Course: Cloud and Network Security – C2 – 2025.

Student: Luke Mbogo

Student No: cs-cns09-25076

Friday, June 13th, 2025.

Week 4 Assignment 1:

VLANs and Secure Switch Configuration (Packet Tracer)

Contents

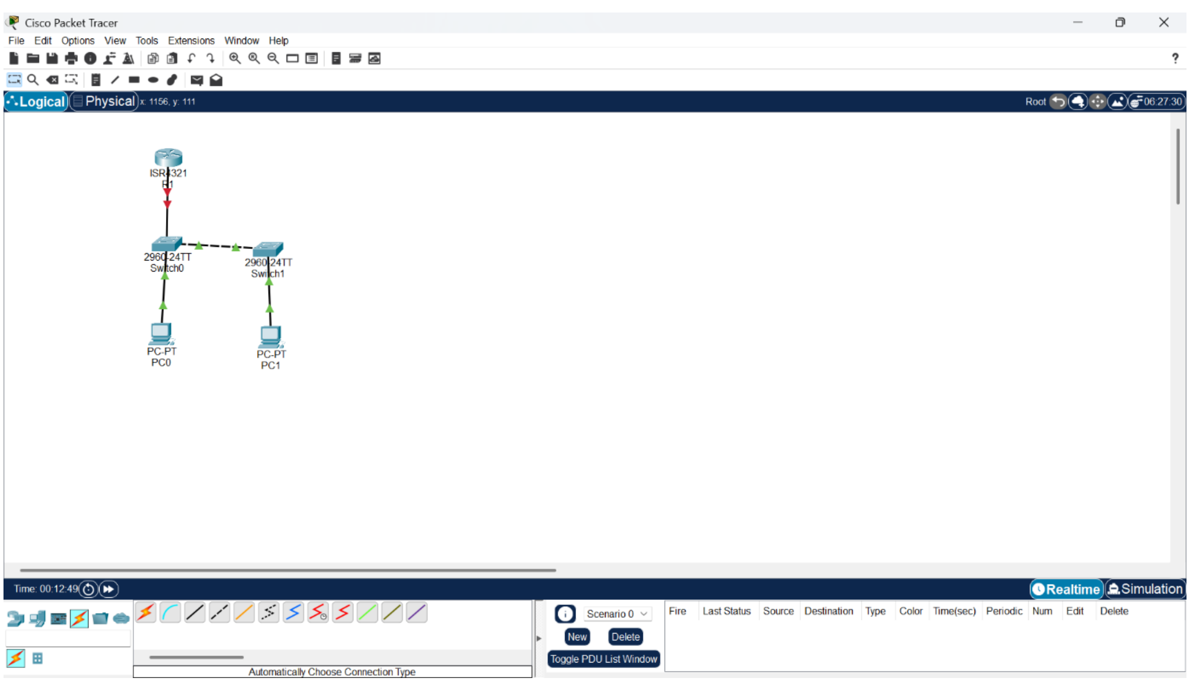
Introduction.

This lab exercise focused on configuring Layer 2 security features on a small enterprise network, including VLAN creation, switch security measures, and DHCP snooping. The goal was to reinforce key switching concepts in a practical, hands-on environment. Using Cisco Packet Tracer or compatible physical devices, we configured and secured a network involving a router, two switches, and two PCs. By the end of the lab, we had successfully implemented VLAN segmentation, trunking, port security, and DHCP snooping, gaining a clearer understanding of how to apply these configurations in a real-world context.

Configure the Network Devices.

Step 1: Cable the Network

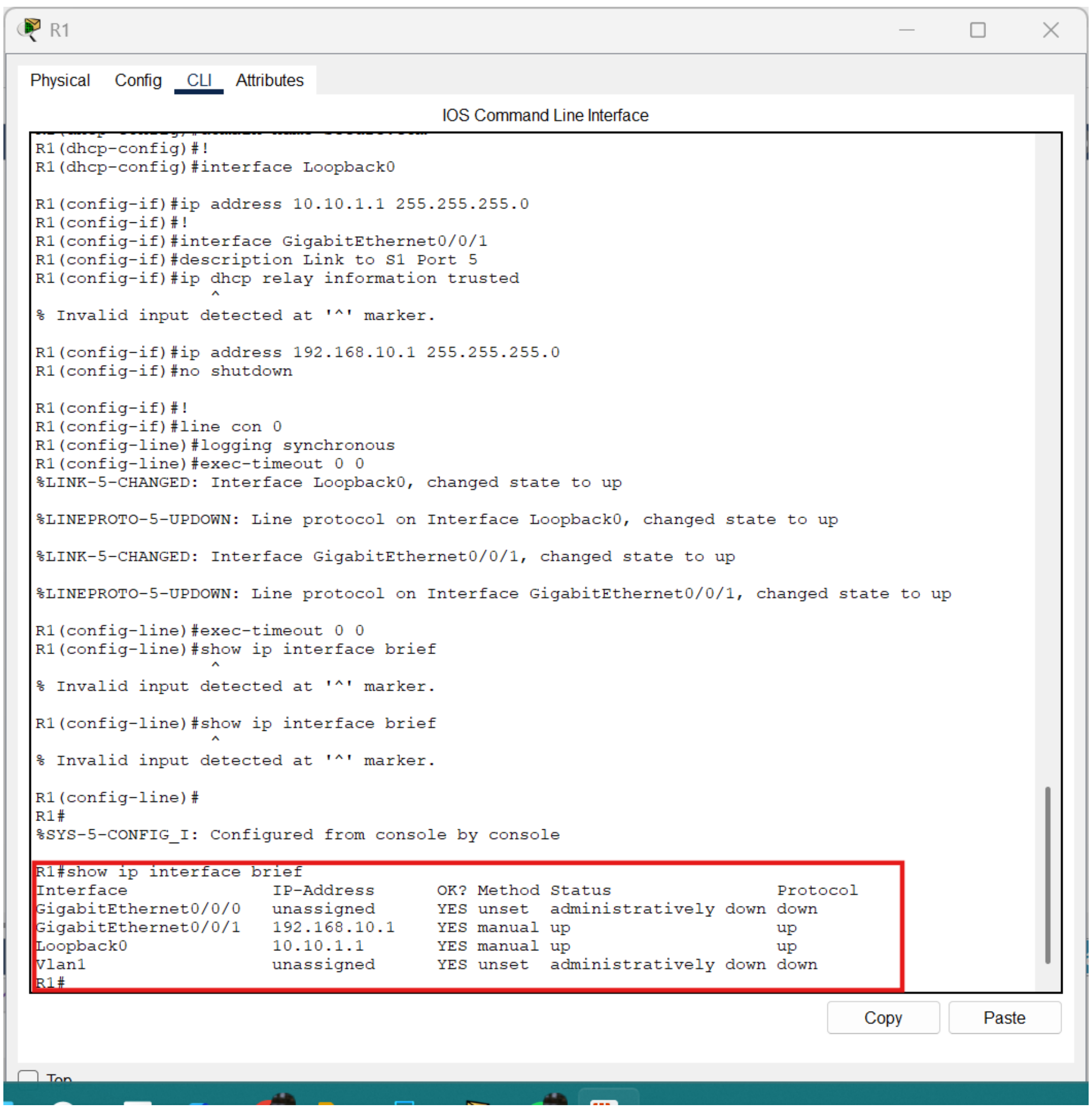
To begin the lab, the network was cabled according to the provided topology diagram. This involved connecting the router (R1) to both switches (S1 and S2), and linking each switch to its respective PC using appropriate Ethernet cables. Console cables were also connected to the network devices for configuration access through a terminal emulator. After all devices were physically connected, they were powered on and initialized to prepare for the configuration process. Bellow is a screenshot of the configuration.



Step 2: Configure R1.

For this step, I started by accessing the router and entering global configuration mode. I changed the hostname to R1 and disabled domain name lookup using no ip domain lookup to avoid delays when entering incorrect commands. After that, I configured DHCP exclusions to reserve IP addresses from 192.168.10.1 to 192.168.10.9 and 192.168.10.201 to 192.168.10.202, so they wouldn't be handed out by DHCP. Then, I configured the GigabitEthernet0/0/1 interface, which connects to switch S1. I assigned it the IP address 192.168.10.1/24, enabled DHCP relay information, and brought the interface up using the no shutdown command.

