

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

## Packet Tracer - Implement Basic Connectivity

### Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.253	255.255.255.0
S2	VLAN 1	192.168.1.254	255.255.255.0
PC1	NIC	192.168.1.1	255.255.255.0
PC2	NIC	192.168.1.2	255.255.255.0

### Objectives

**Part 1: Perform a Basic Configuration on S1 and S2**

**Part 2: Configure the PCs**

**Part 3: Configure the Switch Management Interface**

### Background

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.

- Click S1 and then click the CLI tab.
- Enter the correct command to configure the hostname as S1.



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

- Use **cisco** for the console password.
- Use **class** for the privileged EXEC mode password.

 S1

CLI Attributes

IOS Command Line Interface

```

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

S1#exit

S1 con0 is now available

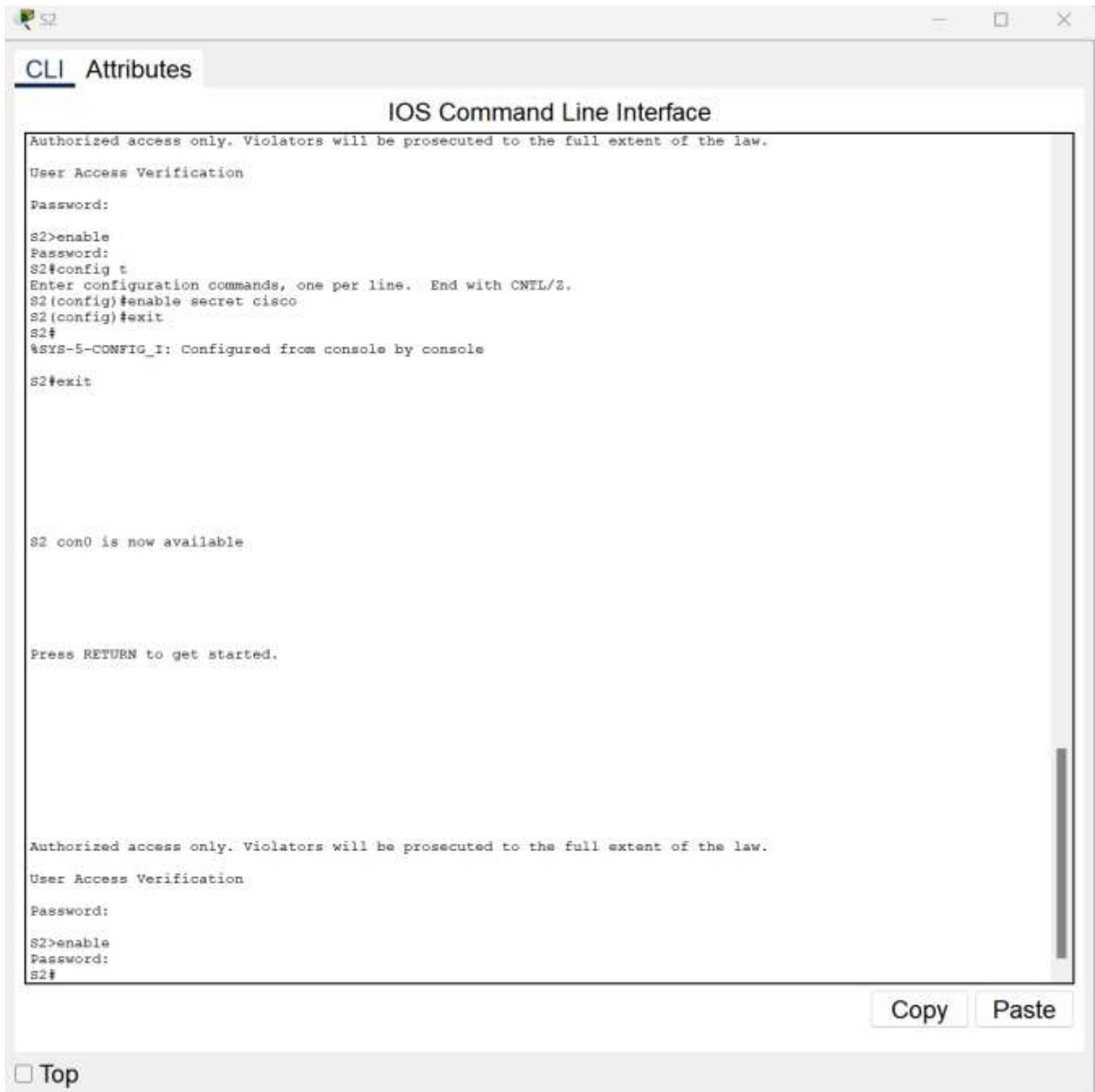
Press RETURN to get started.

Authorized access only. Violators will be prosecuted to the full extent of the law.
User Access Verification
Password:
S1>enable
Password:
Password:
S1#

