.ıl¡.ı|ı. NETWORKING
CISCO. Academy

Christian Dunn CST 329 03A Code: 127 I received assistance from contenthub.netacad.com and itexamanswers.net on my some of my written answers but wrote all answers in my own words.

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.

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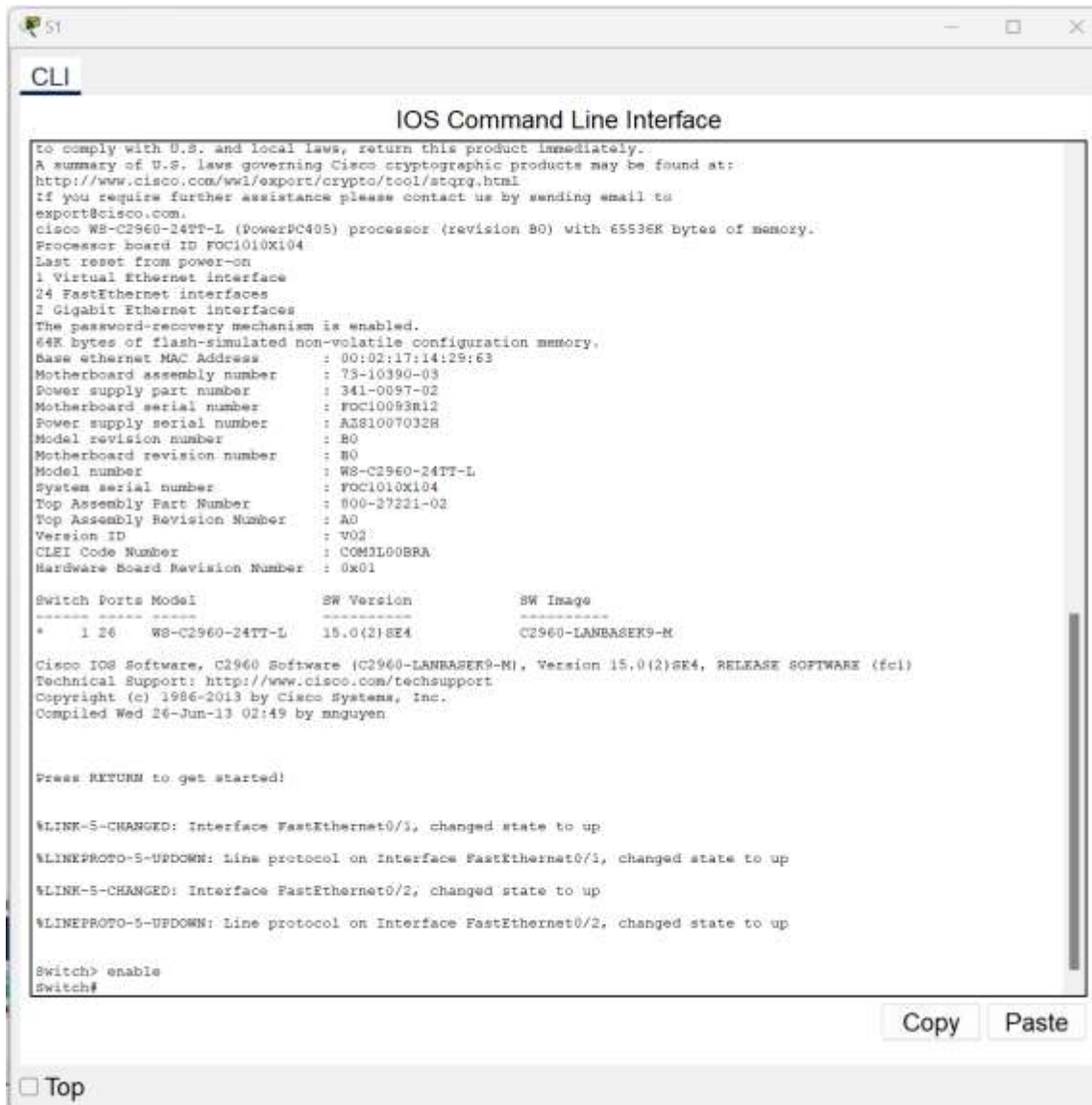
The privileged EXEC command set includes the commands available in user EXEC mode, many additional commands, and the **configure** command through which access to the configuration modes is gained.

a.   Click S1 and then the CLI tab. Press Enter.

b.   Enter privileged EXEC mode by entering the enable command:

```
Switch> enable
Switch#
```

Notice that the prompt changed to reflect privileged EXEC mode.

```
to comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
export@cisco.com.
cisco WS-C2960-24TT-L (PowerPC405) processor (revision B0) with 65536K bytes of memory.
Processor board ID FOC1010X104
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:02:17:14:29:63
Motherboard assembly number     : 73-10390-03
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC10093R12
Power supply serial number      : AZS1007032H
Model revision number           : B0
Motherboard revision number     : B0
Model number                    : WS-C2960-24TT-L
System serial number            : FOC1010X104
Top Assembly Part Number        : 800-27221-02
Top Assembly Revision Number    : A0
Version ID                      : V02
CLEI Code Number                : COM3L00BRA
Hardware Board Revision Number  : 0x01

Switch Ports Model          SW Version        SW Image
------ ----- -----          ----------        ----------
*    1 26    WS-C2960-24TT-L 15.0(2)SE4        C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen



Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up


Switch> enable
Switch#
```

Step 2: Examine the current switch configuration.

Enter the show running-config command.

