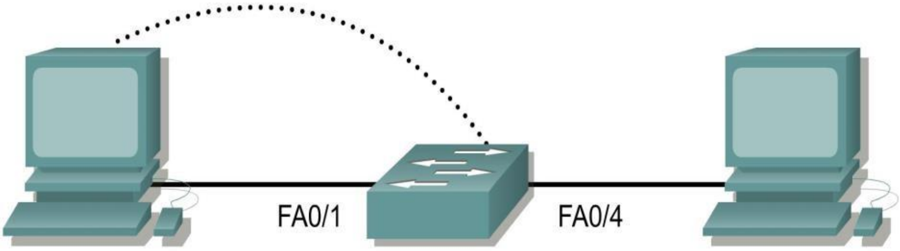
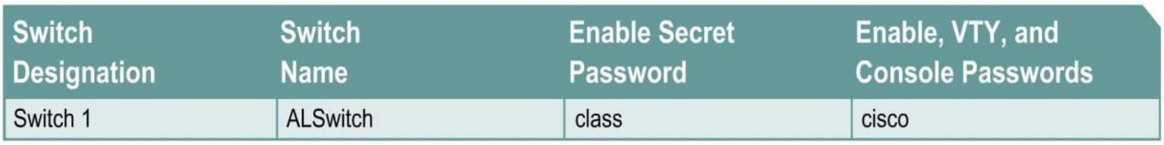
Lab 2a Basic Switch Configuration

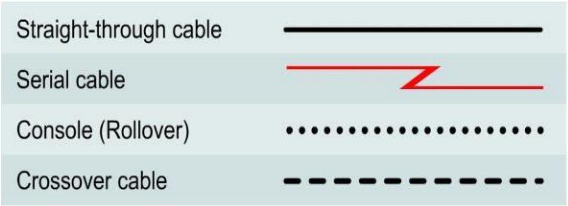
Objective

- Configure a switch with a name and an IP address.
- Configure passwords to ensure that access to the CLI is secured.
- Configure switch port speed and duplex properties for an interface.
- Save the active configuration.
- View the switch browser interface.





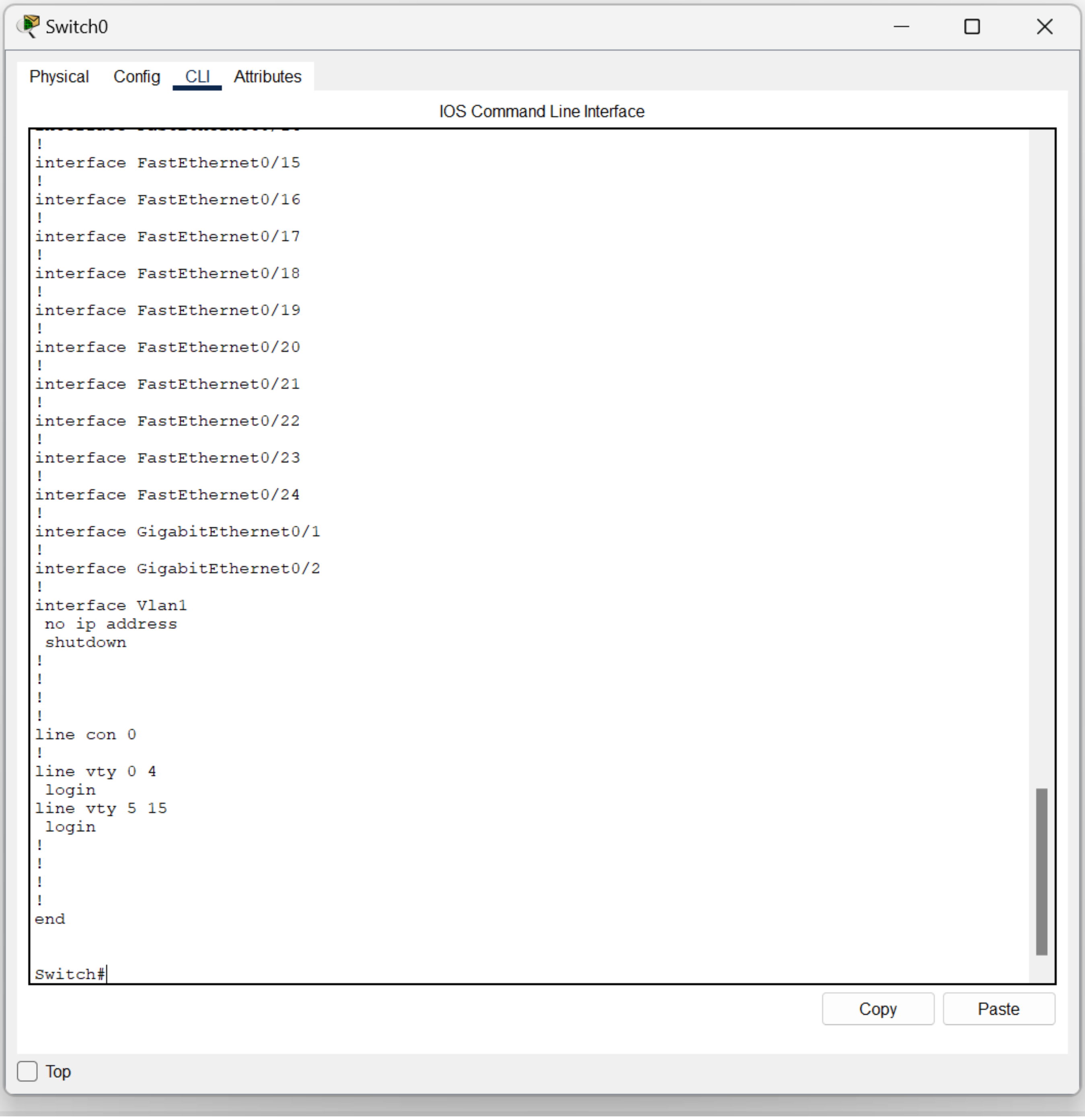
Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, and Console Passwords
Switch 1	ALSwitch	class	cisco



Straight-through cable	────
Serial cable	⚡
Console (Rollover)	••••••
Crossover cable	- - - -

Preparation

Cable a network similar to the one in the diagram. The configuration output used in this lab is for a 2950 series switch.



```
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end


Switch#
```

Step 1 Enter privileged mode

a. Privileged mode gives access to all the switch commands. Many of the privileged commands configure operating parameters. Therefore, privileged access should be password-protected to prevent unauthorized use. The privileged command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes is gained.

Switch>**enable**

Switch#

b. Notice the prompt changed in the configuration to reflect privileged EXEC mode.

Step 2 Examine the current switch configuration

a. Examine the following current running configuration file:

Switch#**show running-config**

b. How many Ethernet or Fast Ethernet interfaces does the switch have? 24

____

c. What is the range of values shown for the VTY lines? 0-4 5-15

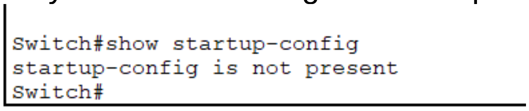
____

d. Examine the current contents of NVRAM as follows:

Switch#**show startup-config**

%% Non-volatile configuration memory is not present

e. Why does the switch give this response? Not present(Faulty NVRAM or corrupted)



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

Step 3 Assign a name to the switch

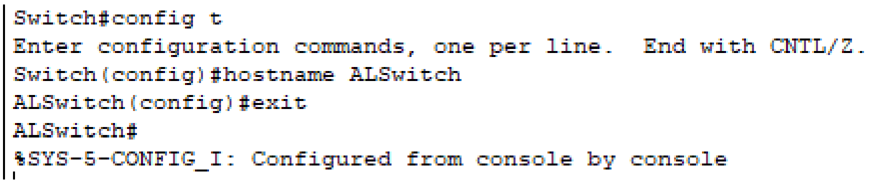
a. Enter **enable** and then the configuration mode. The configuration mode allows the management of the switch. Enter **ALSwitch**, the name this switch will be referred to in the following:

Switch#**configure terminal**

Enter the configuration commands, one for each line. End by pressing **Ctrl-Z**.

