Networking Academy

NAME: BEATRICE ANN DAVID A23CS0055

LAB 1:
2.5.5: Packet Tracer - 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 S2

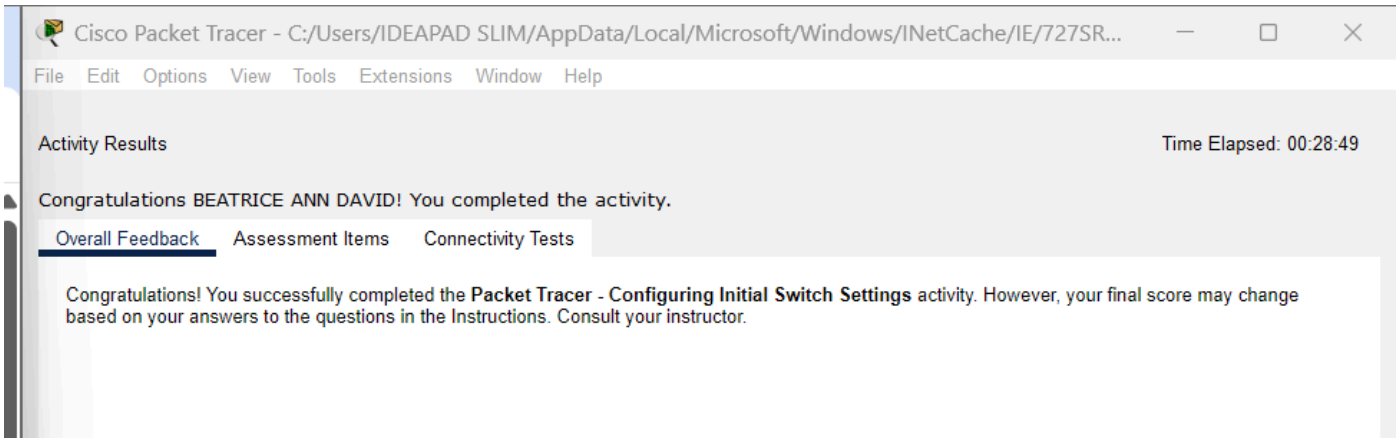
Background / Scenario

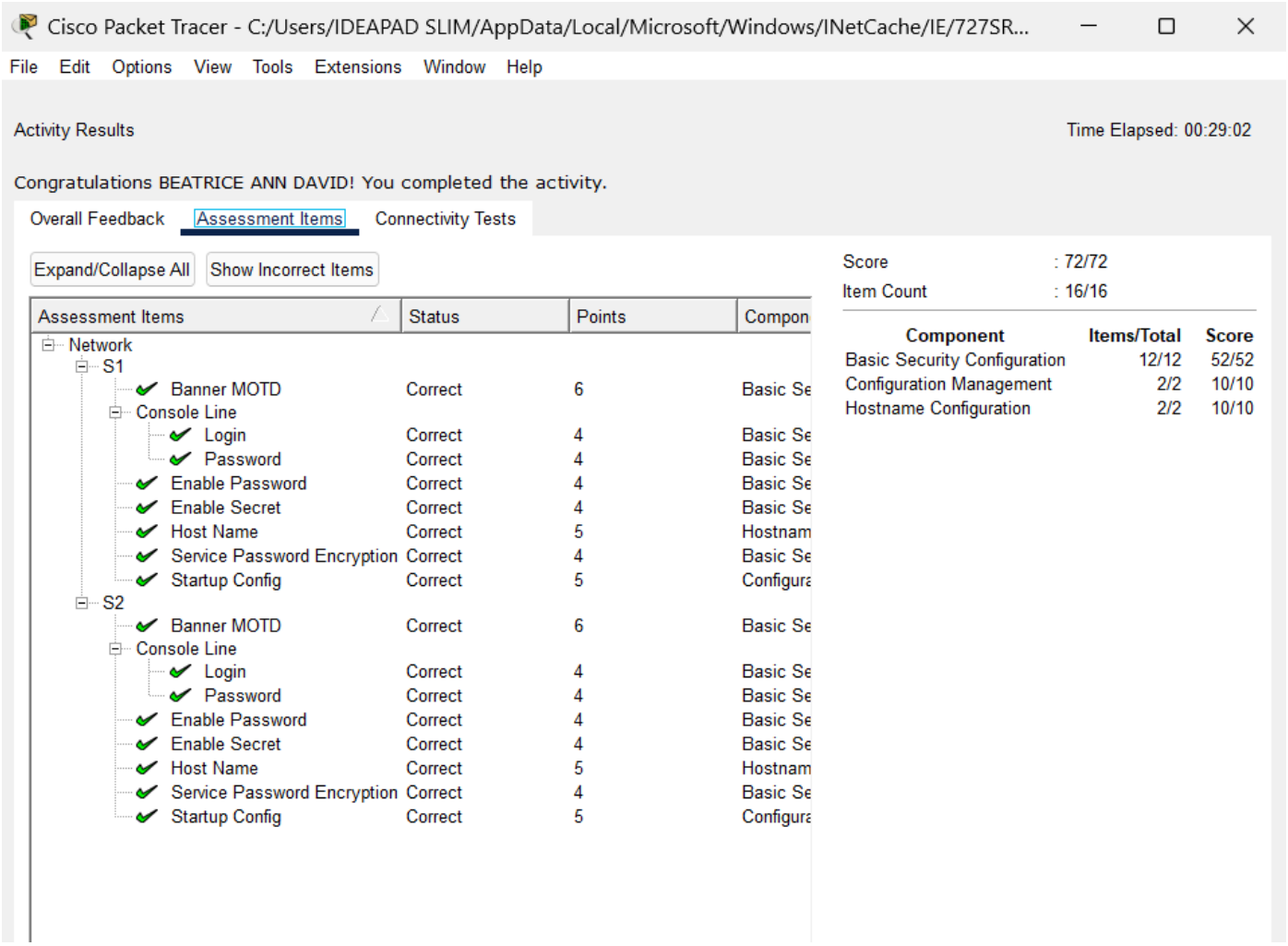
In this activity, you will perform basic switch configuration tasks. You will secure access to the command-line interface (CLI) and console ports using encrypted and plain text passwords. You will also learn how to configure messages for users logging into the switch. These message banners are also used to warn unauthorized users that access is prohibited.

