypted. Passwords can easily be seen using a packet sniffer.

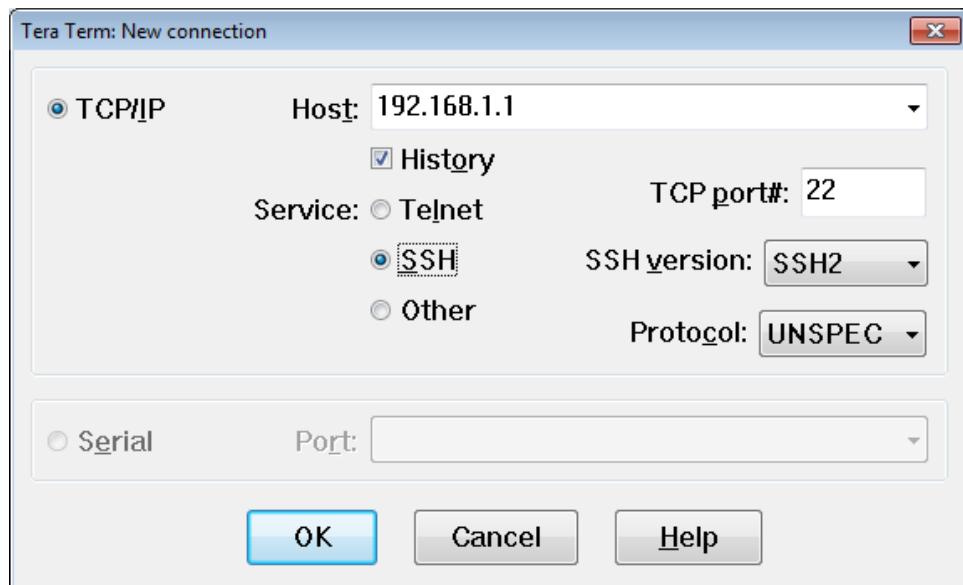
Step 4: Configure the router for SSH access.

- Enable SSH connections and create a user in the local database of the router.

```
R1# configure terminal  
R1(config)# ip domain-name CCNA-lab.com  
R1(config)# username admin privilege 15 secret adminpass1  
R1(config)# line vty 0 4  
R1(config-line)# transport input ssh  
R1(config-line)# login local  
R1(config-line)# exit  
R1(config)# crypto key generate rsa modulus 1024  
R1(config)# exit
```

- Remotely access R1 from PC-A using the Tera Term SSH client.

Open Tera Term and enter the G0/1 interface IP address of R1 in the Host: field of the Tera Term: New Connection window. Ensure that the **SSH** radio button is selected and then click **OK** to connect to the router.



Was remote access successful? _____ Yes

Part 3: Display Router Information

In Part 3, you will use **show** commands from an SSH session to retrieve information from the router.

Step 1: Establish an SSH session to R1.

Using Tera Term on PC-B, open an SSH session to R1 at IP address 192.168.0.1 and log in as **admin** with the password **adminpass1**.

Step 2: Retrieve important hardware and software information.

- Use the **show version** command to answer questions about the router.

```
R1# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M3, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team
```

```
ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
```

```
R1 uptime is 10 minutes
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.152-4.M3.bin"
Last reload type: Normal Reload
Last reload reason: power-on
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
```

Lab – Configuring Basic Router Settings with IOS CLI

Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

```
Cisco CISCO1941/K9 (revision 1.0) with 446464K/77824K bytes of memory.  
Processor board ID FTX1636848Z  
2 Gigabit Ethernet interfaces  
2 Serial(sync/async) interfaces  
1 terminal line  
DRAM configuration is 64 bits wide with parity disabled.  
255K bytes of non-volatile configuration memory.  
250880K bytes of ATA System CompactFlash 0 (Read/Write)
```

License Info:

License UDI:

```
-----  
Device#      PID          SN  
-----  
*0          CISCO1941/K9      FTX1636848Z
```

Technology Package License Information for Module: 'c1900'

```
-----  
Technology    Technology-package        Technology-package  
              Current       Type            Next reboot  
-----  
ipbase       ipbasek9     Permanent     ipbasek9  
security      None         None          None  
data         None         None          None
```

Configuration register is 0x2142 (will be 0x2102 at next reload)

What is the name of the IOS image that the router is running?

Image version may vary, but answers should be something like c1900-universalk9-mz.SPA.152-4.M3.bin.

How much non-volatile random-access memory (NVRAM) does the router have?

Answers may vary, but the output from the **show version** on 1941 router is: 255K bytes of non-volatile configuration memory.

How much Flash memory does the router have?

Answers may vary, but the default output from the **show version** command on the 1941 router is 250880K bytes of ATA System CompactFlash 0 (Read/Write).

- b. The **show** commands often provide multiple screens of outputs. Filtering the output allows a user to display certain sections of the output. To enable the filtering command, enter a pipe (|) character after a **show** command, followed by a filtering parameter and a filtering expression. You can match the output to the filtering statement by using the **include** keyword to display all lines from the output that contain the filtering expression. Filter the **show version** command, using **show version | include register** to answer the following question.

```
R1# show version | include register
Configuration register is 0x2142
```

What is the boot process for the router on the next reload?

Answers may vary. In most cases (0x2102), the router will undergo a normal boot, load the IOS from the Flash memory, and load the startup configuration from the NVRAM if present. If the config register is 0x2142, the router will bypass the startup config and begin at the user-mode command prompt. If the initial boot fails, the router goes into ROMMON mode.

Step 3: Display the startup configuration.

Use the **show startup-config** command on the router to answer the following questions.

```
R1# show start
Using 1674 out of 262136 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 10
enable secret 4 3mxoP2KRPf3sFHYl6Vm6.ssJJi9tOJqqb6DMG/YH5No
!
no aaa new-model
!
no ipv6 cef
ip source-route
```

Lab – Configuring Basic Router Settings with IOS CLI

```
!
no ip domain lookup
ip domain name CCNA-lab.com
ip cef
multilink bundle-name authenticated
!
!
!
license udi pid CISCO2911/K9 sn FTX1636848Z
!
!
username admin privilege 15 secret 7 1304131f020214B383779
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
description Connection to PC-B
ip address 192.168.0.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
description Connection to S1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 200 0000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!
banner motd ^CUnauthorized access prohibited!^C
!
line con 0
```

Lab – Configuring Basic Router Settings with IOS CLI

```
exec-timeout 5 0
password 7 060506324F410A160B0713181F
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
exec-timeout 5 0
password 7 060506324F411F0D1C0713181F
logging synchronous
login local
transport input ssh
!
scheduler allocate 20000 1000
end
```

How are passwords presented in the output?

Passwords are encrypted due to the service password-encryption command. The line con password of ciscoconpass is encrypted as 060506324F410A160B0713181F. The line vty password of ciscovtypass is encrypted as 060506324F411F0D1C0713181F.

Use the **show startup-config | begin vty** command.

```
line vty 0 4
exec-timeout 5 0
password 7 060506324F411F0D1C0713181F
login local
transport input ssh
!
scheduler allocate 20000 1000
end
```

What is the result of using this command?

A user receives the startup configuration output beginning with the line that includes the first instance of the filtering expression.

Step 4: Display the routing table on the router.

Use the **show ip route** command on the router to answer the following questions.

Lab – Configuring Basic Router Settings with IOS CLI

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      + - replicated route, % - next hop override
```

Gateway of last resort is not set

```
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet0/0
L        192.168.0.1/32 is directly connected, GigabitEthernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/1
```

What code is used in the routing table to indicate a directly connected network?

The C designates a directly connected subnet. An L designates a local interface. Both answers are correct.

How many route entries are coded with a C code in the routing table? _____ 2

Step 5: Display a summary list of the interfaces on the router.

Use the **show ip interface brief** command on the router to answer the following question.

```
R1# show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
Embedded-Service-Engine0/0 unassigned    YES unset  administratively down down
GigabitEthernet0/0     192.168.0.1    YES manual up       up
GigabitEthernet0/1     192.168.1.1    YES manual up       up
Serial0/0/0           unassigned     YES unset  administratively down down
Serial0/0/1           unassigned     YES unset  administratively down down
R1#
```

What command changed the status of the Gigabit Ethernet ports from administratively down to up?

no shutdown

Part 4: Configure IPv6 and Verify Connectivity

Step 1: Assign IPv6 addresses to R1 G0/0 and enable IPv6 routing.

Note: Assigning an IPv6 address in addition to an IPv4 address on an interface is known as dual stacking, because both the IPv4 and IPv6 protocol stacks are active. By enabling IPv6 unicast routing on R1, PC-B receives the R1 G0/0 IPv6 network prefix and can autoconfigure its IPv6 address and its default gateway.

Lab – Configuring Basic Router Settings with IOS CLI

- a. Assign an IPv6 global unicast address to interface G0/0, assign the link-local address in addition to the unicast address on the interface, and enable IPv6 routing.

```
R1# configure terminal  
R1(config)# interface g0/0  
R1(config-if)# ipv6 address 2001:db8:acad:a::1/64  
R1(config-if)# ipv6 address fe80::1 link-local  
R1(config-if)# no shutdown  
R1(config-if)# exit  
R1(config)# ipv6 unicast-routing  
R1(config)# exit
```

- b. Use the **show ipv6 int brief** command to verify IPv6 settings on R1.

```
R1#show ipv6 int brief  
Em0/0 [administratively down/down]  
    unassigned  
GigabitEthernet0/0 [up/up]  
    FE80::1  
    2001:DB8:ACAD:A::1  
GigabitEthernet0/1 [up/up]  
    unassigned  
Serial0/0/0 [administratively down/down]  
    unassigned  
Serial0/0/1 [administratively down/down]  
    Unassigned
```

If no IPv6 address is assigned to G0/1, why is it listed as [up/up]?

The [up/up] status reflects the Layer 1 and Layer 2 status of the interface and does not rely on Layer 3 for status.

- c. Issue the **ipconfig** command on PC-B to examine the IPv6 configuration.

What is the IPv6 address assigned to PC-B?

Answers will vary. IPv6 address of 2001:db8:acad:a:d428:7de2:997c:b05a

What is the default gateway assigned to PC-B? _____ fe80::1

Issue a ping from PC-B to the R1 default gateway link local address. Was it successful? _____ Yes

Issue a ping from PC-B to the R1 IPv6 unicast address 2001:db8:acad:a::1. Was it successful? _____
Yes

Reflection

1. In researching a network connectivity issue, a technician suspects that an interface was not enabled. What **show** command could the technician use to troubleshoot this issue?
-

Answers may vary. However, **show ip interface brief** or **show startup-config** would provide the information.

Lab – Configuring Basic Router Settings with IOS CLI

2. In researching a network connectivity issue, a technician suspects that an interface was assigned an incorrect subnet mask. What **show** command could the technician use to troubleshoot this issue?

show startup-config or show running-config

3. After configuring IPv6 on the R1 G0/0 PC-B LAN, if you were to ping from PC-A to the PC-B IPv6 address, would the ping succeed? Why or why not?

The ping would fail because R1 interface G0/1 was not configured with IPv6 and PC-A only has an IPv4 address.

Router Interface Summary Table

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

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

Appendix A: Initializing and Reloading a Router and Switch

Step 1: Initialize and reload the router.

- a. Console into the router and enable privileged EXEC mode.

```
Router> enable  
Router#
```

- b. Type the **erase startup-config** command to remove the startup configuration from NVRAM.

```
Router# erase startup-config  
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]  
[OK]  
Erase of nvram: complete  
Router#
```

- c. Issue the **reload** command to remove an old configuration from memory. When prompted to **Proceed with reload**, press Enter to confirm the reload. (Pressing any other key aborts the reload.)

```
Router# reload  
Proceed with reload? [confirm]  
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:  
Reload Command.
```

Note: You may be prompted to save the running configuration prior to reloading the router. Type **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

- d. After the router reloads, you are prompted to enter the initial configuration dialog. Enter **no** and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

- e. You are prompted to terminate autoinstall. Type **yes** and then press Enter.

```
Would you like to terminate autoinstall? [yes]: yes
```

Step 2: Initialize and reload the switch.

- a. Console into the switch and enter privileged EXEC mode.

```
Switch> enable  
Switch#
```

- b. Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash  
Directory of flash:/
```

2	-rwx	1919	Mar 1 1993 00:06:33 +00:00	private-config.text	
3	-rwx	1632	Mar 1 1993 00:06:33 +00:00	config.text	
4	-rwx	13336	Mar 1 1993 00:06:33 +00:00	multiple-fs	
5	-rwx	11607161	Mar 1 1993 02:37:06 +00:00	c2960-lanbasek9-mz.150-2.SE.bin	
6	-rwx	616	Mar 1 1993 00:07:13 +00:00	vlan.dat	

```
32514048 bytes total (20886528 bytes free)  
Switch#
```

- c. If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat  
Delete filename [vlan.dat]?
```

- d. You are prompted to verify the filename. At this point, you can change the filename or just press Enter if you have entered the name correctly.

- e. You are prompted to confirm deleting this file. Press Enter to confirm deletion. (Pressing any other key aborts the deletion.)

```
Delete flash:/vlan.dat? [confirm]  
Switch#
```

- f. Use the **erase startup-config** command to erase the startup configuration file from NVRAM. You are prompted to confirm removing the configuration file. Press Enter to confirm to erase this file. (Pressing any other key aborts the operation.)

```
Switch# erase startup-config
```

Lab – Configuring Basic Router Settings with IOS CLI

```
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#  
g. Reload the switch to remove any old configuration information from memory. You are prompted to confirm
reloading the switch. Press Enter to proceed with the reload. (Pressing any other key aborts the reload.)
Switch# reload
Proceed with reload? [confirm]

Note: You may be prompted to save the running configuration prior to reloading the switch. Type no and
press Enter.

System configuration has been modified. Save? [yes/no]: no

h. After the switch reloads, you should be prompted to enter the initial configuration dialog. Type no and
press Enter.

Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

Device Configs

Router R1

```
R1#show run
Building configuration...

Current configuration : 1742 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 10
enable secret 4 3mxoP2KRPf3sFHYl6Vm6.ssJJi9tOJqqb6DMG/YH5No
!
no aaa new-model
!
!
!
!
!
!
no ip domain lookup
```

Lab – Configuring Basic Router Settings with IOS CLI

```
ip domain name CCNA-lab.com
ip cef
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1941/K9 sn FTX1636848Z
license accept end user agreement
!
!
username admin privilege 15 password 7 1304131F0202142B383779
!
!
!
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
description Connection to PC-B
ip address 192.168.0.1 255.255.255.0
duplex auto
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:A::1/64
!
interface GigabitEthernet0/1
description Connection to S1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
```

Lab – Configuring Basic Router Settings with IOS CLI

```
no ip http secure-server
!
!
!
!
!
control-plane
!
!
banner motd ^CUnauthorized access prohibited!^C
!
line con 0
  exec-timeout 5 0
  password 7 03075218050022434019181604
  logging synchronous
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  exec-timeout 5 0
  password 7 14141B180F0B3C3F3D38322631
  logging synchronous
  login local
  transport input ssh
!
scheduler allocate 20000 1000
!
end
```



We Really Could Use a Map! (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Describe the three types of routes that are populated in a routing table (to include: directly-connected, static, and dynamic).

This modeling activity should help students feel more comfortable with reading a routing table. Two router tables will be presented to the students – they will read the tables, identify routing information, and reflect on how information was recorded in the table).

Scenario

Use the Ashland and Richmond routing tables shown below. With the help of a classmate, draw a network topology using the information from the tables. To assist you with this activity, follow these guidelines:

- Start with the Ashland router - use its routing table to identify ports and IP addresses/networks.
- Add the Richmond router - use its routing table to identify ports and IP addresses/networks.
- Add any other intermediary and end devices, as specified by the tables.

In addition, record answers from your group to the reflection questions provided with this activity.

Be prepared to share your work with another group or the class.

Resources

```
Ashland> show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
    C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
    L 192.168.1.1/32 is directly connected, GigabitEthernet0/1
  192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
    C 192.168.2.0/24 is directly connected, Serial0/0/0
    L 192.168.2.1/32 is directly connected, Serial0/0/0
  D 192.168.3.0/24 [90/2170368] via 192.168.4.2, 01:53:50, GigabitEthernet0/0
  192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
    C 192.168.4.0/24 is directly connected, GigabitEthernet0/0
    L 192.168.4.1/32 is directly connected, GigabitEthernet0/0
  D 192.168.5.0/24 [90/3072] via 192.168.4.2, 01:59:14, GigabitEthernet0/0
  S 192.168.6.0/24 [1/0] via 192.168.2.2

Ashland>
```

We Really Could Use a Map!

```
Richmond> show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set

S 192.168.1.0/24 [1/0] via 192.168.3.1
D 192.168.2.0/24 [90/2170368] via 192.168.5.2, 01:55:09, GigabitEthernet0/1
  192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
    C 192.168.3.0/24 is directly connected, Serial0/0/0
    L 192.168.3.2/32 is directly connected, Serial0/0/0
D 192.168.4.0/24 [90/3072] via 192.168.5.2, 01:55:09, GigabitEthernet0/1
  192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
    C 192.168.5.0/24 is directly connected, GigabitEthernet0/1
    L 192.168.5.1/32 is directly connected, GigabitEthernet0/1
  192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
    C 192.168.6.0/24 is directly connected, GigabitEthernet0/0
    L 192.168.6.1/32 is directly connected, GigabitEthernet0/0
Richmond>
```

Reflection

1. How many directly connected routes are listed on the Ashland router? What letter represents a direct connection to a network on a routing table?

The answer is C.

2. Find the route to the 192.168.6.0/24 network. What kind of route is this? Was it dynamically discovered by the Ashland router or manually configured by a network administrator on the Ashland router?

The answer is static route.

3. If you were configuring a default (static route) to any network from the Ashland router and wanted to send all data to 192.168.2.2 (the next hop) for routing purposes, how would you write it?

```
Ashland(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.2
```

4. If you were configuring a default (static route) to any network from the Ashland router and wanted to send all data through your exit interface, how would you write it?

```
Ashland(config)# ip route 0.0.0.0 0.0.0.0 S0/0/0
```

5. When would you choose to use static routing, instead of letting dynamic routing take care of the routing paths for you?

If a router has a very reliable port to use, you may wish to route all traffic through (or to) that port, as this decreases processing load on the router. Also, sometimes network administrators will route traffic to certain network through certain ports to secure their networks.

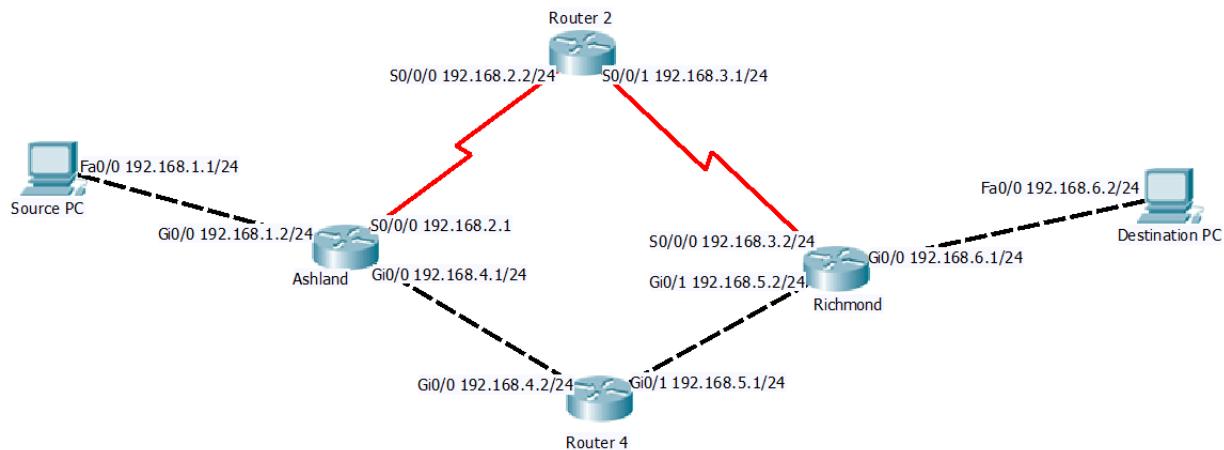
We Really Could Use a Map!

6. What is the significance of the L on the left side of the routing table?

It indicates the “link local” address of the port on the router which is configured by the network administrator.

Modeling Activity Graphic Representation (Instructor Resource Only)

Instructor Note: This is an example model that might be “built” as a result of this activity:



Identify elements of the model that map to IT-related content:

- Routes
- Routing Table
- Exit Interface
- Next Hop Interface
- Static Route
- Default Routing
- Static Routing
- Dynamic Routing
- Link Local

Which Way Should We Go? (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Explain the benefits of using static routes.

This chapter focuses on static routing and dynamic routing. This modeling activity helps students to think about how they can choose a path different from the best path for network communication.

Scenario

A huge sporting event is about to take place in your city. To attend the event, you make concise plans to arrive at the sports arena on time to see the entire game.

There are two routes you can take to drive to the event:

- Highway route - It is easy to follow and fast driving speeds are allowed.
- Alternative, direct route - You found this route using a city map. Depending on conditions, such as the amount of traffic or congestion, this just may be the way to get to the arena on time!

With a partner, discuss these options. Choose a preferred route to arrive at the arena in time to see every second of the huge sporting event.

Compare your optional preferences to network traffic, which route would you choose to deliver data communications for your small- to medium-sized business? Would it be the fastest, easiest route or the alternative, direct route? Justify your choice.

Complete the modeling activity .pdf and be prepared to justify your answers to the class or with another group.

Required Resources

None

Reflection

1. Which route did you choose as your first preference? On what criteria did you base your decision?

Students' answers will vary. Some will choose the fastest, easiest route and some will choose the alternate, direct-route. Criteria mentioned may include time constraints, speed of the route, traffic congestion on the route, and ease of following the route.

2. If traffic congestion were to occur on either route, would this change the path you would take to the arena? Explain your answer.

Most students would change their path in order to arrive at the sports arena on time. Others will decide to keep on the same path to the arena hoping that traffic congestion will subside. In either case, most will appreciate having a choice of routes.

3. A popular phrase that can be argued is "the shortest distance between two points is a straight line." Is this always true with delivery of network data? How do you compare your answer to this modeling activity scenario?

Which Way Should We Go?

Again, traffic can impact the route chosen. Sometimes it may be necessary to choose an alternate path for data delivery. Sometimes the alternate path will allow your data to be delivered more quickly than using the fastest path.

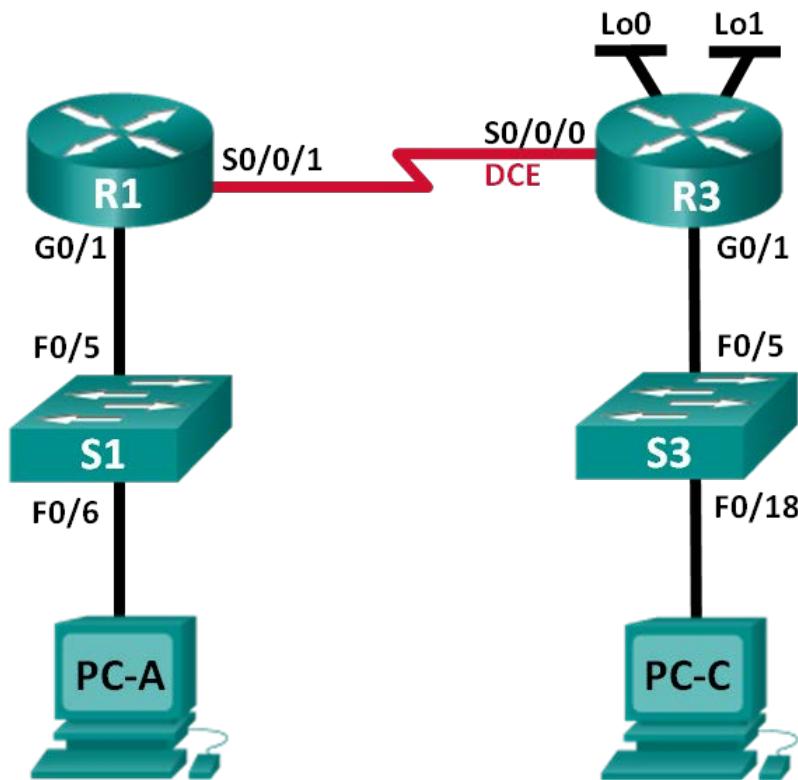
Identify elements of the model that map to IT-related content:

- Routers use routing protocols to record dynamic routes in their routing tables to indicate best-path delivery.
- The best-path delivery method can be changed to a manually configured path called a static route.
- A floating static route can be configured on a router to provide an alternate or backup path if the dynamic route becomes inoperable at any time.

Lab – Configuring IPv4 Static and Default Routes (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.0.1	255.255.255.0	N/A
	S0/0/1	10.1.1.1	255.255.255.252	N/A
R3	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
	Lo1	198.133.219.1	255.255.255.0	N/A
PC-A	NIC	192.168.0.10	255.255.255.0	192.168.0.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Basic Device Settings and Verify Connectivity

Part 3: Configure Static Routes

- Configure a recursive static route.
- Configure a directly connected static route.
- Configure and remove static routes.

Part 4: Configure and Verify a Default Route

Background / Scenario

A router uses a routing table to determine where to send packets. The routing table contains a set of routes that describe which gateway or interface the router uses to reach a specified network. Initially, the routing table contains only directly connected networks. To communicate with distant networks, routes must be specified and added to the routing table.

In this lab, you will manually configure a static route to a specified distant network based on a next-hop IP address or exit interface. You will also configure a static default route. A default route is a type of static route that specifies a gateway to use when the routing table does not contain a path for the destination network.

Note: This lab provides minimal assistance with the actual commands necessary to configure static routing. However, the required commands are provided in Appendix A. Test your knowledge by trying to configure the devices without referring to the appendix.

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

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

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Set Up the Topology and Initialize Devices

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

Step 2: Initialize and reload the router and switch.

Part 2: Configure Basic Device Settings and Verify Connectivity

In Part 2, you will configure basic settings, such as the interface IP addresses, device access, and passwords. You will verify LAN connectivity and identify routes listed in the routing tables for R1 and R3.

Step 1: Configure the PC interfaces.

Step 2: Configure basic settings on the routers.

- a. Configure device names, as shown in the Topology and Addressing Table.
- b. Disable DNS lookup.
- c. Assign **class** as the enable password and assign **cisco** as the console and vty password.
- d. Save the running configuration to the startup configuration file.

Step 3: Configure IP settings on the routers.

- a. Configure the R1 and R3 interfaces with IP addresses according to the Addressing Table.
- b. The S0/0/0 connection is the DCE connection and requires the **clock rate** command. The R3 S0/0/0 configuration is displayed below.

Instructor Note: For Cisco 1941 routers, DCE is automatically detected and the clock rate is automatically set to 2000000, and does not need to be configured.

```
R3(config)# interface s0/0/0
R3(config-if)# ip address 10.1.1.2 255.255.255.252
R3(config-if)# clock rate 128000
R3(config-if)# no shutdown
```

Step 4: Verify connectivity of the LANs.

- a. Test connectivity by pinging from each PC to the default gateway that has been configured for that host.
From PC-A, is it possible to ping the default gateway? _____ Yes
From PC-C, is it possible to ping the default gateway? _____ Yes
- b. Test connectivity by pinging between the directly connected routers.
From R1, is it possible to ping the S0/0/0 interface of R3? _____ Yes

Lab – Configuring IPv4 Static and Default Routes

If the answer is **no** to any of these questions, troubleshoot the configurations and correct the error.

- c. Test connectivity between devices that are not directly connected.

From PC-A, is it possible to ping PC-C? _____ No

From PC-A, is it possible to ping Lo0? _____ No

From PC-A, is it possible to ping Lo1? _____ No

Were these pings successful? Why or why not?

No, the router does not contain routes to the distant networks.

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

Step 5: Gather information.

- a. Check the status of the interfaces on R1 with the **show ip interface brief** command.

R1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	192.168.0.1	YES	manual	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	10.1.1.1	YES	manual	up	up

How many interfaces are activated on R1? _____ Two

- b. Check the status of the interfaces on R3.

R3# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	192.168.1.1	YES	manual	up	up
Serial0/0/0	10.1.1.2	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down
Loopback0	209.165.200.225	YES	manual	up	up
Loopback1	198.133.219.1	YES	manual	up	up

How many interfaces are activated on R3? _____ Four

- c. View the routing table information for R1 using the **show ip route** command.

R1# **show ip route**

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

Lab – Configuring IPv4 Static and Default Routes

```
Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/1
L        10.1.1.1/32 is directly connected, Serial0/0/1
    192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet0/1
L        192.168.0.1/32 is directly connected, GigabitEthernet0/1
```

What networks are present in the Addressing Table of this lab, but not in the routing table for R1?

192.168.1.0, 198.133.219.0, 209.165.200.224

- d. View the routing table information for R3.

```
R3# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      + - replicated route, % - next hop override
```

Gateway of last resort is not set

```
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.2/32 is directly connected, Serial0/0/0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/1
L        192.168.1.1/32 is directly connected, GigabitEthernet0/1
    198.133.219.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.133.219.0/24 is directly connected, Loopback1
L        198.133.219.1/32 is directly connected, Loopback1
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/27 is directly connected, Loopback0
L        209.165.200.225/32 is directly connected, Loopback0
```

What networks are present in the Addressing Table in this lab, but not in the routing table for R3?

192.168.0.0

Why are all the networks not in the routing tables for each of the routers?

The routers are not configured with static or dynamic routing; therefore, the routers only know about the directly connected networks.

Part 3: Configure Static Routes

In Part 3, you will employ multiple ways to implement static and default routes, you will confirm that the routes have been added to the routing tables of R1 and R3, and you will verify connectivity based on the introduced routes.

Note: This lab provides minimal assistance with the actual commands necessary to configure static routing. However, the required commands are provided in Appendix A. Test your knowledge by trying to configure the devices without referring to the appendix.

Step 1: Configure a recursive static route.

With a recursive static route, the next-hop IP address is specified. Because only the next-hop IP is specified, the router must perform multiple lookups in the routing table before forwarding packets. To configure recursive static routes, use the following syntax:

```
Router(config)# ip route network-address subnet-mask ip-address
```

- On the R1 router, configure a static route to the 192.168.1.0 network using the IP address of the Serial 0/0/0 interface of R3 as the next-hop address. Write the command you used in the space provided.

```
R1(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.2
```

- View the routing table to verify the new static route entry.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
      + - replicated route, % - next hop override
```

```
Gateway of last resort is not set
```

```
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/1
L        10.1.1.1/32 is directly connected, Serial0/0/1
    192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet0/1
L        192.168.0.1/32 is directly connected, GigabitEthernet0/1
S        192.168.1.0/24 [1/0] via 10.1.1.2
```

How is this new route listed in the routing table?

```
S    192.168.1.0/24 [1/0] via 10.1.1.2
```

From host PC-A, is it possible to ping the host PC-C? _____ No

These pings should fail. If the recursive static route is correctly configured, the ping arrives at PC-C. PC-C sends a ping reply back to PC-A. However, the ping reply is discarded at R3 because R3 does not have a return route to the 192.168.0.0 network in the routing table.

Step 2: Configure a directly connected static route.

With a directly connected static route, the `exit-interface` parameter is specified, which allows the router to resolve a forwarding decision in one lookup. A directly connected static route is typically used with a point-to-point serial interface. To configure directly connected static routes with an exit interface specified, use the following syntax:

```
Router(config)# ip route network-address subnet-mask exit-intf
```

- a. On the R3 router, configure a static route to the 192.168.0.0 network using S0/0/0 as the exit interface. Write the command you used in the space provided.

```
R3(config)# ip route 192.168.0.0 255.255.255.0 s0/0/0
```

- b. View the routing table to verify the new static route entry.

```
R3# show ip route
```

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

```
Gateway of last resort is not set
```

```
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks  
C      10.1.1.0/30 is directly connected, Serial0/0/0  
L      10.1.1.2/32 is directly connected, Serial0/0/0  
S      192.168.0.0/24 is directly connected, Serial0/0/0  
        192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks  
C      192.168.1.0/24 is directly connected, GigabitEthernet0/1  
L      192.168.1.1/32 is directly connected, GigabitEthernet0/1  
        198.133.219.0/24 is variably subnetted, 2 subnets, 2 masks  
C      198.133.219.0/24 is directly connected, Loopback1  
L      198.133.219.1/32 is directly connected, Loopback1  
        209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks  
C      209.165.200.224/27 is directly connected, Loopback0  
L      209.165.200.225/32 is directly connected, Loopback0
```

How is this new route listed in the routing table?

```
S      192.168.0.0/24 is directly connected, Serial0/0/0
```

- c. From host PC-A, is it possible to ping the host PC-C? _____ Yes

This ping should be successful.

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

Step 3: Configure a static route.

- a. On the R1 router, configure a static route to the 198.133.219.0 network using one of the static route configuration options from the previous steps. Write the command you used in the space provided.

```
R1(config)# ip route 198.133.219.0 255.255.255.0 s0/0/1
```

or

```
R1(config)# ip route 198.133.219.0 255.255.255.0 10.1.1.2
```

- b. On the R1 router, configure a static route to the 209.165.200.224 network on R3 using the other static route configuration option from the previous steps. Write the command you used in the space provided.

```
R1(config)# ip route 209.165.200.224 255.255.255.224 s0/0/1
```

or

```
R1(config)# ip route 209.165.200.224 255.255.255.224 10.1.1.2
```

- c. View the routing table to verify the new static route entry.

Note: The students may have different routing table outputs depending on the type of configured static routes.

```
R1# show ip route
```

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

Gateway of last resort is not set

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.1.1.0/30 is directly connected, Serial0/0/1
L      10.1.1.1/32 is directly connected, Serial0/0/1
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.0.0/24 is directly connected, GigabitEthernet0/1
L      192.168.0.1/32 is directly connected, GigabitEthernet0/1
S      192.168.1.0/24 [1/0] via 10.1.1.2
S      198.133.219.0/24 is directly connected, Serial0/0/1
209.165.200.0/27 is subnetted, 1 subnets
S      209.165.200.224 [1/0] via 10.1.1.2
```

How is this new route listed in the routing table?

```
S      198.133.219.0/24 is directly connected, Serial0/0/1
```

or

```
S      198.133.219.0/24 [1/0] via 10.1.1.2
```

Lab – Configuring IPv4 Static and Default Routes

- d. From host PC-A, is it possible to ping the R1 address 198.133.219.1? _____ Yes
This ping should be successful.

Step 4: Remove static routes for loopback addresses.

- a. On R1, use the **no** command to remove the static routes for the two loopback addresses from the routing table. Write the commands you used in the space provided.

```
R1(config)# no ip route 209.165.200.224 255.255.255.224 10.1.1.2
R1(config)# no ip route 198.133.219.0 255.255.255.0 s0/0/1
```

Note: A static route can be removed with the **no** command without specifying the exit interface or next-hop ip address as displayed below.

```
R1(config)# no ip route 209.165.200.224 255.255.255.224
R1(config)# no ip route 198.133.219.0 255.255.255.0
```

- b. View the routing table to verify the routes have been removed.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route, H - NHRP, 1 - LISP
      + - replicated route, % - next hop override
```

Gateway of last resort is not set

```
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/1
L        10.1.1.1/32 is directly connected, Serial0/0/1
    192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet0/1
L        192.168.0.1/32 is directly connected, GigabitEthernet0/1
S        192.168.1.0/24 [1/0] via 10.1.1.2
```

How many network routes are listed in the routing table on R1? _____ Three

Is the Gateway of last resort set? _____ No

Part 4: Configure and Verify a Default Route

In Part 4, you will implement a default route, confirm that the route has been added to the routing table, and verify connectivity based on the introduced route.

A default route identifies the gateway to which the router sends all IP packets for which it does not have a learned or static route. A default static route is a static route with 0.0.0.0 as the destination IP address and subnet mask. This is commonly referred to as a “quad zero” route.

In a default route, either the next-hop IP address or exit interface can be specified. To configure a default static route, use the following syntax:

Lab – Configuring IPv4 Static and Default Routes

```
Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address or exit-intf}
```

- a. Configure the R1 router with a default route using the exit interface of S0/0/1. Write the command you used in the space provided.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1
```

- b. View the routing table to verify the new static route entry.

```
R1#show ip route
```

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

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

```
S*    0.0.0.0/0 is directly connected, Serial0/0/1  
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks  
C      10.1.1.0/30 is directly connected, Serial0/0/1  
L      10.1.1.1/32 is directly connected, Serial0/0/1  
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks  
C      192.168.0.0/24 is directly connected, GigabitEthernet0/1  
L      192.168.0.1/32 is directly connected, GigabitEthernet0/1  
S      192.168.1.0/24 [1/0] via 10.1.1.2
```

How is this new route listed in the routing table?

```
S*    0.0.0.0/0 is directly connected, Serial0/0/1
```

What is the Gateway of last resort?

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

- c. From host PC-A, is it possible to ping the 209.165.200.225? _____ Yes
d. From host PC-A, is it possible to ping the 198.133.219.1? _____ Yes

These pings should be successful.

Reflection

1. A new network 192.168.3.0/24 is connected to interface G0/0 on R1. What commands could be used to configure a static route to that network from R3?

```
Answers will vary. ip route 192.168.3.0 255.255.255.0 10.1.1.1, ip route 192.168.3.0 255.255.255.0 s0/0/0, or  
ip route 0.0.0.0 0.0.0.0 s0/0/0.
```

Lab – Configuring IPv4 Static and Default Routes

2. Is there a benefit to configuring a directly connected static route instead of a recursive static route?

Configuring a directly attached static route allows the routing table to resolve the exit interface in a single search instead of in two searches as needed for recursive static routes.

3. Why is it important to configure a default route on a router?

A default route prevents the router from dropping packets to unknown destinations.

Router Interface Summary Table

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

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

Appendix A: Configuration Commands for Parts 2, 3, and 4

The commands listed in Appendix A are for reference only. This Appendix does not include all the specific commands necessary to complete this lab.

Basic Device Settings

Configure IP settings on the router.

```
R3(config)# interface s0/0/0
R3(config-if)# ip address 10.1.1.2 255.255.255.252
R3(config-if)# clock rate 128000
R3(config-if)# no shutdown
```

Static Route Configurations

Configure a recursive static route.

Lab – Configuring IPv4 Static and Default Routes

```
R1(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.2
```

Configure a directly connected static route.

```
R3(config)# ip route 192.168.0.0 255.255.255.0 s0/0/0
```

Remove static routes.

```
R1(config)# no ip route 209.165.200.224 255.255.255.224 serial0/0/1
```

or

```
R1(config)# no ip route 209.165.200.224 255.255.255.224 10.1.1.2
```

or

```
R1(config)# no ip route 209.165.200.224 255.255.255.224
```

Default Route Configuration

```
R1(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1
```

Device Configs - R1 and R3

Router R1 (after Part 4)

```
R1#show run
Building configuration...

Current configuration : 1547 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
```

Lab – Configuring IPv4 Static and Default Routes

Lab – Configuring IPv4 Static and Default Routes

```
!
!
banner motd ^CUnauthorized access prohibited!^C
!
line con 0
password 7 01100F175804
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 01100F175804
logging synchronous
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Router R3

```
R3#show run
Building configuration...

Current configuration : 1700 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
```

Lab – Configuring IPv4 Static and Default Routes

```
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
vtp domain TSHOOT
vtp mode transparent
!
redundancy
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface Loopback1
 ip address 198.133.219.1 255.255.255.0
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

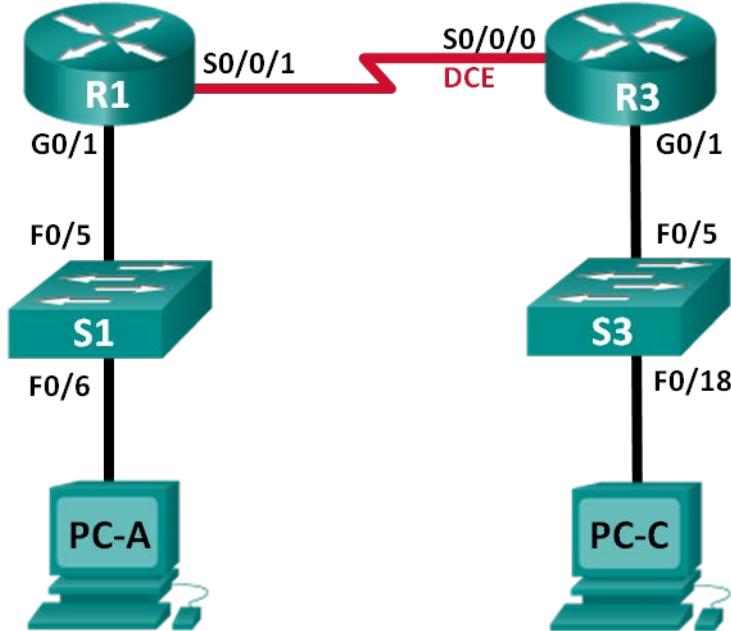
Lab – Configuring IPv4 Static and Default Routes

```
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 clock rate 256000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 192.168.0.0 255.255.255.0 Serial0/0/0
!
!
!
!
control-plane
!
!
!
banner motd ^CUnauthorized access prohibited!^C
!
line con 0
 password 7 110A1016141D
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 00071A150754
logging synchronous
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Lab – Configuring IPv6 Static and Default Routes (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Addressing Table

Device	Interface	IPv6 Address / Prefix Length	Default Gateway
R1	G0/1	2001:DB8:ACAD:A::/64 eui-64	N/A
	S0/0/1	FC00::1/64	N/A
R3	G0/1	2001:DB8:ACAD:B::/64 eui-64	N/A
	S0/0/0	FC00::2/64	N/A
PC-A	NIC	SLAAC	SLAAC
PC-C	NIC	SLAAC	SLAAC

Objectives

Part 1: Build the Network and Configure Basic Device Settings

- Enable IPv6 unicast routing and configure IPv6 addressing on the routers.
- Disable IPv4 addressing and enable IPv6 SLAAC for the PC network interfaces.
- Use **ipconfig** and **ping** to verify LAN connectivity.
- Use **show** commands to verify IPv6 settings.

Part 2: Configure IPv6 Static and Default Routes

- Configure a directly attached IPv6 static route.
- Configure a recursive IPv6 static route.
- Configure a default IPv6 static route.

Background / Scenario

In this lab, you will configure the entire network to communicate using only IPv6 addressing, including configuring the routers and PCs. You will use stateless address auto-configuration (SLAAC) for configuring the IPv6 addresses for the hosts. You will also configure IPv6 static and default routes on the routers to enable communication to remote networks that are not directly connected.

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

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

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will cable and configure the network to communicate using IPv6 addressing.

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

Step 2: Initialize and reload the routers and switches.

Step 3: Enable IPv6 unicast routing and configure IPv6 addressing on the routers.

- a. Using Tera Term, console into the router labeled R1 in the topology diagram and assign the router the name R1.
- b. Within global configuration mode, enable IPv6 routing on R1.
`R1(config)# ipv6 unicast-routing`
- c. Configure the network interfaces on R1 with IPv6 addresses. Notice that IPv6 is enabled on each interface. The G0/1 interface has a globally routable unicast address and EUI-64 is used to create the interface identifier portion of the address. The S0/0/1 interface has a privately routable, unique-local address, which is recommended for point-to-point serial connections.

`R1(config)# interface g0/1`

Lab – Configuring IPv6 Static and Default Routes

```
R1(config-if)# ipv6 address 2001:DB8:ACAD:A::/64 eui-64
R1(config-if)# no shutdown
R1(config-if)# interface serial 0/0/1
R1(config-if)# ipv6 address FC00::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
```

- d. Assign a device name to router R3.
- e. Within global configuration mode, enable IPv6 routing on R3.

```
R3(config)# ipv6 unicast-routing
```

- f. Configure the network interfaces on R3 with IPv6 addresses. Notice that IPv6 is enabled on each interface. The G0/1 interface has a globally routable unicast address and EUI-64 is used to create the interface identifier portion of the address. The S0/0/0 interface has a privately routable, unique-local address, which is recommended for point-to-point serial connections. The clock rate is set because it is the DCE end of the serial cable.

```
R3(config)# interface gigabit 0/1
R3(config-if)# ipv6 address 2001:DB8:ACAD:B::/64 eui-64
R3(config-if)# no shutdown
R3(config-if)# interface serial 0/0/0
R3(config-if)# ipv6 address FC00::2/64
R3(config-if)# clock rate 128000
R3(config-if)# no shutdown
R3(config-if)# exit
```

Step 4: Disable IPv4 addressing and enable IPv6 SLAAC for the PC network interfaces.

- a. On both PC-A and PC-C, navigate to the **Start** menu > **Control Panel**. Click the **Network and Sharing Center** link while viewing with icons. In the Network and Sharing Center window, click the **Change adapter settings** link on the left side of the window to open the Network Connections window.
- b. In the Network Connections window, you see the icons for your network interface adapters. Double-click the Local Area Connection icon for the PC network interface that is connected to the switch. Click the **Properties** to open the Local Area Connection Properties dialogue window.
- c. With the Local Area Connection Properties window open, scroll down through the items and uncheck the item **Internet Protocol Version 4 (TCP/IPv4)** check box to disable the IPv4 protocol on the network interface.
- d. With the Local Area Connection Properties window still open, click the **Internet Protocol Version 6 (TCP/IPv6)** check box, and then click **Properties**.
- e. With the Internet Protocol Version 6 (TCP/IPv6) Properties window open, check to see if the radio buttons for **Obtain an IPv6 address automatically** and **Obtain DNS server address automatically** are selected. If not, select them.
- f. With the PCs configured to obtain an IPv6 address automatically, they will contact the routers to obtain the network subnet and gateway information, and auto-configure their IPv6 address information. In the next step, you will verify the settings.

Step 5: Use ipconfig and ping to verify LAN connectivity.

- a. From PC-A, open a command prompt, type **ipconfig /all** and press Enter. The output should look similar to that shown below. In the output, you should see that the PC now has an IPv6 global unicast address, a link-local IPv6 address, and a link-local IPv6 default gateway address. You may also see a temporary

Lab – Configuring IPv6 Static and Default Routes

IPv6 address and under the DNS server addresses, three site-local addresses that start with FEC0. Site-local addresses are private addresses that were meant to be backwards compatible with NAT. However, they are not supported in IPv6 and are replaced by unique-local addresses.

```
C:\Users\User1> ipconfig /all
Windows IP Configuration

<Output omitted>

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix  . :
  Description . . . . . : Intel(R) 82577LC Gigabit Network Connection
  Physical Address. . . . . : 1C-C1-DE-91-C3-5D
  DHCP Enabled. . . . . : No
  Autoconfiguration Enabled . . . . : Yes
  IPv6 Address. . . . . : 2001:db8:acad:a:7c0c:7493:218d:2f6c(Preferred)
  Temporary IPv6 Address. . . . . : 2001:db8:acad:a:bc40:133a:54e7:d497(Preferred)
  Link-local IPv6 Address . . . . . : fe80::7c0c:7493:218d:2f6c%13(Preferred)
  Default Gateway . . . . . : fe80::6273:5cff:fe0d:1a61%13
  DNS Servers . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
  NetBIOS over Tcpip. . . . . : Disabled
```

Based on your network implementation and the output of the **ipconfig /all** command, did PC-A receive IPv6 addressing information from R1?

If the router has its Gigabit Ethernet interface and IPv6 unicast-routing configured, then the answer should be yes. Note: It may take a few seconds for the PC to auto-negotiate the IPv6 address information from the router.

- b. What is the PC-A global unicast IPv6 address?
-

Answers will vary due to the unique nature of the eui-64 host identifier. In the sample in Step 5a, 2001:db8:acad:a:7c0c:7493:218d:2f6c(Preferred) is global unicast address.

- c. What is the PC-A link-local IPv6 address?
-

Answers will vary due to the unique nature of the link-local address. In the sample in step 5a, fe80::7c0c:7493:218d:2f6c%13(Preferred) is link-local address.

- d. What is the PC-A default gateway IPv6 address?
-

Answers will vary due to the unique nature of the link-local default gateway address.

- e. From PC-A, use the **ping -6** command to issue an IPv6 ping to the link-local default gateway address. You should see replies from the R1 router.

Lab – Configuring IPv6 Static and Default Routes

```
C:\Users\User1> ping -6 <default-gateway-address>

C:\Users\User1> ping -6 fe80::6273:5cff:fe0d:1a61%13

Pinging fe80::6273:5cff:fe0d:1a61%13 with 32 bytes of data:
Reply from fe80::6273:5cff:fe0d:1a61%13: time<1ms
Reply from fe80::6273:5cff:fe0d:1a61%13: time<1ms
Reply from fe80::6273:5cff:fe0d:1a61%13: time<1ms
Reply from fe80::6273:5cff:fe0d:1a61%13: time<1ms

Ping statistics for fe80::6273:5cff:fe0d:1a61%13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Did PC-A receive replies to the ping from PC-A to R1?

If the PC was able to receive IP address information from the router, then answer should be yes.

- f. Repeat Step 5a from PC-C.

Did PC-C receive IPv6 addressing information from R3?

If the router has its Gigabit Ethernet interface and ipv6 unicast-routing configured, then the answer should be yes. Note: It may take a few seconds for the PC to auto-negotiate the IPv6 address information from the router.

- g. What is the PC-C global unicast IPv6 address?
-

Answers will vary due to the unique nature of the eui-64 host identifier.

- h. What is the PC-C link-local IPv6 address?
-

Answers will vary due to the unique nature of the link-local address.

- i. What is the PC-C default gateway IPv6 address?
-

Answers will vary due to the unique nature of the link-local default gateway address.

- j. From PC-C, use the **ping -6** command to ping the PC-C default gateway.

Did PC-C receive replies to the pings from PC-C to R3?

If the PC was able to receive IP address information from the router, then answer should be yes.

- k. Attempt an IPv6 **ping -6** from PC-A to the PC-C IPv6 address.

```
C:\Users\User1> ping -6 PC-C-IPv6-address
```

Was the ping successful? Why or why not?

The answer should be no because the routers have not been configured with static or dynamic routing and know only about the directly connected networks. Without the proper routes, the routers will drop packets destined for unknown networks.

Step 6: Use show commands to verify IPv6 settings.

- Check the status of the interfaces on R1 with the **show ipv6 interface brief** command.

```
R1# show ipv6 interface brief
Em0/0                  [administratively down/down]
    unassigned
GigabitEthernet0/0      [administratively down/down]
    unassigned
GigabitEthernet0/1      [up/up]
    FE80::6273:5CFF:FE0D:1A61
    2001:DB8:ACAD:A:6273:5CFF:FE0D:1A61
Serial0/0/0              [administratively down/down]
    unassigned
Serial0/0/1              [up/up]
    FE80::6273:5CFF:FE0D:1A60
    FC00::1
```

What are the two IPv6 addresses for the G0/1 interface and what kind of IPv6 addresses are they?

Answers will vary on the interface identifier portion of the address. Using the command output depicted above, the answer is: a link-local address at FE80::6273:5CFF:FE0D:1A61 and a global unicast address at 2001:DB8:ACAD:A:6273:5CFF:FE0D:1A61

What are the two IPv6 addresses for the S0/0/1 interface and what kind of IPv6 addresses are they?

Answers will vary on the interface identifier portion of the address. Using the command output depicted above, the answer is: a link-local address at FE80::6273:5CFF:FE0D:1A60 and a unique-local address at FC00::1.

- To see more detailed information on the IPv6 interfaces, type a **show ipv6 interface** command on R1 and press Enter.

```
R1# show ipv6 interface
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::6273:5CFF:FE0D:1A61
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A:6273:5CFF:FE0D:1A61, subnet is 2001:DB8:ACAD::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF0D:1A61
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
```

Lab – Configuring IPv6 Static and Default Routes

```
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.

Serial0/0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::6273:5CFF:FE0D:1A60
  No Virtual link-local address(es):
  Global unicast address(es):
    FC00::1, subnet is FC00::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF0D:1A60
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND RAs are suppressed (periodic)
  Hosts use stateless autoconfig for addresses.
```

What are the multicast group addresses for the Gigabit Ethernet 0/1 interface?

Answers will vary slightly. Based on the command output above:

FF02::1, FF02::2, FF02::1:FF0D:1A61

What are the multicast group addresses for the S0/0/1 interface?

Answers will vary slightly. Based on the command output above:

FF02::1, FF02::2, FF02::1:FF00:1, FF02::1:FF0D:1A60

What is an FF02::1 multicast address used for?

Multicasting to all nodes on the local network segment.

What is an FF02::2 multicast address used for?

Multicasting to all routers on the local network segment.

What kind of multicast addresses are FF02::1:FF00:1 and FF02::1:FF0D:1A60, and what are they used for?

Solicited-node multicast addresses. Each interface unicast or anycast address has to have a solicited-node multicast address for resolving neighbor addresses on the local-link.

- c. View the IPv6 routing table information for R1 using the **show ipv6 route** command. The IPv6 routing table should have two connected routes, one for each interface, and three local routes, one for each interface and one for multicast traffic to a Null0 interface.

```
R1# show ipv6 route
IPv6 Routing Table - default - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
      B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
      IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
      ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
      O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C  2001:DB8:ACAD:A::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L  2001:DB8:ACAD:A:6273:5CFF:FE0D:1A61/128 [0/0]
    via GigabitEthernet0/1, receive
C  FC00::/64 [0/0]
    via Serial0/0/1, directly connected
L  FC00::1/128 [0/0]
    via Serial0/0/1, receive
L  FF00::/8 [0/0]
    via Null0, receive
```

In what way does the routing table output of R1 reveal why you were unable to ping PC-C from PC-A?

The ping to PC-C was unsuccessful because there is no route to the 2001:DB8:ACAD:B::/64 network in the routing table.

Part 2: Configure IPv6 Static and Default Routes

In Part 2, you will configure IPv6 static and default routes three different ways. You will confirm that the routes have been added to the routing tables, and you will verify successful connectivity between PC-A and PC-C.

You will configure three types of IPv6 static routes:

- **Directly Connected IPv6 Static Route** – A directly connected static route is created when specifying the outgoing interface.
- **Recursive IPv6 Static Route** – A recursive static route is created when specifying the next-hop IP address. This method requires the router to execute a recursive lookup in the routing table in order to identify the outgoing interface.
- **Default IPv6 Static Route** – Similar to a quad zero IPv4 route, a default IPv6 static route is created by making the destination IPv6 prefix and prefix length all zeros, ::/0.

Step 1: Configure a directly connected IPv6 static route.

In a directly connected IPv6 static route, the route entry specifies the router outgoing interface. A directly connected static route is typically used with a point-to-point serial interface. To configure a directly attached IPv6 static route, use the following command format:

Lab – Configuring IPv6 Static and Default Routes

```
Router(config)# ipv6 route <ipv6-prefix/prefix-length> <outgoing-interface-type> <outgoing-interface-number>
```

- a. On router R1, configure an IPv6 static route to the 2001:DB8:ACAD:B::/64 network on R3, using the R1 outgoing S0/0/1 interface.

```
R1(config)# ipv6 route 2001:DB8:ACAD:B::/64 serial 0/0/1
R1(config)#
```

- b. View the IPv6 routing table to verify the new static route entry.

```
R1# show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
      B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
      IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
      ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
      O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C  2001:DB8:ACAD:A::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L  2001:DB8:ACAD:A:6273:5CFF:FE0D:1A61/128 [0/0]
    via GigabitEthernet0/1, receive
S  2001:DB8:ACAD:B::/64 [1/0]
    via Serial0/0/1, directly connected
C  FC00::/64 [0/0]
    via Serial0/0/1, directly connected
L  FC00::1/128 [0/0]
    via Serial0/0/1, receive
L  FF00::/8 [0/0]
    via Null0, receive
```

What is the code letter and routing table entry for the newly added route in the routing table?

```
S  2001:DB8:ACAD:B::/64 [1/0]
  via Serial0/0/1, directly connected
```

- c. Now that the static route has been configured on R1, is it now possible to ping the host PC-C from PC-A?

The answer is no, not yet.

These pings should fail. If the recursive static route is correctly configured, the ping arrives at PC-C. PC-C sends a ping reply back to PC-A. However, the ping reply is discarded at R3 because R3 does not have a return route to the 2001:DB8:ACAD:A::/64 network in the routing table. To successfully ping across the network, you must also create a static route on R3.

- d. On router R3, configure an IPv6 static route to the 2001:DB8:ACAD:A::/64 network, using the R3 outgoing S0/0/0 interface.

```
R3(config)# ipv6 route 2001:DB8:ACAD:A::/64 serial 0/0/0
R3(config)#
```

- e. Now that both routers have static routes, attempt an IPv6 **ping -6** from PC-A to the PC-C global unicast IPv6 address.

Lab – Configuring IPv6 Static and Default Routes

```
C:\Users\User1>ping -6 2001:db8:acad:b:8cf0:f8ab:f36e:dfa8

Pinging 2001:db8:acad:b:8cf0:f8ab:f36e:dfa8 with 32 bytes of data:
Reply from 2001:db8:acad:b:8cf0:f8ab:f36e:dfa8: time=17ms
Reply from 2001:db8:acad:b:8cf0:f8ab:f36e:dfa8: time=6ms
Reply from 2001:db8:acad:b:8cf0:f8ab:f36e:dfa8: time=6ms
Reply from 2001:db8:acad:b:8cf0:f8ab:f36e:dfa8: time=6ms

Ping statistics for 2001:db8:acad:b:8cf0:f8ab:f36e:dfa8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 17ms, Average = 8ms
```

Was the ping successful? Why?

With static routes configured on both R1 and R3, the ping should be successful.

Step 2: Configure a recursive IPv6 static route.

In a recursive IPv6 static route, the route entry has the next-hop router IPv6 address. To configure a recursive IPv6 static route, use the following command format:

```
Router(config)# ipv6 route <ipv6-prefix/prefix-length> <next-hop-ipv6-address>
```

- On router R1, delete the directly attached static route and add a recursive static route.

```
R1(config)# no ipv6 route 2001:DB8:ACAD:B::/64 serial 0/0/1
R1(config)# ipv6 route 2001:DB8:ACAD:B::/64 FC00::2
R1(config)# exit
```

- On router R3, delete the directly attached static route and add a recursive static route.

```
R3(config)# no ipv6 route 2001:DB8:ACAD:A::/64 serial 0/0/0
R3(config)# ipv6 route 2001:DB8:ACAD:A::/64 FC00::1
R3(config)# exit
```

- View the IPv6 routing table on R1 to verify the new static route entry.

```
R1# show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
      B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
      IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
      ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
      O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C  2001:DB8:ACAD:A::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L  2001:DB8:ACAD:A:6273:5CFF:FE0D:1A61/128 [0/0]
    via GigabitEthernet0/1, receive
S  2001:DB8:ACAD:B::/64 [1/0]
    via FC00::2
```

Lab – Configuring IPv6 Static and Default Routes

```
C  FC00::/64 [0/0]
    via Serial0/0/1, directly connected
L  FC00::1/128 [0/0]
    via Serial0/0/1, receive
L  FF00::/8 [0/0]
    via Null0, receive
```

What is the code letter and routing table entry for the newly added route in the routing table?

```
S  2001:DB8:ACAD:B::/64 [1/0]
    via FC00::2
```

- d. Verify connectivity by issuing a **ping -6** command from PC-A to PC-C.

Was the ping successful? _____ Yes

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

Step 3: Configure a default IPv6 static route.

In a default static route, the destination IPv6 prefix and prefix length are all zeros.

```
Router(config)# ipv6 route ::/0 <outgoing-interface-type> <outgoing-
interface-number> {and/or} <next-hop-ipv6-address>
```

- a. On router R1, delete the recursive static route and add a default static route.

```
R1(config)# no ipv6 route 2001:DB8:ACAD:B::/64 FC00::2
R1(config)# ipv6 route ::/0 serial 0/0/1
R1(config)#
```

- b. Delete the recursive static route and add a default static route on R3.

```
R3(config)# no ipv6 route 2001:DB8:ACAD:A::/64 FC00::1
R3(config)# ipv6 route ::/0 serial 0/0/0
R3(config)#
```

- c. View the IPv6 routing table on R1 to verify the new static route entry.

```
R1# show ipv6 route
IPv6 Routing Table - default - 6 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
      B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
      IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
      ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
      O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
      ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S  ::/0 [1/0]
    via Serial0/0/1, directly connected
C  2001:DB8:ACAD:A::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L  2001:DB8:ACAD:A:6273:5CFF:FE0D:1A61/128 [0/0]
    via GigabitEthernet0/1, receive
C  FC00::/64 [0/0]
    via Serial0/0/1, directly connected
L  FC00::1/128 [0/0]
```

Lab – Configuring IPv6 Static and Default Routes

```
via Serial0/0/1, receive  
L FF00::/8 [0/0]  
via Null0, receive
```

What is the code letter and routing table entry for the newly added default route in the routing table?

```
S ::/0 [1/0]  
via Serial0/0/1, directly connected
```

- d. Verify connectivity by issuing a **ping -6** command from PC-A to PC-C.

Was the ping successful? _____ Yes

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

Reflection

1. This lab focuses on configuring IPv6 static and default routes. Can you think of a situation where you would need to configure both IPv6 and IPv4 static and default routes on a router?
-
-
-

Many Internet service providers (ISPs) are implementing IPv6 networks, and in the near future may require their clients to connect to their networks using IPv6 addressing. In this situation, network administrators may decide to implement both IPv4 and IPv6 networks and would therefore need to configure both IPv6 and IPv4 routing.

2. In practice, configuring an IPv6 static and default route is very similar to configuring an IPv4 static and default route. Aside from the obvious differences between the IPv6 and IPv4 addressing, what are some other differences when configuring and verifying an IPv6 static route as compared to an IPv4 static route?
-
-
-

When configuring a static IPv6 route, the **ipv6 route** command is used instead of the **ip route** command. Another important difference is the need to use the **show ipv6 route** command to view the IPv6 routing table as compared to the IPv4 routing table with the **show ip route** command.