Switch(config)#**hostname ALSwitch**

ALSwitch(config)#**exit**



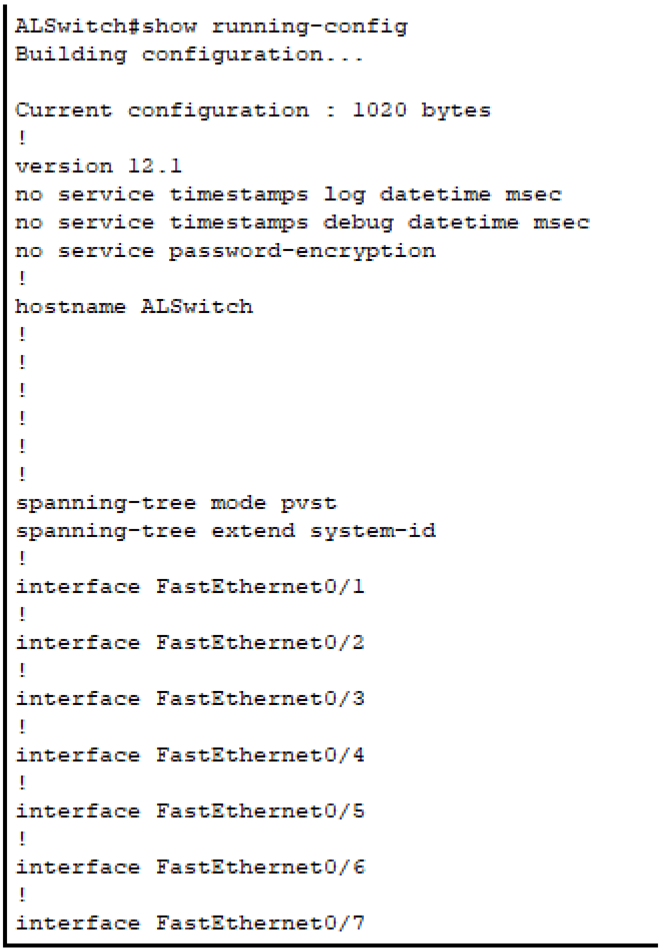
```
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname ALSwitch
ALSwitch(config)#exit
ALSwitch#
%SYS-5-CONFIG_I: Configured from console by console
```

b. Notice the prompt changed in the configuration to reflect its new name. Type **exit** or press **Ctrl-Z** to go back into privileged mode.

Step 4 Examine the current running configuration

a. Exam the current configuration that follows to verify that there is no configuration except for the hostname:

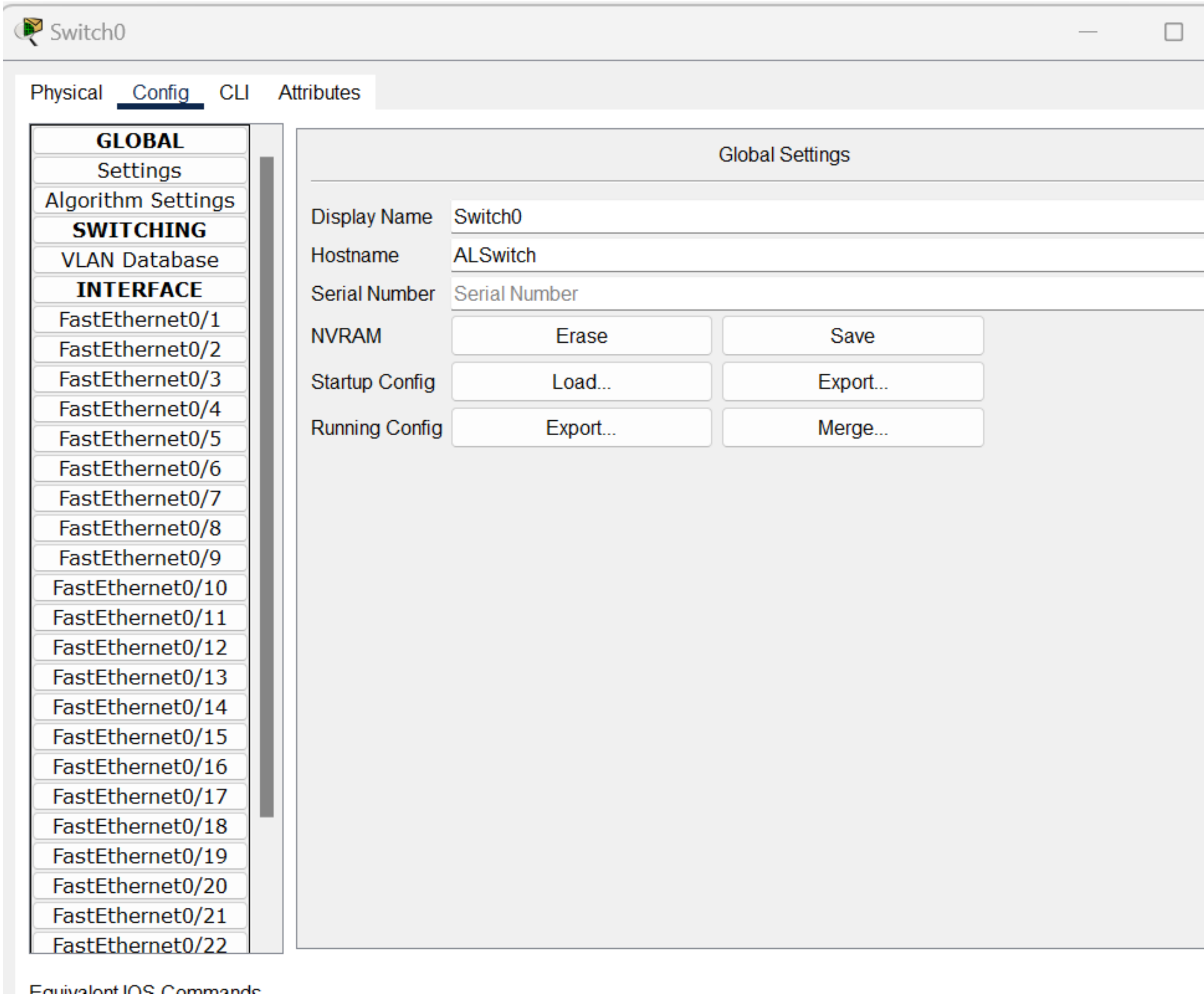
ALSwitch#**show running-config**



```
ALSwitch#show running-config
Building configuration...

Current configuration : 1020 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ALSwitch
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
```

