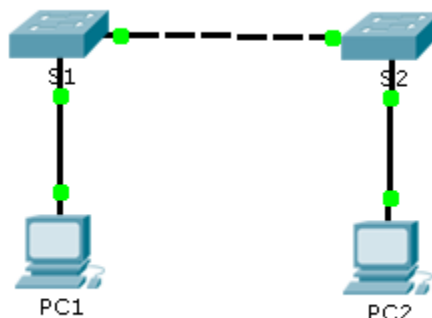


Packet Tracer - Implement Basic Connectivity

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.

1. Perform a Basic Configuration on S1 and S2

Complete the following steps on S1 and S2.

1. Configure S1 with a hostname.

- Click **S1**, and then click the **CLI** tab.
- Enter the correct command to configure the hostname as **S1**.

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.

3. Verify the password configurations for S1.

How can you verify that both passwords were configured correctly?

-After exit, type <enter> and enter the password for the console. Type <enable> and enter the password for the privileged EXEC mode.

e

-Verify your configurations by examining the contents of the running-configuration file:

-S1# show running-config

-2.2.3.3 Packet Tracer - Configuring Initial Switch Settings Instructions

4. Configure a message of the day (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.

5. Save the configuration file to NVRAM.

Which command do you issue to accomplish this step?

-copy running-config startup-config; copy ru st;

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]

-2.2.3.3 Packet Tracer - Configuring Initial Switch Settings Instructions

6. Repeat Steps 1 to 5 for S2.

2. Configure the PCs

Configure PC1 and PC2 with IP addresses.

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.

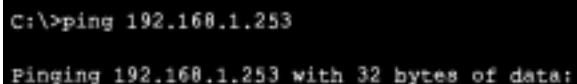
2. Test connectivity to switches.

- 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? Why or why not?



```
C:\>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:
```

-The ping command can be used to test connectivity to another device on the network or a website on the Internet.

-End-to-End Connectivity Test (2.3.3.2)

-Introduction to Networks v6

3. Configure the Switch Management Interface

Configure S1 and S2 with an IP address.

1. Configure S1 with an IP address.

Switches can be used as a plug-and-play device, meaning they do not need to be configured for them to work. Switches forward information from one port to another based on Media Access Control (MAC) addresses. If this is the case, why would we configure it with an IP address?

-Secure Shell (SSH) – SSH is a method for remotely establishing a secure CLI connection through a virtual interface, over a network. Unlike a console connection, SSH connections require active networking services on the device including an active interface configured with an address. SSH is the recommended method for remote management because it provides a secure connection. SSH provides encrypted password authentication and transport of session data. This keeps the user ID, password, and the details of the management session private. Most versions of Cisco IOS include an SSH server and an SSH client that can be used to establish SSH sessions with other devices.

-Provides a secure connection to implement basic connectivity by configuration IP addressing;

-The technician can enter commands to configure, or program, the device to perform various networking functions. Cisco IOS routers and switches perform functions that network professionals depend upon to make their networks operate as expected.

- Access Methods (2.1.2.1)

-Introduction to Networks v6

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 need to enter the **no shutdown** command?

-To enable the virtual interface, use the no shutdown interface configuration command.

-Switch Virtual Interface Configuration (2.3.2.3)

-Introduction to Networks v6

2. Configure S2 with an IP addresses.

Use the information in the addressing table to configure S2 with an IP address.

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 the all the switch ports and interfaces. Alternatively, you can also use the **show running-config** command.

4. Save configurations for S1 and S2 to NVRAM.

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

- To save changes made to the running configuration to the startup configuration file use the copy running-config startup-config privileged EXEC mode command.

-Save the Running Configuration File (2.2.3.1)

-Introduction to Networks v6

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]

-2.2.3.3 Packet Tracer - Configuring Initial Switch Settings Instructions

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's and S2's IP address from PC1 and PC2.

- Click **PC1**, and then click the **Desktop** tab.
- Click **Command Prompt**.
- Ping the IP address for PC2.
- Ping the IP address for S1.
- Ping the IP address for S2.

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

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, recheck your configuration for errors.

Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 1: Perform a Basic Configuration on S1 and S2	Step 3	2	
	Step 5	2	
Part 2: Configure the PCs	Step 2b	2	
Part 3: Configure the Switch Management Interface	Step 1, q1	2	
	Step 1, q2	2	
	Step 4	2	
Questions		12	
Packet Tracer Score		88	
Total Score		100	