Cloud and Network Security-C1-2026

STUDENT NAME: FELIX WEBBO

STUDENT NO: CS-CNS11-26044

MONDAY, FEB 16, 2026

Week 4: Assignment 1

Class Exercise: VLANs and Secure Switch Configuration

1 ABSTRACT.

This report presented the configuration and implementation of Virtual Local Area Networks (VLANs) and Layer 2 switch security mechanisms in an IPv4 enterprise network environment. The laboratory exercise was conducted using Cisco Catalyst 2960 switches and a Cisco 4221 router within a Packet Tracer simulation. VLAN segmentation was established to enhance network organization, improve traffic management, and strengthen administrative control. Additionally, multiple security features, including port security, DHCP snooping, PortFast, and BPDU Guard, were configured to mitigate common Layer 2 attacks such as rogue switch insertion, MAC flooding, and DHCP starvation. The successful completion of the lab demonstrated the importance of VLAN-based segmentation and proactive switch hardening in ensuring secure and efficient network operations.

2 Table of Contents

3 INTRODUCTION

Modern enterprise networks required both efficient traffic segmentation and robust security mechanisms to maintain performance and protect infrastructure. Switches operating at the data link layer were often vulnerable to attacks such as ARP spoofing, unauthorized access through unused ports, and rogue device insertion. As a result, VLAN deployment and secure switch configuration were essential in mitigating such threats.

This laboratory exercise focused on reviewing and applying key Layer 2 security practices. VLANs were configured to isolate management traffic, while switchport security controls were implemented to prevent unauthorized devices from accessing the network. The exercise also incorporated DHCP snooping and spanning-tree enhancements to protect against spoofing and topology manipulation.

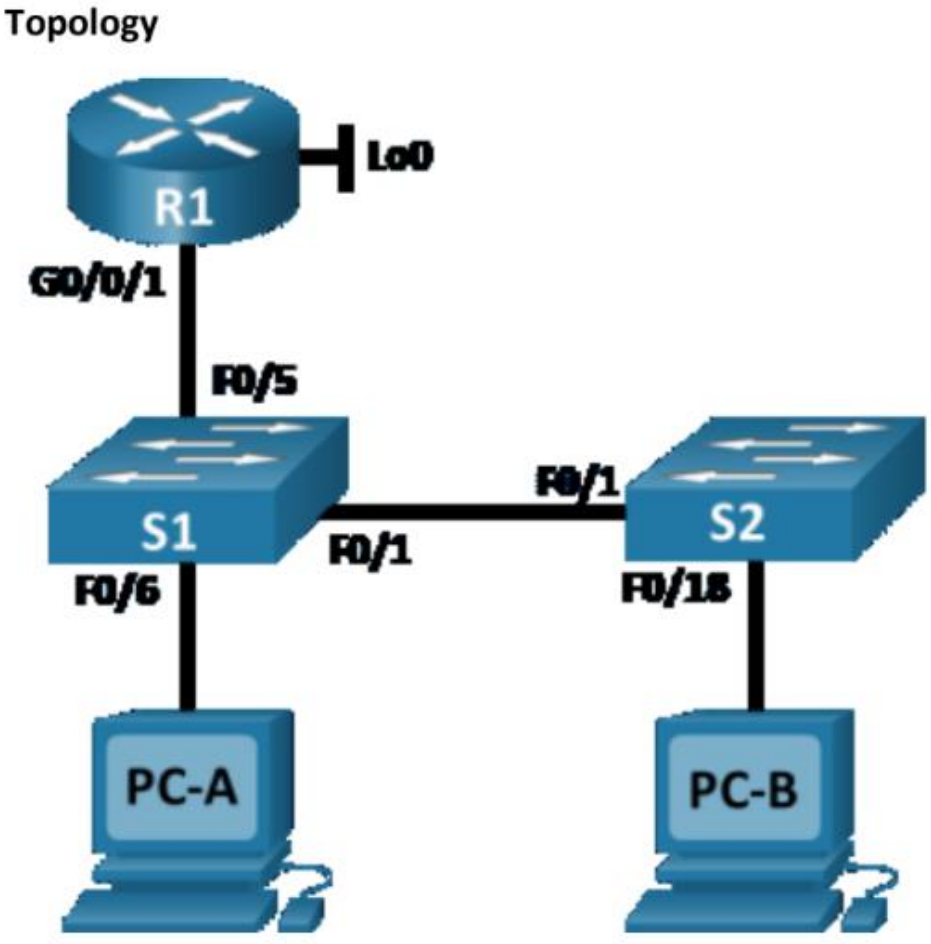
4 OBJECTIVES

The objectives of this laboratory exercise were as follows:

- ✓ To configure the network devices and establish basic connectivity.
- ✓ To implement VLAN 10 as the management VLAN and configure Switch Virtual Interfaces (SVIs).
- ✓ To configure VLAN 333 as the native VLAN and VLAN 999 as the parking lot VLAN.
- ✓ To implement 802.1Q trunking between switches and disable DTP negotiation.
- ✓ To secure unused switchports by assigning them to an unused VLAN and shutting them down.
- ✓ To configure port security features to restrict unauthorized device access.
- ✓ To implement DHCP snooping to protect against rogue DHCP servers and starvation attacks.
- ✓ To enable PortFast and BPDU Guard on access ports to prevent rogue switch insertion.
- ✓ To verify end-to-end connectivity and validate secure network operation.

5 NETWORK TOPOLOGY AND ADDRESSING

The simulated network consisted of one router (R1), two switches (S1 and S2), and two end-user PCs. Management connectivity was achieved through VLAN 10, which served as the primary administrative VLAN.



The addressing scheme included:

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

- Router interface: **192.168.10.1/24**
- Switch S1 management SVI: **192.168.10.201/24**
- Switch S2 management SVI: **192.168.10.202/24**
- PCs were assigned addresses dynamically via DHCP

This addressing design ensured centralized routing while maintaining separate logical segmentation for management operations.

6 METHODOLOGY

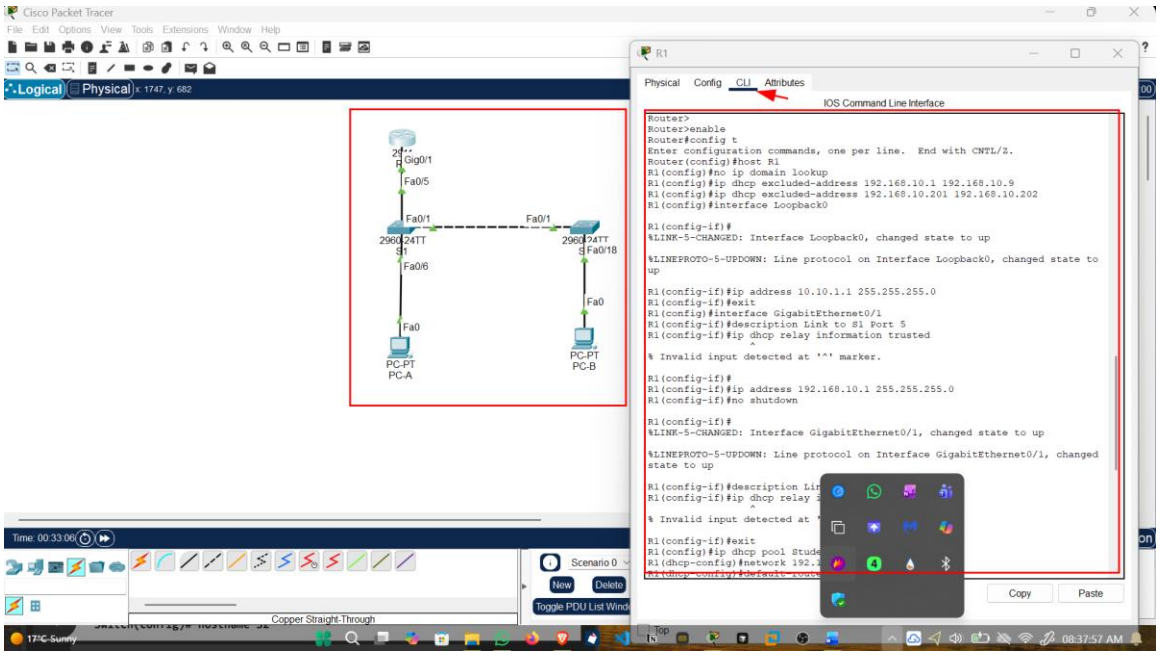
6.1 Part 1: Configure the Network Devices

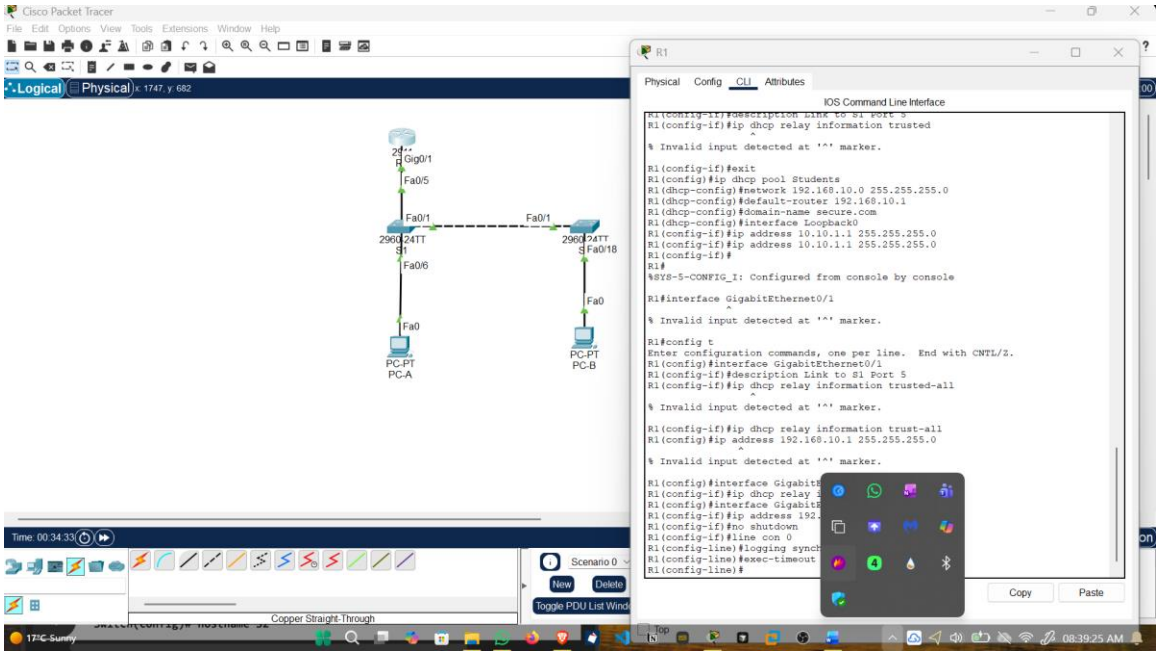
6.1.1 Step 1: Cable the network.

