Course: **Cloud and Network Security – CNS2 – 2025**

Student Name: **Lesamana Moses Metheli**

Student No: **CS-CNS09-25150**

Thursday, June 5, 2025

Week 4 Assignment 1:

VLANs and Secure Switch Configuration

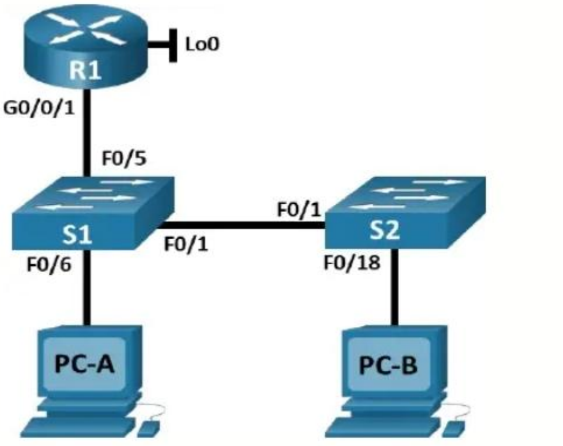
Table of Contents

Introduction

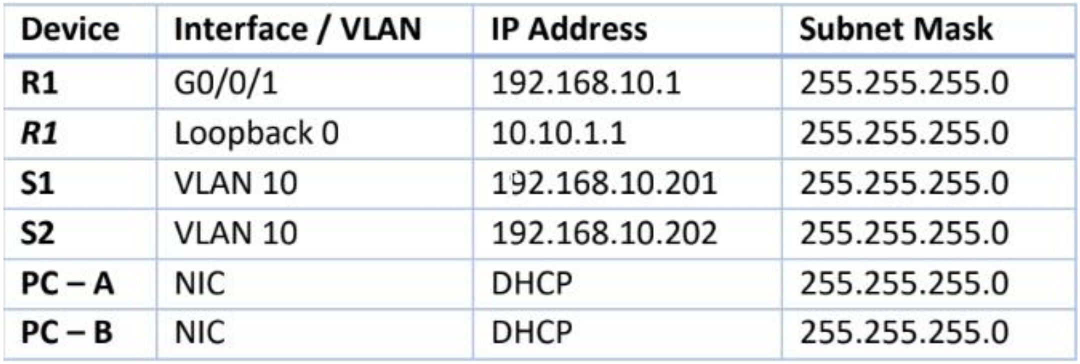
The purpose of this lab was to implement essential Layer 2 switch security mechanisms using Cisco Packet Tracer. As network infrastructure grows in complexity and exposure, it becomes critical to safeguard switches from potential threats such as unauthorized access, rogue DHCP servers, MAC address flooding, and Layer 2 attacks like spoofing or loops. This lab focused on configuring and verifying a secure switching environment using VLANs, trunking, port security, DHCP snooping, PortFast, and BPDU Guard. The configuration was performed on two Cisco switches (S1 and S2) with connected end devices and a router, simulating a real-world campus network. By applying these measures, the lab aimed to ensure traffic segmentation, secure port usage, and the prevention of common Layer 2 attacks.

Packet Tracer Lab: Switch Security Configuration

Topology



Addressing Table



Device	Interface / VLAN	IP Address	Subnet Mask
R1	G0/0/1	192.168.10.1	255.255.255.0
R1	Loopback 0	10.10.1.1	255.255.255.0
S1	VLAN 10	192.168.10.201	255.255.255.0
S2	VLAN 10	192.168.10.202	255.255.255.0
PC – A	NIC	DHCP	255.255.255.0
PC – B	NIC	DHCP	255.255.255.0

Objectives

Part 1: Configure the Network Devices.
Part 2: Configure VLANs on Switches.
Part 3: Configure Switch Security.

Background

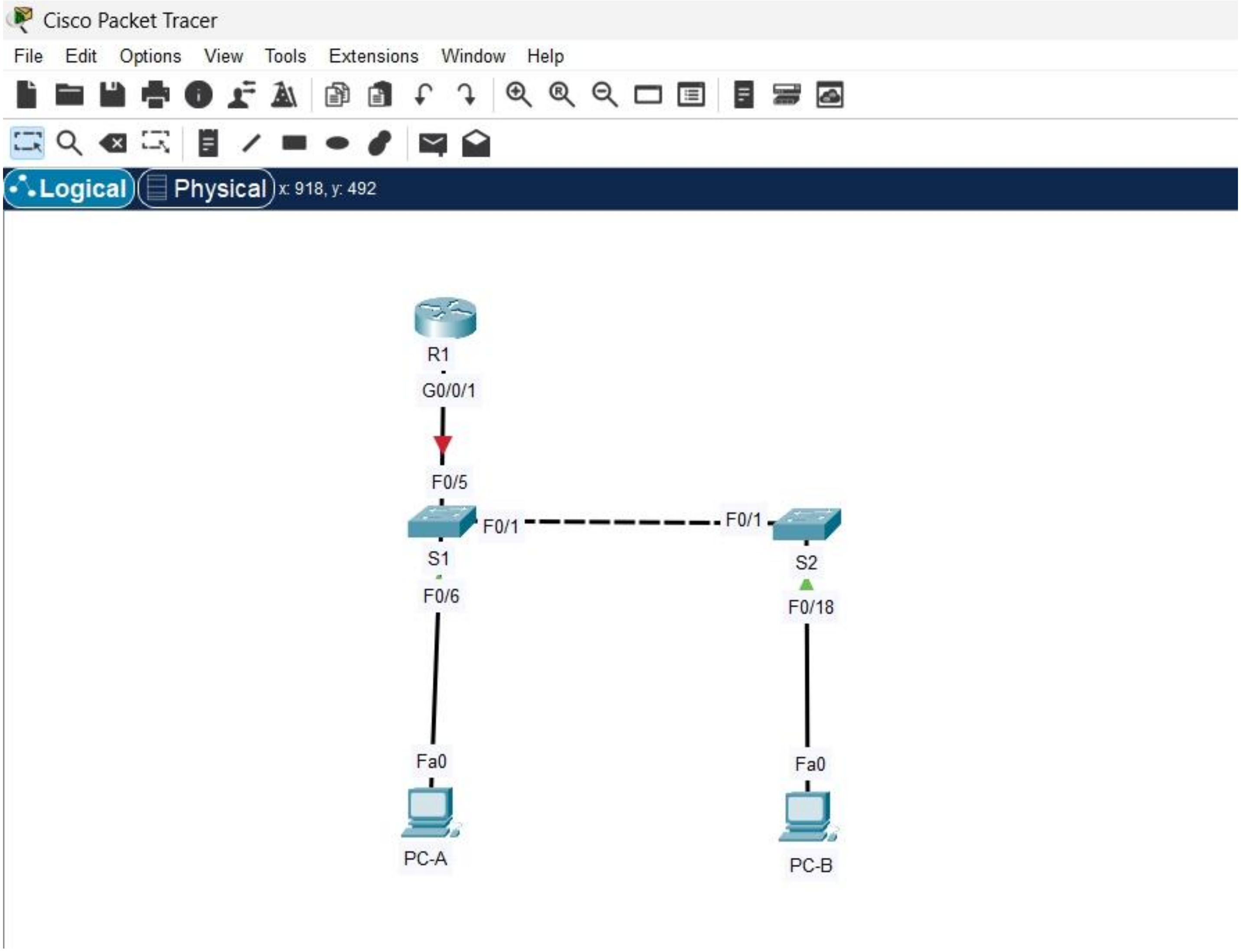
This is a comprehensive lab to review previously covered Layer 2 security features.
Note: The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.3 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.
Note: Make sure that the switches have been erased and have no startup configurations.

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

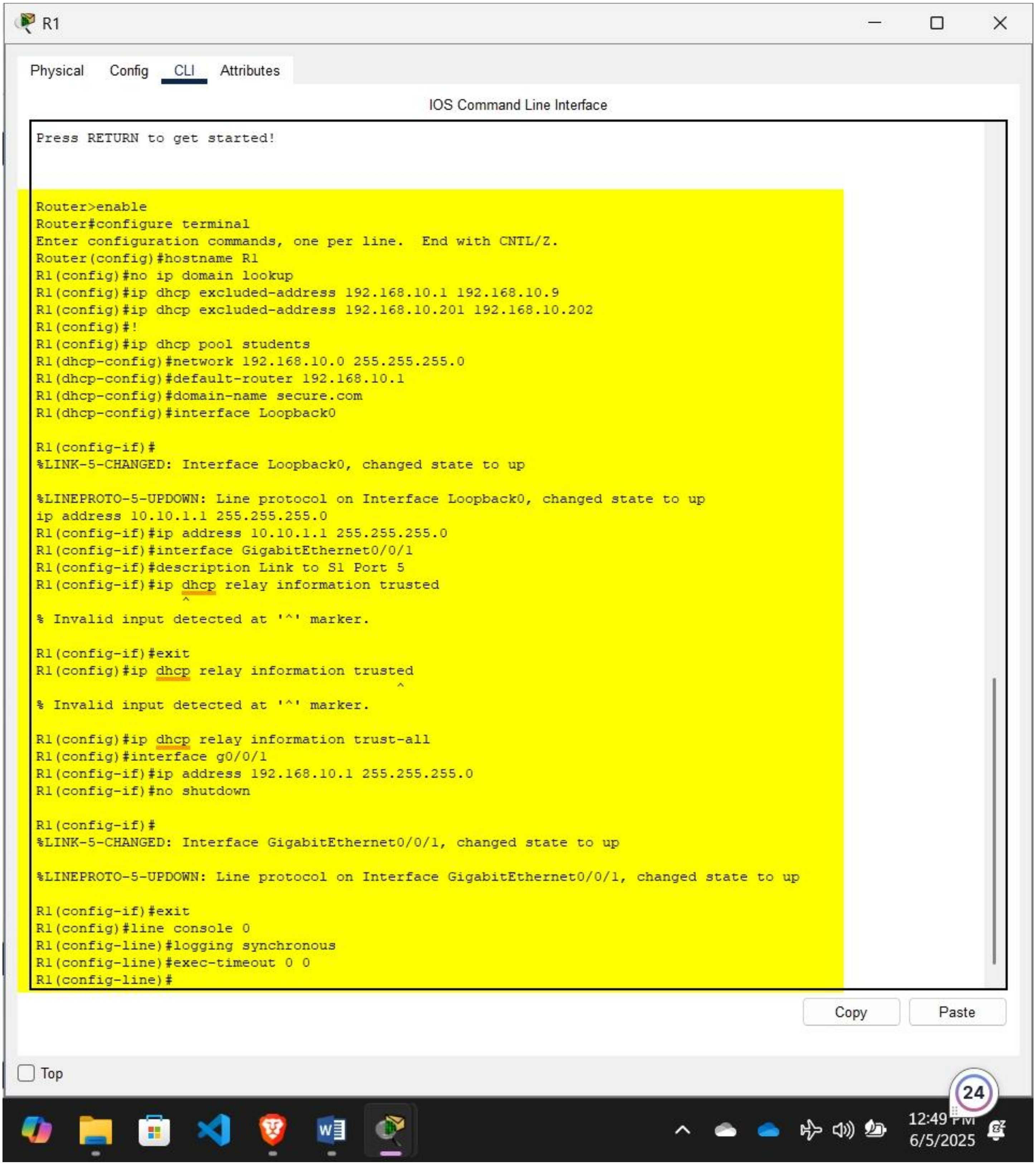
Part 1: Configure the Network Devices.

Step 1: Cable the network.



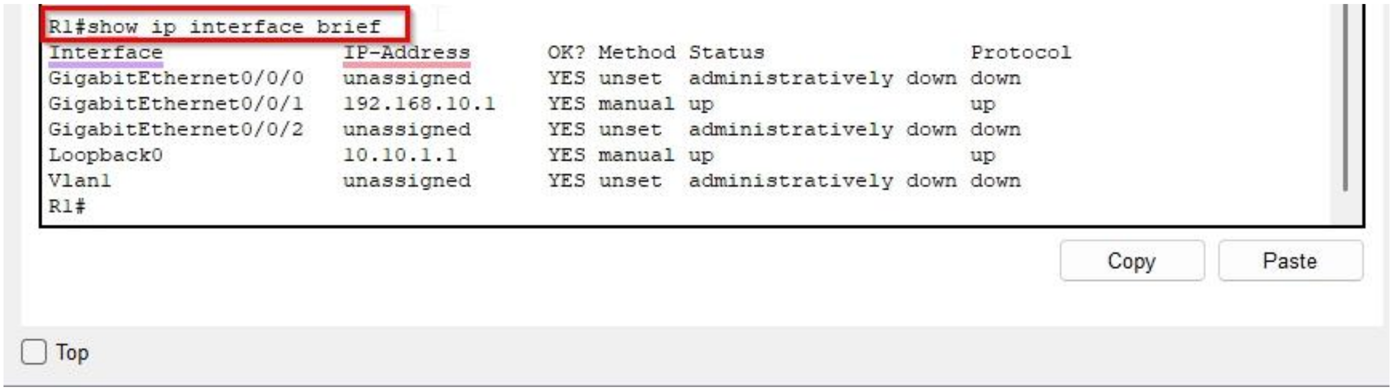
Step 2: Configure R1.

1. Load the following configuration script on R1.



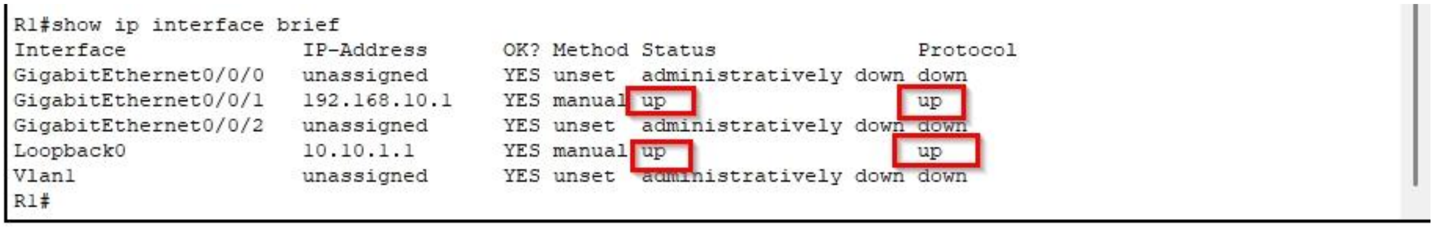
```
Press RETURN to get started!


Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#no ip domain lookup
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)#ip dhcp excluded-address 192.168.10.201 192.168.10.202
R1(config)#!
R1(config)#ip dhcp pool students
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#domain-name secure.com
R1(dhcp-config)#interface Loopback0

R1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
ip address 10.10.1.1 255.255.255.0
R1(config-if)#ip address 10.10.1.1 255.255.255.0
R1(config-if)#interface GigabitEthernet0/0/1
R1(config-if)#description Link to S1 Port 5
R1(config-if)#ip dhcp relay information trusted
                 ^
% Invalid input detected at '^' marker.

R1(config-if)#exit
R1(config)#ip dhcp relay information trusted
                                          ^
% Invalid input detected at '^' marker.

R1(config)#ip dhcp relay information trust-all
R1(config)#interface g0/0/1
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R1(config-if)#exit
R1(config)#line console 0
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 0 0
R1(config-line)#
```

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



```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down down
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Loopback0              10.10.1.1       YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

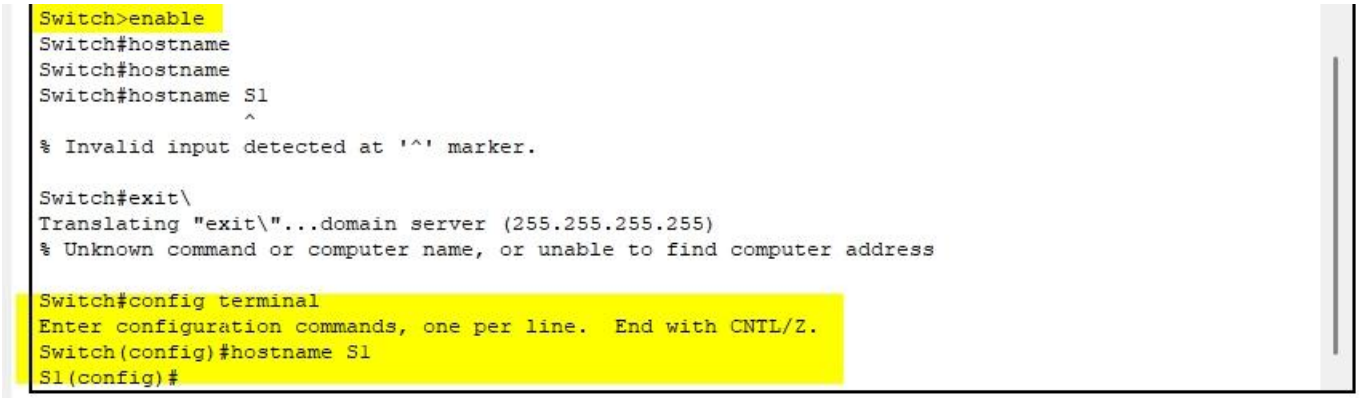
3. Verify IP addressing and interfaces are in an up / up state (troubleshoot as necessary).



