CMPE 305 Data and Digital Communication

MP3 – Basic Switch and OSI Model

Delima, Sheena Mae D.

BSCPE 3-3

09/28/2025

2.7.6 – Implement Basic Connectivity

Objectives	Background
Part 1: Perform a Basic Configuration on S1 and S2 Part 2: Configure the PCs Part 3: Configure the Switch Management Interface	In this activity, you will first create a basic switch configuration. Then, you will implement basic connectivity by configuring IP addressing on switches and PCs. When the IP addressing configuration is complete, you will use various show commands to verify the configuration and use the ping command to verify basic connectivity between devices.

Instructions

Part 1: Perform a Basic Configuration on S1 and S2

Complete the following steps on S1 and S2.

Step 1: Configure S1 with a hostname.

a. Click S1 and then click the CLI tab.

b. Enter the correct command to configure the hostname as S1.

Step 2: Configure the console and encrypted privileged EXEC mode passwords.

a. Use cisco for the console password.

b. Use class for the privileged EXEC mode password.

Step 3: Verify the password configurations for S1.

Question:

How can you verify that both passwords were configured correctly?

You can verify the password configurations by exiting the configuration mode and then logging back in.

- First, exit to the user EXEC mode: S1(config)# end
- You will be prompted for the console password. Enter **cisco**.
- Then, to enter the privileged EXEC mode, type **enable** and enter the password **class**.

Use an appropriate banner text to warn unauthorized access. The following text is an example:

Authorized access only. Violators will be prosecuted to the full extent of the law.

Step 4: Save the configuration file to NVRAM.

Question:

Which command do you issue to accomplish this step? copy run start

Logical | Physical x: 258, y: 150

b. Enter the correct command to configure the hostname as S1.

Step 2: Configure the console and encrypted privileged EXEC mode passwords.

a. Use **cisco** for the console password.

b. Use **class** for the privileged EXEC mode password.

Step 3: Verify the password configurations for S1.

How can you verify that both passwords were configured correctly?

Use an appropriate banner text to warn unauthorized access. The following text is an example:

Authorized access only. Violators will be prosecuted to the full extent of the law.

Step 4: Save the configuration file to NVRAM.

Which command do you issue to accomplish this step?

Step 5: Repeat Steps 1 to 5 for S2.

Part 2: Configure the PCs

Configure PC1 and PC2 with IP addresses.

Time Elapsed: 00:00:00 Completion: 54%

Dock | Check Results | Back | 1/1 | Next

Time: 00:45:54

```
User Access Verification

Password:

S1>en
Password:
S1#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#ena sec class
The enable secret you have chosen is the same as your enable password.
This is not recommended.  Re-enter the enable secret.
S1(config)#show run
                 ^
% Invalid input detected at '^' marker.

S1(config)#^Z
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show run
Building configuration...

Current configuration : 1176 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
!
```

Logical | Physical x: 166, y: 55

b. Enter the correct command to configure the hostname as S1.

Step 2: Configure the console and encrypted privileged EXEC mode passwords.

a. Use **cisco** for the console password.

b. Use **class** for the privileged EXEC mode password.

Step 3: Verify the password configurations for S1.

How can you verify that both passwords were configured correctly?

Use an appropriate banner text to warn unauthorized access. The following text is an example:

Authorized access only. Violators will be prosecuted to the full extent of the law.

Step 4: Save the configuration file to NVRAM.

Which command do you issue to accomplish this step?

Step 5: Repeat Steps 1 to 5 for S2.

Part 2: Configure the PCs

Configure PC1 and PC2 with IP addresses.

Time Elapsed: 00:00:00 Completion: 54%

Dock | Check Results | Back | 1/1 | Next

Time: 00:46:15

CLI | Attributes

IOS Command Line Interface

```
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
enable password class
!
!
!
!
!
!
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
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
```

Logical | Physical x: 194, y: 335

b. Enter the correct command to configure the hostname as S1.

Step 2: Configure the console and encrypted privileged EXEC mode passwords.

a. Use **cisco** for the console password.

b. Use **class** for the privileged EXEC mode password.

Step 3: Verify the password configurations for S1.

How can you verify that both passwords were configured correctly?

Use an appropriate banner text to warn unauthorized access. The following text is an example:

Authorized access only. Violators will be prosecuted to the full extent of the law.

Step 4: Save the configuration file to NVRAM.

Which command do you issue to accomplish this step?

Step 5: Repeat Steps 1 to 5 for S2.

Part 2: Configure the PCs

Configure PC1 and PC2 with IP addresses.

Time Elapsed: 00:00:00 Completion: 54%

Dock | Check Results | Back | 1/1 | Next

Time: 00:46:29

CLI | Attributes

IOS Command Line Interface

```
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
!
!
line con 0
 password cisco
 login
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end


S1#
S1#
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#banner motd #Authorized access only. Violators will be prosecuted to the full
extent of the law.!!! #
S1(config)#^Z
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#exit
```

Copy | Paste

Logical | Physical x: 161, y: 311

b. Enter the correct command to configure the hostname as S1.

