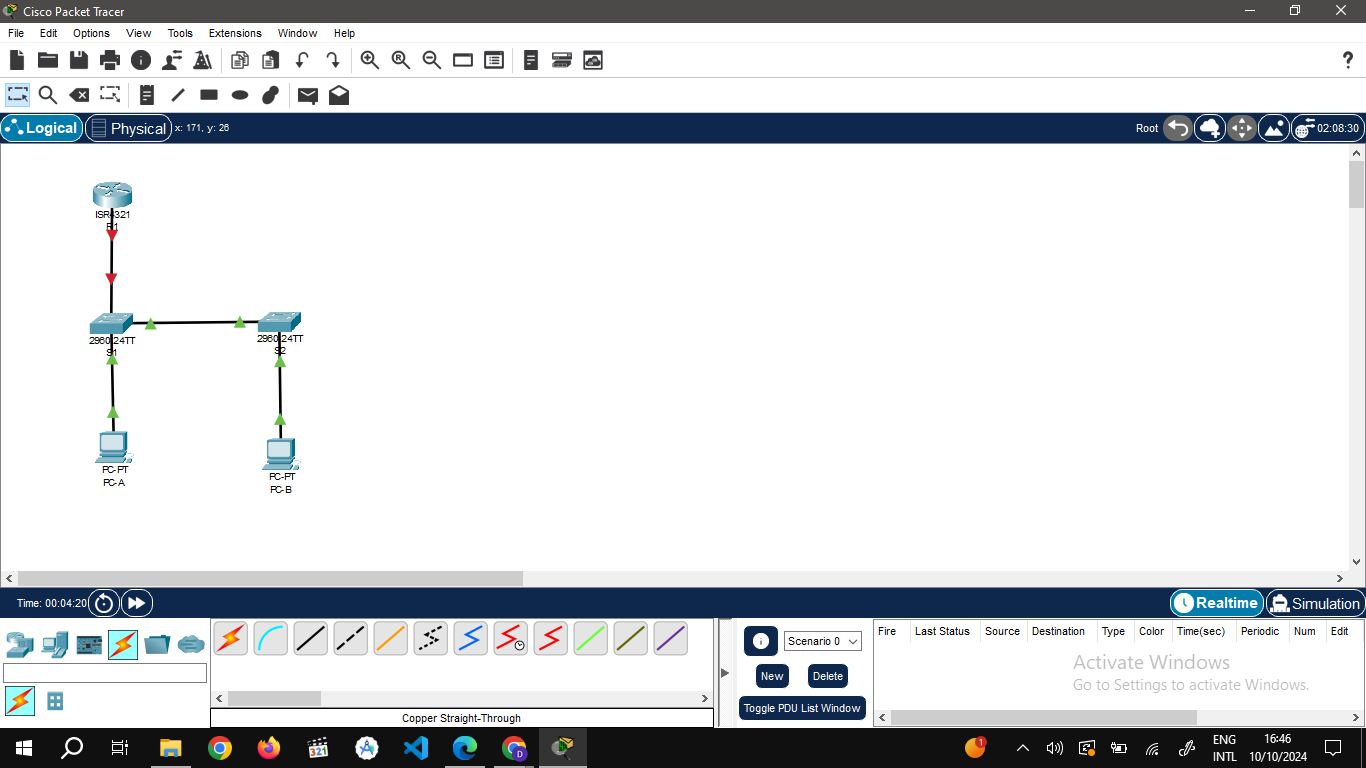
**VLANs and Secure Switch Configuration**

**Introduction.**

This activity involves configuring network devices and implementing Layer 2 security features to ensure secure and efficient communication within a network. The exercise involves setting up routers, switches, PCs, configuring VLANs, and securing unused switchports.

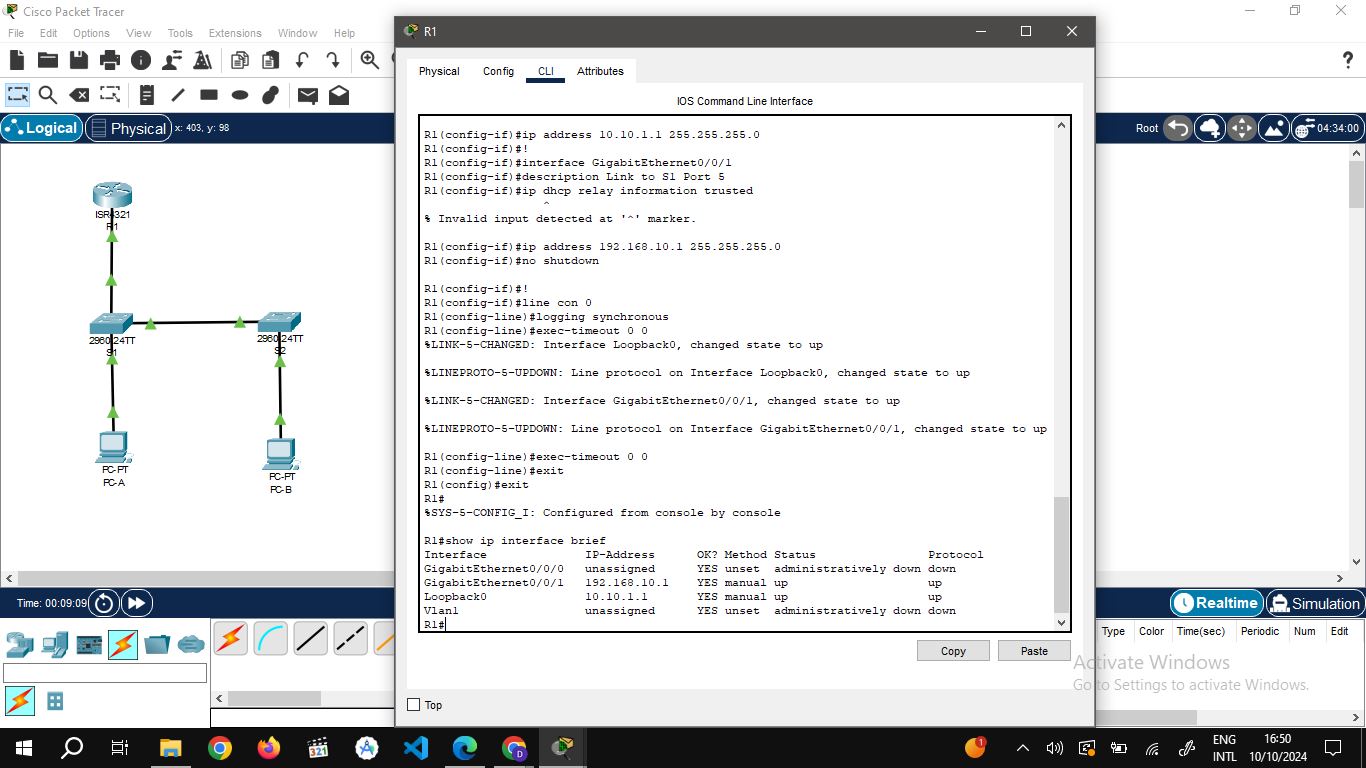
**Part 1: Configure the Network Devices.**

**Step 1: Cable the network.**

****

**Step 2: Configure R1.**

**Verify the running-configuration on R1**

****

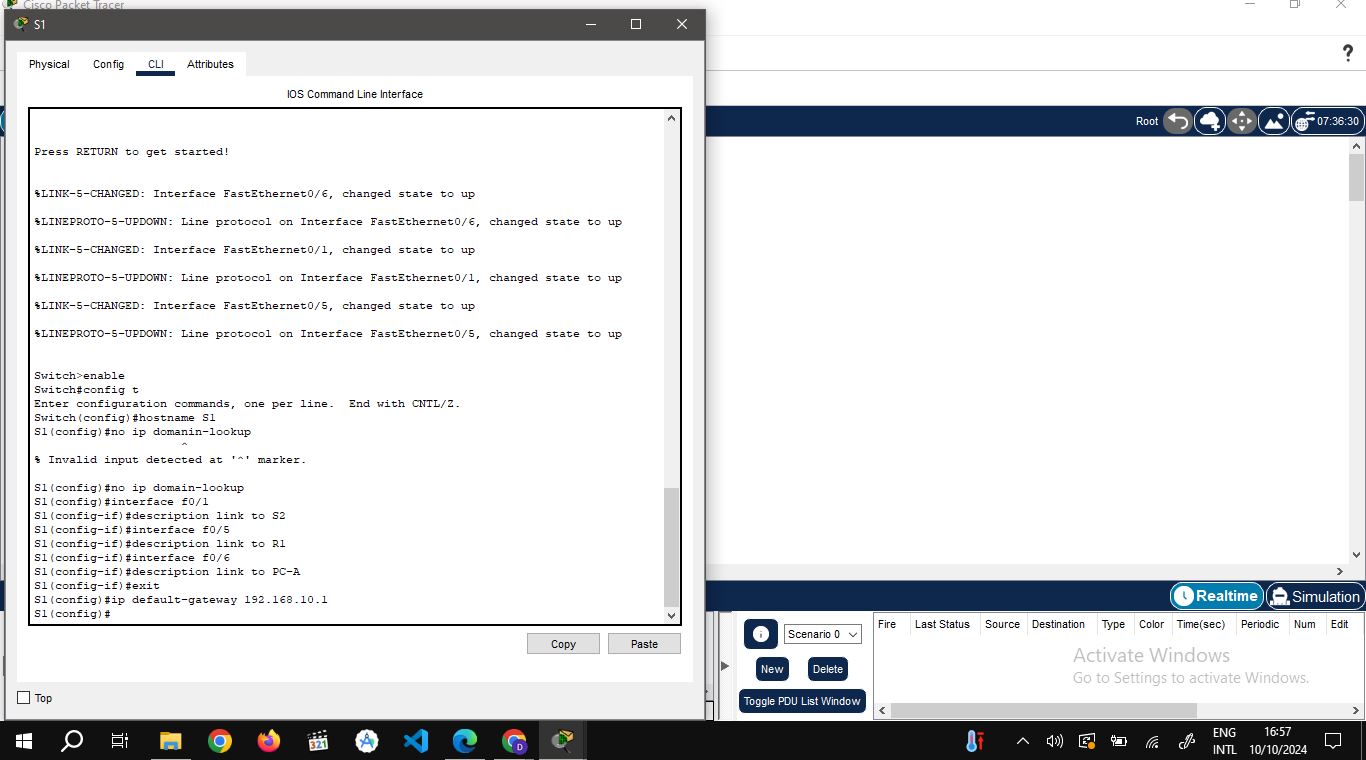
**Step 3: Configure and verify basic switch settings.**

