Alan Palayil
ECE 407

ECE 407
Introduction to Computer Networks Laboratory

Practice 2 – Basic Device Configuration

Objectives

The goal of this experiment is to:

1. Familiarize students with Cisco IOS.
2. Familiarize students with basic device (PC, switch, router) configuration.

Background

Once a connection is established to a Cisco router or a Cisco switch, either via the console port, telnet, or ssh, the command line interface (CLI) of Cisco IOS will be accessible. Cisco IOS provides different command interface user levels, to allow for different user access roles. Cisco IOS command modes are summarized as follows.

1. **User Exec Mode**
   The user EXEC mode is entered when the router/switch is accessed via a serial connection or when accessing the management port of router/switch via telnet/ssh. The command prompt of the user EXEC mode of a router is:

   Router1>

   The user EXEC mode only offers a small set of commands, such as ping, telnet, and traceroute. Configuration parameters cannot be read or altered in this mode. To exit the user exec mode,

   Router1> exit

2. **Privileged EXEC Mode**
   To change or view configuration information of a router, a user must enter the system administrator mode, called the Privileged EXEC Mode. It is used to read configuration files, reboot the router, and set operating parameters. Entering the privileged EXEC mode requires a password, called the "enable secret." To enter the privileged EXEC mode:

   Router1>enable

   If a password is set, then the system will require it at this stage. After typing the password, the following command prompt will be displayed:
   Router1#
3. **Global Configuration Mode**
   The global configuration mode is used to modify system wide configuration parameters, such as routing algorithms and routing tables. To enter the global configuration mode:

Router1#Configure terminal
The argument terminal tells the router that the configuration commands will be entered from a terminal. The alternatives are to issue configuration commands from a configuration file or from a remote machine via a file transfer. The command prompt in the global configuration mode is:

Router1(Config)#

Remarks:

- Typing a question mark (?) in a given command mode generates a list of all available commands in the current command mode. This command helps to determine if a command can be executed in the current mode. It can also be used to determine the list of available options of a command.
- If a certain command enables a feature, then adding a "no" in front of that command disables the same feature. Sometimes it is the other way around, that is, the command to enable a feature uses the command to disable the feature preceded by a "no".

4. **Interface configuration mode**
   The interface configuration mode is needed to modify the configuration parameters of a specific interface. This mode can only be entered from the global configuration mode by typing interface followed by the interface name, e.g.,

   Router1(Config)# interface fastEthernet 0/0

   The command prompt in this mode is,
   Router1(Config-if)#

   Typing Ctrl-Z or exit reverts to the global configuration mode.

5. **Router configuration mode**
   The router configuration mode is used to configure parameters of a specific routing protocol. This mode can only be entered from the global configuration mode by typing router followed by the routing protocol name, e.g.,

   Router1(Config)# router rip

   The command prompt in this mode is

   Router1(Config-router)# router rip

   Typing Ctrl-Z or exit reverts to the global configuration mode.

Exercise 1: Navigating the Cisco IOS of a Switch (2.1.4.6)

Topology

Step 1: **Connecting to the Switch.**

a. Select **End Devices** from the options in the bottom left-hand corner. Drag and drop 1 generic PC onto your work area.

b. *Select **Network Devices** from the options in the bottom left-hand corner. Drag and drop 1 switch onto your work area*.

c. Select **Connections** from the bottom left-hand corner. Choose **console**-through cable type. Click the first **PC0** and assign the cable to the **RS232** connector. Click **Switch0** and select the console to complete the connection.

