VLANs and Secure Switch Configuration

Introduction

A Virtual Local Area Network (VLAN) is a way of logically dividing a physical LAN into multiple separate virtual networks that are broadcast domains. For example, we could have a network that is separate for guests or specific departments. The segmentation is done through software on a network switch. The segmentation allows devices to communicate as if they were on the same physical LAN, even if they are connected to different switches or in different physical locations. There is also traffic isolation provided by the VLANs; a broadcast frame sent within one VLAN is only seen by devices in that same VLAN, not by devices in other VLANs. Thus VLANs are used to improve security, network traffic management, and network administration.

VLANs are one of Layer 2's security features. Others include **port security** (limits the number of MAC addresses allowed on a switch port), **DHCP snooping** (prevents unauthorized DHCP servers from assigning IP addresses), and **dynamic ARP inspection** (validates ARP packets to prevent spoofing).

This lab aims to review previously covered Layer 2 security features while also covering switch security configuration.

Objectives

Part 1: Configure the Network Devices.

- Cable the network.
- Configure R1.
- Configure and verify basic switch settings.

Part 2: Configure VLANs on Switches.

- Configure VLAN 10.
- Configure the SVI for VLAN 10.
- Configure VLAN 333 with the name Native on S1 and S2.

- Configure VLAN 999 with the name ParkingLot on S1 and S2.

Part 3: Configure Switch Security.

- Implement 802.1Q trunking.
- Configure access ports.
- Secure and disable unused switchports.
- Document and implement port security features.
- Implement DHCP snooping security.
- Implement PortFast and BPDU guard.
- Verify end-to-end-connectivity.

Required Resources

• 1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.3 universal image or comparable)

• 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)

• 2 PCs (Windows with a terminal emulation program, such as Tera Term)

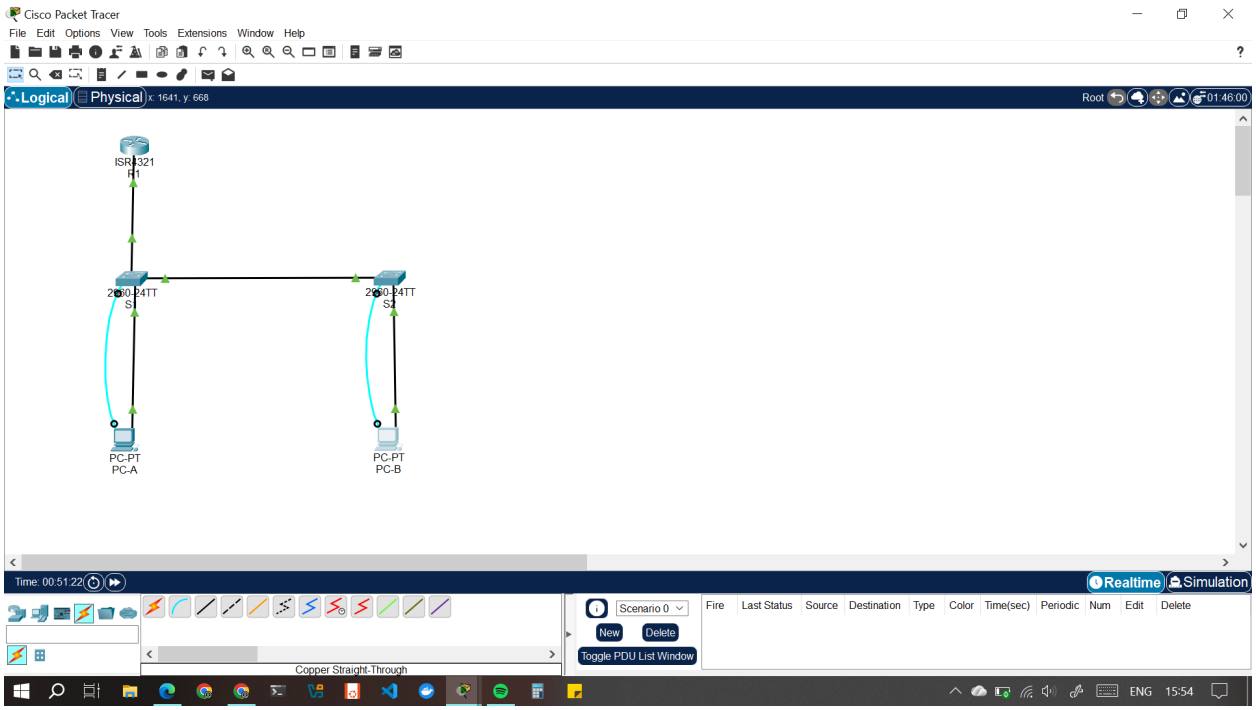
• Console cables to configure the Cisco IOS devices via the console ports

• Ethernet cables as shown in the topology

Part 1: Configure the Network Devices.

Step 1: Cable the network.

1. Cable the network as shown in the topology.
2. Initialize the devices.



Step 2: Configure R1.

1. Load the following configuration script on R1.

   enable

   configure terminal

   hostname R1

   no ip domain lookup

   ip dhcp excluded-address 192.168.10.1 192.168.10.9

   ip dhcp excluded-address 192.168.10.201 192.168.10.202

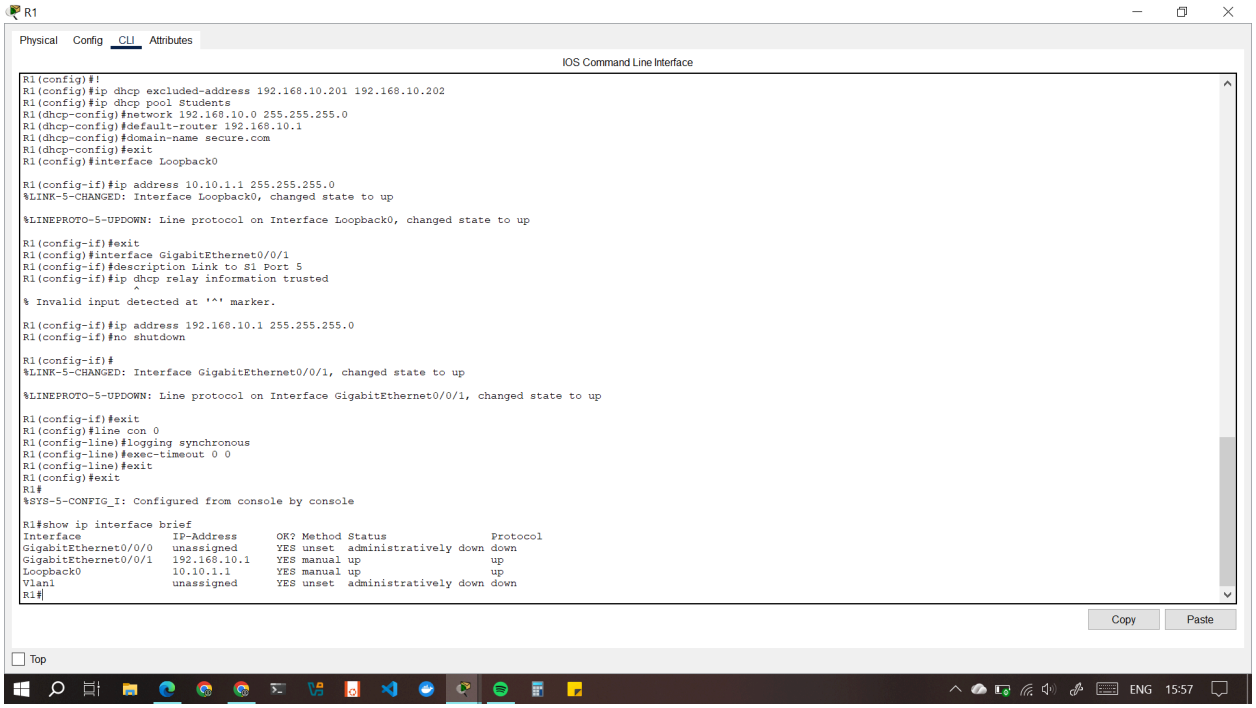
   !

   ip dhcp pool Students

   network 192.168.10.0 255.255.255.0

```
        default-router 192.168.10.1
        domain-name secure.com
!
interface Loopback0
        ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet0/0/1
        description Link to S1 Port 5
        ip dhcp relay information trusted
        ip address 192.168.10.1 255.255.255.0
        no shutdown
!
line con 0
        logging synchronous
        exec-timeout 0 0
```

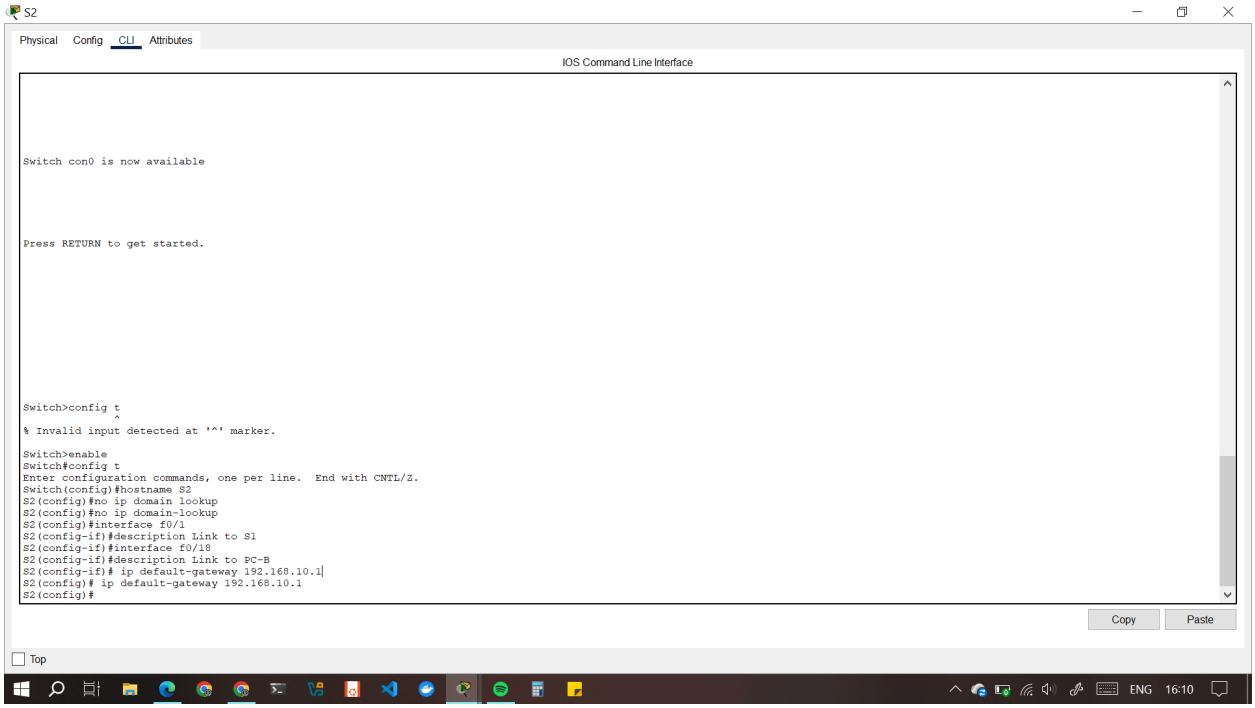
2. Verify the running-configuration on R1 using the following command: **show ip interface brief**

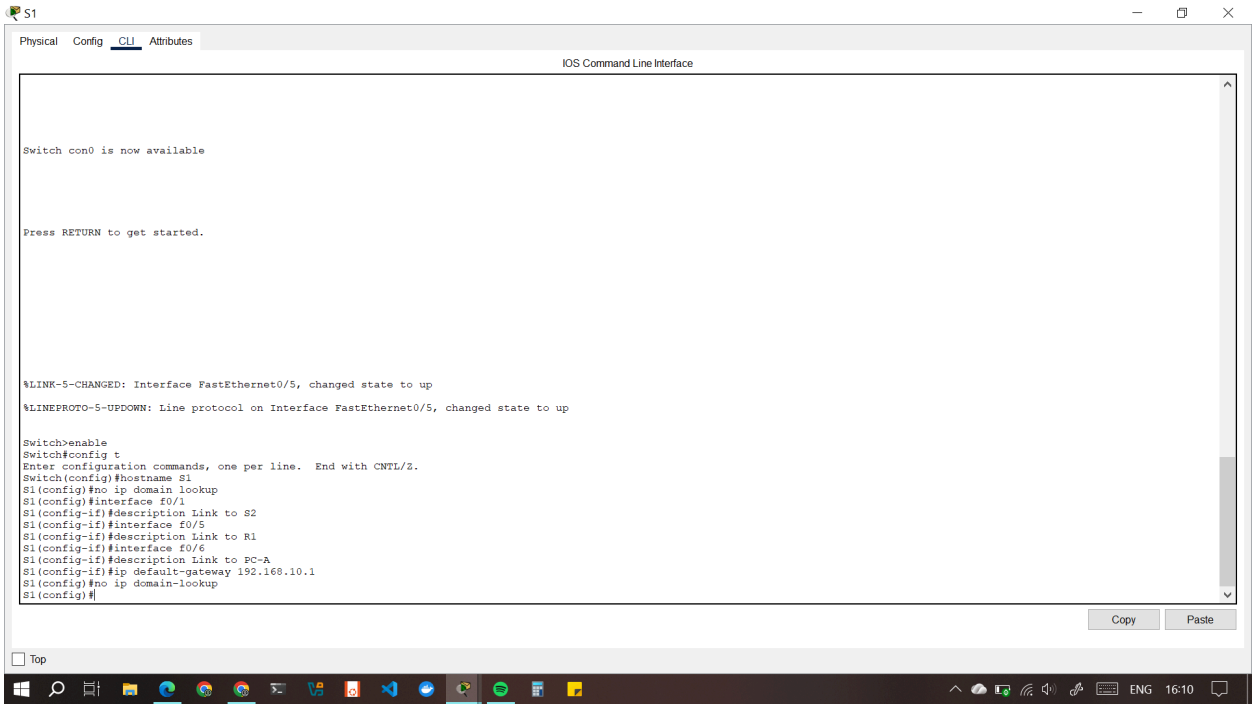


3. Verify IP addressing and interfaces are in an up / up state (troubleshoot as necessary).

Step 3: Configure and verify basic switch settings.

