

Course: Cloud and Network Security-C1-2026

Cyber Shujaa Program

Week 4: Securing Network Layers 1-3

Assignment 1: VLANs & Secure Switch Configuration

Student Name: Salim Katana Karuku

Student ID: CS-CNS11-26048

Contents

Course: Cloud and Network Security-C1-2026	1
Cyber Shujaa Program.....	1
Week 4: Securing Network Layers 1-3	1
Assignment 1: VLANs & Secure Switch Configuration	1
Introduction	3
Objectives	4
Packet Tracer Lab: Switch Security Configuration.....	5
Topology	5
Part 1: Configure the Network Devices.	5
Step 2: Configure R1.	6
Step 3: Configure and verify basic switch settings.	8
1. Part 2: Configure VLANs on Switches.....	11
Step 1: Configure VLAN 10.	11
Step 2: Configure the SVI for VLAN 10.	12
Step 3: Configure VLAN 333 with the name Native on S1 and S2.....	12
Step 4: Configure VLAN 999 with the name ParkingLot on S1 and S2.	13
Part 3: Configure Switch Security.....	13
Step 2: Configure access ports.	16
Step 3: Secure and disable unused switchports.....	18
Step 4: Document and implement port security features.	20
6. Verify port security on S2 F0/18	24
Step 5: Implement DHCP snooping security.....	25
Step 6: Implement PortFast and BPDU guard.	28
Step 7: Verify end-to-end connectivity.....	30
Conclusion	31

Introduction

This assignment focuses on the implementation of Virtual Local Area Networks (VLANs) and secure switch configuration. The purpose of the assignment is to understand how VLANs are used to logically segment a network in order to improve performance, enhance security and simplify network management. It also covers basic switch security measures used to protect a network from unauthorized access and potential threats.

Objectives

The objectives of the assignment were:

1. To create and configure Virtual Local Area Networks (VLANs) on a network switch
2. To assign switch ports to different VLANs according to network requirements.
3. To configure trunk links for inter-VLAN communication
4. To implement basic switch security features such as port security and disabling unused ports.
5. To test and verify VLAN connectivity and switch security configurations

Packet Tracer Lab: Switch Security Configuration

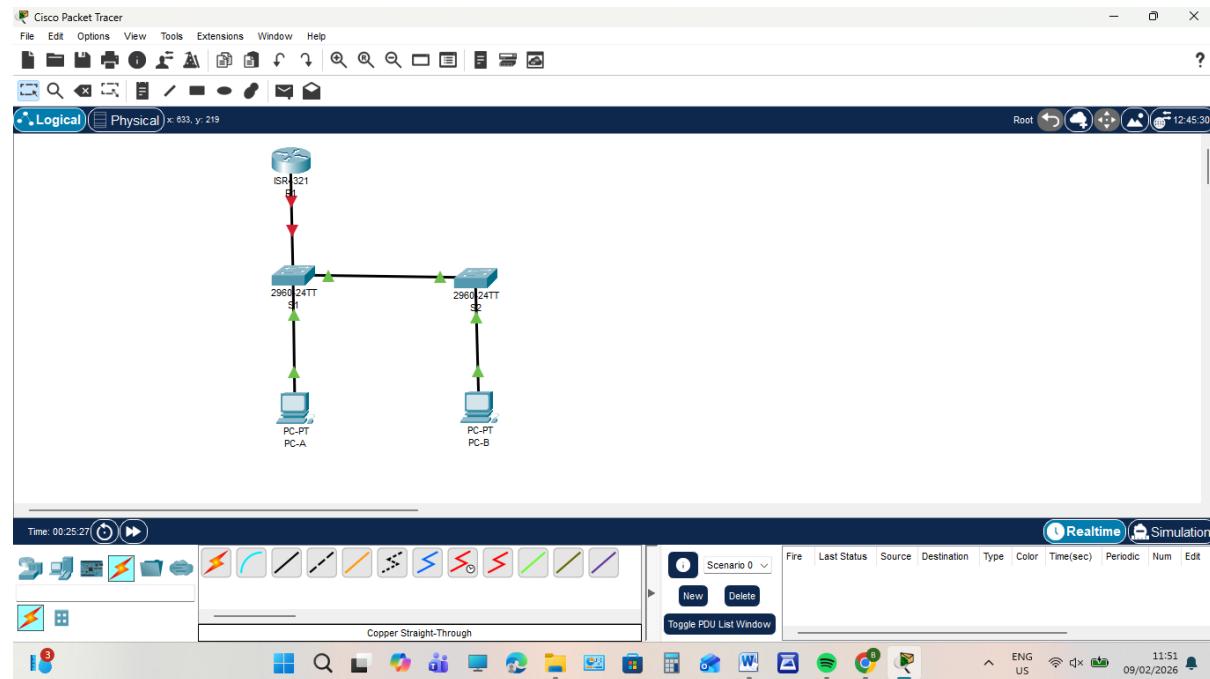
Topology

Part 1: Configure the Network Devices.

Step 1: Cable the network.

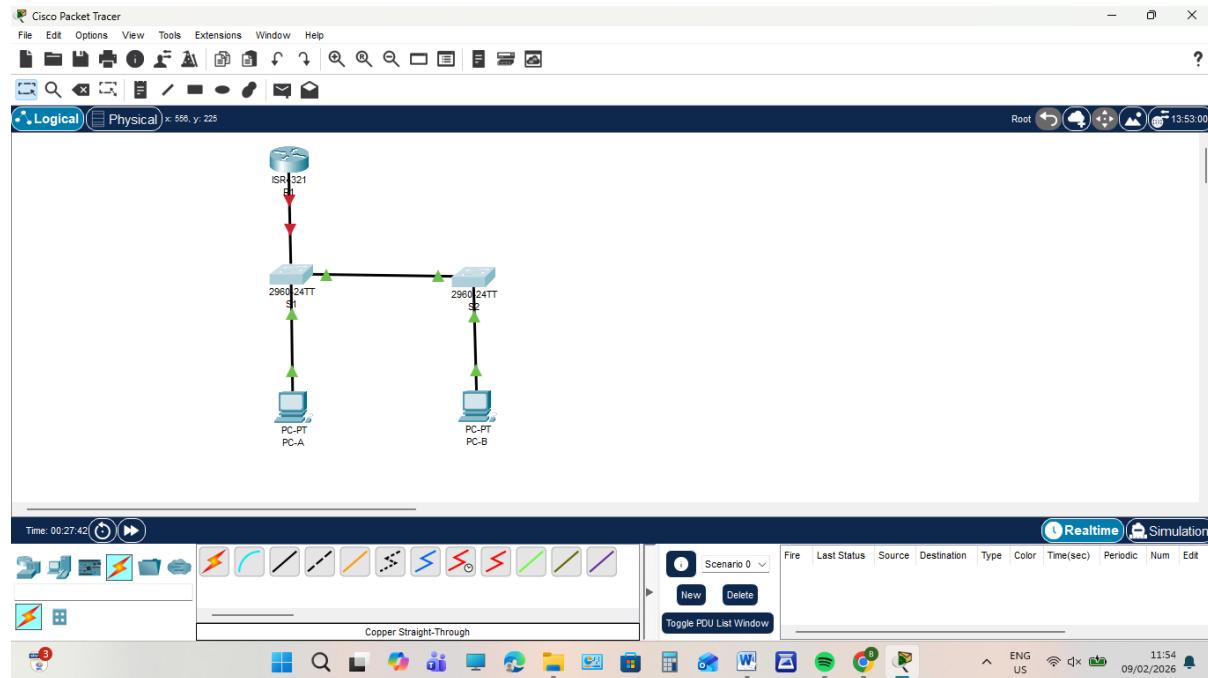
1. Cable the network as shown in the topology.

Here I cable the network as shown bellow



2. Initialize the devices.

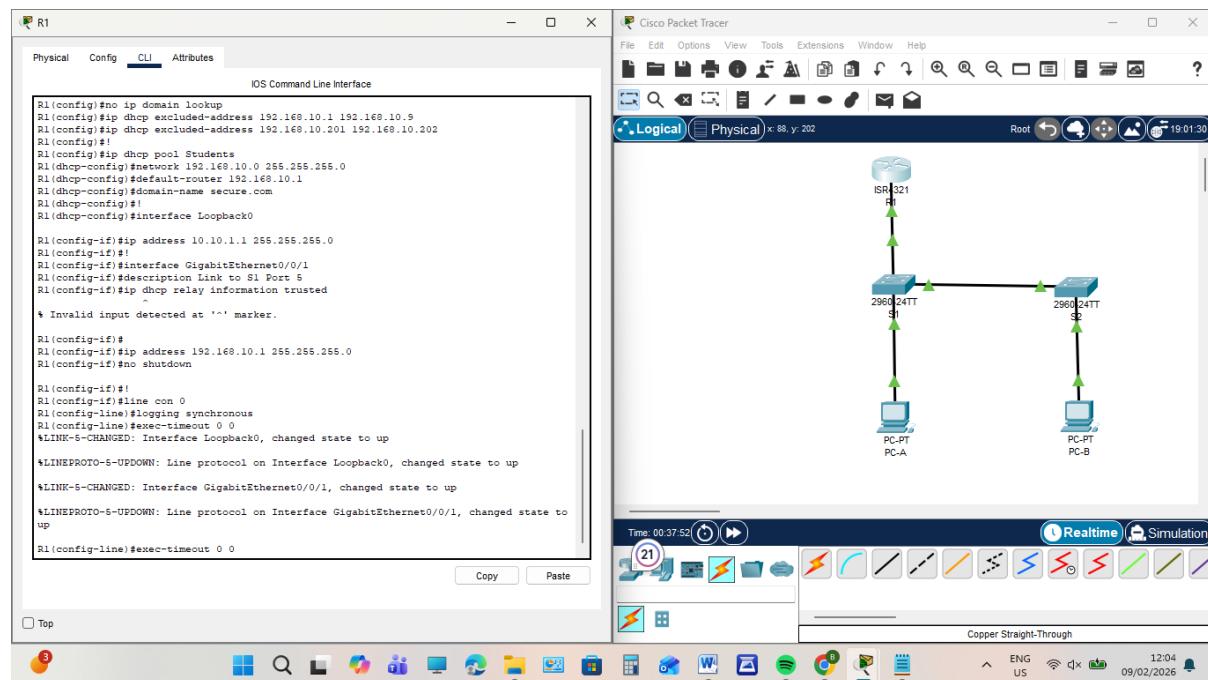
Then I initialize the router and the switches



Step 2: Configure R1.

1. Load the following configuration script on R1.

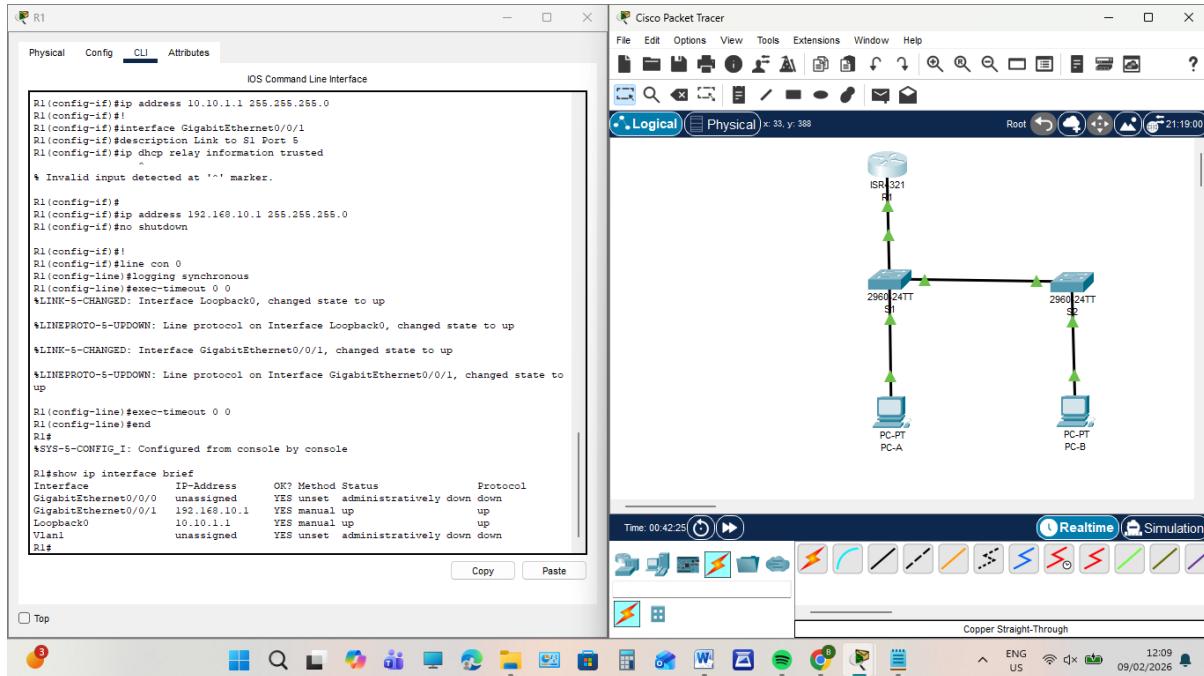
Here I load so that I can conf R1 as shown below



2. Verify the running-configuration on R1 using the following command:

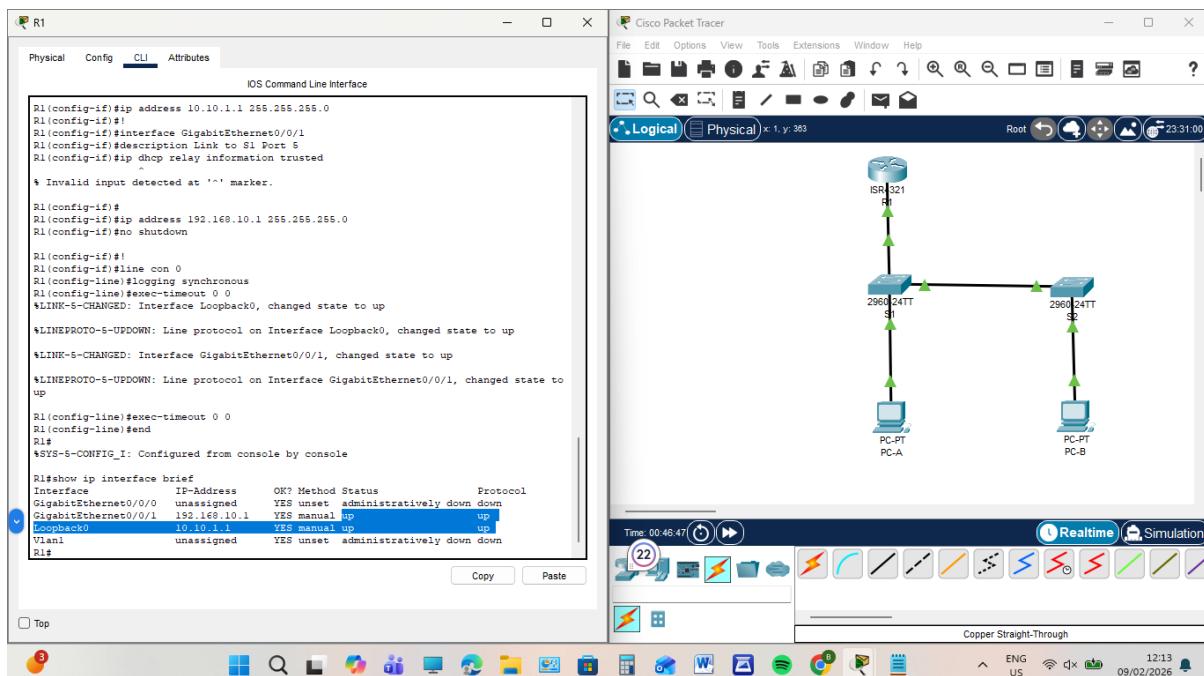
R1# show ip interface brief

Here I used the R1 so that I can show the interface as shown below



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

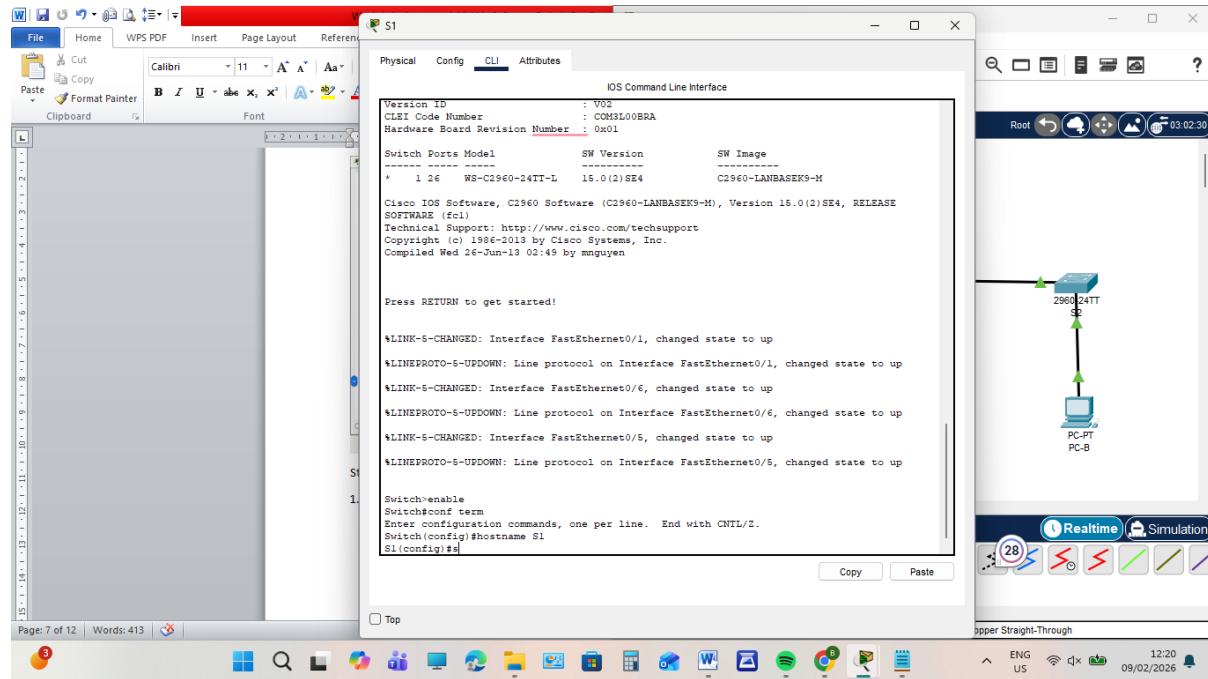
The IP addresses interfaces were verify and both were in an up/up state



Step 3: Configure and verify basic switch settings.