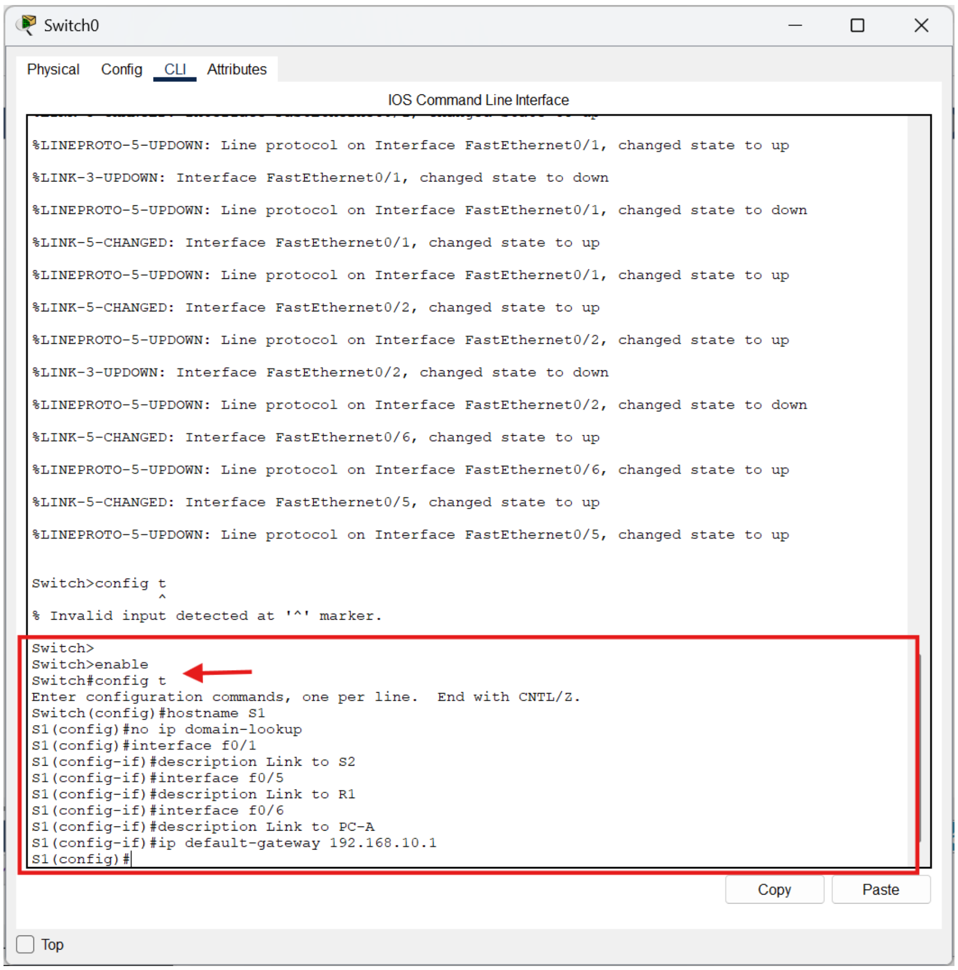
Finally, I used the show ip interface brief command to confirm that all interfaces were up and running correctly. Both the loopback and the Gigabit interface showed a status of **up/up**, which confirmed that the configuration was successful.



Step 3: Configure and Verify Basic Switch Settings

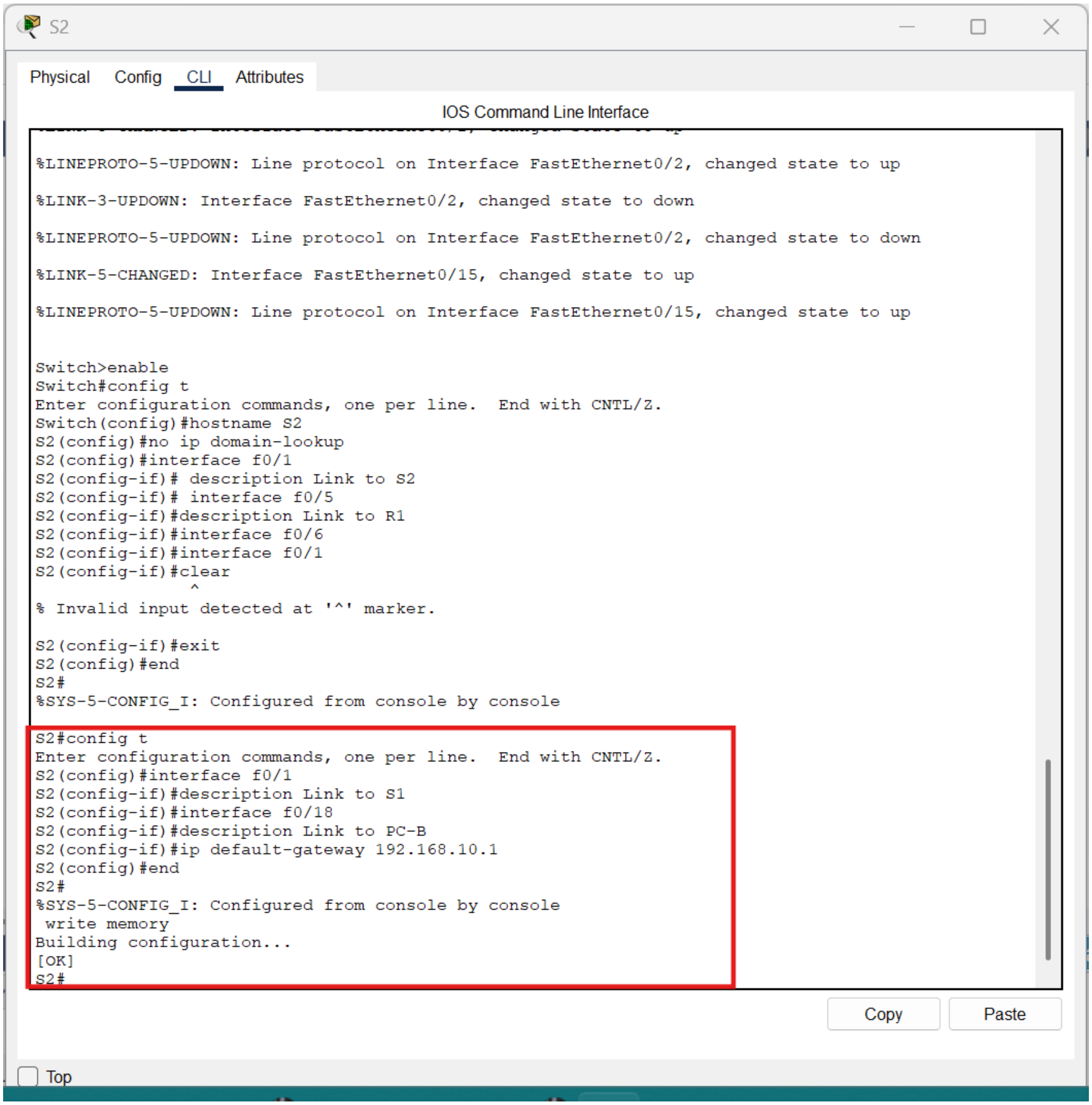
The switches were first renamed to **S1** and **S2** using the hostname command for easier identification. DNS lookup was disabled on both to prevent delays caused by mistyped commands. Interface descriptions were then added for better clarity:

- **S1**:
  - F0/1 – Link to S2
  - F0/5 – Link to R1
  - F0/6 – Link to PC-A



- **S2**:
  - F0/1 – Link to S1
  - F0/18 – Link to PC-B

Lastly, a default gateway of 192.168.10.1 was set on both switches to allow management traffic to reach the router.