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

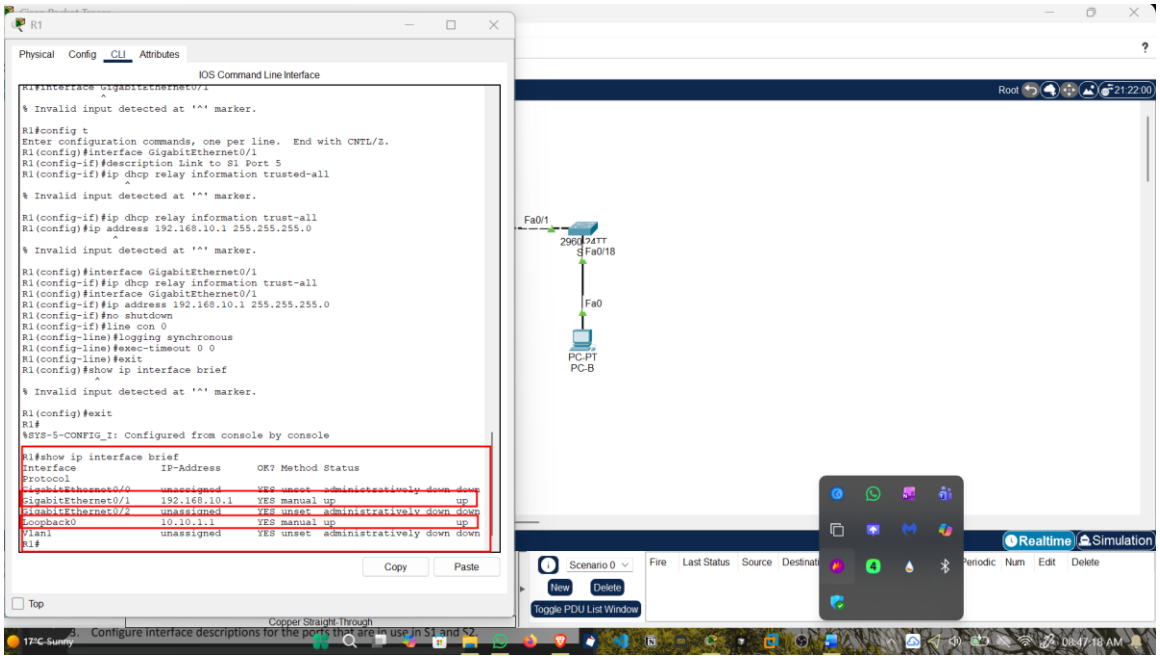
6.1.2 Step 2: Configure R1.

1. Load the following configuration script on R1.





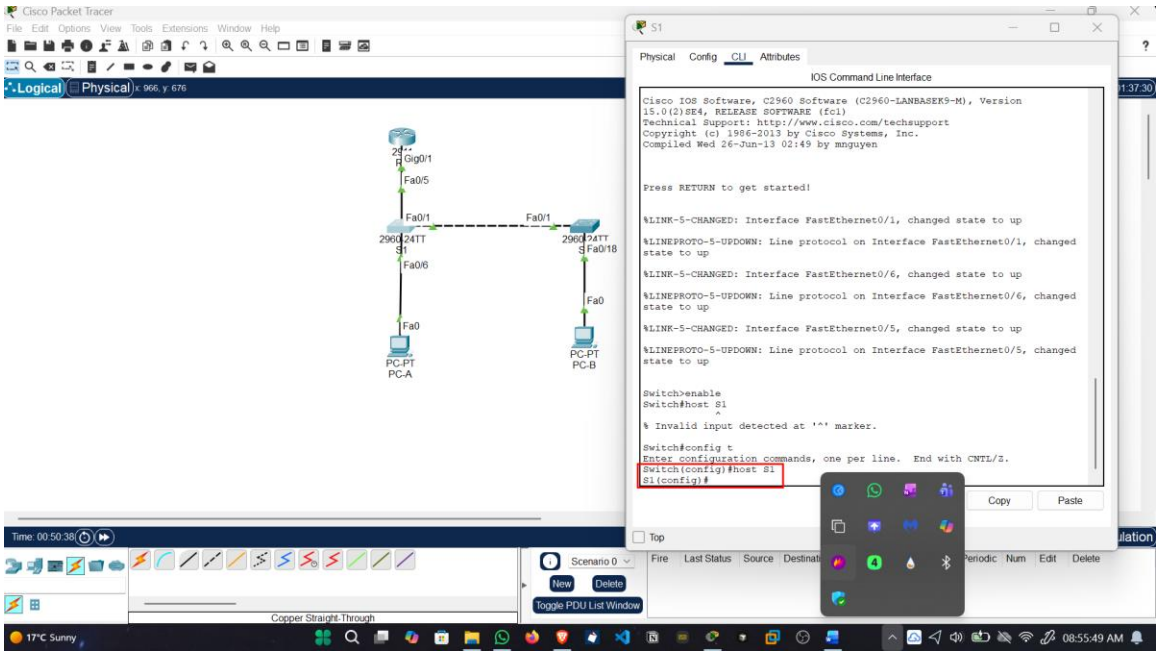
2. Verify the running-configuration on R1 using the following command

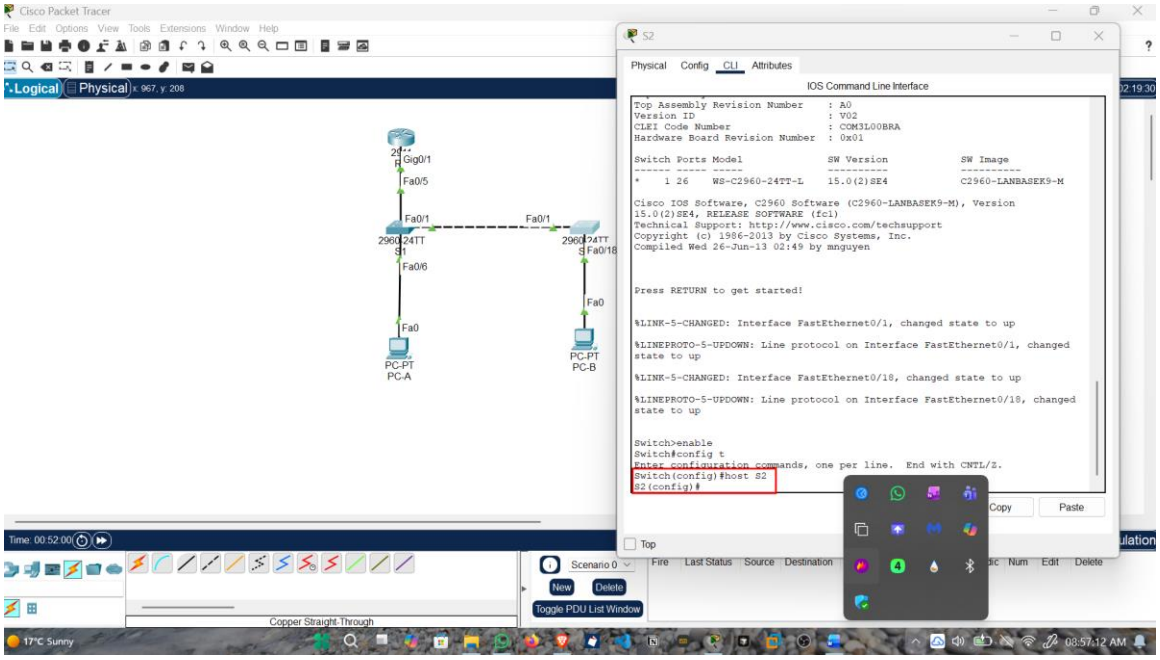


3. Verify IP addressing and interfaces are in an up / up state (troubleshoot as necessary).

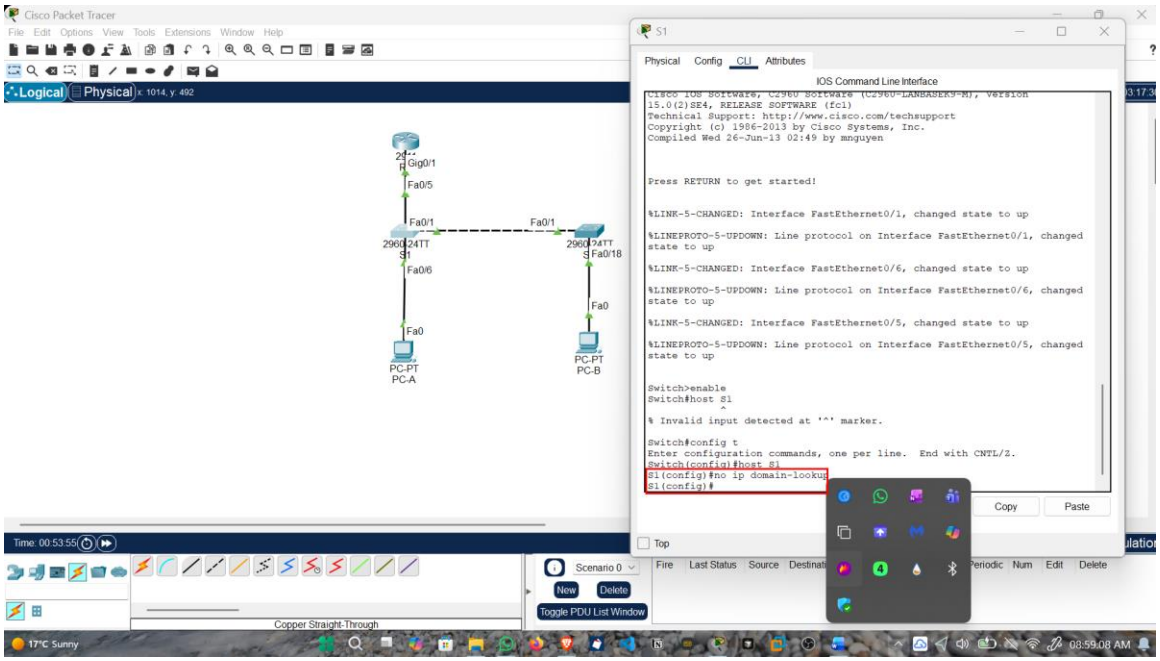
6.1.3 Step 3: Configure and verify basic switch settings.

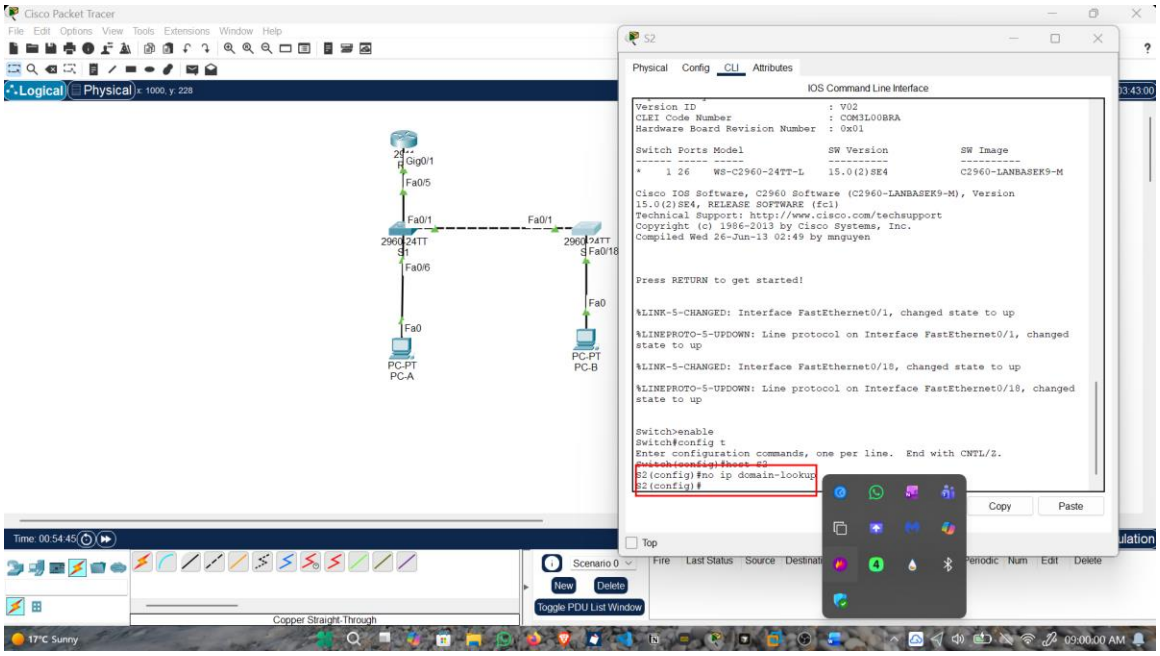
1. Configure the hostname for switches S1 and S2.



