Networking Academy

NAME: BEATRICE ANN DAVID A23CS0055

LAB 1:
2.7.6: 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

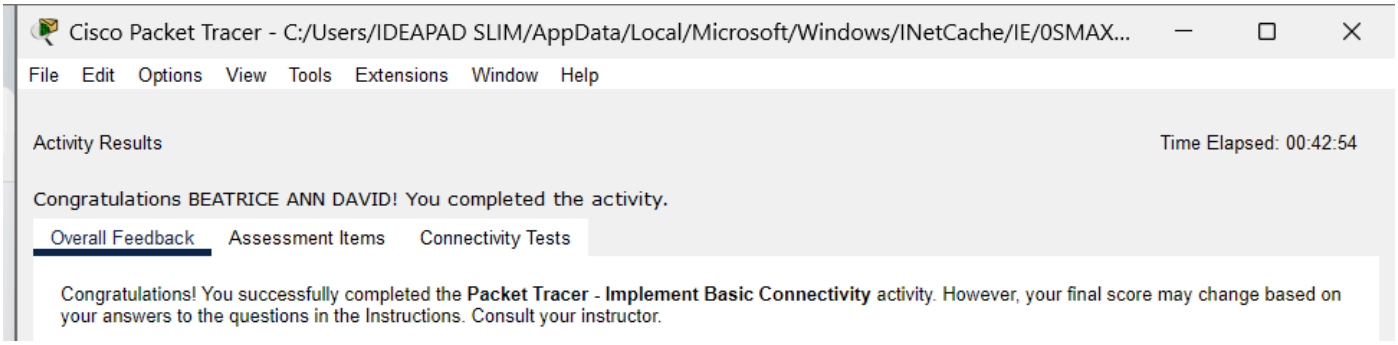
Part 3: Configure the Switch Management Interface