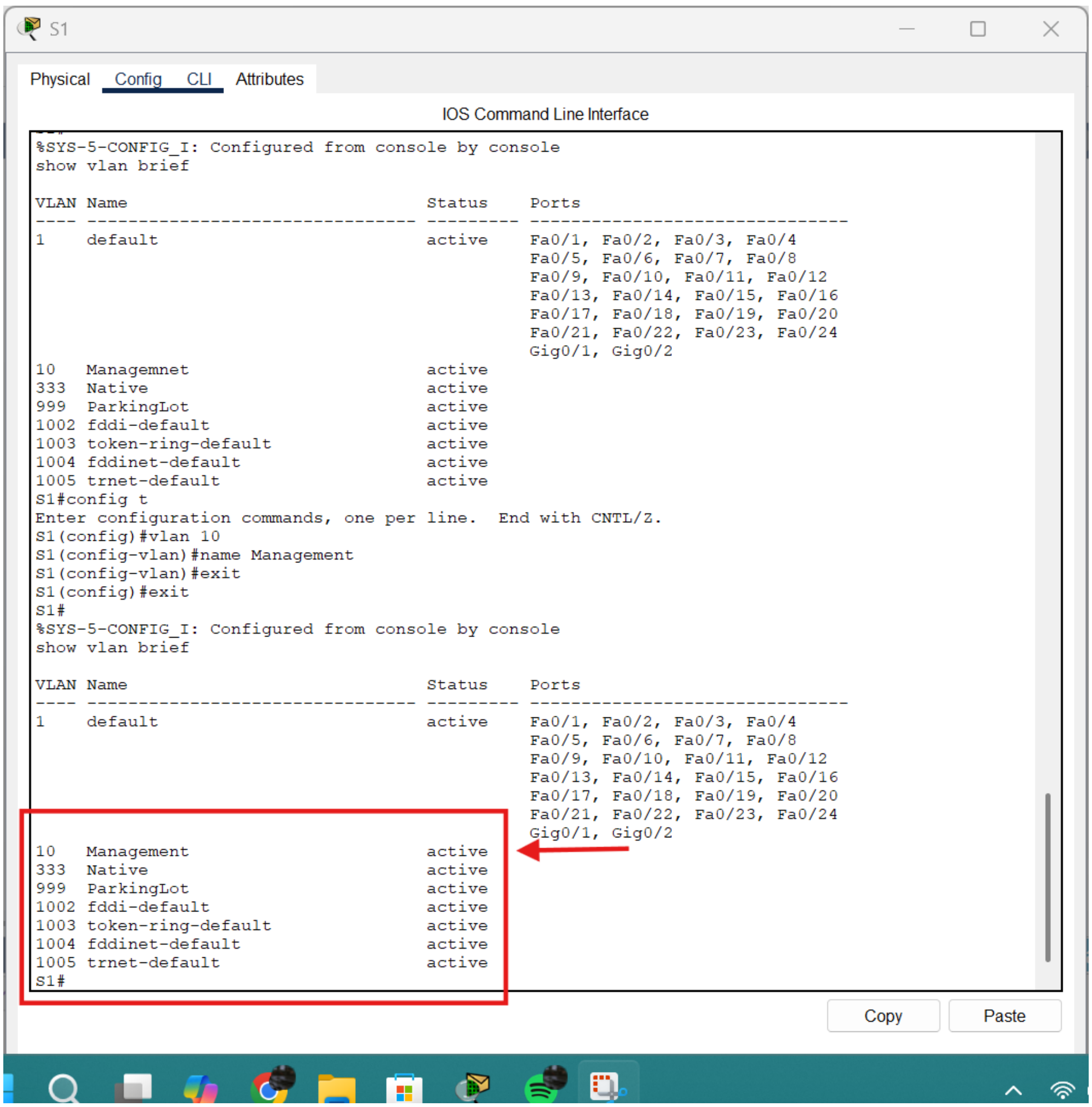


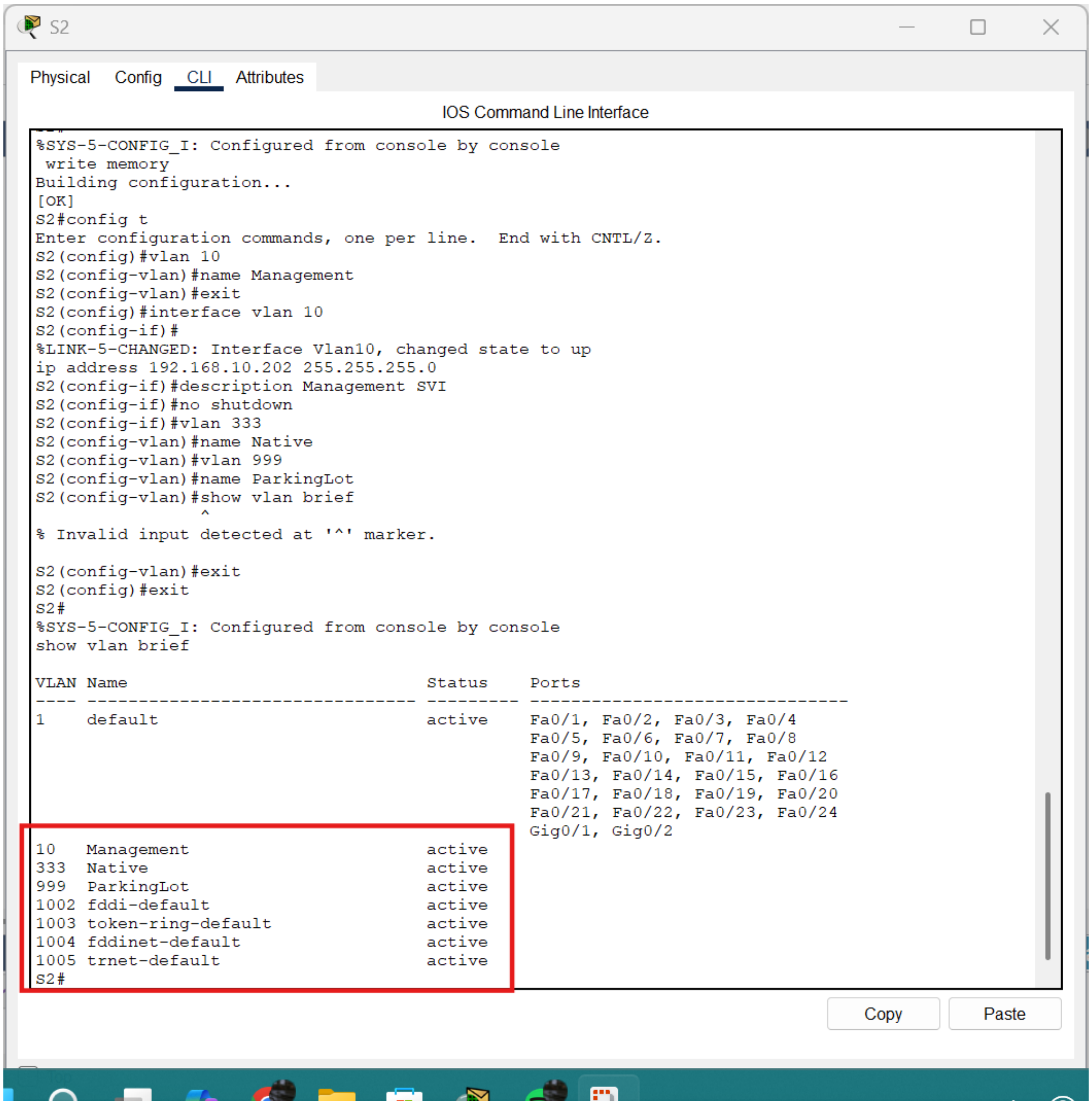

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/15, changed state to up


Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#interface f0/1
S2(config-if)# description Link to S2
S2(config-if)# interface f0/5
S2(config-if)#description Link to R1
S2(config-if)#interface f0/6
S2(config-if)#interface f0/1
S2(config-if)#clear
                ^
% Invalid input detected at '^' marker.

