CLOUD AND NETWORK SECURITY

CHARLES GITHINJI

CS-CNS07-24006

Week 4: Assignment 1

Packet Tracer: Switch Security Configuration

INTRODUCTIONS

This is a compressive lab to review Layer 2 security features. I did VLAN and secure Switch configuration. After the configurations, I will test the connectivity of the devices. The objectives of this lab include:

1. Part 1: Configure the Network Devices. • Cable the network
    - Configure R1.
    - Configure and verify basic switch settings.
2. Part2: Configure VLANs on Switches.
    - Configure VLAN 10
    - Configure the SVI for VLAN 10

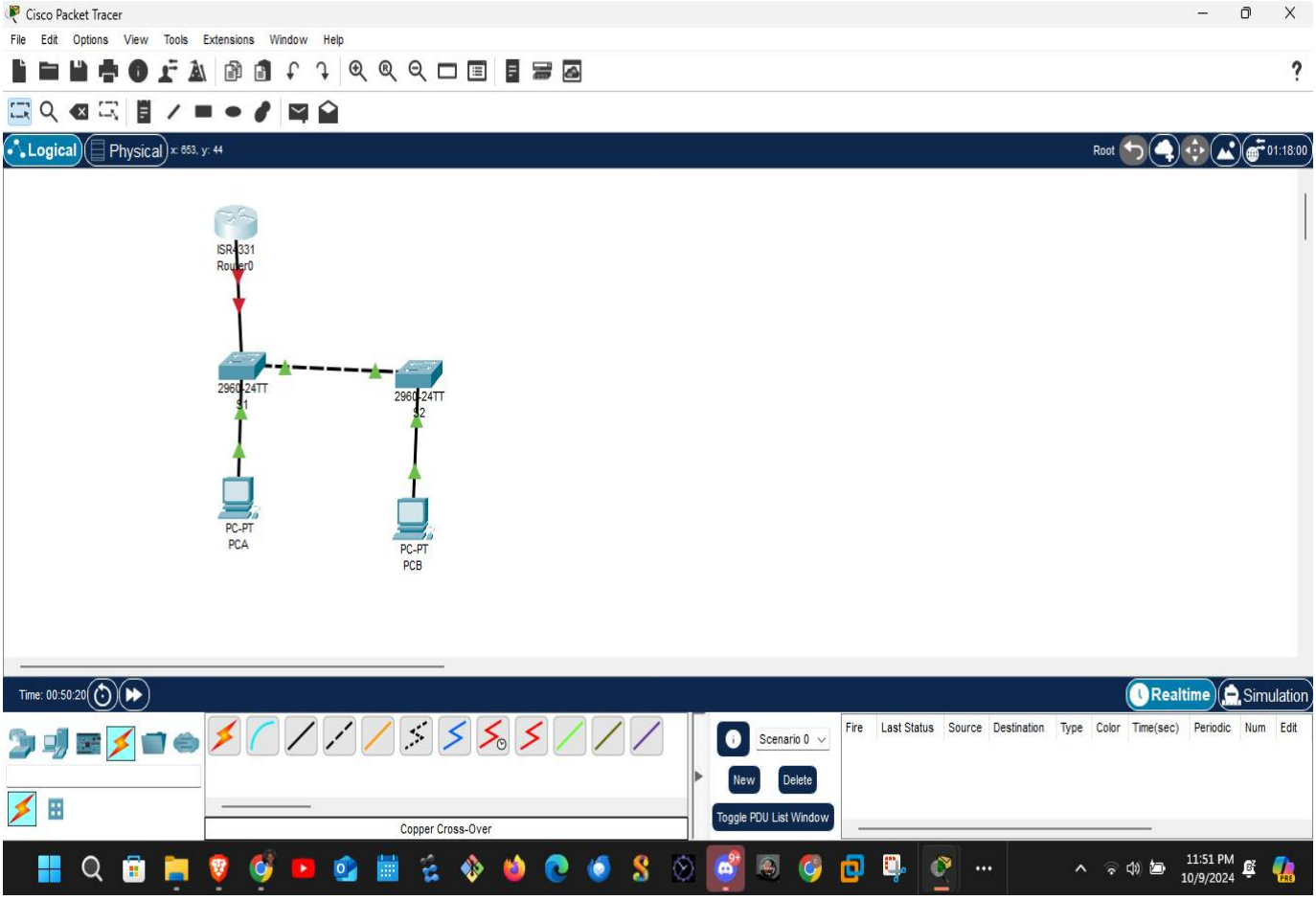
- Configure VLAN 333 with the name Native on S1 and S2.
- Configure VLAN 999 with the name ParkingLot on S1 and S2.

3. Part3: Configure Switch Security.
    - Implement 802.1Q trunking.
    - Configure access ports.
    - Secure and disable unused switchports.
    - Document and implement port security features.
    - Implement DHCP snooping security.
    - Implement PortFast and BPDU guard.
    - Verify end-to-end-connectivity.

Part 1: Configure the Network Devices.

Step 1: Cable the network.

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



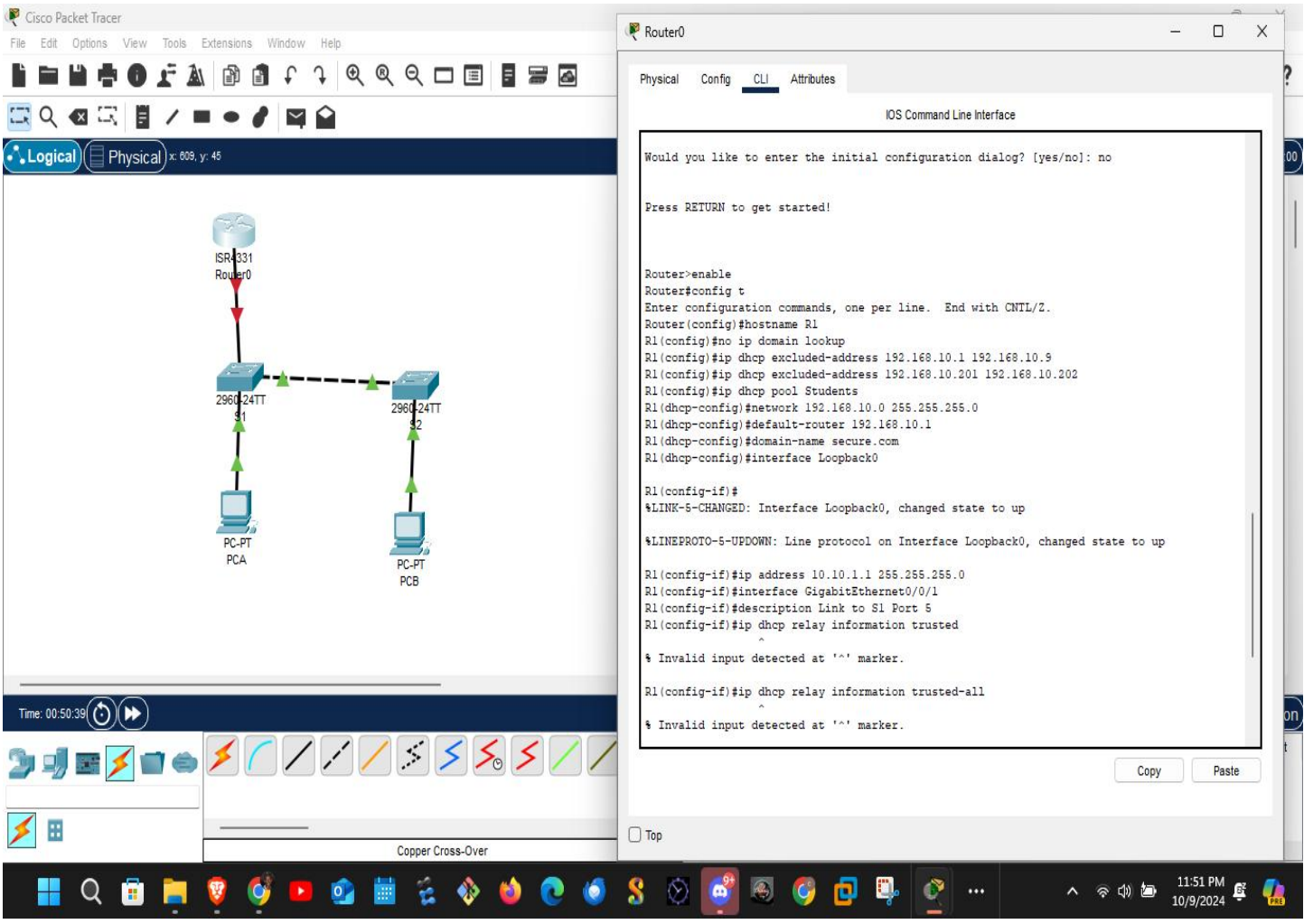
Step 2: Configure R1.