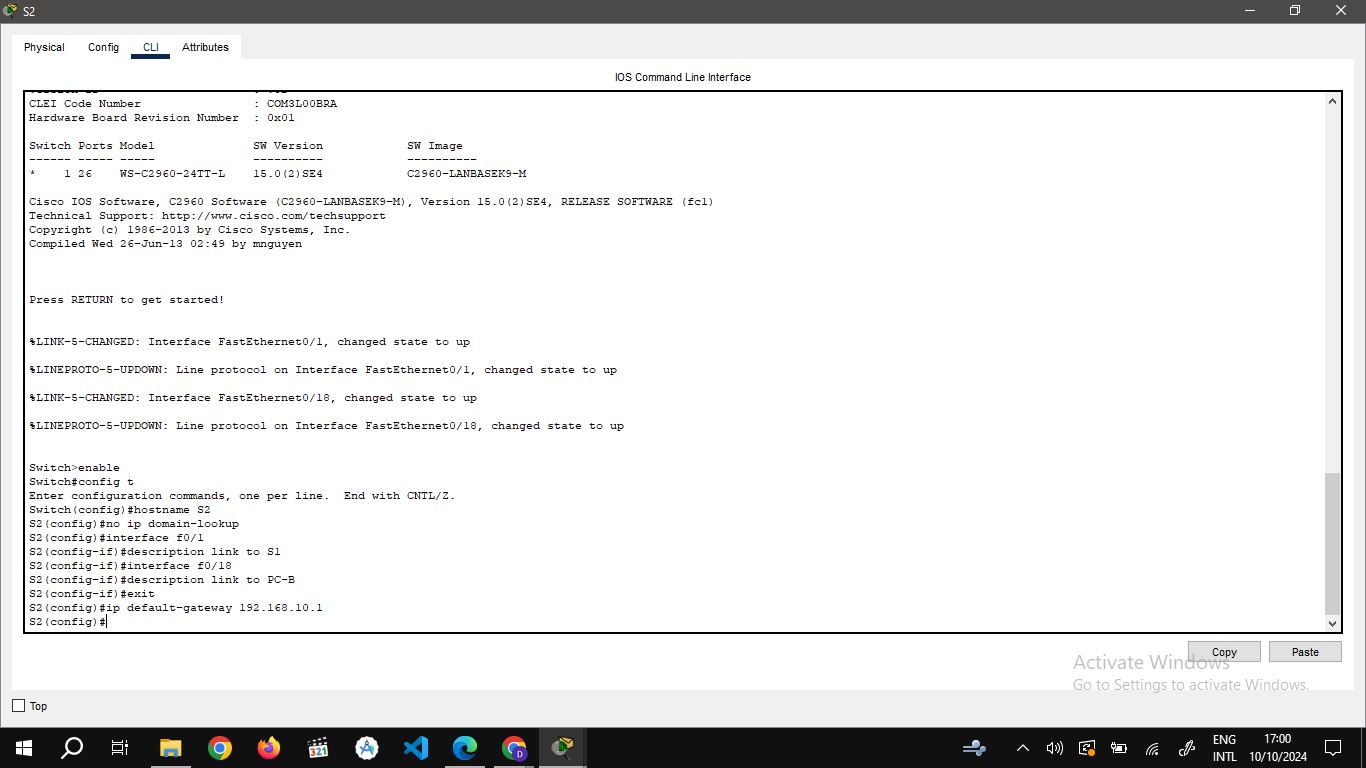
Configure the hostname for switches S1 and S2**.**

Prevent unwanted DNS lookups on both switches**.**

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

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

****

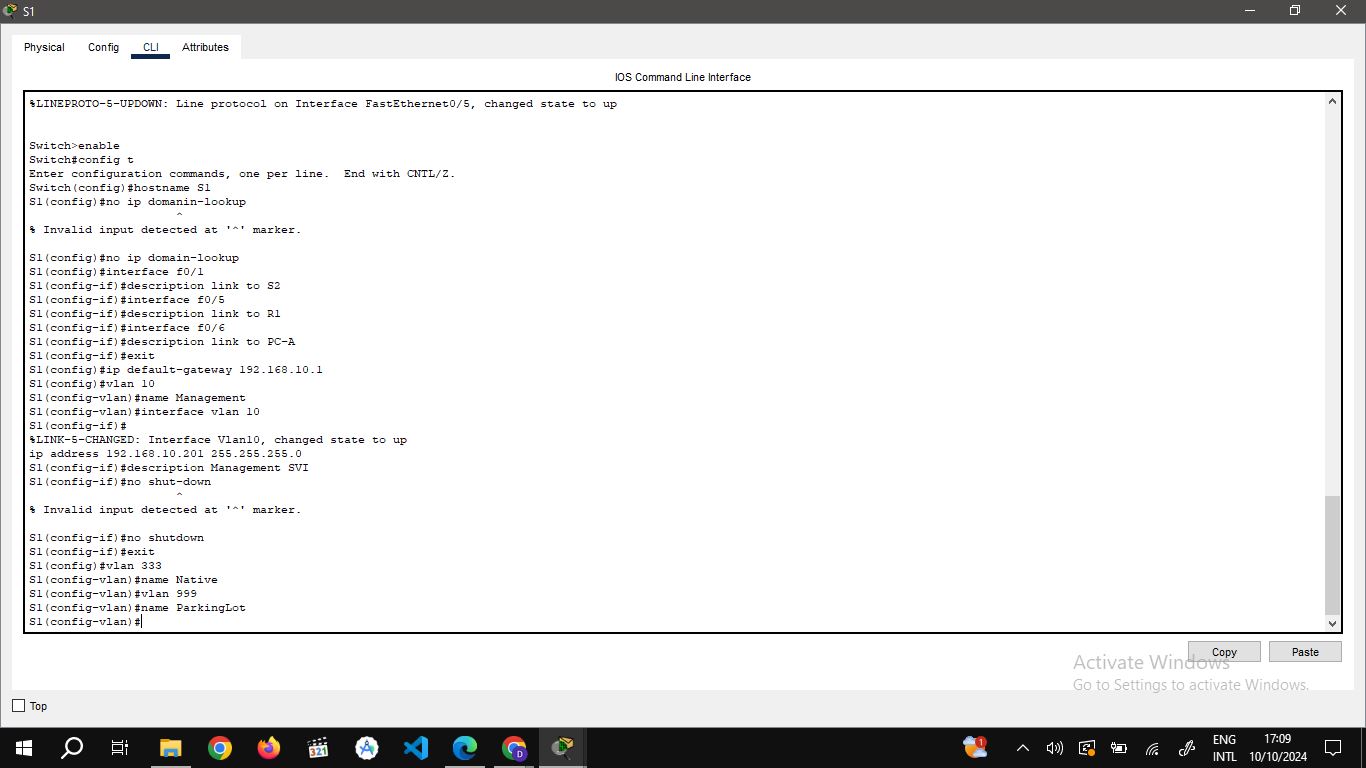
****

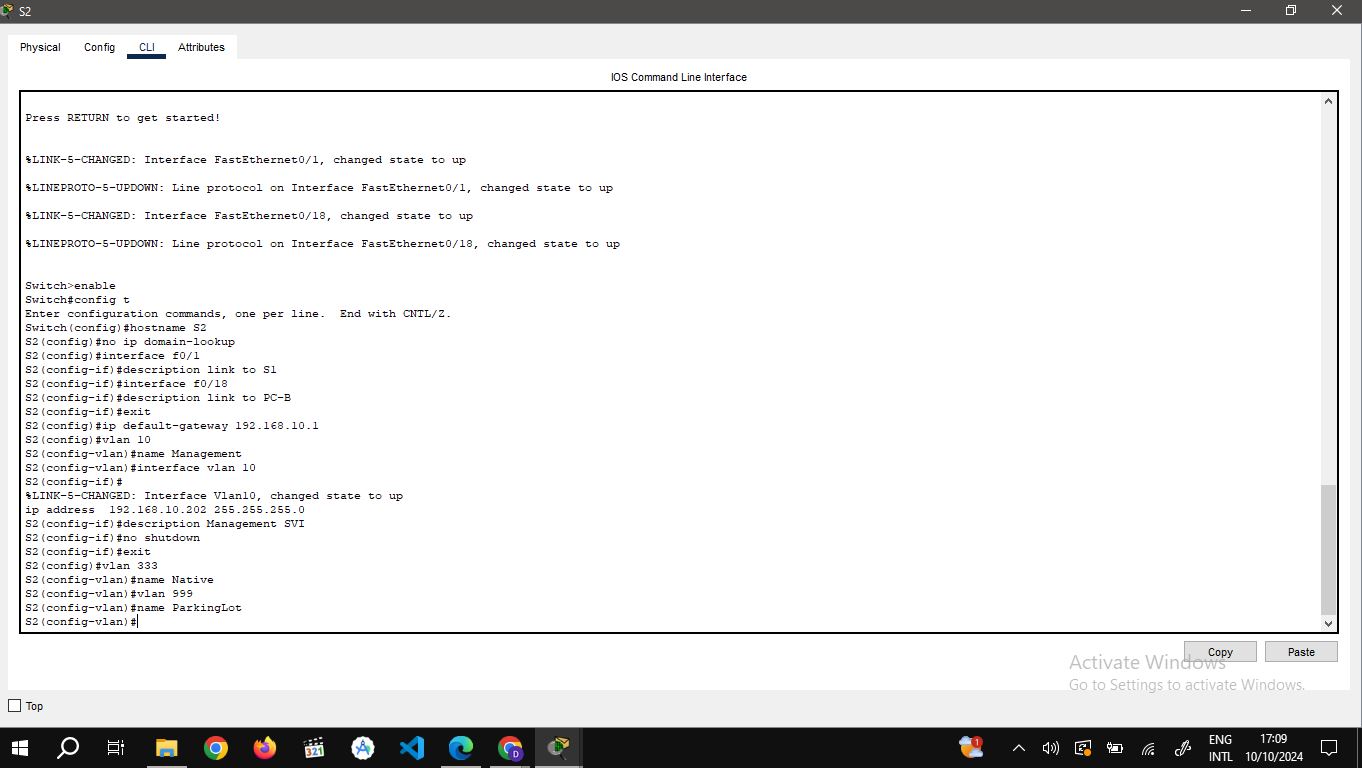
**Part 2: Configure VLANs on Switches.**

Configure VLAN 10.

Configure the SVI for VLAN 10.