S2(config-if)#exit
S2(config)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#description Link to S1
S2(config-if)#interface f0/18
S2(config-if)#description Link to PC-B
S2(config-if)#ip default-gateway 192.168.10.1
S2(config)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console
 write memory
Building configuration...
[OK]
S2#
```

Part 2: Configure VLANs on Switches

To begin, VLAN 10 was added on both **S1** and **S2** and named **Management** to represent the management network. After that, switched virtual interfaces (SVIs) were configured for VLAN 10 on each switch — **S1** was assigned 192.168.10.201 and **S2** got 192.168.10.202. Both interfaces were activated with no shutdown, and descriptions were added for clarity. Next, VLAN 333 was created on both switches and labeled **Native** for trunking purposes. Finally, VLAN 999 was set up with the name **ParkingLot**, which is typically used to isolate unused ports for security.

Below are the screenshots to VLAN 10 being added to both S1 and S2.



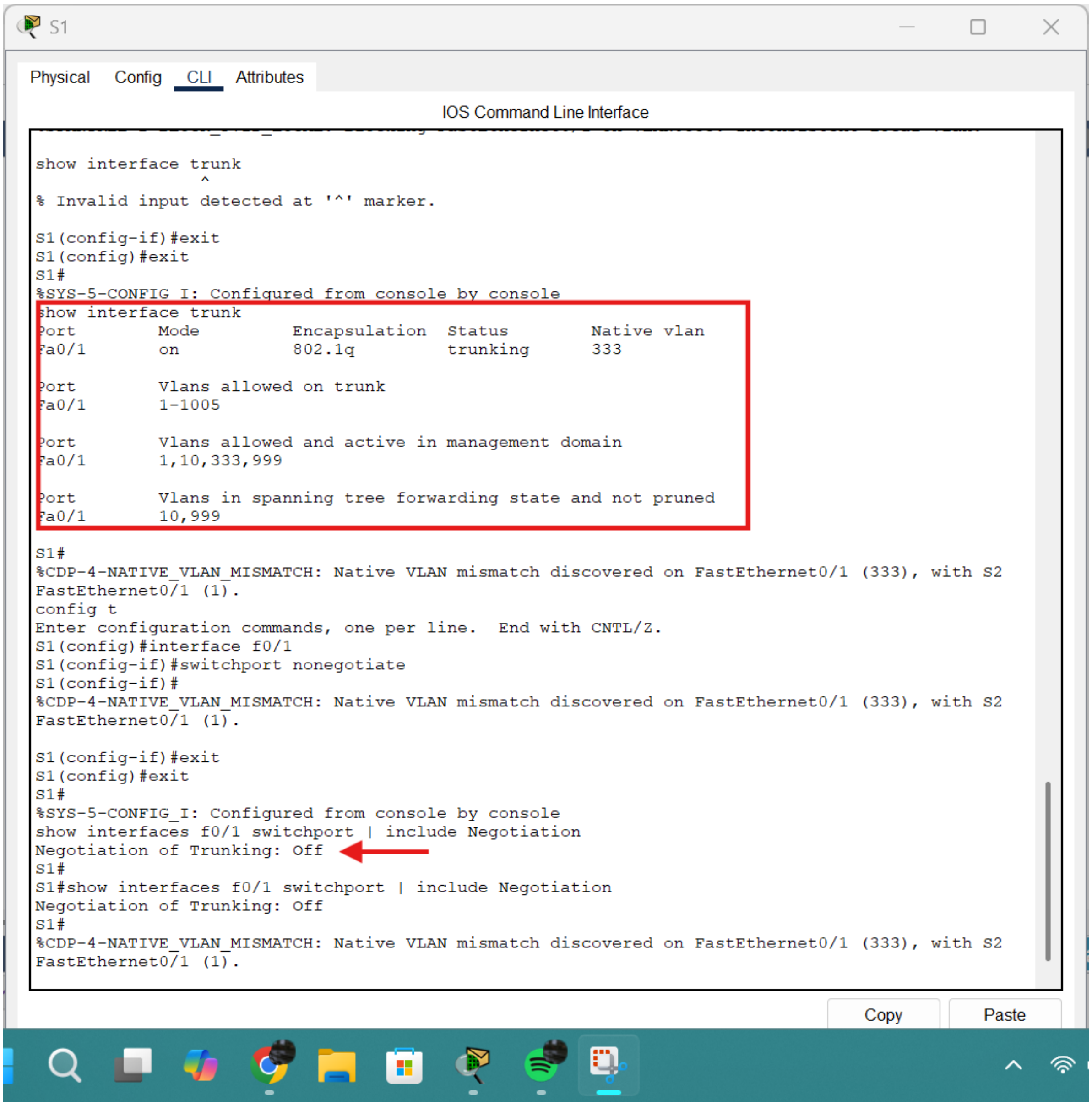


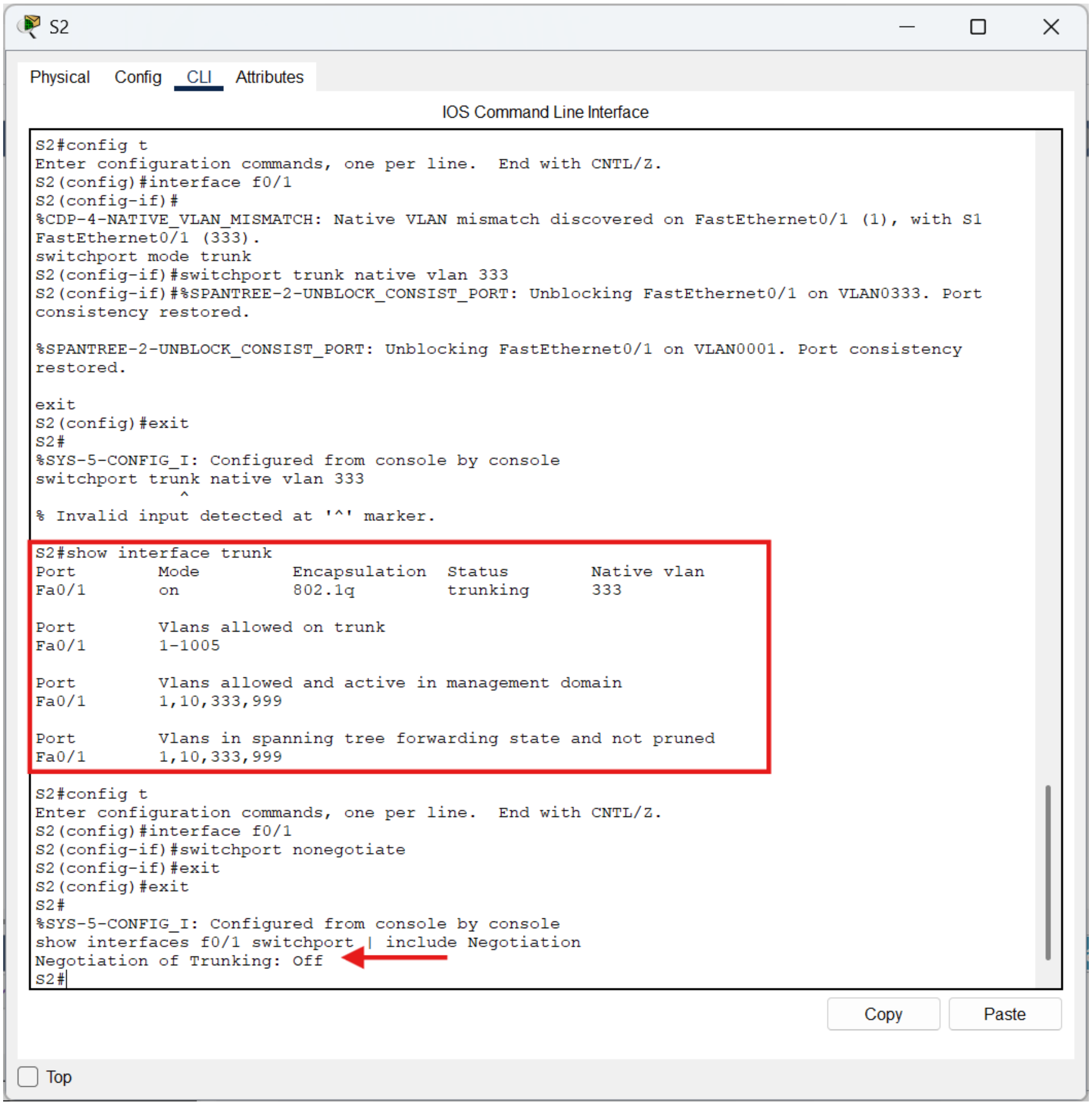
Part 3: Configure Switch Security

Step 1: Implement 802.1Q Trunking

Trunking was configured between **S1** and **S2** on interface **F0/1**, with **VLAN 333** set as the native VLAN. The switchport mode trunk and switchport trunk native vlan 333 commands ensured that tagged and untagged traffic would flow correctly between the switches. After configuration, trunking status was verified using the show interface trunk command, confirming that both switches had active trunks allowing VLANs 1, 10, 333, and 999.