1. Load the following configuration script on R1.

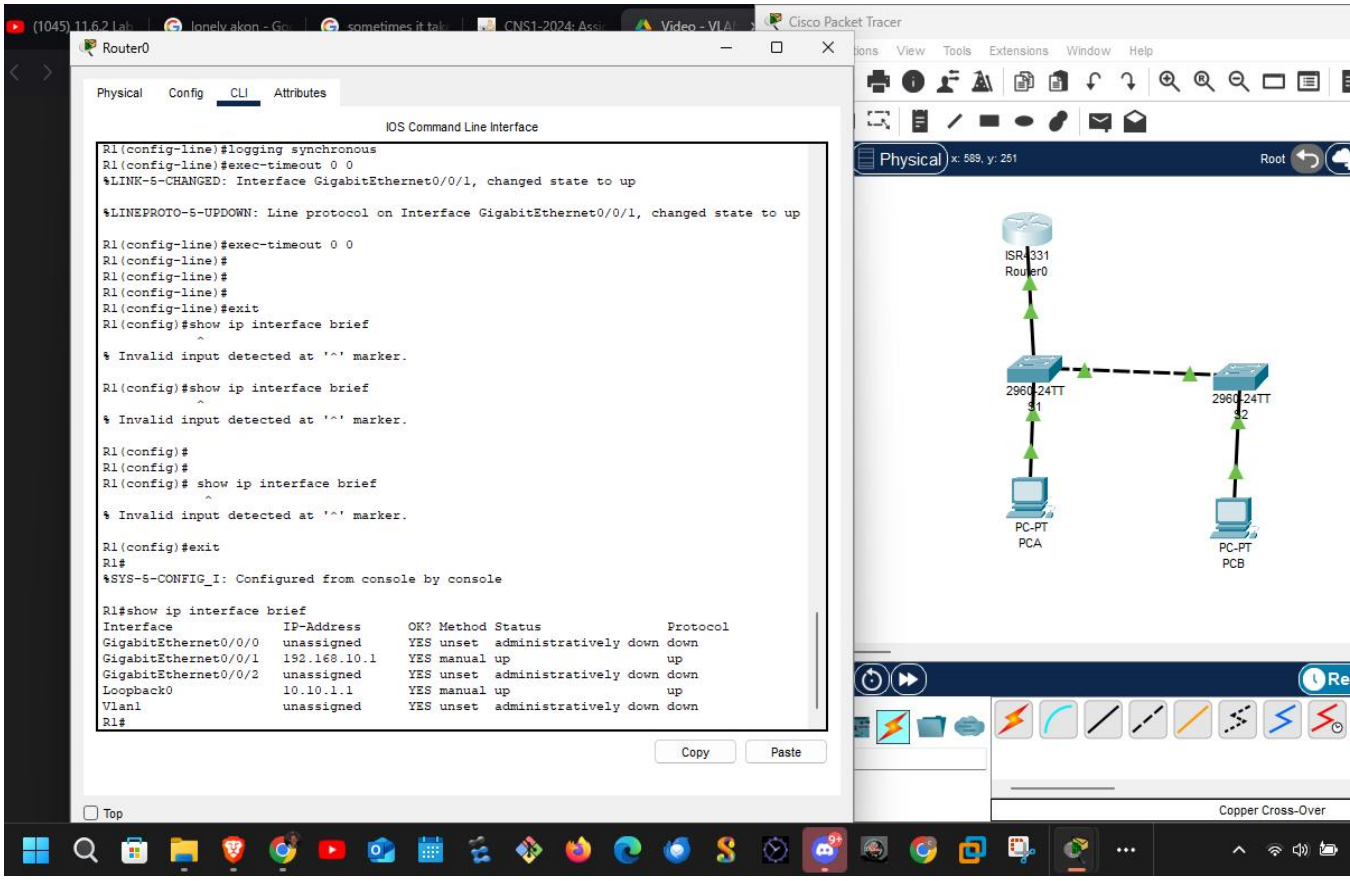
```
enable configure
terminal hostname
R1 no ip domain
lookup
ip dhcp excluded-address 192.168.10.1 192.168.10.9 ip
dhcp excluded-address 192.168.10.201 192.168.10.202
!
ip dhcp pool Students network
192.168.10.0 255.255.255.0 default-
router 192.168.10.1 domain-name
secure.com
!
interface Loopback0
```

ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet0/0/1
description Link to S1 Port 5 ip
dhcp relay information trusted

ip address 192.168.10.1 255.255.255.0
no shutdown
!
line con 0 logging
synchronous exec-
timeout 0 0



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



R1# show ip interface brief

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

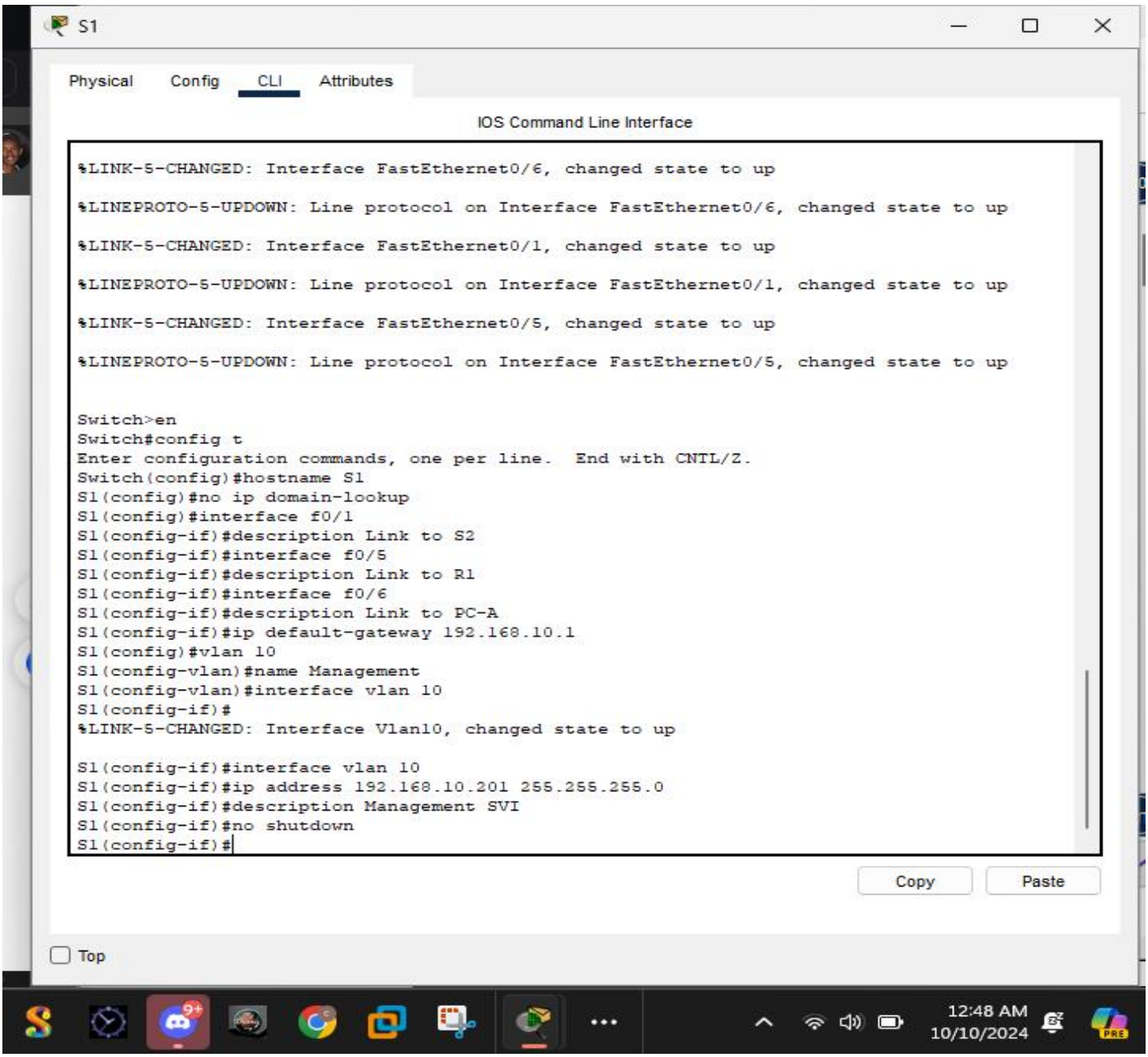
Step 3: Configure and verify basic switch settings.