b. Are there any passwords set on the lines? no

c. What does the configuration show as the hostname of this switch? ALSwitch



Global Settings

Display Name: Switch0

Hostname: ALSwitch

Serial Number: Serial Number

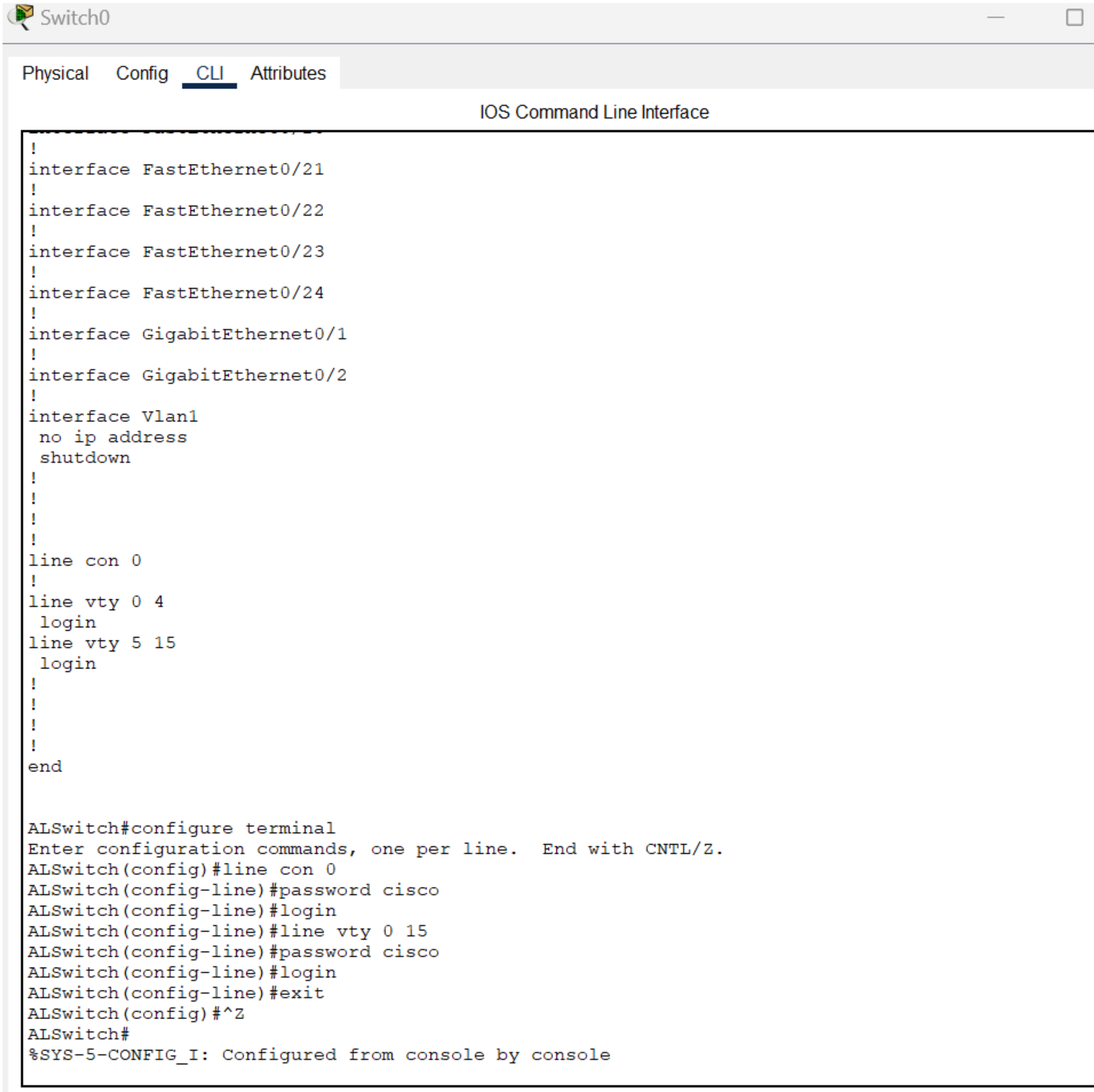
Step 5 Set the access passwords

Enter config-line mode for the console. Set the password on this line as **cisco** for login. Configure the vty lines 0 to 15 with the password cisco as follows:

```
ALSwitch#configure terminal
```

Enter the configuration commands, one for each line. End by pressing **Ctrl-Z**.

```
ALSwitch(config)#line con 0

ALSwitch(config-line)#password cisco

ALSwitch(config-line)#login

ALSwitch(config-line)#line vty 0 15

ALSwitch(config-line)#password cisco

ALSwitch(config-line)#login

ALSwitch(config-line)#exit
```



```
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end


ALSwitch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALSwitch(config)#line con 0
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#login
ALSwitch(config-line)#line vty 0 15
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#login
ALSwitch(config-line)#exit
ALSwitch(config)#^Z
ALSwitch#
%SYS-5-CONFIG_I: Configured from console by console
```

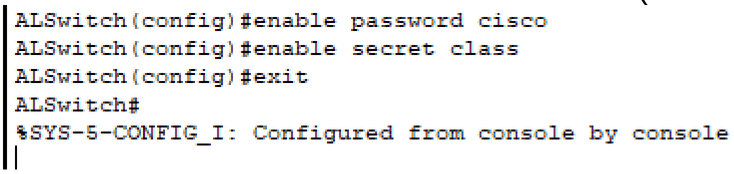
Step 6 Set the command mode passwords

a. Set the **enable password** to cisco and the **enable secret password** to **class** as follows:

ALSwitch(config)#**enable password cisco**
ALSwitch(config)#**enable secret class**

ALSwitch(config)#**exit**

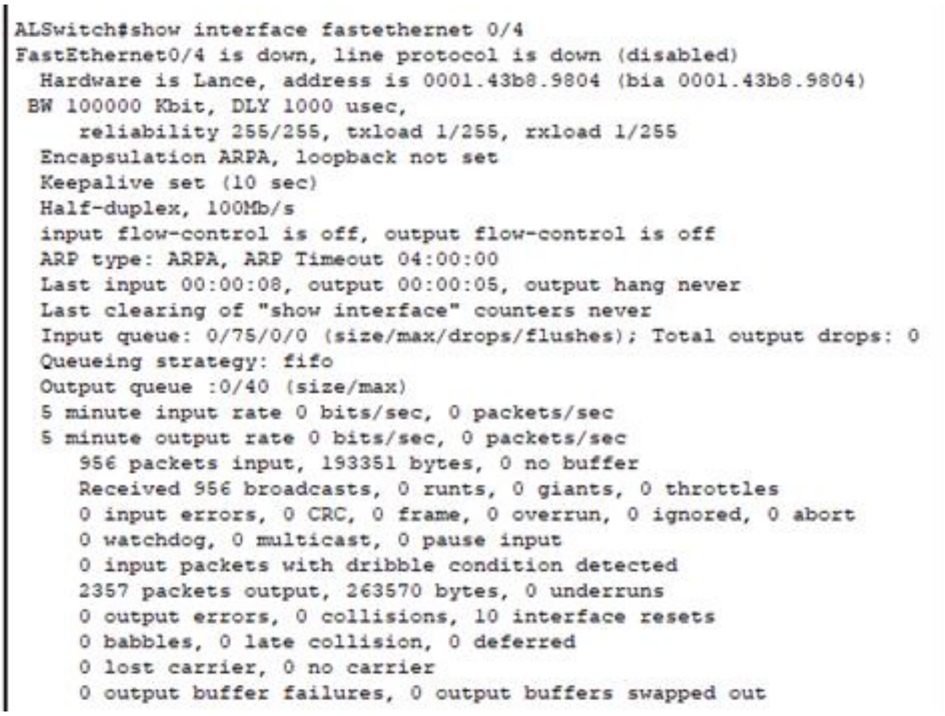
ALSwitch #**show interface fastethernet 0/4** (Note: this can be a trunk or access port)



```
ALSwitch(config)#enable password cisco
ALSwitch(config)#enable secret class
ALSwitch(config)#exit
ALSwitch#
%SYS-5-CONFIG_I: Configured from console by console
```

