

CMPE 305 Data and Digital Communication

MP3 – Basic Switch and OSI Model

Delima, Sheena Mae D.

BSCPE 3-3

09/28/2025

2.5.5 – 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.

Instructions

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.

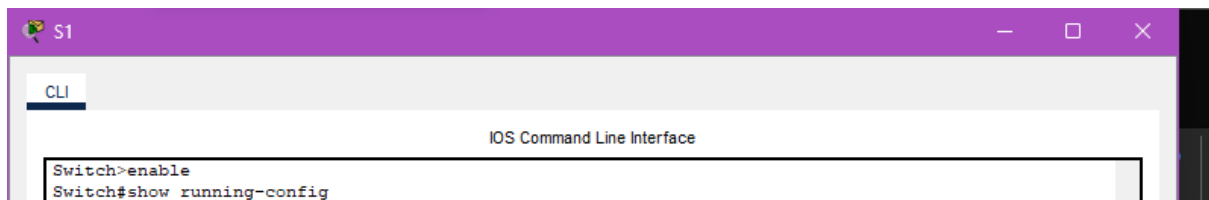
- a. Click S1 and then the CLI tab. Press Enter.
- b. Enter privileged EXEC mode by entering the enable command:

Open Configuration Window for S1

```
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:

1. How many Fast Ethernet interfaces does the switch have? 24 Fast Ethernet interfaces
2. How many Gigabit Ethernet interfaces does the switch have? 2 Gigabit Ethernet interfaces
3. What is the range of values shown for the vty lines? The vty lines are configured in two ranges: 0 to 4 and 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”? The switch responds with “**startup-config is not present**” when you use the `show startup-config` command because the running configuration has **not been saved to NVRAM**. The running-config is the configuration currently in use, stored in RAM. Unless a network administrator explicitly saves it with the `copy running-config startup-config` command, it won't be in NVRAM. Therefore, if the switch were to lose power, it would boot up with its default configuration, not the one shown in the running-config.

Part 2: Create a Basic Switch Configuration

Step 1: Assign a name to a switch.

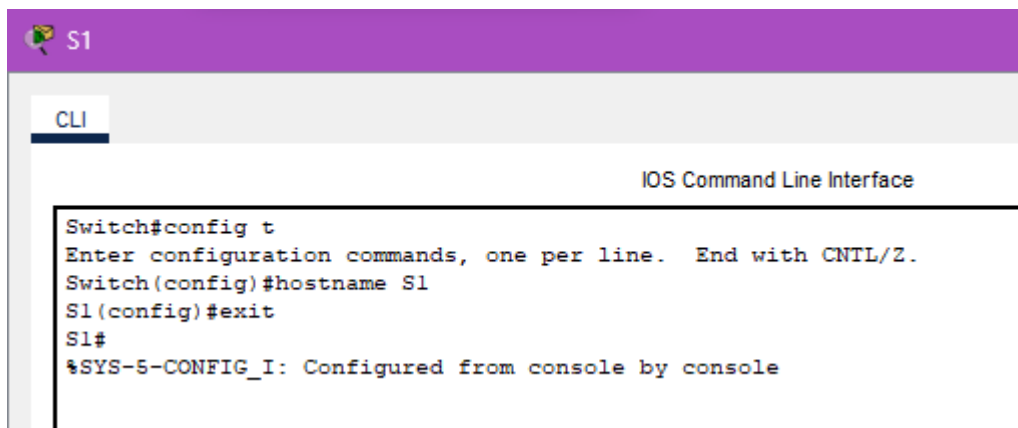
To configure parameters on a switch, you may be required to move between various configuration modes. Notice how the prompt changes as you navigate through the switch.

```
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#

Question: Why is the **login** command required? The **login** command is required because it **activates the password checking** for that specific line. Without the login command, the password letmein command is just an entry in the configuration, but it's not being enforced.

```
S1>en
S1#config t
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
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

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.