1. Configure the hostname for switches S1 and S2.

Here is the hostname for S1



S1

Physical Config CLI Attributes

IOS Command Line Interface

```

Version ID : V02
CLIEI Code Number : COMSL00BRA
Hardware Board Revision Number : 0x01

Switch Ports Model SW Version SW Image
----- -----
* 1 26 WS-C2960-24TT-L 15.0(2)SE4 C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnnguyen

Press RETURN to get started!

*LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
*LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
*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#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#

```

Copy Paste

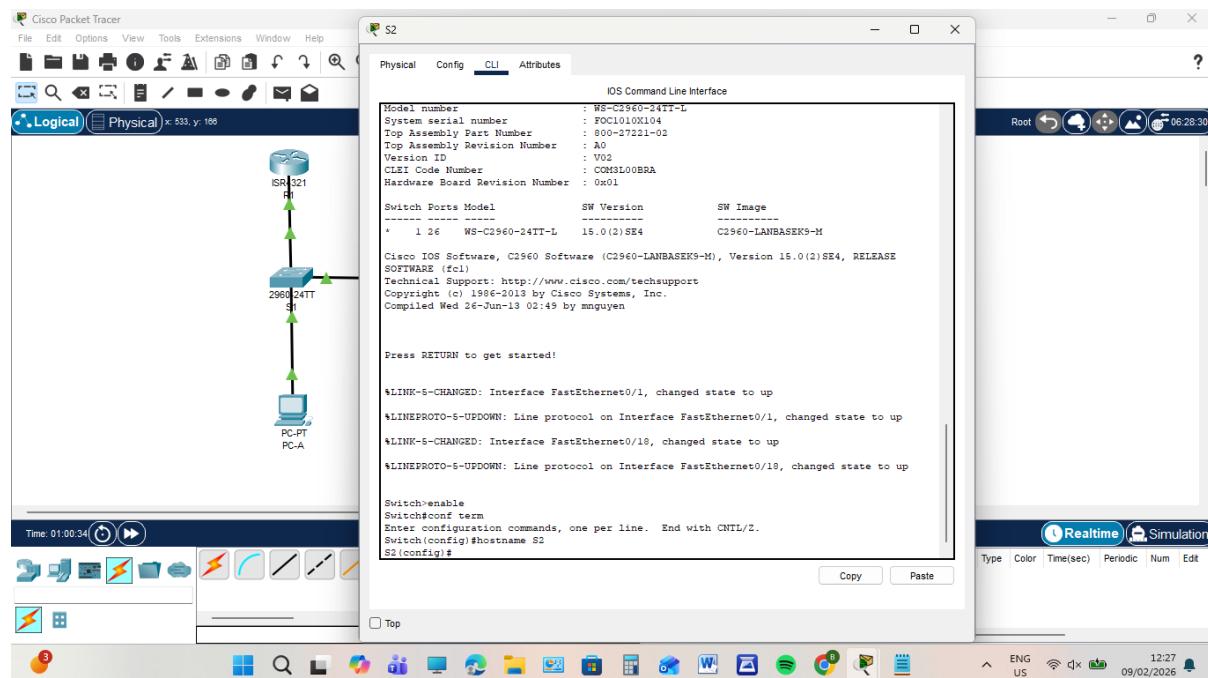
Top

Realtime Simulation

Upper Straight-Through

Page 7 of 12 | Words: 413 | 12:20 09/02/2026

Here is the hostname for S2



S2

Physical Config CLI Attributes

IOS Command Line Interface

```

Model number : WS-C2960-34TT-L
System serial number : FOC1010X104
Top Assembly Part Number : 800-27321-02
Top Assembly Revision Number : A0
Version ID : V02
CLIEI Code Number : COMSL00BRA
Hardware Board Revision Number : 0x01

Switch Ports Model SW Version SW Image
----- -----
* 1 26 WS-C2960-34TT-L 15.0(2)SE4 C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnnguyen

Press RETURN to get started!

*LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
*LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up
*LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up

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

```

Copy Paste

Top

Realtime Simulation

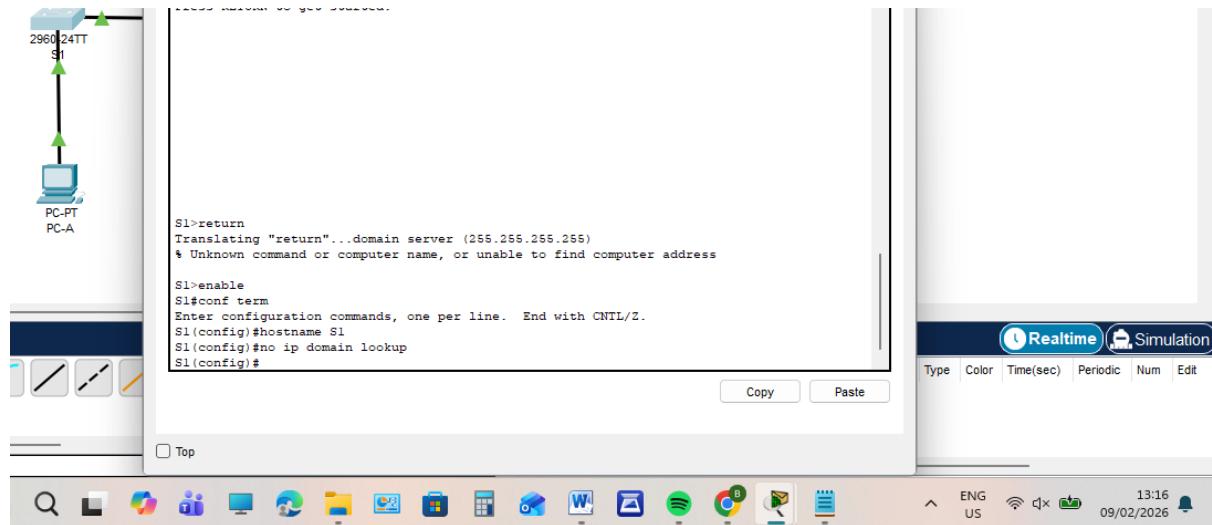
Type Color Time(sec) Periodic Num Edit

Time: 01:00:34

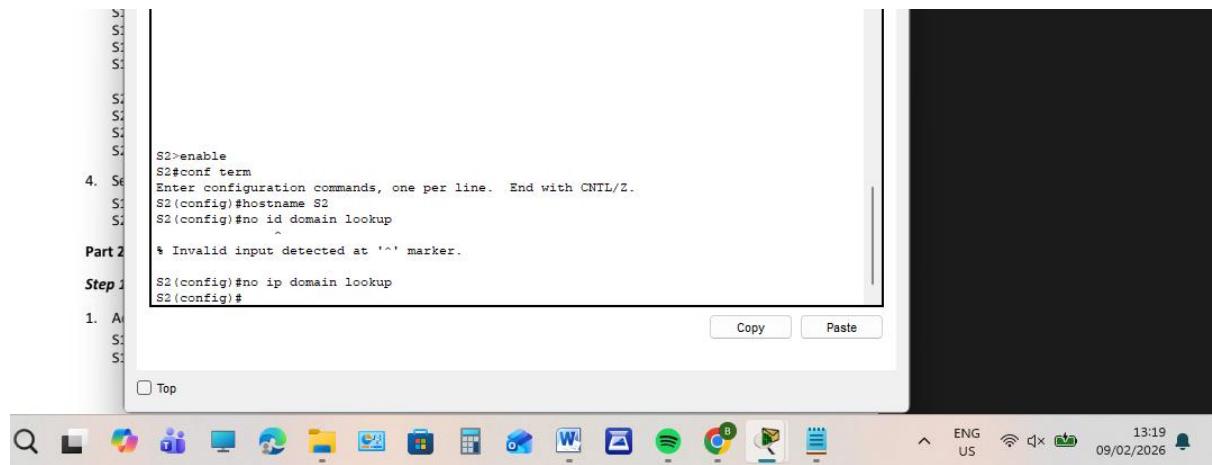
12:27 09/02/2026

2. Prevent unwanted DNS lookups on both switches.

Here for S1

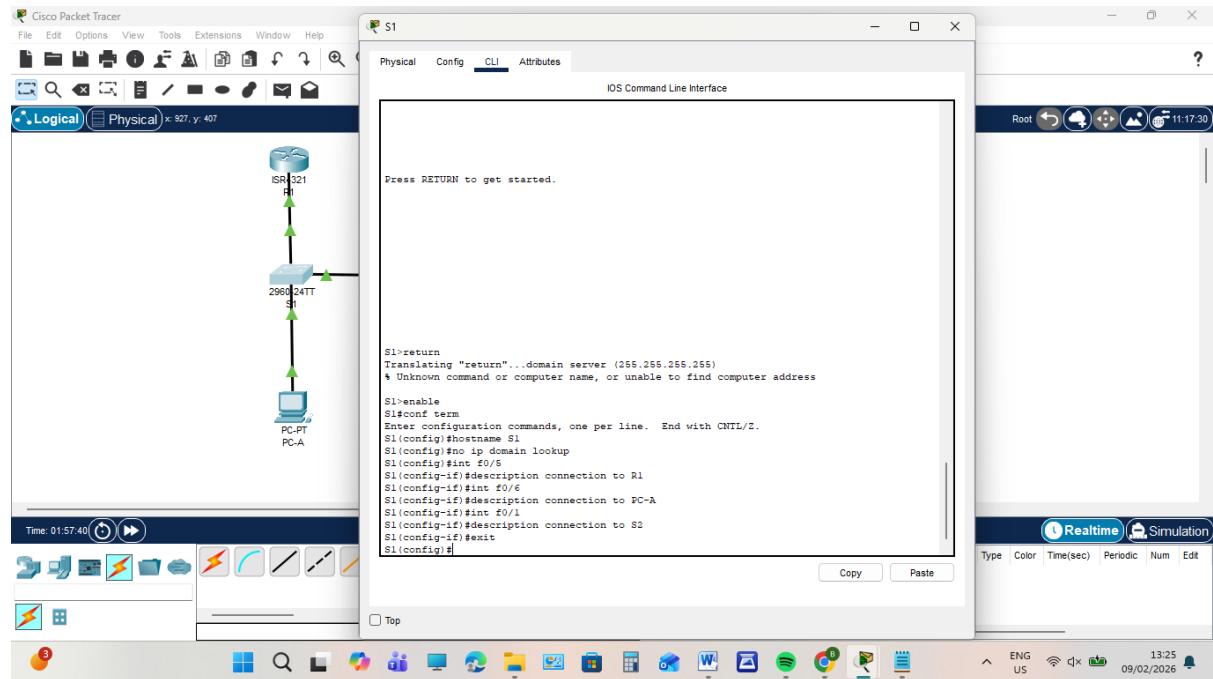


And for S2

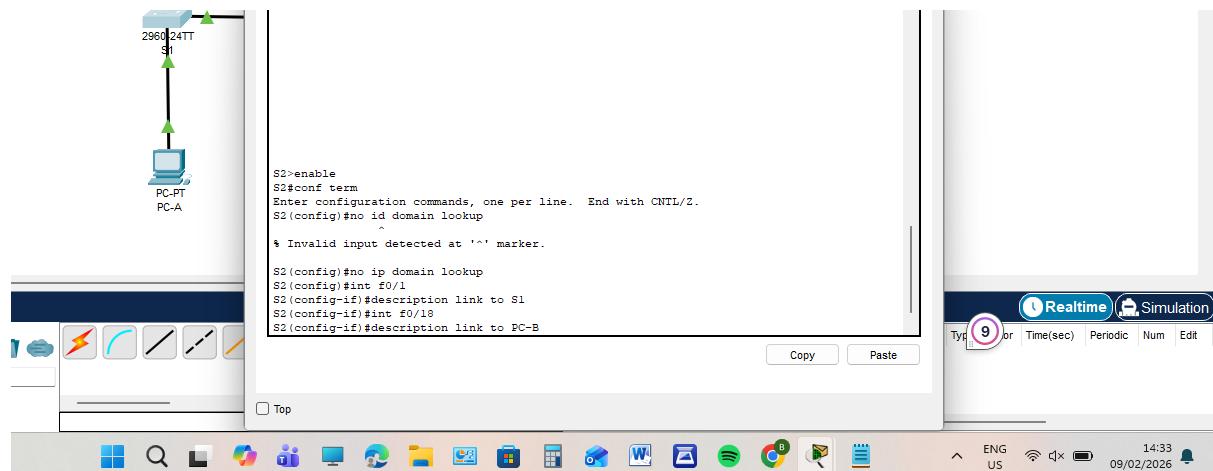


3. Configure interface descriptions for the ports that are in use in S1 and S2.

Interface for S1

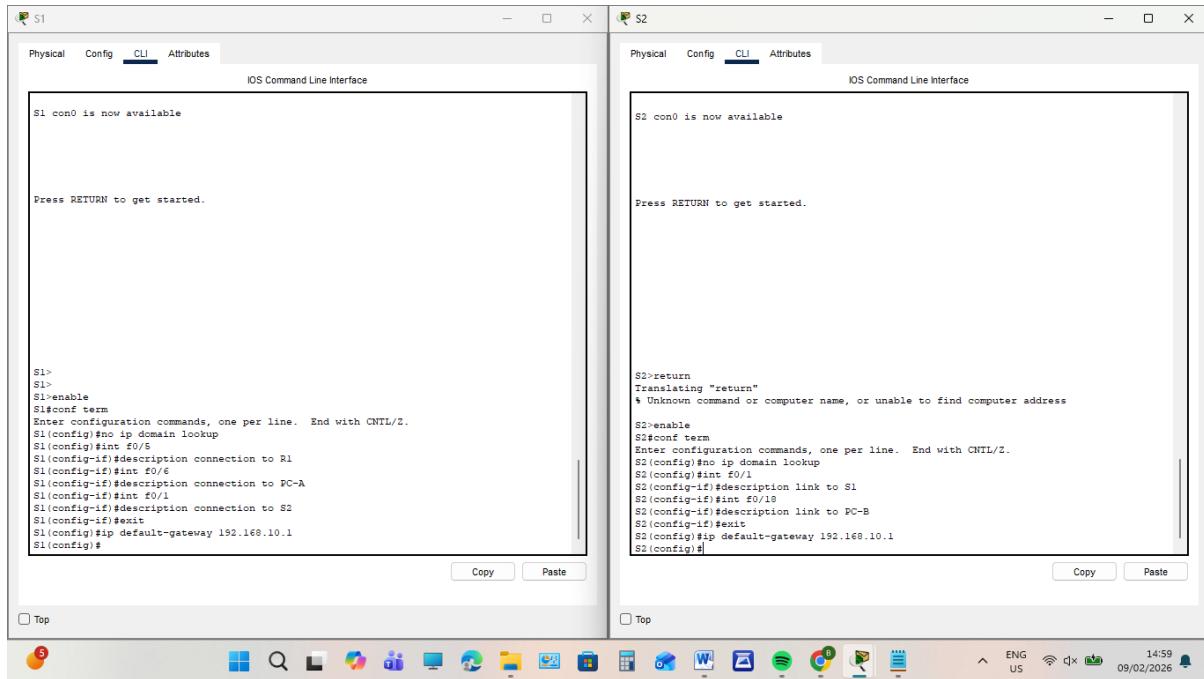


Interface for S2



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

Here is the default-gateway for both S1 and S2



```

S1>
S1>enable
S1>conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#no ip domain lookup
S1(config)#int f0/6
S1(config-if)#description connection to R1
S1(config-if)#int f0/6
S1(config-if)#description connection to PC-A
S1(config-if)#int f0/1
S1(config-if)#description connection to S2
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.10.1
S1(config)#