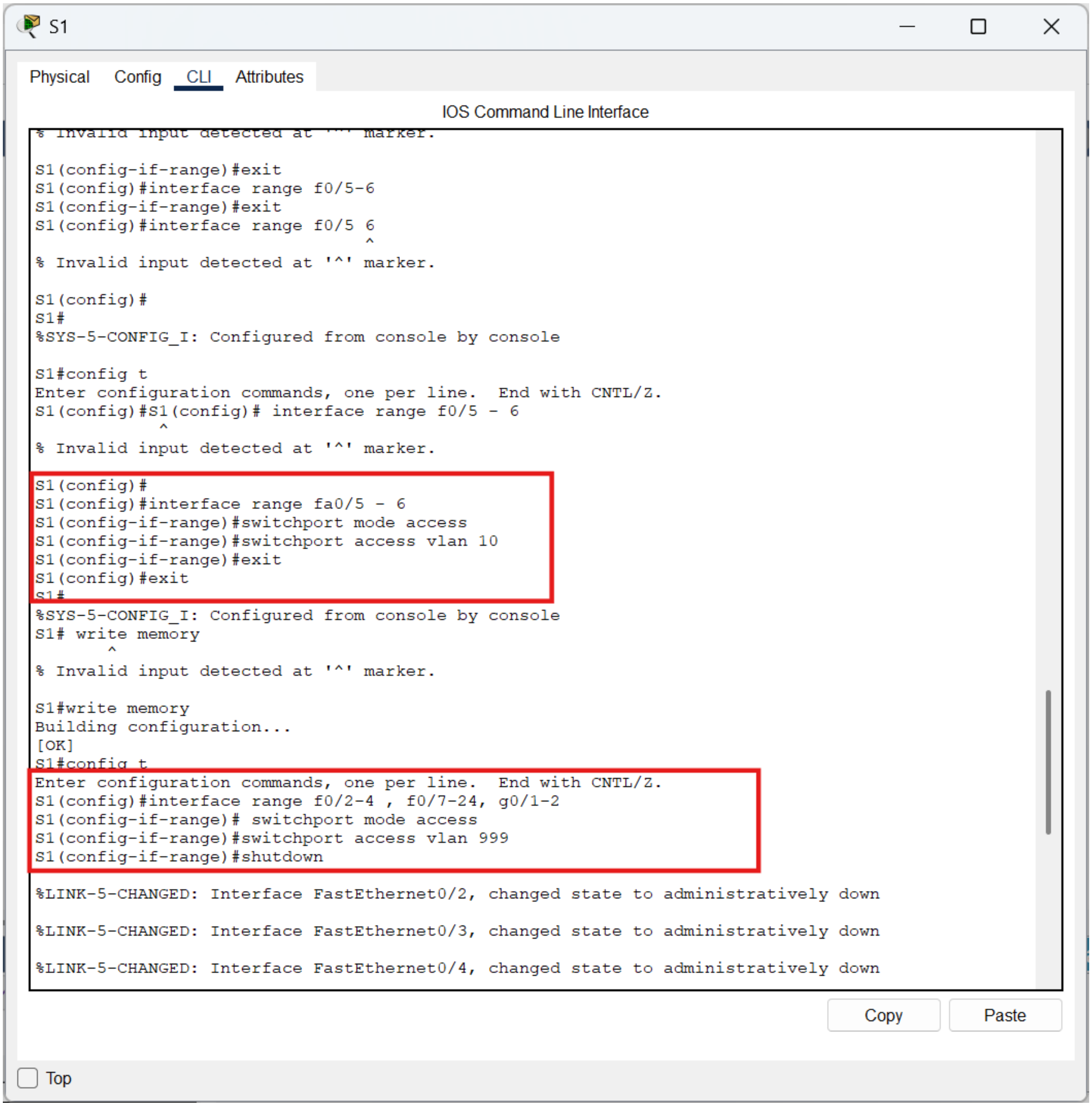
To tighten security and reduce unnecessary traffic, **DTP negotiation** was disabled using the switchport non-negotiate command on both switches. A final check with show interfaces f0/1 switchport | include Negotiation confirmed that trunk negotiation was turned off, ensuring only manual trunk settings are used on this link.





Step 2: Configure Access Ports

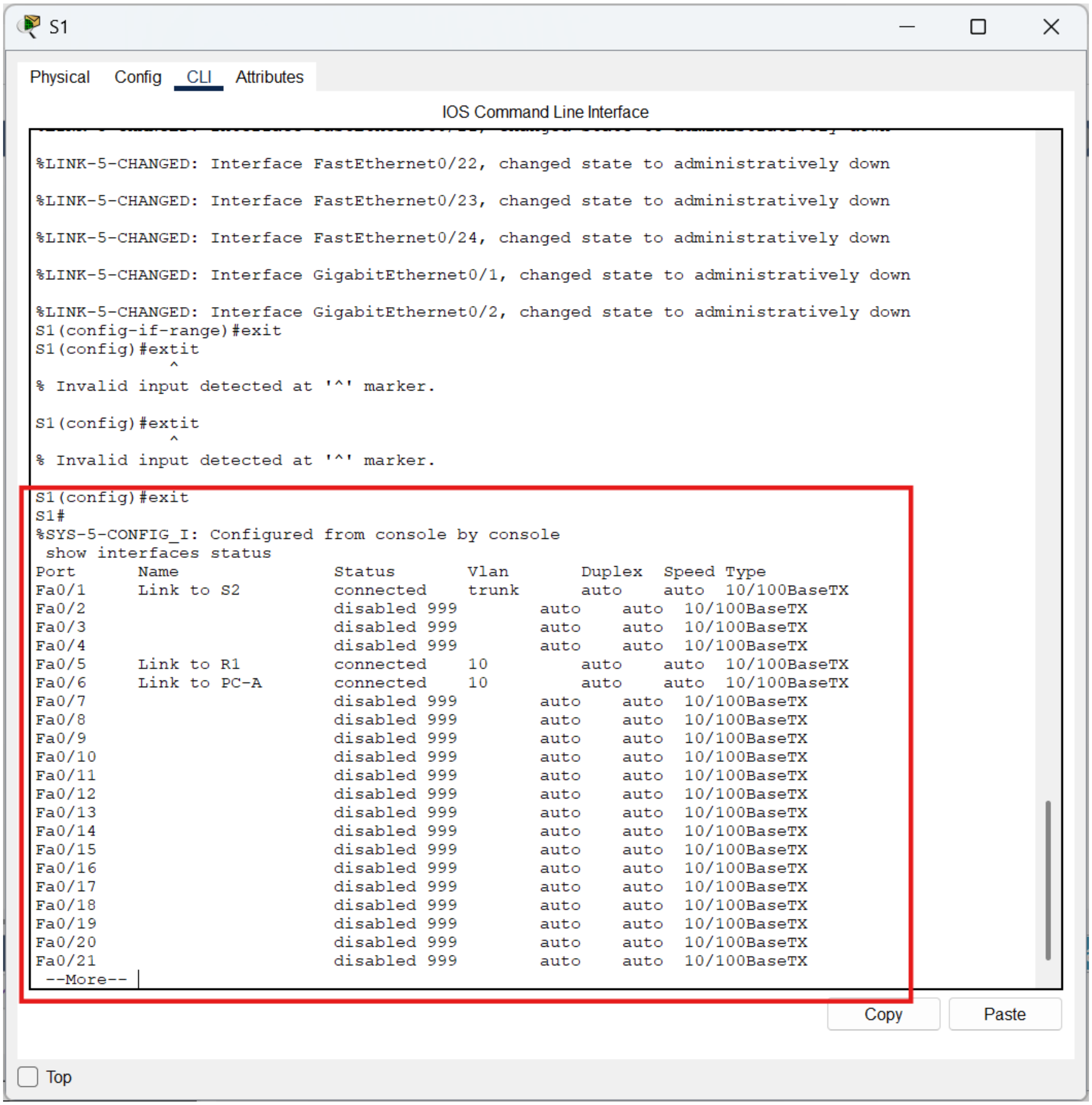
To ensure proper VLAN segmentation, access ports were configured on both switches. On **S1**, interfaces **F0/5** and **F0/6**—connected to R1 and PC-A respectively—were set as access ports assigned to **VLAN 10**. On **S2**, **F0/18**, which connects to PC-B, was also configured as an access port for VLAN 10. This setup ensures that all end devices are correctly placed in the management VLAN.

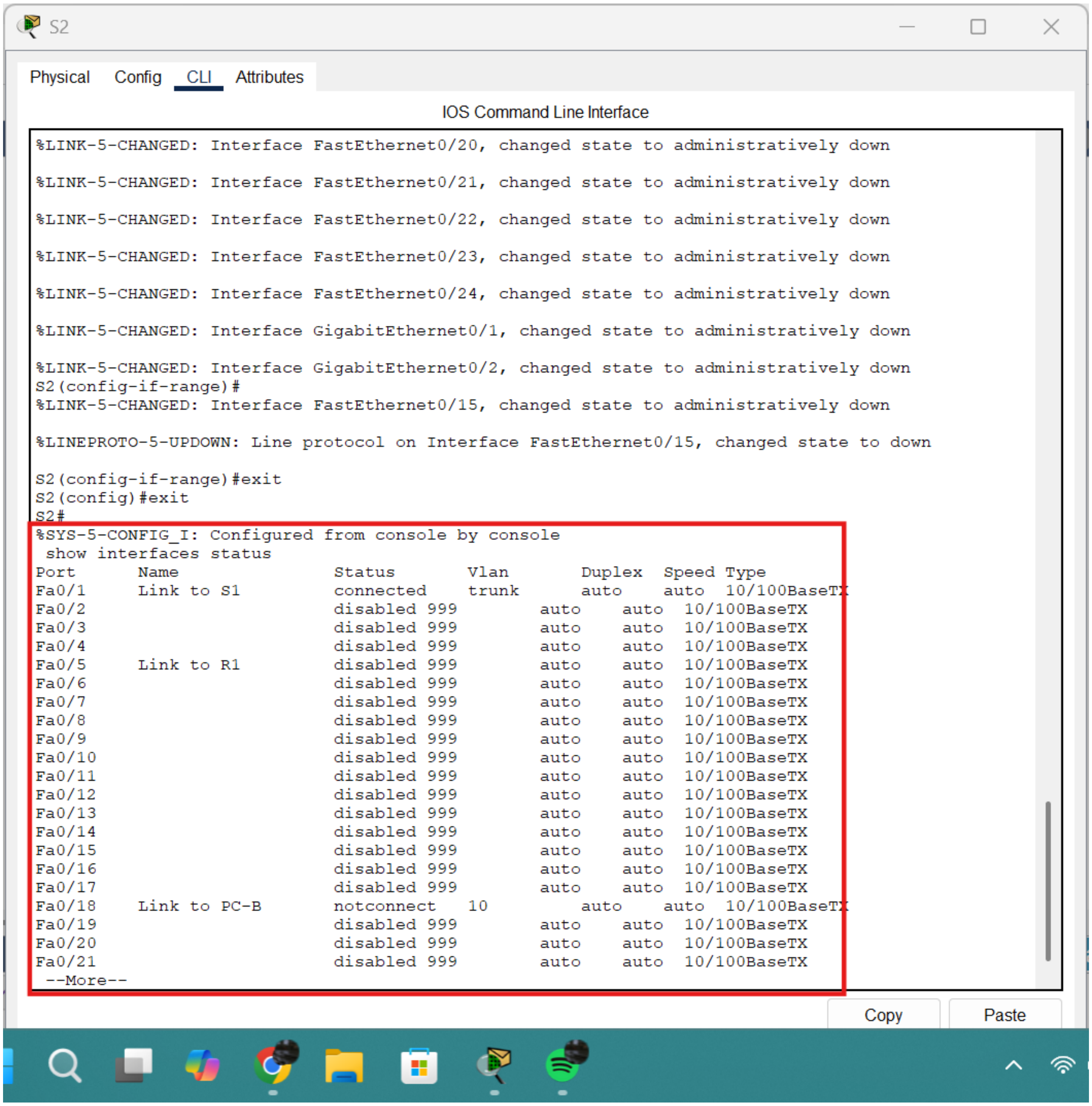


Step 3: Secure and Disable Unused Switchports

To improve security and reduce unnecessary traffic, all unused ports on both switches were moved to **VLAN 999** (ParkingLot VLAN) and shut down. This included ports like **F0/2-4**, **F0/7-24**, and **G0/1-2** on S1, and similar ranges on S2. This step helps prevent unauthorized access and keeps the switch environment clean.

