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 truck 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

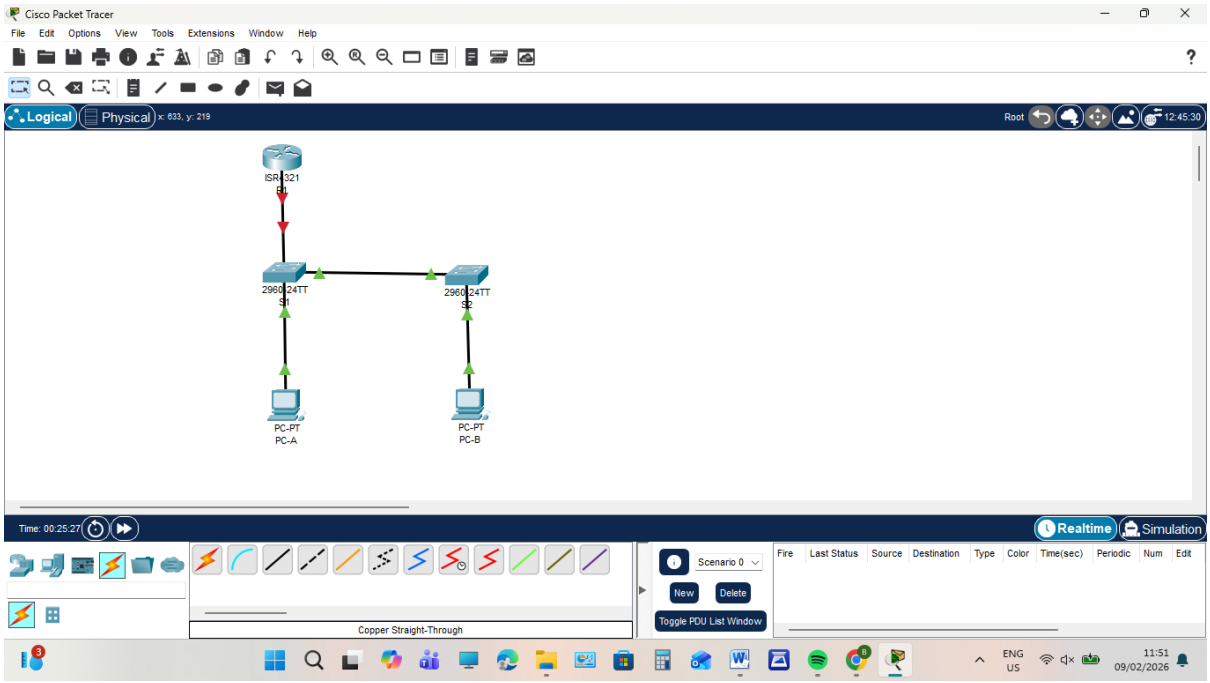
Topology

Part 1: Configure the Network Devices.

Step 1: Cable the network.

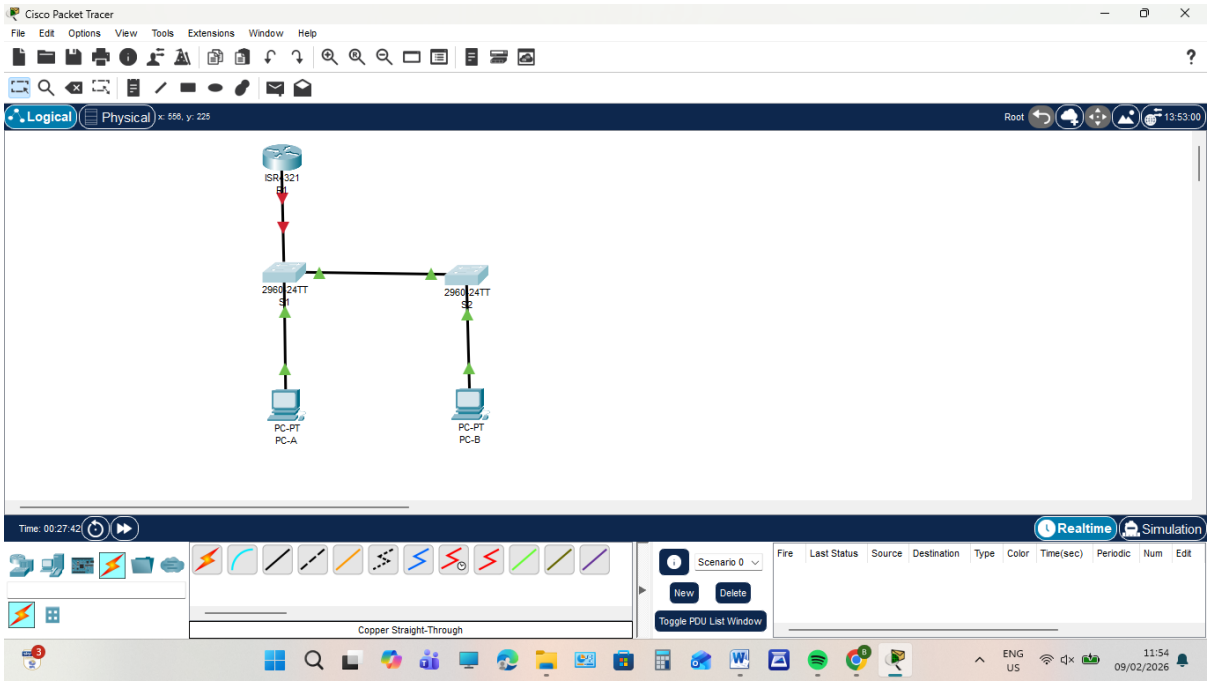
1. Cable the network as shown in the topology.

Here I cable the network as shown bellow



2. Initialize the devices.

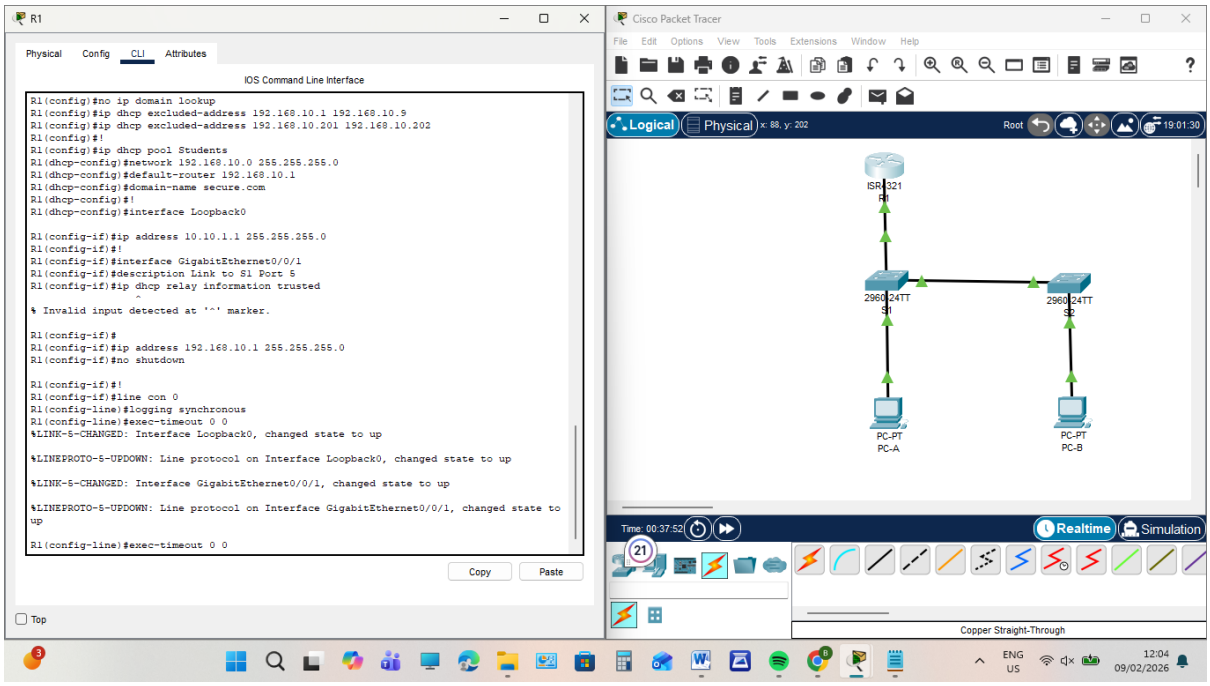
Then I initialize the router and the switches



Step 2: Configure R1.

1. Load the following configuration script on R1.

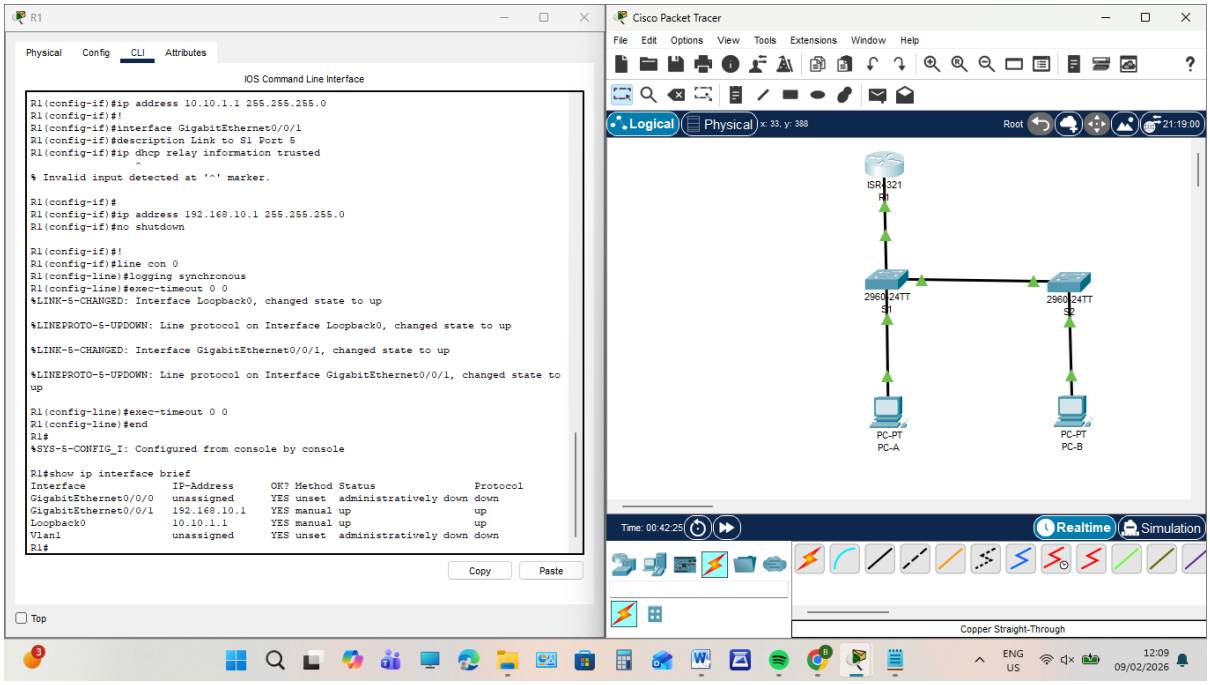
Here I load so that I can conf R1 as shown below



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

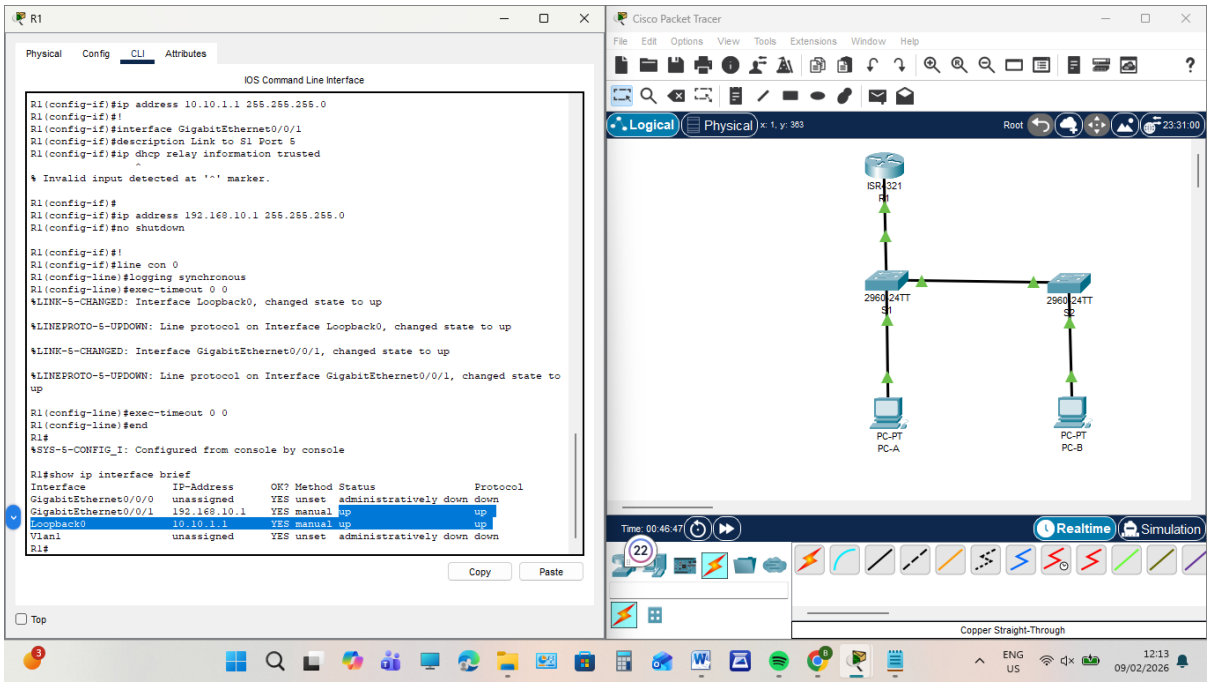
R1# show ip interface brief

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).

