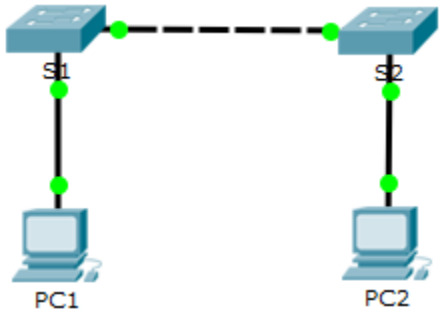
Packet Tracer - Configuring Initial Switch Settings (Lab2-switch)

Topology:



Addressing Table:

Device	Interface	IP Address	Subnet Mask
S1	VLAN1	192.168.1.253	255.255.255.0
S2	VLAN1	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
Part 2: Configure a MOTD Banner
Part 3: Save Configuration Files to NVRAM
Part 4: Configure S2
Part 5: Configure the PCs
Part 6: Configure the Switch Management Interface

Part 1: Perform a Basic Configuration on S1

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: 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 3: Secure access to the console line.

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

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# line console 0
S1(config-line)# password cisco
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 4: Secure privileged mode access.

Set the **enable** password to **cisco**. This password protects access to privileged mode.

```
S1> enable
S1# configure terminal
S1(config)# enable password cisco
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>**

c. Enter the command to access privileged mode.

d. Enter the password you configured to protect privileged EXEC mode.

e. 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 enable secret password to **class**.

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

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

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

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

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

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.

Part 2: 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 3: 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 4: 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 **cisco** password.

c.Configure an enable password of **cisco** and an enable secret password of **class**.

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

```
Authorized access only. Unauthorized access is prohibited and violatorswill 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.

Part 5: 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 is192.168.1.1 and the subnet mask is 255.255.255.0. Enter this information for PC1 in the **IPConfiguration** window.

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

Part 6: 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. If this is the case, why would we configure it with an IP address?
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?

Step 2: Configure S2 with an IP address.

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

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: Save configurations for S1 and S2 to NVRAM.

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

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.

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