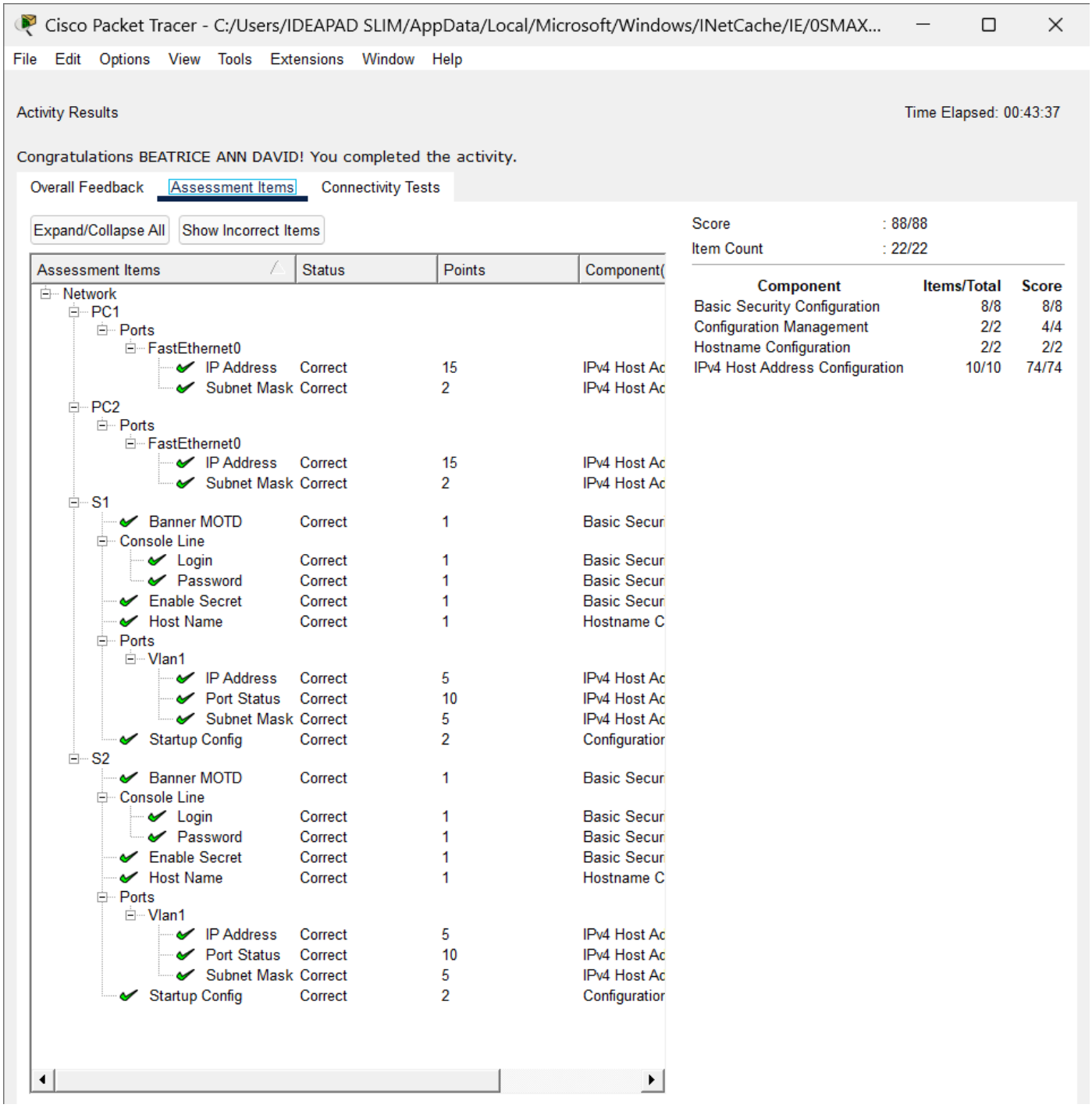
Background

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.

Screenshots:

A. Results





B. Working

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.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#
```

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.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#enable secret class
S1(config)#
```

Step 3: Verify the password configurations for S1.

How can you verify that both passwords were configured correctly?

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

S1#show running-config
Building configuration...

Current configuration : 1154 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$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
```

Step 4: Configure an MOTD banner.

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.

```
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#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:
```

Step 5: Save the configuration file to NVRAM.

Which command do you issue to accomplish this step?

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

Step 6: Repeat Steps 1 to 5 for S2.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#line console 0
S2(config-line)#password cisco
S2(config-line)#login
S2(config-line)#exit
S2(config)#enable secret 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#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#banner motd $Authorized access only. Violators will be prosecuted to the full extend of
the law.$
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.
```

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

User Access Verification

Password:

S2>enable
Password:
Password:
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
S2#
```

Part 2: Configure the PCs

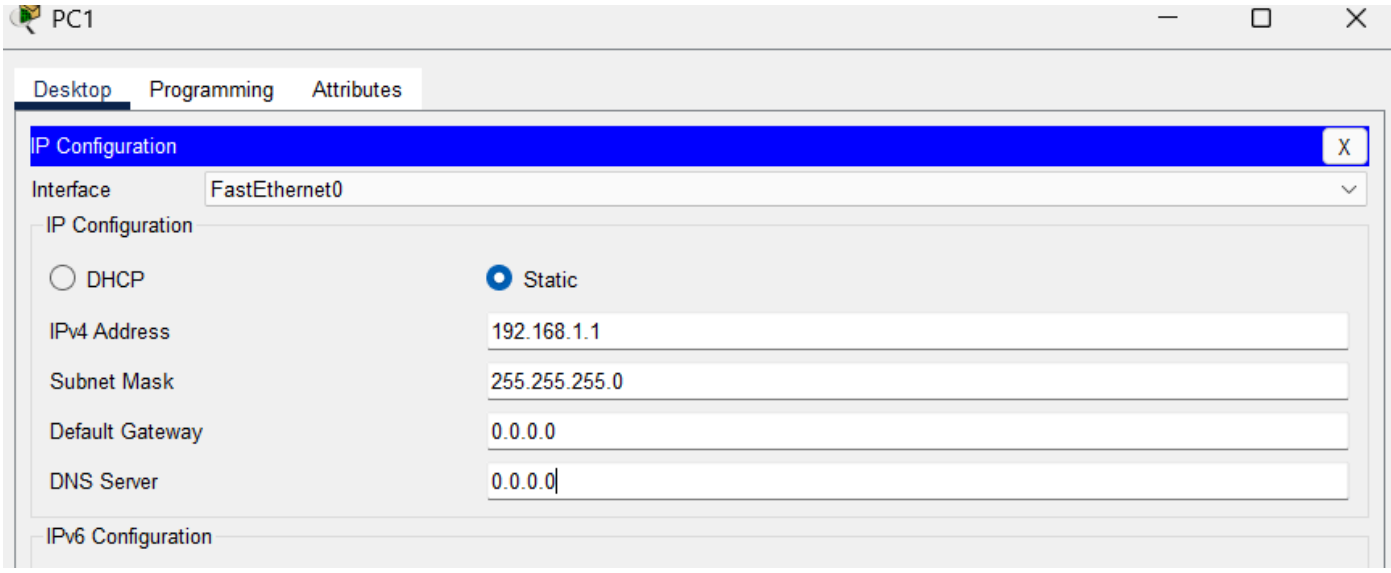
Configure PC1 and PC2 with IP addresses.

Step 1: Configure both PCs with IP addresses.

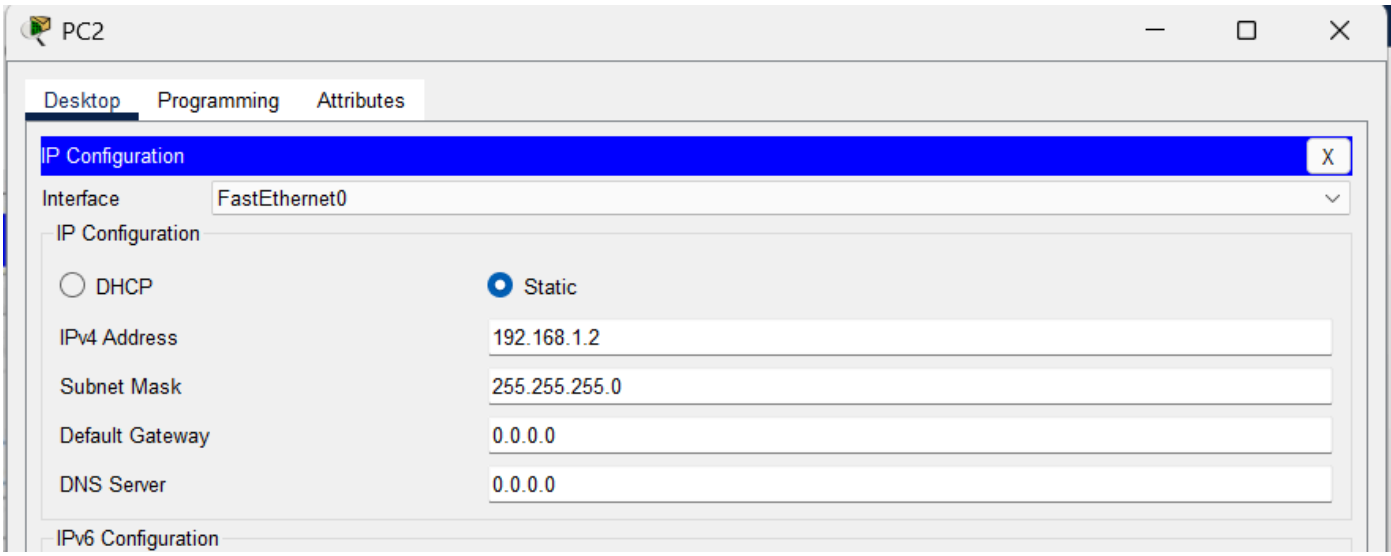
a. Click PC1 and then click the Desktop tab.

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
```

Were you successful? Explain.

```
Cisco Packet Tracer PC Command Line 1.0
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:\>
```

Not successful. Request timed out.

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?

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#
```

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

```
Password:

S1>enable
Password:
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 ?
  A.B.C.D  IP subnet mask
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)#
```

Because VLAN state is down. We want to change the state of VLAN1 to up.

Step 2: Configure S2 with an IP address.

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

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

User Access Verification

Password:

S2>enable
Password:
Password:
S2#show ip interface
Vlan1 is administratively down, line protocol is down
  Internet protocol processing disabled

S2#show ip interface brief
```

```
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                  unassigned      YES manual administratively down down
S2#
S2#
S2#
S2#
S2#
S2#
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface vlan1
S2(config-if)#ip address 192.168.1.254 255.255.255.0
S2(config-if)#no shutdown

S2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

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

S2(config-if)#
```

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

```
interface FastEthernet0/1

S2#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                  192.168.1.254   YES manual up                    up
S2#
S2#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
```

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

```
S2#show running-config
Building configuration...

Current configuration : 1267 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S2
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
!
!
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
!
```

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

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

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

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

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

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.