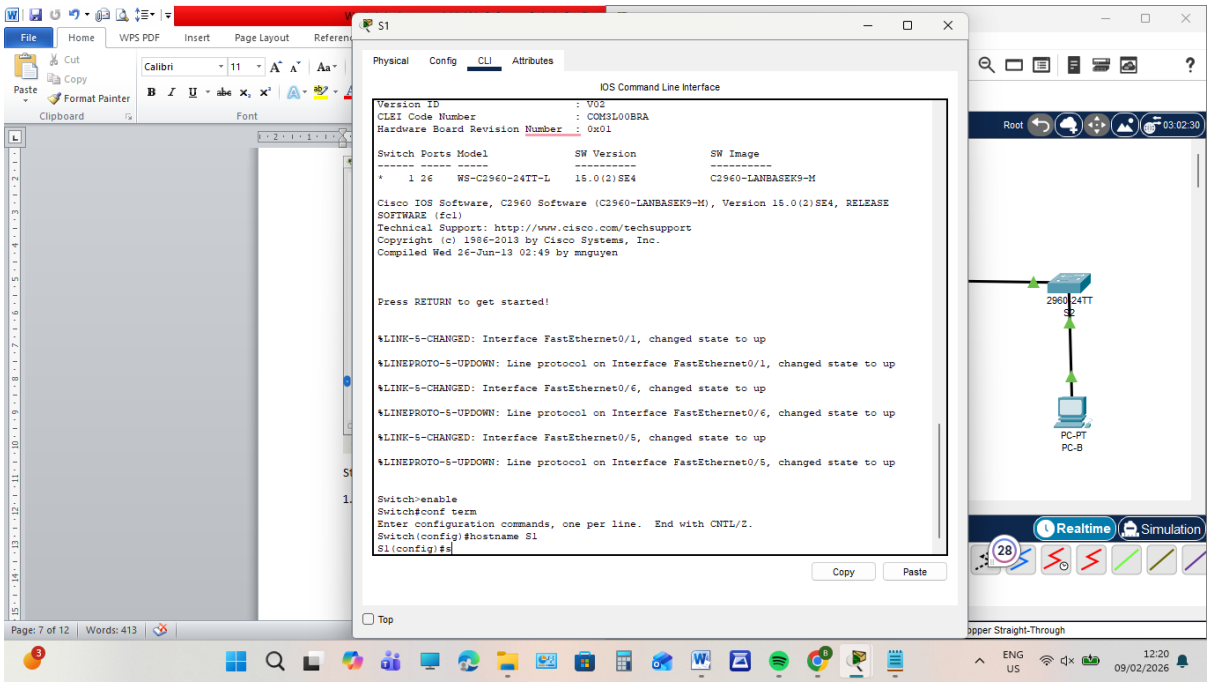
The IP addresses interfaces were verify and both were in an up/up state



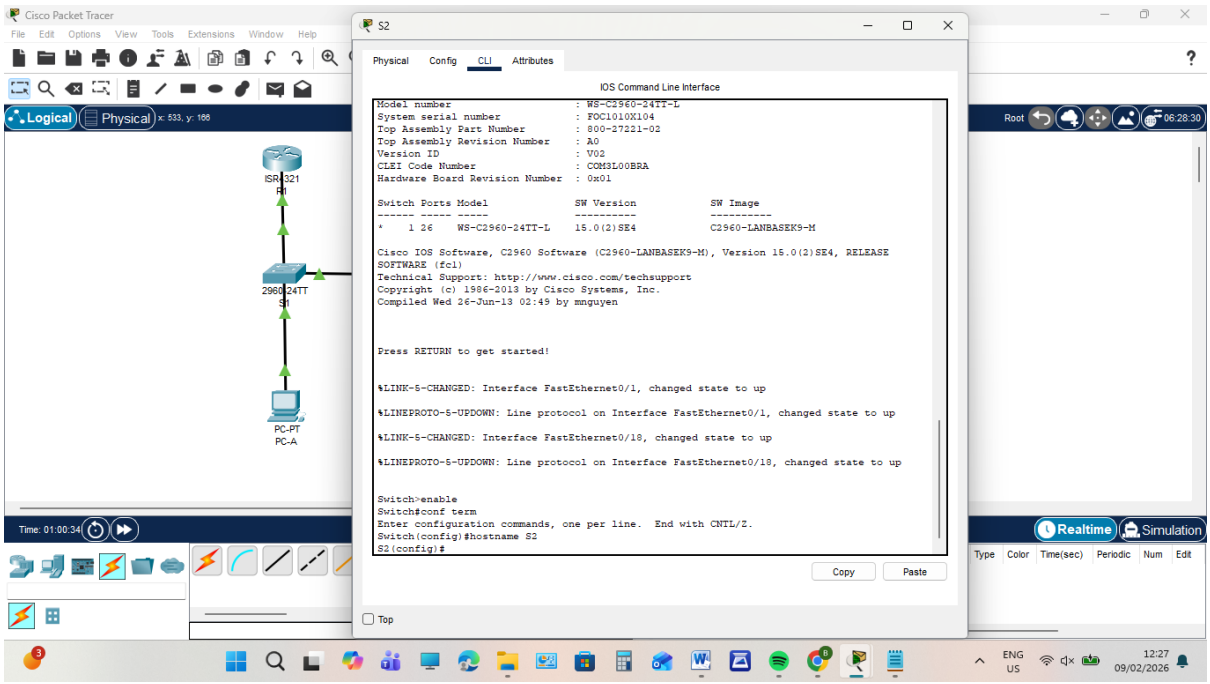
Step 3: Configure and verify basic switch settings.