Router Interface Summary Table

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

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

Device Configs

Router R1

```
R1#show run
Building configuration...

Current configuration : 1222 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ipv6 unicast-routing
ipv6 cef
!
ip cef
multilink bundle-name authenticated
```

Lab – Configuring IPv6 Static and Default Routes

```
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
ipv6 address 2001:DB8:ACAD:A::/64 eui-64
ipv6 enable
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
ipv6 address FC00::1/64
ipv6 enable
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ipv6 route ::/0 Serial0/0/1
!
control-plane
!
line con 0
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
login
```

```
transport input all
!
scheduler allocate 20000 1000
!
end
```

Router R3

```
R3#show run
Building configuration...

Current configuration : 1241 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
ipv6 unicast-routing
ipv6 cef
!
ip cef
multilink bundle-name authenticated
!
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  no ip address
  duplex auto
  speed auto
  ipv6 address 2001:DB8:ACAD:B::/64 eui-64
  ipv6 enable
!
interface Serial0/0/0
```

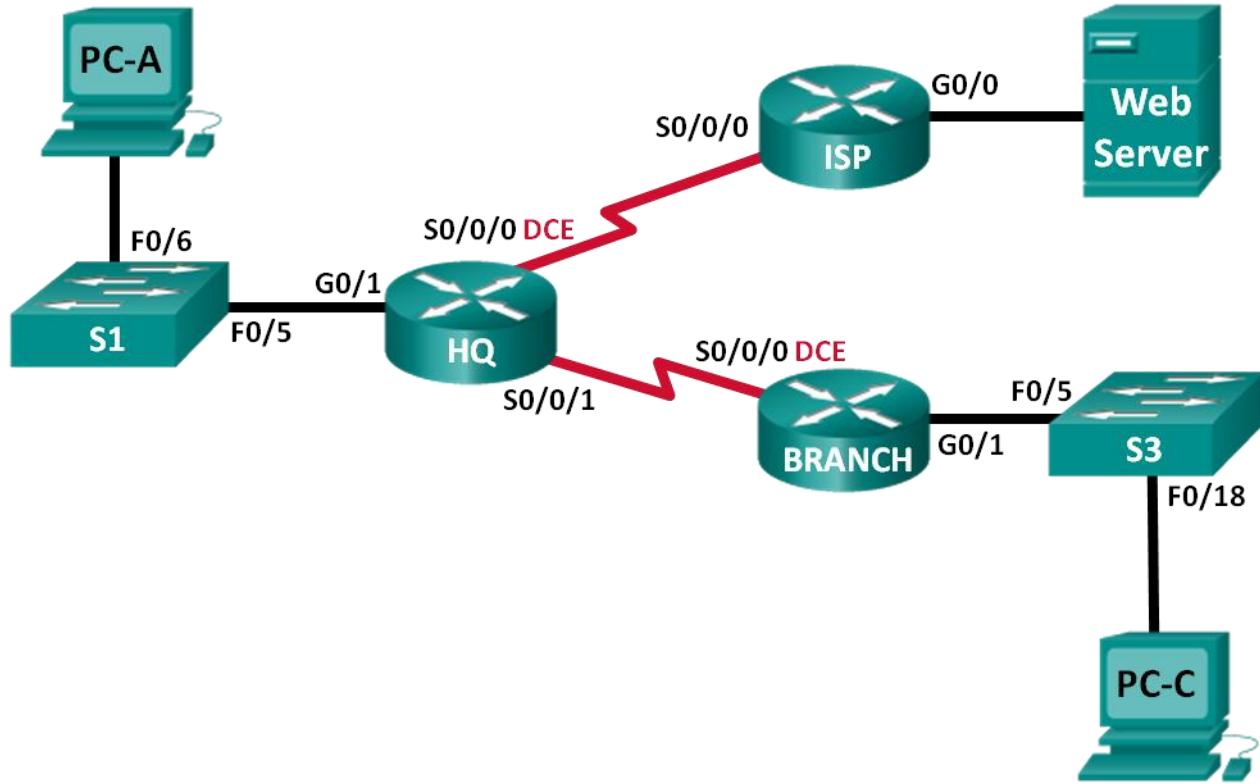
Lab – Configuring IPv6 Static and Default Routes

```
no ip address
ipv6 address FC00::2/64
ipv6 enable
clock rate 256000
!
interface Serial0/0/1
no ip address
shutdown
clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ipv6 route ::/0 Serial0/0/0
!
control-plane
!
line con 0
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Lab – Troubleshooting IPv4 and IPv6 Static Routes (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Addressing Table

Device	Interface	IP Address	Default Gateway
HQ	G0/1	192.168.0.1/25 2001:DB8:ACAD::1/64 FE80::1 link-local	N/A
	S0/0/0 (DCE)	10.1.1.2/30 2001:DB8:ACAD:20::2/64	N/A
	S0/0/1	192.168.0.253/30 2001:DB8:ACAD:2::1/64	N/A
ISP	G0/0	172.16.3.1/24 2001:DB8:ACAD:30::1/64 FE80::1 link-local	N/A
	S0/0/0	10.1.1.1/30 2001:DB8:ACAD:20::1/64	N/A
BRANCH	G0/1	192.168.1.1/24 2001:DB8:ACAD:1::1/64 FE80::1 link-local	N/A
	S0/0/0 (DCE)	192.168.0.254/30 2001:DB8:ACAD:2::2/64	N/A
S1	VLAN 1	N/A	N/A
S3	VLAN 1	N/A	N/A
PC-A	NIC	192.168.0.3/25 2001:DB8:ACAD::3/64	192.168.0.1 FE80::1
Web Server	NIC	172.16.3.3/24 2001:DB8:ACAD:30::3/64	172.16.3.1 FE80::1
PC-C	NIC	192.168.1.3/24 2001:DB8:ACAD:1::3/64	192.168.1.1 FE80::1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Troubleshoot Static Routes in an IPv4 Network

Part 3: Troubleshoot Static Routes in an IPv6 Network

Background / Scenario

As a network administrator, you must be able to configure routing of traffic using static routes. Understanding how to configure and troubleshoot static routing is a requirement. Static routes are commonly used for stub networks and default routes. Your company's ISP has hired you to troubleshoot connectivity issues on the network. You will have access to the HQ, BRANCH, and the ISP routers.

Lab – Troubleshooting IPv4 and IPv6 Static Routes

In this lab, you will begin by loading configuration scripts on each of the routers. These scripts contain errors that will prevent end-to-end communication across the network. You will need to troubleshoot each router to determine the configuration errors, and then use the appropriate commands to correct the configurations. When you have corrected all of the configuration errors, the hosts on the network should be able to communicate with each other.

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

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

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the routers and switches with some basic settings, such as passwords and IP addresses. Preset configurations are also provided for you for the initial router configurations. You will also configure the IP settings for the PCs in the topology.

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

Attach the devices as shown in the topology diagram and cable, as necessary.

Step 2: Initialize and reload the routers and switches.

Step 3: Configure basic settings for each router.

- a. Disable DNS lookup.
- b. Configure device name as shown in the topology.
- c. Assign **class** as the privileged EXEC mode password.
- d. Assign **cisco** as the console and vty passwords.
- e. Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 4: Configure hosts and Web Server.

- a. Configure IP addresses for IPv4 and IPv6.
- b. Configure IPv4 default gateway.

Step 5: Load router configurations.

Router HQ

```
hostname HQ
ipv6 unicast-routing
interface GigabitEthernet0/1
  ipv6 address 2001:DB8:ACAD::1/64
  ip address 192.168.0.1 255.255.255.128
  ipv6 address FE80::1 link-local
!no shutdown
interface Serial0/0/0
  ipv6 address 2001:DB8:ACAD:20::2/64
  ip address 10.1.1.2 255.255.255.252
  clock rate 800000
  no shutdown
interface Serial0/0/1
  ipv6 address 2001:DB8:ACAD:2::3/64
!ipv6 address 2001:DB8:ACAD:2::1/64
  ip address 192.168.0.253 255.255.255.252
  no shutdown
  ip route 172.16.3.0 255.255.255.0 10.1.1.1
  ip route 192.168.1.0 255.255.255.0 192.16.0.254
!ip route 192.168.1.0 255.255.255.0 192.168.0.254
  ipv6 route 2001:DB8:ACAD:1::/64 2001:DB8:ACAD:2::2
  ipv6 route 2001:DB8:ACAD:30::/64 2001:DB8:ACAD::20:1
!ipv6 route 2001:DB8:ACAD:30::/64 2001:DB8:ACAD:20::1
```

Router ISP

```
hostname ISP
ipv6 unicast-routing
interface GigabitEthernet0/0
  ipv6 address 2001:DB8:ACAD:30::1/64
  ip address 172.16.3.11 255.255.255.0
!ip address 172.16.3.1 255.255.255.0
  ipv6 address FE80::1 link-local
  no shutdown
interface Serial0/0/0
  ipv6 address 2001:DB8::ACAD:20:1/64
!ipv6 address 2001:DB8:ACAD:20::1/64
  ip address 10.1.1.1 255.255.255.252
  no shutdown
  ip route 192.168.1.0 255.255.255.0 10.1.1.2
!ip route 192.168.0.0 255.255.254.0 10.1.1.2
  ipv6 route 2001:DB8:ACAD::/62 2001:DB8:ACAD:20::2
```

Router BRANCH

Lab – Troubleshooting IPv4 and IPv6 Static Routes

```
hostname BRANCH
ipv6 unicast-routing
interface GigabitEthernet0/1
  ipv6 address 2001:DB8:ACAD:1::1/64
  ip address 192.168.1.1 255.255.255.0
  ipv6 address FE80::1 link-local
  no shutdown
interface Serial0/0/0
  ipv6 address 2001:DB8:ACAD:2::2/64
  clock rate 128000
  ip address 192.168.0.249 255.255.255.252
!ip address 192.168.0.254 255.255.255.252
  clock rate 128000
  no shutdown
  ip route 0.0.0.0 0.0.0.0 10.1.1.2
!ip route 0.0.0.0 0.0.0.0 192.168.0.253
!ipv6 unicast-routing
  ipv6 route ::/0 2001:DB8:ACAD::1
!ipv6 route ::/0 2001:DB8:ACAD:2::1
```

Part 2: Troubleshoot Static Routes in an IPv4 Network

IPv4 Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
HQ	G0/1	192.168.0.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A
	S0/0/1	192.168.0.253	255.255.255.252	N/A
ISP	G0/0	172.16.3.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
BRANCH	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.0.254	255.255.255.252	N/A
S1	VLAN 1	192.168.0.11	255.255.255.128	192.168.0.1
S3	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.0.3	255.255.255.128	192.168.0.1
Web Server	NIC	172.16.3.3	255.255.255.0	172.16.3.1
PC-C	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Step 1: Troubleshoot the HQ router.

The HQ router is the link between the ISP router and the BRANCH router. The ISP router represents the outside network while the BRANCH router represents the corporate network. The HQ router is configured with static routes to ISP and BRANCH networks.

- Display the status of the interfaces on HQ. Enter **show ip interface brief**. Record and resolve any issues as necessary.
-

The interface g0/1 is status administratively down and protocol down. Issue the **no shutdown** command on interface g0/1 to resolve the issue.

```
HQ# show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
Embedded-Service-Engine0/0 unassigned    YES unset  administratively down down
GigabitEthernet0/0   unassigned    YES unset  administratively down down
GigabitEthernet0/1   192.168.0.1    YES manual administratively down down
Serial0/0/0          10.1.1.2      YES manual up        up
Serial0/0/1          192.168.0.253  YES manual up        up
```

- Ping from HQ router to BRANCH router (192.168.0.254). Were the pings successful? _____ No
- Ping from HQ router to ISP router (10.1.1.1). Were the pings successful? _____ Yes
- Ping from PC-A to the default gateway. Were the pings successful? _____ Yes
- Ping from PC-A to PC-C. Were the pings successful? _____ No

Lab – Troubleshooting IPv4 and IPv6 Static Routes

- f. Ping from PC-A to Web Server. Were the pings successful? _____ No
g. Display the routing table on HQ. What non-directly connected routes are shown in the routing table?

```
static route to 172.16.3.0/24 via 10.1.1.1.
```

```
no route to 192.168.1.0/24
```

```
HQ# show ip route
```

```
<Output omitted>
```

```
Gateway of last resort is not set
```

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.1.1.0/30 is directly connected, Serial0/0/0
L      10.1.1.2/32 is directly connected, Serial0/0/0
      172.16.0.0/24 is subnetted, 1 subnets
S      172.16.3.0 [1/0] via 10.1.1.1
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.0.252/30 is directly connected, Serial0/0/1
L      192.168.0.253/32 is directly connected, Serial0/0/1
```

- h. Based on the results of the pings, routing table output, and static routes in the running configuration, what can you conclude about network connectivity?
-
-

There is a static route to PC-C's network but it does not show in the route table, need to re-enter route with correct destination IP. There is a static route to the 172.16.3.0 network but the Web Server is not reachable.

```
HQ# show run | include ip route
ip route 172.16.3.0 255.255.255.0 10.1.1.1
ip route 192.168.1.0 255.255.255.0 192.16.0.254
```

- i. What commands (if any) need to be entered to resolve routing issues? Record the command(s).
-
-

```
HQ(config)# no ip route 192.168.1.0 255.255.255.0 192.16.0.254
HQ(config)# ip route 192.168.1.0 255.255.255.0 192.168.0.254
```

- j. Repeat any of the steps from b to f to verify whether the problems have been resolved. Record your observations and possible next steps in troubleshooting connectivity.
-
-

Lab – Troubleshooting IPv4 and IPv6 Static Routes

The routing problems have not been resolved. The HQ router still cannot ping the BRANCH router. This may indicate there is an issue on BRANCH router that is preventing PC-A from pinging PC-C successfully. The HQ router can reach ISP router, but PC-A cannot ping Web Server. There may be an issue on the ISP router.

```
HQ# show ip route
```

```
<Output omitted>
```

```
Gateway of last resort is not set
```

```
    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.2/32 is directly connected, Serial0/0/0
    172.16.0.0/24 is subnetted, 1 subnets
S            172.16.3.0 [1/0] via 10.1.1.1
    192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.252/30 is directly connected, Serial0/0/1
L        192.168.0.253/32 is directly connected, Serial0/0/1
S            192.168.1.0/24 [1/0] via 192.168.0.254
```

Step 2: Troubleshoot the ISP router.

For the ISP router, there should be a route to HQ and BRANCH routers. One static route is configured on ISP router to reach the 192.168.1.0/24, 192.168.0.0/25, and 192.168.0.252/30 networks.

- Display the status of interfaces on ISP. Enter **show ip interface brief**. Record and resolve any issues as necessary.

The IP address for G0/0 is incorrectly configured.

```
ISP(config)# interface GigabitEthernet0/0
ISP(config-if)# ip address 172.16.3.1 255.255.255.0
```

```
ISP# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	172.16.3.11	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
Serial0/0/0	10.1.1.1	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down

- Ping from the ISP router to the HQ router (10.1.1.2). Were the pings successful? _____ Yes
- Ping from Web Server to the default gateway. Were the pings successful? _____ Yes
- Ping from Web Server to PC-A. Were the pings successful? _____ No
- Ping from Web Server to PC-C. Were the pings successful? _____ No
- Display the routing table on ISP. What non-directly connected routes are shown in the routing table?

Lab – Troubleshooting IPv4 and IPv6 Static Routes

Static route to 192.168.1.0/24 via 10.1.1.2

No route to 192.168.0.252/30

ISP# **show ip route**

<Output omitted>

Gateway of last resort is not set

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.1.1.0/30 is directly connected, Serial0/0/0
L      10.1.1.1/32 is directly connected, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.16.3.0/24 is directly connected, GigabitEthernet0/0
L      172.16.3.1/32 is directly connected, GigabitEthernet0/0
S      192.168.1.0/24 [1/0] via 10.1.1.2
```

- g. Based on the results of the pings, routing table output, and static routes in the running configuration, what can you conclude about network connectivity?

A summary route to 192.168.0.0/23 is needed to reach both 192.168.1.0/24 and 192.168.0.252/30 network.

- h. What commands (if any) need to be entered to resolve routing issues? Record the command(s).

(Hint: ISP only requires one summarized route to the company's networks 192.168.1.0/24, 192.168.0.0/25, and 192.168.0.252/32.)

```
ISP(config)# no ip route 192.168.1.0 255.255.255.0 10.1.1.2
ISP(config)# ip route 192.168.0.0 255.255.254.0 10.1.1.2
```

- i. Repeat any of the steps from b to e to verify whether the problems have been resolved. Record your observations and possible next steps in troubleshooting connectivity.

After the correction, Web Server can reach PC-A. However, Web Server still cannot ping PC-C. There are still more unresolved issues in the network.

ISP# **show ip route**

<Output omitted>

Gateway of last resort is not set

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.1.1.0/30 is directly connected, Serial0/0/0
```

Lab – Troubleshooting IPv4 and IPv6 Static Routes

```
L      10.1.1.1/32 is directly connected, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.16.3.0/24 is directly connected, GigabitEthernet0/0
L      172.16.3.1/32 is directly connected, GigabitEthernet0/0
S      192.168.0.0/23 [1/0] via 10.1.1.2
```

Step 3: Troubleshoot the BRANCH router.

For the BRANCH router, a default route is set to reach the rest of the network and ISP.

- Display the status of the interfaces on BRANCH. Enter **show ip interface brief**. Record and resolve any issues, as necessary.
-
-

The IP address for S0/0/0 is incorrectly configured.

```
BRANCH(config)# interface s0/0/0
BRANCH(config-if)# ip address 192.168.0.254 255.255.255.252
```

```
BRANCH# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	192.168.1.1	YES	manual	up	up
Serial0/0/0	192.168.0.249	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down

- Ping from the BRANCH router to the HQ router (192.168.0.253). Were the pings successful? _____
Yes
 - Ping from PC-C to the default gateway. Were the pings successful? _____ Yes
 - Ping from PC-C to PC-A. Were the pings successful? _____ No
 - Ping from PC-C to Web Server. Were the pings successful? _____ No
 - Display the routing table on BRANCH. What non-directly connected routes are shown in the routing table?
-
-

None.

```
BRANCH# show ip route
<Output omitted>
```

```
Gateway of last resort is not set
```

```
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.0.252/30 is directly connected, Serial0/0/0
L      192.168.0.254/32 is directly connected, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, GigabitEthernet0/1
L      192.168.1.1/32 is directly connected, GigabitEthernet0/1
```

Lab – Troubleshooting IPv4 and IPv6 Static Routes

- g. Based on the results of the pings, routing table output, and static routes in the running configuration, what can you conclude about network connectivity?

No static routes are displayed in the routing table. The default route was configured incorrectly.

```
BRANCH# show run | include ip route  
ip route 0.0.0.0 0.0.0.0 10.1.1.2
```

- h. What commands (if any) need to be entered to resolve routing issues? Record the command(s).

```
BRANCH(config)# no ip route 0.0.0.0 0.0.0.0 10.1.1.2  
BRANCH(config)# ip route 0.0.0.0 0.0.0.0 192.168.0.253
```

- i. Repeat any of the steps from b to e to verify whether the problems have been resolved. Record your observations and possible next steps in troubleshooting connectivity.

```
BRANCH# show ip route  
<Output omitted>
```

```
Gateway of last resort is 192.168.0.253 to network 0.0.0.0
```

```
S*    0.0.0.0/0 [1/0] via 192.168.0.253  
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks  
C      192.168.0.252/30 is directly connected, Serial0/0/0  
L      192.168.0.254/32 is directly connected, Serial0/0/0  
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks  
C      192.168.1.0/24 is directly connected, GigabitEthernet0/1  
L      192.168.1.1/32 is directly connected, GigabitEthernet0/1
```

Part 3: Troubleshoot Static Routes in an IPv6 Network

Device	Interface	IPv6 Address	Prefix Length	Default Gateway
HQ	G0/1	2001:DB8:ACAD::1	64	N/A
	S0/0/0 (DCE)	2001:DB8:ACAD:20::2	64	N/A
	S0/0/1	2001:DB8:ACAD:2::1	64	N/A
ISP	G0/0	2001:DB8:ACAD:30::1	64	N/A
	S0/0/0	2001:DB8:ACAD:20::1	64	N/A
BRANCH	G0/1	2001:DB8:ACAD:1::1	64	N/A
	S0/0/0 (DCE)	2001:DB8:ACAD:2::2	64	N/A
PC-A	NIC	2001:DB8:ACAD::3	64	FE80::1
Web Server	NIC	2001:DB8:ACAD:30::3	64	FE80::1
PC-C	NIC	2001:DB8:ACAD:1::3	64	FE80::1

Step 1: Troubleshoot the HQ router.

The HQ router is the link between the ISP router and the BRANCH router. The ISP router represents the outside network while the BRANCH router represents the corporate network. The HQ router is configured with static routes to both the ISP and the BRANCH networks.

- Display the status of the interfaces on HQ. Enter **show ipv6 interface brief**. Record and resolve any issues, as necessary.
-
-

The IPv6 address for S0/0/1 is incorrectly configured.

```
HQ(config)# interface s0/0/1
HQ(config-if)# no ipv6 address 2001:DB8:ACAD:2::3/64
HQ(config-if)# ipv6 address 2001:DB8:ACAD:2::1/64
HQ# show ipv6 interface brief
Em0/0 [administratively down/down]
    unassigned
GigabitEthernet0/0 [administratively down/down]
    unassigned
GigabitEthernet0/1 [up/up]
    FE80::1
    2001:DB8:ACAD::1
Serial0/0/0 [up/up]
    FE80::D68C:B5FF:FECE:A0C0
    2001:DB8:ACAD:20::2
Serial0/0/1 [up/up]
    FE80::D68C:B5FF:FECE:A0C0
    2001:DB8:ACAD:2::3ping
```

Lab – Troubleshooting IPv4 and IPv6 Static Routes

- b. Ping from the HQ router to the BRANCH router (2001:DB8:ACAD:2::2). Were the pings successful? _____ **Yes**
- c. Ping from the HQ router to the ISP router (2001:DB8:ACAD:20::1). Were the pings successful? _____ **No**
- d. Ping from PC-A to the default gateway. Were the pings successful? _____ **Yes**
- e. Ping from PC-A to Web Server. Were the pings successful? _____ **No**
- f. Ping from PC-A to PC-C. Were the pings successful? _____ **No**
- g. Display the routing table by issuing a **show ipv6 route** command. What non-directly connected routes are shown in the routing table?

Static route to 2001:DB8:ACAD:1::/64 via 2001:DB8:ACAD:2::2

Static route to 2001:DB8:ACAD:30::/64 via 2001:DB8:ACAD::20:1

```
HQ# show ipv6 route
IPv6 Routing Table - default - 9 entries
<Output omitted>
C 2001:DB8:ACAD::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L 2001:DB8:ACAD::1/128 [0/0]
    via GigabitEthernet0/1, receive
S 2001:DB8:ACAD:1::/64 [1/0]
    via 2001:DB8:ACAD:2::2
C 2001:DB8:ACAD:2::/64 [0/0]
    via Serial0/0/1, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
    via Serial0/0/1, receive
C 2001:DB8:ACAD:20::/64 [0/0]
    via Serial0/0/0, directly connected
L 2001:DB8:ACAD:20::2/128 [0/0]
    via Serial0/0/0, receive
S 2001:DB8:ACAD:30::/64 [1/0]
    via 2001:DB8:ACAD::20:1
L FF00::/8 [0/0]
    via Null0, receive
```

- h. Based on the results of the pings, routing table output, and static routes in the running configuration, what can you conclude about network connectivity?

Static route to 2001:DB8:ACAD:30::/64 has an incorrectly configured next hop address.

- i. What commands (if any) need to be entered to resolve routing issues? Record the command(s).

Lab – Troubleshooting IPv4 and IPv6 Static Routes

```
HQ(config)# no ipv6 route 2001:DB8:ACAD:30::/64 2001:DB8:ACAD::20:1
HQ(config)# ipv6 route 2001:DB8:ACAD:30::/64 2001:DB8:ACAD:20::1
```

- j. Repeat any of the steps from b to f to verify whether the problems have been resolved. Record your observations and possible next steps in troubleshooting connectivity.
-
-

The routing problems have not been resolved. The HQ router still cannot ping ISP router. The ISP router probably has IP address issue. PC-A still cannot ping PC-C and Web Server.

```
HQ# show ipv6 route
IPv6 Routing Table - default - 9 entries
<Output omitted>
C 2001:DB8:ACAD::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L 2001:DB8:ACAD::1/128 [0/0]
    via GigabitEthernet0/1, receive
S 2001:DB8:ACAD:1::/64 [1/0]
    via 2001:DB8:ACAD:2::2
C 2001:DB8:ACAD:2::/64 [0/0]
    via Serial0/0/1, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
    via Serial0/0/1, receive
C 2001:DB8:ACAD:20::/64 [0/0]
    via Serial0/0/0, directly connected
L 2001:DB8:ACAD:20::2/128 [0/0]
    via Serial0/0/0, receive
S 2001:DB8:ACAD:30::/64 [1/0]
    via 2001:DB8:ACAD:20::1
L FF00::/8 [0/0]
    via Null0, receive
```

Step 2: Troubleshoot the ISP router.

- On the ISP router, one static route is configured to reach all the networks on HQ and BRANCH routers.
- a. Display the status of the interfaces on ISP. Enter **show ipv6 interface brief**. Record and resolve any issues, as necessary.
-
-

The IPv6 address for S0/0/0 is incorrectly configured.

```
ISP(config)# interface s0/0/0
ISP(config-if)# no ipv6 address 2001:DB8::ACAD:20:1/64
ISP(config-if)# ipv6 address 2001:DB8:ACAD:20::1/64
ISP# show ipv6 interface brief
```

Lab – Troubleshooting IPv4 and IPv6 Static Routes

```
Em0/0 [administratively down/down]
      unassigned
GigabitEthernet0/0 [up/up]
      FE80::1
      2001:DB8:ACAD:30::1
GigabitEthernet0/1 [administratively down/down]
      unassigned
Serial0/0/0 [up/up]
      FE80::FE99:47FF:FE71:78A0
      2001:DB8::ACAD:20::1
Serial0/0/1 [administratively down/down]
      unassigned
```

- b. Ping from the ISP router to the HQ router (2001:DB8:ACAD:20::2). Were the pings successful? _____
Yes
- c. Ping from Web Server to the default gateway. Were the pings successful? _____ **Yes**
- d. Ping from Web Server to PC-A. Were the pings successful? _____ **Yes**
- e. Ping from Web Server to PC-C. Were the pings successful? _____ **No**
- f. Display the routing table. What non-directly connected routes are shown in the routing table?
-
-

Static route to 2001:DB8:ACAD::/62 via 2001:DB8:ACAD:20::2

```
ISP# show ipv6 route
IPv6 Routing Table - default - 6 entries
<Output omitted>
S 2001:DB8:ACAD::/62 [1/0]
  via 2001:DB8:ACAD:20::2
C 2001:DB8:ACAD:20::/64 [0/0]
  via Serial0/0/0, directly connected
L 2001:DB8:ACAD:20::1/128 [0/0]
  via Serial0/0/0, receive
C 2001:DB8:ACAD:30::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L 2001:DB8:ACAD:30::1/128 [0/0]
  via GigabitEthernet0/0, receive
L FF00::/8 [0/0]
  via Null0, receive
```

- g. Based on the results of the pings, routing table output, and static routes in the running configuration, what can you conclude about network connectivity?
-
-

No issues with the static route

- h. What commands (if any) need to be entered to resolve routing issues? Record the command(s).
-

Lab – Troubleshooting IPv4 and IPv6 Static Routes

None

- i. Repeat any of the steps from b to e to verify whether the problems have been resolved. Record your observations and possible next steps in troubleshooting connectivity.
-
-
-

Not all routing issues have been resolved. Web Server still cannot ping PC-C.

Step 3: Troubleshoot the BRANCH router.

For the BRANCH routers, there is a default route to the HQ router. This default route allows the BRANCH network to the ISP router and Web Server.

- a. Display the status of the interfaces on BRANCH. Enter **show ipv6 interface brief**. Record and resolve any issues, as necessary.
-
-

All interfaces were configured correctly according to the Addressing Table.

```
BRANCH# show ipv6 interface brief
Em0/0 [administratively down/down]
    unassigned
GigabitEthernet0/0 [administratively down/down]
    unassigned
GigabitEthernet0/1 [up/up]
    FE80::1
    2001:DB8:ACAD:1::1
Serial0/0/0 [up/up]
    FE80::FE99:47FF:FE71:7A20
    2001:DB8:ACAD:2::2
Serial0/0/1 [administratively down/down]
    unassigned
```

- b. Ping from the BRANCH router to the HQ router (2001:DB8:ACAD:2::1). Were the pings successful?

_____ Yes

- c. Ping from the BRANCH router to the ISP router (2001:DB8:ACAD:20::1). Were the pings successful?

_____ No

- d. Ping from PC-C to the default gateway. Were the pings successful? _____ Yes

- e. Ping from PC-C to PC-A. Were the pings successful? _____ No

- f. Ping from PC-C to Web Server. Were the pings successful? _____ No

- g. Display the routing table. What non-directly connected routes are shown in the routing table?
-
-

None

```
BRANCH# show ipv6 route
```

Lab – Troubleshooting IPv4 and IPv6 Static Routes

```
IPv6 Routing Table - default - 5 entries
<Output omitted>
C 2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L 2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/1, receive
C 2001:DB8:ACAD:2::/64 [0/0]
    via Serial0/0/0, directly connected
L 2001:DB8:ACAD:2::2/128 [0/0]
    via Serial0/0/0, receive
L FF00::/8 [0/0]
    via Null0, receive
```

- h. Based on the results of the pings, routing table output, and static routes in the running configuration, what can you conclude about network connectivity?

No default route is displayed in the table. The next-hop address was incorrectly configured.

- i. What commands (if any) need to be entered to resolve routing issues? Record the command(s).

```
BRANCH(config) # no ipv6 route ::/0 2001:DB8:ACAD::1
BRANCH(config) # ipv6 route ::/0 2001:DB8:ACAD:2::1
```

- j. Repeat any of the steps from b to f to verify whether the problems have been resolved. Record your observations and possible next steps in troubleshooting connectivity.

```
BRANCH# show ipv6 route
IPv6 Routing Table - default - 6 entries
<Output omitted>
S ::/0 [1/0]
    via 2001:DB8:ACAD:2::1
C 2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/1, directly connected
L 2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/1, receive
C 2001:DB8:ACAD:2::/64 [0/0]
    via Serial0/0/0, directly connected
L 2001:DB8:ACAD:2::2/128 [0/0]
    via Serial0/0/0, receive
L FF00::/8 [0/0]
    via Null0, receive
```

Router Interface Summary Table

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

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

Device Configs**Router HQ (Corrected)**

```
HQ# show run
Building configuration...

Current configuration : 1652 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAug.2
!
no aaa new-model
memory-size iomem 15
!
```

Lab – Troubleshooting IPv4 and IPv6 Static Routes

```
!
!
!
!
!
ip cef
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.0.1 255.255.255.128
duplex auto
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD::1/64
!
interface Serial0/0/0
ip address 10.1.1.2 255.255.255.252
ipv6 address 2001:DB8:ACAD:20::2/64
clock rate 2000000
!
interface Serial0/0/1
ip address 192.168.0.253 255.255.255.252
ipv6 address 2001:DB8:ACAD:2::1/64
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
```

Lab – Troubleshooting IPv4 and IPv6 Static Routes

```
!
ip route 172.16.3.0 255.255.255.0 10.1.1.1
ip route 192.168.1.0 255.255.255.0 192.168.0.254
!
ipv6 route 2001:DB8:ACAD:1::/64 2001:DB8:ACAD:2::2
ipv6 route 2001:DB8:ACAD:30::/64 2001:DB8:ACAD:20::1
!
!
!
control-plane
!
!
!
!
line con 0
password cisco
logging synchronous
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Router ISP (Corrected)

```
ISP# show run
Building configuration...

Current configuration : 1493 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
```

Lab – Troubleshooting IPv4 and IPv6 Static Routes

```
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
!
!
!
!
!
ip cef
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
ip address 172.16.3.1 255.255.255.0
duplex auto
speed auto
ipv6 address Fe80::1 link-local
ipv6 address 2001:DB8:ACAD:30::1/64
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
ip address 10.1.1.1 255.255.255.252
ipv6 address 2001:DB8:ACAD:20::1/64
!
interface Serial0/0/1
no ip address
```

Lab – Troubleshooting IPv4 and IPv6 Static Routes

```
shutdown
clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 192.168.0.0 255.255.254.0 10.1.1.2
!
ipv6 route 2001:DB8:ACAD::/62 2001:DB8:ACAD:20::2
!
!
!
control-plane
!
!
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Router BRANCH (Corrected)

```
BRANCH# show run
Building configuration...

Current configuration : 1522 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

Lab – Troubleshooting IPv4 and IPv6 Static Routes

```
!
hostname BRANCH
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 10
!
!
!
!
!
!
ip cef
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:1::1/64
!
interface Serial0/0/0
```

Lab – Troubleshooting IPv4 and IPv6 Static Routes

```
ip address 192.168.0.254 255.255.255.252
ipv6 address 2001:DB8:ACAD:2::2/64
clock rate 128000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.0.253
!
ipv6 route ::/0 2001:DB8:ACAD:2::1
!
!
control-plane
!
!
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Make It Static! (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Configure a static route.

This modeling activity reviews content from the curriculum regarding how default static routes are written and configured for IPv6 network addresses.

As the use of IPv6 addressing becomes more prevalent, it is important for network administrators to be able to direct network traffic between routers.

To prove that you are able to direct IPv6 traffic correctly and review the IPv6 default static route curriculum concepts, use the topology as shown in the .pdf file provided, specifically for this activity. Work with a partner to write an IPv6 statement for each of the three scenarios. Try to write the route statements without the assistance of completed labs, Packet Tracer files, etc.

- **Scenario 1**

IPv6 default static route from R2 directing all data through your S0/0/0 interface to the next hop address on R1.

- **Scenario 2**

IPv6 default static route from R3 directing all data through your S0/0/1 interface to the next hop address on R2.

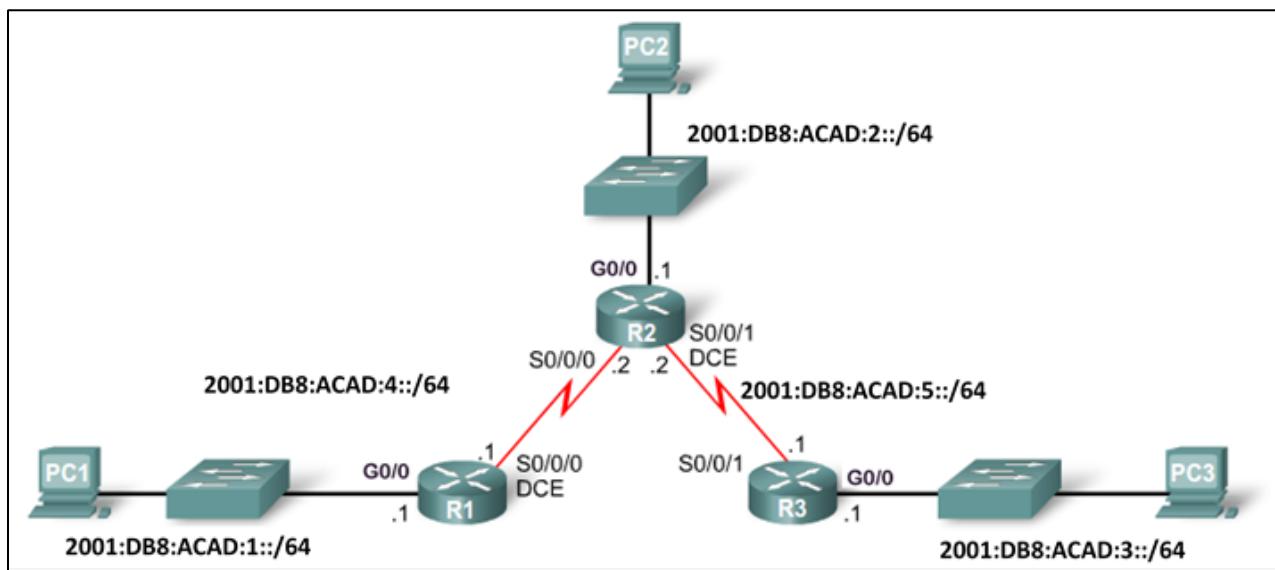
- **Scenario 3**

IPv6 default static route from R2 directing all data through your S0/0/1 interface to the next hop address on R3.

When complete, get together with another group and compare your written answers. Discuss any differences found in your comparisons.

Resources

Topology Diagram



Make It Static!

- **Scenario 1**

IPv6 default static route from R2 directing all data to the next hop address on R1.

Configuration Command	IPv6 Network to Route	Next Hop IPv6 Address
R2(config)# ipv6 route		

- **Scenario 2**

IPv6 default static route from R3 directing all data to the next hop address on R2.

Configuration Command	IPv6 Network to Route	Next Hop IPv6 Address
R3(config)# ipv6 route		

- **Scenario 3**

IPv6 default static route from R2 directing all data to the next hop address on R3.

Configuration Command	IPv6 Network to Route	Next Hop IPv6 Address
R2(config)# ipv6 route		

Instructor Activity Reference

- **Scenario 1**

IPv6 default static route from R2 directing all data to the next hop address on R1.

Configuration Command	IPv6 Network to Route	Next Hop IPv6 Address
R2(config)# ipv6 route	::/0	2001:DB8:ACAD:4::1

Make It Static!

- **Scenario 2**

IPv6 default static route from R3 directing all data to the next hop address on R2

Configuration Command	IPv6 Network to Route	Next Hop IPv6 Address
R3(config)# ipv6 route	::/0	2001:DB8:ACAD:5::2

- **Scenario 3**

IPv6 default static route from R2 directing all data to the next hop address on R3

Configuration Command	IPv6 Network to Route	Next Hop IPv6 Address
R2(config)# ipv6 route	::/0	2001:DB8:ACAD:5::1

Identify elements of the model that map to IT-related content:

- IPv6 address
- Next hop address
- Exit interface
- Default route
- Static route



How Much Does This Cost? (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Explain the operation of dynamic routing protocols.

To prepare for the concepts to be learned in this chapter, students will create physical routes, record progress of travel on the physical routes, and compare/contrast recorded results. Emphasis in this activity will be: number of hops, or steps used, data time recorded to start and finish the complete route, and dropped data, if the route finish is not reached within certain parameters.

Scenario

This modeling activity illustrates the network concept of routing cost.

You will be a member of a team of five students who travel routes to complete the activity scenarios. One digital camera or bring your own device (BYOD) with camera, a stopwatch, and the student file for this activity will be required per group. One person will function as the photographer and event recorder, as selected by each group. The remaining four team members will actively participate in the scenarios below.

A school or university classroom, hallway, outdoor track area, school parking lot, or any other location can serve as the venue for these activities.

Activity 1

The tallest person in the group establishes a start and finish line by marking 15 steps from start to finish, indicating the distance of the team route. Each student will take 15 steps from the start line toward the finish line and then stop on the 15th step—no further steps are allowed.

Note: Not all of the students may reach the same distance from the start line due to their height and stride differences. The photographer will take a group picture of the entire team's final location after taking the 15 steps required.

Activity 2

A new start and finish line will be established; however, this time, a longer distance for the route will be established than the distance specified in Activity 1. No maximum steps are to be used as a basis for creating this particular route. One at a time, students will “walk the new route from beginning to end twice”.

Each team member will count the steps taken to complete the route. The recorder will time each student and at the end of each team member's route, record the time that it took to complete the full route and how many steps were taken, as recounted by each team member and recorded on the team's student file.

Once both activities have been completed, teams will use the digital picture taken for Activity 1 and their recorded data from Activity 2 file to answer the reflection questions.

Group answers can be discussed as a class, time permitting.

Required Resources

- Digital or BYOD camera to record Activity 1's team results. Activity 2's data is based solely upon number of steps taken and the time it took to complete the route and no camera is necessary for Activity 2.

How Much Does This Cost?

- Stopwatch
- Student file accompanying this modeling activity so that Activity 2 results can be recorded as each student finishes the route.

Scenario – Part 2 Recording Matrix

Student Team Member Name	Time Used to Finish the Route	Number of Steps Taken to Finish the Route

Reflection Questions

1. The photographer took a picture of the team's progress after taking 15 steps for Activity 1. Most likely, some team members did not reach the finish line on their 15th step due to height and stride differences. What do you think would happen if network data did not reach the finish line, or destination, in the allowed number of hops or steps?

The data would not be successfully delivered. It would be dropped from the network route.

2. What could be done to help team members reach the finish line if they did not reach it in Activity 1?

Answers will vary, but students should mention increasing the number of steps (hops) allowed or removing the 15-step restriction.

3. Which person would best be selected to deliver data using the network route completed in Activity 2? Justify your answer.

The data took different amounts of time to be delivered, but it was delivered by all team members. The team member taking the shortest amount of time would be the best person to deliver the data.

4. Using the data recorded in Activity 2 and a limit of 255 steps, or hops, did all members of the team take more than 255 steps to finish their route? What would happen if they had to stop on the 254th step, or hop?

The route would not be finished (see same result from Activity 1 and 15 hop limit) and therefore, the route would not be finished – data would be dropped)

5. Use the data that was recorded in Activity 2. Would you say the parameters for the route were enough to finish it successfully if all team members reached the finish line with 255 or less steps, or hops? Justify your answer.

Yes, the numbers of steps allowed were not exceeded, therefore allowing the data to be delivered successfully.

How Much Does This Cost?

6. In network routing, different parameters are set for routing protocols. Use the data recorded for Activity 2. Would you select time, or number of steps, or hops, or a combination of both as your preferred routing type? List at least three reasons for your answers.

Answers will vary, but students could mention:

- Time – the shortest amount of time taken by a team member might be the preferred route.
- Hops – if all team members finished the route within the 255 step, or hop, limit, this might be selected as the preferred route.
- Both – the lowest number of hops taken by a particular team member in the shortest period of time might be the preferred route.

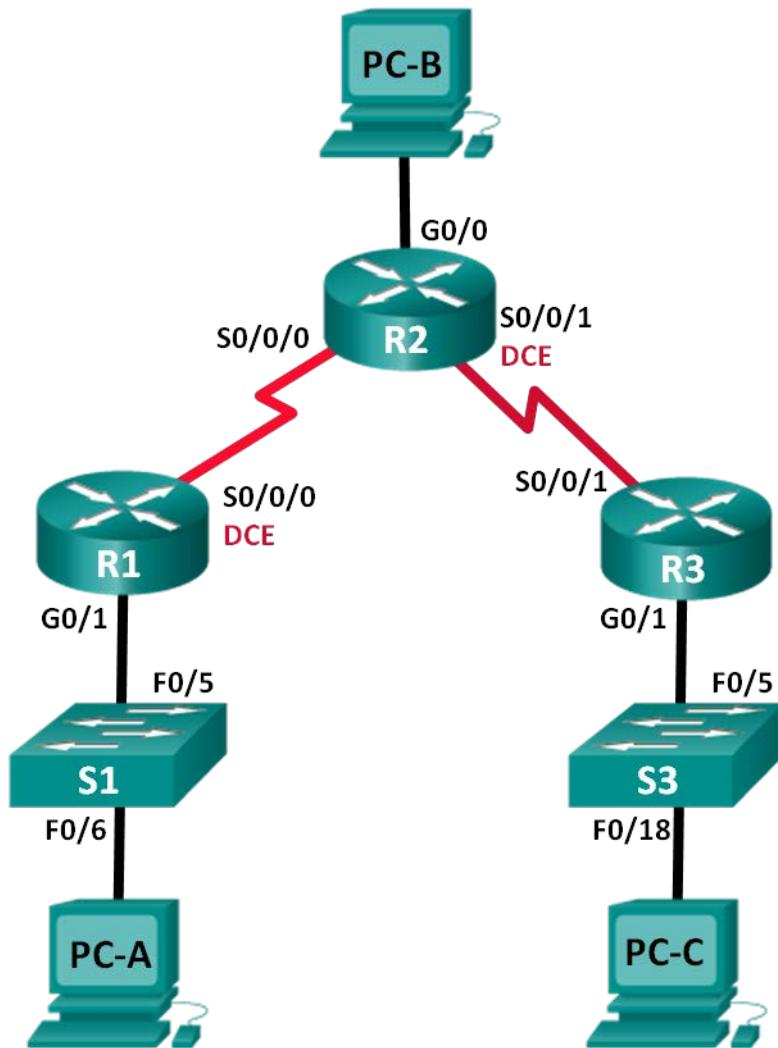
Identify elements of the model that map to IT-related content:

- Routers use number of hops, bandwidth, delay and cost metrics to determine the best path for network communication.
- Routing tables show records of the best routes for data delivery using the protocols configured for and reported by network traffic.
- Network administrators have a choice as to which types of routing protocols to use for network data delivery.
- As long as the parameters of a particular routing protocol are followed, data will be delivered successfully from source to destination.

Lab – Configuring Basic RIPv2 (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	172.30.10.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	G0/0	209.165.201.1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
R3	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	G0/1	172.30.30.1	255.255.255.0	N/A
S1	S0/0/1	10.2.2.1	255.255.255.252	N/A
	N/A	VLAN 1	N/A	N/A
S3	N/A	VLAN 1	N/A	N/A
	NIC	172.30.10.3	255.255.255.0	172.30.10.1
PC-A	NIC	209.165.201.2	255.255.255.0	209.165.201.1
PC-B	NIC	172.30.30.3	255.255.255.0	172.30.30.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure and Verify RIPv2 Routing

- Configure RIPv2 on the routers and verify that it is running.
- Configure a passive interface.
- Examine routing tables.
- Disable automatic summarization.
- Configure a default route.
- Verify end-to-end connectivity.

Background / Scenario

RIP version 2 (RIPv2) is used for routing of IPv4 addresses in small networks. RIPv2 is a classless, distance-vector routing protocol, as defined by RFC 1723. Because RIPv2 is a classless routing protocol, subnet masks are included in the routing updates. By default, RIPv2 automatically summarizes networks at major network boundaries. When automatic summarization has been disabled, RIPv2 no longer summarizes networks to their classful address at boundary routers.

In this lab, you will configure the network topology with RIPv2 routing, disable automatic summarization, propagate a default route, and use CLI commands to display and verify RIP routing information.

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

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

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and Serial cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings.

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

Step 2: Initialize and reload the router and switch.

Step 3: Configure basic settings for each router and switch.

- a. Disable DNS lookup.
- b. Configure device names as shown in the topology.
- c. Configure password encryption.
- d. Assign **class** as the privileged EXEC password.
- e. Assign **cisco** as the console and vty passwords.
- f. Configure a MOTD banner to warn users that unauthorized access is prohibited.
- g. Configure **logging synchronous** for the console line.
- h. Configure the IP addresses listed in the Addressing Table for all interfaces.
- i. Configure a description for each interface with an IP address.
- j. Configure the clock rate, if applicable, to the DCE serial interface.
- k. Copy the running-configuration to the startup-configuration.

Step 4: Configure PC IP Addressing.

Refer to the Addressing Table for IP address information of the PCs.

Step 5: Test connectivity.

At this point, the PCs are unable to ping each other.

- a. Each workstation should be able to ping the attached router. Verify and troubleshoot if necessary.
- b. The routers should be able to ping one another. Verify and troubleshoot if necessary.

Part 2: Configure and Verify RIPv2 Routing

In Part 2, you will configure RIPv2 routing on all routers in the network and then verify that the routing tables are updated correctly. After RIPv2 has been verified, you will disable automatic summarization, configure a default route, and verify end-to-end connectivity.

Step 1: Configure RIPv2 routing.

- Configure RIPv2 on R1 as the routing protocol and advertise the appropriate connected networks.

```
R1# config t  
R1(config)# router rip  
R1(config-router)# version 2  
R1(config-router)# passive-interface g0/1  
R1(config-router)# network 172.30.0.0  
R1(config-router)# network 10.0.0.0
```

The **passive-interface** command stops routing updates out the specified interface. This process prevents unnecessary routing traffic on the LAN. However, the network that the specified interface belongs to is still advertised in routing updates that are sent out across other interfaces.

- Configure RIPv2 on R3 and use the **network** statement to add the appropriate connected networks and prevent routing updates on the LAN interface.
- Configure RIPv2 on R2 and use the network statements to add the appropriate connected networks. Do not advertise the 209.165.201.0 network.

Note: It is not necessary to make the G0/0 interface passive on R2 because the network associated with this interface is not being advertised.

Step 2: Examine the current state of the network.

- The status of the two serial links can quickly be verified using the **show ip interface brief** command on R2.

```
R2# show ip interface brief  
Interface          IP-Address      OK? Method Status       Protocol  
Embedded-Service-Engine0/0 unassigned    YES unset  administratively down down  
GigabitEthernet0/0     209.165.201.1  YES manual up           up  
GigabitEthernet0/1     unassigned     YES unset  administratively down down  
Serial0/0/0          10.1.1.2       YES manual up           up  
Serial0/0/1          10.2.2.2       YES manual up           up
```

- Check connectivity between PCs.

From PC-A, is it possible to ping PC-B? _____ Why?

No, R2 is not advertising the route to PC-B.

From PC-A, is it possible to ping PC-C? _____ Why?

No, R1 and R3 do not have routes to the remote networks, and R2, incorrectly has two equal cost load balancing routes to the 172.30.0.0/16 subnet..

From PC-C, is it possible to ping PC-B? _____ Why?

Lab – Configuring Basic RIPv2

No, R2 is not advertising the route to PC-B.

From PC-C, is it possible to ping PC-A? _____ Why?

No, R1 and R3 do not have routes to the remote networks, and R2, incorrectly has two equal cost loadbalancing routes to the 172.30.0.0/16 subnet..

- c. Verify that RIPv2 is running on the routers.

You can use the **debug ip rip**, **show ip protocols**, and **show run** commands to confirm that RIPv2 is running. The **show ip protocols** command output for R1 is shown below.

```
R1# show ip protocols
Routing Protocol is "rip"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Sending updates every 30 seconds, next due in 7 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Redistributing: rip
Default version control: send version 2, receive 2
  Interface      Send   Recv Triggered RIP  Key-chain
    Serial0/0/0        2       2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  172.30.0.0
Passive Interface(s):
  GigabitEthernet0/1
Routing Information Sources:
  Gateway          Distance      Last Update
    10.1.1.2            120
Distance: (default is 120)
```

When issuing the **debug ip rip** command on R2, what information is provided that confirms RIPv2 is running?

RIP: sending v2 updates to 224.0.0.9 via Serial 0/0/0 (10.1.1.2).

When you are finished observing the debugging outputs, issue the **undebbug all** command at the privileged EXEC prompt.

When issuing the **show run** command on R3, what information is provided that confirms RIPv2 is running?

router rip
version 2

- d. Examine the automatic summarization of routes.

Lab – Configuring Basic RIPv2

The LANs connected to R1 and R3 are composed of discontiguous networks. R2 displays two equal-cost paths to the 172.30.0.0/16 network in the routing table. R2 displays only the major classful network address of 172.30.0.0 and does not display any of the subnets for this network.

```
R2# show ip route
<Output omitted>
    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.2/32 is directly connected, Serial0/0/0
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.2/32 is directly connected, Serial0/0/1
R        172.30.0.0/16 [120/1] via 10.2.2.1, 00:00:23, Serial0/0/1
                  [120/1] via 10.1.1.1, 00:00:09, Serial0/0/0
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.201.0/24 is directly connected, GigabitEthernet0/0
L        209.165.201.1/32 is directly connected, GigabitEthernet0/0
```

R1 displays only its own subnet for the 172.30.10.0/24 network. R1 does not have a route for the 172.30.30.0/24 subnet on R3.

```
R1# show ip route
<Output omitted>
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.1.1.0/30 is directly connected, Serial0/0/0
L        10.1.1.1/32 is directly connected, Serial0/0/0
R        10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:21, Serial0/0/0
    172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.30.10.0/24 is directly connected, GigabitEthernet0/1
L        172.30.10.1/32 is directly connected, GigabitEthernet0/1
```

R3 only displays its own subnet for the 172.30.30.0/24 network. R3 does not have a route for the 172.30.10.0/24 subnets on R1.

```
R3# show ip route
<Output omitted>
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C        10.2.2.0/30 is directly connected, Serial0/0/1
L        10.2.2.1/32 is directly connected, Serial0/0/1
R        10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:23, Serial0/0/1
    172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.30.30.0/24 is directly connected, GigabitEthernet0/1
L        172.30.30.1/32 is directly connected, GigabitEthernet0/1
```

Use the **debug ip rip** command on R2 to determine the routes received in the RIP updates from R3 and list them here.

172.30.0.0/16

R3 is not sending any of the 172.30.0.0 subnets, only the summarized route of 172.30.0.0/16, including the subnet mask. Therefore, the routing tables on R1 and R2 do not display the 172.30.0.0 subnets on R3.

Step 3: Disable automatic summarization.

- a. The **no auto-summary** command is used to turn off automatic summarization in RIPv2. Disable auto summarization on all routers. The routers will no longer summarize routes at major classful network boundaries. R1 is shown here as an example.

```
R1(config)# router rip  
R1(config-router)# no auto-summary
```

- b. Issue the **clear ip route *** command to clear the routing table.

```
R1(config-router)# end  
R1# clear ip route *
```

- c. Examine the routing tables. Remember that it will take some time to converge the routing tables after clearing them.

The LAN subnets connected to R1 and R3 should now be included in all three routing tables.

```
R2# show ip route  
<Output omitted>  
Gateway of last resort is not set  
  
    10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks  
C        10.1.1.0/30 is directly connected, Serial0/0/0  
L        10.1.1.2/32 is directly connected, Serial0/0/0  
C        10.2.2.0/30 is directly connected, Serial0/0/1  
L        10.2.2.2/32 is directly connected, Serial0/0/1  
    172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks  
R        172.30.0.0/16 [120/1] via 10.2.2.1, 00:01:01, Serial0/0/1  
                [120/1] via 10.1.1.1, 00:01:15, Serial0/0/0  
R        172.30.10.0/24 [120/1] via 10.1.1.1, 00:00:21, Serial0/0/0  
R        172.30.30.0/24 [120/1] via 10.2.2.1, 00:00:04, Serial0/0/1  
    209.165.201.0/24 is variably subnetted, 2 subnets, 2 masks  
C        209.165.201.0/24 is directly connected, GigabitEthernet0/0  
L        209.165.201.1/32 is directly connected, GigabitEthernet0/0  
R1# show ip route  
<Output omitted>  
Gateway of last resort is not set  
  
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks  
C        10.1.1.0/30 is directly connected, Serial0/0/0  
L        10.1.1.1/32 is directly connected, Serial0/0/0  
R        10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:12, Serial0/0/0  
    172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks  
C        172.30.10.0/24 is directly connected, GigabitEthernet0/1  
L        172.30.10.1/32 is directly connected, GigabitEthernet0/1  
R        172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:12, Serial0/0/0  
R3# show ip route  
<Output omitted>  
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks  
C        10.2.2.0/30 is directly connected, Serial0/0/1  
L        10.2.2.1/32 is directly connected, Serial0/0/1
```

Lab – Configuring Basic RIPv2

```
R      10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:23, Serial0/0/1
    172.30.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      172.30.30.0/24 is directly connected, GigabitEthernet0/1
L      172.30.30.1/32 is directly connected, GigabitEthernet0/1
R      172.30.10.0 [120/2] via 10.2.2.2, 00:00:16, Serial0/0/1
```

- d. Use the **debug ip rip** command on R2 to examine the RIP updates.

```
R2# debug ip rip
```

After 60 seconds, issue the **no debug ip rip** command.

What routes are in the RIP updates that are received from R3?

172.30.30.0/24

Are the subnet masks included in the routing updates? _____ yes

Step 4: Configure and redistribute a default route for Internet access.

- a. From R2, create a static route to network 0.0.0.0 0.0.0.0, using the **ip route** command. This forwards any traffic with an unknown destination address to PC-B at 209.165.201.2, simulating the Internet by setting a Gateway of Last Resort on router R2.

```
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.2
```

- b. R2 will advertise a route to the other routers if the **default-information originate** command is added to its RIP configuration.

```
R2(config)# router rip
```

```
R2(config-router)# default-information originate
```

Step 5: Verify the routing configuration.

- a. View the routing table on R1.

```
R1# show ip route
```

<Output omitted>

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

```
R*      0.0.0.0/0 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
    10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C      10.1.1.0/30 is directly connected, Serial0/0/0
L      10.1.1.1/32 is directly connected, Serial0/0/0
R      10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
    172.30.0.0/16 is variably subnetted, 3 subnets, 2 masks
C      172.30.10.0/24 is directly connected, GigabitEthernet0/1
L      172.30.10.1/32 is directly connected, GigabitEthernet0/1
R      172.30.30.0/24 [120/2] via 10.1.1.2, 00:00:13, Serial0/0/0
```

How can you tell from the routing table that the subnetted network shared by R1 and R3 has a pathway for Internet traffic?

There is a Gateway of Last Resort, and the default route shows up in the table as being learned via RIP.

Lab – Configuring Basic RIPv2

- b. View the routing table on R2.

How is the pathway for Internet traffic provided in its routing table?

R2 has a default static route to 0.0.0.0 via 209.165.201.2, which is directly connected to G0/0.

Step 6: Verify connectivity.

- a. Simulate sending traffic to the Internet by pinging from PC-A and PC-C to 209.165.201.2.

Were the pings successful? _____ Yes

- b. Verify that hosts within the subnetted network can reach each other by pinging between PC-A and PC-C.

Were the pings successful? _____ Yes

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

Reflection

1. Why would you turn off automatic summarization for RIPv2?
-

So the routers will no longer summarize routes at major classful network boundaries.

2. How did R1 and R3 learn the pathway to the Internet?
-

From RIP routing updates received from the router where the default route was configured (R2).

Router Interface Summary Table

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

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

Device Configs - Final

Router R1

```
R1# show run
Building configuration...

Current configuration : 1787 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
ip cef
!
```

Lab – Configuring Basic RIPv2

```
multilink bundle-name authenticated
!
redundancy
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
description R1 LAN
ip address 172.30.10.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
description Link to R2
ip address 10.1.1.1 255.255.255.252
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
!
router rip
version 2
passive-interface GigabitEthernet0/1
network 10.0.0.0
network 172.30.0.0
no auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^CUnauthorized access is strictly prohibited.^C
!
line con 0
password 7 045802150C2E
logging synchronous
login
```

Lab – Configuring Basic RIPv2

```
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 060506324F41
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Router R2

```
R2#show run
Building configuration...

Current configuration : 2073 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
ip cef
!
redundancy
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
description R2 LAN
ip address 209.165.201.1 255.255.255.0
```

Lab – Configuring Basic RIPv2

```
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
description Link to R1
ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
description Link to R3
ip address 10.2.2.2 255.255.255.252
clock rate 2000000
!
router rip
version 2
network 10.0.0.0
default-information originate
no auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 209.165.201.2
!
control-plane
!
banner motd ^CUnauthorized access is strictly prohibited.^C
!
line con 0
password 7 0822455D0A16
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 110A1016141D
```

```
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Router R3

```
R3#show run
Building configuration...

Current configuration : 1847 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
no ip domain lookup
ip cef
!
multilink bundle-name authenticated
!
redundancy
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  description R3 LAN
  ip address 172.30.30.1 255.255.255.0
  duplex auto
```

Lab – Configuring Basic RIPv2

```
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
description Link to R2
ip address 10.2.2.1 255.255.255.252
!
router rip
version 2
passive-interface GigabitEthernet0/1
network 10.0.0.0
network 172.30.0.0
no auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^CUnauthorized access is strictly prohibited.^C
!
line con 0
password 7 02050D480809
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 14141B180F0B
login
transport input all
!
scheduler allocate 20000 1000
!
end
```



IPv6 - Details, Details... (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Analyze a routing table to determine the route source, administrative distance, and metric for a given route to include IPv4/IPv6.

The focus of this activity is to review IPv6 routing table entries and concepts.

Scenario

After studying the concepts presented in this chapter concerning IPv6, you should be able to read a routing table easily and interpret the IPv6 routing information listed within it.

With a partner, use the IPv6 routing table diagram shown below. Record your answers to the Reflection questions. Then compare your answers with, at least, one other group from the class.

Required Resources

- Routing Table Diagram (as shown below)
- Two PCs or bring your own devices (BYODs): one PC or BYOD will display the Routing Table Diagram for your group to access while recording answers to the Reflection questions on the other PC or BYOD.

Routing Table Diagram

```
R3# show ipv6 route
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
        B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
        IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
        ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
        O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R    2001:DB8:CAFE:1::/64 [120/3]
      via FE80::FE99:47FF:FE71:78A0, Serial0/0/1
R    2001:DB8:CAFE:2::/64 [120/2]
      via FE80::FE99:47FF:FE71:78A0, Serial0/0/1
C    2001:DB8:CAFE:3::/64 [0/0]
      via GigabitEthernet0/0, directly connected
L    2001:DB8:CAFE:3::1/128 [0/0]
      via GigabitEthernet0/0, receive
      (output omitted)
```

Reflection

1. How many different IPv6 networks are shown on the routing table diagram? List them in the table provided below.

Three; you do not count the L route as it is already accounted for in the C route.

Routing Table IPv6 Networks
2001:DB8:CAFE:1::/64
2001:DB8:CAFE:2::/64
2001:DB8:CAFE:3::/64

2. The 2001:DB8:CAFE:3:: route is listed twice on the routing table, once with a /64 and once with a /128. What is the significance of this dual network entry?

The 2001:DB8:CAFE:3::/64 indicates a specific IPv6 network as represented by the first 64 network bits. The 2001:DB8:CAFE:3::1/128 indicates a local route entry. The /128 prefix assists with route lookup-up processes for packages destined for the interfaces.

3. How many routes in this table are RIP routes? What type of RIP routes are listed: RIP, RIPv2, or RIPng?

Two routes are RIP routes, both are RIPng because they show IPv6 network addresses.

4. Use the first RIP route, as listed on the routing table, as a reference. What is the administrative distance of this route? What is the cost? What is the significance of these two values?

The administrative distance is 120. This value is automatically assigned when RIP is configured without making specific changes. The cost for this route is 3 which indicates how many hops it would take to get to the specified network.

5. Use the second RIP route, as referenced by the routing table diagram. How many hops would it take to get to the 2001:DB8:CAFE:2::/64 network? What would happen to this routing table entry if the cost for this route exceeded 15 hops?

Two hops would be necessary to reach 2001:DB8:CAFE:2::/64. The route would disappear if the hop count increased to a cost of 16.

6. You are designing an IPv6 addressing scheme to add another router to your network's physical topology. Use the /64 prefix for this addressing scheme and an IPv6 network base of 2001:DB8:CAFF:2::/64,. What would

IPv6 – Details, Details...

be the next, numerical network assignment you could use if the first three hexets remained the same?
Justify your answer.

The next physical addressing space could possibly be assigned as 2001:DB8:CAFF:3::/64. If the first three hexets stayed the same, increments would be applied to the fourth hexet. The last 64 bits would be reserved for host addressing unless the prefix of /64 changes.

Identify elements of the model that map to IT-related content:

- IPv6 addresses
- RIPng routing protocol
- Administrative distance
- Cost
- Link local addresses
- Hextets
- Network prefixes



Sent or Received (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Describe convergence of data, voice, and video in the context of switched networks.

Students will be able to explain how switches can help LAN end devices send and receive data, voice and video data.

Scenario

Individually, or in groups (per the instructor's decision), discuss various ways hosts send and receive data, voice, and streaming video.

- Develop a matrix (table) listing network data types that can be sent and received. Provide five examples.

Your matrix table might look something like this:

Sent	Received
Client requests a web page from a web server.	Web server send web page to requesting client.

Save your work in either hard- or soft-copy format. Be prepared to discuss your matrix and statements in a class discussion.

Resources

Internet connectivity

Reflection

1. If you are receiving data, how do you think a switch assists in that process?

Students should mention that switches process data to and from end devices - many users can be sending and receiving data at the same time.

2. If you are sending network data, how do you think a switch assists in that process?

Switches allow multiple recipients to send and receive data simultaneously. Compared to hubs, a switch allows for better used of the bandwidth.

Sent or Received

Matrix Answers (will vary)

Instructor Note: This is a representative model that might be "built" as a result of this activity:

Sent	Received
Client requests a web page from a web server.	Automatic updates to your cell telephone applications Web server send web page to requesting client.
Client requests a file from a FTP server.	FTP server sends the requested file to the client.
Client requests a streaming video from a server.	Server transmits video to requesting clients.
Bob sends instant message to Mary.	Mary receives instant from Bob.
Ethernet switch receives an Ethernet frame on ingress port 1.	Ethernet switch forwards frame out egress port 4.
Bob sends VoIP packets from his IP phone.	Mary receives VoIP packets on her IP phone.



It's Network Access Time (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Describe features available for switches to support requirements of a small- to medium-sized business network.

Students will design two networks using Packet Tracer to suffice requirements shown in a LAN and WAN scenarios.

Scenario

Use Packet Tracer for this activity. Work with a classmate to create two network designs to accommodate the following scenarios:

Scenario 1 – Classroom Design (LAN)

- 15 student end devices represented by 1 or 2 PCs.
- 1 instructor end device; a server is preferred.
- Device capability to stream video presentations over LAN connection. Internet connectivity is not required in this design.

Scenario 2 – Administrative Design (WAN)

- All requirements as listed in Scenario 1.
- Add access to and from a remote administrative server for video presentations and pushed updates for network application software.

Both the LAN and WAN designs should fit on to one Packet Tracer file screen. All intermediary devices should be labeled with the switch model (or name) and the router model (or name).

Save your work and be ready to justify your device decisions and layout to your instructor and the class.

Reflection

1. What are some problems that may be encountered if you receive streaming video from your instructor's server through a low-end switch?

Answers will vary – bandwidth might be too low for the video stream to many recipients causing lag time – distortion may result in picture, audio, etc. Some stations could be “kicked out” as a result of traffic overload depending on the application program being used to stream the video, etc. There is also the possibility of “sniffing or snooping” depending on how the switch is configured.

2. How would the traffic flow be determined: multicast or broadcast – in transmission?

When users have to “log in” to the application to receive the video transmission, this would be considered a multicast. If students are set up collectively into a group by the server to push the stream, it would be considered a broadcast on the LAN side.

3. What would influence your decision on the type of switch to use for voice, streaming video and regular data these types of transmissions?

It's Network Access Time

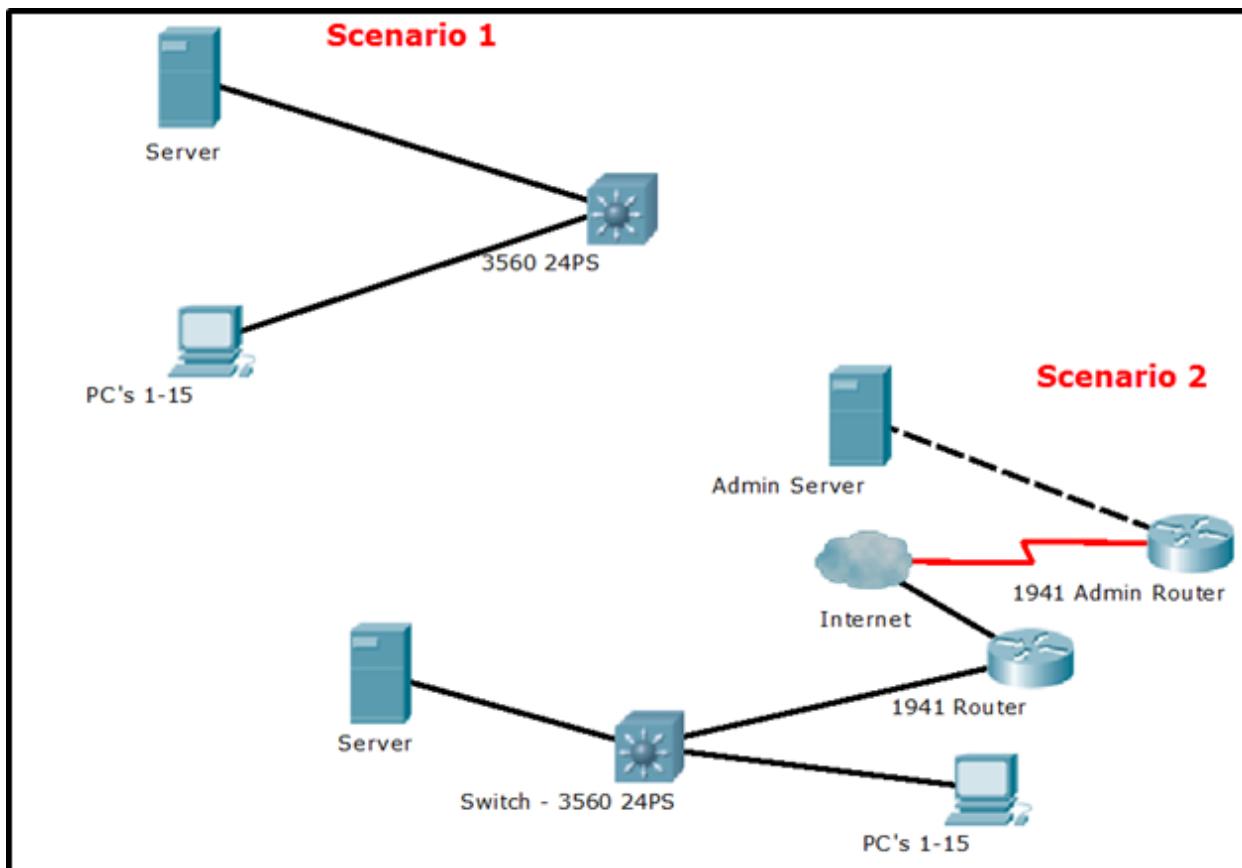
Answers will vary – if the switch will be also used for WAN streams and other intensive download traffic, a higher level switch would be used.