```

Copy Paste

☐ Top



### Step 3: Verify the password configurations for S1.

How can you verify that both passwords were configured correctly?

There are two ways. The first is by exiting the exec mode and then being prompted to provide passwords when logging into the console and privileged exec mode. The second way is by running `show running-config` and being shown the passwords.



CLI Attributes

### IOS Command Line Interface

```
!
end

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

S1#
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
S1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
S1#show start
Using 1227 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
!
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
!
```

Copy

Paste

☐ Top

### Step 6: Repeat Steps 1 to 5 for S2.

The screenshot shows the Packet Tracer CLI window for device S2. The window has a title bar with 'S2' and standard window controls. Below the title bar, there are tabs for 'CLI' and 'Attributes'. The main area is titled 'IOS Command Line Interface'. The CLI shows the following sequence of commands and output:

```
Password:
S2>enable
S2#config ter
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#enable password class
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#exit

S2 con0 is now available

Press RETURN to get started.

User Access Verification
Password:
S2>enable
Password:
S2#config ter
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#banner motd "Authorized access only. Violators will be prosecuted to the full extent of the law."
S2(config)#exit
S2#
```

At the bottom right of the CLI window, there are 'Copy' and 'Paste' buttons. At the bottom left, there is a 'Top' link with a square icon next to it.

CLI

Attributes

### IOS Command Line Interface

```

Password:
S2>enable
Password:
S2#config ter
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#banner motd "Authorized access only. Violators will be prosecuted to the full extent of the law."
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
S2#show run
Building configuration...

Current configuration : 1227 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S2
!
!
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
!

```

Copy

Paste

☐ Top





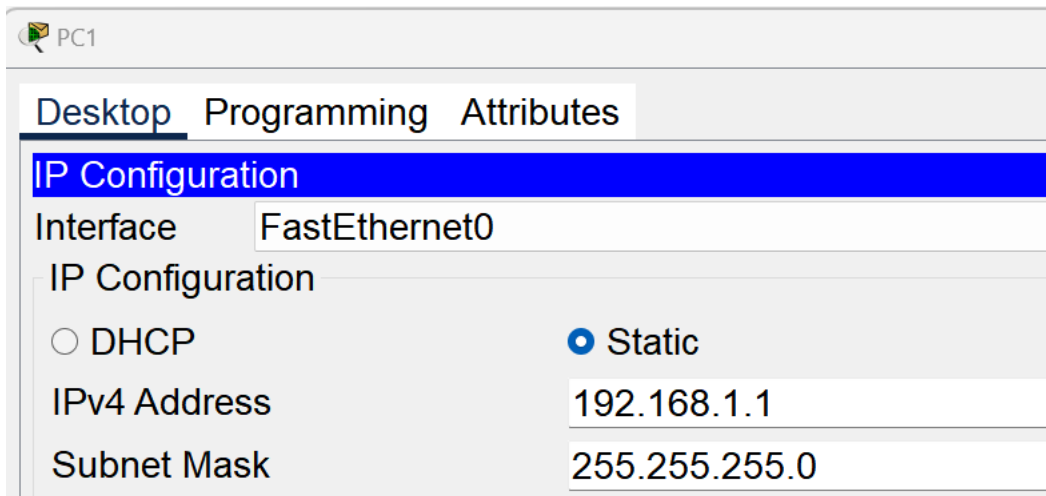
## Part 2: Configure the PCs

Configure PC1 and PC2 with IP addresses.