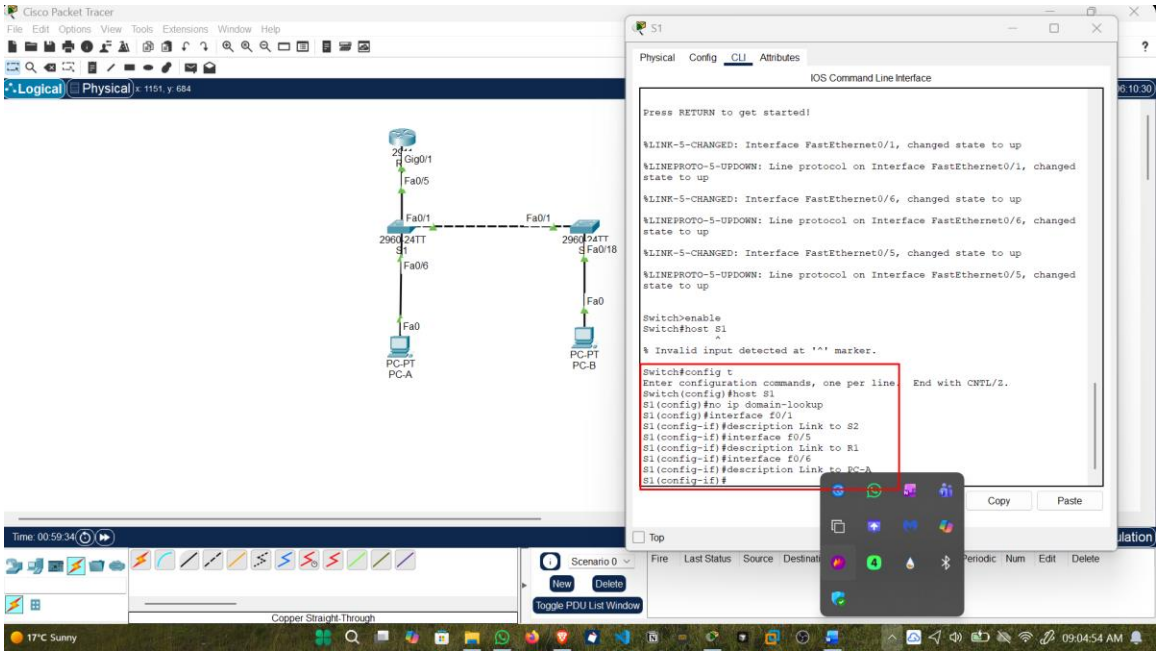


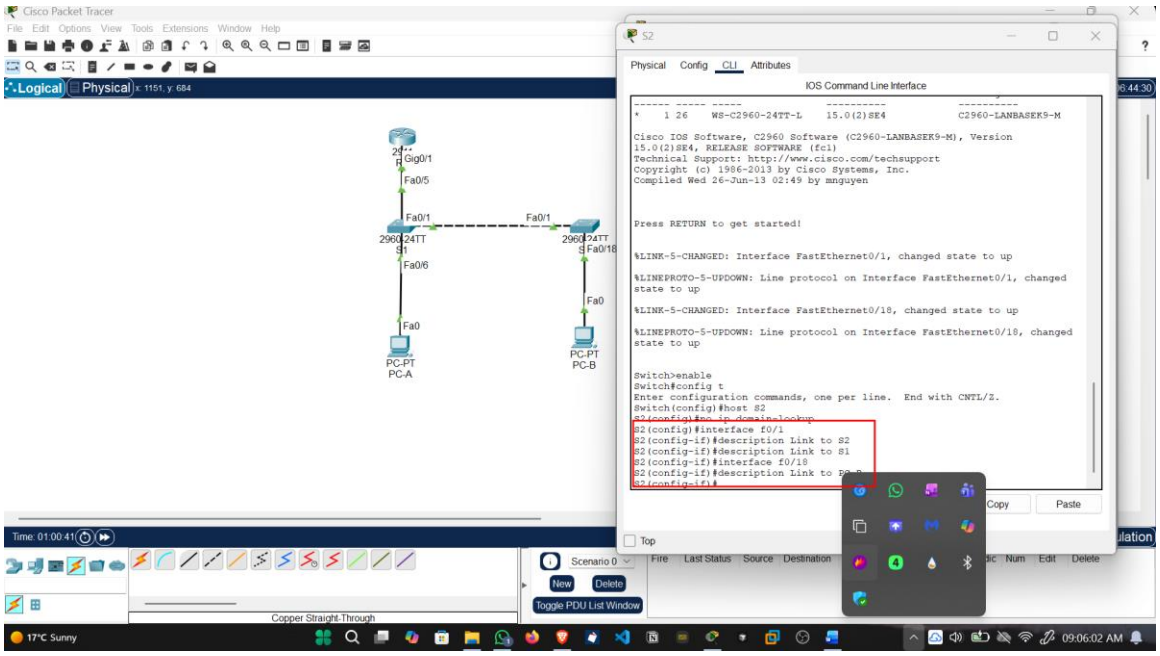
2. Prevent unwanted DNS lookups on both switches.



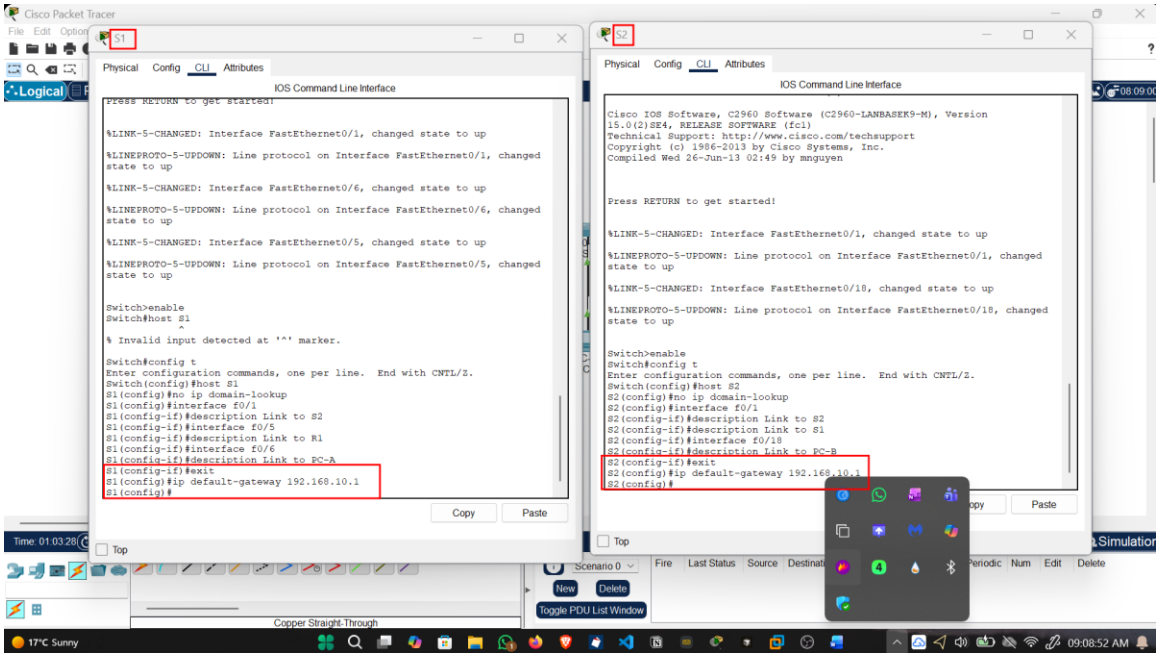


3. Configure interface descriptions for the ports that are in use in S1 and S2.





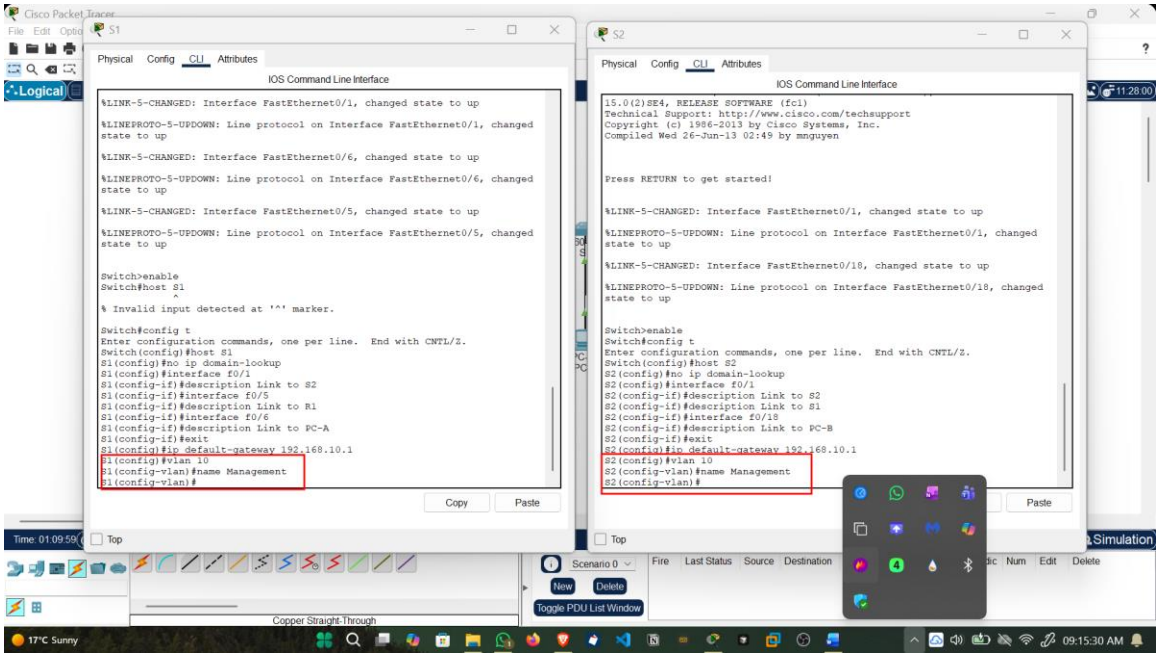
4. Set the default-gateway for the Management VLAN to 192.168.10.1 on both switches.