4. As you learned in the first course of the Academy, video and voice use a special TCP/IP model, transport layer protocol. What protocol is used in this layer and why is it important to voice and video streaming?

(UDP is the protocol used for voice and video – it allows for a continuous stream of data to flow without interruption to report delays back to the sender. There is no guaranteed delivery of data from source to destination hosts)

Packet Tracer Example (answers will vary)

Instructor Note: This is a representative model that might be “built” as a result of this activity:



Identify elements of the model that map to IT-related content:

- Voice, video and regular data can traverse networks using different devices, such as routers and switches.
- The type of switch that is used as an intermediary device provides different functional capacities.
- The type of network traffic will impact the switch's performance in sending and delivering data.
- Sufficient bandwidth is necessary to handle different types of traffic; therefore, network switch types/models and their capabilities are important to the switch model and type.
- Security impacts the switch selection. If the switch will be accessible physically, remotely or over the network locally, it will need to have security configured to include ACLs and/or port security.



Stand By Me (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objective

Describe the role of unicast, broadcast, and multicast in a switched network.

Students are given three scenarios where activity-based numbers will need to be recorded. At the end of the activity, students will answer questions about how this introductory process relates to sending and receiving messages on a switch.

501A	501B	501C	501D	501E
502A	502B	502C	502D	502E
503A	503B	503C	503D	503E
504A	504B	504C	504D	504E
505A	505B	505C	505D	505D

Scenario

When you arrived to class today, you were given a number by your instructor to use for this introductory class activity.

Once class begins, your instructor will ask certain students with specific numbers to stand. Your job is to record the standing students' numbers for each scenario.

Scenario 1

Students with numbers **starting** with the number **5** should stand. Record the numbers of the standing students.
All students will stand and all the numbers will be recorded by each student.

Scenario 2

Students with numbers **ending** in **B** should stand. Record the numbers of the standing students. **More than one student should stand, but not all students will stand. All numbers of standing students will be recorded by all students.**

Scenario 3

Students with the number **504C** should stand. Record the number of the standing student. **Only one student will stand and all students will record that number.**

At the end of this activity, divide into small groups and record answers to the Reflection questions on the PDF for this activity.

Reflection

1. Why do you think you were asked to record the students' numbers when and as requested?

Recording was necessary to see how groups are formed in networking. Recording helps you to identify to which group the students belong. Recording helps to keep a list of who has been seen in certain groups.

2. What is the significance of the number 5 in this activity? How many people were identified with this number?

Stand By Me

All students received a number beginning with 5, as this indicates a full group of students. This is similar to a network broadcast situation.

3. What is the significance of the letter C in this activity? How many people were identified with this number?
-

The letter C allows a smaller grouping of students to be identified – very similar to a multicast situation.

4. Why did only one person stand for 504C?
-

This number is unique to the class – therefore, it indicates a unicast form of network transmission.

5. How do you think this activity represents data travelling on local area networks?
-

When a switch first sees hosts on its network, it will record responses from those hosts in respect to unicasts, multicasts, and broadcasts (flooding). That is how it builds its MAC address table. Once the MAC addresses have been recorded by the switch, specific types of traffic can be switched (unicasts, broadcasts, and multicasts). The significance of the numbers illustrates unicast, multicast, and broadcast selection methods.

Save your work and be prepared to share it with another student or the entire class. (Instructor choice)

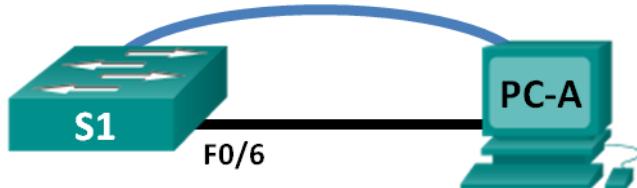
Instructor Note: Identify elements of the model that map to IT-related content:

- Switches record MAC addresses, just as the numbers were recorded during this introductory activity.
- LAN switch unicasts can be sent to and/or received by hosts.
- LAN switch multicasts can be sent to and/or received by hosts.
- LAN broadcasts can be sent to and/or received by hosts.

Lab – Configuring Basic Switch Settings (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Cable the Network and Verify the Default Switch Configuration

Part 2: Configure Basic Network Device Settings

- Configure basic switch settings.
- Configure the PC IP address.

Part 3: Verify and Test Network Connectivity

- Display device configuration.
- Test end-to-end connectivity with ping.
- Test remote management capabilities with Telnet.
- Save the switch running configuration file.

Part 4: Manage the MAC Address Table

- Record the MAC address of the host.
- Determine the MAC addresses that the switch has learned.
- List the **show mac address-table** command options.
- Set up a static MAC address.

Background / Scenario

Cisco switches can be configured with a special IP address known as the switch virtual interface (SVI). The SVI, or management address, can be used for remote access to the switch to display or configure settings. If the VLAN 1 SVI is assigned an IP address, by default all ports in VLAN 1 have access to the SVI IP address.

In this lab, you will build a simple topology using Ethernet LAN cabling and access a Cisco switch using the console and remote access methods. You will examine default switch configurations before configuring basic switch settings. These basic switch settings include device name, interface description, local passwords, message of the day (MOTD) banner, IP addressing, and static MAC address. You will also demonstrate the

Lab – Configuring Basic Switch Settings

use of a management IP address for remote switch management. The topology consists of one switch and one host using only Ethernet and console ports.

Note: The switch used is a Cisco Catalyst 2960 with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in this lab.

Note: Make sure that the switch has been erased and has no startup configuration. Refer to Appendix A for the procedures to initialize and reload a switch.

Required Resources

- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term, and Telnet capability)
- 1 Console cable to configure the Cisco IOS device via the console port
- 1 Ethernet cable as shown in the topology

Part 1: Cable the Network and Verify the Default Switch Configuration

In Part 1, you will set up the network topology and verify default switch settings.

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

- a. Connect the console cable as shown in the topology. Do not connect the PC-A Ethernet cable at this time.

Note: If you are using Netlab, shut down F0/6 on S1. This has the same effect as not connecting PC-A to S1.

- b. Connect to the switch from PC-A using Tera Term or other terminal emulation program.

Why must you use a console connection to initially configure the switch? Why is it not possible to connect to the switch via Telnet or SSH?

No IP addressing parameters are configured yet. A Cisco 2960 switch first placed into service has no networking configured.

Step 2: Verify the default switch configuration.

In this step, you will examine the default switch settings, such as current switch configuration, IOS information, interface properties, VLAN information, and flash memory.

You can access all the switch IOS commands in privileged EXEC mode. Access to privileged EXEC mode should be restricted by password protection to prevent unauthorized use because it provides direct access to global configuration mode and commands used to configure operating parameters. You will set passwords later in this lab.

The privileged EXEC mode command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes is gained. Use the **enable** command to enter privileged EXEC mode.

- a. Assuming the switch had no configuration file stored in nonvolatile random-access memory (NVRAM), A console connection using Tera Term or other terminal emulation program will place you at the user EXEC mode prompt on the switch with a prompt of Switch>. Use the **enable** command to enter privileged EXEC mode.

Switch> **enable**

Lab – Configuring Basic Switch Settings

Switch#

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

Verify that there is a clean default configuration file on the switch by issuing the **show running-config** privileged EXEC mode command. If a configuration file was previously saved, it must be removed. Depending on the switch model and IOS version, your configuration may look slightly different. However, there should be no configured passwords or IP address. If your switch does not have a default configuration, erase and reload the switch.

Note: Appendix A details the steps to initialize and reload a switch.

- b. Examine the current running configuration file.

Switch# **show running-config**

How many FastEthernet interfaces does a 2960 switch have? _____ **24**

How many Gigabit Ethernet interfaces does a 2960 switch have? _____ **2**

What is the range of values shown for the vty lines? _____ **0-4 and 5-15 or 0-15**

- c. Examine the startup configuration file in NVRAM.

Switch# **show startup-config**

startup-config is not present

Why does this message appear? _____

No configurations have been saved to NVRAM.

- d. Examine the characteristics of the SVI for VLAN 1.

Switch# **show interface vlan1**

Is there an IP address assigned to VLAN 1? _____ **No**

What is the MAC address of this SVI? Answers will vary. _____

0CD9:96E2:3D40 in this case.

Is this interface up?

Cisco switches have the **no shutdown** command configured by default on VLAN 1, but VLAN 1 won't reach the up/up state until a port is assigned to it and this port is also up. If there is no port in the up state in VLAN 1, then the VLAN 1 interface will be up, line protocol down. By default, all ports are assigned initially to VLAN 1.

- e. Examine the IP properties of the SVI VLAN 1.

Switch# **show ip interface vlan1**

What output do you see?

Vlan1 is up, line protocol is down
Internet protocol processing disabled

- f. Connect an Ethernet cable from PC-A to port 6 on the switch and examine the IP properties of the SVI VLAN 1. Allow time for the switch and PC to negotiate duplex and speed parameters.

Note: If you are using Netlab, enable interface F0/6 on S1.

Switch# **show ip interface vlan1**

Lab – Configuring Basic Switch Settings

What output do you see?

```
Vlan1 is up, line protocol is up  
  Internet protocol processing disabled
```

- g. Examine the Cisco IOS version information of the switch.

Switch# **show version**

What is the Cisco IOS version that the switch is running? _____

Answers may vary. 15.0(2)SE3

What is the system image filename? _____

Answers may vary. c2960-lanbasek9-mz.150-2.SE3.bin

What is the base MAC address of this switch? Answers will vary.

Answers will vary. 0C:D9:96:E2:3D:00.

- h. Examine the default properties of the FastEthernet interface used by PC-A.

Switch# **show interface f0/6**

Is the interface up or down? _____ It should be up unless there is a cabling problem.

What event would make an interface go up? _____

Connecting a host or other device

What is the MAC address of the interface? _____ 0CD9:96E2:3D06 (Varies)

What is the speed and duplex setting of the interface? _____ Full-duplex, 100Mb/s

- i. Examine the default VLAN settings of the switch.

Switch# **show vlan**

What is the default name of VLAN 1? _____ default

Which ports are in VLAN 1? _____

all ports; F0/1 – F0/24; G0/1, G0/2

Is VLAN 1 active? _____ Yes

What type of VLAN is the default VLAN? _____ enet (Ethernet)

- j. Examine flash memory.

Issue one of the following commands to examine the contents of the flash directory.

Switch# **show flash**

Switch# **dir flash:**

Files have a file extension, such as .bin, at the end of the filename. Directories do not have a file extension.

What is the filename of the Cisco IOS image? _____

c2960-lanbasek9-mz.150-2.SE.bin (may vary)

Part 2: Configure Basic Network Device Settings

In Part 2, you will configure basic settings for the switch and PC.

Step 1: Configure basic switch settings.

- Copy the following basic configuration and paste it into S1 while in global configuration mode.

```
no ip domain-lookup
hostname S1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
```

- Set the SVI IP address of the switch. This allows remote management of the switch.

Before you can manage S1 remotely from PC-A, you must assign the switch an IP address. The default configuration on the switch is to have the management of the switch controlled through VLAN 1. However, a best practice for basic switch configuration is to change the management VLAN to a VLAN other than VLAN 1.

For management purposes, use VLAN 99. The selection of VLAN 99 is arbitrary and in no way implies that you should always use VLAN 99.

First, create the new VLAN 99 on the switch. Then set the IP address of the switch to 192.168.1.2 with a subnet mask of 255.255.255.0 on the internal virtual interface VLAN 99.

```
S1# configure terminal
S1(config)# vlan 99
S1(config-vlan)# exit
S1(config)# interface vlan99
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to down
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)#

```

Notice that the VLAN 99 interface is in the down state even though you entered the **no shutdown** command. The interface is currently down because no switch ports are assigned to VLAN 99.

- Assign all user ports to VLAN 99.

```
S1(config)# interface range f0/1 - 24,g0/1 - 2
S1(config-if-range)# switchport access vlan 99
S1(config-if-range)# exit
S1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

```

To establish connectivity between the host and the switch, the ports used by the host must be in the same VLAN as the switch. Notice in the above output that the VLAN 1 interface goes down because none of the ports are assigned to VLAN 1. After a few seconds, VLAN 99 comes up because at least one active port (F0/6 with PC-A attached) is now assigned to VLAN 99.

- Issue the **show vlan brief** command to verify that all ports are in VLAN 99.

```
S1# show vlan brief
```

Lab – Configuring Basic Switch Settings

VLAN	Name	Status	Ports
1	default	active	
99	VLAN0099	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 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 Gi0/1, Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdninet-default	act/unsup	
1005	trnet-default	act/unsup	

- e. Configure the default gateway for S1. If no default gateway is set, the switch cannot be managed from a remote network that is more than one router away. Although this activity does not include an external IP gateway, assume that you will eventually connect the LAN to a router for external access. Assuming that the LAN interface on the router is 192.168.1.1, set the default gateway for the switch.

```
S1(config)# ip default-gateway 192.168.1.1
S1(config) #
```

- f. Console port access should also be restricted. The default configuration is to allow all console connections with no password needed. To prevent console messages from interrupting commands, use the **logging synchronous** option.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# logging synchronous
S1(config-line)# exit
S1(config) #
```

- g. Configure the virtual terminal (vty) lines for the switch to allow Telnet access. If you do not configure a vty password, you will not be able to Telnet to the switch.

```
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
*Mar 1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```

Why is the **login** command required? _____

Without the **login** command, the switch will not prompt for a password.

Step 2: Configure an IP address on PC-A.

Assign the IP address and subnet mask to the PC as shown in the Addressing Table. An abbreviated version of the procedure is described here. A default gateway is not required for this topology; however, you can enter **192.168.1.1** to simulate a router attached to S1.

- 1) Click the Windows **Start** icon > **Control Panel**.

- 2) Click **View By:** and choose **Small icons.**
- 3) Choose **Network and Sharing Center > Change adapter settings.**
- 4) Select **Local Area Network Connection**, right click and choose **Properties.**
- 5) Choose **Internet Protocol Version 4 (TCP/IPv4) > Properties.**
- 6) Click the **Use the following IP address** radio button and enter the IP address and subnet mask.

Part 3: Verify and Test Network Connectivity

In Part 3, you will verify and document the switch configuration, test end-to-end connectivity between PC-A and S1, and test the switch's remote management capability.

Step 1: Display the switch configuration.

Use the console connection on PC-A to display and verify the switch configuration. The **show run** command displays the entire running configuration, one page at a time. Use the spacebar to advance paging.

- a. A sample configuration is shown here. The settings you configured are highlighted in yellow. The other configuration settings are IOS defaults.

```
S1# show run
Building configuration...

Current configuration : 2206 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
<output omitted>
!
interface FastEthernet0/24
switchport access vlan 99
!
interface GigabitEthernet0/1
switchport access vlan 99
```

Lab – Configuring Basic Switch Settings

```
!
interface GigabitEthernet0/2
switchport access vlan 99
!
interface Vlan1
no ip address
no ip route-cache
!
interface Vlan99
ip address 192.168.1.2 255.255.255.0
no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
password 7 104D000A0618
logging synchronous
login
line vty 0 4
password 7 14141B180F0B
login
line vty 5 15
password 7 14141B180F0B
login
!
end
```

S1#

- b. Verify the management VLAN 99 settings.

```
S1# show interface vlan 99
Vlan99 is up, line protocol is up
Hardware is EtherSVI, address is 0cd9.96e2.3d41 (bia 0cd9.96e2.3d41)
Internet address is 192.168.1.2/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:06, output 00:08:45, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
```

Lab – Configuring Basic Switch Settings

```
5 minute output rate 0 bits/sec, 0 packets/sec
    175 packets input, 22989 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    1 packets output, 64 bytes, 0 underruns
    0 output errors, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

What is the bandwidth on this interface? _____ **1000000 Kb/s (1 Gb/sec)**

What is the VLAN 99 state? _____ **up**

What is the line protocol state? _____ **up**

Step 2: Test end-to-end connectivity with ping.

- From the command prompt on PC-A, ping the address of PC-A first.

```
C:\Users\User1> ping 192.168.1.10
```

- From the command prompt on PC-A, ping the SVI management address of S1.

```
C:\Users\User1> ping 192.168.1.2
```

Because PC-A needs to resolve the MAC address of S1 through ARP, the first packet may time out. If ping results continue to be unsuccessful, troubleshoot the basic device configurations. Check both the physical cabling and logical addressing.

Step 3: Test and verify remote management of S1.

You will now use Telnet to remotely access the switch. In this lab, PC-A and S1 reside side by side. In a production network, the switch could be in a wiring closet on the top floor while your management PC is located on the ground floor. In this step, you will use Telnet to remotely access switch S1 using its SVI management address. Telnet is not a secure protocol; however, you will use it to test remote access. With Telnet, all information, including passwords and commands, are sent across the session in plain text. In subsequent labs, you will use SSH to remotely access network devices.

Instructor Note: Tera Term or other terminal emulation programs with Telnet capability may be used if Telnet from the Windows command prompt is not allowed at your institution.

Note: If you are using Windows 7, the administrator may need to enable the Telnet protocol. To install the Telnet client, open a command window and type **pkgmgr /iu:"TelnetClient"**. An example is shown below.

```
C:\Users\User1> pkgmgr /iu:"TelnetClient"
```

- With the command window still open on PC-A, issue a Telnet command to connect to S1 via the SVI management address. The password is **cisco**.

```
C:\Users\User1> telnet 192.168.1.2
```

- After entering the password **cisco**, you will be at the user EXEC mode prompt. Access privileged EXEC mode using the **enable** command and providing the secret password **class**.

- Type **exit** to end the Telnet session.

Step 4: Save the switch running configuration file.

Save the configuration.

```
S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
```

```
Building configuration...
[OK]
S1#
```

Part 4: Manage the MAC Address Table

In Part 4, you will determine the MAC addresses that the switch has learned, set up a static MAC address on one interface of the switch, and then remove the static MAC address from that interface.

Step 1: Record the MAC address of the host.

Open a command prompt on PC-A and issue the **ipconfig /all** command to determine and record the Layer 2 (physical) addresses of the NIC.

PC-A: 00-50-56-BE-6C-89 (answers will vary)

Step 2: Determine the MAC addresses that the switch has learned.

Display the MAC addresses using the **show mac address-table** command.

```
S1# show mac address-table
```

How many dynamic addresses are there? _____ 1 (can vary)

How many MAC addresses are there in total? _____ 24 (can vary)

Does the dynamic MAC address match the MAC address of PC-A? _____ Yes

Step 3: List the **show mac address-table** options.

- Display the MAC address table options.

```
S1# show mac address-table ?
```

How many options are available for the **show mac address-table** command? _____ 12 (can vary)

- Issue the **show mac address-table dynamic** command to display only the MAC addresses that were learned dynamically.

```
S1# show mac address-table dynamic
```

How many dynamic addresses are there? _____ 1 (can vary)

- View the MAC address entry for PC-A. The MAC address formatting for the command is xxxx.xxxx.xxxx.

```
S1# show mac address-table address <PC-A MAC here>
```

Step 4: Set up a static MAC address.

- Clear the MAC address table.

To remove the existing MAC addresses, use the **clear mac address-table dynamic** command in privileged EXEC mode.

```
S1# clear mac address-table dynamic
```

- Verify that the MAC address table was cleared.

```
S1# show mac address-table
```

How many static MAC addresses are there? _____

Lab – Configuring Basic Switch Settings

at least 20 (other static entries could have been manually created)

Instructor Note: The first 20 static addresses in the MAC address table are built-in.

How many dynamic addresses are there? _____

0 (may be 1, depending on how quickly addresses are re-acquired by the switch)

- c. Examine the MAC table again.

More than likely, an application running on your PC has already sent a frame out the NIC to S1. Look at the MAC address table again in privileged EXEC mode to see if S1 has relearned the MAC address of PC-A.

S1# **show mac address-table**

How many dynamic addresses are there? _____ 1

Why did this change from the last display? _____

The switch dynamically reacquired the PC MAC address.

If S1 has not yet relearned the MAC address for PC-A, ping the VLAN 99 IP address of the switch from PC-A, and then repeat the **show mac address-table** command.

- d. Set up a static MAC address.

To specify which ports a host can connect to, one option is to create a static mapping of the host MAC address to a port.

Set up a static MAC address on F0/6 using the address that was recorded for PC-A in Part 4, Step 1. The MAC address 0050.56BE.6C89 is used as an example only. You must use the MAC address of PC-A, which is different than the one given here as an example.

```
S1(config)# mac address-table static 0050.56BE.6C89 vlan 99 interface  
fastethernet 0/6
```

- e. Verify the MAC address table entries.

S1# **show mac address-table**

How many total MAC addresses are there? _____ 22 (varies)

How many static addresses are there? _____

There are 22 static addresses. Total MAC addresses and static addresses should be the same because there are no other devices currently connected to S1.

- f. Remove the static MAC entry. Enter global configuration mode and remove the command by putting a **no** in front of the command string.

Note: The MAC address 0050.56BE.6C89 is used in the example only. Use the MAC address for PC-A.

```
S1(config)# no mac address-table static 0050.56BE.6C89 vlan 99 interface  
fastethernet 0/6
```

- g. Verify that the static MAC address has been cleared.

S1# **show mac address-table**

How many total static MAC addresses are there? _____ 21 (varies)

Reflection

1. Why should you configure the vty password for the switch?

If you do not configure a vty password you will not be able to telnet to the switch.

Lab – Configuring Basic Switch Settings

2. Why change the default VLAN 1 to a different VLAN number?
-

For improved security.

3. How can you prevent passwords from being sent in plain text?
-

Issue the **service password-encryption** command.

4. Why configure a static MAC address on a port interface?
-

To specify which ports a host can connect to.

Appendix A: Initializing and Reloading a Switch

- a. Console into the switch and enter privileged EXEC mode.

```
Switch> enable  
Switch#
```

- b. Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash  
Directory of flash:/
```

```
2 -rwx 1919 Mar 1 1993 00:06:33 +00:00 private-config.text  
3 -rwx 1632 Mar 1 1993 00:06:33 +00:00 config.text  
4 -rwx 13336 Mar 1 1993 00:06:33 +00:00 multiple-fs  
5 -rwx 11607161 Mar 1 1993 02:37:06 +00:00 c2960-lanbasek9-mz.150-2.SE.bin  
6 -rwx 616 Mar 1 1993 00:07:13 +00:00 vlan.dat
```

```
32514048 bytes total (20886528 bytes free)  
Switch#
```

- c. If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat  
Delete filename [vlan.dat]?
```

- d. You are prompted to verify the filename. If you have entered the name correctly, press Enter; otherwise, you can change the filename.

- e. You are prompted to confirm deletion of this file. Press Enter to confirm.

```
Delete flash:/vlan.dat? [confirm]  
Switch#
```

- f. Use the **erase startup-config** command to erase the startup configuration file from NVRAM. You are prompted to remove the configuration file. Press Enter to confirm.

```
Switch# erase startup-config  
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]  
[OK]  
Erase of nvram: complete  
Switch#
```

- g. Reload the switch to remove any old configuration information from memory. You will then receive a prompt to confirm reloading of the switch. Press Enter to proceed.

Lab – Configuring Basic Switch Settings

```
Switch# reload
```

```
Proceed with reload? [confirm]
```

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Respond by typing **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

- h. After the switch reloads, you should see a prompt to enter the initial configuration dialog. Respond by entering **no** at the prompt and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

```
Switch>
```

Device Configs

Switch S1

```
S1#sh run
Building configuration...
Current configuration : 2359 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!interface FastEthernet0/1
 switchport access vlan 99
!
interface FastEthernet0/2
 switchport access vlan 99
!
interface FastEthernet0/3
```

Lab – Configuring Basic Switch Settings

```
switchport access vlan 99
!
interface FastEthernet0/4
switchport access vlan 99
!
interface FastEthernet0/5
switchport access vlan 99
!
interface FastEthernet0/6
switchport access vlan 99
!
interface FastEthernet0/7
switchport access vlan 99
!
interface FastEthernet0/8
switchport access vlan 99
!
interface FastEthernet0/9
switchport access vlan 99
!
interface FastEthernet0/10
switchport access vlan 99
!
interface FastEthernet0/11
switchport access vlan 99
!
interface FastEthernet0/12
switchport access vlan 99
!
interface FastEthernet0/13
switchport access vlan 99
!
interface FastEthernet0/14
switchport access vlan 99
!
interface FastEthernet0/15
switchport access vlan 99
!
interface FastEthernet0/16
switchport access vlan 99
!
interface FastEthernet0/17
switchport access vlan 99
!
interface FastEthernet0/18
switchport access vlan 99
!
interface FastEthernet0/19
switchport access vlan 99
```

Lab – Configuring Basic Switch Settings

```
!
interface FastEthernet0/20
 switchport access vlan 99
!
interface FastEthernet0/21
 switchport access vlan 99
!
interface FastEthernet0/22
 switchport access vlan 99
!
interface FastEthernet0/23
 switchport access vlan 99
!
interface FastEthernet0/24
 switchport access vlan 99
!
interface GigabitEthernet0/1
 switchport access vlan 99
!
interface GigabitEthernet0/2
 switchport access vlan 99
!
interface Vlan1
 no ip address
!
interface Vlan99
 ip address 192.168.1.2 255.255.255.0
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
 password 7 0822455D0A16
logging synchronous
login
line vty 0 4
 password 7 01100F175804
login
line vty 5 15
 password 7 01100F175804
login
!
end
```

Lab – Configuring Basic Switch Settings

```
login
line vty 0 4
password 7 01100F175804
login
line vty 5 15
password 7 01100F175804
login
!
end
```

Lab – Configuring Switch Security Features (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

Objectives

Part 1: Set up the Topology and Initialize Devices

Part 2: Configure Basic Device Settings and Verify Connectivity

Part 3: Configure and Verify SSH Access on S1

- Configure SSH access.
- Modify SSH parameters.
- Verify the SSH configuration.

Part 4: Configure and Verify Security Features on S1

- Configure and verify general security features.
- Configure and verify port security.

Background / Scenario

It is quite common to lock down access and install strong security features on PCs and servers. It is important that your network infrastructure devices, such as switches and routers, are also configured with security features.

In this lab, you will follow some best practices for configuring security features on LAN switches. You will only allow SSH and secure HTTPS sessions. You will also configure and verify port security to lock out any device with a MAC address not recognized by the switch.

Note: The router used with CCNA hands-on labs is a Cisco 1941 Integrated Services Router (ISR) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switch used is a Cisco Catalyst 2960 with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is

shown in this lab. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the router and switch have been erased and have no startup configurations. If you are unsure, contact your instructor or refer to the previous lab for the procedures to initialize and reload devices.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- 1 Console cable to configure the Cisco IOS devices via the console ports
- 2 Ethernet cables as shown in the topology

Part 1: Set Up the Topology and Initialize Devices

In Part 1, you will set up the network topology and clear any configurations if necessary.

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

Step 2: Initialize and reload the router and switch.

If configuration files were previously saved on the router or switch, initialize and reload these devices back to their default configurations.

Part 2: Configure Basic Device Settings and Verify Connectivity

In Part 2, you will configure basic settings on the router, switch, and PC. Refer to the Topology and Addressing Table at the beginning of this lab for device names and address information.

Step 1: Configure an IP address on PC-A.

Refer to the Addressing Table for the IP Address information.

Step 2: Configure basic settings on R1.

- a. Console into R1 and enter global configuration mode.
- b. Copy the following basic configuration and paste it to running-configuration on R1.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 4
```

```
password cisco
login
interface g0/1
  ip address 172.16.99.1 255.255.255.0
  no shutdown
end
```

- c. Save the running configuration to startup configuration.

Step 3: Configure basic settings on S1.

- Console into S1 and enter global configuration mode.
- Copy the following basic configuration and paste it to running-configuration on S1.

```
no ip domain-lookup
hostname S1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

- c. Create VLAN 99 on the switch and name it **Management**.

```
S1(config)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

- d. Configure the VLAN 99 management interface IP address, as shown in the Addressing Table, and enable the interface.

```
S1(config)# interface vlan 99
S1(config-if)# ip address 172.16.99.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1#
```

- e. Issue the **show vlan** command on S1. What is the status of VLAN 99? _____ Active

- f. Issue the **show ip interface brief** command on S1. What is the status and protocol for management interface VLAN 99?

Status is up, and protocol is down.

Why is the protocol down, even though you issued the **no shutdown** command for interface VLAN 99?

No physical ports on the switch have been assigned to VLAN 99.

- g. Assign ports F0/5 and F0/6 to VLAN 99 on the switch.

```
S1# config t  
S1(config)# interface f0/5  
S1(config-if)# switchport mode access  
S1(config-if)# switchport access vlan 99  
S1(config-if)# interface f0/6  
S1(config-if)# switchport mode access  
S1(config-if)# switchport access vlan 99  
S1(config-if)# end
```

- h. Save the running configuration to startup configuration.

- i. Issue the **show ip interface brief** command on S1. What is the status and protocol showing for interface VLAN 99? _____ Up and up

Note: There may be a delay while the port states converge.

Step 4: Verify connectivity between devices.

- From PC-A, ping the default gateway address on R1. Were your pings successful? _____ Yes
- From PC-A, ping the management address of S1. Were your pings successful? _____ Yes
- From S1, ping the default gateway address on R1. Were your pings successful? _____ Yes
- From PC-A, open a web browser and go to http://172.16.99.11. If you are prompted for a username and password, leave the username blank and use **class** for the password. If you are prompted for a secured connection, answer **No**. Were you able to access the web interface on S1? _____ Yes
- Close the browser.

Note: The non-secure web interface (HTTP server) on a Cisco 2960 switch is enabled by default. A common security measure is to disable this service, as described in Part 4.

Part 3: Configure and Verify SSH Access on S1

Step 1: Configure SSH access on S1.

- Enable SSH on S1. From global configuration mode, create a domain name of **CCNA-Lab.com**.

```
S1(config)# ip domain-name CCNA-Lab.com
```

- Create a local user database entry for use when connecting to the switch via SSH. The user should have administrative level access.

Note: The password used here is NOT a strong password. It is merely being used for lab purposes.

```
S1(config)# username admin privilege 15 secret sshadmin
```

- Configure the transport input for the vty lines to allow SSH connections only, and use the local database for authentication.

```
S1(config)# line vty 0 15  
S1(config-line)# transport input ssh  
S1(config-line)# login local  
S1(config-line)# exit
```

Lab – Configuring Switch Security Features

- d. Generate an RSA crypto key using a modulus of 1024 bits.

```
S1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: S1.CCNA-Lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)
```

```
S1(config)#
S1(config)# end
```

- e. Verify the SSH configuration.

```
S1# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAAQgQCKWqCN0g4XLVdJJUOr+9qoJkFqC/g0OuAV1semrR5/
xy0bbUBPywvqhwSPJtucIKxKw/YfrRCeFwY+dc+/jGSeckAHahuv0jJfOdFcqgiKGeeluAu+iQ2drE+k
butn1LTGmtNhdEJMxri/ZeO3BsFcnHp01hbB6Vsm4XRXGk7OfQ==
```

What version of SSH is the switch using? 1.99

How many authentication attempts does SSH allow? 3

What is the default timeout setting for SSH? 120 seconds

Step 2: Modify the SSH configuration on S1.

Modify the default SSH configuration.

```
S1# config t
S1(config)# ip ssh time-out 75
S1(config)# ip ssh authentication-retries 2
S1# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 75 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAAQgQCKWqCN0g4XLVdJJUOr+9qoJkFqC/g0OuAV1semrR5/
xy0bbUBPywvqhwSPJtucIKxKw/YfrRCeFwY+dc+/jGSeckAHahuv0jJfOdFcqgiKGeeluAu+iQ2drE+k
butn1LTGmtNhdEJMxri/ZeO3BsFcnHp01hbB6Vsm4XRXGk7OfQ==
```

How many authentication attempts does SSH allow? 2

What is the timeout setting for SSH? 75 seconds

Step 3: Verify the SSH configuration on S1.

- a. Using the SSH client software on PC-A (such as Tera Term), open an SSH connection to S1. If you receive a message on your SSH client regarding the host key, accept it. Log in with **admin** for username and **sshadmin** for the password.

Was the connection successful? Yes

Lab – Configuring Switch Security Features

What prompt was displayed on S1? Why?

S1 is showing the prompt at privileged EXEC mode because the privilege 15 option was used when configuring username and password

- b. Type **exit** to end the SSH session on S1.

Part 4: Configure and Verify Security Features on S1

In Part 4, you will shut down unused ports, turn off certain services running on the switch, and configure port security based on MAC addresses. Switches can be subject to MAC address table overflow attacks, MAC spoofing attacks, and unauthorized connections to switch ports. You will configure port security to limit the number of MAC addresses that can be learned on a switch port and disable the port if that number is exceeded.

Step 1: Configure general security features on S1.

- a. Change the message of the day (MOTD) banner on S1 to, “Unauthorized access is strictly prohibited. Violators will be prosecuted to the full extent of the law.”
- b. Issue a **show ip interface brief** command on S1. What physical ports are up?

Ports F0/5 and F0/6

- c. Shut down all unused physical ports on the switch. Use the **interface range** command.

```
S1(config)# interface range f0/1 - 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 - 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 - 2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

- d. Issue the **show ip interface brief** command on S1. What is the status of ports F0/1 to F0/4?

Administratively down.

- e. Issue the **show ip http server status** command.

```
S1# show ip http server status
HTTP server status: Enabled
HTTP server port: 80
HTTP server authentication method: enable
HTTP server access class: 0
HTTP server base path: flash:html
HTTP server help root:
Maximum number of concurrent server connections allowed: 16
Server idle time-out: 180 seconds
```

Lab – Configuring Switch Security Features

```
Server life time-out: 180 seconds
Maximum number of requests allowed on a connection: 25
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-edc-cbc-sha des-cbc-sha rc4-128-md5 rc4-128-sha
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint:
HTTP secure server active session modules: ALL
```

What is the HTTP server status? _____ **Enabled**

What server port is it using? _____ **80**

What is the HTTP secure server status? _____ **Enabled**

What secure server port is it using? _____ **443**

- f. HTTP sessions send everything in plain text. You will disable the HTTP service running on S1.

```
S1(config)# no ip http server
```

- g. From PC-A, open a web browser and go to http://172.16.99.11. What was your result?

The web page could not open. HTTP connections are now refused by S1.

- h. From PC-A, open a web browser and go to https://172.16.99.11. Accept the certificate. Log in with no username and a password of **class**. What was your result?

Secure web session was successful.

- i. Close the web browser.

Step 2: Configure and verify port security on S1.

- a. Record the R1 G0/1 MAC address. From the R1 CLI, use the **show interface g0/1** command and record the MAC address of the interface.

```
R1# show interface g0/1
```

```
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia
  3047.0da3.1821)
```

What is the MAC address of the R1 G0/1 interface?

In the example above, it is **30f7.0da3.1821**

- b. From the S1 CLI, issue a **show mac address-table** command from privileged EXEC mode. Find the dynamic entries for ports F0/5 and F0/6. Record them below.

F0/5 MAC address: _____ **30f7.0da3.1821**

F0/6 MAC address: _____ **00e0.b857.1cc0**

- c. Configure basic port security.

Note: This procedure would normally be performed on all access ports on the switch. F0/5 is shown here as an example.

Lab – Configuring Switch Security Features

- 1) From the S1 CLI, enter interface configuration mode for the port that connects to R1.

```
S1(config)# interface f0/5
```

- 2) Shut down the port.

```
S1(config-if)# shutdown
```

- 3) Enable port security on F0/5.

```
S1(config-if)# switchport port-security
```

Note: Entering the **switchport port-security** command sets the maximum MAC addresses to 1 and the violation action to shutdown. The **switchport port-security maximum** and **switchport port-security violation** commands can be used to change the default behavior.

- 4) Configure a static entry for the MAC address of R1 G0/1 interface recorded in Step 2a.

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx  
(xxxx.xxxx.xxxx is the actual MAC address of the router G0/1 interface)
```

Note: Optionally, you can use the **switchport port-security mac-address sticky** command to add all the secure MAC addresses that are dynamically learned on a port (up to the maximum set) to the switch running configuration.

- 5) Enable the switch port.

```
S1(config-if)# no shutdown  
S1(config-if)# end
```

- d. Verify port security on S1 F0/5 by issuing a **show port-security interface** command.

```
S1# show port-security interface f0/5  
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     : 1  
Configured MAC Addresses : 1  
Sticky MAC Addresses    : 0  
Last Source Address:Vlan : 0000.0000.0000:0  
Security Violation Count : 0
```

What is the port status of F0/5?

The status is Secure-up, which indicates that the port is secure, but the status and protocol are up.

- e. From R1 command prompt, ping PC-A to verify connectivity.

```
R1# ping 172.16.99.3
```

- f. You will now violate security by changing the MAC address on the router interface. Enter interface configuration mode for G0/1 and shut it down.

```
R1# config t  
R1(config)# interface g0/1  
R1(config-if)# shutdown
```

Lab – Configuring Switch Security Features

- g. Configure a new MAC address for the interface, using **aaaa.bbbb.cccc** as the address.

```
R1(config-if)# mac-address aaaa.bbbb.cccc
```

- h. If possible, have a console connection open on S1 at the same time that you do the next two steps. You will eventually see messages displayed on the console connection to S1 indicating a security violation. Enable the G0/1 interface on R1.

```
R1(config-if)# no shutdown
```

- i. From R1 privileged EXEC mode, ping PC-A. Was the ping successful? Why or why not?

No, the F0/5 port on S1 is shut down because of the security violation.

- j. On the switch, verify port security with the following commands.

```
S1# show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Action
Fa0/5	1	1	1	Shutdown

Total Addresses in System (excluding one mac per port) :0
Max Addresses limit in System (excluding one mac per port) :8192

```
S1# show port-security interface f0/5
```

Port Security	: Enabled
Port Status	: Secure-shutdown
Violation Mode	: Shutdown
Aging Time	: 0 mins
Aging Type	: Absolute
SecureStatic Address Aging	: Disabled
Maximum MAC Addresses	: 1
Total MAC Addresses	: 1
Configured MAC Addresses	: 1
Sticky MAC Addresses	: 0
Last Source Address:Vlan	: aaaa.bbbb.cccc:99
Security Violation Count	: 1

```
S1# show interface f0/5
```

FastEthernet0/5 is down, line protocol is down (err-disabled)

```
Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
```

```
S1# show port-security address
```

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
----	-----	----	-----	-----

Lab – Configuring Switch Security Features

```
99      30f7.0da3.1821      SecureConfigured      Fa0/5      -  
-----  
Total Addresses in System (excluding one mac per port) :0  
Max Addresses limit in System (excluding one mac per port) :8192
```

- k. On the router, shut down the G0/1 interface, remove the hard-coded MAC address from the router, and re-enable the G0/1 interface.

```
R1(config-if)# shutdown  
R1(config-if)# no mac-address aaaa.bbbb.cccc  
R1(config-if)# no shutdown  
R1(config-if)# end
```

- l. From R1, ping PC-A again at 172.16.99.3. Was the ping successful? _____ No
- m. On the switch, issue the **show interface f0/5** command to determine the cause of ping failure. Record your findings.

F0/5 port on S1 is still in an error disabled state.

```
S1# show interface f0/5  
FastEthernet0/5 is down, line protocol is down (err-disabled)  
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)  
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,  
    reliability 255/255, txload 1/255, rxload 1/255
```

- n. Clear the S1 F0/5 error disabled status.

```
S1# config t  
S1(config)# interface f0/5  
S1(config-if)# shutdown  
S1(config-if)# no shutdown
```

Note: There may be a delay while the port states converge.

- o. Issue the **show interface f0/5** command on S1 to verify F0/5 is no longer in error disabled mode.

```
S1# show interface f0/5  
FastEthernet0/5 is up, line protocol is up (connected)  
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)  
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,  
    reliability 255/255, txload 1/255, rxload 1/255
```

- p. From the R1 command prompt, ping PC-A again. The ping should be successful.

Reflection

1. Why would you enable port security on a switch?

It would help prevent unauthorized devices from accessing your network if they plugged into a switch on your network.

2. Why should unused ports on a switch be disabled?

One excellent reason is that a user could not connect a device to the switch on an unused port and access the LAN.

Router Interface Summary Table

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

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

Device Configs**Router R1**

```
R1#sh run
Building configuration...
Current configuration : 1232 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no ip domain-lookup
!
interface GigabitEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
```

Lab – Configuring Switch Security Features

```
ip address 172.16.99.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
clock rate 2000000
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!line con 0
password 7 030752180500
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line 67
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
password 7 13061E01080344
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
S1#sh run
Building configuration...
```

Lab – Configuring Switch Security Features

```
Current configuration : 3762 bytes
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUG.2
!
username admin privilege 15 secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrbp4RFmfqY
!
no ip domain-lookup
ip domain-name CCNA-Lab.com
!
crypto pki trustpoint TP-self-signed-2530358400
    enrollment selfsigned
    subject-name cn=IOS-Self-Signed-Certificate-2530358400
    revocation-check none
    rsakeypair TP-self-signed-2530358400
!
crypto pki certificate chain TP-self-signed-2530358400
    certificate self-signed 01
        3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
        31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
        69666963 6174652D 32353330 33353834 3030301E 170D3933 30333031 30303030
        35395A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
        4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 35333033
        35383430 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
        8100C0E3 1B8AF1E4 ADA4C4AD F82914AF BF8BCEC9 30CFBF54 D76B3940 38353E50
        A9AE0FCE 9CA05B91 24312B31 22D5F89D D249023E AEEC442D F55315F6 D456DA95
        16B758FB 8083B681 C1B3A3BF 99420EC7 A7E0AD11 CF031CD1 36A997C0 E72BE4DD
        1D745542 1DC958C1 443B6727 F7047747 D94B8CAD 0A99CBDC ADC914C8 D820DC30
        E6B70203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
        551D2304 18301680 1464D1A8 83DEE145 E35D68C1 D078ED7D 4F6F0B82 9D301D06
        03551D0E 04160414 64D1A883 DEE145E3 5D68C1D0 78ED7D4F 6F0B829D 300D0609
        2A864886 F70D0101 05050003 81810098 D65CFA1C 3942148D 8961D845 51D53202
        EA59B526 7DB308C9 F79859A0 D93D56D6 C584AB83 941A2B7F C44C0E2F DFAF6B8D
        A3272A5C 2363116E 1AA246DD 7E54B680 2ABB1F2D 26921529 E1EF4ACC A4FBD14A
        BAD41C98 E8D83DEC B85A330E D453510D 89F64023 7B9782E7 200F615A 6961827F
        8419A84F 56D71664 5123B591 A62C55
    quit
!
ip ssh time-out 75
ip ssh authentication-retries 2
!
interface FastEthernet0/1
    shutdown
```

Lab – Configuring Switch Security Features

```
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
switchport access vlan 99
switchport mode access
switchport port-security
switchport port-security mac-address 30f7.0da3.1821
!
interface FastEthernet0/6
switchport access vlan 99
switchport mode access
!
interface FastEthernet0/7
shutdown

interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
```

Lab – Configuring Switch Security Features

```
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
ip address 172.16.99.11 255.255.255.0
!
ip default-gateway 172.16.99.1
no ip http server
ip http secure-server
!
banner motd ^CWarning! Unauthorized Access is Prohibited.^C
!
line con 0
password cisco
logging synchronous
login
line vty 0 4
```

Lab – Configuring Switch Security Features

```
login local
transport input ssh
line vty 5 15
login local
transport input ssh
!
end
```



Switch Trio (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objective

Verify the Layer 2 configuration of a switch port connected to an end station.

Students will use Packet Tracer to configure the first three ports of a switch a permanent MAC address (one MAC address per port) and security shutdown feature. They will validate security implementation and explain the process to another student or the class (Instructor choice).

Scenario

You are the network administrator for a small- to medium-sized business. Corporate headquarters for your business has mandated that on all switches in all offices, security must be implemented. The memorandum delivered to you this morning states:

"By Monday, April 18, 20xx, the first three ports of all configurable switches located in all offices must be secured with MAC addresses — one address will be reserved for the PC, one address will be reserved for the laptop in the office, and one address will be reserved for the office server.

If a port's security is breached, we ask you to shut it down until the reason for the breach can be certified.

Please implement this policy no later than the date stated in this memorandum. For questions, call 1.800.555.1212. Thank you. The Network Management Team"

Work with a partner in the class and create a Packet Tracer example to test this new security policy. Once you have created your file, test it with, at least, one device to ensure it is operational or validated.

Save your work and be prepared to share it with the entire class. (Instructor choice)

Reflection

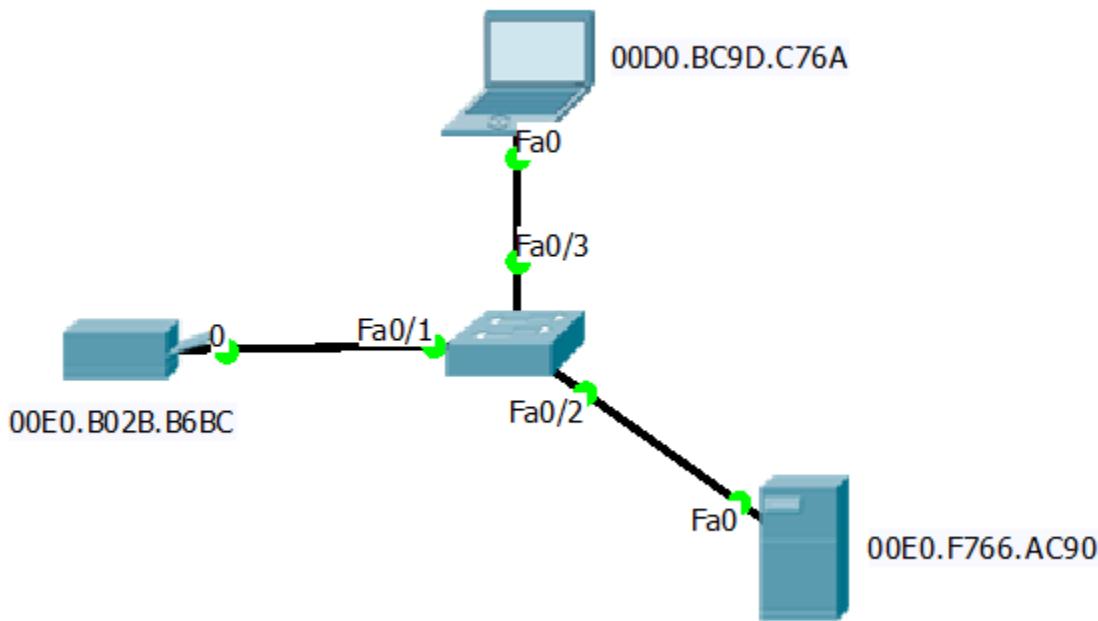
1. Why would one port on a switch be secured on a switch using these scenario parameters (and not all the ports on the same switch)?

Answers will vary – students may mention that securing every port on a switch would make it difficult for many users to connect to the switch, therefore limiting port use to certain pieces of equipment – laptop mobility might be compromised, as users would not be able to connect to the switch unless they knew which port they were allowed to use.

2. Why would a network administrator use a network simulator to create, configure, and validate a security plan, instead of using the small- to medium-sized business' actual, physical equipment?

Using a network simulator can save time and quality of network data delivery by pre-testing and validating new configurations.

Original Physical Topology (for concept representation only)



After configuring port security for the Printer, Server and Laptop – all devices are reporting to the switch on their correct ports.

```
Switch# show port-security address
          Secure Mac Address Table
-----
Vlan   Mac Address     Type      Ports      Remaining Age
           (mins)
-----
1      00E0.B02B.B6BC  SecureSticky  FastEthernet0/1  -
1      00E0.F766.AC90  SecureSticky  FastEthernet0/2  -
1      00D0.BC9D.C76A  SecureSticky  FastEthernet0/3  -
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

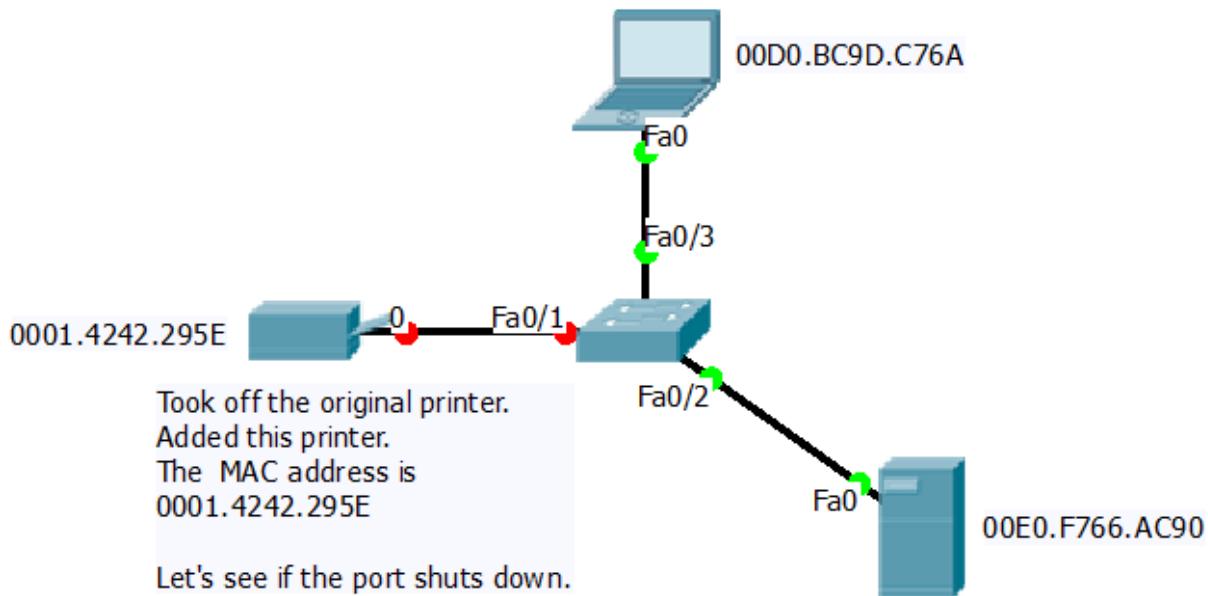
Switch Trio

Output showing port security status for Fa0/1:

```
Switch# show port-security int fa0/1
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     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 00E0.B02B.B6BC:1
Security Violation Count : 0
```

Topology Change with Security Violation (for concept representation only)

After exchanging the original Printer with a new one, Fa0/1 shuts down on the switch.



Instructor Note: Identify elements of the model that map to IT-related content:

- Switches can be secured by assigning MAC addresses to any and all ports – manually or configuration-based
- LAN switch ports can be shut down if security on the port is breached.
- Network administrators can implement best practice policies devised by management to ensure that networks are not compromised through security attacks.

Vacation Station (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objective

Explain the purpose of VLANs in a switched network.

To prepare for learning VLAN concepts in a switched network for this chapter, students will envision how and why network VLAN-switching groups are created.

Scenario

You have purchased a vacation home at the beach for rental purposes. There are three, identical floors on each level of the home. Each floor offers one digital television for renters to use.

According to the local Internet service provider, only three stations may be offered within a television package. It is your job to decide which television packages you offer your guests.

- Divide the class into groups of three students per group.
- Choose three different stations to make one subscription package for each floor of your rental home.
- Complete the PDF for this activity.

Share your completed group-reflection answers with the class.

Television Station Subscription Package – Floor 1		
Local News <input type="checkbox"/>	Sports <input type="checkbox"/>	Weather <input type="checkbox"/>
Home Improvement <input type="checkbox"/>	Movies <input type="checkbox"/>	History <input type="checkbox"/>
Television Station Subscription Package – Floor 2		
Local News <input type="checkbox"/>	Sports <input type="checkbox"/>	Weather <input type="checkbox"/>
Home Improvement <input type="checkbox"/>	Movies <input type="checkbox"/>	History <input type="checkbox"/>
Television Station Subscription Package – Floor 3		
Local News <input type="checkbox"/>	Sports <input type="checkbox"/>	Weather <input type="checkbox"/>
Home Improvement <input type="checkbox"/>	Movies <input type="checkbox"/>	History <input type="checkbox"/>

Reflection

1. What were some of the criteria you used to select the final three stations?

Vacation Station

Answers will vary, but some answers might include: local news is usually important to everyone, weather is important to beach vacationers, home improvement might be important to rental property use, watching sports and movies are popular vacation pastimes, and history provides vacationers with information about places they are currently visiting or plan to visit.

2. Why do you think this Internet service provider offers different television station options to subscribers? Why not offer all stations to all subscribers?
-

Limiting options to certain groups allows for ISPs to conserve televised bandwidth to groups with the options selected. It also allows them to charge additional prices for additional options.

3. Compare this scenario to data communications and networks for small- to medium-sized businesses. Why would it be a good idea to divide your small- to medium-sized business networks into logical and physical groups?
-

Answers will vary. Some answers might include: dividing networks into groups allows businesses to: improve network performance; regulate network management and security; use data, voice, network-controlled traffic options more effectively; and group data traffic based upon network-desired functions.

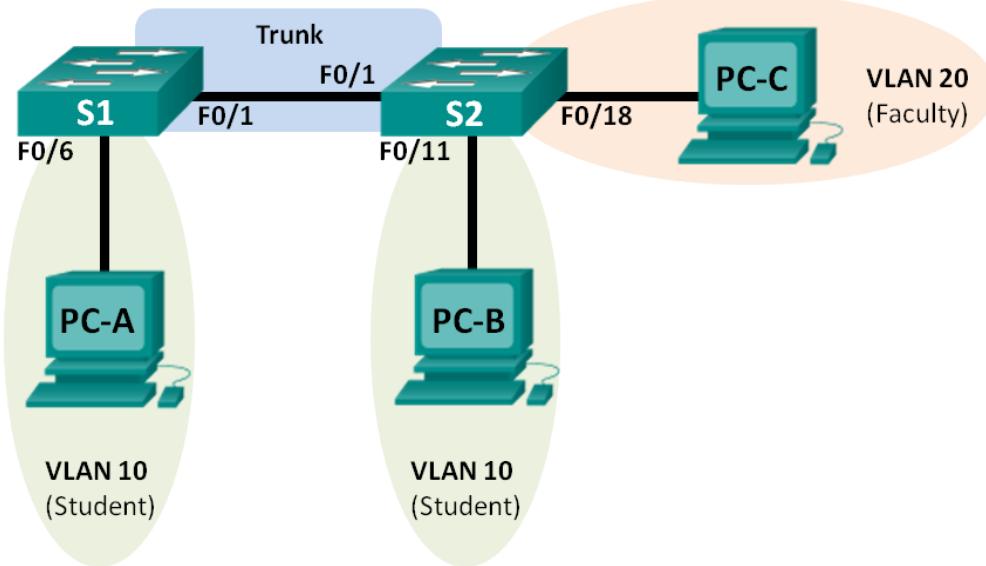
Identify elements of the model that map to IT-related content:

- In this scenario, the ISPs cable modem could function as a network switch.
- Floors 1-3 could be compared to network VLAN groups.
- The digital televisions could be compared to hosts within the VLAN groups.

Lab - Configuring VLANs and Trunking (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Objectives

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Create VLANs and Assign Switch Ports
- Part 3: Maintain VLAN Port Assignments and the VLAN Database
- Part 4: Configure an 802.1Q Trunk between the Switches
- Part 5: Delete the VLAN Database

Background / Scenario

Modern switches use virtual local-area networks (VLANs) to improve network performance by separating large Layer 2 broadcast domains into smaller ones. VLANs can also be used as a security measure by controlling which hosts can communicate. In general, VLANs make it easier to design a network to support the goals of an organization.

Lab - Configuring VLANs and Trunking

VLAN trunks are used to span VLANs across multiple devices. Trunks allow the traffic from multiple VLANs to travel over a single link, while keeping the VLAN identification and segmentation intact.

In this lab, you will create VLANs on both switches in the topology, assign VLANs to switch access ports, verify that VLANs are working as expected, and then create a VLAN trunk between the two switches to allow hosts in the same VLAN to communicate through the trunk, regardless of which switch the host is actually attached to.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

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

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

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

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

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Initialize and reload the switches as necessary.

Step 3: Configure basic settings for each switch.

- a. Console into the switch and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the switch.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
logging synchronous
login
exit
```

Lab - Configuring VLANs and Trunking

- c. Configure the host name as shown in the topology.
- d. Configure the IP address listed in the Addressing Table for VLAN 1 on the switch.
- e. Administratively deactivate all unused ports on the switch.
- f. Copy the running configuration to the startup configuration.

Step 4: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Step 5: Test connectivity.

Verify that the PC hosts can ping one another.

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

- Can PC-A ping PC-B? _____ Yes
- Can PC-A ping PC-C? _____ No
- Can PC-A ping S1? _____ No
- Can PC-B ping PC-C? _____ No
- Can PC-B ping S2? _____ No
- Can PC-C ping S2? _____ No
- Can S1 ping S2? _____ Yes

If you answered no to any of the above questions, why were the pings unsuccessful?

Pings were unsuccessful when trying to ping a device on a different subnet. For those pings to be successful, a default gateway must exist to route traffic from one subnet to another.

Part 2: Create VLANs and Assign Switch Ports

In Part 2, you will create student, faculty, and management VLANs on both switches. You will then assign the VLANs to the appropriate interface. The **show vlan** command is used to verify your configuration settings.

Step 1: Create VLANs on the switches.

- a. Create the VLANs on S1.

```
S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# end
```

- b. Create the same VLANs on S2.

- c. Issue the **show vlan** command to view the list of VLANs on S1.

```
S1# show vlan
```

Lab - Configuring VLANs and Trunking

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 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 Gi0/1, Gi0/2
10	Student	active	
20	Faculty	active	
99	Management	active	

1002	fddi-default	act/unsup
1003	token-ring-default	act/unsup
1004	fdдинet-default	act/unsup
1005	trnet-default	act/unsup

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
10	enet	100010	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
99	enet	100099	1500	-	-	-	-	-	0	0

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Remote SPAN VLANs

Primary Secondary Type Ports

What is the default VLAN? _____ **VLAN 1**

What ports are assigned to the default VLAN?

All switch ports are assigned to VLAN 1 by default.

Step 2: Assign VLANs to the correct switch interfaces.

- Assign VLANs to the interfaces on S1.
- Assign PC-A to the Student VLAN.

S1(config)# **interface f0/6**

Lab - Configuring VLANs and Trunking

```
S1(config-if)# switchport mode access  
S1(config-if)# switchport access vlan 10
```

- 2) Move the switch IP address VLAN 99.

```
S1(config)# interface vlan 1  
S1(config-if)# no ip address  
S1(config-if)# interface vlan 99  
S1(config-if)# ip address 192.168.1.11 255.255.255.0  
S1(config-if)# end
```

- b. Issue the **show vlan brief** command and verify that the VLANs are assigned to the correct interfaces.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, 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, Gi0/1 Gi0/2
10	Student	active	Fa0/6
20	Faculty	active	
99	Management	active	
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

- c. Issue the **show ip interface brief** command.

```
S1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	unset	up	up
Vlan99	192.168.1.11	YES	manual	up	down
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	administratively down	down
FastEthernet0/3	unassigned	YES	unset	administratively down	down
FastEthernet0/4	unassigned	YES	unset	administratively down	down
FastEthernet0/5	unassigned	YES	unset	administratively down	down
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	administratively down	down

```
<output omitted>
```

What is the status of VLAN 99? Why?

The status of VLAN 99 is up/down, because it has not been assigned to an active port yet.

- d. Use the Topology to assign VLANs to the appropriate ports on S2.

Lab - Configuring VLANs and Trunking

- e. Remove the IP address for VLAN 1 on S2.
- f. Configure an IP address for VLAN 99 on S2 according to the Addressing Table.
- g. Use the **show vlan brief** command to verify that the VLANs are assigned to the correct interfaces.

```
S2# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
10	Student	active	Fa0/11
20	Faculty	active	Fa0/18
99	Management	active	
1002	fdmi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdmnet-default	act/unsup	
1005	trnet-default	act/unsup	

Is PC-A able to ping PC-B? Why?

No. Interface F0/1 is not assigned to VLAN 10, so VLAN 10 traffic will not be sent over it.

Is S1 able to ping S2? Why?

No. The IP addresses for the switches now reside in VLAN 99. VLAN 99 traffic will not be sent over interface F0/1.

Part 3: Maintain VLAN Port Assignments and the VLAN Database

In Part 3, you will change VLAN assignments to ports and remove VLANs from the VLAN database.

Step 1: Assign a VLAN to multiple interfaces.

- a. On S1, assign interfaces F0/11 – 24 to VLAN 10.

```
S1(config)# interface range f0/11-24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# end
```

- b. Issue the **show vlan brief** command to verify VLAN assignments.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/7, Fa0/8, Fa0/9

Lab - Configuring VLANs and Trunking

			Fa0/10, Gi0/1, Gi0/2
10	Student	active	Fa0/6, 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
20	Faculty	active	
99	Management	active	
1002	fdmi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdmnet-default	act/unsup	
1005	trnet-default	act/unsup	

- c. Reassign F0/11 and F0/21 to VLAN 20.

```
S1(config)# interface range f0/11, f0/21
S1(config-if-range)# switchport access vlan 20
S1(config-if-range)# end
```

- d. Verify that VLAN assignments are correct.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Gi0/1, Gi0/2
10	Student	active	Fa0/6, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/22, Fa0/23 Fa0/24
20	Faculty	active	Fa0/11, Fa0/21
99	Management	active	
1002	fdmi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdmnet-default	act/unsup	
1005	trnet-default	act/unsup	

Step 2: Remove a VLAN assignment from an interface.

- a. Use the **no switchport access vlan** command to remove the VLAN 10 assignment to F0/24.

```
S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end
```

- b. Verify that the VLAN change was made.

Which VLAN is F0/24 now associated with?

VLAN 1, the default VLAN.

```
S1# show vlan brief
VLAN Name Status Ports
```

Lab - Configuring VLANs and Trunking

1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/24, Gi0/1, Gi0/2
10	Student	active	Fa0/6, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdtnet-default	act/unsup	
1005	trnet-default	act/unsup	

Step 3: Remove a VLAN ID from the VLAN database.

- Add VLAN 30 to interface F0/24 without issuing the VLAN command.

```
S1(config)# interface f0/24
S1(config-if)# switchport access vlan 30
% Access VLAN does not exist. Creating vlan 30
```

Note: Current switch technology no longer requires that the **vlan** command be issued to add a VLAN to the database. By assigning an unknown VLAN to a port, the VLAN adds to the VLAN database.

- Verify that the new VLAN is displayed in the VLAN table.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Gi0/1, Gi0/2
10	Student	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
30	VLAN0030	active	Fa0/24
99	Management	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdtnet-default	act/unsup	
1005	trnet-default	act/unsup	

What is the default name of VLAN 30?

VLAN0030

- Use the **no vlan 30** command to remove VLAN 30 from the VLAN database.

```
S1(config)# no vlan 30
S1(config)# end
```

Lab - Configuring VLANs and Trunking

- d. Issue the **show vlan brief** command. F0/24 was assigned to VLAN 30.

After deleting VLAN 30, what VLAN is port F0/24 assigned to? What happens to the traffic destined to the host attached to F0/24?

Port F0/24 is not assigned to any VLAN. This port will not transfer any traffic.

S1# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Gi0/1, Gi0/2
10	Student	active	Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
99	Management	active	
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdininet-default	act/unsup	
1005	trnet-default	act/unsup	

- e. Issue the **no switchport access vlan** command on interface F0/24.