1. Configure the hostname for switches S1 and S2.
2. Prevent unwanted DNS lookups on both switches.
3. Configure interface descriptions for the ports that are in use in S1 and S2.
4. Set the default-gateway for the Management VLAN to 192.168.10.1 on both switches.

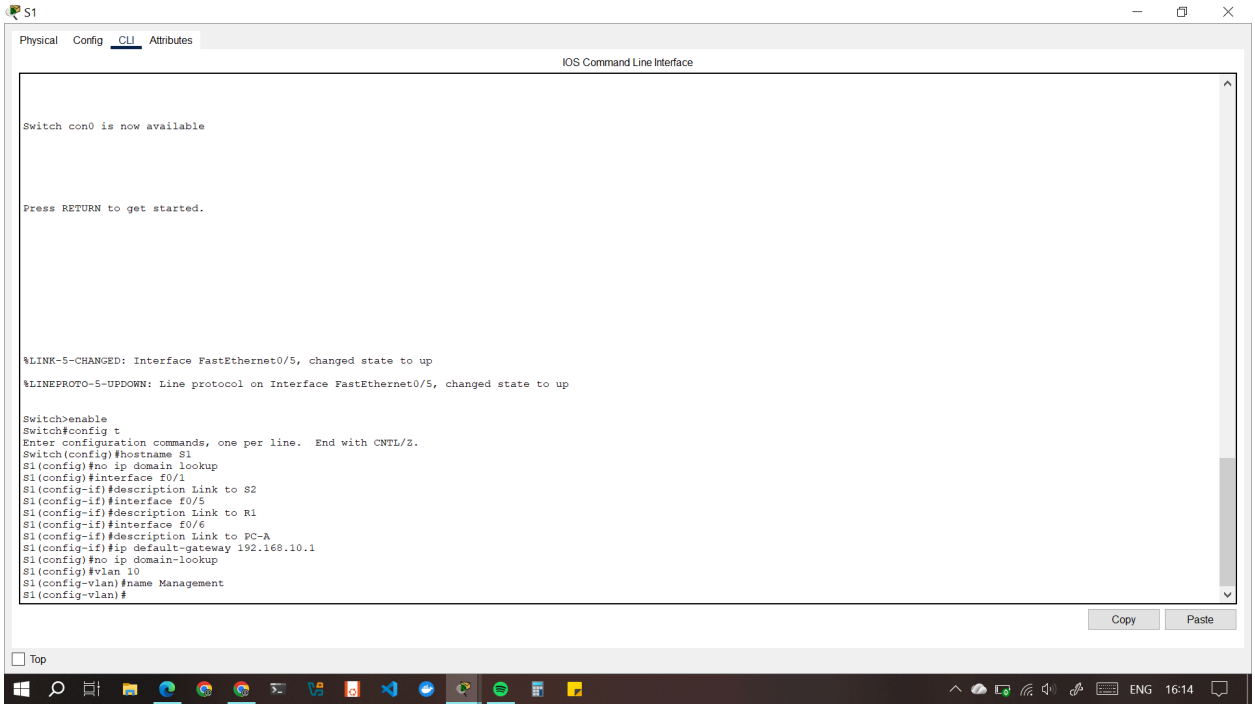

S2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch con0 is now available
Press RETURN to get started.
Switch>config t
^
% Invalid input detected at '^' marker.
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain lookup
S2(config)#no ip domain-lookup
S2(config)#interface f0/1
S2(config-if)#description Link to S1
S2(config-if)#interface f0/18
S2(config-if)#description Link to PC-B
S2(config-if)# ip default-gateway 192.168.10.1
S2(config)# ip default-gateway 192.168.10.1
S2(config)#
Copy
Paste
Top
ENG
16:10

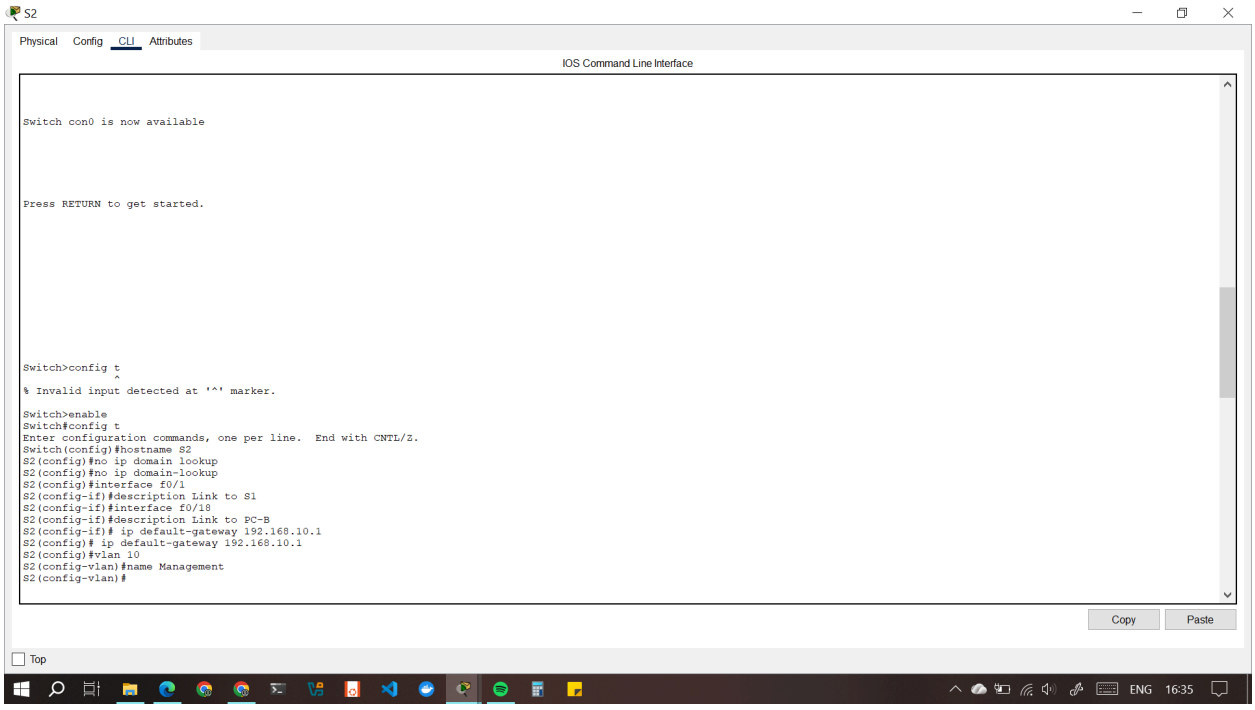

S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch con0 is now available
Press RETURN to get started.
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
Switch>enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain lookup
S1(config)#interface f0/1
S1(config-if)#description Link to S2
S1(config-if)#interface f0/5
S1(config-if)#description Link to R1
S1(config-if)#interface f0/6
S1(config-if)#description Link to PC-A
S1(config-if)#ip default-gateway 192.168.10.1
S1(config)#no ip domain-lookup
S1(config)#
Copy
Paste
Top
ENG
16:10

Part 2: Configure VLANs on Switches.

Step 1: Configure VLAN 10.

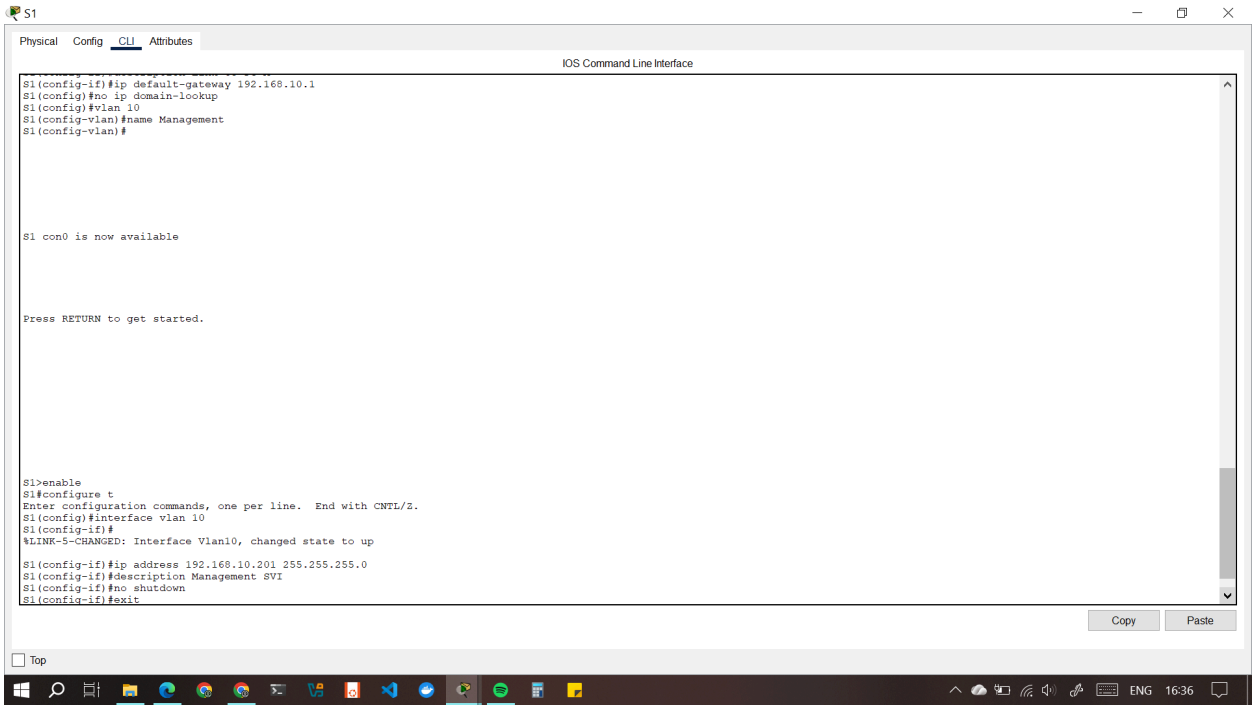
1. Add VLAN 10 to S1 and S2 and name the VLAN Management.