```
User Access Verification

Password:

S1>
```

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
```

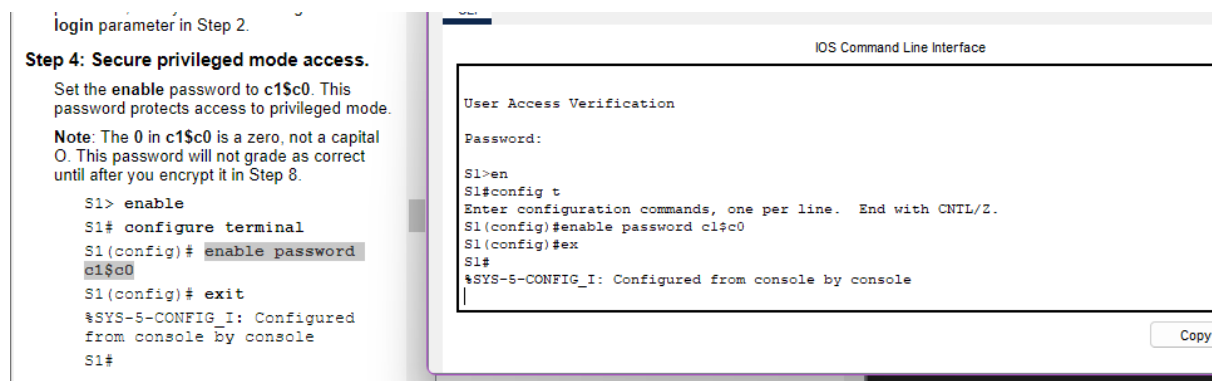
```
S1# configure terminal
```

```
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.

- Enter the **exit** command again to log out of the switch.
- Press **<Enter>** and you will now be asked for a password:

User Access Verification

Password:

- The first password is the console password you configured for **line con 0**. Enter this password to return to user EXEC mode.
- Enter the command to access privileged mode.
- Enter the second password you configured to protect privileged EXEC mode.
- Verify your configuration by examining the contents of the running-configuration file:

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

Cisco Packet Tracer - C:\Users\Myline\Downloads\2.5.5-P...

File Edit Options View Tools Extensions Window

Logical Physical x: 388, y: 435

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

me Elapsed: 01:12:59 Completion: 18%

Dock Check Results Back 1/1 Next

Time: 01:12:08

4331 4321 1941

CLI

IOS Command Line Interface

```

User Access Verification

Password:

S1>en
Password:
S1#show running-config
Building configuration...

Current configuration : 1131 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
!
enable password c1$c0
!
!
!
!
!
!
spanning-tree mode puvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!

```

[illegible]

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)# 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.

The screenshot shows a Cisco IOS Command Line Interface (CLI) window. On the left, there is a sidebar with a document icon and text explaining the security risk of passwords in plain text and the purpose of the 'enable secret' command. The main window displays the CLI session where the user enters 'enable secret itsasecret' and then 'exit'. The output shows the configuration is saved to the configuration file. Below the CLI window, there are 'Copy' and 'Paste' buttons.

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.

CLI

IOS Command Line Interface

```
!
!
end

S1#
S1#
S1#
S1#
S1#
S1#
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#enable secret itsasecret
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Copy Paste

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**

Questions:

What is displayed for the enable secret password?

enable secret 5 \$1\$mERr\$ILwq/b7kc.7X/ejA4Aosn0

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

The enable secret password is displayed differently because it is **encrypted using a strong, one-way cryptographic hash function**. The 5 in the output indicates that it's using the **SHA-1** algorithm, which is a much more secure method than the older, unencrypted enable password command. This hashing process converts the password you entered into an irreversible scrambled string. It's designed this way so that if someone gains access to the configuration file, they cannot simply read the password in plain text. This is a crucial security measure to protect against unauthorized access.

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?

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

CLI

IOS Command Line Interface

```
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
enable secret 5 $1$mERr$ILWq/b7kc.7X/ejA4Aosn0
enable password c1$c0
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
```

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**

Question: 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.

They will be displayed in **encrypted form**. The service password-encryption command automatically applies a weak encryption to any new plaintext passwords you configure after it's been enabled.