```



```

S2>return
Translating "return"
% Unknown command or computer name, or unable to find computer address
S2>enable
S2>conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#no ip domain lookup
S2(config)#int f0/6
S2(config-if)#description link to S1
S2(config-if)#int f0/10
S2(config-if)#description link to PC-B
S2(config-if)#exit
S2(config)#ip default-gateway 192.168.10.1
S2(config)#

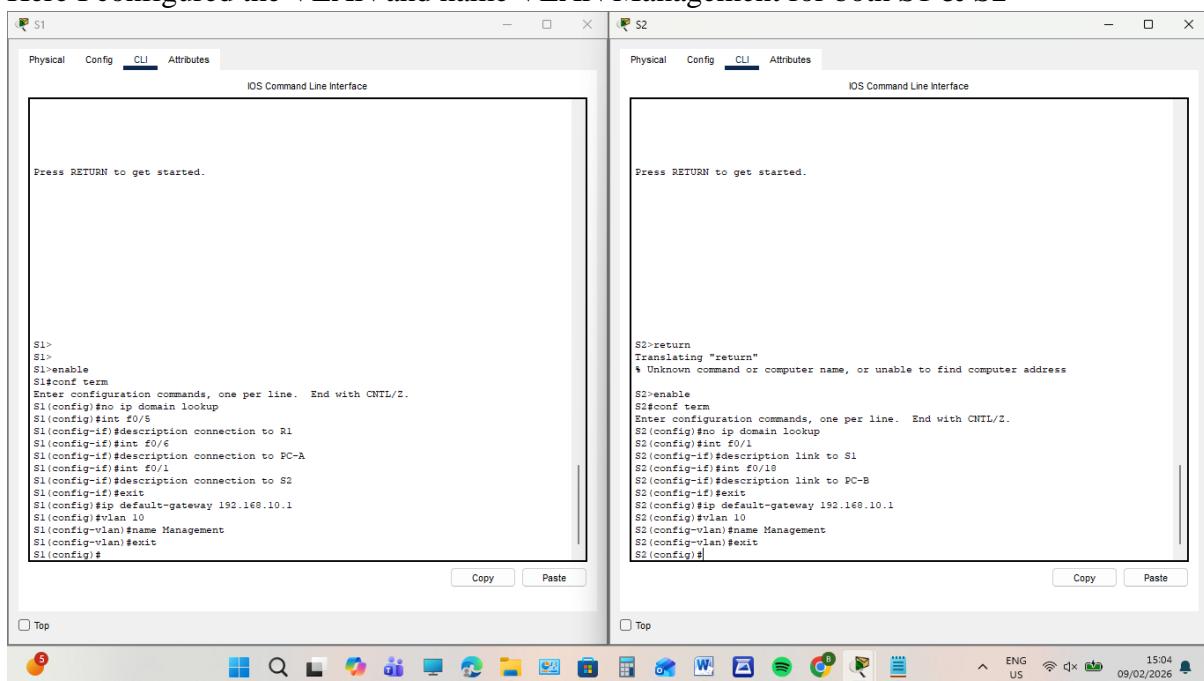
```

1. Part 2: Configure VLANs on Switches.

Step 1: Configure VLAN 10.

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

Here I configured the VLAN and name VLAN Management for both S1 & S2



```

S1>
S1>enable
S1>conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#no ip domain lookup
S1(config)#int f0/6
S1(config-if)#description connection to R1
S1(config-if)#int f0/6
S1(config-if)#description connection to PC-A
S1(config-if)#int f0/1
S1(config-if)#description connection to S2
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.10.1
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#

```



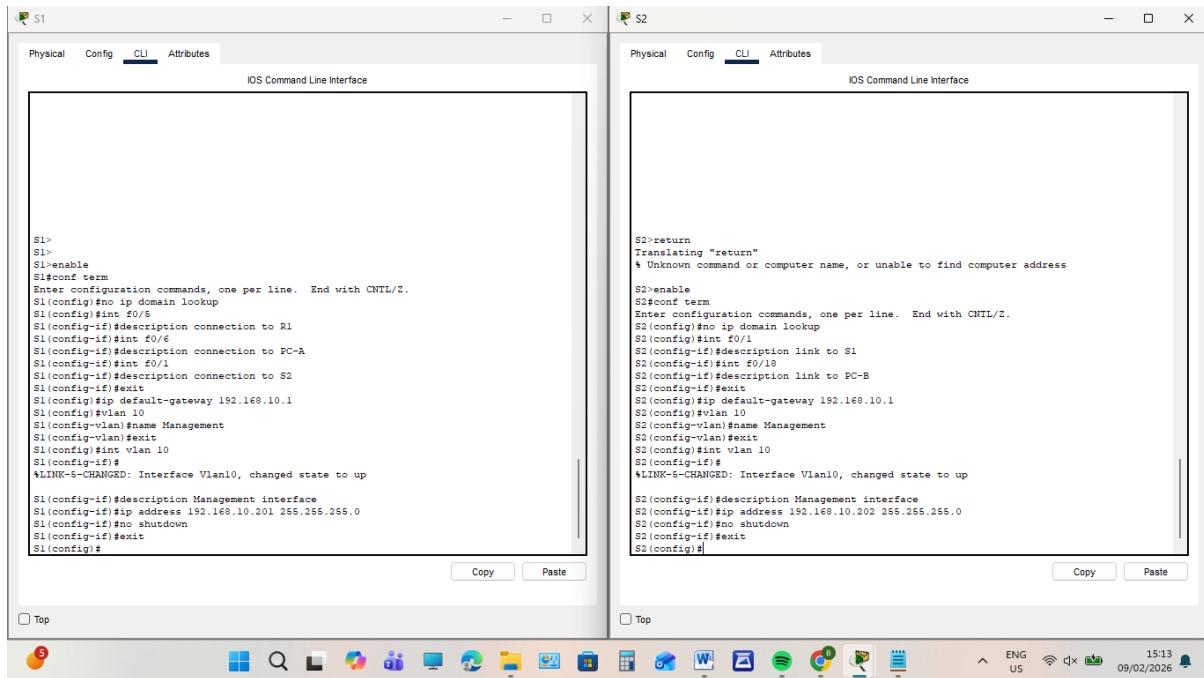
```

S2>return
Translating "return"
% Unknown command or computer name, or unable to find computer address
S2>enable
S2>conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#no ip domain lookup
S2(config)#int f0/1
S2(config-if)#description link to S1
S2(config-if)#int f0/10
S2(config-if)#description link to PC-B
S2(config-if)#exit
S2(config)#ip default-gateway 192.168.10.1
S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#exit
S2(config)#

```

Step 2: Configure the SVI for VLAN 10.

Then I configure the IP address according to the ones given for both S1 & S2



```

S1>
S1>
S1>enable
S1>conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#no ip domain lookup
S1(config)#int f0/5
S1(config-if)#description connection to R1
S1(config-if)#int f0/6
S1(config-if)#description connection to PC-A
S1(config-if)#int f0/1
S1(config-if)#description connection to S2
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.10.1
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#int vlan 10
S1(config-if)#
$LINK-5-CHANGED: Interface Vlan10, changed state to up

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

$LINK-5-CHANGED: Interface Vlan10, changed state to up

S2>return
Translating "return"
Unknown command or computer name, or unable to find computer address

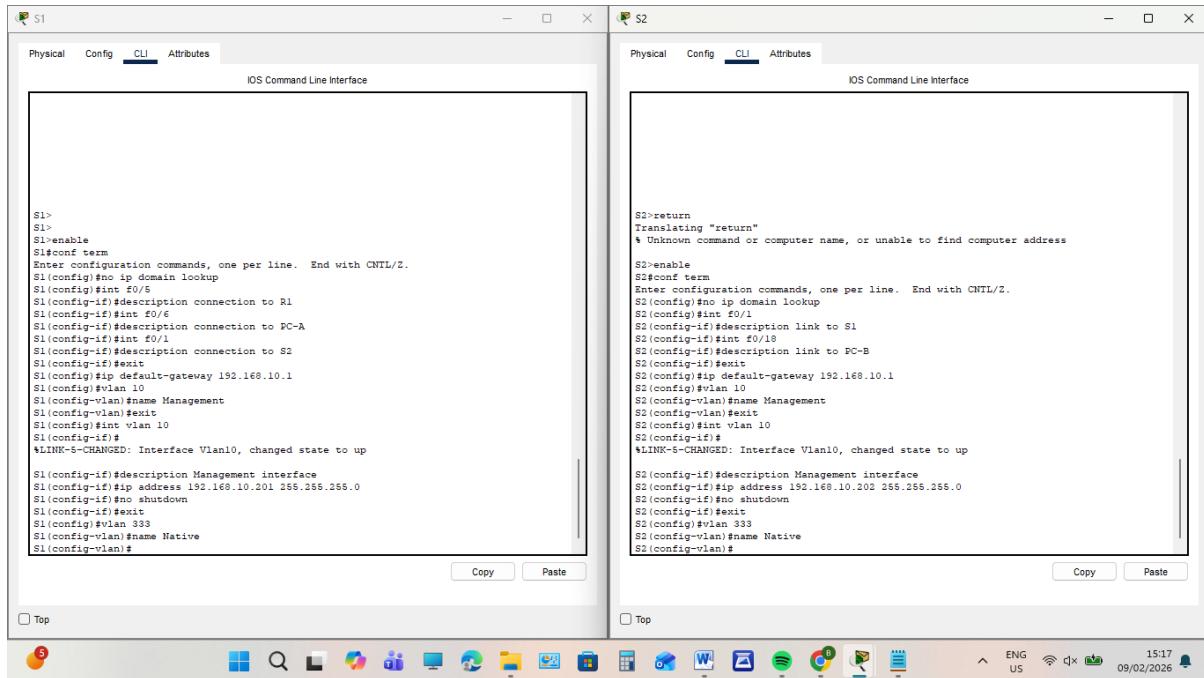
S2>enable
S2>conf term
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#no ip domain lookup
S2(config)#int f0/1
S2(config-if)#description link to S1
S2(config-if)#int f0/18
S2(config-if)#description link to PC-B
S2(config-if)#exit
S2(config)#ip default-gateway 192.168.10.1
S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#exit
S2(config)#int vlan 10
S2(config-if)#
$LINK-5-CHANGED: Interface Vlan10, changed state to up

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

```

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

Here I configure the VLAN for both S1 & S2



```

S1>
S1>
S1>enable
S1>conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#no ip domain lookup
S1(config-if)#description connection to R1
S1(config-if)#int f0/6
S1(config-if)#description connection to PC-A
S1(config-if)#int f0/1
S1(config-if)#description connection to S2
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.10.1
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#int vlan 10
S1(config-if)#
$LINK-5-CHANGED: Interface Vlan10, changed state to up

S1(config-if)#description Management interface
S1(config-if)#ip address 192.168.10.201 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#

S2>return
Translating "return"
Unknown command or computer name, or unable to find computer address

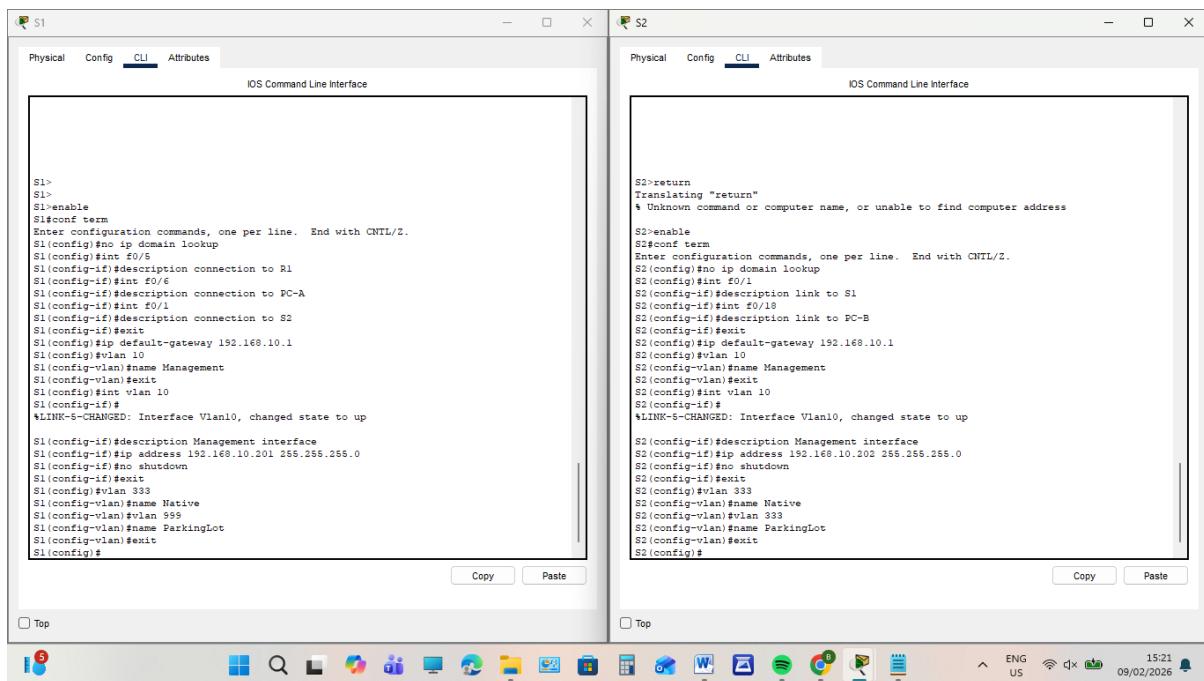
S2>enable
S2>conf term
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#no ip domain lookup
S2(config)#int f0/1
S2(config-if)#description link to S1
S2(config-if)#int f0/18
S2(config-if)#description link to PC-B
S2(config-if)#exit
S2(config)#ip default-gateway 192.168.10.1
S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#exit
S2(config)#int vlan 10
S2(config-if)#
$LINK-5-CHANGED: Interface Vlan10, changed state to up

S2(config-if)#description Management interface
S2(config-if)#ip address 192.168.10.202 255.255.255.0
S2(config-if)#no shutdown
S2(config-if)#exit
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.

Here are both for S1 & S2



```

S1>
S1>
S1>enable
S1>conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#ip domain lookup
S1(config)#int f0/5
S1(config-if)#description connection to R1
S1(config-if)#int f0/6
S1(config-if)#description connection to PC-A
S1(config-if)#int f0/1
S1(config-if)#description connection to S2
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.10.1
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#int vlan 10
S1(config-if)#
*LINK-5-CHANGED: Interface Vlan10, changed state to up
S1(config-if)#description Management interface
S1(config-if)#ip address 192.168.10.201 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#exit
S1(config)#

```