Note: In Packet Tracer, the Catalyst 2960 switch uses IOS version 12.2 by default. If required, the IOS version can be updated from a file server in the Packet Tracer topology. The switch can then be configured to boot to IOS version 15.0, if that version is required.

Screenshots:

A. Result:





B. Working:

Part 1: Verify the Default Switch Configuration

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 the commands available in user EXEC mode, many additional commands, and the **configure** command through which access to the configuration modes is 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 to reflect privileged EXEC mode.

Step 2: Examine the current switch configuration.

Enter the show running-config command.

```
Switch# show running-config
```

Answer the following questions:

How many Fast Ethernet interfaces does the switch have?

24

How many Gigabit Ethernet interfaces does the switch have?
2

What is the range of values shown for the vty lines?
0 to 4
5 to 15

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

Why does the switch respond with “startup-config is not present?”
Because there is no content in NVRAM

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?
Because it used to enable password checking

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 configuration by examining the contents of the running-configuration file:

```
S1# show running-config
```

Notice that the console and enable passwords are both in plain text. This could pose a security risk if someone is looking over your shoulder or obtains access to config files stored in a backup location.

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.

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

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

```
S1# show run
```

What is displayed for the enable secret password?

5 1mERr$ILwq/b7kc.7X/ejA4Aosn0

Why is the enable secret password displayed differently from what we configured?
Because it supposed to be encrypted (shouldn’t be understandable)

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.

Encrypted. Whatever passwords set in the future will be in encrypted form.

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?

When you press enter after “press return to get started”

Why should every switch have a MOTD banner?
Because it’s a security warning to all intruders

Part 4: Save and Verify Configuration Files to NVRAM

Step 1: Verify that the configuration is accurate using the show run command.

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?

cop r st

Examine the startup configuration file.

Which command will display the contents of NVRAM?

show startup-config

Are all the changes that were entered recorded in the file?
Yes

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. Device name: **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 an appropriate message to those logging into the switch.

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.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#line console 0
S2(config-line)#password letmein
S2(config-line)#login
S2(config-line)#exit
S2(config)#enable password c1$c0
S2(config)#enable secret itsasecret
S2(config)#banner motd "Unauthorized access is strictly prohibited"
S2(config)#service password-encryption
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#show running-config
Building configuration...

Current configuration : 1252 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S2
!
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password 7 08221D0A0A49
!
!
```