### Step 1: Configure both PCs with IP addresses.

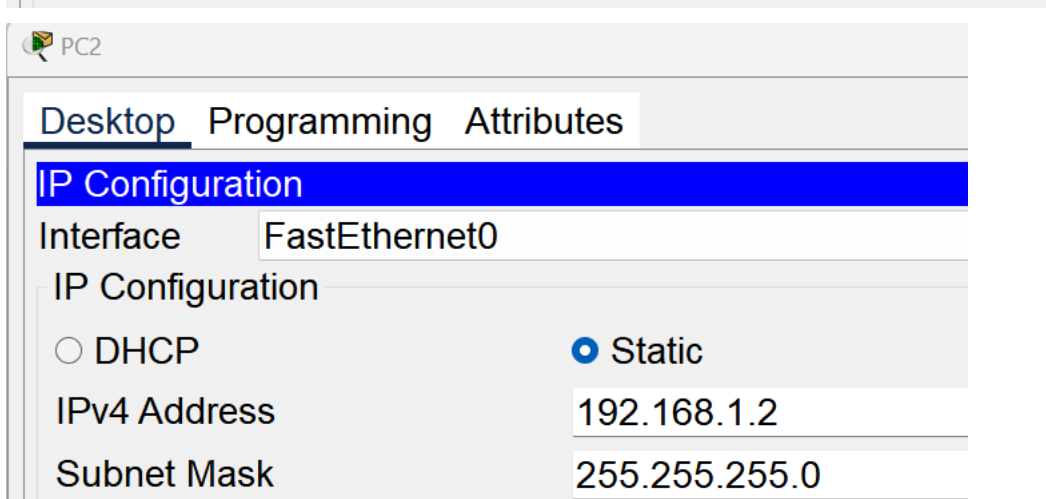
- Click PC1 and then click the Desktop tab.
- Click IP Configuration. In the Addressing Table above, you can see that the IP address for PC1 is 192.168.1.1 and the subnet mask is 255.255.255.0. Enter this information for PC1 in the IP Configuration window.

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



PC1 configuration window showing the IP Configuration tab. The interface is FastEthernet0. The IP configuration is set to Static with an IPv4 Address of 192.168.1.1 and a Subnet Mask of 255.255.255.0.

Desktop Programming Attributes	
IP Configuration	
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.1.1
Subnet Mask	255.255.255.0



PC2 configuration window showing the IP Configuration tab. The interface is FastEthernet0. The IP configuration is set to Static with an IPv4 Address of 192.168.1.2 and a Subnet Mask of 255.255.255.0.

Desktop Programming Attributes	
IP Configuration	
Interface	FastEthernet0
IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.1.2
Subnet Mask	255.255.255.0

### Step 2: Test connectivity to switches.

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

```
Cisco Packet Tracer PC Command Line 1.0
C:\>
C:\>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Were you successful? Explain.

I was not successful because I have not yet configured the switches with IP addresses.

### 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.

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

An IP address needs to be assigned to the switches to be controlled remotely.

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#
```

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

User Access Verification

Password:

S1>enable
Password:
S1# config ter
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

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

S1(config-if)#
S1(config-if)#exit
S1(config)#
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

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

The **no shutdown** command leaves the interface in an active state.

