

## Lab – Building a Switch and Router Network

### Topology



### Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

### Objectives

#### Part 1: Set Up the Topology and Initialize Devices

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

#### Part 2: Configure Devices and Verify Connectivity

- Assign static IP information to the PC interfaces.
- Configure the router and switch.
- Verify network connectivity.

#### Part 3: Display Device Information

- Retrieve hardware and software information from the network devices.
- Interpret the output from the routing table.
- Display interface information on the router.
- Display a summary list of the interfaces on the router and switch.

#### Part 4: Secure Remote Access to the Router

- Set the IP domain name and generate secure keys.
- Create a SSH user and configure VTY lines for SSH-only access.
- Verify SSH Implementation.

### Background / Scenario

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. You will also access the router remotely via SSH.

Before beginning the lab, verify that there are no previously saved configurations on the devices. Please refer to your instructor for assistance.

Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

### Required Equipment

- 1 Router (Cisco 1941 with Cisco IOS Release 15.4(3) universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 10) with terminal emulation program, such as Tera Term
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

### Part 1: Set Up Topology and Initialized Devices

- a. Attach the devices shown in the topology diagram, and then cable, as necessary.
- b. Power on all the devices in the topology.
- c. Please refer to your instructor for assistance if the devices have previously saved 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 Topology and Addressing Table at the beginning of this lab for device names and address information.

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

- a. Configure the IP address, subnet mask, and default gateway settings on PC-A.
- b. Configure the IP address, subnet mask, and default gateway settings on PC-B.
- c. Ping PC-B from a command prompt window on PC-A. 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 according to the Addressing Table.
- d. Assign **class** as the privileged EXEC encrypted password.
- e. Assign **cisco** as the console password and enable login.

- f. Encrypt the plaintext passwords.
- g. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- h. Configure the IP addresses according to the Addressing Table and activate both Ethernet interfaces on the router.
- i. Save the running configuration to the startup configuration file.

**Note:** Use the question mark (?) to help with the correct sequence of parameters needed to execute this command.

Were the pings successful? Explain.

---

---

---

### Step 3: Configure the switch.

- a. Console into the switch and enable privileged EXEC mode.
- b. Enter configuration mode.
- c. Assign a device name to the router.
- d. Assign **class** as the privileged EXEC encrypted password.
- e. Assign **cisco** as the console password and enable login.
- f. Encrypt the plaintext passwords.
- g. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- h. Configure the IP address for the SVI for VLAN 1 according to the Addressing Table and activate the interface.
- i. Configure the default gateway according to the Addressing Table.
- j. Save the running configuration to the startup configuration file.

## Part 3: Display Device Information

### Step 1: Retrieve hardware and software information from the network devices.

- a. Use the **show version** command to answer the following questions about the router.
- b. What is the name of the IOS image that the router is running?

---

- c. Use the **show version** command to answer the following questions about the switch.  
What is the name of the IOS image that the switch is running?

---

What is the model number of the switch?

---

### Step 2: 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? \_\_\_\_\_

What interface types are associated to the C coded routes?

---

### Step 3: Display interface information on the router.

Use the **show interface g0/1** to answer the following questions.

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

---

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

---

How is the Internet address displayed in this command?

---

### Step 4: 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# show ip interface brief
Interface                IP-Address      OK? Method Status          Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0       192.168.0.1     YES manual  up              up
GigabitEthernet0/1       192.168.1.1     YES manual  up              up
Serial0/0/0              unassigned      YES unset  administratively down down
Serial0/0/1              unassigned      YES unset  administratively down down
R1#
```

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

```
S1# show ip interface brief
Interface                IP-Address      OK? Method Status          Protocol
Vlan1                    192.168.1.2     YES manual  up              up
FastEthernet0/1          unassigned      YES unset  down            down
FastEthernet0/2          unassigned      YES unset  down            down
FastEthernet0/3          unassigned      YES unset  down            down
FastEthernet0/4          unassigned      YES unset  down            down
FastEthernet0/5          unassigned      YES unset  up              up
FastEthernet0/6          unassigned      YES unset  up              up
FastEthernet0/7          unassigned      YES unset  down            down
FastEthernet0/8          unassigned      YES unset  down            down
FastEthernet0/9          unassigned      YES unset  down            down
FastEthernet0/10         unassigned      YES unset  down            down
FastEthernet0/11         unassigned      YES unset  down            down
FastEthernet0/12         unassigned      YES unset  down            down
FastEthernet0/13         unassigned      YES unset  down            down
FastEthernet0/14         unassigned      YES unset  down            down
```

FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/20	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down
FastEthernet0/24	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

S1#

## Part 4: Secure Remote Access to the Router

### Step 1: Set the IP domain name and generate secure keys.

- On R1, configure the domain name as **academy.net**.

```
R1(config)# ip domain-name academy.net
```

- Generate RSA keys with a **1024** key length.

```
R1(config)# crypto key generate rsa modulus 1024
```

```
The name for the keys will be: R1.academy.net
```

```
% The key modulus size is 1024 bits
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 2 seconds)
```

```
*Jun 26 04:58:35.679: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

### Step 2: Create a SSH user and configure VTY lines for SSH-only access.

- Create a user with **SSHuser** as the username and **cisco** as the secret password.

```
R1(config)# username SSHuser secret cisco
```

- Configure the VTY lines to use the local username database for login credentials.

```
R1(config)# line vty 0 4
```

```
R1(config-line)# login local
```

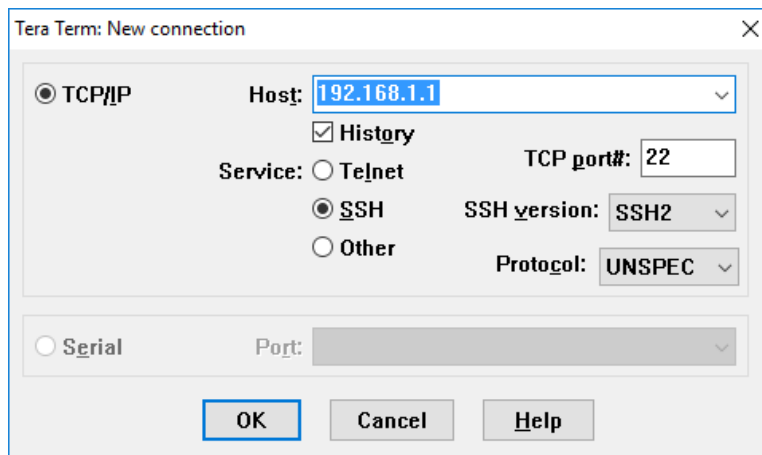
- The VTY lines should only allow SSH for remote access.

```
R1(config-line)# transport input ssh
```

### Step 3: Verify SSH Implementation.

- On PCA, click **Start** and type **Tera Term**. Select **Tera Term** in the results list.

- b. Enter **192.168.1.1** in the Host field. Click **OK** to continue.



Tera Term: New connection

☒ TCP/IP      Host: 192.168.1.1

☒ History

Service: ☐ Telnet      TCP port#: 22

☒ SSH      SSH version: SSH2

☐ Other      Protocol: UNSPEC

☐ Serial      Port:

OK Cancel Help

- c. Click **Continue** in the Security Warning dialog box. Enter the username **SSHuser** and password **cisco**. Click **OK** to continue.

What is the displayed message?

---

You should be at the prompt of R1. If you are not successful, verify the configurations are correct and the credentials were entered correctly. Please refer to your instructor for further assistance.

### Reflection

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

## Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
<b>Note:</b> To find out how the router is configured, look at the interfaces to identify the router type 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.				