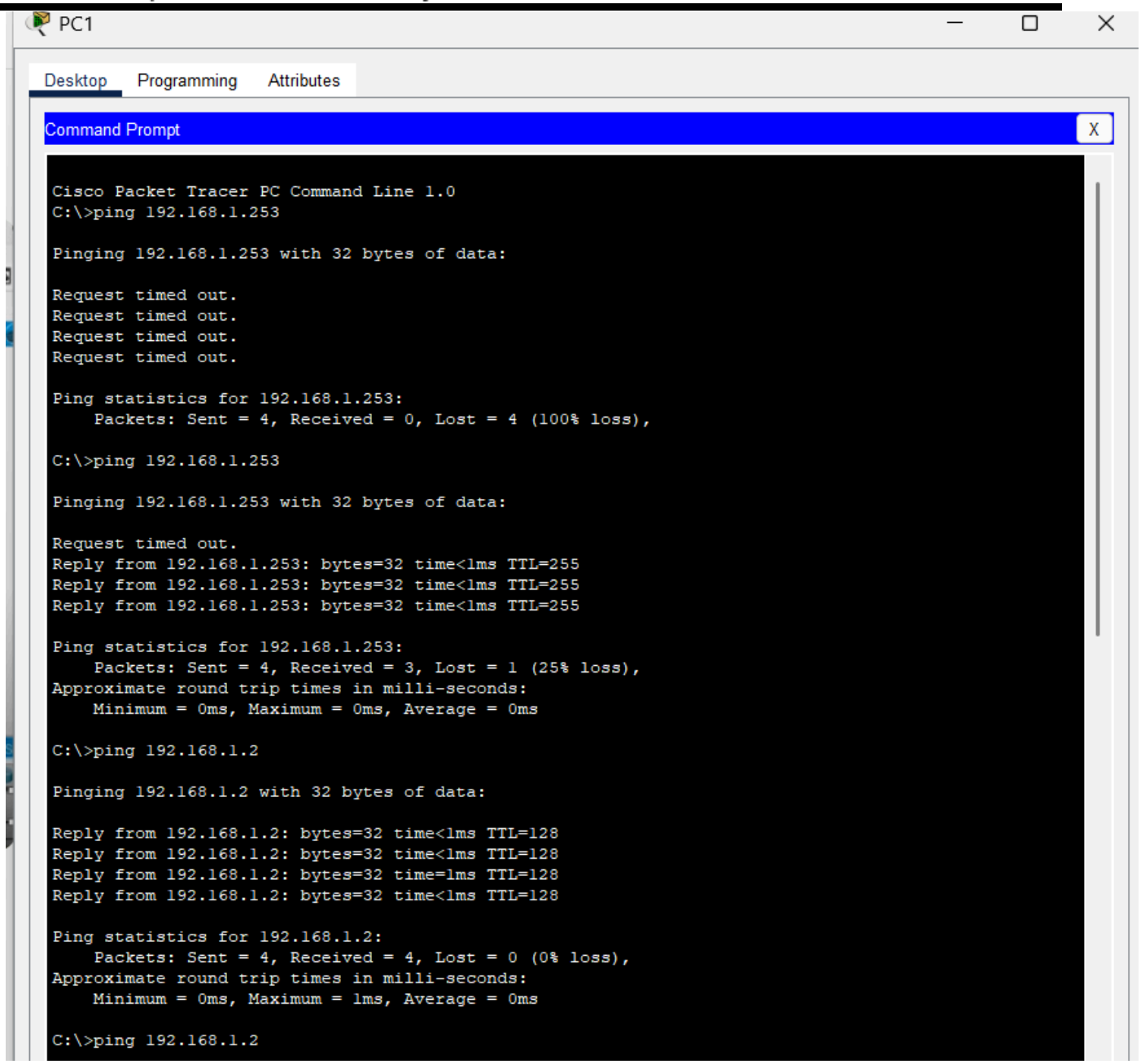
d. Ping the IP address for S1.

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.

Packet Tracer - Implement Basic Connectivity



Packet Tracer - Implement Basic Connectivity

```
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    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=6ms 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 = 6ms, Average = 1ms

C:\>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Request timed out.
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 = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

```
Building configuration...
[OK]
S1#ping ?
  WORD  Ping destination address or hostname
  ipv6  IPv6 echo
  <cr>
S1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

S1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/5 ms

S1#ping 192.168.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.254, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/2/6 ms

S1#ping 192.168.1.254

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#
```