



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Advanced Networking
ACCA5024
Lab Manual

2026-27

HND/BSc (Hons) Computing (Computer Networks and
Cyber Security)
Applied Computing
Wales Institute of Science and Art
University of Wales Trinity Saint David
Swansea

Module Leader
Dr Kapilan Radhakrishnan



Table of content

Lab	Page no
Lab 1: Navigate the IOS by Using Tera Term for Console Connectivity	1
Lab 2: Basic Switch and End Device Configuration	7
Lab 3: View Network Device MAC Addresses	10
Lab 4: View the Switch MAC Address Table	16
Lab 5: Configuring Basic Router Settings with IOS CLI	20
Lab 6 : Calculate IPv4 Subnets	30
Lab 7: Design and Implement a VLSM Addressing Scheme	34
Lab 8 - Identify IPv6 Addresses	39
Lab 9 - Configure IPv6 Addresses on Network Devices	42
Lab 10 - Build a Switch and Router Network IPv4 and IPv6	45
Lab 11 - Use Ping and Traceroute to Test Network Connectivity	50
Lab 12 - Troubleshoot Connectivity Issues	60
Lab 13: Configuring IPv4 Static and Default Routes	64
Lab 14: Configuring IPv6 Static and Default Routes	71
Lab 15: Troubleshooting IPv4 and IPv6 Static Routes	79
Lab 16 - Secure Network Devices	89
Lab 17 - Configure Network Devices with SSH	94
Lab 18: Configuring Switch Security Features Topology	99
Lab 19 - Configuring Basic RIPv2	109
Lab20: Configuring Basic RIPv2 and RIPv6	117
Appendix - Configure and Verify Password Recovery	129

Acknowledgement

The content, learning resources, practical activities, and instructional materials used in this module are sourced wholly or in part from Cisco Networking Academy (Cisco Academy) curriculum materials. We gratefully acknowledge Cisco Networking Academy for the development and provision of these educational resources.



Lab 1: Navigate the IOS by Using Tera Term for Console Connectivity

Topology



Objectives

Part 1: Access a Cisco Switch through the Serial Console Port

Part 2: Display and Configure Basic Device Settings

Part 3: (Optional) Access a Cisco Router Using a Mini-USB Console Cable

Note: NetLab users or others using remote access equipment should complete only Part 2.

Background / Scenario

Various models of Cisco routers and switches are used in all types of networks. These devices are managed using a local console connection or a remote connection. Nearly all Cisco devices have a serial console port to which you can connect. Newer models used in this lab, such as Cisco 4221, also have a USB console port.

In this lab, you will learn how to access a Cisco device via a direct local connection to the console port, using the terminal emulation program called Tera Term. You will also learn how to configure the serial port settings for the Tera Term console connection. After you have established a console connection with the Cisco device, you can display or configure device settings. You will only display settings and configure the clock in this lab.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.3 (universalk9 image). The switches used in the labs 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 the lab for the correct interface identifiers.

Note: Make sure that the switch and router have been erased and have no startup configuration. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows with a terminal emulation program, such as Tera Term)
- Rollover (DB-9 to RJ-45) console cable to configure the switch or router via the RJ-45 console port
- Mini-USB cable to configure the router via the USB console port

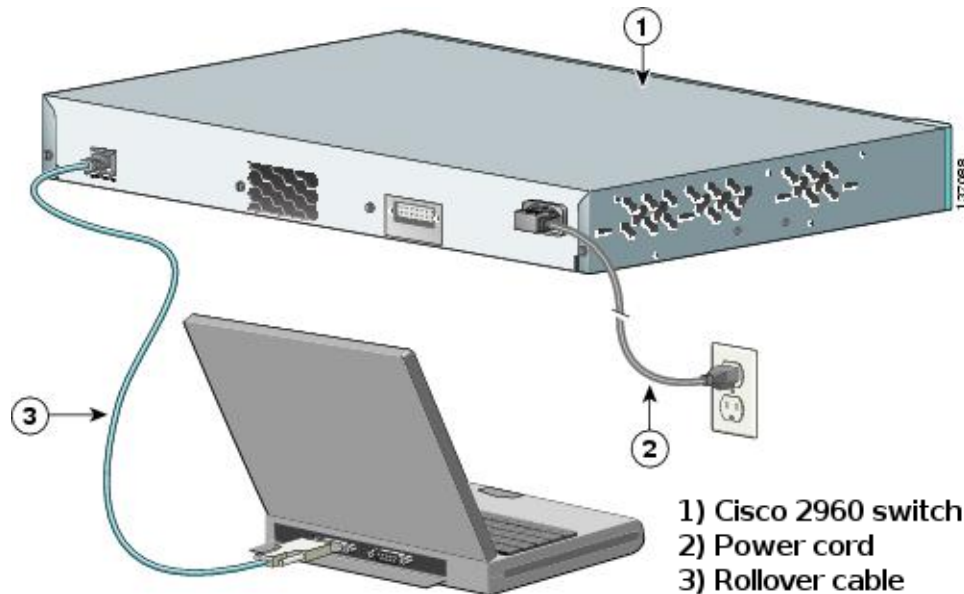
Instructions

Part 1: Access a Cisco Switch through the Serial Console Port

You will connect a PC to a Cisco switch using a rollover console cable. This connection will allow you to access the CLI and display settings or configure the switch.

Step 1: Connect a Cisco switch and computer using a rollover console cable.

- a. Connect the rollover console cable to the RJ-45 console port of the switch. Connect the other cable end to the serial COM port on the computer.



Note: Serial COM ports are no longer available on most computers. A USB-to-DB9 adapter can be used with the rollover console cable for console connection between the computer and a Cisco device. USB-to-DB9 adapters can be purchased at any computer electronics retailer.

Note: If using a USB-to-DB9 adapter to connect to the COM port, you may be required to install a driver for the adapter provided by the manufacturer of your computer. To determine the COM port used by the adapter, please see Part 3 Step 3. The correct COM port number is required to connect to the Cisco IOS device using a terminal emulator in Step 2.

- b. Turn on the Cisco switch and computer.

Step 2: Configure Tera Term to establish a console session with the switch.

Tera Term is a terminal emulation program. This program allows you to access the terminal output of the switch. It also allows you to configure the switch.

- a. Start Tera Term by clicking the **Windows Start** button located in the task bar. Locate **Tera Term** under **All Programs**.

Note: If the program is not installed on the system, Tera Term can be downloaded from the following link by selecting **Tera Term**:

<https://tssh2.osdn.jp/>

- b. In the New Connection dialog box, click the **Serial** radio button. Verify that the correct COM port is selected and click **OK** to continue.

- c. From the Tera Term **Setup** menu, choose the **Serial port...** to verify the serial settings. The default parameters for the console port are 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control. The Tera Term default settings match the console port settings for communications with the Cisco IOS switch.
- d. When you can see the terminal output, you are ready to configure a Cisco switch.

Part 2: Display and Configure Basic Device Settings

In this section, you are introduced to the user and privileged EXEC modes. You will determine the IOS version, display the clock settings, and configure the clock on the switch.

Step 1: Display the switch IOS image version.

- a. After the switch has completed its startup process, the following message is displayed. Enter **n** to continue.

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

Note: If you do not see the above message, please contact your instructor to reset your switch to the initial configuration.

- b. While you are in the user EXEC mode, display the IOS version for your switch.

```
Switch> show version
```

```
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2012 by Cisco Systems, Inc.
```

```
Compiled Sat 28-Jul-12 00:29 by prod_rel_team
```

```
ROM: Bootstrap program is C2960 boot loader
```

```
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE (fc1)
```

```
Switch uptime is 2 minutes
```

```
System returned to ROM by power-on
```

```
System image file is "flash://c2960-lanbasek9-mz.150-2.SE.bin"
```

```
<output omitted>
```

Which IOS image version is currently in use by your switch?

Step 2: Configure the clock.

As you learn more about networking, you will see that configuring the correct time on a Cisco switch can be helpful when you are troubleshooting problems. The following steps manually configure the internal clock of the switch.

- a. Display the current clock settings.

```
Switch> show clock
```

```
*00:30:05.261 UTC Mon Mar 1 1993
```

- b. The clock setting is changed from within the privileged EXEC mode. Enter the privileged EXEC mode by typing **enable** at the user EXEC mode prompt.

```
Switch> enable
```

- c. Configure the clock setting. The question mark (?) provides help and allows you to determine the expected input for configuring the current time, date, and year. Press Enter to complete the clock configuration.

```
Switch# clock set ?
hh:mm:ss Current Time
```

```
Switch# clock set 15:08:00 ?
<1-31> Day of the month
MONTH Month of the year
```

```
Switch# clock set 15:08:00 Oct 26 ?
<1993-2035> Year
```

```
Switch# clock set 15:08:00 Oct 26 2012
Switch#
*Oct 26 15:08:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:31:43
UTC Mon Mar 1 1993 to 15:08:00 UTC Fri Oct 26 2012, configured from console by
console.
```

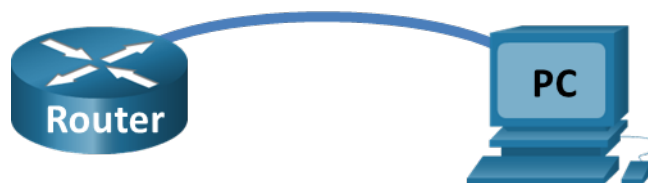
- d. Enter the **show clock** command to verify that the clock setting has updated.

```
Switch# show clock
15:08:07.205 UTC Fri Oct 26 2012
```

Part 3: (Optional) Access a Cisco Router Using a Mini-USB Console Cable

If you are using a Cisco 4221 router, or other Cisco IOS devices with a mini-USB console port, you can access the device console port using a mini-USB cable connected to the USB port on your computer.

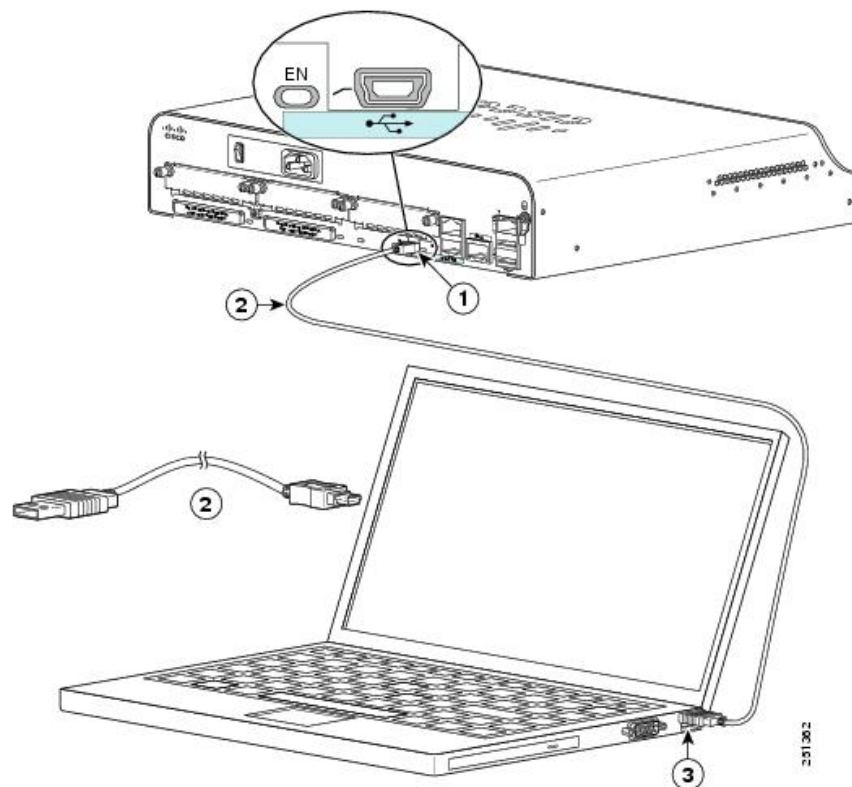
Note: The mini-USB console cable is the same type of mini-USB cable that is used with other electronics devices, such as USB hard drives, USB printers, or USB hubs. These mini-USB cables can be purchased from Cisco Systems, Inc. or other third-party vendors. Please verify that you are using a mini-USB cable, not a micro-USB cable, to connect to the mini-USB console port on a Cisco IOS device.



Note: You must use either the USB port or the RJ-45 port. Do not use both ports simultaneously. When the USB port is used, it takes priority over the RJ-45 console port.

Step 1: Set up the physical connection with a mini-USB cable.

- a. Connect the mini-USB cable to the mini-USB console port of the router. Connect the other cable end to a USB port on the computer.



- 1) USB 5-pin mini Type-B console port
- 2) USB 5-pin mini Type-B to USB Type-A Console Cable
- 3) USB Type-A connector

- b. Turn on the Cisco router and computer.

Step 2: Verify that the USB console is ready.

If you are using a Microsoft Windows-based PC and the USB console port LED indicator (labeled EN) does not turn green, please install the Cisco USB console driver.

A USB driver must be installed prior to connecting a Microsoft Windows-based PC to a Cisco IOS device with a USB cable. The driver can be found on www.cisco.com with the related Cisco IOS device. The USB driver can be downloaded from the following link:

<https://software.cisco.com/download/home/282774238/type/282855122/release/3.1>

Note: You must have a valid Cisco Connection Online (CCO) account to download this file.

Note: This link is related to the Cisco 1941 router. However, the USB console driver is not Cisco IOS device-model specific. This USB console driver only works with Cisco routers and switches. The computer requires a reboot after finishing the installation of the USB driver.

Note: After the files are extracted, the folder contains instructions for installation, removal, and the necessary drivers for different operating systems and architectures. Please choose the appropriate version for your system.

When the LED indicator for the USB console port has turned green, the USB console port is ready for access.

Step 3: (Optional) Enable the COM port for the Windows 7 PC.

If you are using a Microsoft Windows 7 PC, you may need to perform the following steps to enable the COM port:

- Click the **Windows Start** icon to access the **Control Panel**.
- Open the Device Manager.
- Click the **Ports (COM & LPT)** tree link to expand it. Right-click the **USB Serial Port** icon and choose **Update Driver Software**.
- Choose **Browse my computer for driver software**.
- Choose **Let me pick from a list of device drivers on my computer** and click **Next**.
- Choose the **Cisco Serial** driver and click **Next**.
- Note the port number assigned at the top of the window. In this sample, COM 5 is used for communication with the router. Click **Close**.
- Open Tera Term. Click the **Serial** radio button and choose the appropriate serial port, which is **Port COM5: Cisco Serial (COM 5)** in this example. This port should now be available for communication with the router. Click **OK**.

Reflection Questions

- How do you prevent unauthorized personnel from accessing your Cisco device through the console port?
- What are the advantages and disadvantages of using the serial console connection compared to the USB console connection to a Cisco router or switch?

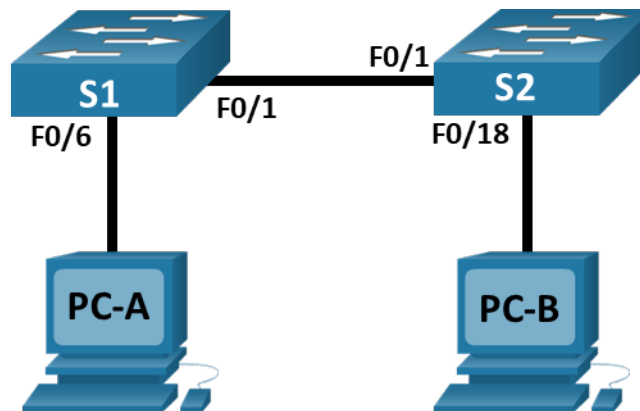
Router Interface Summary Table

Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
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)
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)
4221	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
4300	Gigabit Ethernet 0/0/0 (G0/0/0)	Gigabit Ethernet 0/0/1 (G0/0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)

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.

Lab 2: Basic Switch and End Device Configuration

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.1	255.255.255.0
S2	VLAN 1	192.168.1.2	255.255.255.0
PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0

Objectives

- Set Up the Network Topology
- Configure PC Hosts
- Configure and Verify Basic Switch Settings

Background / Scenario

In this lab, you will build a simple network with two hosts and two switches. You will also configure basic settings including hostname, local passwords, and login banner. Use **show** commands to display the running configuration, IOS version, and interface status. Use the **copy** command to save device configurations.