```

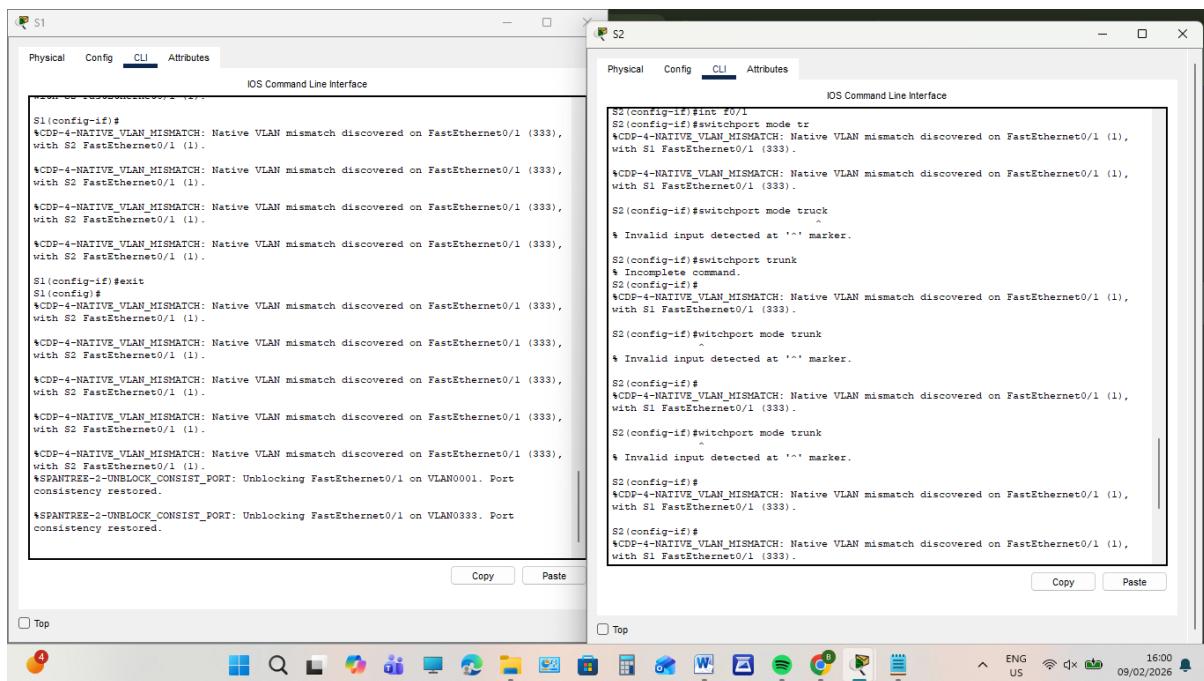
S2>return
Translating "return"
* Unknown command or computer name, or unable to find computer address
S2>enable
S2>conf term
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#ip domain lookup
S2(config-if)#int f0/5
S2(config-if)#description link to S1
S2(config-if)#int f0/18
S2(config-if)#description link to PC-B
S2(config-if)#exit
S2(config)#ip default-gateway 192.168.10.1
S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#exit
S2(config)#int vlan 10
S2(config-if)#
*LINK-5-CHANGED: Interface Vlan10, changed state to up
S2(config-if)#description Management interface
S2(config-if)#ip address 192.168.10.202 255.255.255.0
S2(config-if)#no shutdown
S2(config-if)#
S2(config)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#vlan 333
S2(config-vlan)#name ParkingLot
S2(config-vlan)#exit
S2(config)#

```

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-if)#
*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2 FastEthernet0/1 (1).

*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2 FastEthernet0/1 (1).

*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2 FastEthernet0/1 (1).

*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2 FastEthernet0/1 (1).

*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2 FastEthernet0/1 (1).

*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2 FastEthernet0/1 (1).

*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2 FastEthernet0/1 (1).

*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2 FastEthernet0/1 (1).

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

*SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0333. Port consistency restored.

S2(config-if)#
*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S1 FastEthernet0/1 (333).

*S2(config-if)#
*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S1 FastEthernet0/1 (333).

*S2(config-if)#
*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S1 FastEthernet0/1 (333).

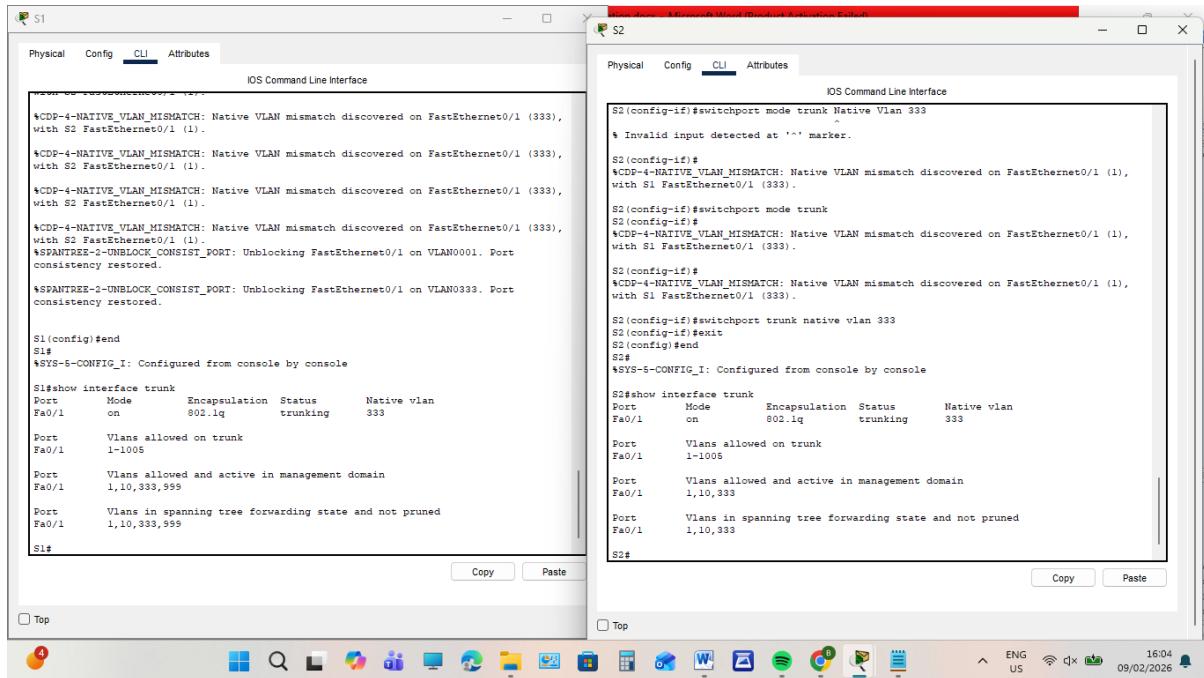
*S2(config-if)#
*CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (1), with S1 FastEthernet0/1 (333).

```

2. Verify that trunking is configured on both switches.

S1# show interface trunk

➤ Here are for both S1 & S2



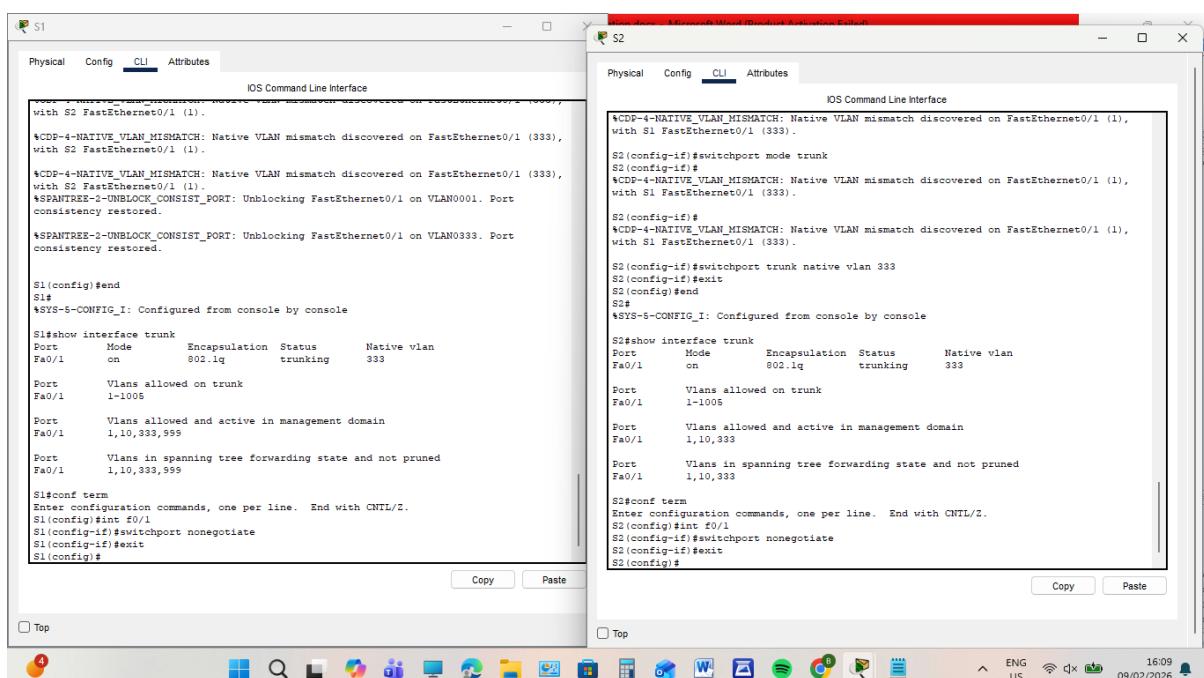
```

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
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
Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,333
S2#

```

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

➤ The negotiation on F0/1 for both S1 & S2 as shown below



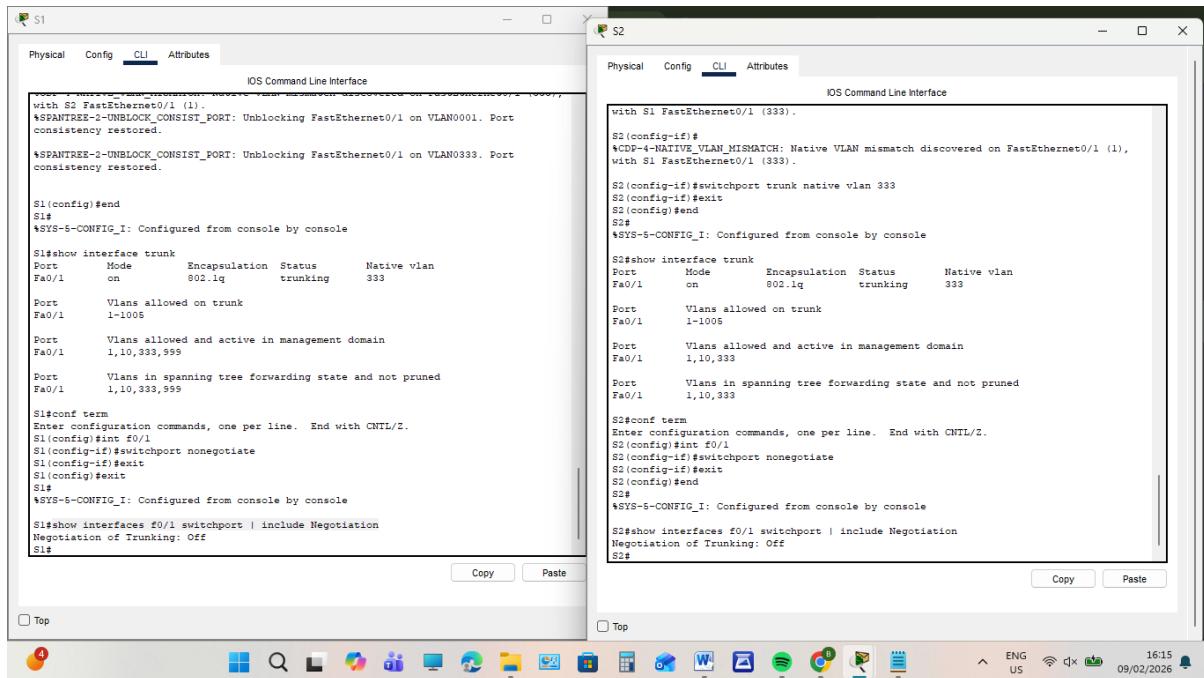
```

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#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int f0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#exit
S1(config)#
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
Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,333
S2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#int f0/1
S2(config-if)#switchport nonegotiate
S2(config-if)#exit
S2(config)#

```

4. Verify with the show interfaces command.

- The show interface command for both S1 & S2 is as shown below



The image shows two side-by-side windows of the Cisco IOS Command Line Interface (CLI) running on Windows. Both windows have tabs for Physical, Config, CLI, and Attributes, with CLI selected. The left window is titled 'S1' and the right is 'S2'. Both windows display the output of the 'show interface' command.

```

S1# show interface
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    1,10,333,998

S1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int f0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#exit
S1#
$SYS-5-CONFIG_I: Configured from console by console
S1#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S1#

```



```

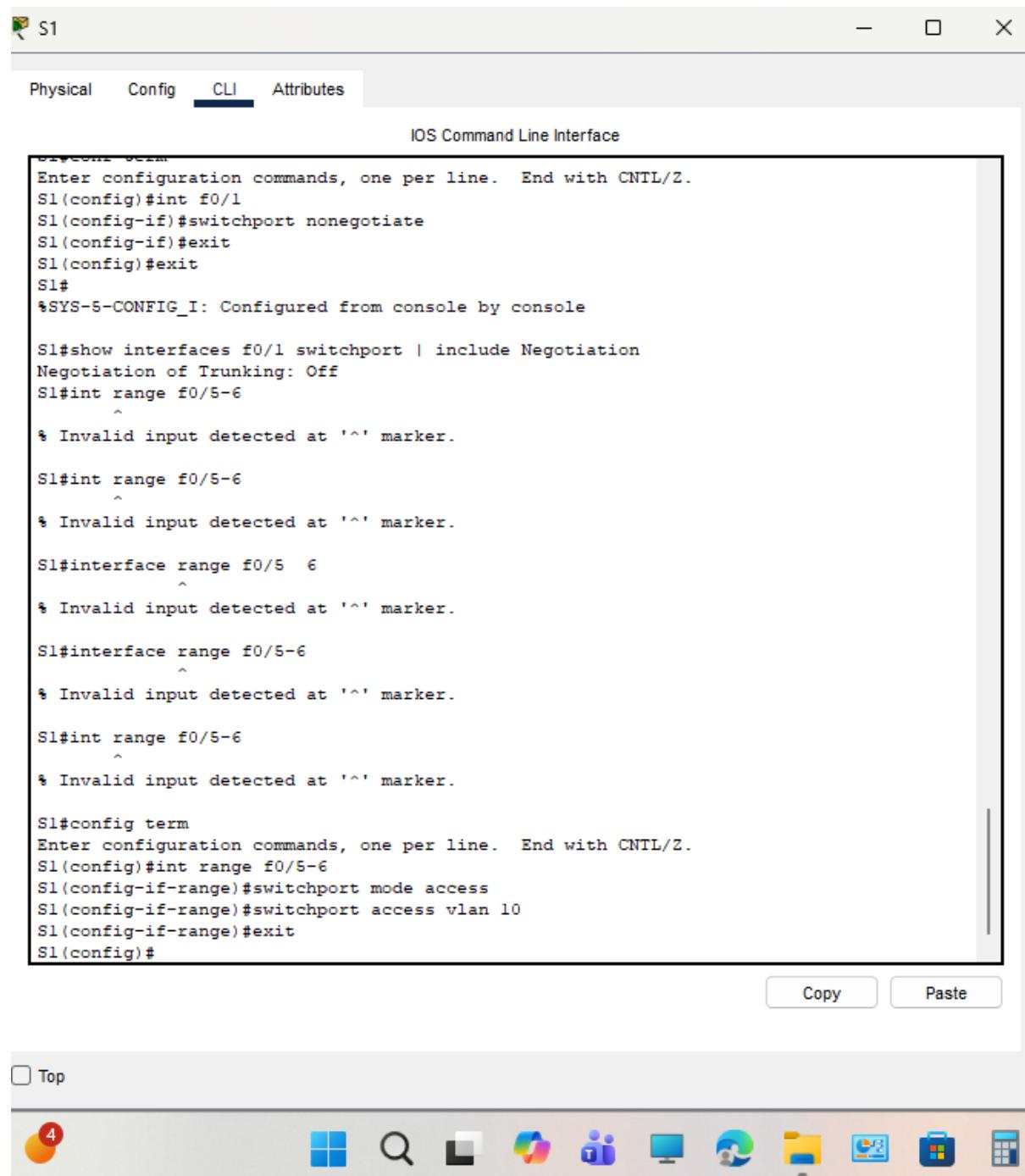
S2# show interface
Port      Mode       Encapsulation  Status      Native vlan
Fa0/1    on        802.1q        trunking     333
Port      Vlans allowed on trunk
Fa0/1    1-1005
Port      Vlans allowed and active in management domain
Fa0/1    1,10,333
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1,10,333

S2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#int f0/1
S2(config-if)#switchport nonegotiate
S2(config-if)#exit
S2(config)#end
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.



Physical Config **CLI** Attributes

IOS Command Line Interface

```
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int 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#int range f0/5-6
^
% Invalid input detected at '^' marker.