Verification using the show interfaces status command showed that all unused ports were successfully disabled and assigned to VLAN 999, while active ports remained correctly configured and connected.

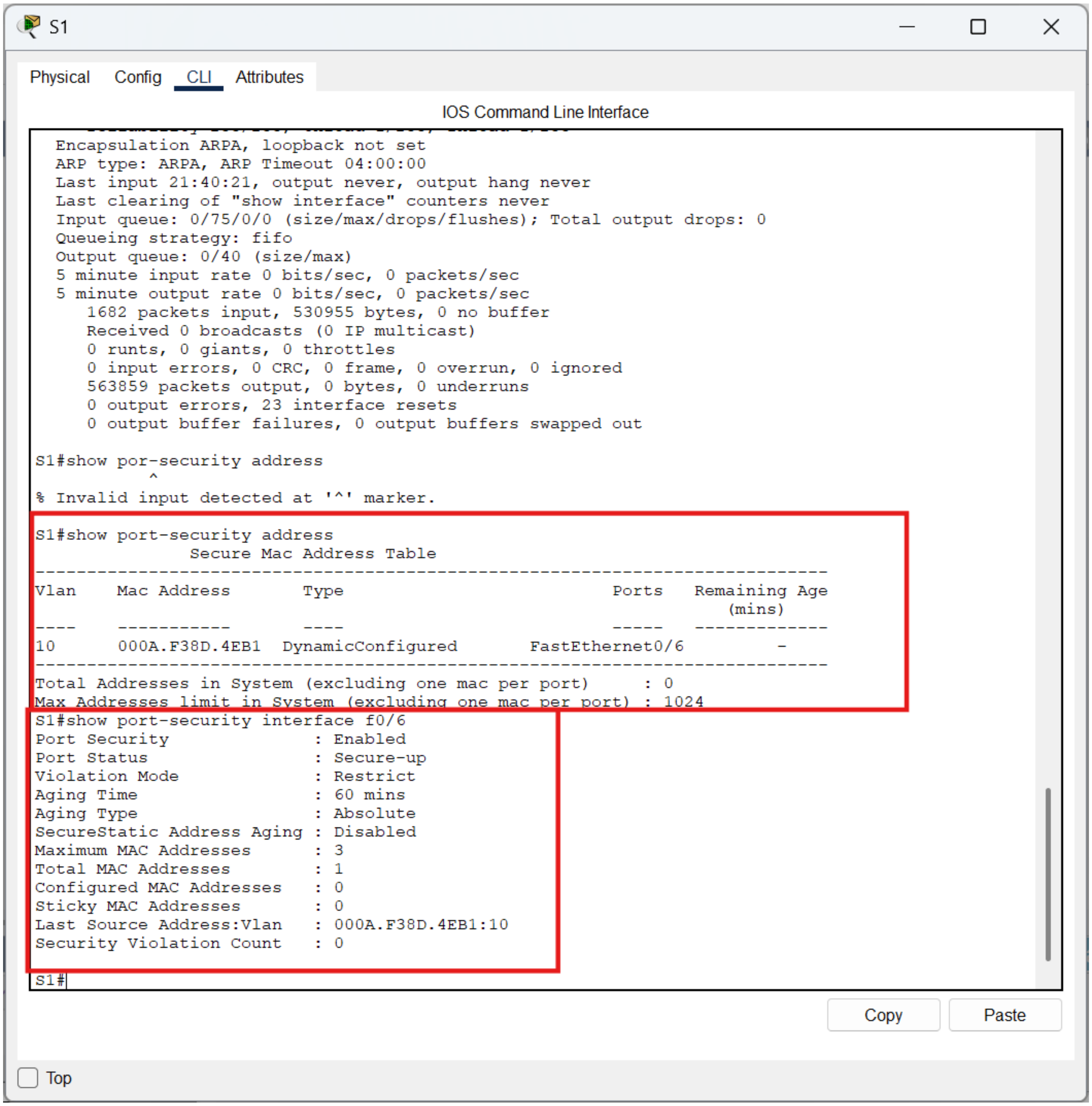




Step 4: Configure Port Security on Access Ports

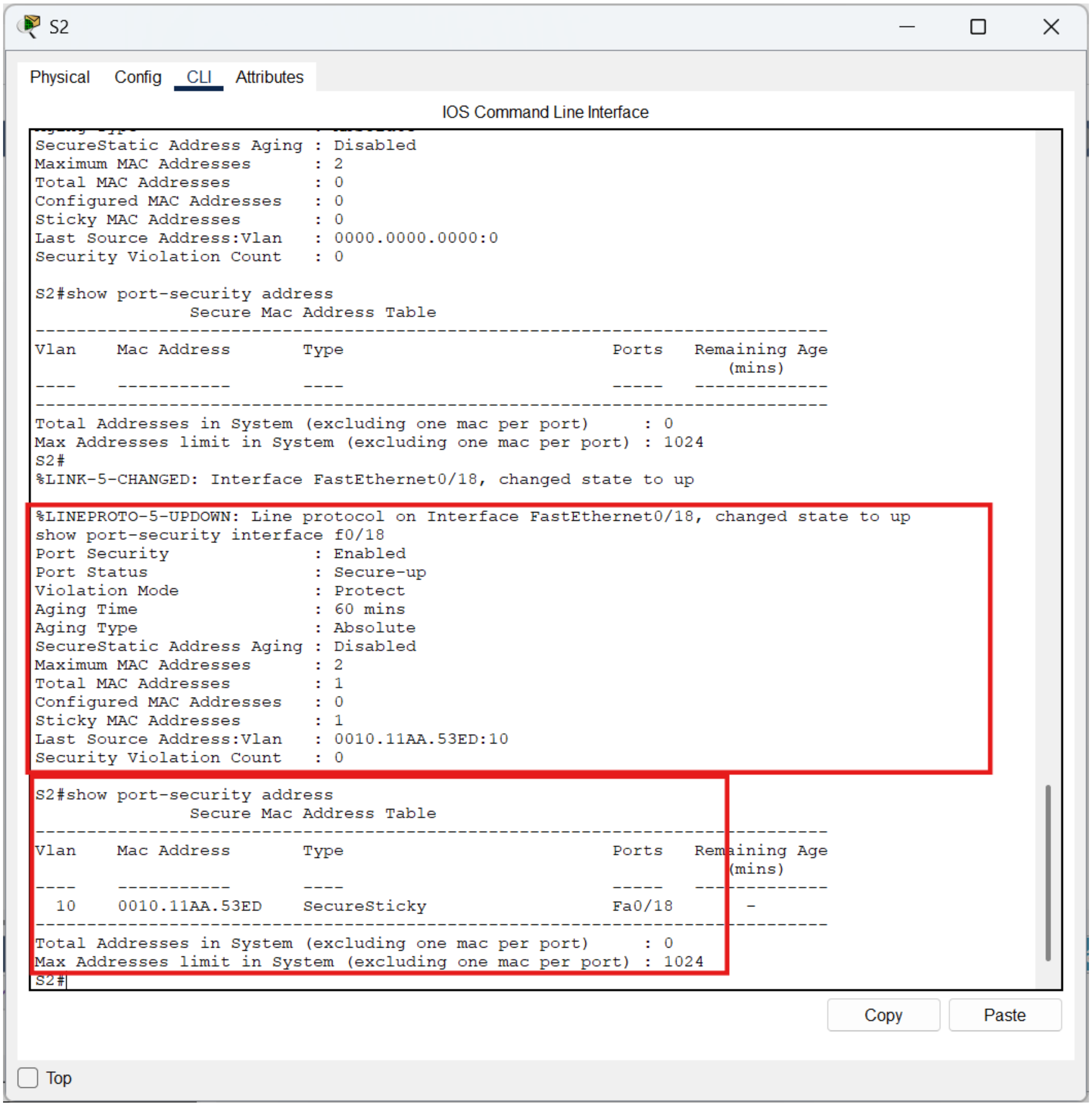
Started by checking the default port security settings on **S1's F0/6**. As expected, port security was **disabled**, violation mode was set to **shutdown**, and max MAC address count was **1** by default.

To enhance security, port security was enabled on **F0/6**, the max allowed MAC addresses increased to **3**, violation mode changed to **restrict**, and aging was set to **60 minutes** based on **inactivity**. After connecting a host, the interface moved to **secure-up** state, and one MAC address was dynamically learned.



On **S2**, port **F0/18** was secured using **sticky MAC address** learning, which allows automatic MAC binding. Configurations included a **maximum of 2 MACs**, **protect** mode for violations (which quietly drops unknown traffic), and **60-minute aging**.

Verification commands showed that both ports were secured, each had dynamically/stickily learned one MAC address, and were in **secure-up** status.



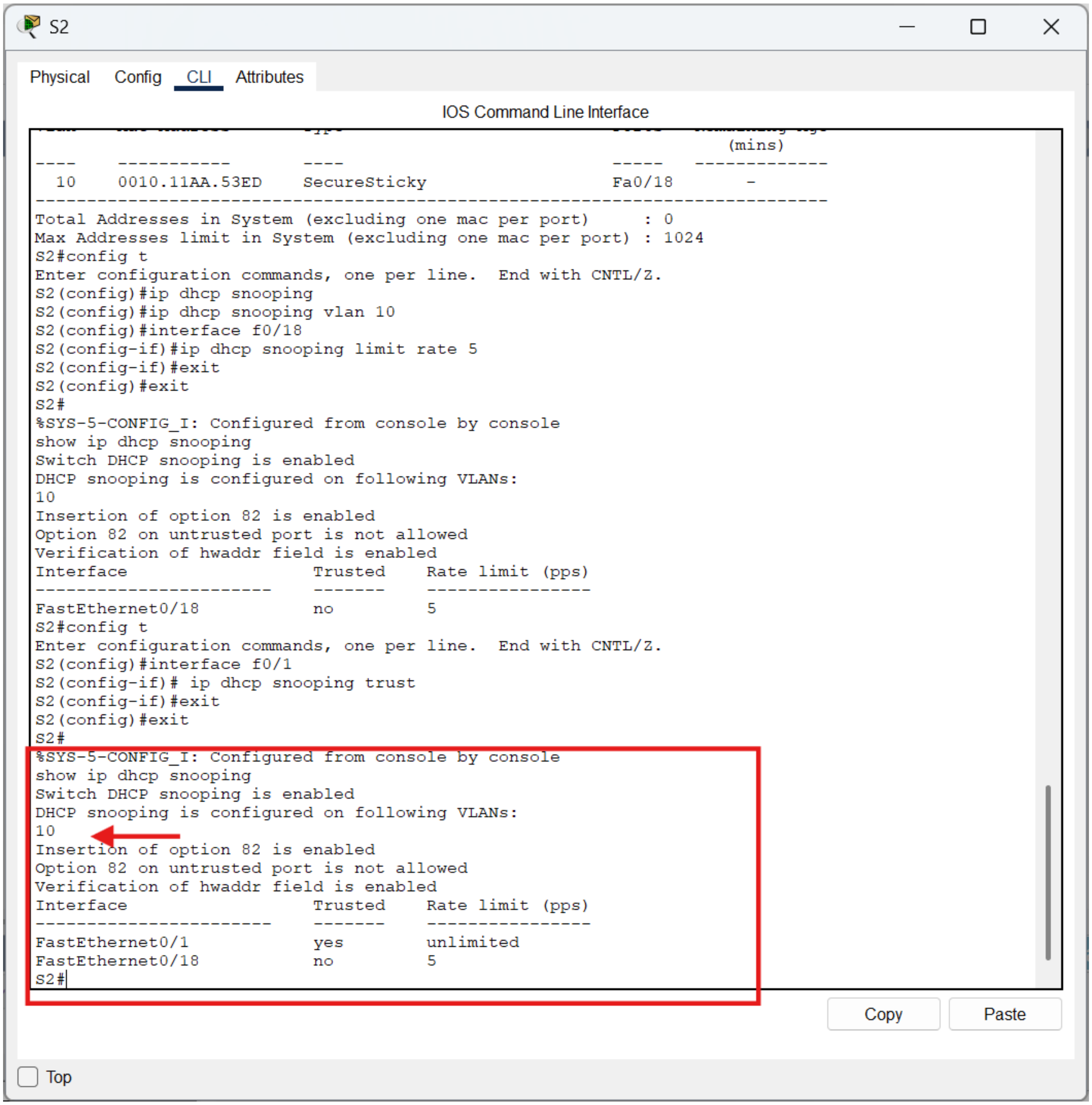
```
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