Or

ALSwitch #**show interface gigabitethernet 0/1** (Note: this can be a trunk or access port)



```
ALSwitch#show interface fastethernet 0/4
FastEthernet0/4 is down, line protocol is down (disabled)
  Hardware is Lance, address is 0001.43b8.9804 (bia 0001.43b8.9804)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Half-duplex, 100Mb/s
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
     0 output errors, 0 collisions, 10 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

b. Which password takes precedence, the enable password or enable secret password?
Enable Password over secret

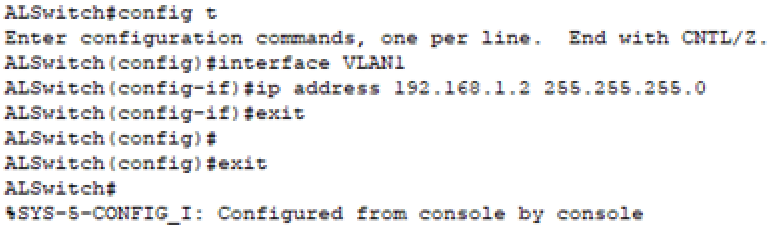
____

Step 7 Configure the layer 3 access to the switch

a. Set the IP address of the switch to 192.168.1.2 with a subnet mask of 255.255.255.0 as follows:

Note: This is done on the internal virtual interface VLAN 1.

ALSwitch(config)#**interface VLAN 1**
ALSwitch(config-if)#**ip address 192.168.1.2 255.255.255.0**
ALSwitch(config-if)#**exit**

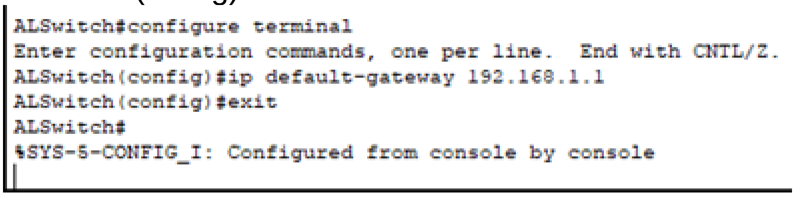


```
ALSwitch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ALSwitch(config)#interface VLAN1
ALSwitch(config-if)#ip address 192.168.1.2 255.255.255.0
ALSwitch(config-if)#exit
ALSwitch(config)#
ALSwitch(config)#exit
ALSwitch#
%SYS-5-CONFIG_I: Configured from console by console
```

b. Set the default gateway for the switch and the default management VLAN to 192.168.1.1 as follows:

ALSwitch(config)#**ip default-gateway 192.168.1.1**

ALSwitch(config)#**exit**

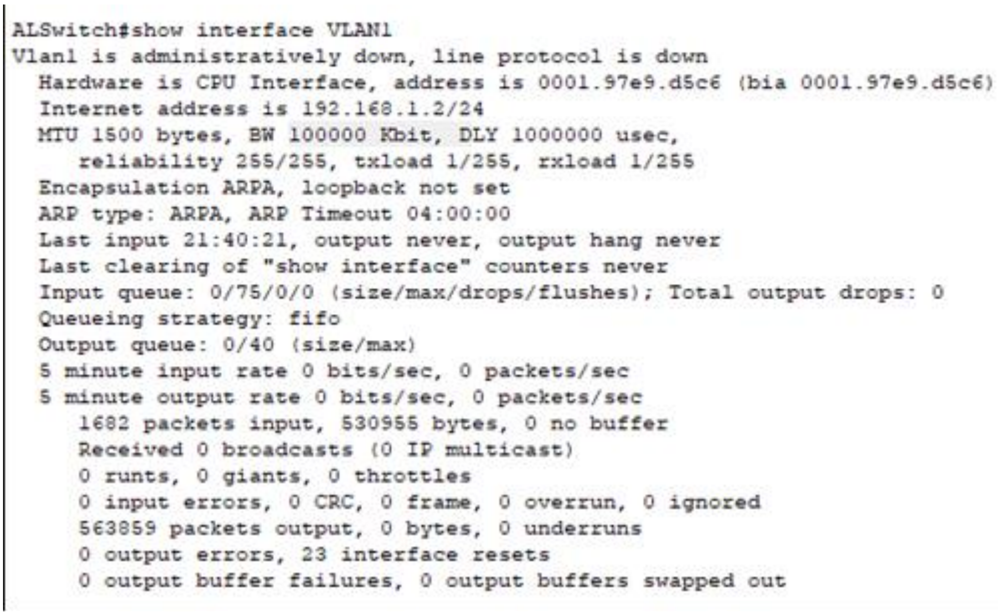


```
ALSwitch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ALSwitch(config)#ip default-gateway 192.168.1.1
ALSwitch(config)#exit
ALSwitch#
%SYS-5-CONFIG_I: Configured from console by console
```

Step 8 Verify the management LANs settings

a. Verify the interface settings on VLAN 1 as follows:

ALSwitch#**show interface VLAN 1**



```
ALSwitch#show interface VLAN1
Vlan1 is administratively down, line protocol is down
  Hardware is CPU Interface, address is 0001.97e9.d5c6 (bia 0001.97e9.d5c6)
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

b. What is the bandwidth on this interface?100000 kbit ______________________

c. What are the VLAN states: VLAN1 is administratively down ____, Line protocol is down ______

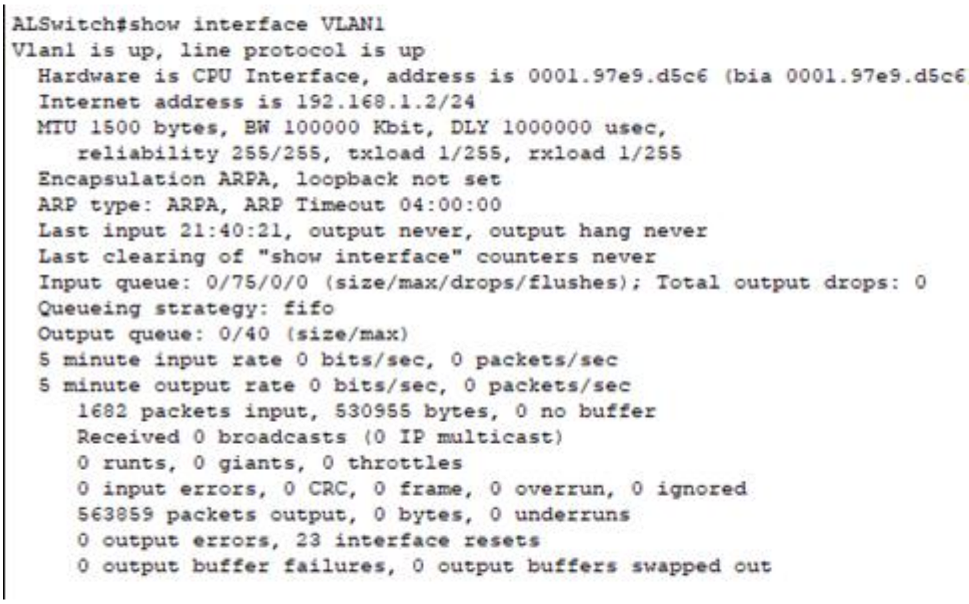
d. Enable the virtual interface using the **no shutdown** command