S1#int range f0/5-6
^
% Invalid input detected at '^' marker.

S1#interface range f0/5  6
^
% Invalid input detected at '^' marker.

S1#interface range f0/5-6
^
% Invalid input detected at '^' marker.

S1#int range f0/5-6
^
% Invalid input detected at '^' marker.

S1#config term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int range f0/5-6
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#exit
S1(config)#

Copy    Paste
```

Top



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

S2

Physical Config **CLI** Attributes

IOS Command Line Interface

```

S2(config-if)#switchport trunk native vlan 333
S2(config-if)#exit
S2(config)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

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

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

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

S2#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S2#
S2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#int range f0/18
S2(config-if-range)#switchport access vlan 10
S2(config-if-range)#exit
S2(config)#

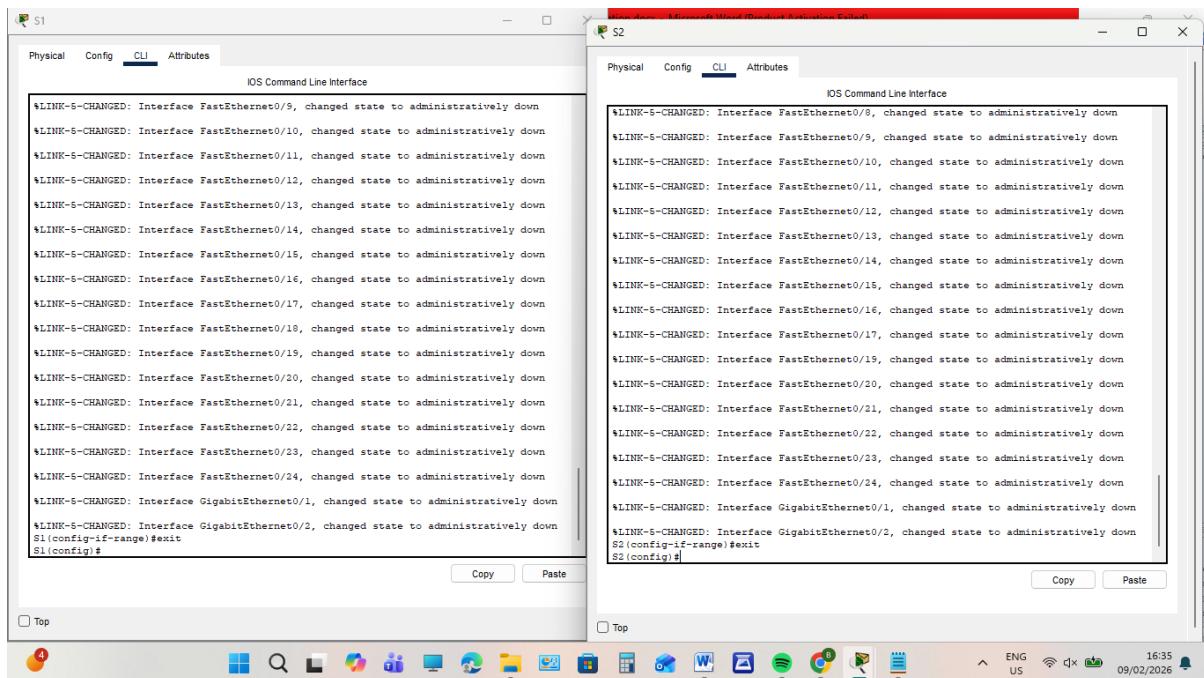
```

Top

File Explorer Word OneNote Paint Spotify Google Chrome Mail Task View ENG US 16:27 09/02/2026

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.



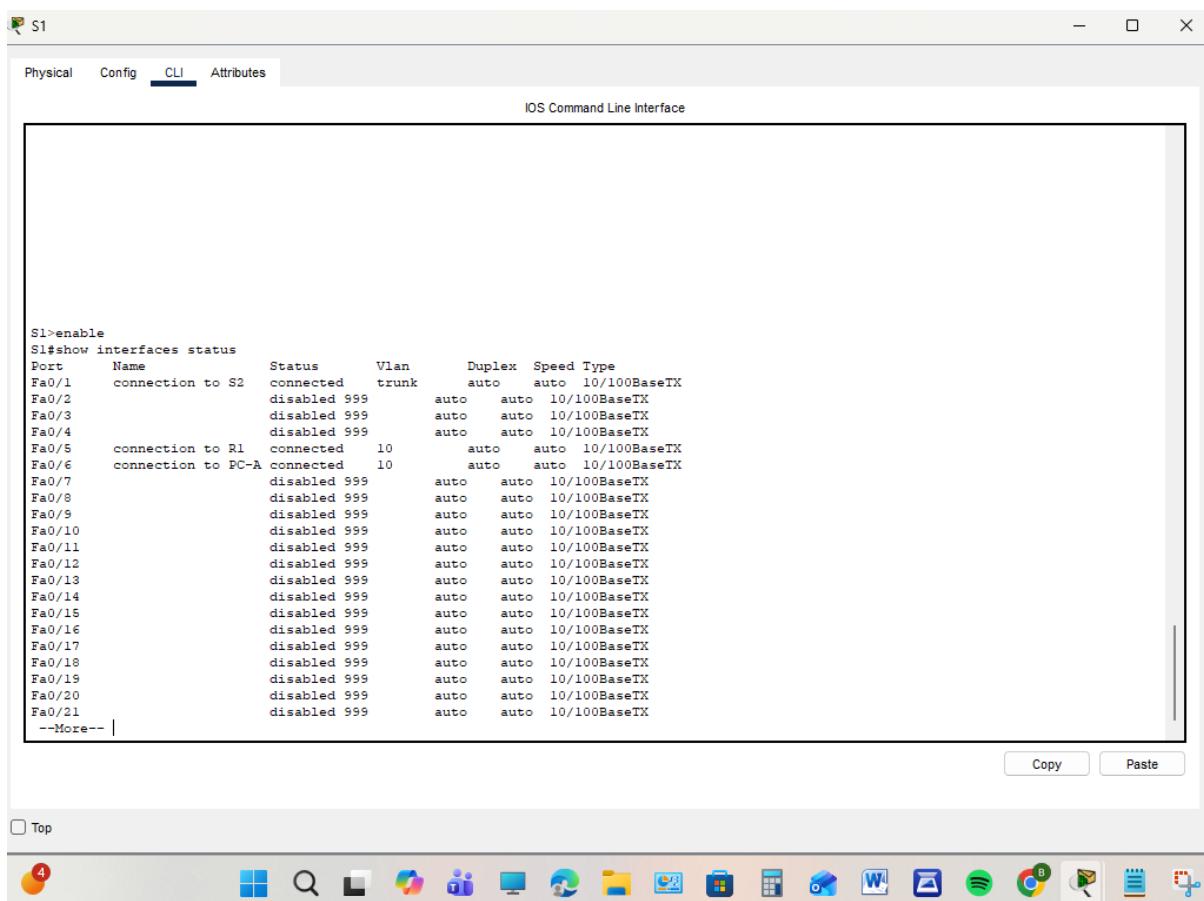
```

S1# configure terminal
S1(config)# interface range Fa0/9-Fa0/21
S1(config-if-range)# switchport access vlan 999
S1(config-if-range)# shutdown
S1(config-if-range)# exit
S1(config)#
S1# show interfaces status
S1>enable
S1>show interfaces status
Port      Name       Status     Vlan      Duplex   Speed Type
Fa0/1    connection 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    connection to R1  connected  10      auto     auto  10/100BaseTX
Fa0/6    connection 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
--More-- |
S2# configure terminal
S2(config)# interface range Fa0/9-Fa0/21
S2(config-if-range)# switchport access vlan 999
S2(config-if-range)# shutdown
S2(config-if-range)# exit
S2(config)#
S2# show interfaces status
S2>enable
S2>show interfaces status
Port      Name       Status     Vlan      Duplex   Speed Type
Fa0/1    connection 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    connection to R1  connected  10      auto     auto  10/100BaseTX
Fa0/6    connection 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
--More-- |

```

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

S1# show interfaces status

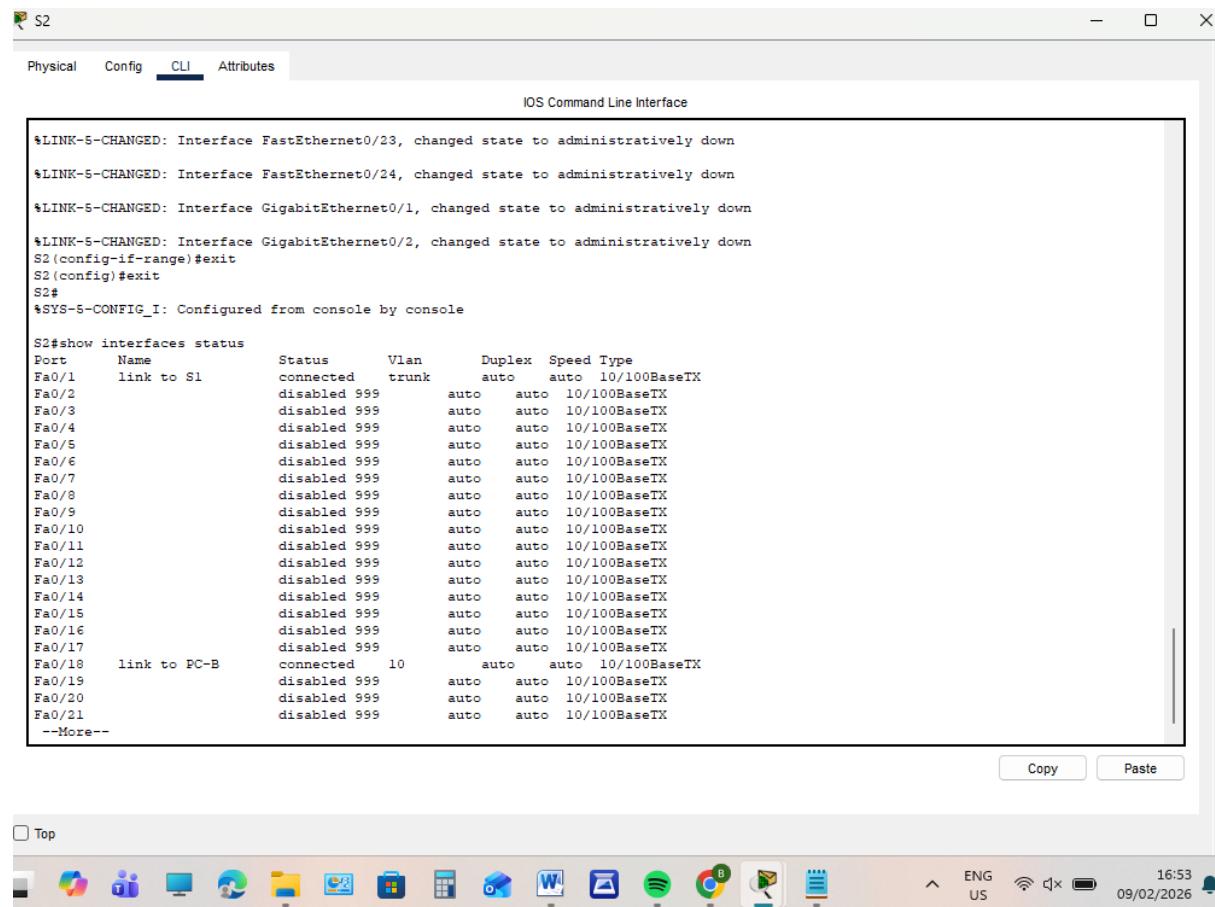


```

S1# show interfaces status
S1>enable
S1>show interfaces status
Port      Name       Status     Vlan      Duplex   Speed Type
Fa0/1    connection 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    connection to R1  connected  10      auto     auto  10/100BaseTX
Fa0/6    connection 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
--More-- |

```

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     auto  10/100BaseTX
Fa0/3    disabled   999      auto     auto     auto  10/100BaseTX
Fa0/4    disabled   999      auto     auto     auto  10/100BaseTX
Fa0/5    disabled   999      auto     auto     auto  10/100BaseTX
Fa0/6    disabled   999      auto     auto     auto  10/100BaseTX
Fa0/7    disabled   999      auto     auto     auto  10/100BaseTX
Fa0/8    disabled   999      auto     auto     auto  10/100BaseTX
Fa0/9    disabled   999      auto     auto     auto  10/100BaseTX
Fa0/10   disabled   999      auto     auto     auto  10/100BaseTX
Fa0/11   disabled   999      auto     auto     auto  10/100BaseTX
Fa0/12   disabled   999      auto     auto     auto  10/100BaseTX
Fa0/13   disabled   999      auto     auto     auto  10/100BaseTX
Fa0/14   disabled   999      auto     auto     auto  10/100BaseTX
Fa0/15   disabled   999      auto     auto     auto  10/100BaseTX
Fa0/16   disabled   999      auto     auto     auto  10/100BaseTX
Fa0/17   disabled   999      auto     auto     auto  10/100BaseTX
Fa0/18   link to PC-B  connected  10      auto     auto  10/100BaseTX
Fa0/19   disabled   999      auto     auto     auto  10/100BaseTX
Fa0/20   disabled   999      auto     auto     auto  10/100BaseTX
Fa0/21   disabled   999      auto     auto     auto  10/100BaseTX
--More--

```

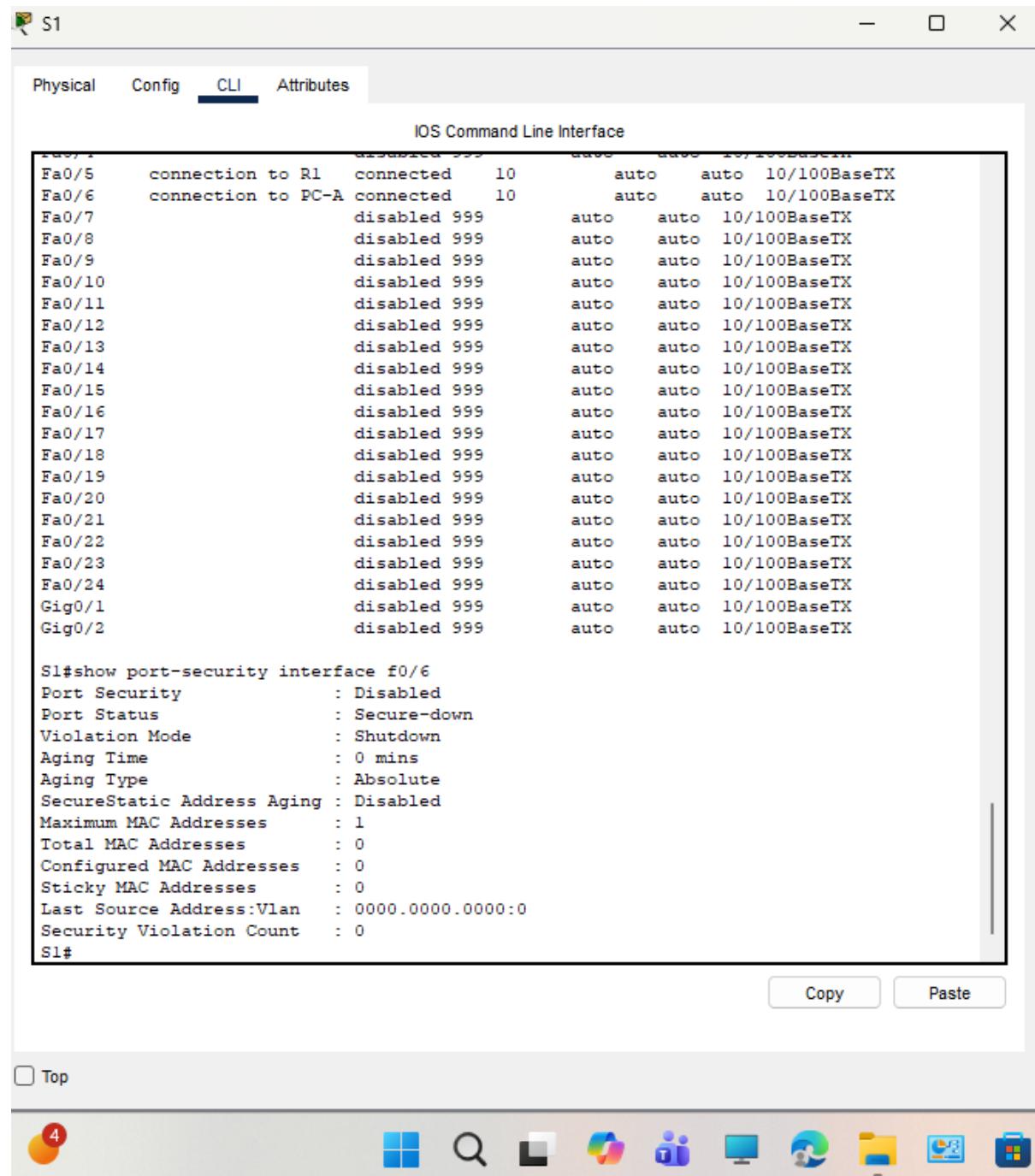
Copy Paste



Step 4: Document and implement port security features.