You will apply IP addressing for this lab to the PCs and switches to enable communication between the devices. Use the **ping** utility to verify connectivity.

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: Make sure that the switches have been erased and have no startup configurations. Refer to Appendix A for the procedure to initialize and reload a switch.

Required Resources

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

Instructions

Part 1: Set Up the Network Topology

In this step, you will cable the devices together according to the network topology.

- a. Power on the devices.
- b. Connect the two switches.
- c. Connect the PCs to their respective switches.
- d. Visually inspect network connections.

Part 2: Configure PC Hosts

- a. Configure static IP address information on the PCs according to the Addressing Table.
- b. Verify PC settings and connectivity.

Part 3: Configure and Verify Basic Switch Settings

- a. Console into the switch. Enter the global configuration mode.
- b. Give the switch a name according to the Addressing Table.
- c. Prevent unwanted DNS lookups.
- d. Enter local passwords. Use **class** as the privileged EXEC password and **cisco** as the password for console access.
- e. Configure and enable the SVI according to the Addressing Table.
- f. Enter a login MOTD banner to warn about unauthorized access.
- g. Save the configuration.
- h. Display the current configuration.
- i. Display the IOS version and other useful switch information.
- j. Display the status of the connected interfaces on the switch.
- k. Configure switch S2.
- l. Record the interface status for the following interfaces.

Interface	S1 Status	S1 Protocol	S2 Status	S2 Protocol
F0/1				
F0/6				
F0/18				
VLAN 1				

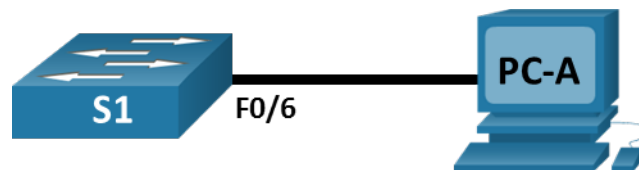
- m. From a PC, ping S1 and S2. The pings should be successful.
- n. From a switch, ping PC-A and PC-B. The pings should be successful.

Reflection Question

- Why some FastEthernet ports on the switches are up and others are down?
- What could prevent a ping from being sent between the PCs?

Lab 3: View Network Device MAC Addresses

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.2	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Devices and Verify Connectivity

Part 2: Display, Describe, and Analyze Ethernet MAC Addresses

Background / Scenario

Every device on an Ethernet LAN is identified by a Layer 2 MAC address. This address is assigned by the manufacturer and stored in the firmware of the NIC. This lab will explore and analyze the components that make up a MAC address, and how you can find this information on a switch and a PC.

You will cable the equipment as shown in the topology. You will configure the switch and PC to match the addressing table. You will verify your configurations by testing for network connectivity.

After the devices have been configured and network connectivity has been verified, you will use various commands to retrieve information from the devices to answer questions about your network equipment.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.2(2) (lanbasek9 image). Other 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.

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

Required Resources

- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 1 PC (Windows with a terminal emulation program, such as Tera Term)
- Console cable to configure the Cisco switch via the console ports
- Ethernet cables as shown in the topology

Instructions

Part 1: Configure Devices and Verify Connectivity

In this part, you will set up the network topology and configure basic settings, such as the interface IP addresses and device name. For device name and address information, refer to the Topology and Addressing Table.

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

- Attach the devices shown in the topology and cable as necessary.
- Power on all the devices in the topology.

Step 2: Configure the IPv4 address for the PC.

- Configure the IPv4 address, subnet mask, and default gateway address for PC-A.
- From the command prompt on PC-A, ping the switch address.

Were the pings successful? Explain.

Step 3: Configure basic settings for the switch.

In this step, you will configure the device name and the IP address, and disable DNS lookup on the switch.

- Console into the switch and enter global configuration mode.

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

- Assign a hostname to the switch based on the Addressing Table.

```
Switch(config)# hostname S1
```

- Disable DNS lookup.

```
S1(config)# no ip domain-lookup
```

- Configure and enable the SVI interface for VLAN 1.

```
S1(config)# interface vlan1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
```

```
*Mar 1 00:07:59.048: %SYS-5-CONFIG_I: Configured from console by console
```

Step 4: Verify network connectivity.

Ping the switch from PC-A.

Were the pings successful?

Part 2: Display, Describe, and Analyze Ethernet MAC Addresses

Every device on an Ethernet LAN has a MAC address that is assigned by the manufacturer and stored in the firmware of the NIC. Ethernet MAC addresses are 48-bits long. They are displayed using six sets of hexadecimal digits that are usually separated by dashes, colons, or periods. The following example shows the same MAC address using the three different notation methods:

00-05-9A-3C-78-00

00:05:9A:3C:78:00

0005.9A3C.7800

Note: MAC addresses are also called physical addresses, hardware addresses, or Ethernet hardware addresses.

You will issue commands to display the MAC addresses on a PC and a switch, and analyze the properties of each one.

Step 1: Analyze the MAC address for the PC-A NIC.

Before you analyze the MAC address on PC-A, look at an example from a different PC NIC. You can issue the **ipconfig /all** command to view the MAC address of your NIC. An example screen output is shown below. When using the **ipconfig /all** command, notice that MAC addresses are referred to as physical addresses. Reading the MAC address from left to right, the first six hex digits refer to the vendor (manufacturer) of this device. These first six hex digits (3 bytes) are also known as the organizationally unique identifier (OUI). This 3-byte code is assigned to the vendor by the IEEE organization.

To find the manufacturer, use the keywords **IEEE OUI standards** to find an OUI lookup tool on the internet or navigate to <http://standards-oui.ieee.org/oui.txt> to find the registered OUI vendor codes. The last six digits are the NIC serial number assigned by the manufacturer.

- a. Using the output from the **ipconfig /all** command, answer the following questions.

```
C:\> ipconfig /all
```

```
<output omitted>
```

```
Ethernet adapter Ethernet:
```

```

Connection-specific DNS Suffix  . : 
Description . . . . . : Intel(R) 82577LM Gigabit Network Connection
Physical Address. . . . . : 5C-26-0A-24-2A-60
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b875:731b:3c7b:c0b1%10 (Preferred)
IPv4 Address. . . . . : 192.168.1.147 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, September 6, 2019 11:08:36 AM
Lease Expires . . . . . : Saturday, September 7, 2019 11:08:36 AM
Default Gateway . . . . . : 192.168.1.1

```

```
<output omitted>
```

What is the OUI portion of the MAC address for this device?

What is the serial number portion of the MAC address for this device?

Using the example above, find the name of the vendor that manufactured this NIC.

- b. From the command prompt on PC-A, issue the **ipconfig /all** command and identify the OUI portion of the MAC address for the NIC of PC-A.

Identify the serial number portion of the MAC address for the NIC of PC-A.

Identify the name of the vendor that manufactured the NIC of PC-A.

Step 2: Analyze the MAC address for the S1 F0/6 interface.

You can use a variety of commands to display MAC addresses on the switch.

- a. Console into S1 and use the **show interfaces vlan 1** command to find the MAC address information. A sample is shown below. Use output generated by your switch to answer the questions.

```
S1# show interfaces vlan 1
Vlan1 is up, line protocol is up
  Hardware is EtherSVI, address is 001b.0c6d.8f40 (bia 001b.0c6d.8f40)
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:14:51, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    34 packets output, 11119 bytes, 0 underruns
    0 output errors, 2 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
```

What is the MAC address for VLAN 1 on S1?

What is the MAC serial number for VLAN 1?

What is the OUI for VLAN 1?

Based on this OUI, what is the name of the vendor?

What does bia stand for?

Why does the output show the same MAC address twice?

- b. Another way to display the MAC address on the switch is to use the **show arp** command. Use the **show arp** command to display MAC address information. This command maps the Layer 2 address to its corresponding Layer 3 address. A sample is shown below. Use output generated by your switch to answer the questions.

S1# **show arp**

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.2	-	001b.0c6d.8f40	ARPA	Vlan1
Internet	192.168.1.3	0	5c26.0a24.2a60	ARPA	Vlan1

What Layer 2 addresses are displayed on S1?

Step 3: View the MAC addresses on the switch.

Issue the **show mac address-table** command on S1. A sample is shown below. Use output generated by your switch to answer the questions.

S1# **show mac address-table**

Mac Address Table

```
-----
```

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0180.c200.0000	STATIC	CPU
All	0180.c200.0001	STATIC	CPU
All	0180.c200.0002	STATIC	CPU
All	0180.c200.0003	STATIC	CPU
All	0180.c200.0004	STATIC	CPU
All	0180.c200.0005	STATIC	CPU
All	0180.c200.0006	STATIC	CPU
All	0180.c200.0007	STATIC	CPU
All	0180.c200.0008	STATIC	CPU
All	0180.c200.0009	STATIC	CPU
All	0180.c200.000a	STATIC	CPU
All	0180.c200.000b	STATIC	CPU
All	0180.c200.000c	STATIC	CPU
All	0180.c200.000d	STATIC	CPU
All	0180.c200.000e	STATIC	CPU
All	0180.c200.000f	STATIC	CPU
All	0180.c200.0010	STATIC	CPU
All	ffff.ffff.ffff	STATIC	CPU
1	5c26.0a24.2a60	DYNAMIC	Fa0/6

Total Mac Addresses for this criterion: 21

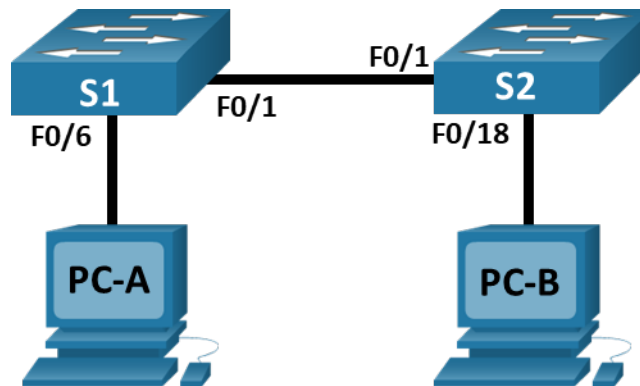
Did the switch display the MAC address of PC-A? If you answered yes, what port was it on?

Reflection Questions

1. Can you have broadcasts at the Layer 2 level? If so, what would the MAC address be?
2. Why would you need to know the MAC address of a device?

Lab 4: View the Switch MAC Address Table

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.11	255.255.255.0
S2	VLAN 1	192.168.1.12	255.255.255.0
PC-A	NIC	192.168.1.1	255.255.255.0
PC-B	NIC	192.168.1.2	255.255.255.0

Objectives

Part 1: Build and Configure the Network

Part 2: Examine the Switch MAC Address Table

Background / Scenario

The purpose of a Layer 2 LAN switch is to deliver Ethernet frames to host devices on the local network. The switch records host MAC addresses that are visible on the network, and maps those MAC addresses to its own Ethernet switch ports. This process is called building the MAC address table. When a switch receives a frame from a PC, it examines the frame's source and destination MAC addresses. The source MAC address is recorded and mapped to the switch port from which it arrived. Then the destination MAC address is looked up in the MAC address table. If the destination MAC address is a known address, then the frame is forwarded out of the corresponding switch port associated with that MAC address. If the MAC address is unknown, then the frame is broadcasted out of all switch ports, except the one from which it came. It is important to observe and understand the function of a switch and how it delivers data on the network. The way a switch operates has implications for network administrators whose job it is to ensure secure and consistent network communication.

Switches are used to interconnect and deliver information to computers on local area networks. Switches deliver Ethernet frames to host devices identified by network interface card MAC addresses.

In Part 1, you will build a multi-switch topology with a trunk linking the two switches. In Part 2, you will ping various devices and observe how the two switches build their MAC address tables.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.2(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.

Required Resources

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

Note: The Fast Ethernet interfaces on Cisco 2960 switches are autosensing and an Ethernet straight-through cable may be used between switches S1 and S2. If using another model Cisco switch, it may be necessary to use an Ethernet crossover cable.

Instructions

Part 1: Build and Configure the Network

Step 1: Cable the network according to the topology.

Step 2: Configure PC hosts.

Step 3: Initialize and reload switches as necessary.

Step 4: Configure basic settings for each switch.

- Configure device name as shown in the topology.
- Configure IP address as listed in Addressing Table.
- Assign **cisco** as the console and vty passwords.
- Assign **class** as the privileged EXEC password.

Part 2: Examine the Switch MAC Address Table

A switch learns MAC addresses and builds the MAC address table, as network devices initiate communication on the network.

Step 1: Record network device MAC addresses.

- Open a command prompt on PC-A and PC-B and type **ipconfig /all**.

What are the Ethernet adapter physical addresses?

PC-A MAC Address:

PC-B MAC Address:

- Console into switch S1 and S2 and type the **show interface F0/1** command on each switch.

On the second line of command output, what is the hardware addresses (or burned-in address [bia])?

S1 Fast Ethernet 0/1 MAC Address:

S2 Fast Ethernet 0/1 MAC Address:

Step 2: Display the switch MAC address table.

Console into switch S2 and view the MAC address table, both before and after running network communication tests with ping.

- Establish a console connection to S2 and enter privileged EXEC mode.
- In privileged EXEC mode, type the **show mac address-table** command and press Enter.

S2# **show mac address-table**

Even though there has been no network communication initiated across the network (i.e., no use of ping), it is possible that the switch has learned MAC addresses from its connection to the PC and the other switch.

Are there any MAC addresses recorded in the MAC address table?

What MAC addresses are recorded in the table? To which switch ports are they mapped and to which devices do they belong? Ignore MAC addresses that are mapped to the CPU.

If you had not previously recorded MAC addresses of network devices in Step 1, how could you tell which devices the MAC addresses belong to, using only the output from the **show mac address-table** command? Does it work in all scenarios?

Step 3: Clear the S2 MAC address table and display the MAC address table again.

- In privileged EXEC mode, type the **clear mac address-table dynamic** command and press Enter.

S2# **clear mac address-table dynamic**

- Quickly type the **show mac address-table** command again.

Does the MAC address table have any addresses in it for VLAN 1? Are there other MAC addresses listed?

Wait 10 seconds, type the **show mac address-table** command, and press Enter. Are there new addresses in the MAC address table?

Step 4: From PC-B, ping the devices on the network and observe the switch MAC address table.

- From PC-B, open a command prompt and type **arp -a**.

Not including multicast or broadcast addresses, how many device IP-to-MAC address pairs have been learned by ARP?

- b. From the PC-B command prompt, ping PC-A, S1, and S2.

Did all devices have successful replies? If not, check your cabling and IP configurations.

- c. From a console connection to S2, enter the **show mac address-table** command.

Has the switch added additional MAC addresses to the MAC address table? If so, which addresses and devices?

From PC-B, open a command prompt and retype **arp -a**.

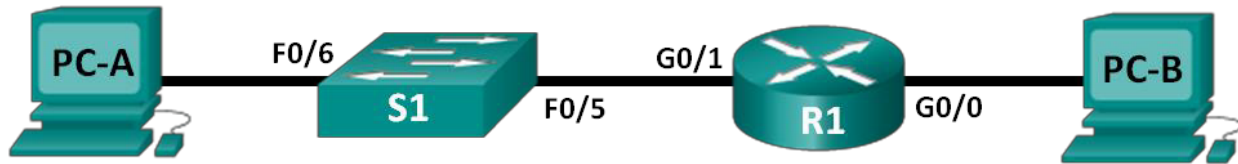
Does the PC-B ARP cache have additional entries for all network devices that were sent pings?

Reflection Question

On Ethernet networks, data is delivered to devices by their MAC addresses. For this to happen, switches and PCs dynamically build ARP caches and MAC address tables. With only a few computers on the network this process seems fairly easy. What might be some of the challenges on larger networks?

Lab 5: Configuring Basic Router Settings with IOS CLI

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.

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.

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

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

```
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.

-
- 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?

-
- 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#
```

- l. 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?

Step 3: Verify network connectivity.

