Computer Practical – Week 2

Objectives

The aim of this week's practical includes:

- Gain further familiarity with Packet Tracer
- To enhance the understanding of the command structure of Cisco IOS
- To practice the skill of accessing a Cisco switch and do basic switch configuration
- To know the basic method for connectivity test

Tasks

Accordingly you will need to complete the following tasks in this week's computer practical class:

a. Packet Tracer Activity - Configure initial switch settings
b. Packet Tracer Activity - Implement basic connectivity
c. Packet Tracer Activity - Skill integration challenge

Instructions of the activities are given on the next pages.

Assessment

This week's Practical is assessed in class, and it is worth 1% of the total score of the course.

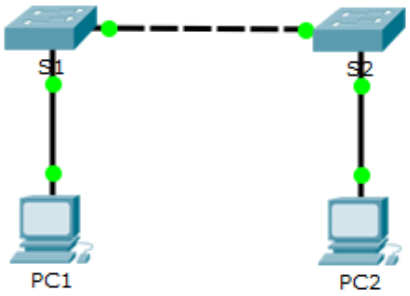
Note: To be awarded marks for the assessment, a student must attend this week's Computer Practical class and submit ALL the three completed Packet Tracer activity files using the "Computer Practical-Week 2-Submission-XXX-classes" link in Week 2 section of Learnonline site (XXX stands for the day your computer practical class in on). The submission must be made in your Computer Practical class in Week 2, unless your tutor gives you the permission to submit outside the class.

Packet Tracer - Configuring Initial Switch Settings

Reminder:

a. Download from Learnonline course website (**Computer Practical-Week2 folder**) the Packet Tracer activity file: **`week2-computer-prac-PKA-a-ConfigInitialSwitchSettings.pka`**
b. Open the Packet Tracer activity file downloaded and set up User Profile for this PT activity.
c. Follow the instruction **given below** to complete this Packet Tracer activity.
d. Save the completed PT activity file as you will need to include it as part of your submission.

Topology



Objectives

Part 1: Verify the Default Switch Configuration

Part 2: Configure a Basic Switch Configuration

Part 3: Configure a MOTD Banner

Part 4: Save Configuration Files to NVRAM

Part 5: Configure S2

Background

In this activity, you will perform basic switch configurations. You will secure access to the command-line interface (CLI) and console ports using encrypted passwords. You will also learn how to configure messages for users logging into the switch. These banners are also used to warn unauthorized users that access is prohibited.

Part 1: Verify the Default Switch Configuration

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.

Note: Although you can click on the CLI tab to access the switch's CLI within Packet Tracer, when working with real devices, you will need to establish a console connection or using remote access method such as Telnet to access the switch's CLI.

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 to display current operating configuration (stored in random-access memory (RAM), and will be lost at power off)

```
Switch# show running-config
```

b. Enter the **show startup-config** command to display contents of startup configuration (stored in non-volatile RAM (NVRAM))

```
Switch# show startup-config
```

c. Answer the following questions:

1) How many FastEthernet interfaces does the switch have? _____

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

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

4) Why does the switch respond with `startup-config is not present`?

_____

_____

Part 2: 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?

_____

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

Set the enable secret password to **itsasecret**, to secure access to privileged EXEC mode.

```
S1> enable
S1# config t
S1(config)# enable secret itsasecret
S1(config)# exit
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. Enter the **show running-config** command again to verify the new **enable secret** password is configured.

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

```
S1# show run
```

What is displayed for the **enable secret** password? _____

Why is the **enable secret** password displayed differently from what we configured?

_____

Step 6: Encrypt the console passwords.

As you noticed in the previous step, the **enable secret** password was encrypted, but the **console** password was still in plain text. We will now encrypt 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?

_____

Part 3: 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 message 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?

_____

_____

2) Why should every switch have a MOTD banner?

_____

_____

Part 4: 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? _____

Step 3: Examine the startup configuration file.

Which command will display the contents of NVRAM? _____

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

Part 5: Configure S2

You have completed the configuration on S1. You will now configure S2. If you cannot remember the commands, refer to Parts 1 to 4 for assistance.

Configure S2 with the following parameters:

a. Name device: **S2**

b. Protect access to the console using the **letmein** password.

c. Configure an enable secret password of **itsasecret**.

d. Configure a message to those logging into the switch with the following message:

```
Authorized access only. Unauthorized access is prohibited and violators
will be prosecuted to the full extent of the law.
```

e. Encrypt all plain text passwords.

f. Ensure that the configuration is correct.

g. Save the configuration file to avoid loss if the switch is powered down.

At the end of the activity, your completion should be 64/64 (It was 12/64 when you first open the .pka file). If not, click on "Check Results" to see where you have done incorrectly.

Packet Tracer - Implementing Basic Connectivity

Before start:

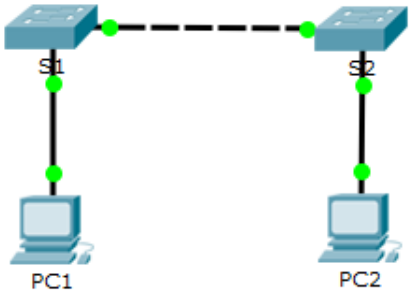
Review some of the key concepts related to this activity by answering the following questions:

- What does SVI stand for? When would you need to assign a SVI an IP address? (You can find answers to the questions from Week 1 topic slides or readings)

Reminder:

a. Download from Learnonline course website (**Computer Practical-Week2 folder**) the Packet Tracer activity file: **`week2-computer-prac-PKA-b-ImplementBasicConnectivity.pka`**
b. Open the Packet Tracer activity file downloaded and set up User Profile for this PT activity.
c. Follow the instruction **given below** to complete this Packet Tracer activity.
d. Save the completed PT activity file as you will need to include it as part of your submission.
e. Refer to the instruction of the previous PT activity (Configuring Initial Switch Settings) if you need to recall some of commands used for the following steps.

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

Objectives

Part 1: Perform a Basic Configuration on S1 and S2

Part 2: Configure the PCs

Part 3: Configure the Switch Management Interface

Background

In this activity, you will first perform basic switch configurations. Then, you will implement basic connectivity by configuring IP addressing on switches and PCs. When the IP addressing configuration is complete, you will use

various **show** commands to verify configurations and use the **ping** command to verify basic connectivity between devices.

Part 1: Perform a Basic Configuration on S1 and S2

Complete the following steps on S1 and S2.

Step 1: Configure S1 with a hostname.

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

b. Enter the correct command to configure the hostname as **S1**.

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

a. Use **cisco** for the console password.

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

Step 3: Verify the password configurations for S1.

How can you verify that both passwords were configured correctly?

_____

_____

Step 4: Configure an MOTD banner.

Use an appropriate banner text to warn unauthorized access. The following text is an example:

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

Step 5: Save the configuration file to NVRAM.

Which command do you issue to accomplish this step?

_____

_____

Step 6: Repeat Steps 1 to 5 for S2.

Configure S2 with the hostname S2. Other parameters for S2 are the same as S1.

Part 2: Configure the PCs

Configure PC1 and PC2 with IP addresses.

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 192.168.1.1 and the subnet mask is 255.255.255.0. Enter this information for PC1 in the **IP Configuration** window.

c. Repeat steps 1a and 1b for PC2. (refer to the addressing table given at the start of the document for PC2's IP address)

Step 2: Test connectivity between PCs and 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 of PC2 and press Enter.

```
Packet Tracer PC Command Line 1.0
PC> ping 192.168.1.2
```

Were you successful? _____

The ping should be successful. If not check the PC's IP address (and subnet mask configurations)

c. 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.

_____

Part 3: Configure the Switch Management Interface

To manage a Cisco device, one can establish a local console connection from a computer (with a terminal emulation program installed) to the device. A Cisco device can also be managed via a remote connection. A Cisco switch has a special interface, known as a switch virtual interface (SVI). The SVI can be configured with an IP address, commonly referred to as the management address. The management address is used for remote access to the switch to display or configure settings. In this part, you will configure the SVIs of the switches, and demonstrate the use of a management IP address for remote switch management.

Note that switches can be used as plug-and-play devices. This means that they do not need to be configured with an IP address for them to work. Switches forward information from one port to another based on MAC addresses. The IP address configured for a switch's management interface is for remote switch management purpose only.

Step 1: Configure S1's Management Interface

a. Use the following commands to configure S1 with an IP address.

```
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#
```

Why do you enter the **no shutdown** command?

_____

b. Configure the VTY line for the switch to allow Telnet access. If you do not configure a VTY password, you will not be able to telnet to the switch.

```
S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
```

```
S1(config-line)# end
S1#
*Mar  1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```

Step 2: Configure S2's Management Interface

Use the information in the Addressing Table to configure S2 with an IP address and set up the password for the VTY line of the switch to allow Telnet access.

Step 3: Verify the IP address configuration on S1 and S2.

Use the **show ip interface brief** command to display the IP address and status of all the switch ports and interfaces. You can also use the **show running-config** command.

Step 4: Verify the telnet connections to S1 and S2.

a. Click PC1 or PC2 and then click the **Desktop** tab.

b. In the **Desktop** tab, click **Command Prompt**.

c. Telnet S1

```
PC>telnet 192.168.1.253
```

d. When you are asked to enter a password, enter the one you have setup for the vty lines

Now you have got the access to S1, and you can display and configure the settings of S1 via this telnet connection. To terminate a telnet connection, type "exit".

e. repeat the above steps (a to d) to verify the telnet connection to S2

Step 5: Save configurations for S1 and S2 to NVRAM.

Which command is used to save the configuration file in RAM to NVRAM?

_____

Step 6: Verify network connectivity.

Network connectivity can be verified using the **ping** command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure. Ping S1 and S2 from PC1 and PC2.

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

b. Click **Command Prompt**.

c. Ping the IP address for PC2.

d. Ping the IP address for S1.

e. Ping the IP address for S2.

Note: You can also use the **ping** command on the switch CLI and on PC2.

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

At the end of the activity, your completion should be 88/88 (It was 2/88 when you first open the .pka file). If not, click on "Check Results" to see where you have done incorrectly.

Week 2 Packet Tracer Skill Integration Challenge

In your Week 2 Computer Practical class, after you have completed the previous two Packet Tracer activities, as the last task of the class, your tutor will provide you a Packet Tracer activity file. The given Packet Tracer activity provides you the opportunity to use the commands and skills that you have learned from previous activities to complete a basic switch and end device configuration task.

Follow the instructions and requirements included in the .pka file provided by your tutor to complete this activity.