1. On S1, issue the show port-security interface f0/6 command to display the default port security

Settings for interface F0/6



```

IOS Command Line Interface

Fa0/1      disabled    auto    auto   10/100BaseTX
Fa0/5      connection to R1 connected 10      auto    auto   10/100BaseTX
Fa0/6      connection 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#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#

```

Top

Copy Paste

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

S1

Physical Config **CLI** Attributes

IOS Command Line Interface

```

Fa0/10      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#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#config term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int 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
^
% Invalid input detected at '^' marker.

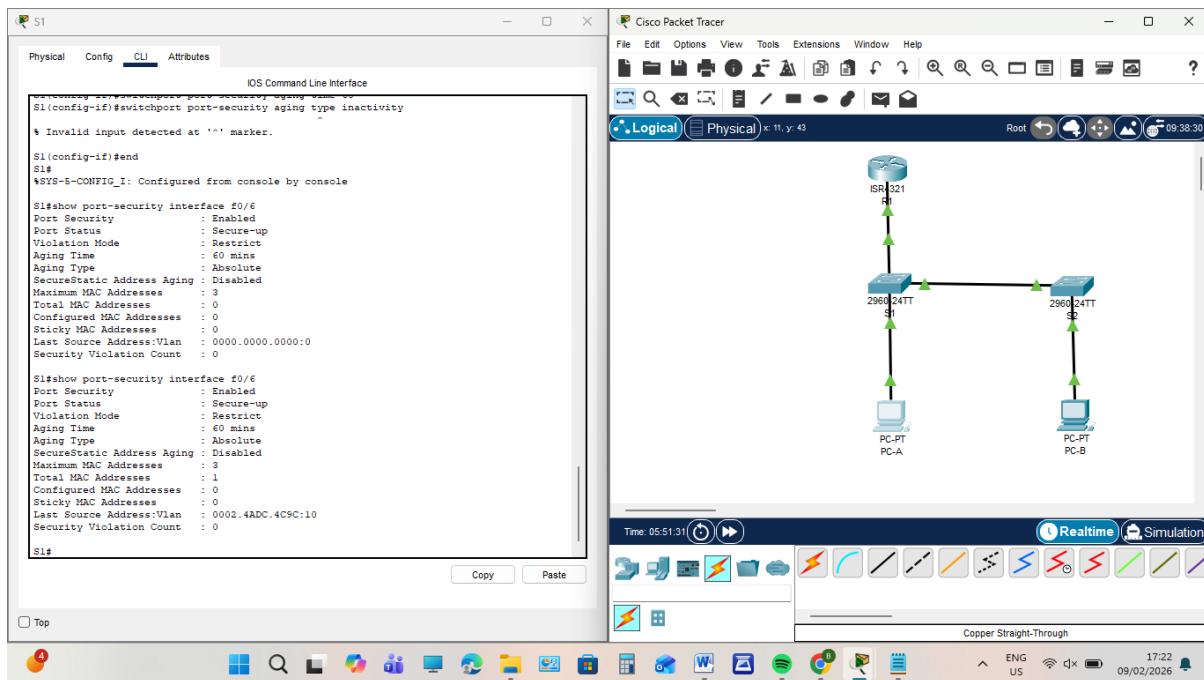
S1(config-if)#end
S1#
*SYS-5-CONFIG_I: Configured from console by console
S1#

```

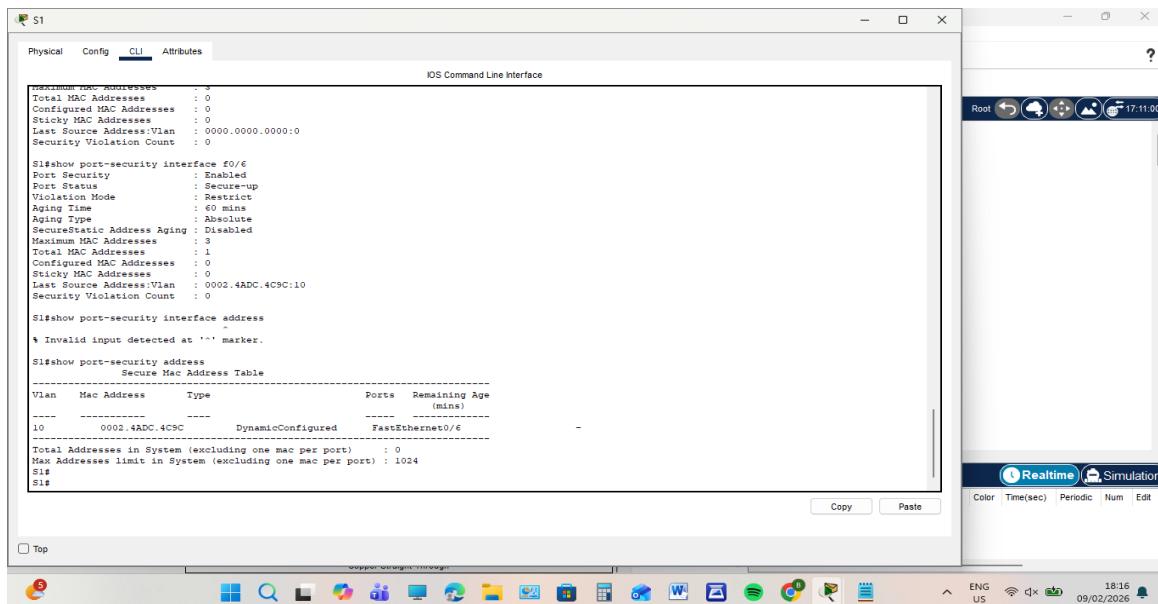
Top

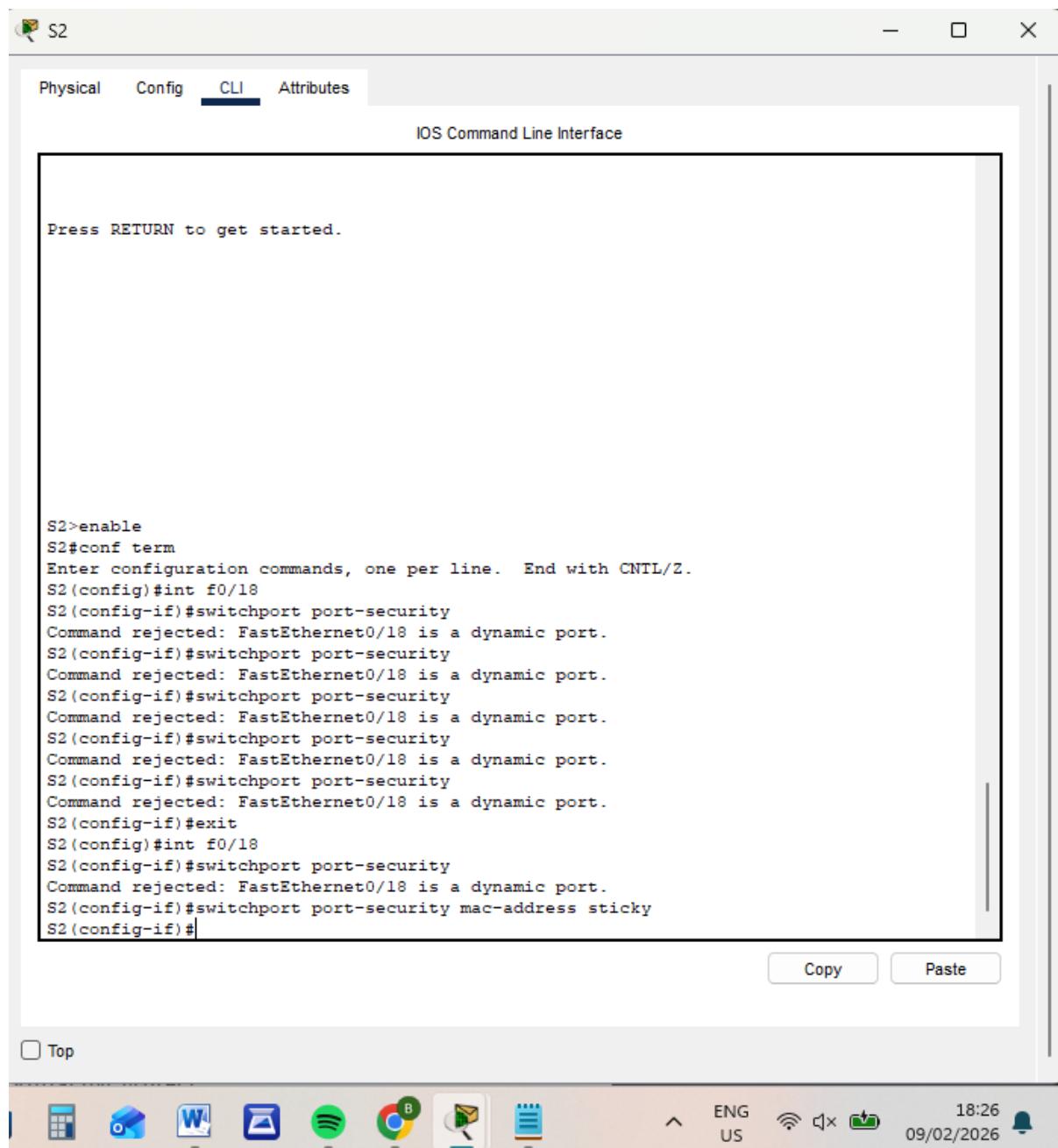
3. Verify port security on S1 F0/6.



S1# 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.



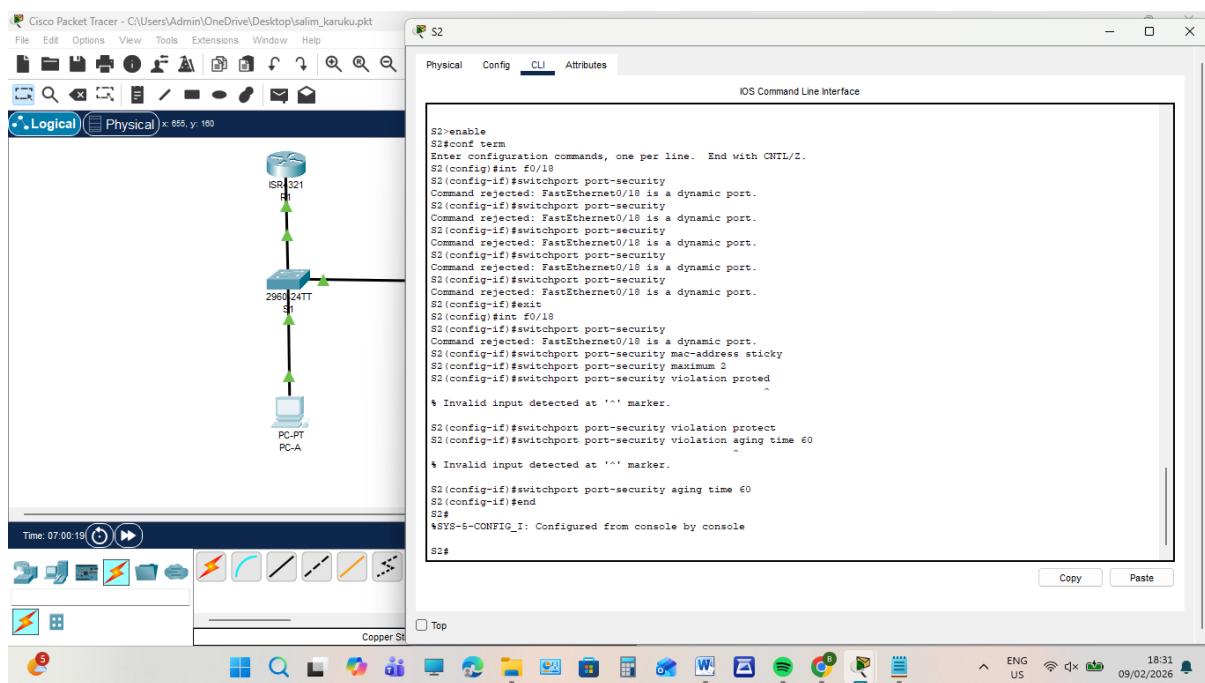
The screenshot shows a Cisco IOS Command Line Interface window titled "S2". The tab bar at the top includes "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs is a banner reading "IOS Command Line Interface". A large text area displays the following command session:

```
Press RETURN to get started.

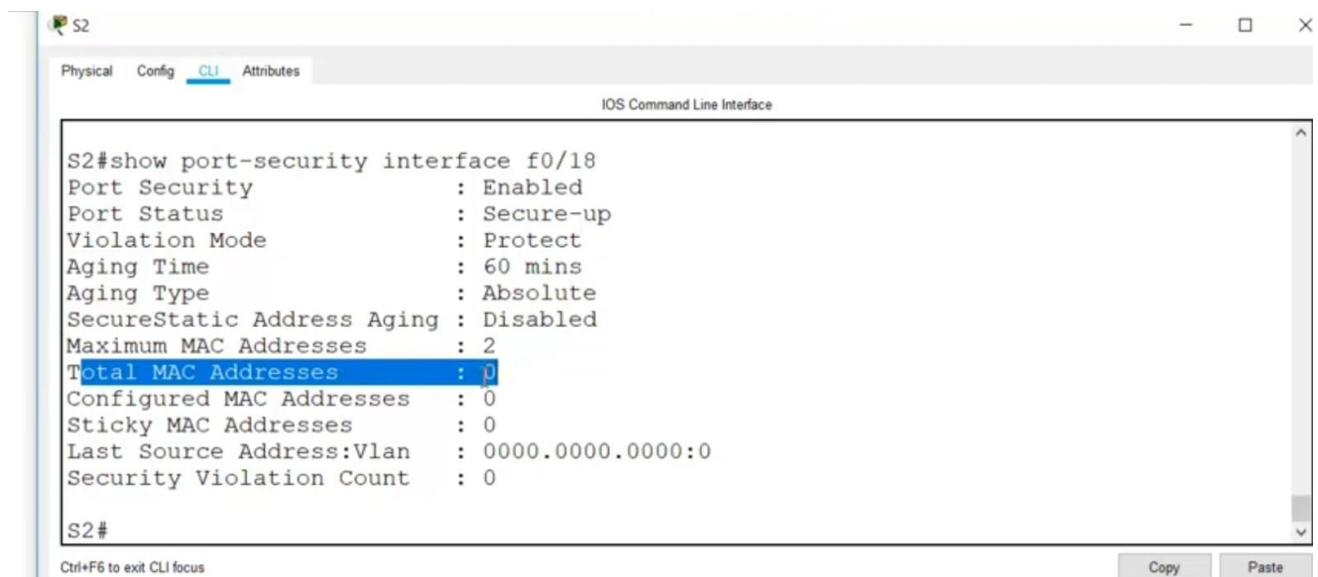
S2>enable
S2#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#int f0/18
S2(config-if)#switchport port-security
Command rejected: FastEthernet0/18 is a dynamic port.
S2(config-if)#switchport port-security
Command rejected: FastEthernet0/18 is a dynamic port.
S2(config-if)#switchport port-security
Command rejected: FastEthernet0/18 is a dynamic port.
S2(config-if)#switchport port-security
Command rejected: FastEthernet0/18 is a dynamic port.
S2(config-if)#switchport port-security
Command rejected: FastEthernet0/18 is a dynamic port.
S2(config-if)#exit
S2(config)#int f0/18
S2(config-if)#switchport port-security
Command rejected: FastEthernet0/18 is a dynamic port.
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#[
```

At the bottom of the window are "Copy" and "Paste" buttons. The taskbar at the very bottom includes icons for various applications like File Explorer, Word, Excel, and Google Chrome, along with system status indicators for battery, signal, and date/time (18:26, 09/02/2026).