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

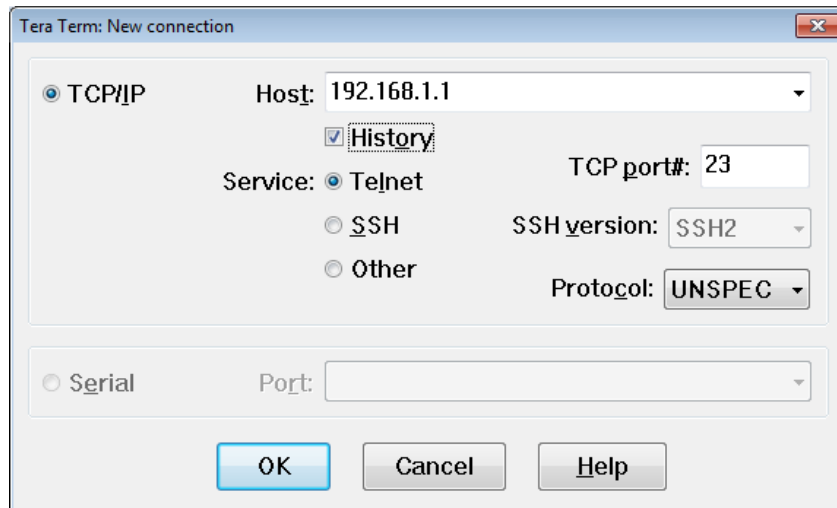
Note: It may be necessary to disable the PCs firewall.

Were the pings successful? _____

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

- 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?

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

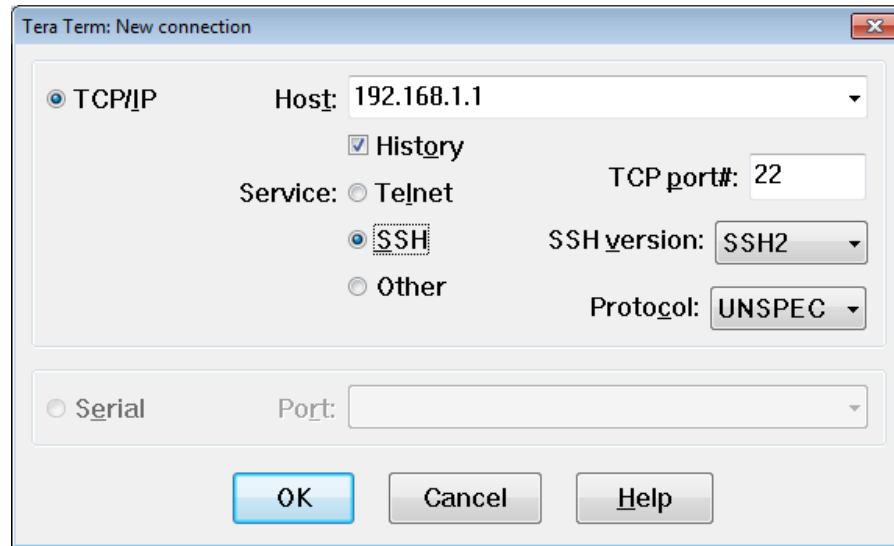
Step 4: Configure the router for SSH access.

- 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? _____

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.

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

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

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

How much Flash memory does the router have?

- 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.

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

Step 3: Display the startup configuration.

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

How are passwords presented in the output?

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

What is the result of using this command?

Step 4: Display the routing table on the router.

Use the **show ip route** command on the router to answer the following questions. What code is used in the routing table to indicate a directly connected network?

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

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.

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

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.

- 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.

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

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

What is the IPv6 address assigned to PC-B?

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

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

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

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?

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?

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?

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  -rw-          1919   Mar 1 1993 00:06:33 +00:00  private-config.text
 3  -rw-          1632   Mar 1 1993 00:06:33 +00:00  config.text
 4  -rw-         13336   Mar 1 1993 00:06:33 +00:00  multiple-fs
 5  -rw-       11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
 6  -rw-           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
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>
```

Lab 6: Calculate IPv4 Subnets

Objectives

Part 1: Determine IPv4 Address Subnetting

Part 2: Calculate IPv4 Address Subnetting

Background / Scenario

The ability to work with IPv4 subnets and determine network and host information based on a given IP address and subnet mask is critical to understanding how IPv4 networks operate. The first part is designed to reinforce how to compute network IP address information from a given IP address and subnet mask. When given an IP address and subnet mask, you will be able to determine other information about the subnet.

Required Resources

- 1 PC (Windows with Internet access)
- Optional: IPv4 address calculator

Instructions

Fill out the tables below with appropriate answers given the IPv4 address, original subnet mask, and new subnet mask.

Part 1:

Given:	
Host IP Address:	192.168.200.139
Original Subnet Mask	255.255.255.0
New Subnet Mask:	255.255.255.224
Find:	
Number of Subnet Bits	
Number of Subnets Created	
Number of Host Bits per Subnet	
Number of Hosts per Subnet	
Network Address of this Subnet	
IPv4 Address of First Host on this Subnet	
IPv4 Address of Last Host on this Subnet	
IPv4 Broadcast Address on this Subnet	

Part 2:

Given:	
Host IP Address:	10.101.99.228
Original Subnet Mask	255.0.0.0
New Subnet Mask:	255.255.128.0
Find:	
Number of Subnet Bits	
Number of Subnets Created	
Number of Host Bits per Subnet	
Number of Hosts per Subnet	
Network Address of this Subnet	
IPv4 Address of First Host on this Subnet	
IPv4 Address of Last Host on this Subnet	
IPv4 Broadcast Address on this Subnet	

Part 3:

Given:	
Host IP Address:	172.22.32.12
Original Subnet Mask	255.255.0.0
New Subnet Mask:	255.255.224.0
Find:	
Number of Subnet Bits	
Number of Subnets Created	
Number of Host Bits per Subnet	
Number of Hosts per Subnet	
Network Address of this Subnet	
IPv4 Address of First Host on this Subnet	
IPv4 Address of Last Host on this Subnet	
IPv4 Broadcast Address on this Subnet	

Part 4:

Given:	
Host IP Address:	192.168.1.245
Original Subnet Mask	255.255.255.0
New Subnet Mask:	255.255.255.252
Find:	
Number of Subnet Bits	
Number of Subnets Created	
Number of Host Bits per Subnet	
Number of Hosts per Subnet	
Network Address of this Subnet	
IPv4 Address of First Host on this Subnet	
IPv4 Address of Last Host on this Subnet	
IPv4 Broadcast Address on this Subnet	

Part 5:

Given:	
Host IP Address:	128.107.0.55
Original Subnet Mask	255.255.0.0
New Subnet Mask:	255.255.255.0
Find:	
Number of Subnet Bits	
Number of Subnets Created	
Number of Host Bits per Subnet	
Number of Hosts per Subnet	
Network Address of this Subnet	
IPv4 Address of First Host on this Subnet	
IPv4 Address of Last Host on this Subnet	
IPv4 Broadcast Address on this Subnet	

Part 6:

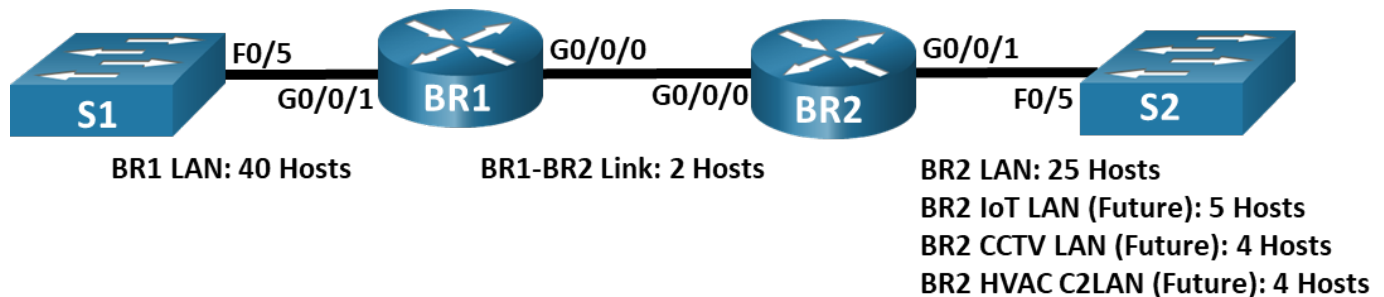
Given:	
Host IP Address:	192.135.250.180
Original Subnet Mask	255.255.255.0
New Subnet Mask:	255.255.255.248
Find:	
Number of Subnet Bits	
Number of Subnets Created	
Number of Host Bits per Subnet	
Number of Hosts per Subnet	
Network Address of this Subnet	
IPv4 Address of First Host on this Subnet	
IPv4 Address of Last Host on this Subnet	
IPv4 Broadcast Address on this Subnet	

Reflection Question

Why is the subnet mask so important when analyzing an IPv4 address?

Lab 7: Design and Implement a VLSM Addressing Scheme

Topology



Objectives

Part 1: Examine Network Requirements

Part 2: Design the VLSM Address Scheme

Part 3: Cable and Configure the IPv4 Network

Background / Scenario

Variable Length Subnet Mask (VLSM) was designed to avoid wasting IP addresses. With VLSM, a network is subnetted and then re-subnetted. This process can be repeated multiple times to create subnets of various sizes based on the number of hosts required in each subnet. Effective use of VLSM requires address planning.

In this lab, use the 192.168.33.128/25 network address to develop an address scheme for the network displayed in the topology diagram. VLSM is used to meet the IPv4 addressing requirements. After you have designed the VLSM address scheme, you will configure the interfaces on the routers with the appropriate IP address information. The future LANS at BR2 will need to have addresses allocated, but no interfaces will be configured at this time.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(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 the 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.

Required Resources

- 2 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 1 PCs (Windows with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology
- Windows Calculator (optional)

Instructions

Part 1: Examine Network Requirements

In Part 1, you will examine the network requirements to develop a VLSM address scheme for the network displayed in the topology diagram using the 192.168.33.128/25 network address.

Note: You can use the Windows Calculator application and search the internet for an IP subnet calculator to help with your calculations.

Step 1: Determine how many host addresses and subnets are available.

How many host addresses are available in a /25 network?

What is the total number of host addresses needed in the topology diagram?

How many subnets are needed in the network topology?

Step 2: Determine the largest subnet.

What is the subnet description (e.g. BR1 LAN or BR1-BR2 link)?

How many IP addresses are required in the largest subnet?

What subnet mask can support that many host addresses?

How many total host addresses can that subnet mask support?

Can you subnet the 192.168.33.128/25 network address to support this subnet?

What are the network addresses that would result from this subnetting?

Use the first network address for this subnet.

Step 3: Determine the second largest subnet.

What is the subnet description?

How many IP addresses are required for the second largest subnet?

What subnet mask can support that many host addresses?

How many total host addresses can that subnet mask support?

Can you subnet the remaining subnet again and still support this subnet?

What are the network addresses that would result from this subnetting?

Use the first network address for this subnet.

Step 4: Determine the third largest subnet.

What is the subnet description?

How many IP addresses are required for the next largest subnet?

What subnet mask can support that many host addresses?

How many total host addresses can that subnet mask support?

Can you subnet the remaining subnet again and still support this subnet?

What are the network addresses that would result from this subnetting?

Use the first network address for this subnet.

Use the second network address for the CCTV LAN.

Use the third network address for the HVAC C2 LAN.

Step 5: Determine the fourth largest subnet.

What is the subnet description?

How many IP addresses are required for the next largest subnet?

What subnet mask can support that many host addresses?

How many total host addresses can that subnet mask support?

Can you subnet the remaining subnet again and still support this subnet?

What are the network addresses that would result from this subnetting?

Use the first network address for this subnet.

Part 2: Design the VLSM Address Scheme

Step 1: Calculate the subnet information.

Use the information that you obtained in Part 1 to fill in the following table.

Subnet Description	Number of Hosts Needed	Network Address /CIDR	First Host Address	Broadcast Address
BR1 LAN	40			
BR2 LAN	25			
BR2 IoT LAN	5			
BR2 CCTV LAN	4			
BR2 HVAC C2LAN	4			
BR1-BR2 Link	2			

Step 2: Complete the device interface address table.

Assign the first host address in the subnet to the Ethernet interfaces. BR1 should be assigned the first host address in the BR1-BR2 Link.

Device	Interface	IP Address	Subnet Mask	Device Interface
BR1	G0/0/0	192.168.33.249	255.255.255.252	BR1-BR2 Link
	G0/0/1	192.168.33.129	255.255.255.192	40 Host LAN
BR2	G0/0/0	192.168.33.250	255.255.255.252	BR1-BR2 Link
	G0/0/1	192.168.33.193	255.255.255.224	25 Host LAN

Part 3: Cable and Configure the IPv4 Network

In Part 3, you will cable the network to match the topology and configure the three routers using the VLSM address scheme that you developed in Part 2.

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

Step 2: Configure basic settings on each router.

- Assign the device name to the routers.
- Disable DNS lookup to prevent the routers from attempting to translate incorrectly entered commands as though they were hostnames.
- Assign **class** as the privileged EXEC encrypted password for both routers.
- Assign **cisco** as the console password and enable login for the routers.
- Assign **cisco** as the VTY password and enable login for the routers.
- Encrypt the plaintext passwords for the routers.
- Create a banner that will warn anyone accessing the device that unauthorized access is prohibited on both routers.

Step 3: Configure the interfaces on each router.

- a. Assign an IP address and subnet mask to each interface using the table that you completed in Part 2.
- b. Configure an interface description for each interface.
- c. Activate the interfaces.

Step 4: Save the configuration on all devices.**Step 5: Test Connectivity.**

- a. From BR1, ping BR2's G0/0/0 interface.
- b. From BR2, ping BR1's G0/0/0 interface.
- c. Troubleshoot connectivity issues if pings were not successful.

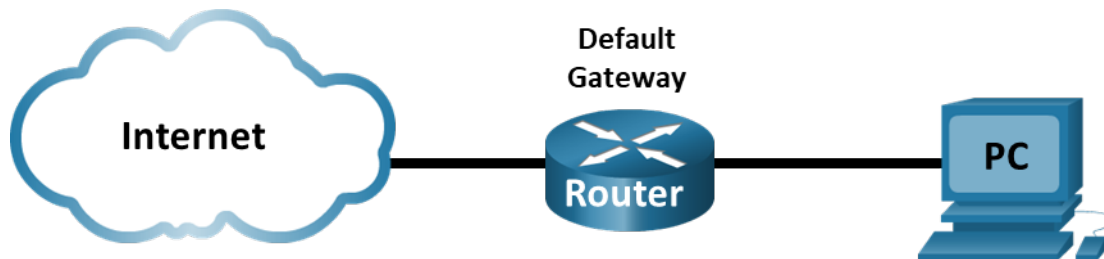
Note: Pings to the GigabitEthernet LAN interfaces on other routers will not be successful. A routing protocol needs to be in place for other devices to be aware of those subnets. The GigabitEthernet interfaces also need to be in an up/up state before a routing protocol can add the subnets to the routing table. The focus of this lab is on VLSM and configuring the interfaces.

Reflection Question

Can you think of a shortcut for calculating the network addresses of consecutive /30 subnets?

Lab 8 - Identify IPv6 Addresses

Topology



Objectives

Part 1: Practice with Different Types of IPv6 Addresses

Part 2: Examine a Host IPv6 Network Interface and Address

Background / Scenario

With the depletion of the Internet Protocol version 4 (IPv4) network address space and the adoption and transition to IPv6, networking professionals must understand how both IPv4 and IPv6 networks function. Many devices and applications already support IPv6. This includes extensive Cisco device Internetwork Operating System (IOS) support and workstation/server operating system support, such as that found in Windows and Linux.

This lab focuses on IPv6 addresses and the components of the address. In Part 1, you will identify the IPv6 address types and IPv6 addresses abbreviation. In Part 2, you will view the IPv6 settings on a PC.

Required Resources

- 1 PC (Windows with Internet access)

Instructions

Part 1: Practice with Different Types of IPv6 Addresses

In this part, you will identify the different types of IPv6 addresses and practice compressing and decompressing IPv6 addresses.

Step 1: Match the IPv6 address to its type.

Match the IPv6 addresses to their corresponding address type. Notice that the addresses have been compressed to their abbreviated notation and that the slash network prefix number is not shown. Some answer choices must be used more than once.

Answer choices:

- Loopback address
- Global unicast address
- Link-local address
- Unique-local address
- Multicast address

IPv6 Address	Answer
2001:0db8:1:acad::fe55:6789:b210	
::1	
fc00:22:a:2::cd4:23e4:76fa	
2033:db8:1:1:22:a33d:259a:21fe	
fe80::3201:cc01:65b1	
ff00::	
ff00::db7:4322:a231:67c	
ff02::2	

Step 2: Practice compressing and decompressing IPv6 addresses.

Using the rules of IPv6 address abbreviation, either compress or decompress the following addresses:

- 2002:0ec0:0200:0001:0000:04eb:44ce:08a2
- fe80:0000:0000:0001:0000:60bb:008e:7402
- fe80::7042:b3d7:3dec:84b8
- ff00::
- 2001:0030:0001:acad:0000:330e:10c2:32bf

Part 2: Examine a Host IPv6 Network Interface and Address

In Part 2, you will check the IPv6 network settings of your PC to identify your network interface IPv6 address.

Step 1: Check your PC IPv6 network address settings.

Verify that the IPv6 protocol is installed and active on your PC-A (check your Local Area Connection settings).

- Navigate to the **Control Panel**.
- In the Category View, click **Network and Sharing Center** icon. Click **View network status and tasks**.
- In the Network and Sharing Center window, you will see your active networks.
- On the left side of the window, click **Change adapter settings**. You should now see icons representing your installed network adapters. Right-click your active network interface (it may be an **Ethernet** or a **Wi-Fi**), and then click **Properties**.
- In the Properties window, scroll through the list of items to determine whether IPv6 is present, which indicates that it is installed, and if it is also check marked, which indicates that it is active.
- Select the item **Internet Protocol Version 6 (TCP/IPv6)** and click **Properties**. You should see the IPv6 settings for your network interface. Your IPv6 properties window is likely set to **Obtain an IPv6 address automatically**. This does not mean that IPv6 relies on the Dynamic Host Configuration Protocol (DHCP). Instead of using DHCP, IPv6 looks to the local router for IPv6 network information and then auto-

configures its own IPv6 addresses. To manually configure IPv6, you must provide the IPv6 address, the subnet prefix length, and the default gateway. Click **Cancel** to exit the properties windows.

Note: The local router can refer host requests for IPv6 information, especially Domain Name System (DNS) information, to a DHCPv6 server on the network.

- g. After you have verified that IPv6 is installed and active on your PC, you should check your IPv6 address information.

Open a command prompt and type **ipconfig /all** and press Enter. Your output should look similar to this:

```
C:\Users\user> ipconfig /all
```

```
Windows IP Configuration
```

```
<output omitted>
```

```
Wireless LAN adapter Wireless Network Connection:
```

```

Connection-specific DNS Suffix . . : 
Description . . . . . : Intel(R) Centrino(R) Advanced-N 6200 AGN
Physical Address. . . . . : 02-37-10-41-FB-48
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8d4f:4f4d:3237:95e2%14 (Preferred)
IPv4 Address. . . . . : 192.168.2.106(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, January 06, 2013 9:47:36 AM
Lease Expires . . . . . : Monday, January 07, 2013 9:47:38 AM
Default Gateway . . . . . : 192.168.2.1
DHCP Server . . . . . : 192.168.2.1
DHCPv6 IAID . . . . . : 335554320
DHCPv6 Client DUID. . . . . : 00-01-00-01-14-57-84-B1-1C-C1-DE-91-C3-5D

DNS Servers . . . . . : 192.168.1.1
                        8.8.4.4

```

```
<output omitted>
```

- h. You can see from the output that the client PC has an IPv6 link-local address with a randomly generated interface ID.

What does it indicate about the network regarding IPv6 global unicast address, IPv6 unique-local address, or IPv6 gateway address?

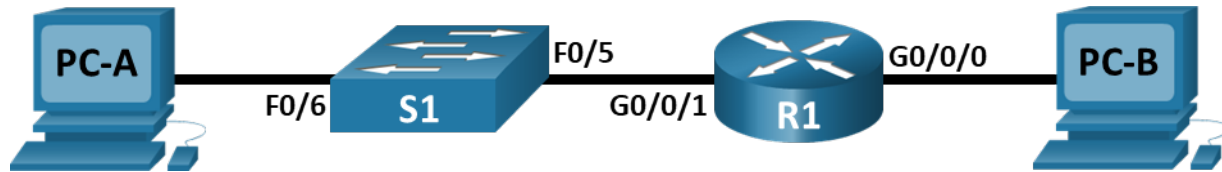
What kind of IPv6 addresses did you find when using **ipconfig /all**?

Reflection Questions

1. How do you think you must support IPv6 in the future?
2. Do you think IPv4 networks continue on, or will everyone eventually switch over to IPv6? How long do you think it will take?

Lab 9 - Configure IPv6 Addresses on Network Devices

Topology



Addressing Table

Device	Interface	IPv6 Address	Prefix Length	Default Gateway
R1	G0/0/0	2001:db8:acad:a::1	64	N/A
	G0/0/1	2001:db8:acad:1::1	64	N/A
S1	VLAN 1	2001:db8:acad:1::b	64	N/A
PC-A	NIC	2001:db8:acad:1::3	64	fe80::1
PC-B	NIC	2001:db8:acad:a::3	64	fe80::1

Objectives

Part 1: Set Up Topology and Configure Basic Router and Switch Settings

Part 2: Configure IPv6 Addresses Manually

Part 3: Verify End-to-End Connectivity

Background / Scenario

In this lab, you will configure hosts and device interfaces with IPv6 addresses. You will issue **show** commands to view IPv6 unicast addresses. You will also verify end-to-end connectivity using **ping** and **traceroute** commands.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(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 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.

Note: The default 2960 Switch Database Manager (SDM) template does not support IPv6. It may be necessary to issue the command **sdm prefer dual-ipv4-and-ipv6 default** to enable IPv6 addressing before applying an IPv6 address to the VLAN 1 SVI.

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.

```
S1# show sdm prefer
```

Follow these steps to assign the dual-ipv4-and-ipv6 template as the default SDM template:

```
S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

Required Resources

- 1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 2 PCs (Windows with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Gigabit Ethernet interfaces on Cisco 4221 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.

Instructions

Part 1: Cable the Network and Configure Basic Router and Switch Settings

After cabling the network, initializing and reloading the router and switch, complete the following:

Step 1: Configure the router.

Assign the hostname and configure basic device settings.

Step 2: Configure the switch.

Assign the hostname and configure basic device settings.

Part 2: Configure IPv6 Addresses Manually

Step 1: Assign the IPv6 addresses to Ethernet interfaces on R1.

- Assign the IPv6 global unicast addresses, listed in the Addressing Table, to both Ethernet interfaces on R1.
- Verify that the correct IPv6 unicast address is assigned to each interface.
Note: The link-local address (fe80::) displayed is based on EUI-64 addressing, which automatically uses the interface Media Access Control (MAC) address to create a 128-bit IPv6 link-local address.
- To get the link-local address to match the global unicast address on the interface, manually enter the link-local addresses on each of the Ethernet interfaces on R1.
Note: Each router interface belongs to a separate network. Packets with a link-local address never leave the local network; therefore, you can use the same link-local address on both interfaces.
- Use a command of your choice to verify that the link-local address has been changed to **fe80::1**.

Which two multicast groups have been assigned to interface G0/0/0?

Step 2: Enable IPv6 routing on R1.

- a. On a PC-B command prompt, enter the **ipconfig** command to examine IPv6 address information assigned to the PC interface.

Has an IPv6 unicast address been assigned to the network interface card (NIC) on PC-B?

- b. Enable IPv6 routing on R1 using the **IPv6 unicast-routing** command.
- c. Use a command to verify the new multicast group are assigned to interface G0/0/0. Notice that the all-router multicast group (ff02::2) now appears for interface G0/0/0.

Note: This will allow the PCs to obtain their IP address and default gateway information automatically using Stateless Address Autoconfiguration (SLAAC).

- d. Now that R1 is part of the all-router multicast group FF02::2, re-issue the **ipconfig** command on PC-B and examine the IPv6 address information.

Why did PC-B receive the Global Routing Prefix and Subnet ID that you configured on R1?

Step 3: Assign IPv6 addresses to the management interface (SVI) on S1.

- a. Assign the IPv6 address for S1. Also assign a link-local address for this interface.
- b. Use a command of your choice to verify that the IPv6 addresses are properly assigned to the management interface.

Step 4: Assign static IPv6 addresses to the PCs.

- a. Open the Ethernet Properties window on for each PC and assign IPv6 addressing.
- b. Verify both PCs have the correct IPv6 address information. Each PC should have two Global IPv6 addresses: one static and one SLACC

Part 3: Verify End-to-End Connectivity

From PC-A, ping **fe80::1**. This is the link-local address assigned to G0/0/1 on R1.

Ping the S1 management interface from PC-A.

Use the **tracert** command on PC-A to verify that you have end-to-end connectivity to PC-B.

From PC-B, ping PC-A.

From PC-B, ping the link-local address for G0/0/0 on R1.

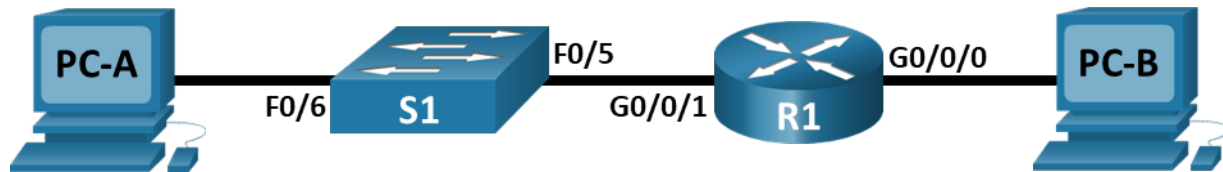
Note: If end-to-end connectivity is not established, troubleshoot your IPv6 address assignments to verify that you entered the addresses correctly on all devices.

Reflection Questions

3. Why can the same link-local address, fe80::1, be assigned to both Ethernet interfaces on R1?
4. What is the Subnet ID of the IPv6 unicast address 2001:db8:acad::aaaa:1234/64?

Lab 10 - Build a Switch and Router Network IPv4 and IPv6

Topology



Addressing Table

Device	Interface	IP Address / Prefix	Default Gateway
R1	G0/0/0	192.168.0.1 /24	N/A
		2001:db8:acad::1/64	
		fe80::1	
	G0/0/1	192.168.1.1 /24	N/A
		2001:db8:acad:1::1/64	
		fe80::1	
S1	VLAN 1	192.168.1.2 /24	192.168.1.1
PC-A	NIC	192.168.1.3 /24	192.168.1.1
		2001:db8:acad:1::3/64	fe80::1
PC-B	NIC	192.168.0.3 /24	192.168.0.1
		2001:db8:acad::3/64	fe80::1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Devices and Verify Connectivity

Background / Scenario

This is a comprehensive lab to review previously covered IOS commands. In this lab, you will cable the equipment as shown in the topology diagram. You will then configure the devices to match the addressing table. After the configurations have been saved, you will verify your configurations by testing for network connectivity.

After the devices have been configured and network connectivity has been verified, you will use IOS commands to retrieve information from the devices to answer questions about your network equipment.

This lab provides minimal assistance with the actual commands necessary to configure the router. Test your knowledge by trying to configure the devices without referring to the content or previous activities.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(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 the lab for the correct interface identifiers.

Note: Ensure that the routers and switches have been erased and have no startup configurations. Consult with your instructor for the procedure to initialize and reload a router and switch.

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
```

Use the following commands to assign the **dual-ipv4-and-ipv6** template as the default SDM template.

```
S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

Required Resources

- 1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 2 PCs (Windows with a terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Gigabit Ethernet interfaces on Cisco 4221 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.

Instructions

Part 1: Set Up Topology and Initialize Devices

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

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

Step 2: Initialize and reload the router and switch.

If configuration files were previously saved on the router and switch, initialize and reload these devices back to their default configurations.

Part 2: Configure Devices and Verify Connectivity

In Part 2, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords. Refer to the **Error! Reference source not found.** and **Error! Reference source not found.** at the beginning of this lab for device names and address information.

Step 1: Assign static IP information to the PC interfaces.

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

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

Note: If pings are not successful, the Windows Firewall may need to be turned off.

Why were the pings not successful?

Step 2: Configure the router.

- a. Console into the router and enable privileged EXEC mode.
- b. Enter configuration mode.
- c. Assign a device name to the router.
- d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- e. Assign **class** as the privileged EXEC encrypted password.
- f. Assign **cisco** as the console password and enable login.
- g. Assign **cisco** as the VTY password and enable login.
- h. Encrypt the plaintext passwords.
- i. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- j. Configure and activate both interfaces on the router.
- k. Configure an interface description for each interface indicating which device is connected to it.
- l. To enable IPv6 routing, enter the command `ipv6 unicast-routing`.

```
R1(config)# ipv6 unicast-routing
```
- m. Save the running configuration to the startup configuration file.
- n. Set the clock on the router.
Note: Use the question mark (?) to help with the correct sequence of parameters needed to execute this command.
- o. Ping PC-B from a command prompt window on PC-A.
Note: If pings are not successful, the Windows Firewall may need to be turned off.
 Were the pings successful? Explain.

Step 3: Configure the switch.

In this step, you will configure the hostname, the VLAN 1 interface and its default gateway.

- a. Console into the switch and enable privileged EXEC mode.
- b. Enter configuration mode.
- c. Assign a device name to the switch.
- d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- e. Configure and activate the VLAN interface on the switch S1.
- f. Configure the default gateway for the switch S1.

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

Step 4: Verify connectivity end-to-end connectivity.

- a. From PC-A, ping PC-B.
 - b. From S1, ping PC-B.
- All the pings should be successful.

Part 3: Display Device Information

In Part 3, you will use **show** commands to retrieve interface and routing information from the router and switch.

Step 1: Display the routing table on the router.

- a. Use the **show ip route** command on the router R1 to answer the following questions.

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

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

What interface types are associated to the C coded routes?

- b. Use the **show ipv6 route** command on router R1 to display the IPv6 routes.

Step 2: Display interface information on the router R1.

- a. Use the **show ip interface g0/0/1** to answer the following questions.

What is the operational status of the G0/0/1 interface?

What is the Media Access Control (MAC) address of the G0/1 interface?

How is the Internet address displayed in this command?

- b. For the IPv6 information, enter the **show ipv6 interface *interface*** command.

Step 3: Display a summary list of the interfaces on the router and switch.

There are several commands that can be used to verify an interface configuration. One of the most useful of these is the **show ip interface brief** command. The command output displays a summary list of the interfaces on the device and provides immediate feedback to the status of each interface.

- a. Enter the **show ip interface brief** command on the router R1.

```
R1# show ip interface brief
```

- b. To see the IPv6 interface information, enter the **show ipv6 interface brief** command on R1.

```
R1# show ipv6 interface brief
```

- c. Enter the **show ip interface brief** command on the switch S1.