1. Configure the hostname for switches S1 and S2.

   Open configuration window

   Switch# config t

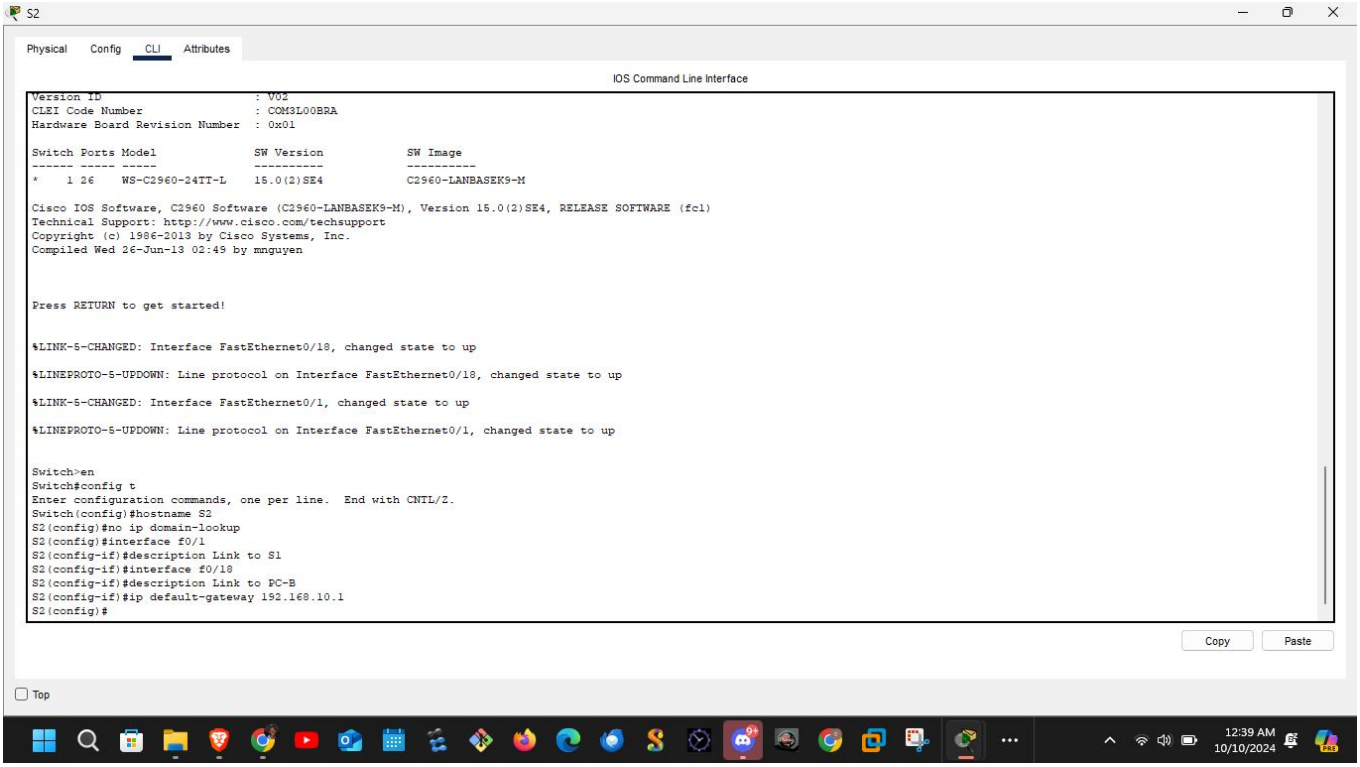
   Switch(config)# hostname S1



Open configuration window

Switch# config t

Switch(config)# hostname S2



2. Prevent unwanted DNS lookups on both switches.

   S1(config)# no ip domain-lookup

   S2(config)# no ip domain-lookup

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

   S1(config)# interface f0/1
   S1(config-if)# description Link to S2
   S1(config–if)# interface f0/5
   S1(config-if)# description Link to R1
   S1(config–if)# interface f0/6
   S1(config-if)# description Link to PC-A

S1

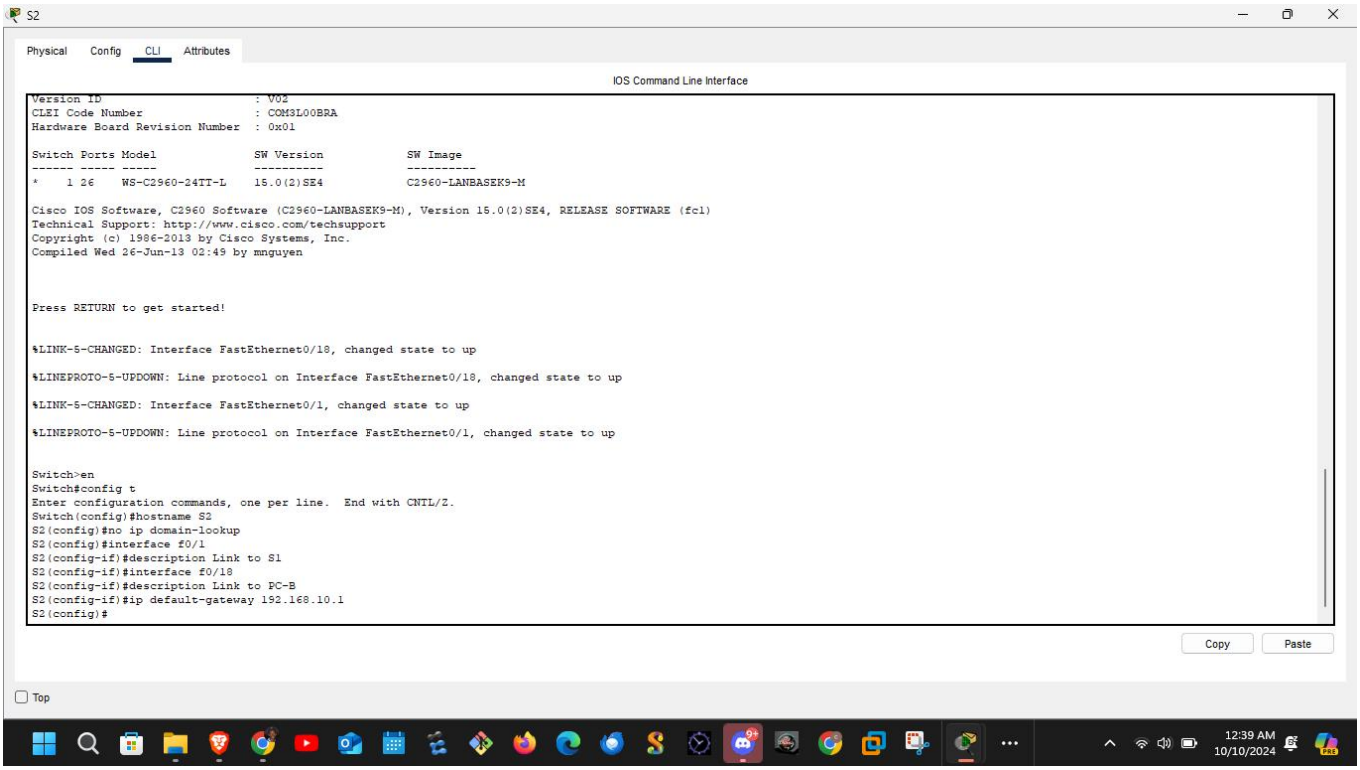
Physical Config CLI Attributes

IOS Command Line Int

```
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#interface f0/1
S1(config-if)#description Link to S2
S1(config-if)#interface f0/5
S1(config-if)#description Link to R1
S1(config-if)#interface f0/6
S1(config-if)#description Link to PC-A
S1(config-if)#ip default-gateway 192.168.10.1
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#interface vlan 10
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S1(config-if)#interface vlan 10
S1(config-if)#ip address 192.168.10.201 255.255.255.0
S1(config-if)#description Management SVI
S1(config-if)#no shutdown
S1(config-if)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#interface vlan 10
S1(config-if)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#interface f0/1
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

S1(config-if)#switchport trunk native vlan 333
S1(config-if)#
```

Top

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



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

S1(config)# ip default-gateway 192.168.10.1
S2(config)# ip default-gateway 192.168.10.1
In the above figures respectivley for S1 and S2

Part 2: Configure VLANs on Switches.

Step 1: Configure VLAN 10.