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

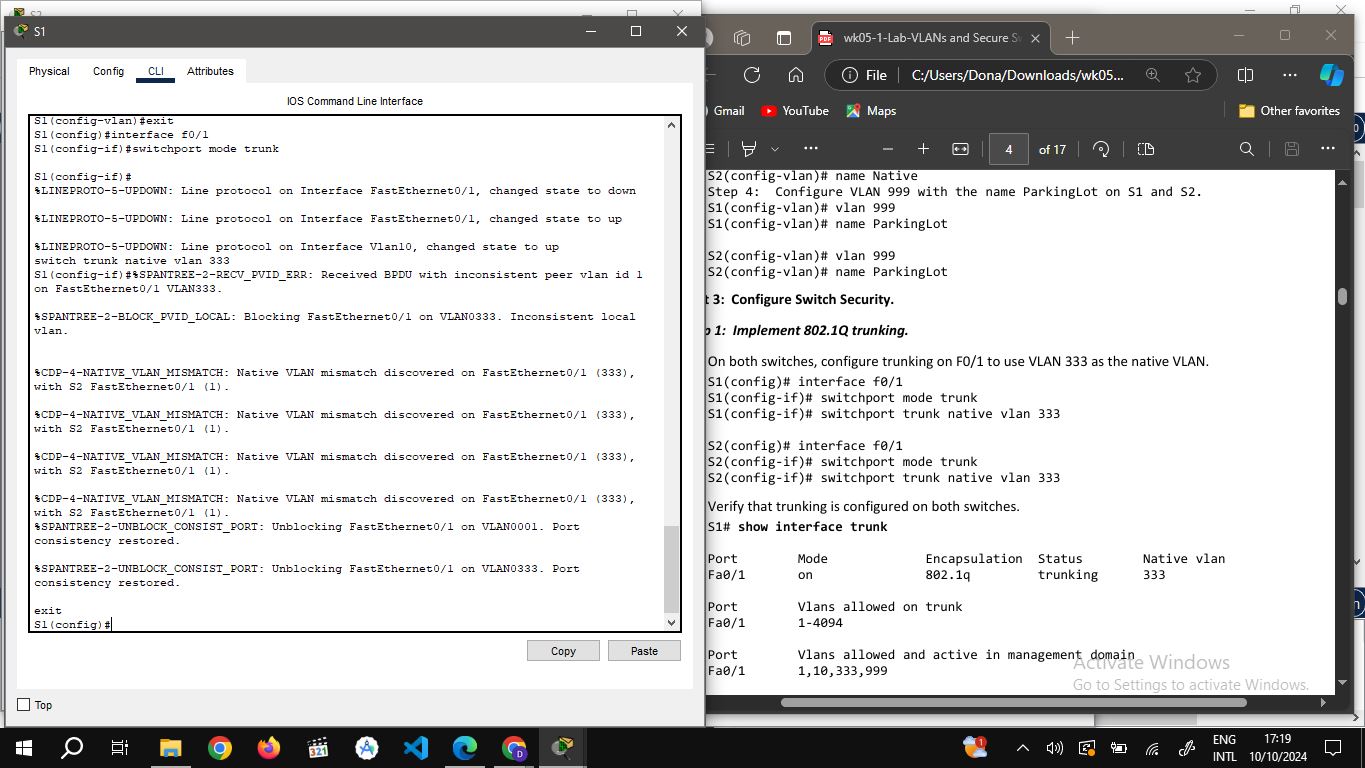
****

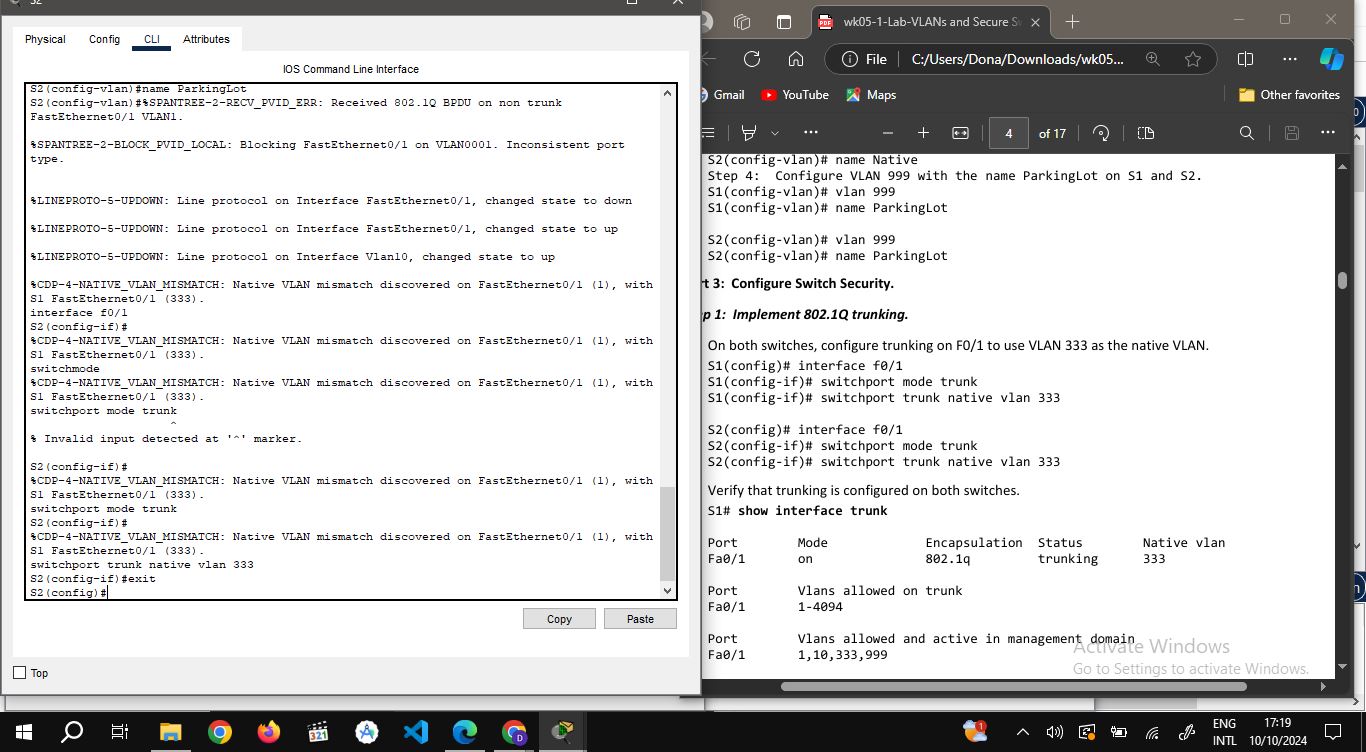
****

**Part 3: Configure Switch Security.**

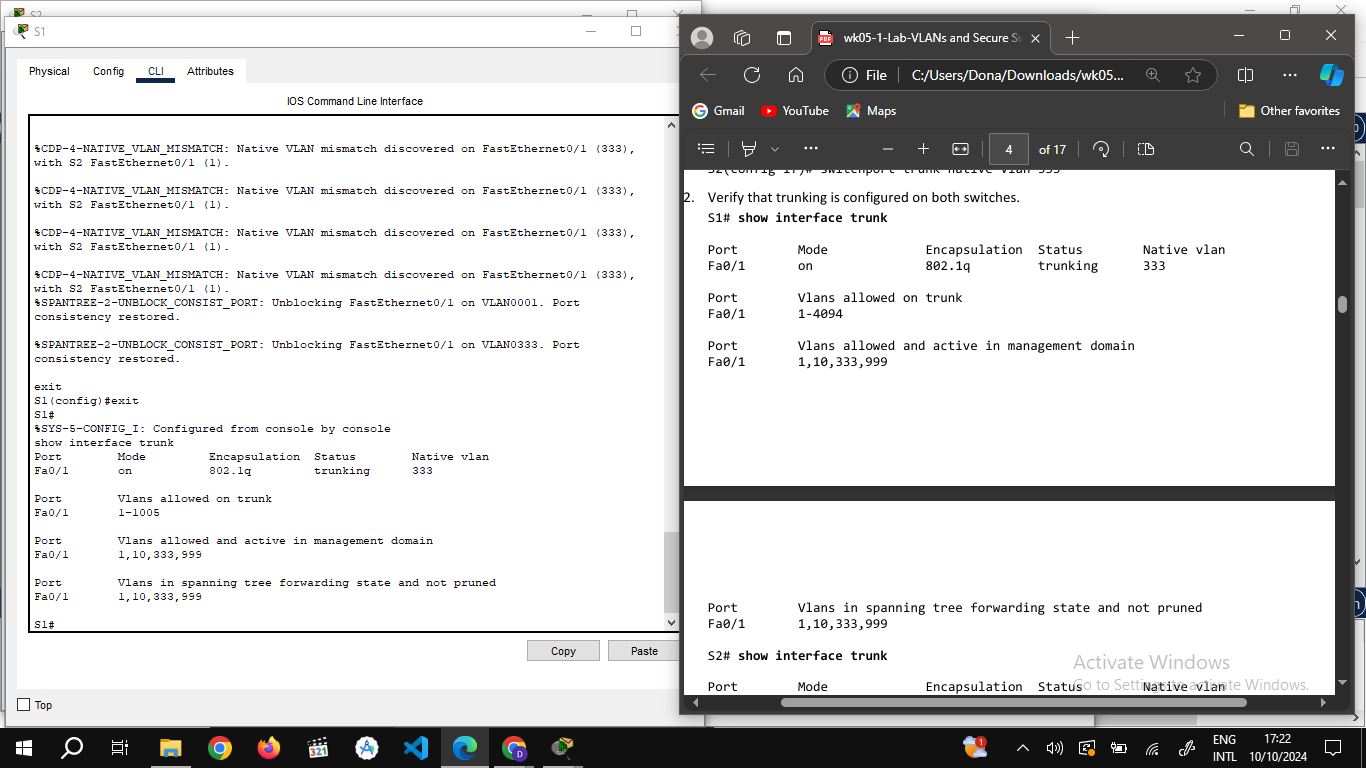
**Step 1: Implement 802.1Q trunking.**

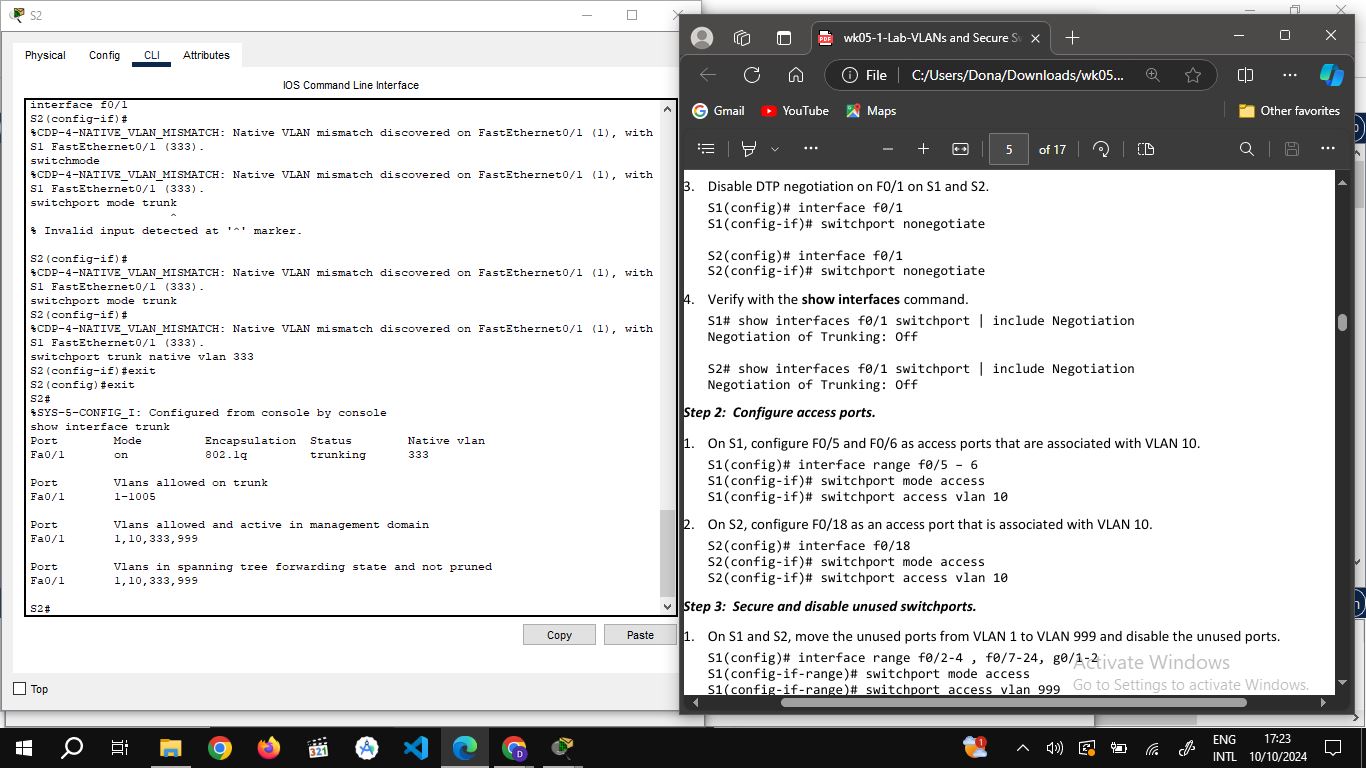
1.On both switches, configure trunking on F0/1 to use VLAN 333 as the native VLAN.