6.2 Part 2: Configure VLANs on Switches.

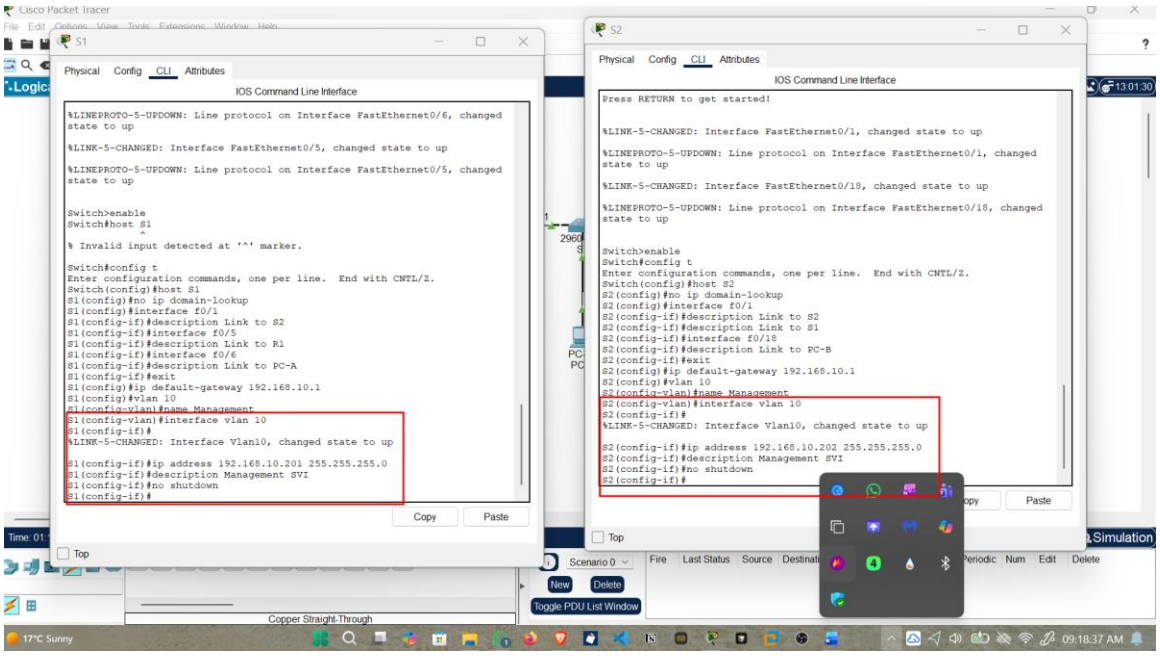
6.2.1 Step 1: Configure VLAN 10.

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

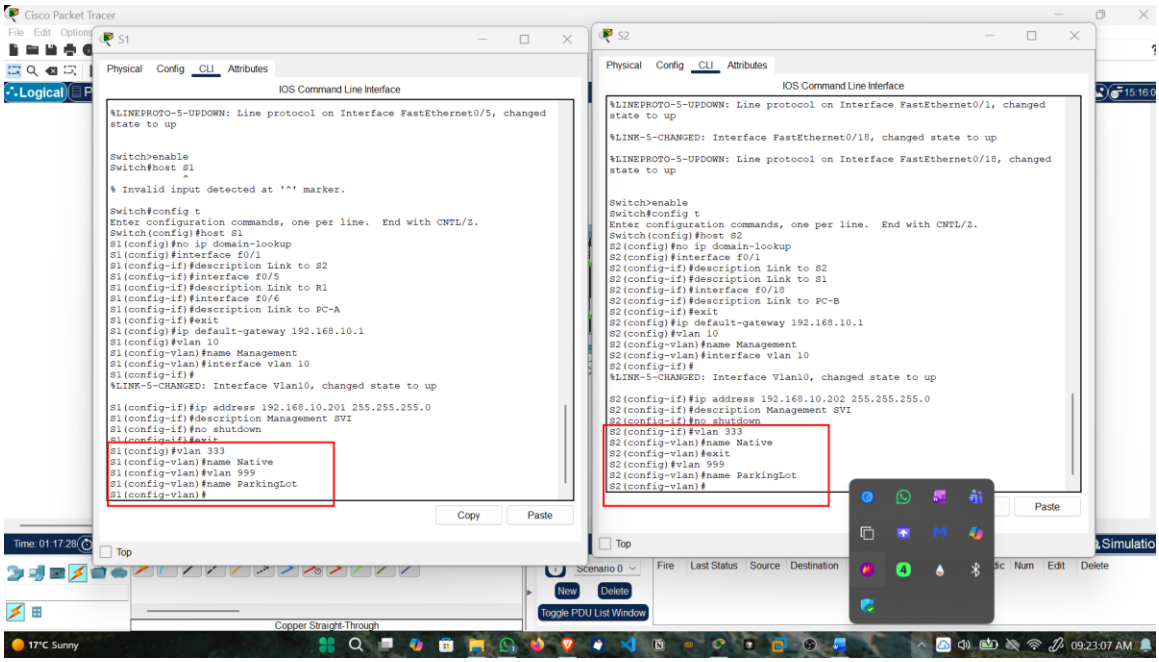


6.2.2 Step 2: Configure the SVI for VLAN 10.

1. 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.



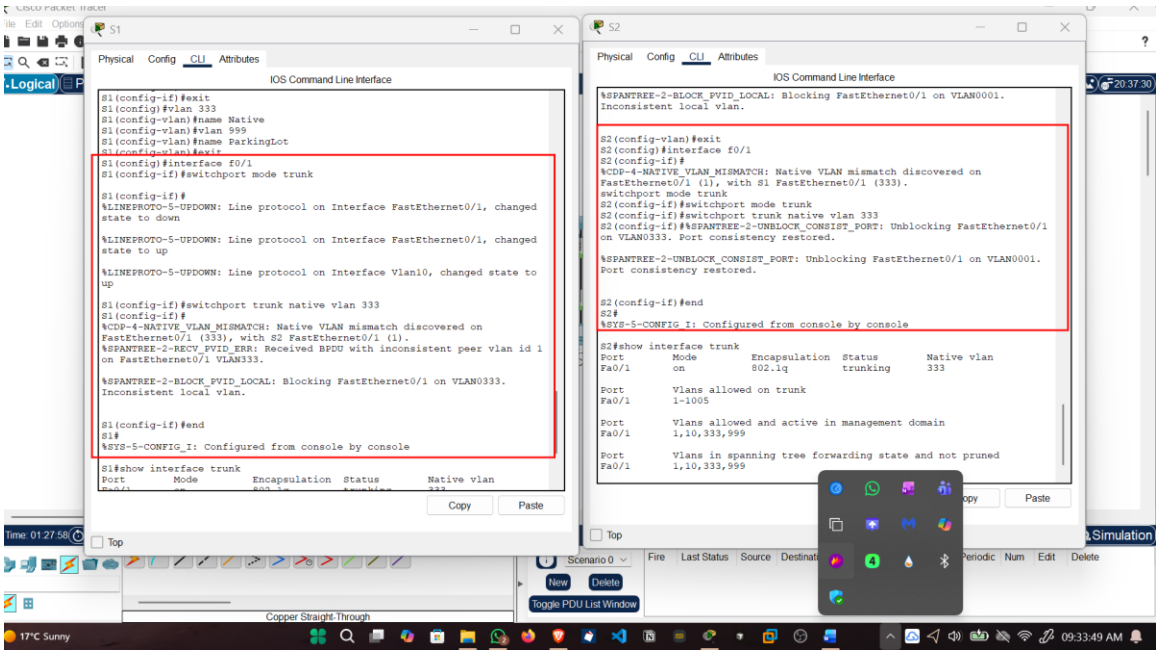
6.2.3 Step 3: Configure VLAN 333 with the name Native on S1 and S2 and VLAN 999 with the name ParkingLot on S1 and S2.



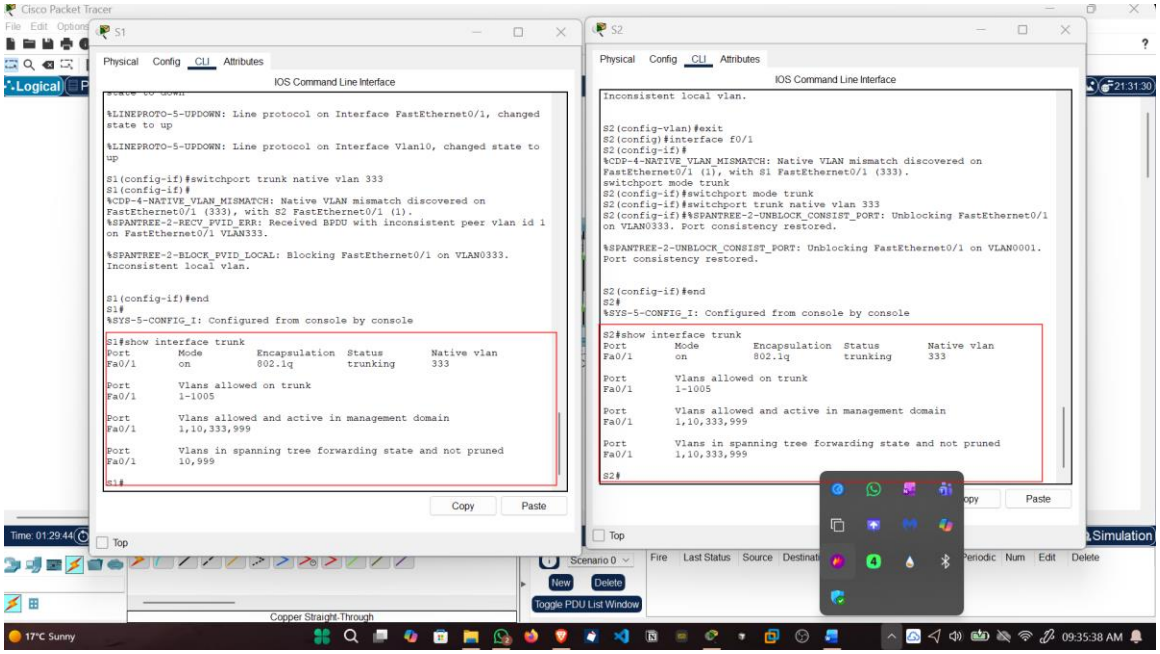
6.3 Part 3: Configure Switch Security.

6.3.1 Step 1: Implement 802.1Q trunking.

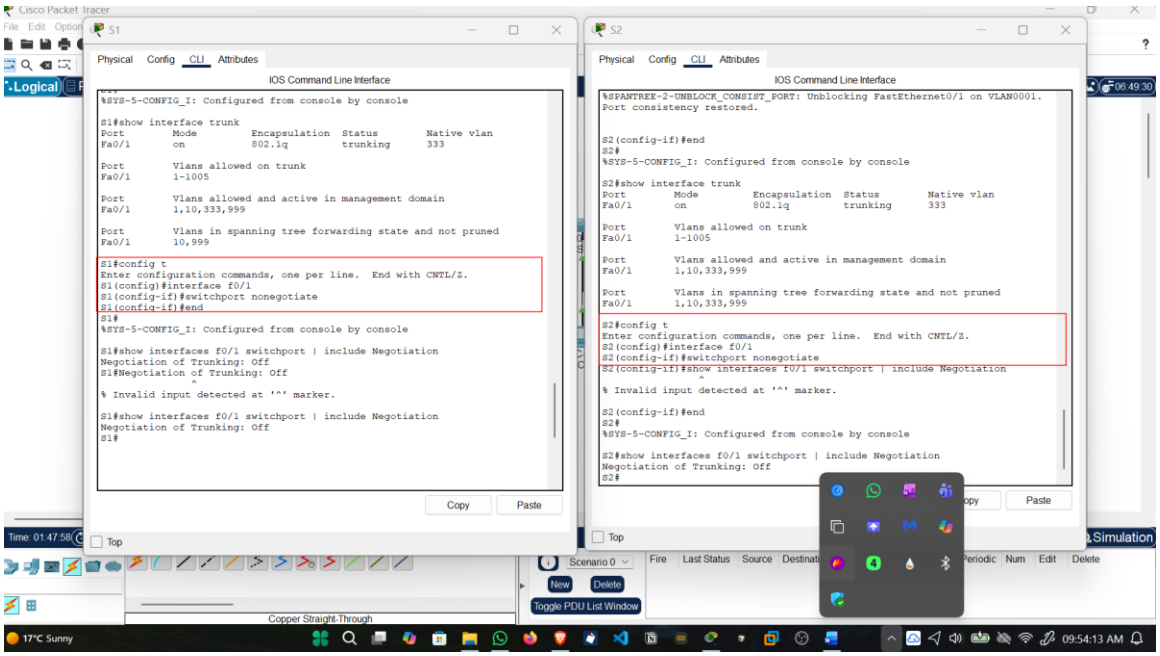
1. On both switches, configure trunking on F0/1 to use VLAN 333 as the native VLAN.