```
S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end
```

- f. Issue the **show vlan brief** command to determine the VLAN assignment for F0/24. To which VLAN is F0/24 assigned?
-

VLAN 1

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/24, Gi0/1, Gi0/2
10	Student	active	Fa0/6, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
99	Management	active	
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdininet-default	act/unsup	
1005	trnet-default	act/unsup	

Lab - Configuring VLANs and Trunking

Note: Before removing a VLAN from the database, it is recommended that you reassign all the ports assigned to that VLAN.

Why should you reassign a port to another VLAN before removing the VLAN from the VLAN database?

The interfaces assigned to a VLAN that is removed from the VLAN database are unavailable for use until they are reassigned to another VLAN. This can be a tricky thing to troubleshoot as trunked interfaces do not show up in the port list as well (Part 4 contains more information about trunked interfaces).

Part 4: Configure an 802.1Q Trunk Between the Switches

In Part 4, you will configure interface F0/1 to use the Dynamic Trunking Protocol (DTP) to allow it to negotiate the trunk mode. After this has been accomplished and verified, you will disable DTP on interface F0/1 and manually configure it as a trunk.

Step 1: Use DTP to initiate trunking on F0/1.

The default DTP mode of a 2960 switch port is dynamic auto. This allows the interface to convert the link to a trunk if the neighboring interface is set to trunk or dynamic desirable mode.

- a. Set F0/1 on S1 to negotiate trunk mode.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode dynamic desirable
*Mar  1 05:07:28.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to down
*Mar  1 05:07:29.744: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
S1(config-if)#
*Mar  1 05:07:32.772: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
S1(config-if)#
*Mar  1 05:08:01.789: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
*Mar  1 05:08:01.797: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

You should also receive link status messages on S2.

```
S2#
*Mar  1 05:07:29.794: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
S2#
*Mar  1 05:07:32.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
S2#
*Mar  1 05:08:01.839: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
*Mar  1 05:08:01.850: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
```

- b. Issue the **show vlan brief** command on S1 and S2. Interface F0/1 is no longer assigned to VLAN 1. Trunked interfaces are not listed in the VLAN table.

Lab - Configuring VLANs and Trunking

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/24, Gi0/1, Gi0/2
10	Student	active	Fa0/6, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/22, Fa0/23
20	Faculty	active	Fa0/11, Fa0/21
99	Management	active	
1002	fdmi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdmnet-default	act/unsup	
1005	trnet-default	act/unsup	

- c. Issue the **show interfaces trunk** command to view trunked interfaces. Notice that the mode on S1 is set to desirable, and the mode on S2 is set to auto.

```
S1# show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	desirable	802.1q	trunking	1
Port	Vlans allowed on trunk			
Fa0/1	1-4094			
Port	Vlans allowed and active in management domain			
Fa0/1	1,10,20,99			
Port	Vlans in spanning tree forwarding state and not pruned			
Fa0/1	1,10,20,99			

```
S2# show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	auto	802.1q	trunking	1
Port	Vlans allowed on trunk			
Fa0/1	1-4094			
Port	Vlans allowed and active in management domain			
Fa0/1	1,10,20,99			
Port	Vlans in spanning tree forwarding state and not pruned			
Fa0/1	1,10,20,99			

Note: By default, all VLANs are allowed on a trunk. The **switchport trunk** command allows you to control what VLANs have access to the trunk. For this lab, keep the default settings which allows all VLANs to traverse F0/1.

Lab - Configuring VLANs and Trunking

- d. Verify that VLAN traffic is traveling over trunk interface F0/1.

Can S1 ping S2? _____ Yes

Can PC-A ping PC-B? _____ Yes

Can PC-A ping PC-C? _____ No

Can PC-B ping PC-C? _____ No

Can PC-A ping S1? _____ No

Can PC-B ping S2? _____ No

Can PC-C ping S2? _____ No

If you answered no to any of the above questions, explain below.

PC-C cannot ping PC-A or PC-B because PC-C is in a different VLAN. The switches are in different VLANs than the PCs; therefore, the pings were unsuccessful.

Step 2: Manually configure trunk interface F0/1.

The **switchport mode trunk** command is used to manually configure a port as a trunk. This command should be issued on both ends of the link.

- a. Change the switchport mode on interface F0/1 to force trunking. Make sure to do this on both switches.

```
S1(config)# interface f0/1  
S1(config-if)# switchport mode trunk
```

```
S2(config)# interface f0/1  
S2(config-if)# switchport mode trunk
```

- b. Issue the **show interfaces trunk** command to view the trunk mode. Notice that the mode changed from **desirable** to **on**.

```
S2# show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-4094

Port	Vlans allowed and active in management domain
Fa0/1	1,10,20,99

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/1	1,10,20,99

Why might you want to manually configure an interface to trunk mode instead of using DTP?

Not all equipment uses DTP. Using the **switchport mode trunk** command ensures that the port will become a trunk no matter what type of equipment is connected to the other end of the link.

Part 5: Delete the VLAN Database

In Part 5, you will delete the VLAN Database from the switch. It is necessary to do this when initializing a switch back to its default settings.

Step 1: Determine if the VLAN database exists.

Issue the **show flash** command to determine if a **vlan.dat** file exists in flash.

```
S1# show flash
```

Directory of flash:/

2	-rwx	1285	Mar 1 1993 00:01:24 +00:00	config.text
3	-rwx	43032	Mar 1 1993 00:01:24 +00:00	multiple-fs
4	-rwx	5	Mar 1 1993 00:01:24 +00:00	private-config.text
5	-rwx	11607161	Mar 1 1993 02:37:06 +00:00	c2960-lanbasek9-mz.150-2.SE.bin
6	-rwx	736	Mar 1 1993 00:19:41 +00:00	vlan.dat

32514048 bytes total (20858880 bytes free)

Note: If there is a **vlan.dat** file located in flash, then the VLAN database does not contain its default settings.

Step 2: Delete the VLAN database.

- a. Issue the **delete vlan.dat** command to delete the **vlan.dat** file from flash and reset the VLAN database back to its default settings. You will be prompted twice to confirm that you want to delete the **vlan.dat** file. Press Enter both times.

```
S1# delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
S1#
```

- b. Issue the **show flash** command to verify that the **vlan.dat** file has been deleted.

```
S1# show flash
```

Directory of flash:/

2	-rwx	1285	Mar 1 1993 00:01:24 +00:00	config.text
3	-rwx	43032	Mar 1 1993 00:01:24 +00:00	multiple-fs
4	-rwx	5	Mar 1 1993 00:01:24 +00:00	private-config.text
5	-rwx	11607161	Mar 1 1993 02:37:06 +00:00	c2960-lanbasek9-mz.150-2.SE.bin

32514048 bytes total (20859904 bytes free)

To initialize a switch back to its default settings, what other commands are needed?

Lab - Configuring VLANs and Trunking

To get a switch back to its default settings, the **erase startup-config** and **reload** commands need to be issued after the **delete vlan.dat** command.

Reflection

1. What is needed to allow hosts on VLAN 10 to communicate to hosts on VLAN 20?

Answers will vary, but Layer 3 routing is needed to route traffic between VLANs.

2. What are some primary benefits that an organization can receive through effective use of VLANs?

Answers will vary, but VLAN benefits include: better security, cost savings (efficient use of bandwidth and uplinks), higher performance (smaller broadcast domains), broadcast storm mitigation, improved IT staff efficiency, simpler project and application management.

Device Configs - Final

Switch S1

Building configuration...

```
Current configuration : 2571 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUG.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
```

Lab - Configuring VLANs and Trunking

```
!
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
  shutdown
!
interface FastEthernet0/3
  shutdown
!
interface FastEthernet0/4
  shutdown
!
interface FastEthernet0/5
  shutdown
!
interface FastEthernet0/6
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/7
  shutdown
!
interface FastEthernet0/8
  shutdown
!
interface FastEthernet0/9
  shutdown
!
interface FastEthernet0/10
  shutdown
!
interface FastEthernet0/11
  switchport access vlan 20
  switchport mode access
  shutdown
!
interface FastEthernet0/12
  switchport access vlan 10
  switchport mode access
  shutdown
!
interface FastEthernet0/13
  switchport access vlan 10
  switchport mode access
  shutdown
!
interface FastEthernet0/14
  switchport access vlan 10
```

Lab - Configuring VLANs and Trunking

```
switchport mode access
shutdown
!
interface FastEthernet0/15
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/16
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/17
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/18
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/19
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/20
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/21
switchport access vlan 20
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/23
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/24
```

Lab - Configuring VLANs and Trunking

```
switchport mode access
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
!
interface Vlan99
ip address 192.168.1.11 255.255.255.0
!
ip http server
ip http secure-server
!
!
banner motd ^C
Unauthorized Access is Prohibited!
^C
!
line con 0
password cisco
logging synchronous
login
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
end
```

Switch S2

```
Building configuration...
```

```
Current configuration : 1875 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S2
!
```

Lab - Configuring VLANs and Trunking

```
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
shutdown
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
switchport access vlan 10
switchport mode access
!
```

Lab - Configuring VLANs and Trunking

```
interface FastEthernet0/12
    shutdown
!
interface FastEthernet0/13
    shutdown
!
interface FastEthernet0/14
    shutdown
!
interface FastEthernet0/15
    shutdown
!
interface FastEthernet0/16
    shutdown
!
interface FastEthernet0/17
    shutdown
!
interface FastEthernet0/18
    switchport access vlan 20
    switchport mode access
!
interface FastEthernet0/19
    shutdown
!
interface FastEthernet0/20
    shutdown
!
interface FastEthernet0/21
    shutdown
!
interface FastEthernet0/22
    shutdown
!
interface FastEthernet0/23
    shutdown
!
interface FastEthernet0/24
    shutdown
!
interface GigabitEthernet0/1
    shutdown
!
Interface GigabitEthernet0/2
    shutdown
!
interface Vlan1
    no ip address
!
```

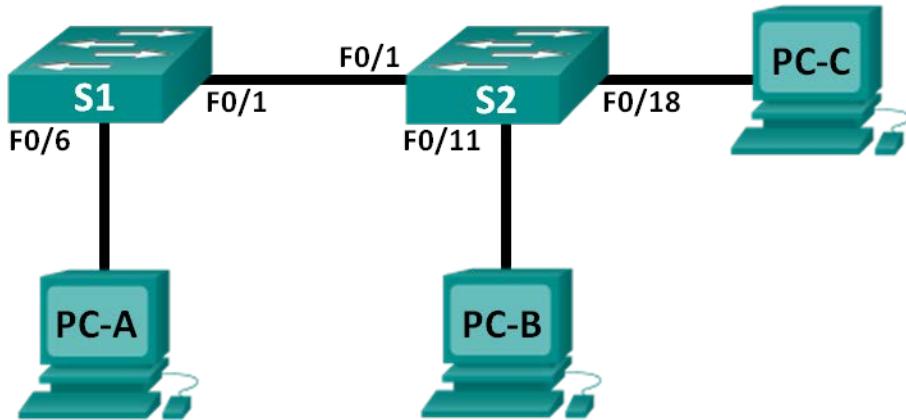
Lab - Configuring VLANs and Trunking

```
interface Vlan99
    ip address 192.168.1.12 255.255.255.0
!
ip http server
ip http secure-server
!
!
banner motd ^C
    Unauthorized Access is Prohibited!
^C
!
line con 0
    password cisco
    logging synchronous
    login
line vty 0 4
    password cisco
    login
line vty 5 15
    password cisco
    login
!
end
```

Lab - Troubleshooting VLAN Configurations (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
S2	VLAN 1	192.168.1.3	255.255.255.0	N/A
PC-A	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Switch Port Assignment Specifications

Ports	Assignment	Network
F0/1	802.1Q Trunk	N/A
F0/6-12	VLAN 10 – Students	192.168.10.0/24
F0/13-18	VLAN 20 – Faculty	192.168.20.0/24
F0/19-24	VLAN 30 – Guest	192.168.30.0/24

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Troubleshoot VLAN 10

Part 3: Troubleshoot VLAN 20

Background / Scenario

VLANs provide logical segmentation within an internetwork and improve network performance by separating large broadcast domains into smaller ones. By separating hosts into different networks, VLANs can be used to control which hosts can communicate. In this lab, a school has decided to implement VLANs in order to separate traffic from different end users. The school is using 802.1Q trunking to facilitate VLAN communication between switches.

The S1 and S2 switches have been configured with VLAN and trunking information. Several errors in the configuration have resulted in connectivity issues. You have been asked to troubleshoot and correct the configuration errors and document your work.

Note: The switches used with this lab are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

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

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the switches with some basic settings, such as passwords and IP addresses. Preset VLAN-related configurations, which contain errors, are provided for you for the initial switch configurations. You will also configure the IP settings for the PCs in the topology.

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

Step 2: Configure PC hosts.

Step 3: Initialize and reload the switches as necessary.

Step 4: Configure basic settings for each switch.

- a. Disable DNS lookup.
- b. Configure the IP address according to the Addressing Table.
- c. Assign **cisco** as the console and vty passwords and enable login for console and vty lines.
- d. Assign **class** as the privileged EXEC password.
- e. Configure **logging synchronous** to prevent console messages from interrupting command entry.

Step 5: Load switch configurations.

The configurations for the switches S1 and S2 are provided for you. There are errors within these configurations, and it is your job to determine the incorrect configurations and correct them.

Switch S1 Configuration:

Lab - Troubleshooting VLAN Configurations

```
hostname S1
vlan 10
  name Students
vlan 2
!vlan 20
name Faculty
vlan 30
  name Guest
interface range f0/1-24
  switchport mode access
  shutdown
!interface f0/1
! switchport mode trunk
! no shutdown
interface range f0/7-12
!interface range f0/6-12
  switchport access vlan 10
interface range f0/13-18
  switchport access vlan 2
! switchport access vlan 20
interface range f0/19-24
  switchport access vlan 30
end
```

Switch S2 Configuration:

```
hostname S2
vlan 10
  name Students
vlan 20
  name Faculty
vlan 30
  name Guest
interface f0/1
  switchport mode trunk
  switchport trunk allowed vlan 1,10,2,30
! switchport trunk allowed vlan 1,10,20,30
interface range f0/2-24
  switchport mode access
  shutdown
!interface range f0/6-12
! switchport access vlan 10
interface range f0/13-18
  switchport access vlan 20
interface range f0/19-24
  switchport access vlan 30
  shutdown
end
```

Step 6: Copy the running configuration to the startup configuration.

Part 2: Troubleshoot VLAN 10

In Part 2, you must examine VLAN 10 on S1 and S2 to determine if it is configured correctly. You will troubleshoot the scenario until connectivity is established.

Step 1: Troubleshoot VLAN 10 on S1.

- a. Can PC-A ping PC-B? _____ No
- b. After verifying that PC-A was configured correctly, examine the S1 switch to find possible configuration errors by viewing a summary of the VLAN information. Enter the **show vlan brief** command.

S1# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Gi0/1, Gi0/2
2	Faculty	active	Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18
10	Students	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
30	Guest	active	Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdinnet-default	act/unsup	
1005	trnet-default	act/unsup	

- c. Are there any problems with the VLAN configuration?

Yes. The port for PC-A is not assigned to the correct VLAN. The port for F0/1 is assigned to VLAN 1; therefore, it is not acting as a trunk port.

- d. Examine the switch for trunk configurations using the **show interfaces trunk** and the **show interfaces f0/1 switchport** commands.

S1# **show interfaces trunk**

S1# **show interfaces f0/1 switchport**
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none

Lab - Troubleshooting VLAN Configurations

```
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

- e. Are there any problems with the trunking configuration?
-

Yes. No trunk ports exist and F0/1 is configured as an access port instead of a trunk port.

- f. Examine the running configuration of the switch to find possible configuration errors.

Are there any problems with the current configuration?

Yes. F0/1-5 are all configured as access ports and all ports on the switch are shutdown.

- g. Correct the errors found regarding F0/1 and VLAN 10 on S1. Record the commands used in the space below.
-
-
-
-
-
-

```
S1(config)# interface f0/1
S1(config-if)# no shutdown
S1(config-if)# switchport mode trunk
S1(config-if)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# switchport access vlan 10
```

- h. Verify the commands had the desired effects by issuing the appropriate **show** commands.

```
S1# show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/1	1-4094

Lab - Troubleshooting VLAN Configurations

```
Port      Vlans allowed and active in management domain
Fa0/1     1-2,10,30
```

```
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1-2,10,30
```

S1# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Gi0/1, Gi0/2
2	Faculty	active	Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18
10	Students	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12
30	Guest	active	Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdinnet-default	act/unsup	
1005	trnet-default	act/unsup	

- i. Can PC-A ping PC-B? _____ **No**

Step 2: Troubleshoot VLAN 10 on S2.

- a. Using the previous commands, examine the S2 switch to find possible configuration errors.
Are there any problems with the current configuration?

Yes. No ports were assigned access to VLAN 10 and ports F0/1 and F0/11 are shutdown.

S2# **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Gi0/1 Gi0/2
10	Students	active	Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18
20	Faculty	active	Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
30	Guest	active	
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdinnet-default	act/unsup	
1005	trnet-default	act/unsup	

Lab - Troubleshooting VLAN Configurations

- b. Correct the errors found regarding interfaces and VLAN 10 on S2. Record the commands below.

```
S2(config)# interface range f0/6-12
S2(config-if-range)# switchport access vlan 10
S2(config-if-range)# interface f0/11
S2(config-if)# no shutdown
```

- c. Can PC-A ping PC-B? _____ Yes

Part 3: Troubleshoot VLAN 20

In Part 3, you must examine VLAN 20 on S1 and S2 to determine if it is configured correctly. To verify functionality, you will reassign PC-A into VLAN 20, and then troubleshoot the scenario until connectivity is established.

Step 1: Assign PC-A to VLAN 20.

- On PC-A, change the IP address to 192.168.20.2/24 with a default gateway of 192.168.20.1.
- On S1, assign the port for PC-A to VLAN 20. Write the commands needed to complete the configuration.

```
S1(config)# interface f0/6
S1(config-if)# switchport access vlan 20
```

- c. Verify that the port for PC-A has been assigned to VLAN 20.

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Gi0/1, Gi0/2
2	Faculty	active	Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18
10	Students	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
20	VLAN0020	active	Fa0/6
30	Guest	active	Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Lab - Troubleshooting VLAN Configurations

d. Can PC-A ping PC-C? _____ No

Step 2: Troubleshoot VLAN 20 on S1.

- Using the previous commands, examine the S1 switch to find possible configuration errors.
Are there any problems with the current configuration?

Yes. VLAN 2 was created instead of VLAN 20 and ports have been assigned to VLAN 2 instead of VLAN 20.

- Correct the errors found regarding VLAN 20.

```
S1(config)# interface range f0/13-18
S1(config-if-range)# switchport access vlan 20
S1(config-if-range)# exit
S1(config)# no vlan 2
S1(config)# vlan 20
S1(config-vlan)# name Faculty
```

- Can PC-A ping PC-C? _____ No

Step 3: Troubleshoot VLAN 20 on S2.

- Using the previous commands, examine the S2 switch to find possible configuration errors.
Are there any problems with the current configuration?

Yes. The trunked interface has been misconfigured to allow communication for VLAN 2 instead of VLAN 20 and port f0/18 is shutdown.

```
S2# show interfaces trunk

Port      Mode          Encapsulation  Status      Native vlan
Fa0/1     on           802.1q        trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-2,10,30

Port      Vlans allowed and active in management domain
Fa0/1     1,10,30

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1     1,10,30

S2# show run interface f0/18
Building configuration...

Current configuration : 95 bytes
!
interface FastEthernet0/18
```

Lab - Troubleshooting VLAN Configurations

```
switchport access vlan 20
switchport mode access
shutdown
end
```

- b. Correct the errors found regarding VLAN 20. Record the commands used below.
-
-
-
-

```
S2(config)# interface f0/18
S2(config-if)# no shutdown
S2(config)# interface f0/1
S2(config-if)# switchport trunk allowed vlan remove 2
S2(config-if)# switchport trunk allowed vlan add 20
```

- c. Can PC-A ping PC-C? _____ Yes

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

Reflection

1. Why is a correctly configured trunk port critical in a multi-VLAN environment?
-
-

An 802.1Q trunk port allows for transmission of multiple VLANs across one link. An incorrectly configured trunk port can prevent VLANs from communicating across switches.

2. Why would a network administrator limit traffic for specific VLANs on a trunk port?
-
-

To prevent unwanted VLAN traffic from traveling through that trunk port.

Device Configs

Instructor Note: The VLANs configured do not display in the running configuration but are stored in the `vlan.dat` file.

Switch S1

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Gi0/1, Gi0/2
10	Students	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/12
20	Faculty	active	Fa0/6, Fa0/13, Fa0/14, Fa0/15

Lab - Troubleshooting VLAN Configurations

		Fa0/16, Fa0/17, Fa0/18
30 Guest	active	Fa0/19, Fa0/20, Fa0/21, Fa0/22
		Fa0/23, Fa0/24
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

```
S1#show run
Building configuration...
```

```
Current configuration : 3966 bytes
!
version 15.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$Hf8a$8iwF0hp1dYGtxwlUsJuE5/
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
interface FastEthernet0/1
 switchport mode trunk
!
interface FastEthernet0/2
 switchport mode access
```

Lab - Troubleshooting VLAN Configurations

```
shutdown
!
interface FastEthernet0/3
switchport mode access
shutdown
!
interface FastEthernet0/4
switchport mode access
shutdown
!
interface FastEthernet0/5
switchport mode access
shutdown
!
interface FastEthernet0/6
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/8
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/9
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/10
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/11
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/12
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/13
```

Lab - Troubleshooting VLAN Configurations

```
switchport access vlan 20
switchport mode access
shutdown
!
interface FastEthernet0/14
switchport access vlan 20
switchport mode access
shutdown
!
interface FastEthernet0/15
switchport access vlan 20
switchport mode access
shutdown
!
interface FastEthernet0/16
switchport access vlan 20
switchport mode access
shutdown
!
interface FastEthernet0/17
switchport access vlan 20
switchport mode access
shutdown
!
interface FastEthernet0/18
switchport access vlan 20
switchport mode access
shutdown
!
interface FastEthernet0/19
switchport access vlan 30
switchport mode access
shutdown
!
interface FastEthernet0/20
switchport access vlan 30
switchport mode access
shutdown
!
interface FastEthernet0/21
switchport access vlan 30
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport access vlan 30
switchport mode access
shutdown
!
```

Lab - Troubleshooting VLAN Configurations

```
interface FastEthernet0/23
switchport access vlan 30
switchport mode access
shutdown
!
interface FastEthernet0/24
switchport access vlan 30
switchport mode access
shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 192.168.1.2 255.255.255.0
no ip route-cache
!
ip http server
ip http secure-server
logging esm config
!
line con 0
password cisco
logging synchronous
login
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
end
```

Switch S2

```
S2# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Gi0/1, Gi0/2
10	Students	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12
20	Faculty	active	Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18
30	Guest	active	Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24
1002	fdi-default	act/unsup	

Lab - Troubleshooting VLAN Configurations

```
1003 token-ring-default          act/unsup
1004 fddinet-default            act/unsup
1005 trnet-default              act/unsup
S2# show run
Building configuration...
Current configuration : 3966 bytes
!
! Last configuration change at 00:07:17 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname S2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$T7f6$AYijjsmnLmWzgIAET.DDj/
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface FastEthernet0/1
  switchport trunk allowed vlan 1,10,20,30
  switchport mode trunk
!
interface FastEthernet0/2
  switchport mode access
  shutdown
!
interface FastEthernet0/3
```

Lab - Troubleshooting VLAN Configurations

```
switchport mode access
shutdown
!
interface FastEthernet0/4
switchport mode access
shutdown
!
interface FastEthernet0/5
switchport mode access
shutdown
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/7
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/8
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/9
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/10
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/11
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/12
switchport access vlan 10
switchport mode access
shutdown
!
interface FastEthernet0/13
switchport access vlan 20
switchport mode access
shutdown
```

Lab - Troubleshooting VLAN Configurations

```
!
interface FastEthernet0/14
 switchport access vlan 20
 switchport mode access
 shutdown

!
interface FastEthernet0/15
 switchport access vlan 20
 switchport mode access
 shutdown

!
interface FastEthernet0/16
 switchport access vlan 20
 switchport mode access
 shutdown

!
interface FastEthernet0/17
 switchport access vlan 20
 switchport mode access
 shutdown

!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access

!
interface FastEthernet0/19
 switchport access vlan 30
 switchport mode access
 shutdown

!
interface FastEthernet0/20
 switchport access vlan 30
 switchport mode access
 shutdown

!
interface FastEthernet0/21
 switchport access vlan 30
 switchport mode access
 shutdown

!
interface FastEthernet0/22
 switchport access vlan 30
 switchport mode access
 shutdown

!
interface FastEthernet0/23
 switchport access vlan 30
 switchport mode access
```

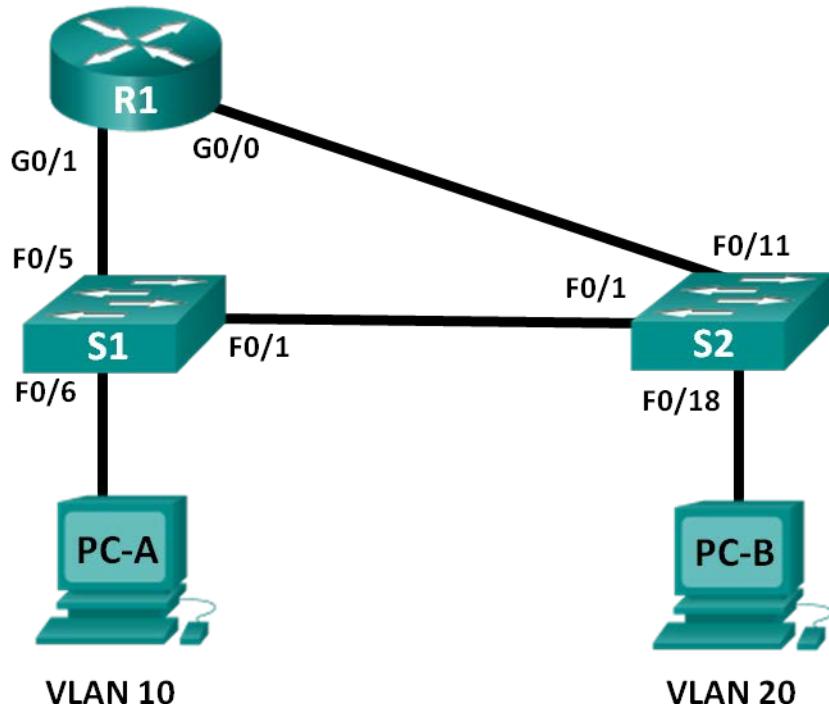
Lab - Troubleshooting VLAN Configurations

```
shutdown
!
interface FastEthernet0/24
switchport access vlan 30
switchport mode access
shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  ip address 192.168.1.3 255.255.255.0
  no ip route-cache
!
ip http server
ip http secure-server
logging esm config
!
line con 0
  password cisco
  logging synchronous
  login
line vty 0 4
  password cisco
  login
line vty 5 15
  password cisco
  login
!
end
```

Lab – Configuring Per-Interface Inter-VLAN Routing (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.20.1	255.255.255.0	N/A
	G0/1	192.168.10.1	255.255.255.0	N/A
S1	VLAN 10	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 10	192.168.10.12	255.255.255.0	192.168.10.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Configure Switches with VLANs and Trunking

Part 3: Verify Trunking, VLANs, Routing, and Connectivity

Background / Scenario

Legacy inter-VLAN routing is seldom used in today's networks; however, it is helpful to configure and understand this type of routing before moving on to router-on-a-stick (trunk-based) inter-VLAN routing or configuring Layer-3 switching. Also, you may encounter per-interface inter-VLAN routing in organizations with very small networks. One of the benefits of legacy inter-VLAN routing is ease of configuration.

In this lab, you will set up one router with two switches attached via the router Gigabit Ethernet interfaces. Two separate VLANs will be configured on the switches, and you will set up routing between the VLANs.

Note: This lab provides minimal assistance with the actual commands necessary to configure the router and switches. The required switch VLAN configuration commands are provided in Appendix A of this lab. Test your knowledge by trying to configure the devices without referring to the appendix.

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

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

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and clear any configurations, if necessary.

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

Step 2: Initialize and reload the router and switches.

Step 3: Configure basic settings for R1.

- a. Console into R1 and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on R1.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
```

Lab – Configuring Per-Interface Inter-VLAN Routing

- ```
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```
- c. Configure addressing on G0/0 and G0/1 and enable both interfaces.
  - d. Copy the running configuration to the startup configuration.

### Step 4: Configure basic settings on both switches.

- a. Console into the switch and enter global configuration mode.
- b. Copy the following basic configuration and paste it to running-configuration on the switch.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

- c. Configure the host name as shown in the topology.
- d. Copy the running configuration to the startup configuration.

### Step 5: Configure basic settings on PC-A and PC-B.

Configure PC-A and PC-B with IP addresses and a default gateway address according to the Addressing Table.

## Part 2: Configure Switches with VLANs and Trunking

In Part 2, you will configure the switches with VLANs and trunking.

### Step 1: Configure VLANs on S1.

- a. On S1, create VLAN 10. Assign **Student** as the VLAN name.
- b. Create VLAN 20. Assign **Faculty-Admin** as the VLAN name.
- c. Configure F0/1 as a trunk port.
- d. Assign ports F0/5 and F0/6 to VLAN 10 and configure both F0/5 and F0/6 as access ports.
- e. Assign an IP address to VLAN 10 and enable it. Refer to the Addressing Table.
- f. Configure the default gateway according to the Addressing Table.

**Step 2: Configure VLANs on S2.**

- a. On S2, create VLAN 10. Assign **Student** as the VLAN name.
- b. Create VLAN 20. Assign **Faculty-Admin** as the VLAN name.
- c. Configure F0/1 as a trunk port.
- d. Assign ports F0/11 and F0/18 to VLAN 20 and configure both F0/11 and F0/18 as access ports.
- e. Assign an IP address to VLAN 10 and enable it. Refer to the Addressing Table.
- f. Configure the default gateway according to the Addressing Table.

**Part 3: Verify Trunking, VLANs, Routing, and Connectivity**

**Step 1: Verify the R1 routing table.**

- a. On R1, issue the **show ip route** command. What routes are listed on R1?

---

The 192.168.10.0/24 and 192.168.20.0/24 networks are listed on R1.

```
R1# show ip route
*Mar 25 15:05:00.003: %SYS-5-CONFIG_I: Configured from console by console
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
 + - replicated route, % - next hop override
Gateway of last resort is not set
 192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/1
L 192.168.10.1/32 is directly connected, GigabitEthernet0/1
 192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/0
L 192.168.20.1/32 is directly connected, GigabitEthernet0/0
```

- b. On both S1 and S2, issue the **show interface trunk** command. Is the F0/1 port on both switches set to trunk? \_\_\_\_\_ **Yes**

```
S1# show interface trunk
```

| Port  | Mode                                          | Encapsulation | Status   | Native vlan |
|-------|-----------------------------------------------|---------------|----------|-------------|
| Fa0/1 | on                                            | 802.1q        | trunking | 1           |
| Port  | Vlans allowed on trunk                        |               |          |             |
| Fa0/1 | 1-4094                                        |               |          |             |
| Port  | Vlans allowed and active in management domain |               |          |             |
| Fa0/1 | 1,10,20                                       |               |          |             |

## Lab – Configuring Per-Interface Inter-VLAN Routing

---

Port            Vlans in spanning tree forwarding state and not pruned  
Fa0/1            1,10,20

- c. Issue a **show vlan brief** command on both S1 and S2. Verify that VLANs 10 and 20 are active and that the proper ports on the switches are in the correct VLANs. Why is F0/1 not listed in any of the active VLANs?

---

It is a trunk port and is not assigned to a VLAN.

S1# **show vlan brief**

| VLAN | Name               | Status    | Ports                                                                                                                                                                                    |
|------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | default            | active    | Fa0/2, Fa0/3, Fa0/4, Fa0/7<br>Fa0/8, Fa0/9, Fa0/10, Fa0/11<br>Fa0/12, Fa0/13, Fa0/14, Fa0/15<br>Fa0/16, Fa0/17, Fa0/18, Fa0/19<br>Fa0/20, Fa0/21, Fa0/22, Fa0/23<br>Fa0/24, Gi0/1, Gi0/2 |
| 10   | Student            | active    | Fa0/5, Fa0/6                                                                                                                                                                             |
| 20   | Faculty-Admin      | active    |                                                                                                                                                                                          |
| 1002 | fdmi-default       | act/unsup |                                                                                                                                                                                          |
| 1003 | token-ring-default | act/unsup |                                                                                                                                                                                          |
| 1004 | fdmnet-default     | act/unsup |                                                                                                                                                                                          |
| 1005 | trnet-default      | act/unsup |                                                                                                                                                                                          |

S2# **show vlan brief**

| VLAN | Name               | Status    | Ports                                                                                                                                                                                  |
|------|--------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | default            | active    | Fa0/2, Fa0/3, Fa0/4, Fa0/5<br>Fa0/6, Fa0/7, Fa0/8, Fa0/9<br>Fa0/10, Fa0/12, Fa0/13, Fa0/14<br>Fa0/15, Fa0/16, Fa0/17, Fa0/19<br>Fa0/20, Fa0/21, Fa0/22, Fa0/23<br>Fa0/24, Gi0/1, Gi0/2 |
| 10   | Student            | active    |                                                                                                                                                                                        |
| 20   | Faculty-Admin      | active    | Fa0/11, Fa0/18                                                                                                                                                                         |
| 1002 | fdmi-default       | act/unsup |                                                                                                                                                                                        |
| 1003 | token-ring-default | act/unsup |                                                                                                                                                                                        |
| 1004 | fdmnet-default     | act/unsup |                                                                                                                                                                                        |
| 1005 | trnet-default      | act/unsup |                                                                                                                                                                                        |

- d. Ping from PC-A in VLAN 10 to PC-B in VLAN 20. If Inter-VLAN routing is functioning correctly, the pings between the 192.168.10.0 network and the 192.168.20.0 should be successful.

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

- e. Verify connectivity between devices. You should be able to ping between all devices. Troubleshoot if you are not successful.

## Lab – Configuring Per-Interface Inter-VLAN Routing

---

### Reflection

What is an advantage of using legacy inter-VLAN routing?

---

---

Answers may vary. Configuration of both the router and switches is relatively easy and straightforward. No subinterfaces are required on the router and trunking does NOT have to be configured between the router and switch.

### Router Interface Summary Table

| Router Interface Summary |                                |                                |                       |                       |
|--------------------------|--------------------------------|--------------------------------|-----------------------|-----------------------|
| Router Model             | Ethernet Interface #1          | Ethernet Interface #2          | Serial Interface #1   | Serial Interface #2   |
| 1800                     | Fast Ethernet 0/0<br>(F0/0)    | Fast Ethernet 0/1<br>(F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900                     | Gigabit Ethernet 0/0<br>(G0/0) | Gigabit Ethernet 0/1<br>(G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801                     | Fast Ethernet 0/0<br>(F0/0)    | Fast Ethernet 0/1<br>(F0/1)    | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811                     | Fast Ethernet 0/0<br>(F0/0)    | Fast Ethernet 0/1<br>(F0/1)    | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900                     | Gigabit Ethernet 0/0<br>(G0/0) | Gigabit Ethernet 0/1<br>(G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |

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

### Appendix A: Configuration Commands

#### Switch S1

```
S1(config)# vlan 10
S1(config-vlan)# name Student
S1(config-vlan)# exit
S1(config)# vlan 20
S1(config-vlan)# name Faculty-Admin
S1(config-vlan)# exit
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# interface range f0/5 - 6
S1(config-if-range)# switchport mode access
```

## Lab – Configuring Per-Interface Inter-VLAN Routing

---

```
S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# interface vlan 10
S1(config-if)# ip address 192.168.10.11 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.10.1
```

## Switch S2

```
S2(config)# vlan 10
S2(config-vlan)# name Student
S2(config-vlan)# exit
S2(config)# vlan 20
S2(config-vlan)# name Faculty-Admin
S2(config-vlan)# exit
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
S2(config-if)# interface f0/11
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if-range)# interface vlan 10
S2(config-if)#ip address 192.168.10.12 255.255.255.0
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.10.1
```

## Device Configs

**Instructor Note:** The VLANs configured do not display in the switch running configuration but are stored in the `vlan.dat` file.

## Router R1

```
R1#show run
Building configuration...

Current configuration : 1640 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
```

## Lab – Configuring Per-Interface Inter-VLAN Routing

---

```
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
redundancy
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
ip address 192.168.20.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.10.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
```

## Lab – Configuring Per-Interface Inter-VLAN Routing

---

```
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
!
!
line con 0
password cisco
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### Switch S1

```
S1# show vlan brief
```

| VLAN | Name               | Status    | Ports                                                                                                                                                                                    |
|------|--------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | default            | active    | Fa0/2, Fa0/3, Fa0/4, Fa0/7<br>Fa0/8, Fa0/9, Fa0/10, Fa0/11<br>Fa0/12, Fa0/13, Fa0/14, Fa0/15<br>Fa0/16, Fa0/17, Fa0/18, Fa0/19<br>Fa0/20, Fa0/21, Fa0/22, Fa0/23<br>Fa0/24, Gi0/1, Gi0/2 |
| 10   | Student            | active    | Fa0/5, Fa0/6                                                                                                                                                                             |
| 20   | Faculty-Admin      | active    |                                                                                                                                                                                          |
| 1002 | fdmi-default       | act/unsup |                                                                                                                                                                                          |
| 1003 | token-ring-default | act/unsup |                                                                                                                                                                                          |
| 1004 | fdmynet-default    | act/unsup |                                                                                                                                                                                          |

## Lab – Configuring Per-Interface Inter-VLAN Routing

---

```
1005 trnet-default act/unsup

S1#show run
Building configuration...

Current configuration : 1644 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
```

## Lab – Configuring Per-Interface Inter-VLAN Routing

---

```
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 192.168.10.11 255.255.255.0
!
 ip default-gateway 192.168.10.1
 ip http server
 ip http secure-server
!
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
```

## Lab – Configuring Per-Interface Inter-VLAN Routing

---

```
login
line vty 5 15
password cisco
login
!
end
```

### Switch S2

```
S2# show vlan brief
```

| VLAN | Name               | Status    | Ports                                                                                                                                                                                  |
|------|--------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | default            | active    | Fa0/2, Fa0/3, Fa0/4, Fa0/5<br>Fa0/6, Fa0/7, Fa0/8, Fa0/9<br>Fa0/10, Fa0/12, Fa0/13, Fa0/14<br>Fa0/15, Fa0/16, Fa0/17, Fa0/19<br>Fa0/20, Fa0/21, Fa0/22, Fa0/23<br>Fa0/24, Gi0/1, Gi0/2 |
| 10   | Student            | active    |                                                                                                                                                                                        |
| 20   | Faculty-Admin      | active    | Fa0/11, Fa0/18                                                                                                                                                                         |
| 1002 | fdmi-default       | act/unsup |                                                                                                                                                                                        |
| 1003 | token-ring-default | act/unsup |                                                                                                                                                                                        |
| 1004 | fddinet-default    | act/unsup |                                                                                                                                                                                        |
| 1005 | trnet-default      | act/unsup |                                                                                                                                                                                        |

```
S2#sh run
Building configuration...
```

```
Current configuration : 1644 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S2
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUG.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
interface FastEthernet0/1
 switchport mode trunk
!
```

## Lab – Configuring Per-Interface Inter-VLAN Routing

---

```
<Output Omitted>
interface FastEthernet0/10
!
interface FastEthernet0/11
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
 switchport access vlan 20
 switchport mode access
!
!interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 192.168.10.12 255.255.255.0
!
ip default-gateway 192.168.10.1
ip http server
ip http secure-server
```

## Lab – Configuring Per-Interface Inter-VLAN Routing

---

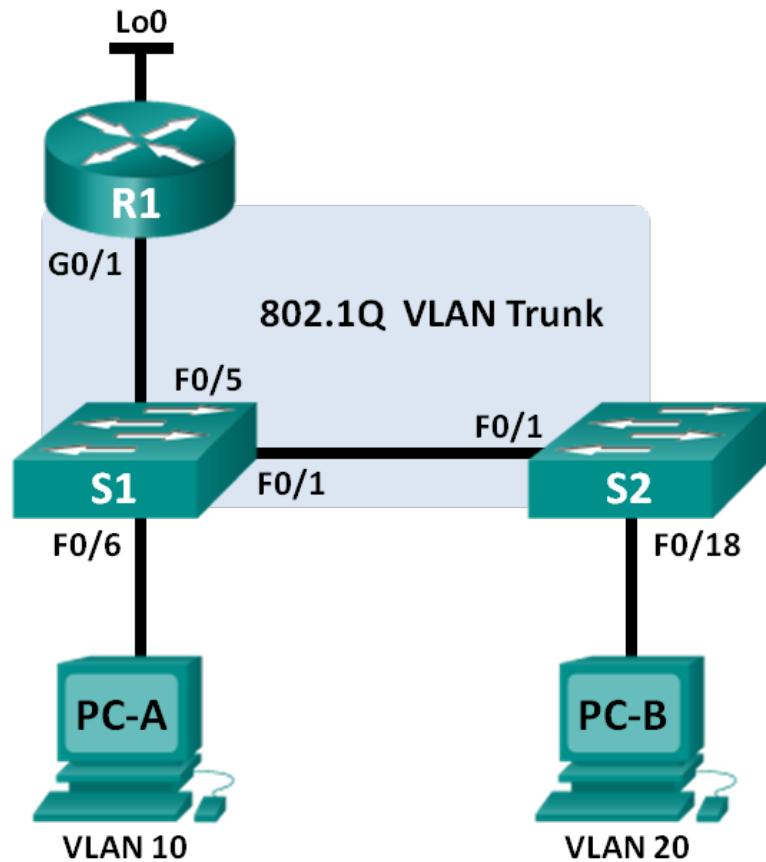
```
!
line con 0
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
end
```

# Lab – Configuring 802.1Q Trunk-Based Inter-VLAN Routing

## (Instructor Version – Optional Lab)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

### Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1.1	192.168.1.1	255.255.255.0	N/A
	G0/1.10	192.168.10.1	255.255.255.0	N/A
	G0/1.20	192.168.20.1	255.255.255.0	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.20.3	255.255.255.0	192.168.20.1

## Switch Port Assignment Specifications

Ports	Assignment	Network
S1 F0/1	802.1Q Trunk	N/A
S2 F0/1	802.1Q Trunk	N/A
S1 F0/5	802.1Q Trunk	N/A
S1 F0/6	VLAN 10 – Students	192.168.10.0/24
S2 F0/18	VLAN 20 – Faculty	192.168.20.0/24

## Objectives

**Part 1: Build the Network and Configure Basic Device Settings**

**Part 2: Configure Switches with VLANs and Trunking**

**Part 3: Configure Trunk-Based Inter-VLAN Routing**

## Background / Scenario

A second method of providing routing and connectivity for multiple VLANs is through the use of an 802.1Q trunk between one or more switches and a single router interface. This method is also known as router-on-a-stick inter-VLAN routing. In this method, the physical router interface is divided into multiple subinterfaces that provide logical pathways to all VLANs connected.

In this lab, you will configure trunk-based inter-VLAN routing and verify connectivity to hosts on different VLANs as well as with a loopback on the router.

**Note:** This lab provides minimal assistance with the actual commands necessary to configure trunk-based inter-VLAN routing. However, the required configuration commands are provided in Appendix A of this lab. Test your knowledge by trying to configure the devices without referring to the appendix.

**Note:** The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS, Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS, Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary.

from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

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

**Instructor Note:** Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

### Required Resources

- 1 Router (Cisco 1941 with Cisco IOS, release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS, release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

## Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the PC hosts, switches, and router.

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

**Step 2: Configure PC hosts.**

**Step 3: Initialize and reload the router and switches as necessary.**

**Step 4: Configure basic settings for each switch.**

- a. Console into the switch and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the switch.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

- c. Configure the device name as shown in the topology.
- d. Configure the IP address listed in the Addressing Table for VLAN 1 on the switch.
- e. Configure the default gateway on the switch.
- f. Administratively deactivate all unused ports on the switch.

- g. Copy the running configuration to the startup configuration.

**Step 5: Configure basic settings for the router.**

- a. Console into the router and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. Configure the Lo0 IP address as shown in the Address Table. Do not configure sub-interfaces at this time. They will be configured in Part 3.
- d. Copy the running configuration to the startup configuration.

## **Part 2: Configure Switches with VLANs and Trunking**

In Part 2, you will configure the switches with VLANs and trunking.

**Note:** The required commands for Part 2 are provided in Appendix A. Test your knowledge by trying to configure S1 and S2 without referring to the appendix.

**Step 1: Configure VLANs on S1.**

- a. On S1, configure the VLANs and names listed in the Switch Port Assignment Specifications table. Write the commands you used in the space provided.

---

---

---

---

---

```
S1(config)# vlan 10
S1(config-vlan)# name Students
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# exit
```

- b. On S1, configure the interface connected to R1 as a trunk. Also configure the interface connected to S2 as a trunk. Write the commands you used in the space provided.

---

```
S1(config)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# interface f0/1
S1(config-if)# switchport mode trunk
```

- c. On S1, assign the access port for PC-A to VLAN 10. Write the commands you used in the space provided.

---

---

---

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

### Step 2: Configure VLANs on Switch 2.

- On S2, configure the VLANs and names listed in the Switch Port Assignment Specifications table.
- On S2, verify that the VLAN names and numbers match those on S1. Write the command you used in the space provided.

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

VLAN Name Status Ports
----- -----
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4, 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, Gi0/1
Gi0/2

10 Students active
20 Faculty active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
```

- On S2, assign the access port for PC-B to VLAN 20.
- On S2, configure the interface connected to S1 as a trunk.

### Part 3: Configure Trunk-Based Inter-VLAN Routing

In Part 3, you will configure R1 to route to multiple VLANs by creating subinterfaces for each VLAN. This method of inter-VLAN routing is called router-on-a-stick.

## Lab – Configuring 802.1Q Trunk-Based Inter-VLAN Routing

---

**Note:** The required commands for Part 3 are provided in Appendix A. Test your knowledge by trying to configure trunk-based or router-on-a-stick inter-VLAN routing without referring to the appendix.

### Step 1: Configure a subinterface for VLAN 1.

- Create a subinterface on R1 G0/1 for VLAN 1 using 1 as the subinterface ID. Write the command you used in the space provided.

```
R1(config)# interface g0/1.1
```

- Configure the subinterface to operate on VLAN 1. Write the command you used in the space provided.

```
R1(config-subif)# encapsulation dot1Q 1
```

- Configure the subinterface with the IP address from the Address Table. Write the command you used in the space provided.

```
R1(config-subif)# ip address 192.168.1.1 255.255.255.0
```

### Step 2: Configure a subinterface for VLAN 10.

- Create a subinterface on R1 G0/1 for VLAN 10 using 10 as the subinterface ID.
- Configure the subinterface to operate on VLAN 10.
- Configure the subinterface with the address from the Address Table.

### Step 3: Configure a subinterface for VLAN 20.

- Create a subinterface on R1 G0/1 for VLAN 20 using 20 as the subinterface ID.
- Configure the subinterface to operate on VLAN 20.
- Configure the subinterface with the address from the Address Table.

### Step 4: Enable the G0/1 interface.

Enable the G0/1 interface. Write the commands you used in the space provided.

```
R1(config)# interface g0/1
R1(config-if)# no shutdown
```

### Step 5: Verify connectivity.

Enter the command to view the routing table on R1. What networks are listed?

```
192.168.1.0, 192.168.10.0, 192.168.20.0, and 209.165.200.224
```

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

## Lab – Configuring 802.1Q Trunk-Based Inter-VLAN Routing

---

\* - candidate default, U - per-user static route, o - ODR  
P - periodic downloaded static route

Gateway of last resort is not set

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1.1
L 192.168.1.1/32 is directly connected, GigabitEthernet0/1.1
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/1.10
L 192.168.10.1/32 is directly connected, GigabitEthernet0/1.10
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/1.20
L 192.168.20.1/32 is directly connected, GigabitEthernet0/1.20
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.224/27 is directly connected, Loopback0
L 209.165.200.225/32 is directly connected, Loopback0
```

From PC-A, is it possible to ping the default gateway for VLAN 10? \_\_\_\_\_ Yes

From PC-A, is it possible to ping PC-B? \_\_\_\_\_ Yes

From PC-A, is it possible to ping Lo0? \_\_\_\_\_ Yes

From PC-A, is it possible to ping S2? \_\_\_\_\_ Yes

If the answer is **no** to any of these questions, troubleshoot the configurations and correct any errors.

### Reflection

What are the advantages of trunk-based or router-on-a-stick inter-VLAN routing?

---

---

Router-on-a-stick inter-VLAN routing allows for one interface to route to multiple VLANs unlike the legacy inter-VLAN method which requires one port per VLAN.

## Router Interface Summary Table

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

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

## Appendix A – Configuration Commands

### Switch S1

```
S1(config)# vlan 10
S1(config-vlan)# name Students
S1(config-vlan)# vlan 20
S1(config-vlan)# name Faculty
S1(config-vlan)# exit
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
```

### Switch S2

```
S2(config)# vlan 10
S2(config-vlan)# name Students
S2(config-vlan)# vlan 20
S2(config-vlan)# name Faculty
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```

## Lab – Configuring 802.1Q Trunk-Based Inter-VLAN Routing

---

```
S2(config-if)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
```

### Router R1

```
R1(config)# interface g0/1.1
R1(config-subif)# encapsulation dot1Q 1
R1(config-subif)# ip address 192.168.1.1 255.255.255.0
R1(config-subif)# interface g0/1.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# interface g0/1.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)# interface g0/1
R1(config-if)# no shutdown
```

### Device Configs

**Instructor Note:** The VLANs configured do not display in the switch running configuration but are stored in the `vlan.dat` file. The output from the `show vlan brief` command is provided.

### Router R1

```
R1# show run
Building configuration...

Current configuration : 1731 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGh01QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
!
!
!
```

## Lab – Configuring 802.1Q Trunk-Based Inter-VLAN Routing

## Lab – Configuring 802.1Q Trunk-Based Inter-VLAN Routing

---

```
!
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### Switch S1

```
S1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 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, Gi0/1, Gi0/2
10	Students	active	Fa0/6
20	Faculty	active	
1002	fdmi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdmynet-default	act/unsup	
1005	trnet-default	act/unsup	

```
S1# show run
```

```
Building configuration...
```

```
Current configuration : 1627 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!
!
```

## Lab – Configuring 802.1Q Trunk-Based Inter-VLAN Routing

---

```
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
switchport mode trunk
!
interface FastEthernet0/6
switchport access vlan 10
switchport mode access
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
```

## Lab – Configuring 802.1Q Trunk-Based Inter-VLAN Routing

---

```
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
!
```

```
line con 0
password cisco
logging synchronous
login
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
end
```

### Switch S2

```
S2# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/2, Fa0/3, Fa0/4, 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 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
10	Students	active	
20	Faculty	active	Fa0/18
1002	fdmi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdmynet-default	act/unsup	
1005	trnet-default	act/unsup	

```
S2# show run
```

```
Building configuration...
```

```
Current configuration : 1633 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
```

## Lab – Configuring 802.1Q Trunk-Based Inter-VLAN Routing

---

```
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
interface FastEthernet0/1
switchport mode trunk
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
shutdown
!
interface FastEthernet0/6
shutdown
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
```

## Lab – Configuring 802.1Q Trunk-Based Inter-VLAN Routing

---

```
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
switchport access vlan 20
switchport mode access
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
```

## Lab – Configuring 802.1Q Trunk-Based Inter-VLAN Routing

---

```
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
 ip address 192.168.1.12 255.255.255.0
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end
```



## The Inside Track (Instructor Version – Optional Lab)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

### Objective

Explain how Layer 3 switches forward data in a small- to medium-sized business LAN.

Students will choose which type of inter-VLAN routing they would prefer if designing a network for local area network communications.

### Scenario

Your company has just purchased a three-level building. You are the network administrator and must design the company inter-VLAN routing network scheme to serve a few employees on each floor.

Floor 1 is occupied by the HR Department, Floor 2 is occupied by the IT Department, and Floor 3 is occupied by the Sales Department. All Departments must be able to communicate with each other, but at the same time have their own separate working networks.

You brought three Cisco 2960 switches and a Cisco 1941 series router from the old office location to serve network connectivity in the new building. New equipment is non-negotiable.

Refer to the PDF for this activity for further instructions.

### Resources

- Software presentation program

### Directions

Work with a partner to complete this activity.

#### Step 1: Design your topology.

- a. Use one 2960 switch per floor of your new building.
- b. Assign one department to each switch.
- c. Pick one of the switches to connect to the 1941 series router.

#### Step 2: Plan the VLAN scheme.

- a. Devise VLAN names and numbers for the HR, IT, and Sales Departments.
- b. Include a management VLAN, possibly named Management or Native, numbered to your choosing.
- c. Use either IPv4 or v6 as your addressing scheme for the LANs. If using IPv4, you must also use VLSM.

#### Step 3: Design a graphic to show your VLAN design and address scheme.

#### Step 4: Choose your inter-VLAN routing method.

- a. Legacy (per interface)
- b. Router-on-a-Stick

- c. Multilayer switching

**Step 5: Create a presentation justifying your inter-VLAN routing method of choice.**

- a. No more than eight slides can be created for the presentation.
- b. Present your group's design to the class or to your instructor.
  - 1) Be able to explain the method you chose. What makes it different or more desirable to your business than the other two methods?
  - 2) Be able to show how data moves throughout your network. Verbally explain how the networks are able to communicate using your inter-VLAN method of choice.

**Instructor Resource Information**

- All students should be able to differentiate between the three inter-VLAN routing methods
- All students should be able to explain how they chose the method of inter-VLAN routing for their business
- All students should be able to explain how data flows on their chosen inter-VLAN routing method

**Identify elements of the model that map to IT-related content:**

- Legacy or per-interface inter-VLAN routing
- Router-on-a-Stick inter-VLAN routing
- Multi-layer switching inter-VLAN routing



## Permit Me to Assist You (Instructor Version – Optional Lab)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

### Objective

Explain the purpose and operation of ACLs.

Students will design a process for selecting a candidate for security clearance. Groups will be formed and “applicants” will be permitted or denied the job.

### Scenario

- Each individual in the class will record five questions they would ask a candidate who is applying for a security clearance for a network assistant position within a small- to medium-sized business. The list of questions should be listed in order of importance to selecting a good candidate for the job. The preferred answers will also be recorded.
- After three minutes of brainstorming the list of questions, the instructor will ask two students to serve as interviewers. These two students will use only their list of questions and answers for the next part of this activity. The instructor will explain to only the two interviewers that they have the discretion, at any time, to stop the process and state “you are all permitted to the next level of interviews” or “I am sorry, but you do not have the qualifications to continue to the next level of interviews.” The interviewer does not need to complete all of the questions on the list.
- The rest of the class will be split in half and assigned to one of the interviewers.
- Once everyone is settled into their group with an interviewer, the group application interviews will begin.
- The two selected interviewers will ask the first question on the list that they created; an example would be “are you over the age of 18?” If the applicant does not meet the age requirement, as specified by the interviewer’s original questions and answers, the applicant will be eliminated from the pool of applicants and must move to another area within the room where they will observe the rest of the application process.

At this point, or later in the process, instructors may wish to state: “You have 2 minutes to complete the interview process.” This is to provide time management to the activity.

The next question will then be asked by the interviewer. If applicants answer correctly, they may stay with the applicant group. The entire class will then get together and discuss their observations regarding the process to permit or deny them the opportunity to continue on to the next level of interviews.

### Reflection

1. What factors did you consider when devising your list of criteria for network assistant security clearance?

Answers will vary – age, experience, knowledge of networking, etc.

2. How difficult was it to devise five security questions to deliver during the interviews? Why were you asked to list your questions in order of importance to selecting a good candidate?

All of the students should mention that the most important qualifications should be listed first in order to eliminate those candidates who do not meet their criteria, quickly.

3. Why would the process of elimination be stopped, even if there were still a few applicants available?

## **Permit Me to Assist You**

---

---

Answers will vary, but the most likely answer would be to provide a pool of applicants who will be permitted or denied the opportunity to move to the next level of employment application process.

4. How could this scenario and the results be applied to network traffic?
- 

Some traffic can be permitted on networks, and some will be denied.

### **Packet Tracer Example (answers will vary)**

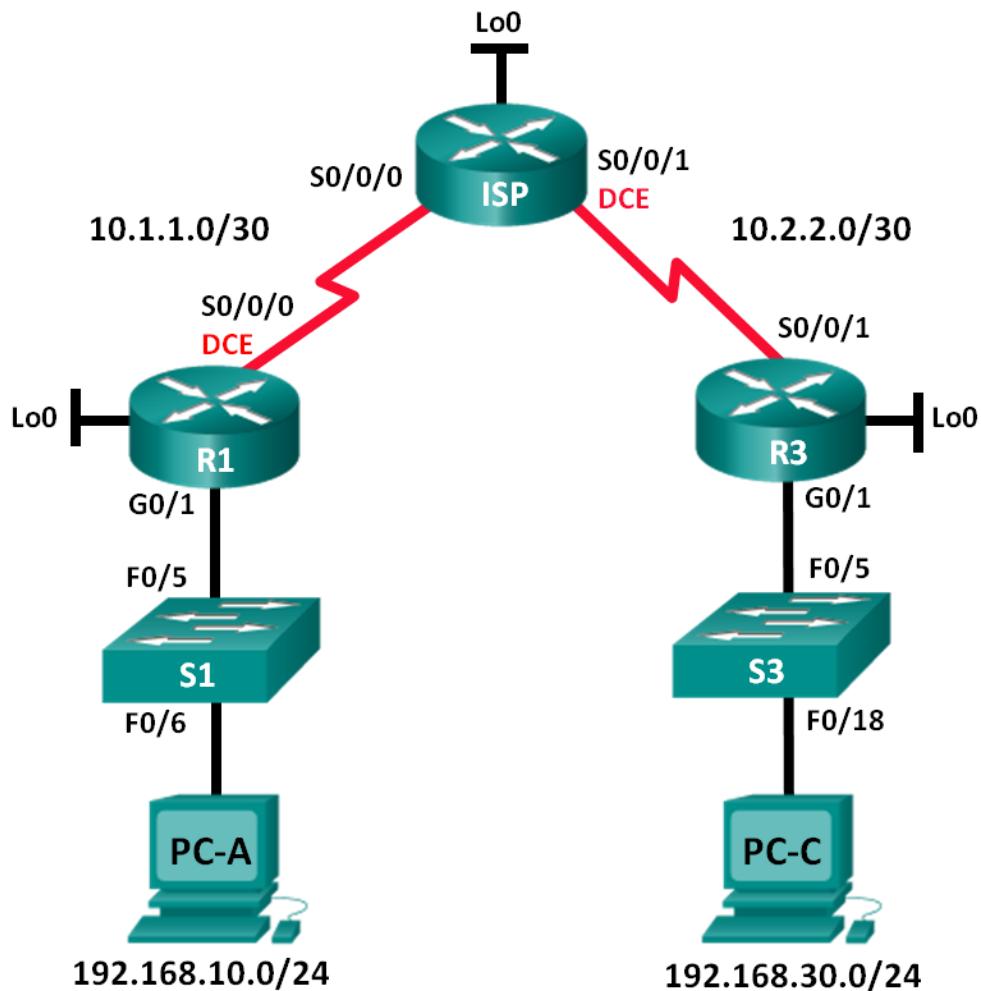
**Instructor Note:** Identify elements of the model that map to IT-related content:

- ACLs are processes that determine desirable and undesirable network traffic.
- Criteria must be established in advance of permitting or denying network traffic.
- The order of importance must be established when developing criteria for permitting or denying network participation.
- At the end of the process, more than one host may be denied or permitted network participation, based on the criteria specified.

## Lab – Configuring and Verifying Standard IPv4 ACLs (Instructor Version – Optional Lab)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

### Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

## Objectives

### Part 1: Set Up the Topology and Initialize Devices

- Set up equipment to match the network topology.
- Initialize and reload the routers and switches.

### Part 2: Configure Devices and Verify Connectivity

- Assign a static IP address to PCs.
- Configure basic settings on routers.
- Configure basic settings on switches.
- Configure RIP routing on R1, ISP, and R3.
- Verify connectivity between devices.

### Part 3: Configure and Verify Standard Numbered and Named ACLs

- Configure, apply, and verify a numbered standard ACL.
- Configure, apply, and verify a named ACL.

### Part 4: Modify a Standard ACL

- Modify and verify a named standard ACL.
- Test the ACL.

## Background / Scenario

Network security is an important issue when designing and managing IP networks. The ability to configure proper rules to filter packets, based on established security policies, is a valuable skill.

## Lab – Configuring and Verifying Standard IPv4 ACLs

---

In this lab, you will set up filtering rules for two offices represented by R1 and R3. Management has established some access policies between the LANs located at R1 and R3, which you must implement. The ISP router sitting between R1 and R3 will not have any ACLs placed on it. You would not be allowed any administrative access to an ISP router because you can only control and manage your own equipment.

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

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

**Instructor Note:** Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

### Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

### Part 1: Set Up the Topology and Initialize Devices

In Part 1, you set up the network topology and clear any configurations, if necessary.

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

**Step 2: Initialize and reload the routers and switches.**

### Part 2: Configure Devices and Verify Connectivity

In Part 2, you configure basic settings on the routers, switches, and PCs. Refer to the Topology and Addressing Table for device names and address information.

**Step 1: Configure IP addresses on PC-A and PC-C.**

**Step 2: Configure basic settings for the routers.**

- a. Console into the router and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
```

```
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. Configure the device name as shown in the topology.
- d. Create loopback interfaces on each router as shown in the Addressing Table.
- e. Configure interface IP addresses as shown in the Topology and Addressing Table.
- f. Assign a clock rate of **128000** to the DCE serial interfaces.
- g. Enable Telnet access.
- h. Copy the running configuration to the startup configuration.

### Step 3: (Optional) Configure basic settings on the switches.

- a. Console into the switch and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the switch.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

- c. Configure the device name as shown in the topology.
- d. Configure the management interface IP address as shown in the Topology and Addressing Table.
- e. Configure a default gateway.
- f. Enable Telnet access.
- g. Copy the running configuration to the startup configuration.

### Step 4: Configure Rip routing on R1, ISP, and R3.

- a. Configure RIP version 2 and advertise all networks on R1, ISP, and R3. The RIP configuration for R1 and ISP is included for reference.

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.10.0
R1(config-router)# network 192.168.20.0
R1(config-router)# network 10.1.1.0
```

```
ISP(config)# router rip
ISP(config-router)# version 2
ISP(config-router)# network 209.165.200.224
ISP(config-router)# network 10.1.1.0
ISP(config-router)# network 10.2.2.0
```

```
R3(config)# router RIP
R1(config-router)# version 2
R3(config-router)# network 192.168.30.0
R3(config-router)# network 192.168.40.0
R3(config-router)# network 10.2.2.0
```

- b. After configuring Rip on R1, ISP, and R3, verify that all routers have complete routing tables, listing all networks. Troubleshoot if this is not the case.

### Step 5: Verify connectivity between devices.

**Note:** It is very important to test whether connectivity is working **before** you configure and apply access lists! You want to ensure that your network is properly functioning before you start to filter traffic.

- From PC-A, ping PC-C and the loopback interface on R3. Were your pings successful? \_\_\_\_\_ Yes
- From R1, ping PC-C and the loopback interface on R3. Were your pings successful? \_\_\_\_\_ Yes
- From PC-C, ping PC-A and the loopback interface on R1. Were your pings successful? \_\_\_\_\_ Yes
- From R3, ping PC-A and the loopback interface on R1. Were your pings successful? \_\_\_\_\_ Yes

## Part 3: Configure and Verify Standard Numbered and Named ACLs

### Step 1: Configure a numbered standard ACL.

Standard ACLs filter traffic based on the source IP address only. A typical best practice for standard ACLs is to configure and apply it as close to the destination as possible. For the first access list, create a standard numbered ACL that allows traffic from all hosts on the 192.168.10.0/24 network and all hosts on the 192.168.20.0/24 network to access all hosts on the 192.168.30.0/24 network. The security policy also states that a **deny any** access control entry (ACE), also referred to as an ACL statement, should be present at the end of all ACLs.

What wildcard mask would you use to allow all hosts on the 192.168.10.0/24 network to access the 192.168.30.0/24 network?

\_\_\_\_\_ 0.0.0.255

Following Cisco's recommended best practices, on which router would you place this ACL? \_\_\_\_\_ R3

On which interface would you place this ACL? In what direction would you apply it?

G0/1. The ACL should be applied going out. Students may answer with placing the ACL on the S0/0/1 interface on R3 going **in**. Emphasize to them that this would effectively block the LANs on R1 from getting to the 192.168.40.0/24 network as well!

- Configure the ACL on R3. Use 1 for the access list number.

```
R3(config)# access-list 1 remark Allow R1 LANs Access
```

## Lab – Configuring and Verifying Standard IPv4 ACLs

---

```
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255
R3(config)# access-list 1 deny any
```

- b. Apply the ACL to the appropriate interface in the proper direction.

```
R3(config)# interface g0/1
R3(config-if)# ip access-group 1 out
```

- c. Verify a numbered ACL.

The use of various **show** commands can aid you in verifying both the syntax and placement of your ACLs in your router.

To see access list 1 in its entirety with all ACEs, which command would you use?

---

```
R3# show access-lists 1
```

or

```
R3# show access-lists
```

What command would you use to see where the access list was applied and in what direction?

---

```
R3# show ip interface g0/1
```

or

```
R3# show ip interface
```

- 1) On R3, issue the **show access-lists 1** command.

```
R3# show access-list 1
Standard IP access list 1
 10 permit 192.168.10.0, wildcard bits 0.0.0.255
 20 permit 192.168.20.0, wildcard bits 0.0.0.255
 30 deny any
```

- 2) On R3, issue the **show ip interface g0/1** command.