****

****

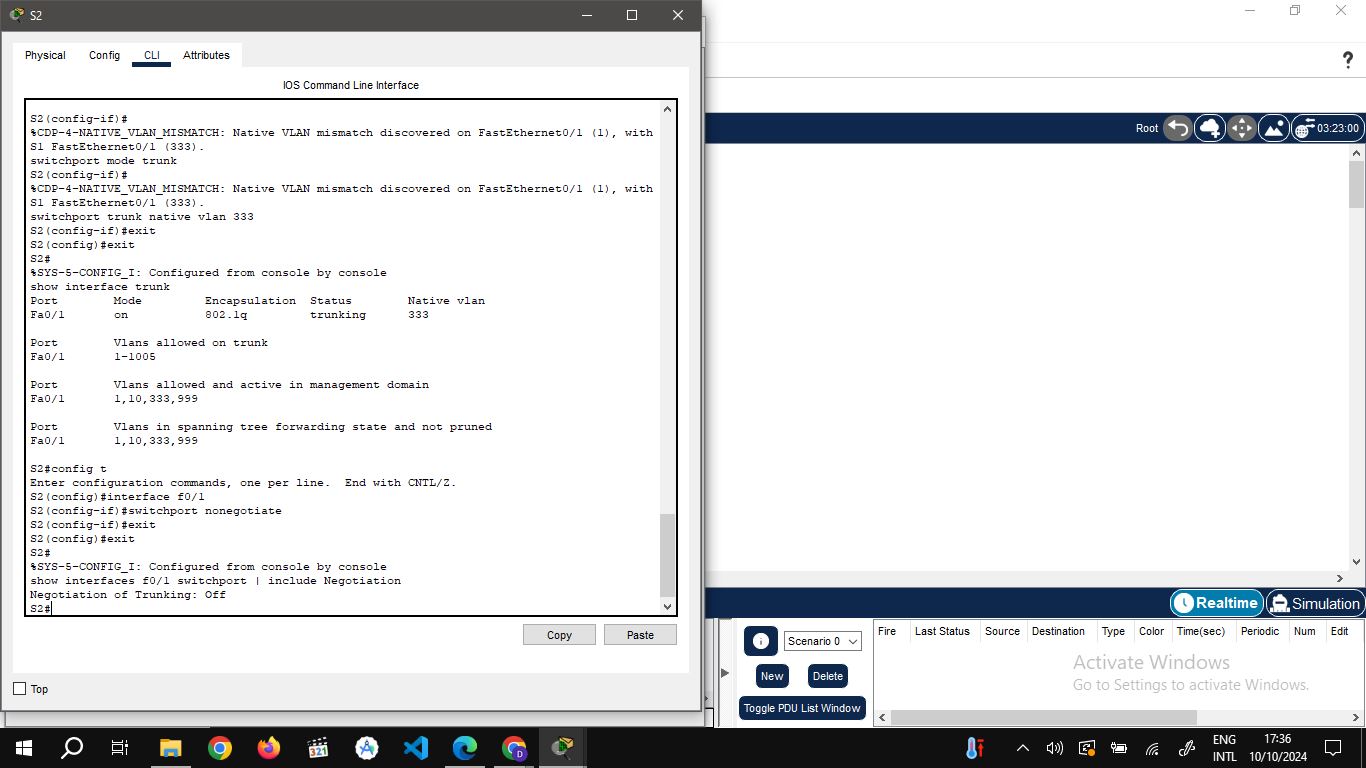
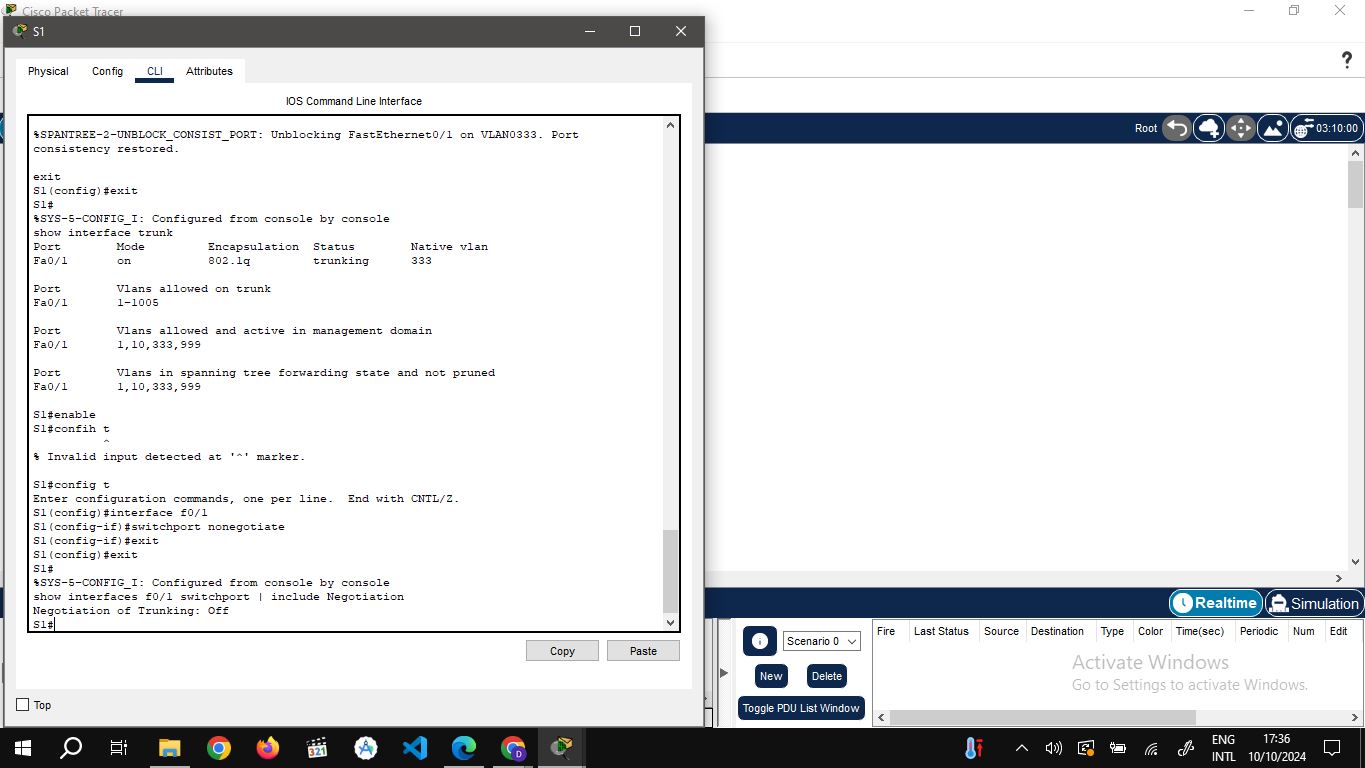
2. Verify that trunking is configured on both switches.





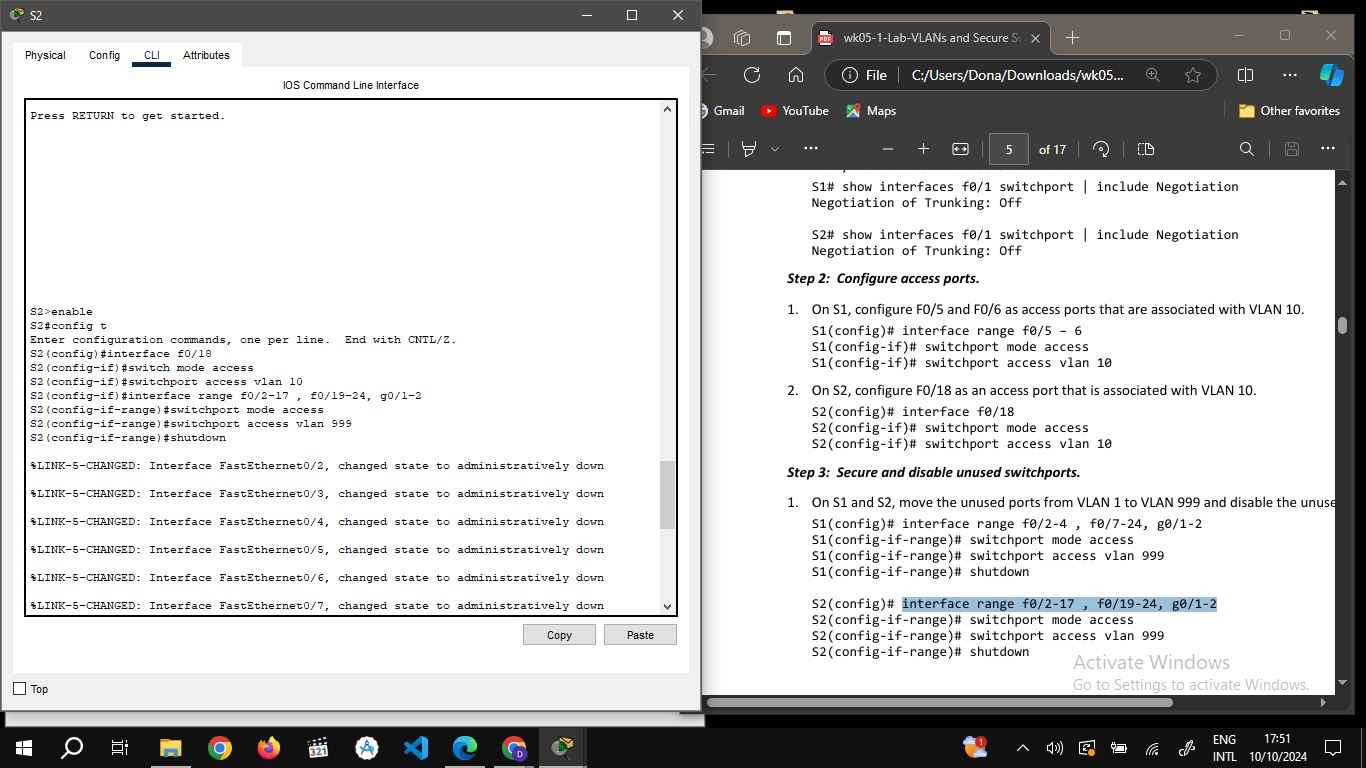
3.Disable DTP negotiation on F0/1 on S1 and S2.