### 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.

## CLI Attributes

### IOS Command Line Interface

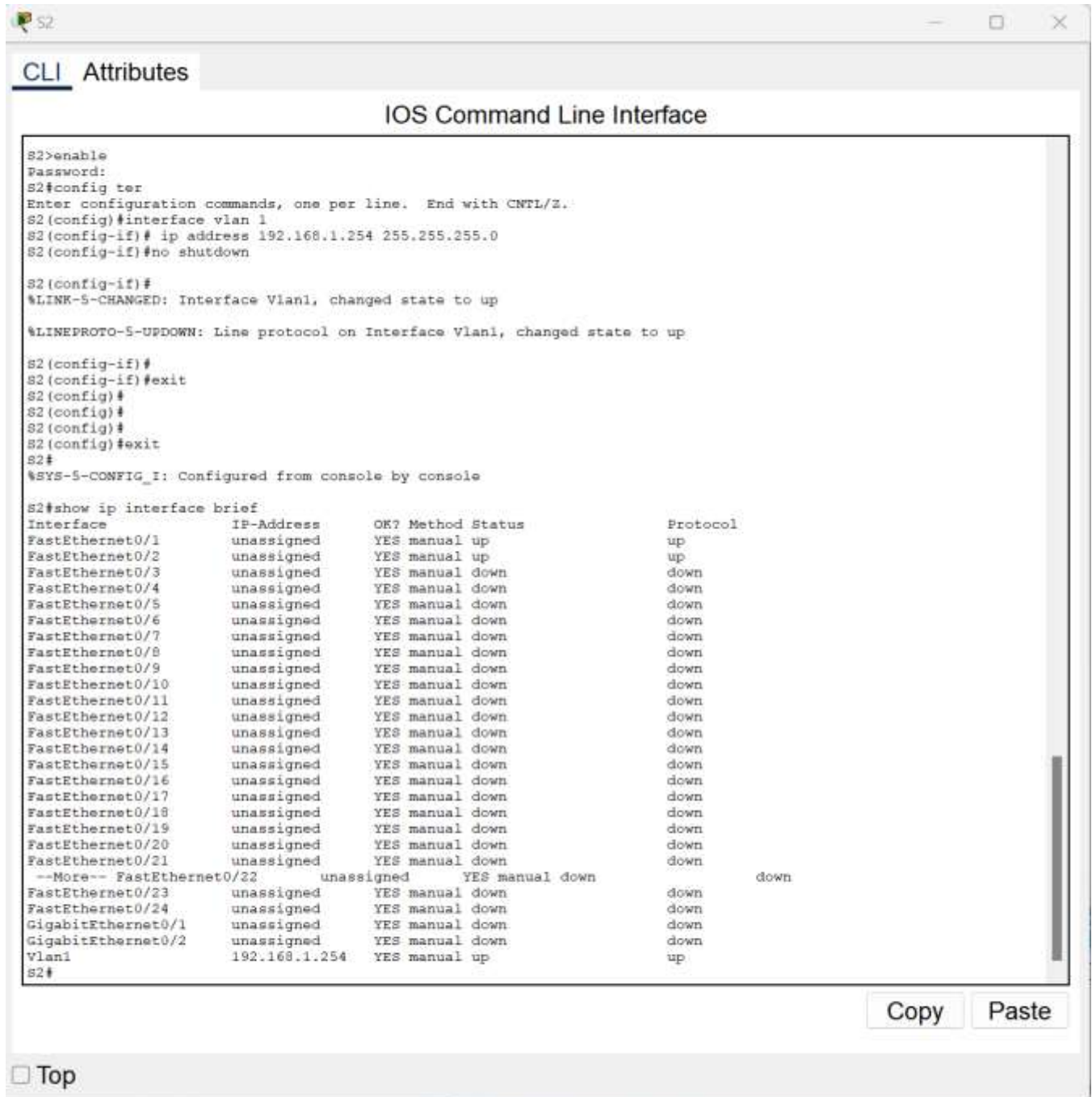
```

S1(config-if)#
S1(config-if)#exit
S1(config)#
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#S1#
S1#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	down	down