```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down down
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Loopback0              10.10.1.1       YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

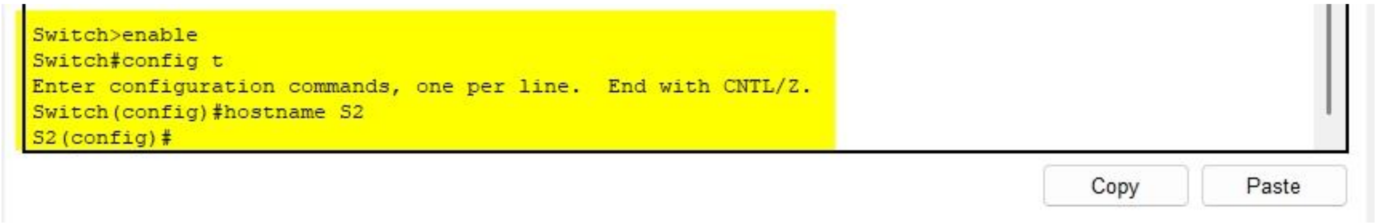
Step 3: Configure and verify basic switch settings.

1. Configure the hostname for switches S1 and S2.
   Switch S1



```
Switch>enable
Switch#hostname
Switch#hostname
Switch#hostname S1
                ^
% Invalid input detected at '^' marker.

Switch#exit\
Translating "exit\"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

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

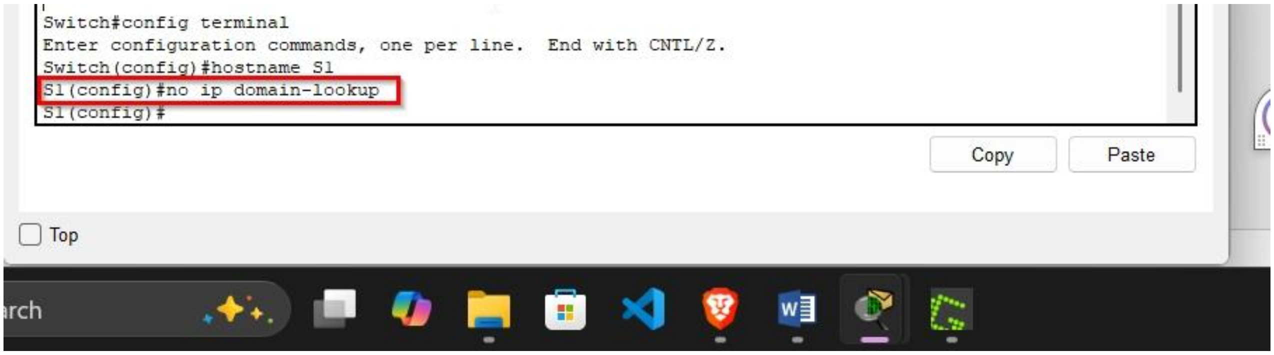
Switch S2



```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#
```

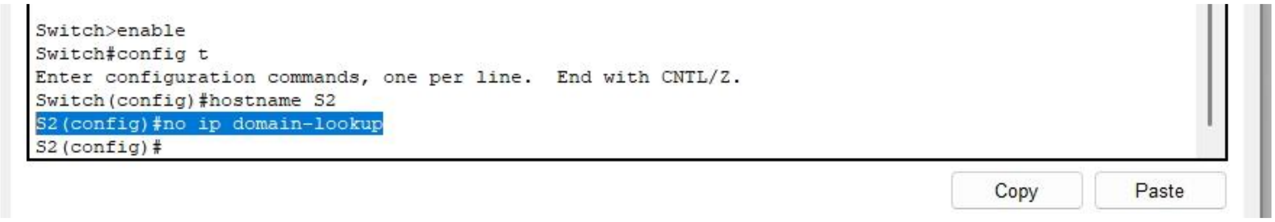
2. Prevent unwanted DNS lookups on both switches.

S1(config)#no ip domain-lookup



```
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#
```

S2(config)#no ip domain-lookup



```
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)#
```

3. Configure interface descriptions for the ports that are in use in S1 and S2.

S1(config)# interface f0/1

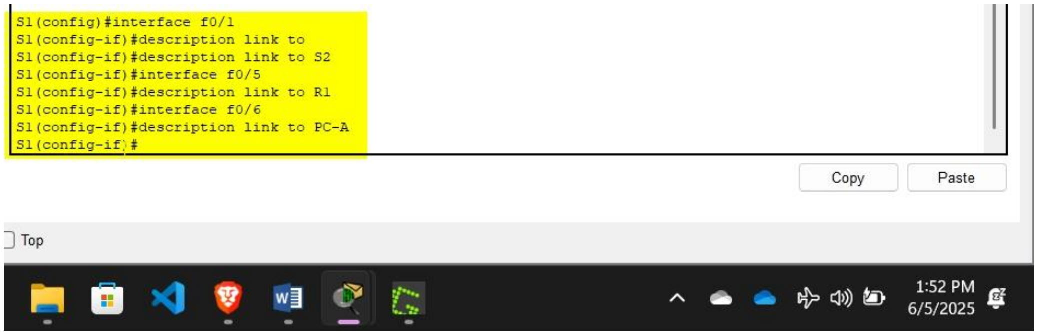
S1(config-if)# description Link to S2

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



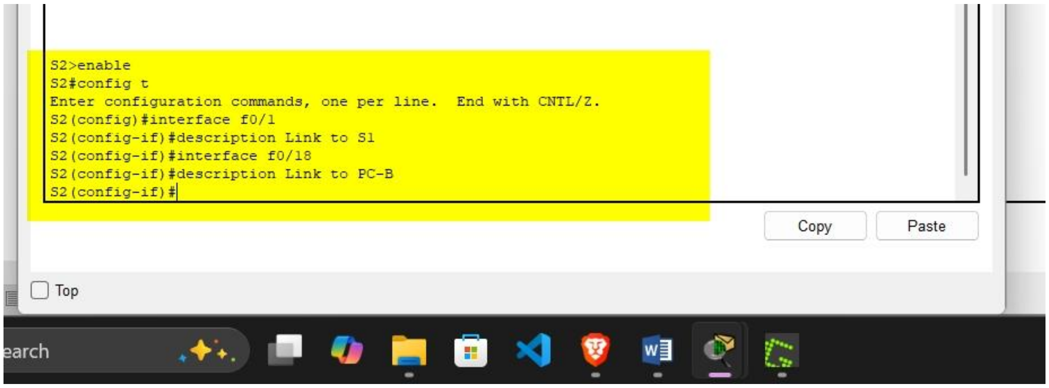
```
S1(config)#interface f0/1
S1(config-if)#description link to
S1(config-if)#description link to S2
S1(config-if)#interface f0/5
S1(config-if)#description link to R1
S1(config-if)#interface f0/6
S1(config-if)#description link to PC-A
S1(config-if)#
```

S2(config)# interface f0/1

S2(config-if)# description Link to S1

S2(config–if)# interface f0/18

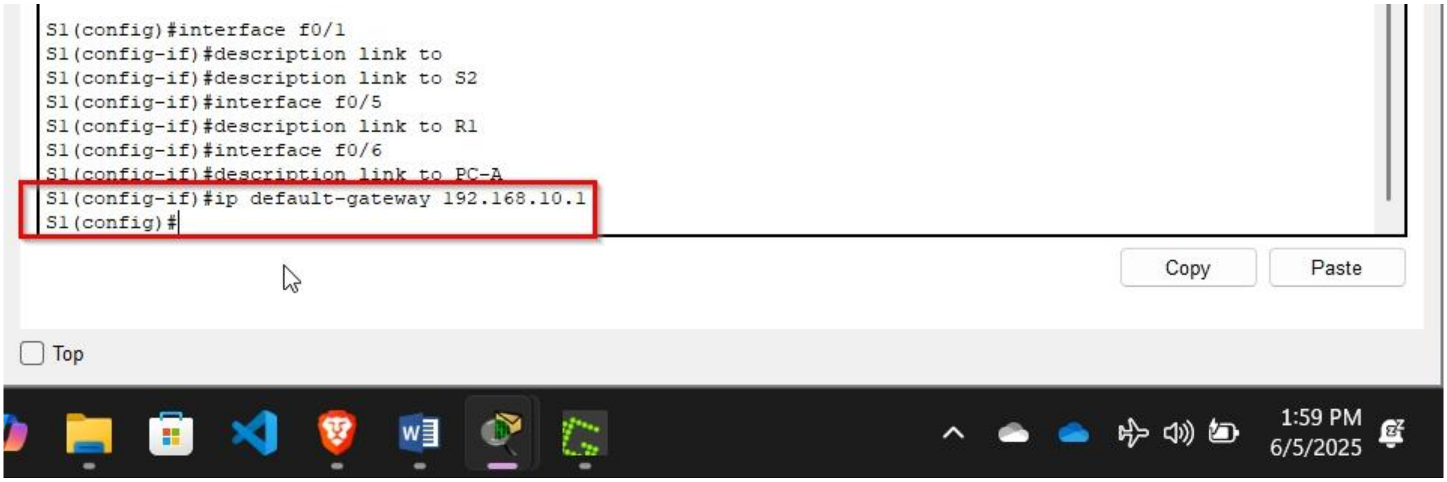
S2(config-if)# description Link to PC-B



```
S2>enable
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#
```

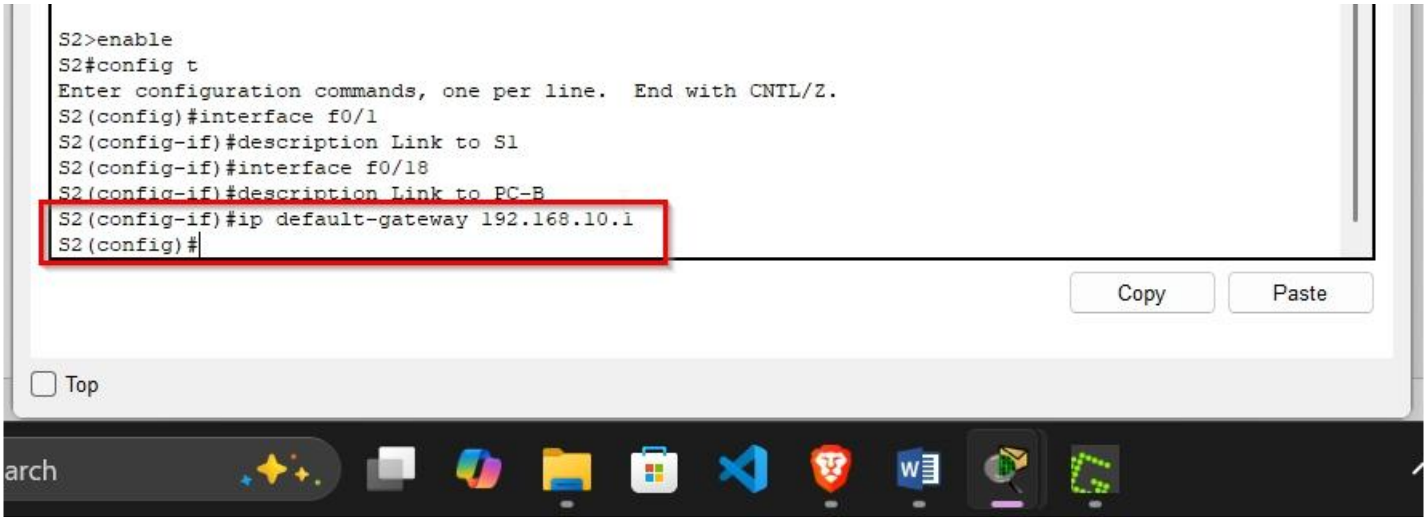
4. Set the default-gateway for the Management VLAN to 192.168.10.1 on both switches.

S1(config)# ip default-gateway 192.168.10.1



```
S1(config)#interface f0/1
S1(config-if)#description link to
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)#
```

S2(config)# ip default-gateway 192.168.10.1



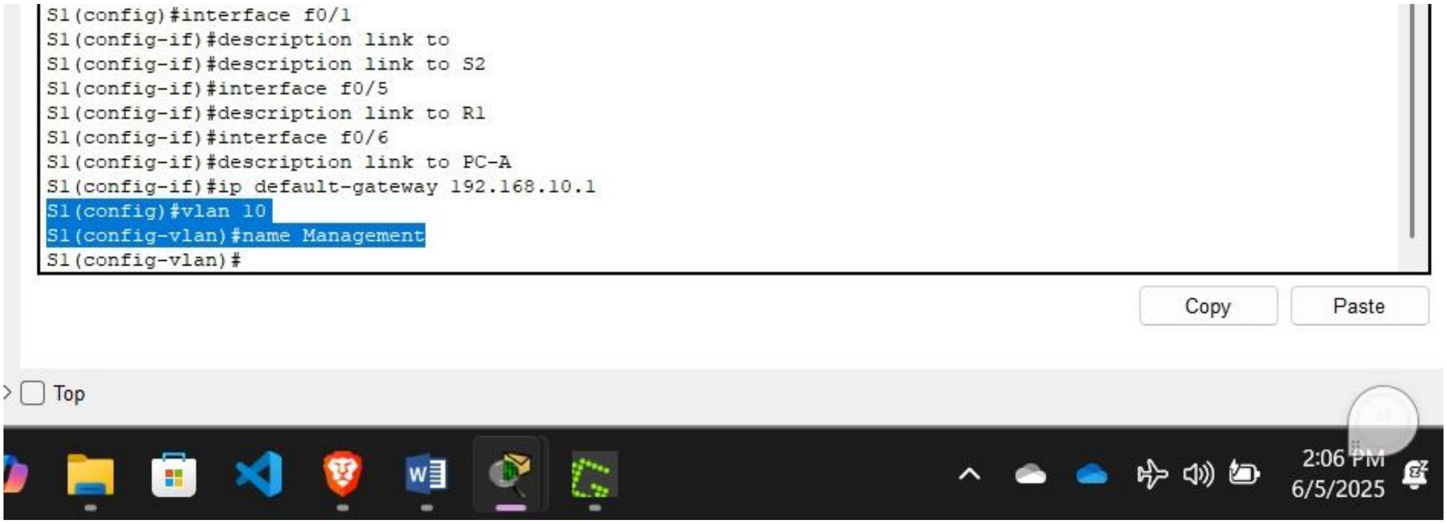
```
S2>enable
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#description Link to S1
S2(config-if)#interface f0/18
S2(config-if)#description Link to PC-B
S2(config-if)#ip default-gateway 192.168.10.1
S2(config)#
```

Part 2: Configure VLANs on Switches.

Step 1: Configure VLAN 10.

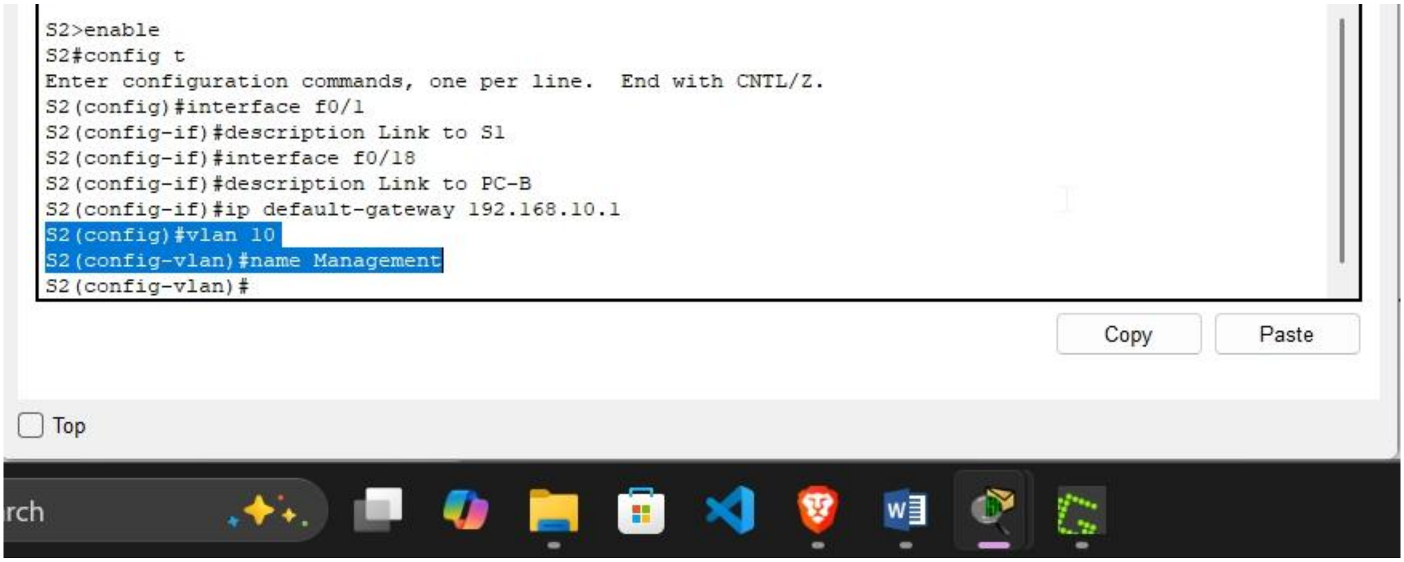
Add VLAN 10 to S1 and S2 and name the VLAN Management.

S1(config)#vlan 10
S1(config-vlan)#name Management



