Department of ICT

Faculty of Technology

University of Ruhuna

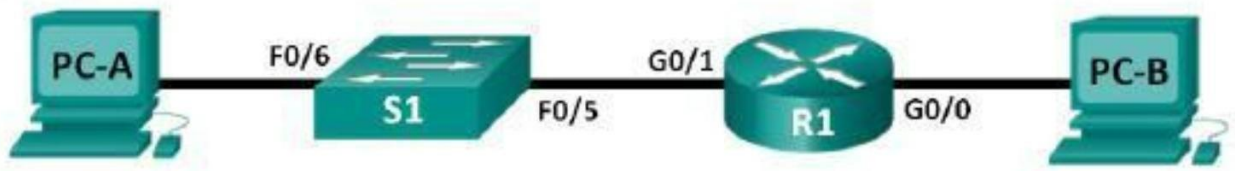
Computer Networks – ICT1253 **Level 1 - Semester - 2**

Lab Sheet 06

==========

Lab – 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.

Required Resources

1 Router (Cisco 1941)
1 Switch (Cisco 2960)
2 PCs

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.

Part 1: Set Up the Topology and Initialize Devices.

Cable the network as shown in the topology.

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

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 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)#
```

The logging synchronous command will tell the router that if any informational items get displayed on the screen, your prompt and command line should be moved to a new line, so as not to confuse you.

The informational line does not get inserted into the middle of the command you are trying to type. If you were to continue typing, the command would execute properly, even though it looks wrong on the screen.

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

```
telnet 192.168.1.1
```

Was remote access successful? ……..

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

Step 4: Configure the router for SSH access.

a. 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 general-keys modulus 1024
R1(config)# exit
```

Both the hostname and the domain name will be used in the process of generating encryption keys.

The password will have to be provided before you can access the CLI of the router when using SSH.

b. Remotely access R1 from PC-A.

telnet 192.168.1.1

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 remote access 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.

SSH -l admin 192.168.0.1

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.

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? .....