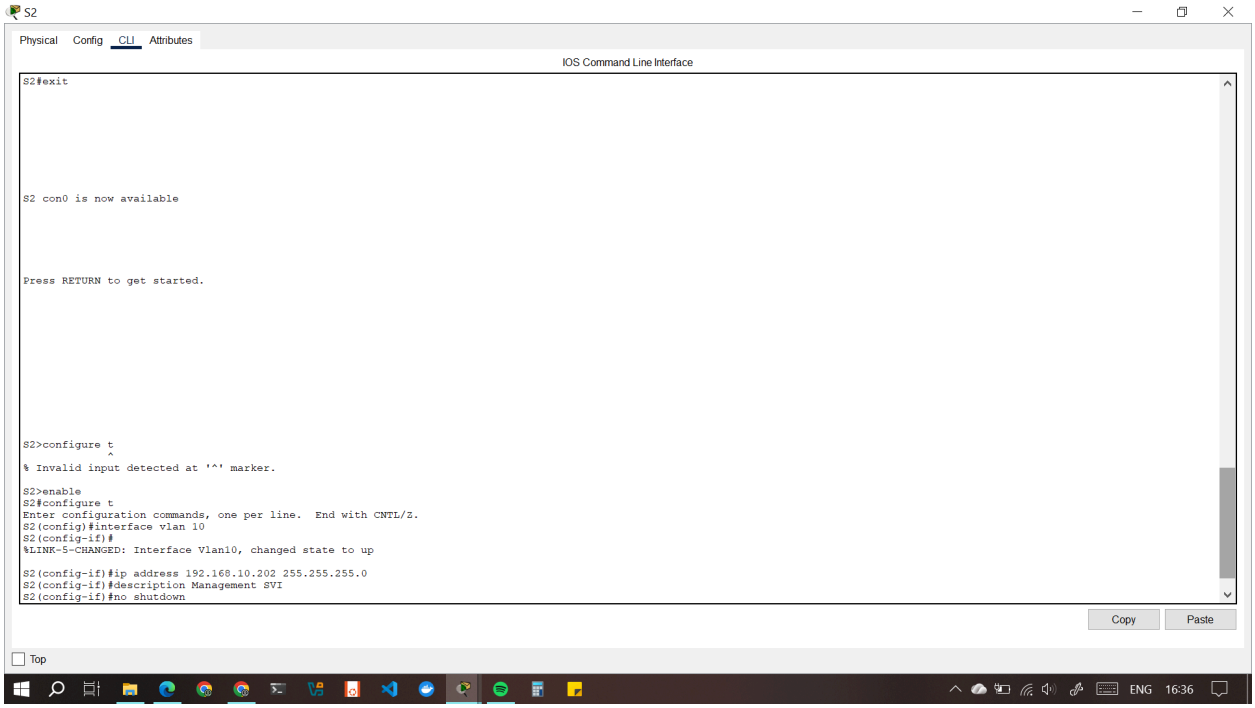




Step 2: Configure the SVI for VLAN 10.

2. Configure the IP address according to the Addressing Table for SVI for VLAN 10 on S1 and S2. Enable the SVI interfaces and provide a description for the interface.





Step 3: Configure VLAN 333 with the name Native on S1 and S2.

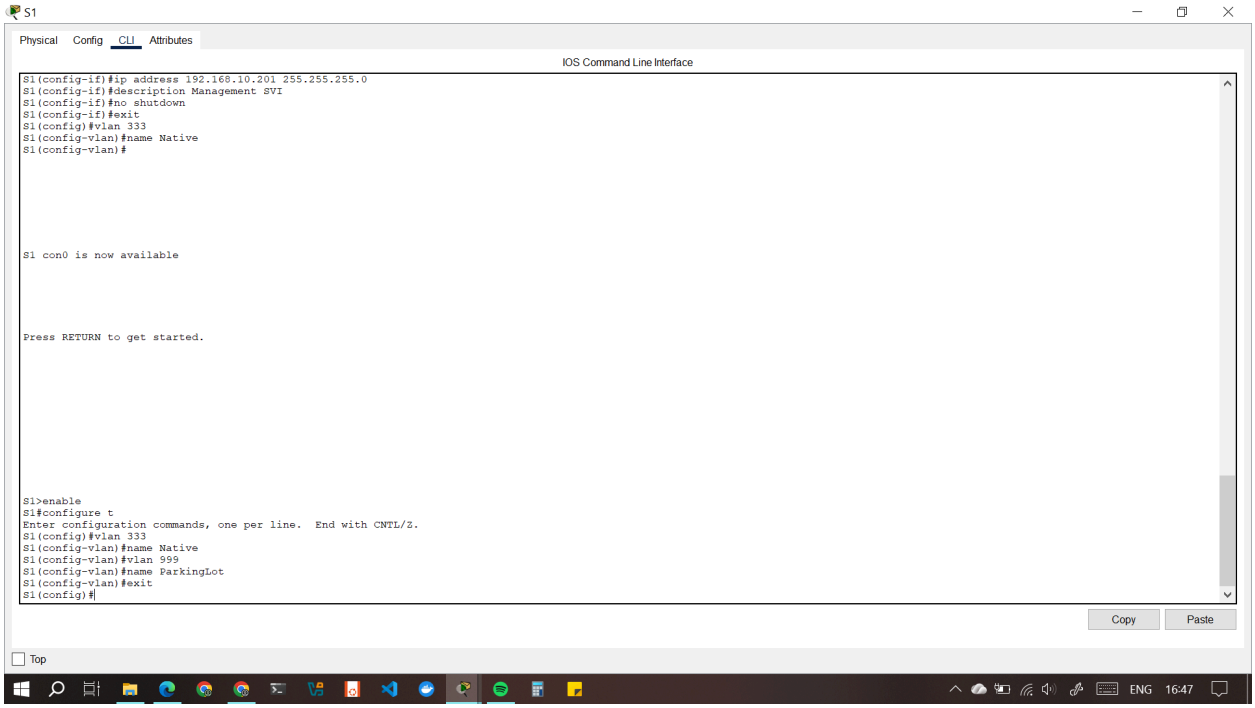
Step 4: Configure VLAN 999 with the name ParkingLot on S1 and S2.

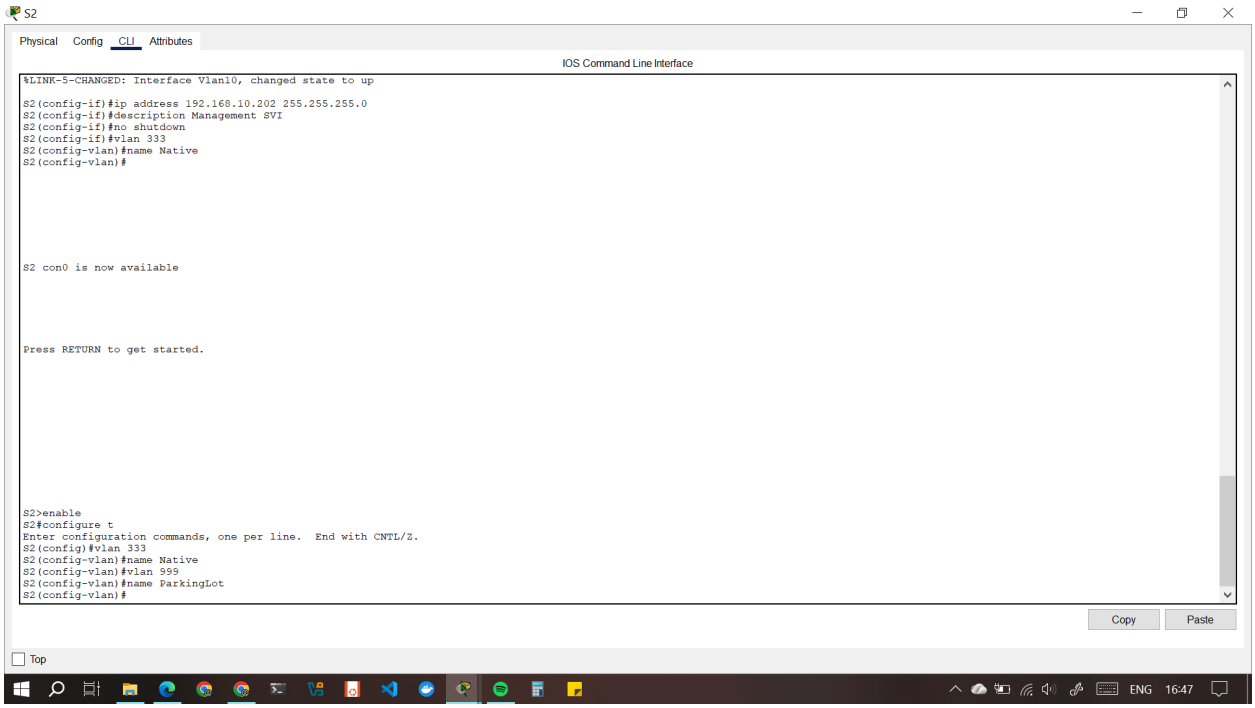
S1(config-vlan)# vlan 999

S1(config-vlan)# name ParkingLot

S2(config-vlan)# vlan 999

S2(config-vlan)# name ParkingLot



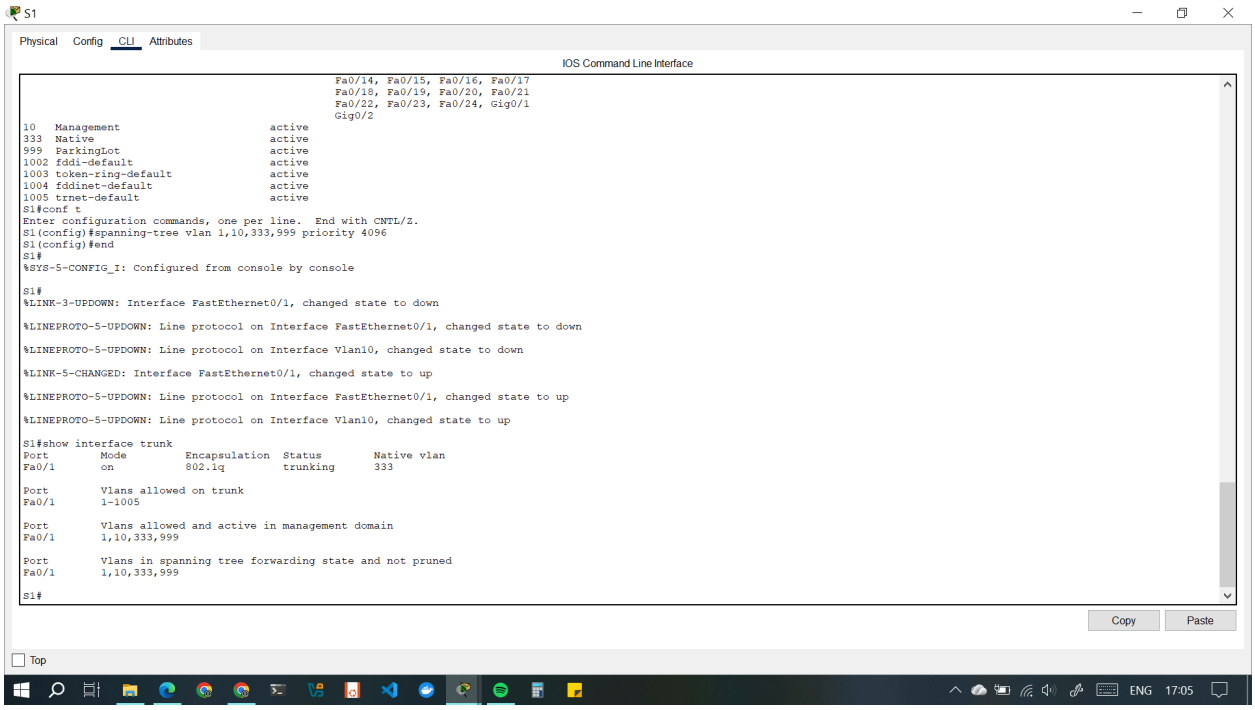


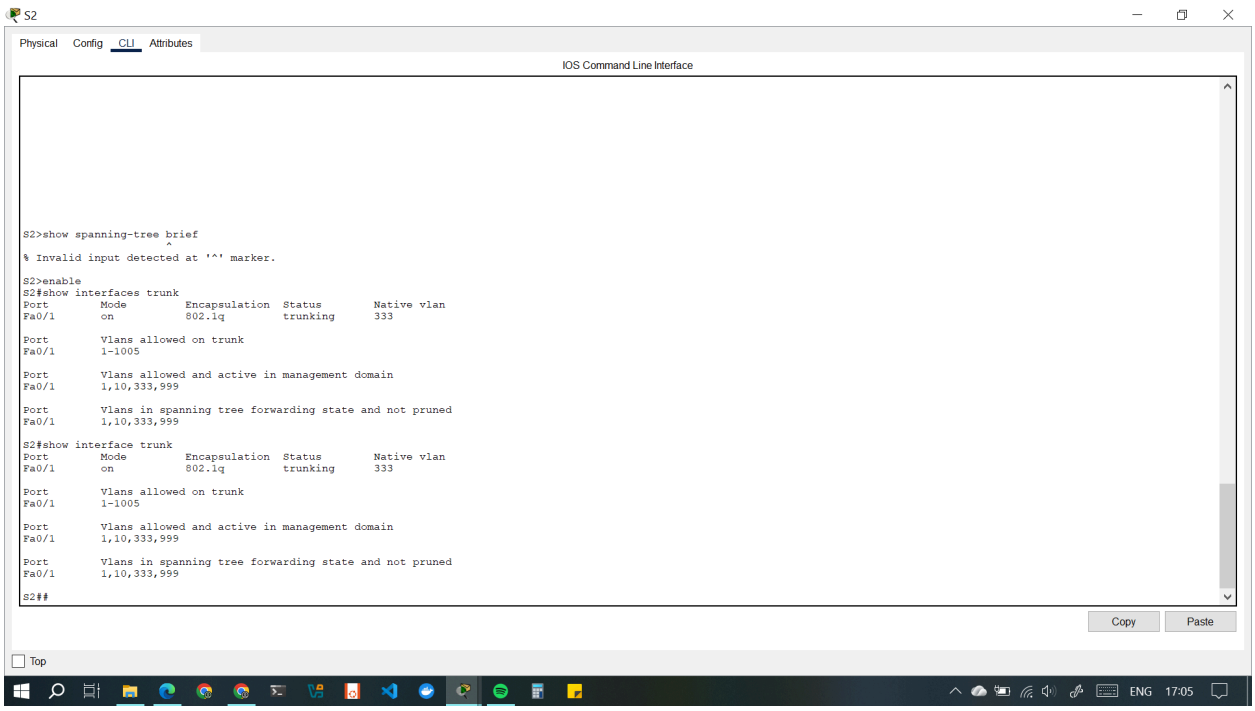
Part 3: Configure Switch Security.