```
S1(config)#interface f0/1
S1(config-if)#description link to
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)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#
```

S2(config)#vlan 10
S2(config-vlan)#name Management

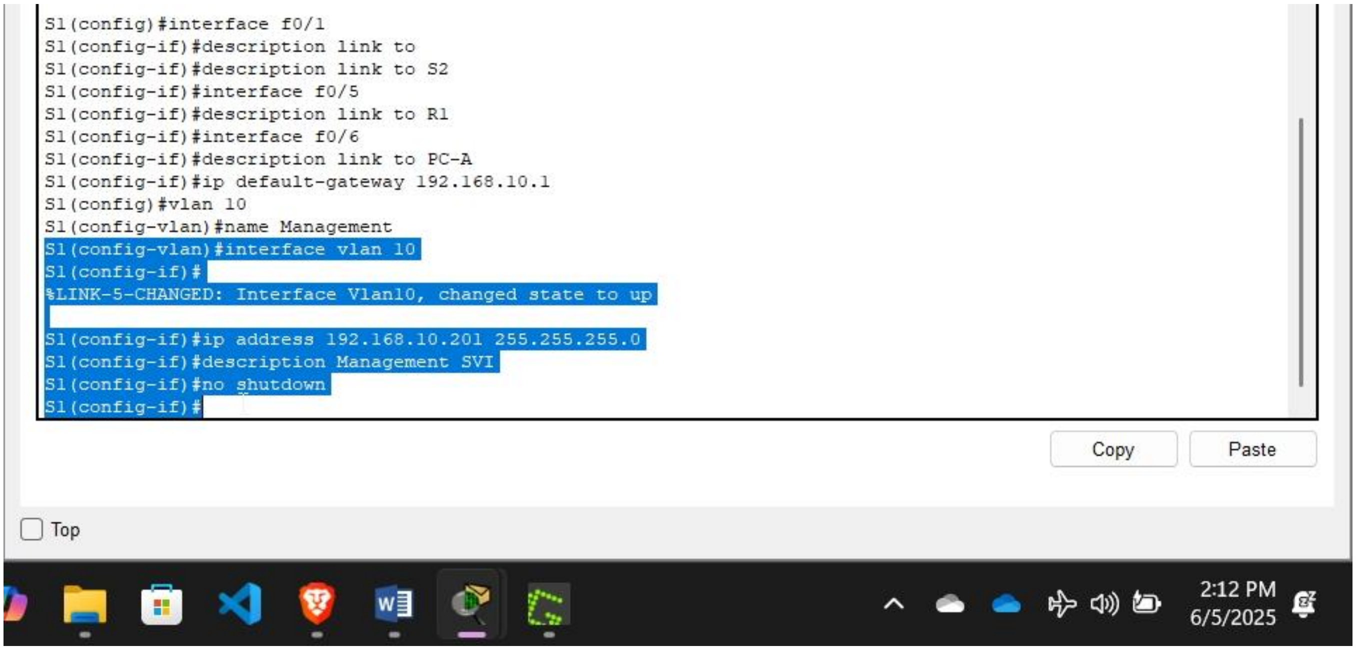


```
S2>enable
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#description Link to S1
S2(config-if)#interface f0/18
S2(config-if)#description Link to PC-B
S2(config-if)#ip default-gateway 192.168.10.1
S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#
```

Step 2: Configure the SVI for VLAN 10.

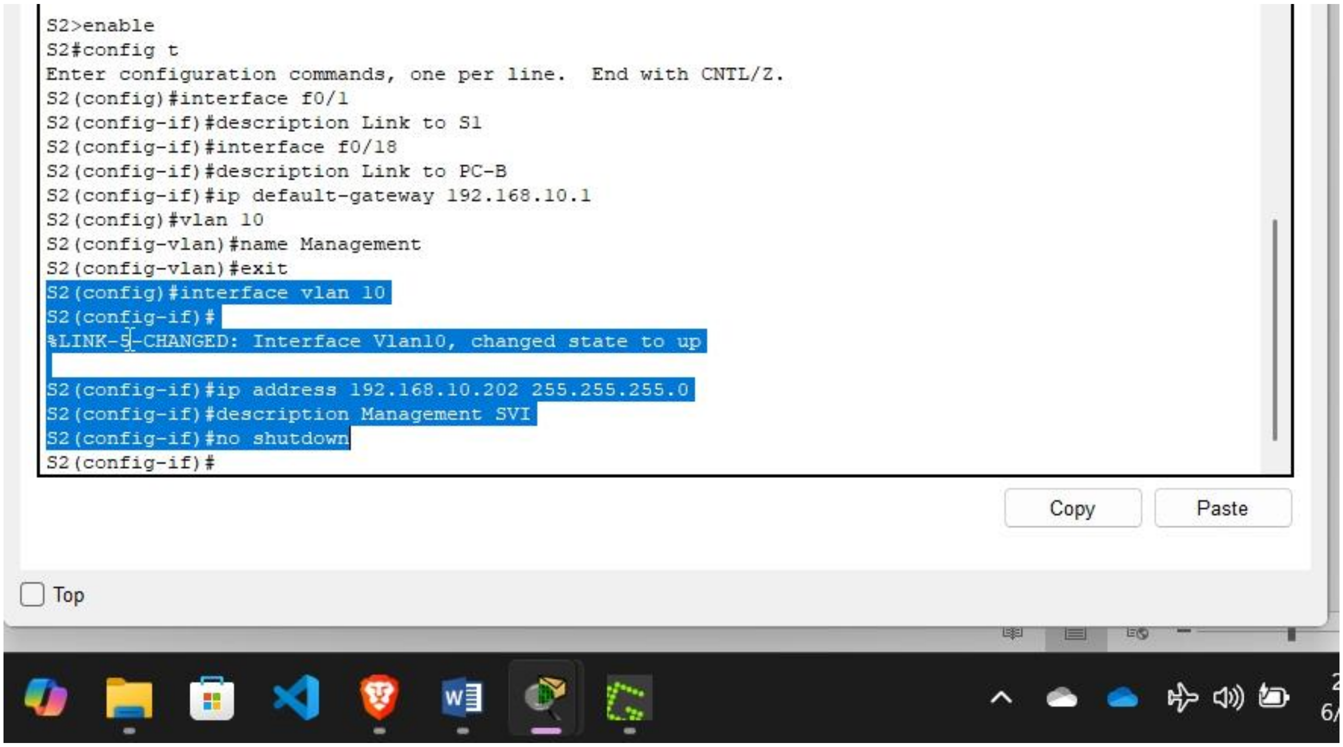
Configure the IP address according to the Addressing Table for SVI for VLAN 10 on S1 and S2. Enable the SVI interfaces and provide a description for the interface.

S1(config-vlan)#interface vlan 10
S1(config-if)#ip address 192.168.10.201 255.255.255.0
S1(config-if)#description Management SVI
S1(config-if)#no shutdown



```
S1(config)#interface f0/1
S1(config-if)#description link to
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)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#interface vlan 10
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S1(config-if)#ip address 192.168.10.201 255.255.255.0
S1(config-if)#description Management SVI
S1(config-if)#no shutdown
S1(config-if)#
```

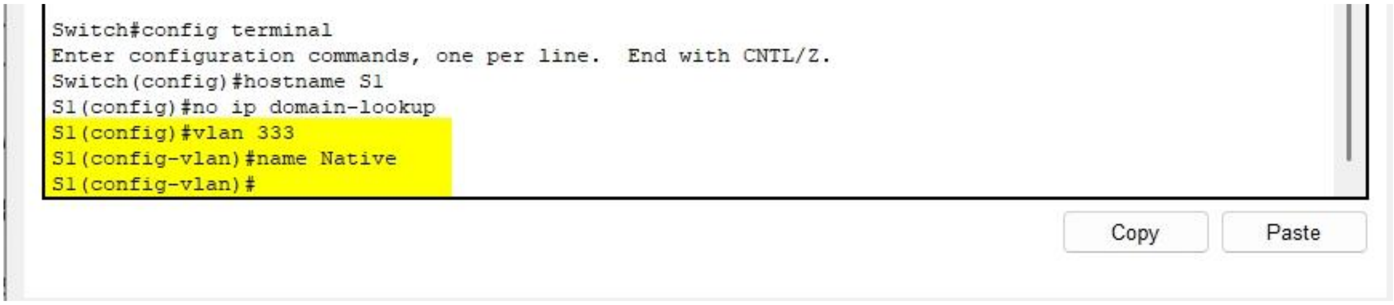
S2(config)#interface vlan 10
S2(config-if)#ip address 192.168.10.202 255.255.255.0
S2(config-if)#description Management SVI
S2(config-if)#no shutdown



```
S2>enable
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
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)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#exit
S2(config)#interface vlan 10
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S2(config-if)#ip address 192.168.10.202 255.255.255.0
S2(config-if)#description Management SVI
S2(config-if)#no shutdown
S2(config-if)#
```

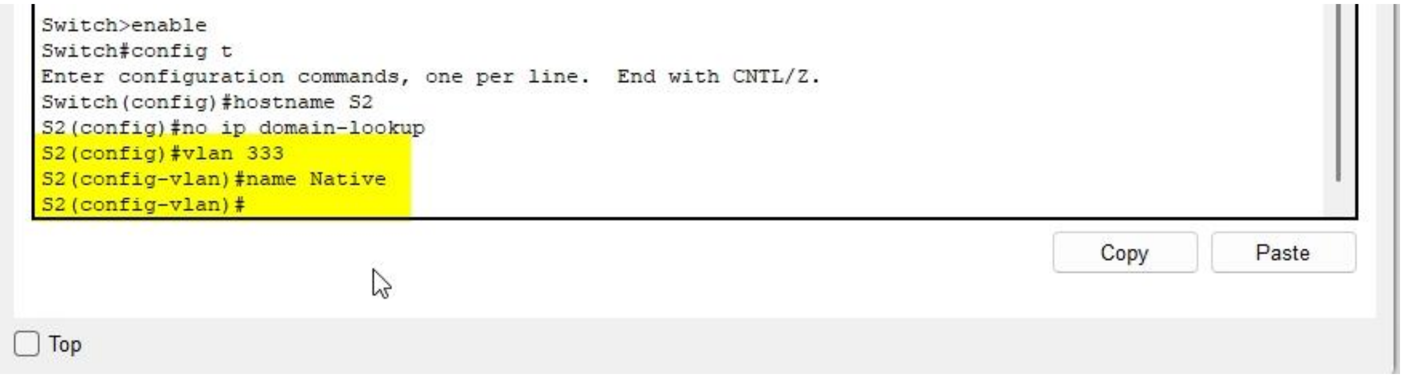
Step 3: Configure VLAN 333 with the name Native on S1 and S2.

S1(config)# vlan 333
S1(config-vlan)# name Native



```
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#
```

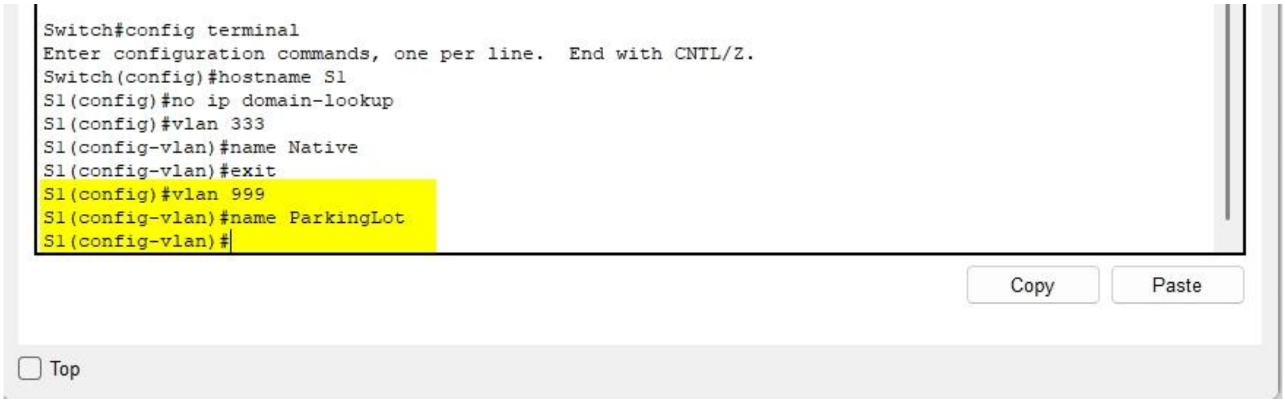
S2(config)# vlan 333
S2(config-vlan)# name Native



```
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)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#
```

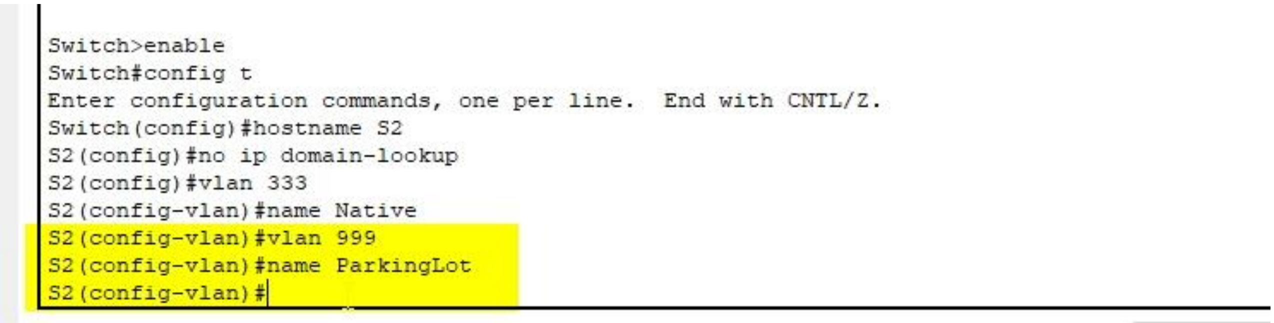
Step 4: Configure VLAN 999 with the name ParkingLot on S1 and S2.

S1(config-vlan)# vlan 999
S1(config-vlan)# name ParkingLot