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

S1

Physical Config CLI Attributes

IOS Command Line Interface

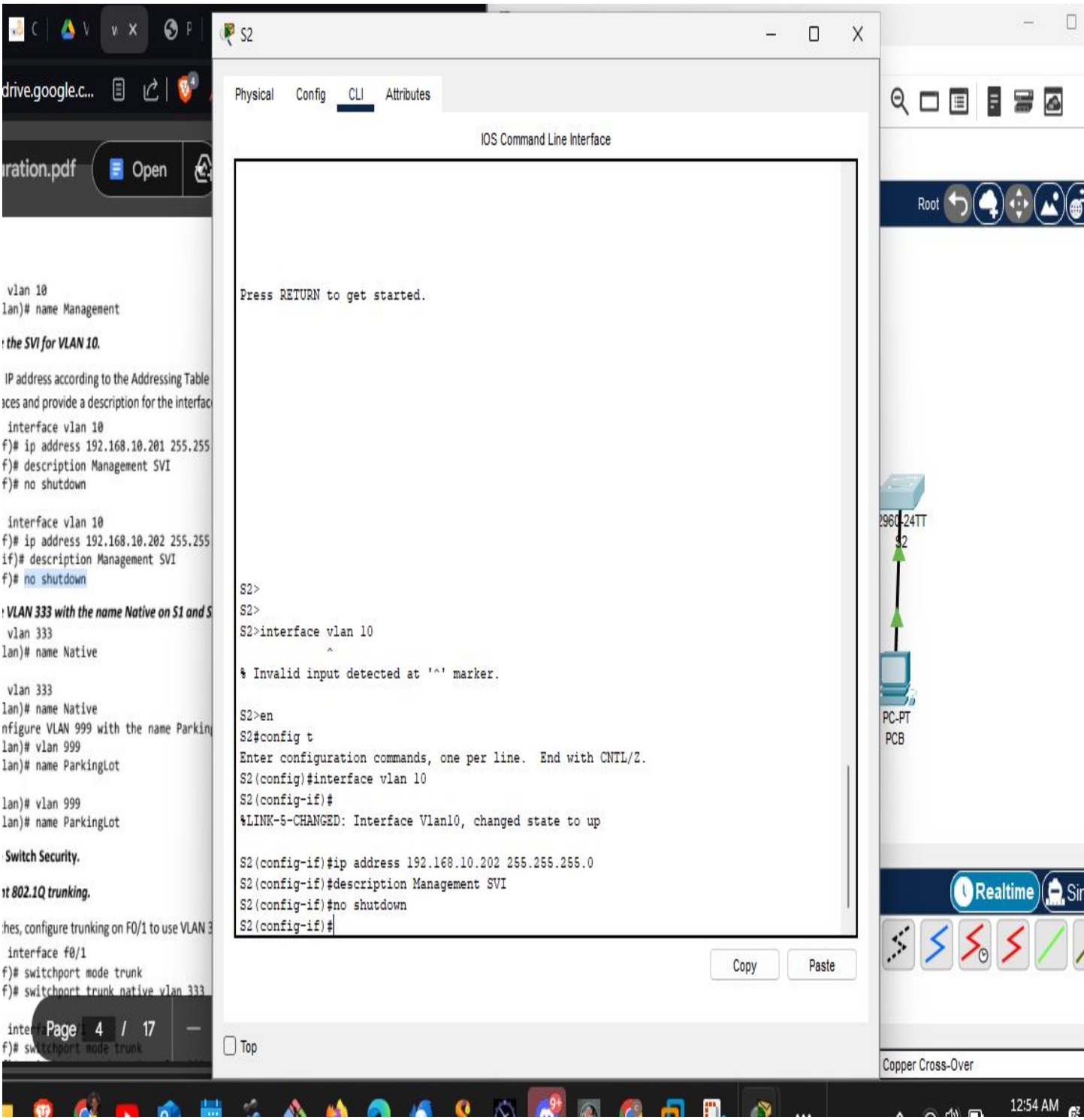
```
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, 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>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#interface f0/1
S1(config-if)#description Link to S2
S1(config-if)#interface f0/5
S1(config-if)#description Link to R1
S1(config-if)#interface f0/6
S1(config-if)#description Link to PC-A
S1(config-if)#ip default-gateway 192.168.10.1
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#interface vlan 10
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S1(config-if)#interface vlan 10
S1(config-if)#ip address 192.168.10.201 255.255.255.0
S1(config-if)#description Management SVI
S1(config-if)#no shutdown
S1(config-if)#
```