Step 2: **Observe the power up process using a terminal session.**

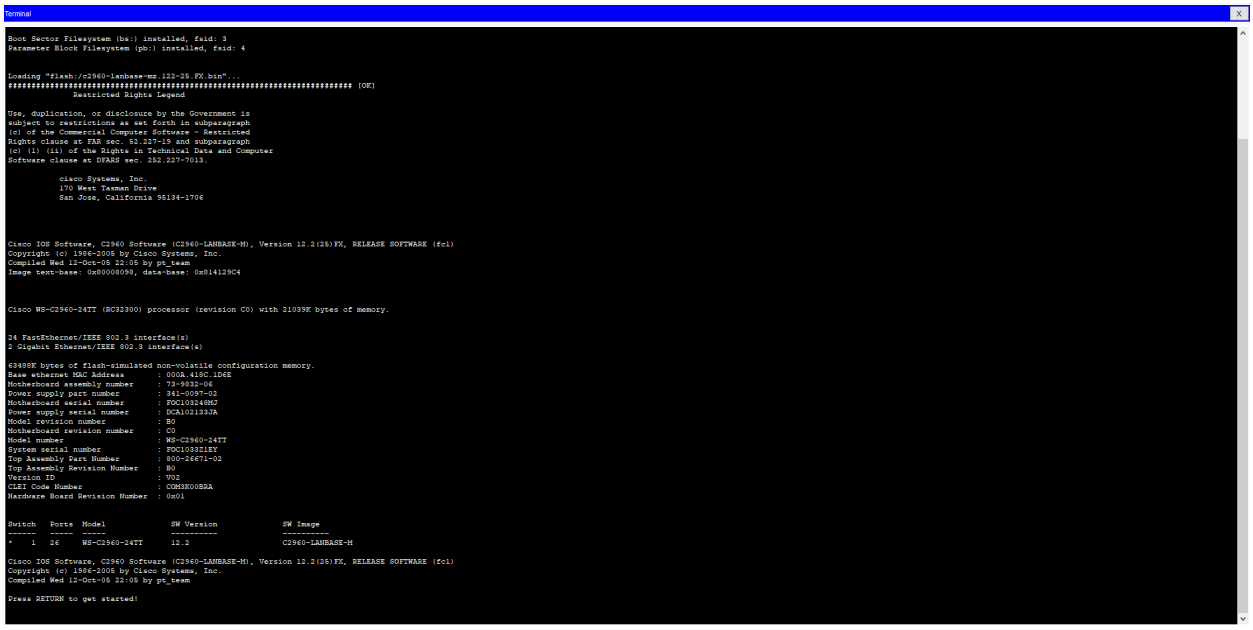
a. Click **PC0**.

b. Select **Desktop** > **Terminal**.

c. Review the terminal configuration. What is the setting for bits per second? **9600**

Click **OK** to continue.

d. The terminal displays the output from when the switch was powering up. What is the prompt displayed on the screen?\



e. Press **Return** to access the prompt.

f. To reload the switch to observe the power up process during startup, enter **enable** at the prompt.

switch> **enable**

g. Enter **reload** at the prompt to start the reload of the switch. Press **Enter** to confirm.

Switch# **reload**

Proceed with reload? [confirm]

Step 3: **Explore the IOS Help.**

a. The IOS can provide help for commands depending on the command mode being accessed. The prompt currently being displayed is called **User EXEC** and the device is waiting for a command. The most basic form of help is to type a question mark (?) at the prompt to display a list of commands.

S1> **?**

Which command begins with the letter 'C'?

Connect

b. At the prompt, type **t**, followed by a question mark (**?**).

S1> **t?**

Which commands are displayed?

Telnet, Terminal, Traceroute

c. At the prompt, type **te**, followed by a question mark (**?**).

S1> **te?**

Which commands are displayed?

Telnet, Terminal

This type of help is known as **Context-Sensitive** Help, providing more information as the commands are expanded.

Step 4: **Enter privileged EXEC mode.**

a. At the prompt, type the question mark (**?**).

S1> **?**

What information is displayed that describes the **enable** command?

Turn on privileged commands

b. Type **en** and press the **Tab** key.

S1> **en<Tab>**

What displays after pressing the **Tab** key?

enable

This is called command completion or tab completion. When part of a command is typed, the **Tab** key can be used to complete the partial command. If the characters typed are enough to make the command unique, as in the case with the **enable** command, the remaining portion is displayed.

What would happen if you were to type **te<Tab>** at the prompt?

c. Enter the **enable** command and press **ENTER**. How does the prompt change?

It switches from Switch> to Switch#

d. When prompted, type the question mark (**?**).

S1# **?**

Previously in user EXEC mode there was one command that started with the letter 'C'. Now how many commands are displayed that begin with the letter 'C'? (**Hint**: you could type c? to list just the commands beginning with 'C'.)

Clear, Clock, Configure, Connect, Copy

Step 5: **Enter Global Configuration mode.**

a. When in privileged EXEC mode, one of the commands starting with the letter 'C' is **configured**. Type either the full command or enough of the command to make it unique along with the <**Tab**> key to issue the command and press **<ENTER>**.

S1# **configure**

What is the message that is displayed?

Enter configuration mode

b. Press the **<ENTER>** key to accept the default parameter enclosed in brackets **[terminal]**.