Step 1: Implement 802.1Q trunking.

1. On both switches, configure trunking on F0/1 to use VLAN 333 as the native VLAN.

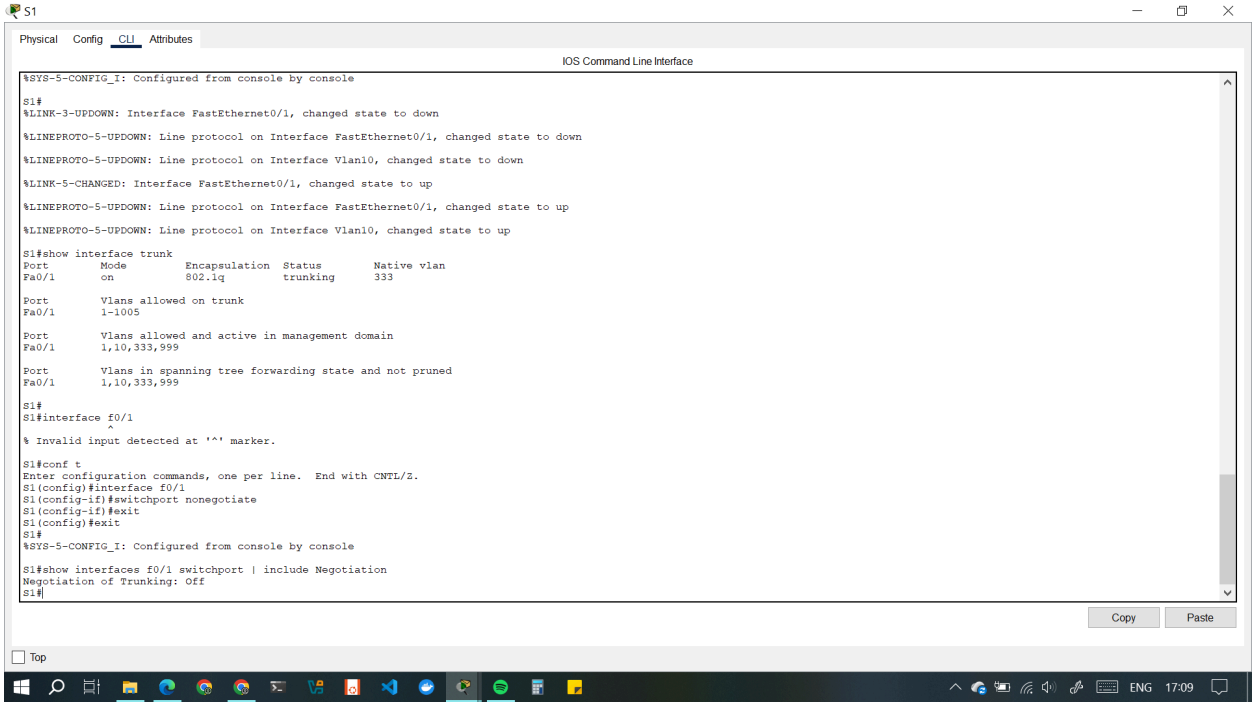
2. Verify that trunking is configured on both switches.

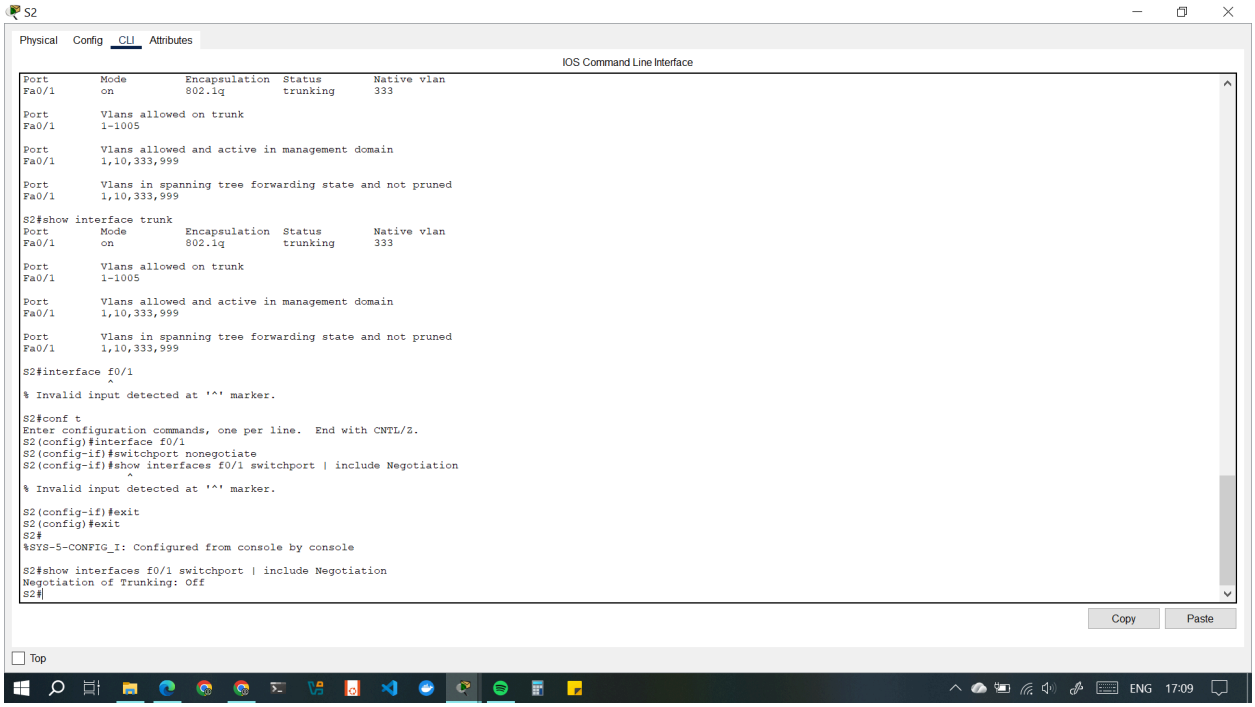




3. Disable DTP negotiation on F0/1 on S1 and S2.

4. Verify with the show interfaces command.

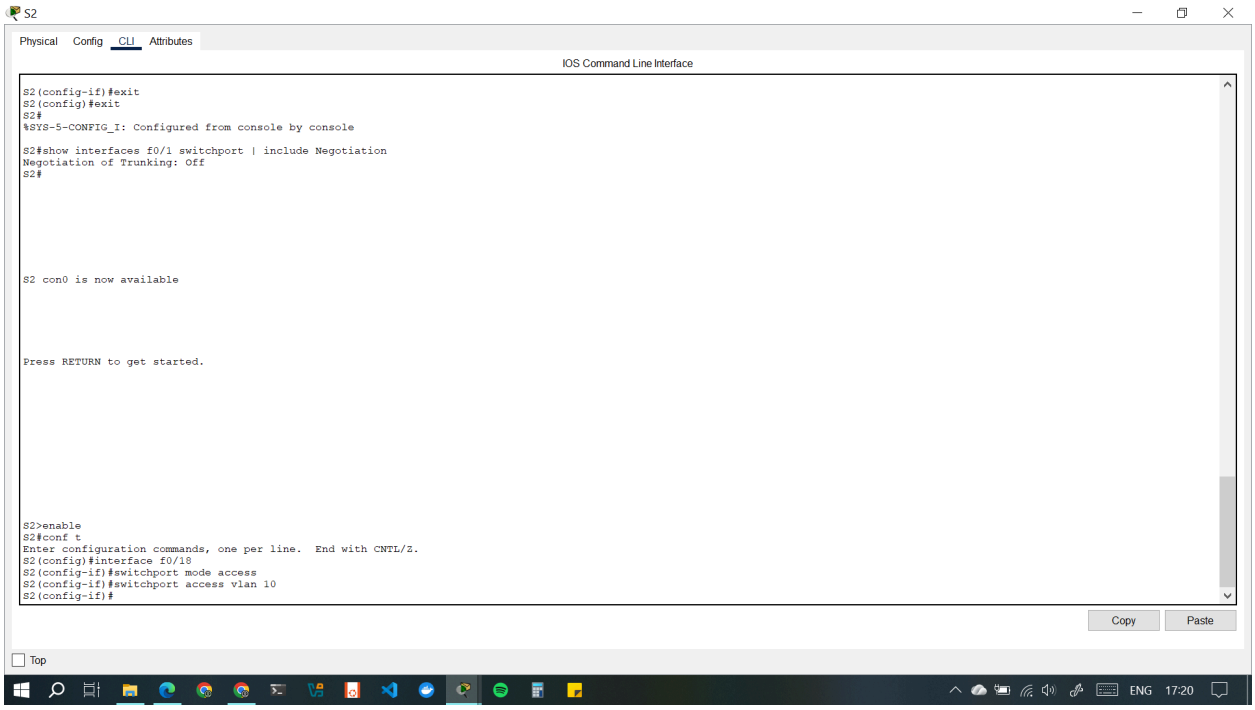


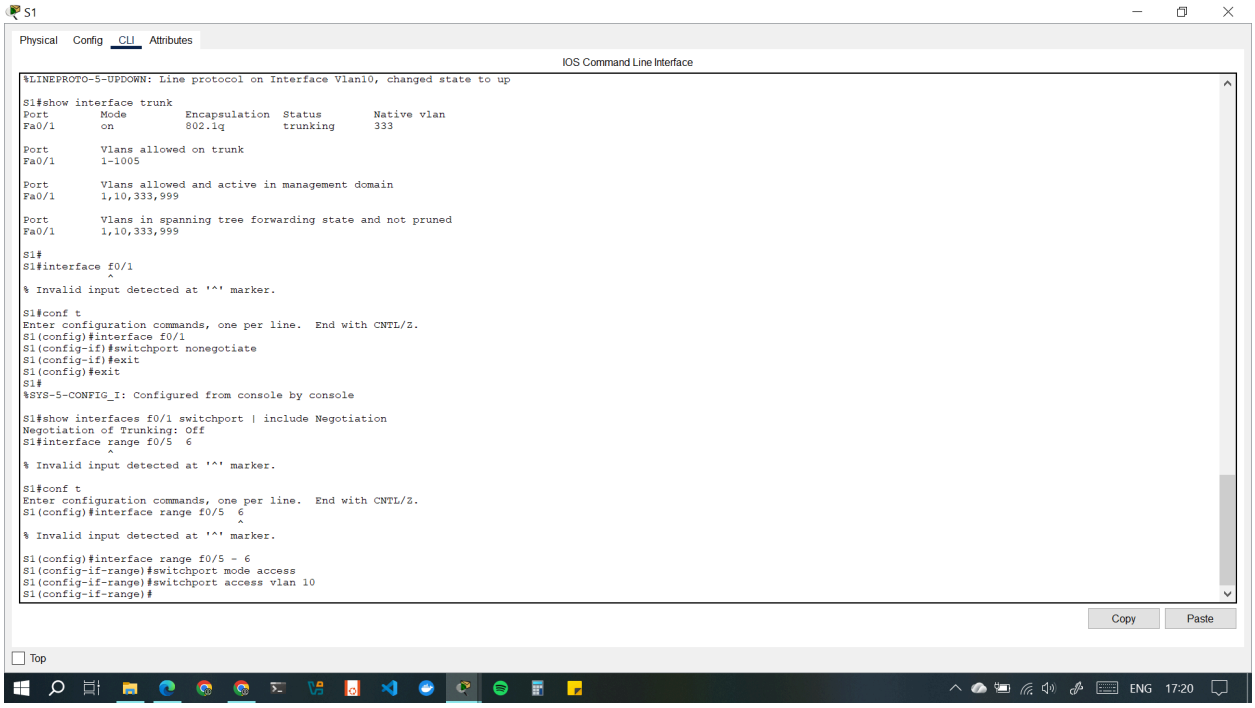


Step 2: Configure access ports.