The command works as a global setting. Once you run service password-encryption, it affects all future passwords you create that would normally be saved in plain text, such as password, line, and VTY passwords. It **does not affect** the enable secret password, which is already encrypted with a much stronger algorithm. While this encryption is a weak, easily reversible type, it's a basic security step to prevent someone from viewing your passwords by simply looking at the configuration file.

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.

IOS Command Line Interface

```
!
end

S1#
S1#
S1#
S1#
S1#
S1#
S1#
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#service password-encryption
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

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!"
```

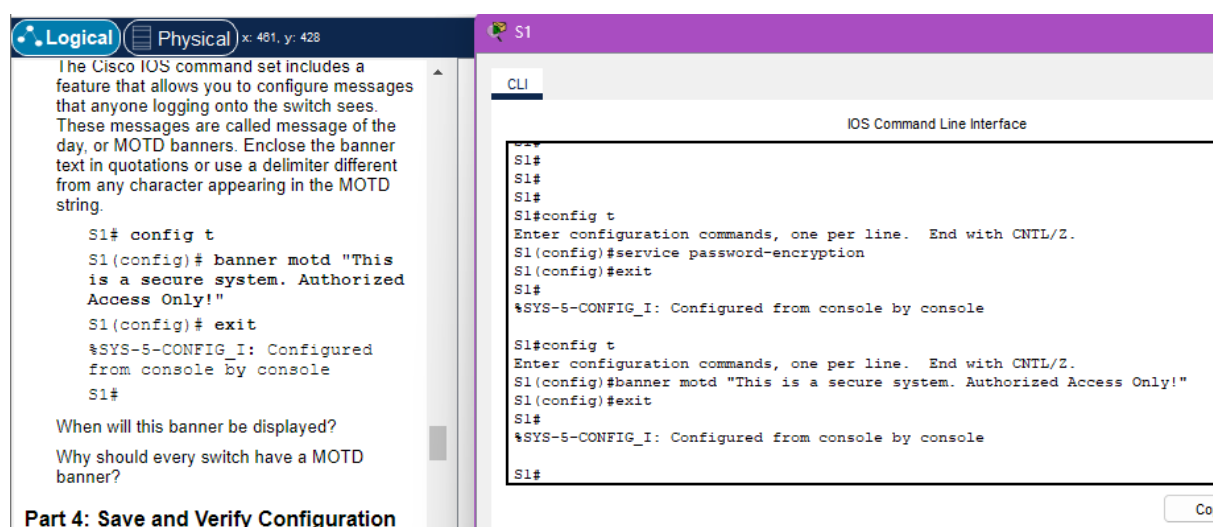
```
S1(config)# exit
```

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

```
S1#
```

Questions:

1. When will this banner be displayed? **The MOTD banner will be displayed before a user logs in to the switch. It appears right after the "Press RETURN to get started" prompt and before any password or login prompts.**
2. Why should every switch have a MOTD banner? **Every switch should have a MOTD banner because it's a legal warning to unauthorized users. A MOTD banner serves as a clear notice that the device is a private, secure system and that only authorized personnel should attempt to access it. Without a banner, it can be more difficult to prosecute unauthorized access. It acts as a digital "No Trespassing" sign, helping to protect the organization legally by establishing that any unauthorized access is a deliberate violation.**



The screenshot displays the Cisco Packet Tracer interface. On the left, the 'Logical' view shows a text box with the following content:

```
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#
```

Below the text box, two questions are listed:

- When will this banner be displayed?
- Why should every switch have a MOTD banner?

At the bottom of the left pane, the text 'Part 4: Save and Verify Configuration' is visible.

On the right, the 'CLI' view shows the command-line interface for switch S1. The output is as follows:

```
S1#
S1#
S1#
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#service password-encryption
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#banner motd "This is a secure system. Authorized Access Only!"
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

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]
```

Questions:

1. What is the shortest, abbreviated version of the **copy running-config startup-config** command? **copy run start**

Examine the startup configuration file.