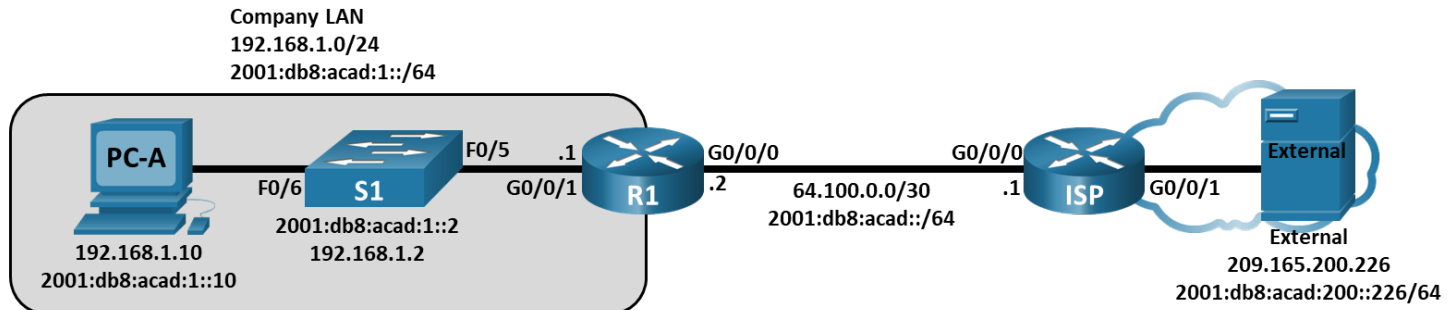
```
S1# show ip interface brief
```

Reflection Questions

1. If the G0/0/1 interface showed that it was administratively down, what interface configuration command would you use to turn the interface up?
2. What would happen if you had incorrectly configured interface G0/0/1 on the router with an IP address of 192.168.1.2?

Lab 11 - Use Ping and Traceroute to Test Network Connectivity

Topology



Addressing Table

Device	Interface	IP Address / Prefix	Default Gateway
R1	G0/0/0	64.100.0.2 /30	N/A
		2001:db8:acad::2 /64	
		fe80::2	
R1	G0/0/1	192.168.1.1 /24	N/A
		2001:db8:acad:1::1 /64	
		fe80::1	
ISP	G0/0/0	64.100.0.1 /30	N/A
		2001:db8:acad::1 /64	
		fe80::1	
ISP	G0/0/1	209.165.200.225 /27	N/A
		2001:db8:acad:200::225 /64	
		fe80::225	
S1	VLAN 1	192.168.1.2 /24	192.168.1.1
		2001:db8:acad:1::2 /64	fe80::1
		fe80::2	
PC-A	NIC	2001:db8:acad:1::10 /64	fe80::1
		192.168.1.10 /24	192.168.1.1
External	NIC	209.165.200.226 /27	209.165.200.225
		2001:db8:acad:200::226 /64	fe80::226

Objectives

Part 1: Build and Configure the Network

Part 2: Use Ping Command for Basic Network Testing

Part 3: Use Tracert and Traceroute Commands for Basic Network Testing

Part 4: Troubleshoot the Topology

Background / Scenario

Ping and traceroute are two tools that are indispensable when testing TCP/IP network connectivity. Ping is a network administration utility used to test the reachability of a device on an IP network. This utility also measures the round-trip time for messages sent from the originating host to a destination computer. The ping utility is available on Windows, Unix-like operating systems (OS), and the Cisco Internetwork Operating System (IOS).

The traceroute utility is a network diagnostic tool for displaying the path or route and measuring the transit delays of packets travelling an IP network. The tracert utility is available on Windows, and a similar utility, traceroute, is available on Unix-like OS and Cisco IOS.

In this lab, the **ping** and **traceroute** commands are examined and command options are explored to modify the command behavior. Cisco devices and PCs are used in this lab for command exploration. The necessary Cisco device configurations are provided in this lab.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(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 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.

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
```

Use the following commands to assign the **dual-ipv4-and-ipv6** template as the default SDM template.

```
S1# configure terminal
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
S1(config)# end
S1# reload
```

Required Resources

- 2 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 2 PCs (Windows with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Instructions

Part 1: Build and Configure the Network

In Part 1, you will set up the network in the topology and configure the PCs and Cisco devices. The initial configurations for the routers and switches are provided for your reference. In this topology, static routing is used to route packets between networks.

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

Step 2: Erase the configurations on the routers and switches, and reload the devices.

Step 3: Configure PC IP addresses and default gateways according to the Addressing Table.

Step 4: Configure the R1 and ISP routers and S1 switch using the initial configurations provided below.

At the switch or router global configuration mode prompt, copy and paste the configuration for each device. Save the configuration to startup-config.

Initial configurations for the R1 router:

```
hostname R1
no ip domain lookup
ipv6 unicast-routing
interface g0/0/0
  ip address 64.100.0.2 255.255.255.252
  ipv6 address 2001:db8:acad::2/64
  ipv6 address fe80::2 link-local
  ip nat outside
  no shutdown
interface g0/0/1
  ip add 192.168.1.1 255.255.255.0
  ipv6 address 2001:db8:acad:1::1/64
  ipv6 address fe80::1 link-local
  ip nat inside
  no shutdown
ip route 0.0.0.0 0.0.0.0 64.100.0.1
ipv6 route 0::/0 2001:db8:acad::1
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface g0/0/0 overload
```

Initial configurations for ISP:

```
hostname ISP
no ip domain lookup
ipv6 unicast-routing
interface g0/0/0
  ip address 64.100.0.1 255.255.255.252
  ipv6 address 2001:db8:acad::1/64
  ipv6 address fe80::1 link-local
  no shutdown
interface g0/0/1
  ip add 209.165.200.225 255.255.255.224
  ipv6 address 2001:db8:acad:200::225/64
  ipv6 address fe80::225 link-local
  no shutdown
#ip route 0.0.0.0 0.0.0.0 64.100.0.2
```

```
ipv6 route ::/0 2001:db8:acad::2
```

Initial configurations for S1:

```
hostname S1
no ip domain-lookup
interface vlan 1
 ip add 192.168.1.2 255.255.255.0
 ipv6 address 2001:db8:acad:1::2/64
 ipv6 address fe80::2 link-local
 no shutdown
 exit
 ip default-gateway 192.168.1.1
 end
```

Step 5: Configure an IP host table on the R1 router.

The IP host table allows you to use a hostname to connect to a remote device rather than an IP address. The host table provides name resolution for the device with the following configurations. Copy and paste the following configurations for the R1 router. The configurations will allow you to use the hostnames for **ping** and **traceroute** commands on the R1 router.

```
ip host Externalv4 209.165.200.226
ipv6 host Externalv6 2001:db8:acad:200::226
ip host ISIPv4 64.100.0.1
ipv6 host ISIPv6 2001:db8:acad::1
ip host PC-Av4 192.168.1.10
ipv6 host PC-Av6 2001:db8:acad:1::10
ip host R1v4 64.100.0.2
ipv6 host R1v6 2001:db8:acad::2
ip host S1v4 192.168.1.2
ipv6 host S1v6 2001:db8:acad:1::2
end
```

Part 2: Use Ping Command for Basic Network Testing

In Part 2 of this lab, use the **ping** command to verify end-to-end connectivity. Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and then waiting for an ICMP response. It can record the round trip time and any packet loss or routing loops.

IP packets have a limited lifetime on the network. IP packets use an 8 bit Time to Live (IPv4) or Hop Limit (IPv6) header field value which specifies the maximum number of layer three hops that can be traversed on the path to their destination. Hosts on a network will set its own 8 bit value with a maximum value of 255.

So each time an IP packet arrives at a layer three network device this value is reduced by one before it is forwarded to its destination. So if this value eventually reaches zero the IP packet is discarded.

You will examine the results with the **ping** command and the additional ping options that are available on Windows-based PCs and Cisco devices.

Step 1: Test network connectivity from the R1 network using PC-A.

All the pings from PC-A to other devices in the topology should be successful. If they are not, check the topology and the cabling, as well as the configuration of the Cisco devices and the PCs.

- a. Ping from PC-A to its default gateway using the IPv4 address (R1's GigabitEthernet 0/0/1 interface).

```
C:\> ping 192.168.1.1
```

```
Pinging 192.168.1.1 with 32 bytes of data:
```

```
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
```

```
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
```

```
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
```

```
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
```

```
Ping statistics for 192.168.1.1:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

In this example, four (4) ICMP requests, 32 bytes each, were sent and the responses were received in less than one millisecond with no packet loss. The transmission and reply time can increase as the ICMP requests and responses are processed by more devices during the journey to and from the final destination.

This can also be done using the IPv6 address of the default gateway (R1's GigabitEthernet 0/0/1 interface).

```
C:\> ping 2001:db8:acad:1::1
```

```
Pinging 2001:db8:acad:1::1 with 32 bytes of data:
```

```
Reply from 2001:db8:acad:1::1: time=5ms
```

```
Reply from 2001:db8:acad:1::1: time=1ms
```

```
Reply from 2001:db8:acad:1::1: time=1ms
```

```
Reply from 2001:db8:acad:1::1: time=1ms
```

```
Ping statistics for 2001:db8:acad:1::1:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 1ms, Maximum = 5ms, Average = 2ms
```

- b. From PC-A, ping the addresses listed in the following table and record the average round trip time and IPv4 Time to Live (TTL) or IPv6 Hop Limit. **Optional:** Use WireShark to see the IPv6 Hop Limit value.

Destination	Average Round Trip Time (ms)	TTL / Hop Limit
192.168.1.10		
2001:db8:acad:1::10		
192.168.1.1 (R1)		
2001:db8:acad:1::1 (R1)		
192.168.1.2 (S1)		
2001:db8:acad:1::2(S1)		
64.100.0.2 (R1)		
2001:db8:acad::2 (R1)		
64.100.0.1 (ISP)		

Destination	Average Round Trip Time (ms)	TTL / Hop Limit
2001:db8:acad::1 (ISP)		
209.165.200.225 (ISP G0/0/1)		
2001:db8:acad:200::225 (ISP G0/0/1)		
209.165.200.226 (External)		
2001:db8:acad:200::226 (External)		

Step 2: Use extended ping commands on PC-A.

The default **ping** command sends four requests at 32 bytes each. It waits 4,000 milliseconds (4 seconds) for each response to be returned before displaying the “Request timed out” message. The **ping** command can be fine-tuned for troubleshooting a network.

- At the command prompt, type **ping** and press Enter.

```
C:\> ping
```

- Using the **-t** option, ping External to verify that External is reachable.

```
C:\Users\User1> ping -t 209.165.200.226
```

To illustrate the results when a host is unreachable, disconnect the cable between the ISP router and External, or shut down the GigabitEthernet 0/0/1 interface on the ISP router.

While the network is functioning correctly, the **ping** command can determine whether the destination responded and how long it took to receive a reply from the destination. If a network connectivity problem exists, the **ping** command displays an error message.

- Reconnect the Ethernet cable or enable the GigabitEthernet 0/0/1 interface on the ISP router (using the **no shutdown** command) before moving onto the next step. After about 30 seconds, the ping should be successful again.
- Press **Ctrl+C** to stop the ping command.
- The above steps can be repeated for IPv6 address to obtain ICMP error message.

What ICMP error messages did you receive?

- Enable the GigabitEthernet 0/0/1 interface on the ISP router (using the **no shutdown** command) before moving onto the next step. After about 30 seconds, the ping should be successful again.

Step 3: Test network connectivity from the R1 network using Cisco devices.

The **ping** command is also available on Cisco devices. In this step, the **ping** command is examined using the R1 router and the S1 switch.

- Ping External on the external network using the IP address of 209.165.200.226 from the R1 router.

```
R1# ping 209.165.200.226
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

The exclamation point (!) indicates that the ping was successful from the R1 router to External. The round trip takes an average of 1 ms with no packet loss, as indicated by a 100% success rate.

- b. Because a local host table was configured on the R1 router, you can ping Externalv4 on the external network using the hostname configured from the R1 router.

Note: The hostname is not case-sensitive. You can substitute the hostname for the IP address if desired on R1 in this lab.

```
R1# ping externalv4
```

What is the IP address used?

- c. There are more options available for the **ping** command. At the CLI, type **ping** and press Enter. Use **ipv6** as the protocol. Input **2001:db8:acad:200::226** or **external** for the Target IPv6 address. Press Enter to accept the default value for other options.

```
R1# ping
Protocol [ip]: ipv6
Target IPv6 address: 2001:db8:acad:200::226
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands? [no]:
Sweep range of sizes? [no]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:200::226, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

- d. You can use an extended ping to observe when there is a network issue. Start the **ping** command to 209.165.200.226 with a repeat a count of 50000. Then, disconnect the cable between the ISP router and EXTERNAL or shut down the GigabitEthernet 0/0/1 interface on the ISP router.

Reconnect the Ethernet cable or enable the GigabitEthernet 0/0/1 interface on the ISP router after the exclamation points (!) have replaced by the letter U and periods (.). After about 30 seconds, the ping should be successful again. Press **Ctrl+Shift+6** to stop the **ping** command if desired.

```
R1# ping
Protocol [ip]:
Target IP address: 209.165.200.226
Repeat count [5]: 10000
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Sending 500, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!.U.U.U.U.
U.U.....!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

!!!!!!!!!!

Success rate is 99 percent (9970/10000), round-trip min/avg/max = 1/1/10 ms

The letter U in the results indicates that a destination is unreachable. An error protocol data unit (PDU) was received by the R1 router. Each period (.) in the output indicates that the ping timed out while waiting for a reply from External. In this example, 1% of the packets were lost during the simulated network outage.

Note: You can also use the following commands for the same results:

```
R1# ping 209.165.200.226 repeat 10000
```

or

```
R1# ping 2001:db8:acad:200::226 repeat 10000
```

The **ping** command is extremely useful when troubleshooting network connectivity. However, ping cannot indicate the location of problem when a ping is not successful. The **tracert** (or **tracert**) command can display network latency and path information.

Part 3: Use Tracert and Traceroute Commands for Basic Network Testing

The commands for tracing routes can be found on PCs and network devices. For a Windows-based PC, the **tracert** command uses ICMP messages to trace the path to the final destination. The **tracert** command utilizes the User Datagram Protocol (UDP) datagrams for tracing routes to the final destination for Cisco devices and other Unix-like PCs.

In Part 3, you will examine the traceroute commands and determine the path that a packet travels to its final destination. You will use the **tracert** command from the Windows PCs and the **tracert** command from the Cisco devices. You will also examine the options that are available for fine tuning the traceroute results.

Step 1: Use the tracert command from PC-A to EXTERNAL.

- At the command prompt, type **tracert 209.165.200.226**.

```
C:\> tracert 209.165.200.226
```

The tracert results indicates the path from PC-A to EXTERNAL is from PC-A to R1 to ISP to EXTERNAL. The path to EXTERNAL traveled through two router hops to the final destination of EXTERNAL.

Step 2: Explore additional options for the tracert command.

- At the command prompt, type **tracert** and press Enter to see the available options.

```
C:\> tracert
```

- Use the **-d** option. Notice that the IP address of 209.165.200.226 is not resolved as EXTERNAL.

```
C:\> tracert -d 209.165.200.226
```

Step 3: Use the traceroute command from the R1 router to External.

At the command prompt, type **tracert 209.165.200.226** or **tracert 2001:db8:acad:200::226** on the R1 router. The hostnames are resolved because a local IP host table was configured on the R1 router.

```
R1# traceroute 209.165.200.226
```

```
R1# traceroute 2001:db8:acad:200::226
```

Step 4: Use the traceroute command from the S1 switch to External.

On the S1 switch, type **traceroute 209.165.200.226** or **traceroute 2001:db8:acad:200::226**. The hostnames are not displayed in the traceroute results because a local IP host table was not configured on this switch.

```
S1# traceroute 209.165.200.226
```

```
S1# traceroute 2001:db8:acad:200::226
```

The **traceroute** command has additional options. You can use the **?** or just press Enter after typing **traceroute** at the prompt to explore these options.

The following link provides more information regarding the **ping** and **traceroute** commands for a Cisco device:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6057.shtml

Part 4: Troubleshoot the Topology

Step 1: Copy and paste the following configuration into the ISP router.