Copy Paste

Top

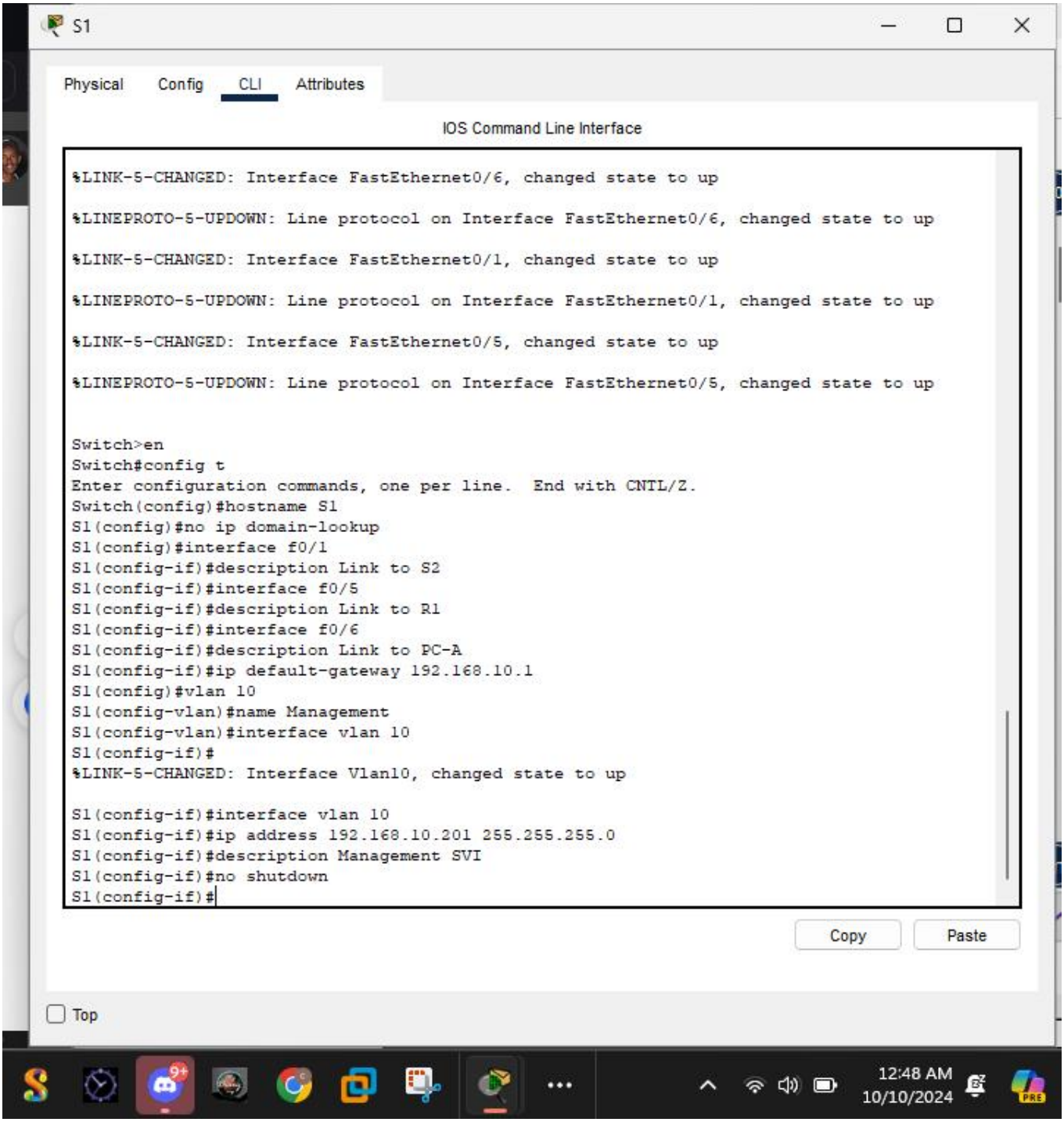
12:48 AM
10/10/2024

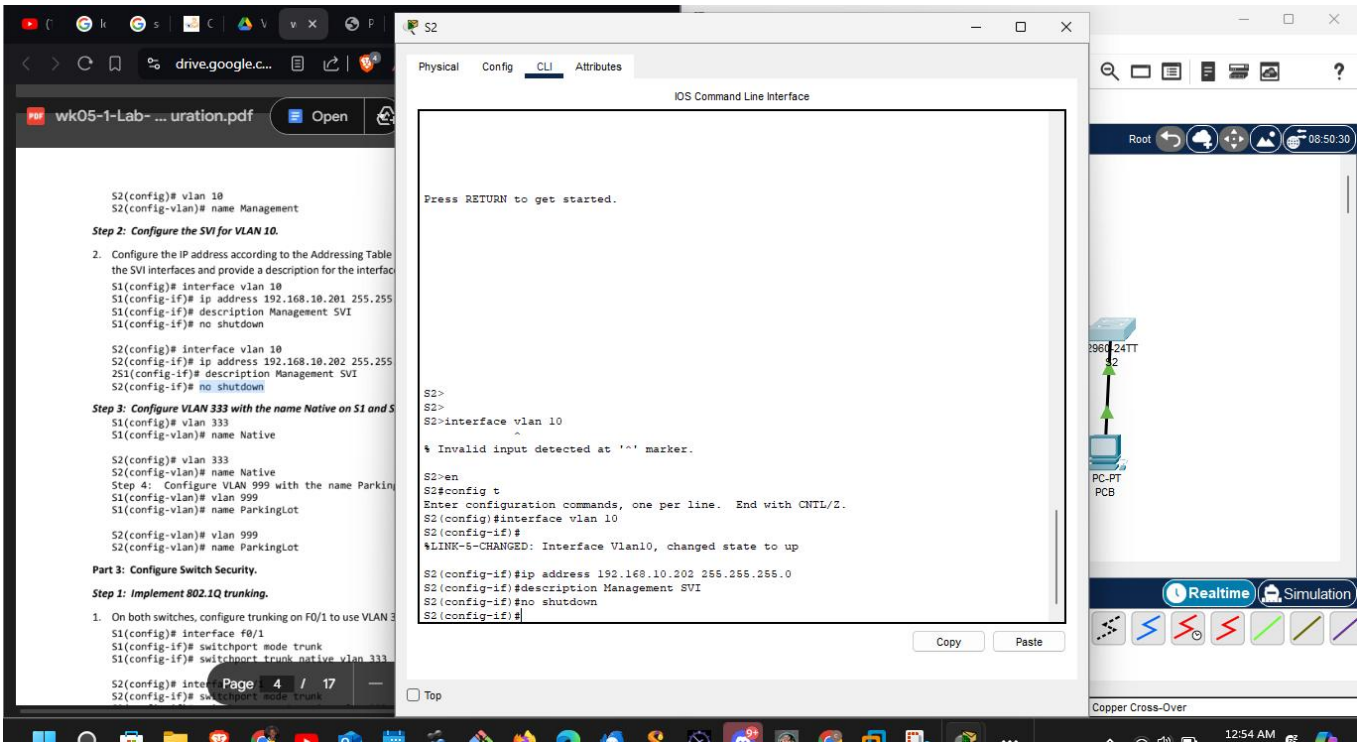
2


S2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Press RETURN to get started.
S2>
S2>
S2>interface vlan 10
^
% Invalid input detected at '^' marker.
S2>en
S2#config t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface vlan 10
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
S2(config-if)#ip address 192.168.10.202 255.255.255.0
S2(config-if)#description Management SVI
S2(config-if)#no shutdown
S2(config-if)#
Copy
Paste
Top
Root
PC-PT
PCB
Realtime
Copper Cross-Over
12:54 AM
Page 4 / 17

Step 2: Configure the SVI for VLAN 10.

2. 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.





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

S1

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#interface f0/1
S1(config-if)#description Link to S2
S1(config-if)#interface f0/5
S1(config-if)#description Link to R1
S1(config-if)#interface f0/6
S1(config-if)#description Link to PC-A
S1(config-if)#ip default-gateway 192.168.10.1
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#interface vlan 10
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S1(config-if)#interface vlan 10
S1(config-if)#ip address 192.168.10.201 255.255.255.0
S1(config-if)#description Management SVI
S1(config-if)#no shutdown
S1(config-if)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#interface vlan 10
S1(config-if)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#interface f0/1
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

S1(config-if)#switchport trunk native vlan 333
S1(config-if)#
```

Top

Physical Config CLI Attributes

IOS Command Line Interface

```
Press RETURN to get started.

S2>enable
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int vlan 10
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S2(config-if)#ip add 192.168.10.202 255.255.255.0
S2(config-if)#description Management SVI
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#
```

Copy Paste

☐ Top

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

Physical Config CLI Attributes

IOS Command Line Interface

```
S1>enable
S1#ip int show brief
      ^
% Invalid input detected at '^' marker.

S1#ip show int brief
      ^
% Invalid input detected at '^' marker.

S1#config t
Enter configuration commands, one per line.  End with CNTL/
Z.
S1(config)#int vlan 10
S1(config-if)#ip add 192.168.10.201 255.255.255.0
S1(config-if)#description Management SVI
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#
```

Copy Paste

☐ Top

Physical Config CLI Attributes

IOS Command Line Interface

```
Press RETURN to get started.


S2>enable
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int vlan 10
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S2(config-if)#ip add 192.168.10.202 255.255.255.0
S2(config-if)#description Management SVI
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#vlan 999
S2(config-vlan)#name ParkingLot
S2(config-vlan)#
```

Copy Paste

Top

Part 3: Configure Switch Security.

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

S1

Physical Config CLI Attributes

IOS Command Line Interface

```
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#interface f0/1
S1(config-if)#description Link to S2
S1(config-if)#interface f0/5
S1(config-if)#description Link to R1
S1(config-if)#interface f0/6
S1(config-if)#description Link to PC-A
S1(config-if)#ip default-gateway 192.168.10.1
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#interface vlan 10
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S1(config-if)#interface vlan 10
S1(config-if)#ip address 192.168.10.201 255.255.255.0
S1(config-if)#description Management SVI
S1(config-if)#no shutdown
S1(config-if)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#interface vlan 10
S1(config-if)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#interface f0/1
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

S1(config-if)#switchport trunk native vlan 333
S1(config-if)#
```

Top

Physical Config CLI Attributes

IOS Command Line Interface

```
S2>ena
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int f0/1
S2(config-if)#switchport mode trunk

S2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed
state to up

S2(config-if)#switchport trunk native vlan 333
S2(config-if)#%SPANTREE-2-RECV_PVID_ERR: Received BPDU with
inconsistent peer vlan id 1 on FastEthernet0/1 VLAN333.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0333.
Inconsistent local vlan.


S2(config-if)#
```

Copy Paste

☐ Top

2. Verify that trunking is configured on both switches.

Physical Config CLI Attributes

IOS Command Line Interface

```
Enter configuration commands, one per line.  End with CNTL/
Z.
S1(config)#int
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch
discovered on FastEthernet0/1 (1), with S2 FastEthernet0/1
(333)
% Incomplete command.
S1(config)#int f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 333
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

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#
```

Copy Paste

☐ Top

S1

Physical Config CLI Attributes

IOS Command Line Interface

```
vlan.


%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.


S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

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

Copy Paste

Top

1:13 AM
10/10/2024

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

Physical Config CLI Attributes

IOS Command Line Interface

```
(333)
% Incomplete command.
S1(config)#int f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 333
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

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 t
Enter configuration commands, one per line.  End with CNTL/
Z.
S1(config)#int f0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#
```

Copy Paste

☐ Top

Physical Config CLI Attributes

IOS Command Line Interface

```
FastEthernet0/1 (333), with S1 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)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#show int 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

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

Copy Paste

☐ Top

4. Verify with the show interfaces command.

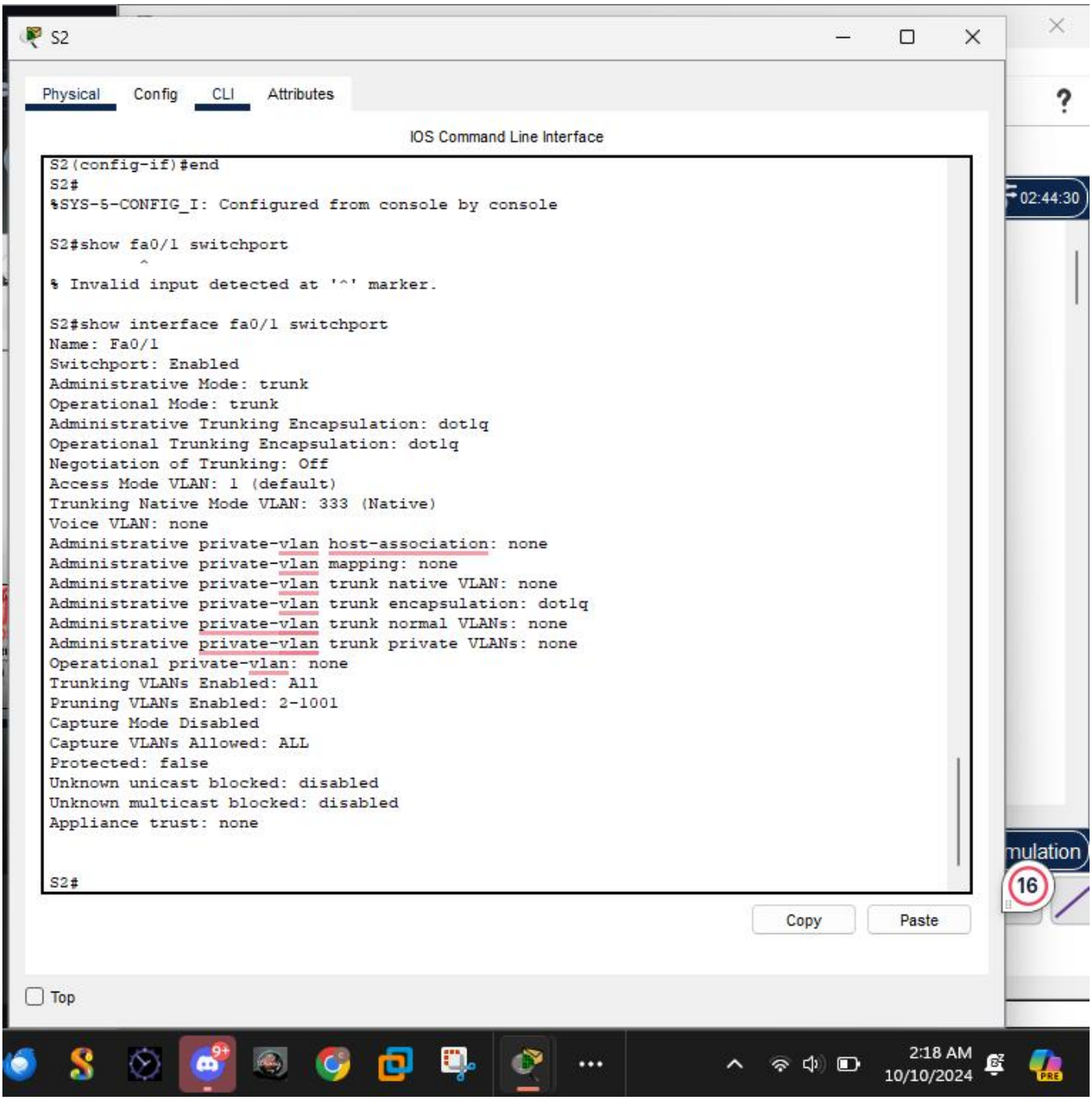
Physical Config CLI Attributes

IOS Command Line Interface

```
Press RETURN to get started.