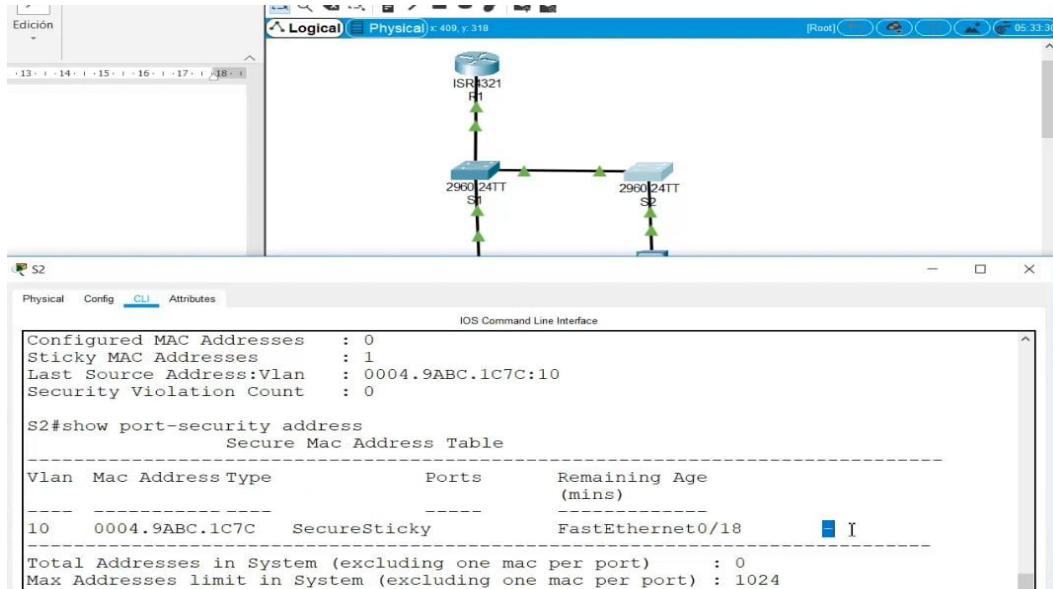
5. Configure the following port security settings on S2 F/18:



6. Verify port security on S2 F0/18

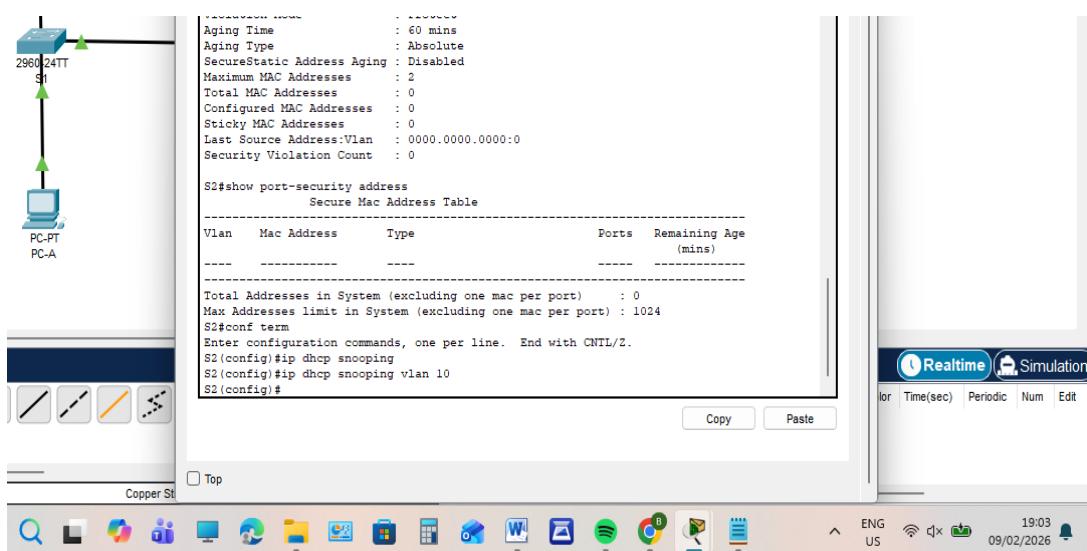


S2# show port-security address

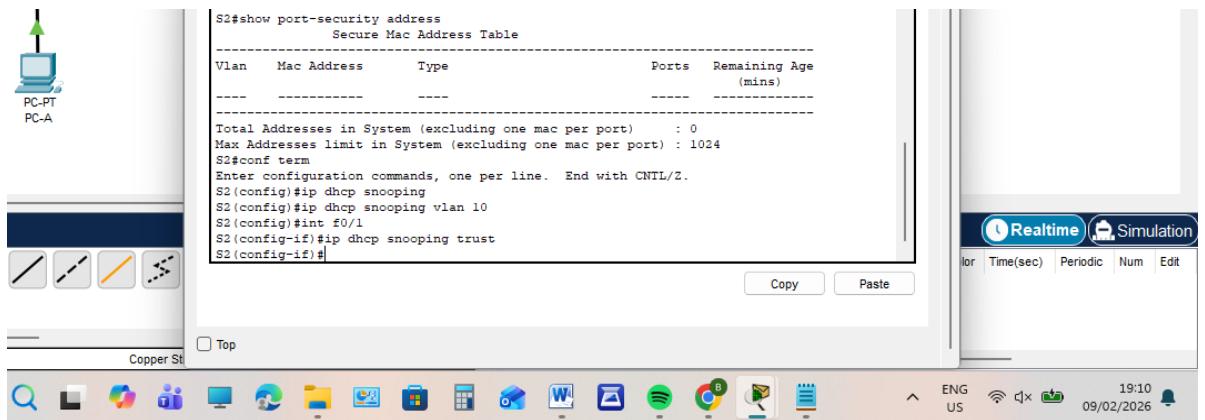


Step 5: Implement DHCP snooping security.

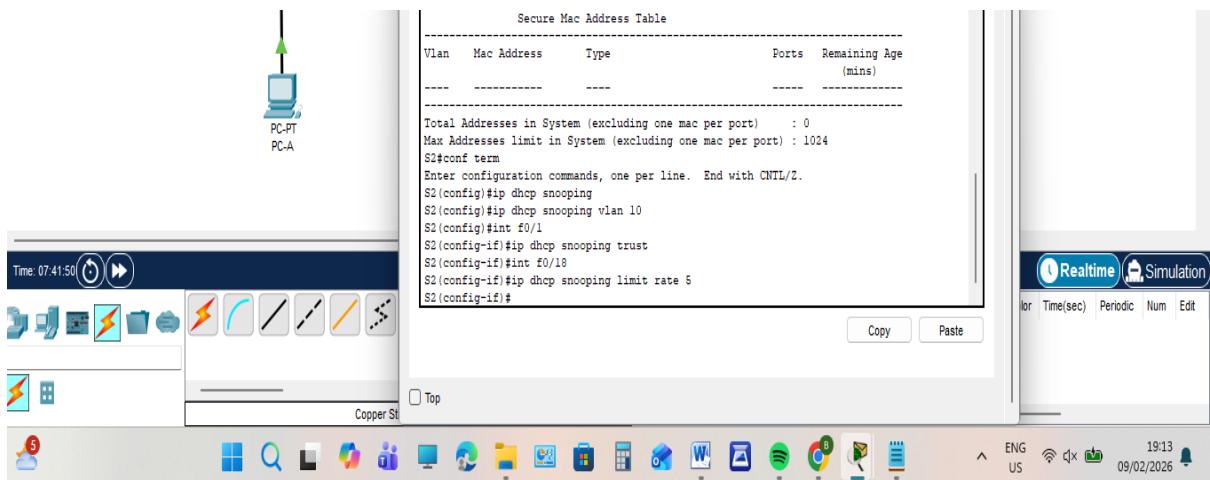
1. On S2, enable DHCP snooping and configure DHCP snooping on VLAN 10.



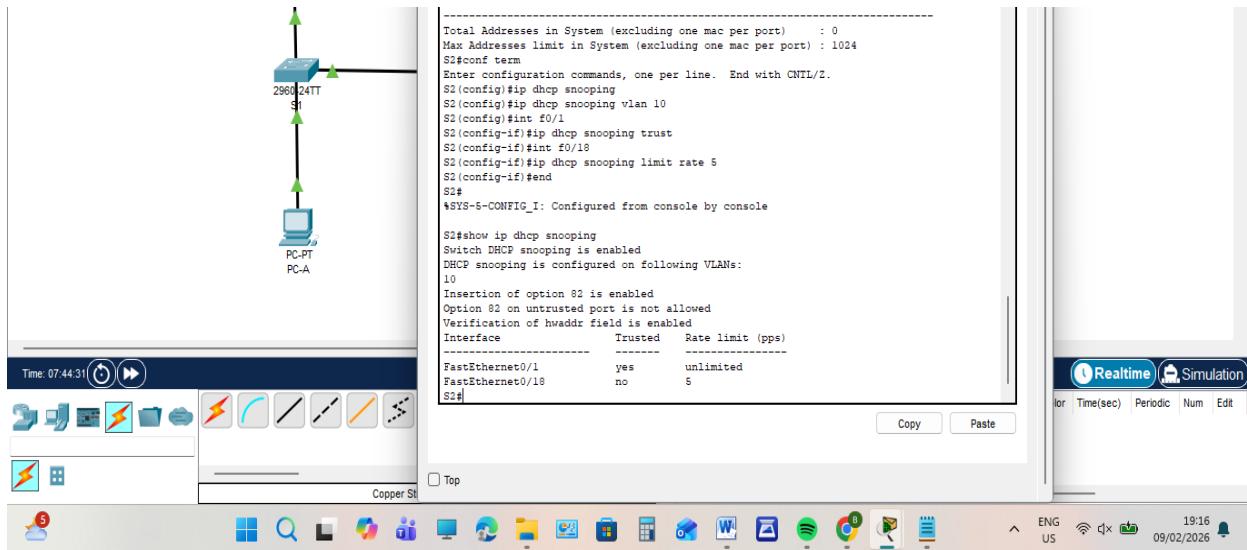
2. Configure the trunk port on S2 as a trusted port.



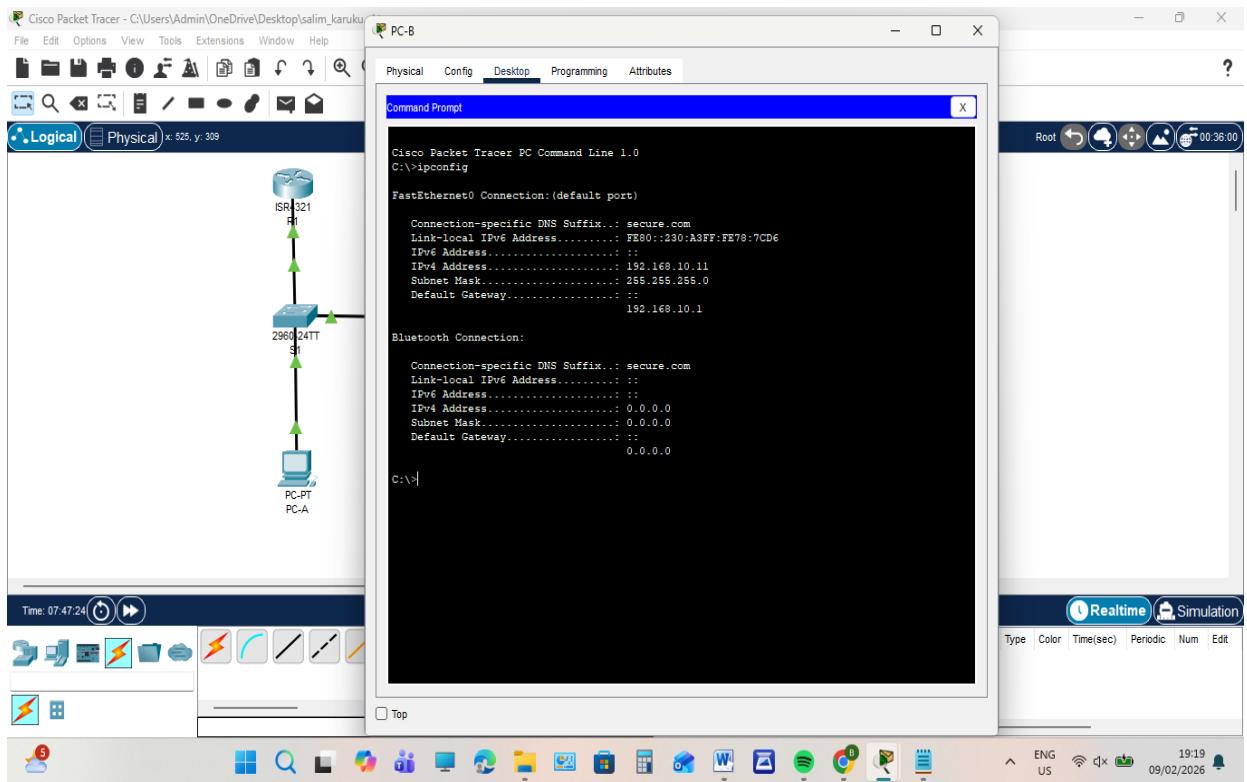
3. Limit the untrusted port, F18 on S2, to five DHCP packets per second.



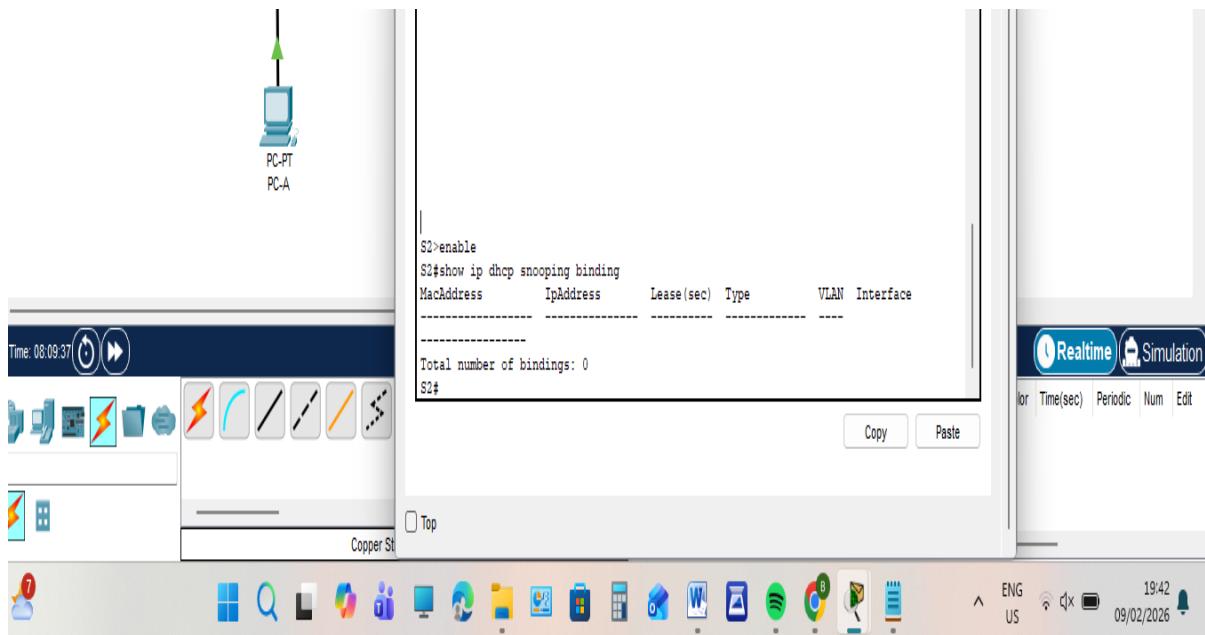
4. Verify DHCP Snooping on S2.