```
R3# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
 Internet address is 192.168.30.1/24
 Broadcast address is 255.255.255.255
 Address determined by non-volatile memory
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.10
 Outgoing access list is 1
 Inbound access list is not set
 Output omitted
```

- 3) Test the ACL to see if it allows traffic from the 192.168.10.0/24 network access to the 192.168.30.0/24 network. From the PC-A command prompt, ping the PC-C IP address. Were the pings successful? \_\_\_\_\_ Yes

## Lab – Configuring and Verifying Standard IPv4 ACLs

---

- 4) Test the ACL to see if it allows traffic from the 192.168.20.0/24 network access to the 192.168.30.0/24 network. You must do an extended ping and use the loopback 0 address on R1 as your source. Ping PC-C's IP address. Were the pings successful? \_\_\_\_\_ Yes

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.30.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.20.1
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 192.168.30.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

- d. From the R1 prompt, ping PC-C's IP address again.

```
R1# ping 192.168.30.3
```

Was the ping successful? Why or why not?

---

---

---

No, the pings failed. When you ping from the router, it uses the closest interface to the destination as its source address. The pings had a source address of 10.1.1.1. The access list on R3 only allows the 192.168.10.0/24 and the 192.168.20.0/24 networks access.

### Step 2: Configure a named standard ACL.

Create a named standard ACL that conforms to the following policy: allow traffic from all hosts on the 192.168.40.0/24 network access to all hosts on the 192.168.10.0/24 network. Also, only allow host PC-C access to the 192.168.10.0/24 network. The name of this access list should be called BRANCH-OFFICE-POLICY.

Following Cisco's recommended best practices, on which router would you place this ACL? \_\_\_\_\_ R1

On which interface would you place this ACL? In what direction would you apply it?

---

G0/1. The ACL should be applied going out. Students may answer with placing the ACL on the S0/0/0 interface on R1 going in. Emphasize to them that this would effectively block all traffic from the LANs on R3 from getting to the 192.168.20.0/24 network.

- a. Create the standard named ACL BRANCH-OFFICE-POLICY on R1.

## Lab – Configuring and Verifying Standard IPv4 ACLs

---

```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# permit host 192.168.30.3
R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255
R1(config-std-nacl)# end
R1#
*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console
```

Looking at the first permit ACE in the access list, what is another way to write this?

---

```
R1(config-std-nacl)# permit 192.168.30.3 0.0.0.0
```

- b. Apply the ACL to the appropriate interface in the proper direction.

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out
```

- c. Verify a named ACL.

- 1) On R1, issue the **show access-lists** command.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
 10 permit 192.168.30.3
 20 permit 192.168.40.0, wildcard bits 0.0.0.255
```

Is there any difference between this ACL on R1 with the ACL on R3? If so, what is it?

---

---

---

---

---

---

Although there is no line 30 with a **deny any** on R1, it is implied. You may wish to emphasize this to your students. Having them actually configure the **deny any** ACE is a good practice and reinforces the concept as it shows up in the ACL when issuing a **show access-lists** command. It is easy to forget the implicit **deny any** when troubleshooting ACLs. This could easily result in traffic being denied that should have been allowed.

- 2) On R1, issue the **show ip interface g0/1** command.

```
R1# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
 Internet address is 192.168.10.1/24
 Broadcast address is 255.255.255.255
 Address determined by non-volatile memory
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Multicast reserved groups joined: 224.0.0.10
 Outgoing access list is BRANCH-OFFICE-POLICY
 Inbound access list is not set
<Output omitted>
```

## Lab – Configuring and Verifying Standard IPv4 ACLs

---

- 3) Test the ACL. From the command prompt on PC-C, ping PC-A's IP address. Were the pings successful? \_\_\_\_\_ **Yes**
- 4) Test the ACL to ensure that only the PC-C host is allowed access to the 192.168.10.0/24 network. You must do an extended ping and use the G0/1 address on R3 as your source. Ping PC-A's IP address. Were the pings successful? \_\_\_\_\_ **No**

```
R3# ping
Protocol [ip]:
Target IP address: 192.168.10.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.30.1
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 192.168.10.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.1
U.U.U
```

- 5) Test the ACL to see if it allows traffic from the 192.168.40.0/24 network access to the 192.168.10.0/24 network. You must perform an extended ping and use the loopback 0 address on R3 as your source. Ping PC-A's IP address. Were the pings successful? \_\_\_\_\_ **Yes**

```
R3# ping
Protocol [ip]:
Target IP address: 192.168.10.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.40.1
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 192.168.10.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.40.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/40/60 ms
```

## Part 4: Modify a Standard ACL

It is common in business for security policies to change. For this reason, ACLs may need to be modified. In Part 4, you will change one of the previous ACLs you configured to match a new management policy being put in place.

Management has decided that users from the 209.165.200.224/27 network should be allowed full access to the 192.168.10.0/24 network. Management also wants ACLs on all of their routers to follow consistent rules. A **deny any** ACE should be placed at the end of all ACLs. You must modify the BRANCH-OFFICE-POLICY ACL.

You will add two additional lines to this ACL. There are two ways you could do this:

**OPTION 1:** Issue a **no ip access-list standard BRANCH-OFFICE-POLICY** command in global configuration mode. This would effectively take the whole ACL out of the router. Depending upon the router IOS, one of the following scenarios would occur: all filtering of packets would be cancelled and all packets would be allowed through the router; or, because you did not take off the **ip access-group** command on the G0/1 interface, filtering is still in place. Regardless, when the ACL is gone, you could retype the whole ACL, or cut and paste it in from a text editor.

**OPTION 2:** You can modify ACLs in place by adding or deleting specific lines within the ACL itself. This can come in handy, especially with ACLs that have many lines of code. The retying of the whole ACL or cutting and pasting can easily lead to errors. Modifying specific lines within the ACL is easily accomplished.

**Note:** For this lab, use Option 2.

### Step 1: Modify a named standard ACL.

- From R1 privileged EXEC mode, issue a **show access-lists** command.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
 10 permit 192.168.30.3 (8 matches)
 20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
```

- Add two additional lines at the end of the ACL. From global config mode, modify the ACL, BRANCH-OFFICE-POLICY.

```
R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31
R1(config-std-nacl)# 40 deny any
R1(config-std-nacl)# end
```

- Verify the ACL.

- On R1, issue the **show access-lists** command.

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
 10 permit 192.168.30.3 (8 matches)
 20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
 30 permit 209.165.200.224, wildcard bits 0.0.0.31
 40 deny any
```

Do you have to apply the BRANCH-OFFICE-POLICY to the G0/1 interface on R1?

---

No, the **ip access-group BRANCH-OFFICE-POLICY out** command is still in place on G0/1.

## Lab – Configuring and Verifying Standard IPv4 ACLs

---

- 2) From the ISP command prompt, issue an extended ping. Test the ACL to see if it allows traffic from the 209.165.200.224/27 network access to the 192.168.10.0/24 network. You must do an extended ping and use the loopback 0 address on ISP as your source. Ping PC-A's IP address. Were the pings successful? \_\_\_\_\_ Yes

### Reflection

1. As you can see, standard ACLs are very powerful and work quite well. Why would you ever have the need for using extended ACLs?

---

---

---

Standard ACLs can only filter based on the source address. Also, they are not granular. They allow or deny EVERYTHING (protocols and services). Extended ACLs, while harder to write, are well-suited to complex networks where you may need to allow only certain ports access to networks while denying others.

2. Typically, more typing is required when using a named ACL as opposed to a numbered ACL. Why would you choose named ACLs over numbered?

---

---

---

Students could list two reasons here. The first reason is that using named ACLs gives you the ability to modify specific lines within the ACL itself, without retyping the whole thing. NOTE: Newer versions of the IOS allows numbered ACLs to be modified just like named ACLs. Secondly, having a named ACL is a good best practice as it helps to document the purpose of the ACL with a descriptive name.

## Router Interface Summary Table

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

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

## Device Configs

### Router R1

```
R1#sh run
Building configuration...

Current configuration : 1590 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrbp4RFmfqY
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
```

## Lab – Configuring and Verifying Standard IPv4 ACLs

---

```
!
interface Loopback0
 ip address 192.168.20.1 255.255.255.0
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 ip access-group BRANCH-OFFICE-POLICY out
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 128000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 128000
!
!
router rip
 version 2
 network 10.1.1.0
 network 192.168.10.0
 network 192.168.20.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ip access-list standard BRANCH-OFFICE-POLICY
 permit 192.168.30.3
 permit 192.168.40.0 0.0.0.255
 permit 209.165.200.224 0.0.0.31
 deny any

control-plane
!
!
!
line con 0
```

```
line aux 0
line vty 0 4
password class
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### Router R3

```
R3#sh run
Building configuration...

Current configuration : 1506 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrbp4RFmfqY
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
interface Loopback0
 ip address 192.168.40.1 255.255.255.0
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 ip access-group 1 out
 duplex auto
 speed auto
!
```

## Lab – Configuring and Verifying Standard IPv4 ACLs

---

```
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
ip address 10.2.2.1 255.255.255.252
!
!
router rip
version 2
network 10.2.2.0
network 192.168.30.0
network 192.168.40.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
access-list 1 remark Allow R1 LANs Access
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
access-list 1 deny any
!
control-plane
!
line con 0
line aux 0
line vty 0 4
password class
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### Router ISP

```
ISP#sh run
Building configuration...

Current configuration : 1313 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encrypt
```

## Lab – Configuring and Verifying Standard IPv4 ACLs

---

```
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrb4RFmfqY
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 clock rate 128000
!
router rip
 version 2
 network 10.1.1.0
 network 10.2.2.0
 network 209.165.200.224
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
```

```
control-plane
!
line con 0
line aux 0
line vty 0 4
password class
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### Switch S1

```
S1# show run
Building configuration...

Current configuration : 2990 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrb4RFmfqY
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!<output omitted>
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.10.11 255.255.255.0
!
```

```
ip default-gateway 192.168.10.1
ip http server
ip http secure-server
!
!
line con 0
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
end
```

### Switch S3

```
S3# show start
Using 1696 out of 65536 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S3
!
boot-start-marker
boot-end-marker
!
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrb4RFmfqY
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!<output omitted>
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.30.11 255.255.255.0
!
```

## Lab – Configuring and Verifying Standard IPv4 ACLs

---

```
ip default-gateway 192.168.30.1
ip http server
ip http secure-server
!
!
line con 0
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
end
```

## Lab – Configuring and Verifying VTY Restrictions (Instructor Version – Optional Lab)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

### Topology



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

### Objectives

- Part 1: Configure Basic Device Settings
- Part 2: Configure and Apply the Access Control List on R1
- Part 3: Verify the Access Control List Using Telnet
- Part 4: Challenge - Configure and Apply the Access Control List on S1

### Background / Scenario

It is a good practice to restrict access to the router management interfaces, such as the console and vty lines. An access control list (ACL) can be used to allow access for specific IP addresses, ensuring that only the administrator PCs have permission to telnet or SSH into the router.

**Note:** In the Cisco device outputs, ACL is abbreviated as access-list.

In this lab, you will create and apply a named standard ACL to restrict remote access to the router vty lines.

After the ACL has been created and applied, you will test and verify the ACL by accessing the router from different IP addresses using Telnet.

This lab will provide the commands necessary for creating and applying the ACL.

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

## Lab – Configuring and Verifying VTY Restrictions

---

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

**Instructor Note:** Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

### Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

**Note:** The Gigabit Ethernet interfaces on Cisco 1941 routers are autosensing and an Ethernet straight-through cable may be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

### Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the interface IP addresses, device access, and passwords on the router.

**Step 1: Cable the network as shown in the topology diagram.**

**Step 2: Configure the PC-A and PC-B network settings according to the Addressing Table.**

**Step 3: Initialize and reload the router and switch.**

- a. Console into the router and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. Configure IP addresses on the interfaces listed in the Addressing Table.
- d. Save the running configuration to the startup configuration file.
- e. Console into the switch and enter global configuration mode.
- f. Copy the following basic configuration and paste it to the running-configuration on the switch.

```
no ip domain-lookup
```

```
hostname S1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

- g. Configure IP address on VLAN1 interface listed in the Addressing Table.
  - h. Configure the default gateway for the switch.
  - i. Save the running configuration to the startup configuration file.

## Part 2: Configure and Apply the Access Control List on R1

In Part 2, you will configure a named standard ACL and apply it to the router virtual terminal lines to restrict remote access to the router.

### **Step 1: Configure and apply a standard named ACL.**

- a. Console into the router R1 and enable privileged EXEC mode.
  - b. From global configuration mode, view the command options under **ip access-list** by using a space and a question mark.

```
R1(config)# ip access-list ?
extended Extended Access List
helper Access List acts on helper-address
log-update Control access list log updates
logging Control access list logging
resequence Resequence Access List
standard Standard Access List
```

- c. View the command options under **ip access-list standard** by using a space and a question mark.

```
R1(config)# ip access-list standard ?
<1-99> Standard IP access-list number
<1300-1999> Standard IP access-list number (expanded range)
WORD Access-list name
```

- d. Add **ADMIN-MGT** to the end of the **ip access-list standard** command and press Enter. You are now in the standard named access-list configuration mode (config-std-nacl).

```
R1(config)# ip access-list standard ADMIN-MGT
R1(config-std-nacl)#
```

- e. Enter your ACL permit or deny access control entry (ACE), also known as an ACL statement, one line at a time. Remember that there is an implicit **deny any** at the end of the ACL, which effectively denies all traffic. Enter a question mark to view your command options.

## Lab – Configuring and Verifying VTY Restrictions

---

```
R1(config-std-nacl)# ?
Standard Access List configuration commands:
<1-2147483647> Sequence Number
default Set a command to its defaults
deny Specify packets to reject
exit Exit from access-list configuration mode
no Negate a command or set its defaults
permit Specify packets to forward
remark Access list entry comment
```

- f. Create a permit ACE for Administrator PC-A at 192.168.1.3 and an additional permit ACE to allow other reserved administrative IP addresses from 192.168.1.4 to 192.168.1.7. Notice how the first permit ACE signifies a single host by using the **host** keyword. The ACE **permit 192.168.1.3 0.0.0.0** could have been used instead. The second permit ACE allows hosts 192.168.1.4 through 192.168.1.7, by using the 0.0.0.3 wildcard, which is the inverse of a 255.255.255.252 subnet mask.

```
R1(config-std-nacl)# permit host 192.168.1.3
R1(config-std-nacl)# permit 192.168.1.4 0.0.0.3
R1(config-std-nacl)# exit
```

You do not need to enter a deny ACE because there is an implicit **deny any** ACE at the end of the ACL.

- g. Now that the named ACL is created, apply it to the vty lines.

```
R1(config)# line vty 0 15
R1(config-line)# access-class ADMIN-MGT in
R1(config-line)# exit
```

## Part 3: Verify the Access Control List Using Telnet

In Part 3, you will use Telnet to access the router, verifying that the named ACL is functioning correctly.

**Note:** SSH is more secure than Telnet; however, SSH requires that the network device be configured to accept SSH connections. Telnet is used with this lab for convenience.

- a. Open a command prompt on PC-A and verify that you can communicate with the router by issuing a **ping** command.

```
C:\Users\user1> ping 192.168.1.1
```

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
```

```
Ping statistics for 192.168.1.1:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\Users\user1>
```

- b. Using the command prompt on PC-A, launch the Telnet client program to telnet into the router. Enter the login and then the enable passwords. You should be successfully logged in, see the banner message, and receive an R1 router command prompt.

```
C:\Users\user1> telnet 192.168.1.1
```

## Lab – Configuring and Verifying VTY Restrictions

---

Unauthorized access is prohibited!

User Access Verification

Password:

R1>enable

Password:

R1#

Was the Telnet connection successful? \_\_\_\_\_

The Telnet connection should be successful, and the student should be prompted for a password from router R1.

- c. Type **exit** at the command prompt and press Enter to exit the Telnet session.
- d. Change your IP address to test if the named ACL blocks non-permitted IP addresses. Change the IPv4 address to 192.168.1.100 on PC-A.
- e. Attempt to telnet into R1 at 192.168.1.1 again. Was the Telnet session successful?

If the IP address on PC-A was changed, the Telnet connection should not be successful.

What message was received? \_\_\_\_\_

Connecting To 192.168.1.1...Could not open connection to the host, on port 23: Connect failed

- f. Change the IP address on PC-A to test if the named ACL permits a host with an IP address from the 192.168.1.4 to 192.168.1.7 range to telnet into the router. After changing the IP address on PC-A, open a Windows command prompt and attempt to telnet into router R1.

Was the Telnet session successful?

---

---

If the IP address on PC-A was changed to an address from 192.168.1.4 to 192.168.1.7, then the telnet connection should be successful.

- g. From privileged EXEC mode on R1, type the **show ip access-lists** command and press Enter. From the command output, notice how the Cisco IOS automatically assigns line numbers to the ACL ACEs in increments of 10 and shows the number of times each permit ACE has been successfully matched (in parenthesis).

```
R1# show ip access-lists
Standard IP access list ADMIN-MGT
 10 permit 192.168.1.3 (2 matches)
 20 permit 192.168.1.4, wildcard bits 0.0.0.3 (2 matches)
```

Because two successful Telnet connections to the router were established, and each Telnet session was initiated from an IP address that matches one of the permit ACEs, there are matches for each permit ACE.

Why do you think that there are two matches for each permit ACE when only one connection from each IP address was initiated?

---

---

## Lab – Configuring and Verifying VTY Restrictions

---

Answer will vary. The students may recognize that the two matches to the permit ACEs correspond to how the Telnet protocol operates while establishing the telnet connections. The fact that there are two matches per single connection refers to how many times control information is sent to the router generating a match to the router permit ACE.

How would you determine at what point the Telnet protocol causes the two matches during the Telnet connection?

---

---

Answers will vary. Students should recognize that a protocol analyzer like Wireshark, would allow them to capture and analyze the Telnet protocol packets, to determine when the ACL permit ACE matches are generated.

- h. On R1, enter into global configuration mode.
- i. Enter into access-list configuration mode for the ADMIN-MGT named access list and add a **deny any** ACE to the end of the access list.

```
R1(config)# ip access-list standard ADMIN-MGT
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
```

**Note:** Because there is an implicit **deny any** ACE at the end of all ACLs, adding an explicit **deny any** ACE is unnecessary. However, the explicit deny any at the end of the ACL is can still be useful to the network administrator to log or simply know how many times the **deny any** access-list ACE was matched.

- j. Try to telnet from PC-B to R1. This creates a match to the **deny any** ACE in the ADMIN-MGT named access list.
- k. From privileged EXEC mode, type **show ip access-lists** command and press Enter. You should now see multiple matches to the **deny any** ACE.

```
R1# show ip access-lists
Standard IP access list ADMIN-MGT
 10 permit 192.168.1.3 (2 matches)
 20 permit 192.168.1.4, wildcard bits 0.0.0.3 (2 matches)
 30 deny any (3 matches)
```

The failed Telnet connection produces more matches to the explicit deny ACE than a successful one. Why do you think this happens?

---

Answers may vary. Students may recognize that the Telnet protocol must make three attempts to create a Telnet session.

## Part 4: Challenge - Configure and Apply the Access Control List on S1

### Step 1: Configure and apply a standard named ACL for the vty lines on S1.

- a. Without referring back to the R1 configuration commands, try to configure the ACL on S1, allowing only the PC-A IP address.

## Lab – Configuring and Verifying VTY Restrictions

---

- b. Apply the ACL to the S1 vty lines. Remember that there are more vty lines on a switch than a router.

### Step 2: Test the vty ACL on S1.

Telnet from each of the PCs to verify that the vty ACL is working properly. You should be able to telnet to S1 from PC-A, but not from PC-B.

#### Reflection

1. As evidenced by the remote vty access, ACLs are powerful content filters that can be applied to more than just inbound and outbound network interfaces. What other ways might ACLs be applied?
- 
- 

Answers may vary. Students may recognize that ACLs can be applied to network applications like server applications as well.

2. Does an ACL applied to a vty remote management interface improve the security of Telnet connection? Does this make Telnet a more viable remote access management tool?
- 
- 

Answers may vary. Students should recognize that even though ACLs help restrict remote management access to network devices, they do nothing to encrypt the actual data that is sent over the network. If this information is captured or sniffed by a third party program on the network, then the network is not secure.

3. Why does it make sense to apply an ACL to vty lines instead of specific interfaces?
- 
- 

Answers may vary. Students should recognize that by applying the ACL to the logical vty lines, it does not make any difference what interface the Telnet or SSH request comes in on. The vty ACLs are interface independent. In addition, the vty ACL can be applied once instead of applying it to multiple interfaces.

**Router Interface Summary Table**

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

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

**Device Configs****Router R1**

Building configuration...

```
Current configuration : 1467 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAug.2
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
```

## Lab – Configuring and Verifying VTY Restrictions

---

```
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
ip address 192.168.0.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ip access-list standard ADMIN-MGT
permit 192.168.1.3
permit 192.168.1.4 0.0.0.3
deny any
!
control-plane
!
banner motd ^CNo unauthorized access allowed!^C
!
line con 0
password 7 070C285F4D06
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
```

## Lab – Configuring and Verifying VTY Restrictions

---

```
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
access-class ADMIN-MGT in
password 7 13061E010803
logging synchronous
login
transport input all
line vty 5 15
access-class ADMIN-MGT in
password 7 13061E010803
logging synchronous
login
!
scheduler allocate 20000 1000
!
end
```

### Switch S1

Building configuration...

```
Current configuration : 1782 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
```

## Lab – Configuring and Verifying VTY Restrictions

---

```
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
```

## Lab – Configuring and Verifying VTY Restrictions

---

```
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
ip access-list standard ADMIN-MGT
 permit 192.168.1.3
!
banner motd ^CNo unauthorized access allowed!^C
!
line con 0
 password 7 01100F175804
 logging synchronous
 login
line vty 0 4
 access-class ADMIN-MGT in
 password 7 01100F175804
 logging synchronous
 login
line vty 5 14
 access-class ADMIN-MGT in
 password 7 01100F175804
 logging synchronous
 login
line vty 15
 password 7 0822455D0A16
 login
!
end
```



## FTP Denied (Instructor Version – Optional Lab)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

### Objective

Implement packet filtering using extended IPv4 ACLs according to networking requirements (to include named and numbered ACLs).

Students will use Packet Tracer to write and apply an ACL to deny a particular host from accessing the FTP process on their small- to medium-size business network.

### Scenario

It was recently reported that viruses are on the rise within your small- to medium-sized business network. Your network administrator has been tracking network performance and has determined that one particular host is constantly downloading files from a remote FTP server. This host just may be the virus source perpetuating throughout the network!

Use Packet Tracer to complete this activity. Write a named ACL to deny the host access to the FTP server. Apply the ACL to the most effective interface on the router.

To complete the physical topology, you must use:

- One PC host station
- Two switches
- One Cisco 1941 series Integrated Services Router
- One server

Using the Packet Tracer text tool, record the ACL you prepared. Validate that the ACL works to deny access to the FTP server by trying to access the FTP server's address. Observe what happens while in simulation mode. Save your file and be prepared to share it with another student, or with the entire class. (**Instructor choice**)

### Reflection

1. What was the most difficult part of completing this modeling activity?

---

Answers will vary – writing the ACL, naming it, applying it, changing it, etc.

2. How often do you think network administrators need to change their ACLs on their networks?

---

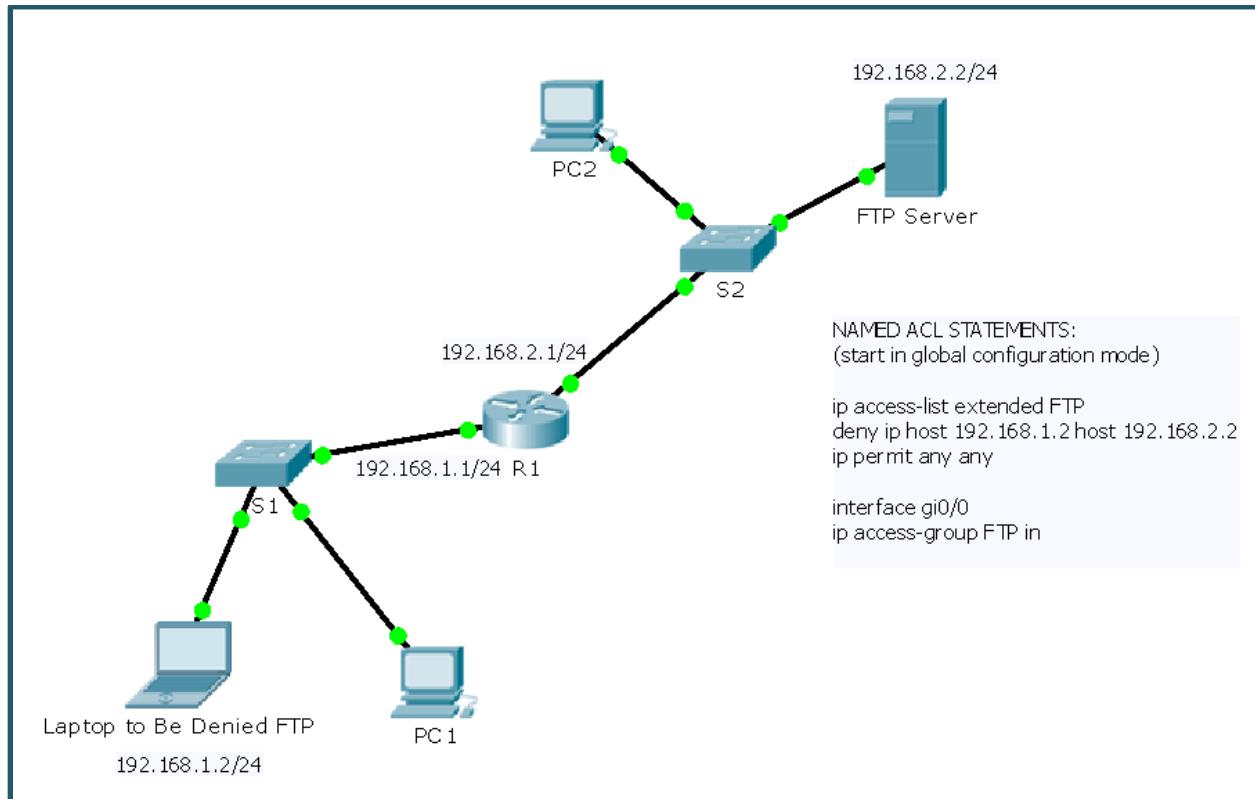
ACLs are implemented to address security issues, regulate network traffic, and provide stability to the operation of a network. Therefore, any time network performance, security and stability degrade, ACLs should be considered as one way to mitigate those network challenges.

3. Why would you consider using a named extended ACL instead of a regular extended ACL?

---

Named ACLs are easy to correct or change – you can edit the ACL statements by line and use the “no...” command. This saves time in having to rewrite and reapply an entire ACL to a network.

### Packet Tracer Example (topology, ACL names and IP addresses will vary)



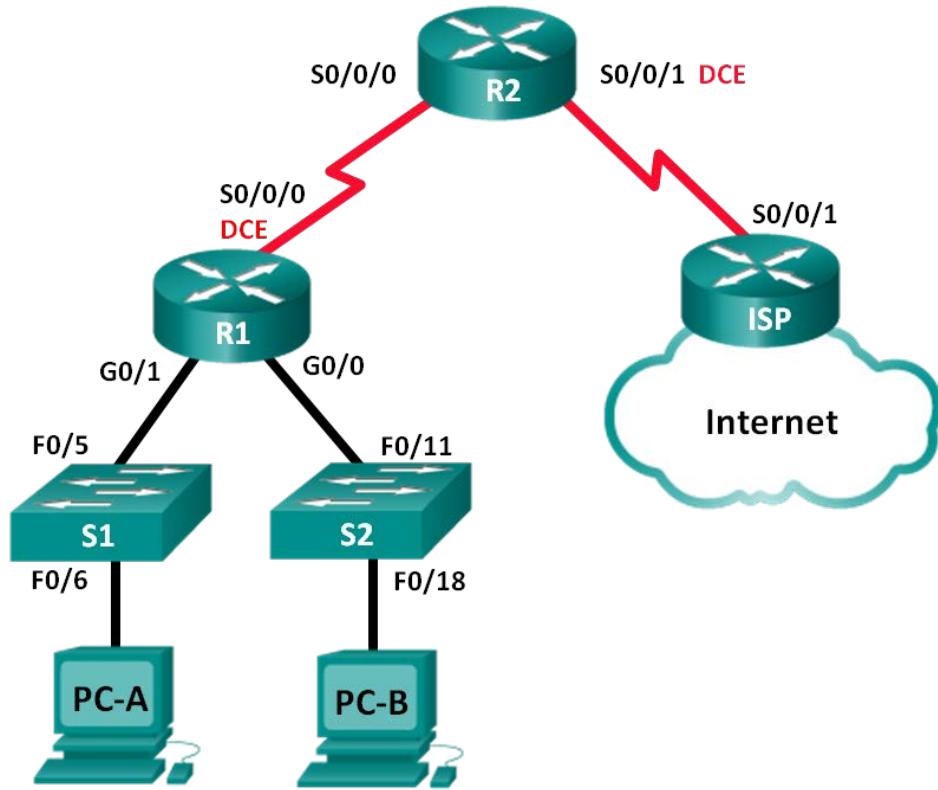
**Instructor Note:** Identify elements of the model that map to IT-related content:

- ACLs are processes that determine whether to permit or deny network traffic.
- Criteria must be established in advance of permitting or denying network traffic.
- The order of importance must be established when developing criteria for permitting or denying network participation.
- A named ACL saves time vs. using a regular extended or standard ACL if when corrections must be made to the configuration of the ACL or to its placement.
- ACLs must be tested for the validity of their operation, as an ACL may need to be rewritten and/or reapplied correctly if it does not work correctly.

## Lab - Configuring Basic DHCPv4 on a Router (Instructor Version)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only.

### Topology



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.2.253	255.255.255.252	N/A
R2	S0/0/0	192.168.2.254	255.255.255.252	N/A
	S0/0/1 (DCE)	209.165.200.226	255.255.255.224	N/A
ISP	S0/0/1	209.165.200.225	255.255.255.224	N/A
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

### Objectives

**Part 1: Build the Network and Configure Basic Device Settings**

**Part 2: Configure a DHCPv4 Server and a DHCP Relay Agent**

## Background / Scenario

The Dynamic Host Configuration Protocol (DHCP) is a network protocol that lets network administrators manage and automate the assignment of IP addresses. Without DHCP, the administrator must manually assign and configure IP addresses, preferred DNS servers, and default gateways. As the network grows in size, this becomes an administrative problem when devices are moved from one internal network to another.

In this scenario, the company has grown in size, and the network administrators can no longer assign IP addresses to devices manually. Your job is to configure the R2 router to assign IPv4 addresses on two different subnets connected to router R1.

**Note:** This lab provides minimal assistance with the actual commands necessary to configure DHCP. However, the required commands are provided in Appendix A. Test your knowledge by trying to configure the devices without referring to the appendix.

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

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

**Instructor Note:** Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

## Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

## Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the routers and switches with basic settings, such as passwords and IP addresses. You will also configure the IP settings for the PCs in the topology.

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

**Step 2: Initialize and reload the routers and switches.**

**Step 3: Configure basic settings for each router.**

- a. Console into the router and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
```

```
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. Configure the host name as shown in the topology.
- d. Configure the IPv4 addresses on the router as shown in the topology.
- e. Set the DCE serial interfaces with a clock rate of 128000.

### Step 4: Configure dynamic, default, and static routing on the routers.

- a. Configure RIPv2 for R1.

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.0.0
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.2.252
R1(config-router)# no auto-summary
```

- b. Configure RIPv2 and a default route to the ISP on R2.

```
R2(config)# router rip
R1(config-router)# version 2
R2(config-router)# network 192.168.2.252
R2(config-router)# default-information originate
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

- c. Configure a summary static route on ISP to reach the networks on the R1 and R2 routers.

```
ISP(config)# ip route 192.168.0.0 255.255.252.0 209.165.200.226
```

- d. Copy the running configuration to the startup configuration.

### Step 5: Verify network connectivity between the routers.

If any pings between routers fail, correct the errors before proceeding to the next step. Use **show ip route** and **show ip interface brief** to locate possible issues.

### Step 6: Verify the host PCs are configured for DHCP.

## Part 2: Configure a DHCPv4 Server and a DHCP Relay Agent

To automatically assign address information on the network, you will configure R2 as a DHCPv4 server and R1 as a DHCP relay agent.

### Step 1: Configure DHCPv4 server settings on router R2.

On R2, you will configure a DHCP address pool for each of the R1 LANs. Use the pool name **R1G0** for the G0/0 LAN and **R1G1** for the G0/1 LAN. You will also configure the addresses to be excluded from the address pools. Best practice dictates that excluded addresses be configured first, to guarantee that they are not accidentally leased to other devices.

## Lab - Configuring Basic DHCPv4 on a Router

Exclude the first 9 addresses in each R1 LAN starting with .1. All other addresses should be available in the DHCP address pool. Make sure that each DHCP address pool includes a default gateway, the domain **ccna-lab.com**, a DNS server (209.165.200.225), and a lease time of 2 days.

On the lines below, write the commands necessary for configuring DHCP services on router R2, including the DHCP-excluded addresses and the DHCP address pools.

**Note:** The required commands for Part 2 are provided in Appendix A. Test your knowledge by trying to configure DHCP on R1 and R2 without referring to the appendix.

```
R2(config)# ip dhcp excluded-address 192.168.0.1 192.168.0.9
R2(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)# ip dhcp pool R1G1
R2(dhcp-config)# network 192.168.1.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.1.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
R2(dhcp-config)# exit
R2(config)# ip dhcp pool R1G0
R2(dhcp-config)# network 192.168.0.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.0.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
```

On PC-A or PC-B, open a command prompt and enter the **ipconfig /all** command. Did either of the host PCs receive an IP address from the DHCP server? Why?

## Lab - Configuring Basic DHCPv4 on a Router

---

The host computers will not have received IP addresses from the DHCP server at R2 until R1 is configured as a DHCP relay agent.

### Step 2: Configure R1 as a DHCP relay agent.

Configure IP helper addresses on R1 to forward all DHCP requests to the R2 DHCP server.

On the lines below, write the commands necessary to configure R1 as a DHCP relay agent for the R1 LANs.

---

---

---

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.2.254
R1(config-if)# exit
R1(config)# interface g0/1
R1(config-if)# ip helper-address 192.168.2.254
```

### Step 3: Record IP settings for PC-A and PC-B.

On PC-A and PC-B, issue the **ipconfig /all** command to verify that the PCs have received IP address information from the DHCP server on R2. Record the IP and MAC address for each PC.

---

Answers may vary.

Based on the DHCP pool that was configured on R2, what are the first available IP addresses that PC-A and PC-B can lease?

---

PC-B: 192.168.0.10, and PC-A: 192.168.1.10

### Step 4: Verify DHCP services and address leases on R2.

- On R2, enter the **show ip dhcp binding** command to view DHCP address leases.

```
R2# show ip dhcp binding
Bindings from all pools not associated with VRF:
 IP address Client-ID/ Lease expiration Type
 Hardware address/
 User name
 192.168.0.10 011c.c1de.91c3.5d Mar 13 2013 02:07 AM Automatic
 192.168.1.10 0100.2170.0c05.0c Mar 13 2013 02:09 AM Automatic
```

Along with the IP addresses that were leased, what other piece of useful client identification information is in the output?

---

The client hardware addresses identify the specific computers that have joined the network.

- On R2, enter the **show ip dhcp server statistics** command to view the DHCP pool statistics and message activity.

```
R2# show ip dhcp server statistics
Memory usage 42175
```

## Lab - Configuring Basic DHCPv4 on a Router

---

```
Address pools 2
Database agents 0
Automatic bindings 2
Manual bindings 0
Expired bindings 0
Malformed messages 0
Secure arp entries 0

Message Received
BOOTREQUEST 0
DHCPDISCOVER 2
DHCPREQUEST 2
DHCPDECLINE 0
DHCPRELEASE 0
DHCPINFORM 2

Message Sent
BOOTREPLY 0
DHCPOFFER 2
DHCPACK 4
DHCPNAK 0
```

How many types of DHCP messages are listed in the output?

---

Ten different types of DHCP messages are listed.

- c. On R2, enter the **show ip dhcp pool** command to view the DHCP pool settings.

```
R2# show ip dhcp pool
```

```
Pool R1G1 :
 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
 192.168.1.11 192.168.1.1 - 192.168.1.254 1

Pool R1G0 :
 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
 192.168.0.11 192.168.0.1 - 192.168.0.254 1
```

In the output of the **show ip dhcp pool** command, what does the current index refer to?

The next available address for leasing.

- d. On R2, enter the **show run | section dhcp** command to view the DHCP configuration in the running configuration.

```
R2# show run | section dhcp
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp excluded-address 192.168.1.1 192.168.1.9
ip dhcp pool R1G1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 domain-name ccna-lab.com
 dns-server 209.165.200.225
 lease 2
ip dhcp pool R1G0
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
 domain-name ccna-lab.com
 dns-server 209.165.200.225
 lease 2
```

- e. On R1, enter the **show run interface** command for interfaces G0/0 and G0/1 to view the DHCP relay configuration in the running configuration.

```
R1# show run interface g0/0
Building configuration...

Current configuration : 132 bytes
!
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.0
 ip helper-address 192.168.2.254
 duplex auto
 speed auto
end
```

```
R1# show run interface g0/1
Building configuration...

Current configuration : 132 bytes
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 192.168.2.254
 duplex auto
 speed auto
end
```

## Reflection

What do you think is the benefit of using DHCP relay agents instead of multiple routers acting as DHCP servers?

---

---

---

Having a separate router DHCP server for each subnet would add more complexity and decrease centralized management for the network. It would also require that each router work harder to manage its own DHCP addressing, in addition to the primary function of routing traffic. One DHCP server (router or computer) that is dedicated to the job is easier to manage and more centralized.

## Router Interface Summary Table

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

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

## Appendix A – DHCP Configuration Commands

### Router R1

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.2.254
R1(config-if)# exit
R1(config-if)# interface g0/1
R1(config-if)# ip helper-address 192.168.2.254
```

### Router R2

```
R2(config)# ip dhcp excluded-address 192.168.0.1 192.168.0.9
```

## Lab - Configuring Basic DHCPv4 on a Router

---

```
R2(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.9
R2(config)# ip dhcp pool R1G1
R2(dhcp-config)# network 192.168.1.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.1.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
R2(dhcp-config)# exit
R2(config)# ip dhcp pool R1G0
R2(dhcp-config)# network 192.168.0.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.0.1
R2(dhcp-config)# dns-server 209.165.200.225
R2(dhcp-config)# domain-name ccna-lab.com
R2(dhcp-config)# lease 2
```

### Device Configs

#### Router R1

```
R1# show run
Building configuration...

Current configuration : 1478 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.0
 ip helper-address 192.168.2.254
```

## Lab - Configuring Basic DHCPv4 on a Router

---

```
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
ip helper-address 192.168.2.254
duplex auto
speed auto
!
interface Serial0/0/0
ip address 192.168.2.253 255.255.255.252
clock rate 128000
!
interface Serial0/0/1
no ip address
shutdown!
!
router rip
version 2
network 192.168.0.0
network 192.168.1.0
network 192.168.2.252
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
```

```
!
end
```

## **Router R2**

```
R2# show run
Building configuration...

Current configuration : 1795 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp excluded-address 192.168.1.1 192.168.1.9
!
ip dhcp pool R1G1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 domain-name ccna-lab.com
 dns-server 209.165.200.225
 lease 2
!
ip dhcp pool R1G0
 network 192.168.0.0 255.255.255.0
 default-router 192.168.0.1
 domain-name ccna-lab.com
 dns-server 209.165.200.225
 lease 2
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
 no ip address
```

## Lab - Configuring Basic DHCPv4 on a Router

---

```
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
ip address 192.168.2.254 255.255.255.252
!
interface Serial0/0/1
ip address 209.165.200.226 255.255.255.224
clock rate 128000
!
!
router rip
version 2
network 192.168.2.252
default-information originate
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 209.165.200.225
!
control-plane
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
```

```
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### Router ISP

```
ISP# show run
Building configuration...

Current configuration : 1247 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 10
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
```

## Lab - Configuring Basic DHCPv4 on a Router

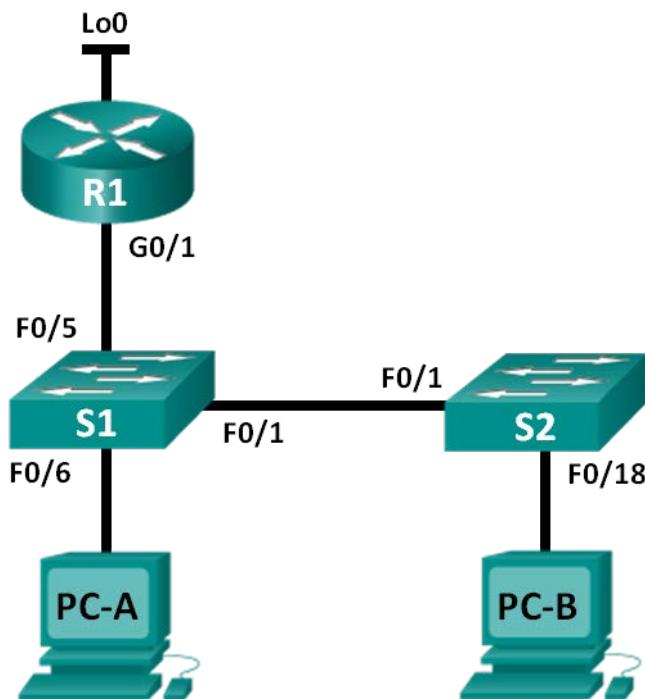
---

```
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
ip address 209.165.200.225 255.255.255.224
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 192.168.0.0 255.255.252.0 209.165.200.226
!
control-plane
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

## Lab – Configuring Basic DHCPv4 on a Switch (Instructor Version – Optional Lab)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

### Topology



### Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	G0/1	192.168.1.10	255.255.255.0
	Lo0	209.165.200.225	255.255.255.224
S1	VLAN 1	192.168.1.1	255.255.255.0
	VLAN 2	192.168.2.1	255.255.255.0

### Objectives

#### Part 1: Build the Network and Configure Basic Device Settings

#### Part 2: Change the SDM Preference

- Set the SDM preference to lanbase-routing on S1.

#### Part 3: Configure DHCPv4

- Configure DHCPv4 for VLAN 1.
- Verify DHCPv4 and connectivity.

### Part 4: Configure DHCP for Multiple VLANs

- Assign ports to VLAN 2.
- Configure DHCPv4 for VLAN 2.
- Verify DHCPv4 and connectivity.

### Part 5: Enable IP Routing

- Enable IP routing on the switch.
- Create static routes.

## Background / Scenario

A Cisco 2960 switch can function as a DHCPv4 server. The Cisco DHCPv4 server assigns and manages IPv4 addresses from identified address pools that are associated with specific VLANs and switch virtual interfaces (SVIs). The Cisco 2960 switch can also function as a Layer 3 device and route between VLANs and a limited number of static routes. In this lab, you will configure DHCPv4 for both single and multiple VLANs on a Cisco 2960 switch, enable routing on the switch to allow for communication between VLANs, and add static routes to allow for communication between all hosts.

**Note:** This lab provides minimal assistance with the actual commands necessary to configure DHCP. However, the required commands are provided in Appendix A. Test your knowledge by trying to configure the devices without referring to the appendix.

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

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

**Instructor Note:** Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

## Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

## Part 1: Build the Network and Configure Basic Device Settings

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

**Step 2: Initialize and reload the router and switches.**

**Step 3: Configure basic setting on devices.**

- a. Console into the router and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. Console into the switches and enter global configuration mode.
- d. Copy the following basic configuration and paste it to the running-configuration on the switches.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

- e. Assign device names as shown in the topology.
- f. Configure the IP addresses on R1 G0/1 and Lo0 interfaces, according to the Addressing Table.
- g. Configure the IP addresses on S1 VLAN 1 and VLAN 2 interfaces, according to the Addressing Table.
- h. Save the running configuration to the startup configuration file.

## Part 2: Change the SDM Preference

The Cisco Switch Database Manager (SDM) provides multiple templates for the Cisco 2960 switch. The templates can be enabled to support specific roles depending on how the switch is used in the network. In this lab, the sdm lanbase-routing template is enabled to allow the switch to route between VLANs and to support static routing.

### Step 1: Display the SDM preference on S1.

On S1, issue the **show sdm prefer** command in privileged EXEC mode. If the template has not been changed from the factory default, it should still be the **default** template. The **default** template does not support static routing. If IPv6 addressing has been enabled, the template will be **dual-ipv4-and-ipv6 default**.

```
S1# show sdm prefer
The current template is "default" template.
```

## Lab – Configuring Basic DHCPv4 on a Switch

---

The selected template optimizes the resources in the switch to support this level of features for 0 routed interfaces and 255 VLANs.

number of unicast mac addresses:	8K
number of IPv4 IGMP groups:	0.25K
number of IPv4/MAC qos aces:	0.125k
number of IPv4/MAC security aces:	0.375k

S1# **show sdm prefer**

The current template is "dual-ipv4-and-ipv6 default" template.  
The selected template optimizes the resources in the switch to support this level of features for 0 routed interfaces and 255 VLANs.

number of unicast mac addresses:	4K
number of IPv4 IGMP groups + multicast routes:	0.25K
number of IPv4 unicast routes:	0
number of IPv6 multicast groups:	0.375k
number of directly-connected IPv6 addresses:	0
number of indirect IPv6 unicast routes:	0
number of IPv4 policy based routing aces:	0
number of IPv4/MAC qos aces:	0.125k
number of IPv4/MAC security aces:	0.375k
number of IPv6 policy based routing aces:	0
number of IPv6 qos aces:	0.625k
number of IPv6 security aces:	125

S1# **show sdm prefer**

The current template is "lanbase-routing" template.  
The selected template optimizes the resources in the switch to support this level of features for 0 routed interfaces and 255 VLANs.

number of unicast mac addresses:	4K
number of IPv4 IGMP groups + multicast routes:	0.25K
number of IPv4 unicast routes:	0.75K
number of directly-connected IPv4 hosts:	0.75K
number of indirect IPv4 routes:	16
number of IPv6 multicast groups:	0.375k
number of directly-connected IPv6 addresses:	0.75K
number of indirect IPv6 unicast routes:	16
number of IPv4 policy based routing aces:	0
number of IPv4/MAC qos aces:	0.125k
number of IPv4/MAC security aces:	0.375k
number of IPv6 policy based routing aces:	0
number of IPv6 qos aces:	0.375k
number of IPv6 security aces:	127

## Lab – Configuring Basic DHCPv4 on a Switch

---

What is the current template?

---

Answers will vary. “default” or “dual-ipv4-and-ipv6 default” or “lanbase-routing”.

### Step 2: Change the SDM Preference on S1.

- Set the SDM preference to **lanbase-routing**. (If lanbase-routing is the current template, please proceed to Part 3.) From global configuration mode, issue the **sdm prefer lanbase-routing** command.

```
S1(config)# sdm prefer lanbase-routing
```

Changes to the running SDM preferences have been stored, but cannot take effect until the next reload.

Use 'show sdm prefer' to see what SDM preference is currently active.

```
S1# show sdm prefer
```

```
The current template is "default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.
```

```
number of unicast mac addresses: 8K
number of IPv4 IGMP groups: 0.25K
number of IPv4/MAC qos aces: 0.125k
number of IPv4/MAC security aces: 0.375k
```

On next reload, template will be "lanbase-routing" template.

Which template will be available after reload? \_\_\_\_\_ **lanbase-routing**

- The switch must be reloaded for the template to be enabled.

```
S1# reload
```

```
System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]
```

**Note:** The new template will be used after reboot even if the running configuration has not been saved. To save the running configuration, answer **yes** to save the modified system configuration.

### Step 3: Verify the lanbase-routing template is loaded.

Issue the **show sdm prefer** command to verify that the lanbase-routing template has been loaded on S1.

```
S1# show sdm prefer
```

```
The current template is "lanbase-routing" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.
```

```
number of unicast mac addresses: 4K
number of IPv4 IGMP groups + multicast routes: 0.25K
number of IPv4 unicast routes: 0.75K
 number of directly-connected IPv4 hosts: 0.75K
 number of indirect IPv4 routes: 16
number of IPv6 multicast groups: 0.375k
```

```
number of directly-connected IPv6 addresses: 0.75K
 number of indirect IPv6 unicast routes: 16
 number of IPv4 policy based routing aces: 0
 number of IPv4/MAC qos aces: 0.125k
 number of IPv4/MAC security aces: 0.375k
 number of IPv6 policy based routing aces: 0
 number of IPv6 qos aces: 0.375k
 number of IPv6 security aces: 127
```

## Part 3: Configure DHCPv4

In Part 3, you will configure DHCPv4 for VLAN 1, check IP settings on host computers to validate DHCP functionality, and verify connectivity for all devices in VLAN 1.

### Step 1: Configure DHCP for VLAN 1.

- Exclude the first 10 valid host addresses from network 192.168.1.0/24. Write the command you used in the space provided.

---

```
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

- Create a DHCP pool named **DHCP1**. Write the command you used in the space provided.

---

```
S1(config)# ip dhcp pool DHCP1
```

- Assign the network 192.168.1.0/24 for available addresses. Write the command you used in the space provided.

---

```
S1(dhcp-config)# network 192.168.1.0 255.255.255.0
```

- Assign the default gateway as 192.168.1.1. Write the command you used in the space provided.

---

```
S1(dhcp-config)# default-router 192.168.1.1
```

- Assign the DNS server as 192.168.1.9. Write the command you used in the space provided.

---

```
S1(dhcp-config)# dns-server 192.168.1.9
```

- Assign a lease time of 3 days. Write the command you used in the space provided.

---

```
S1(dhcp-config)# lease 3
```

- Save the running configuration to the startup configuration file.

### Step 2: Verify DHCP and connectivity.

- On PC-A and PC-B, open the command prompt and issue the **ipconfig** command. If IP information is not present, or if it is incomplete, issue the **ipconfig /release** command, followed by the **ipconfig /renew** command.

For PC-A, list the following:

IP Address: \_\_\_\_\_ **192.168.1.11**

## Lab – Configuring Basic DHCPv4 on a Switch

---

Subnet Mask: \_\_\_\_\_ **255.255.255.0**

Default Gateway: \_\_\_\_\_ **192.168.1.1**

For PC-B, list the following:

IP Address: \_\_\_\_\_ **192.168.1.12**

Subnet Mask: \_\_\_\_\_ **255.255.255.0**

Default Gateway: \_\_\_\_\_ **192.168.1.1**

- b. Test connectivity by pinging from PC-A to the default gateway, PC-B, and R1.

From PC-A, is it possible to ping the VLAN 1 default gateway? \_\_\_\_\_ **Yes**

From PC-A, is it possible to ping PC-B? \_\_\_\_\_ **Yes**

From PC-A, is it possible to ping R1 G0/1? \_\_\_\_\_ **Yes**

If the answer is no to any of these questions, troubleshoot the configurations and correct the error.

## Part 4: Configure DHCPv4 for Multiple VLANs

In Part 4, you will assign PC-A to a port accessing VLAN 2, configure DHCPv4 for VLAN 2, renew the IP configuration of PC-A to validate DHCPv4, and verify connectivity within the VLAN.

### Step 1: Assign a port to VLAN 2.

Place port F0/6 into VLAN 2. Write the command you used in the space provided.

---

---

```
S1(config)# interface f0/6
S1(config-if)# switchport access vlan 2
```

### Step 2: Configure DHCPv4 for VLAN 2

- a. Exclude the first 10 valid host addresses from network 192.168.2.0. Write the command you used in the space provided.
- 

```
S1(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10
```

- b. Create a DHCP pool named **DHCP2**. Write the command you used in the space provided.
- 

```
S1(config)# ip dhcp pool DHCP2
```

- c. Assign the network 192.168.2.0/24 for available addresses. Write the command you used in the space provided.
- 

```
S1(dhcp-config)# network 192.168.2.0 255.255.255.0
```

- d. Assign the default gateway as 192.168.2.1. Write the command you used in the space provided.
- 

```
S1(dhcp-config)# default-router 192.168.2.1
```

- e. Assign the DNS server as 192.168.2.9. Write the command you used in the space provided.
-

## Lab – Configuring Basic DHCPv4 on a Switch

---

---

```
S1(dhcp-config)# dns-server 192.168.2.9
```

- f. Assign a lease time of 3 days. Write the command you used in the space provided.
- 

```
S1(dhcp-config)# lease 3
```

- g. Save the running configuration to the startup configuration file.

### Step 3: Verify DHCPv4 and connectivity.

- a. On PC-A, open the command prompt and issue the **ipconfig /release** command, followed by **ipconfig /renew** command.

For PC-A, list the following:

IP Address: \_\_\_\_\_ **192.168.2.11**

Subnet Mask: \_\_\_\_\_ **255.255.255.0**

Default Gateway: \_\_\_\_\_ **192.168.2.1**

- b. Test connectivity by pinging from PC-A to the VLAN 2 default gateway and PC-B.

From PC-A, is it possible to ping the default gateway? \_\_\_\_\_ **Yes**

From PC-A, is it possible to ping PC-B? \_\_\_\_\_ **No**

Were these pings successful? Why?

---

---

Because the default gateway is in the same network as PC-A, PC-A can ping the default gateway. PC-B is in a different network; therefore, the ping from PC-A is not successful.

- c. Issue the **show ip route** command on S1.

```
S1# show ip route
Default gateway is not set
```

Host	Gateway	Last Use	Total Uses	Interface
ICMP redirect cache is empty				

What was the result of this command?

---

---

No default gateway has been set and no routing table is present on the switch.

---

## Part 5: Enable IP Routing

In Part 5, you will enable IP routing on the switch, which will allow for inter-VLAN communication. For all networks to communicate, static routes on S1 and R1 must be implemented.

### Step 1: Enable IP routing on S1.

- a. From global configuration mode, use the **ip routing** command to enable routing on S1.

```
S1(config)# ip routing
```

## Lab – Configuring Basic DHCPv4 on a Switch

---

- b. Verify inter-VLAN connectivity.

From PC-A, is it possible to ping PC-B? \_\_\_\_\_ **Yes**

What function is the switch performing?

---

The switch is routing between VLANs.

- c. View the routing table information for S1.

S1# **show ip route**

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

Gateway of last resort is not set

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Vlan1
L 192.168.1.1/32 is directly connected, Vlan1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Vlan2
L 192.168.2.1/32 is directly connected, Vlan2
```

What route information is contained in the output of this command?

---

---

The switch exhibits a routing table showing VLANs as directly connected networks 192.168.1.0/24 and 192.168.2.0/24.

- d. View the routing table information for R1.

R1# **show ip route**

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

Gateway of last resort is not set

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.10/32 is directly connected, GigabitEthernet0/1
```

## Lab – Configuring Basic DHCPv4 on a Switch

---

```
209.165.200.0/27 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.0/27 is directly connected, Loopback0
L 209.165.200.225/32 is directly connected, Loopback0
```

What route information is contained in the output of this command?

---

---

The router output shows directly connected networks of 192.168.1.0 and to 209.165.200.224 but has no entry for the 192.168.2.0 network.

e. From PC-A, is it possible to ping R1? \_\_\_\_\_ No

From PC-A, is it possible to ping Lo0? \_\_\_\_\_ No

Consider the routing table of the two devices, what must be added to communicate between all networks?

---

In order for communication to occur between all networks, routes must be added to the routing tables.

### Step 2: Assign static routes.

Enabling IP routing allows the switch to route between VLANs assigned on the switch. For all VLANs to communicate with the router, static routes must be added to the routing table of both the switch and the router.

a. On S1, create a default static route to R1. Write the command you used in the space provided.

---

```
S1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.10
```

b. On R1, create a static route to VLAN 2. Write the command you used in the space provided.

---

```
R1(config)# ip route 192.168.2.0 255.255.255.0 g0/1
```

c. View the routing table information for S1.

```
S1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
 + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.10 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 192.168.1.10
 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Vlan1
L 192.168.1.1/32 is directly connected, Vlan1
 192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Vlan2
```

Gateway of last resort is 192.168.1.10 to network 0.0.0.0

```
S* 0.0.0.0/0 [1/0] via 192.168.1.10
 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, Vlan1
L 192.168.1.1/32 is directly connected, Vlan1
 192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Vlan2
```

## Lab – Configuring Basic DHCPv4 on a Switch

---

L 192.168.2.1/32 is directly connected, Vlan2

How is the default static route represented?

---

Gateway of last resort is 192.168.1.10 to network 0.0.0.0

- d. View the routing table information for R1.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP, 1 - LISP
 + - replicated route, % - next hop override
```

Gateway of last resort is not set

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.10/32 is directly connected, GigabitEthernet0/1
S 192.168.2.0/24 is directly connected, GigabitEthernet0/1
 209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.165.200.0/27 is directly connected, Loopback0
L 209.165.200.225/32 is directly connected, Loopback0
```

How is the static route represented?

---

S 192.168.2.0/24 is directly connected, GigabitEthernet0/1

- e. From PC-A, is it possible to ping R1? \_\_\_\_\_ Yes

From PC-A, is it possible to ping Lo0? \_\_\_\_\_ Yes

## Reflection

1. In configuring DHCPv4, why would you exclude the static addresses prior to setting up the DHCPv4 pool?

---

---

If the static addresses were excluded after the DHCPv4 pool was created, a window of time exists where the excluded addresses could be given out dynamically to hosts.

2. If multiple DHCPv4 pools are present, how does the switch assign the IP information to hosts?

---

The switch will assign IP configurations based on the VLAN assignment of the port to which the host is connected.

3. Besides switching, what functions can the Cisco 2960 switch perform?

---

The switch can function as a DHCP server and can perform static and inter-VLAN routing.

## Router Interface Summary Table

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

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

## Appendix A: Configuration Commands

### Configure DHCPv4

```
S1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.10
S1(config)# ip dhcp pool DHCP1
S1(dhcp-config)# network 192.168.1.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.1.1
S1(dhcp-config)# dns-server 192.168.1.9
S1(dhcp-config)# lease 3
```

### Configure DHCPv4 for Multiple VLANs

```
S1(config)# interface f0/6
S1(config-if)# switchport access vlan 2
S1(config)# ip dhcp excluded-address 192.168.2.1 192.168.2.10
S1(config)# ip dhcp pool DHCP2
S1(dhcp-config)# network 192.168.2.0 255.255.255.0
S1(dhcp-config)# default-router 192.168.2.1
S1(dhcp-config)# dns-server 192.168.2.9
S1(dhcp-config)# lease 3
```

### Enable IP Routing

```
S1(config)# ip routing
S1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.10
R1(config)# ip route 192.168.2.0 255.255.255.0 g0/1
```

## Device Configs

### Router R1

```
R1#show run
Building configuration...

Current configuration : 1489 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.0
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

## Lab – Configuring Basic DHCPv4 on a Switch

---

```
interface GigabitEthernet0/1
 ip address 192.168.1.10 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 192.168.2.0 255.255.255.0 GigabitEthernet0/1
!
!
!
!
control-plane
!
!
!
line con 0
 password cisco
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password cisco
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

### Switch S1

```
S1#show run
Building configuration...

Current configuration : 3636 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGh01QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
ip routing
ip dhcp excluded-address 192.168.1.1 192.168.1.10
ip dhcp excluded-address 192.168.2.1 192.168.2.10
!
ip dhcp pool DHCP1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 dns-server 192.168.1.9
 lease 3
!
ip dhcp pool DHCP2
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
 dns-server 192.168.2.9
 lease 3
!
!
no ip domain-lookup
!
!
crypto pki trustpoint TP-self-signed-2531409152
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2531409152
 revocation-check none
 rsakeypair TP-self-signed-2531409152
!
!
crypto pki certificate chain TP-self-signed-2531409152
```

## Lab – Configuring Basic DHCPv4 on a Switch

---

```
certificate self-signed 01
3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 32353331 34303931 3532301E 170D3933 30333031 30303030
35365A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 35333134
30393135 3230819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100CA1B 27DE634E CF9FE284 C86127EF 41E7A52F 0A82FA2B 7C5448B7 184EA1AB
C22510E1 38A742BC D9F416FD 93A52DC6 BA77A928 B317DA75 1B3E2C66 C2D9061B
806132D9 E3189012 467C7A2C DCAC3EF4 4C419338 790AA98B C7A81D73 8621536C
4A90659E 267BA2E3 36F801A4 F06BEC65 386A40DA 255D9790 F9412706 9E73A660
45230203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
551D2304 18301680 14A7356A D364AE65 E1E9D42F 9B059B27 B69BB9C6 FD301D06
03551D0E 04160414 A7356AD3 64AE65E1 E9D42F9B 059B27B6 9BB9C6FD 300D0609
2A864886 F70D0101 05050003 8181002A D78919E7 0D75567C EF60036C 6C4B051A
2ABC5B9C DA1C1E48 AF33C405 5C64E074 B954C5B5 D825BE61 7340C695 03049797
D869E516 3936D0EC C871F140 66A1DEB2 BA57AB0D D2AB2706 17674B3A 7423C276
B96CFB88 DE98A86E 7B539B68 7DEE53BB ED16BFA0 A89A5CA4 79F15F49 59DDF6E5
E716514A 5CFC7522 8E76778E 029E8F
quit
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
switchport access vlan 2
!
interface FastEthernet0/7
```

## Lab – Configuring Basic DHCPv4 on a Switch

---

```
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 ip address 192.168.2.1 255.255.255.0
!
ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.1.10
!
```

## Lab – Configuring Basic DHCPv4 on a Switch

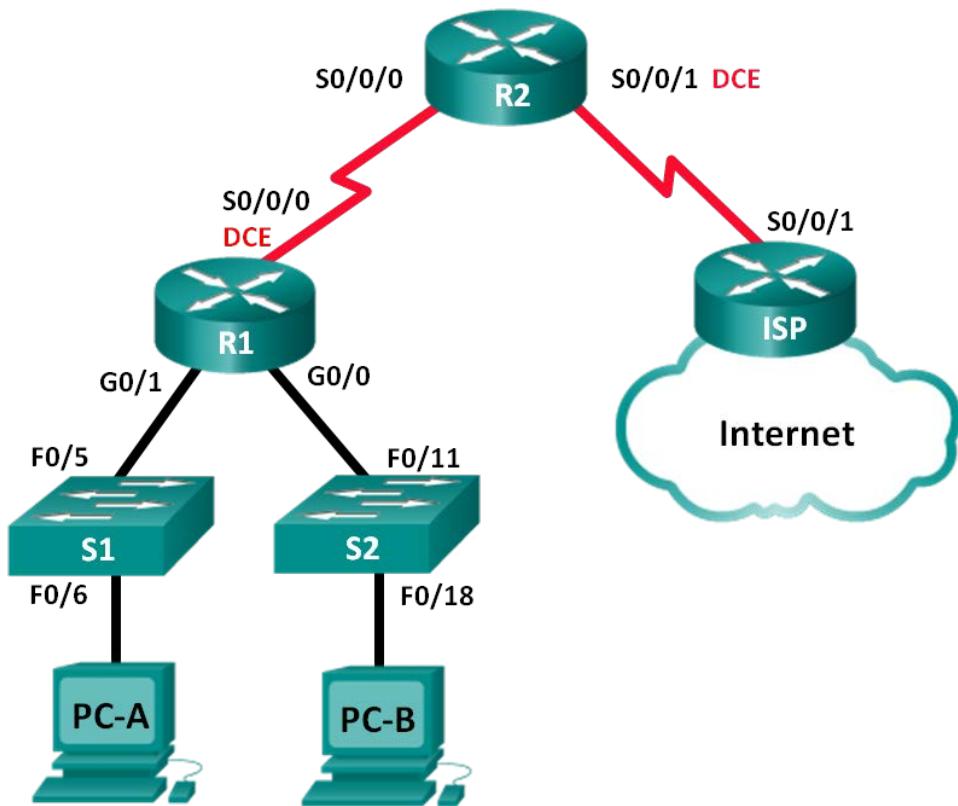
---

```
!
!
line con 0
password cisco
login
line vty 0 4
password cisco
login
line vty 5 15
password cisco
login
!
end
```

## Lab - Troubleshooting DHCPv4 (Instructor Version – Optional Lab)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

### Topology



## Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.128	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	192.168.0.253	255.255.255.252	N/A
R2	S0/0/0	192.168.0.254	255.255.255.252	N/A
	S0/0/1 (DCE)	209.165.200.226	255.255.255.252	N/A
ISP	S0/0/1	209.165.200.225	255.255.255.252	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.0.2	255.255.255.128	192.168.0.1
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP

## Objectives

**Part 1: Build the Network and Configure Basic Device Settings**

**Part 2: Troubleshoot DHCPv4 Issues**

## Background / Scenario

The Dynamic Host Configuration Protocol (DHCP) is a network protocol that lets the network administrators manage and automate the assignment of IP addresses. Without DHCP, the administrator must manually assign and configure IP addresses, preferred DNS servers, and the default gateway. As the network grows in size, this becomes an administrative problem when devices are moved from one internal network to another.

In this scenario, the company has grown in size, and the network administrators can no longer assign IP addresses to devices manually. The R2 router has been configured as a DHCP server to assign IP addresses to the host devices on router R1 LANs. Several errors in the configuration have resulted in connectivity issues. You are asked to troubleshoot and correct the configuration errors and document your work.

Ensure that the network supports the following:

- 1) The router R2 should function as the DHCP server for the 192.168.0.0/25 and 192.168.1.0/24 networks connected to R1.
- 2) All PCs connected to S1 and S2 should receive an IP address in the correct network via DHCP.

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

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

**Instructor Note:** Instructions for erasing the switches and routers are provided in the Lab Manual.

## Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

## Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the routers and switches with basic settings, such as passwords and IP addresses. You will also configure the IP settings for the PCs in the topology.

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

**Step 2: Initialize and reload the routers and switches.**

**Step 3: Configure basic settings for each router.**

- a. Disable DNS lookup.
- b. Configure device name as shown in the topology.
- c. Assign **class** as the privileged EXEC password.
- d. Assign **cisco** as the console and vty passwords.
- e. Configure **logging synchronous** to prevent console messages from interrupting command entry.
- f. Configure the IP addresses for all the router interfaces.
- g. Set clock rate to **128000** for all DCE router interfaces.
- h. Configure RIP for R1.