S1>ena
S1#config t
Enter configuration commands, one per line.  End with CNTL/
Z.
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show int f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S1#
```

Copy Paste

☐ Top



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

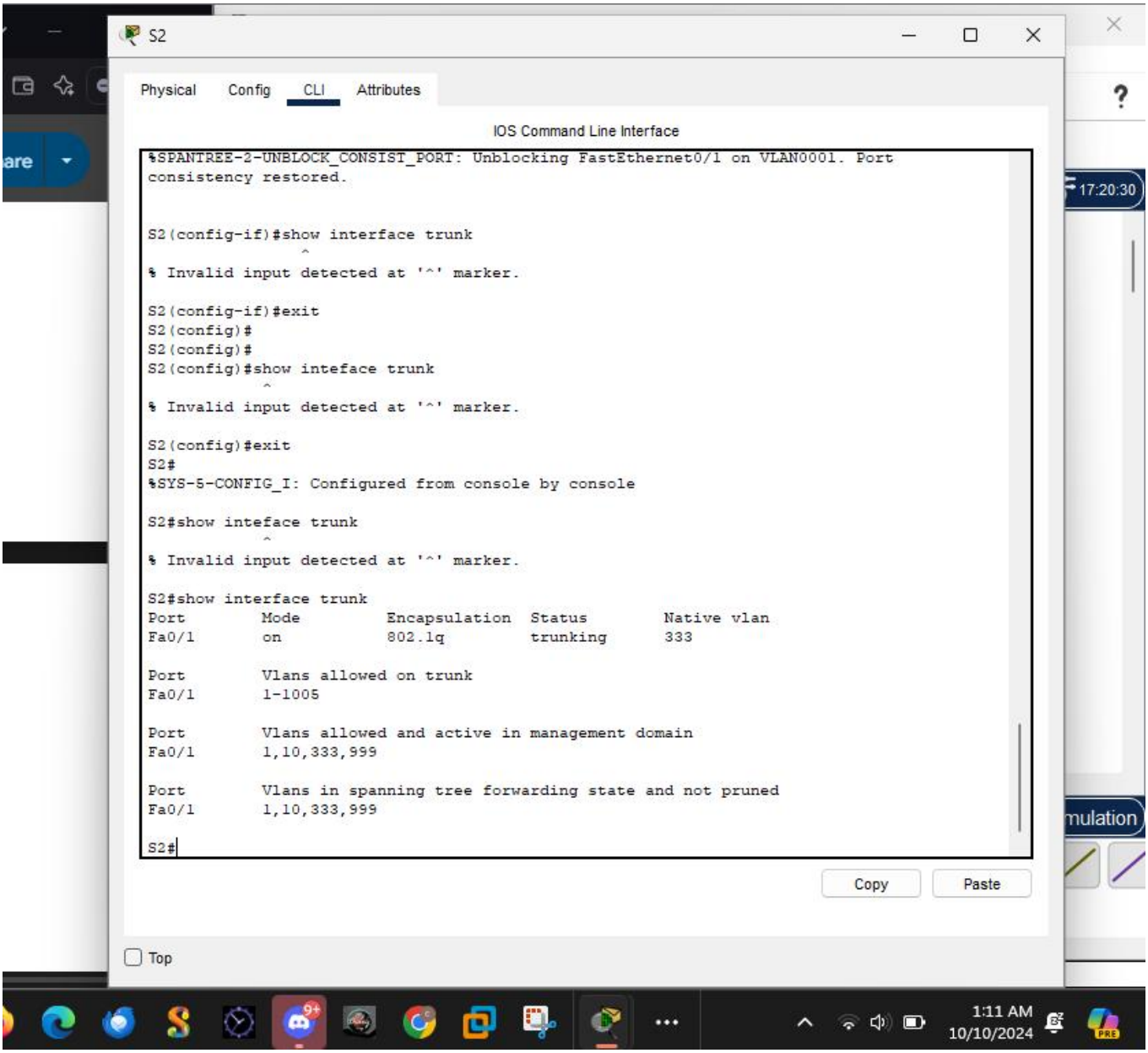
IOS Command Line Interface

```
Press RETURN to get started.



S1>ena
S1#config t
Enter configuration commands, one per line.  End with CNTL/
Z.
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show int f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S1#config t
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)#
```

Copy Paste

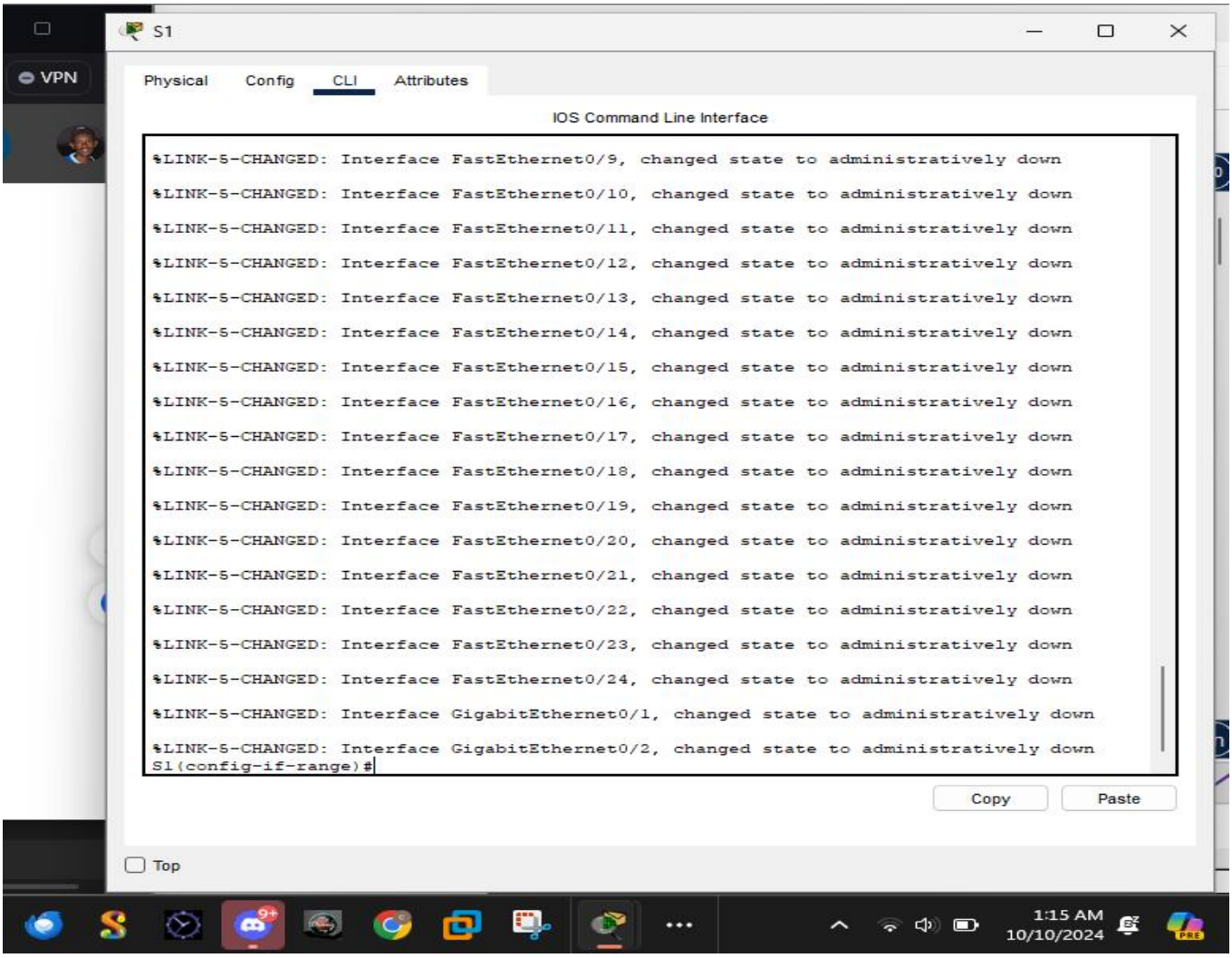
☐ Top

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

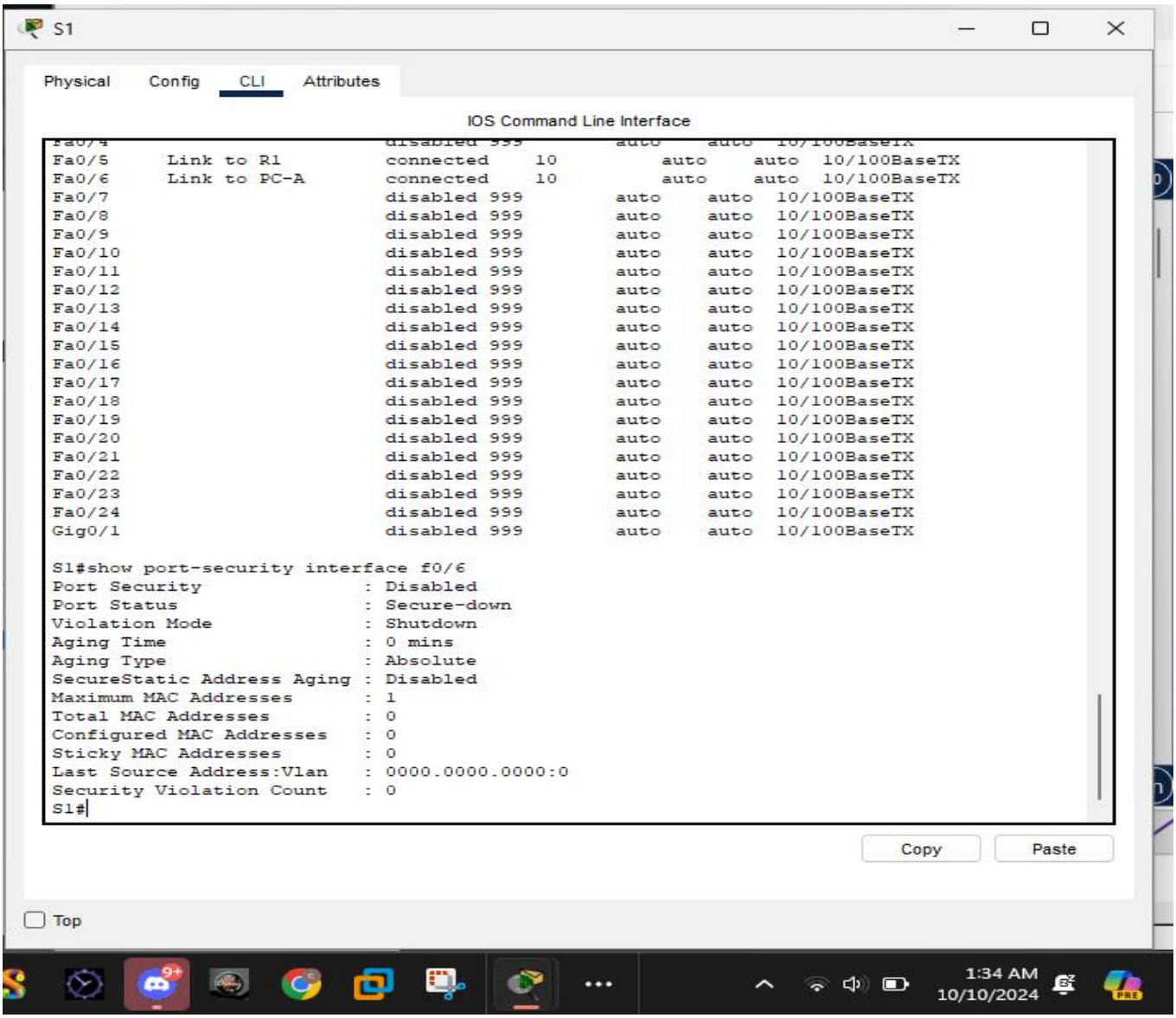
Physical Config CLI Attributes

IOS Command Line Interface