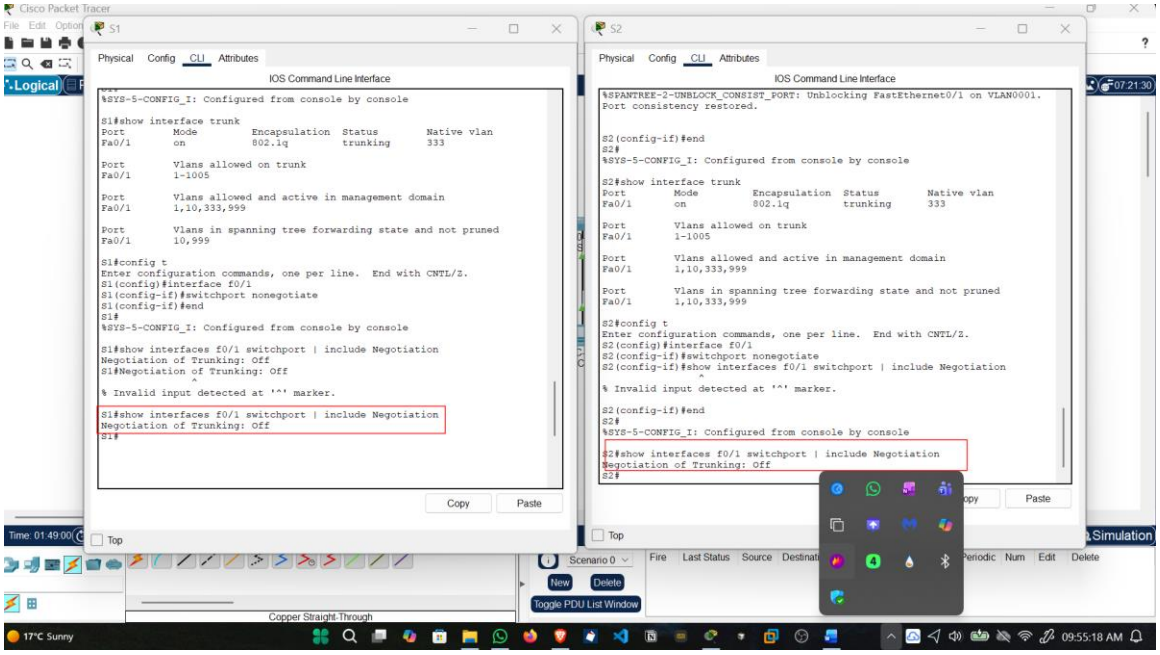
2. Verify that trunking is configured on both switches.