ALSwitch#**configure terminal**

ALSwitch(config)#**interface VLAN 1**

ALSwitch(config-if)#**no shutdown**

ALSwitch(config-if)#**exit**



```
ALSwitch#show interface VLAN1
Vlan1 is up, line protocol is up
  Hardware is CPU Interface, address is 0001.97e9.d5c6 (bia 0001.97e9.d5c6
  Internet address is 192.168.1.2/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 21:40:21, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1682 packets input, 530955 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     563859 packets output, 0 bytes, 0 underruns
     0 output errors, 23 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

e. What is the queuing strategy? FIFO___________________________________

Step 9 Save the configuration

a. The basic configuration of the switch has just been completed. Back up the running configuration file to NVRAM as follows:

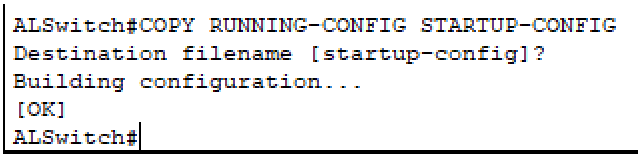
Note: This will ensure that the changes made will not be lost if the system is rebooted or loses power.

ALSwitch#**copy running-config startup-config**

Destination filename [startup-config]?[**Enter**]

Building configuration... [OK]

ALSwitch#



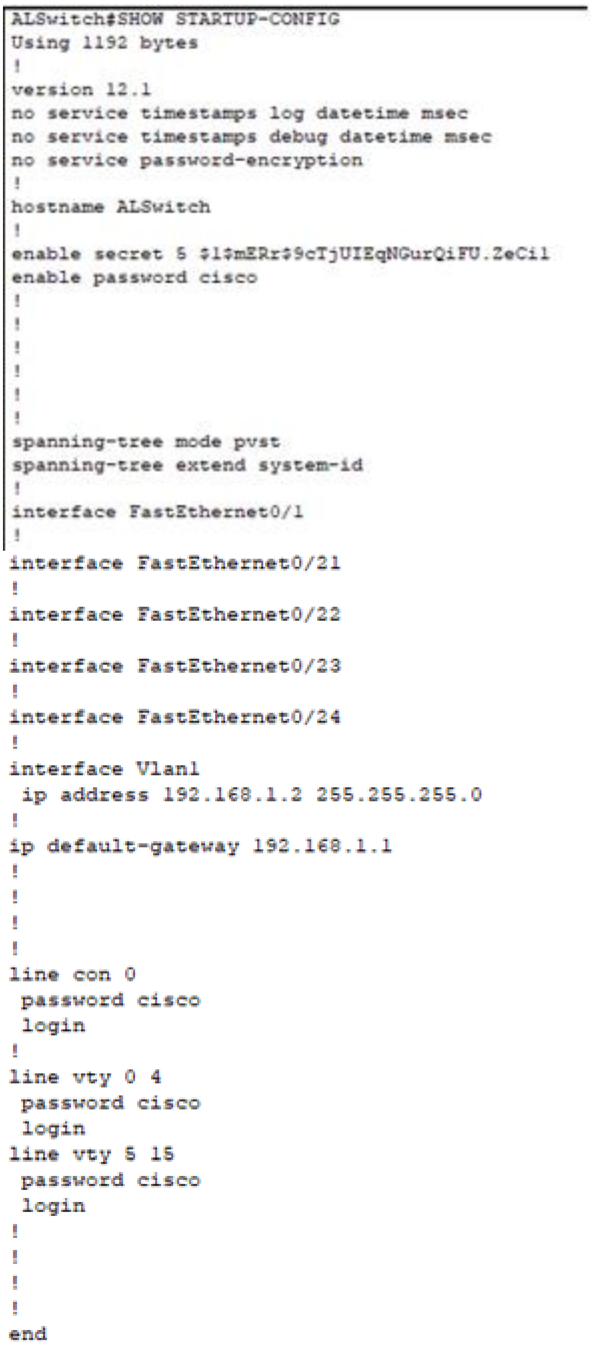
```
ALSwitch#COPY RUNNING-CONFIG STARTUP-CONFIG
Destination filename [startup-config]?
Building configuration...
[OK]
ALSwitch#
```

b. Configuration upload is successfully completed.

Step 10 Examine the startup configuration file

a. To see the configuration that is stored in NVRAM, type **show startup-config** from the privileged EXEC (enable mode).

ALSwitch#**show startup-config**