2. Which command will display the contents of NVRAM? **show startup-config (or its abbreviation, show start).**
3. Are all the changes that were entered recorded in the file? **Yes, all the changes that were entered are recorded in the startup configuration file. This is because the copy running-config startup-config command explicitly saves the current, active configuration (running-config) to the non-volatile memory (NVRAM), where it becomes the startup configuration. The [OK] message confirms the successful transfer. This ensures that any changes, like hostname, passwords, and banners, will be preserved even if the switch is rebooted or loses power.**

The screenshot shows a Cisco Packet Tracer interface. On the left, the 'Logical' tab is active, displaying the lab instructions for Step 1. The instructions include a paragraph about saving the configuration file, followed by the commands `S1# copy running-config startup-config`, `Destination filename [startup-config]?[Enter]`, `Building configuration...`, and `[OK]`. Below this, three questions are listed, corresponding to the ones in the text above. At the bottom of the left pane, there is a 'Time Elapsed' of 01:37:01, a 'Completion' of 50%, and buttons for 'Dock', 'Check Results', 'Back', '1/1', and 'Next'.

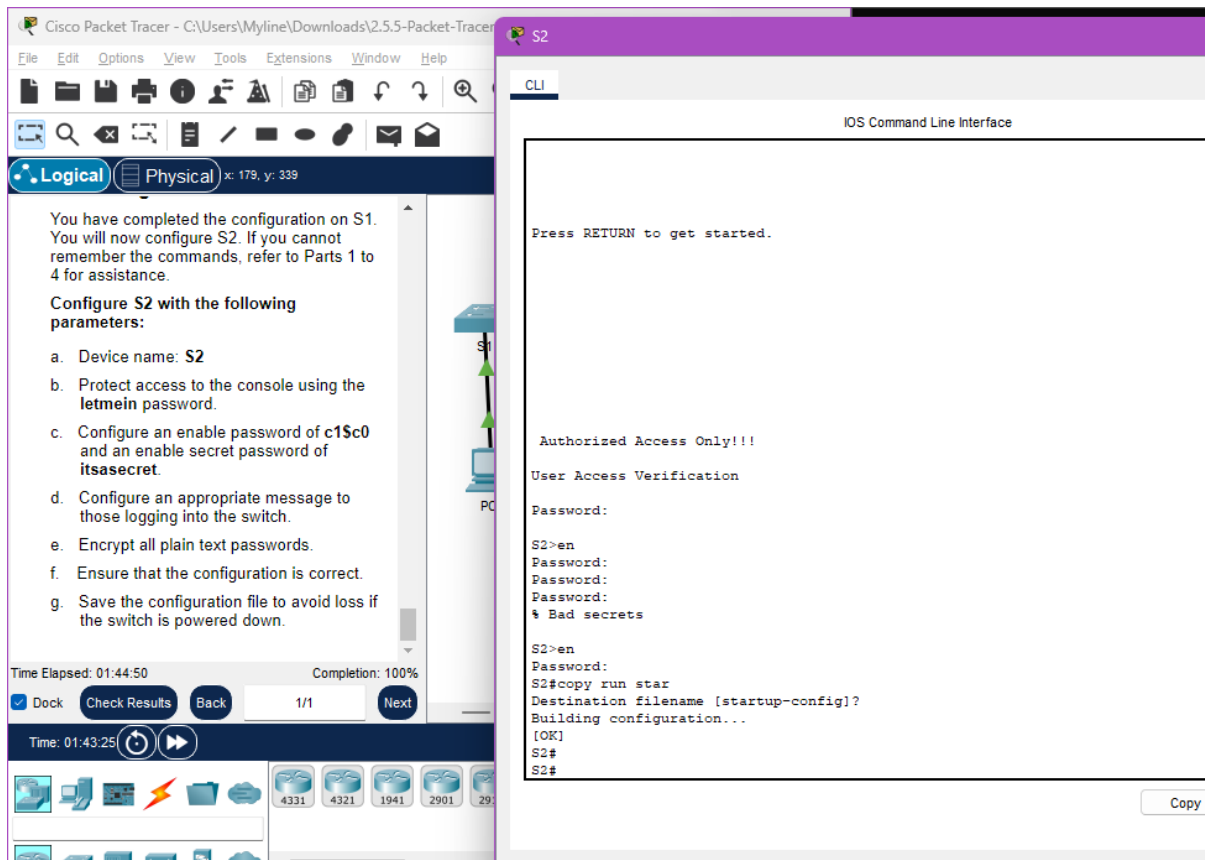
On the right, the 'Physical' tab is active, showing a switch labeled 'S1'. The 'CLI' window for S1 is open, displaying the 'IOS Command Line Interface'. The commands entered in the CLI are: `Enter configuration commands, one per line. End with CNTL/Z.`, `S1(config)#service password-encryption`, `S1(config)#exit`, `S1#`, `*SYS-5-CONFIG_I: Configured from console by console`, `S1#config t`, `Enter configuration commands, one per line. End with CNTL/Z.`, `S1(config)#banner motd "This is a secure system. Authorized Access Only!"`, `S1(config)#exit`, `S1#`, `*SYS-5-CONFIG_I: Configured from console by console`, `S1#copy running-config startup-config`, `Destination filename [startup-config]?`, `Building configuration...`, `[OK]`, and `S1#`. A 'Copy' button is visible at the bottom right of the CLI window.