```
S1>
S1>en
S1#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Link 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     Link to R1         connected    10         auto    auto  10/100BaseTX
Fa0/6     Link 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--
```

Copy Paste

Top



3. v

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. Record your answers in the table below.

S1

Physical Config CLI Attributes

IOS Command Line Interface

```
Fa0/4                           disabled 999          auto    auto  10/100BaseTX
Fa0/5     Link to R1            connected    10          auto    auto  10/100BaseTX
Fa0/6     Link 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

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#
```

Copy Paste

Top

1:34 AM
10/10/2024

Physical Config CLI Attributes

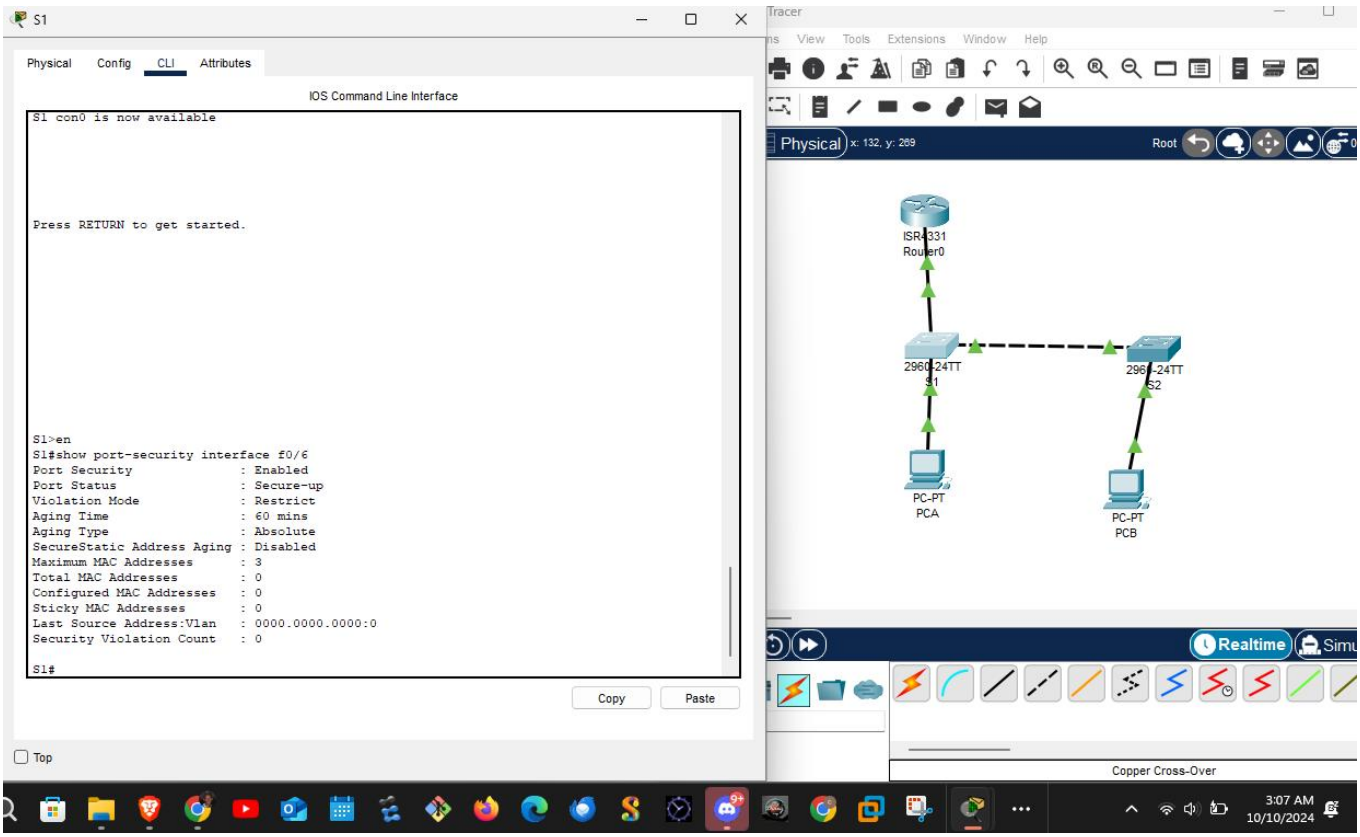
IOS Command Line Interface

```
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

S2#
S2#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
S2#
```

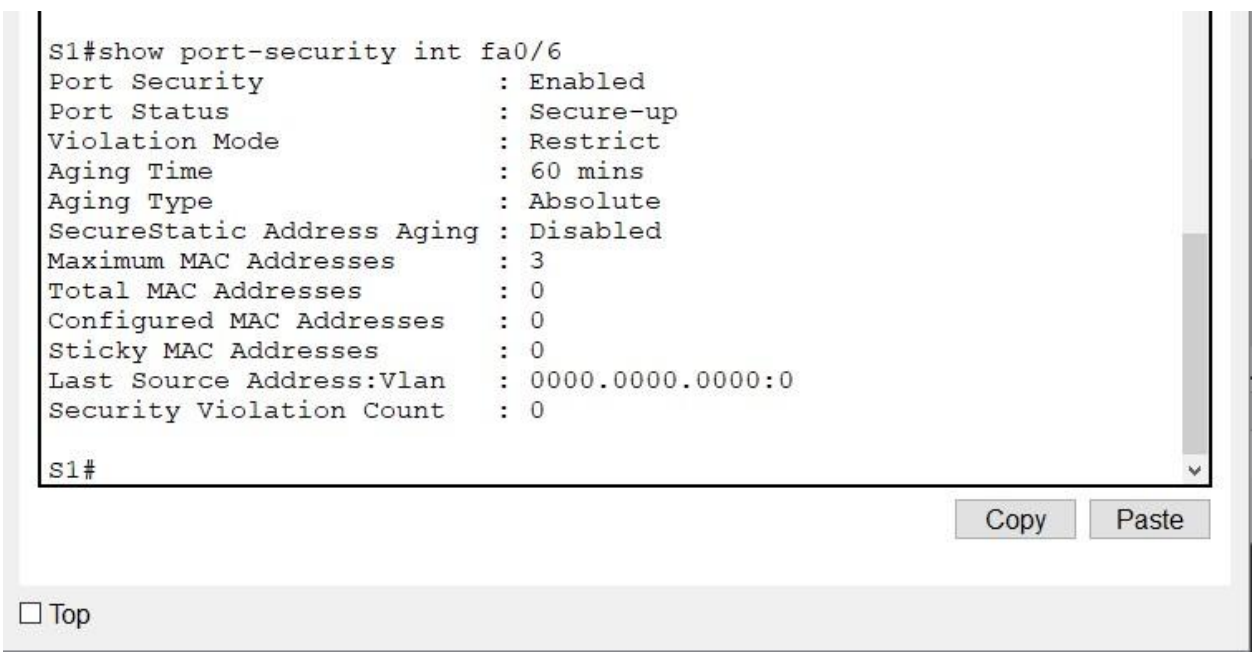
Copy Paste

☐ Top

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



3. Verify port security on S1 F0/6.