```
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#
```

S2(config-vlan)# vlan 999
S2(config-vlan)# name ParkingLot



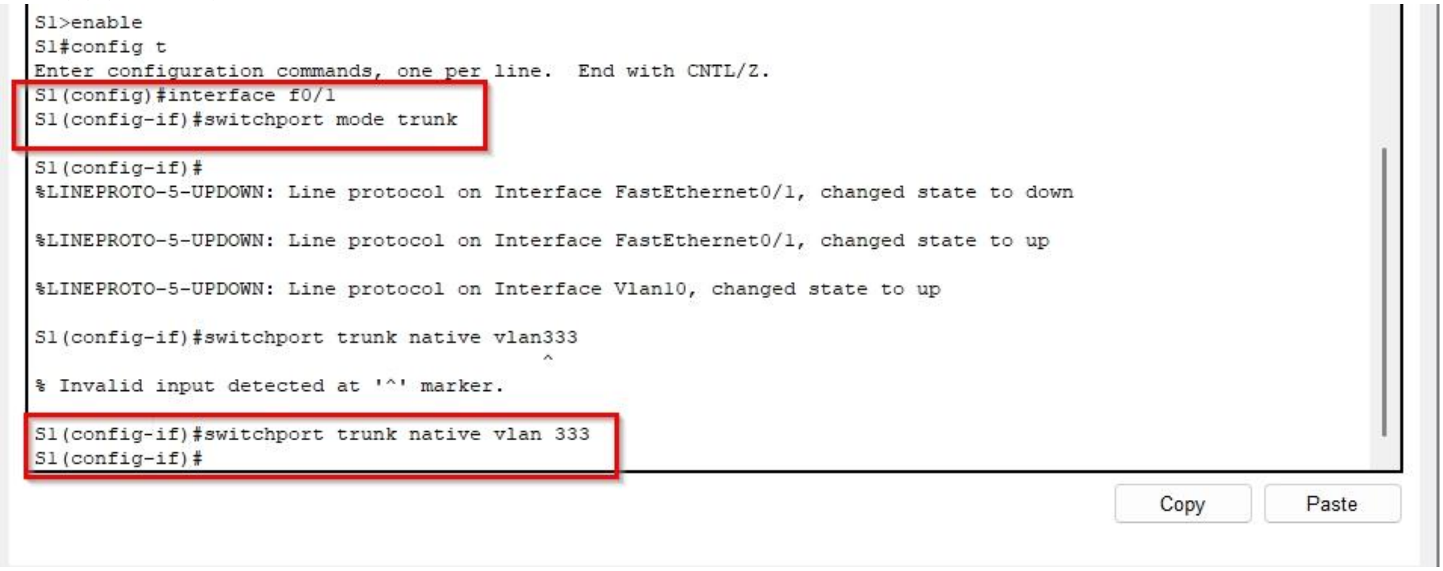
```
Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#vlan 999
S2(config-vlan)#name ParkingLot
S2(config-vlan)#
```

Part 3: Configure Switch Security.

Step 1: Implement 802.1Q trunking.

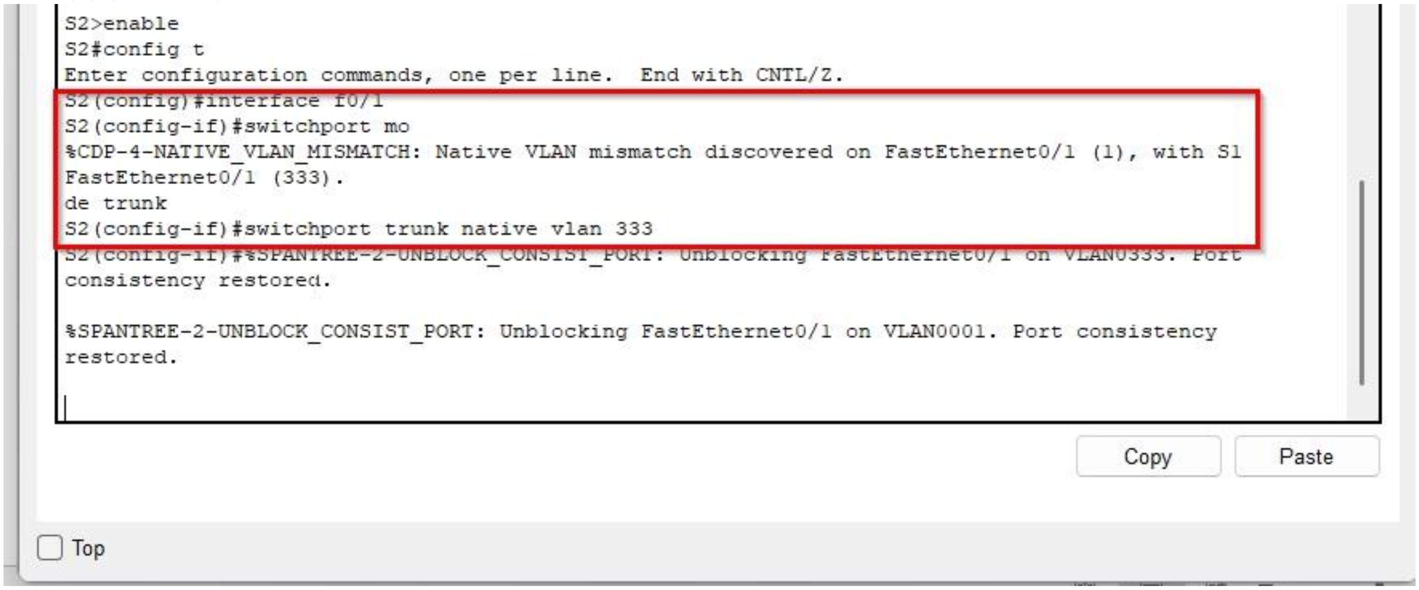
1. On both switches, configure trunking on F0/1 to use VLAN 333 as the native VLAN.

S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 333



```
S1>enable
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

S1(config-if)#switchport trunk native vlan333
                                           ^
% Invalid input detected at '^' marker.

S1(config-if)#switchport trunk native vlan 333
S1(config-if)#
```

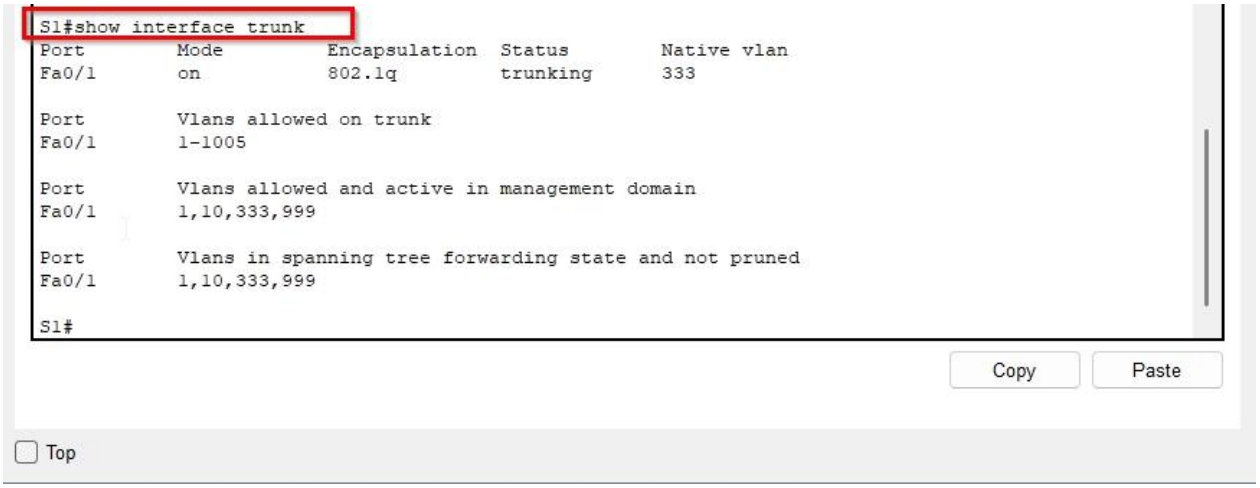
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 333



```
S2>enable
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#switchport mo
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S1
FastEthernet0/1 (333).
de trunk
S2(config-if)#switchport trunk native vlan 333
S2(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0333. Port
consistency restored.

%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0001. Port consistency
restored.
```

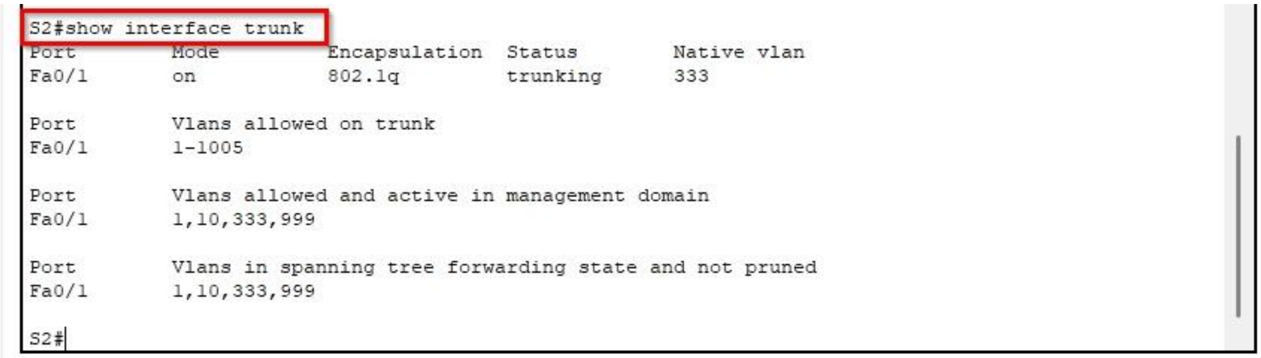
2. Verify that trunking is configured on both switches.

S1# show interface trunk



```
S1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      333

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,333,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,333,999

S1#
```

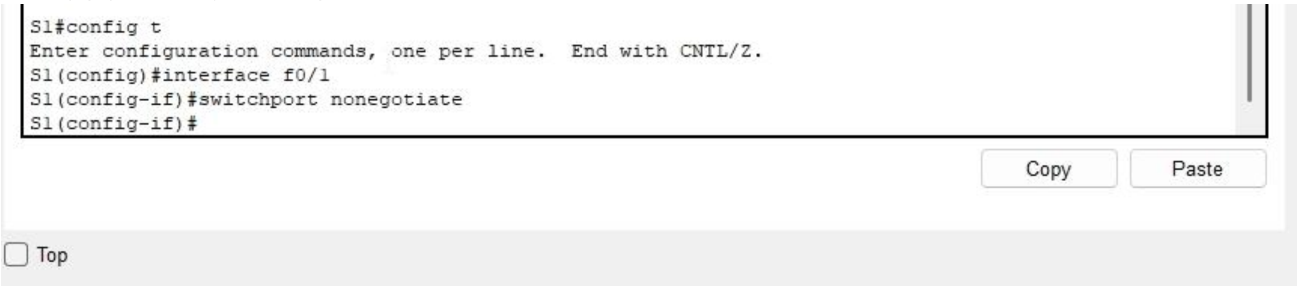
S2# show interface trunk



```
S2#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      333

Port        Vlans allowed on trunk
Fa0/1       1-1005

Port        Vlans allowed and active in management domain
Fa0/1       1,10,333,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,333,999

S2#
```

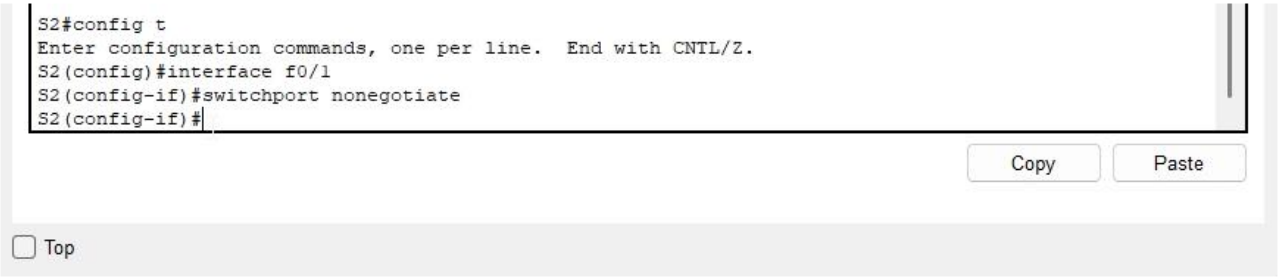
3. Disable DTP negotiation on F0/1 on S1 and S2.

S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate



```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#
```

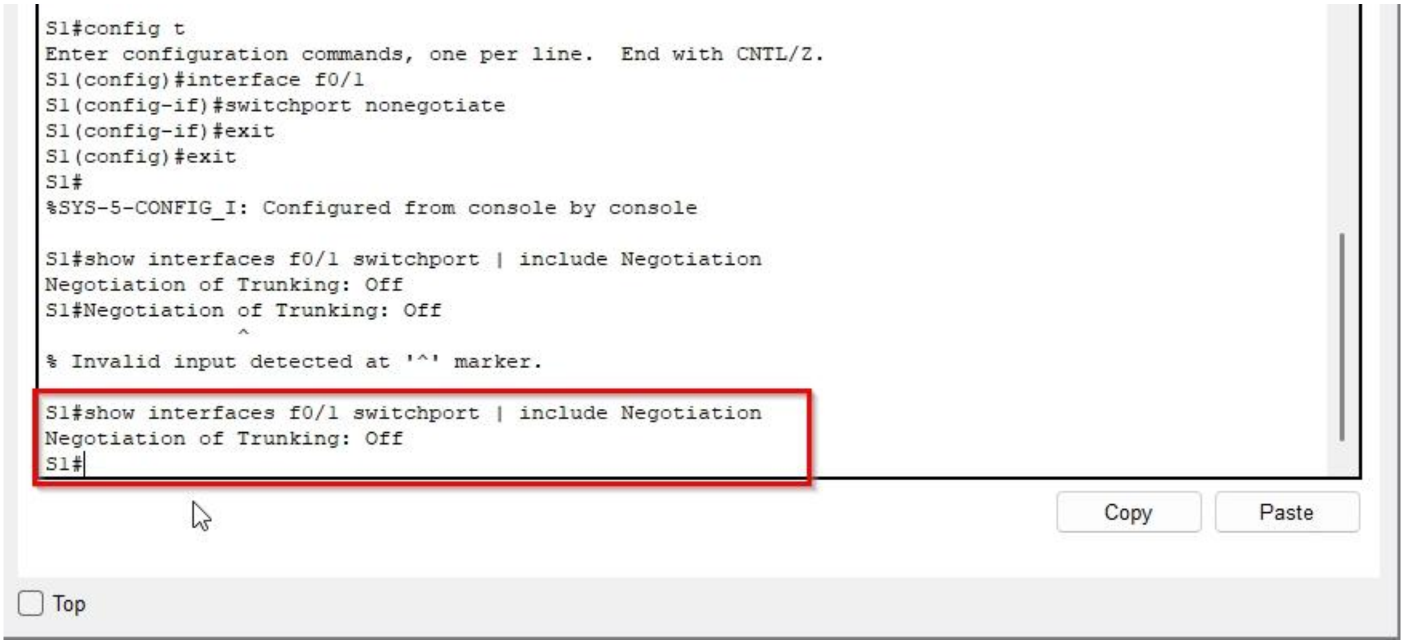
S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate



```
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#switchport nonegotiate
S2(config-if)#
```

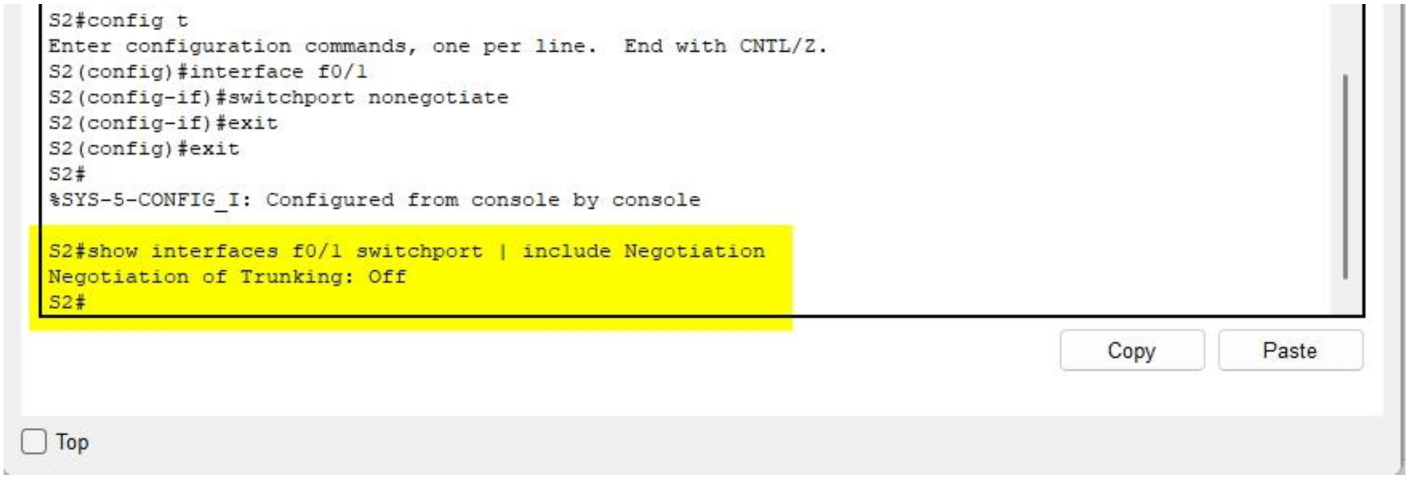
4. Verify with the show interfaces command.

S1# show interfaces f0/1 switchport | include Negotiation



```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S1#Negotiation of Trunking: Off
                     ^
% Invalid input detected at '^' marker.

S1#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S1#
```

S2# show interfaces f0/1 switchport | include Negotiation

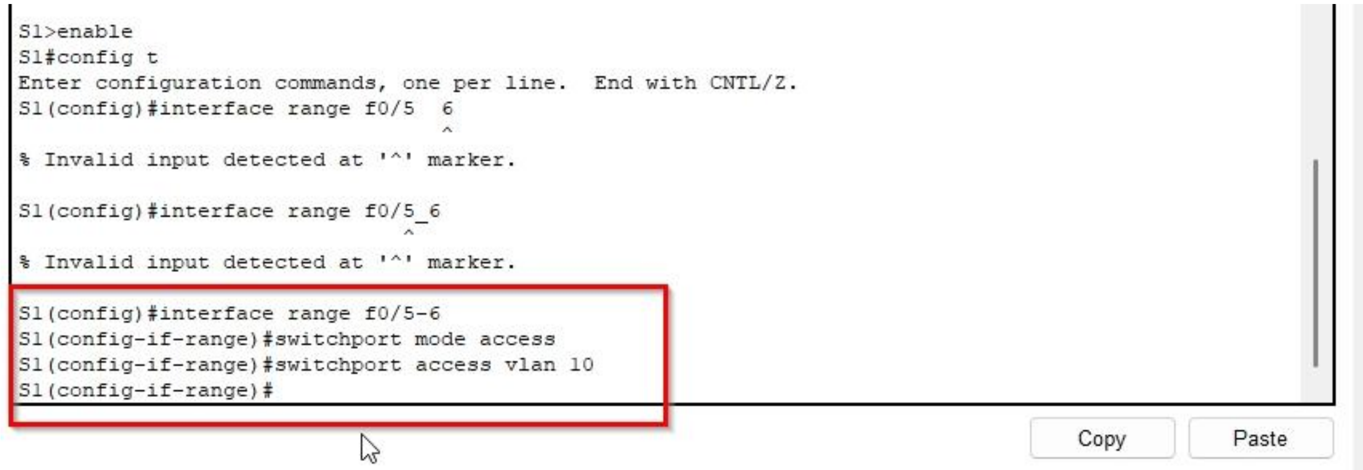


```
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#switchport nonegotiate
S2(config-if)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S2#
```

Step 2: Configure access ports.

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

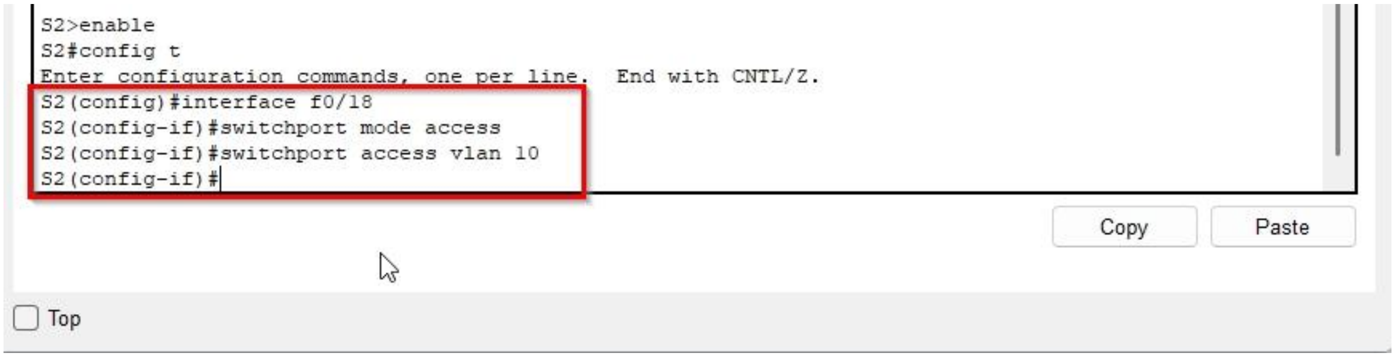
S1(config)# interface range f0/5 – 6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10



```
S1>enable
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range f0/5  6
                                 ^
% Invalid input detected at '^' marker.

S1(config)#interface range f0/5_6
                              ^
% Invalid input detected at '^' marker.

S1(config)#interface range f0/5-6
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#
```

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

S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 10

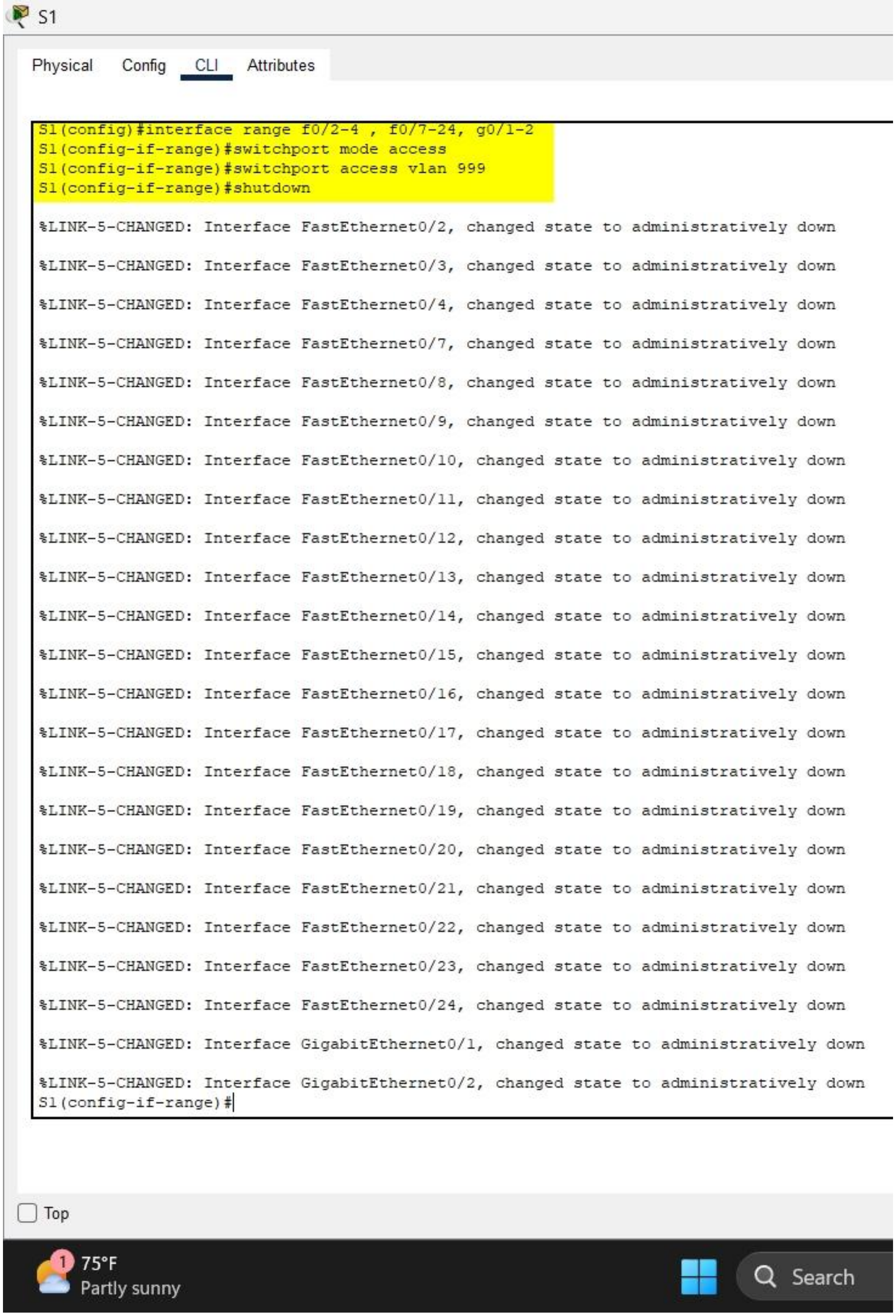


```
S2>enable
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#
```

Step 3: Secure and disable unused switchports.

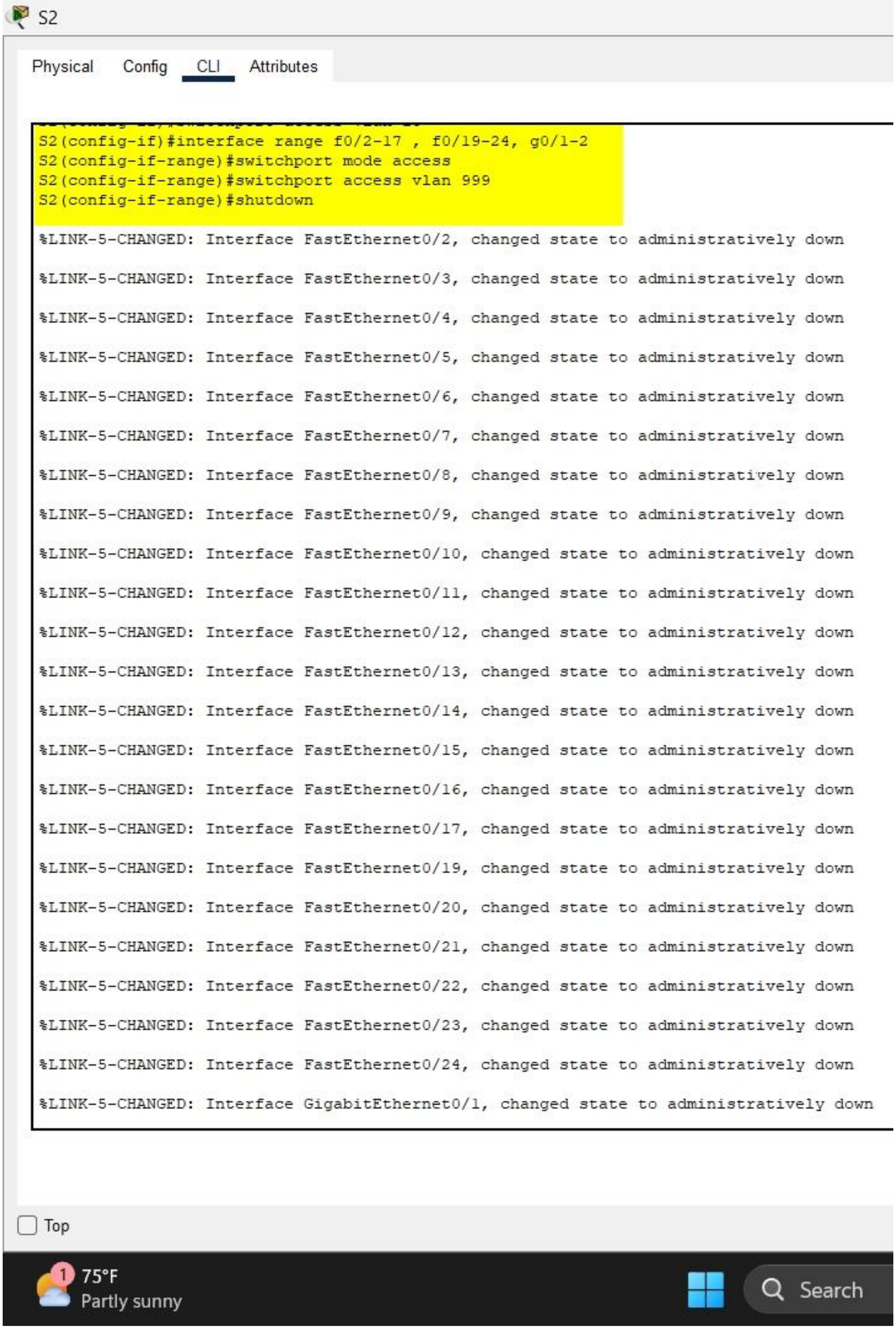
1. On S1 and S2, move the unused ports from VLAN 1 to VLAN 999 and disable the unused ports.

S1(config)# interface range f0/2-4 , f0/7-24, g0/1-2
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
S1(config-if-range)# shutdown



```
S1(config)#interface range f0/2-4 , f0/7-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(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 FastEthernet0/7, 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