```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# network 192.168.0.0
R1(config-router)# network 192.168.1.0
R1(config-router)# no auto-summary
R1(config-router)# exit
```

- i. Configure RIP and a static default route on R2.

```
R2(config)# router rip
R2(config-router)# version 2
R2(config-router)# network 192.168.0.0
R2(config-router)# default-information originate
R2(config-router)# no auto-summary
R2(config-router)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

- j. Configure a summary static route on ISP to the networks on R1 and R2 routers.

```
ISP(config)# ip route 192.168.0.0 255.255.254.0 209.165.200.226
```

**Step 4: Verify network connectivity between the routers.**

If any pings between the routers fail, correct the errors before proceeding to the next step. Use **show ip route** and **show ip interface brief** to locate possible issues.

**Step 5: Configure basic settings for each switch.**

- a. Disable DNS lookup.
- b. Configure device name as shown in the topology.
- c. Configure the IP address for the VLAN 1 interface and the default gateway for each switch.
- d. Assign **class** as the privileged EXEC mode password.
- e. Assign **cisco** as the console and vty passwords.
- f. Configure **logging synchronous** for the console line.

**Step 6: Verify the hosts are configured for DHCP.**

**Step 7: Load the initial DHCP configuration for R1 and R2.**

**Router R1**

```
!interface GigabitEthernet0/0
! ip helper-address 192.168.0.254
interface GigabitEthernet0/1
 ip helper-address 192.168.0.253
 ! ip helper-address 192.168.0.254
```

**Router R2**

```
ip dhcp excluded-address 192.168.11.1 192.168.11.9
!ip dhcp excluded-address 192.168.1.1 192.168.1.9
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp pool R1G1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
ip dhcp pool R1G0
 network 192.168.0.0 255.255.255.128
 default-router 192.168.11.1
!default-router 192.168.0.1
```

**Part 2: Troubleshoot DHCPv4 Issues**

After configuring routers R1 and R2 with DHCPv4 settings, several errors in the DHCP configurations were introduced and resulted in connectivity issues. R2 is configured as a DHCP server. For both pools of DHCP addresses, the first nine addresses are reserved for the routers and switches. R1 relays the DHCP information to all the R1 LANs. Currently, PC-A and PC-B have no access to the network. Use the **show** and **debug** commands to determine and correct the network connectivity issues.

**Step 1: Record IP settings for PC-A and PC-B.**

- a. For PC-A and PC-B, at the command prompt, enter **ipconfig /all** to display the IP and MAC addresses.

## Lab - Troubleshooting DHCPv4

---

- b. Record the IP and MAC addresses in the table below. The MAC address can be used to determine which PC is involved in the debug message.

	IP Address/Subnet Mask	MAC Address
PC-A	No IP address is assigned by DHCP. (Students may record an APIPA address starting with 169.254.x.x. This is a private local address that Microsoft OS assigns when the host cannot reach a DHCP server to obtain an IP address.)	0050:56BE:768C
PC-B	No IP address is assigned by DHCP. (Students may record an APIPA address starting with 169.254.x.x. This is a private local address that Microsoft OS assigns when the host cannot reach a DHCP server to obtain an IP address.)	0050:56BE:F6DB

### Step 2: Troubleshoot DHCP issues for the 192.168.1.0/24 network on router R1.

Router R1 is a DHCP relay agent for all the R1 LANs. In this step, only the DHCP process for the 192.168.1.0/24 network will be examined. The first nine addresses are reserved for other network devices, such as routers, switches, and servers.

- a. Use a DHCP **debug** command to observe the DHCP process on R2 router.

```
R2# debug ip dhcp server events
```

- b. On R1, display the running configuration for the G0/1 interface.

```
R1# show run interface g0/1
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 192.168.0.253
 duplex auto
 speed auto
```

If there are any DHCP relay issues, record any commands that are necessary to correct the configurations errors.

---

---

---

DHCP relay was incorrectly configured for G0/1 interface. The command **ip helper-address 192.168.0.254** needs to be added to the R1 router. The incorrect helper address should be removed from the configuration. The issue can be resolved using the following commands:

```
R1(config)# interface g0/1
R1(config-if)# no ip helper-address 192.168.0.253
R1(config-if)# ip helper-address 192.168.0.254
```

- c. In a command prompt on PC-A, type **ipconfig /renew** to receive an address from the DHCP server. Record the configured IP address, subnet mask, and default gateway for PC-A.
-

## Lab - Troubleshooting DHCPv4

---

IP address: 192.168.1.3, subnet mask: 255.255.255.0, default gateway: 192.168.1.1

- d. Observe the debug messages on R2 router for the DHCP renewal process for PC-A. The DHCP server attempted to assign 192.168.1.1/24 to PC-A. This address is already in use for G0/1 interface on R1. The same issue occurs with IP address 192.168.1.2/24 because this address has been assigned to S1 in the initial configuration. Therefore, an IP address of 192.168.1.3/24 has been assigned to PC-A. The DHCP assignment conflict indicates there may be an issue with the excluded-address statement on the DHCP server configuration on R2.

```
*Mar 5 06:32:16.939: DHCPD: Sending notification of DISCOVER:
*Mar 5 06:32:16.939: DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:32:16.939: DHCPD: circuit id 00000000
*Mar 5 06:32:16.939: DHCPD: Seeing if there is an internally specified pool class:
*Mar 5 06:32:16.939: DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:32:16.939: DHCPD: circuit id 00000000
*Mar 5 06:32:16.943: DHCPD: Allocated binding 2944C764
*Mar 5 06:32:16.943: DHCPD: Adding binding to radix tree (192.168.1.1)
*Mar 5 06:32:16.943: DHCPD: Adding binding to hash tree
*Mar 5 06:32:16.943: DHCPD: assigned IP address 192.168.1.1 to client
0100.5056.be76.8c.
*Mar 5 06:32:16.951: %DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged
192.168.1.1.
*Mar 5 06:32:16.951: DHCPD: returned 192.168.1.1 to address pool R1G1.
*Mar 5 06:32:16.951: DHCPD: Sending notification of DISCOVER:
*Mar 5 06:32:16.951: DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:32:16.951: DHCPD: circuit id 00000000
*Mar 5 06:32:1
R2#6.951: DHCPD: Seeing if there is an internally specified pool class:
*Mar 5 06:32:16.951: DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:32:16.951: DHCPD: circuit id 00000000
*Mar 5 06:32:16.951: DHCPD: Allocated binding 31DC93C8
*Mar 5 06:32:16.951: DHCPD: Adding binding to radix tree (192.168.1.2)
*Mar 5 06:32:16.951: DHCPD: Adding binding to hash tree
*Mar 5 06:32:16.951: DHCPD: assigned IP address 192.168.1.2 to client
0100.5056.be76.8c.
*Mar 5 06:32:18.383: %DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged
192.168.1.2.
*Mar 5 06:32:18.383: DHCPD: returned 192.168.1.2 to address pool R1G1.
*Mar 5 06:32:18.383: DHCPD: Sending notification of DISCOVER:
*Mar 5 06:32:18.383: DHCPD: htype 1 chaddr 0050.56be.6c89
*Mar 5 06:32:18.383: DHCPD: circuit id 00000000
*Mar 5 06:32:18.383: DHCPD: Seeing if there is an internally specified pool class:
*Mar 5 06:32:18.383: DHCPD: htype 1 chaddr 0050.56be.6c89
*Mar 5 06:32:18.383: DHCPD: circuit id 00000000
*Mar 5 06:32:18.383: DHCPD: Allocated binding 2A40E074
*Mar 5 06:32:18.383: DHCPD: Adding binding to radix tree (192.168.1.3)
*Mar 5 06:32:18.383: DHCPD: Adding binding to hash tree
*Mar 5 06:32:18.383: DHCPD: assigned IP address 192.168.1.3 to client
0100.5056.be76.8c.
<output omitted>
```

- e. Display the DHCP server configuration on R2. The first nine addresses for 192.168.1.0/24 network are not excluded from the DHCP pool.

## Lab - Troubleshooting DHCPv4

---

```
R2# show run | section dhcp
ip dhcp excluded-address 192.168.11.1 192.168.11.9
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp pool R1G1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
ip dhcp pool R1G0
 network 192.168.0.0 255.255.255.128
 default-router 192.168.1.1
```

Record the commands to resolve the issue on R2.

---

---

```
R2(config)# no ip dhcp excluded-address 192.168.11.1 192.168.11.9
R2(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.9
```

- f. At the command prompt on PC-A, type **ipconfig /release** to return the 192.168.1.3 address back to the DHCP pool. The process can be observed in the debug message on R2.  
\*Mar 5 06:49:59.563: DHCPD: Sending notification of TERMINATION:  
\*Mar 5 06:49:59.563: DHCPD: address 192.168.1.3 mask 255.255.255.0  
\*Mar 5 06:49:59.563: DHCPD: reason flags: RELEASE  
\*Mar 5 06:49:59.563: DHCPD: htype 1 chaddr 0050.56be.768c  
\*Mar 5 06:49:59.563: DHCPD: lease time remaining (secs) = 85340  
\*Mar 5 06:49:59.563: DHCPD: returned 192.168.1.3 to address pool R1G1.
- g. At the command prompt on PC-A, type **ipconfig /renew** to be assigned a new IP address from the DHCP server. Record the assigned IP address and default gateway information.

---

IP address/subnet mask: 192.168.1.10/24 Default gateway: 192.168.1.1

The process can be observed in the debug message on R2.

```
*Mar 5 06:50:11.863: DHCPD: Sending notification of DISCOVER:
*Mar 5 06:50:11.863: DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:50:11.863: DHCPD: circuit id 00000000
*Mar 5 06:50:11.863: DHCPD: Seeing if there is an internally specified pool class:
*Mar 5 06:50:11.863: DHCPD: htype 1 chaddr 0050.56be.768c
*Mar 5 06:50:11.863: DHCPD: circuit id 00000000
*Mar 5 06:50:11.863: DHCPD: requested address 192.168.1.3 has already been assigned.
*Mar 5 06:50:11.863: DHCPD: Allocated binding 3003018C
*Mar 5 06:50:11.863: DHCPD: Adding binding to radix tree (192.168.1.10)
*Mar 5 06:50:11.863: DHCPD: Adding binding to hash tree
*Mar 5 06:50:11.863: DHCPD: assigned IP address 192.168.1.10 to client
0100.5056.be76.8c.
<output omitted>
```

- h. Verify network connectivity.

Can PC-A ping the assigned default gateway? \_\_\_\_\_ Yes

Can PC-A ping the R2 router? \_\_\_\_\_ Yes

Can PC-A ping the ISP router? \_\_\_\_\_ Yes

### Step 3: Troubleshoot DHCP issues for 192.168.0.0/25 network on R1.

Router R1 is a DHCP relay agent for all the R1 LANs. In this step, only the DHCP process for the 192.168.0.0/25 network is examined. The first nine addresses are reserved for other network devices.

- Use a DHCP **debug** command to observe the DHCP process on R2.

```
R2# debug ip dhcp server events
```

- Display the running configuration for the G0/0 interface on R1 to identify possible DHCP issues.

```
R1# show run interface g0/0
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.128
 duplex auto
 speed auto
```

Record the issues and any commands that are necessary to correct the configurations errors.

---

---

---

DHCP relay was not configured on the R1 G0/0 interface. The issue can be resolved using the following commands:

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.0.254
```

- From the command prompt on PC-B, type **ipconfig /renew** to receive an address from the DHCP server. Record the configured IP address, subnet mask, and default gateway for PC-B.

IP address: 192.168.0.10, subnet mask: 255.255.255.128, default gateway: 192.168.11.1

- Observe the debug messages on R2 router for the renewal process for PC-A. The DHCP server assigned 192.168.0.10/25 to PC-B.

```
*Mar 5 07:15:09.663: DHCPD: Sending notification of DISCOVER:
*Mar 5 07:15:09.663: DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar 5 07:15:09.663: DHCPD: circuit id 00000000
*Mar 5 07:15:09.663: DHCPD: Seeing if there is an internally specified pool class:
*Mar 5 07:15:09.663: DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar 5 07:15:09.663: DHCPD: circuit id 00000000
*Mar 5 07:15:09.707: DHCPD: Sending notification of ASSIGNMENT:
*Mar 5 07:15:09.707: DHCPD: address 192.168.0.10 mask 255.255.255.128
*Mar 5 07:15:09.707: DHCPD: htype 1 chaddr 0050.56be.f6db
*Mar 5 07:15:09.707: DHCPD: lease time remaining (secs) = 86400
```

- Verify network connectivity.

Can PC-B ping the DHCP assigned default gateway? \_\_\_\_\_ No

Can PC-B ping its default gateway (192.168.0.1)? \_\_\_\_\_ Yes

Can PC-B ping the R2 router? \_\_\_\_\_ Yes

Can PC-B ping the ISP router? \_\_\_\_\_ Yes

- If any issues failed in Step e, record the problems and any commands to resolve the issues.

---

PC-B is unable to ping the DHCP assigned default gateway. The issue can be resolved using the following commands.

```
R2(config)# ip dhcp pool R1G0
R2(dhcp-config)# default-router 192.168.0.1
```

- g. Release and renew the IP configurations on PC-B. Repeat Step e to verify network connectivity.
- h. Discontinue the debug process by using the **undebbug all** command.

```
R2# undebbug all
All possible debugging has been turned off
```

### Reflection

What are the benefits of using DHCP?

---

---

Answers will vary. DHCP can prevent address conflicts caused by a previous assigned IP address still in use, supply additional configuration values, such as a DNS server, and can be used with mobile or portable computers.

## Router Interface Summary Table

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

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

## Device Configs

### Router R1 (Corrected)

```
R1# show run
Building configuration...

Current configuration : 1419 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAug.2
!
no aaa new-model
memory-size iomem 15
!
```

## Lab - Troubleshooting DHCPv4

---

```
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
ip address 192.168.0.1 255.255.255.128
ip helper-address 192.168.0.254
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
ip helper-address 192.168.0.254
duplex auto
speed auto
!
interface Serial0/0/0
ip address 192.168.0.253 255.255.255.252
clock rate 128000
!
interface Serial0/0/1
no ip address
shutdown
!
!
router rip
version 2
network 192.168.0.0
network 192.168.1.0
```

## Lab - Troubleshooting DHCPv4

---

```
no auto-summary

!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### Router R2 (Corrected)

```
R2# show run
Building configuration...

Current configuration : 1552 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
```

## Lab - Troubleshooting DHCPv4

---

```
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
!
!
ip dhcp excluded-address 192.168.0.1 192.168.0.9
ip dhcp excluded-address 192.168.1.1 192.168.1.9
!
ip dhcp pool R1G1
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
ip dhcp pool R1G0
 network 192.168.0.0 255.255.255.128
 default-router 192.168.0.1
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1941/K9 sn FTX163283R9
license accept end user agreement
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
```

## Lab - Troubleshooting DHCPv4

---

```
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
ip address 192.168.0.254 255.255.255.252
!
interface Serial0/0/1
ip address 209.165.200.226 255.255.255.252
clock rate 128000
!
!
router rip
version 2
network 192.168.0.0
default-information originate
no auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 209.165.200.225
!
!
!
control-plane
!
!
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
```

```
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

## Router ISP

```
ISP#show run
Building configuration...

Current configuration : 1247 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 10
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
```

## Lab - Troubleshooting DHCPv4

---

```
!
!
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
ip address 209.165.200.225 255.255.255.252
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 192.168.0.0 255.255.254.0 209.165.200.226
!
!
!
!
control-plane
!
!
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
```

## Lab - Troubleshooting DHCPv4

---

```
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

## Lab – Configuring Stateless and Stateful DHCPv6 (Instructor Version)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only.

### Topology



### Addressing Table

Device	Interface	IPv6 Address	Prefix Length	Default Gateway
R1	G0/1	2001:DB8:ACAD:A::1	64	N/A
S1	VLAN 1	Assigned by SLAAC	64	Assigned by SLAAC
PC-A	NIC	Assigned by SLAAC and DHCPv6	64	Assigned by R1

### Objectives

**Part 1: Build the Network and Configure Basic Device Settings**

**Part 2: Configure the Network for SLAAC**

**Part 3: Configure the Network for Stateless DHCPv6**

**Part 4: Configure the Network for Stateful DHCPv6**

### Background / Scenario

The dynamic assignment of IPv6 global unicast addresses can be configured in three ways:

- Stateless Address Autoconfiguration (SLAAC) only
- Stateless Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- Stateful DHCPv6

With SLAAC (pronounced slack), a DHCPv6 server is not needed for hosts to acquire IPv6 addresses. It can be used to receive additional information that the host needs, such as the domain name and the domain name server (DNS) address. When SLAAC is used to assign the IPv6 host addresses and DHCPv6 is used to assign other network parameters, it is called Stateless DHCPv6.

With Stateful DHCPv6, the DHCP server assigns all information, including the host IPv6 address.

Determination of how hosts obtain their dynamic IPv6 addressing information is dependent on flag settings contained within the router advertisement (RA) messages.

In this lab, you will initially configure the network to use SLAAC. After connectivity has been verified, you will configure DHCPv6 settings and change the network to use Stateless DHCPv6. After verification that Stateless DHCPv6 is functioning correctly, you will change the configuration on R1 to use Stateful DHCPv6. Wireshark will be used on PC-A to verify all three dynamic network configurations.

## Lab – Configuring Stateless and Stateful DHCPv6

---

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

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

**Instructor Note:** Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

**Note:** The **default bias** template (used by the Switch Database Manager (SDM)) does not provide IPv6 address capabilities. Verify that SDM is using either the **dual-ipv4-and-ipv6** template or the **lanbase-routing** template. The new template will be used after reboot even if the config is not saved.

```
S1# show sdm prefer
```

Follow these steps to assign the **dual-ipv4-and-ipv6** template as the default SDM template:

```
S1# config t
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

### Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7 or Vista with Wireshark and terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

**Instructor Note:** Wireshark needs to be preinstalled on PC-A.

**Note:** DHCPv6 client services are disabled on Windows XP. It is recommended to use a Windows 7 host for this lab.

## Part 1: Build the Network and Configure Basic Device Settings

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

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

**Step 2: Initialize and reload the router and switch as necessary.**

**Step 3: Configure R1.**

- a. Console into R1 and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on R1.

```
no ip domain-lookup
service password-encryption
hostname R1
enable secret class
```

```
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. Save the running configuration to the startup configuration.

**Step 4: Configure S1.**

- a. Console into S1 and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on S1.

```
no ip domain-lookup
service password-encryption
hostname S1
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

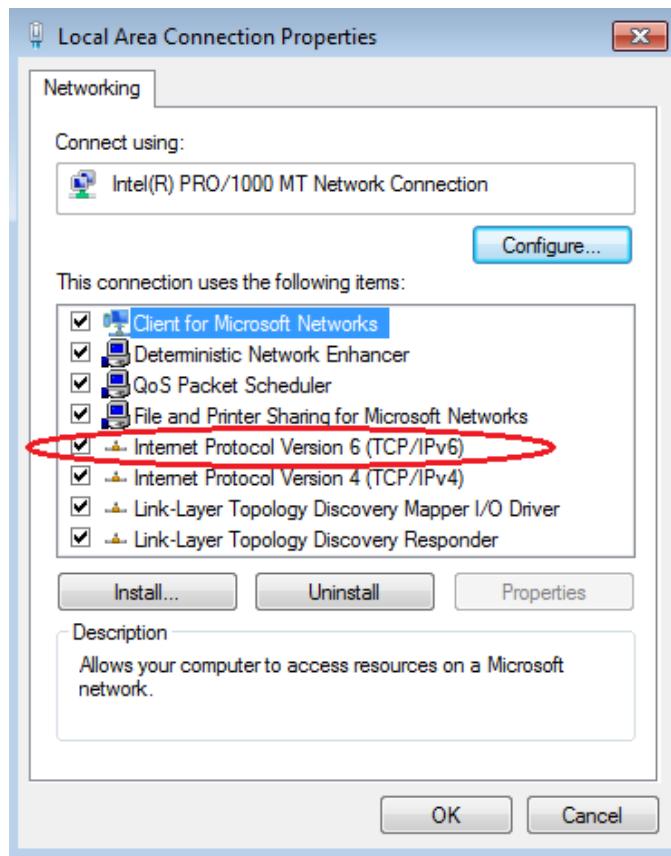
- c. Administratively disable all inactive interfaces.
- d. Save running configuration to the startup configuration.

**Part 2: Configure the Network for SLAAC**

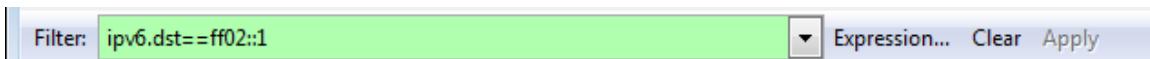
**Step 1: Prepare PC-A.**

- a. Verify that the IPv6 protocol has been enabled on the Local Area Connection Properties window. If the Internet Protocol Version 6 (TCP/IPv6) check box is not checked, click to enable it.

## Lab – Configuring Stateless and Stateful DHCPv6



- b. Start a Wireshark capture of traffic on the NIC.
- c. Filter the data capture to see only RA messages. This can be done by filtering on IPv6 packets with a destination address of FF02::1, which is the all-unicast client group address. The filter entry used with Wireshark is **ipv6.dst==ff02::1**, as shown here.



### Step 2: Configure R1.

- a. Enable IPv6 unicast routing.
- b. Assign the IPv6 unicast address to interface G0/1 according to the Addressing Table.
- c. Assign FE80::1 as the IPv6 link-local address for interface G0/1.
- d. Activate interface G0/1.

### Step 3: Verify that R1 is part of the all-router multicast group.

Use the **show ipv6 interface g0/1** command to verify that G0/1 is part of the All-router multicast group (FF02::2). RA messages are not sent out G0/1 without that group assignment.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::1
 No Virtual link-local address(es):
 Global unicast address(es):
```

## Lab – Configuring Stateless and Stateful DHCPv6

---

```
2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es):
 FF02::1
 FF02::2
 FF02::1:FF00:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

### Step 4: Configure S1.

Use the **ipv6 address autoconfig** command on VLAN 1 to obtain an IPv6 address through SLAAC.

```
S1(config)# interface vlan 1
S1(config-if)# ipv6 address autoconfig
S1(config-if)# end
```

### Step 5: Verify that SLAAC provided a unicast address to S1.

Use the **show ipv6 interface** command to verify that SLAAC provided a unicast address to VLAN1 on S1.

```
S1# show ipv6 interface
Vlan1 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::ED9:96FF:FE8:8A40
 No Virtual link-local address(es):
 Stateless address autoconfig enabled
 Global unicast address(es):
 2001:DB8:ACAD:A:ED9:96FF:FE8:8A40, subnet is 2001:DB8:ACAD:A::/64 [EUI/CAL/PRE]
 valid lifetime 2591988 preferred lifetime 604788
 Joined group address(es):
 FF02::1
 FF02::1:FFE8:8A40
 MTU is 1500 bytes
 ICMP error messages limited to one every 100 milliseconds
 ICMP redirects are enabled
 ICMP unreachables are sent
 Output features: Check hwidb
 ND DAD is enabled, number of DAD attempts: 1
 ND reachable time is 30000 milliseconds (using 30000)
 ND NS retransmit interval is 1000 milliseconds
 Default router is FE80::1 on Vlan1
```

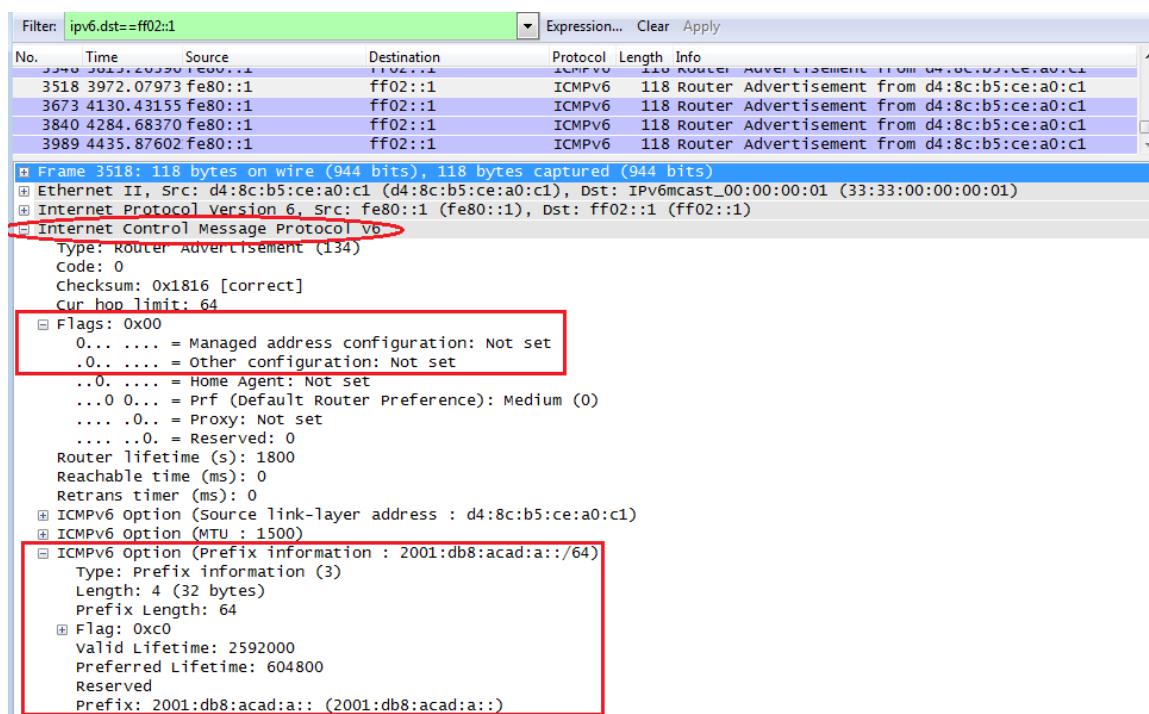
## Lab – Configuring Stateless and Stateful DHCPv6

### Step 6: Verify that SLAAC provided IPv6 address information on PC-A.

- From a command prompt on PC-A, issue the **ipconfig /all** command. Verify that PC-A is showing an IPv6 address with the 2001:db8:acad:a::/64 prefix. The Default Gateway should have the FE80::1 address.

```
Ethernet adapter Local Area Connection:
 Connection-specific DNS Suffix :
 Description : Intel(R) PRO/1000 MT Network Connection
 Physical Address : 00-50-56-BE-76-8C
 DHCP Enabled. : Yes
 Autoconfiguration Enabled : Yes
 IPv6 Address. : 2001:db8:acad:a:24ba:a0a0:9f0:ff88 (Preferred)
 Temporary IPv6 Address. : 2001:db8:acad:a:c05b:d3f7:31be:100e (Preferred)
 Link-local IPv6 Address : fe80::24ba:a0a0:9f0:ff88%11 (Preferred)
 Autoconfiguration IPv4 Address. : 169.254.255.136 (Preferred)
 Subnet Mask. : 255.255.0.0
 Default Gateway : fe80::1:11
 DNS Servers : fec0:0:0:ffff::1%1
 fec0:0:0:ffff::2%1
 fec0:0:0:ffff::3%1
 NetBIOS over Tcpip. : Enabled
```

- From Wireshark, look at one of the RA messages that were captured. Expand the Internet Control Message Protocol v6 layer to view the Flags and Prefix information. The first two flags control DHCPv6 usage and are not set if DHCPv6 is not configured. The prefix information is also contained within this RA message.



### Part 3: Configure the Network for Stateless DHCPv6

#### Step 1: Configure an IPv6 DHCP server on R1.

- Create an IPv6 DHCP pool.

```
R1(config)# ipv6 dhcp pool IPV6POOL-A
```

## Lab – Configuring Stateless and Stateful DHCPv6

---

- b. Assign a domain name to the pool.

```
R1(config-dhcpv6)# domain-name ccna-statelessDHCPv6.com
```

- c. Assign a DNS server address.

```
R1(config-dhcpv6)# dns-server 2001:db8:acad:a::abcd
R1(config-dhcpv6)# exit
```

- d. Assign the DHCPv6 pool to the interface.

```
R1(config)# interface g0/1
R1(config-if)# ipv6 dhcp server IPV6POOL-A
```

- e. Set the DHCPv6 network discovery (ND) **other-config-flag**.

```
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# end
```

### Step 2: Verify DHCPv6 settings on interface G0/1 on R1.

Use the **show ipv6 interface g0/1** command to verify that the interface is now part of the IPv6 multicast all-DHCPv6-servers group (FF02::1:2). The last line of the output from this **show** command verifies that the other-config-flag has been set.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::1
 No Virtual link-local address(es):
 Global unicast address(es):
 2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
 Joined group address(es):
 FF02::1
 FF02::2
 FF02::1:2
 FF02::1:FF00:1
 FF05::1:3
 MTU is 1500 bytes
 ICMP error messages limited to one every 100 milliseconds
 ICMP redirects are enabled
 ICMP unreachables are sent
 ND DAD is enabled, number of DAD attempts: 1
 ND reachable time is 30000 milliseconds (using 30000)
 ND advertised reachable time is 0 (unspecified)
 ND advertised retransmit interval is 0 (unspecified)
 ND router advertisements are sent every 200 seconds
 ND router advertisements live for 1800 seconds
 ND advertised default router preference is Medium
 Hosts use stateless autoconfig for addresses.
 Hosts use DHCP to obtain other configuration.
```

### Step 3: View network changes to PC-A.

Use the **ipconfig /all** command to review the network changes. Notice that additional information, including the domain name and DNS server information, has been retrieved from the DHCPv6 server. However, the IPv6 global unicast and link-local addresses were obtained previously from SLAAC.

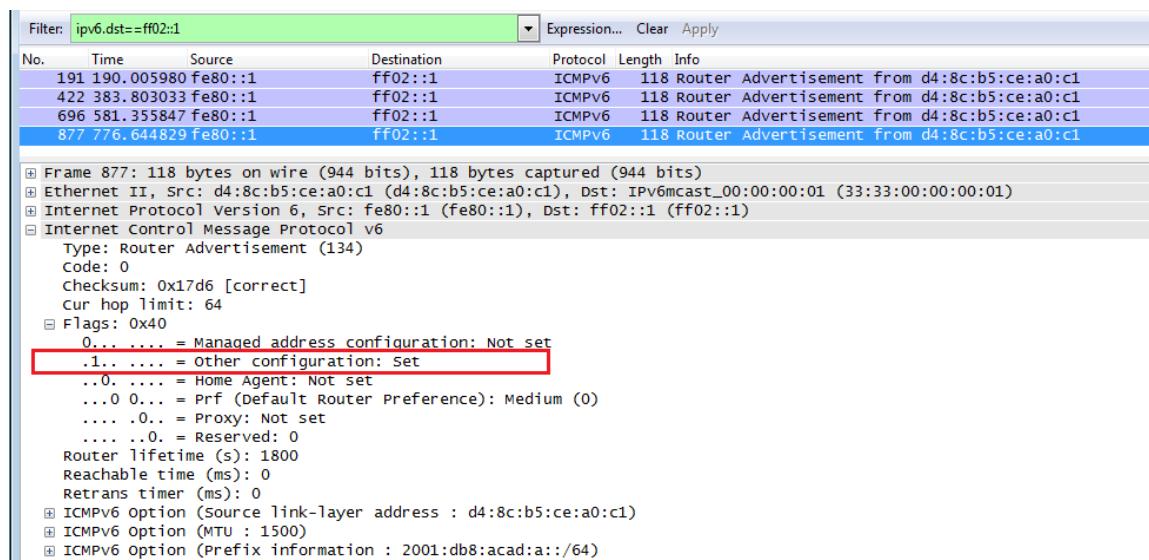
## Lab – Configuring Stateless and Stateful DHCPv6

```
Ethernet adapter Local Area Connection:
 Connection-specific DNS Suffix . : ccna-statelessDHCPv6.com
 Description Intel(R) PRO/1000 MT Network Connection
 Physical Address 00-50-56-BE-76-8C
 DHCP Enabled. Yes
 Autoconfiguration Enabled Yes
 IPv6 Address. 2001:db8:acad:a:24ba:a0a0:9f0:ff88<Preferred>
 Temporary IPv6 Address. 2001:db8:acad:a:103a:4344:4b5e:ab1d<Preferred>
 Link-local IPv6 Address fe80::24ba:a0a0:9f0:ff88%11<Preferred>
 Autoconfiguration IPv4 Address 169.254.255.136<Preferred>
 Subnet Mask 255.255.0.0
 Default Gateway fe80::1%11
 DHCPv6 IAID 234884137
 DHCPv6 Client DUID. 00-01-00-01-17-F6-72-3D-00-0C-29-8D-54-44
 DNS Servers 2001:db8:acad:a::abcd
 NetBIOS over Tcpip Enabled
 Connection-specific DNS Suffix Search List :
 ccna-statelessDHCPv6.com

Tunnel adapter isatap.{E2FC1866-B195-460A-BF40-F04F42A38FFE}:
 Media State Media disconnected
 Connection-specific DNS Suffix ccna-statelessDHCPv6.com
 Description Microsoft ISATAP Adapter
 Physical Address 00-00-00-00-00-00-E0
 DHCP Enabled. No
 Autoconfiguration Enabled Yes
```

### Step 4: View the RA messages in Wireshark.

Scroll down to the last RA message that is displayed in Wireshark and expand it to view the ICMPv6 flag settings. Notice that the other configuration flag is set to 1.



### Step 5: Verify that PC-A did not obtain its IPv6 address from a DHCPv6 server.

Use the **show ipv6 dhcp binding** and **show ipv6 dhcp pool** commands to verify that PC-A did not obtain an IPv6 address from the DHCPv6 pool.

```
R1# show ipv6 dhcp binding
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
```

## Lab – Configuring Stateless and Stateful DHCPv6

---

```
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-statelessDHCPv6.com
Active clients: 0
```

### Step 6: Reset PC-A IPv6 network settings.

- Shut down interface F0/6 on S1.

**Note:** Shutting down the interface F0/6 prevents PC-A from receiving a new IPv6 address before you reconfigure R1 for Stateful DHCPv6 in Part 4.

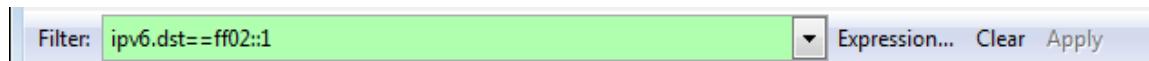
```
S1(config)# interface f0/6
S1(config-if)# shutdown
```

- Stop Wireshark capture of traffic on the PC-A NIC.
- Reset the IPv6 settings on PC-A to remove the Stateless DHCPv6 settings.
  - Open the Local Area Connection Properties window, deselect the **Internet Protocol Version 6 (TCP/IPv6)** check box, and click **OK** to accept the change.
  - Open the Local Area Connection Properties window again. Click to enable the **Internet Protocol Version 6 (TCP/IPv6)** check box, and then click **OK** to accept the change.

## Part 4: Configure the Network for Stateful DHCPv6

### Step 1: Prepare PC-A.

- Start a Wireshark capture of traffic on the NIC.
- Filter the data capture to see only RA messages. This can be done by filtering on IPv6 packets with a destination address of FF02::1, which is the all-unicast client group address.



### Step 2: Change the DHCPv6 pool on R1.

- Add the network prefix to the pool.
- Change the domain name to **ccna-statefulDHCPv6.com**.

**Note:** You must remove the old domain name. It is not replaced by the **domain-name** command.

```
R1(config-dhcpv6)# no domain-name ccna-statelessDHCPv6.com
R1(config-dhcpv6)# domain-name ccna-StatefulDHCPv6.com
R1(config-dhcpv6)# end
```

- Verify DHCPv6 pool settings.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (0 in use, 0 conflicts)
DNS server: 2001:DB8:ACAD:A::ABCD
Domain name: ccna-StatefulDHCPv6.com
Active clients: 0
```

## Lab – Configuring Stateless and Stateful DHCPv6

---

- d. Enter debug mode to verify the Stateful DHCPv6 address assignment.

```
R1# debug ipv6 dhcp detail
IPv6 DHCP debugging is on (detailed)
```

### Step 3: Set the flag on G0/1 for Stateful DHCPv6.

**Note:** Shutting down the G0/1 interface before making changes ensures that an RA message is sent when the interface is activated.

```
R1(config)# interface g0/1
R1(config-if)# shutdown
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# no shutdown
R1(config-if)# end
```

### Step 4: Enable interface F0/6 on S1.

Now that R1 has been configured for Stateful DHCPv6, you can reconnect PC-A to the network by activating interface F0/6 on S1.

```
S1(config)# interface f0/6
S1(config-if)# no shutdown
S1(config-if)# end
```

### Step 5: Verify Stateful DHCPv6 settings on R1.

- a. Issue the **show ipv6 interface g0/1** command to verify that the interface is in Stateful DHCPv6 mode.

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::1
 No Virtual link-local address(es):
 Global unicast address(es):
 2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
 Joined group address(es):
 FF02::1
 FF02::2
 FF02::1:2
 FF02::1:FF00:1
 FF05::1:3
 MTU is 1500 bytes
 ICMP error messages limited to one every 100 milliseconds
 ICMP redirects are enabled
 ICMP unreachables are sent
 ND DAD is enabled, number of DAD attempts: 1
 ND reachable time is 30000 milliseconds (using 30000)
 ND advertised reachable time is 0 (unspecified)
 ND advertised retransmit interval is 0 (unspecified)
 ND router advertisements are sent every 200 seconds
 ND router advertisements live for 1800 seconds
 ND advertised default router preference is Medium
 Hosts use DHCP to obtain routable addresses.
```

## Lab – Configuring Stateless and Stateful DHCPv6

Hosts use DHCP to obtain other configuration.

- In a command prompt on PC-A, type **ipconfig /release6** to release the currently assigned IPv6 address. Then type **ipconfig /renew6** to request an IPv6 address from the DHCPv6 server.
- Issue the **show ipv6 dhcp pool** command to verify the number of active clients.

```
R1# show ipv6 dhcp pool
```

DHCPv6 pool: IPV6POOL-A

Address allocation prefix: 2001:DB8:ACAD:A::/64 valid 172800 preferred 86400 (1 in use, 0 conflicts)

DNS server: 2001:DB8:ACAD:A::ABCD

Domain name: ccna-StatefulDHCPv6.com

Active clients: 1

- Issue the **show ipv6 dhcp binding** command to verify that PC-A received its IPv6 unicast address from the DHCP pool. Compare the client address to the link-local IPv6 address on PC-A using the **ipconfig /all** command. Compare the address provided by the **show** command to the IPv6 address listed with the **ipconfig /all** command on PC-A.

```
R1# show ipv6 dhcp binding
```

Client: FE80::D428:7DE2:997C:B05A

DUID: 0001000117F6723D000C298D5444

Username : unassigned

IA NA: IA ID 0x0E000C29, T1 43200, T2 69120

Address: 2001:DB8:ACAD:A:B55C:8519:8915:57CE

preferred lifetime 86400, valid lifetime 172800

expires at Mar 07 2013 04:09 PM (171595 seconds)

### Ethernet adapter Local Area Connection:

```
Connection-specific DNS Suffix . : ccna-StatefulDHCPv6.com
Description : Intel(R) PRO/1000 MT Network Connection
Physical Address : 00-50-56-BE-6C-89
DHCP Enabled. : Yes
Autoconfiguration Enabled : Yes
IPv6 Address. : 2001:db8:acad:a:b55c:8519:8915:57ce<Preferred>
Lease Obtained. : Tuesday, March 05, 2013 11:53:11 AM
Lease Expires : Thursday, March 07, 2013 11:53:11 AM
IPv6 Address. : 2001:db8:acad:a:d428:7de2:997c:b05a<Preferred>
Temporary IPv6 Address. : 2001:db8:acad:a:dd37:1e42:948c:225b<Preferred>
Link-local IPv6 Address : fe80::d428:7de2:997c:b05a:11<Preferred>
Autoconfiguration IPv4 Address : 162.251.176.98<Preferred>
Subnet Mask : 255.255.0.0
Default Gateway : fe80::1%11
DHCPv6 IAID : 234884137
DHCPv6 Client DUID. : 00-01-00-01-17-F6-72-3D-00-0C-29-8D-54-44
DNS Servers : 2001:db8:acad:a::abcd
NetBIOS over Tcpip. : Enabled
Connection-specific DNS Suffix Search List :
ccna-StatefulDHCPv6.com
```

- Issue the **undebbug all** command on R1 to stop debugging DHCPv6.

**Note:** Typing **u all** is the shortest form of this command and is useful to know if you are trying to stop debug messages from continually scrolling down your terminal session screen. If multiple debugs are in process, the **undebbug all** command stops all of them.

```
R1# u all
```

All possible debugging has been turned off

## Lab – Configuring Stateless and Stateful DHCPv6

---

f. Review the debug messages that appeared on your R1 terminal screen.

1) Examine the solicit message from PC-A requesting network information.

```
*Mar 5 16:42:39.775: IPv6 DHCP: Received SOLICIT from FE80::D428:7DE2:997C:B05A on
GigabitEthernet0/1
*Mar 5 16:42:39.775: IPv6 DHCP: detailed packet contents
*Mar 5 16:42:39.775: src FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)
*Mar 5 16:42:39.775: dst FF02::1:2
*Mar 5 16:42:39.775: type SOLICIT(1), xid 1039238
*Mar 5 16:42:39.775: option ELAPSED-TIME(8), len 2
*Mar 5 16:42:39.775: elapsed-time 6300
*Mar 5 16:42:39.775: option CLIENTID(1), len 14
```

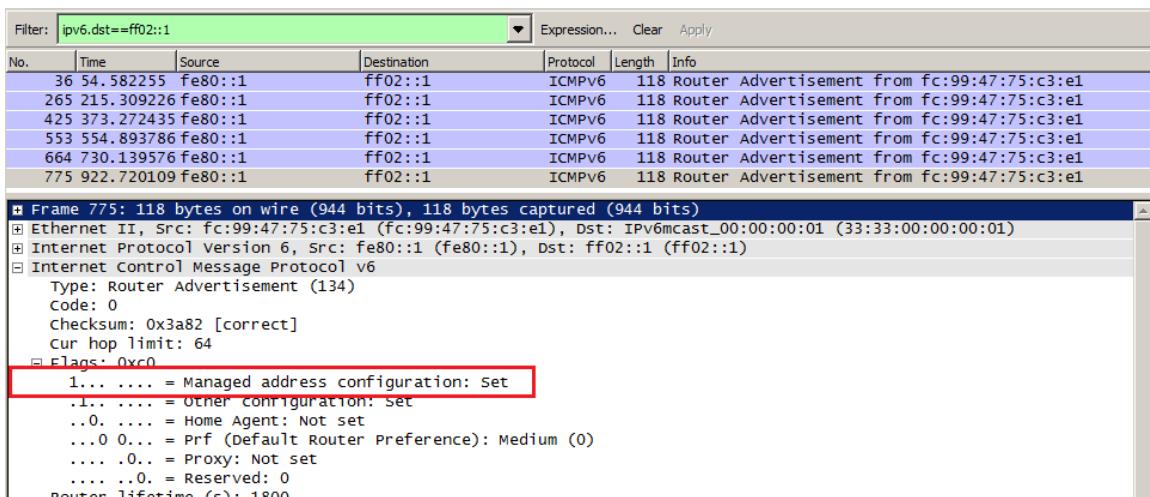
2) Examine the reply message sent back to PC-A with the DHCP network information.

```
*Mar 5 16:42:39.779: IPv6 DHCP: Sending REPLY to FE80::D428:7DE2:997C:B05A on
GigabitEthernet0/1
*Mar 5 16:42:39.779: IPv6 DHCP: detailed packet contents
*Mar 5 16:42:39.779: src FE80::1
*Mar 5 16:42:39.779: dst FE80::D428:7DE2:997C:B05A (GigabitEthernet0/1)
*Mar 5 16:42:39.779: type REPLY(7), xid 1039238
*Mar 5 16:42:39.779: option SERVERID(2), len 10
*Mar 5 16:42:39.779: 00030001FC994775C3E0
*Mar 5 16:42:39.779: option CLIENTID(1), len 14
*Mar 5 16:42:39.779: 00010001
R1#17F6723D000C298D5444
*Mar 5 16:42:39.779: option IA-NA(3), len 40
*Mar 5 16:42:39.779: IAID 0x0E000C29, T1 43200, T2 69120
*Mar 5 16:42:39.779: option IAADDR(5), len 24
*Mar 5 16:42:39.779: IPv6 address 2001:DB8:ACAD:A:B55C:8519:8915:57CE
*Mar 5 16:42:39.779: preferred 86400, valid 172800
*Mar 5 16:42:39.779: option DNS-SERVERS(23), len 16
*Mar 5 16:42:39.779: 2001:DB8:ACAD:A::ABCD
*Mar 5 16:42:39.779: option DOMAIN-LIST(24), len 26
*Mar 5 16:42:39.779: ccna-StatefulDHCPv6.com
```

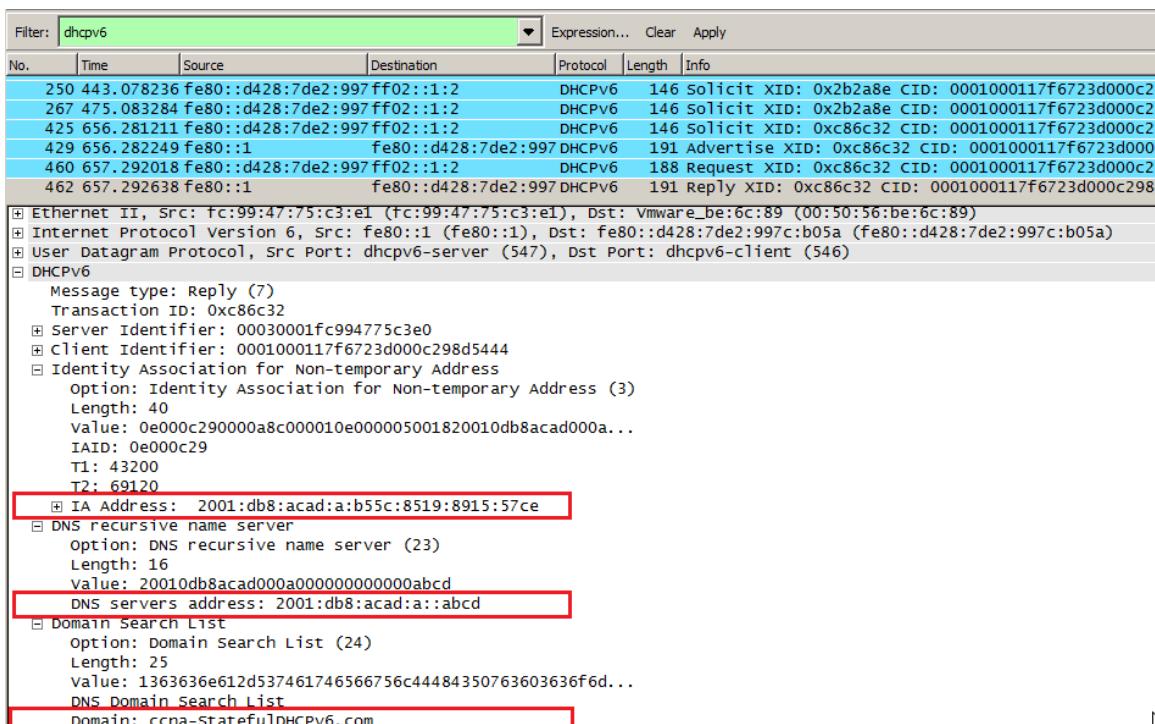
### Step 6: Verify Stateful DHCPv6 on PC-A

- a. Stop the Wireshark capture on PC-A.
- b. Expand the most recent RA message listed in Wireshark. Verify that the **Managed address configuration** flag has been set.

## Lab – Configuring Stateless and Stateful DHCPv6



- c. Change the filter in Wireshark to view **DHCPv6** packets only by typing **dhcpv6**, and then **Apply** the filter. Highlight the last DHCPv6 reply listed and expand the DHCPv6 information. Examine the DHCPv6 network information that is contained in this packet.



## Reflection

1. What IPv6 addressing method uses more memory resources on the router configured as a DHCPv6 server, Stateless DHCPv6 or Stateful DHCPv6? Why?
- 
- 
-

## Lab – Configuring Stateless and Stateful DHCPv6

---

Stateful DHCPv6 uses more memory resources. Answers will vary, but Stateful DHCPv6 requires the router to store dynamic state information about the DHCPv6 clients. Stateless DHCPv6 clients do not use the DHCP server to obtain address information, so this information does not need to be stored.

2. Which type of dynamic IPv6 address assignment is recommended by Cisco, Stateless DHCPv6 or Stateful DHCPv6?
- 
- 

Cisco recommends Stateless DHCPv6 when implementing and deploying IPv6 networks without a Cisco Network Register (CNR).

### Router Interface Summary Table

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

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

### Device Configs - Part 1 and 2 combined for R1 and S1

#### Router R1 (After parts 1 and 2 of this lab)

```
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
```

## Lab – Configuring Stateless and Stateful DHCPv6

---

```
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C
Unauthorized Access is Prohibited!
^C
!
line con 0
password 7 070C285F4D06
logging synchronous
login
line aux 0
!
line vty 0 4
```

```
password 7 13061E010803
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### Switch S1 (After parts 1 and 2 of this lab)

```
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGh0lQM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
shutdown
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
```

## Lab – Configuring Stateless and Stateful DHCPv6

---

```
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
```

```
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized Access is Prohibited!
^C
!
line con 0
password 7 05080F1C2243
logging synchronous
login
line vty 0 4
password 7 02050D480809
login
line vty 5 15
password 7 02050D480809
login
!
end
```

### Router R1 (Final)

```
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 dhcp pool IPV6POOL-A
```

## Lab – Configuring Stateless and Stateful DHCPv6

---

```
address prefix 2001:DB8:ACAD:A::/64
dns-server 2001:DB8:ACAD:A::ABCD
domain-name ccna-StatefulDHCPv6.com
!
ipv6 cef
multilink bundle-name authenticated
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:A::1/64
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp server IPV6POOL-A
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!
banner motd ^C
Unauthorized Access is Prohibited!
^C
!
line con 0
password 7 070C285F4D06
logging synchronous
login
line aux 0
```

## Lab – Configuring Stateless and Stateful DHCPv6

---

```
!
line vty 0 4
password 7 13061E010803
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

## Lab - Troubleshooting DHCPv6 (Instructor Version)

**Instructor Note:** Red font color or Gray highlights indicate text that appears in the instructor copy only.

### Topology



### Addressing Table

Device	Interface	IPv6 Address	Prefix Length	Default Gateway
R1	G0/1	2001:DB8:ACAD:A::1	64	N/A
S1	VLAN 1	Assigned by SLAAC	64	Assigned by SLAAC
PC-A	NIC	Assigned by SLAAC and DHCPv6	64	Assigned by SLAAC

### Objectives

**Part 1: Build the Network and Configure Basic Device Settings**

**Part 2: Troubleshoot IPv6 Connectivity**

**Part 3: Troubleshoot Stateless DHCPv6**

### Background / Scenario

The ability to troubleshoot network issues is a very useful skill for network administrators. It is important to understand IPv6 address groups and how they are used when troubleshooting a network. Knowing what commands to use to extract IPv6 network information is necessary to effectively troubleshoot.

In this lab, you will load configurations on R1 and S1. These configurations will contain issues that prevent Stateless DHCPv6 from functioning on the network. You will troubleshoot R1 and S1 to resolve these issues.

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

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

**Instructor Note:** Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

**Note:** The default bias template used by the Switch Database Manager (SDM) does not provide IPv6 address capabilities. Verify that SDM is using either the **dual-ipv4-and-ipv6** template or the **lanbase-routing** template. The new template will be used after reboot even if the configuration is not saved.

```
S1# show sdm prefer
```

Follow this configuration to assign the **dual-ipv4-and-ipv6** template as the default SDM template:

```
S1# config t
```

```
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

### Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

## Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and clear any configurations if necessary. You will configure basic settings on the router and switch. Then you will load the provided IPv6 configurations before you start troubleshooting.

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

**Step 2:** Initialize and reload the router and the switch.

**Step 3:** Configure basic settings on the router and switch.

- a. Disable DNS lookup.
- b. Configure device names as shown in the topology.
- c. Encrypt plain text passwords.
- d. Create a MOTD banner warning users that unauthorized access is prohibited.
- e. Assign **class** as the encrypted privileged EXEC mode password.
- f. Assign **cisco** as the console and vty passwords and enable login.
- g. Configure **logging synchronous** to prevent console messages from interrupting command entry.

**Step 4:** Load the IPv6 configuration to R1.

```
ip domain name ccna-lab.com
! ipv6 unicast-routing
ipv6 dhcp pool IPV6POOL-A
 dns-server 2001:DB8:ACAD:CAFE::A
 domain-name ccna-lab.com
interface g0/0
 no ip address
 shutdown
 duplex auto
 speed auto
interface g0/1
 no ip address
 duplex auto
```

## Lab – Troubleshooting DHCPv6

---

```
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:ACAD:A::11/64
! no ipv6 address 2001:db8:acad:a::11/64
! ipv6 address 2001:db8:acad:a::1/64
! ipv6 nd other-config-flag
! ipv6 dhcp server IPV6POOL-A
! no shutdown
end
```

### Step 5: Load the IPv6 configuration to S1.

```
interface range f0/1-24
shutdown
!interface range f0/5-6
! no shutdown
interface range g0/1-2
shutdown
interface Vlan1
shutdown
! ipv6 address autoconfig
! no shutdown
end
```

### Step 6: Save the running configurations on R1 and S1.

### Step 7: Verify that IPv6 is enabled on PC-A.

Verify that IPv6 has been enabled in the Local Area Connection Properties window on PC-A.

## Part 2: Troubleshoot IPv6 Connectivity

In Part 2, you will test and verify Layer 3 IPv6 connectivity on the network. Continue troubleshooting the network until Layer 3 connectivity has been established on all devices. Do not continue to Part 3 until you have successfully completed Part 2.

### Step 1: Troubleshoot IPv6 interfaces on R1.

- According to the topology, which interface must be active on R1 for network connectivity to be established? Record any commands used to identify which interfaces are active.

---

G0/1

```
R1# show ip interface brief
```

- If necessary, take the steps required to bring up the interface. Record the commands used to correct the configuration errors and verify that the interface is active.
- 
- 

```
R1(config)# interface g0/1
```

## Lab – Troubleshooting DHCPv6

---

```
R1(config-if) # no shutdown
```

- c. Identify the IPv6 addresses configured on R1. Record the addresses found and the commands used to view the IPv6 addresses.
- 
- 

```
2001:DB8:ACAD:A::11/64
```

```
show ipv6 interface or show ipv6 interface g0/1. Show run interface g0/1 can also be used.
```

- d. Determine if a configuration error has been made. If any errors are identified, record all the commands used to correct the configuration.
- 
- 

```
R1(config) # interface g0/1
```

```
R1(config-if) # no ipv6 address 2001:db8:acad:a::11/64
```

```
R1(config-if) # ipv6 address 2001:db8:acad:a::1/64
```

- e. On R1, what multicast group is needed for SLAAC to function?
- 

```
All-routers multicast group (FF02::2)
```

- f. What command is used to verify that R1 is a member of that group?
- 

```
show ipv6 interface or show ipv6 interface g0/1
```

```
R1# show ipv6 interface
```

```
GigabitEthernet0/1 is down, line protocol is down
```

```
 IPv6 is tentative, link-local address is FE80::1 [TEN]
```

```
 No Virtual link-local address(es) :
```

```
 Global unicast address(es) :
```

```
 2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64 [TEN]
```

```
 Joined group address(es) :
```

```
 FF02::1
```

```
 MTU is 1500 bytes
```

```
 ICMP error messages limited to one every 100 milliseconds
```

```
 ICMP redirects are enabled
```

```
 ICMP unreachable messages are sent
```

```
 ND DAD is enabled, number of DAD attempts: 1
```

```
 ND reachable time is 30000 milliseconds (using 30000)
```

```
 ND advertised reachable time is 0 (unspecified)
```

```
 ND advertised retransmit interval is 0 (unspecified)
```

```
 ND router advertisements are sent every 200 seconds
```

```
 ND router advertisements live for 1800 seconds
```

```
 ND advertised default router preference is Medium
```

```
 Hosts use stateless autoconfig for addresses.
```

## Lab – Troubleshooting DHCPv6

---

- g. If R1 is not a member of the multicast group that is needed for SLAAC to function correctly, make the necessary changes to the configuration so that it joins the group. Record any commands necessary to correct the configurations errors.

---

```
R1(config)# ipv6 unicast-routing
```

- h. Re-issue the command to verify that interface G0/1 has joined the all-routers multicast group (FF02::2).

**Note:** If you are unable to join the all-routers multicast group, you may need to save your current configuration and reload the router.

### Step 2: Troubleshoot S1.

- a. Are the interfaces needed for network connectivity active on S1? \_\_\_\_\_ No

Record any commands that are used to activate necessary interfaces on S1.

---

---

---

---

```
S1(config)# interface range f0/5-6
```

```
S1(config-if)# no shutdown
```

```
S1(config-if)# interface vlan 1
```

```
S1(config-if)# no shutdown
```

- b. What command could you use to determine if an IPv6 unicast address has been assigned to S1?

---

Issue the **show ipv6 interface** or **show ipv6 interface vlan1** command.

- c. Does S1 have an IPv6 unicast address configured? If so, what is it?

---

No IPv6 address has been assigned.

- d. If S1 is not receiving a SLAAC address, make the necessary configuration changes to allow it to receive one. Record the commands used.

---

---

```
S1(config)# interface vlan 1
S1(config-if)# ipv6 address autoconfig
```

- e. Re-issue the command that verifies that the interface now receives a SLAAC address.

- f. Can S1 ping the IPv6 unicast address assigned to the G0/1 interface assigned to R1?

---

Yes, S1 should be able to ping the 2001:db8:acad:a::1 IPv6 address.

### Step 3: Troubleshoot PC-A.

- a. Issue the command used on PC-A to verify the IPv6 address assigned. Record the command.

## Lab – Troubleshooting DHCPv6

---

**ipconfig /all**

- b. What is the IPv6 unicast address SLAAC is providing to PC-A?

If all the changes were made to R1 and S1, PC-A should receive an IPv6 address with the 2001:db8:acad:a::/64 prefix.

- c. Can PC-A ping the default gateway address that was assigned by SLAAC?

Yes, PC-A should be able to ping the FE80::1 address.

- d. Can PC-A ping the management interface on S1?

---

---

---

Yes, PC-A should be able to ping the IPv6 address assigned to VLAN 1. This address can be found by issuing the **show ipv6 interface vlan1** command on S1 and then looking for the IPv6 address with a prefix of 2001:db8:acad:a::/64.

**Note:** Continue troubleshooting until you can ping R1 and S1 from PC-A.

## Part 3: Troubleshoot Stateless DHCPv6

In Part 3, you will test and verify that Stateless DHCPv6 is working correctly on the network. You will need to use the correct IPv6 CLI commands on the router to determine if Stateless DHCPv6 is working. You may want to use debug to help determine if the DHCP server is being solicited.

### Step 1: Determine if Stateless DHCPv6 is functioning correctly.

- a. What is the name of the IPv6 DHCP pool? How did you determine this?

---

---

IPV6POOL-A. Issue the **show ipv6 dhcp pool** command to determine the name of the DHCPv6 Server pool. You can also issue the **show run | section ipv6 dhcp** command to see this information.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6POOL-A
 DNS server: 2001:DB8:ACAD:CAFE::A
 Domain name: ccna-lab.com
 Active clients: 0
```

- b. What network information is listed in the DHCPv6 pool?

---

---

A DNS server is listed with a 2001:DB8:ACAD:CAFE::A, and a domain name is listed as ccna-lab.com.

- c. Was the DHCPv6 information assigned to PC-A? How did you determine this?

---

---

No, this can be determined by issuing an **ipconfig /all** command at the command prompt on PC-A.

## Lab – Troubleshooting DHCPv6

---

### Step 2: Troubleshoot R1.

- a. What commands can be used to determine if R1 is configured for Stateless DHCPv6?

---

The **show ipv6 interface** command can be used to determine if an interface has the Stateless DHCPv6 flag set. The **show run** command can also be used to view the configuration on the interface.

```
R1# show ipv6 interface
GigabitEthernet0/1 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::1
 No Virtual link-local address(es):
 Global unicast address(es):
 2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
 Joined group address(es):
 FF02::1
 FF02::2
 FF02::1:FF00:1
 MTU is 1500 bytes
 ICMP error messages limited to one every 100 milliseconds
 ICMP redirects are enabled
 ICMP unreachable messages are sent
 ND DAD is enabled, number of DAD attempts: 1
 ND reachable time is 30000 milliseconds (using 30000)
 ND advertised reachable time is 0 (unspecified)
 ND advertised retransmit interval is 0 (unspecified)
 ND router advertisements are sent every 200 seconds
 ND router advertisements live for 1800 seconds
 ND advertised default router preference is Medium
 Hosts use stateless autoconfig for addresses.
```

- b. Is the G0/1 interface on R1 in Stateless DHCPv6 mode?

---

No. The interface is not part of the all-DHCPv6 Servers group because the FF02::1:2 group address is not listed. It also does not mention the state of the DHCP server at the bottom of the output.

- c. What command can be used to have R1 join the all-DHCPv6 server group?

---

Issue the command **ipv6 dhcp server IPV6POOL-A** on interface G0/1.

```
R1(config)# interface g0/1
R1(config-if)# ipv6 dhcp server IPV6POOL-A
```

- d. Verify that the all-DHCPv6 server group is configured for interface G0/1.

```
R1# show ipv6 interface
GigabitEthernet0/1 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::1
```

## Lab – Troubleshooting DHCPv6

---

```
No Virtual link-local address(es) :
Global unicast address(es) :
 2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
Joined group address(es) :
 FF02::1
 FF02::2
 FF02::1:2
 FF02::1:FF00:1
 FF05::1:3
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

- e. Will PC-A receive the DHCP information now? Explain?
- 

No, the **show ipv6 interface** command is still not showing that hosts are going to use DHCP to obtain other configuration information. This can be verified by issuing an **ipconfig /all** on PC-A.

- f. What is missing from the configuration of G0/1 that causes hosts to use the DHCP server to retrieve other network information?
- 

The **ipv6 nd other-config-flag** command is needed to tell hosts to use the DHCP server to retrieve other network information.

```
R1(config)# interface g0/1
R1(config-if)# ipv6 nd other-config-flag
R1# show ipv6 interface
GigabitEthernet0/1 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::1
 No Virtual link-local address(es) :
 Global unicast address(es) :
 2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
 Joined group address(es) :
 FF02::1
 FF02::2
 FF02::1:2
 FF02::1:FF00:1
 FF05::1:3
 MTU is 1500 bytes
```

## Lab – Troubleshooting DHCPv6

---

```
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
Hosts use DHCP to obtain other configuration.
```

- g. Reset the IPv6 settings on PC-A.
  - 1) Open the Local Area Connection Properties window, deselect the Internet Protocol Version 6 (TCP/IPv6) check box, and then click **OK** to accept the change.
  - 2) Open the Local Area Connection Properties window again, click the Internet Protocol Version 6 (TCP/IPv6) check box, and then click **OK** to accept the change.
- h. Issue the command to verify changes have been made on PC-A.

**Note:** Continue troubleshooting until PC-A receives the additional DHCP information from R1.

### Reflection

1. What command is needed in the DHCPv6 pool for Stateful DHCPv6 that is not needed for Stateless DHCPv6? Why?

---

---

The **address prefix <ipv6 prefix address>** command is needed for Stateful DHCPv6. Hosts receive their IPv6 unicast addresses from the DHCP server so this command is needed to provide the IPv6 prefix to use for the network.

2. What command is needed on the interface to change the network to use Stateful DHCPv6 instead of Stateless DHCPv6?

---

---

The **ipv6 nd managed-config-flag** command is used to set the Stateful DHCPv6 flag. This is transmitted to all hosts on the network through the router advertisement messages sent by R1.

**Router Interface Summary Table**

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

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

**Device Configs****Router R1 (Final)**

```
R1#sh run
Building configuration...