Step 2: Configure the console and encrypted privileged EXEC mode passwords.

a. Use **cisco** for the console password.

b. Use **class** for the privileged EXEC mode password.

Step 3: Verify the password configurations for S1.

How can you verify that both passwords were configured correctly?

Use an appropriate banner text to warn unauthorized access. The following text is an example:

Authorized access only. Violators will be prosecuted to the full extent of the law.

Step 4: Save the configuration file to NVRAM.

Which command do you issue to accomplish this step?

Step 5: Repeat Steps 1 to 5 for S2.

Part 2: Configure the PCs

Configure PC1 and PC2 with IP addresses.

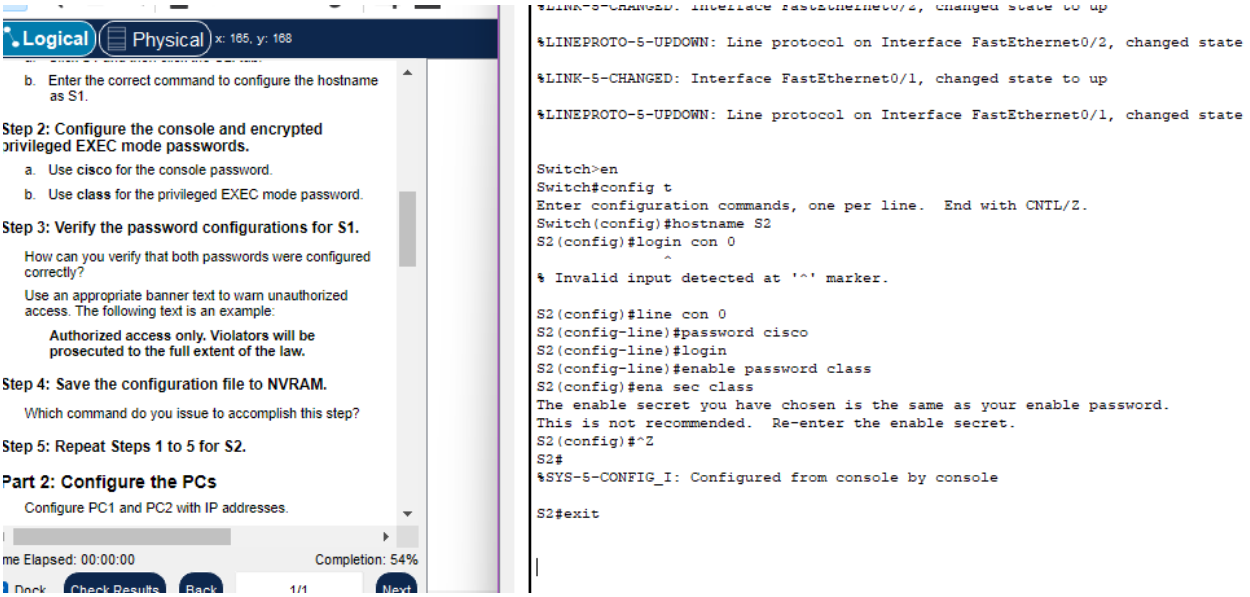
Time Elapsed: 00:00:00 Completion: 54%

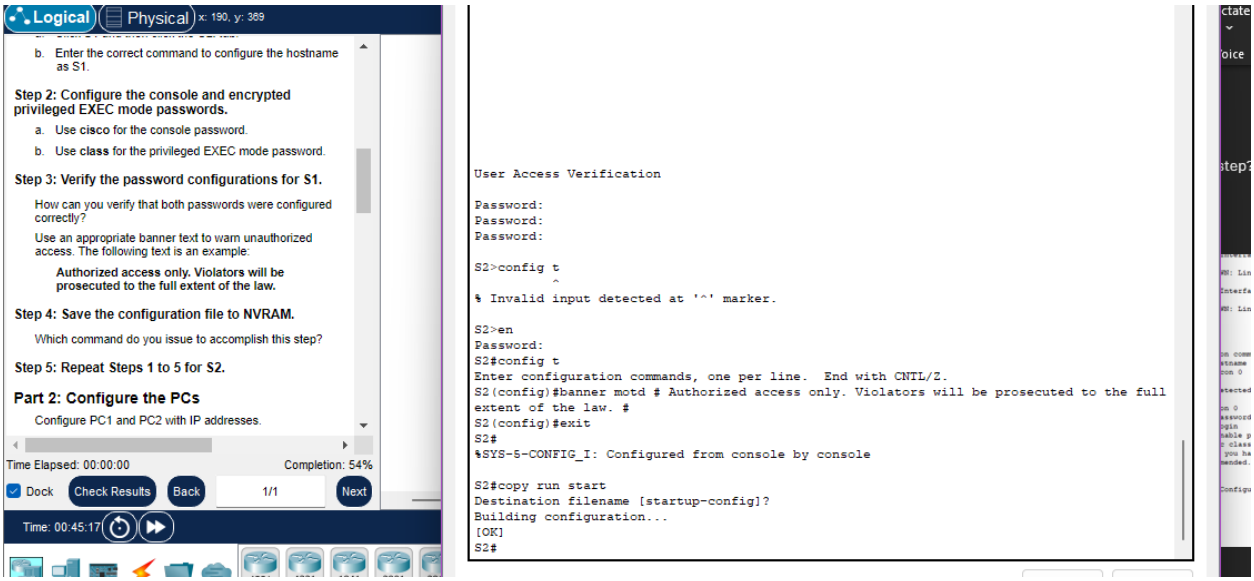
Dock | Check Results | Back | 1/1 | Next

Time: 00:47:04

```
S1 con0 is now available



Press RETURN to get started.



Authorized access only. Violators will be prosecuted t

User Access Verification

Password:

S1>en
Password:
S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
?Bad filename
%Error parsing filename (Bad file number)
S1#
```

Step 5: Repeat Steps 1 to 5 for S2.