1. Configure the hostname for switches S1 and S2.

Here is the hostname for S1

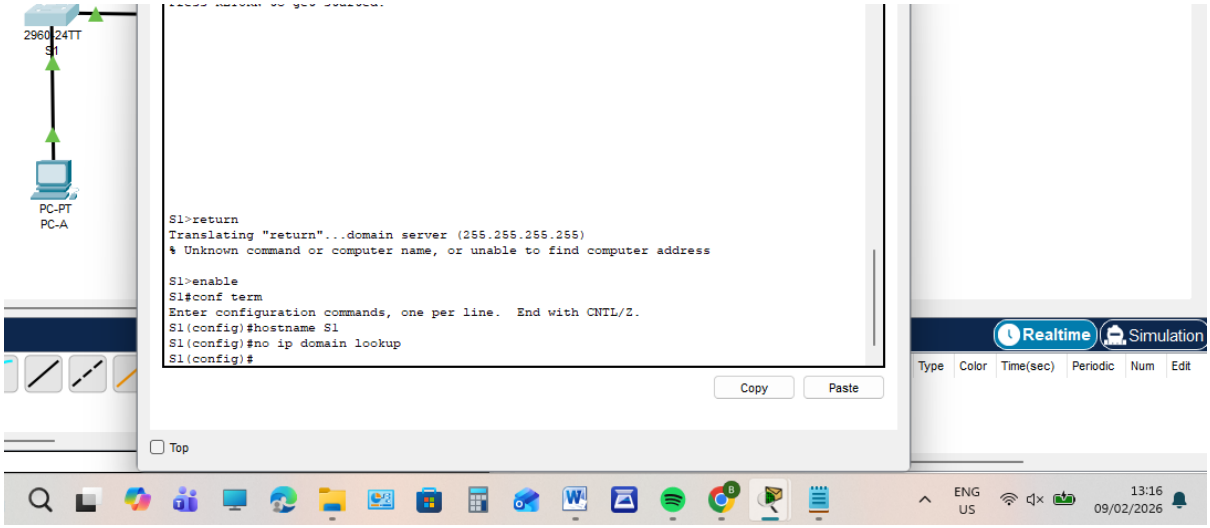


Here is the hostname for S2

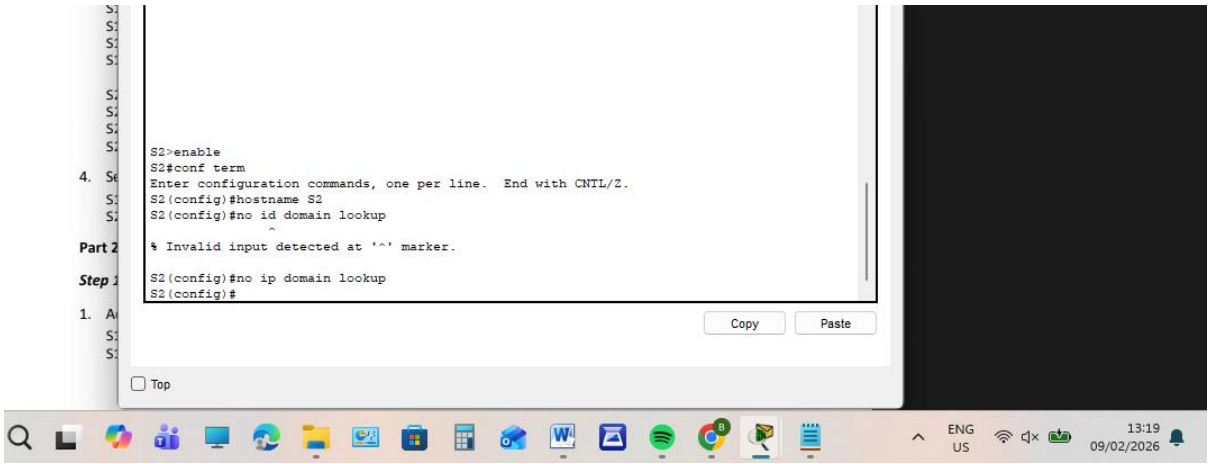


2. Prevent unwanted DNS lookups on both switches.

Here for S1

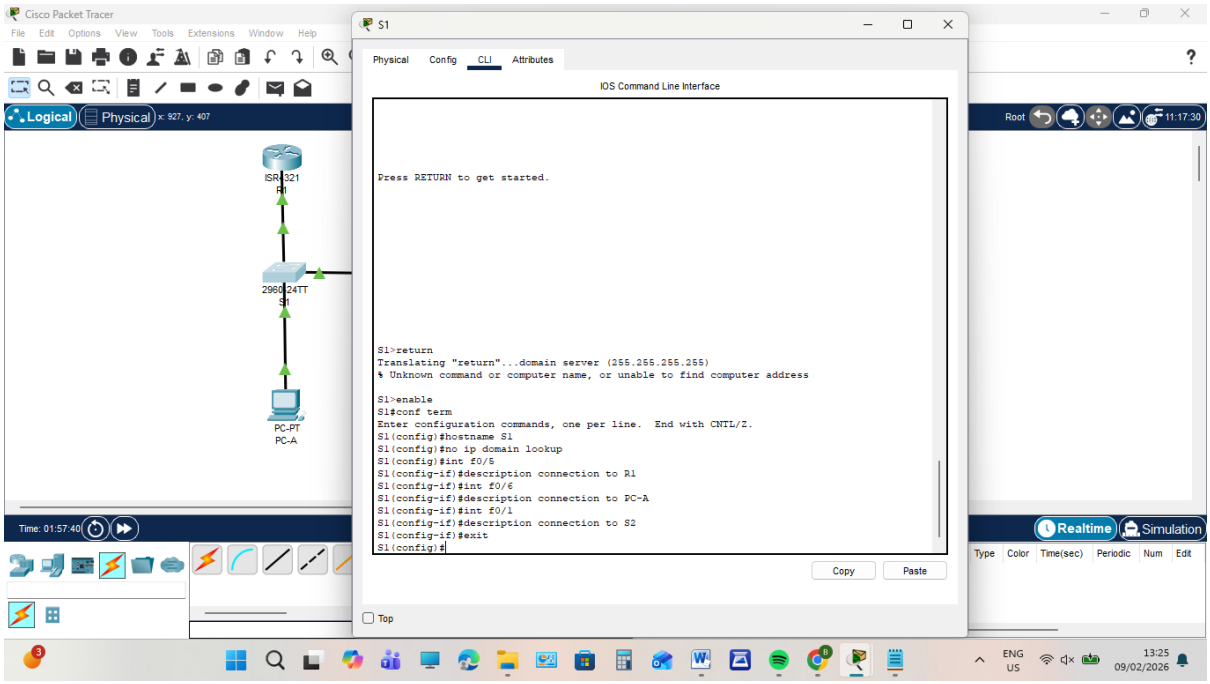


And for S2

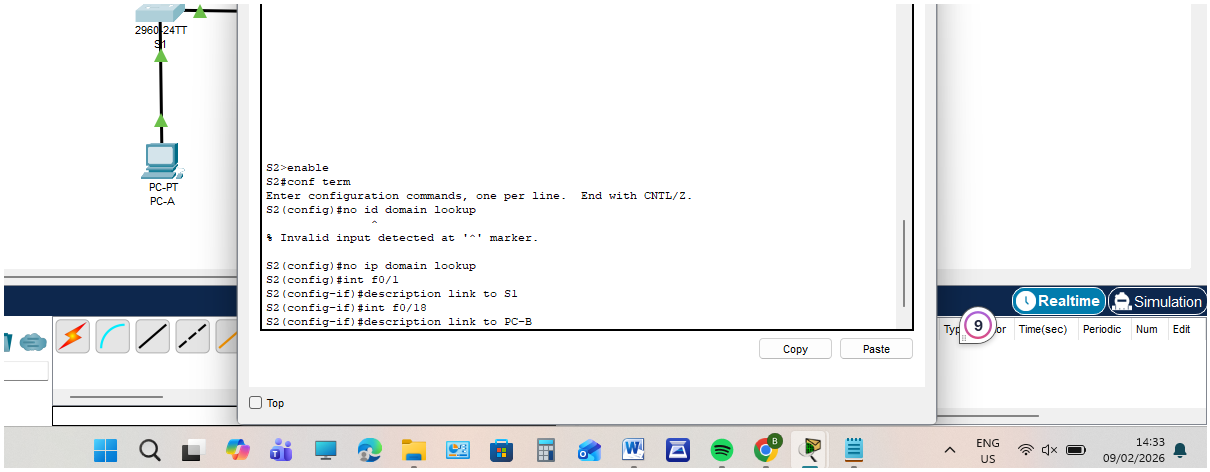


3. Configure interface descriptions for the ports that are in use in S1 and S2.

Interface for S1

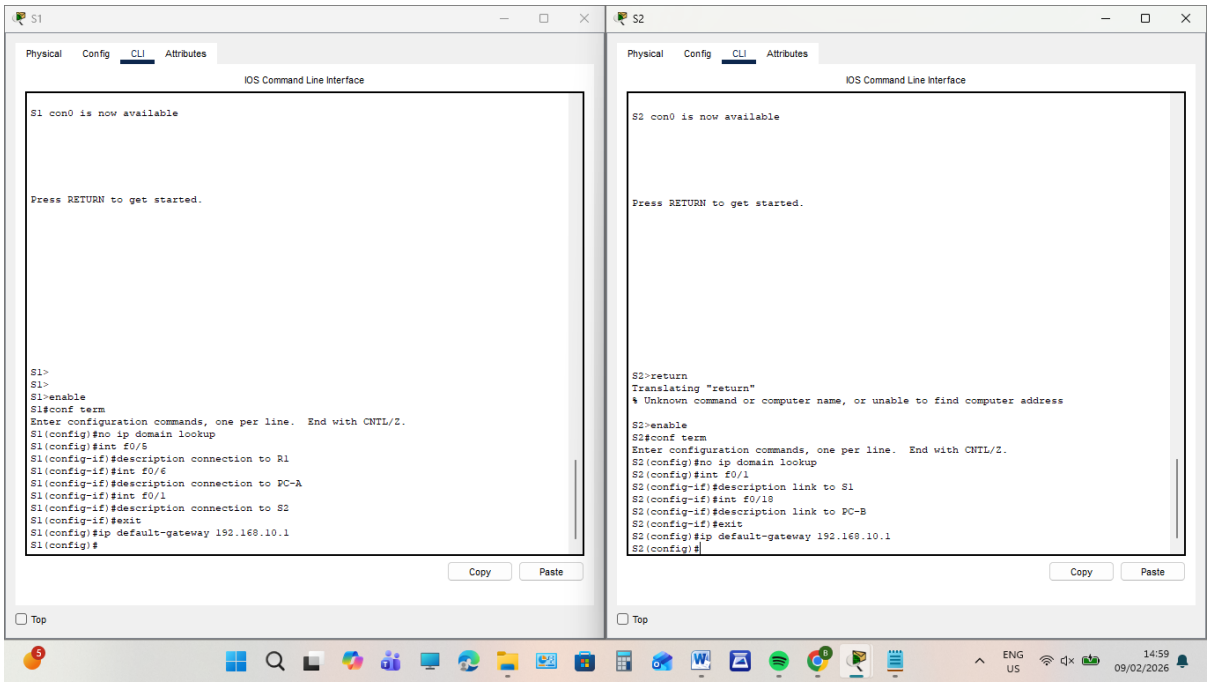


Interface for S2



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

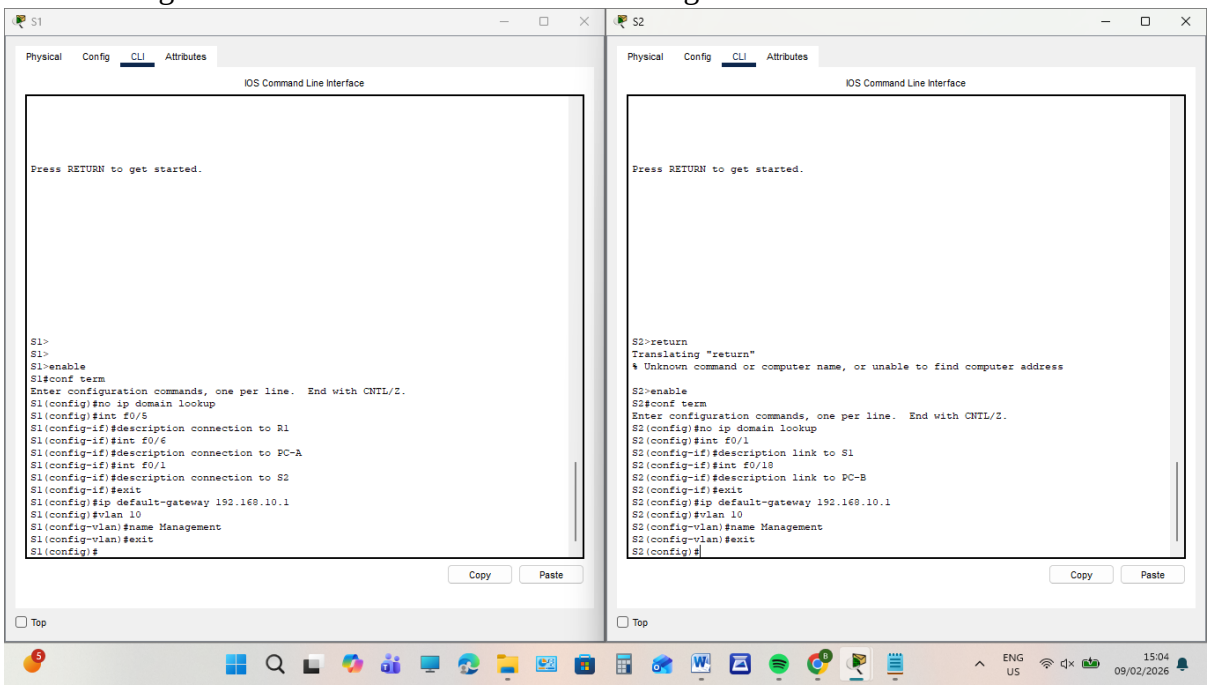


1. Part 2: Configure VLANs on Switches.

Step 1: Configure VLAN 10.

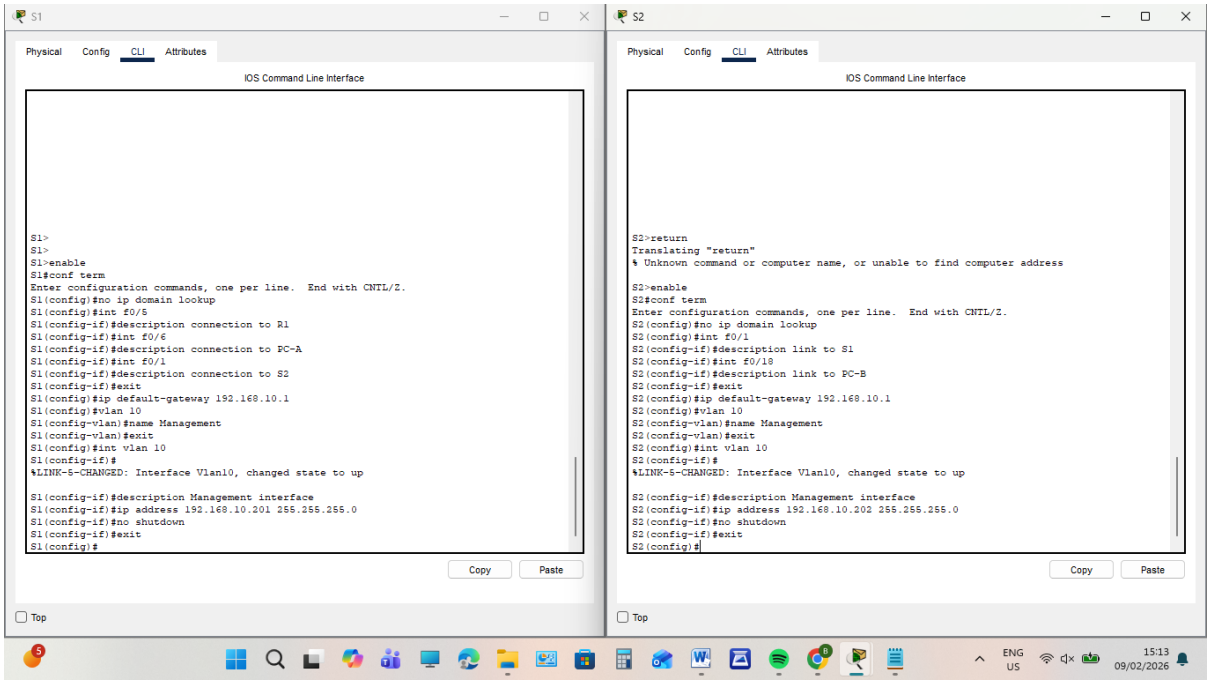
1. Add VLAN 10 to S1 and S2 and name the VLAN Management.

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



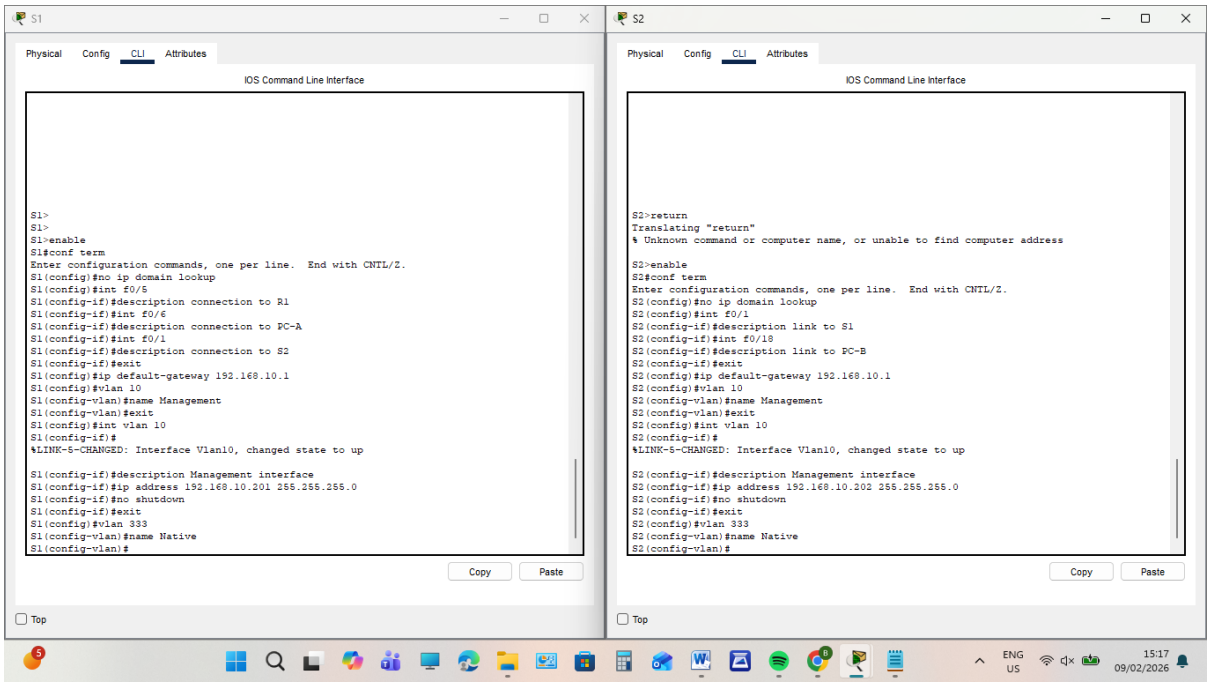
Step 2: Configure the SVI for VLAN 10.

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



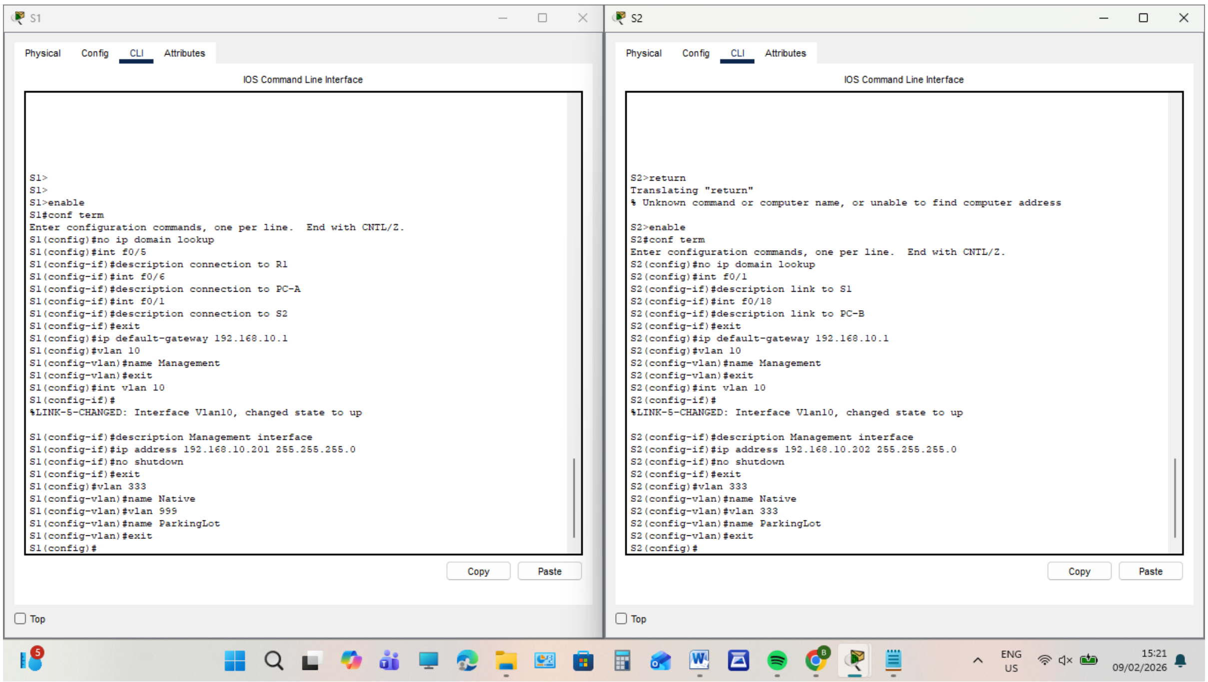
Step 3: Configure VLAN 333 with the name Native on S1 and S2.

Here I configure the VLAN for both S1 & S2



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

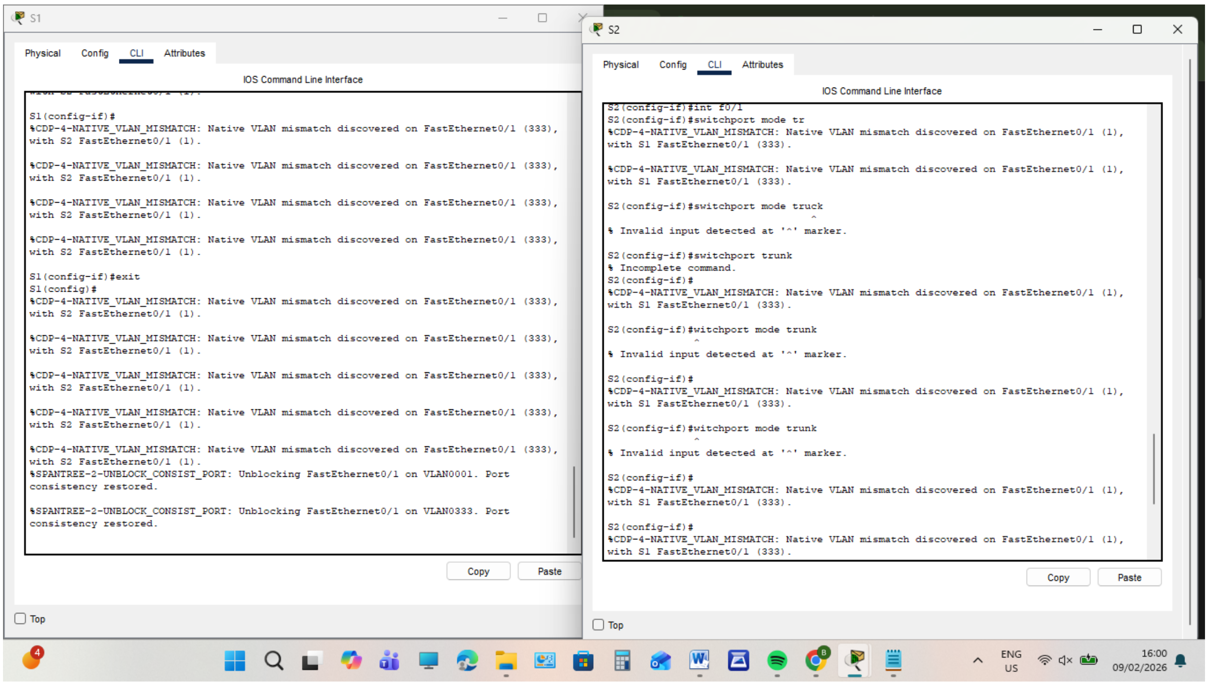
Here are both for S1 & S2



Part 3: Configure Switch Security.

Step 1: Implement 802.1Q trunking.

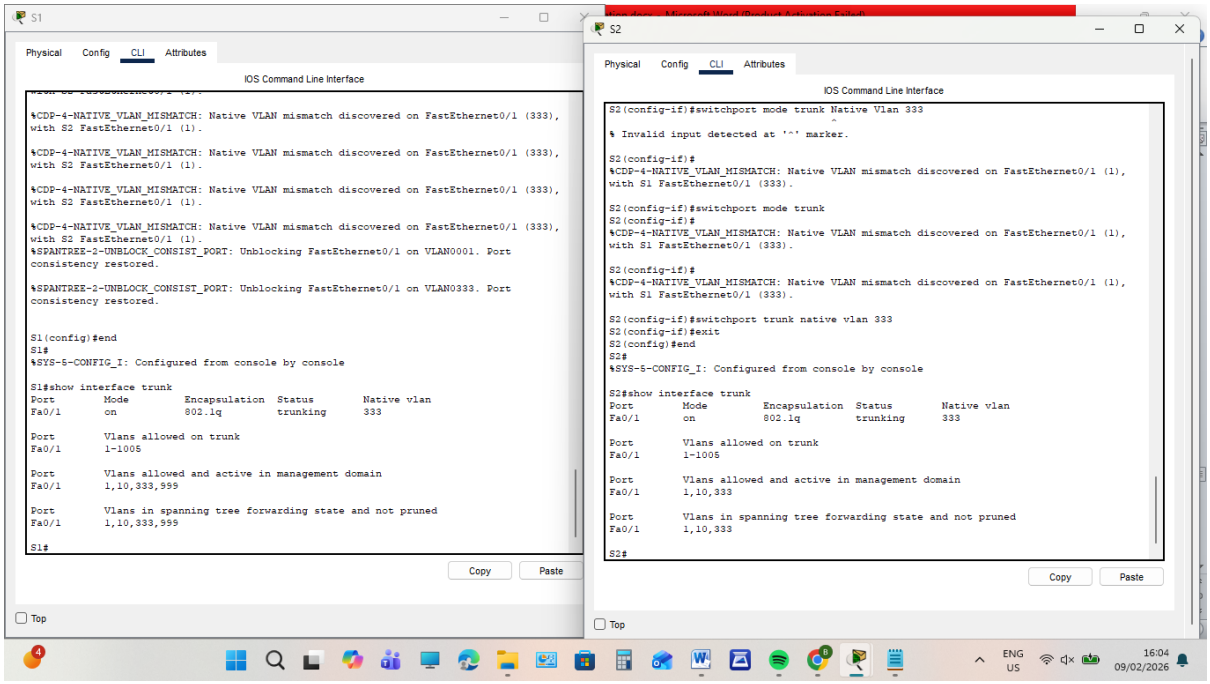
1. On both switches, configure trunking on F0/1 to use VLAN 333 as the native VLAN.