Current configuration : 1829 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
memory-size iomem 10
!
ipv6 unicast-routing
```

## Lab – Troubleshooting DHCPv6

---

```
ipv6 dhcp pool IPV6POOL-A
 dns-server 2001:DB8:ACAD:CAFE::A
 domain-name ccna-lab.com
!
ipv6 cef
!
no ip domain lookup
ip domain name ccna-lab.com
ip cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::1 link-local
 ipv6 address 2001:DB8:ACAD:A::1/64
 ipv6 nd other-config-flag
 ipv6 dhcp server IPV6POOL-A
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
```

## Lab – Troubleshooting DHCPv6

---

```
control-plane
!
banner motd ^CC
 Unauthorized Access is Prohibited!
^C
!
line con 0
exec-timeout 0 0
password 7 0205085A1815
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 104D05181604
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### Switch S1 (Final)

```
S1#sh run
Building configuration...

Current configuration : 3365 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUG.2
!
no aaa new-model
system mtu routing 1500
```

## Lab – Troubleshooting DHCPv6

---

```
ip subnet-zero
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 shutdown
!
interface FastEthernet0/2
 shutdown
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
 shutdown
!
interface FastEthernet0/8
 shutdown
!
interface FastEthernet0/9
 shutdown
!
interface FastEthernet0/10
 shutdown
!
interface FastEthernet0/11
 shutdown
!
interface FastEthernet0/12
 shutdown
!
interface FastEthernet0/13
 shutdown
!
```

## Lab – Troubleshooting DHCPv6

---

```
interface FastEthernet0/14
 shutdown
!
interface FastEthernet0/15
 shutdown
!
interface FastEthernet0/16
 shutdown
!
interface FastEthernet0/17
 shutdown
!
interface FastEthernet0/18
 shutdown
!
interface FastEthernet0/19
 shutdown
!
interface FastEthernet0/20
 shutdown
!
interface FastEthernet0/21
 shutdown
!
interface FastEthernet0/22
 shutdown
!
interface FastEthernet0/23
 shutdown
!
interface FastEthernet0/24
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 ipv6 address autoconfig
!
ip http server
ip http secure-server
!
control-plane
!
banner motd ^C
```

## Lab – Troubleshooting DHCPv6

---

```
Unauthorized Access is Prohibited!
^C
!
line con 0
password 7 104D000A0618
logging synchronous
login
line vty 0 4
password 7 104D000A0618
login
line vty 5 15
password 7 104D000A0618
login
!
end
```



## IoE and DHCP (Instructor Version – Optional Lab)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

### Objective

Configure DHCP for IPv4 or IPv6 on a Cisco 1941 router.

At the end of this chapter, students should be able to configure a Cisco 1941 router for IPv4 and IPv6 DHCP end-device addressing. In this activity, students will use Packet Tracer to configure DHCP addressing for end devices in a home environment.

### Scenario

This chapter presents the concept of using the DHCP process in a small- to medium-sized business network; however, DHCP also has other uses!

With the advent of the Internet of Everything (IoE), any device in your home capable of wired or wireless connectivity to a network will be able to be accessed from just about anywhere.

Using Packet Tracer for this modeling activity, perform the following tasks:

- Configure a Cisco 1941 router (or DHCP-server-capable ISR device) for IPv4 or IPv6 DHCP addressing.
- Think of five devices in your home you would like to receive IP addresses from the router's DHCP service. Set the end devices to claim DHCP addresses from the DHCP server.
- Show output validating that each end device secures an IP address from the server. Save your output information via a screen capture program or use the **PrtScrn** key command.
- Present your findings to a fellow classmate or to the class.

### Required Resources

Packet Tracer software

### Reflection

1. Why would a user want to use a Cisco 1941 router to configure DHCP on his home network? Wouldn't a smaller ISR be good enough to use as a DHCP server?

---

Answers will vary. The 1941 routers are more expensive than smaller ISRs, but they offer more options to implement security plans and are more robust in processing/bandwidth power.

2. How do you think small- medium-sized businesses are able to use DHCP IP address allocation in the IoE and IPv6 network world? Brainstorm and record five possible answers.

---

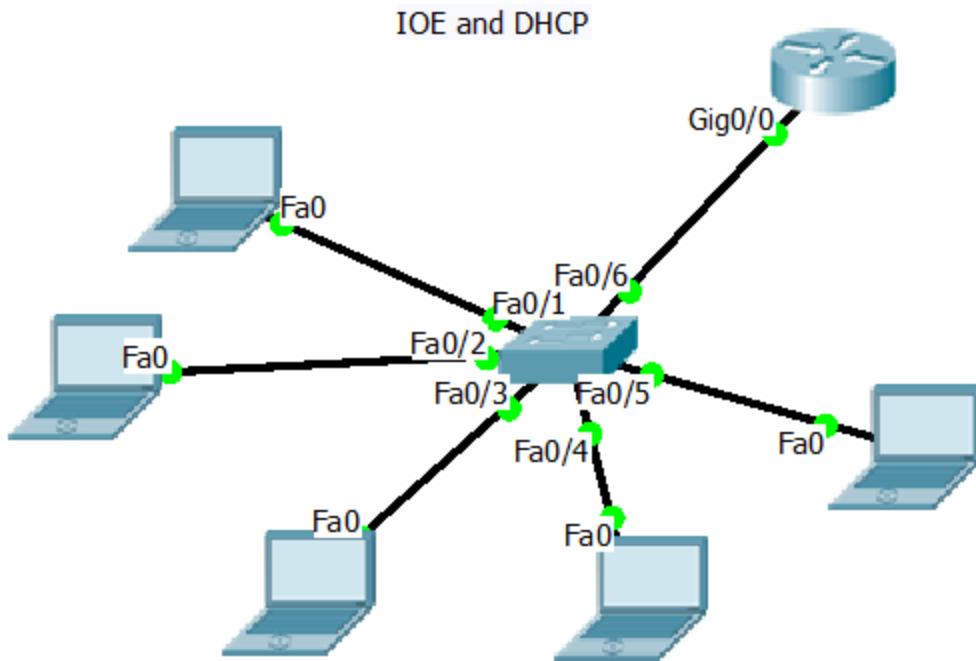
Small landscaping firms may be able to turn on sprinkler systems for customers when they go on vacation, based on the landscaping firm's DHCP server IP address allocations.

Small electric companies may be able to check error codes on any device with an IP address to evaluate the end-device for repair by using their own DHCP servers' IP address allocations.

Small automotive businesses may be able to provide estimates for repair based on DHCP IP addressing of automobiles with auto addresses linked to the business' DHCP server.

A homeowner may be able to start the washer or dryer from any location, based upon a DNS server location and their own DHCP server address.

Televisions may be controlled to turn off, turn on, select stations to record, record programs, and more using a DNS server and personal DHCP server.

**Instructor Activity Representative Topology and Output**

```
Router# show run
(output omitted)

hostname Router

ip dhcp excluded-address 192.168.1.1 192.168.1.10
!
ip dhcp pool HOME-ADDRESSES
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
(output omitted)

spanning-tree mode pvst
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
```

Router# show ip dhcp binding			
IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.1.11	0090.0CC1.A57B	--	Automatic
192.168.1.14	0060.3E80.2074	--	Automatic
192.168.1.13	0001.C9B3.382D	--	Automatic
192.168.1.12	000A.F345.487C	--	Automatic
192.168.1.15	00E0.F995.0C3B	--	Automatic

### Identify elements of the model that map to IT-related content:

- DHCP servers can allocate IP addresses to any network-capable device.
- DHCP servers can provide small- to medium-sized businesses with functionality that is not provided with static addressing.
- Network administrators, who configure network DHCP servers, such as routers, switches or dedicated servers, can save time in implementing an IP addressing scheme.



## Conceptual NAT (Instructor Version – Optional Lab)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

### Objective

Describe NAT characteristics.

This activity introduces students to the concept of network address translation.

### Scenario

You work for a large university or school system. Because you are the network administrator, many professors, administrative workers, and other network administrators need your assistance with their networks on a daily basis. They call you at all working hours of the day and, because of the number of telephone calls, you cannot complete your regular network administration tasks.

You need to find a way to limit when you take calls and from whom. You also need to mask your telephone number so that when you call someone, another number is displayed to the recipient.

This scenario describes a very common problem for most small- to medium-sized businesses. Visit, “How Network Address Translation Works” located at <http://computer.howstuffworks.com/nat.htm/printable> to view more information about how the digital world handles these types of workday interruptions.

Use the PDF provided accompanying this activity to reflect further on how a process, known as NAT, could be the answer to this scenario’s challenge.

### Resources

Internet connection

### Directions

#### Step 1: Read Information on the Internet Site.

- a. Go to “How Network Address Translation Works” located at <http://computer.howstuffworks.com/nat.htm/printable>
- b. Read the information provided to introduce the basic concepts of NAT.
- c. Record five facts you find to be interesting about the NAT process.

#### Step 2: View the NAT graphics.

- a. On the same Internet page, look at the types of NAT that are available for configuration on most networks.
- b. Define the four NAT types:
  - 1) Static NAT
  - 2) Dynamic NAT
  - 3) NAT Overload
  - 4) NAT Overlap

#### Step 3: Meet together in a full-class setting.

- a. Report your five NAT facts to the class.

## **Conceptual NAT**

---

- b. As other students state their interesting facts to the class, check off the stated fact if you already recorded it.
- c. If a student reports a fact to the class that you did not record, add it to your list.

### **Instructor Resource Information**

- It is suggested that you display the Web page used as a basis for this activity while comparing facts students report after reading the article.
- Make sure you correct any misunderstandings found in the reading of the web article before moving to the curriculum content.
- At the end of the class or group meeting, reiterate that NAT is a process used to conserve network address allocations and provide a measure of security for users.

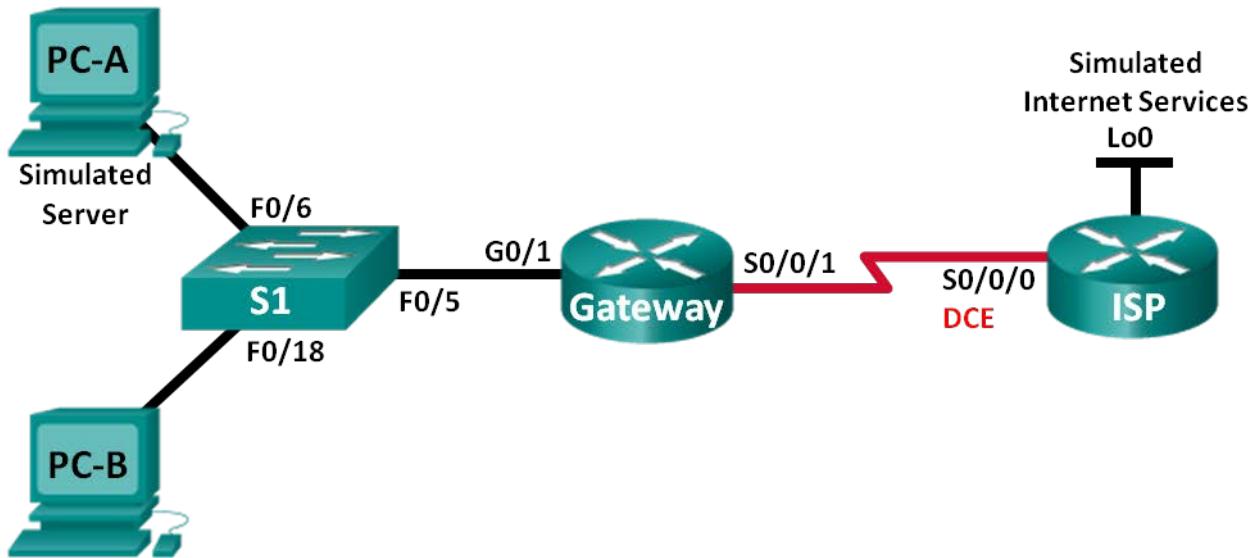
### **Identify elements of the model that map to IT-related content:**

- NAT
- Static NAT
- Dynamic NAT
- NAT Overload
- NAT Overlap

## Lab – Configuring Dynamic and Static NAT (Instructor Version – Optional Lab)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

### Topology



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A (Simulated Server)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

### Objectives

- Part 1: Build the Network and Verify Connectivity
- Part 2: Configure and Verify Static NAT
- Part 3: Configure and Verify Dynamic NAT

### Background / Scenario

Network Address Translation (NAT) is the process where a network device, such as a Cisco router, assigns a public address to host devices inside a private network. The main reason to use NAT is to reduce the number

## Lab – Configuring Dynamic and Static NAT

---

of public IP addresses that an organization uses because the number of available IPv4 public addresses is limited.

In this lab, an ISP has allocated the public IP address space of 209.165.200.224/27 to a company. This provides the company with 30 public IP addresses. The addresses, 209.165.200.225 to 209.165.200.241, are for static allocation and 209.165.200.242 to 209.165.200.254 are for dynamic allocation. A static route is used from the ISP to the gateway router, and a default route is used from the gateway to the ISP router. The ISP connection to the Internet is simulated by a loopback address on the ISP router.

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

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

**Instructor Note:** Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

### Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

## Part 1: Build the Network and Verify Connectivity

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

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

Attach the devices as shown in the topology diagram, and cable as necessary.

### Step 2: Configure PC hosts.

### Step 3: Initialize and reload the routers and switches as necessary.

### Step 4: Configure basic settings for each router.

- a. Console into the router and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
```

```
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. Configure the host name as shown in the topology.
- d. Copy the running configuration to the startup configuration.

### Step 5: Create a simulated web server on ISP.

- a. Create a local user named **webuser** with an encrypted password of **webpass**.

```
ISP(config)# username webuser privilege 15 secret webpass
```

- b. Enable the HTTP server service on ISP.

```
ISP(config)# ip http server
```

- c. Configure the HTTP service to use the local user database.

```
ISP(config)# ip http authentication local
```

### Step 6: Configure static routing.

- a. Create a static route from the ISP router to the Gateway router using the assigned public network address range 209.165.200.224/27.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

- b. Create a default route from the Gateway router to the ISP router.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

### Step 7: Save the running configuration to the startup configuration.

### Step 8: Verify network connectivity.

- a. From the PC hosts, ping the G0/1 interface on the Gateway router. Troubleshoot if the pings are unsuccessful.
- b. Display the routing tables on both routers to verify that the static routes are in the routing table and configured correctly on both routers.

## Part 2: Configure and Verify Static NAT

Static NAT uses a one-to-one mapping of local and global addresses, and these mappings remain constant. Static NAT is particularly useful for web servers or devices that must have static addresses that are accessible from the Internet.

### Step 1: Configure a static mapping.

A static map is configured to tell the router to translate between the private inside server address 192.168.1.20 and the public address 209.165.200.225. This allows a user from the Internet to access PC-A. PC-A is simulating a server or device with a constant address that can be accessed from the Internet.

```
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225
```

### Step 2: Specify the interfaces.

Issue the **ip nat inside** and **ip nat outside** commands to the interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

### Step 3: Test the configuration.

- a. Display the static NAT table by issuing the **show ip nat translations** command.

```
Gateway# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.225 192.168.1.20 --- ---
```

What is the translation of the Inside local host address?

192.168.1.20 = \_\_\_\_\_ 209.165.200.225

The Inside global address is assigned by?

The router from the NAT pool.

The Inside local address is assigned by?

The administrator for the workstation.

- b. From PC-A, ping the Lo0 interface (192.31.7.1) on ISP. If the ping was unsuccessful, troubleshoot and correct the issues. On the Gateway router, display the NAT table.

```
Gateway# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1
--- 209.165.200.225 192.168.1.20 --- ---
```

A NAT entry was added to the table with ICMP listed as the protocol when PC-A sent an ICMP request (ping) to 192.31.7.1 on ISP.

What port number was used in this ICMP exchange? \_\_\_\_\_ 1, answers will vary.

**Note:** It may be necessary to disable the PC-A firewall for the ping to be successful.

- c. From PC-A, telnet to the ISP Lo0 interface and display the NAT table.

```
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034 192.31.7.1:23 192.31.7.1:23
--- 209.165.200.225 192.168.1.20 --- ---
```

**Note:** The NAT for the ICMP request may have timed out and been removed from the NAT table.

What was the protocol used in this translation? \_\_\_\_\_ tcp

What are the port numbers used?

Inside global / local: \_\_\_\_\_ 1034, answers will vary.

Outside global / local: \_\_\_\_\_ 23

## Lab – Configuring Dynamic and Static NAT

---

- d. Because static NAT was configured for PC-A, verify that pinging from ISP to PC-A at the static NAT public address (209.165.200.225) is successful.
- e. On the Gateway router, display the NAT table to verify the translation.

```
Gateway# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:12 192.168.1.20:12 209.165.201.17:12 209.165.201.17:12
--- 209.165.200.225 192.168.1.20 --- ---
```

Notice that the Outside local and Outside global addresses are the same. This address is the ISP remote network source address. For the ping from the ISP to succeed, the Inside global static NAT address 209.165.200.225 was translated to the Inside local address of PC-A (192.168.1.20).

- f. Verify NAT statistics by using the **show ip nat statistics** command on the Gateway router.

```
Gateway# show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
 Serial0/0/1
Inside interfaces:
 GigabitEthernet0/1
 Hits: 39 Misses: 0
 CEF Translated packets: 39, CEF Punted packets: 0
 Expired translations: 3
Dynamic mappings:

 Total doors: 0
 Appl doors: 0
 Normal doors: 0
 Queued Packets: 0
```

**Note:** This is only a sample output. Your output may not match exactly.

## Part 3: Configure and Verify Dynamic NAT

Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis. When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool. Dynamic NAT results in a many-to-many address mapping between local and global addresses.

### Step 1: Clear NATs.

Before proceeding to add dynamic NATs, clear the NATs and statistics from Part 2.

```
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics
```

### Step 2: Define an access control list (ACL) that matches the LAN private IP address range.

ACL 1 is used to allow 192.168.1.0/24 network to be translated.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

### Step 3: Verify that the NAT interface configurations are still valid.

Issue the **show ip nat statistics** command on the Gateway router to verify the NAT configurations.

```
Gateway# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
 Serial0/0/1
Inside interfaces:
 FastEthernet0/1
Hits: 0 Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

### Step 4: Define the pool of usable public IP addresses.

```
Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200.254
netmask 255.255.255.224
```

### Step 5: Define the NAT from the inside source list to the outside pool.

**Note:** Remember that NAT pool names are case-sensitive and the pool name entered here must match that used in the previous step.

```
Gateway(config)# ip nat inside source list 1 pool public_access
```

### Step 6: Test the configuration.

- From PC-B, ping the Lo0 interface (192.31.7.1) on ISP. If the ping was unsuccessful, troubleshoot and correct the issues. On the Gateway router, display the NAT table.

```
Gateway# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.225 192.168.1.20 --- ---
icmp 209.165.200.242:1 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1
--- 209.165.200.242 192.168.1.21 --- ---
```

What is the translation of the Inside local host address for PC-B?

192.168.1.21 = \_\_\_\_\_ 209.165.200.242

A dynamic NAT entry was added to the table with ICMP as the protocol when PC-B sent an ICMP message to 192.31.7.1 on ISP.

What port number was used in this ICMP exchange? \_\_\_\_\_ 1, answers will vary.

- From PC-B, open a browser and enter the IP address of the ISP-simulated web server (Lo0 interface). When prompted, log in as **webuser** with a password of **webpass**.
- Display the NAT table.

```
Pro Inside global Inside local Outside local Outside global
```

## Lab – Configuring Dynamic and Static NAT

---

```
--- 209.165.200.225 192.168.1.20 --- ---
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1039 192.168.1.21:1039 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1040 192.168.1.21:1040 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1047 192.168.1.21:1047 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1048 192.168.1.21:1048 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80 192.31.7.1:80
tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80 192.31.7.1:80
--- 209.165.200.242 192.168.1.22 --- ---
```

What protocol was used in this translation? \_\_\_\_\_ **tcp**

What port numbers were used?

Inside: \_\_\_\_\_ **1038 to 1052. Answers will vary.**

Outside: \_\_\_\_\_ **80**

What well-known port number and service was used? \_\_\_\_\_ **port 80, www or http**

- d. Verify NAT statistics by using the **show ip nat statistics** command on the Gateway router.

```
Gateway# show ip nat statistics
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 00:06:40 ago
Outside interfaces:
 Serial0/0/1
Inside interfaces:
 GigabitEthernet0/1
Hits: 345 Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
pool public_access: netmask 255.255.255.224
start 209.165.200.242 end 209.165.200.254
type generic, total addresses 13, allocated 1 (7%), misses 0
```

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

**Note:** This is only a sample output. Your output may not match exactly.

### Step 7: Remove the static NAT entry.

In Step 7, the static NAT entry is removed and you can observe the NAT entry.

- Remove the static NAT from Part 2. Enter **yes** when prompted to delete child entries.

```
Gateway(config)# no ip nat inside source static 192.168.1.20 209.165.200.225
```

```
Static entry in use, do you want to delete child entries? [no]: yes
```

- Clear the NATs and statistics.
- Ping the ISP (192.31.7.1) from both hosts.
- Display the NAT table and statistics.

```
Gateway# show ip nat statistics
```

```
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
```

```
Peak translations: 15, occurred 00:00:43 ago
```

```
Outside interfaces:
```

```
Serial0/0/1
```

```
Inside interfaces:
```

```
GigabitEthernet0/1
```

```
Hits: 16 Misses: 0
```

```
CEF Translated packets: 285, CEF Punted packets: 0
```

```
Expired translations: 11
```

```
Dynamic mappings:
```

```
-- Inside Source
```

```
[Id: 1] access-list 1 pool public_access refcount 4
```

```
pool public_access: netmask 255.255.255.224
```

```
start 209.165.200.242 end 209.165.200.254
```

```
type generic, total addresses 13, allocated 2 (15%), misses 0
```

```
Total doors: 0
```

```
Appl doors: 0
```

```
Normal doors: 0
```

```
Queued Packets: 0
```

```
Gateway# show ip nat translation
```

Pro	Inside global	Inside local	Outside local	Outside global
-----	---------------	--------------	---------------	----------------

```
icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512 192.31.7.1:512
```

```
--- 209.165.200.243 192.168.1.20 --- ---
```

```
icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512 192.31.7.1:512
```

```
--- 209.165.200.242 192.168.1.21 --- ---
```

**Note:** This is only a sample output. Your output may not match exactly.

### Reflection

- Why would NAT be used in a network?

---

---

---

## Lab – Configuring Dynamic and Static NAT

---

Answers will vary, but should include: whenever there are not enough public IP addresses and to avoid the cost of purchasing public addresses from an ISP. NAT can also provide a measure of security by hiding internal addresses from outside networks.

2. What are the limitations of NAT?

---

---

NAT needs IP information or port number information in the IP header and TCP header of packets for translation. Here is a partial list of protocols that cannot be used with NAT: SNMP, LDAP, Kerberos version 5.

### Router Interface Summary Table

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

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

### Device Configs

#### Gateway (After Part 2)

```
Gateway# show run
Building configuration...

Current configuration : 1666 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

## Lab – Configuring Dynamic and Static NAT

---

```
hostname Gateway
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
ip address 209.165.201.18 255.255.255.252
ip nat outside
ip virtual-reassembly in
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat inside source static 192.168.1.20 209.165.200.225
ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

```
!
control-plane
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### Gateway (Final)

```
Gateway# show run
Building configuration...

Current configuration : 1701 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Gateway
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUG.2
!
no aaa new-model
memory-size iomem 15
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
```

## Lab – Configuring Dynamic and Static NAT

---

```
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
ip address 209.165.201.18 255.255.255.252
ip nat outside
ip virtual-reassembly in
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat pool public_access 209.165.200.242 209.165.200.254 netmask 255.255.255.224
ip nat inside source list 1 pool public_access
ip route 0.0.0.0 0.0.0.0 209.165.201.17
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
control-plane
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
```

## Lab – Configuring Dynamic and Static NAT

---

```
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### ISP (Final)

```
ISP# show run
Building configuration...

Current configuration : 1557 bytes
!
! Last configuration change at 09:16:34 UTC Sun Mar 24 2013
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 10
!
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
username webuser privilege 15 secret 4 ZMYyKvmzVsyor8jHyP9ox.cMoz9loLfZN75illtozY2
!
interface Loopback0
 ip address 192.31.7.1 255.255.255.255
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
```

## Lab – Configuring Dynamic and Static NAT

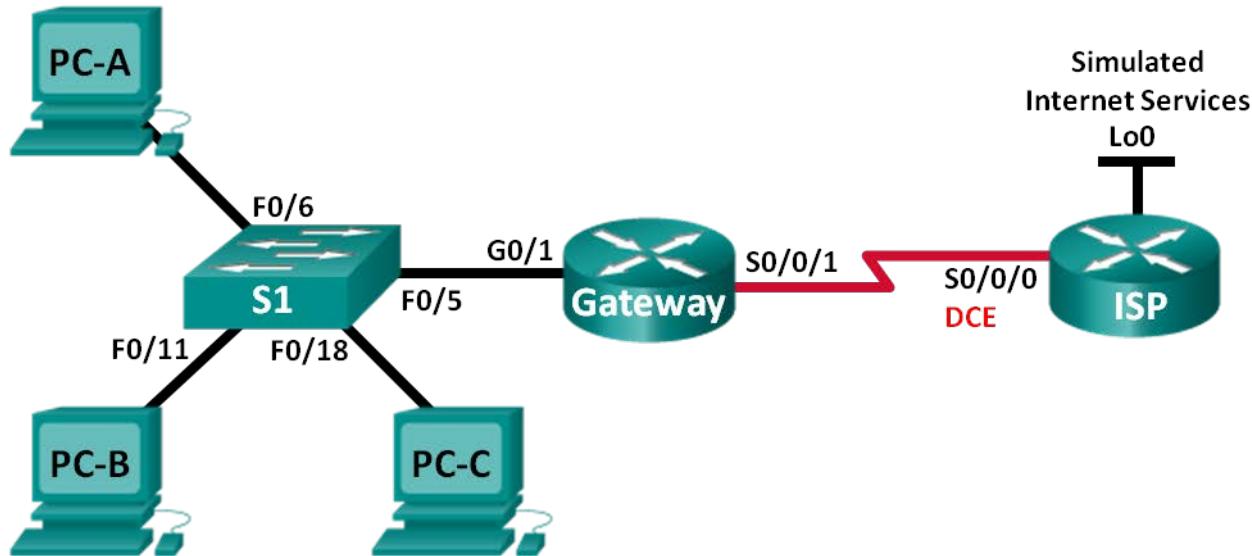
---

```
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
ip address 209.165.201.17 255.255.255.252
clock rate 128000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
ip http server
ip http authentication local
no ip http secure-server
!
ip route 209.165.200.224 255.255.255.224 209.165.201.18
!
control-plane
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin laptb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

## Lab – Configuring Port Address Translation (PAT) (Instructor Version)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only.

### Topology



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.201.18	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	N/A
	Lo0	192.31.7.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.22	255.255.255.0	192.168.1.1

### Objectives

- Part 1: Build the Network and Verify Connectivity
- Part 2: Configure and Verify NAT Pool Overload
- Part 3: Configure and Verify PAT

### Background / Scenario

In the first part of the lab, your company is allocated the public IP address range of 209.165.200.224/29 by the ISP. This provides the company with six public IP addresses. Dynamic NAT pool overload uses a pool of IP addresses in a many-to-many relationship. The router uses the first IP address in the pool and assigns

## Lab – Configuring Port Address Translation (PAT)

---

connections using the IP address plus a unique port number. After the maximum number of translations for a single IP address have been reached on the router (platform and hardware specific), it uses the next IP address in the pool. NAT pool overload is a form port address translation (PAT) that overloads a group of public IPv4 addresses.

In Part 2, the ISP has allocated a single IP address, 209.165.201.18, to your company for use on the Internet connection from the company Gateway router to the ISP. You will use the PAT to convert multiple internal addresses into the one usable public address. You will test, view, and verify that the translations are taking place, and you will interpret the NAT/PAT statistics to monitor the process.

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

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

**Instructor Note:** Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

### Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

## Part 1: Build the Network and Verify Connectivity

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

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

**Step 2: Configure PC hosts.**

**Step 3: Initialize and reload the routers and switches.**

**Step 4: Configure basic settings for each router.**

- a. Console into the router and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
```

```
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. Configure the host name as shown in the topology.
- d. Copy the running configuration to the startup configuration.

**Step 5: Configure static routing.**

- a. Create a static route from the ISP router to the Gateway router.

```
ISP(config)# ip route 209.165.200.224 255.255.255.248 209.165.201.18
```

- b. Create a default route from the Gateway router to the ISP router.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

**Step 6: Verify network connectivity.**

- a. From the PC hosts, ping the G0/1 interface on the Gateway router. Troubleshoot if the pings are unsuccessful.
- b. Verify that the static routes are configured correctly on both routers.

**Part 2: Configure and Verify NAT Pool Overload**

In Part 2, you will configure the Gateway router to translate the IP addresses from the 192.168.1.0/24 network to one of the six usable addresses in the 209.165.200.224/29 range.

**Step 1: Define an access control list that matches the LAN private IP addresses.**

ACL 1 is used to allow the 192.168.1.0/24 network to be translated.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

**Step 2: Define the pool of usable public IP addresses.**

```
Gateway(config)# ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

**Step 3: Define the NAT from the inside source list to the outside pool.**

```
Gateway(config)# ip nat inside source list 1 pool public_access overload
```

**Step 4: Specify the interfaces.**

Issue the **ip nat inside** and **ip nat outside** commands to the interfaces.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

**Step 5: Verify the NAT pool overload configuration.**

- a. From each PC host, ping the 192.31.7.1 address on the ISP router.

## Lab – Configuring Port Address Translation (PAT)

---

- b. Display NAT statistics on the Gateway router.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:25 ago
Outside interfaces:
 Serial0/0/1
Inside interfaces:
 GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 3
 pool public_access: netmask 255.255.255.248
 start 209.165.200.225 end 209.165.200.230
 type generic, total addresses 6, allocated 1 (16%), misses 0
```

Total doors: 0  
Appl doors: 0  
Normal doors: 0  
Queued Packets: 0

- c. Display NATs on the Gateway router.

```
Gateway# show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.165.200.225:0 192.168.1.20:1 192.31.7.1:1 192.31.7.1:0
icmp 209.165.200.225:1 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1
icmp 209.165.200.225:2 192.168.1.22:1 192.31.7.1:1 192.31.7.1:2
```

**Note:** Depending on how much time has elapsed since you performed the pings from each PC, you may not see all three translations. ICMP translations have a short timeout value.

How many Inside local IP addresses are listed in the sample output above? \_\_\_\_\_ 3

How many Inside global IP addresses are listed? \_\_\_\_\_ 1

How many port numbers are paired with the Inside global addresses? \_\_\_\_\_ 3

What would be the result of pinging the Inside local address of PC-A from the ISP router? Why?

---

---

The ping would fail because the router knows the location of the Inside global address in its routing table but the Inside local address is not advertised.

## Part 3: Configure and Verify PAT

In Part 3, you will configure PAT by using an interface instead of a pool of addresses to define the outside address. Not all of the commands in Part 2 will be reused in Part 3.

**Step 1: Clear NATs and statistics on the Gateway router.**

**Step 2: Verify the configuration for NAT.**

- a. Verify that statistics have been cleared.
- b. Verify that the outside and inside interfaces are configured for NATs.
- c. Verify that the ACL is still configured for NATs.

What command did you use to confirm the results from steps a to c?

---

```
Gateway# show ip nat statistics
```

**Step 3: Remove the pool of useable public IP addresses.**

```
Gateway(config)# no ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
```

**Step 4: Remove the NAT translation from inside source list to outside pool.**

```
Gateway(config)# no ip nat inside source list 1 pool public_access overload
```

**Step 5: Associate the source list with the outside interface.**

```
Gateway(config)# ip nat inside source list 1 interface serial 0/0/1 overload
```

**Step 6: Test the PAT configuration.**

- a. From each PC, ping the 192.31.7.1 address on the ISP router.
- b. Display NAT statistics on the Gateway router.

```
Gateway# show ip nat statistics
Total active translations: 3 (0 static, 3 dynamic; 3 extended)
Peak translations: 3, occurred 00:00:19 ago
Outside interfaces:
 Serial0/0/1
Inside interfaces:
 GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 interface Serial0/0/1 refcount 3
```

```
Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

- c. Display NAT translations on Gateway.

```
Gateway# show ip nat translations
Pro Inside global Inside local Outside local Outside global
```

## Lab – Configuring Port Address Translation (PAT)

---

icmp 209.165.201.18:3 192.168.1.20:1	192.31.7.1:1	192.31.7.1:3
icmp 209.165.201.18:1 192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
icmp 209.165.201.18:4 192.168.1.22:1	192.31.7.1:1	192.31.7.1:4

### Reflection

What advantages does PAT provide?

Answers will vary, but should include that PAT minimizes the number of public addresses needed to provide Internet access, and that PAT, like NAT, serves to “hide” private addresses from outside networks.

### Router Interface Summary Table

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

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

### Device Configs

#### Router Gateway (After Part 2)

```
Gateway# show run
Building configuration...
```

```
Current configuration : 1790 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Gateway
```

## Lab – Configuring Port Address Translation (PAT)

---

```
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 ip address 209.165.201.18 255.255.255.252
 ip nat outside
 ip virtual-reassembly in
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat pool public_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248
ip nat inside source list 1 pool public_access overload
ip route 0.0.0.0 0.0.0.0 209.165.201.17
!
```

## Lab – Configuring Port Address Translation (PAT)

---

```
access-list 1 permit 192.168.1.0 0.0.0.255
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### Router Gateway (After Part 3)

```
Gateway# show run
Building configuration...

Current configuration : 1711 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Gateway
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
```

## Lab – Configuring Port Address Translation (PAT)

---

```
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
!
interface Serial0/0/1
ip address 209.165.201.18 255.255.255.252
ip nat outside
ip virtual-reassembly in
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat inside source list 1 interface Serial0/0/1 overload
ip route 0.0.0.0 0.0.0.0 209.165.201.17
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
Control-plane
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
```

## Lab – Configuring Port Address Translation (PAT)

---

```
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

### Router ISP

```
ISP# show run
Building configuration...

Current configuration : 1487 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 10
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
interface Loopback0
 ip address 192.31.7.1 255.255.255.255
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

## Lab – Configuring Port Address Translation (PAT)

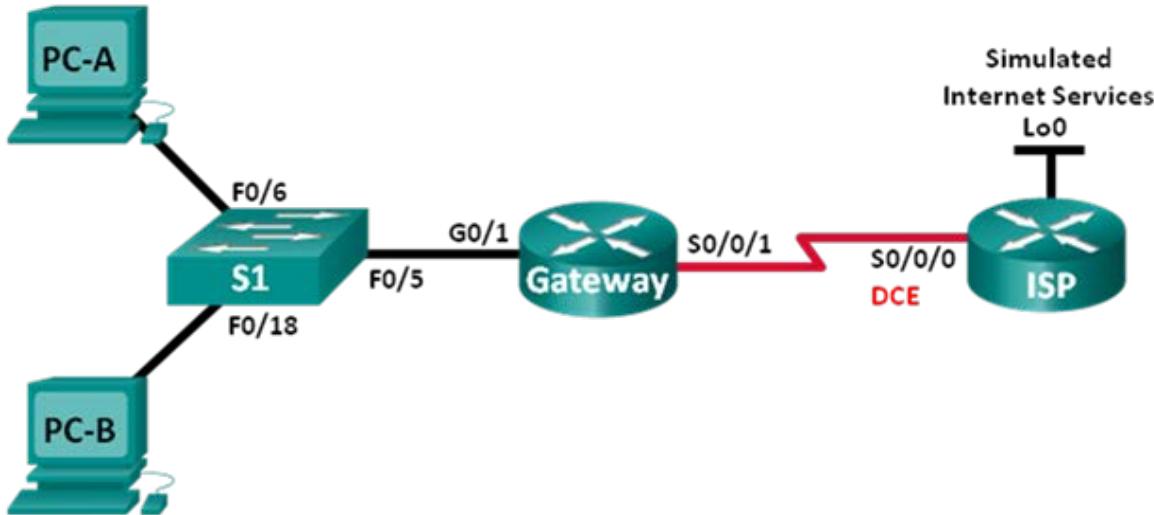
---

```
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
ip address 209.165.201.17 255.255.255.252
clock rate 128000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 209.165.200.224 255.255.255.224 209.165.201.18
!
control-plane
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

## Lab - Troubleshooting NAT Configurations (Instructor Version – Optional Lab)

**Instructor Note:** Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

### Topology



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.200.225	255.255.255.252	N/A
ISP	S0/0/0 (DCE)	209.165.200.226	255.255.255.252	N/A
	Lo0	198.133.219.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.4	255.255.255.0	192.168.1.1

### Objectives

**Part 1: Build the Network and Configure Basic Device Settings**

**Part 2: Troubleshoot Static NAT**

**Part 3: Troubleshoot Dynamic NAT**

### Background / Scenario

In this lab, the Gateway router was configured by an inexperienced network administrator at your company. Several errors in the configuration have resulted in NAT issues. Your boss has asked you to troubleshoot and correct the NAT errors and document your work. Ensure that the network supports the following:

## Lab - Troubleshooting NAT Configurations

---

- PC-A acts as a web server with a static NAT and will be reachable from the outside using the 209.165.200.254 address.
- PC-B acts as a host computer and dynamically receives an IP address from the created pool of addresses called NAT\_POOL, which uses the 209.165.200.240/29 range.

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

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

**Instructor Note:** Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

### Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

## Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure the routers with basic settings. Additional NAT-related configurations are provided. The NAT configurations for the Gateway router contains errors that you will identify and correct as you proceed through the lab.

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

**Step 2: Configure PC hosts.**

**Step 3: Initialize and reload the switch and routers.**

**Step 4: Configure basic settings for each router.**

- a. Console into the router and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
```

## Lab - Troubleshooting NAT Configurations

---

- ```
line vty 0 4
password cisco
login
```
- c. Configure the host name as shown in the topology.
 - d. Copy the running configuration to the startup configuration.

Step 5: Configure static routing.

- a. Create a static route from the ISP router to the Gateway router which was assigned public network address range 209.165.200.224/27.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 s0/0/0
```

- b. Create a default route from the Gateway router to the ISP router.

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

Step 6: Load router configurations.

The configurations for the routers are provided for you. There are errors with the configuration for the Gateway router. Identify and correct the configurations errors.

Gateway Router Configuration

```
interface g0/1
  ip nat outside
! ip nat inside
  no shutdown
interface s0/0/0
  ip nat outside
! no ip nat outside
interface s0/0/1
! ip nat outside
  no shutdown
  ip nat inside source static 192.168.2.3 209.165.200.254
! ip nat inside source static 192.168.1.3 209.165.200.254
ip nat pool NAT_POOL 209.165.200.241 209.165.200.246 netmask 255.255.255.248
ip nat inside source list NAT_ACL pool NATPOOL
! ip nat inside source list NAT_ACL pool NAT_POOL
ip access-list standard NAT_ACL
  permit 192.168.10.0 0.0.0.255
! permit 192.168.1.0 0.0.0.255
banner motd $AUTHORIZED ACCESS ONLY$
end
```

Step 7: Save the running configuration to the startup configuration.

Part 2: Troubleshoot Static NAT

In Part 2, you will examine the static NAT for PC-A to determine if it is configured correctly. You will troubleshoot the scenario until the correct static NAT is verified.

- a. To troubleshoot issues with NAT, use the **debug ip nat** command. Turn on NAT debugging to see translations in real-time across the Gateway router.

Lab - Troubleshooting NAT Configurations

```
Gateway# debug ip nat
```

- b. From PC-A, ping Lo0 on the ISP router. Do any NAT debug translations appear on the Gateway router?

No.

- c. On the Gateway router, enter the command that allows you to see all current NAT translations on the Gateway router. Write the command in the space below.

show ip nat translations

```
Gateway# show ip nat translations
```

| Pro | Inside global | Inside local | Outside local | Outside global |
|-----|-----------------|--------------|---------------|----------------|
| --- | 209.165.200.254 | 192.168.2.3 | --- | --- |

Why are you seeing a NAT translation in the table, but none occurred when PC-A pinged the ISP loopback interface? What is needed to correct the issue?

The static translation is for an incorrect inside local address.

- d. Record any commands that are necessary to correct the static NAT configuration error.

```
Gateway(config)# no ip nat inside source static 192.168.2.3 209.165.200.254
Gateway(config)# ip nat inside source static 192.168.1.3 209.165.200.254
```

- e. From PC-A, ping Lo0 on the ISP router. Do any NAT debug translations appear on the Gateway router?

No

- f. On the Gateway router, enter the command that allows you to observe the total number of current NATs. Write the command in the space below.

show ip nat statistics

```
Gateway# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 1, occurred 00:08:12 ago
Outside interfaces:
    GigabitEthernet0/1, Serial0/0/0
Inside interfaces:
Hits: 0 Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NAT_ACL pool NATPOOL refcount 0

Total doors: 0
Appl doors: 0
```

Lab - Troubleshooting NAT Configurations

```
Normal doors: 0  
Queued Packets: 0
```

Is the static NAT occurring successfully? Why?

No NAT translation is occurring because both of G0/1 and S0/0/0 interfaces are configured with the **ip nat outside** command. No active interfaces area assigned as inside.

- g. On the Gateway router, enter the command that allows you to view the current configuration of the router. Write the command in the space below.

show running-config

```
Gateway# show running-config  
Building configuration...  
  
Current configuration : 1806 bytes  
!  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname Gateway  
!  
boot-start-marker  
boot-end-marker  
!  
!  
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2  
!  
no aaa new-model  
!  
no ip domain lookup  
ip cef  
no ipv6 cef  
!  
multilink bundle-name authenticated  
!  
redundancy  
!  
interface GigabitEthernet0/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
ip address 192.168.1.1 255.255.255.0  
ip nat outside
```

Lab - Troubleshooting NAT Configurations

```
ip virtual-reassembly in
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
ip nat outside
ip virtual-reassembly in
shutdown
clock rate 2000000
!
interface Serial0/0/1
ip address 209.165.200.225 255.255.255.252
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat pool NAT_POOL 209.165.200.241 209.165.200.246 netmask 255.255.255.248
ip nat inside source list NAT_ACL pool NATPOOL
ip nat inside source static 192.168.1.3 209.165.200.254
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
ip access-list standard NAT_ACL
permit 192.168.10.0 0.0.0.255
!
!
!
control-plane
!
!
banner motd ^CAUTHORIZED ACCESS ONLY^C
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
```

Lab - Troubleshooting NAT Configurations

```
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

- h. Are there any problems with the current configuration that prevent the static NAT from occurring?

Yes. The inside and outside NAT interfaces are incorrectly configured.

- i. Record any commands that are necessary to correct the static NAT configuration errors.

```
Gateway(config)# interface g0/1
Gateway(config-if)# no ip nat outside
Gateway(config-if)# ip nat inside
Gateway(config-if)# exit
Gateway(config)# interface s0/0/0
Gateway(config-if)# no ip nat outside
Gateway(config-if)# exit
Gateway(config)# interface s0/0/1
Gateway(config-if)# ip nat outside
Gateway(config-if)# exit
```

- j. From PC-A, ping Lo0 on the ISP router. Do any NAT debug translations appear on the Gateway router?

Yes

```
*Mar 18 23:53:50.707: NAT*: s=192.168.1.3->209.165.200.254, d=198.133.219.1 [187]
*Mar 18 23:53:50.715: NAT*: s=198.133.219.1, d=209.165.200.254->192.168.1.3 [187]
Gateway#
*Mar 18 23:53:51.711: NAT*: s=192.168.1.3->209.165.200.254, d=198.133.219.1 [188]
*Mar 18 23:53:51.719: NAT*: s=198.133.219.1, d=209.165.200.254->192.168.1.3 [188]
*Mar 18 23:53:52.707: NAT*: s=192.168.1.3->209.165.200.254, d=198.133.219.1 [189]
Gateway#
*Mar 18 23:53:52.715: NAT*: s=198.133.219.1, d=209.165.200.254->192.168.1.3 [189]
*Mar 18 23:53:53.707: NAT*: s=192.168.1.3->209.165.200.254, d=198.133.219.1 [190]
Gateway#
*Mar 18 23:53:53.715: NAT*: s=198.133.219.1, d=209.165.200.254->192.168.1.3 [190]
```

- k. Use the **show ip nat translations verbose** command to verify static NAT functionality.

Note: The timeout value for ICMP is very short. If you do not see all the translations in the output, redo the ping.

```
Gateway# show ip nat translations verbose
Pro Inside global           Inside local          Outside local        Outside global
icmp 209.165.200.254:1     192.168.1.3:1       198.133.219.1:1    198.133.219.1:1
```

Lab - Troubleshooting NAT Configurations

```
create 00:00:04, use 00:00:01 timeout:60000, left 00:00:58,
flags:
extended, use_count: 0, entry-id: 12, lc_entries: 0
--- 209.165.200.254      192.168.1.3      ---      ---
create 00:30:09, use 00:00:04 timeout:0,
flags:
static, use_count: 1, entry-id: 2, lc_entries: 0
```

Is the static NAT translation occurring successfully? _____ Yes

If static NAT is not occurring, repeat the steps above to troubleshoot the configuration.

Part 3: Troubleshoot Dynamic NAT

- From PC-B, ping Lo0 on the ISP router. Do any NAT debug translations appear on the Gateway router?
_____ No
- On the Gateway router, enter the command that allows you to view the current configuration of the router. Are there any problems with the current configuration that prevent dynamic NAT from occurring?

Yes. The NAT pool is incorrectly identified in the source statement. The NAT access list has an incorrect network statement.

- Record any commands that are necessary to correct the dynamic NAT configuration errors.

```
Gateway(config)# no ip nat inside source list NAT_ACL pool NATPOOL
Gateway(config)# ip nat inside source list NAT_ACL pool NAT_POOL
Gateway(config)# ip access-list standard NAT_ACL
Gateway(config-std-nacl)# no permit 192.168.10.0 0.0.0.255
Gateway(config-std-nacl)# permit 192.168.1.0 0.0.0.255
```

- From PC-B, ping Lo0 on the ISP router. Do any NAT debug translations appear on the Gateway router?

Yes

```
*Mar 19 00:01:17.303: NAT*: s=192.168.1.4->209.165.200.241, d=198.133.219.1 [198]
*Mar 19 00:01:17.315: NAT*: s=198.133.219.1, d=209.165.200.241->192.168.1.4 [198]
Gateway#
*Mar 19 00:01:18.307: NAT*: s=192.168.1.4->209.165.200.241, d=198.133.219.1 [199]
*Mar 19 00:01:18.315: NAT*: s=198.133.219.1, d=209.165.200.241->192.168.1.4 [199]
*Mar 19 00:01:19.303: NAT*: s=192.168.1.4->209.165.200.241, d=198.133.219.1 [200]
Gateway#
*Mar 19 00:01:19.315: NAT*: s=198.133.219.1, d=209.165.200.241->192.168.1.4 [200]
*Mar 19 00:01:20.303: NAT*: s=192.168.1.4->209.165.200.241, d=198.133.219.1 [201]
*Mar 19 00:01:20.311: NAT*: s=198.133.219.1, d=209.165.200.241->192.168.1.4 [201]
```

- Use the **show ip nat statistics** to view NAT usage.

```
Gateway# show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 0 extended)
```

Lab - Troubleshooting NAT Configurations

```
Peak translations: 3, occurred 00:02:58 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 24 Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:
-- Inside Source
[Id: 2] access-list NAT_ACL pool NAT_POOL refcount 1
pool 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

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Is the NAT occurring successfully? _____ Yes

What percentage of dynamic addresses has been allocated? _____ 16%

- f. Turn off all debugging using the **undebug all** command.

Reflection

1. What is the benefit of a static NAT?

A static NAT translation allows users from outside the LAN to access a computer or server on the internal network.

2. What issues would arise if 10 host computers in this network were attempting simultaneous Internet communication?

Not enough public addresses exist in the NAT pool to satisfy 10 simultaneous user sessions. As hosts drop off, different hosts will be able to claim the pool addresses to access the Internet.

Router Interface Summary Table

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

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

Device Config

Router Gateway

```
Gateway#show run
```

```
Building configuration...
```

```
Current configuration : 1805 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Gateway
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ip domain lookup
ip cef
no ipv6 cef
```

Lab - Troubleshooting NAT Configurations

```
!
multilink bundle-name authenticated
!
redundancy
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
!
interface Serial0/0/1
ip address 209.165.200.225 255.255.255.252
ip nat outside
ip virtual-reassembly in
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat pool NAT_POOL 209.165.200.241 209.165.200.246 netmask 255.255.255.248
ip nat inside source list NAT_ACL pool NAT_POOL
ip nat inside source static 192.168.1.3 209.165.200.254
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
ip access-list standard NAT_ACL
permit 192.168.1.0 0.0.0.255
!
control-plane
!
banner motd ^CAUTHORIZED ACCESS ONLY^C
!
line con 0
```

Lab - Troubleshooting NAT Configurations

```
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Router ISP

```
ISP#show run
Building configuration...

Current configuration : 1482 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
no ip domain lookup
ip cef
!
no ipv6 cef
multilink bundle-name authenticated
!
interface Loopback0
 ip address 198.133.219.1 255.255.255.255
```

Lab - Troubleshooting NAT Configurations

```
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
ip address 209.165.200.226 255.255.255.252
clock rate 128000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 209.165.200.224 255.255.255.224 Serial0/0/0
!
control-plane
!
line con 0
password cisco
logging synchronous
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password cisco
login
```

Lab - Troubleshooting NAT Configurations

```
transport input all
line vty 5 15
password cisco
login
transport input all
!
scheduler allocate 20000 1000
!
end
```



NAT Check (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objective

Configure, verify and analyze static NAT, dynamic NAT and NAT with overloading.

Instructor Note: This activity can be completed individually or in small or large groups.

Scenario

Network address translation is not currently included in your company's network design. It has been decided to configure some devices to use NAT services for connecting to the mail server.

Before deploying NAT live on the network, you prototype it using a network simulation program.

Resources

- Packet Tracer software
- Word processing or presentation software

Directions

Step 1: Create a very small network topology using Packet Tracer, including, at minimum:

- a. Two 1941 routers, interconnected
- b. Two LAN switches, one per router
- c. One mail server, connected to the LAN on one router
- d. One PC or laptop, connected the LAN on the other router

Step 2: Address the topology.

- a. Use private addressing for all networks, hosts, and device.
- b. DHCP addressing of the PC or laptop is optional.
- c. Static addressing of the mail server is mandatory.

Step 3: Configure a routing protocol for the network.

Step 4: Validate full network connectivity without NAT services.

- a. Ping from one end of the topology and back to ensure the network is functioning fully.
- b. Troubleshoot and correct any problems preventing full network functionality.

Step 5: Configure NAT services on either router from the host PC or laptop to the mail server

Step 6: Produce output validating NAT operations on the simulated network.

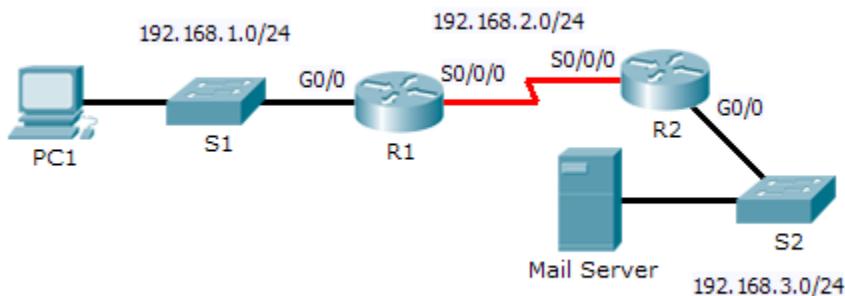
- a. Use the **show ip nat statistics**, **show access-lists**, and **show ip nat translations** commands to gather information about NAT's operation on the router
- b. Copy and paste or save screenshots of the topology and output information to a word processing or presentation document.

NAT Check

Step 7: Explain the NAT design and output to another group or to the class.

Suggested Activity Example (student designs will vary):

NAT Topology Diagram



```
R2# show ip nat translations
```

```
Pro Inside global     Inside local     Outside local     Outside global
icmp 192.168.1.1:2    192.168.1.2:2    192.168.3.2:2    192.168.3.2:2
```

```
R2# show ip nat statistics
```

```
Total translations: 1 (0 static, 1 dynamic, 1 extended)
Outside Interfaces: GigabitEthernet0/0
Inside Interfaces: Serial0/0/0
Hits: 2 Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool R1 refCount 1
pool R1: netmask 255.255.255.0
  start 192.168.1.1 end 192.168.1.254
  type generic, total addresses 254 , allocated 1 (0%), misses 0
```

```
R2# show access-lists
```

```
Standard IP access list 1
 permit 192.168.1.0 0.0.0.255 (6 match(es))
```

Identify elements of the model that map to IT-related content:

NAT

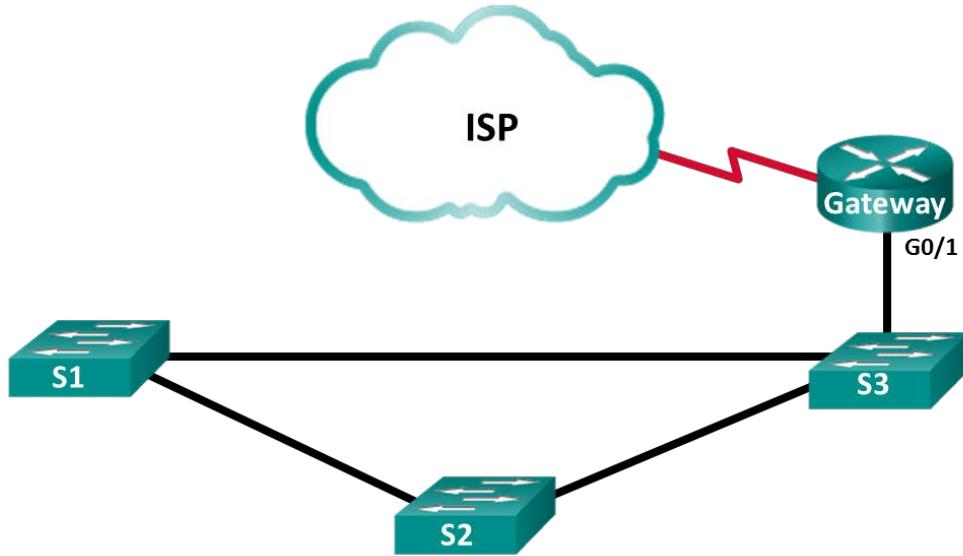
1. Configuration

- 2. Operation
- 3. Troubleshooting

Lab - Configure CDP and LLDP (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

| Device | Interface | IP Address | Subnet Mask |
|---------|--------------|-----------------|-----------------|
| Gateway | G0/1 | 192.168.1.254 | 255.255.255.0 |
| | S0/0/1 | 209.165.200.226 | 255.255.255.252 |
| ISP | S0/0/1 (DCE) | 209.165.200.225 | 255.255.255.252 |

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Network Discovery with CDP

Part 3: Network Discovery with LLDP

Background / Scenario

Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol for network discovery on the data link layer. It can share information such as device names and IOS versions, with other physically connected Cisco devices. Link Layer Discovery Protocol (LLDP) is vendor-neutral protocol using on the data link layer for network discovery. It is mainly used with network devices in the local area network (LAN). The network devices advertise information, such as their identities and capabilities to their neighbors.

In this lab, you must document the ports that are connected to other switches using CDP and LLDP. You will document your findings in a network topology diagram. You will also enable or disable these discovery protocols as necessary.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco

IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

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

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

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

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings on the router and switches.

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

The Ethernet ports used on the switches are not specified in the topology. You may choose to use any Ethernet ports to cable the switches as shown in the topology diagram.

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

Step 3: Configure basic device settings for the switches.

- a. Console into the device and enable privileged EXEC mode.
- b. Enter configuration mode.
- c. Disable DNS lookup to prevent the switch from attempting to translate incorrectly entered commands as though they were host names.
- d. Configure the hostname according to the topology.
- e. Verify that the switchports with connected Ethernet cables are enabled.
- f. Save the running configuration to the startup configuration file.

Step 4: Configure basic device settings for the routers.

- a. Console into the device and enable privileged EXEC mode.
- b. Enter configuration mode.
- c. Copy and paste the following configurations into the routers.

ISP:

```
hostname ISP
no ip domain lookup
interface Serial0/0/1
  ip address 209.165.200.225 255.255.255.252
  no shutdown
```

Gateway:

```
hostname Gateway
no ip domain lookup
interface GigabitEthernet0/1
  ip address 192.168.1.254 255.255.255.0
  ip nat inside
  no shutdown
interface Serial0/0/1
  ip address 209.165.200.226 255.255.255.252
  ip nat outside
  no shutdown
  ip nat inside source list 1 interface Serial0/0/1 overload
  access-list 1 permit 192.168.1.0 0.0.0.255
```

- d. Save the running configuration to the startup configuration file.

Part 2: Network Discovery with CDP

On Cisco devices, CDP is enabled by default. You will use CDP to discover the ports that are currently connected.

- a. On router Gateway, enter the **show cdp** command in the privileged EXEC mode to verify that CDP is currently enabled on router Gateway.

```
Gateway# show cdp
```

Global CDP information:

```
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
```

How often are CDP packets sent?

CDP packets are sent out every 60 seconds.

If CDP is disabled on Gateway, enable CDP by issuing the **cdp run** command in the global configuration mode.

```
Gateway(config)# cdp run
```

```
Gateway(config)# end
```

- b. Issue the **show cdp interface** to list the interfaces that are participating in CDP advertisements.

```
Gateway# show cdp interface
```

```
Embedded-Service-Engine0/0 is administratively down, line protocol is down
```

```
  Encapsulation ARPA
```

```
  Sending CDP packets every 60 seconds
```

```
  Holdtime is 180 seconds
```

```
GigabitEthernet0/0 is administratively down, line protocol is down
```

```
  Encapsulation ARPA
```

```
  Sending CDP packets every 60 seconds
```

```
  Holdtime is 180 seconds
```

```
GigabitEthernet0/1 is up, line protocol is up
```

Lab – Configure CDP and LLDP

```
Encapsulation ARPA
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
Serial0/0/0 is administratively down, line protocol is down
Encapsulation HDLC
Sending CDP packets every 60 seconds
Holdtime is 180 seconds
Serial0/0/1 is up, line protocol is up
Encapsulation HDLC
Sending CDP packets every 60 seconds
Holdtime is 180 seconds

cdp enabled interfaces : 5
interfaces up          : 2
interfaces down        : 3
```

How many interfaces are participating in the CDP advertisement? Which interfaces are up?

Five interfaces are participating in CDP. The interfaces S0/0/1 and G0/1 are up.

- c. Issue the **show cdp neighbors** command to determine the CDP neighbors.

```
Gateway# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
```

| Device ID | Local Intrfce | Holdtme | Capability | Platform | Port ID |
|-----------|---------------|---------|------------|-----------|-----------|
| ISP | Ser 0/0/1 | 158 | R B S I | CISCO1941 | Ser 0/0/1 |
| S3 | Gig 0/1 | 170 | S I | WS-C2960- | Fas 0/5 |

- d. For more details on CDP neighbors, issue the **show cdp neighbors detail** command.

```
Gateway# show cdp neighbors detail
-----
Device ID: ISP
Entry address(es):
  IP address: 209.165.200.225
Platform: Cisco CISCO1941/K9,  Capabilities: Router Source-Route-Bridge
Switch IGMP
Interface: Serial0/0/1,  Port ID (outgoing port): Serial0/0/1
Holdtime : 143 sec
```

Version :

```
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.4(3)M2,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Fri 06-Feb-15 17:01 by prod_rel_team
```

Lab – Configure CDP and LLDP

```
advertisement version: 2
Management address(es):
  IP address: 209.165.200.225

-----
Device ID: S3
Entry address(es):
Platform: cisco WS-C2960-24TT-L, Capabilities: Switch IGMP
Interface: GigabitEthernet0/1, Port ID (outgoing port): FastEthernet0/5
Holdtime : 158 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 23-Oct-14 14:49 by prod_rel_team
```

```
advertisement version: 2
Protocol Hello: OUI=0x00000C, Protocol ID=0x0112; payload len=27,
value=00000000FFFFFFFFFF010221FF000000000000CD996E87400FF0000
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
```

- e. What can you learn about ISP and S3 from the outputs of the **show cdp neighbors detail** command?
-

The output displays the IOS version, device model, and the IP Address on S0/0/1 interface for ISP. On S3, the output shows information, such as the IOS version, VTP management domain, and native VLAN, duplex.

- f. Configure the SVI on S3. Use an available IP address in 192.168.1.0 / 24 network. Configure 192.168.1.254 as the default gateway.

```
S3(config)# interface vlan 1
S3(config-if)# ip address 192.168.1.3 255.255.255.0
S3(config-if)# no shutdown
S3(config-if)# exit
S3(config)# ip default-gateway 192.168.1.254
```

- g. Issue the **show cdp neighbors detail** command on Gateway. What additional information is available?
-

The output includes the IP address for SVI on S3 that was just configured.

```
Gateway# show cdp neighbors detail | begin s3
Device ID: S3
Entry address(es):
```

Lab – Configure CDP and LLDP

```
IP address: 192.168.1.3
Platform: cisco WS-C2960-24TT-L, Capabilities: Switch IGMP
Interface: GigabitEthernet0/1, Port ID (outgoing port): FastEthernet0/5
Holdtime : 163 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 23-Oct-14 14:49 by prod_rel_team

advertisement version: 2
Protocol Hello: OUI=0x00000C, Protocol ID=0x0112; payload len=27,
value=00000000FFFFFFFFFF010221FF000000000000CD996E87400FF0000
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
Management address(es):
IP address: 192.168.1.3
```

Total cdp entries displayed : 2

- h. For security reasons, it is a good idea to turn off CDP on an interface facing an external network. Issue the **no cdp enable** in the interface configuration mode on the S0/0/1 interface on Gateway.

```
Gateway(config)# interface s0/0/1
Gateway(config-if)# no cdp enable
Gateway(config-if)# end
```

To verify that CDP has been turned off on the interface S0/0/1, issue the **show cdp neighbors** or **show cdp interface** command. You may need to wait for the hold time to expire. The hold time is the amount of time the network devices will hold the CDP packets until the devices discard them.

```
Gateway# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
```

| Device ID | Local Intrfce | Holddtme | Capability | Platform | Port ID |
|-----------|---------------|----------|------------|-----------|---------|
| S3 | Gig 0/1 | 161 | S I | WS-C2960- | Fas 0/5 |

The interface S0/0/1 on Gateway no longer has a CDP adjacency with the ISP router. But it still has CDP adjacencies with other interfaces.

```
Gateway# show cdp interface
Embedded-Service-Engine0/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

Lab – Configure CDP and LLDP

```
GigabitEthernet0/0 is administratively down, line protocol is down  
  Encapsulation ARPA  
    Sending CDP packets every 60 seconds  
    Holdtime is 180 seconds  
GigabitEthernet0/1 is up, line protocol is up  
  Encapsulation ARPA  
    Sending CDP packets every 60 seconds  
    Holdtime is 180 seconds  
Serial0/0/0 is administratively down, line protocol is down  
  Encapsulation HDLC  
    Sending CDP packets every 60 seconds  
    Holdtime is 180 seconds  
  
cdp enabled interfaces : 4  
interfaces up : 1  
interfaces down : 3
```

- i. To disable CDP globally, issue the **no cdp run** command in the global configuration mode.

```
Gateway# conf t  
Gateway(config)# no cdp run  
Gateway(config)# end
```

Which command(s) would you use to verify that CDP has been disabled?

show cdp, show cdp neighbors, show cdp neighbors detail, or show cdp interface

- j. Enable CDP globally on Gateway. How many interfaces are CDP enabled? Which interfaces are CDP disabled?

Four interfaces are CDP enabled. The interface S0/0/1 is CDP disabled.

- k. Console into all the switches and use the CDP commands to determine the Ethernet ports that connected to other devices. An example of the CDP commands for S3 is displayed below.

```
S3# show cdp neighbors  
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge  
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,  
                  D - Remote, C - CVTA, M - Two-port Mac Relay
```

| Device ID | Local Intrfce | Holdtme | Capability | Platform | Port ID |
|-----------|---------------|---------|------------|-----------|---------|
| Gateway | Fas 0/5 | 143 | R B S I | CISCO1941 | Gig 0/1 |
| S2 | Fas 0/2 | 173 | S I | WS-C2960- | Fas 0/4 |
| S1 | Fas 0/4 | 171 | S I | WS-C2960- | Fas 0/4 |

Part 3: Network Discovery with LLDP

On Cisco devices, LLDP maybe enabled by default. You will use LLDP to discover the ports that are currently connected.

- a. On Gateway, enter the **show lldp** command in the privileged EXEC mode.

Lab – Configure CDP and LLDP

```
Gateway# show lldp  
% LLDP is not enabled
```

If LLDP is disabled, enter the **lldp run** command in the global configuration mode.

```
Gateway(config)# lldp run
```

- b. Use the **show lldp** command to verify that LLDP is enabled on Gateway.

```
Gateway# show lldp
```

Global LLDP Information:

```
Status: ACTIVE  
LLDP advertisements are sent every 30 seconds  
LLDP hold time advertised is 120 seconds  
LLDP interface reinitialisation delay is 2 seconds
```

Issue the **show lldp neighbors** command. Which devices are neighbors to Gateway?

Currently there are no neighbors.

- c. If there are no LLDP neighbors for Gateway, enable LLDP on the switches and ISP. Issue **lldp run** in the global configuration mode on the devices.