Part 2: Configure the PCs

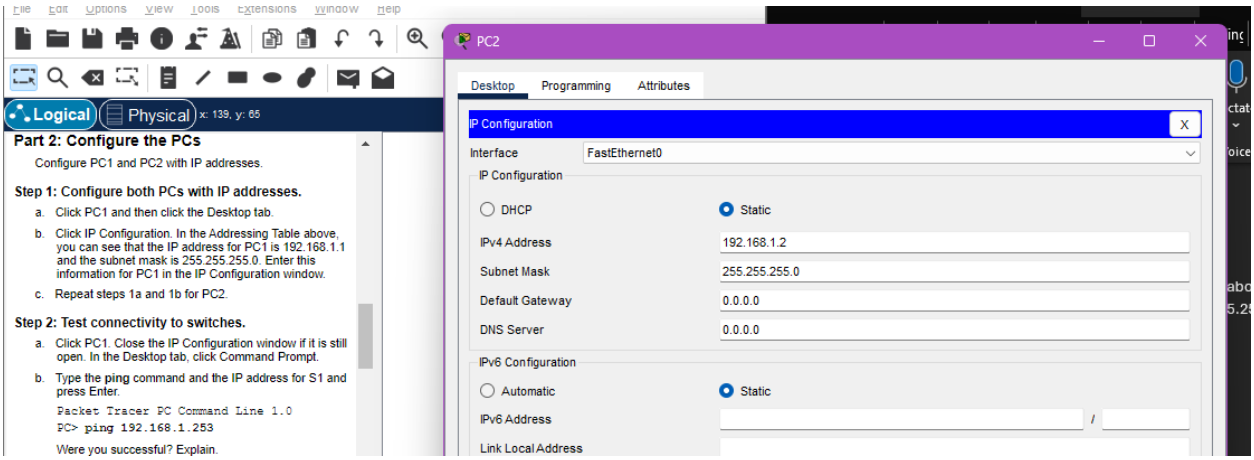
Configure PC1 and PC2 with IP addresses.

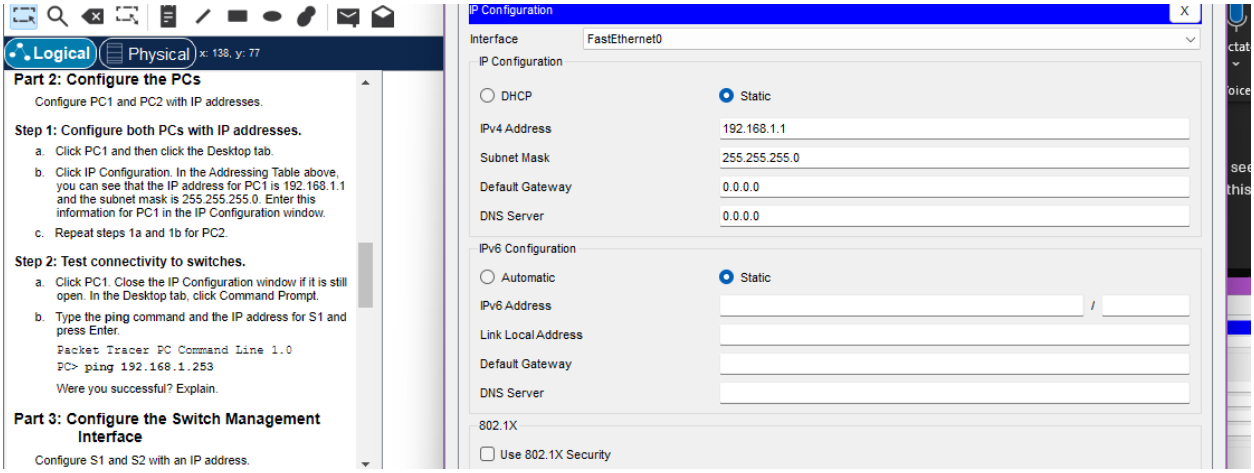
Step 1: Configure both PCs with IP addresses.

a. Click PC1 and then click the Desktop tab.

b. Click IP Configuration. In the Addressing Table above, you can see that the IP address for PC1 is 192.168.1.1 and the subnet mask is 255.255.255.0. Enter this information for PC1 in the IP Configuration window.

c. Repeat steps 1a and 1b for PC2.