```
ALSwitch#SHOW STARTUP-CONFIG
Using 1192 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ALSwitch
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
enable password cisco
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
ip default-gateway 192.168.1.1
!
!
!
!
line con 0
 password cisco
 login
!
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
!
!
!
end
```

b. What is displayed? C.____

c. Are all the changes that were entered recorded in the file? Yes all are perfect________________

Step 11 Exit the switch

Logoff the switch by typing **exit** as follows: ALSwitch#**exit**

Once these steps are completed, logoff by typing **exit**, and turn all the devices off.

Step 12

Once you have completed the configurations, do the following steps: i) add two more PCs, ii) ping between PCs, iii) trace route between PCs, and iv) telnet from one of the PC to the switch.

References:

CISCO Networking Academy Program: Switching Basics and Intermediate Routing v 3.1

Lab 2b - Switch configuration

Objectives

□ Perform an initial configuration of a Cisco 2960 switch.

Tasks

In this activity, you will connect 4 PCs to a Cisco Catalyst 2960 switch and you will configure the following settings on the Cisco Catalyst 2960.

□ Host name
□ Console password
□ vty password
□ Privileged EXEC mode password
□ Privileged EXEC mode secret

a) What additional feature does Cisco 2960 switch compared to Cisco 2950 switch?
Compared to the Cisco 2950 switch, the Cisco 2960 switch has more sophisticated security features including 802.1X, Layer 3 routing, and improved QoS (Quality of Service).

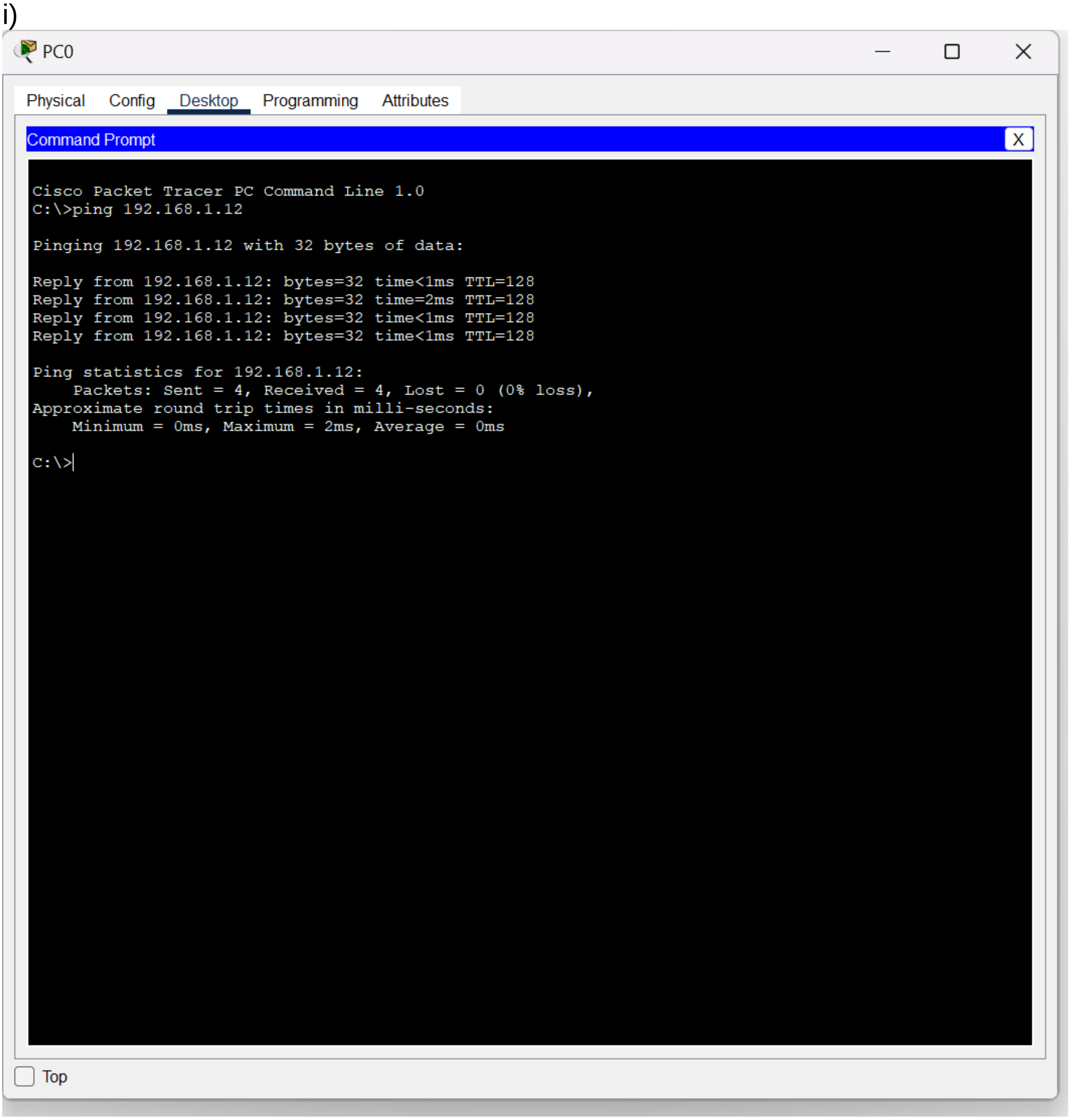
Once you have completed the configurations, do the following steps: i) ping between PCs, ii) trace route between PCs, and iii) telnet from one of the PC to theswitch.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname <2b>
<2b>(config)#line console 0
<2b>(config-line)#password 2b
<2b>(config-line)#login
<2b>(config-line)#exit
<2b>(config)#line vty 0 15
<2b>(config-line)#password 2b
<2b>(config-line)#login
<2b>(config-line)#exit
<2b>(config)#enable password 2b
<2b>(config)#enable secret 2b
The enable secret you have chosen is the same as your enable password.
This is not recommended. Re-enter the enable secret.
<2b>(config)#enable secret 2bb
<2b>(config)#write memory
^
% Invalid input detected at '^' marker.
<2b>(config)# write memory
^
% Invalid input detected at '^' marker.
<2b>(config)# exit
<2b>#
```

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

<2b># copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
<2b>#
```

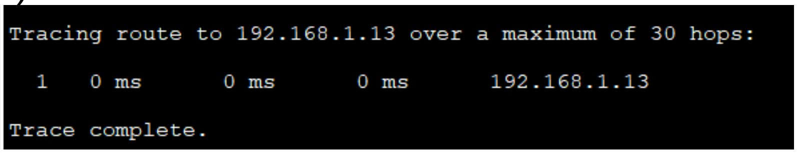
a) <2b>#

i)



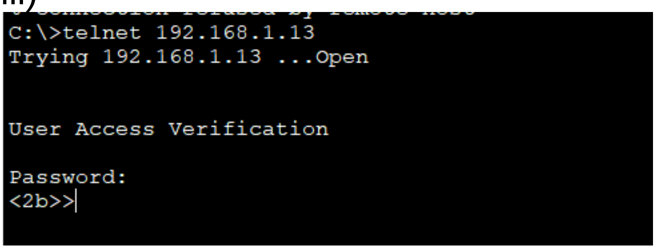
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:

Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=2ms TTL=128
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>
```

ii)



```
Tracing route to 192.168.1.13 over a maximum of 30 hops:

  1   0 ms      0 ms      0 ms      192.168.1.13

Trace complete.
```

iii)



```
C:\>telnet 192.168.1.13
Trying 192.168.1.13 ...Open


User Access Verification

Password:
<2b>>
```

Extra part of the code

```
<2b>#
<2b># enable
<2b># configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
<2b>(config)# line vty 0 15
<2b>(config-line)# password 2bb
<2b>(config-line)# login
<2b>(config-line)# exit
<2b>(config)# interface vlan 1
<2b>(config-if)# ip address 192.168.1.13 255.255.255.0
<2b>(config-if)#no shutdown

<2b>(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
%IP-4-DUPADDR: Duplicate address 192.168.1.13 on Vlan1, sourced by 0001.43D0.5166

<2b>(config-if)#exit
<2b>(config)# show ip address brief
^
% Invalid input detected at '^' marker.
<2b>(config)#Switch# show ip interface brief
^
% Invalid input detected at '^' marker.
<2b>(config)# exit
<2b>#
%SYS-5-CONFIG_I: Configured from console by console

<2b>#Switch# show ip interface brief
^
% Invalid input detected at '^' marker.
<2b>#show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 unassigned YES manual up up
FastEthernet0/2 unassigned YES manual up up
FastEthernet0/3 unassigned YES manual up up
FastEthernet0/4 unassigned YES manual up up
FastEthernet0/5 unassigned YES manual down down
FastEthernet0/6 unassigned YES manual down down
FastEthernet0/7 unassigned YES manual down down
FastEthernet0/8 unassigned YES manual down down
```

```
FastEthernet0/9 unassigned YES manual down down
FastEthernet0/10 unassigned YES manual down down
FastEthernet0/11 unassigned YES manual down down
FastEthernet0/12 unassigned YES manual down down
FastEthernet0/13 unassigned YES manual down down
FastEthernet0/14 unassigned YES manual down down
FastEthernet0/15 unassigned YES manual down down
FastEthernet0/16 unassigned YES manual down down
FastEthernet0/17 unassigned YES manual down down
FastEthernet0/18 unassigned YES manual down down
FastEthernet0/19 unassigned YES manual down down
FastEthernet0/20 unassigned YES manual down down
FastEthernet0/21 unassigned YES manual down down
FastEthernet0/22 unassigned YES manual down down
FastEthernet0/23 unassigned YES manual down down
FastEthernet0/24 unassigned YES manual down down
GigabitEthernet0/1 unassigned YES manual down down
GigabitEthernet0/2 unassigned YES manual down down
Vlan1 192.168.1.13 YES manual up up
<2b>#
```

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

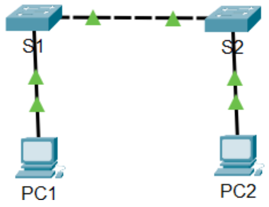
Part 4: Save Configuration Files to NVRAM

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.