How does the prompt change?

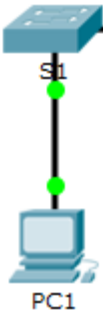
It now states Switch(config)#

Step 3: This is called global configuration mode. This mode will be explored further in upcoming activities and labs. For now, exit back to privileged EXEC mode by typing **end**, **exit** or **Ctrl-Z**.

S1(config)# **exit**
S1#

Exercise 2: Configuring Initial Switch Settings (2.2.3.4)

Topology



A. Verify the Default Switch Configuration

Step 0: Implement the previous topology using packet tracer.

Step 1: Enter privileged EXEC mode.

You can access all switch commands from privileged EXEC mode. However, because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use.

The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained.

a. Click **S1** and then the **CLI** tab. Press Enter.

b. Enter privileged EXEC mode by entering the **enable** command:

Switch> **enable**
Switch#

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

Step 2: Examine the current switch configuration.

a. Enter the **show running-config** command.

Switch# **show running-config**

b. Answer the following questions:

1) How many FastEthernet interfaces does the switch have?

24 interfaces

2) How many Gigabit Ethernet interfaces does the switch have?

2

3) What is the range of values shown for the vty lines?

0-4 & 5-15

4) Which command will display the current contents of non-volatile random-access memory (NVRAM)?

show startup-config

Why does the switch respond with startup-config not present?

It is because the configuration file was located in NVRAM, here we are in the RAM.

B. Create a Basic Switch Configuration

Step 1: Assign a name to a switch.

To configure parameters on a switch, you may be required to move between various configuration modes. Notice how the prompt changes as you navigate through the switch.

Switch# **configure terminal**
Switch(config)# **hostname S1**
S1(config)# **exit**
S1#

Step 2: Secure access to the console line.

To secure access to the console line, access config-line mode and set the console password to **letmein**.

S1# **configure terminal**
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# **line console 0**
S1(config-line)# **password letmein**
S1(config-line)# **login**
S1(config-line)# **exit**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by console
S1#

Why is the **login** command required?

The password checking requires the login and password

Step 3: Verify that console access is secured.

Exit privileged mode to verify that the console port password is in effect.

S1# **exit**
Switch con0 is now available
Press RETURN to get started.

User Access Verification
Password:
S1>

Note: If the switch did not prompt you for a password, then you did not configure the **login** parameter in Step 2.

Step 4: Secure privileged mode access.

Set the **enabled** password to **c1$c0**. This password protects access to privileged mode.

Note: The **0** in **c1$c0** is a zero, not a capital O. This password will not grade as correct until after you encrypt it in Step 8.

S1> **enable**
S1# **configure terminal**
S1(config)# **enable password c1$c0**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by console
S1#

Step 5: Verify that privileged mode access is secure.

a. Enter the **exit** command again to log out of the switch.
b. Press **<Enter>** and you will now be asked for a password:

   User Access Verification
   Password:

c. The first password is the console password you configured for **line con 0**. Enter this password to return to user EXEC mode.
d. Enter the command to access privileged mode.
e. Enter the second password you configured to protect privileged EXEC mode.
f. Verify your configurations by examining the contents of the running-configuration file:

   S1# **show running-config**

Notice how the console and enable passwords are both in plain text. This could pose a security risk if someone is looking over your shoulder.

Step 6: Configure an encrypted password to secure access to privileged mode.

The **enable password** should be replaced with the newer encrypted secret password using the **enable secret** command. Set the enabled secret password to **itsasecret**.

S1# **config t**

S1(config)# **enable secret itsasecret**

S1(config)# **exit**

S1#

Note: The **enable secret** password overrides the **enable** password. If both are configured on the switch, you must enter the **enabled secret** password to enter privileged EXEC mode.

Step 7: Verify that the enabled secret password is added to the configuration file.

a. Enter the **show running-config** command again to verify the new **enabled secret** password is configured.

Note: You can abbreviate **show running-config** as

S1# **show run**

b. What is displayed for the **enable secret** password?

```
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
```

c. Why is the **enabled secret** password displayed differently from what we configured?

It is because the secret is encrypted where the password is shown.

Step 8: Encrypt the enable and console passwords.

As you noticed in Step 7, the **enable secret** password was encrypted, but the **enable** and **console** passwords were still in plain text. We will now encrypt these plain text passwords using the **service password-encryption** command.