1. On S1, configure F0/5 and F0/6 as access ports that are associated with VLAN 10.

2. On S2, configure F0/18 as an access port that is associated with VLAN 10.

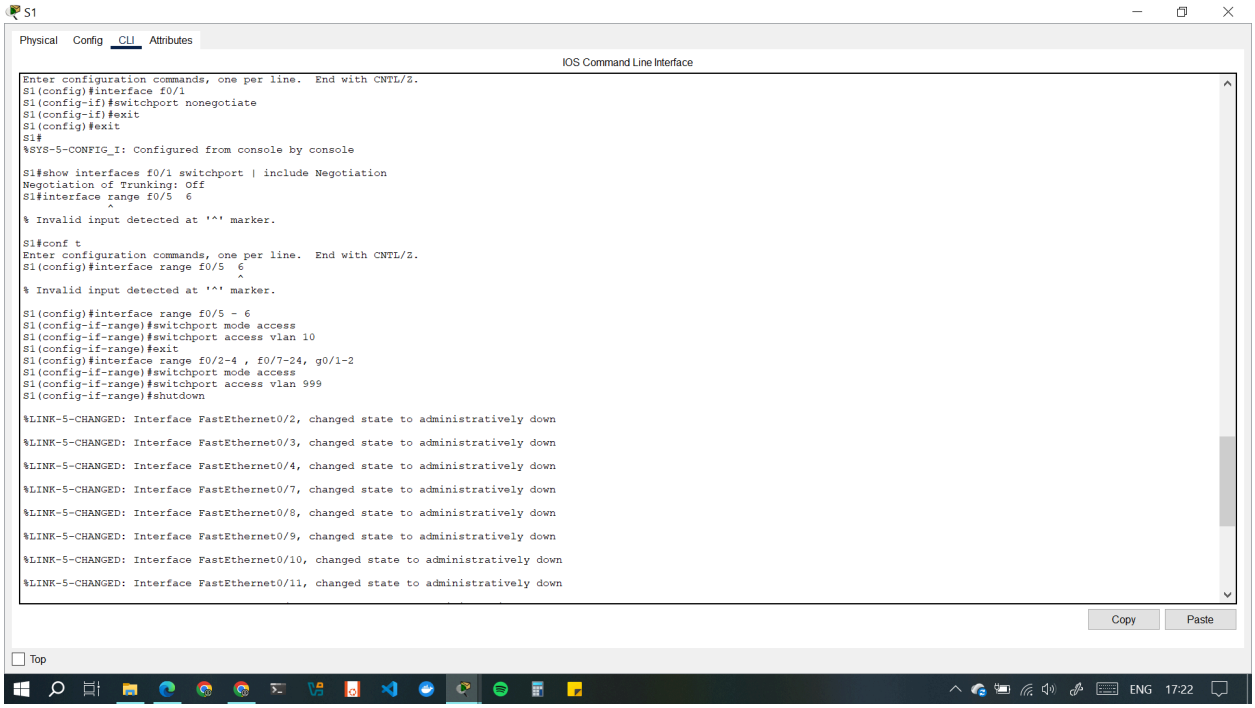


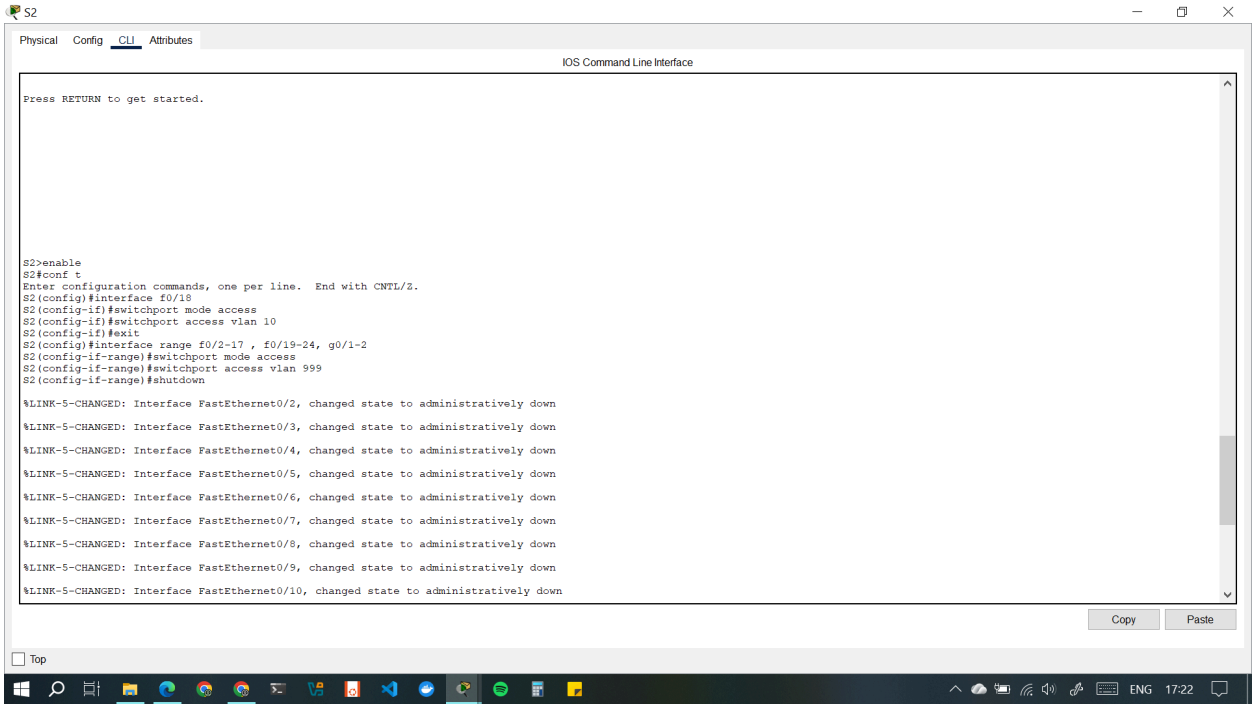


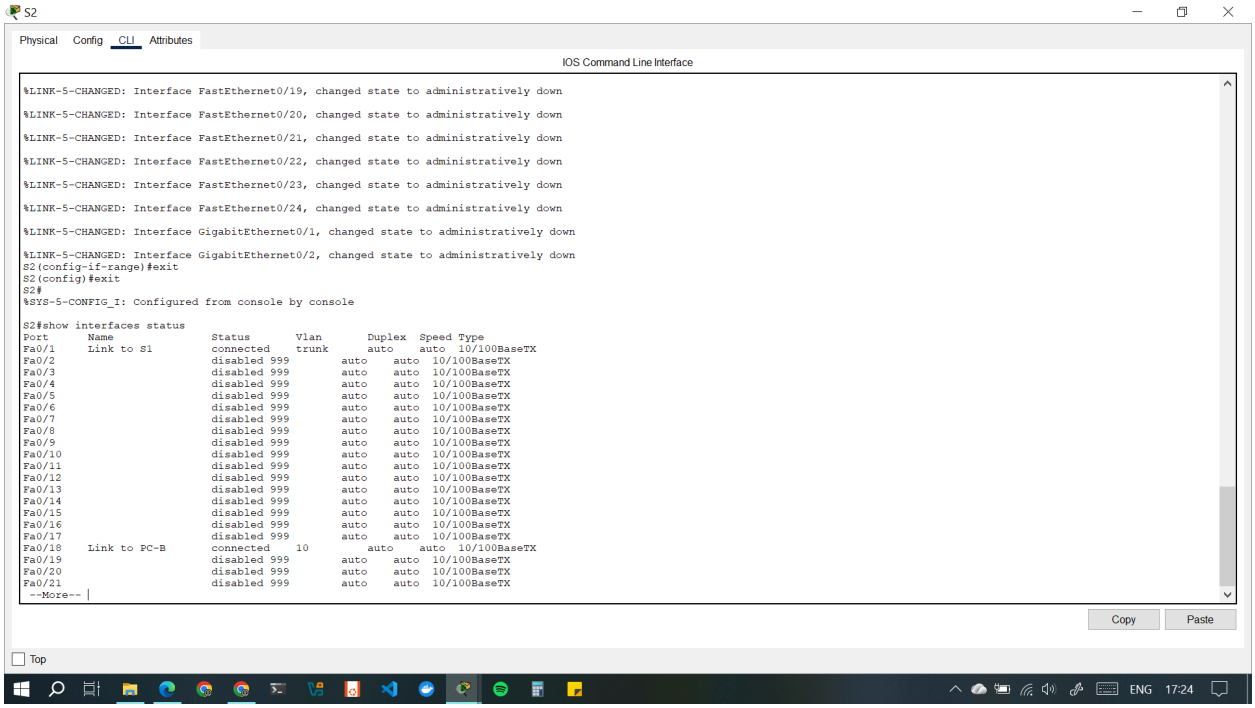
Step 3: Secure and disable unused switchports.

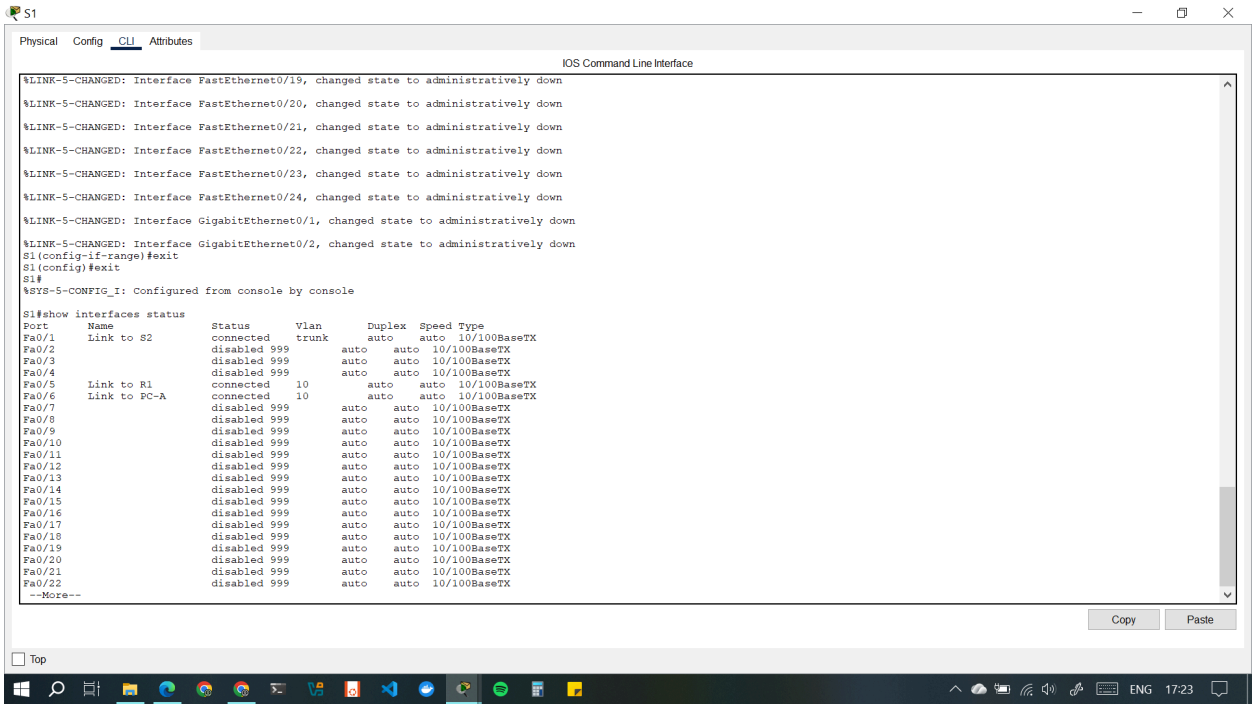
1. On S1 and S2, move the unused ports from VLAN 1 to VLAN 999 and disable the unused ports.

2. Verify that unused ports are disabled and associated with VLAN 999 by issuing the show command.




S2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started.
S2>enable
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#exit
S2(config)#interface range f0/2-17 , f0/19-24, g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 999
S2(config-if-range)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down
Copy
Paste
Top
ENG
17:22





Step 4: Document and implement port security features.

