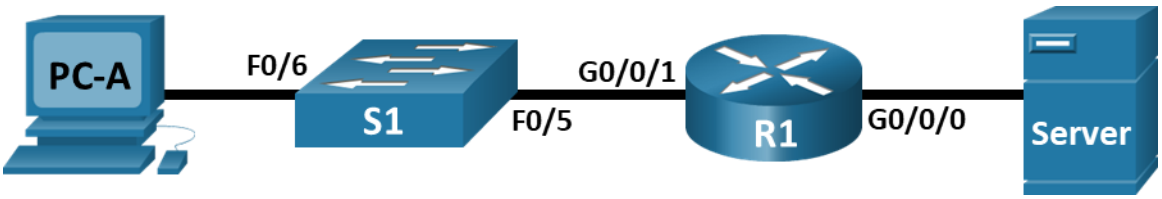
DIN DAHANAYKE
D/BIS/20/0011

Packet Tracer - Configure Basic Router Settings - Physical Mode

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	
		2001:db8:acad:1::1 /64	
		fe80::1	
	Loopback0	10.0.0.1 /24	
		2001:db8:acad:2::1 /64	
		fe80::1	
PC-A	NIC	192.168.1.10 /24	192.168.1.1
		2001:db8:acad:1::10 /64	fe80::1
Server	NIC	192.168.0.10 /24	192.168.0.1
		2001:db8:acad::10 /64	fe80::1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Devices and Verify Connectivity

Part 3: Display Router Information

Background / Scenario

This is a comprehensive Packet Tracer Physical Mode (PTPM) activity to review previously covered IOS router commands. In Parts 1 and 2, you will cable the equipment and complete basic configurations and interface settings on the router.

In Part 3, you will use SSH to connect to the router remotely and use the IOS commands to retrieve information from the device to answer questions about the router.

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

Instructions

Part 1: Set Up the Topology and Initialize Devices

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

a. Click and drag the **Cisco 4321 ISR**, the **Cisco 2960 Switch**, and the **Server** from the **Shelf** to the **Rack**.

b. Click and drag the **PC** from the **Shelf** to the **Table**.

c. Cable the devices as specified in the topology diagram. Use **Copper Straight-through** cables for network connections.

d. From the **PC**, connect a **Console Cable** to the **Cisco 4321 ISR**.

e. Power on the **Cisco 4321 ISR**, **PC-A**, and **Server**. The power button for **Server** is on the bottom right. The 2960 switch should power on automatically.

Part 2: Configure Devices and Verify Connectivity

Step 1: Configure the PC interfaces.

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

b. Configure the IP address, subnet mask, and default gateway settings on **Server**.

Step 2: Configure the router.

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

Router>en

b. Enter configuration mode.
Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

c. Assign a device name to the router.

Router(config)#hostname R1

d. Set the router's domain name as ccna-lab.com.

R1(config)#ip domain-name ccna-lab.com

e. Encrypt the plaintext passwords.

R1(config)#service password-encryption

f. Configure the system to require a minimum 12-character password.

R1(config)#security password min-length 12

g. Configure the username **SSHadmin** with an encrypted password of **55Hadm!n2020**.

```
R1(config)#username SSHadmin secret 55Hadm!n2020
```

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

```
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar 1 0:33:21.606: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

i. Assign **$cisco!PRIV*** as the privileged EXEC password.

```
R1(config)#enable secret $cisco!PRIV*
```

j. Assign **$cisco!!CON*** as the console password. Configure sessions to disconnect after four minutes of inactivity, and enable login.

```
R1(config)#line console 0

R1(config-line)#password $cisco!!CON*
R1(config-line)#exec-timeout 4 0
R1(config-line)#login
R1(config-line)#exit
```

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

```
R1(config)#line vty 0 15
R1(config-line)#password $cisco!!VTY*
R1(config-line)#transport input ssh
R1(config-line)#exec-timeout 4 0
R1(config-line)#login local
R1(config-line)#exit

R1(config)#
```

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

```
R1(config)#banner motd @Unauthorized Access is Prohibited@
```

m. Enable IPv6 routing.

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

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

```
R1(config)#interface g0/0/0
R1(config-if)#description connection to server
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#ipv6 address 2001:db8:acad::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to
up

R1(config-if)#interface g0/0/1
R1(config-if)#description connection to switch
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to
up

R1(config-if)#int loopback 0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

R1(config-if)#description loopback
R1(config-if)#ip address 10.0.0.1 255.255.255.0
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
```

```
R1(config)#
```

The router should not allow vty logins for two minutes if three failed login attempts occur within 60 seconds.

```
R1(config)#login block-for 120 attempts 3 within 60
```

o. Set the clock on the router.