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



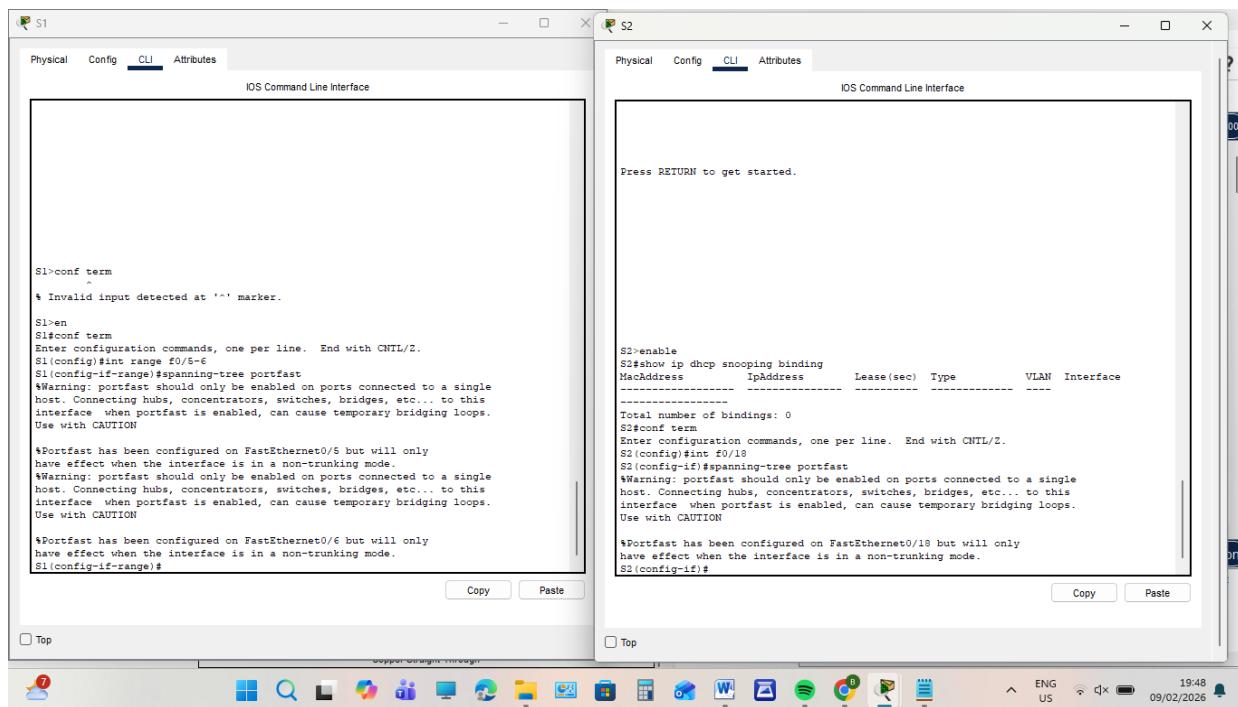
6. Verify the DHCP snooping binding using the show ip dhcp snooping binding command.



Step 6: Implement PortFast and BPDU guard.

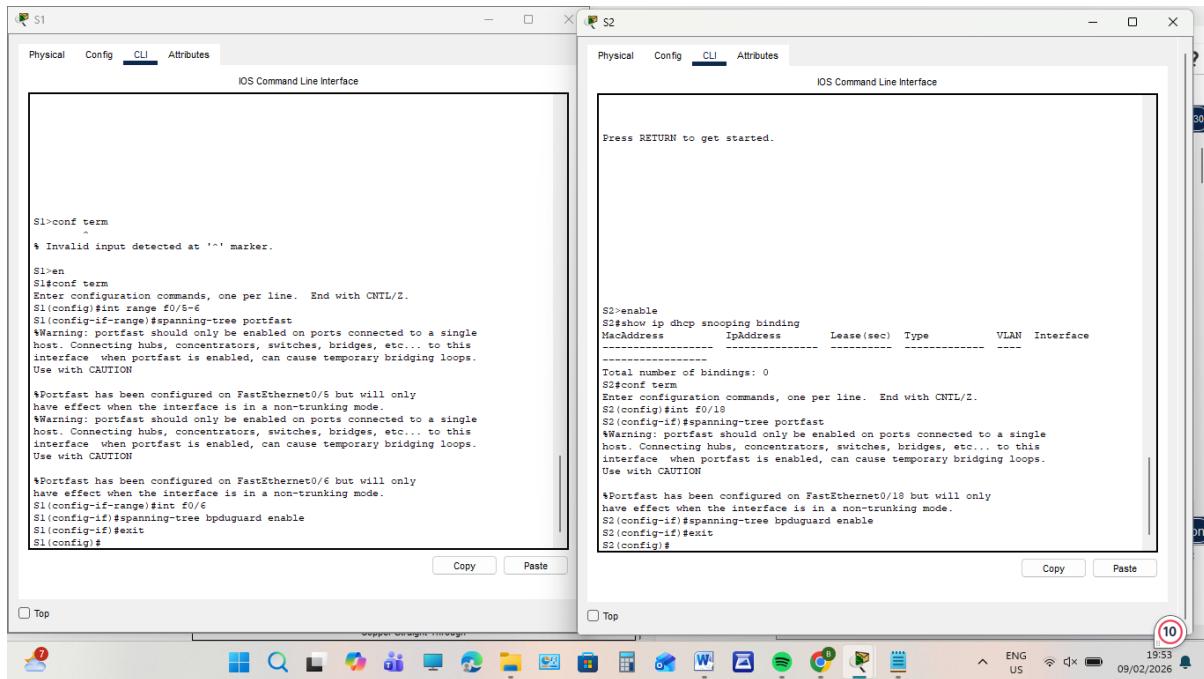
1. Configure PortFast on all the access ports that are in use on both switches.

- Here are for both S1 & S2



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

- The following are the BPDU guard for both S1 & S2



```

S1>conf term
! Invalid input detected at `^` marker.

S1>en
S1>conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface range F0/5
S1(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 FastEthernet0/5 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)#int F0/6
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#exit
S1(config)#

```



```

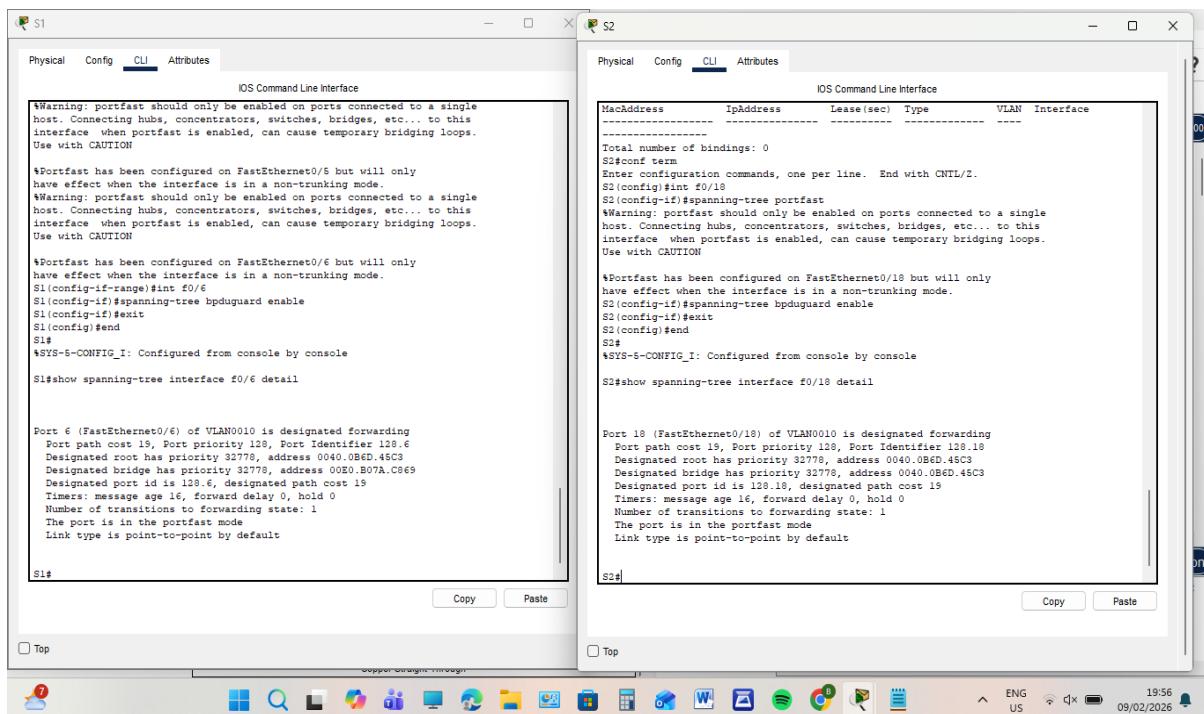
S2>enable
S2>show ip dhcp snooping binding
MacAddress         IpAddress          Lease(sec) Type          VLAN   Interface
-----  -----
Total number of bindings: 0
S2>conf term
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#int F0/18
S2(config-if)#spanning-tree portfast
Warning: 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)#spanning-tree bpduguard enable
S2(config-if)#exit
S2(config)#

```

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

- BPDU guard and PortFast for both S1 & S2 below



```

S1>show spanning-tree interface f0/6 detail

Port 6 (FastEthernet0/6) of VLAN0010 is designated forwarding
  Port path cost is 19, Port priority 128, Port Identifier 128.6
  Designated root has priority 32778, address 0040.0BED.46C3
  Designated bridge has priority 32778, address 00E0.B07A.C065
  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
  Link type is point-to-point by default

S1#

```



```

S2>show spanning-tree interface f0/18 detail

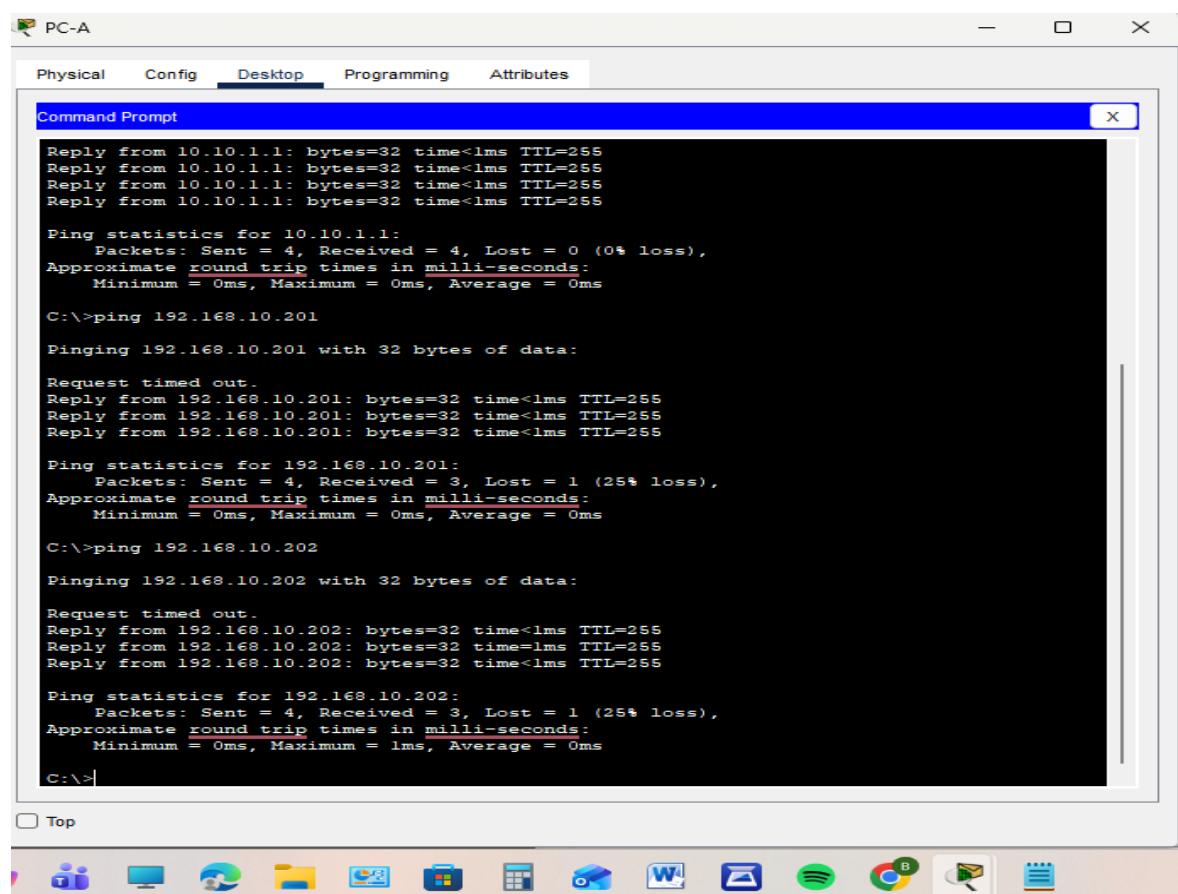
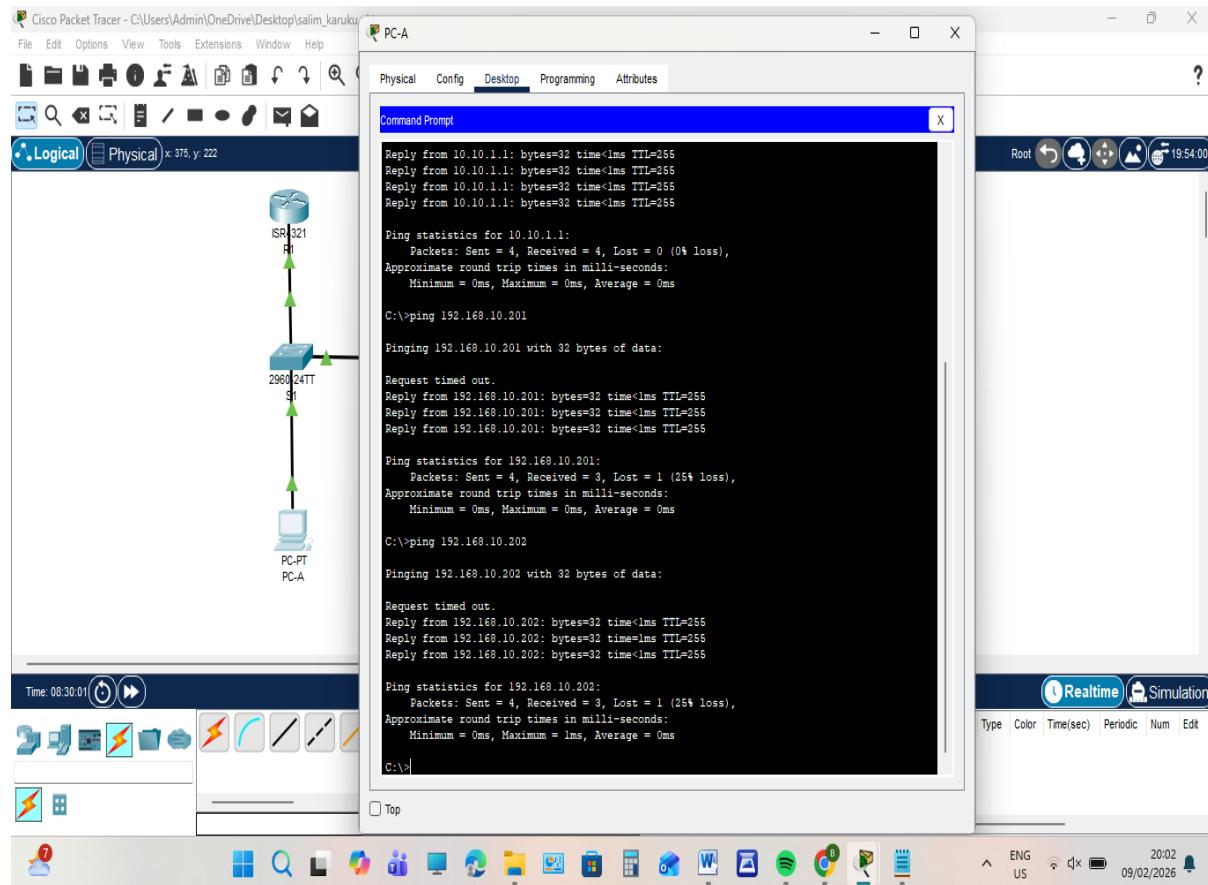
Port 18 (FastEthernet0/18) of VLAN0010 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.18
  Designated root has priority 32778, address 0040.0BED.46C3
  Designated bridge has priority 32778, address 00E0.B07A.C065
  Designated port id is 128.18, designated path cost 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-point by default
  Link type is point-to-point by default

S2#

```

Step 7: Verify end-to-end connectivity.

I verify the connectivity by pinging the IP addresses and the ping was successfully as shown below



Conclusion

This assignment successfully demonstrated the configuration of VLANs and secure switch settings. By implementing VLANs, the network was logically segmented which improved performance and enhanced security. The application of basic switch security features helped prevent unauthorized access to the network. Overall the assignment provided practical experience and a better understanding of VLAN implementation and switch security in modern network.