The interfaces F0/6 on S1 and F0/18 on S2 are configured as access ports. In this step, you will also

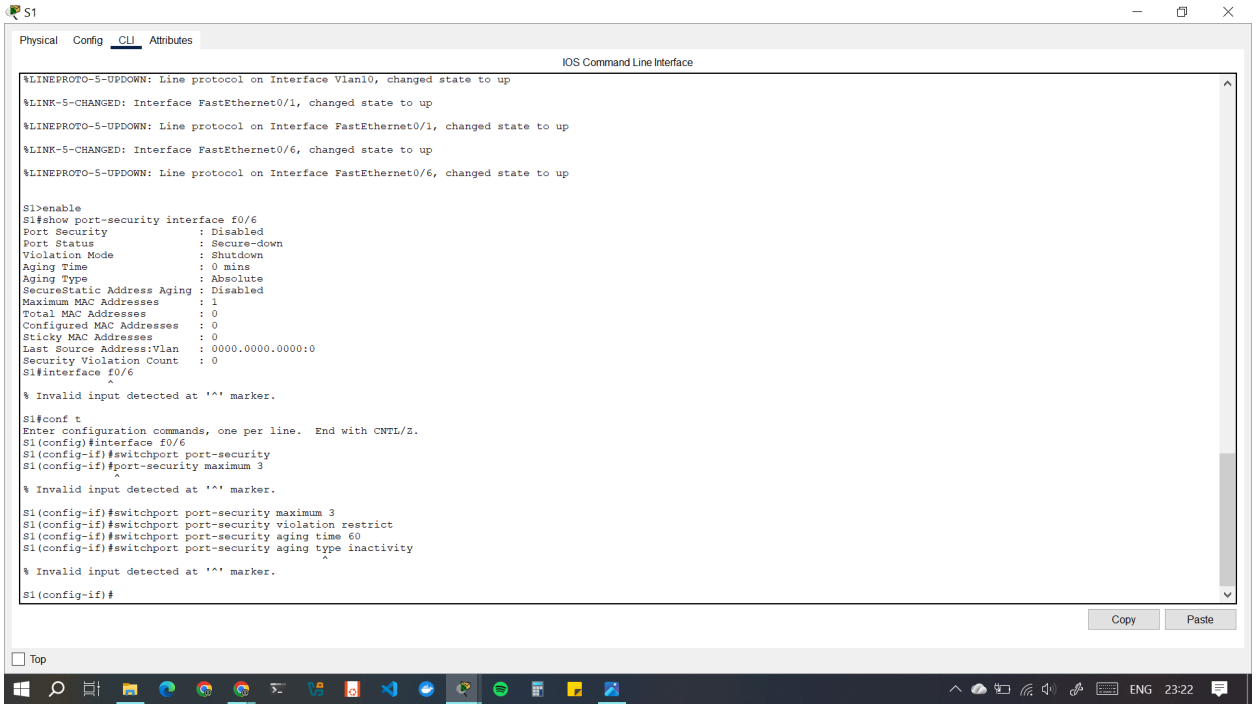
configure port security on these two access ports.

1. On S1, issue the **show port-security interface f0/6** command to display the default port security settings for interface F0/6. Record your answers in the table below.

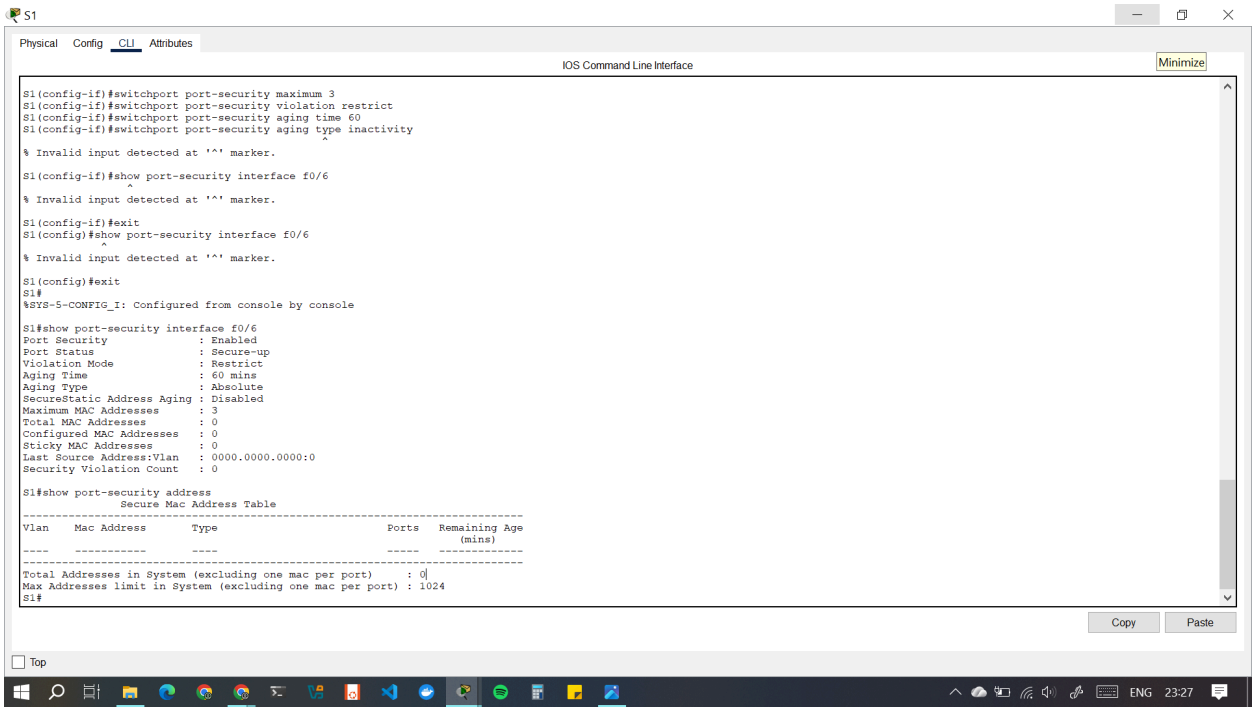
Default Port Security Configuration	
Feature	**Default Setting**
Port security	**Disabled**
Max. number of MAC addresses	**1**
Violation mode	**Shutdown**
Aging Time	**0 mins**
Aging Type	**Absolute**
Secure Static Address Aging	**Disabled**
Sticky MAC Address	**0**

2. On S1, enable port security on F0/6 with the following settings:

- Maximum number of MAC addresses: 3
- Violation type: restrict
- Aging time: 60 min
- Aging type: inactivity



3. Verify port security on S1 F0/6 using **show port-security interface f0/6 and show port-security address.**



4. Enable port security for F0/18 on S2. Configure the port to add MAC addresses learned on the port automatically to the running configuration.

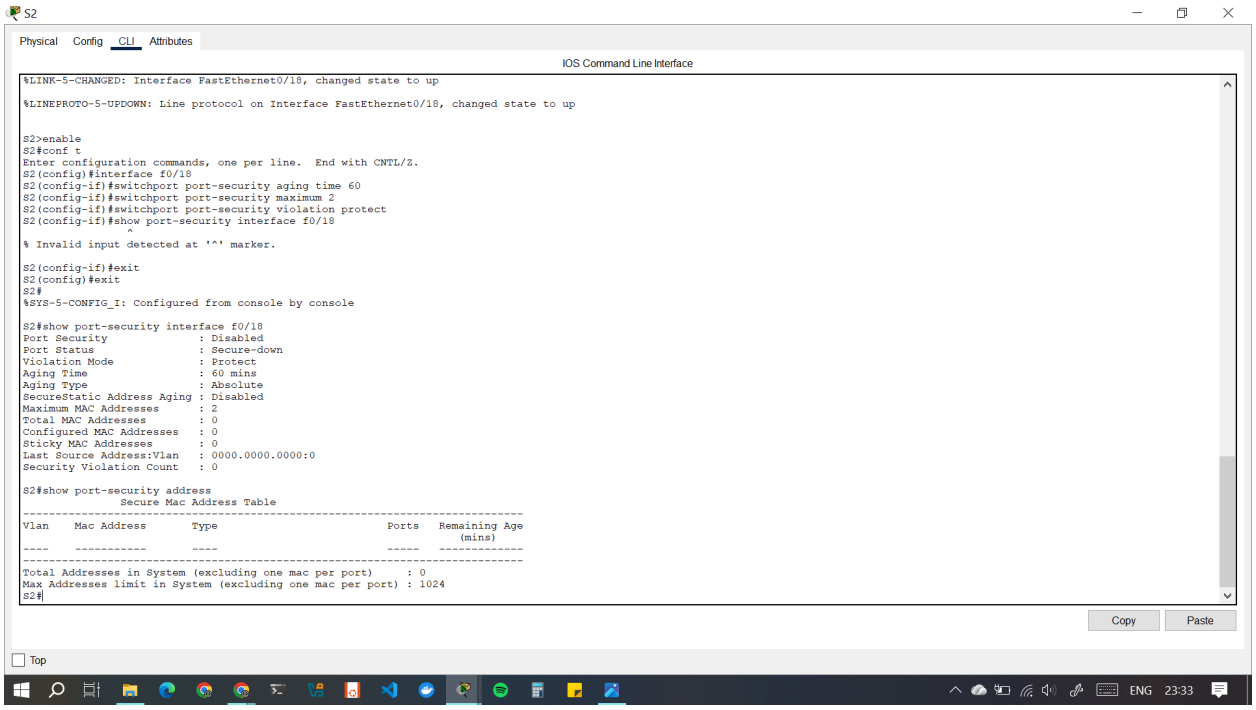
5. Configure the following port security settings on S2 F/18:

• Maximum number of MAC addresses: 2

• Violation type: Protect

• Aging time: 60 min

6. Verify port security on S2 F0/18.



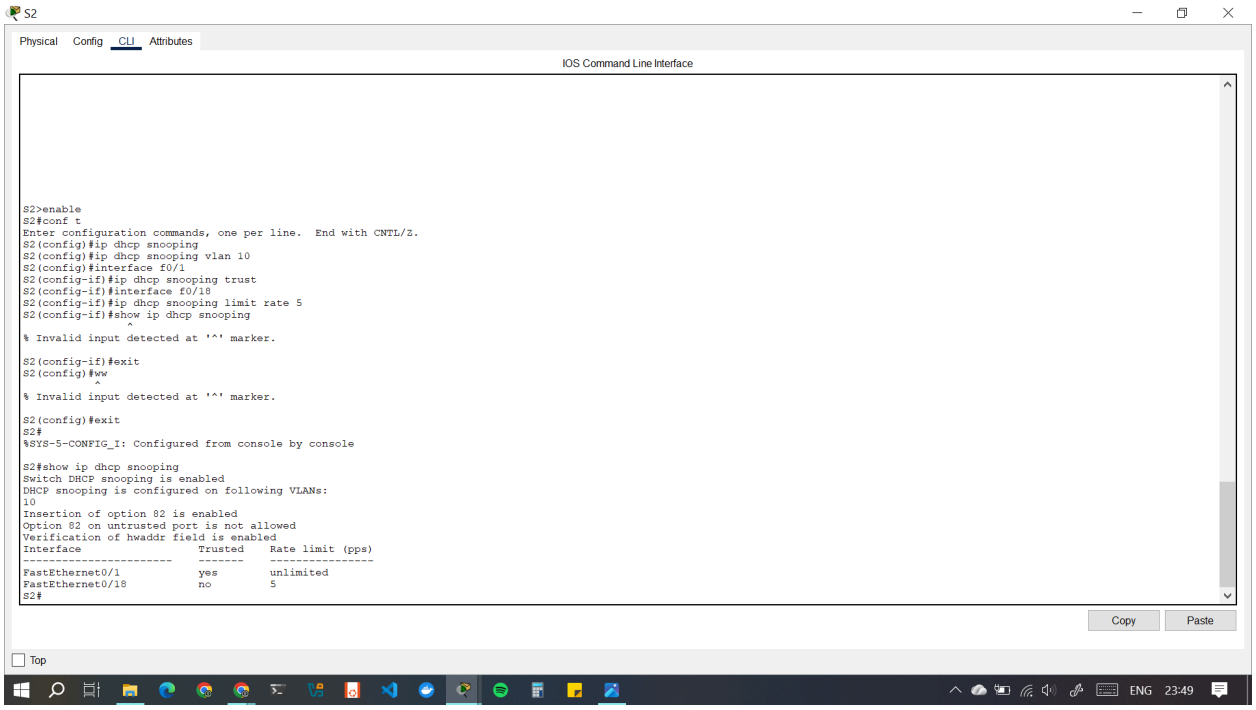
Step 5: Implement DHCP snooping security.

