# 1.1 – ITN - PacketKnows– Configure 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

**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.

**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**

**Part 1: Verify the Default Switch Configuration**

Step 1: Examine the current switch configuration.

a. Enter the show running-config command.

Switch#

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?*

*It displays this message because the configuration file was not saved to NVRAM. Currently it is only located in RAM.*

**Part 2: Create a Basic Switch Configuration**

Step 1: Assign a name to a switch.

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.

Enter configuration commands, one per line. End with CNTL/Z.

%SYS-5-CONFIG_I: Configured from console by console

In order for the password checking process to work, it requires both the login and password commands

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.

Step 5: Verify that privileged mode access is secure.

a. Enter the command to access privileged mode.

b. Enter the second password you configured to protect privileged EXEC mode.

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

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.

**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*

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? The service

password-encryption command encrypts all current and future passwords.

**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.

When will this banner be displayed?

Why should every switch have a MOTD banner?

Every switch should have a banner to warn unauthorized users that access is prohibited but can also be used for sending messages to network personnel/technicians (such as impending system shutdowns or who to contact for access)

**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.

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.