Step 2: Test connectivity to switches.

a. Click PC1. Close the IP Configuration window if it is still open. In the Desktop tab, click Command Prompt.

b. Type the **ping** command and the IP address for S1 and press Enter.

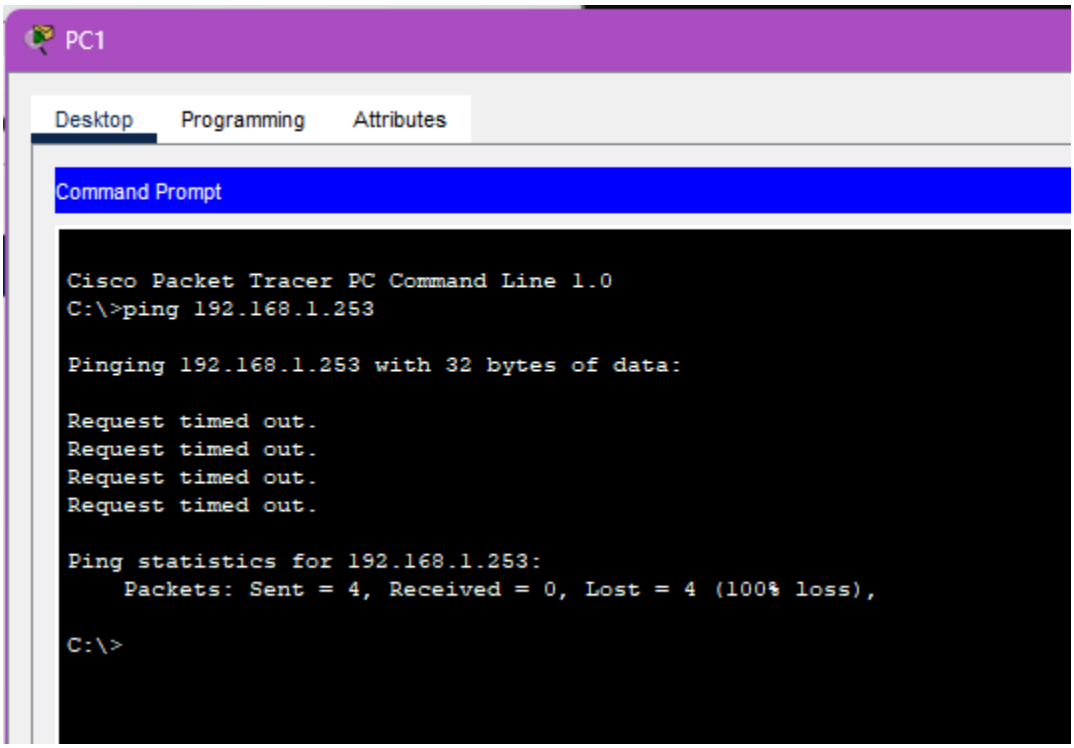
Packet Tracer PC Command Line 1.0

PC> **ping 192.168.1.253**

Question:

Were you successful? Explain.

No. Switches S1 andS2 are not yet configured on their physical interface, especially the IP address, that is why the output is request time out. Likewise, since this is an unmanaged, default VLAN, the PCs are not part of it and cannot communicate with the switch's VLAN interface. The instructions in Part 3 will address this by configuring the management interfaces and enabling connectivity.



Part 3: Configure the Switch Management Interface

Configure S1 and S2 with an IP address.

Step 1: Configure S1 with an IP address.

Switches can be used as plug-and-play devices. This means that they do not need to be configured for them to work. Switches forward information from one port to another based on MAC addresses.

Question:

If this is the case, why would we configure it with an IP address?

We configure a switch with an IP address for **remote management**. While a switch can forward traffic without an IP address, configuring one allows network administrators to access and manage the device from a remote location using protocols like Telnet or SSH. This prevents the need to be physically present at the switch to make configuration changes.

Use the following commands to configure S1 with an IP address.