```
S1(config)# lldp run  
S2(config)# lldp run  
S3(config)# lldp run  
ISP(config)# lldp run
```

- d. Issue the **show lldp neighbors** command on the switches and router to list the LLDP enabled ports. The output for Gateway is shown below.

```
Gateway# show lldp neighbors
```

Capability codes:

```
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device  
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
```

| Device ID | Local Intf | Hold-time | Capability | Port ID |
|-----------|------------|-----------|------------|---------|
| S3 | Gi0/1 | 120 | B | Fa0/5 |

Total entries displayed: 1

- e. Issue the **show lldp neighbors detail** command on Gateway.

```
Gateway# show lldp neighbors detail
```

```
-----  
Local Intf: Gi0/1  
Chassis id: 0cd9.96e8.7400  
Port id: Fa0/5  
Port Description: FastEthernet0/5  
System Name: S3
```

System Description:

Lab – Configure CDP and LLDP

```
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 23-Oct-14 14:49 by prod_rel_team
```

```
Time remaining: 103 seconds
System Capabilities: B
Enabled Capabilities: B
Management Addresses:
    IP: 192.168.1.3
Auto Negotiation - supported, enabled
Physical media capabilities:
    100base-TX(FD)
    100base-TX(HD)
    10base-T(FD)
    10base-T(HD)
Media Attachment Unit type: 16
Vlan ID: 1
```

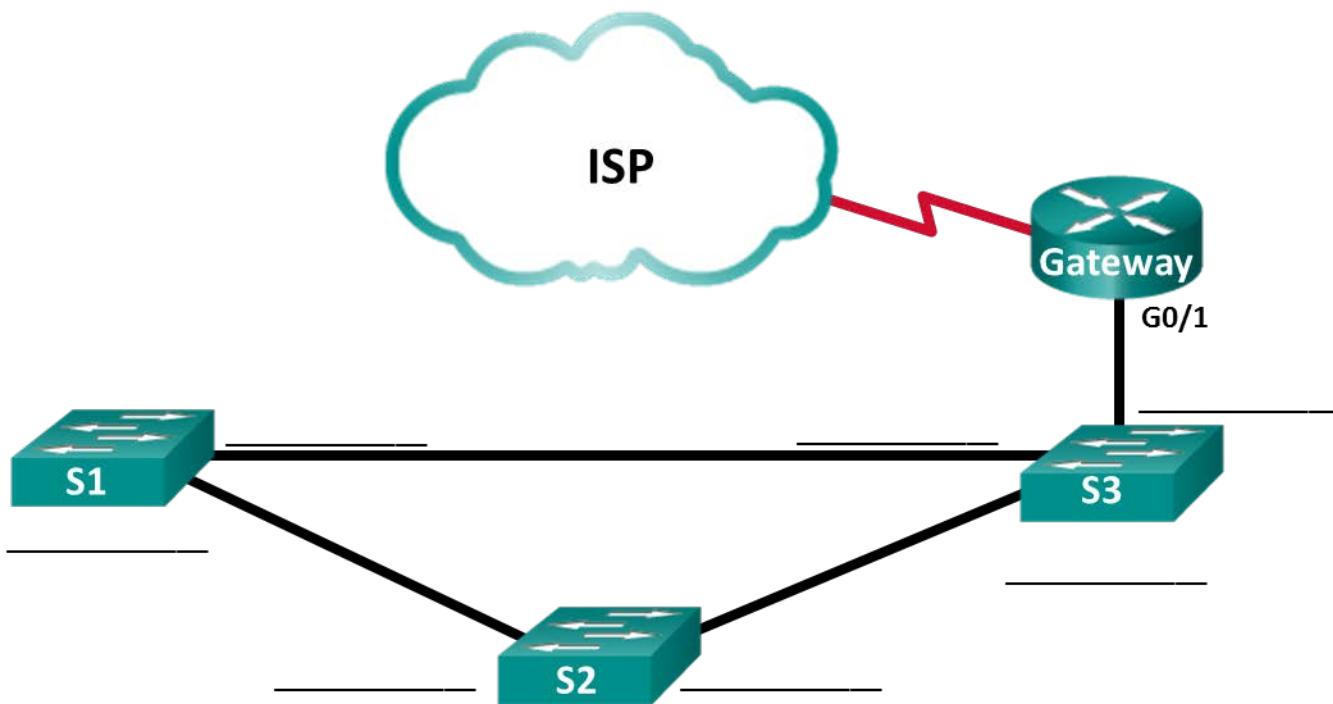
Total entries displayed: 1

What port is used on S3 to connect to the Gateway router?

Port Fa0/5 is used on S3 is connected to the Gi0/1 port on Gateway.

- f. Use the **show** command outputs from CDP and LLDP to document the connected ports in the network topology.

Lab – Configure CDP and LLDP



Reflection

Within a network, on which interfaces should you not use discovery protocols? Explain.

Discovery protocols should not be used on interfaces that are facing the external networks because these protocols provide insights about the internal network. This information allows attackers to gain valuable information about the internal network and exploit the network.

Router Interface Summary Table

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

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

Device Configs - Final

Router ISP

```
ISP# show run
Building configuration...

Current configuration : 1285 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 15
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
```

Lab – Configure CDP and LLDP

```
!
cts logging verbose
!
redundancy
!
lldp run
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
!
interface Serial0/0/1
ip address 209.165.200.225 255.255.255.252
clock rate 125000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
login
transport input none
```

Lab – Configure CDP and LLDP

```
!
scheduler allocate 20000 1000
!
end
```

Router Gateway

```
Gateway# show run
Building configuration...

Current configuration : 1524 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Gateway
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 15
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
redundancy
!
lldp run
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.254 255.255.255.0
 ip nat inside
```

Lab – Configure CDP and LLDP

```
ip virtual-reassembly in
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 125000
!
interface Serial0/0/1
ip address 209.165.200.226 255.255.255.252
ip nat outside
ip virtual-reassembly in
no cdp enable
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat inside source list 1 interface Serial0/0/1 overload
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
control-plane
!
line con 0
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
login
transport input none
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
S1# show run
Building configuration...

Current configuration : 1308 bytes
!
version 15.0
```

Lab – Configure CDP and LLDP

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
system mtu routing 1500
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
lldp run
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
```

Lab – Configure CDP and LLDP

```
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
    no ip address
!
ip http server
ip http secure-server
!
line con 0
line vty 5 15
!
end
```

Switch S2

```
S2# show run
Building configuration...

Current configuration : 1308 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S2
!
boot-start-marker
boot-end-marker
```

Lab – Configure CDP and LLDP

```
!
no aaa new-model
system mtu routing 1500
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
lldp run
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
```

Lab – Configure CDP and LLDP

```
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
!
ip http server
ip http secure-server
!
line con 0
line vty 5 15
!
end
```

Switch S3

```
S3# show run
Building configuration...

Current configuration : 1364 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S3
!
boot-start-marker
boot-end-marker
!
no aaa new-model
system mtu routing 1500
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
lldp run
```

Lab – Configure CDP and LLDP

```
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
```

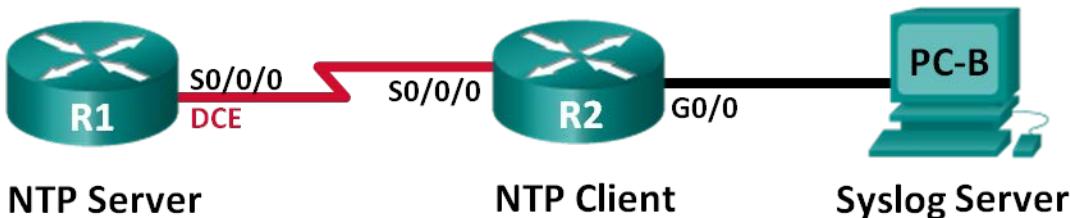
Lab – Configure CDP and LLDP

```
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
    no ip address
!
ip http server
ip http secure-server
!
line con 0
line vty 5 15
!
end
```

Lab – Configuring Syslog and NTP (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|--------|--------------|------------|-----------------|-----------------|
| R1 | S0/0/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N/A |
| R2 | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/A |
| | G0/0 | 172.16.2.1 | 255.255.255.0 | N/A |
| PC-B | NIC | 172.16.2.3 | 255.255.255.0 | 172.16.2.1 |

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure NTP

Part 3: Configure Syslog

Background / Scenario

Syslog messages that are generated by the network devices can be collected and archived on a syslog server. The information can be used for monitoring, debugging, and troubleshooting purposes. The administrator can control where the messages are stored and displayed. Syslog messages can be timestamped for analysis of the sequence of network events; therefore, it is important to synchronize the clock across the network devices with a Network Time Protocol (NTP) server.

In this lab, you will configure R1 as the NTP server and R2 as a Syslog and NTP client. The syslog server application, such as Tftp32d or other similar program, will be running on PC-B. Furthermore, you will control the severity level of log messages that are collected and archived on the syslog server.

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

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

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term, and Syslog software, such as Tftpd32)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Configure Basic Device Settings

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

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

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings for each router.

- a. Console into the router and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

- c. Configure the host name as shown in the topology.
- d. Apply the IP addresses to Serial and Gigabit Ethernet interfaces according to the Addressing Table and activate the physical interfaces.
- e. Set the clock rate to **128000** for the DCE serial interface.

Step 4: Configure routing.

Enable RIPv2 on the routers. Add all the networks into the RIPv2 process.

Step 5: Configure PC-B.

Configure the IP address and default gateway for PC-B according to the Addressing Table.

Step 6: Verify end-to-end connectivity.

Verify that each device is able to ping every other device in the network successfully. If not, troubleshoot until there is end-to-end connectivity.

Step 7: Save the running configuration to the startup configuration.

Part 2: Configure NTP

In Part 2, you will configure R1 as the NTP server and R2 as the NTP client of R1. Synchronized time is important for syslog and debug functions. If the time is not synchronized, it is difficult to determine what network event caused the message.

Step 1: Display the current time.

Issue the **show clock** command to display the current time on R1.

```
R1# show clock  
*12:30:06.147 UTC Tue May 14 2013
```

Record the information regarding the current time displayed in the following table.

| | |
|-----------|-------------------------------------------------|
| Date | Answer will vary. In this example: May 14, 2013 |
| Time | Answer will vary. In this example: 12:30:06.147 |
| Time Zone | Answer will vary. In this example: UTC |

Step 2: Set the time.

Use the **clock set** command to set the time on R1. The following is an example of setting the date and time.

```
R1# clock set 9:39:00 05 july 2013  
R1#  
*Jul  5 09:39:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 12:30:54  
UTC Tue May 14 2013 to 09:39:00 UTC Fri Jul 5 2013, configured from console by  
console.
```

Note: The time can also be set using the **clock timezone** command in the global configuration mode. For more information regarding this command, research the **clock timezone** command at www.cisco.com to determine the zone for your region.

Step 3: Configure the NTP master.

Configure R1 as the NTP master by using the **ntp master stratum-number** command in global configuration mode. The stratum number indicates the number of NTP hops away from an authoritative time source. In this lab, the number 5 is the stratum level of this NTP server.

```
R1(config)# ntp master 5
```

Step 4: Configure the NTP client.

- Issue **show clock** command on R2. Record the current time displayed on R2 in the following table.

| | |
|-----------|-------------------|
| Date | Answer will vary. |
| Time | Answer will vary. |
| Time Zone | Answer will vary. |

- b. Configure R2 as the NTP client. Use the **ntp server** command to point to the IP address or hostname of the NTP server. The **ntp update-calendar** command periodically updates the calendar with NTP time.

```
R2(config)# ntp server 10.1.1.1  
R2(config)# ntp update-calendar
```

Step 5: Verify NTP configuration.

- a. Use the **show ntp associations** command to verify that R2 has an NTP association with R1.

```
R2# show ntp associations
```

| address | ref clock | st | when | poll | reach | delay | offset | disp |
|-----------------------------------------------------------------------------|-------------|----|------|------|-------|--------|--------|-------|
| *~10.1.1.1 | 127.127.1.1 | 5 | 11 | 64 | 177 | 11.312 | -0.018 | 4.298 |
| * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured | | | | | | | | |

- b. Issue **show clock** on R1 and R2 to compare the timestamp.

Note: It could take a few minutes before the timestamp on R2 is synchronized with R1.

```
R1# show clock  
09:43:32.799 UTC Fri Jul 5 2013  
R2# show clock  
09:43:37.122 UTC Fri Jul 5 2013
```

Part 3: Configure Syslog

Syslog messages from network devices can be collected and archived on a syslog server. In this lab, Tftpd32 will be used as the syslog server software. The network administrator can control the types of messages that can be sent to the syslog server.

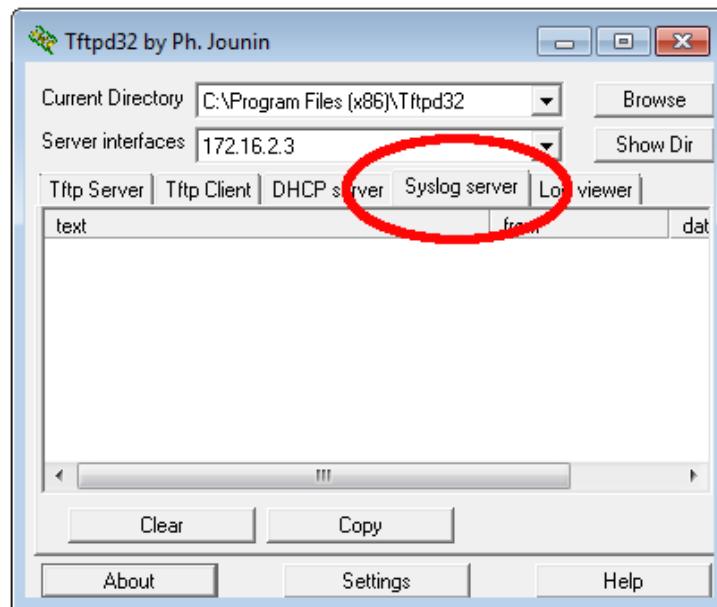
Step 1: (Optional) Install syslog server.

If a syslog server is not already installed on the PC, download and install the latest version of a syslog server, such as Tftpd32, on the PC. The latest version of Tftpd32 can be found at the following link:

<http://tftpd32.jounin.net/>

Step 2: Start the syslog server on PC-B.

After starting the Tftpd32 application, click the **syslog server** tab.



Step 3: Verify that the timestamp service is enabled on R2.

Use the **show run** command to verify that the timestamp service is enabled for logging on R2.

```
R2# show run | include timestamp
service timestamps debug datetime msec
service timestamps log datetime msec
```

If the timestamp service is not enabled, use the following command to enable it.

```
R2(config)# service timestamps log datetime msec
```

Step 4: Configure R2 to log messages to the syslog server.

Configure R2 to send Syslog messages to the syslog server, PC-B. The IP address of the PC-B syslog server is 172.16.2.3.

```
R2(config)# logging host 172.16.2.3
```

Step 5: Display the default logging settings.

Use the **show logging** command to display the default logging settings.

```
R2# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)
```

No Active Message Discriminator.

No Inactive Message Discriminator.

```
Console logging: level debugging, 47 messages logged, xml disabled,
filtering disabled
```

```
Monitor logging: level debugging, 0 messages logged, xml disabled,
```

Lab – Configuring Syslog and NTP

```
filtering disabled
Buffer logging: level debugging, 47 messages logged, xml disabled,
filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled

No active filter modules.
```

```
Trap logging: level informational, 49 message lines logged
Logging to 172.16.2.3 (udp port 514, audit disabled,
link up),
6 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled
```

Logging Source-Interface: VRF Name:

What is the IP address of the syslog server? 172.16.2.3

What protocol and port is syslog using? UDP port 514

At what level is trap logging enabled? informational

Step 6: Configure and observe the effect of logging severity levels on R2.

- Use the **logging trap ?** command to determine the various trap levels availability. When configuring a level, the messages sent to the syslog server are the trap level configured and any lower levels.

```
R2(config)# logging trap ?
<0-7>      Logging severity level
alerts       Immediate action needed          (severity=1)
critical     Critical conditions            (severity=2)
debugging    Debugging messages             (severity=7)
emergencies  System is unusable            (severity=0)
errors       Error conditions              (severity=3)
informational Informational messages       (severity=6)
notifications Normal but significant conditions (severity=5)
warnings     Warning conditions            (severity=4)
<cr>
```

If the **logging trap warnings** command was issued, which severity levels of messages are logged?

warnings (level 4) errors (level 3), critical (level 2), alerts (level 1), and emergency (level 0)

- Change the logging severity level to 4.

```
R2(config)# logging trap warnings
```

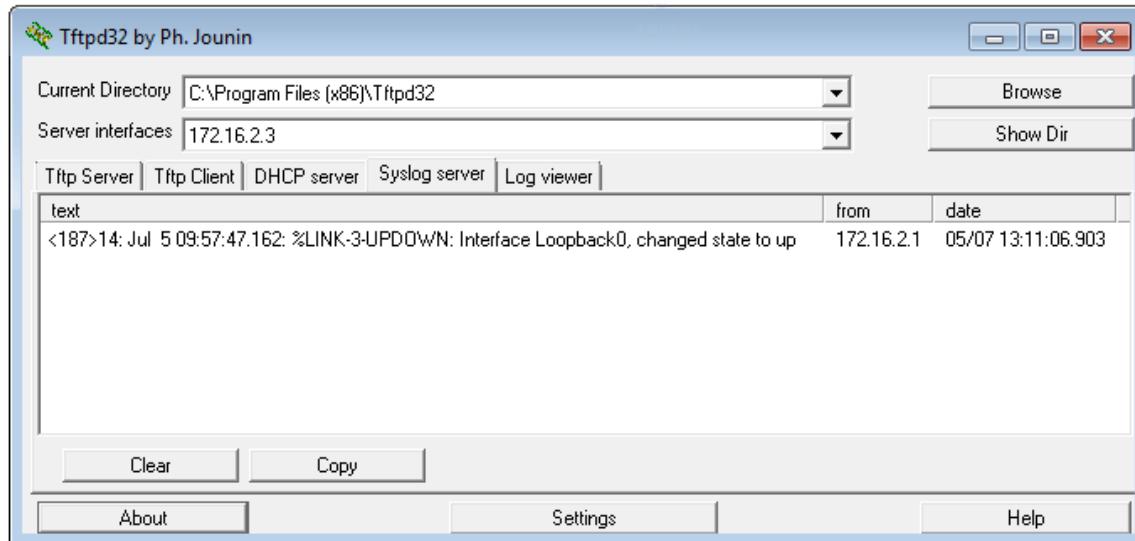
or

```
R2(config)# logging trap 4
```

- Create interface Loopback0 on R2 and observe the log messages on both the terminal window and the syslog server window on PC-B.

Lab – Configuring Syslog and NTP

```
R2(config)# interface lo 0
R2(config-if)#
Jul  5 09:57:47.162: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
Jul  5 09:57:48.162: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
```



- d. Remove the Loopback 0 interface on R2 and observe the log messages.

```
R2(config-if)# no interface lo 0
R2(config)#
Jul  5 10:02:58.910: %LINK-5-CHANGED: Interface Loopback0, changed state to
administratively down
Jul  5 10:02:59.910: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to down
```

At severity level 4, are there any log messages on the syslog server? If any log messages appeared, explain what appeared and why.

There was a summary warning log message indicating a change in the interface state. The addition of the interface was not enough to trigger and send more detailed informational messages to the syslog server at level 4.

- e. Change the logging severity level to 6.

```
R2(config)# logging trap informational
```

or

```
R2(config)# logging trap 6
```

- f. Clear the syslog entries on PC-B. Click **Clear** in the Tftpd32 dialog box.

- g. Create the Loopback 1 interface on R2.

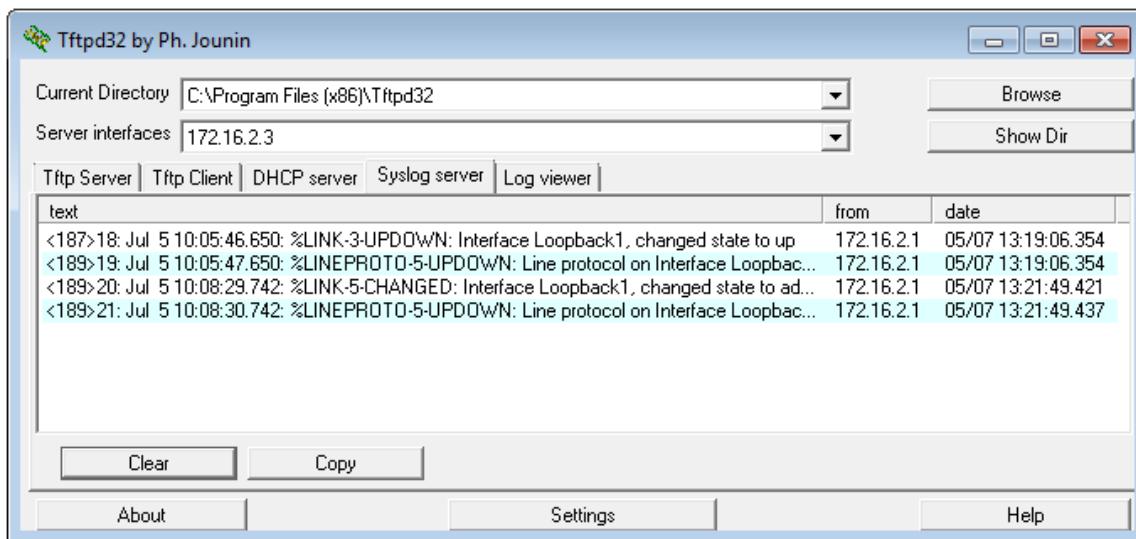
```
R2(config)# interface lo 1
```

Lab – Configuring Syslog and NTP

```
Jul  5 10:05:46.650: %LINK-3-UPDOWN: Interface Loopback1, changed state to up
Jul  5 10:05:47.650: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to up
```

- h. Remove the Loopback 1 interface from R2.

```
R2(config-if)# no interface lo 1
R2(config-if)#
Jul  5 10:08:29.742: %LINK-5-CHANGED: Interface Loopback1, changed state to
administratively down
Jul  5 10:08:30.742: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1,
changed state to down
```



- i. Observe the syslog server output. Compare this result with the results at trapping level 4. What is your observation?

More log messages were trapped when the severity was set to 6 (informational) than when it was set at 4 (warnings).

Reflection

What is the problem with setting the level of severity too high (lowest level number) or too low (highest level number) for syslog?

When the severity level is set too high (lowest level number), the generated log could be missing important, but not critical messages. However, setting it too low (highest level number), it can generate too many entries and fill the logs with unnecessary information.

Router Interface Summary Table

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

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

Device Configs

Router R1

```
R1#show run
Building configuration...

Current configuration : 1572 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAug.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
```

Lab – Configuring Syslog and NTP

```
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
redundancy
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
ip address 10.1.1.1 255.255.255.252
clock rate 128000
!
interface Serial0/0/1
no ip address
shutdown
!
router rip
version 2
network 10.1.1.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^CUnauthorized access is prohibited.^C
!
line con 0
password 7 110A1016141D
logging synchronous
login
```

Lab – Configuring Syslog and NTP

```
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 01100F175804
login
transport input all
!
scheduler allocate 20000 1000
ntp master 5
!
end
```

Router R2

Building configuration...

```
Current configuration : 1742 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
```

Lab – Configuring Syslog and NTP

```
shutdown
!
interface GigabitEthernet0/0
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router rip
 version 2
 network 10.1.1.0
 network 172.16.2.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
logging host 172.16.2.3
!
control-plane
!
banner motd ^CUnauthorized access is prohibited.^C
!
line con 0
 password 7 121A0C041104
 logging synchronous
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
```

Lab – Configuring Syslog and NTP

```
line vty 0 4
password 7 01100F175804
login
transport input all
!
scheduler allocate 20000 1000
ntp update-calendar
ntp server 10.1.1.1
!
end
```

Lab – Managing Router Configuration Files with Terminal Emulation Software (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Addressing Table

| Device | Interface | IP Address | Subnet Mask | Default Gateway |
|--------|-----------|--------------|---------------|-----------------|
| R1 | G0/1 | 192.168.1.1 | 255.255.255.0 | N/A |
| S1 | VLAN 1 | 192.168.1.11 | 255.255.255.0 | 192.168.1.1 |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |

Objectives

Part 1: Configure Basic Device Settings

Part 2: Use Terminal Emulation Software to Create a Backup Configuration File

Part 3: Use a Backup Configuration File to Restore a Router

Background / Scenario

It is a recommended best practice to maintain backup configuration files for routers and switches in the event that they need to be restored to a previous configuration. Terminal emulation software can be used to easily back up or restore a router or switch configuration file.

In this lab, you will use Tera Term to back up a router running configuration file, erase the router startup configuration file, reload the router, and then restore the missing router configuration from the backup configuration file.

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

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

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Instructor Note: This lab uses Tera Term 4.75. Tera Term should be installed on the PC prior to starting the lab. You can download the latest version from a number of Internet sites. Simply search for a Tera Term download.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Configure Basic Device Settings

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

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

Attach the devices as shown in the topology and cable as necessary.

Step 2: Configure the PC-A network settings according to the Addressing Table.

Step 3: Initialize and reload the router and switch.

Step 4: Configure the router.

- a. Console into the router and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on R1.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```
- c. Configure and activate the G0/1 interface on the router using the information contained in the Addressing Table.
- d. Save the running configuration to the startup configuration file.

Step 5: Configure the switch.

- a. Console into the switch and enter into global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on S1.

```
no ip domain-lookup
```

```
hostname S1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

- c. Configure the default SVI management interface with the IP address information contained in the Addressing Table.
- d. Configure the switch default gateway.
- e. Save the running configuration to the startup configuration file.

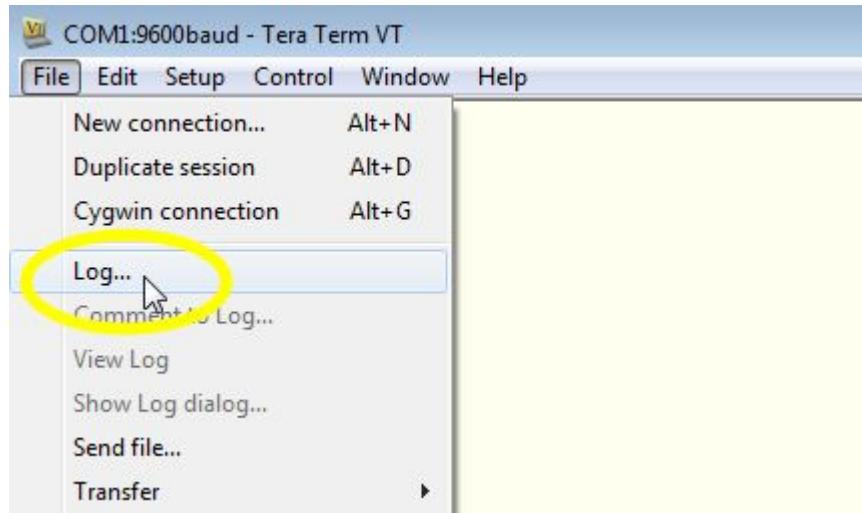
Part 2: Use Terminal Emulation Software to Create a Backup Configuration File

Step 1: Establish a Tera Term console session to the router.

Launch the Tera Term Program, and in the New Connection window, select the **Serial** radio button and the appropriate communications port for your PC (i.e., COM1).

Note: If Tera Term is not installed, you can download the latest version from a number of Internet sites. Simply search for a Tera Term download.

- a. In Tera Term, press Enter to connect to the router.
- b. From the **File** menu, choose **Log...**, and save the **teraterm.log** file to the Desktop. Ensure that the **Append** and **Plain text** check boxes are enabled (checked).

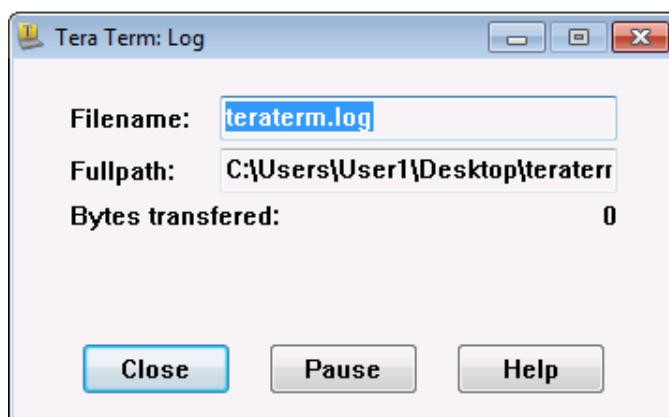


- c. The Tera Term log file will create a record of every command issued and every output displayed.

Note: You can use this feature to capture the output from several commands in sequence and use it for network documentation purposes. For example, you could issue the **show version**, **show ip interface brief**, and **show running-config** commands to capture information about the router.

Step 2: Display the router running-configuration.

- a. Use the console password to log in to the router.
- b. Enter privileged EXEC mode.
- c. Enter the **show running-config** command.
- d. Continue pressing the space bar when **--More--** is displayed until you see the router R1# prompt return.
- e. Click the **Tera Term: Log** icon on the Task bar. Click **Close** to end log session.



Note: You can also copy and paste the text from the Tera Term window directly into a text editor.

Part 3: Use a Backup Configuration File to Restore a Router

Step 1: Erase the router startup-configuration and reload.

- a. From privileged EXEC mode erase the startup configuration.

```
R1# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
```

- b. Reload the router.

```
R1# reload
Proceed with reload? [confirm]
```

- c. At the System Configuration Dialog prompt, type **no**; a router prompt displays, indicating an unconfigured router.

```
--- System Configuration Dialog ---
```

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

```
Press RETURN to get started!
```

```
<output omitted>
Router>
```

- d. Enter privileged EXEC mode and enter a **show running-config** command to verify that all of the previous configurations were erased.

Step 2: Edit the saved configuration backup file to prepare it for restoring the router configuration.

To restore the router configuration from a saved running configuration backup file, you must edit the text.

- a. Open the **teraterm.log** text file.
- b. Remove each instance of **--More--** in the text file.

Note: The **--More--** was generated by pressing the Spacebar when displaying the running configuration.

- c. Delete the initial lines of the backup configuration file, so that the first line starts with the first configuration command as shown below.

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
```

- d. In the lines for interface GigabitEthernet0/1, insert a new line to enable the interface.

```
interface GigabitEthernet0/1
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
```

Change to:

```
interface GigabitEthernet0/1
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
  no shutdown
```

- e. After you have made all of the edits to the backup configuration file, save your changes to filename **R1-config-backup**.

Note: When saving the file, an extension such as **.txt**, may be added to the filename automatically.

Step 3: Restore the router configuration.

You can restore the edited running configuration directly to the console terminal in router global configuration mode, and the configurations are entered as if they were commands entered individually at the command prompt.

- a. From the Tera Term console connection to the router, enter global configuration mode.
- b. From the **File** menu, select **Send file....**
- c. Locate **R1-config-backup** and select **Open**.
- d. Save the running configuration to the startup configuration file.
R1# copy running-config startup-config
- e. Verify the new running configuration.

Step 4: Back up and restore the switch.

Go back to the beginning of Part 2 and follow the same steps to backup and restore the switch configuration.

Reflection

Why do you think it is important to use a text editor instead of a word processor to copy and save your command configurations?

A word processor could possibly add special control characters to the text making it difficult to use to restore the router.

Router Interface Summary Table

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

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

Device Configs – Final

Router R1

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
```

Lab – Managing Router Configuration Files with Terminal Emulation Software

```
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
!
no ipv6 cef
!
no ip domain lookup
ip cef
multilink bundle-name authenticated
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C Unauthorized Access is Prohibited! ^C
!
line con 0
password 7 104D000A0618
```

```
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 104D000A0618
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
```

Lab – Managing Router Configuration Files with Terminal Emulation Software

```
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
ip default-gateway 192.168.1.1
ip http server
```

Lab – Managing Router Configuration Files with Terminal Emulation Software

```
ip http secure-server
banner motd ^C Unauthorized access is prohibited! ^C
!
line con 0
password 7 070C285F4D06
login
line vty 0 4
password 7 070C285F4D06
login
line vty 5 15
login
!
end
```

Lab – Managing Device Configuration Files Using TFTP, Flash, and USB (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: (Optional) Download TFTP Server Software
- Part 3: Use TFTP to Back Up and Restore the Switch Running Configuration
- Part 4: Use TFTP to Back Up and Restore the Router Running Configuration
- Part 5: Back Up and Restore Running Configurations Using Router Flash Memory
- Part 6: (Optional) Use a USB Drive to Back Up and Restore the Running Configuration

Background / Scenario

Cisco networking devices are often upgraded or swapped out for a number of reasons. It is important to maintain backups of the latest device configurations, as well as a history of configuration changes. A TFTP server is often used to backup configuration files and IOS images in production networks. A TFTP server is a centralized and secure method used to store the backup copies of the files and restore them as necessary. Using a centralized TFTP server, you can back up files from many different Cisco devices.

In addition to a TFTP server, most of the current Cisco routers can back up and restore files locally from CompactFlash (CF) memory or a USB flash drive. The CF is a removable memory module that has replaced the limited internal flash memory of earlier router models. The IOS image for the router resides in the CF memory, and the router uses this IOS Image for the boot process. With the larger size of the CF memory, additional files can be stored for backup purposes. A removable USB flash drive can also be used for backup purposes.

In this lab, you will use TFTP server software to back up the Cisco device running configuration to the TFTP server or flash memory. You can edit the file using a text editor and copy the new configuration back to a Cisco device.

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

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

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Instructor Note: If time is limited, the lab can be divided up and performed over multiple sessions. For example, after building the network in Part 1, any combination of the remaining lab parts can be performed in any order.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term, and a TFTP server)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology
- USB flash drive (Optional)

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses for router R1, switch S1 and PC-A.

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

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Initialize and reload the router and switch.

Step 3: Configure basic settings for each device.

- a. Configure basic device parameters as shown in the Addressing Table.
- b. To prevent the router and switch from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup.
- c. Assign **class** as the privileged EXEC encrypted password.
- d. Configure the passwords and allow login for console and vty lines using the **cisco** as the password.
- e. Configure the default gateway for the switch.
- f. Encrypt the clear text passwords.
- g. Configure the IP address, subnet mask, and default gateway for PC-A.

Step 4: Verify connectivity from PC-A.

- a. Ping from PC-A to S1.
- b. Ping from PC-A to R1.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Part 2: (Optional) Download TFTP Server Software

A number of free TFTP servers are available on the Internet for download. The Tftpd32 server is used with this lab.

Note: Downloading a TFTP server from a website requires Internet access.

Step 1: Verify availability of a TFTP server on PC-A.

- a. Click the **Start** menu and select **All Programs**.
- b. Search for a TFTP server on PC-A.
- c. If a TFTP server is not found, a TFTP server can be downloaded from the Internet.

Step 2: Download a TFTP server.

- a. Tftpd32 is used in this lab. This server can be downloaded from the following link:
http://tftpd32.jounin.net/tftpd32_download.html
- b. Choose the appropriate version for your system and install the server.

Part 3: Use TFTP to Back Up and Restore the Switch Running Configuration

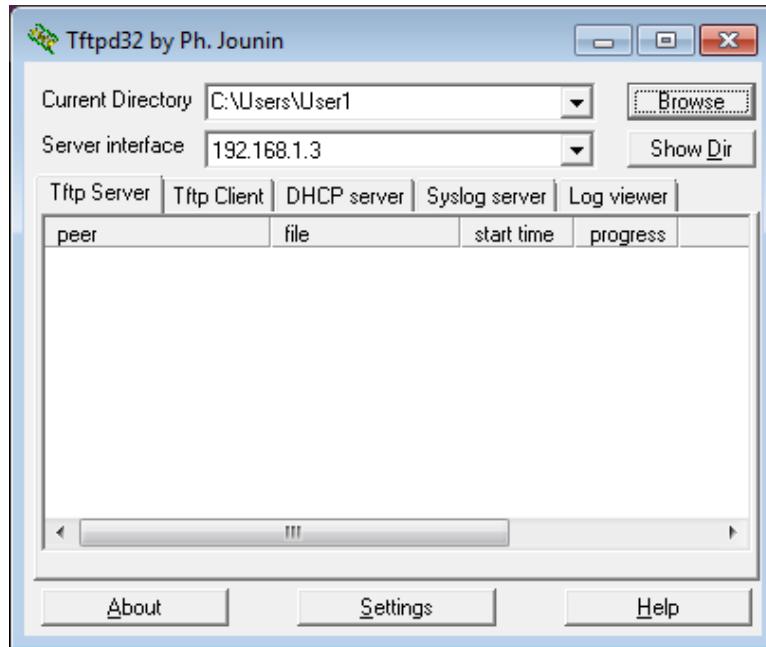
Step 1: Verify connectivity to switch S1 from PC-A.

The TFTP application uses the UDP Layer 4 transport protocol, which is encapsulated in an IP packet. For TFTP file transfers to function, there must be Layer 1 and 2 (Ethernet, in this case) and Layer 3 (IP) connectivity between the TFTP client and the TFTP server. The LAN topology in this lab uses only Ethernet at Layers 1 and 2. However, TFTP transfers can also be accomplished over WAN links that use other Layer 1 physical links and Layer 2 protocols. As long as there is IP connectivity between the client and server, as demonstrated by ping, the TFTP transfer can take place. If the pings are not successful, troubleshoot the basic device configurations before continuing.

Note: A common misconception is that you can TFTP a file over the console connection. This is not the case because the console connection does not use IP. The TFTP transfer can be initiated from the client device (router or switch) using the console connection, but there must be IP connectivity between the client and server for the file transfer to take place.

Step 2: Start the TFTP server.

- a. Click the **Start** menu and select **All Programs**.
- b. Find and select **Tftpd32** or **Tftpd64**. The following window displays that the TFTP server is ready.



- c. Click **Browse** to choose a directory where you have write permission, such as C:\Users\User1, or the Desktop.

Step 3: Explore the copy command on a Cisco device.

- a. Console into switch S1 and, from the privileged EXEC mode prompt, enter **copy ?** to display the options for source or “from” location and other available copy options. You can specify **flash:** or **flash0:** as the source, however, if you simply provide a filename as the source, **flash0:** is assumed and is the default. Note that **running-config** is also an option for the source location.

```
S1# copy ?
/erase           Erase destination file system.
/error           Allow to copy error file.
/noverify        Don't verify image signature before reload.
/verify          Verify image signature before reload.
archive:        Copy from archive: file system
cns:            Copy from cns: file system
flash0:          Copy from flash0: file system
flash1:          Copy from flash1: file system
flash:           Copy from flash: file system
ftp:             Copy from ftp: file system
http:            Copy from http: file system
https:           Copy from https: file system
null:            Copy from null: file system
nvram:           Copy from nvram: file system
rcp:             Copy from rcp: file system
running-config  Copy from current system configuration
scp:             Copy from scp: file system
startup-config  Copy from startup configuration
system:          Copy from system: file system
tar:             Copy from tar: file system
```

```
tftp:          Copy from tftp: file system
tmpsys:        Copy from tmpsys: file system
xmodem:        Copy from xmodem: file system
ymodem:        Copy from ymodem: file system
```

- b. Use the ? to display the destination options after a source file location is chosen. The **flash:** file system for S1 is the source file system in this example.

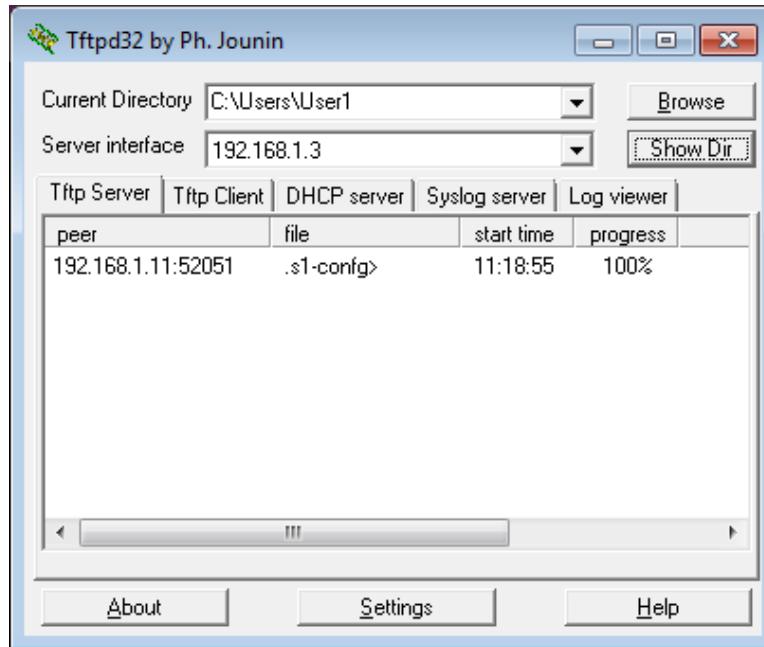
```
S1# copy flash: ?
archive:      Copy to archive: file system
flash0:        Copy to flash0: file system
flash1:        Copy to flash1: file system
flash:         Copy to flash: file system
ftp:          Copy to ftp: file system
http:          Copy to http: file system
https:         Copy to https: file system
idconf:        Load an IDConf configuration file
null:          Copy to null: file system
nvram:         Copy to nvram: file system
rcp:           Copy to rcp: file system
running-config Update (merge with) current system configuration
scp:           Copy to scp: file system
startup-config Copy to startup configuration
syslog:        Copy to syslog: file system
system:        Copy to system: file system
tftp:          Copy to tftp: file system
tmpsys:        Copy to tmpsys: file system
xmodem:        Copy to xmodem: file system
ymodem:        Copy to ymodem: file system
```

Step 4: Transfer the running-config file from switch S1 to TFTP server on PC-A.

- a. From the privileged EXEC mode on the switch, enter the **copy running-config tftp:** command. Provide the remote host address of the TFTP server (PC-A), 192.168.1.3. Press Enter to accept default destination filename (**s1-config**) or provide your own filename. The exclamation marks (!! indicate the transfer process is in progress and is successful.

```
S1# copy running-config tftp:
Address or name of remote host []? 192.168.1.3
Destination filename [s1-config]?
!!
1465 bytes copied in 0.663 secs (2210 bytes/sec)
S1#
```

The TFTP server also displays the progress during the transfer.



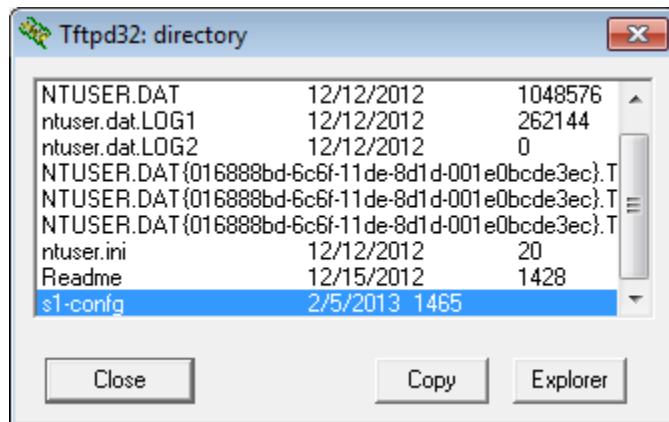
Note: If you do not have permission to write to the current directory that is used by the TFTP server, the following error message displays:

```
S1# copy running-config tftp:  
Address or name of remote host []? 192.168.1.3  
Destination filename [s1-config]?  
%Error opening tftp://192.168.1.3/s1-config (Permission denied)
```

You can change the current directory in TFTP server by clicking **Browse** and choosing a different folder.

Note: Other issues, such as a firewall blocking TFTP traffic, can prevent the TFTP transfer. Please check with your instructor for further assistance.

- In the Tftpd32 server window, click **Show Dir** to verify that the **s1-config** file has been transferred to your current directory. Click **Close** when finished.



Step 5: Create a modified switch running configuration file.

The saved running configuration file, **s1-config**, can also be restored to the switch by using the **copy** command from the switch. The original or a modified version of the file can be copied to the flash file system of the switch.

- a. Navigate to the TFTP directory on PC-A by using the file system of PC-A, and then locate the **s1-config** file. Open this file using a text editor program, such as WordPad.
- b. With the file open, locate the **hostname S1** line. Replace **S1** with **Switch1**. Delete all the self-generated crypto keys, as necessary. A sample of the keys is displayed below. These keys are not exportable and can cause errors while updating the running configuration.

```
crypto pki trustpoint TP-self-signed-1566151040
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-1566151040
  revocation-check none
  rsakeypair TP-self-signed-1566151040
!
!
crypto pki certificate chain TP-self-signed-1566151040
  certificate self-signed 01
    3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
    31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
<output omitted>
  E99574A6 D945014F B6FE22F3 642EE29A 767EABF7 403930CA D2C59E23 102EC12E
  02F9C933 B3296D9E 095EBDAF 343D17F6 AF2831C7 6DA6DFE3 35B38D90 E6F07CD4
  40D96970 A0D12080 07A1C169 30B9D889 A6E2189C 75B988B9 0AF27EDC 6D6FA0E5
  CCFA6B29 729C1E0B 9DADACD0 3D7381
  quit
```

- c. Save this file as a plain text file with a new filename, **Switch1-config.txt**, in this example.

Note: When saving the file, an extension, such as **.txt**, may be added to the filename automatically.

- d. In the Tftpd32 server window, click **Show Dir** to verify that the **Switch1-config.txt** file is located in the current directory.

Step 6: Upload running configuration file from TFTP server to switch S1.

- a. From the privileged EXEC mode on the switch, enter the **copy tftp running-config** command. Provide the remote host address of the TFTP server, 192.168.1.3. Enter the new filename, **Switch1-config.txt**. The exclamation mark (!) indicates the transfer process is in progress and is successful.

```
S1# copy tftp: running-config
Address or name of remote host []? 192.168.1.3
Source filename []? Switch1-config.txt
Destination filename [running-config]?
Accessing tftp://192.168.1.3/Switch1-config.txt...
Loading Switch1-config.txt from 192.168.1.3 (via Vlan1): !
[OK - 1580 bytes]
[OK]
1580 bytes copied in 9.118 secs (173 bytes/sec)
*Mar 1 00:21:16.242: %PKI-4-NOAUTOSAVE: Configuration was modified. Issue "write memory" to save new certificate
```

```
*Mar 1 00:21:16.251: %SYS-5-CONFIG_I: Configured from tftp://192.168.1.3/Switch1-  
cfg.txt by console  
Switch1#
```

After the transfer has completed, the prompt has changed from S1 to Switch1, because the running configuration is updated with the **hostname Switch1** command in the modified running configuration.

- b. Enter the **show running-config** command to examine running configuration file.

```
Switch1# show running-config  
Building configuration...  
  
Current configuration : 3062 bytes  
!  
! Last configuration change at 00:09:34 UTC Mon Mar 1 1993  
!  
version 15.0  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname Switch1  
!  
boot-start-marker  
boot-end-marker  
<output omitted>
```

Note: This procedure merges the running-config from the TFTP server with the current running-config in the switch or router. If changes were made to the current running-config, the commands in the TFTP copy are added. Alternatively, if the same command is issued, it updates the corresponding command in the switch or router current running-config.

If you want to completely replace the current running-config with the one from the TFTP server, you must erase the switch startup-config and reload the device. You will then need to configure the VLAN 1 management address, so there is IP connectivity between the TFTP server and the switch.

Part 4: Use TFTP to Back Up and Restore the Router Running Configuration

The backup and restore procedure from Part 3 can also be performed with a router. In Part 4, the running configuration file will be backed up and restored using a TFTP server.

Step 1: Verify connectivity to router R1 from PC-A.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 2: Transfer the running configuration from router R1 to TFTP server on PC-A.

- a. From the privileged EXEC mode on R1, enter the **copy running-config tftp** command. Provide the remote host address of the TFTP server, 192.168.1.3, and accept the default filename.
- b. Verify that the file has been transferred to the TFTP server.

Step 3: Restore the running configuration file to the router.

- a. Erase the startup-config file on the router.
- b. Reload the router.
- c. Configure the G0/1 interface on the router with an IP address 192.168.1.1.
- d. Verify connectivity between the router and PC-A.
- e. Use the **copy** command to transfer the running-config file from the TFTP server to the router. Use **running-config** as the destination.
- f. Verify the router has updated the running-config.

Part 5: Back Up and Restore Configurations Using Router Flash Memory

For the 1941 and other newer Cisco routers, there is no internal flash memory. The flash memory for these routers uses CompactFlash (CF) memory. The use of CF memory allows for more available flash memory and easier upgrades without the need to open the router case. Besides storing the necessary files, such as IOS images, the CF memory can store other files, such as a copy of the running configuration. In Part 5, you will create a backup copy of the running configuration file and save it on the CF memory on the router.

Note: If the router does not use CF, the router may not have enough flash memory for storing the backup copy of running configuration file. You should still read through the instructions and become familiar with the commands.

Step 1: Display the router file systems.

The **show file systems** command displays the available file systems on the router. The **flash0:** file system is the default file system on this router as indicated by the asterisk (*) symbol (at the beginning of the line). The hash (#) sign (at the end of the highlighted line) indicates that it is a bootable disk. The **flash0:** file system can also be referenced using the name **flash:**. The total size of the **flash0:** is 256 MB with 62 MB available. Currently the **flash1:** slot is empty as indicated by the — under the headings, Size (b) and Free (b). Currently **flash0:** and **nvrpm:** are the only available file systems.

```
R1# show file systems
File Systems:

      Size(b)   Free(b)    Type  Flags  Prefixes
      --       --       opaque  rw    archive:
      --       --       opaque  rw    system:
      --       --       opaque  rw    tmpsys:
      --       --       opaque  rw    null:
      --       --       network rw    tftp:
* 260153344  64499712  disk   rw    flash0: flash:#  
      --       --       disk   rw    flash1:
      262136   242776   nvram  rw    nvrpm:
      --       --       opaque  wo    syslog:
      --       --       opaque  rw    xmodem:
      --       --       opaque  rw    ymodem:
      --       --       network rw    rcp:
      --       --       network rw    http:
      --       --       network rw    ftp:
      --       --       network rw    scp:
      --       --       opaque  ro    tar:
```

```
-           -   network      rw   https:  
-           -   opaque       ro   cns:
```

Where is the startup-config file located?

nvrwam:

Note: Verify there is at least 1 MB (1,048,576 bytes) of free space. If there is not enough space in the flash memory, please contact your instructor for further instructions. You can determine the size of flash memory and space available using the **show flash** or **dir flash:** command at the privileged EXEC prompt.

Step 2: Copy the router running configuration to flash.

A file can be copied to flash by using the **copy** command at the privileged EXEC prompt. In this example, the file is copied into **flash0:**, because there is only one flash drive available as displayed in the previous step, and it is also the default file system. The **R1-running-config-backup** file is used as the filename for the backup running configuration file.

Note: Remember that filenames are case-sensitive in the IOS file system.

- Copy the running configuration to flash memory.

```
R1# copy running-config flash:  
Destination filename [running-config]? R1-running-config-backup  
2169 bytes copied in 0.968 secs (2241 bytes/sec)
```

- Use **dir** command to verify the running-config has been copied to flash.

```
R1# dir flash:  
Directory of flash0:/  
  
 1 drw-          0 Nov 15 2011 14:59:04 +00:00  ipsdir  
<output omitted>  
 20 -rw- 67998028 Aug 7 2012 17:39:16 +00:00  c1900-universalk9-mz.SPA.152-  
4.M3.bin  
 22 -rw- 2169 Feb 4 2013 23:57:54 +00:00  R1-running-config-backup  
 24 -rw- 5865 Jul 10 2012 14:46:22 +00:00  ipnat  
 25 -rw- 6458 Jul 17 2012 00:12:40 +00:00  lpIPSec  
  
260153344 bytes total (64503808 bytes free)
```

- Use the **more** command to view the running-config file in flash memory. Examine the file output and scroll to the Interface section. Notice the **no shutdown** command is not included with the GigabitEthernet0/1. The interface is shut down when this file is used to update the running configuration on the router.

```
R1# more flash:R1-running-config-backup  
<output omitted>  
interface GigabitEthernet0/1  
 ip address 192.168.1.1 255.255.255.0  
 duplex auto  
 speed auto  
<output omitted>
```

Step 3: Erase the startup configuration and reload the router.

Step 4: Restore the running configuration from flash.

- a. Verify the router has the default initial configuration.
- b. Copy the saved running-config file from flash to update the running-config.

```
Router# copy flash:R1-running-config-backup running-config
```

- c. Use the **show ip interface brief** command to view the status of the interfaces. The interface GigabitEthernet0/1 was not enabled when the running configuration was updated, because it is administratively down.

```
R1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	192.168.1.1	YES	TFTP	administratively down	down
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	unassigned	YES	unset	administratively down	down

The interface can be enabled using the **no shutdown** command in the interface configuration mode on the router.

Another option is to add the **no shutdown** command for the GigabitEthernet0/1 interface to the saved file before updating the router running configuration file. This will be done in Part 6 using a saved file on a USB flash drive.

Note: Because the IP address was configured by using a file transfer, TFTP is listed under the Method heading in the **show ip interface brief** output.

Part 6: (Optional) Use a USB Drive to Back Up and Restore the Running Configuration

A USB flash drive can be used to backup and restore files on a router with an available USB port. Two USB ports are available on the 1941 routers.

Note: USB ports are not available on all routers, but you should still become familiar with the commands.

Note: Because some ISR G1 routers (1841, 2801, or 2811) use File Allocation Table (FAT) file systems, there is a maximum size limit for the USB flash drives that can be used in this part of the lab. The recommended maximum size for an ISR G1 is 4 GB. If you receive the following message, the file system on the USB flash drive may be incompatible with the router or the capacity of the USB flash drive may have exceed maximum size of the FAT file system on the router.

```
*Feb  8 13:51:34.831: %USBFLASH-4-FORMAT: usbflash0 contains unexpected values in partition table or boot sector. Device needs formatting before use!
```

Step 1: Insert a USB flash drive into a USB port on the router.

Notice the message on the terminal when inserting the USB flash drive.

```
R1#  
* *Feb  5 20:38:04.678: %USBFLASH-5-CHANGE: usbflash0 has been inserted!
```

Step 2: Verify that the USB flash file system is available.

```
R1# show file systems  
File Systems:
```

	Size (b)	Free (b)	Type	Flags	Prefixes
	-	-	opaque	rw	archive:
	-	-	opaque	rw	system:
	-	-	opaque	rw	tmpsys:
	-	-	opaque	rw	null:
	-	-	network	rw	tftp:
*	260153344	64512000	disk	rw	flash0: flash:#
	-	-	disk	rw	flash1:
	262136	244676	nvram	rw	nvram:
	-	-	opaque	wo	syslog:
	-	-	opaque	rw	xmodem:
	-	-	opaque	rw	ymodem:
	-	-	network	rw	rcp:
	-	-	network	rw	http:
	-	-	network	rw	ftp:
	-	-	network	rw	scp:
	-	-	opaque	ro	tar:
	-	-	network	rw	https:
	-	-	opaque	ro	cns:
	7728881664	7703973888	usbflash	rw	usbflash0:

Step 3: Copy the running configuration file to the USB flash drive.

Use the **copy** command to copy the running configuration file to the USB flash drive.

```
R1# copy running-config usbflash0:  
Destination filename [running-config]? R1-running-config-backup.txt  
2198 bytes copied in 0.708 secs (3105 bytes/sec)
```

Step 4: List the file on the USB flash drive.

Use the **dir** command (or **show** command) on the router to list the files on the USB flash drive. In this sample, a flash drive was inserted into USB port 0 on the router.

```
R1# dir usbflash0:  
Directory of usbflash0:/  
  
1 -rw- 16216 Nov 15 2006 09:34:04 +00:00 ConditionsFR.txt  
2 -rw- 2462 May 26 2006 21:33:40 +00:00 Nlm.ico  
3 -rw- 24810439 Apr 16 2010 10:28:00 +00:00 Twice.exe  
4 -rw- 71 Jun 4 2010 11:23:06 +00:00 AUTORUN.INF  
5 -rw- 65327 Mar 11 2008 10:54:26 +00:00 ConditionsEN.txt  
6 -rw- 2198 Feb 5 2013 21:36:40 +00:00 R1-running-config-backup.txt  
  
7728881664 bytes total (7703973888 bytes free)
```

Step 5: Erase the startup-config and reload the router.

Step 6: Modify the saved file.

- Remove the USB drive from the router.

```
Router#  
*Feb 5 21:41:51.134: %USBFLASH-5-CHANGE: usbflash0 has been removed!
```

- b. Insert the USB drive into the USB port of a PC.
- c. Modify the file using a text editor. The **no shutdown** command is added to the GigabitEthernet0/1 interface. Save the file as a plain text file on to the USB flash drive.

```
!  
interface GigabitEthernet0/1  
ip address 192.168.1.1 255.255.255.0  
no shutdown  
duplex auto  
speed auto  
!
```

- d. Remove the USB flash drive from the PC safely.

Step 7: Restore the running configuration file to the router.

- a. Insert the USB flash drive into a USB port on the router. Notice the port number where the USB drive has been inserted if there is more than one USB port available on the router.

```
*Feb 5 21:52:00.214: %USBFLASH-5-CHANGE: usbflash1 has been inserted!
```

- b. List the files on the USB flash drive.

```
Router# dir usbflash1:  
Directory of usbflash1:/  
  
1 -rw- 16216 Nov 15 2006 09:34:04 +00:00 ConditionsFR.txt  
2 -rw- 2462 May 26 2006 21:33:40 +00:00 Nlm.ico  

```

- c. Copy the running configuration file to the router.

```
Router# copy usbflash1:R1-running-config-backup.txt running-config  
Destination filename [running-config]?  
2344 bytes copied in 0.184 secs (12739 bytes/sec)  
R1#
```

- d. Verify that the GigabitEthernet0/1 interface is enabled.

```
R1# show ip interface brief  
Interface IP-Address OK? Method Status Protocol  
Embedded-Service-Engine0/0 unassigned YES unset administratively down down  
GigabitEthernet0/0 unassigned YES unset administratively down down  
GigabitEthernet0/1 192.168.1.1 YES TFTP up up  
Serial0/0/0 unassigned YES unset administratively down down  
Serial0/0/1 unassigned YES unset administratively down down
```

The G0/1 interface is enabled because the modified running configuration included the **no shutdown** command.

Reflection

1. What command do you use to copy a file from the flash to a USB drive?

copy flash:filename usbflash0:

2. What command do you use to copy a file from the USB flash drive to a TFTP server?

copy usbflash0:filename tftp:

Router Interface Summary Table

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

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

Device Configs

Router R1

```
R1# show run
Building configuration...

Current configuration : 1283 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
```

Lab – Managing Device Configuration Files Using TFTP, Flash and USB

```
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUG.2
!
no aaa new-model
memory-size iomem 15
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
```

```
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
password 14141B180F0B
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 070C285F4D06
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
S1#show run
Building configuration...

Current configuration : 1498 bytes
!
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
```

```
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUG.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
```

```
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
    ip address 192.168.1.11 255.255.255.0
!
ip default-gateway 192.168.1.1
ip http server
ip http secure-server
!
!
!
line con 0
    password 045802150C2E
    login
line vty 0 4
    password 045802150C2E
    login
line vty 5 15
    password 045802150C2E
    login
!
end
```

Lab – Configure and Verify Password Recovery (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Objectives

- Part 1: Configure Basic Device Settings
- Part 2: Reboot Router and Enter ROMMON
- Part 3: Reset Password and Save New Configuration
- Part 4: Verify the Router is Loading Correctly

Background / Scenario

The purpose of this lab is to reset the enable password on a specific Cisco router. The enable password protects access to privileged EXEC and configuration mode on Cisco devices. The enable password can be recovered, but the enable secret password is encrypted and will need to be replaced with a new password.

In order to bypass a password, a user must be familiar with the ROM monitor (ROMMON) mode, as well as the configuration register setting for Cisco routers. ROMMON is basic CLI software stored in ROM that can be used to troubleshoot boot errors and recover a router when an IOS is not found.

In this lab, you will change the configuration register in order to reset the enable password on a Cisco router.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cable to connect to the Cisco IOS device via the console port

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and copy the basic configuration into R1. The password is encrypted to setup the scenario of needing to recover from an unknown enabled password.

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

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings on the router.

Instructor note: The encrypted password is **NoRecovery123**.

- a. Console into the router and enter global configuration mode.
- b. Copy the following basic configuration and paste it to the running-configuration on the router.
`no ip domain-lookup`

```
service password-encryption
hostname R1
enable secret 5 $1$SBb4$n.EuL28kPTzxMLFiyMLl5/
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
logging sync
end
write
exit
```

- c. Press **Enter** and try to enable Privileged Exec mode.

As you can see, access to a Cisco IOS device is very limited if the enable password is unknown. It is important for a network engineer to be able to recover from an unknown enable password issue on a Cisco IOS device.

Part 2: Reboot Router and Enter ROMMON

Step 1: Reboot the router.

- a. While still consoled into R1, remove the power cord from the back of R1.

Note: If you are working in a NETLAB pod, ask your instructor how to power cycle the router.

- b. From the console session on PC-A, issue a hard break to interrupt the routers normal boot process and enter ROMMON mode.

Note: To issue a hard break in Tera Term, press the **Alt** and the **B** keys simultaneously.

Step 2: Reset the configuration register.

- a. From the ROMMON prompt, type a ?, then press **Enter**. This will display a list of available ROMMON commands. Look for the **confreg** command in this list.

```
rommon 1 > ?
alias           set and display aliases command
boot            boot up an external process
break           set/show/clear the breakpoint
confreg        configuration register utility
cont             continue executing a downloaded image
context          display the context of a loaded image
cookie           display contents of motherboard cookie PROM in hex
dev              list the device table
dir              list files in file system
frame            print out a selected stack frame
help             monitor builtin command help
history          monitor command history
iomemset         set IO memory percent
meminfo          main memory information
repeat           repeat a monitor command
reset            system reset
rommon-pref      Select ROMMON
set              display the monitor variables
```

Lab – Configure and Verify Password Recovery

showmon	display currently selected ROM monitor
stack	produce a stack trace
sync	write monitor environment to NVRAM
sysret	print out info from last system return
tftpdnld	tftp image download
unalias	unset an alias
unset	unset a monitor variable
hwpart	Read HW resources partition
rommon 2 >	

Note: The number at the end of the ROMMON prompt will increment by one each time a command is entered.

- b. Type **confreg 0x2142** and press **Enter**. Changing the register to Hex 2142 tells the router not to automatically load the startup configuration when booting. The router will need to be rebooted for the configuration register change to take effect.

```
frommon 2 > confreq 0x2142
```

```
You must reset or power cycle for new config to take effect  
rommon 3 >
```

- c. Issue the **reset ROMON** command to reboot the router.

rommon 3 > **reset**

System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
Technical Support: <http://www.cisco.com/techsupport>
Copyright (c) 2011 by Cisco Systems, Inc.

Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

```
 Readonly ROMMON initialized  
program load complete, entry point: 0x80803000, size: 0x1b340  
program load complete, entry point: 0x80803000, size: 0x1b340
```

IOS Image Load Test

Lab – Configure and Verify Password Recovery

- ```
< output omitted >
```
- d. When asked if you would like to enter the initial configuration dialog, type **no** and press **Enter**.  
Would you like to enter the initial configuration dialog? [yes/no]: **no**
  - e. The router will complete its boot process and display the User Exec prompt. Enter Privileged Exec mode.  
Router> **enable**  
Router#

## Part 3: Reset Password and Save New Configuration

- a. While in Privileged Exec mode, copy the startup configuration to the running configuration.  
Router# **copy startup-config running-config**  
Destination filename [running-config]?  
1478 bytes copied in 0.272 secs (5434 bytes/sec)
- b. Enter global configuration mode.
- c. Reset the enable secret password to **cisco**.  
R1(config)# **enable secret cisco**
- d. Reset the configuration register back to 0x2102 to allow the startup configuration to automatically load the next time the router is rebooted.  
R1(config)# **config-register 0x2102**
- e. Exit global configuration mode.
- f. Copy the running configuration to the startup configuration.  
R1# **copy running-config startup-config**  
Destination filename [startup-config]?  
Building configuration...  
[OK]  
R1#

You have successfully reset the enable password on a router.

## Part 4: Verify the Router is Loading Correctly

**Step 1:** Reboot R1.

**Step 2:** Verify that the startup configuration loaded automatically.

**Step 3:** Enter Privileged Exec mode.

The new enable secret password should be cisco. If you are able to enter Privileged Exec mode, then you have successfully completed this lab.

## Reflection

Why is it of critical importance that a router be physically secured to prevent unauthorized access?

---

Because the password recovery procedure is based on a console connection, which requires direct physical access to the device, preventing unauthorized users access to the physical device is an imperative part of an overall security plan.

### Device Configs

#### Router R1

```
R1#sh run
Building configuration...

Current configuration : 1488 bytes
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 5 1KeL6$8EZ80eEADp2oed0cy5J0L.
!
no aaa new-model
memory-size iomem 15
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
cts logging verbose
!
redundancy
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

## Lab – Configure and Verify Password Recovery

---

```
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
logging synchronous
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
login
transport input none
!
scheduler allocate 20000 1000
!
end
```