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:

- Device name: **S2**
- Protect access to the console using the **letmein** password.
- Configure an enable password of **c1\$c0** and an enable secret password of **itsasecret**.
- Configure an appropriate message to those logging into the switch.
- Encrypt all plain text passwords.
- Ensure that the configuration is correct.
- Save the configuration file to avoid loss if the switch is powered down.



File Edit Options View Tools Extensions Window Help

Logical Physical

x & y: 323

Building configuration...
[OK]

What is the shortest, abbreviated version of the **copy running-config startup-config** command?

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:

- Device name: **S2**
- Protect access to the console using the **letmein** password.
- Configure an enable password of **c15c0** and an enable secret password of **itsasecret**.
- Configure an appropriate message to those logging into the switch.
- Encrypt all plain text passwords.
- Ensure that the configuration is correct.
- Save the configuration file to avoid loss if the switch is powered down.

Time Elapsed: 02:05:14
Completion: 100%

Dock Check Results

Back 1/1 Next

Root

Activity Results

Congratulations Guest! You completed the activity.

Overall Feedback **Assessment Items** Connectivity Tests

Expand/Collapse All Show Incorrect Items

| Assessment Items | Status | Points | Component(s) | Feedback |
|-----------------------------|---------|--------|---------------------|----------|
| Network | | | | |
| S1 | | | | |
| Banner MOTD | Correct | 6 | Basic Security C... | |
| Console Line | | | | |
| Login | Correct | 4 | Basic Security C... | |
| Password | Correct | 4 | Basic Security C... | |
| Enable Password | Correct | 4 | Basic Security C... | |
| Enable Secret | Correct | 4 | Basic Security C... | |
| Host Name | Correct | 5 | Hostname Config... | |
| Service Password Encryption | Correct | 4 | Basic Security C... | |
| Startup Config | Correct | 5 | Configuration Ma... | |
| S2 | | | | |
| Banner MOTD | Correct | 6 | Basic Security C... | |
| Console Line | | | | |
| Login | Correct | 4 | Basic Security C... | |
| Password | Correct | 4 | Basic Security C... | |
| Enable Password | Correct | 4 | Basic Security C... | |
| Enable Secret | Correct | 4 | Basic Security C... | |
| Host Name | Correct | 5 | Hostname Config... | |
| Service Password Encryption | Correct | 4 | Basic Security C... | |
| Startup Config | Correct | 5 | Configuration Ma... | |

Score : 72/72

Item Count : 16/16

| Component | Items/Total | Score |
|------------------------------|-------------|-------|
| Basic Security Configuration | 12/12 | 52/52 |
| Configuration Management | 2/2 | 10/10 |
| Hostname Configuration | 2/2 | 10/10 |