**Part 1 solutions**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer code

Description automatically generated

Step 2

b) - 12

- 2

- 0-4

- show startup-config

- there is no configuration saved in the **NVRAM**.

A white background with black text

Description automatically generated

**Part 2**

Step 1

A white screen with black text

Description automatically generated

Step 2

The **login** command is required on a Cisco device to enable user authentication when accessing the device via the console, VTY (virtual terminal lines for remote access), or auxiliary lines. It ensures that when someone attempts to access the device, they are prompted to enter a password before gaining access. Without the login command, even if a password is set, the device will not prompt for it, essentially allowing anyone to access the device without authentication.

Step3

A screenshot of a computer

Description automatically generated

Step 4

A black text on a white background

Description automatically generated

Step 5



A screenshot of a computer

Description automatically generated



A white background with black text

Description automatically generated

Remaining output of above image can be seen in part 1 solutions

A white background with black text

Description automatically generated

Step 6

A close-up of a white background

Description automatically generated

Step 7

A computer code on a white background

Description automatically generated

Remaining output of above image can be seen in part 1 solutions

b) enable secret is displayed as this:



c) The **enable secret** password is displayed differently from what you configured because it is **hashed** for security purposes. When you configure the enable secret password, the Cisco device hashes the password using the MD5 (Message Digest 5) algorithm before storing it. This ensures that the password is not stored or displayed in plain text, protecting it from unauthorized access.

Step 8

A white background with black text

Description automatically generated

After enabling the **service password-encryption** command, **any additional passwords configured on the switch will be displayed in encrypted form** in the configuration file. This happens because the service password-encryption command globally enables Type 7 encryption for all plain-text passwords.

**Part 3**

A close-up of a computer screen

Description automatically generated

The banner will be displayed **every time someone attempts to access the switch**, whether through console, Telnet, or SSH. The banner appears before the login prompt, warning users before they enter any credentials.

Every switch should have an MOTD banner to reinforce security policies and provide necessary legal warnings about unauthorized access.

**Part 4**

Step 1

A computer screen shot of a white screen

Description automatically generated

Remaining output of above image can be seen in part 1 solutions

A screenshot of a computer

Description automatically generated

Step 2

A white background with black text

Description automatically generated

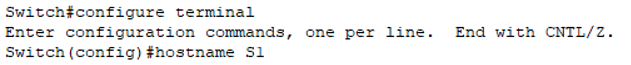
copy r s

Step 3

* **show startup-config** will display the contents of NVRAM
* Only changes that have been saved to the startup configuration will be recorded in the file; unsaved changes will be lost upon reboot.

**Part 5**

a)



Hostname will be named S2 instead

b) S1 replaced by S2

A white background with black text

Description automatically generated

c)

A screen shot of a computer error

Description automatically generated

A close-up of a computer screen

Description automatically generated

d) and e)

A close-up of a computer error

Description automatically generated

f) configuration is correct

g)

A computer screen shot of a computer code

Description automatically generated