S1# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

S1(config)# **interface vlan 1**

S1(config-if)# **ip address 192.168.1.253 255.255.255.0**

S1(config-if)# **no shutdown**

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

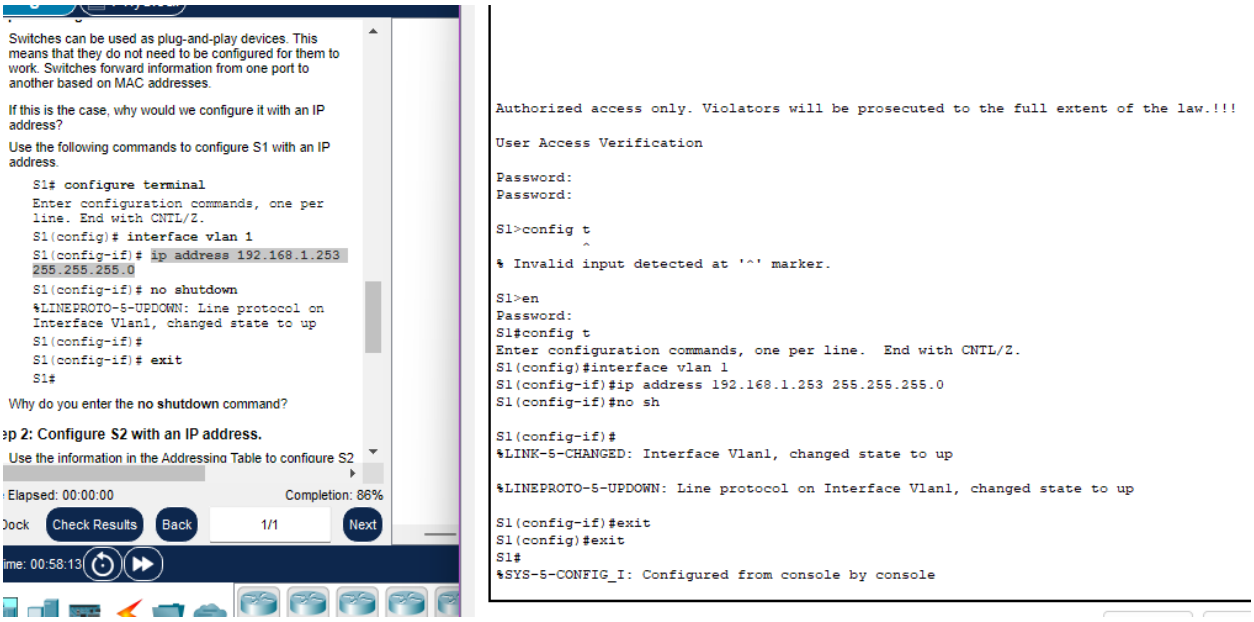
S1(config-if)#

S1(config-if)# **exit**

S1#

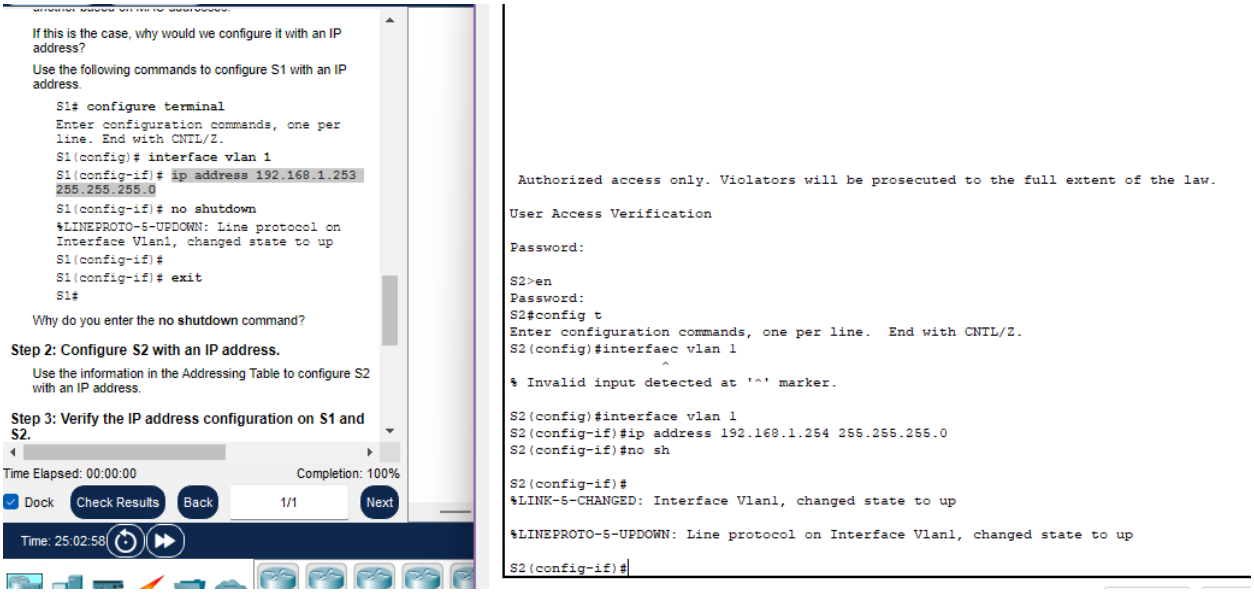
Question: Why do you enter the **no shutdown** command?

The **no shutdown** command is used to **activate the VLAN 1 interface**. By default, this virtual interface is turned off, or "administratively down." The no shutdown command basically turns the interface on and brings it to an "up" state, making it active and allowing the switch's IP address to be reachable on the network. Without this command, the IP address we configured would be useless because the interface would be disabled.