2. Verify that trunking is configured on both switches.

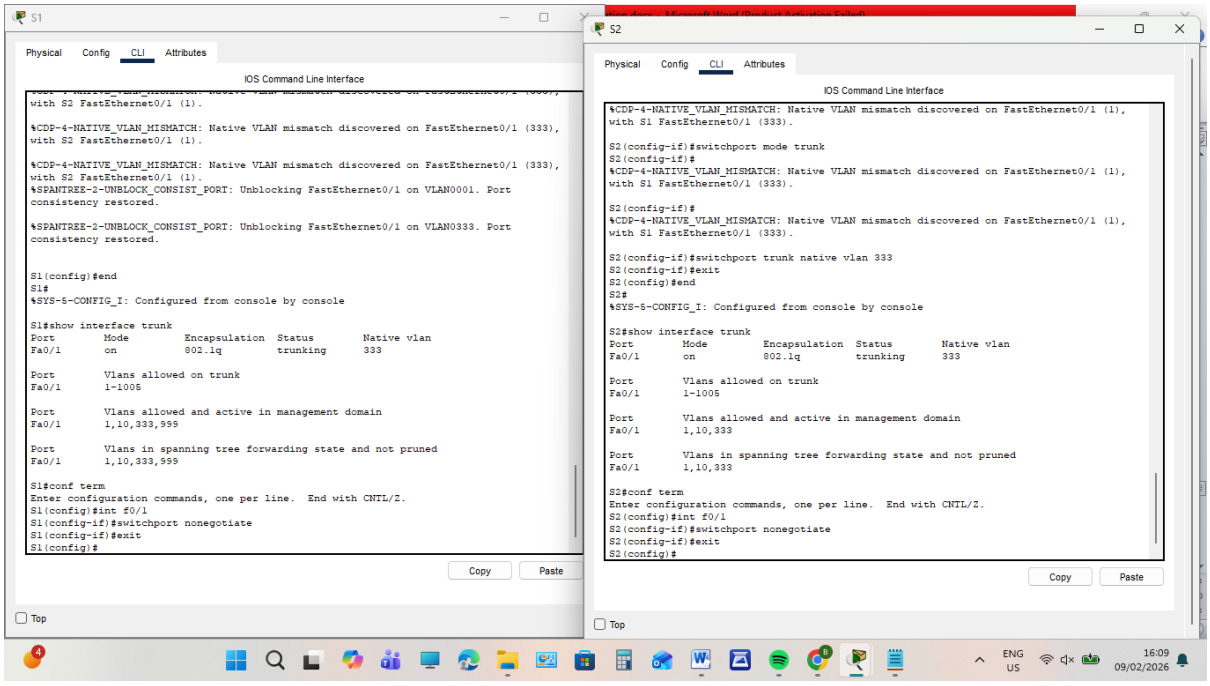
S1# show interface trunk

- Here are for both S1 & S2



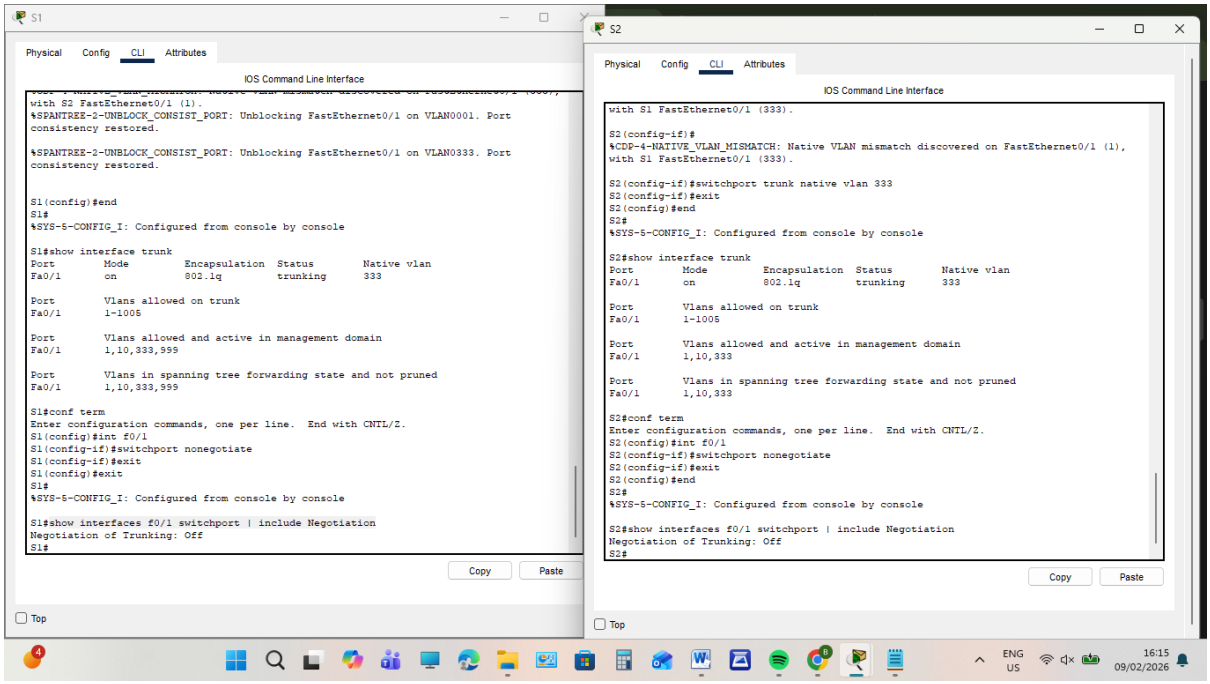
3. Disable DTP negotiation on F0/1 on S1 and S2.

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



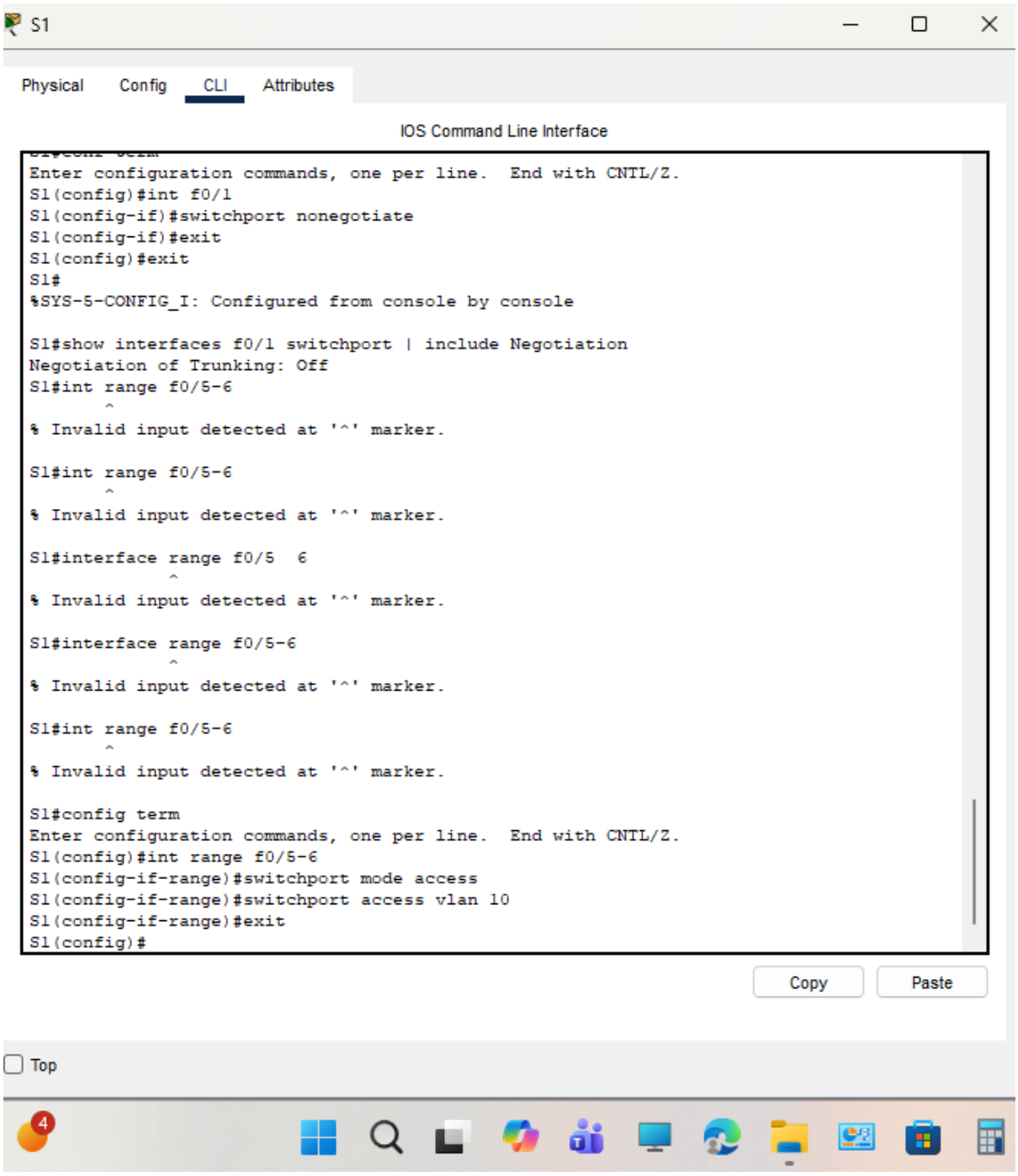
4. Verify with the show interfaces command.

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

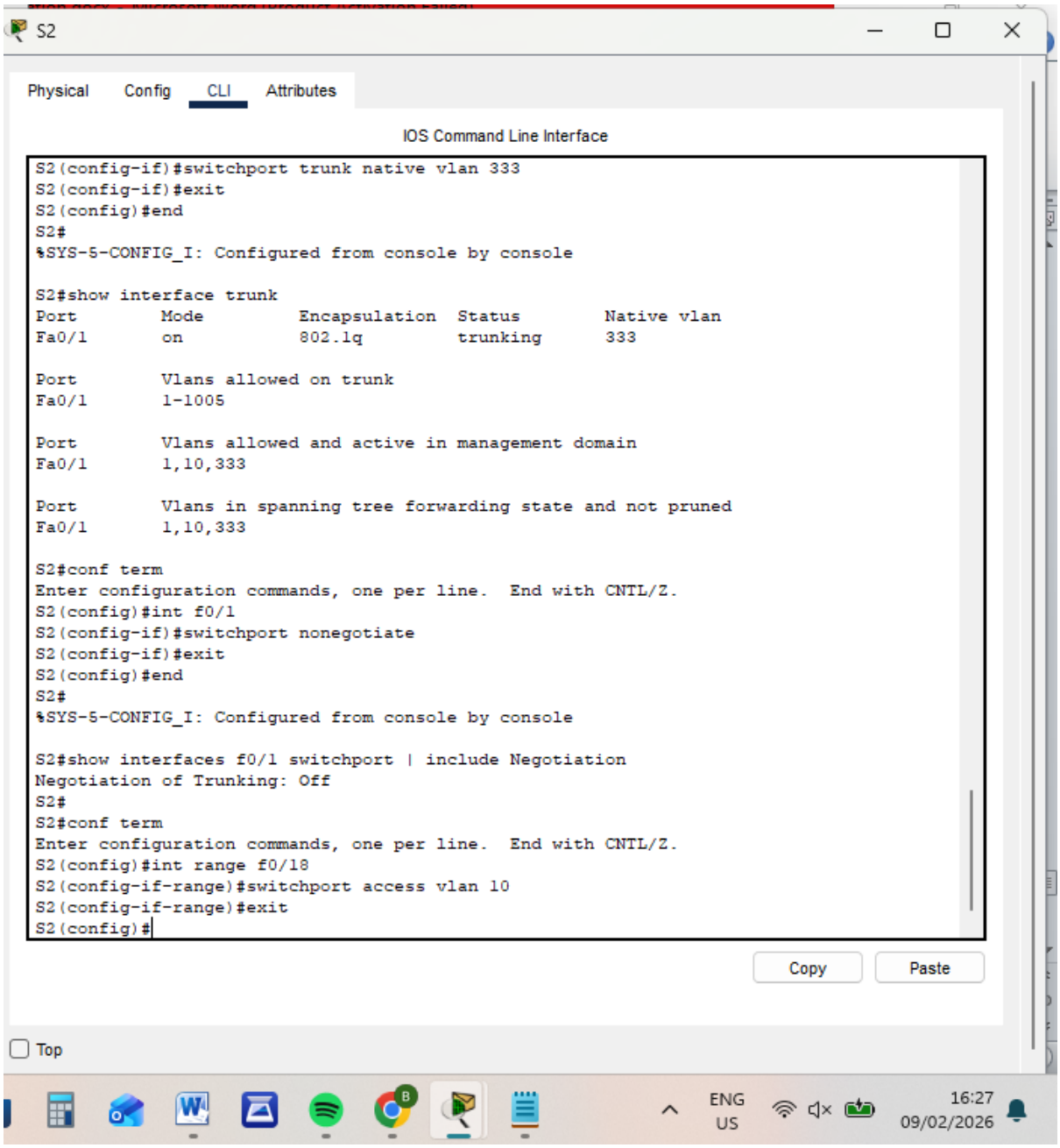


Step 2: Configure access ports.