```
R1#clock set ?
hh:mm:ss Current Time
R1#clock set 12:37:00 ?
<1-31> Day of the month
MONTH Month of the year
R1#clock set 08:20:00 19 ?
MONTH Month of the year
R1#clock set 08:20:00 19 February 2022
R1#
```

p. 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?

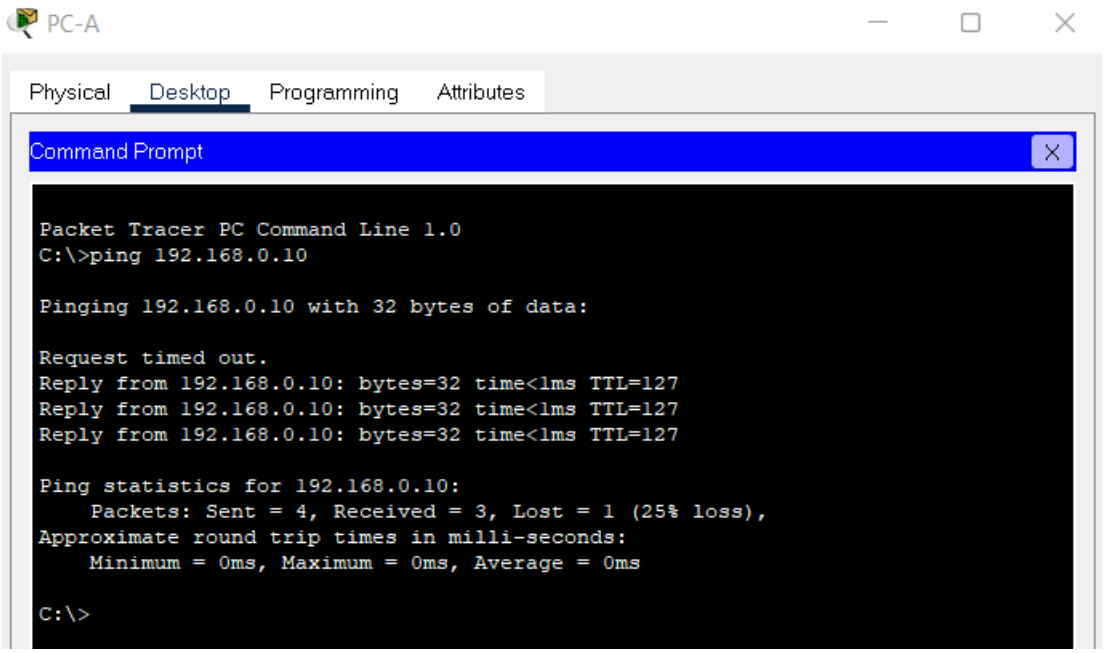
All the configurations will be lost

Step 3: Verify network connectivity.

a. Using the command line at **PC-A**, ping the IPv4 and IPv6 addresses for **Server**.

Were the pings successful?

Yes.



b. From **PC-A**, remotely access **R1** using the Telnet / SSH client.

Using the Telnet / SSH client on PC-A, open an SSH session to the R1 Loopback interface IPv4 address. Ensure that the Connection Type is set to **SSH** and use **SSHadmin** as the username. When prompted, enter the password **55Hadm!n2020**.

Was remote access successful?

c. Using the Telnet / SSH client on **PC-A**, open an SSH session to the R1 Loopback interface IPv6 address. Ensure that the Connection Type is set to **SSH** and use **SSHadmin** as the username. When prompted, enter the password **55Hadm!n2020**.

Was remote access successful?
Successful

Why is the Telnet protocol considered to be a security risk?
A Telnet session can be seen in plaintext. It is not encrypted. Passwords can easily be seen using a packet sniffer.

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 Telnet / SSH client on PC-A, open an SSH session to the R1 Loopback interface IPv6 address and log in as **SSHadmin** with the password **55Hadm!n2020**.

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?

"bootflash:/isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin"

How much non-volatile random-access memory (NVRAM) does the router have?
32768K bytes of non-volatile configuration memory.

How much Flash memory does the router have?
3223551K bytes of flash memory at bootflash

b. The **show** commands often provide multiple screens of outputs. Filtering the output lets you 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 would be the boot process for the router on the next reload if the configuration register was 0x2142?

In most scenarios (0x2102), the router will boot normally, load the IOS from Flash memory, and, if present, load the startup configuration from the NVRAM. The router will skip the startup config and go directly to the user-mode command prompt if the config register is 0x2142. The router enters ROMMON mode if the initial boot fails

Step 3: Display the startup configuration.

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

How are passwords presented in the output?

Passwords are encrypted.

b. Use the **show running-config | section vty** command.

What is the result of using this command?

```
line vty 0 4
 exec-timeout 4 0
 password 7 08654F471A1A0A56533D383D60
 login local
 transport input ssh
line vty 5 15
 exec-timeout 4 0
 password 7 08654F471A1A0A56533D383D60
 login local
transport input ssh
```

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?

C 10.0.0.0/24 is directly connected, Loopback0

C 192.168.0.0/24 is directly connected, GigabitEthernet0/0/0

C 192.168.1.0/24 is directly connected, GigabitEthernet0/0/1

How many route entries are coded with a C code in the routing table?
3

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?
no shutdown

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

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

The [up/up] status represents the interface's Layer 1 and Layer

2 status rather than relying on Layer 3.

c. On **Server**, change its configuration so that it no longer has a static IPv6 address. Then, issue the **ipconfig** command on **Server** to examine the IPv6 configuration.

What is the IPv6 address assigned to Server?

2001:DB8:ACAD:0:207:ECFF:FEA5:6286

What is the default gateway assigned to **Server**?
FE80::1

From **PC-B**, issue a ping to the **R1** default gateway link local address. Was it successful?
Successful

```
C:\>
C:\>
C:\>ping fe80::1

Pinging fe80::1 with 32 bytes of data:

Reply from FE80::1: bytes=32 time<1ms TTL=255
Reply from FE80::1: bytes=32 time=3ms TTL=255
Reply from FE80::1: bytes=32 time<1ms TTL=255
Reply from FE80::1: bytes=32 time<1ms TTL=255

Ping statistics for FE80::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\>
```


From **Server**, issue a ping to the **R1** IPv6 unicast address 2001:db8:acad::1. Was it successful?
Successful

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

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

Reply from 2001:DB8:ACAD::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD::1: bytes=32 time<1ms TTL=255
Reply from 2001:DB8:ACAD::1: bytes=32 time<1ms TTL=255

Ping statistics for 2001:DB8:ACAD::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Reflection Questions

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?
    - **show ip interface brief,**
    - **show interfaces**
    - **show startup-config**

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