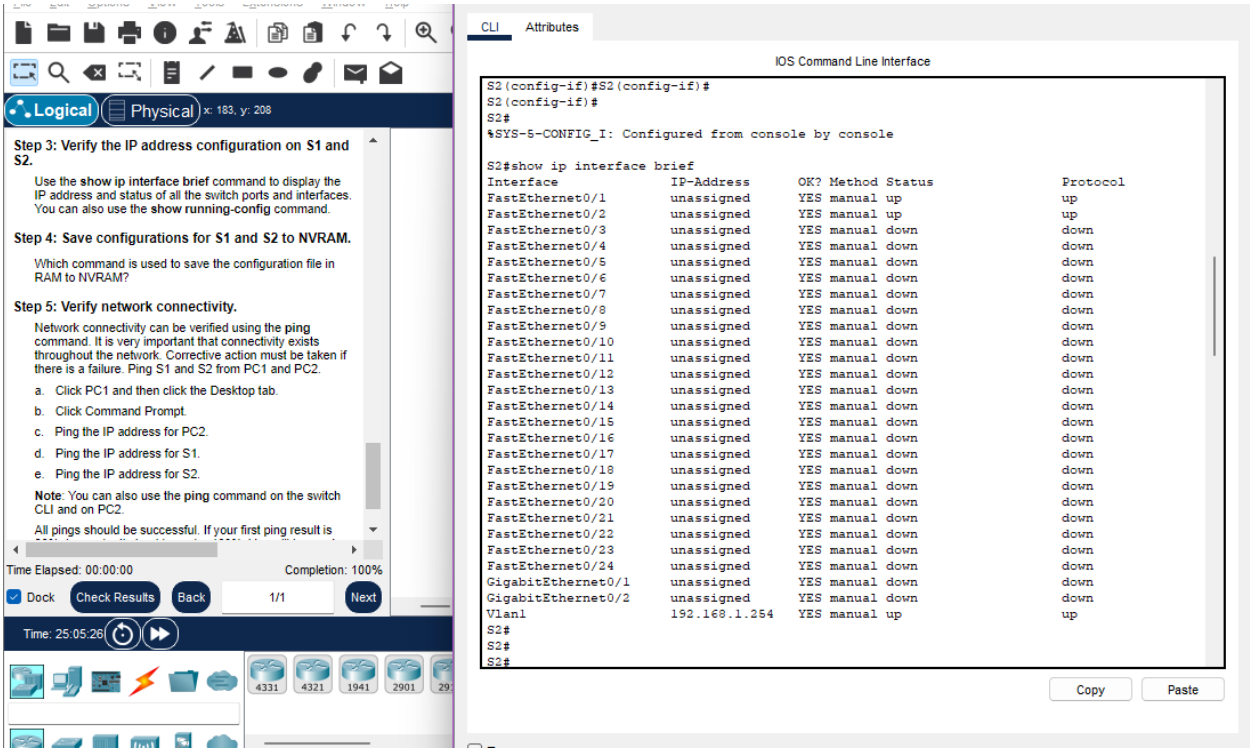
Step 2: Configure S2 with an IP address.

Use the information in the Addressing Table to configure S2 with an IP address.



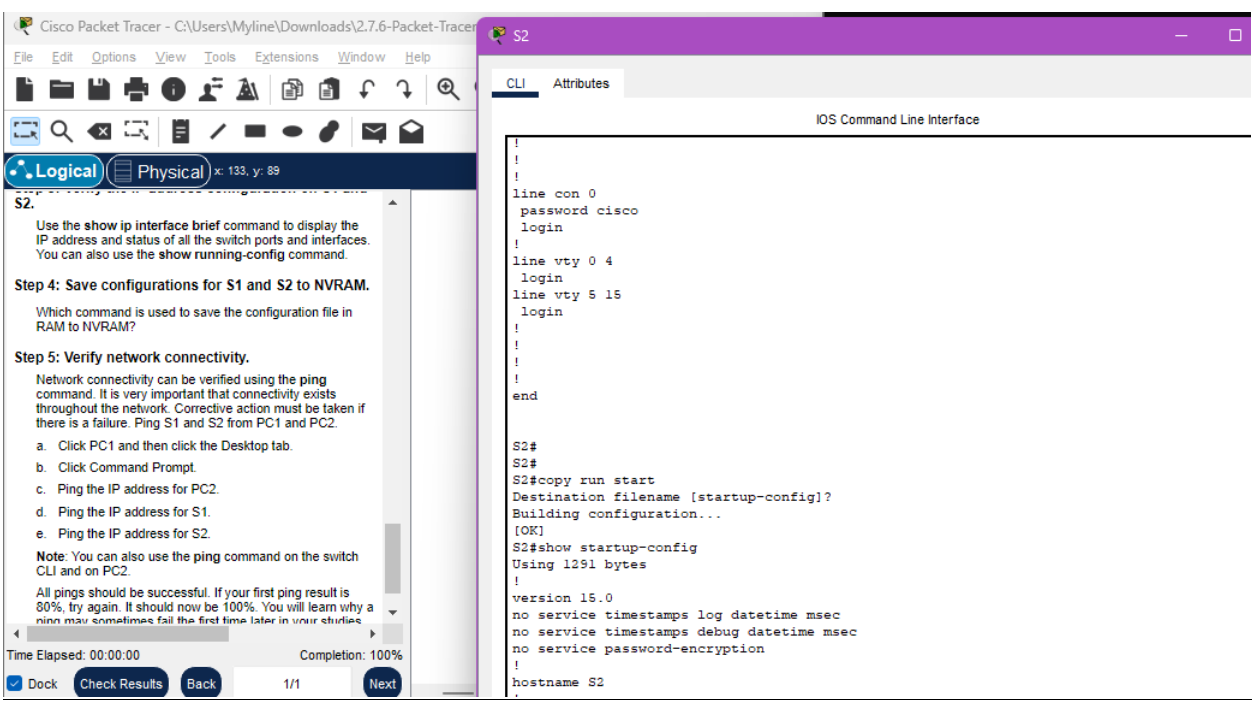
Step 3: Verify the IP address configuration on S1 and S2.