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

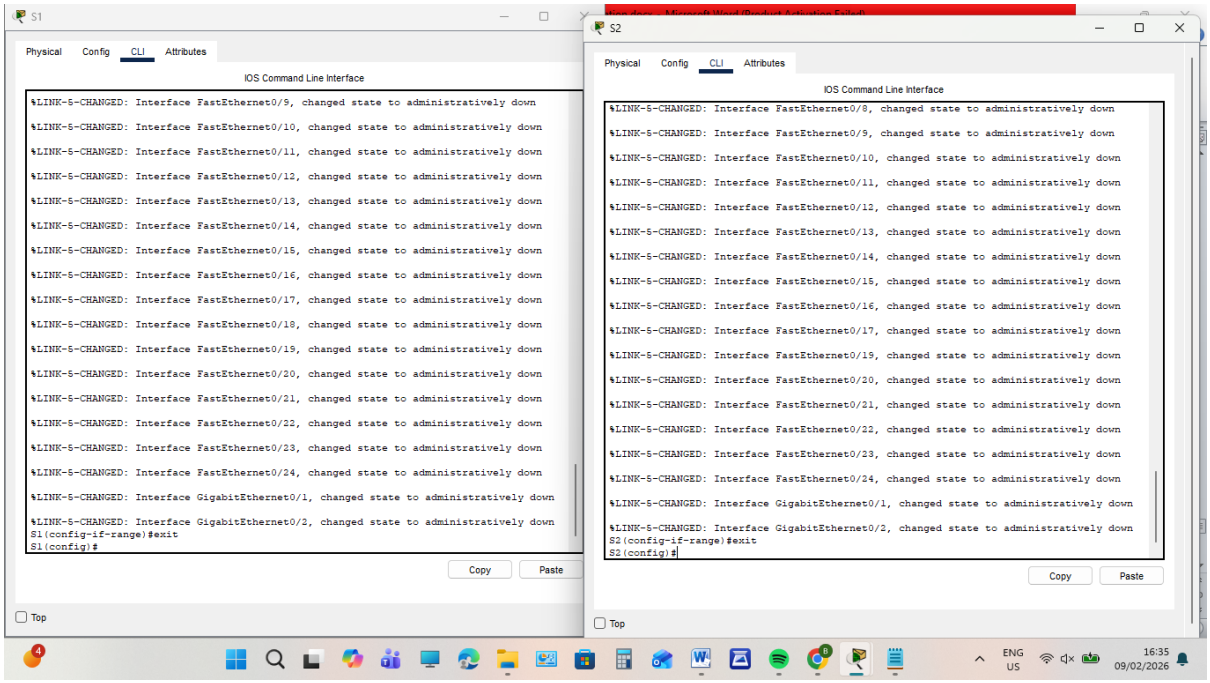


2. On S2, configure F0/18 as an access port that is associated with VLAN 10.



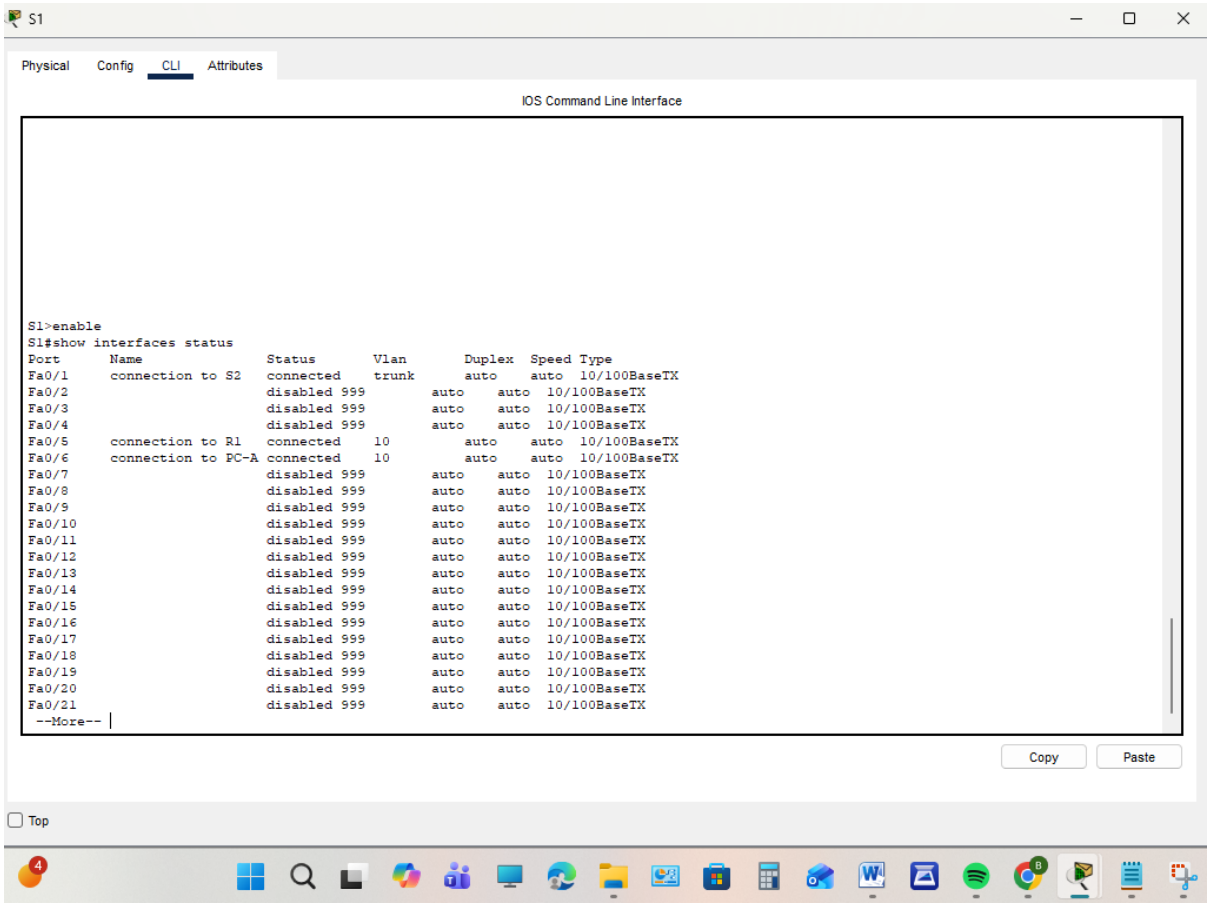
Step 3: Secure and disable unused switchports.

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

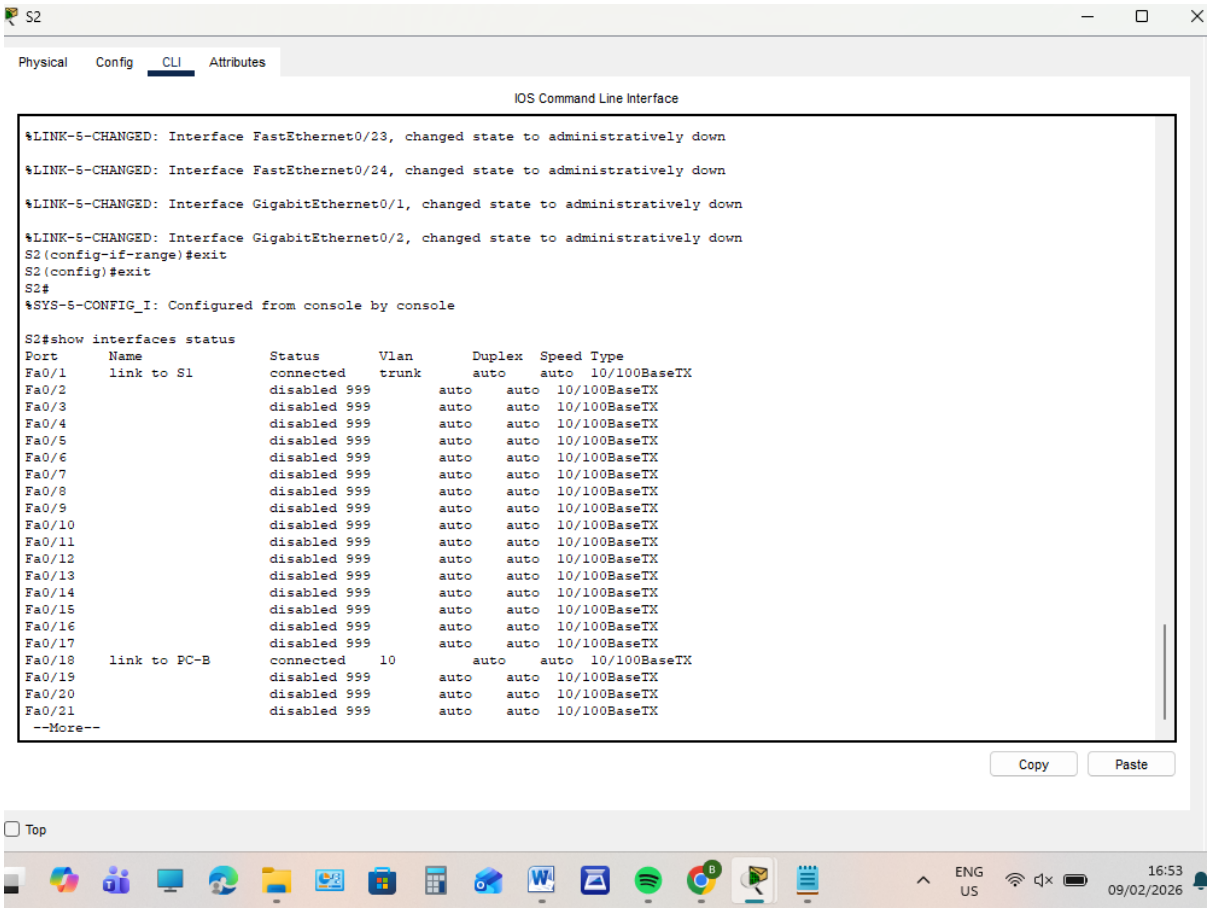


2. Verify that unused ports are disabled and associated with VLAN 999 by issuing the show command.

S1# show interfaces status



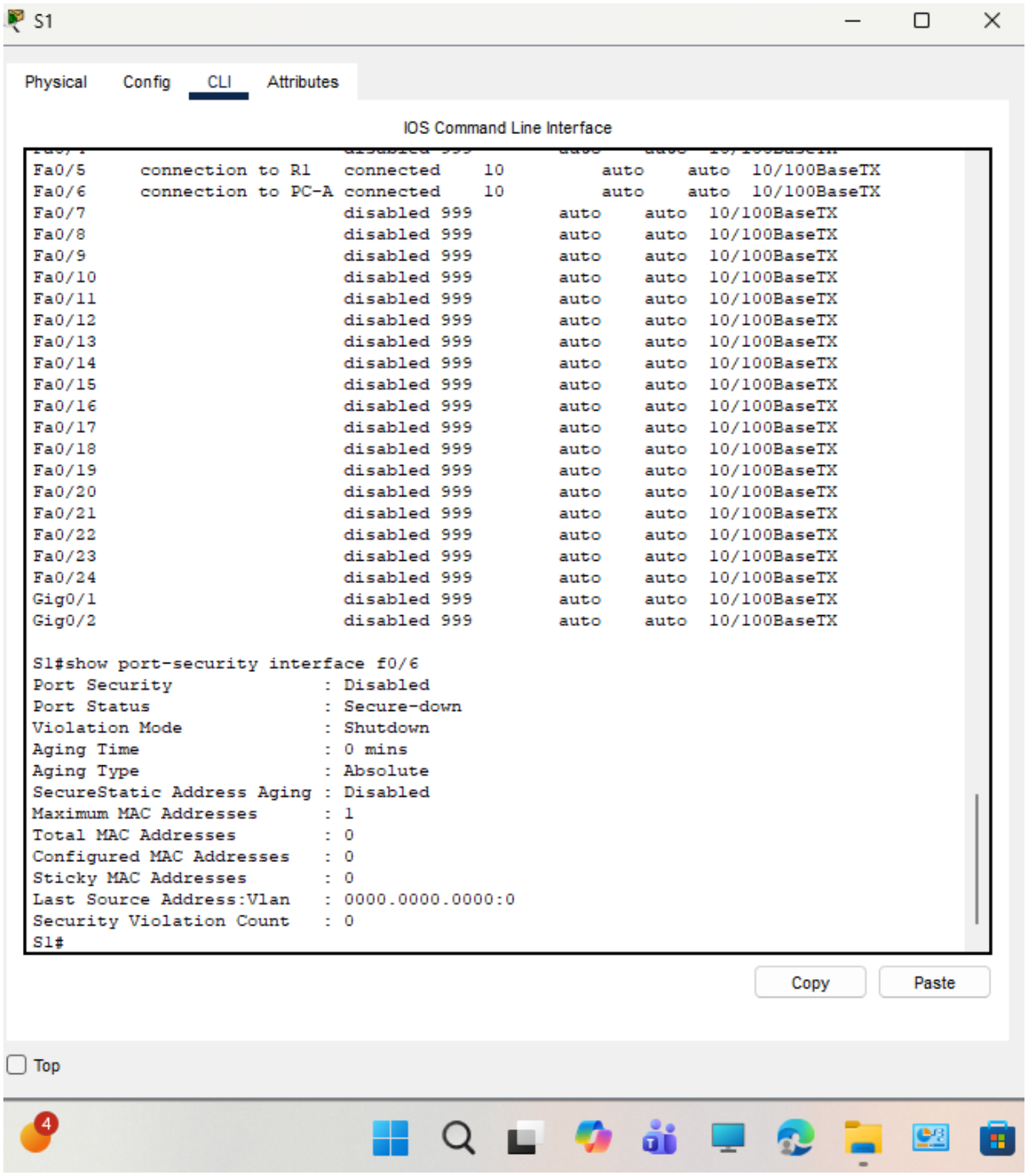
S2# show interfaces status



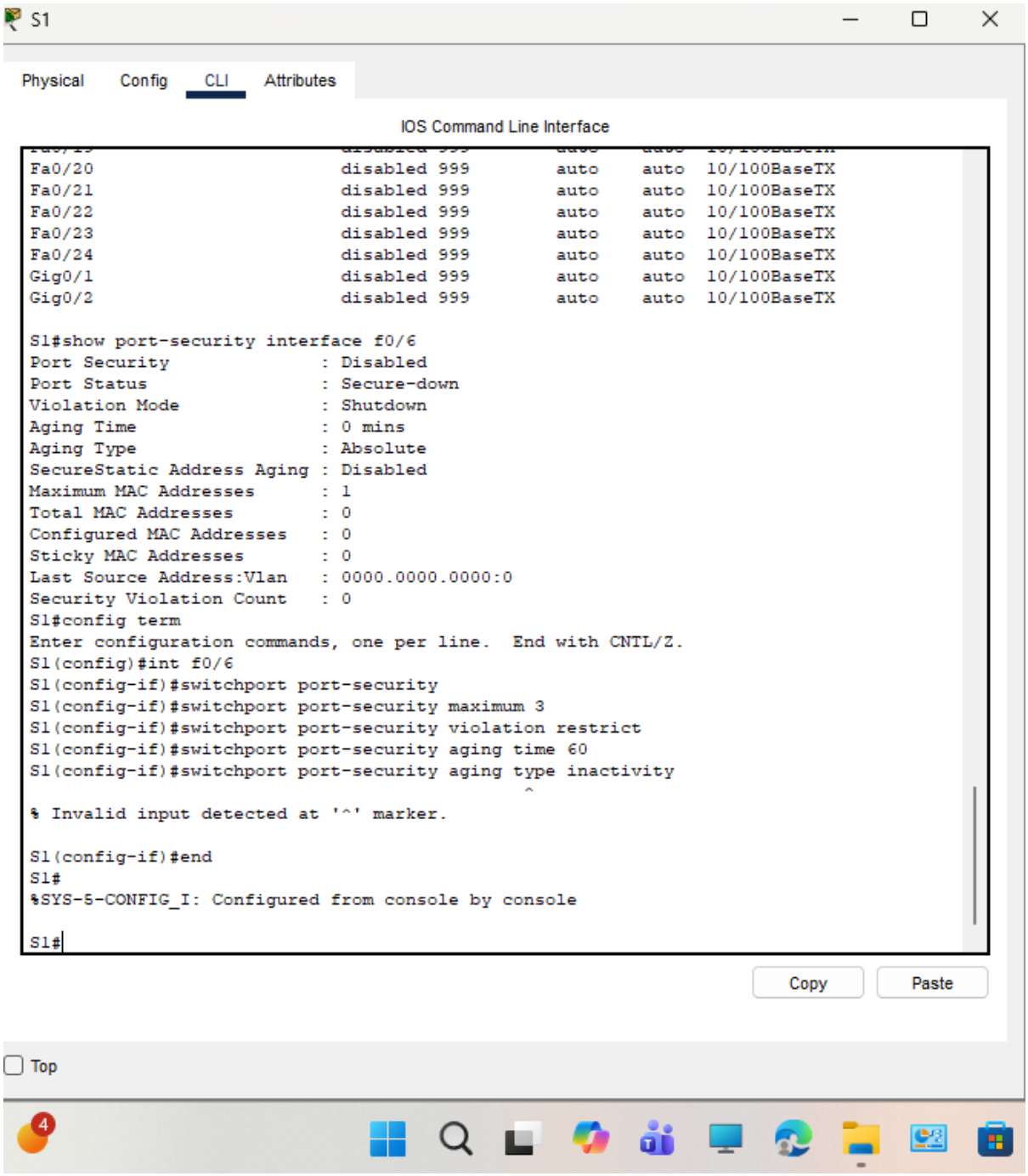
Step 4: Document and implement port security features.