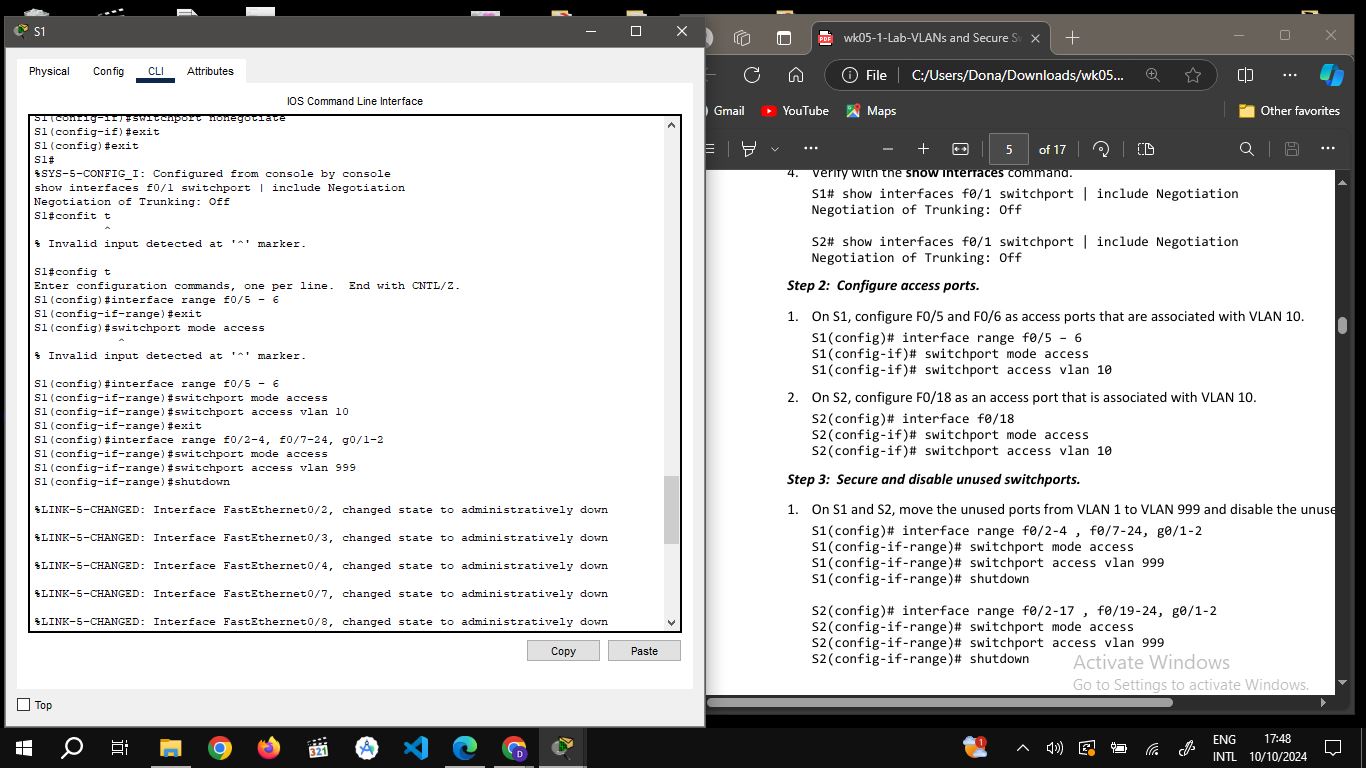
4. Verify with the show interfaces command.



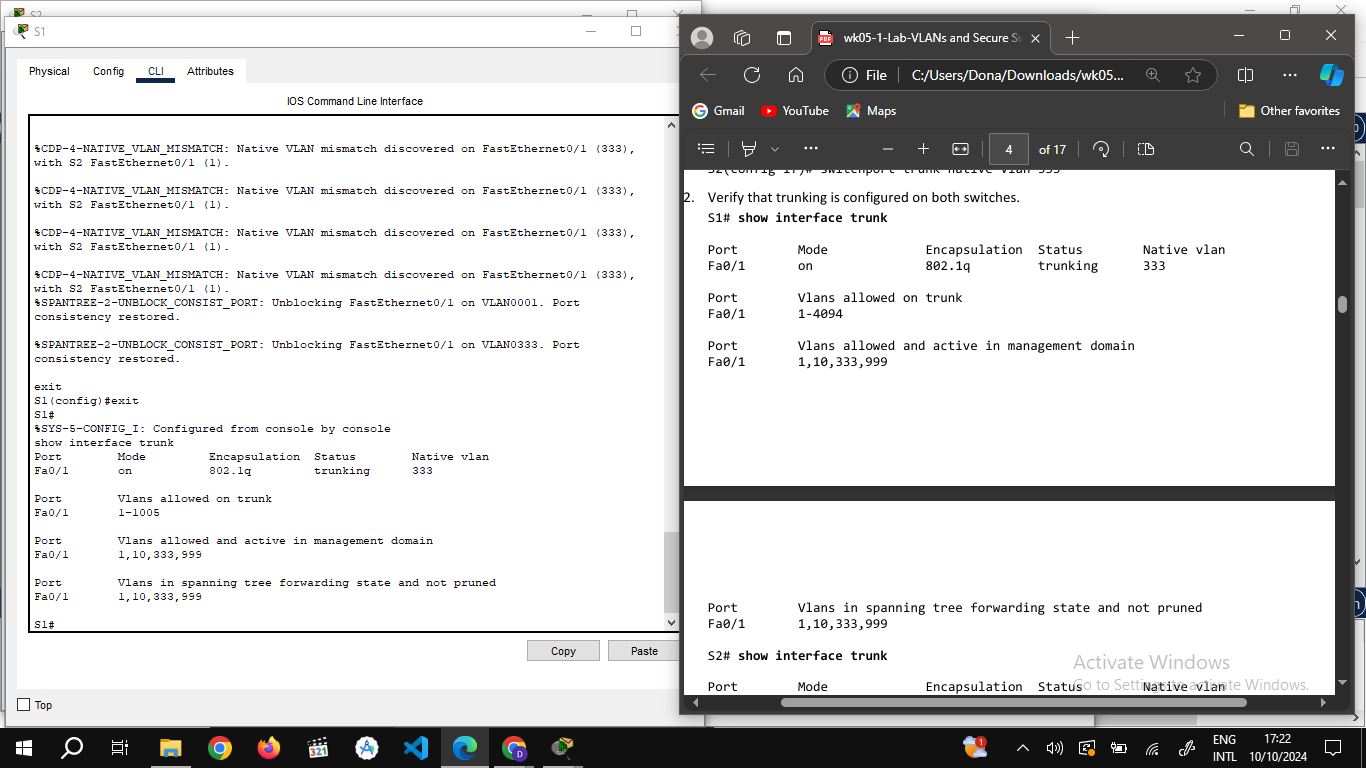
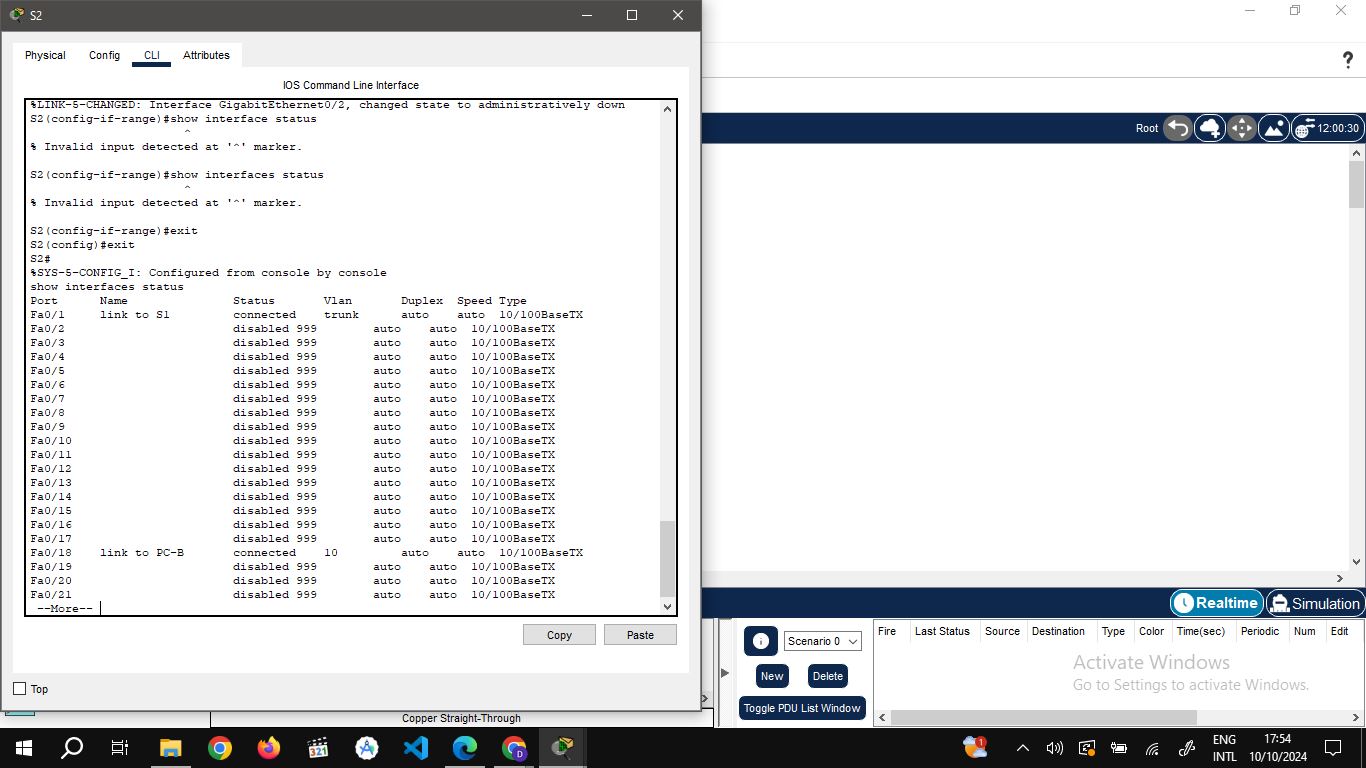
**Step 2: Configure access ports.**