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

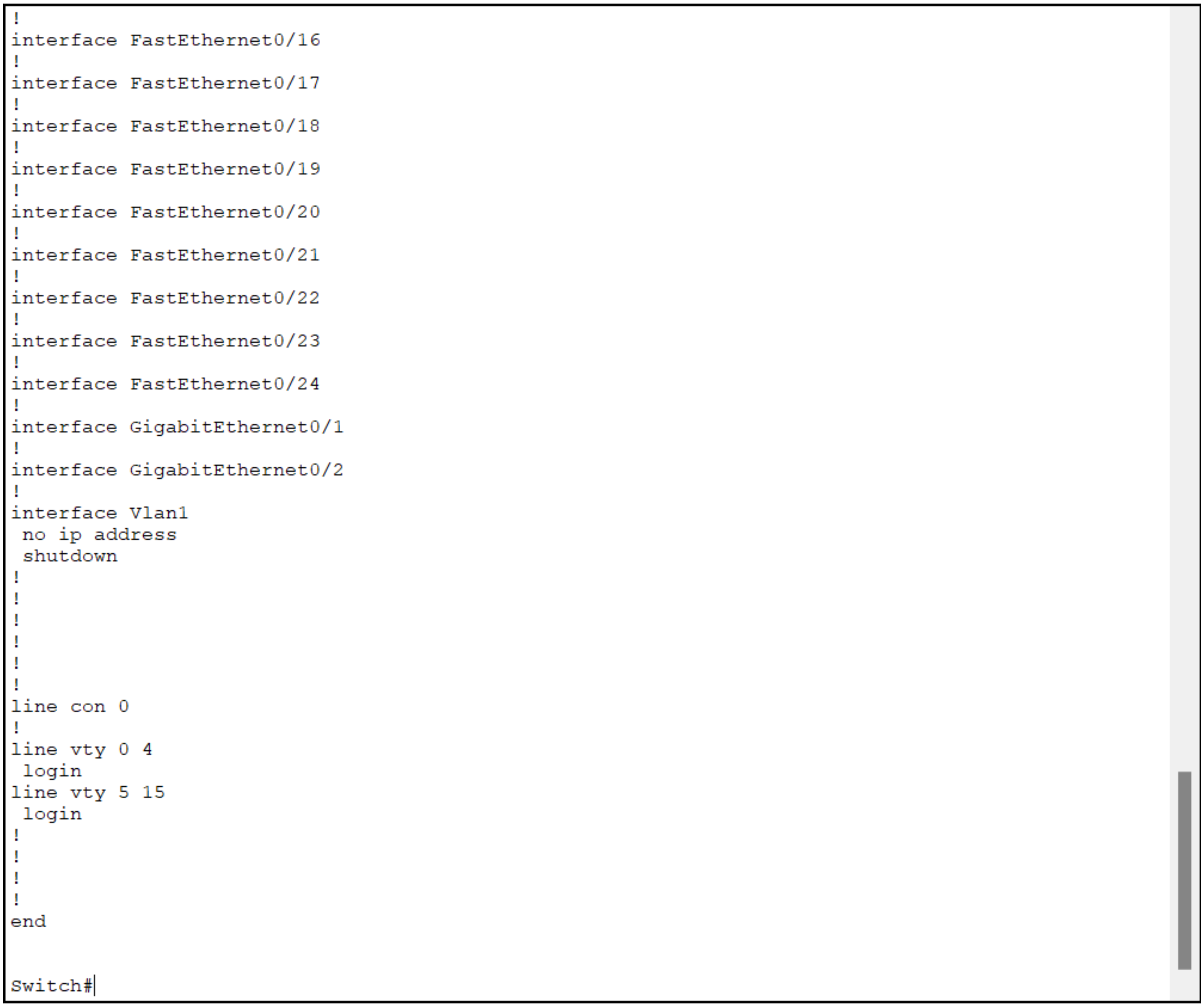
How many Gigabit Ethernet interfaces does the switch have? 2

What is the range of values shown for the vty lines? 0 4 5 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?”
factory reset/corrupted nvram/not configured



```
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end


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.

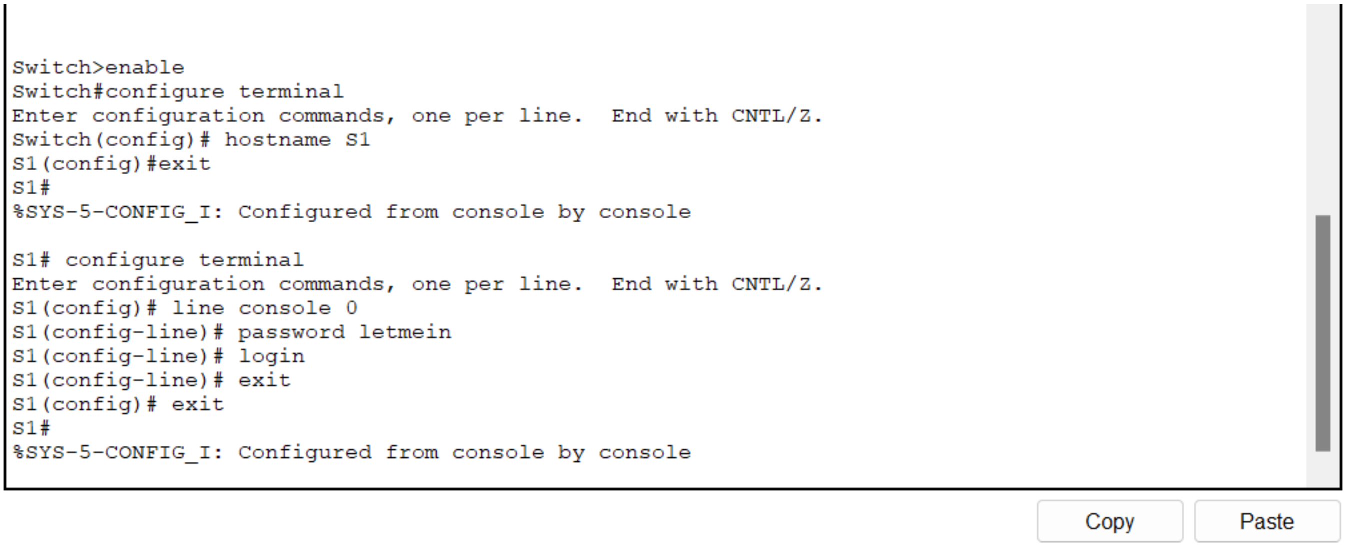
```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)# exit
S1#
```

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#
```



```
Switch>enable
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# 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
```

- Why is the **login** command required? **login** ensures the requirement to enter the password before granting access to the device. Without the login command, the device won't prompt for a password even if one is set, which could lead to unauthorized access.

