

1.2 Packet Tracer – Implement Basic Connectivity

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	E0	192.168.1.1	255.255.255.0
PC2	E0	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/Scenario

In this activity, you will first create a basic switch configuration. 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 the configuration and use the **ping** command to verify basic connectivity between devices.

NOTE

- **Power all the devices first by clicking the triangle button on the upper navbar.**
- **Right click the device then click the web console first to configure on the device.**
- **Always type “save” when configuring IP Addresses of PC’s**

Instructions

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. Right Click S1 and then click the Console.
- b. Enter the correct command to configure the hostname as S1.

```
Switch#configure terminal
Switch(config)#hostname S1
```

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

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

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

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

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

Step 3: Verify the password configurations for S1.

Use an appropriate banner text to warn unauthorized access. Use #(Number Sign) for this activity. The following text is an example:

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

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

Step 4: Save the configuration file to NVRAM.

```
S1#copy running-config startup-config
```

Step 5: Repeat Steps 1 to 5 for S2.

Part 2: Configure the PCs

Configure PC1 and PC2 with IP addresses.

Step 1: Configure both PCs with IP addresses.

- Right click PC1 and then click the console tab.
- 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.

Note: Format use the command "ip ip-address/subnet mask" or "ip ip-address subnet"

```
PC1> ip 192.168.1.1/24
```

```
PC1> save
```

```
PC2> ip 192.168.1.2 255.255.255.0
```

```
PC1> save
```

Step 2: Test connectivity to switches.

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

Part 3: Configure the Switch Management Interface

Configure S1 and S2 with an IP address.

Step 1: Configure S1 with an IP address.

Switches can be used as plug-and-play devices. This means that they do not need to be configured for them to work. Switches forward information from one port to another based on MAC addresses.

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

```
S1(config)#interface vlan 1  
  
S1(config-if)#ip address 192.168.1.253 255.255.255.0 or  
S1(config-if)#ip address 192.168.1.253/24  
  
S1(config-if)#no shutdown  
  
S1(config-if)#exit  
  
S1(config)#exit  
  
S1#copy running-config startup-config
```

Step 2: Configure S2 with an IP address.

Use the information in the Addressing Table to configure S2 with an IP address.

```
Switch>en  
  
Switch#configure terminal  
  
Switch(config)#hostname S2  
  
S2(config)#line console 0  
  
S2(config-line)#password cisco  
  
S2(config-line)#login  
  
S2(config-line)#exit
```

```
S2(config)#enable secret class

S2(config)#banner motd #Authorized access only. Violators will
be prosecuted to the full extent of the law.#

S2(config)#interface vlan 1

S2(config-if)#ip address 192.168.1.254 255.255.255.0

S2(config-if)#no shutdown

S2(config-if)#exit

S2(config)#exit

S2#copy running-config startup-config
```

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 5: 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.

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.