**Step 3: Secure and disable unused switchports.**



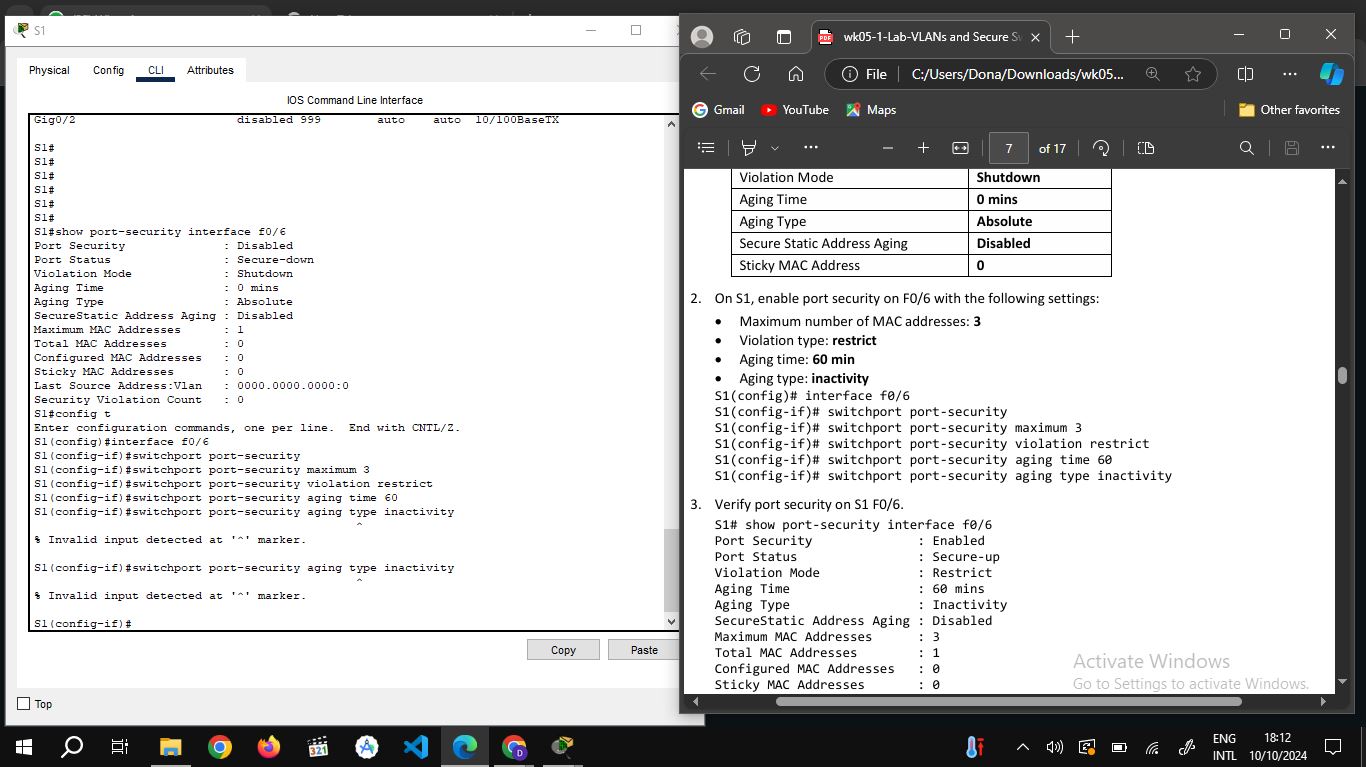


**Show interface status.**

****

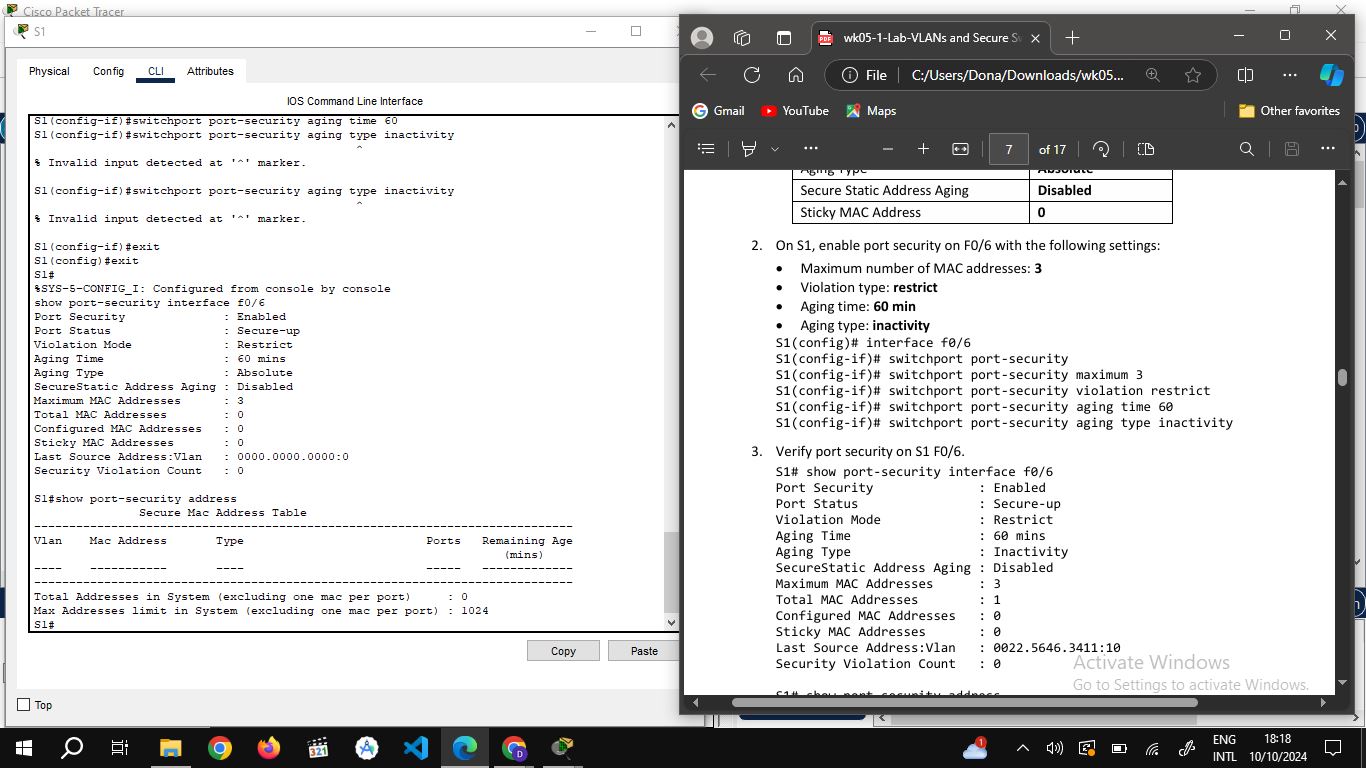
**Step 4: Document and implement port security features.**

**Port security interface f0/6 on S1 and enable it.**

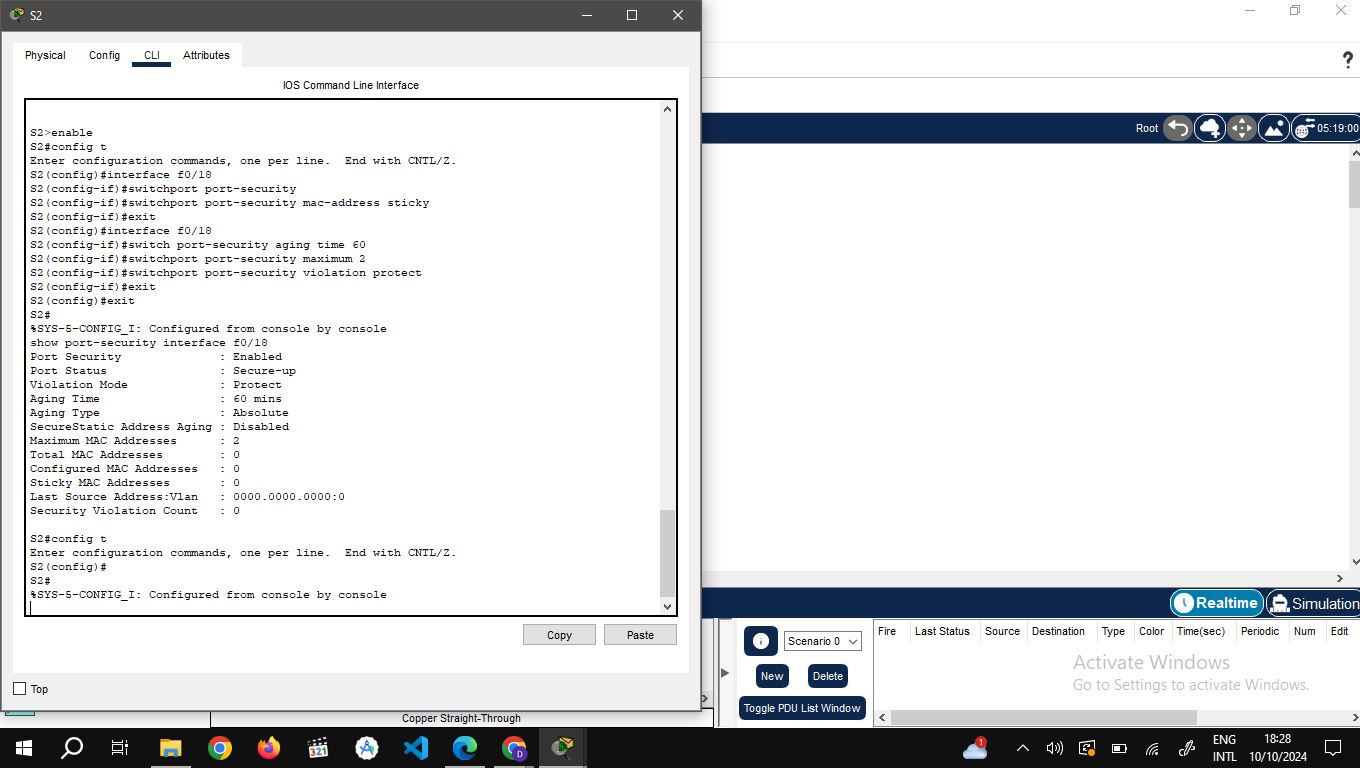
****

|  |  |
| --- | --- |
| **Default Port Security Configuration**  **Feature** | **Default Setting** |
| Port Security | Enabled |
| Maximum number of MAC  addresses | **3** |
| Violation Mode | Restrict |
| Aging Time | 60mins |
| Aging Type | Inactivity |
| Secure Static Address Aging  Sticky MAC Address | Disabled  0 |