Use the **show ip interface brief** command to display the IP address and status of all the switch ports and interfaces. You can also use the **show running-config** command.



Step 4: Save configurations for S1 and S2 to NVRAM.

Question: Which command is used to save the configuration file in RAM to NVRAM? copy run start



Step 5: Verify network connectivity.

Network connectivity can be verified using the **ping** command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure. Ping S1 and S2 from PC1 and PC2.

a. Click PC1 and then click the Desktop tab.

b. Click Command Prompt.

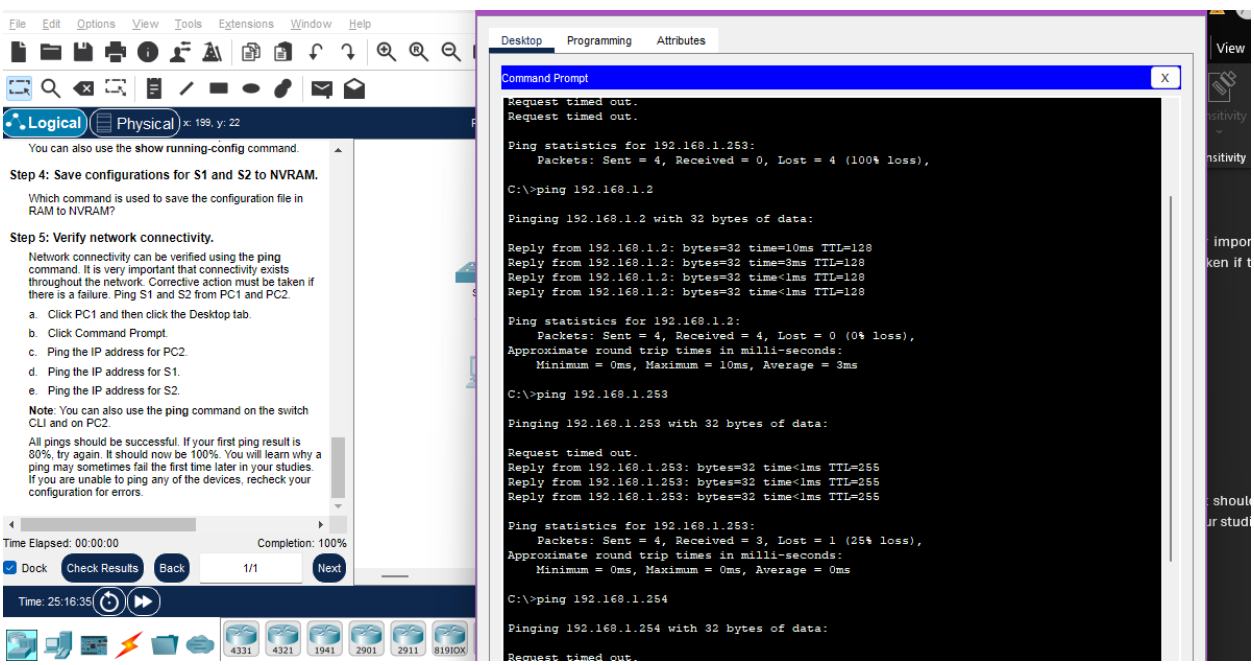
c. Ping the IP address for PC2.

d. Ping the IP address for S1.

e. Ping the IP address for S2.

Note: You can also use the **ping** command on the switch CLI and on PC2.

All pings should be successful. If your first ping result is 80%, try again. It should now be 100%. You will learn why a ping may sometimes fail the first time later in your studies. If you are unable to ping any of the devices, recheck your configuration for errors.



Logical | Physical x: 135, y: 83

You can also use the **show running-config** command.

Step 4: Save configurations for S1 and S2 to NVRAM.

Which command is used to save the configuration file in RAM to NVRAM?

Step 5: Verify network connectivity.

Network connectivity can be verified using the **ping** command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure. Ping S1 and S2 from PC1 and PC2.

a. Click PC1 and then click the Desktop tab.

b. Click Command Prompt.

c. Ping the IP address for PC2.

d. Ping the IP address for S1.

e. Ping the IP address for S2.

Note: You can also use the **ping** command on the switch CLI and on PC2.

All pings should be successful. If your first ping result is 80%, try again. It should now be 100%. You will learn why a ping may sometimes fail the first time later in your studies. If you are unable to ping any of the devices, recheck your configuration for errors.