1. On S2, enable DHCP snooping and configure DHCP snooping on VLAN 10.

2. Configure the trunk port on S2 as a trusted port.

3. Limit the untrusted port, F18 on S2, to five DHCP packets per second.

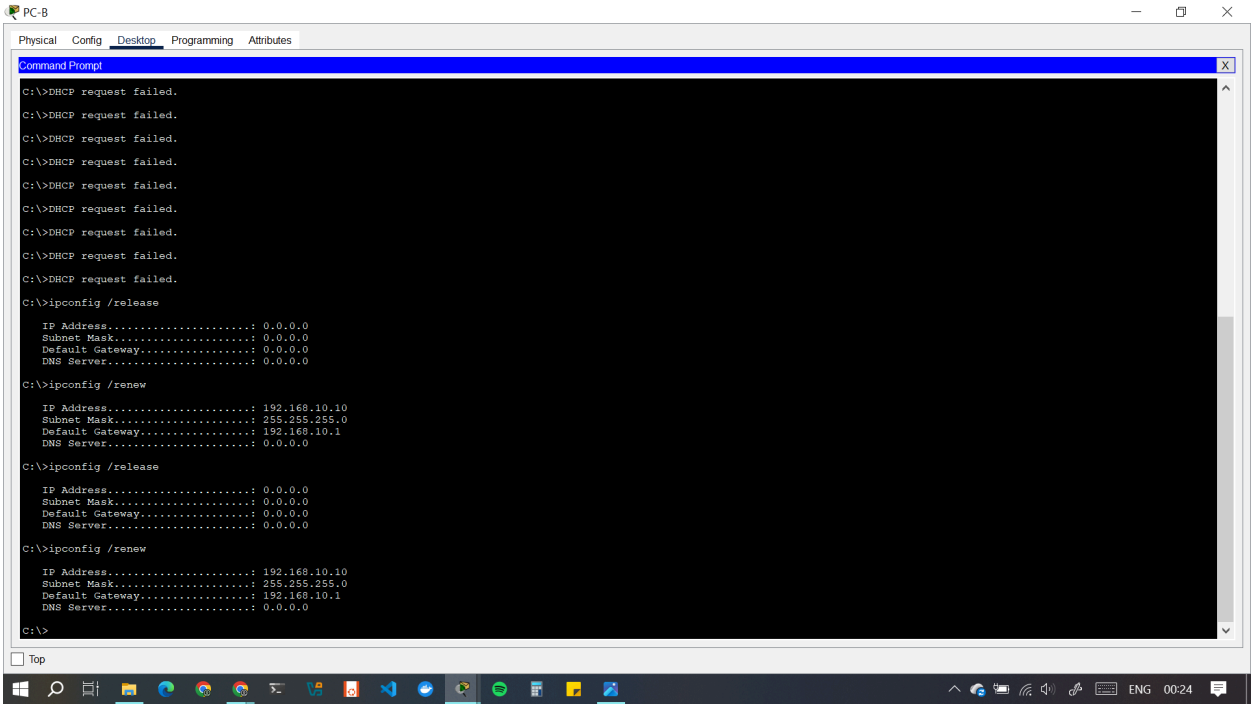
4. Verify DHCP Snooping on S2.



5. From the command prompt on PC-B, release and then renew the IP address.

C:\Users\Student> ipconfig /release

C:\Users\Student> ipconfig /renew



6. Verify the DHCP snooping binding using the show ip dhcp snooping binding command.

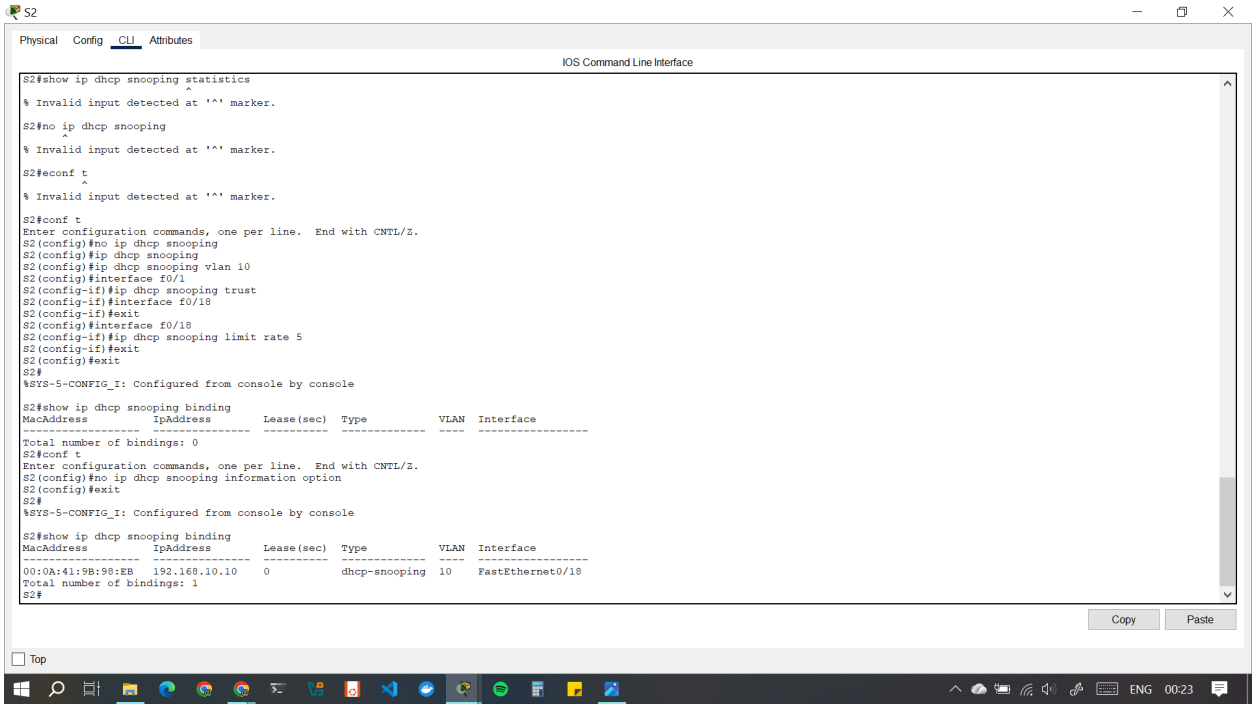
S2# show ip dhcp snooping binding

MacAddress IpAddress Lease(sec) Type VLAN Interface

——————— ——————— ———— ——————— —— ——————————

00:50:56:90:D0:8E 192.168.10.11 86213 dhcp-snooping 10 FastEthernet0/18

Total number of bindings: 1



Step 6: Implement PortFast and BPDU guard.

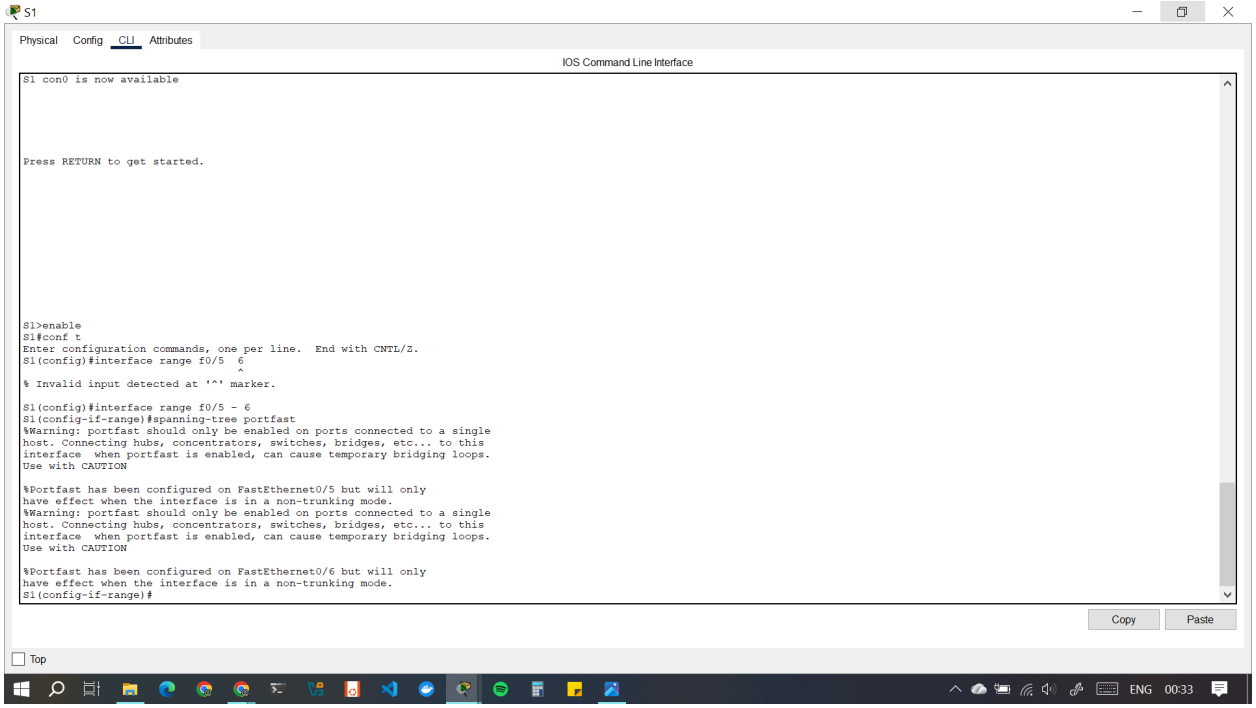
1. Configure PortFast on all the access ports that are in use on both switches.

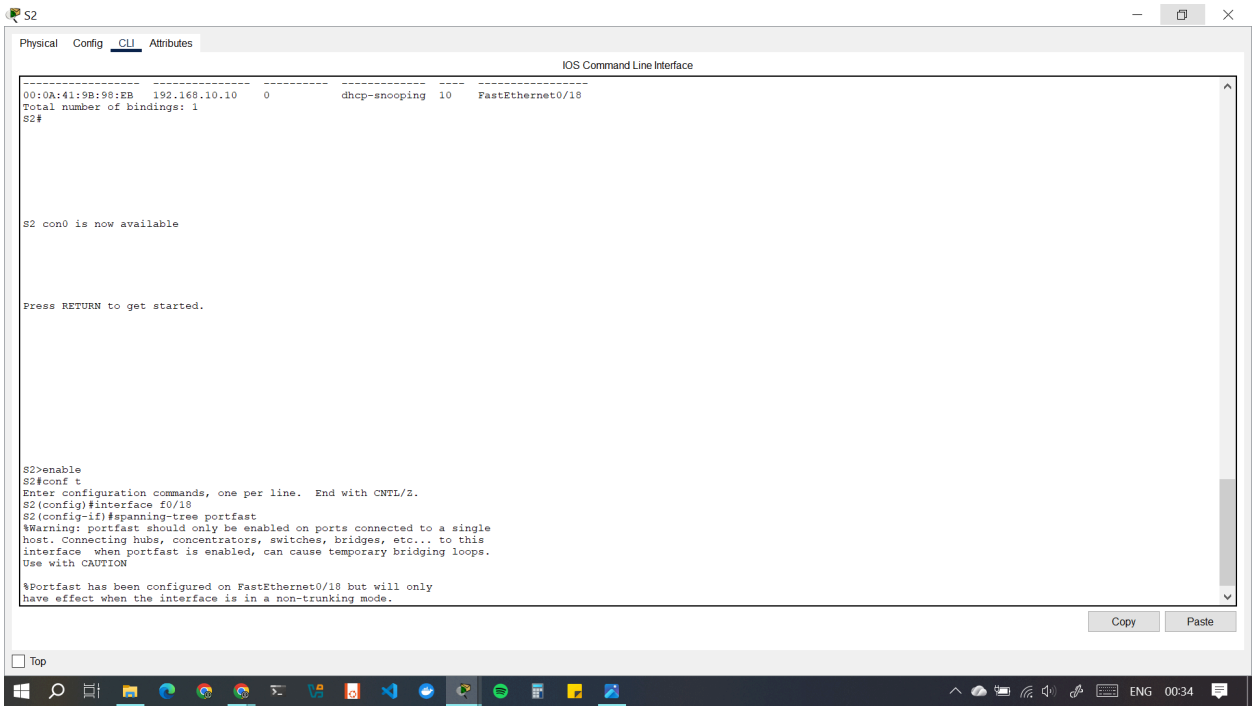
S1(config)# interface range f0/5 – 6

S1(config-if)# spanning-tree portfast

S2(config)# interface f0/18

S2(config-if)# spanning-tree portfast





2. Enable BPDU guard on S1 and S2 VLAN 10 access ports connected to PC-A and PC-B.

S1(config)# interface f0/6

S1(config-if)# spanning-tree bpduguard enable

S2(config)# interface f0/18

S2(config-if)# spanning-tree bpduguard enable

3. Verify that BPDU guard and PortFast are enabled on the appropriate ports.

S1# show spanning-tree interface f0/6 detail

Port 8 (FastEthernet0/6) of VLAN0010 is designated forwarding

Port path cost 19, Port priority 128, Port Identifier 128.6.