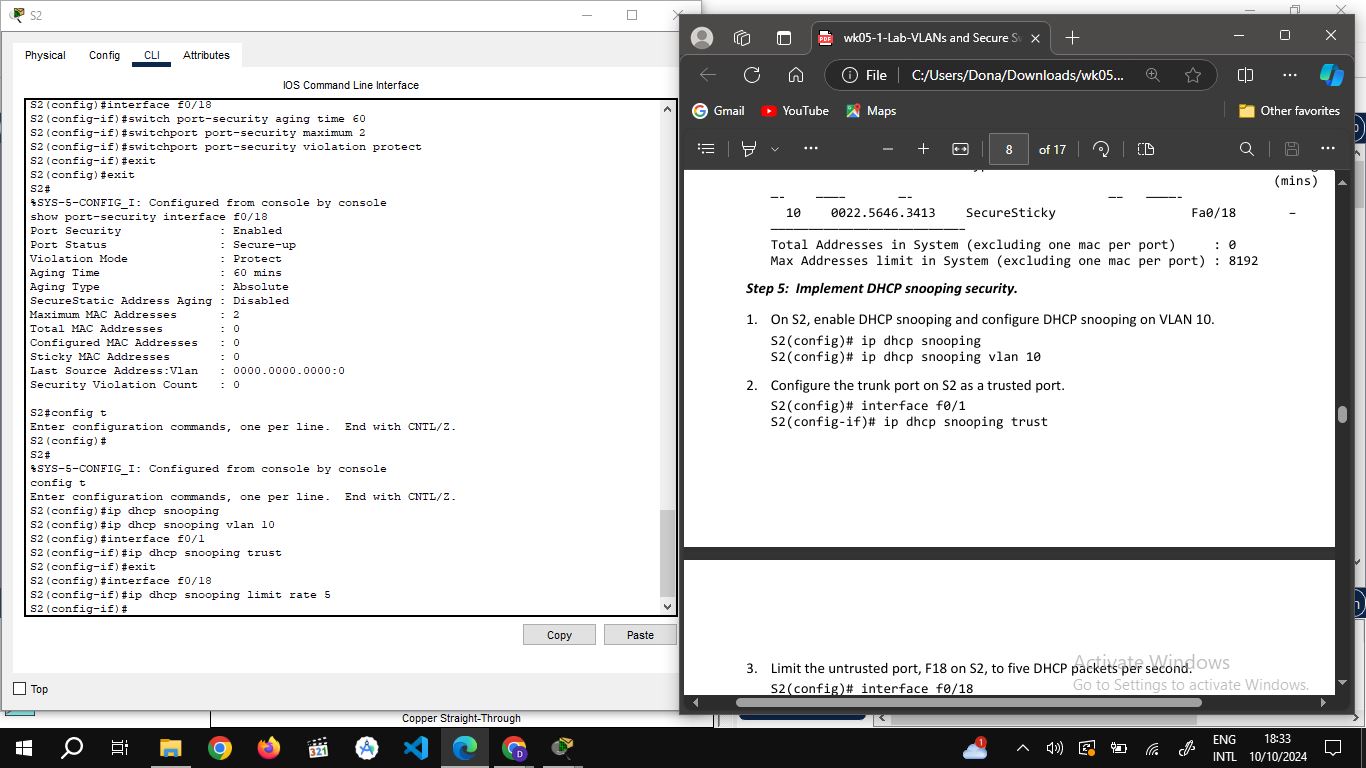
**Verify port security on S1 F0/6.**

****

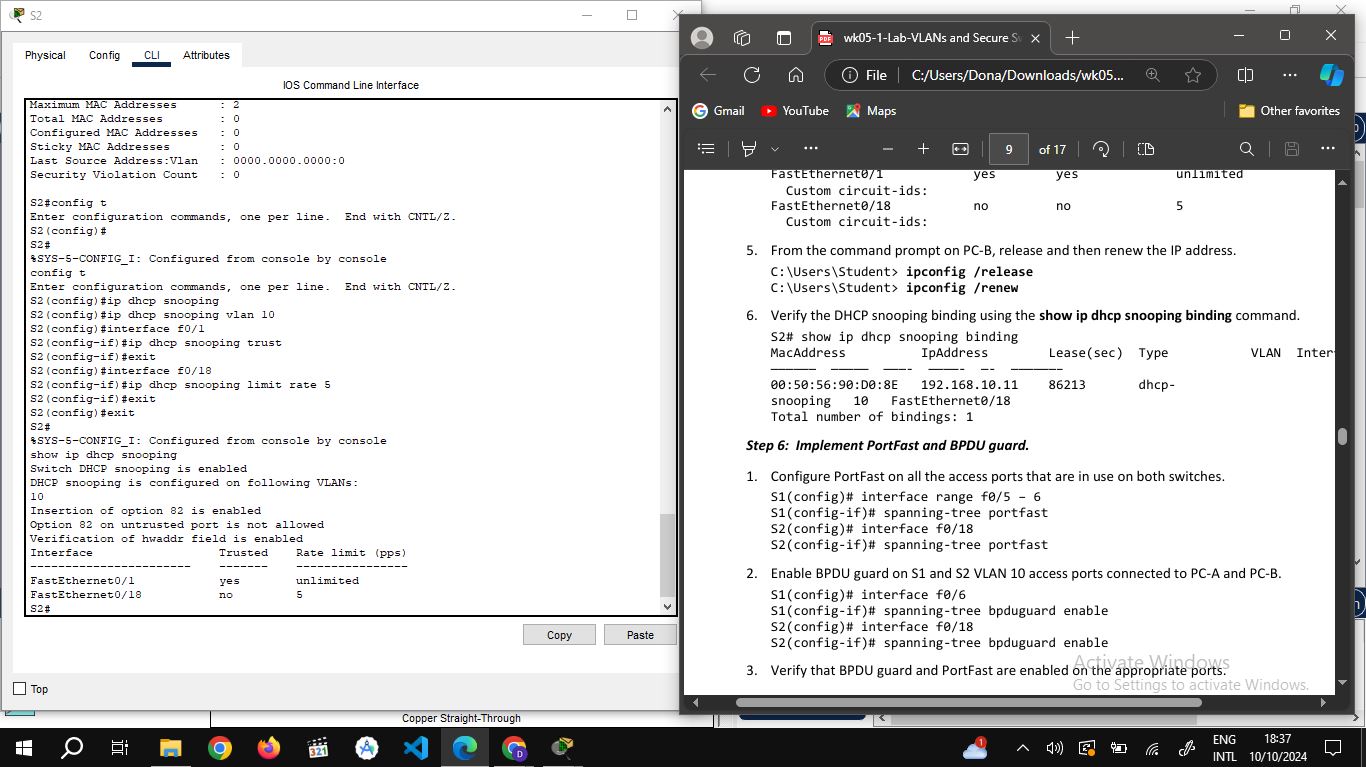
**4.** **Enable port security for F0/18 on S2 and show security interface.**

****

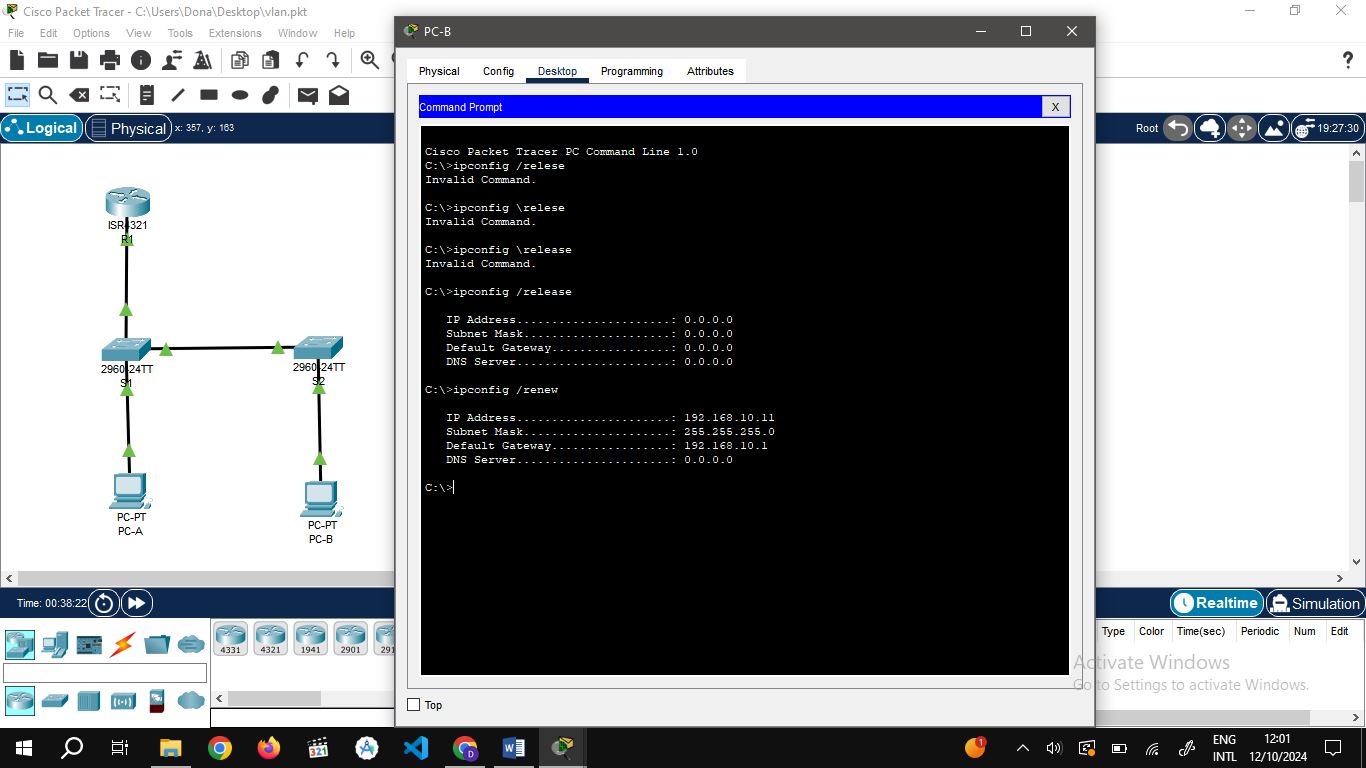
**Step 5: Implement DHCP snooping security.**