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>
```

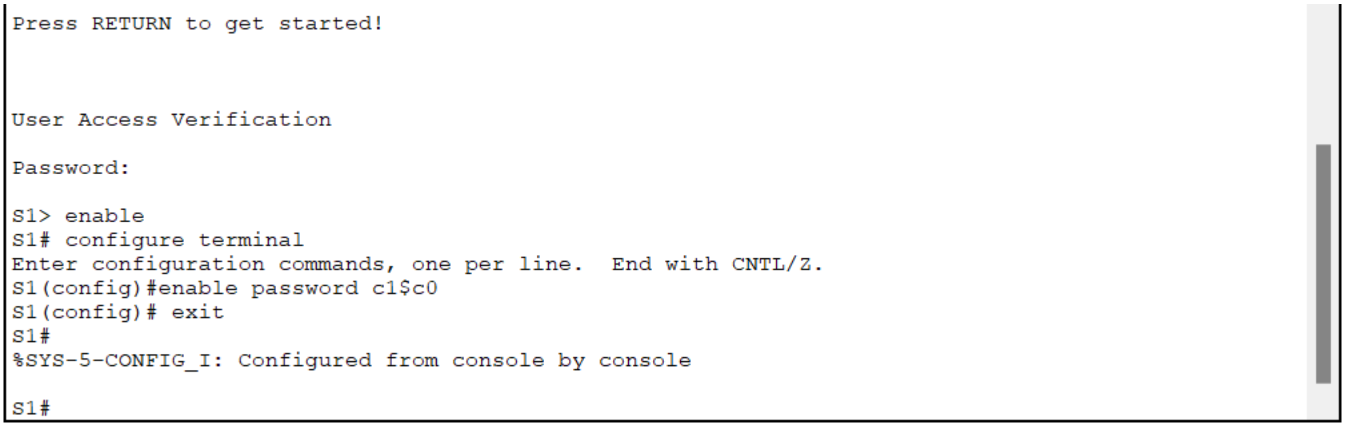
Note: If the switch did not prompt you for a password, then you did not configure the **login** parameter in Step 2.

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#
```



```
Press RETURN to get started!



User Access Verification

Password:

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 enable. 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.

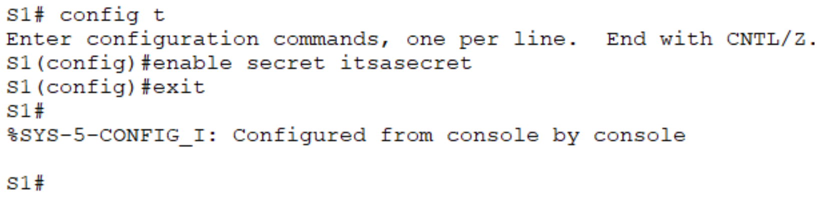
Step 6: Configure an encrypted password to secure access to privileged mode.

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#
```

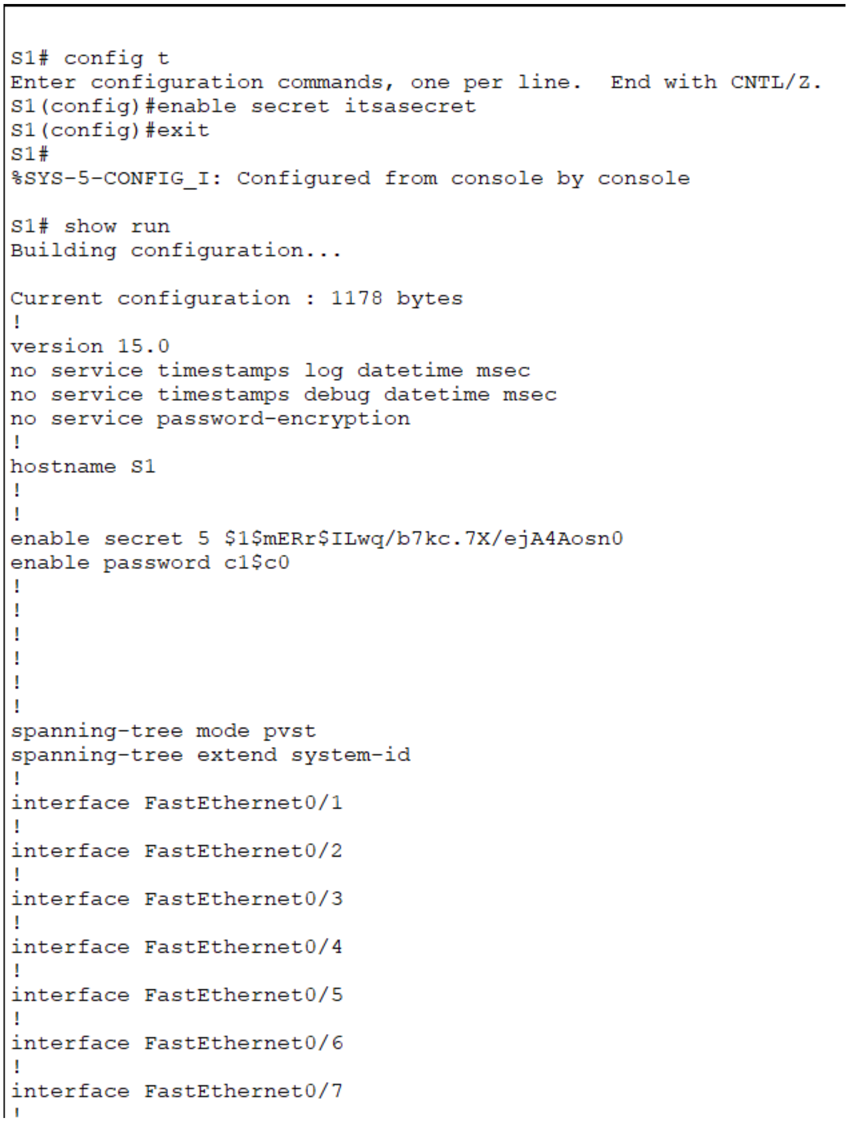
Note: The **enable secret** password overrides the **enable** password. If both are configured on the switch, you must enter the **enable secret** password to enter privileged EXEC mode.



```
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.



```
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# 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
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
```

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

```
S1# show run (click tab)
```

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? Its encrypted

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.

- **With service password-encryption enabled**, passwords will be encrypted using a weak reversible algorithm (Type 7), which can decrypted easily.

□ **enable secret uses strong MD5 encryption** (Type 5) and difficult to decrypt.

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? Before logging in

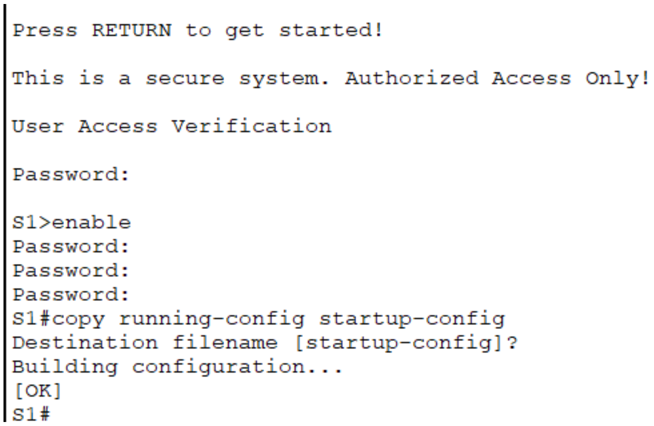
Why should every switch have a MOTD banner? A MOTD banner enhances security by informing the users about access limitations, grants legal, and regulatory compliances, and notifies the users about any information on network usage. This is simple yet effective in steps to protect the network devices and send unauthorized access to a minimum when dissuaded effectively.

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...
```



```
Press RETURN to get started!

This is a secure system. Authorized Access Only!

User Access Verification

Password:

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

```
[OK]
```

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

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? Not necessarily

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.