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

Answer the following questions:

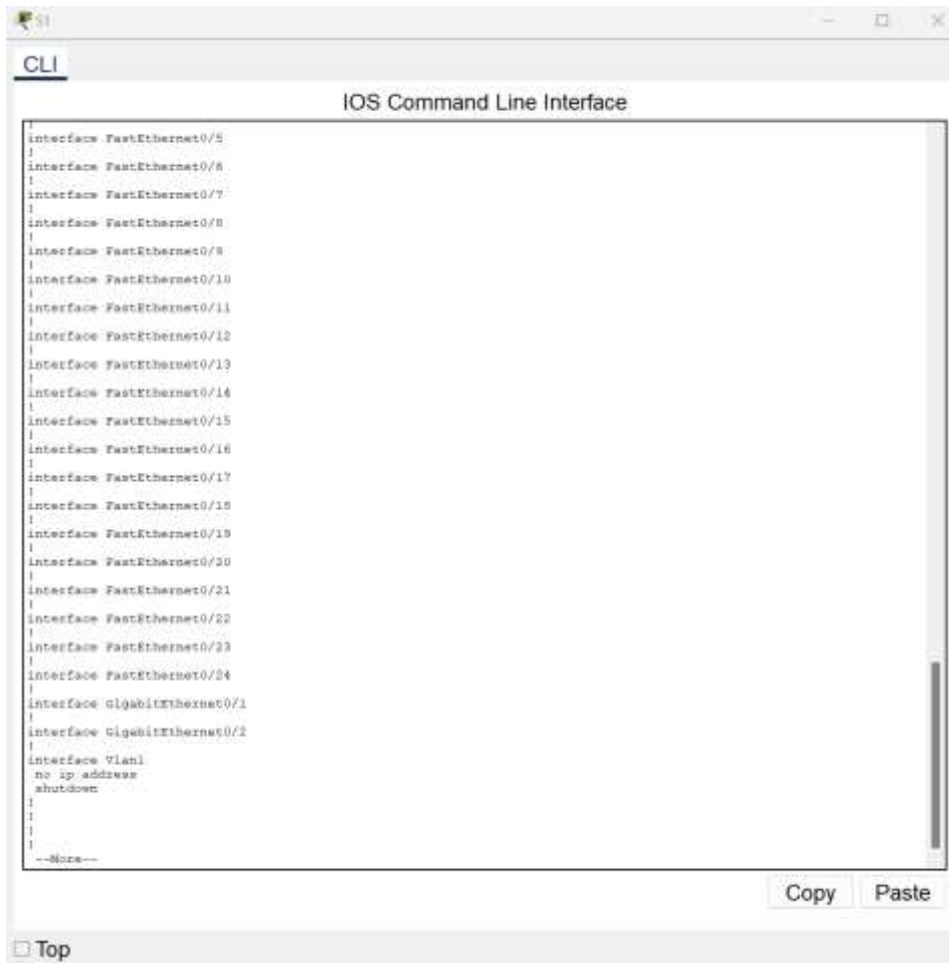How many Fast Ethernet interfaces does the switch have?

24

How many Gigabit Ethernet interfaces does the switch have?

2

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

16

```
line vty 0 4
 login
line vty 5 15
 login
```

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

show startup- configuration

```
Switch# show star
Switch# show startup-config
startup-config is not present
Switch#
```

Why does the switch respond with "startup-config is not present?"

It does not show because it was not saved

```
[OK]
Switch# show startup-config
Using 1086 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
```

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#

```
Switch#  configure ter
Switch#  configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# hostname S1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

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?

In order to secure the console and be able to get back in and make changes.

```
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
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

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.

```
S1 con0 is now available




Press RETURN to get started.








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#

S1> enable
S1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# enable password c1$c0
S1(config)# exit
S1#
%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.

```
User Access Verification

Password:
Password:

S1> enable
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 pvst
spanning-tree extend system-id
!
 --More--
```

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.

```
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

S1#
```

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
```

```
S1# show run
Building configuration...

Current configuration : 1178 bytes
!
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

S1#
```

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?

The enable secret password seems to have been encrypted, leaving the enable password as we originally set it.

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

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#
```

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.

The service password-encryption script ensures that all passwords will be encrypted.

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#
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#
```

When will this banner be displayed?

The MOTD will be displayed whenever someone access the switch.

Why should every switch have a MOTD banner?

It is a good way to relay messages to people accessing the network and to specifically inform personnel when access is secure.

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]
```

```
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

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

copy run start

```
S1# copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Examine the startup configuration file.

Which command will display the contents of NVRAM?

After saving show startup-configuration will now display the contents.

```
S1# show start
Using 1258 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname S1
!
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password 7 08221D0A0A49
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 --More--
```

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**

```
Switch(config)#hostname S2
S2(config)#line console 0
```

b. Protect access to the console using the **letmein** password.

```
S2(config-line)#password letmein
S2(config-line)#login
```

c. Configure an enable password of **c1$c0** and an enable secret password of **itsasecret**.

```
S2(config-line)#enable password c1$c0
S2(config)# enable secret itsasecret
```

d. Configure an appropriate message to those logging into the switch.

```
S2(config)#banner motd "This is a secure sysytem. Authorized Access Only!"
```

e. Encrypt all plain text passwords.

```
S2(config)#service password-encryption
```

f. Ensure that the configuration is correct.

```
S2# show start
Using 1259 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
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 --More--
```

g. Save the configuration file to avoid loss if the switch is powered down.

```
S2(config)# do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
```