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

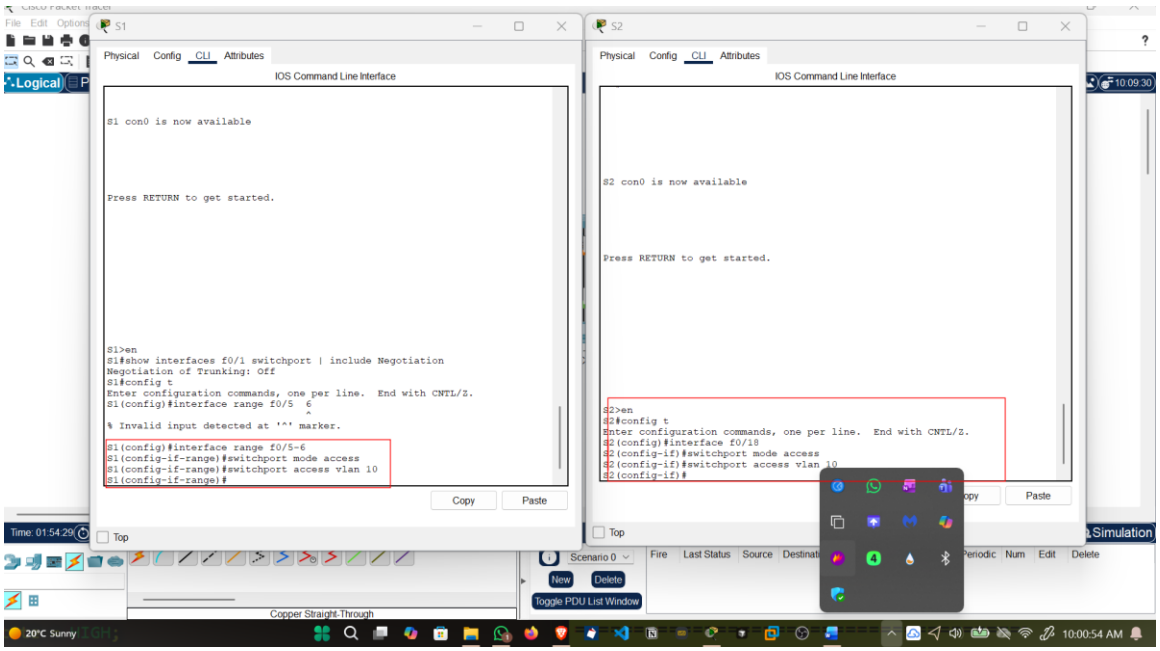


4. Verify with the show interfaces command.

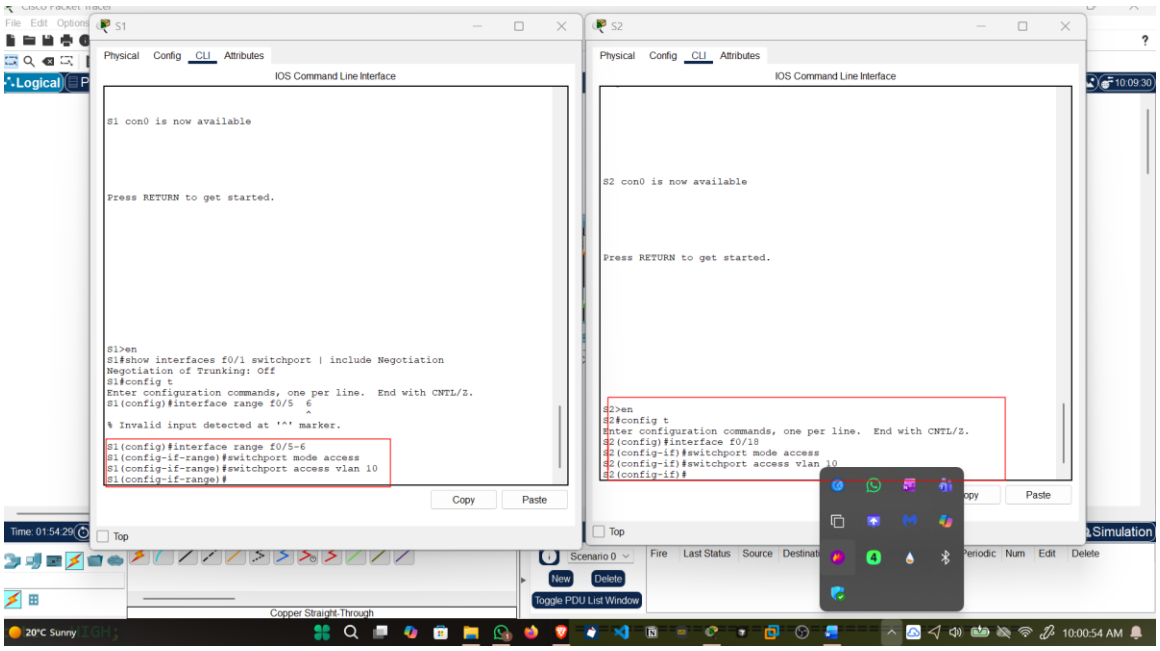


6.3.2 Step 2: Configure access ports.

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

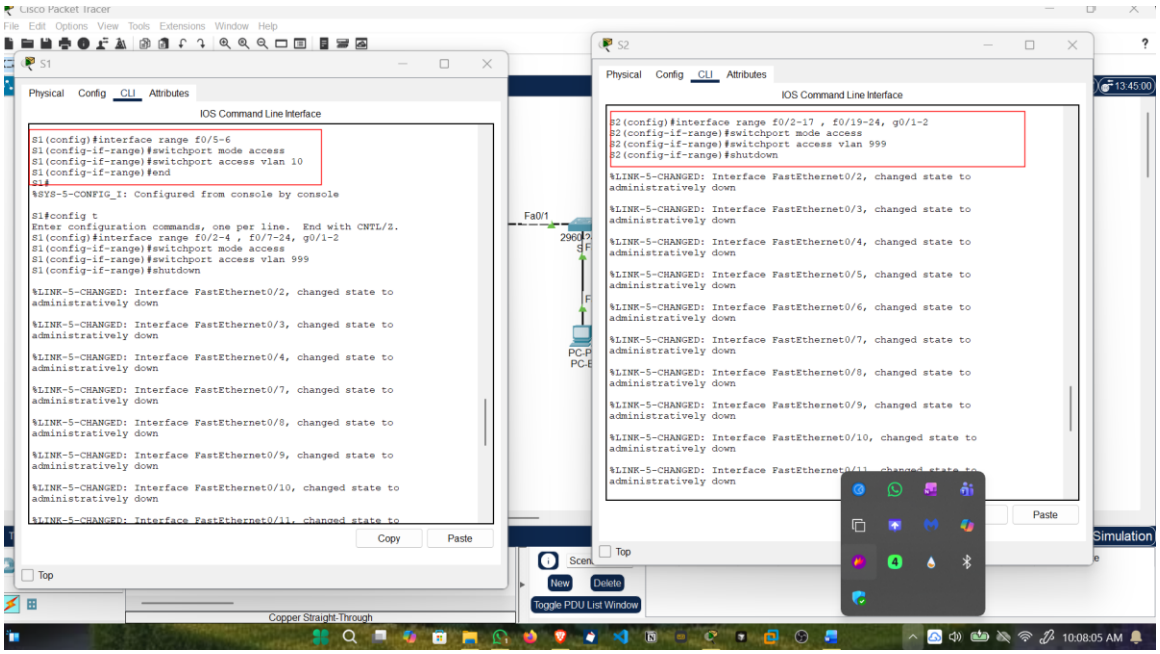


2. On S2, configure F0/18 as an access port that is associated with VLAN 10.

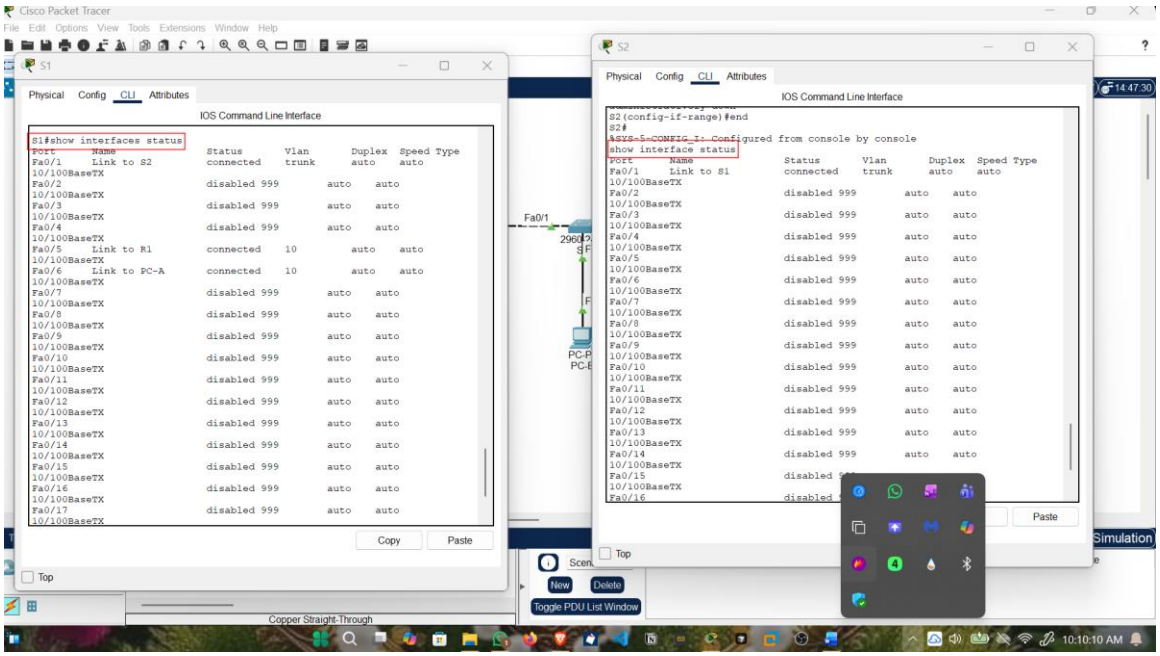


6.3.3 Step 3: Secure and disable unused switchports.

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

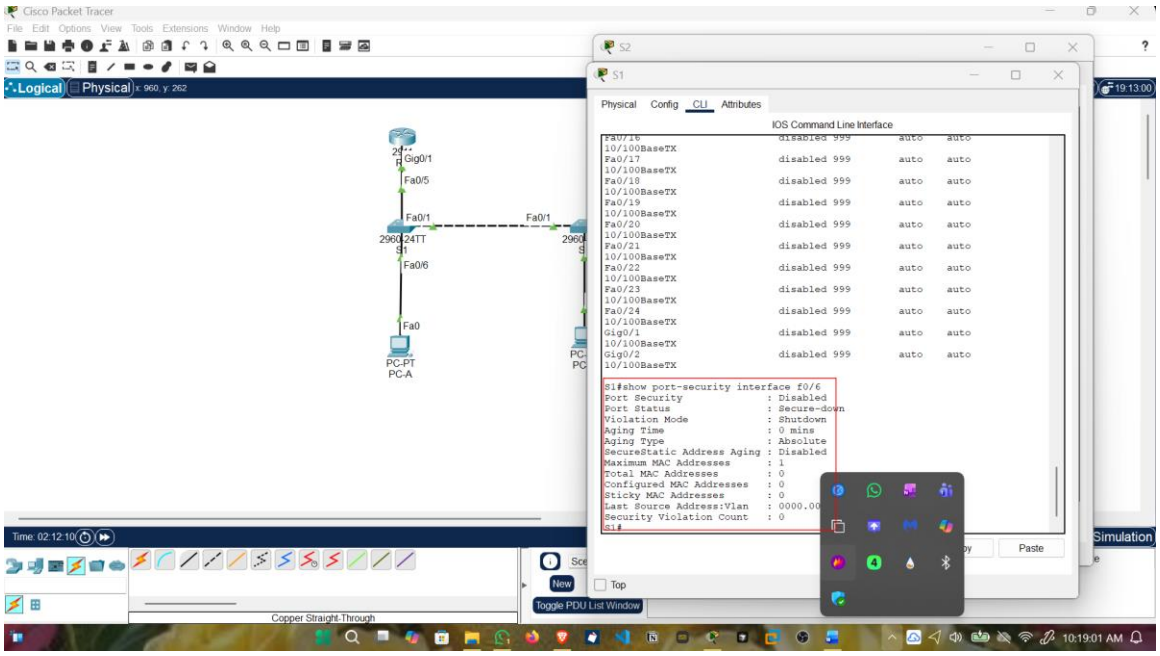


2. Verify that unused ports are disabled and associated with VLAN 999 by issuing the show command.

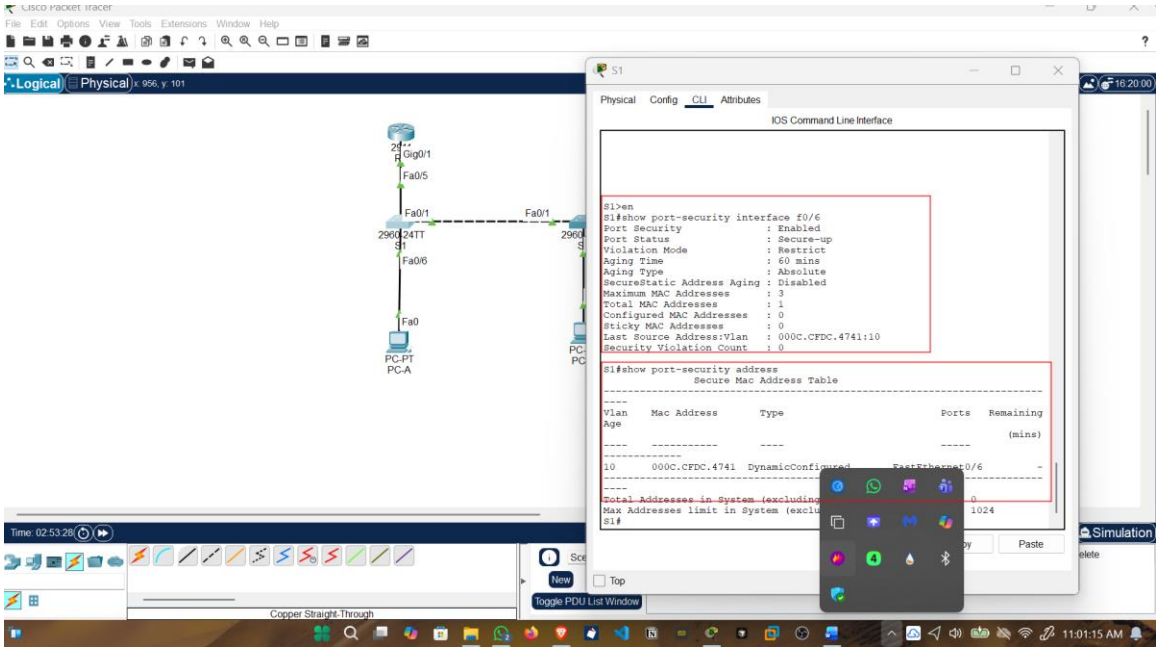


6.3.4 Step 4: Document and implement port security features.

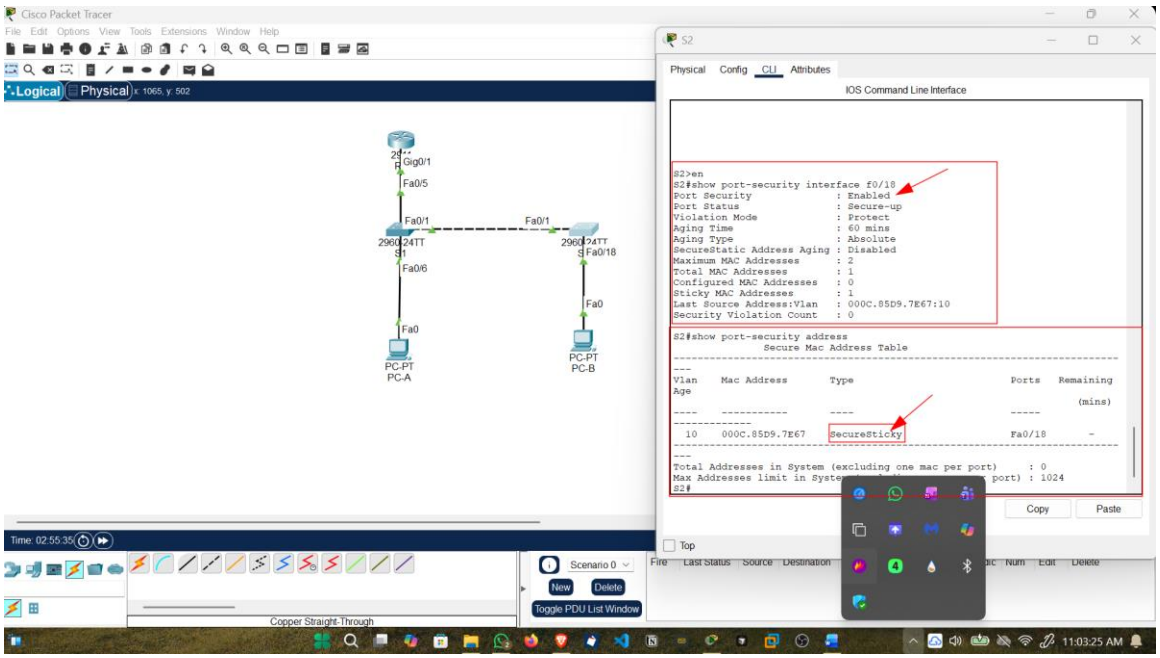
1. On S1, issue the show port-security interface f0/6 command to display the default port security settings for interface F0/6.



2. On S1, enable port security on F0/6 with the following settings:
    a. Maximum number of MAC addresses: 3
    b. Violation type: restrict
    c. Aging time: 60 min
    d. Aging type: inactivity
3. Verify port security on S1 F0/6.

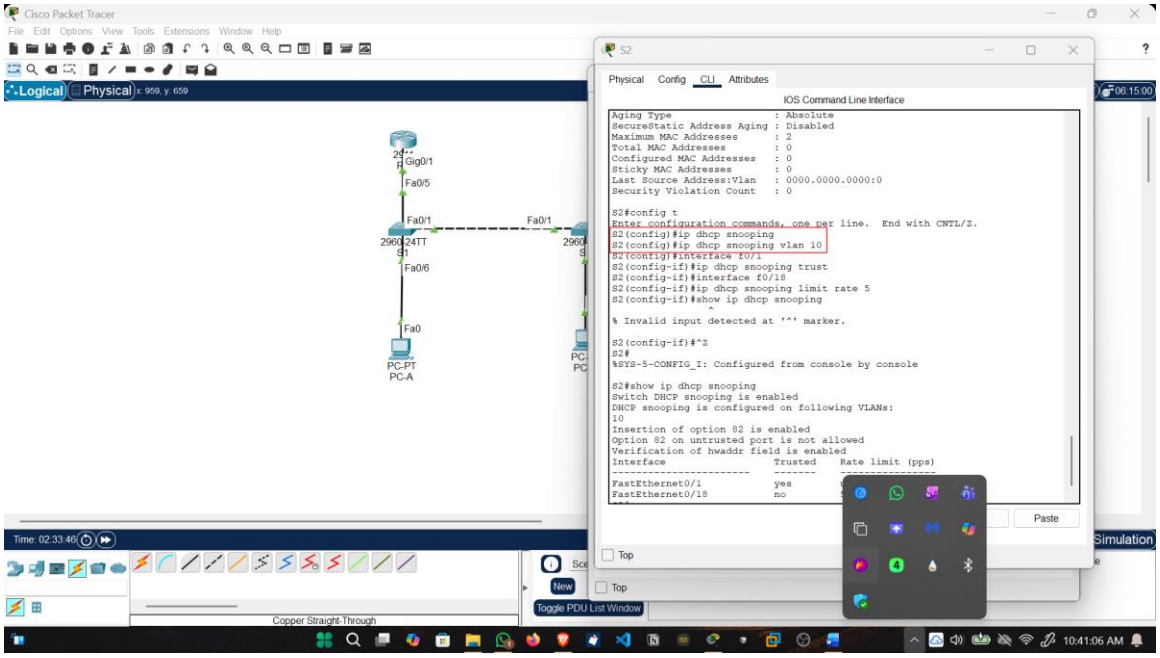


4. Enable port security for F0/18 on S2. Configure the port to add MAC addresses learned on the port automatically to the running configuration.
5. Configure the following port security settings on S2 F/18:
    a. Maximum number of MAC addresses: 2
    b. Violation type: Protect
    c. Aging time: 60 min
6. Verify port security on S2 F0/18.

