Packet Tracer - Basic Router Configuration Review

Addressing Table

Device	Interface	IP Address / Prefix	Default Gateway
R2	G0/0/0	10.0.4.1 /24	N/A
		2001:db8:acad:4::1 /64	
		fe80::2:a	
	G0/0/1	10.0.5.1 /24	
		2001:db8:acad:5::1 /64	
		fe80::2:b	
	S0/1/0	10.0.3.2 /24	
		2001:db8:acad:3::2 /64	
		fe80::1:c	
	S0/1/1	209.165.200.225 /30	
		2001:db8:feed:224::1/64	
		fe80::1:d	
PC1	NIC	10.0.1.10 /24	10.0.1.1
		2001:db8:acad:1::10 /64	fe80::1:a
PC2	NIC	10.0.2.10 /24	10.0.2.1
		2001:db8:acad:2::10 /64	fe80::1:b
PC3	NIC	10.0.4.10 /24	10.0.4.1
		2001:db8:acad:4::10 /64	fe80::2:a
PC4	NIC	10.0.5.10 /24	10.0.5.1
		2001:db8:acad:5::10 /64	fe80::2:b

Objectives

Part 1: Configure Devices and Verify Connectivity

- Assign static IPv4 and IPv6 addresses to the PC interfaces.
- Configure basic router settings.
- Configure the router for SSH.
- Verify network connectivity.

Part 2: Display Router Information

- Retrieve hardware and software information from the router.
- Interpret the startup configuration.

- Interpret the routing table.
- Verify the status of the interfaces.

Background / Scenario

This activity requires you to configure the **R2** router using the settings from the Addressing Table and the specifications listed. The **R1** router and the devices connected to it have been configured. This is a comprehensive review of previously covered IOS router commands. In Part 1, you will complete basic configurations and interface settings on the router. In Part 2, you will use SSH to connect to the router remotely and utilize the IOS commands to retrieve information from the device to answer questions about the router. For review purposes, this lab provides the commands necessary for specific router configurations.

Instructions

Part 1: Configure Devices and Verify Connectivity

Step 1: Configure the PC interfaces.

a. Configure the IPv4 and IPv6 addresses on PC3 as listed in the Addressing Table.

b. Configure the IPv4 and IPv6 addresses on PC4 as listed in the Addressing Table.

Step 2: Configure the router.

a. On the **R2** router, open a terminal. Move to privileged EXEC mode.

b. Enter configuration mode.

c. Assign a device name of **R2** to the router.

d. Configure **c1sco1234** as the encrypted privileged EXEC mode password.

e. Set the domain name of the router to **ccna-lab.com**.

f. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.

g. Encrypt the plaintext passwords.

h. Configure the username **SSHadmin** with an encrypted password of **55Hadm!n**.

i. Generate a set of crypto keys with a 1024 bit modulus.

j. Assign **cisco** as the console password, configure sessions to disconnect after six minutes of inactivity, and enable login. To prevent console messages from interrupting commands, use the **logging synchronous** command.

k. Assign **cisco** as the vty password, configure the vty lines to accept SSH connections only, configure sessions to disconnect after six minutes of inactivity, and enable login using the local database.

l. Create a banner that warns anyone accessing the device that unauthorized access is prohibited. NOTE: The banner motd must include the word WARNING to score correctly.

m. Enable IPv6 Routing.

n. Configure all four interfaces on the router with the IPv4 and IPv6 addressing information from the addressing table above. Configure all four interfaces with descriptions. Activate all four interfaces.

o. Save the running configuration to the startup configuration file.

Step 3: Verify network connectivity.

a. Using the command line at **PC3**, ping the IPv4 and IPv6 addresses for **PC4**.

Were the pings successful?

b. From the CLI on **R2** ping the S0/1/1 address of **R1** for both IPv4 and IPv6. The addresses assigned to the S0/1/1 interface on R1 are:

IPv4 address = 10.0.3.1

IPv6 address = 2001:db8:acad:3::1

Were the pings successful?

From the command line of **PC3** ping the ISP address 209.165.200.226.

Were the pings successful?

From **PC3** attempt to ping an address on the ISP for testing, 64.100.1.1.

Were the pings successful?

c. From the command line of **PC3** open an SSH session to the R2 G0/0/0 IPv4 address and log in as **SSHadmin** with the password **55Hadm!n.**

```
C:\> ssh -l SSHadmin 10.0.4.1
```

```
Password:
```

Was remote access successful?

Part 2: Display Router Information

In Part 2, you will use **show** commands from an SSH session to retrieve information from the router.

Step 1: Establish an SSH session to R2.

From the command line of PC3 open an SSH session to the **R2** G0/0/0 IPv6 address and log in as **SSHadmin** with the password **55Hadm!n**.

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 running configuration.

a.   Use the **show running-config** command on the router to answer the following questions filtering for lines containing the word "password".

How are passwords presented in the output?

b.   Use the show running-config | begin vty command.

What is the result of using this command?

Note: A more specific command would be **show running-config | section vty**; however, the current version of Packet Tracer does not support the **section** filtering 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.

a.   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?

What filtering command would you use to display only the interfaces with addresses assigned?

b.   Use the **show ipv6 int brief** command to verify IPv6 settings on R2.

What is the meaning of the [up/up] part of the output?