S2#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S2#
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up
show port-security interface f0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 60 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0010.11AA.53ED:10
Security Violation Count   : 0

S2#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
  10    0010.11AA.53ED    SecureSticky                  Fa0/18      -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S2#
```

Step 5: Implement DHCP Snooping Security

To enhance security against rogue DHCP servers, DHCP snooping was enabled globally on S2 and specifically for VLAN 10. The trunk port, FastEthernet0/1, was configured as a trusted interface because it connects to the core network or another switch. The access port, FastEthernet0/18, which connects to PC-B, was configured to limit DHCP traffic to 5 packets per second to prevent flooding attacks.

After enabling DHCP snooping, verification using the show ip dhcp snooping command confirmed that snooping was active on VLAN 10. The trust and rate-limit settings were correctly applied to the respective ports. A DHCP renewal was performed from PC-B using the ipconfig

/release and ipconfig /renew commands. The binding table was then checked using show ip dhcp snooping binding, which displayed the MAC and IP address of PC-B along with the lease duration and the VLAN/interface used.

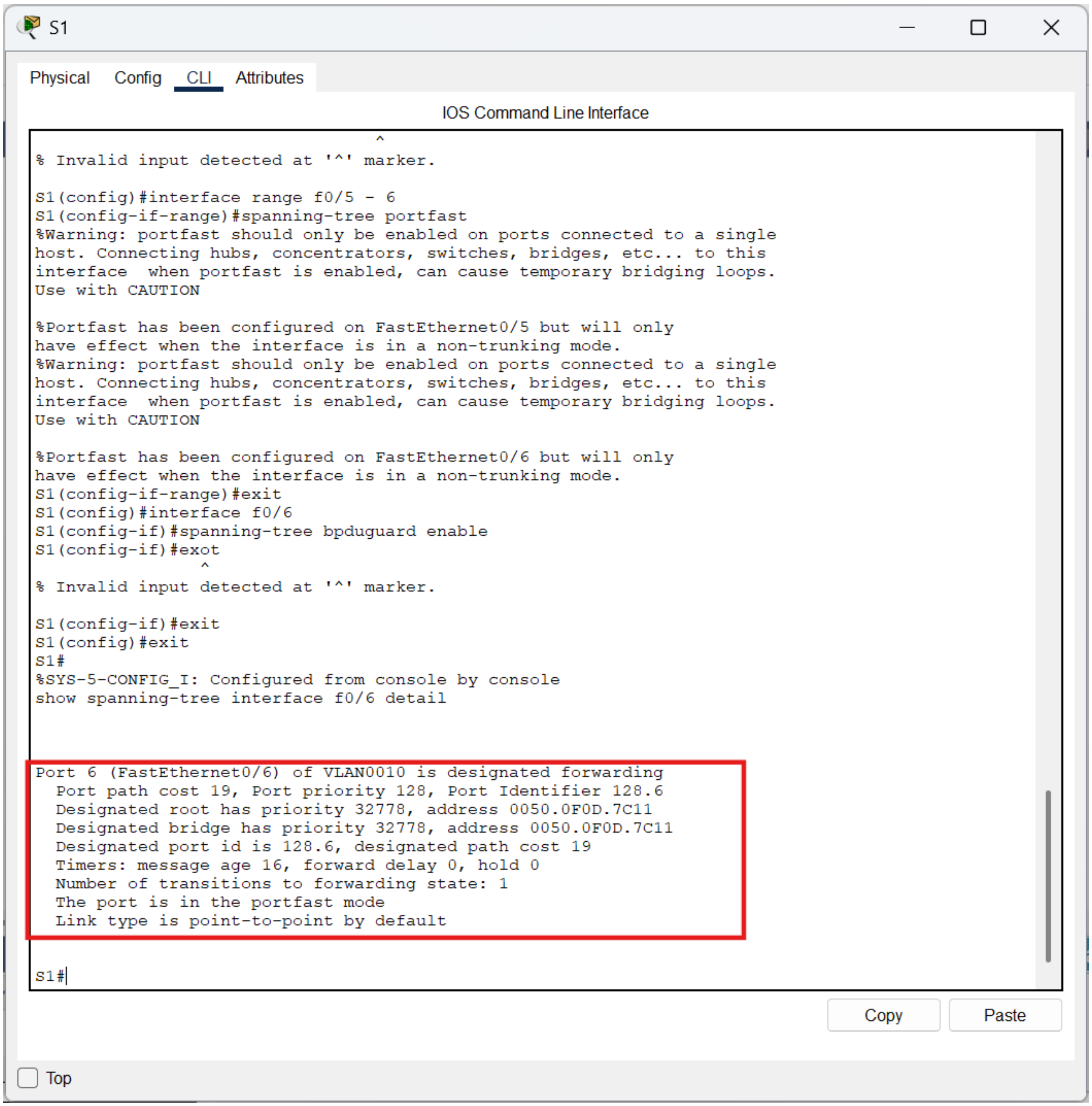


Step 6: Implement PortFast and BPDU Guard

To speed up the transition of access ports into the forwarding state and prevent loops caused by accidental switch connections, PortFast was enabled on all access ports in use. This included ports F0/5 and F0/6 on S1, and F0/18 on S2.

Additionally, BPDU Guard was enabled on access ports that connect to end devices. On S1, BPDU Guard was applied to port F0/6, which is connected to PC-A. On S2, it was enabled on F0/18, which connects to PC-B. This configuration helps ensure that if a device sends a BPDU (indicating it's acting like a switch), the port will shut down to protect the topology.

Verification using the show spanning-tree interface f0/6 detail command on S1 confirmed that PortFast was enabled and BPDU Guard was active. The port was shown to be in forwarding state, and no BPDUs had been received, indicating correct and secure operation.

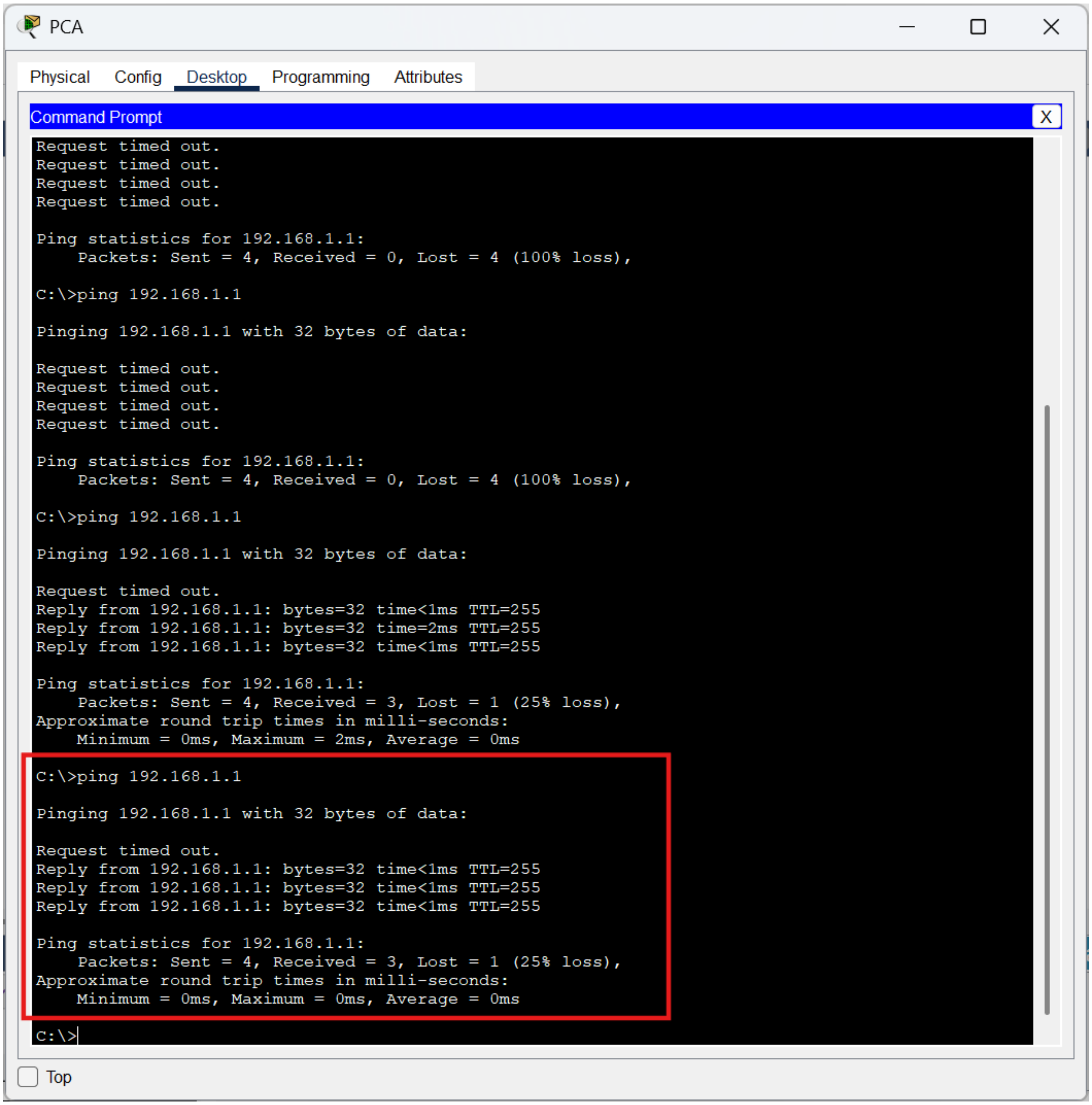