****

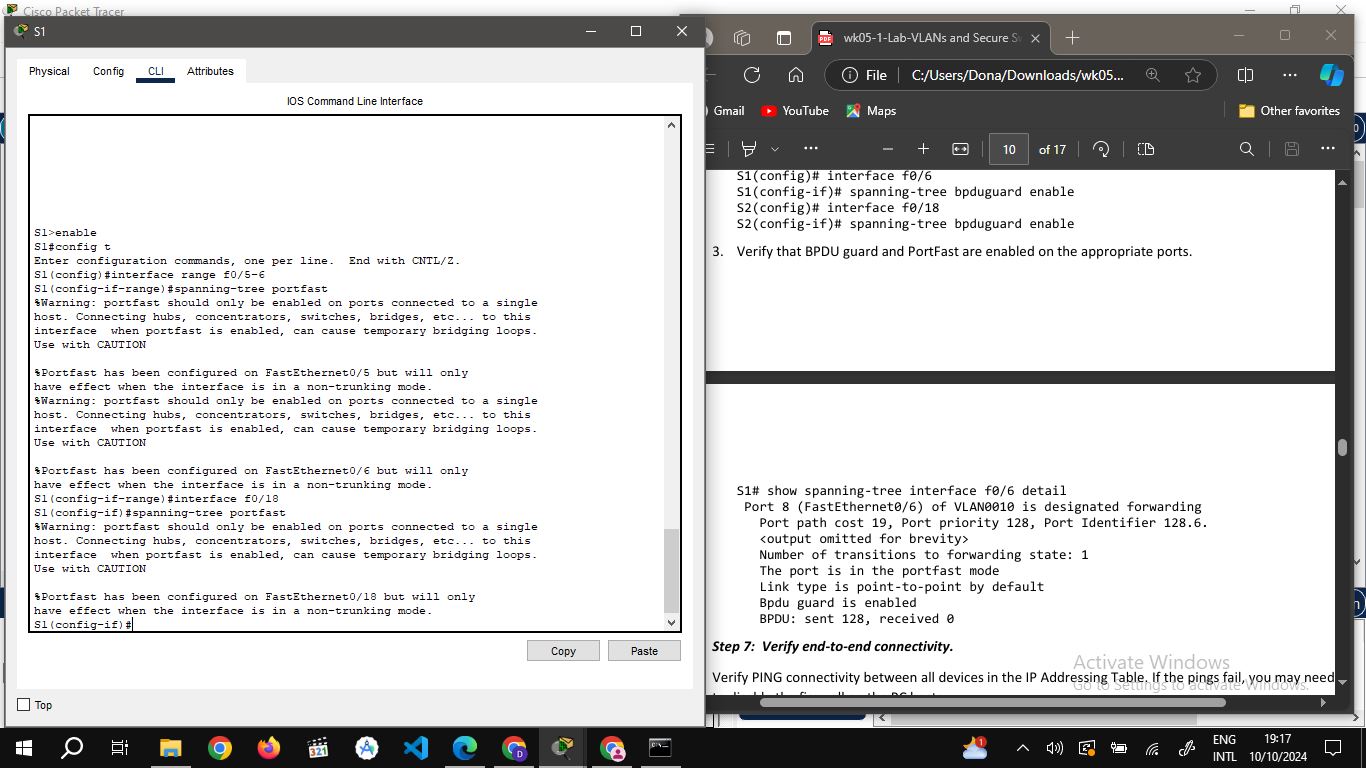
**Verify DHCP Snooping on S2.**

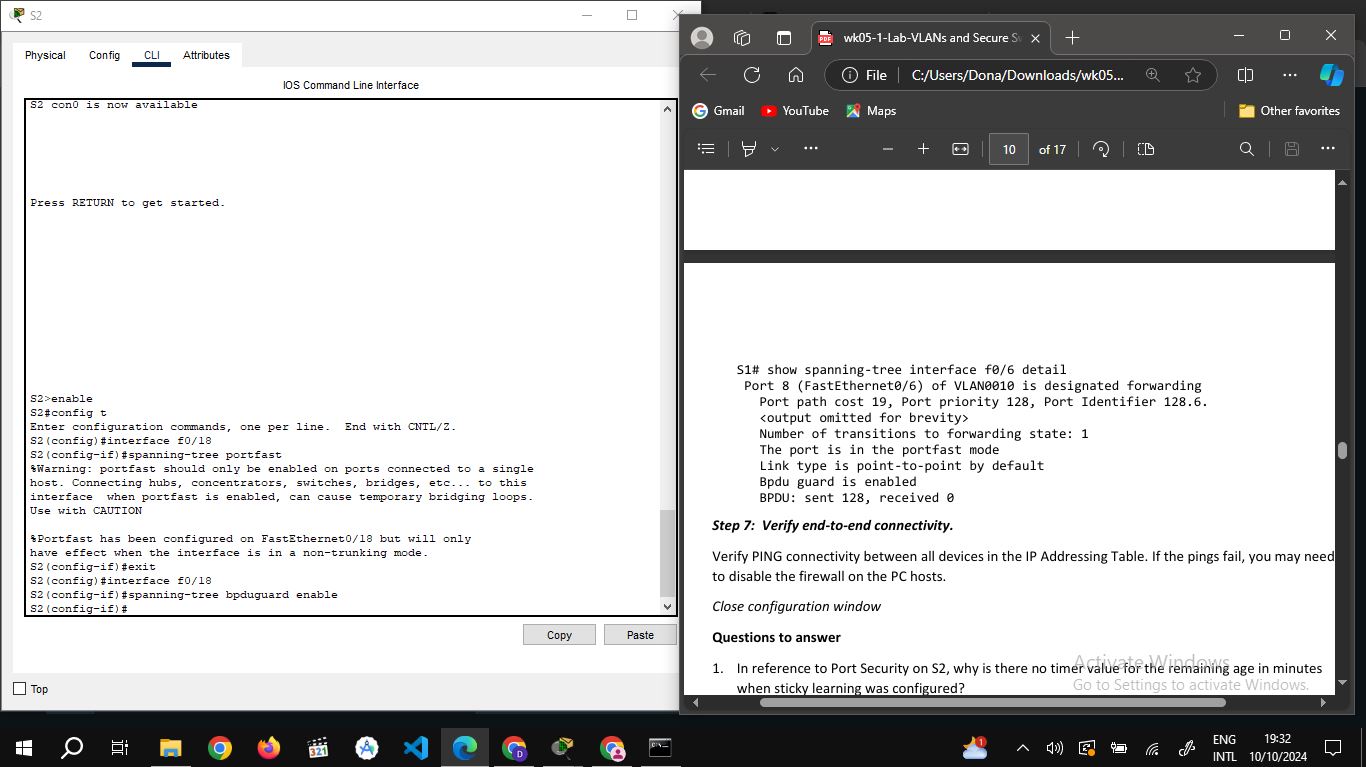
****

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

****

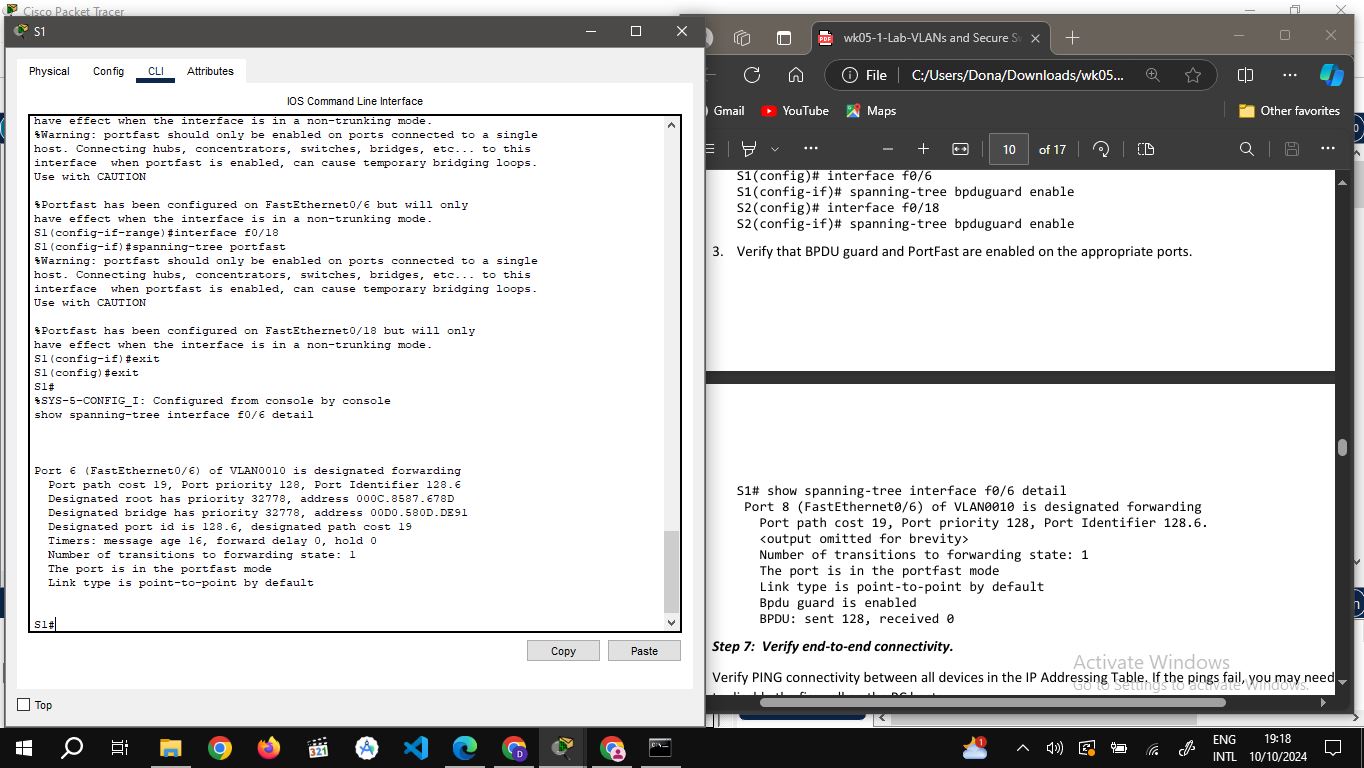
**Step 6: Implement PortFast and BPDU guard on S1 and S2.**

****

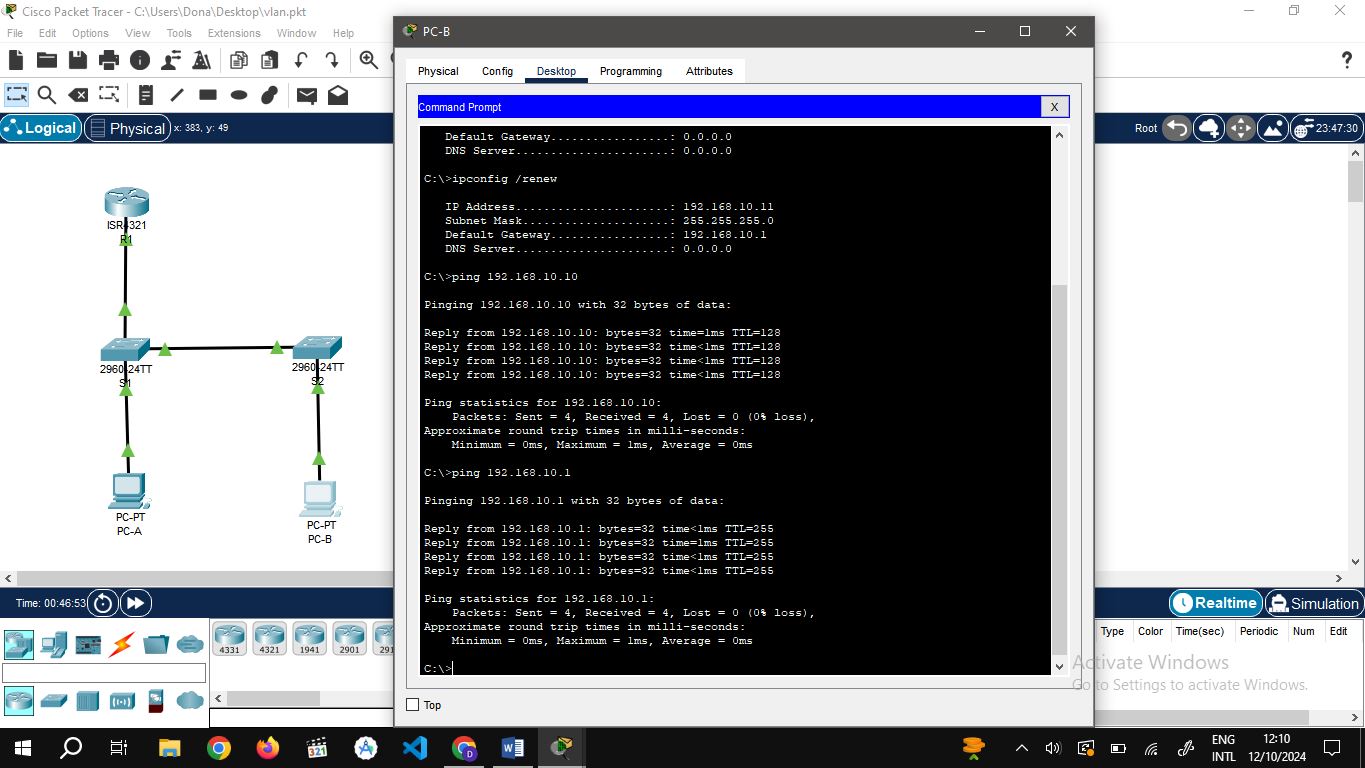
****

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

**show spanning-tree interface f0/6 detail**

****

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

****

**CONCLUSION.**

In conclusion, I have gained practical experience configuring VLANs. I learned how to implement VLANs, secure access ports, and manage unused switchports, which are vital for network segmentation and security. One of the challenges I faced was improper configuration of the network, which resulted to getting errors as the output. I learnt how to troubleshoot the problems which improved my troubleshooting skills and deepened my understanding of secure network design.