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

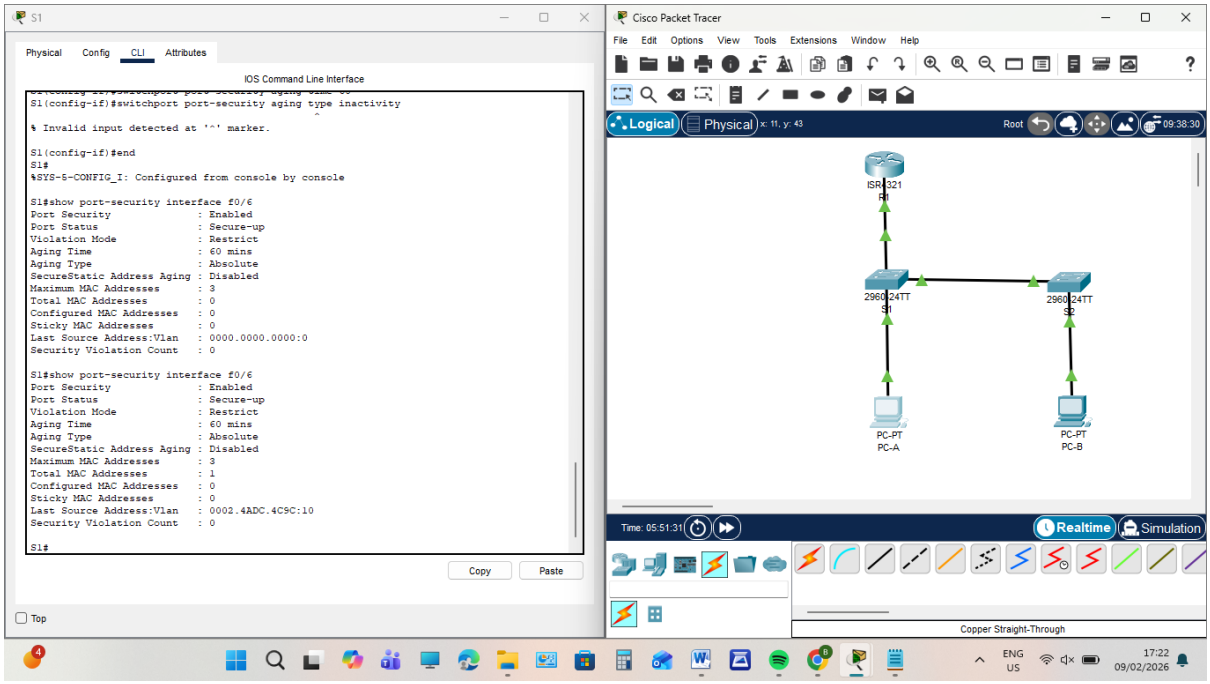
Settings for interface F0/6



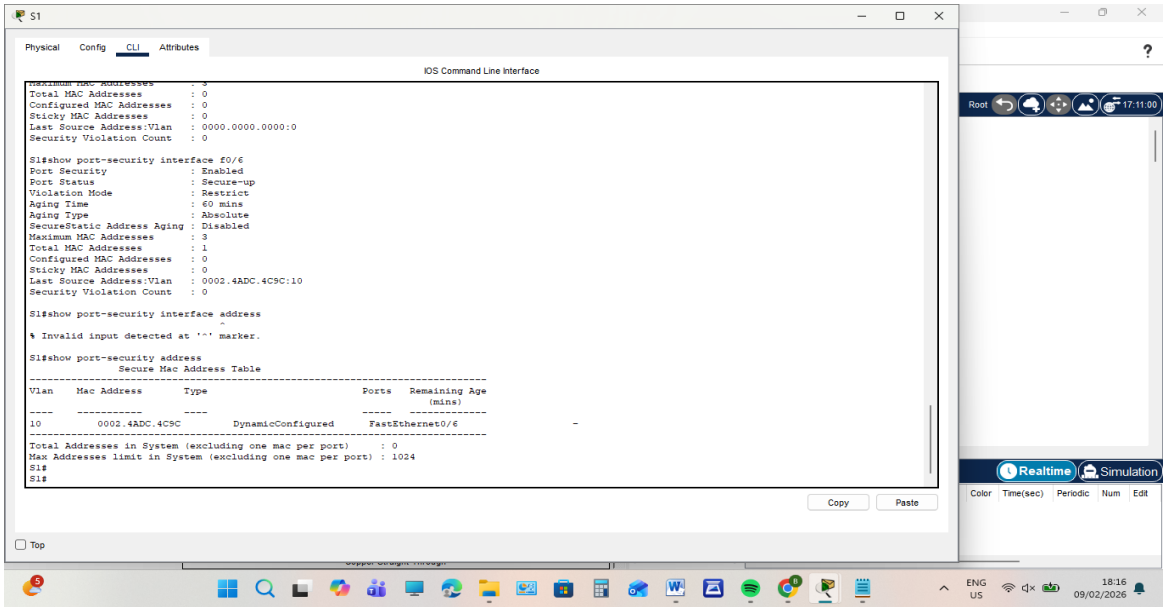
2. On S1, enable port security on F0/6 with the following settings:



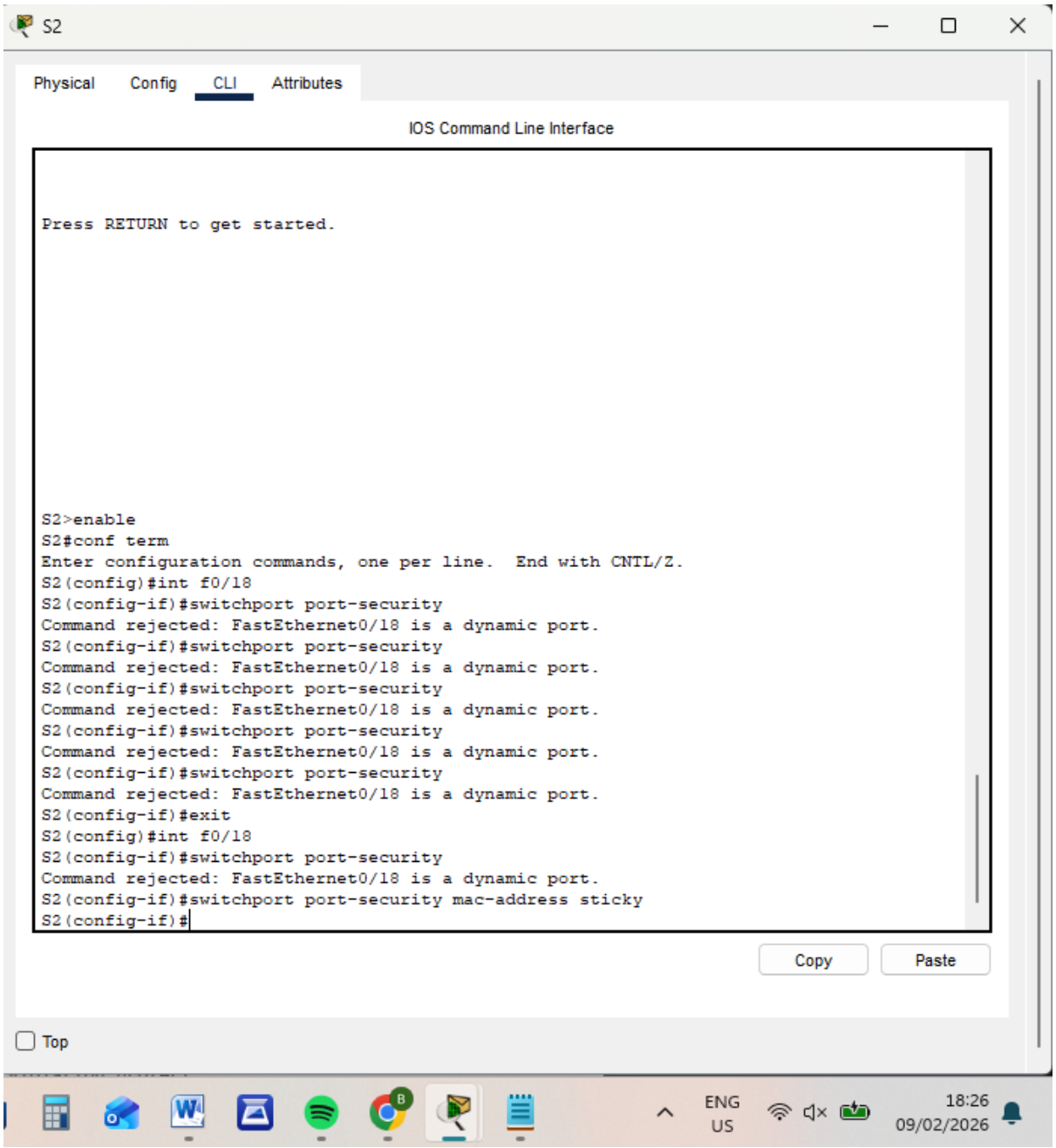
3. Verify port security on S1 F0/6.



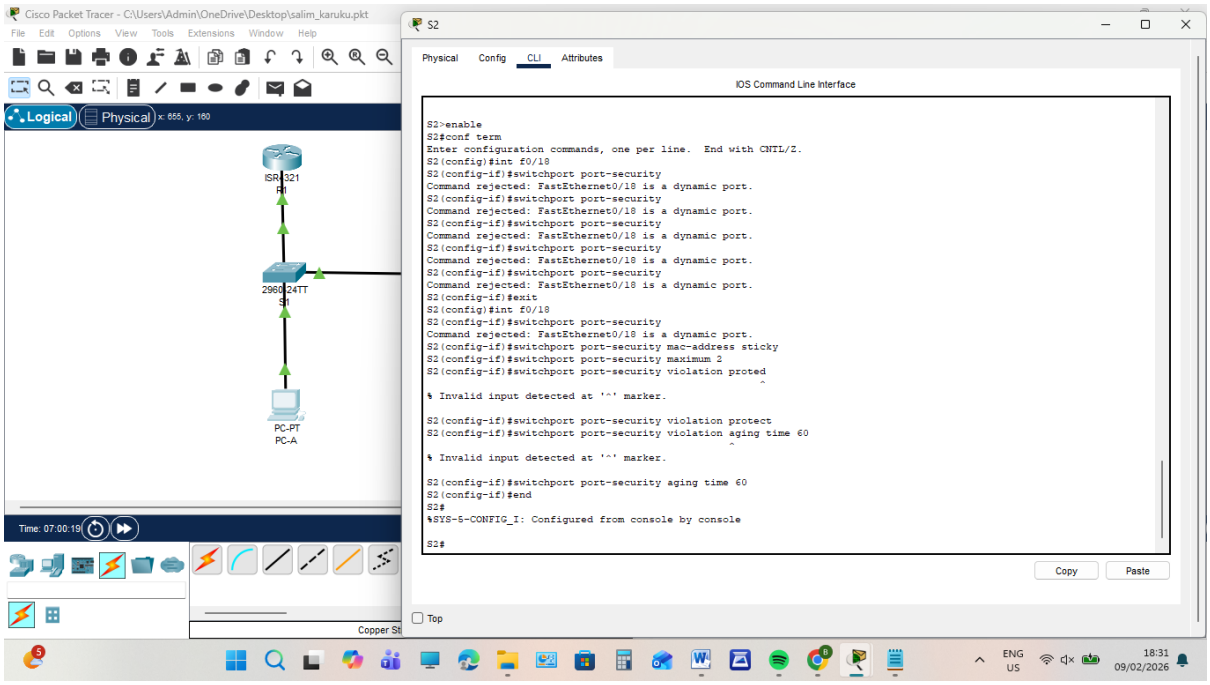
S1# show port-security address



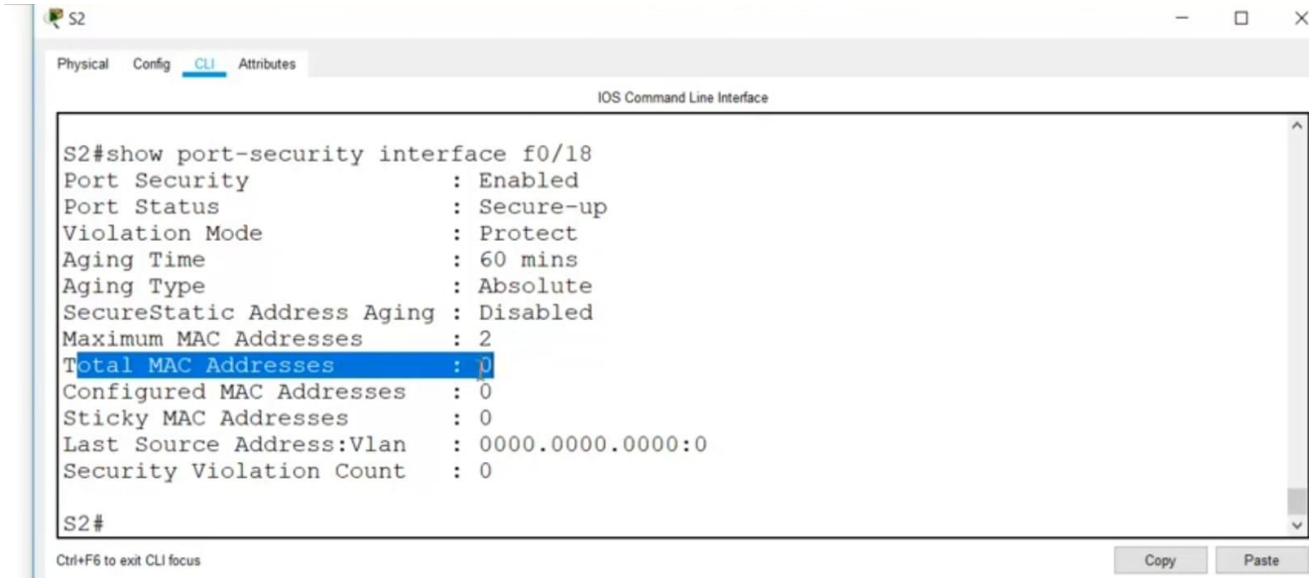
4. Enable port security for F0/18 on S2. Configure the port to add MAC addresses learned on the port automatically to the running configuration.