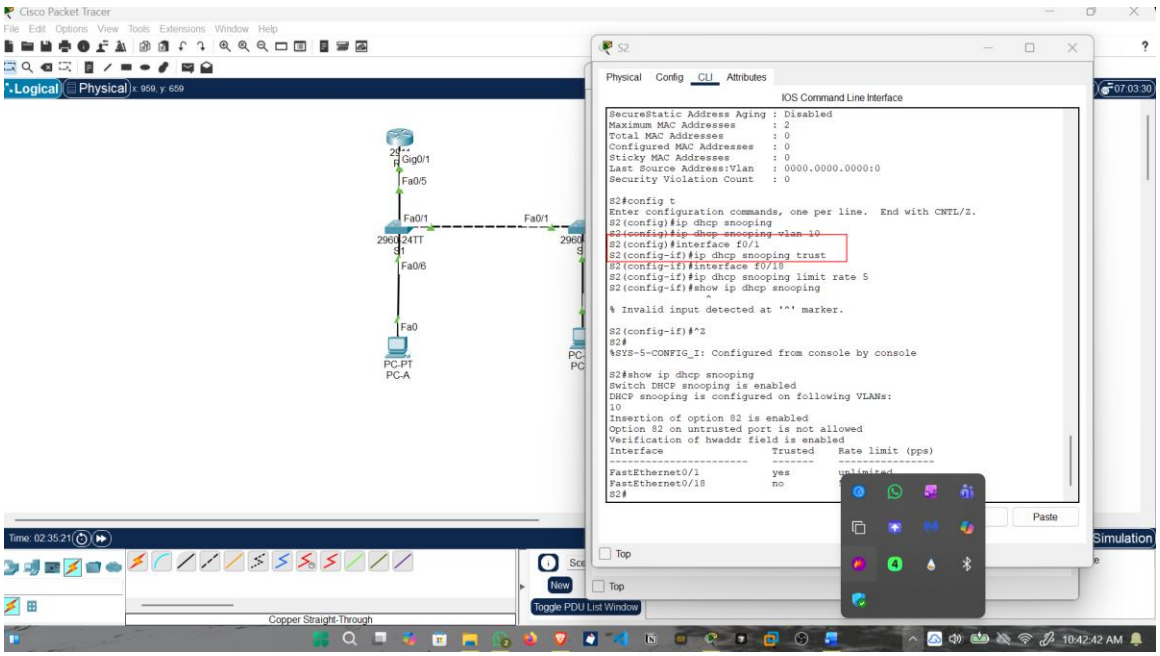


6.3.5 Step 5: Implement DHCP snooping security.

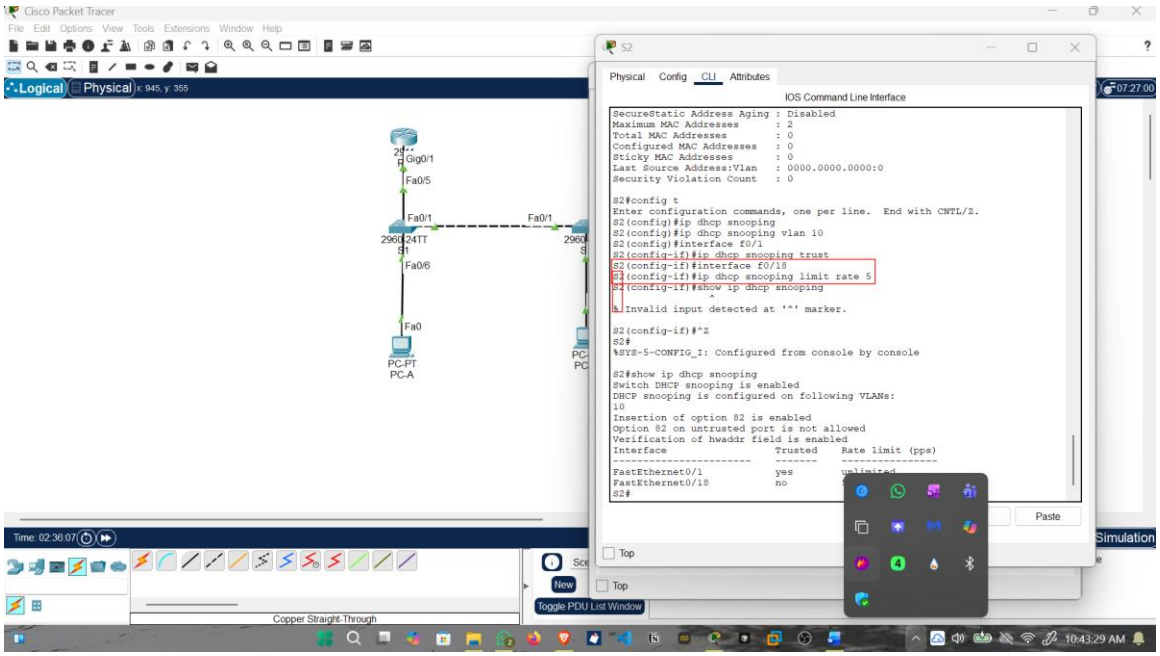
1. On S2, enable DHCP snooping and configure DHCP snooping on VLAN 10.



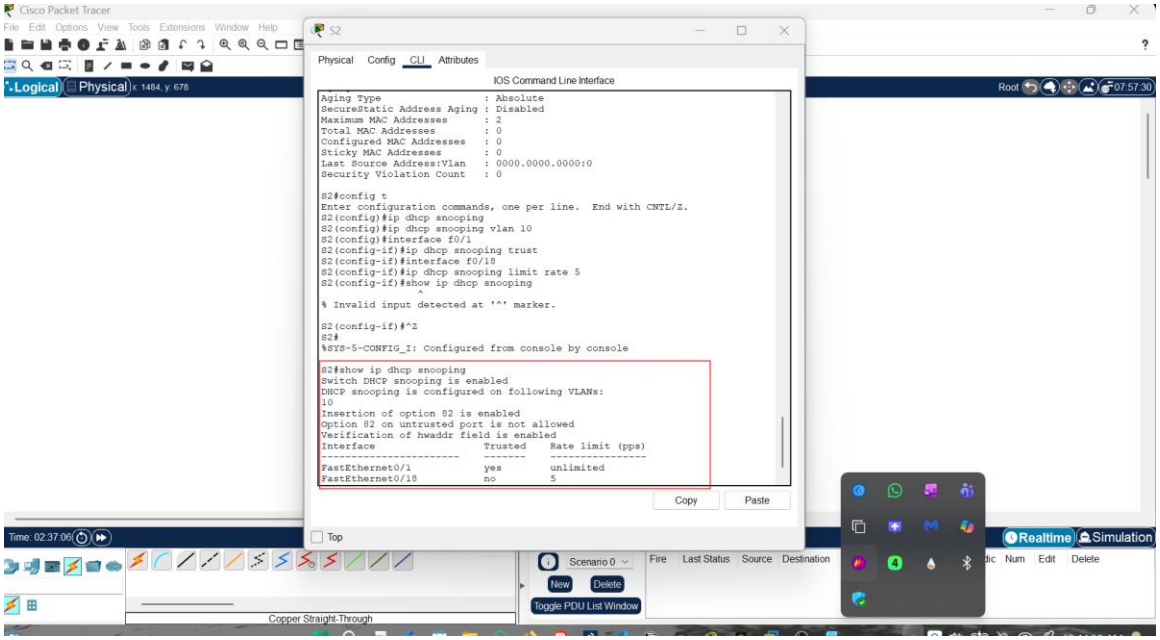
2. Configure the trunk port on S2 as a trusted port.



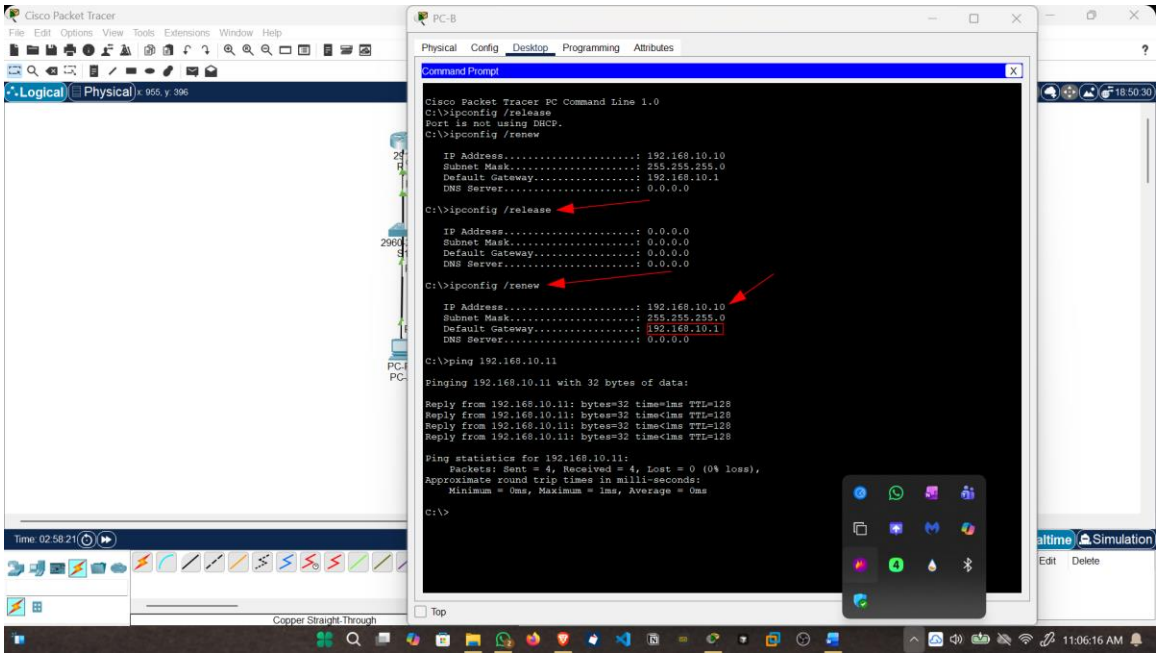
3. Limit the untrusted port, F18 on S2, to five DHCP packets per second.