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S1(config-if-range)#
```

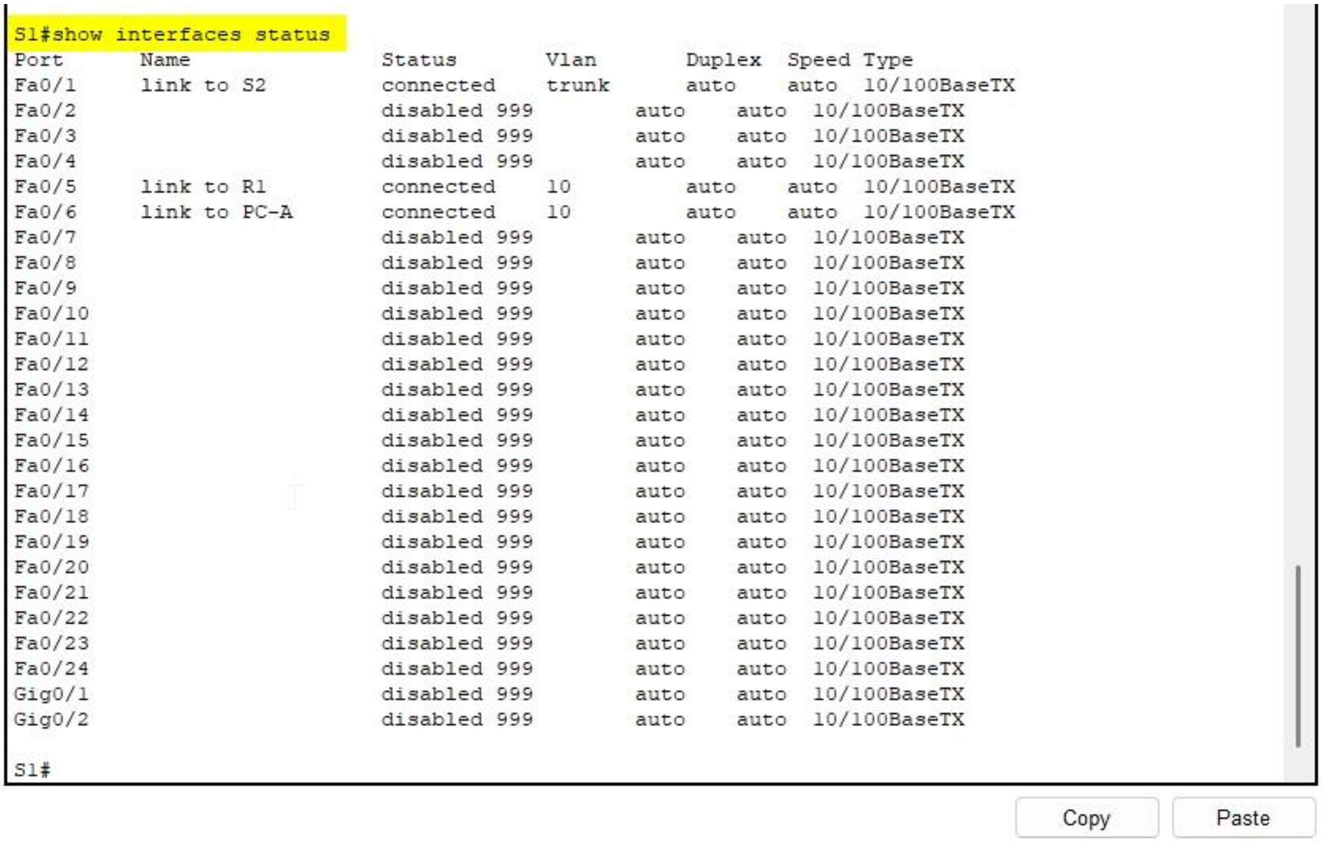
S2(config)# interface range f0/2-17 , f0/19-24, g0/1-2
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 999
S2(config-if-range)# shutdown



```
S2(config-if)#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

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
```

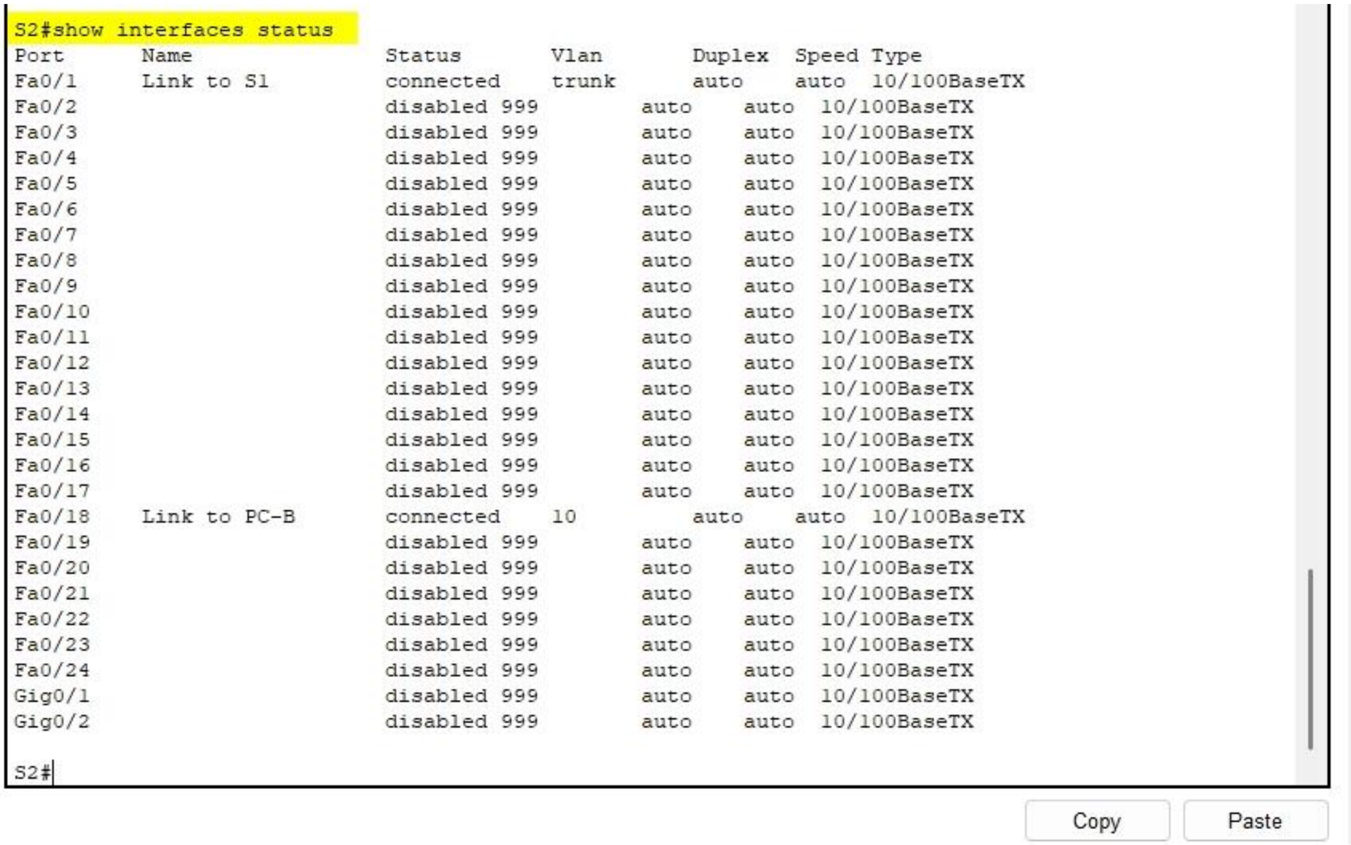
2. Verify that unused ports are disabled and associated with VLAN 999 by issuing the show command.

S1# show interfaces status



```
S1#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     link to S2         connected    trunk      auto    auto  10/100BaseTX
Fa0/2                        disabled 999        auto    auto  10/100BaseTX
Fa0/3                        disabled 999        auto    auto  10/100BaseTX
Fa0/4                        disabled 999        auto    auto  10/100BaseTX
Fa0/5     link to R1         connected    10         auto    auto  10/100BaseTX
Fa0/6     link to PC-A       connected    10         auto    auto  10/100BaseTX
Fa0/7                        disabled 999        auto    auto  10/100BaseTX
Fa0/8                        disabled 999        auto    auto  10/100BaseTX
Fa0/9                        disabled 999        auto    auto  10/100BaseTX
Fa0/10                       disabled 999        auto    auto  10/100BaseTX
Fa0/11                       disabled 999        auto    auto  10/100BaseTX
Fa0/12                       disabled 999        auto    auto  10/100BaseTX
Fa0/13                       disabled 999        auto    auto  10/100BaseTX
Fa0/14                       disabled 999        auto    auto  10/100BaseTX
Fa0/15                       disabled 999        auto    auto  10/100BaseTX
Fa0/16                       disabled 999        auto    auto  10/100BaseTX
Fa0/17                       disabled 999        auto    auto  10/100BaseTX
Fa0/18                       disabled 999        auto    auto  10/100BaseTX
Fa0/19                       disabled 999        auto    auto  10/100BaseTX
Fa0/20                       disabled 999        auto    auto  10/100BaseTX
Fa0/21                       disabled 999        auto    auto  10/100BaseTX
Fa0/22                       disabled 999        auto    auto  10/100BaseTX
Fa0/23                       disabled 999        auto    auto  10/100BaseTX
Fa0/24                       disabled 999        auto    auto  10/100BaseTX
Gig0/1                       disabled 999        auto    auto  10/100BaseTX
Gig0/2                       disabled 999        auto    auto  10/100BaseTX

S1#
```

S2# show interfaces status

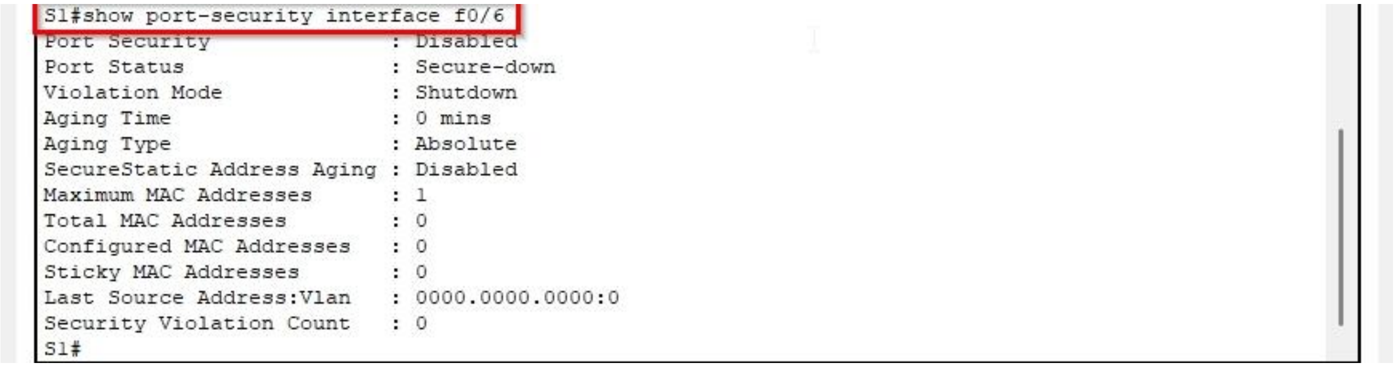


```
S2#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Link to S1         connected    trunk      auto    auto  10/100BaseTX
Fa0/2                        disabled 999        auto    auto  10/100BaseTX
Fa0/3                        disabled 999        auto    auto  10/100BaseTX
Fa0/4                        disabled 999        auto    auto  10/100BaseTX
Fa0/5                        disabled 999        auto    auto  10/100BaseTX
Fa0/6                        disabled 999        auto    auto  10/100BaseTX
Fa0/7                        disabled 999        auto    auto  10/100BaseTX
Fa0/8                        disabled 999        auto    auto  10/100BaseTX
Fa0/9                        disabled 999        auto    auto  10/100BaseTX
Fa0/10                       disabled 999        auto    auto  10/100BaseTX
Fa0/11                       disabled 999        auto    auto  10/100BaseTX
Fa0/12                       disabled 999        auto    auto  10/100BaseTX
Fa0/13                       disabled 999        auto    auto  10/100BaseTX
Fa0/14                       disabled 999        auto    auto  10/100BaseTX
Fa0/15                       disabled 999        auto    auto  10/100BaseTX
Fa0/16                       disabled 999        auto    auto  10/100BaseTX
Fa0/17                       disabled 999        auto    auto  10/100BaseTX
Fa0/18    Link to PC-B       connected    10         auto    auto  10/100BaseTX
Fa0/19                       disabled 999        auto    auto  10/100BaseTX
Fa0/20                       disabled 999        auto    auto  10/100BaseTX
Fa0/21                       disabled 999        auto    auto  10/100BaseTX
Fa0/22                       disabled 999        auto    auto  10/100BaseTX
Fa0/23                       disabled 999        auto    auto  10/100BaseTX
Fa0/24                       disabled 999        auto    auto  10/100BaseTX
Gig0/1                       disabled 999        auto    auto  10/100BaseTX
Gig0/2                       disabled 999        auto    auto  10/100BaseTX

S2#
```

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.

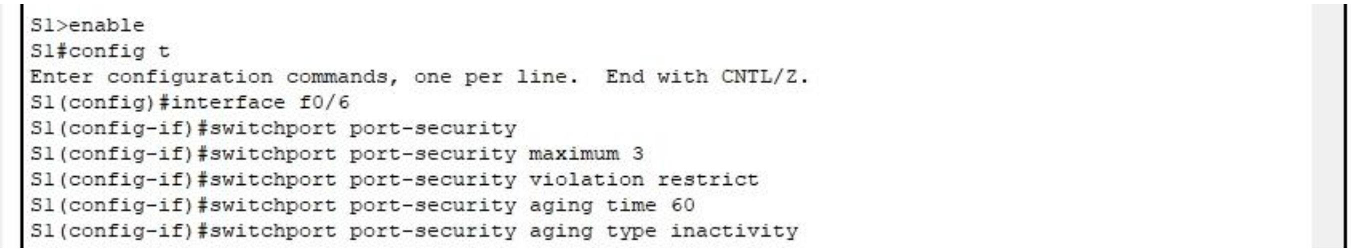


```
S1#show port-security interface f0/6
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

Default Port Security Configuration	
Feature Default Setting	**Feature Default Setting**
Port Security	Disabled
Maximum number of MAC addresses	1
Violation Mode	Shutdown
Aging Time	0
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:

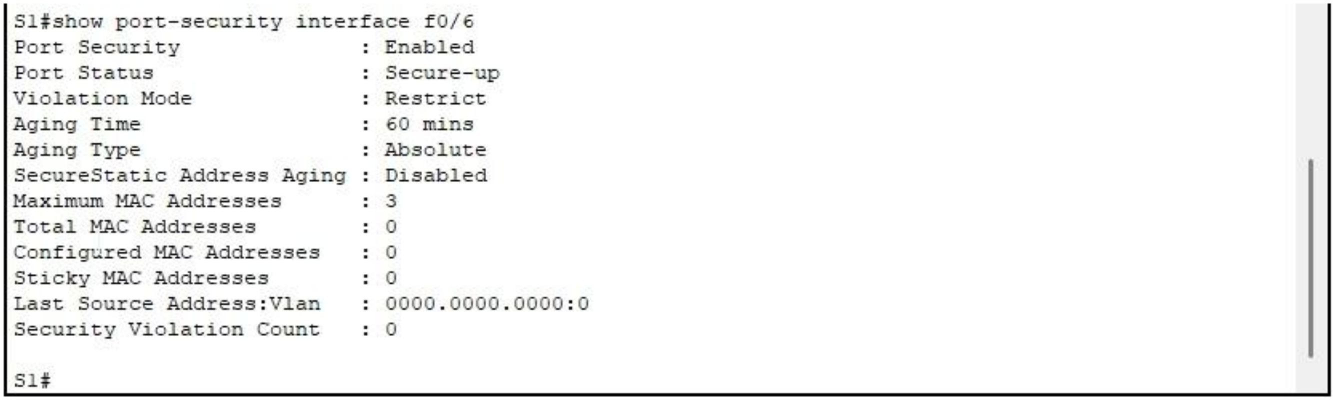
- Maximum number of MAC addresses: 3
- Violation type: restrict
- Aging time: 60 min
- Aging type: inactivity



```
S1>enable
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/6
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3
S1(config-if)#switchport port-security violation restrict
S1(config-if)#switchport port-security aging time 60
S1(config-if)#switchport port-security aging type inactivity
```

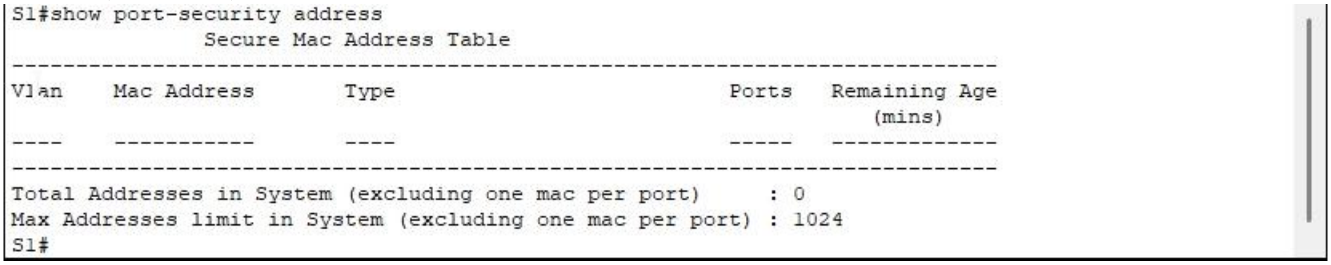
3. Verify port security on S1 F0/6.