```
                                   ^
% Invalid input detected at '^' marker.

S1(config)#interface range f0/5 - 6
S1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

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

%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if-range)#exit
S1(config)#interface f0/6
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#exot
                ^
% Invalid input detected at '^' marker.

S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
show spanning-tree interface f0/6 detail


Port 6 (FastEthernet0/6) of VLAN0010 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.6
  Designated root has priority 32778, address 0050.0F0D.7C11
  Designated bridge has priority 32778, address 0050.0F0D.7C11
  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


S1#
```

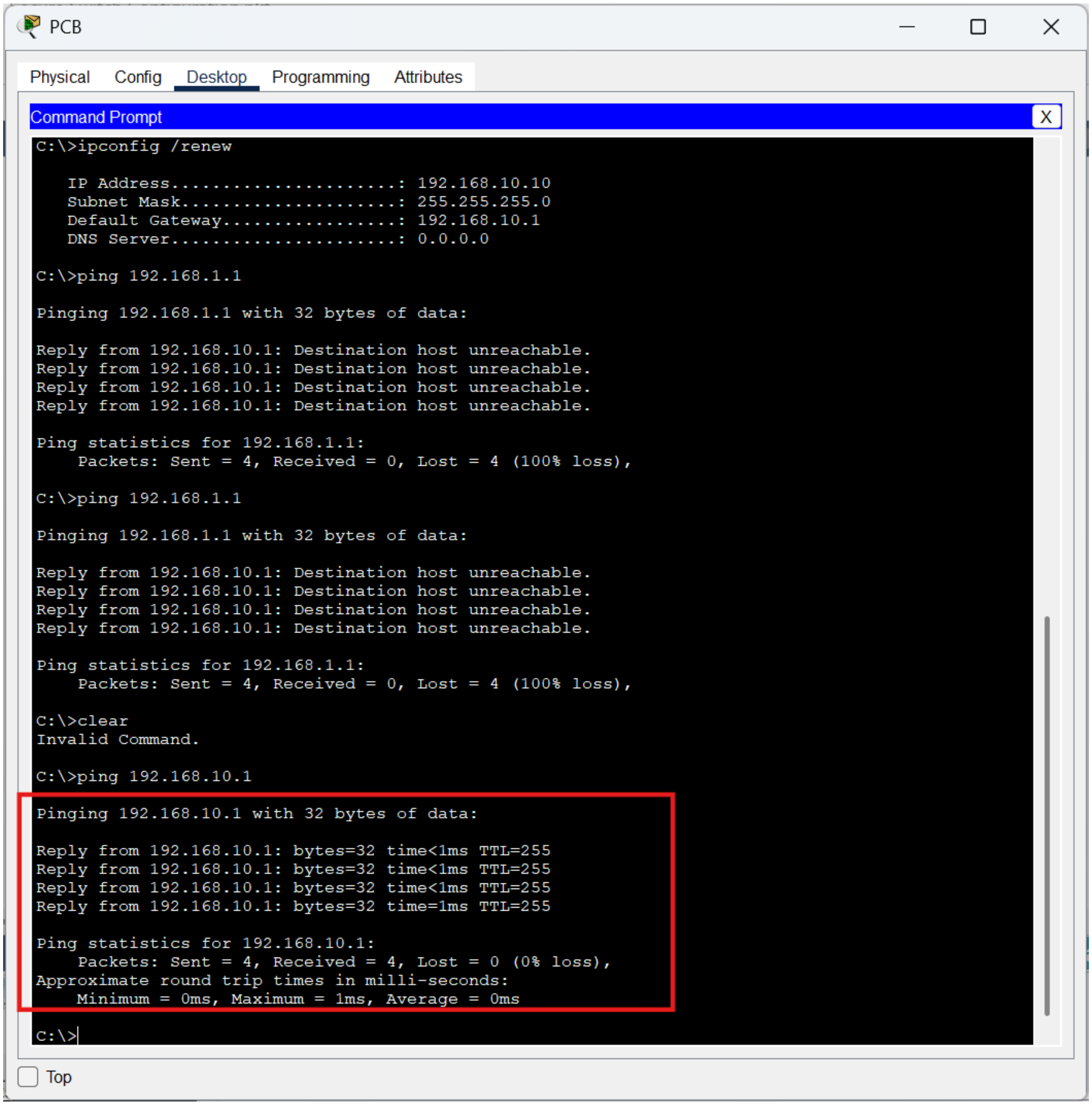
Step 7: Verify End-to-End Connectivity

To ensure your network is working correctly, test **ping connectivity** between all devices listed in the IP Addressing Table. This includes pings from PC-A to PC-B, to the switches' VLAN 10 interfaces, and to the router if one is configured. This step confirms that IP addressing, VLANs, trunking, and security configurations have all been set up correctly across the network.

PCA.



PCB.



Summary

After completing the configurations and analyzing the related questions, several key observations can be made regarding port security features and their impact on network behavior:

1. Sticky MAC Address Aging on S2:

When sticky learning is enabled, **some switches do not support aging timers** for sticky addresses. That's why no remaining age is displayed for sticky MACs on S2. The MAC address remains permanently unless manually cleared or the port is reset.

2. DHCP Failure Due to Port Security Limits:
If you apply the running config on S2 with port security on **F0/18**, **PC-B may not get an IP address** via DHCP. This is because:

- The port already has **two sticky MAC addresses** bound.
- The limit for MAC addresses is set to 2.
- The violation mode is **protect**, which silently drops additional frames without alerting the user or logging errors.

3. Aging Types – Absolute vs Inactivity:
Port security supports two aging modes:

- **Absolute aging** removes all secure addresses after the specified time expires, regardless of traffic activity.
- **Inactivity aging** removes secure addresses **only if no traffic** is seen from those addresses for the set duration, making it more flexible in dynamic environments.

Devices used.

The activity also involved troubleshooting network issues such as DHCP failures, incorrect IP assignments, and inter-VLAN connectivity — all of which helped solidify our grasp of Layer 2 protocols and security practices. The following devices and resources were used in the lab:

- **1 Router**: Cisco 4221 (Cisco IOS XE Release 16.9.3 universal image)
- **2 Switches**: Cisco Catalyst 2960 (Cisco IOS Release 15.0(2) lanbasek9 image)
- **2 PCs**: Windows OS (with command-line interface tools)

Conclusion.

Through this configuration exercise, I successfully set up VLANs, trunking, switch security features, port security, DHCP snooping, and BPDU guard to create a secure and segmented switched network. Each step enhanced both the **functionality** and **security posture** of the network, ensuring controlled access, minimized threats, and reliable device communication. This lab not only reinforced practical switch configuration skills but also highlighted how each setting affects real-time network behavior.