S1# **config t**

S1(config)# **service password-encryption**

S1(config)# **exit**

If you configure any more passwords on the switch, will they be displayed in the configuration file as plain text or in encrypted form? Explain.

They will be in encrypted form as this encrypts the current passwords and anymore which are added.

C. Configure a MOTD Banner

Step 1: Configure a message of the day (MOTD) banner.

The Cisco IOS command set includes a feature that allows you to configure messages that anyone logging onto the switch sees. These messages are called messages of the day, or MOTD banners. Enclose the banner text in quotations or use a delimiter different from any character appearing in the MOTD string.

S1# **config t**
S1(config)# **banner motd "This is a secure system. Authorized Access Only!"**
S1(config)# **exit**
%SYS-5-CONFIG_I: Configured from console by console
S1#

1) When will this banner be displayed?

   It is a message of the day which will be seen by anyone logging onto the switch.

2) Why should every switch have a MOTD banner?

   It may be displayed to warn unauthorized users against breaching into the switch. Or just for a universal message that may be shown.

D. Save Configuration Files to NVRAM

Step 1: Verify that the configuration is accurate using the show run command.

Step 2: Save the configuration file.

You have completed the basic configuration of the switch. Now back up the running configuration file to NVRAM to ensure that the changes made are not lost if the system is rebooted or loses power.

S1# **copy running-config startup-config**
Destination filename [startup-config]?**[Enter]**
Building configuration...
[OK]

What is the shortest, abbreviated version of the **copy running-config startup-config** command?

cop r s

Step 3: Examine the startup configuration file.

Which command will display the contents of NVRAM?

show startup-config

Are all the changes that were entered recorded in the file?

Yes as it appears to be the same as the running configuration.

Exercise 3: Configuring Initial Router Settings (6.4.1.3)

Topology

A. Verify the Default Router Configuration

Step 0: Implement the previous topology in Packet Tracer.

Step 1: Establish a console connection to R1.

a. Choose the blue **Console** cable from the available connections.

b. Click **PCA** and select **RS 232**.

c. Drag the cable, click **R1** and select **Console**.

d. Click **PCA** > **Desktop** tab > **Terminal**.

e. Click **OK** and press **ENTER**. You are now able to configure **R1**.

Step 2: Enter privileged mode and examine the current configuration.

You can access all the router commands from privileged EXEC mode. However, because many of the privileged commands configure system parameters, privileged access should be password-protected to prevent unauthorized use.

a. Enter privileged EXEC mode by entering the **enable** command.

Router> **enable**
Router#

Notice that the prompt changed in the configuration to reflect privileged EXEC mode.

b. Enter the **show running-config** command:

Router# **show running-config**

c. Answer the following questions:

What is the router's hostname?	Router
How many Fast Ethernet interfaces does the Router have?	4
How many Gigabit Ethernet interfaces does the Router have?	2
How many Serial interfaces does the router have?	2
What is the range of values shown for the vty lines?	0-4

d. Display the current contents of NVRAM.

Router# **show startup-config**

startup-config is not present

Why does the router respond with the startup-config not present message?

It shows this because the file is not saved on the NVRAM, only the RAM.

B. Configure and Verify the Initial Router Configuration

To configure parameters on a router, you may be required to move between various configuration modes. Notice how the prompt changes as you navigate through the router.

Note: You can use the same command you used to configure the switch in exercise 2.

Step 1: Configure the initial settings on R1.

a. Configure **R1** as the hostname.

b. Configure **letmein** as the console password and enable login.

c. Configure **itsasecret** as the encrypted privileged EXEC password.

d. Encrypt all plain text passwords.

e. Configure a message of the day banner that warns against unauthorized access. A sample banner can be **Unauthorized access is strictly prohibited.**

It only checks for the word "access" in the student's banner motd command.

Step 2: Verify the initial settings on R1.

a. Verify the initial settings by viewing the configuration for R1. What command do you use?

show running-config

b. Exit the current console session until you see the following message:

R1 con0 is now available

Press RETURN to get started.

c. Press **ENTER**; you should see the following message:

Unauthorized access is strictly prohibited.

User Access Verification

Password:

Why should every router have a message-of-the-day (MOTD) banner?

Once again it helps in order to warn unauthorized users against logging in. But also for maintenance messages within the server.

If you are not prompted for a password, what console line command did you forget to configure?