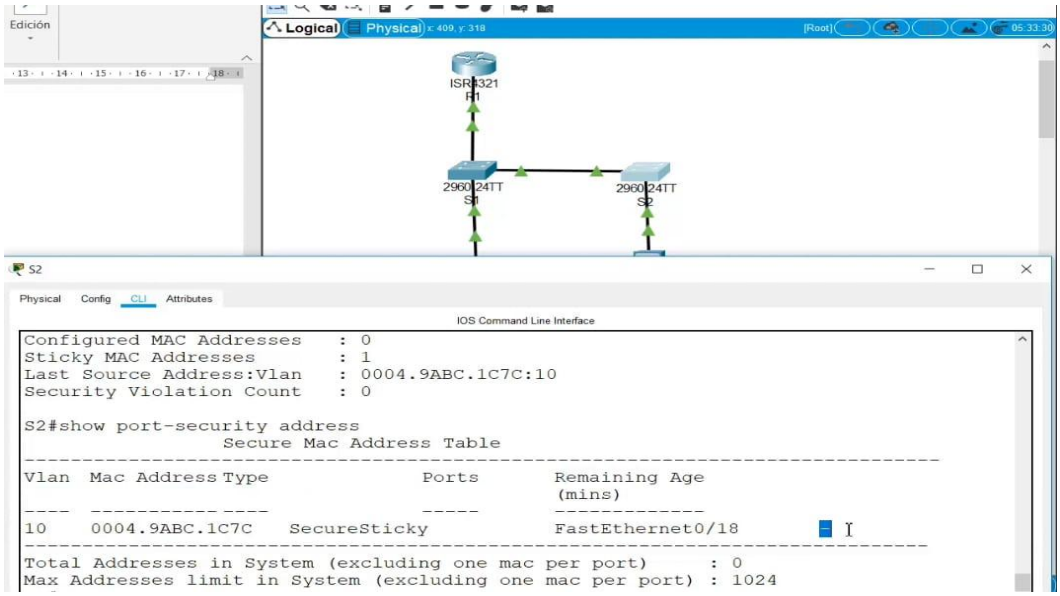
5. Configure the following port security settings on S2 F/18:



6. Verify port security on S2 F0/18

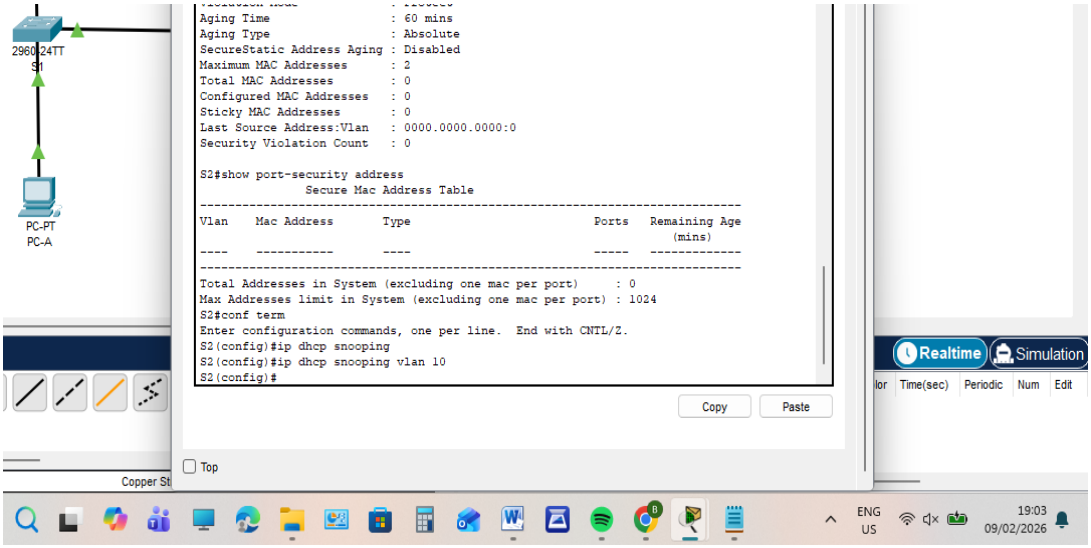


S2# show port-security address

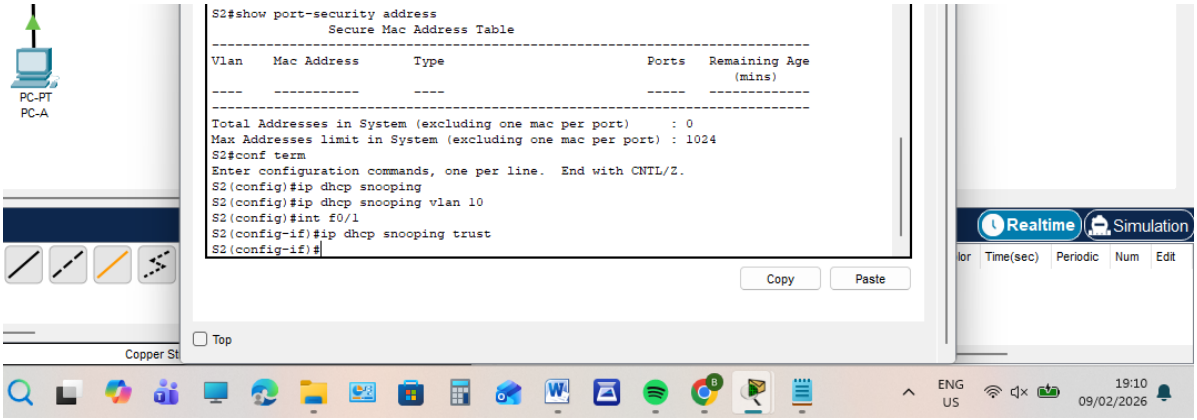


Step 5: Implement DHCP snooping security.

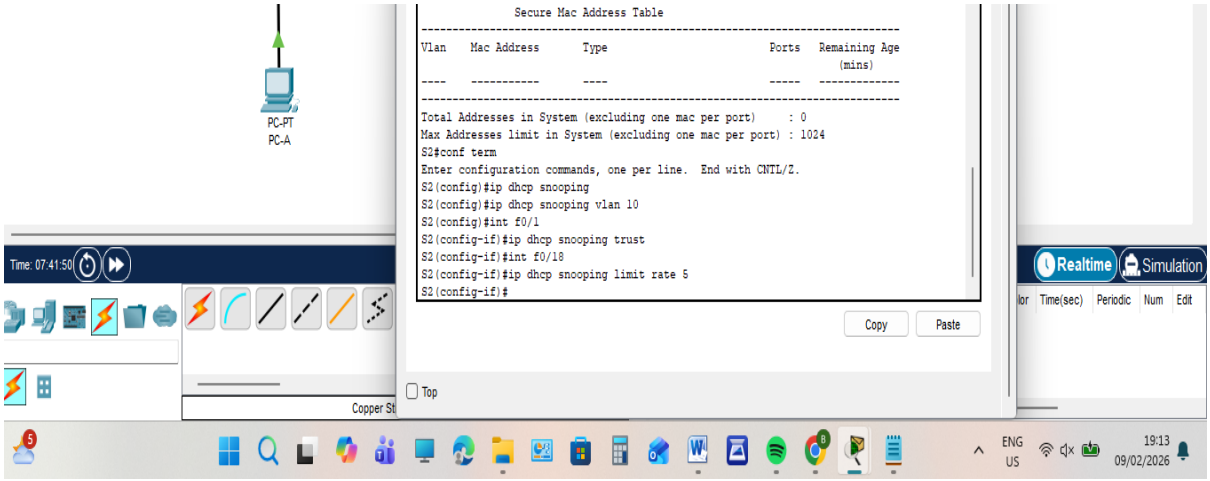
1. On S2, enable DHCP snooping and configure DHCP snooping on VLAN 10.



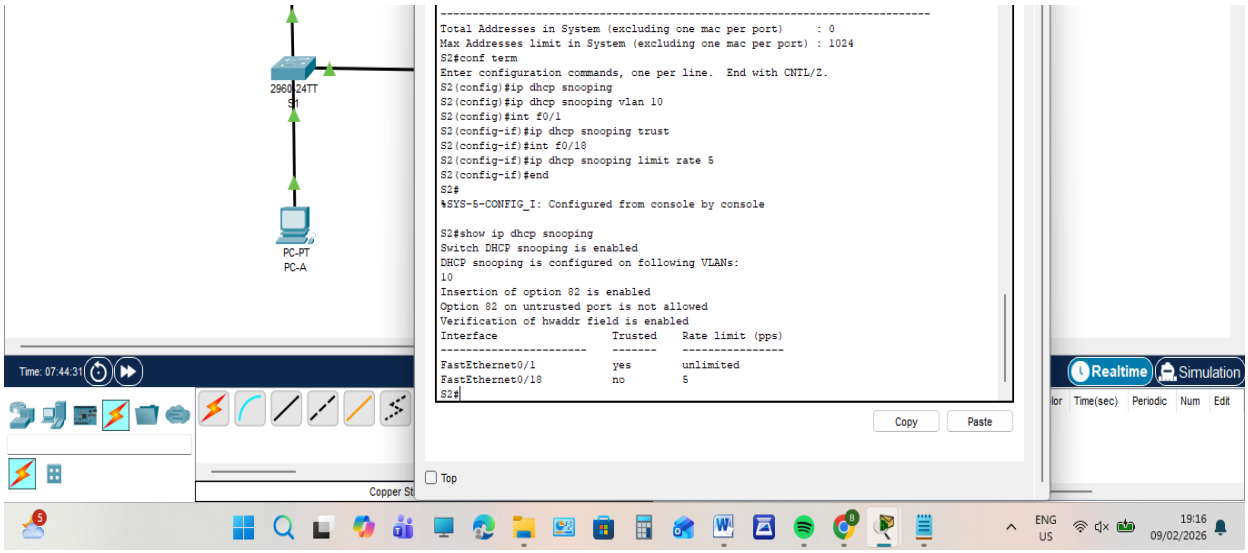
2. Configure the trunk port on S2 as a trusted port.



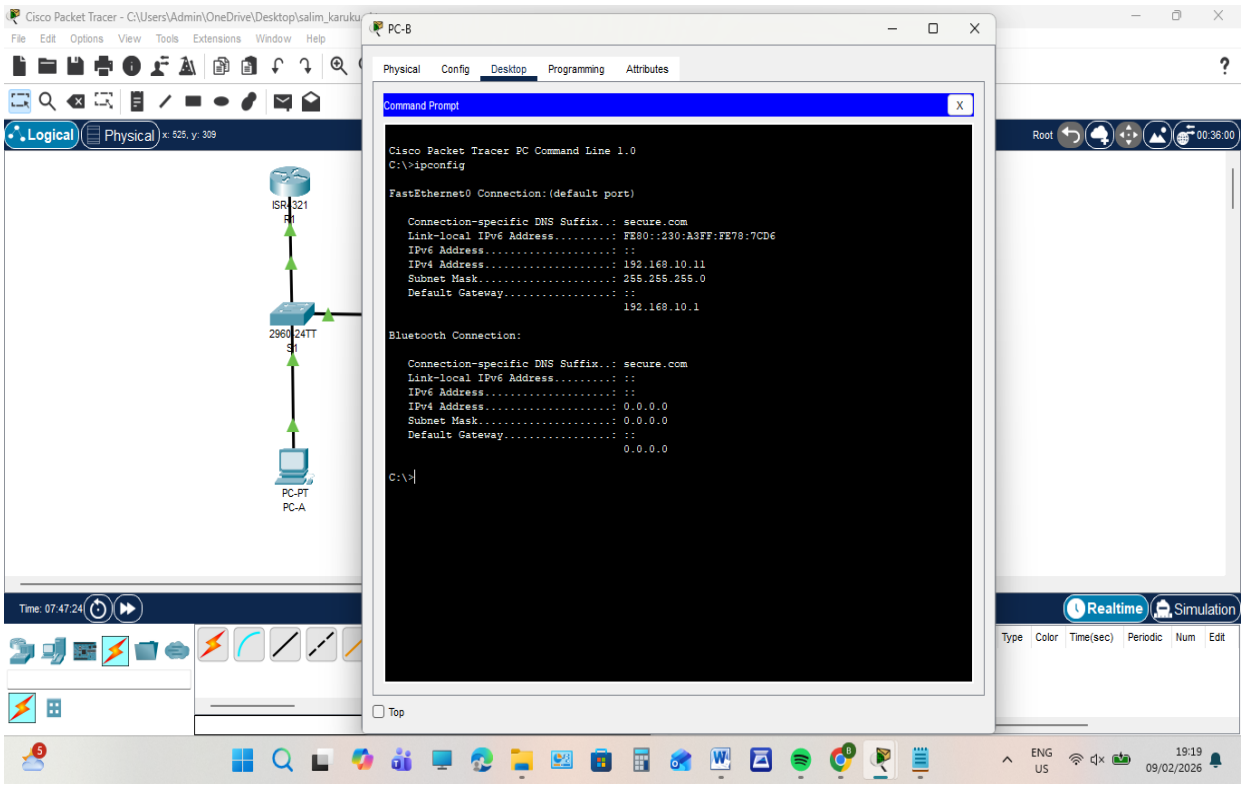
3. Limit the untrusted port, F18 on S2, to five DHCP packets per second.



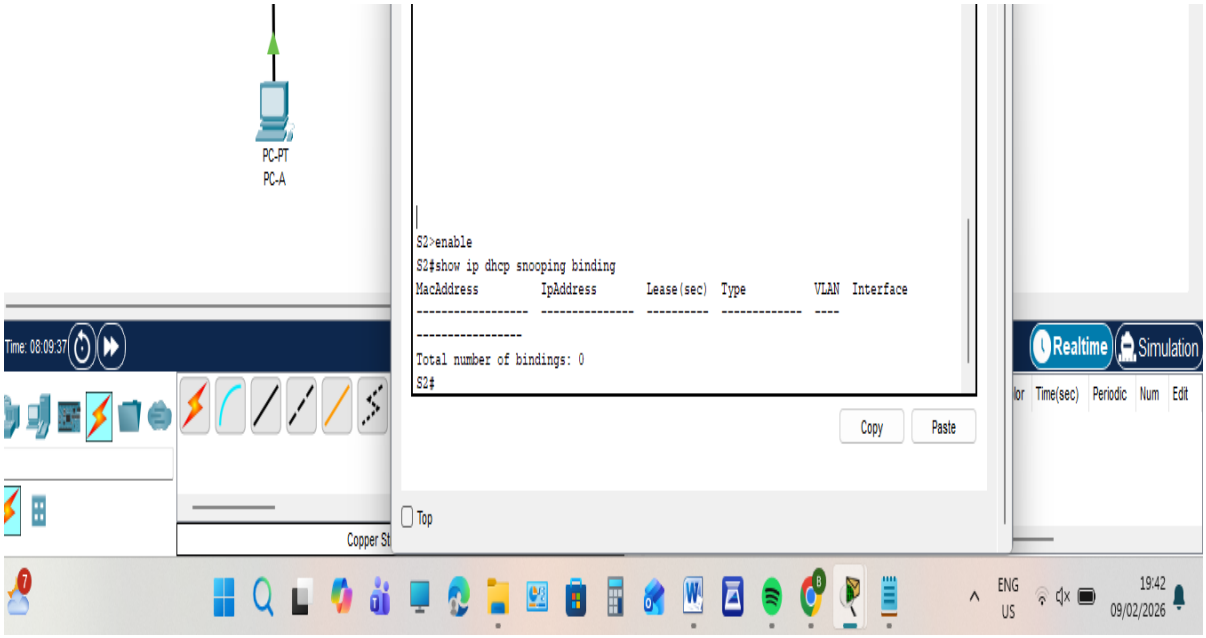
4. Verify DHCP Snooping on S2.