```
hostname ISP
interface g0/0/0
 ip address 64.100.0.1 255.255.255.252
 ipv6 address 2001:db8:acad::1/64
 no shutdown
interface g0/0/1
 ip address 192.168.8.1 255.255.255.0
 no ipv6 address 2001:db8:acad:200::225/64
 ipv6 address 2001:db8:acad:201::225/64
 no shutdown
end
```

Step 2: From the R1 network, use ping and tracert or traceroute commands to troubleshoot and correct the problem on the ISP network.

- a. Use the **ping** and **tracert** commands from PC-A.

You can use the **tracert** command to determine end-to-end network connectivity. This tracert result indicates that PC-A can reach its default gateway of 192.168.1.1, but PC-A does not have network connectivity with External.

One way to locate the network issue is to ping each hop in the network to EXTERNAL. First determine if PC-A can reach the ISP router g0/0/0 interface with an IP address of 64.100.0.1.

- b. PC-A can reach the ISP router. Based on the successful ping results from PC-A to the ISP router, the network connectivity issue is with 209.165.200.224/24 network. Ping the default gateway to External, which is the GigabitEthernet 0/0/1 interface of the ISP router.

PC-A cannot reach the GigabitEthernet 0/0/1 interface of the ISP router, as displayed by the results from the **ping** command.

The tracert and ping results conclude that PC-A can reach the R1 and ISP routers, but not the External or default gateway for External.

- c. Use the **show** commands to examine the running configurations for the ISP router.

The outputs of the **show run** and **show ip interface brief** commands indicate that the GigabitEthernet 0/0/1 interface is up/up, but was configured with an incorrect IP address.

- d. Correct the found issues.
- e. Verify that PC-A can ping and traceroute to EXTERNAL.

Note: This can also be accomplished using **ping** and **traceroute** commands from the CLI on the ISP router and the S1 switch after verifying that there are no network connectivity issues on the 192.168.1.0/24 network.

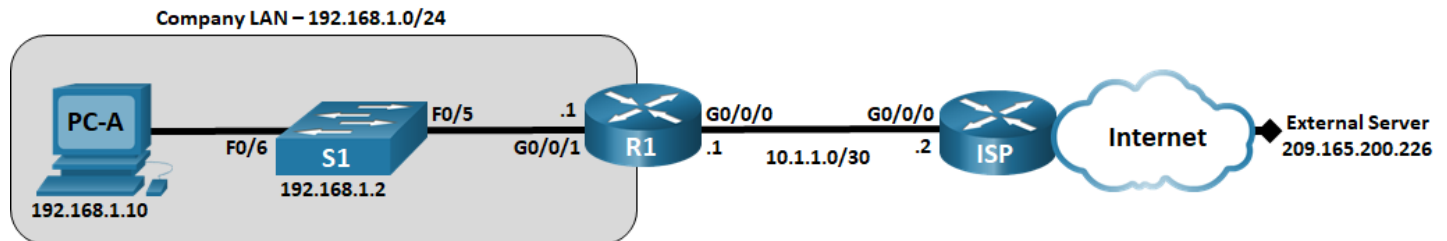
- f. Now repeat the process for IPv6 connectivity. **Note:** If you find an incorrect IPv6 address, you will need to remove it because it is not replaced by a new ipv6 address command.

Reflection Questions

1. What could prevent ping or traceroute responses from reaching the originating device beside network connectivity issues?
2. If you ping a non-existent address on the remote network, such as 209.165.200.227, what is the message displayed by the **ping** command? What does this mean? If you ping a valid host address and receive this response, what should you check?
3. If you ping an address that does not exist in any network in your topology, such as 192.168.5.3, from a Windows-based PC, what is the message displayed by the **ping** command? What does this message indicate?
4. What is the IPv4 TTL value set on the Windows host? What is the IPv4 TTL value set on a Cisco device?
5. What is the IPv6 Hop Limit value set on the Windows host? What is the IPv6 Hop Limit value set on a Cisco device?

Lab 12 - Troubleshoot Connectivity Issues

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/0/1	192.168.1.1	255.255.255.0	N/A
	G0/0/0	10.1.1.1	255.255.255.252	N/A
ISP	G0/0/0	10.1.1.2	255.255.255.252	N/A
	Lo0	209.165.200.226	255.255.255.255	N/A
S1	VLAN 1	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: Identify the Problem

Part 2: Implement Network Changes

Part 3: Verify Full Functionality

Part 4: Document Findings and Configuration Changes

Background / Scenario

In this lab, the company that you work for is experiencing problems with their Local Area Network (LAN). You have been asked to troubleshoot and resolve the network issues. In Part 1, you will connect to devices on the LAN and use troubleshooting tools to identify the network issues, establish a theory of probable cause, and test that theory. In Part 2, you will establish a plan of action to resolve and implement a solution. In Part 3, you will verify full functionality has been restored. Part 4 provides space for you to document your troubleshooting findings along with the configuration changes that you made to the LAN devices.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(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 the lab for the correct interface identifiers.

Required Resources

- 2 Routers (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)

- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 1 PC (Windows with a 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

Troubleshooting Configuration

The following settings must be configured on the devices shown in the topology. Paste the configurations onto the specified devices prior to starting the lab.

S1:

```
no ip domain-lookup
hostname S1
ip domain-name ccna-lab.com
username admin01 privilege 15 secret cisco12345
interface FastEthernet0/1
shutdown
interface FastEthernet0/2
shutdown
interface FastEthernet0/3
shutdown
interface FastEthernet0/4
shutdown
interface FastEthernet0/5
speed 10
duplex half
interface Vlan1
ip address 192.168.1.2 255.255.255.0
ip default-gateway 192.168.1.0
banner motd $ Authorized Users Only! $
line vty 0 4
login local
transport input ssh
line vty 5 15
login local
transport input ssh
crypto key generate rsa general-keys modulus 1024
end
```

R1:

```
hostname R1
no ip domain lookup
ip domain name ccna-lab.com
username admin01 privilege 15 secret cisco12345
interface GigabitEthernet0/0/1
ip address 192.168.1.1 255.255.255.0
no negotiation auto
```

```

speed 100
no shutdown
interface GigabitEthernet0/0/0
ip address 10.1.1.1 255.255.255.252
no shutdown
banner motd $ Authorized Users Only! $
line vty 0 4
login local
transport input ssh
crypto key generate rsa general-keys modulus 1024
end

```

ISP:

```

hostname ISP
no ip domain lookup
interface GigabitEthernet0/0/0
ip address 10.1.1.2 255.255.255.252
no shut
interface Lo0
ip address 209.165.200.226 255.255.255.255
ip route 0.0.0.0 0.0.0.0 10.1.1.1
end

```

Part 1: Identify the Problem.

The only available information about the network problem is that the users are experiencing slow response times and that they are not able to reach an external device on the internet at IP address 209.165.200.226. To determine probable cause(s) for these network issues, you will need to utilize network commands and tools on the LAN equipment shown in the topology.

Note: The user name **admin01** with a password of **cisco12345** will be required to log into the network equipment.

Step 1: Troubleshoot the network.

Use the tools available to you to troubleshoot the network, keeping in mind that the requirement is to restore connectivity to the external server and the eliminate slow response times.

Note: While using SSH to connect to network devices, issue the **terminal monitor** privileged exec command to enable log output to the SSH console.

Step 2: Document the probable causes.

List the probable causes for the network problems that employees are experiencing. Type your answer here.

Part 2: Implement Network Changes

You have communicated the problems that you discovered in Part 1 to your supervisor. She has approved these changes and has requested that you implement them.

Part 3: Verify Full Functionality

Verify that full functionality has been restored. PC-A, S1, and R1 should be able to reach the external server, and ping replies from PC-A to the external server should exhibit no significant variation in response times.

Part 4: Document Findings and Configuration Changes

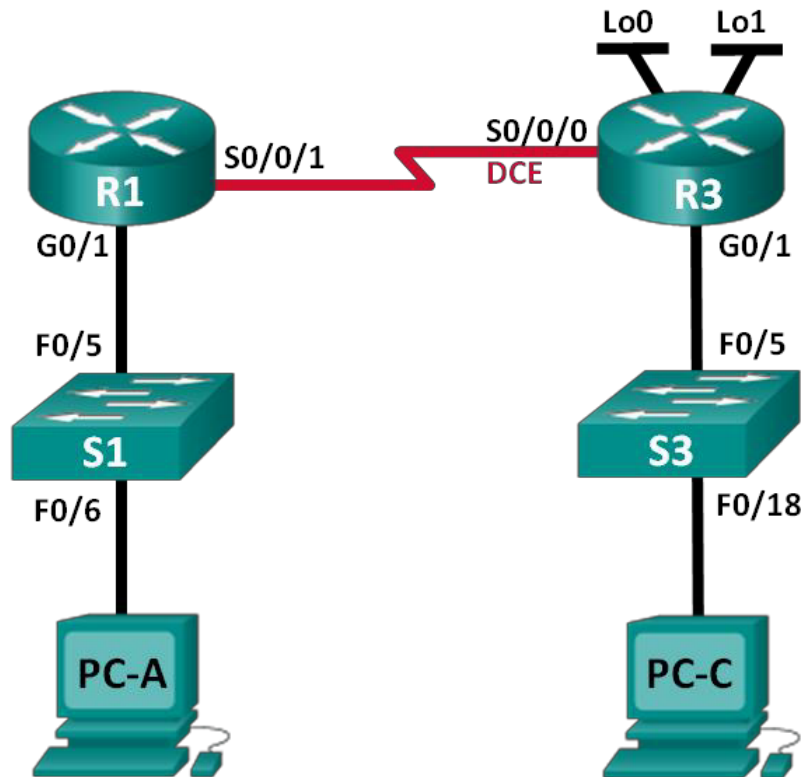
Use the space provided below to document the issues found during your troubleshooting and the configurations changes made to resolve those issues.

Reflection Question

This lab had you troubleshoot all devices before making any changes. Is there another way to apply the troubleshooting methodology?

Lab 13: Configuring IPv4 Static and Default Routes

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.

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: Initialise 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.

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

Step 3: Configure IP settings on the routers.

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

```
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.

- 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? _____ From PC-C, is it possible to ping the default gateway? _____
- Test connectivity by pinging between the directly connected routers.
From R1, is it possible to ping the S0/0/0 interface of R3? _____
If the answer is **no** to any of these questions, troubleshoot the configurations and correct the error.
- Test connectivity between devices that are not directly connected.
From PC-A, is it possible to ping PC-C? _____ From PC-A, is it possible to ping Lo0? ____ From PC-A, is it possible to ping Lo1? _____
Were these pings successful? Why or why not?

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

Step 5: Gather information.

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

How many interfaces are activated on R1? _____

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

How many interfaces are activated on R3? _____

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

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

- d. View the routing table information for R3.

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

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

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
```

- a. 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.

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

How is this new route listed in the routing table?

From host PC-A, is it possible to ping the host PC-C?

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
```

- 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.

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

How is this new route listed in the routing table?

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

- 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.

- 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.

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

How is this new route listed in the routing table?

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

Step 4: Remove static routes for loopback addresses.

- 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.

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

How many network routes are listed in the routing table on R1? _____ Is the Gateway of last resort set? _____

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:

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

- 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.

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

How is this new route listed in the routing table?

What is the Gateway of last resort?

- From host PC-A, is it possible to ping the 209.165.200.225? _____
- From host PC-A, is it possible to ping the 198.133.219.1? _____ These pings should be successful.

Reflection

- 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?

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

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

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.

```
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
```

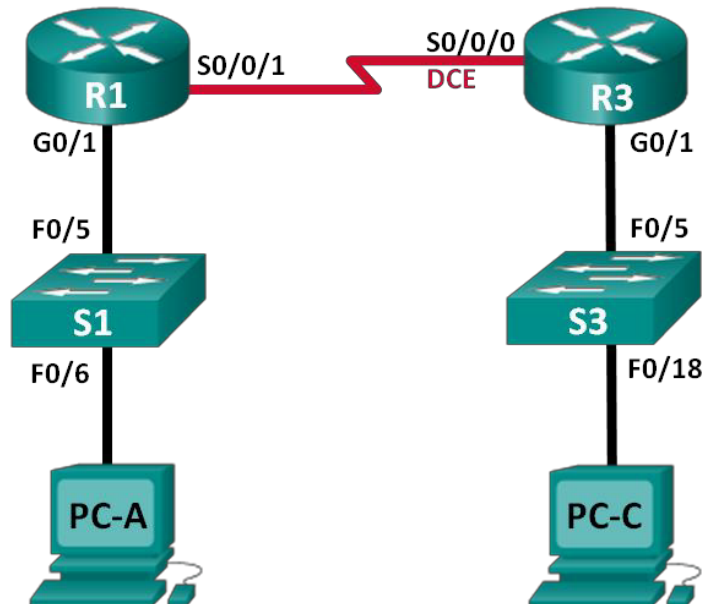
```
Or R1(config)# no ip route 209.165.200.224 255.255.255.224
```

Default Route Configuration

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

Lab 14: Configuring IPv6 Static and Default Routes

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.

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.

- Using Tera Term, console into the router labeled R1 in the topology diagram and assign the router the name R1.
- Within global configuration mode, enable IPv6 routing on R1.

```
R1(config)# ipv6 unicast-routing
```

- 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
```

```
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 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?

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

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

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

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

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

f. Repeat Step 5a from PC-C.

Did PC-C receive IPv6 addressing information from R3? _____

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

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

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

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?

Step 6: Use show commands to verify IPv6 settings.

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

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

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

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

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

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

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

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

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

-
- 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.

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

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:

```
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.

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

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

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.

Was the ping successful? Why?

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>
```

- a. 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
```

- b. 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
```

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

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

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

Was the ping successful? _____

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

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

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

Was the ping successful? _____

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

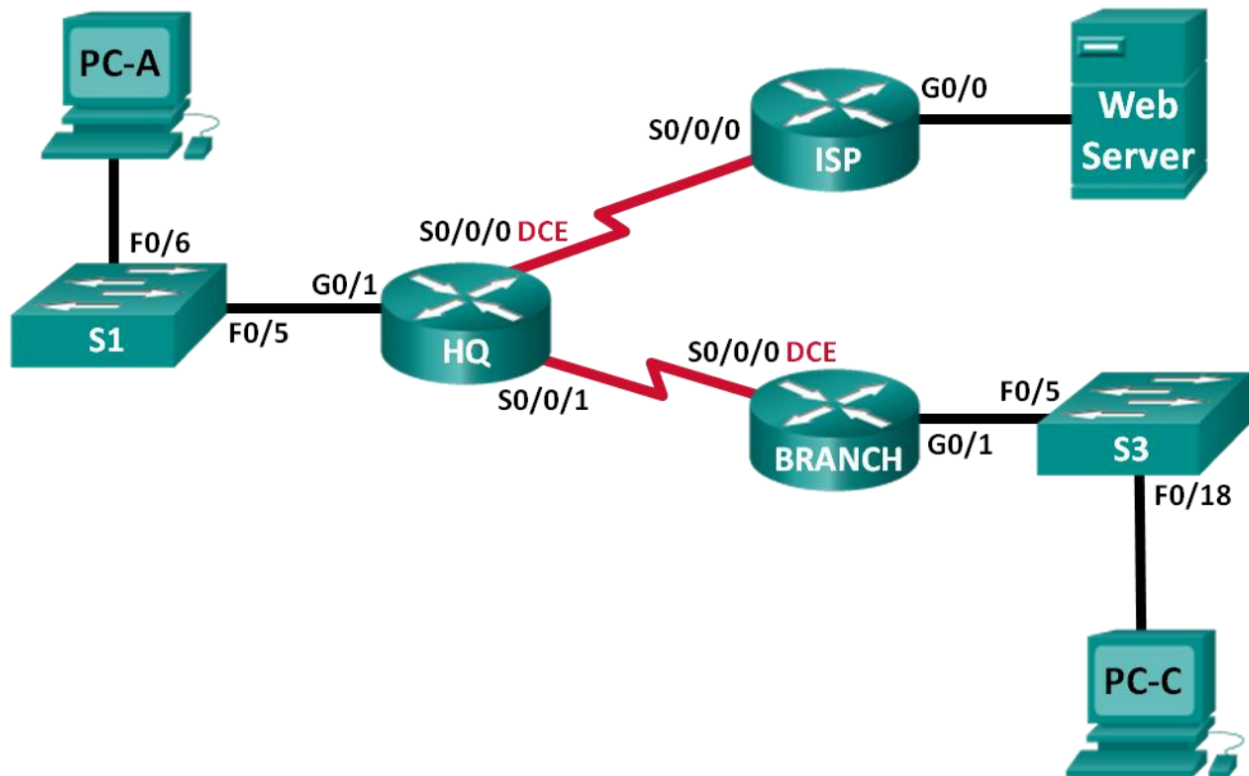
Reflection

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?