R1(config-line)#login

d. Enter the passwords necessary to return to privileged EXEC mode.

If you configure any more passwords on the router, are they displayed in the configuration file as plain text or in encrypted form? Explain.

Within the service password and encryption command it will encrypt all the passwords already stored and any entered later.

C. Save the Running Configuration File

Step 1: Save the configuration file to NVRAM.

a. You have configured the initial settings for **R1**. Now back up the running configuration file to NVRAM to ensure that the changes made are not lost if the system is rebooted or loses power.

What command did you enter to save the configuration to NVRAM?

copy running-config startup-config

What is the shortest, unambiguous version of this command?

copy r s

Which command displays the contents of the NVRAM?

show startup-configuration or you can also use show start

b. Verify that all of the parameters configured are recorded. If not, analyze the output and determine which commands were not done or were entered incorrectly. You can also click **Check Results** in the instruction window.

Step 2: Optional bonus: Save the startup configuration file to flash.

Although you will be learning more about managing the flash storage in a router in later chapters, you may be interested to know now that —, as an added backup procedure —, you can save your startup configuration file to flash. By default, the router still loads the startup configuration from NVRAM, but if NVRAM becomes corrupt, you can restore the startup configuration by copying it over from flash.

Complete the following steps to save the startup configuration to flash.

a. Examine the contents of flash using the **show flash** command:

R1# **show flash**

How many files are currently stored in flash? 3

Which of these files would you guess is the IOS image?

c1900-universalk9-mz.SPA.151-4.M4.bin

Why do you think this file is the IOS image?

The final length is different along with the .bin.

b. Save the startup configuration file to flash using the following commands:

R1# **copy startup-config flash**

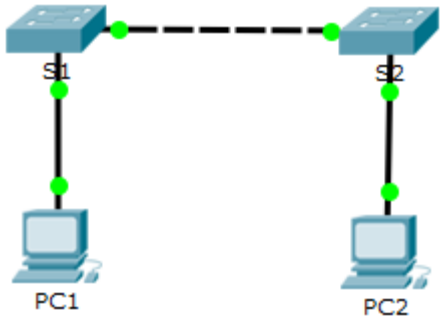
Destination filename [startup-config]

The router prompts to store the file in flash using the name in brackets. If the answer is yes, then press **ENTER**; if not, type an appropriate name and press **ENTER**.

c. Use the **show flash** command to verify the startup configuration file is now stored in flash.

Exercise 4: Implementing Basic Connectivity (2.3.2.5)

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	NIC	192.168.1.1	255.255.255.0
PC2	NIC	192.168.1.2	255.255.255.0

A. Perform a Basic Configuration on S1 and S2

Step 0: Implement the previous topology in Packet Tracer.

Step 1: Configure S1 with a hostname.

a. Click **S1**, and then click the **CLI** tab.

b. Enter the privileged EXEC mode. Then enter the global configuration mode.

Switch> **enable**

Switch# **configure terminal**

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

c. Configure the hostname as **S1**.

Switch(config)# **hostname S1**

S1(config)#

Step 2: Configure the console and privileged EXEC mode passwords.

a. Configure **cisco** as the console password and enable login.

S1(config)# **line console 0**
S1(config-line)# **password cisco**
S1(config-line)# **login**
S1(config-line)# **exit**

b. Use **class** for the encrypted privileged EXEC mode password.

S1(config)# **enable secret class**

Step 3: Verify the password configurations for S1.

a. To verify that the passwords were configured correctly, enter **end** to exit the global configuration mode. Type **exit** to exit the privileged EXEC mode.

S1(config)# **end**
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1# **exit**

b. Press **Enter** and you will be prompted for a password to enter the user EXEC mode.

What password did you use?

cisco

c. Type **enable** to enter the privileged EXEC mode. Enter the password when prompted.

What password did you use?

class

d. Enter **configure terminal** to enter global configuration mode.

Step 4: Configure a message of the day (MOTD) banner.

In this step, you will configure a message of the day banner to warn unauthorized access. The following text is an example:

Authorized access only. Violators will be prosecuted to the full extent of the law.

Use the **banner motd** command with the sample message. You can choose another message.

S1(config)# **banner motd "Authorized access only. Violators will be prosecuted to the full extent of the law."**

Step 5: Save the configuration file to NVRAM.

a. Exit to privileged EXEC mode.