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



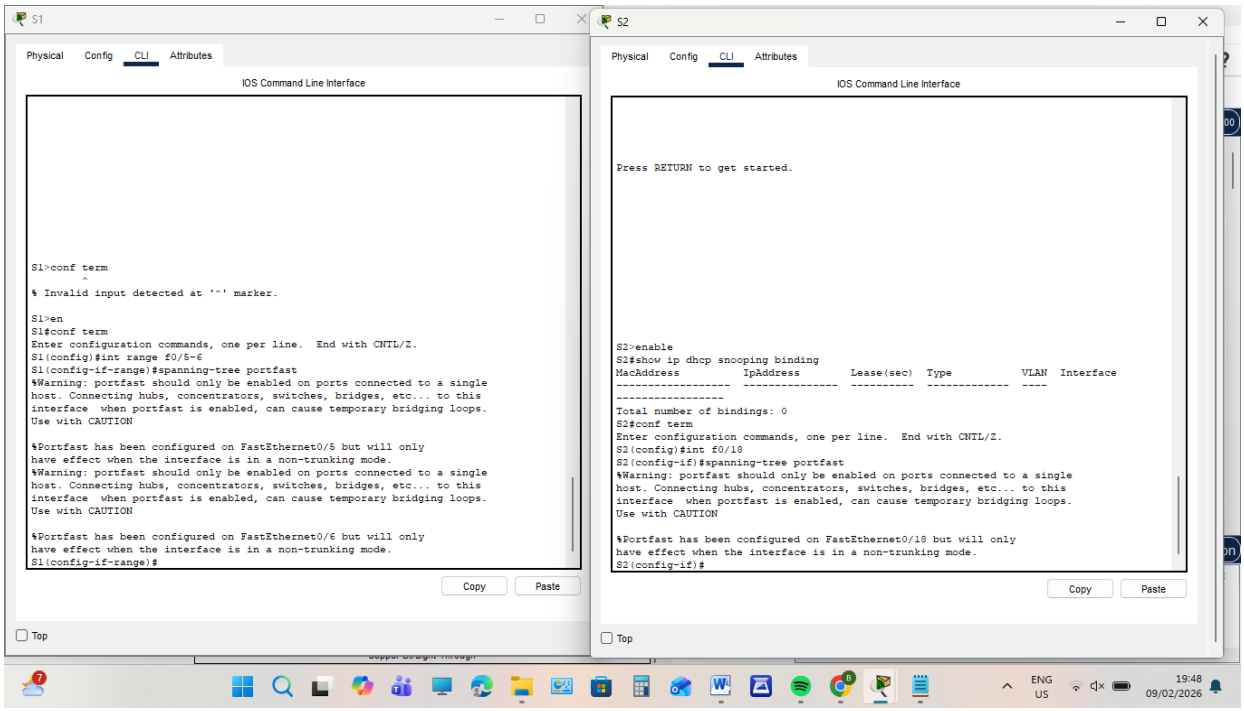
6. Verify the DHCP snooping binding using the show ip dhcp snooping binding command.



Step 6: Implement PortFast and BPDU guard.

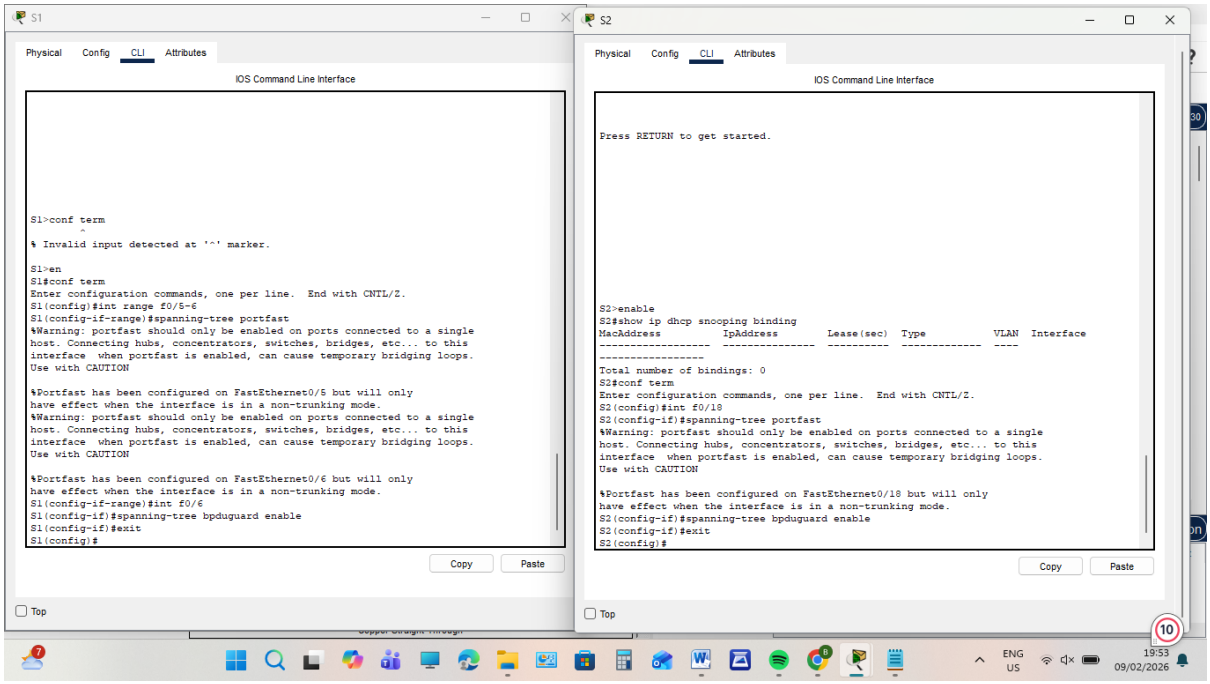
1. Configure PortFast on all the access ports that are in use on both switches.

- Here are for both S1 & S2



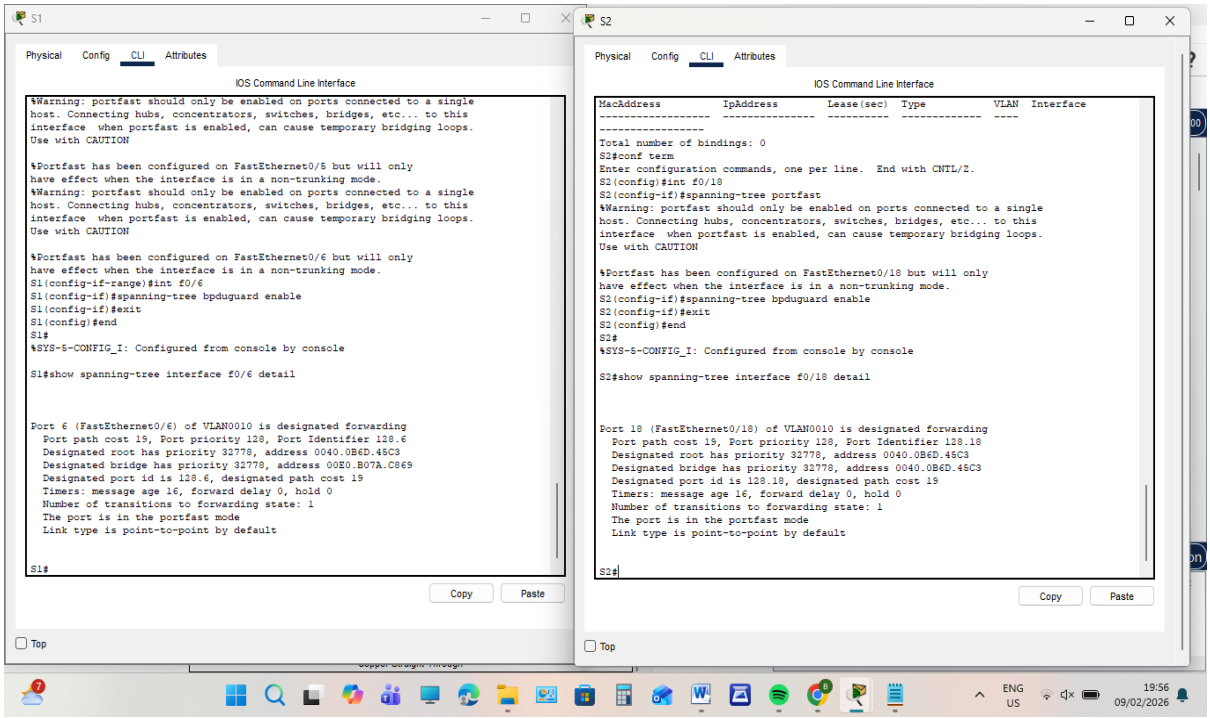
2. Enable BPDU guard on S1 and S2 VLAN 10 access ports connected to PC-A and PC-B.

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



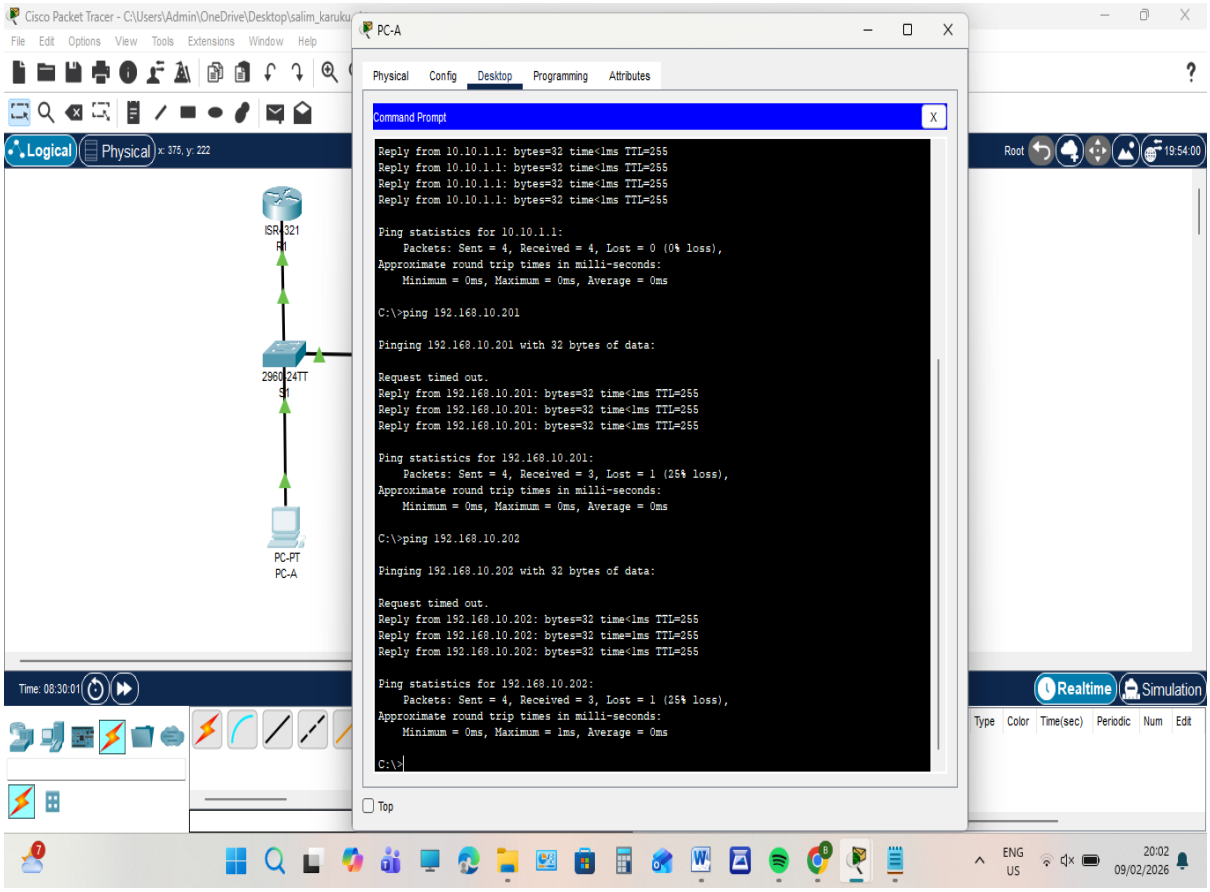
3. Verify that BPDU guard and PortFast are enabled on the appropriate ports.

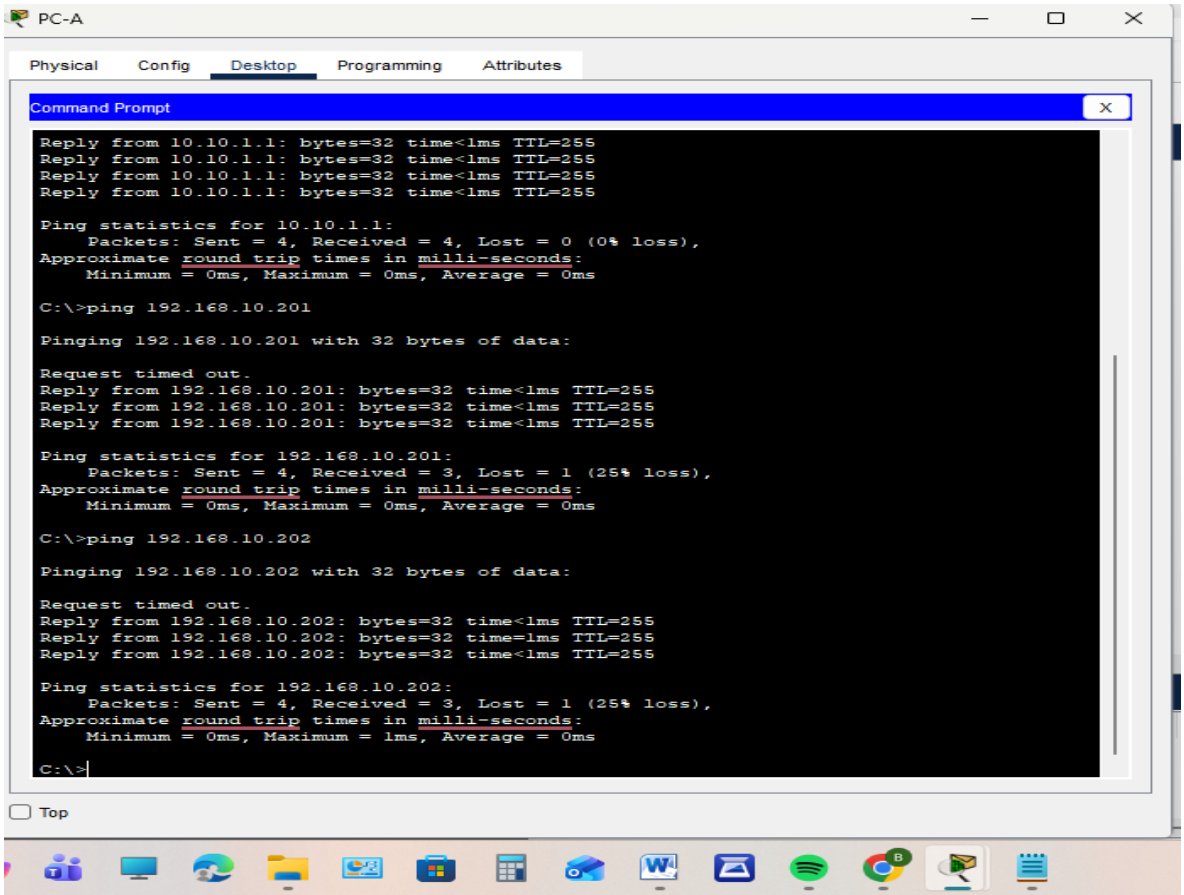
- BPDU guard and PortFast for both S1 & S2 below



Step 7: Verify end-to-end connectivity.

I verify the connectivity by pinging the IP addresses and the pinging 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.