**Lab 5 A: Packet Tracer - Configuring Initial Switch Settings**

**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 and plain text 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 mode.**

You can access all switch commands from privileged 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:

How many FastEthernet interfaces does the switch have?

How many Gigabit Ethernet interfaces does the switch have?

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

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

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:**     **Secure privileged mode access.**

Set the **enable** 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-configuration**

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 **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 **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-configuration**command again to verify the new **enable secret** password is configured.

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

S1# **show run**

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

c.     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 why?

**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#

When will this banner be displayed?

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 password of **c1$c0**and 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.

**Lab 5 B: Packet Tracer - Implement Basic Connectivity**

**Addressing Table**

|  |  |  |  |
| --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** |
| S1 |  | 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 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.**

**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.**

**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.

**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? Why or why not?

**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 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?

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?

**Step 2:**   **Configure S2 with an IP addresses.**

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 the all the switch ports and interfaces. Alternatively, 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’s and S2's IP address 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 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.