S1# show port-security interface f0/6



```
S1#show port-security interface f0/6
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 60 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

S1#
```

S1# show port-security address



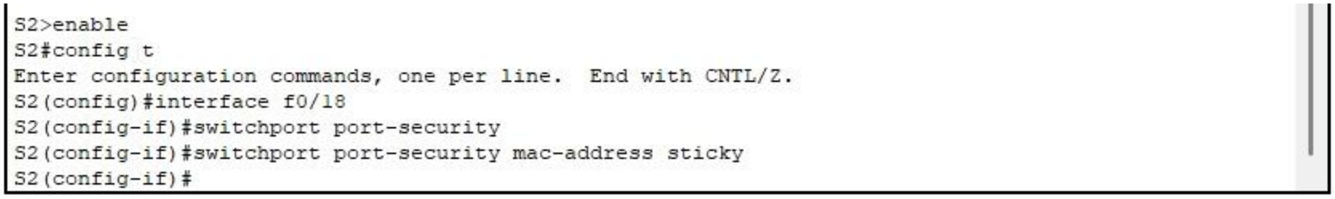
```
S1#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S1#
```

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.

S2(config)# interface f0/18

S2(config-if)# switchport port-security

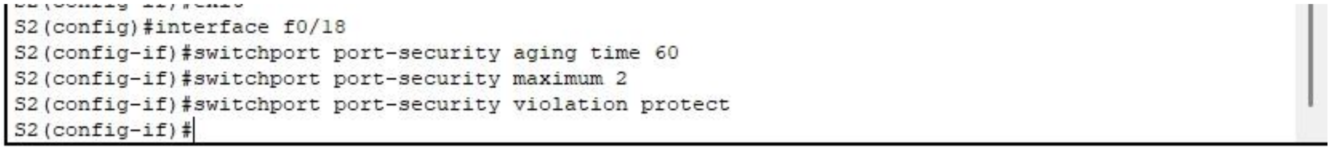
S2(config-if)# switchport port-security mac-address sticky



```
S2>enable
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#
```

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

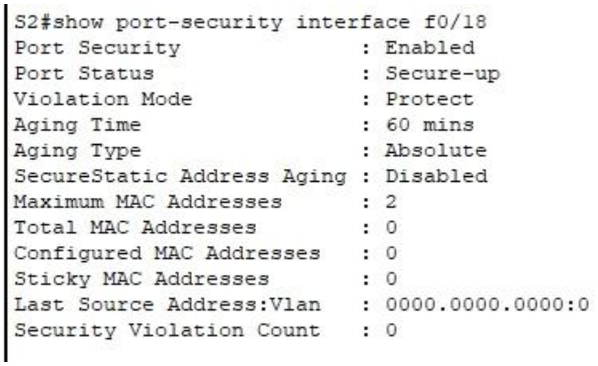
- Maximum number of MAC addresses: 2
- Violation type: Protect
- Aging time: 60 min



```
S2(config)#interface f0/18
S2(config-if)#switchport port-security aging time 60
S2(config-if)#switchport port-security maximum 2
S2(config-if)#switchport port-security violation protect
S2(config-if)#
```

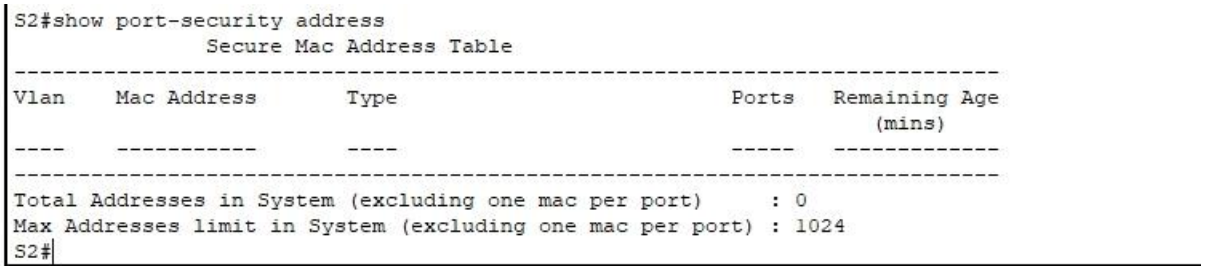
6. Verify port security on S2 F0/18.

S2# show port-security interface f0/18



```
S2#show port-security interface f0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 60 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

S2# show port-security address



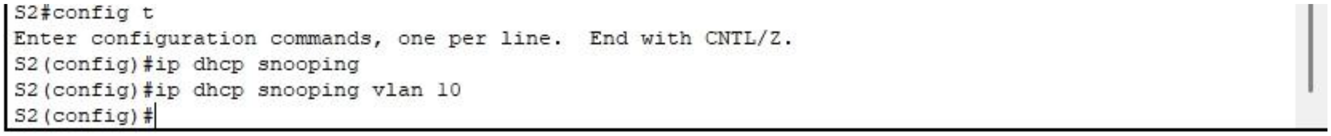
```
S2#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S2#
```

Step 5: Implement DHCP snooping security.

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

S2(config)# ip dhcp snooping

S2(config)# ip dhcp snooping vlan 10

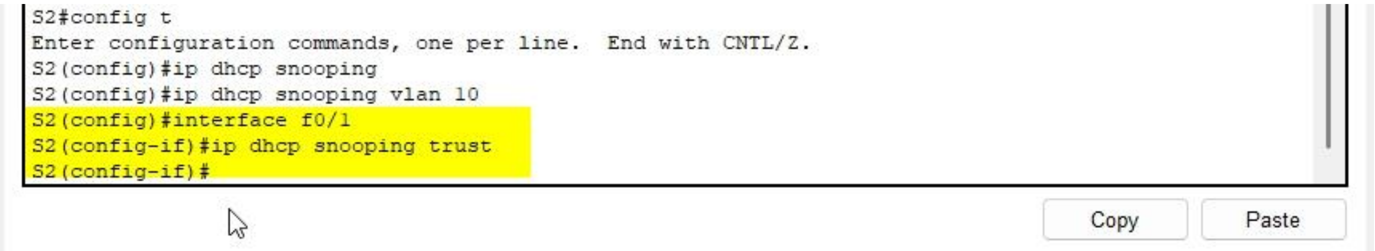


```
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#ip dhcp snooping
S2(config)#ip dhcp snooping vlan 10
S2(config)#
```

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

S2(config)# interface f0/1

S2(config-if)# ip dhcp snooping trust

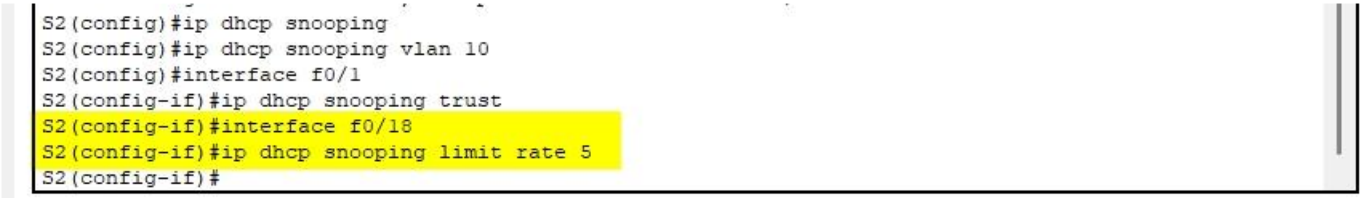


```
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#ip dhcp snooping
S2(config)#ip dhcp snooping vlan 10
S2(config)#interface f0/1
S2(config-if)#ip dhcp snooping trust
S2(config-if)#
```

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

S2(config)# interface f0/18

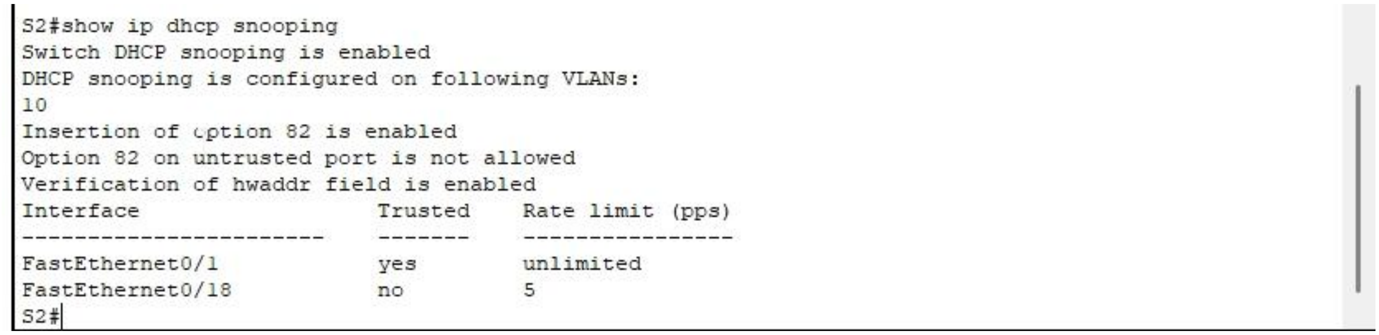
S2(config-if)# ip dhcp snooping limit rate 5



```
S2(config)#ip dhcp snooping
S2(config)#ip dhcp snooping vlan 10
S2(config)#interface f0/1
S2(config-if)#ip dhcp snooping trust
S2(config-if)#interface f0/18
S2(config-if)#ip dhcp snooping limit rate 5
S2(config-if)#
```

4. Verify DHCP Snooping on S2.

S2# show ip dhcp snooping

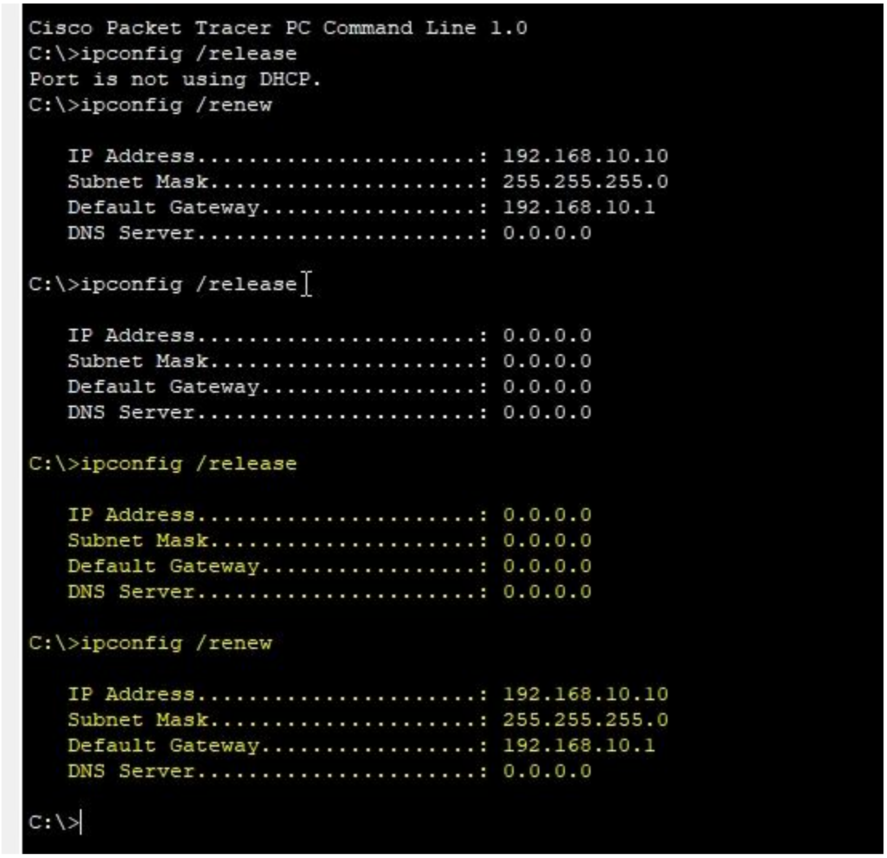


```
S2#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
Insertion of cption 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/1            yes        unlimited
FastEthernet0/18           no         5
S2#
```

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

C:\Users\Student> **ipconfig /release**

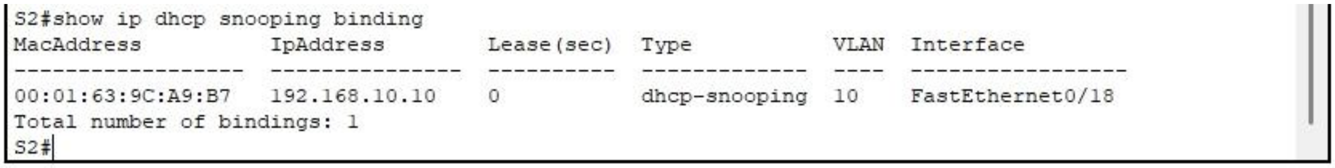
C:\Users\Student> **ipconfig /renew**



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /release
Port is not using DHCP.
C:\>ipconfig /renew

   IP Address......................: 192.168.10.10
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.10.1
   DNS Server......................: 0.0.0.0

C:\>ipconfig /release

   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0
   DNS Server......................: 0.0.0.0

C:\>ipconfig /release

   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0
   DNS Server......................: 0.0.0.0

C:\>ipconfig /renew

   IP Address......................: 192.168.10.10
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.10.1
   DNS Server......................: 0.0.0.0

C:\>
```

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

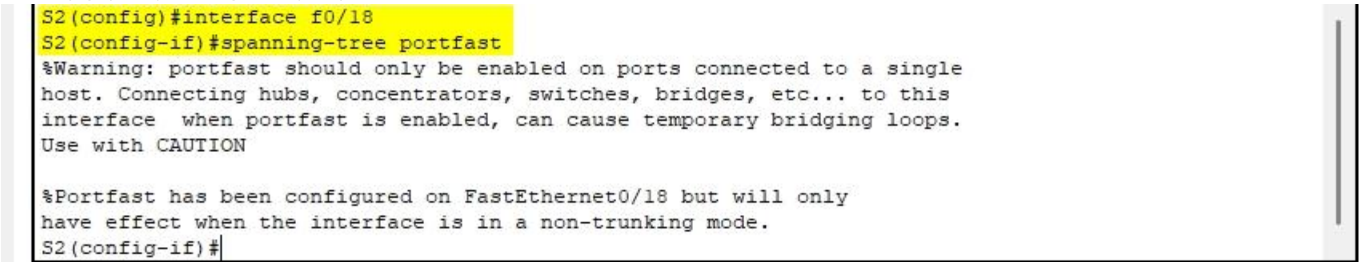
S2# show ip dhcp snooping binding



```
S2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
00:01:63:9C:A9:B7   192.168.10.10    0           dhcp-snooping  10    FastEthernet0/18
Total number of bindings: 1
S2#
```

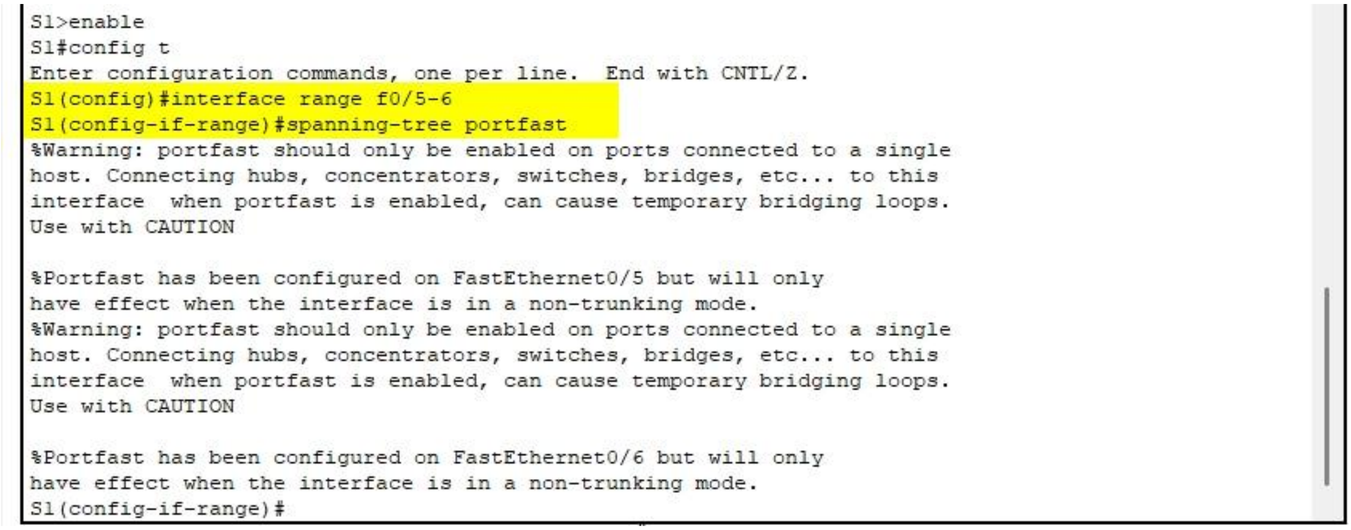
Step 6: Implement PortFast and BPDU guard.