<output omitted for brevity>

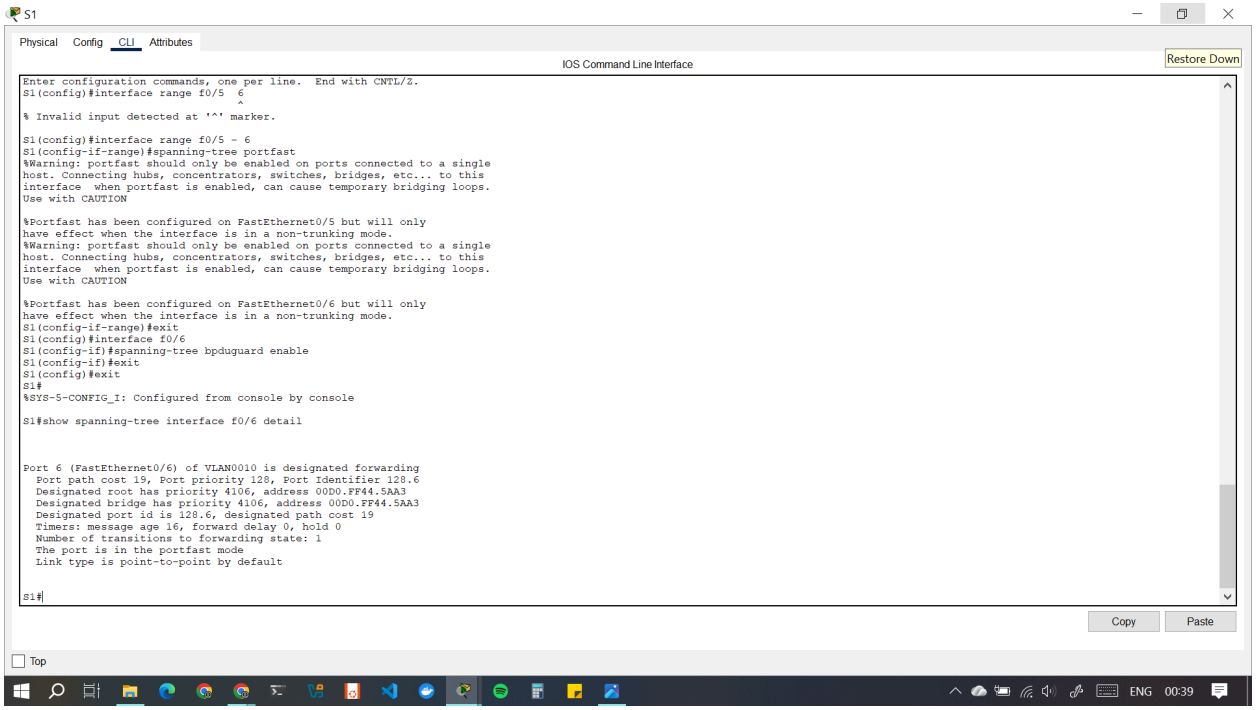
Number of transitions to forwarding state: 1

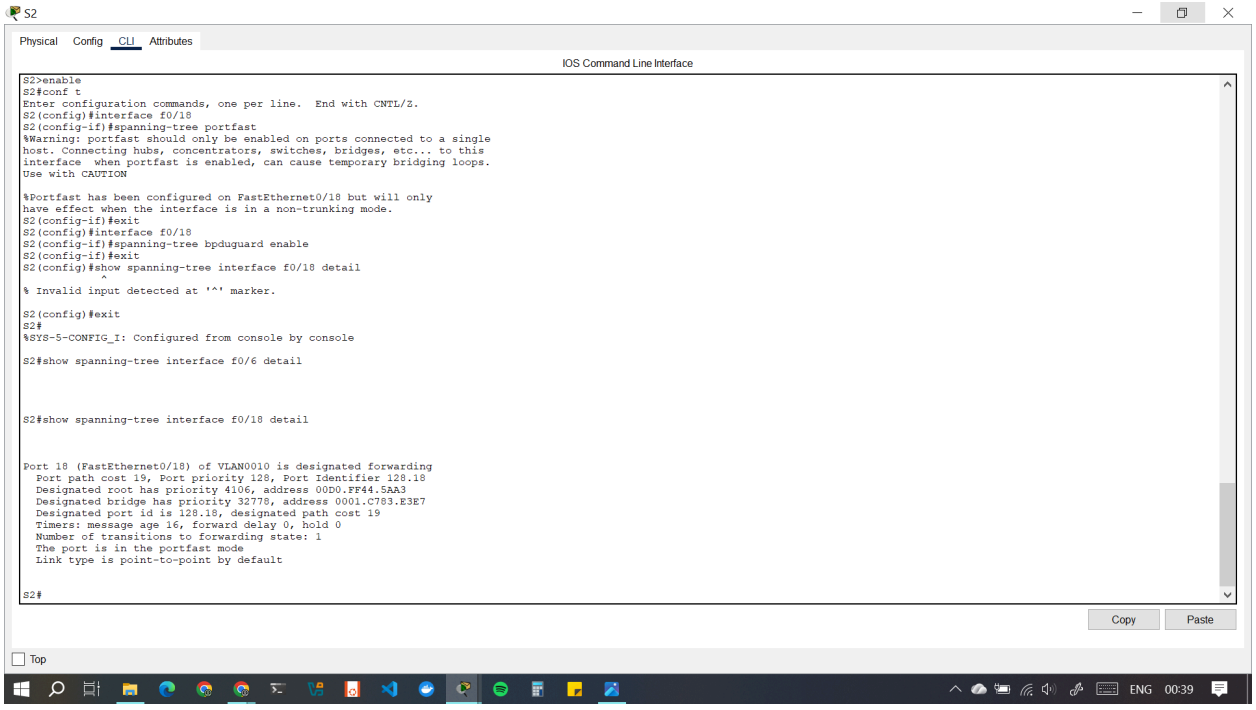
The port is in the portfast mode

Link type is point-to-point by default

Bpdu guard is enabled

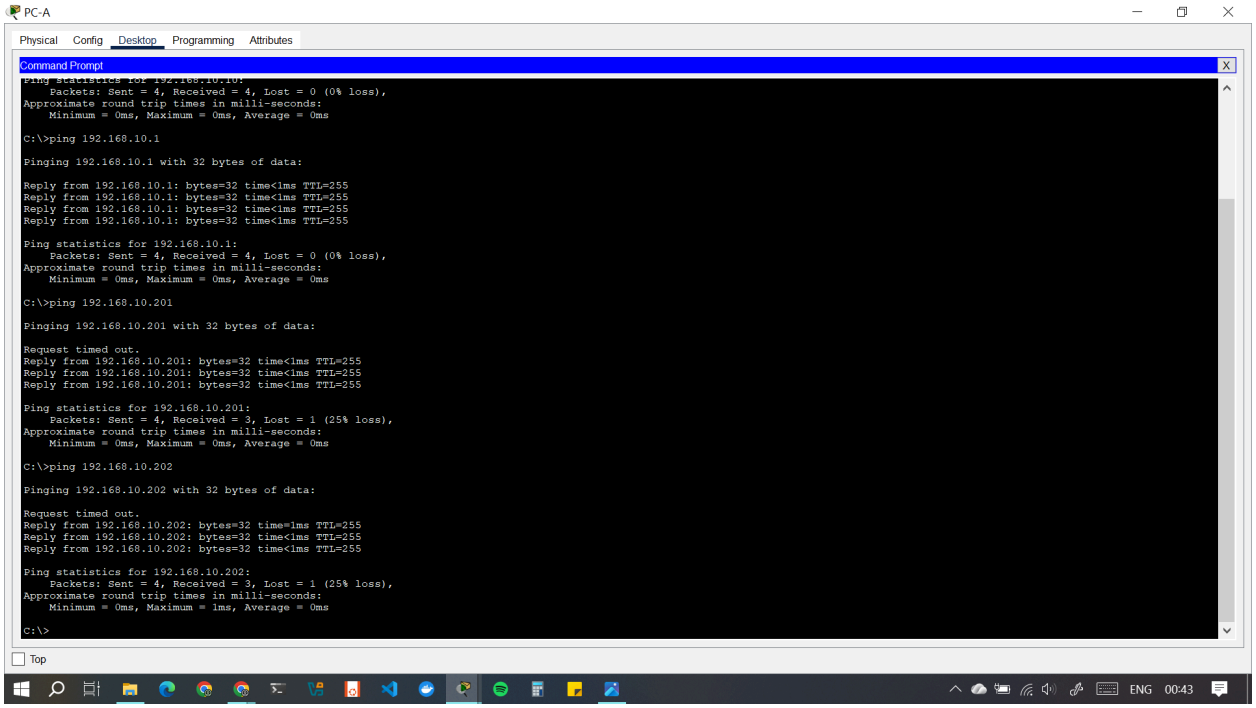
BPDU: sent 128, received 0

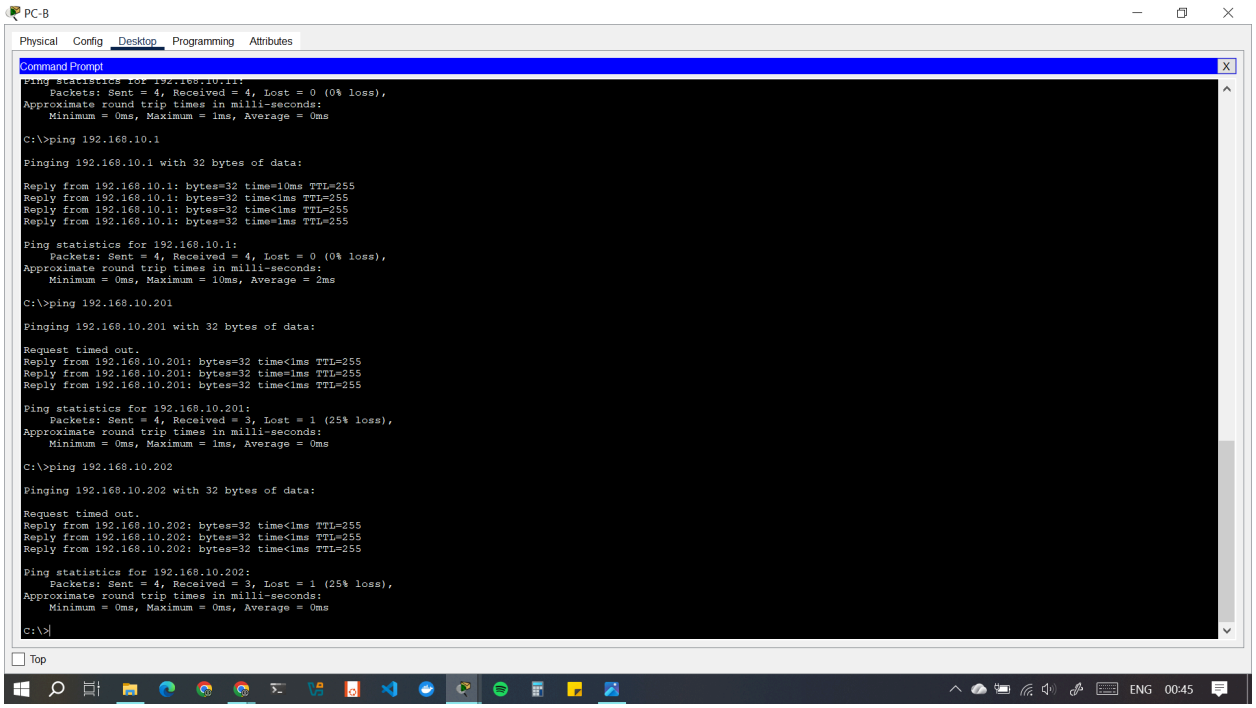




Step 7: Verify end-to-end connectivity.

Verify PING connectivity between all devices in the IP Addressing Table. If the pings fail, you may need to disable the firewall on the PC hosts.





Questions to Answer

1. In reference to Port Security on S2, why is there no timer value for the remaining age in minuteswhen sticky learning was configured?

This switch does not support the port security aging of sticky secure addresses.

2. In reference to Port Security on S2, if you load the running-config script on S2, why will PC-B on port 18 never get an IP address via DHCP?

Port security is set for only two MAC addresses and port 18 has two "sticky" MAC address bound to the port. Additionally, the violation is protect, which will never send a console/syslog message or increment the violation counter.

3. In reference to Port Security, what is the difference between the absolute aging type and inactivity aging type?

If the inactivity type is set, then the secure addresses on the port will be removed only if there is no data traffic from the secure source addresses for the specified time period.

If the absolute type is set, then all secure addresses on this port age out exactly after the time specified ends.

Conclusion

In this practical, DHCP Snooping was successfully implemented to enhance network security by controlling DHCP message flow and preventing rogue DHCP servers from issuing unauthorized IP addresses. The configuration process demonstrated how trusted and untrusted ports determine which interfaces can send or receive DHCP server messages. During troubleshooting, it was observed that clients failed to obtain IP addresses when DHCP Snooping was misconfigured, specifically due to the insertion of DHCP Option 82 information, which the router's DHCP server could not process. Disabling Option 82 resolved the issue, allowing proper DHCP lease allocation and binding creation.

Additionally, it was established that DHCP Snooping should be enabled on all switches with connected end devices—S1 and S2 in this case—to ensure consistent protection across the network. Trusted ports were correctly configured on uplinks to the DHCP server and between switches, while access ports remained untrusted.

Overall, this exercise reinforced key networking concepts, including VLAN configuration, DHCP operations, and Layer 2 security mechanisms, highlighting the importance of precise configuration and verification in maintaining a secure and reliable enterprise network.