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?

Lab 15: Troubleshooting 1Pv4 and 1Pv6 Static Routes

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::1/30	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::/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.

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.

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.

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

Step 4: Configure hosts and Web Server.

- Configure IP addresses for IPv4 and IPv6.
- 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
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
  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
ipv6 route 2001:DB8:ACAD:1::/64 2001:DB8:ACAD:2::2
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 ipv6
  address FE80::1 link-local
  no
  shutdown
interface Serial0/0/0
  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
ipv6 route 2001:DB8:ACAD::/62 2001:DB8:ACAD:20::2

```

Router BRANCH

```

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
  clock rate
  128000 no
  shutdown
ip route 0.0.0.0 0.0.0.0
10.1.1.2 ipv6 route ::/0
2001:DB8:ACAD::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.

- b. Ping from HQ router to BRANCH router (192.168.0.254). Were the pings successful? _____
- c. Ping from HQ router to ISP router (10.1.1.1). Were the pings successful? _____
- d. Ping from PC-A to the default gateway. Were the pings successful? _____
- e. Ping from PC-A to PC-C. Were the pings successful? _____
- f. Ping from PC-A to Web Server. Were the pings successful? _____
- g. Display the routing table on HQ. What non-directly connected routes are shown in the routing table?

- 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?

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

- 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.

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.

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

- b. Ping from the ISP router to the HQ router (10.1.1.2). Were the pings successful? _____
- c. Ping from Web Server to the default gateway. Were the pings successful? _____
- d. Ping from Web Server to PC-A. Were the pings successful? _____
- e. Ping from Web Server to PC-C. Were the pings successful? _____

- f. Display the routing table on ISP. What non-directly connected routes are shown in the routing table?

- 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?

- 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.)

- 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.

Step 3: Troubleshoot the BRANCH router.

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

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

- b. Ping from the BRANCH router to the HQ router (192.168.0.253). Were the pings successful? _____

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

- d. Ping from PC-C to PC-A. Were the pings successful? _____

- e. Ping from PC-C to Web Server. Were the pings successful? _____

- f. Display the routing table on BRANCH. What non-directly connected routes are shown in the routing table?

- 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?

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

-
- 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.
-

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.

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

- b. Ping from the HQ router to the BRANCH router (2001:DB8:ACAD:2::2). Were the pings successful? ____ c.
Ping from the HQ router to the ISP router (2001:DB8:ACAD:20::1). Were the pings successful? ____ d.
Ping from PC-A to the default gateway. Were the pings successful?
e. Ping from PC-A to Web Server. Were the pings successful?
f. Ping from PC-A to PC-C. Were the pings successful?
g. Display the routing table by issuing a **show ipv6 route** command. What non-directly connected routes are shown in the routing table?
-

- 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?

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

- 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.

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.

- b. Ping from the ISP router to the HQ router (2001:DB8:ACAD:20::2). Were the pings successful?

- c. Ping from Web Server to the default gateway. Were the pings successful? _____

- d. Ping from Web Server to PC-A. Were the pings successful? _____

- e. Ping from Web Server to PC-C. Were the pings successful? _____

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

- 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?

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

- 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.

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.

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

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

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

- e. Ping from PC-C to PC-A. Were the pings successful?

- f. Ping from PC-C to Web Server. Were the pings successful?

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

- 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?

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

- 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 16 - Secure Network Devices

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/1	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: Configure the Router for SSH Access

Part 3: Configure the Switch for SSH Access

Part 4: SSH from the CLI on the Switch

Background / Scenario

In the past, Telnet was the most common network protocol used to remotely configure network devices. Telnet does not encrypt the information between the client and server. This allows a network sniffer to intercept passwords and configuration information.

Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals. SSH is most often used to log in to a remote device and execute commands. However, it can also transfer files using the associated Secure FTP (SFTP) or Secure Copy (SCP) protocols.

The network devices that are communicating must be configured to support SSH in order for SSH to function. In this lab, you will enable the SSH server on a router and then connect to that router using a PC with an SSH client installed. On a local network, the connection is normally made using Ethernet and IP.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(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 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.

Required Resources

- 1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 1 PC (Windows with a 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

Instructions

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.

Step 2: Initialize and reload the router and switch.

Step 3: Configure the router.

- Console into the router and enable privileged EXEC mode.
- Enter configuration mode.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the VTY password and enable login.
- Encrypt the plaintext passwords.
- Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.
- Configure and activate the G0/0/1 interface on the router using the information contained in the Addressing Table.
- Save the running configuration to the startup configuration file.

Step 4: Configure PC-A.

- Configure PC-A with an IP address and subnet mask.
- Configure a default gateway for PC-A.

Step 5: Verify network connectivity.

Ping R1 from PC-A. If the ping fails, troubleshoot the connection.

Part 2: Configure the Router for SSH Access

Using Telnet to connect to a network device is a security risk because all the information is transmitted in a clear text format. SSH encrypts the session data and provides device authentication, which is why SSH is recommended for remote connections. In Part 2, you will configure the router to accept SSH connections over the VTY lines.

Step 1: Configure device authentication.

The device name and domain are used as part of the crypto key when it is generated. Therefore, these names must be entered prior to issuing the **crypto key** command.

- a. Configure device name.
- b. Configure the domain for the device.

Step 2: Configure the encryption key method.

Step 3: Configure a local database username.

Configure a username using **admin** as the username and **Adm1nP@55** as the password.

Step 4: Enable SSH on the VTY lines.

- a. Enable Telnet and SSH on the inbound VTY lines using the **transport input** command.
- b. Change the login method to use the local database for user verification.

Step 5: Save the running configuration to the startup configuration file.

Step 6: Establish an SSH connection to the router.

- a. Start Tera Term from PC-A.
- b. Establish an SSH session to R1. Use the username **admin** and password **Adm1nP@55**. You should be able to establish an SSH session with R1.

Part 3: Configure the Switch for SSH Access

In Part 3, you will configure the switch to accept SSH connections. After the switch has been configured, establish an SSH session using Tera Term.

Step 1: Configure the basic settings on the switch.

- a. Console into the switch and enable privileged EXEC mode.
- b. Enter configuration mode.
- c. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- d. Assign **class** as the privileged EXEC encrypted password.
- e. Assign **cisco** as the console password and enable login.
- f. Assign **cisco** as the VTY password and enable login.
- g. Encrypt the plain text passwords.
- h. Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.
- i. Configure and activate the VLAN 1 interface on the switch according to the Addressing Table.
- j. Save the running configuration to the startup configuration file.

Step 2: Configure the switch for SSH connectivity.

Use the same commands that you used to configure SSH on the router in Part 2 to configure SSH for the switch.

- Configure the device name as listed in the Addressing Table.
- Configure the domain for the device.
- Configure the encryption key method.
- Configure a local database username.
- Enable Telnet and SSH on the VTY lines.
- Change the login method to use the local database for user verification.

Step 3: Establish an SSH connection to the switch.

Start Tera Term from PC-A, and then SSH to the SVI interface on S1.

Are you able to establish an SSH session with the switch?

Part 4: SSH From the CLI on the Switch

The SSH client is built into the Cisco IOS and can be run from the CLI. In Part 4, you will SSH to the router from the CLI on the switch.

Step 1: View the parameters available for the Cisco IOS SSH client.

Use the question mark (?) to display the parameter options available with the **ssh** command.

```
S1# ssh ?
  -c      Select encryption algorithm
  -l      Log in using this user name
  -m      Select HMAC algorithm
  -o      Specify options
  -p      Connect to this port
  -v      Specify SSH Protocol Version
  -vrf    Specify vrf name
  WORD    IP address or hostname of a remote system
```

Step 2: SSH to R1 from S1.

- You must use the **-l admin** option when you SSH to R1. This allows you to log in as user **admin**. When prompted, enter **Adm1nP@55** for the password.

```
S1# ssh -l admin 192.168.1.1
Password:
Authorized Users Only!
R1>
```

- You can return to S1 without closing the SSH session to R1 by pressing **Ctrl+Shift+6**. Release the **Ctrl+Shift+6** keys and press **x**. The switch privileged EXEC prompt displays.

```
R1>
S1#
```

- To return to the SSH session on R1, press Enter on a blank CLI line. You may need to press Enter a second time to see the router CLI prompt.

```
S1#
```

```
[Resuming connection 1 to 192.168.1.1 ... ]
```

```
R1>
```

- d. To end the SSH session on R1, type **exit** at the router prompt.

```
R1# exit
```

```
[Connection to 192.168.1.1 closed by foreign host]
```

```
S1#
```

What versions of SSH are supported from the CLI?

Reflection Question

How would you provide multiple users, each with their own username, access to a network device?

Lab 17 - Configure Network Devices with SSH

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0/1	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: Configure the Router for SSH Access

Part 3: Configure the Switch for SSH Access

Part 4: SSH from the CLI on the Switch

Background / Scenario

In the past, Telnet was the most common network protocol used to remotely configure network devices. Telnet does not encrypt the information between the client and server. This allows a network sniffer to intercept passwords and configuration information.

Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals. SSH is most often used to log in to a remote device and execute commands. However, it can also transfer files using the associated Secure FTP (SFTP) or Secure Copy (SCP) protocols.

The network devices that are communicating must be configured to support SSH in order for SSH to function. In this lab, you will enable the SSH server on a router and then connect to that router using a PC with an SSH client installed. On a local network, the connection is normally made using Ethernet and IP.

Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.4 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.2(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 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.

Required Resources

- 1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.4 universal image or comparable)

- 1 Switch (Cisco 2960 with Cisco IOS Release 15.2(2) lanbasek9 image or comparable)
- 1 PC (Windows with a 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

Instructions

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.

Step 2: Initialize and reload the router and switch.

Step 3: Configure the router.

- Console into the router and enable privileged EXEC mode.
- Enter configuration mode.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the VTY password and enable login.
- Encrypt the plaintext passwords.
- Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.
- Configure and activate the G0/0/1 interface on the router using the information contained in the Addressing Table.
- Save the running configuration to the startup configuration file.

Step 4: Configure PC-A.

- Configure PC-A with an IP address and subnet mask.
- Configure a default gateway for PC-A.

Step 5: Verify network connectivity.

Ping R1 from PC-A. If the ping fails, troubleshoot the connection.

Part 2: Configure the Router for SSH Access

Using Telnet to connect to a network device is a security risk because all the information is transmitted in a clear text format. SSH encrypts the session data and provides device authentication, which is why SSH is recommended for remote connections. In Part 2, you will configure the router to accept SSH connections over the VTY lines.

Step 1: Configure device authentication.

The device name and domain are used as part of the crypto key when it is generated. Therefore, these names must be entered prior to issuing the **crypto key** command.

- a. Configure device name.
- b. Configure the domain for the device.

Step 2: Configure the encryption key method.

Step 3: Configure a local database username.

Configure a username using **admin** as the username and **Adm1nP@55** as the password.

Step 4: Enable SSH on the VTY lines.

- a. Enable Telnet and SSH on the inbound VTY lines using the **transport input** command.
- b. Change the login method to use the local database for user verification.

Step 5: Save the running configuration to the startup configuration file.

Step 6: Establish an SSH connection to the router.

- a. Start Tera Term from PC-A.
- b. Establish an SSH session to R1. Use the username **admin** and password **Adm1nP@55**. You should be able to establish an SSH session with R1.

Part 3: Configure the Switch for SSH Access

In Part 3, you will configure the switch to accept SSH connections. After the switch has been configured, establish an SSH session using Tera Term.

Step 1: Configure the basic settings on the switch.

- a. Console into the switch and enable privileged EXEC mode.
- b. Enter configuration mode.
- c. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- d. Assign **class** as the privileged EXEC encrypted password.
- e. Assign **cisco** as the console password and enable login.
- f. Assign **cisco** as the VTY password and enable login.
- g. Encrypt the plain text passwords.
- h. Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.
- i. Configure and activate the VLAN 1 interface on the switch according to the Addressing Table.
- j. Save the running configuration to the startup configuration file.

Step 2: Configure the switch for SSH connectivity.

Use the same commands that you used to configure SSH on the router in Part 2 to configure SSH for the switch.

- Configure the device name as listed in the Addressing Table.
- Configure the domain for the device.
- Configure the encryption key method.
- Configure a local database username.
- Enable Telnet and SSH on the VTY lines.
- Change the login method to use the local database for user verification.

Step 3: Establish an SSH connection to the switch.

Start Tera Term from PC-A, and then SSH to the SVI interface on S1.

Are you able to establish an SSH session with the switch?

Part 4: SSH From the CLI on the Switch

The SSH client is built into the Cisco IOS and can be run from the CLI. In Part 4, you will SSH to the router from the CLI on the switch.

Step 1: View the parameters available for the Cisco IOS SSH client.

Use the question mark (?) to display the parameter options available with the **ssh** command.

```
S1# ssh ?
  -c      Select encryption algorithm
  -l      Log in using this user name
  -m      Select HMAC algorithm
  -o      Specify options
  -p      Connect to this port
  -v      Specify SSH Protocol Version
  -vrf    Specify vrf name
  WORD    IP address or hostname of a remote system
```

Step 2: SSH to R1 from S1.

- You must use the **-l admin** option when you SSH to R1. This allows you to log in as user **admin**. When prompted, enter **Adm1nP@55** for the password.

```
S1# ssh -l admin 192.168.1.1
Password:
Authorized Users Only!
R1>
```

- You can return to S1 without closing the SSH session to R1 by pressing **Ctrl+Shift+6**. Release the **Ctrl+Shift+6** keys and press **x**. The switch privileged EXEC prompt displays.

```
R1>
S1#
```

- To return to the SSH session on R1, press Enter on a blank CLI line. You may need to press Enter a second time to see the router CLI prompt.

```
S1#
```

```
[Resuming connection 1 to 192.168.1.1 ... ]
```

```
R1>
```

- d. To end the SSH session on R1, type **exit** at the router prompt.

```
R1# exit
```

```
[Connection to 192.168.1.1 closed by foreign host]
```

```
S1#
```

What versions of SSH are supported from the CLI?

Reflection Question

How would you provide multiple users, each with their own username, access to a network device?

Lab 18: Configuring Switch Security Features 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.

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.

- Console into R1 and enter global configuration mode.
- 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.

- a. Console into S1 and enter global configuration mode.
- b. 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? _____
- f. Issue the **show ip interface brief** command on S1. What is the status and protocol for management interface VLAN 99?

Why is the protocol down, even though you issued the **no shutdown** command for interface 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? _____

Note: There may be a delay while the port states converge.

Step 4: Verify connectivity between devices.

- a. From PC-A, ping the default gateway address on R1. Were your pings successful? _____
- b. From PC-A, ping the management address of S1. Were your pings successful? _____
- c. From S1, ping the default gateway address on R1. Were your pings successful? _____
- d. 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?
- e. 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.

- a. Enable SSH on S1. From global configuration mode, create a domain name of **CCNA-Lab.com**.

```
S1(config)# ip domain-name CCNA-Lab.com
```

- b. 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
```

- c. 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
```

- 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
```

What version of SSH is the switch using? _____

How many authentication attempts does SSH allow? _____ What is the default timeout setting for SSH? _____

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
```

How many authentication attempts does SSH allow? _____

What is the timeout setting for SSH? _____ 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? _____ What prompt was displayed on S1?
Why?

- 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?

- 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?

- e. Issue the **show ip http server status** command.

What is the HTTP server status? _____ What server port is it using? _____
What is the HTTP secure server status? _____ What secure server port is it
using? _____

- 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?

-
- 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?
-
- 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?

-
- 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: _____ F0/6 MAC
address: _____

- 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.

- 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?

-
- 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
```

- 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?

-
- j. On the switch, verify port security with the following commands.