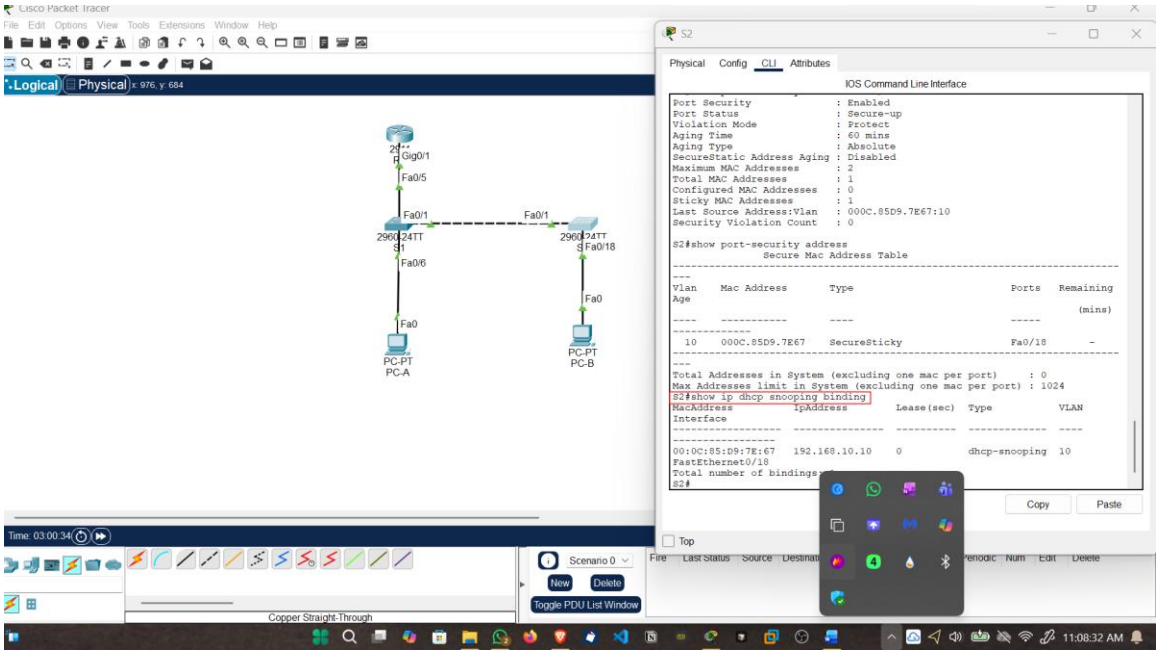
4. Verify DHCP Snooping on S2.



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

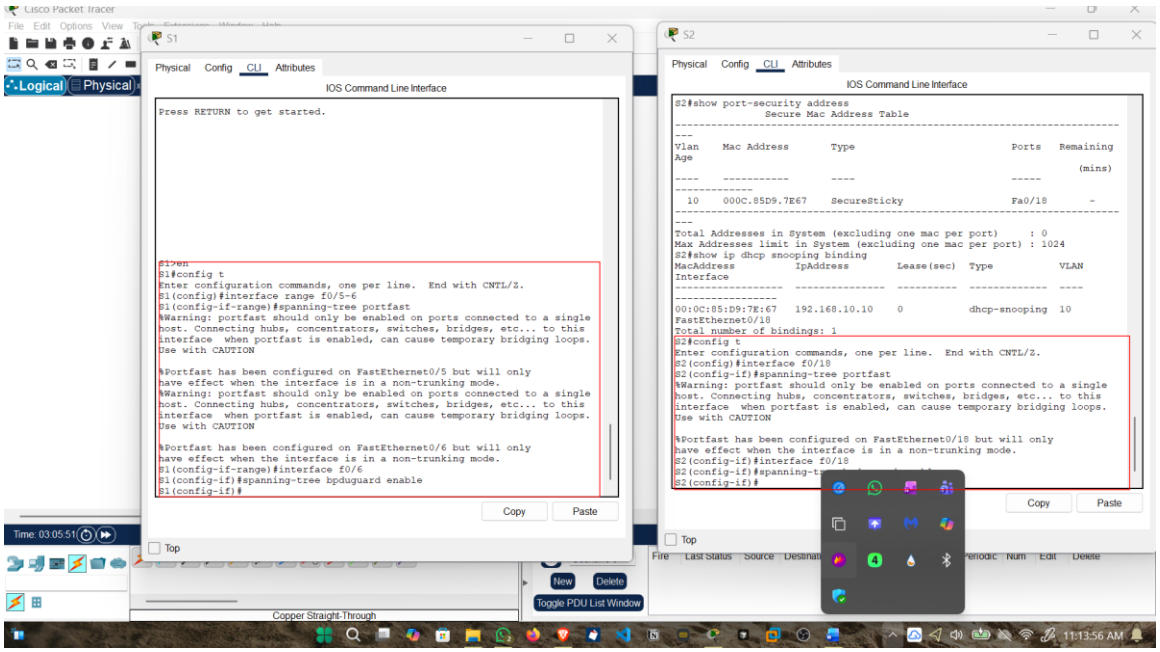


6. Verify the DHCP snooping binding using the show ip dhcp snooping binding command.

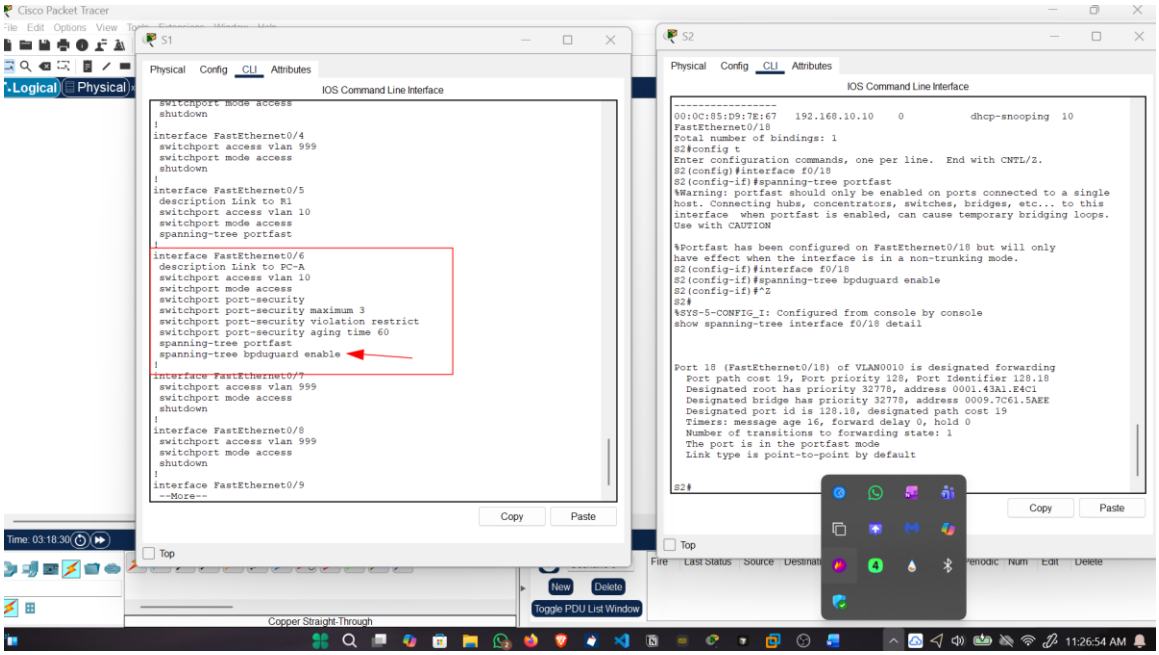


6.3.6 Step 6: Implement PortFast and BPDU guard.

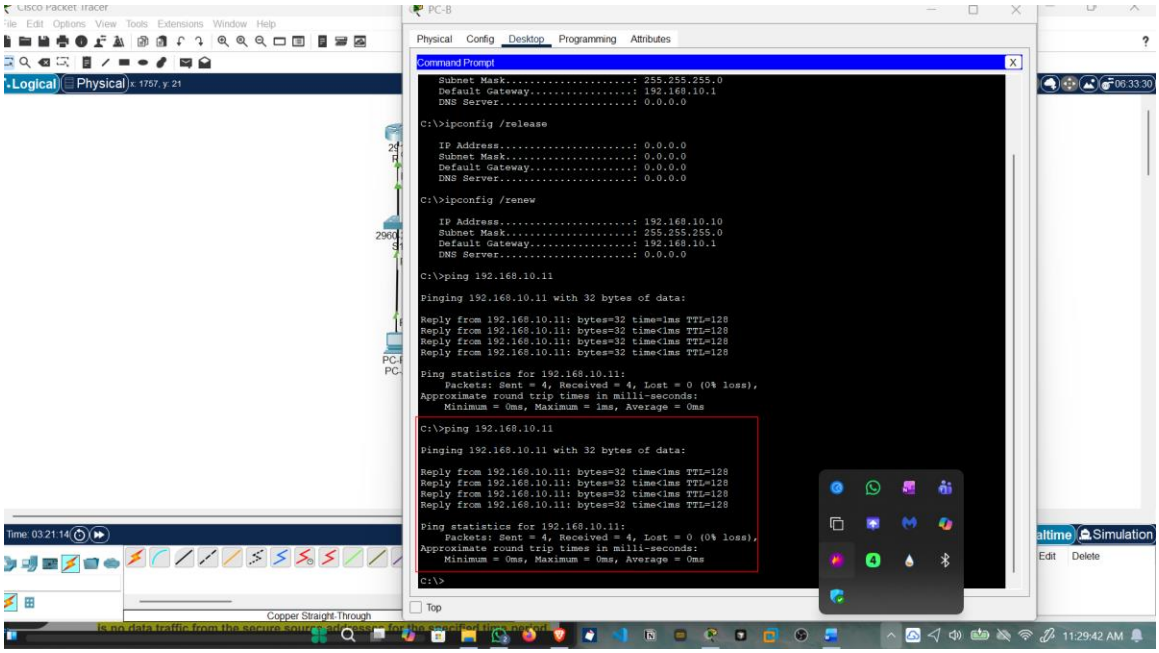
1. Configure PortFast on all the access ports that are in use on both switches.
2. Enable BPDU guard on S1 and S2 VLAN 10 access ports connected to PC-A and PC-B.



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



6.3.7 Step 7: Verify end-to-end connectivity.



6.4 Answers to Questions

1. Why was there no remaining age timer with sticky learning?

   Sticky MAC addresses were saved in the running configuration and treated as permanent secure entries, so they did not age out like dynamic MAC addresses. Therefore, no remaining age timer was displayed.

2. Why would PC-B never get a DHCP IP address after loading the config?

   Port security allowed only two sticky MAC addresses on Fa0/18. Any new MAC address traffic, including DHCP requests, was dropped under **protect** mode, preventing PC-B from completing DHCP and obtaining an IP address.

3. Difference between absolute aging and inactivity aging?

   ✓ **Absolute aging:** Secure MAC addresses were removed after a fixed time, regardless of activity.

- ✓ **Inactivity aging:** Secure MAC addresses were removed only if no traffic was seen from them during the timer period.

7 CONCLUSION

The implementation of VLAN segmentation and Layer 2 security mechanisms enhanced both the organization and protection of the switched network environment. Management VLANs and SVIs provided secure remote administrative access, while trunking and native VLAN configuration reduced exposure to VLAN-based attacks. Security features including port security, DHCP snooping, PortFast, and BPDU Guard effectively mitigated threats such as unauthorized device connections, rogue DHCP activity, and spanning-tree manipulation. Overall, the exercise emphasized the critical role of secure switch configuration in ensuring network integrity, availability, and stable enterprise communication.

8 REFERENCES

1. Cyber Shujaa Manual Lab
2. Network Academy