FastEthernet0/4	unassigned	YES	manual	down	down
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	192.168.1.253	YES	manual	up	up



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

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

copy run start

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

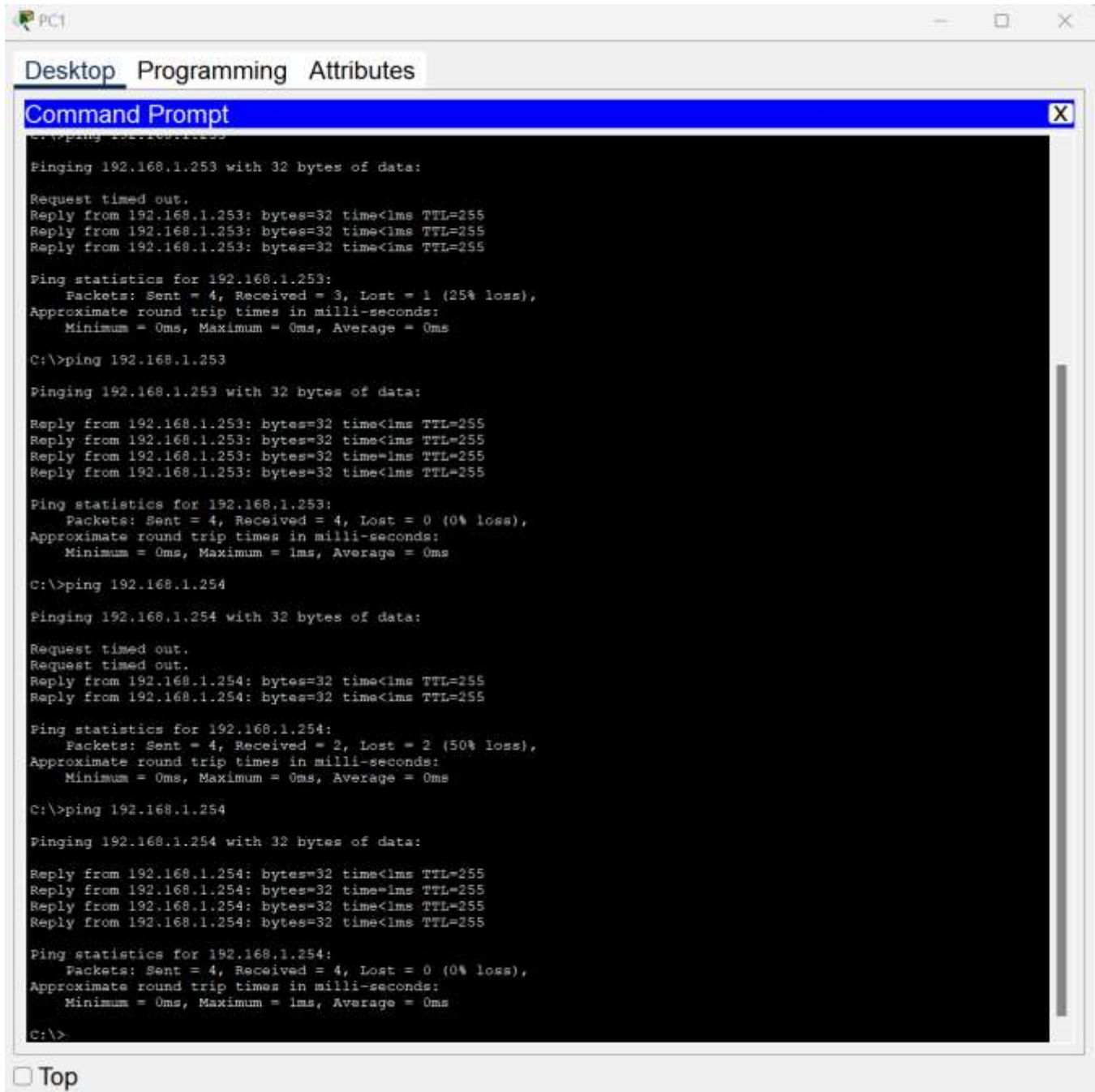
```
S1#  
S1#copy run start  
Destination filename [startup-config]?  
Building configuration...  
[OK]  
S1#  
S1#
```

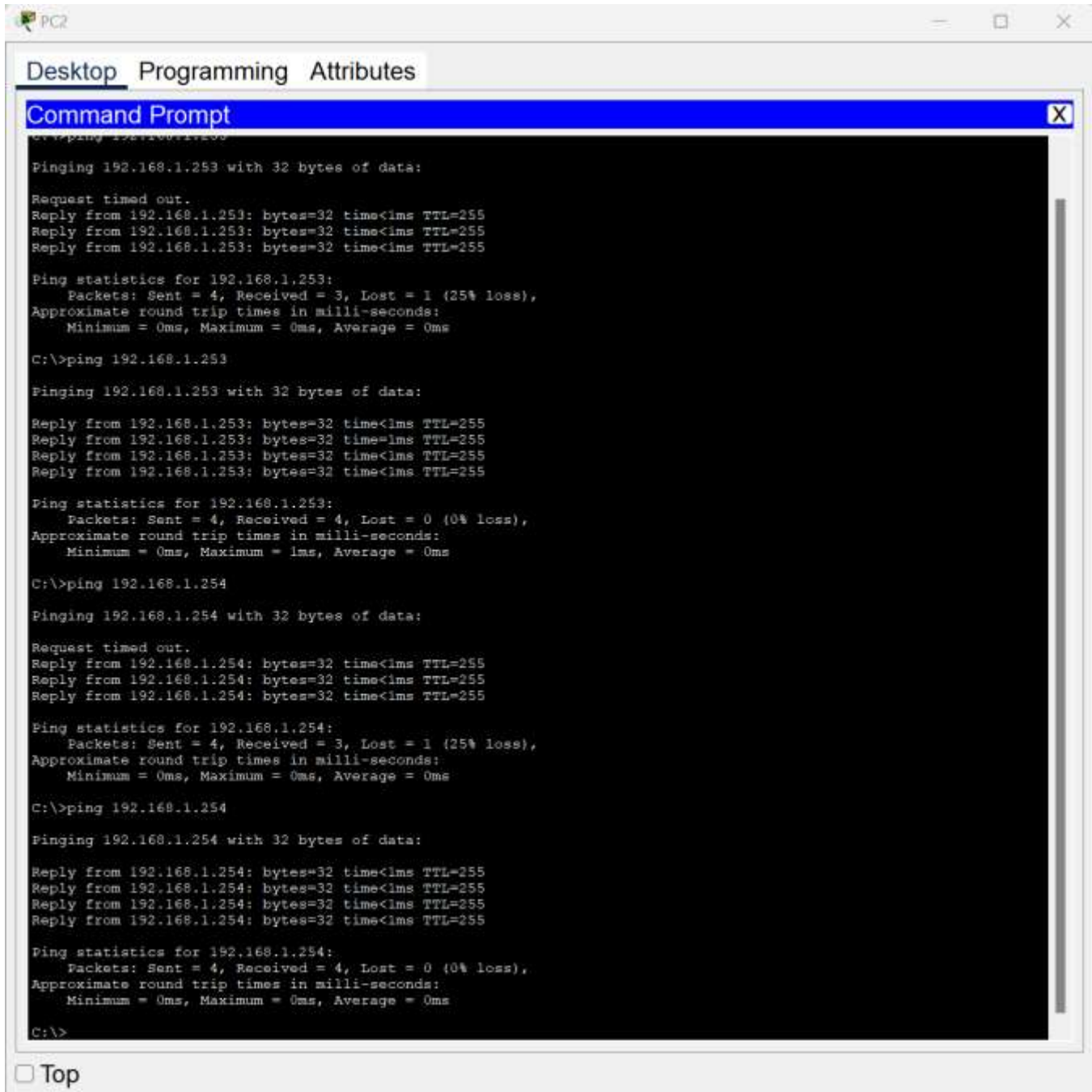
### Step 5: Verify network connectivity.

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.