Time Elapsed: 00:00:00 Completion: 100%

Dock | Check Results | Back | 1/1 | Next

Time: 25:17:59

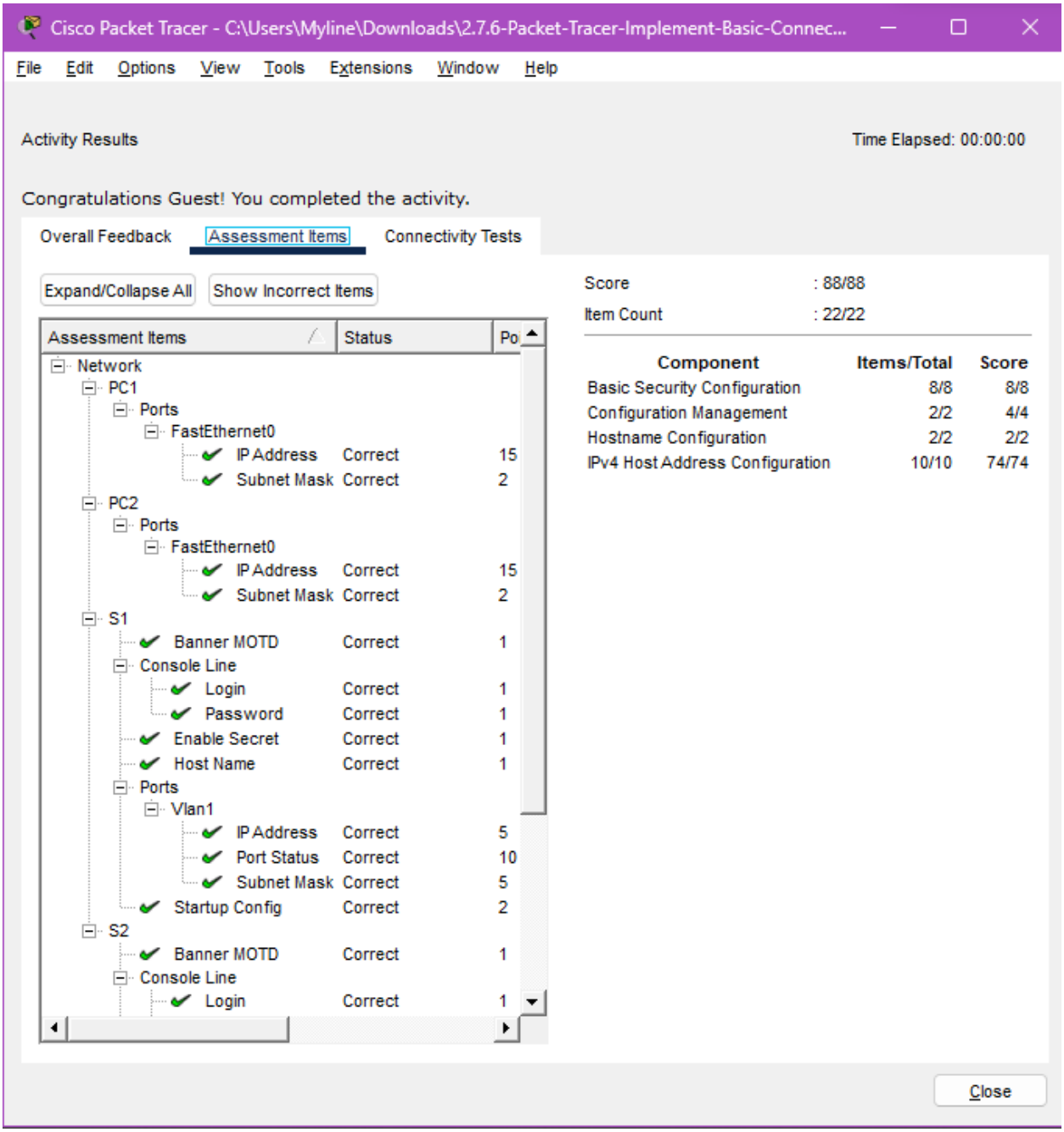
4331 4321 1941 2901 2911

Desktop | Programming | Attributes

Command Prompt

```
C:\>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Reply from 192.168.1.253: bytes=32 time<1ms TTL=255
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time=1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

COMPLETION:


Cisco Packet Tracer - C:\Users\Myline\Downloads\2.7.6-Packet-Tracer-Implement-Basic-Connec...
File Edit Options View Tools Extensions Window Help
Activity Results
Time Elapsed: 00:00:00
Congratulations Guest! You completed the activity.
Overall Feedback
Assessment Items
Connectivity Tests
Expand/Collapse All
Show Incorrect Items
Assessment Items
Status
Network
PC1
Ports
FastEthernet0
IP Address Correct 15
Subnet Mask Correct 2
PC2
Ports
FastEthernet0
IP Address Correct 15
Subnet Mask Correct 2
S1
Banner MOTD Correct 1
Console Line
Login Correct 1
Password Correct 1
Enable Secret Correct 1
Host Name Correct 1
Ports
Vlan1
IP Address Correct 5
Port Status Correct 10
Subnet Mask Correct 5
Startup Config Correct 2
S2
Banner MOTD Correct 1
Console Line
Login Correct 1
Score : 88/88
Item Count : 22/22
Component Items/Total Score
Basic Security Configuration 8/8 8/8
Configuration Management 2/2 4/4
Hostname Configuration 2/2 2/2
IPv4 Host Address Configuration 10/10 74/74
Close