```
S1# show port-security
```

```
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
              (Count)          (Count)          (Count)
-----
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**

```
Secure Mac Address
Table
-----
-- Vlan  Mac Address      Type                Ports      Remaining
Age                                           (mins)
-----
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? _____
- m. On the switch, issue the **show interface f0/5** command to determine the cause of ping failure. Record your findings.

-
- 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.

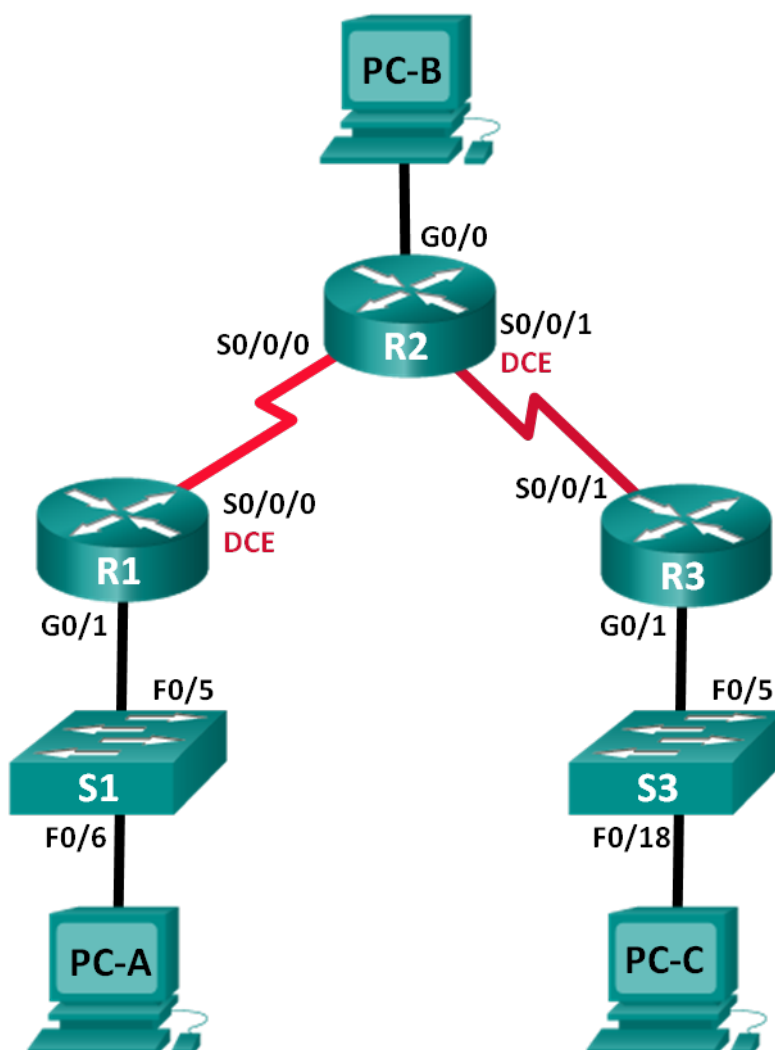
Reflection

1. Why would you enable port security on a switch?

-
2. Why should unused ports on a switch be disabled?
-

Lab 19: Configuring Basic RIPv2

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
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.30.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A

S1	N/A	VLAN 1	N/A	N/A
S3	N/A	VLAN 1	N/A	N/A
PC-A	NIC	172.30.10.3	255.255.255.0	172.30.10.1
PC-B	NIC	209.165.201.2	255.255.255.0	209.165.201.1
PC-C	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.

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 2: 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 3: 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.

- a. 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.

- b. Configure RIPv2 on R3 and use the **network** statement to add the appropriate connected networks and prevent routing updates on the LAN interface.
- c. 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.

- a. 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

- b. Check connectivity between PCs.

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

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

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

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

- 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?

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

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

d. Examine the automatic summarization of routes.

The LANs connected to R1 and R3 are composed of discontinuous 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.

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.

- 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

```

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

```

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

```

- 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
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?

Are the subnet masks included in the routing updates? _____

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?

- b. View the routing table on R2.

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

Step 6: Verify connectivity.

- Simulate sending traffic to the Internet by pinging from PC-A and PC-C to 209.165.201.2.
Were the pings successful? _____
- Verify that hosts within the subnetted network can reach each other by pinging between PC-A and PC-C.
Were the pings successful? _____

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

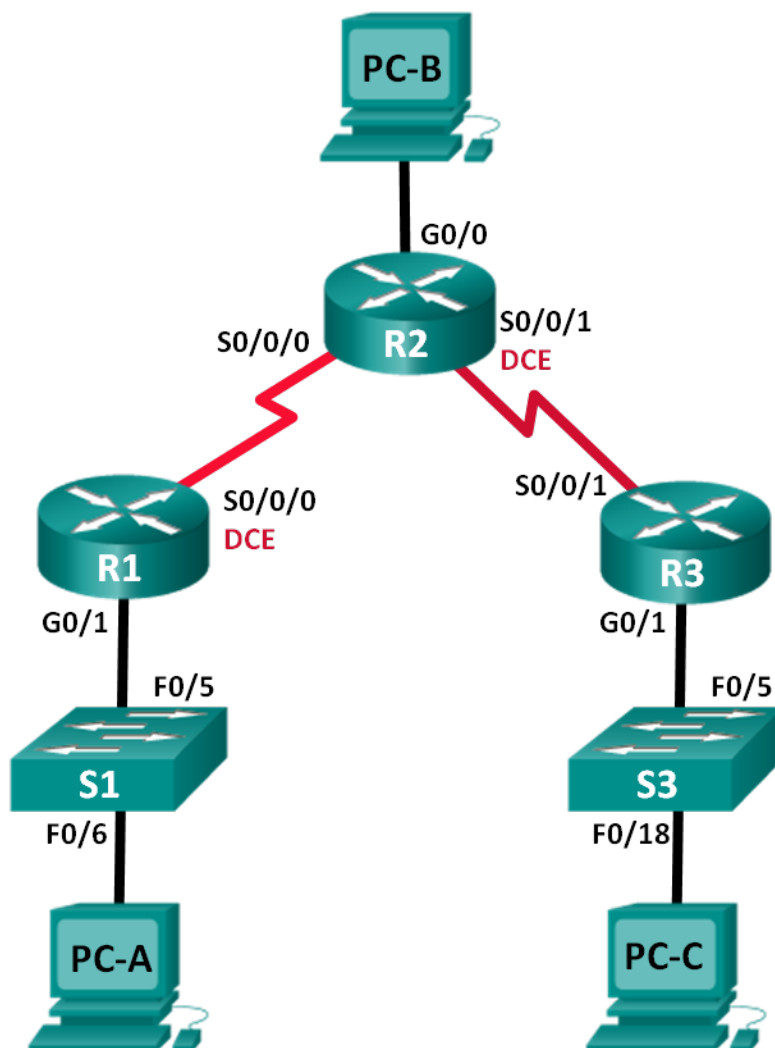
Reflection

- Why would you turn off automatic summarization for RIPv2?

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

Lab 20: Configuring Basic RIPv2 and RIPvng

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
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
R3	G0/1	172.30.30.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A

S1	N/A	VLAN 1	N/A	N/A
S3	N/A	VLAN 1	N/A	N/A
PC-A	NIC	172.30.10.3	255.255.255.0	172.30.10.1
PC-B	NIC	209.165.201.2	255.255.255.0	209.165.201.1
PC-C	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 and verify RIPv2 is running on routers.
- Configure a passive interface.
- Examine routing tables.
- Disable automatic summarization.
- Configure a default route.
- Verify end-to-end connectivity.

Part 3: Configure IPv6 on Devices

Part 4: Configure and Verify RIPvng Routing

- Configure and verify RIPvng is running on routers.
- Examine routing tables.
- 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.

RIPvng (RIP Next Generation) is a distance-vector routing protocol for routing IPv6 addresses, as defined by RFC 2080. RIPvng is based on RIPv2 and has the same administrative distance and 15-hop limitation.

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. You will then configure the network topology with IPv6 addresses, configure RIPvng, propagate a default route, and use CLI commands to display and verify RIPvng 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 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.

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 4: 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.

- Disable DNS lookup.
- Configure device names as shown in the topology.
- Configure password encryption.
- Assign **class** as the privileged EXEC password.
- Assign **cisco** as the console and vty passwords.
- Configure a MOTD banner to warn users that unauthorized access is prohibited.
- Configure **logging synchronous** for the console line.
- Configure the IP address listed in the Addressing Table for all interfaces.
- Configure a description to each interface with an IP address.
- Configure the clock rate if applicable to the DCE serial interface.
- 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.

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

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

Part 5: Configure and Verify RIPv2 Routing

In Part 2, you will configure RIPv2 routing on all routers in the network and then verify that 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.

- On R1, configure RIPv2 as the routing protocol and advertise the appropriate 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 appropriate networks and prevent routing updates on the LAN interface.
- Configure RIPv2 on R2. 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 current state of 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? _____

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

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

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

- 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?

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

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

d. Examine the automatic summarization of routes.

The LANs connected to R1 and R3 are composed of discontinuous 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 subnets for the 172.30.0.0 network. R1 does not have any routes for the 172.30.0.0 subnets 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 subnets for the 172.30.0.0 network. R3 does not have any routes for the 172.30.0.0 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.

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.

- 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
```

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

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

- Examine the routing tables. Remember will it 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
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 exam 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? _____

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

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 unknown destination address traffic to the R2 G0/0 toward PC-B, simulating the Internet by setting a Gateway of Last Resort on the R2 router.

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?

- b. View the routing table on R2.

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

Step 6: Verify connectivity.

- Simulate sending traffic to the Internet by pinging from PC-A and PC-C to 209.165.201.2.
Were the pings successful? _____
- Verify that hosts within the subnetted network can reach each other by pinging between PC-A and PC-C.
Were the pings successful? _____

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

Part 6: Configure IPv6 on Devices

In Part 3, you will configure all interfaces with IPv6 addresses and verify connectivity.

Addressing Table

Device	Interface	IPv6 Address / Prefix Length	Default Gateway
R1	G0/1	2001:DB8:ACAD:A::1/64 FE80::1 link-local	N/A
	S0/0/0	2001:DB8:ACAD:12::1/64 FE80::1 link-local	N/A
R2	G0/0	2001:DB8:ACAD:B::2/64 FE80::2 link-local	N/A
	S0/0/0	2001:DB8:ACAD:12::2/64 FE80::2 link-local	N/A

	S0/0/1	2001:DB8:ACAD:23::2/64 FE80::2 link-local	N/A
R3	G0/1	2001:DB8:ACAD:C::3/64 FE80::3 link-local	N/A
	S0/0/1	2001:DB8:ACAD:23::3/64 FE80::3 link-local	N/A
PC-A	NIC	2001:DB8:ACAD:A::A/64	FE80::1
PC-B	NIC	2001:DB8:ACAD:B::B/64	FE80::2
PC-C	NIC	2001:DB8:ACAD:C::C/64	FE80::3

Step 1: Configure PC hosts.

Refer to the Addressing Table for PC host address information.

Step 2: Configure IPv6 on routers.

Note: Assigning an IPv6 address in addition to an IPv4 address on an interface is known as dual stacking. This is because both IPv4 and IPv6 protocol stacks are active.

- For each router interface, assign the global and link local address from the Addressing Table.
 - Enable IPv6 routing on each router.
 - Enter the appropriate command to verify IPv6 addresses and link status. Write the command in the space below.
-
- Each workstation should be able to ping the attached router. Verify and troubleshoot if necessary.
 - The routers should be able to ping one another. Verify and troubleshoot if necessary.

Part 7: Configure and Verify RIPng Routing

In Part 4, you will configure RIPng routing on all routers, verify that routing tables are updated correctly, configure and distribute a default route, and verify end-to-end connectivity.

Step 1: Configure RIPng routing.

With IPv6, it is common to have multiple IPv6 addresses configured on an interface. The network statement has been eliminated in RIPng. RIPng routing is enabled at the interface level instead, and is identified by a locally significant process name as multiple processes can be created with RIPng.

- Issue the **ipv6 rip Test1 enable** command for each interface on R1 that is to participate in RIPng routing, where **Test1** is the locally significant process name.

```
R1(config)# interface g0/1
R1(config)# ipv6 rip Test1 enable
R1(config)# interface s0/0/0
R1(config)# ipv6 rip Test1 enable
```
- Configure RIPng for the serial interfaces on R2 with **Test2** as the process name. Do not configure for the G0/0 interface.
- Configure RIPng for each interface on R3 with **Test3** as the process name.

- d. Verify that RIPng is running on the routers.

The **show ipv6 protocols**, **show run**, **show ipv6 rip database**, and **show ipv6 rip process name** commands can all be used to confirm that RIPng is running. On R1, issue the **show ipv6 protocols** command.

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip Test1"
  Interfaces:
    Serial0/0/0
    GigabitEthernet0/1
  Redistribution:
    None
```

How is the RIPng listed in the output? _____

- e. Issue the **show ipv6 rip Test1** command.

```
R1# show ipv6 rip Test1
RIP process "Test1", port 521, multicast-group FF02::9, pid 314
  Administrative distance is 120. Maximum paths is 16
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 1, trigger updates 0
  Full Advertisement 0, Delayed Events 0
  Interfaces:
    GigabitEthernet0/1
    Serial0/0/0
  Redistribution:
    None
```

How are RIPv2 and RIPng similar?

- f. Inspect the IPv6 routing table on each router. Write the appropriate command used to view the routing table in the space below.
- _____

On R1, how many routes have been learned by RIPng? _____

On R2, how many routes have been learned by RIPng? _____

On R3, how many routes have been learned by RIPng? _____

- g. Check connectivity between PCs.

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

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

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

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

Why are some pings successful and others not?

Step 2: Configure and redistribute a default route.

- a. From R2, create a static default route to network ::0/64 using the **ipv6 route** command, and the IP address of exit interface G0/0. This forwards any unknown destination address traffic to the R2 G0/0 interface toward PC-Bs, simulating the Internet. Write the command used in the space below.
- b. Static routes can be included in RIPng updates by using the **ipv6 rip process name default-information originate** command in interface configuration mode. Configure the serial links on R2 to send the default route in RIPng updates.

```
R2(config)# int s0/0/0
R2(config-rtr)# ipv6 rip Test2 default-information originate
R2(config)# int s0/0/1
R2(config-rtr)# ipv6 rip Test2 default-information originate
```

Step 3: Verify the routing configuration.

- a. View the IPv6 routing table on R2.

```
R2# show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       D - EIGRP, EX - EIGRP external
S    ::/64 [1/0]
    via 2001:DB8:ACAD:B::B
R    2001:DB8:ACAD:A::/64 [120/2]
    via FE80::1, Serial0/0/0
C    2001:DB8:ACAD:B::/64 [0/0]
    via ::, GigabitEthernet0/1
L    2001:DB8:ACAD:B::2/128 [0/0]
    via ::, GigabitEthernet0/1
R    2001:DB8:ACAD:C::/64 [120/2]
    via FE80::3, Serial0/0/1
C    2001:DB8:ACAD:12::/64 [0/0]
    via ::, Serial0/0/0
L    2001:DB8:ACAD:12::2/128 [0/0]
    via ::, Serial0/0/0
C    2001:DB8:ACAD:23::/64 [0/0]
    via ::, Serial0/0/1
L    2001:DB8:ACAD:23::2/128 [0/0]
    via ::, Serial0/0/1
L    FF00::/8 [0/0]
    via ::, Null0
```

How can you tell from the routing table that R2 has a pathway for Internet traffic?

- b. View the routing tables on R1 and R3.

How is the pathway for Internet traffic provided in their routing tables?

Step 4: Verify connectivity.

Simulate sending traffic to the Internet by pinging from PC-A and PC-C to 2001:DB8:ACAD:B::B/64.

Were the pings successful? _____

Reflection

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

2. In both scenarios, how did R1 and R3 learn the pathway to the Internet?

3. How are configuring RIPv2 and RIPv6 different?

Appendix: Configure and Verify Password Recovery

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 8: 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.

- Console into the router and enter global configuration mode.
- 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.EuL28kPTzxMLFiyML15/
  
```

```
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 9: 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
showmon       display currently selected ROM monitor
stack         produce a stack trace
sync          write monitor environment to NVRAM
```

Note: The number at the end of the ROMMON prompt will increment by one each time a command is entered.

- ```
rommon 3 >
```

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 10: 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)
```

```
R1#
```

- b. Enter global configuration mode.
- c. Reset the enable secret password to **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 11: 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?

---



---



---