S1(config)# **exit**

S1#

%SYS-5-CONFIG_I: Configured from console by console

S1#

b. Enter the **copy running-config startup-config** command to save the configuration.

S1# **copy running-config startup-config**

Destination filename [startup-config]?

Building configuration...

[OK]

Step 6: Repeat Steps 1 through 5 on S2.

B. Configure the PCs

Step 1: Configure both PCs with IP addresses.

a. Click **PC1**, and then click the **Desktop** tab.

b. Click **IP Configuration**. In the **Addressing Table** above, you can see that the IP address for PC1 is supposed to be 192.168.1.1 and the subnet mask 255.255.255.0. Enter this information for PC1 in the **IP Configuration** window.

c. Repeat steps 1a and 1b for PC2.

Step 2: Test connectivity to switches.

a. Click **PC1**. Close the **IP Configuration** window if it is still open. In the **Desktop** tab, click **Command Prompt**.

b. Type the **ping** command and the IP address for S1, and press **Enter**.

Packet Tracer PC Command Line 1.0

PC> **ping 192.168.1.253**

Were you successful? Explain.

No, as the switches do not have the proper IP address.

C. Configure the Switch Management Interface

Step 1: Configure S1 with an IP address.

Switches can be used without any configurations. Switches forward information from one port to another based on Media Access Control (MAC) addresses. Why does a switch need an IP address?

It is necessary in order to connect to a switch remotely.

a. In the global configuration mode, enter the following commands to configure S1 with an IP address in VLAN 1.

S1# **configure terminal**

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

S1(config)# **interface vlan 1**
S1(config-if)# **ip address 192.168.1.253 255.255.255.0**
S1(config-if)# **no shutdown**
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
S1(config-if)#
S1(config-if)# **exit**
S1#

What is the **no shutdown** command?

It enables the interface to an active state.

b. Save the configuration.

S1# **copy running-config startup-config**
Destination filename [startup-config]?
Building configuration...
[OK]
S1#

c. Verify the IP address configuration on S1.

S1# **show ip interface brief**
<output omitted>
Vlan1 192.168.1.253 YES manual up up

Step 2: Configure S2 with an IP address.

Use the information in the addressing table to repeat the same process in Step 1 to configure S2 with an IP address. Remember to save and verify your configurations.

Step 3: Verify network connectivity.

Network connectivity can be verified using the **ping** command. It is very important that connectivity exists throughout the network.

a. Click **PC1**, and then click the **Desktop** tab.

b. Open the **Command Prompt**.

1) Ping the IP address for PC2.

2) Ping the IP address for S1.

3) Ping the IP address for S2.

c. From PC2, ping the other devices in the network.

d. From S1, ping the other devices in the network. The ping to PC1 is displayed below as an example.

S1> **ping 192.168.1.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

e. From S2, ping the other devices in the network.

All pings should be successful. If your first ping result is 80%, retry; it should now be 100%. You will learn why a ping may fail the first time later in your studies. If you are unable to ping any of the devices, check your configuration for errors.

Remarks:

- If the router terminal is in the configuration mode, exit by typing NO.
  Would you like to enter the initial configuration dialog? [yes/no]:no
  Press RETURN to get started!
- When in privileged exec command mode, any misspelled or unrecognized commands will attempt to be translated by the router as a domain name. Since there is no domain server configured, there will be a delay while the request timed out. This can take between several seconds to several minutes. To terminate the wait, simultaneously hold down the <CTRL><SHIFT>6 keys then release and press x:
- Cisco IOS supports two commands that set access to the privileged exec mode. One command, enable password, contains weak cryptography and should never be used if the enable secret command is available. The enable secret command uses a very secure MD5 cryptographic hash algorithm. Password security relies on the password algorithm, and the password. . In production environments, strong passwords should be used at all times. A strong password consists of at least nine characters of upper and lower-case letters, numbers, and symbols.
- Cisco IOS refers to RAM configuration storage as running-configuration, and NVRAM configuration storage as startup-configuration. For configurations to survive rebooting or power restarts, the RAM configuration must be copied into non-volatile RAM (NVRAM). This does not occur automatically, NVRAM must be manually updated after any changes are made.
- **To erase the NVRAM configuration file:**

  Router1# erase startup-config
  Erasing the nvram file system will remove all configuration files!
  Continue? [confirm] <ENTER> [OK]
  Erase of nvram: complete Reload the router:
  Router1# reload
  Proceed with reload? [confirm] <ENTER>