Packet Tracer - Basic Router Configuration Review (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

14.3.5 Packet Tracer – Basic Router Configuration Review

Answer 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.

```
router> enable
```

b. Enter configuration mode.

```
router# configure terminal
```

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

```
router(config)# hostname R2
```

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

```
R2(config)#enable secret c1sco1234
```

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

```
R2(config)# ip domain-name ccna-lab.com
```

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

```
R2(config)# no ip domain lookup
```

g. Encrypt the plaintext passwords.

```
R2(config)# service password-encryption
```

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

```
R2(config)# username SSHadmin secret 55Hadm!n
```

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

```
R2(config)# crypto key generate rsa
```

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.

```
R2(config)# line console 0
R2(config-line)# password cisco
R2(config-line)# logging synchronous
R2(config-line)# exec-timeout 6 0
R2(config-line)# login
```

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.

```
R2(config)# line vty 0 4
R2(config-line)# password cisco
R2(config-line)# exec-timeout 6 0
R2(config-line)# transport input ssh
R2(config-line)# login local
```

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

```
R2(config)# banner motd $ WARNING Authorized Users Only! $
```

m. Enable IPv6 Routing.

```
R2(config)# ipv6 unicast-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.

```
R2(config)# interface g0/0/0
R2(config-if)# description Connection to S3
R2(config-if)# ip address 10.0.4.1 255.255.255.0
R2(config-if)# ipv6 address fe80::2:a link-local
R2(config-if)# ipv6 address 2001:db8:acad:4::1/64
R2(config-if)# no shutdown
R2(config)# interface g0/0/1
R2(config-if)# description Connection to S4
R2(config-if)# ip address 10.0.5.1 255.255.255.0
R2(config-if)# ipv6 address fe80::2:b link-local
R2(config-if)# ipv6 address 2001:db8:acad:5::1/64
R2(config-if)# no shutdown
R2(config)# interface s0/1/0
R2(config-if)# description Link to R1
R2(config-if)# ip address 10.0.3.2 255.255.255.0
R2(config-if)# ipv6 address fe80::1:c link-local
R2(config-if)# ipv6 address 2001:db8:acad:3::2/64
R2(config-if)# no shutdown
R2(config-if)# interface s0/1/1
R2(config-if)# description Link to Internet
R2(config-if)# ip address 209.165.200.225 255.255.255.252
```

```
R2(config-if)# ipv6 address fe80::1:d link-local
```

```
R2(config-if)# ipv6 address 2001:db8:feed:224::1/64
R2(config-if)# no shutdown
```

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

```
R2# copy running-config startup-config
```

Step 3: Verify network connectivity.

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

Were the pings successful?

YES.

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?

YES.

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

Were the pings successful?

Yes, the traffic is being forwarded by the PC via the default gateway router.

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

Were the pings successful?

No, the router's routing has not been configured, so only locally connected networks are accessible. R2's default route is not configured.

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?

YES.