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
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/18 but will only
have effect when the interface is in a non-trunking mode.
S2(config-if)#
```

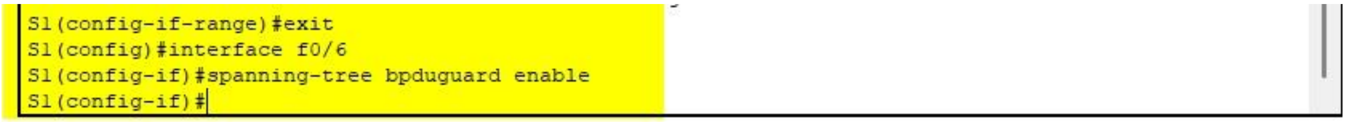
S2(config)# interface f0/18
S2(config-if)# spanning-tree portfast



```
S1>enable
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range f0/5-6
S1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if-range)#
```

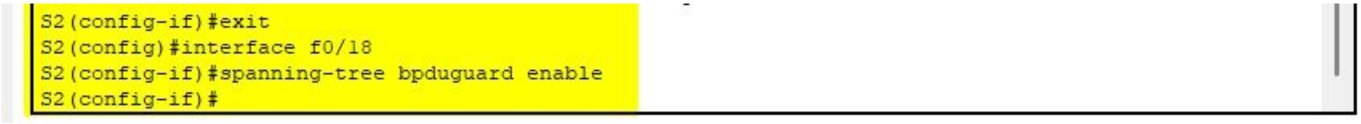
2. Enable BPDU guard on S1 and S2 VLAN 10 access ports connected to PC-A and PC-B.

S1(config)# interface f0/6
S1(config-if)# spanning-tree bpduguard enable



```
S1(config-if-range)#exit
S1(config)#interface f0/6
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#
```

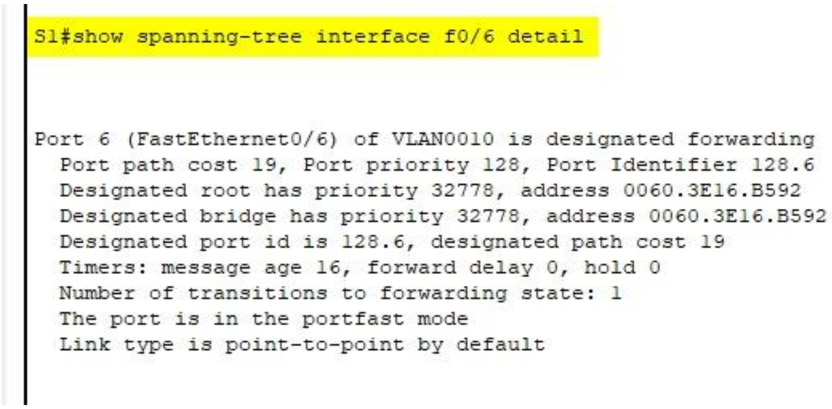
S2(config)# interface f0/18
S2(config-if)# spanning-tree bpduguard enable



```
S2(config-if)#exit
S2(config)#interface f0/18
S2(config-if)#spanning-tree bpduguard enable
S2(config-if)#
```

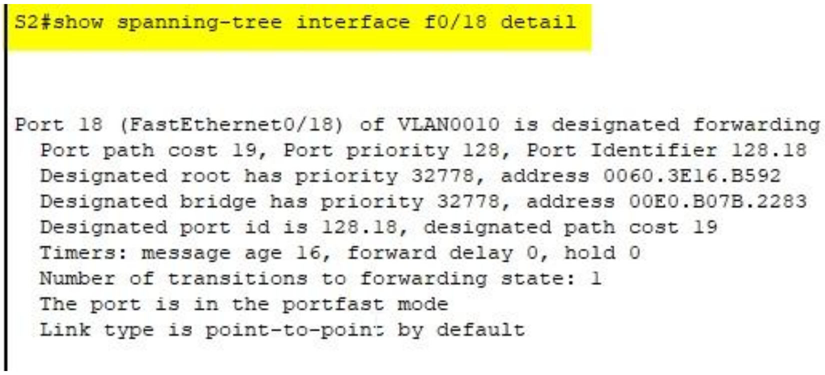
3. Verify that BPDU guard and PortFast are enabled on the appropriate ports.

S1# show spanning-tree interface f0/6 detail



```
S1#show spanning-tree interface f0/6 detail


Port 6 (FastEthernet0/6) of VLAN0010 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.6
  Designated root has priority 32778, address 0060.3E16.B592
  Designated bridge has priority 32778, address 0060.3E16.B592
  Designated port id is 128.6, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port is in the portfast mode
  Link type is point-to-point by default
```

S2# show spanning-tree interface f0/18 detail

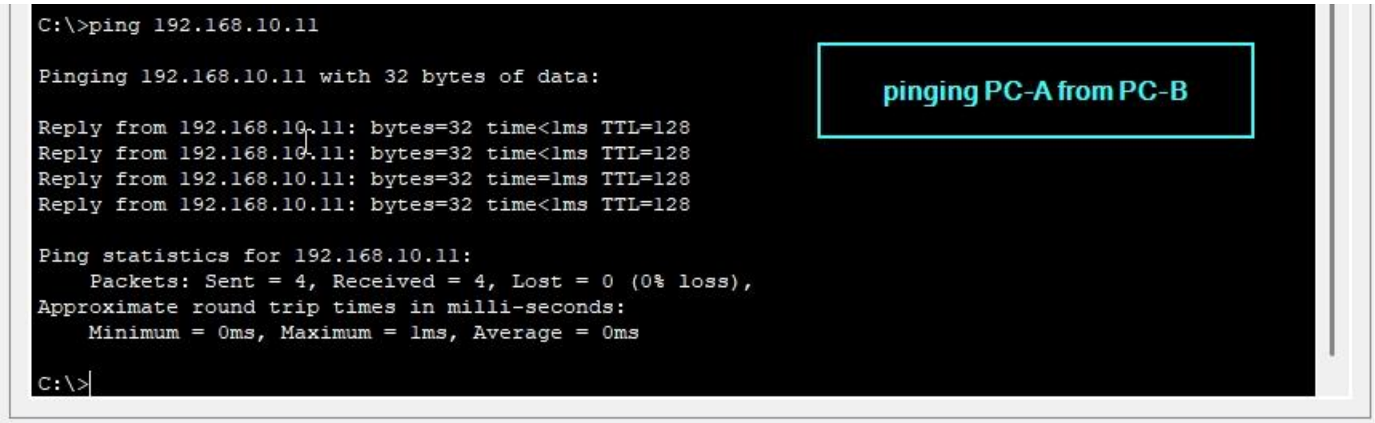


```
S2#show spanning-tree interface f0/18 detail


Port 18 (FastEthernet0/18) of VLAN0010 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.18
  Designated root has priority 32778, address 0060.3E16.B592
  Designated bridge has priority 32778, address 00E0.B07B.2283
  Designated port id is 128.18, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port is in the portfast mode
  Link type is point-to-poin: by default
```

Step 7: Verify end-to-end connectivity.

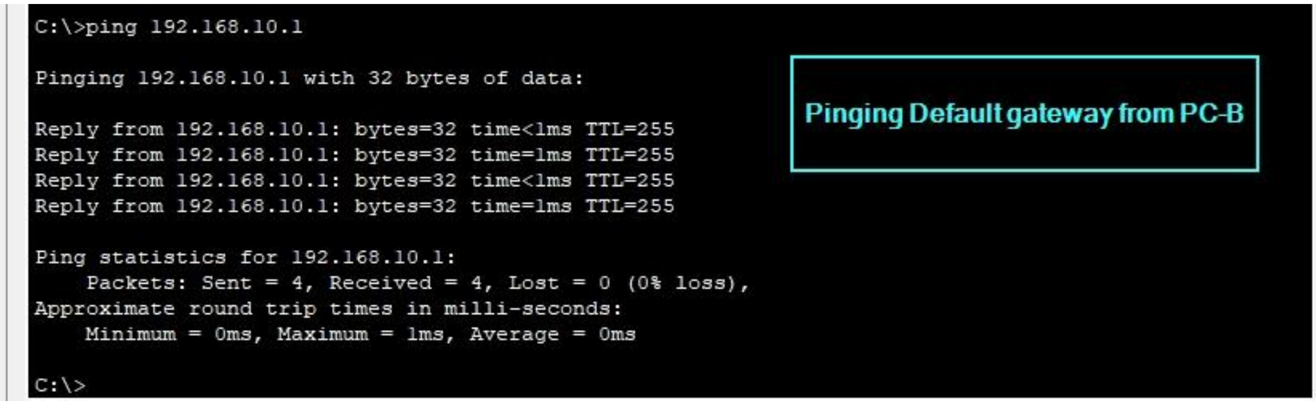
Verify PING connectivity between all devices in the IP Addressing Table. If the pings fail, you may need to disable the firewall on the PC hosts.

Pinging PC-A from PC-B



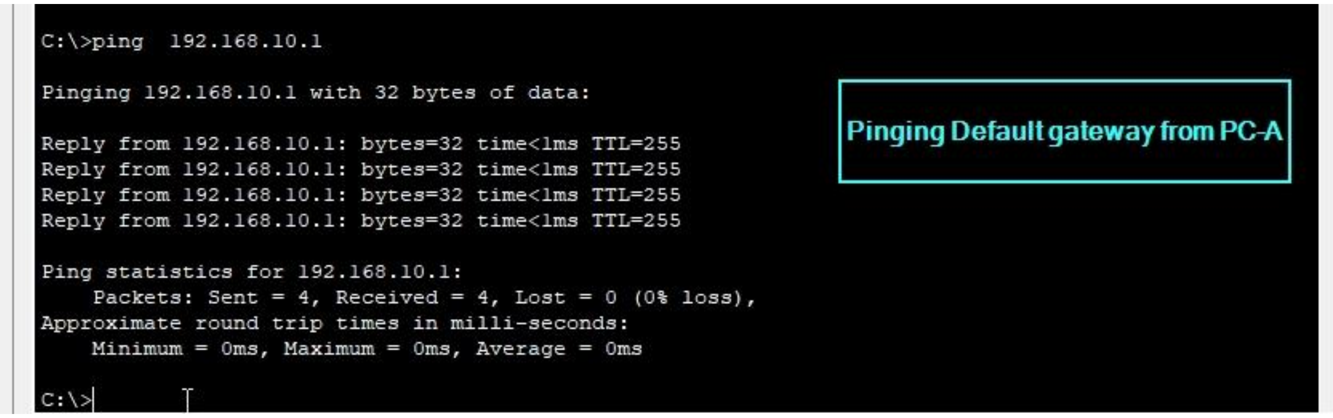
```
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128
Reply from 192.168.10.11: bytes=32 time=1ms TTL=128
Reply from 192.168.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Pinging default gateway from PC-B



```
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Pinging default gateway from PC-A



```
C:\>ping  192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Answer to Questions

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

This switch doesn't support aging (automatic removal) of sticky MAC addresses. So, once a MAC address is learned and saved using sticky, it stays unless you remove it manually. That's why there's no timer showing how long the MAC address will last.

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 18 is only allowed to learn two MAC addresses, and both of them are already saved (sticky). Since PC-B has a different MAC address, the switch blocks it. The port is set to "protect" mode, so it quietly drops PC-B's traffic without showing any warning or error messages.

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

- *Inactivity aging: The MAC address is removed if there's no activity from that device for a certain amount of time.*
- *Absolute aging: The MAC address is removed after a set amount of time, no matter if the device is active or not.*

Device Configurations – Final

Switch S1

```
S1#show running-config
Building configuration...

Current configuration : 3129 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
description link to S2
switchport trunk native vlan 333
switchport mode trunk
switchport nonegotiate
!
interface FastEthernet0/2
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/3
```

```
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/4
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/5
description link to R1
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/6
description link to PC-A
switchport access vlan 10
switchport mode access
switchport port-security
switchport port-security maximum 3
switchport port-security violation restrict
switchport port-security aging time 60
spanning-tree portfast
spanning-tree bpduguard enable
!
interface FastEthernet0/7
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/8
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/9
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/10
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/11
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/12
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/13
```

```
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/14
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/15
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/16
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/17
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/18
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/19
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/20
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/21
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/22
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/23
switchport access vlan 999
switchport mode access
shutdown
!
interface FastEthernet0/24
switchport access vlan 999
switchport mode access
```

```
shutdown
!
interface GigabitEthernet0/1
switchport access vlan 999
switchport mode access
shutdown
!
interface GigabitEthernet0/2
switchport access vlan 999
switchport mode access
shutdown
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
description Management SVI
ip address 192.168.10.201 255.255.255.0
!
ip default-gateway 192.168.10.1
!
!
!
!
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
!
!
!
end
```

Switch S2

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

Current configuration : 3342 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S2
!
!
!
no ip domain-lookup
```

```
!
!
ip dhcp snooping vlan 10
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 description Link to S1
 switchport trunk native vlan 333
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/3
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/4
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport access vlan 999
 switchport mode access
 spanning-tree portfast
 shutdown
!
interface FastEthernet0/6
 switchport access vlan 999
 switchport mode access
 spanning-tree portfast
 shutdown
!
interface FastEthernet0/7
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/9
```

```
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/11
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/12
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/13
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/14
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/15
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/16
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/17
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/18
 description Link to PC-B
 switchport access vlan 10
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation protect
 switchport port-security mac-address sticky 0001.639C.A9B7
 switchport port-security aging time 60
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/19
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/20
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/21
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/22
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/23
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/24
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface GigabitEthernet0/1
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface GigabitEthernet0/2
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description Management SVI
 ip address 192.168.10.202 255.255.255.0
!
```

```
ip default-gateway 192.168.10.1
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```

Conclusion

The lab successfully demonstrated the implementation of several critical switch security features that are widely recommended in enterprise environments. VLANs and trunking were configured to ensure logical segmentation of network traffic. Port security was applied to limit the number of allowed MAC addresses per port, helping prevent MAC flooding attacks. DHCP snooping was implemented to secure the network against rogue DHCP servers by identifying trusted and untrusted ports. Additionally, PortFast and BPDU Guard were configured to enhance the network's resilience against Layer 2 loops and misconfigurations. The final network setup allowed for secure and reliable connectivity between end devices, validating the effectiveness of the implemented security mechanisms. This lab emphasized the importance of proactive switch security configuration in maintaining network integrity and performance.