```
S1#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
S1#
```

Copy Paste

☐ Top

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.

```
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int fa0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security mac-address sticky
```

5. Configure the following port security settings on S2 F/18:
   - Maximum number of MAC addresses: **2**
   - Violation type: **Protect**
   - Aging time: **60 min**

```
S2(config-if)#switchport port-security maximum 2
S2(config-if)#switchport port-security violation protect
S2(config-if)#switchport port-security aging time 60
S2(config-if)#
```

6. Verify port security on S2 F0/18.

```
S2#show port-security int 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        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

S2#
```

Copy Paste

☐ Top

```
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#
```

Copy Paste

☐ Top

Step 5: Implement DHCP snooping security.

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

S2

Physical Config CLI Attributes

IOS Command Line Interface

```
----------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#ip dhcp snooping
S2(config)#ip dhcp snooping vlan 10
S2(config)#int f0/1
S2(config-if)#ip dhcp snooping trust
S2(config-if)#exit
S2(config)#int f0/18
S2(config-if)#dhcp snooping ?
% Unrecognized command
S2(config-if)#ip dhcp snooping ?
  limit  DHCP Snooping limit
  trust  DHCP Snooping trust config
S2(config-if)#ip dhcp snooping
S2(config)#ip dhcp snooping limit ?
% Unrecognized command
S2(config)#ip dhcp snooping limit rate 5
                              ^
% Invalid input detected at '^' marker.

S2(config)#ip dhcp snooping limit rate 5
                              ^
% Invalid input detected at '^' marker.

S2(config)#ip dhcp snooping ?
  database     DHCP Snooping database agent
  information  DHCP Snooping information
  verify       DHCP Snooping verify
  vlan         DHCP Snooping vlan
  <cr>
S2(config)#int f0/18
S2(config-if)#ip dhcp snooping rate 5
                               ^
% Invalid input detected at '^' marker.

S2(config-if)#ip dhcp snooping limit rate 5
S2(config-if)#
```

Copy Paste

Top

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

```
S2(config)#int f0/1
S2(config-if)#ip dhcp snooping trust
S2(config-if)#exit
```

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

```
S2(config)#int f0/18
S2(config-if)#ip dhcp snooping rate 5
                               ^
% Invalid input detected at '^' marker.

S2(config-if)#ip dhcp snooping limit rate 5
S2(config-if)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console
```

4. Verify DHCP Snooping on S2.

S2

Physical Config CLI Attributes

IOS Command Line Interface

```
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#ip dhcp snooping limit rate 5
S2(config-if)#end
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/1            yes        unlimited
FastEthernet0/18           no         5
S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   Management                       active    Fa0/18
333  Native                           active
999  ParkingLot                       active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S2#
```

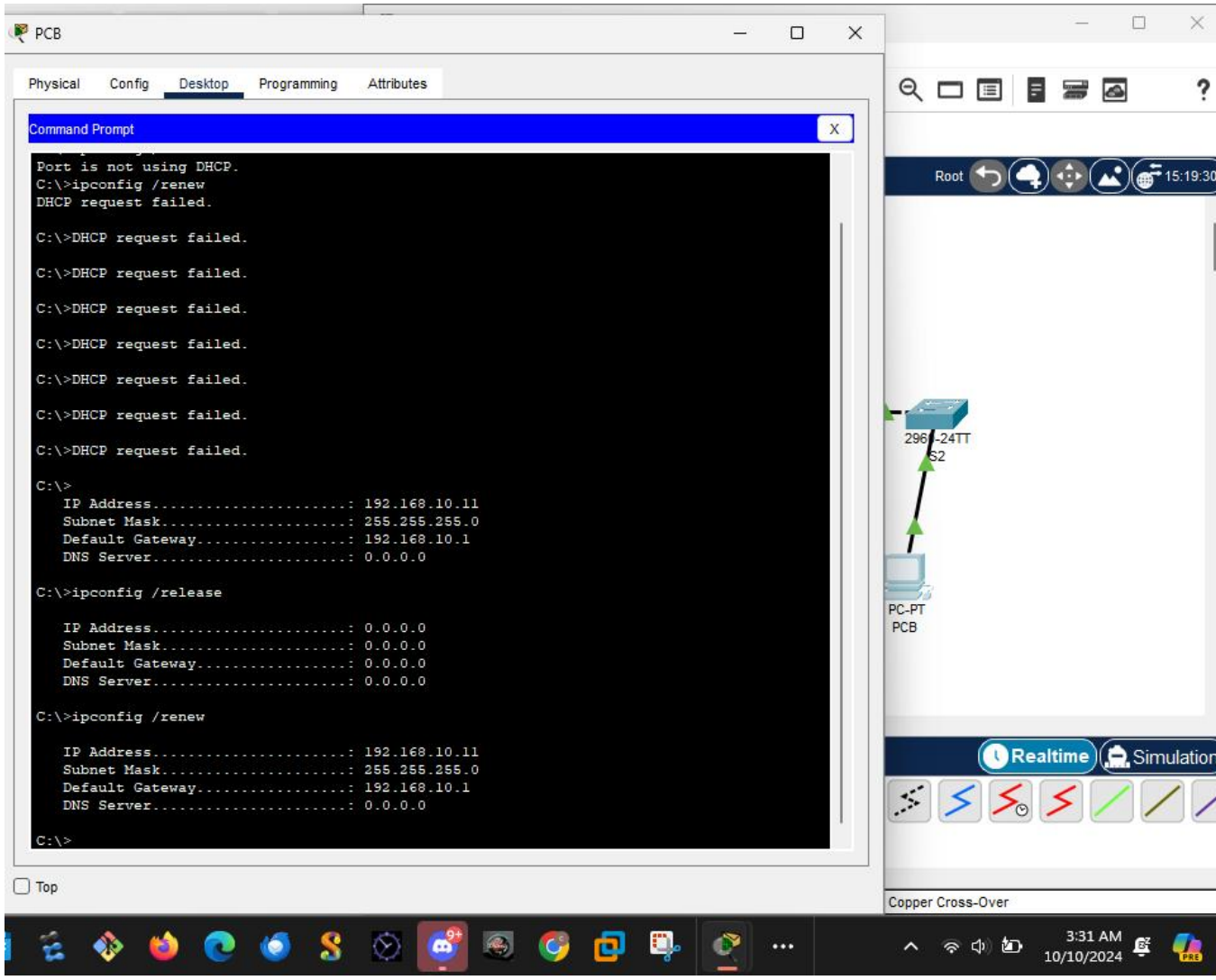
Copy Paste

Top

3:25 AM
10/10/2024

2
5.

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



3

At first I had problem as the request was failing but I resolved the issue

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /release
Port is not using DHCP.
C:\>ipconfig /renew
DHCP request failed.

C:\>DHCP request failed.

C:\>
```

Top

S1

Physical Config CLI Attributes

IOS Command Line Interface

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

S1#show port-security interface f0/6
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 60 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 3
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#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   Management                       active    Fa0/5, Fa0/6
333  Native                           active
999  ParkingLot                       active    Fa0/2, Fa0/3, Fa0/4, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S1#
```

Copy Paste

Top

3:26 AM
10/10/2024

S2

Physical Config CLI Attributes

IOS Command Line Interface

```
Interface                  Trusted    Rate limit (pps)
------------------------   -------    ----------------
FastEthernet0/1            yes        unlimited
FastEthernet0/18           no         5
S2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
10   Management                       active    Fa0/18
333  Native                           active
999  ParkingLot                       active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
S2#no dhcp snooping
      ^
% Invalid input detected at '^' marker.

S2#noip dhcp snooping
        ^
% Invalid input detected at '^' marker.

S2#no ip dhcp snooping
      ^
% Invalid input detected at '^' marker.

S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#no ip dhcp snooping
S2(config)#
```

Copy Paste

Top

3:30 AM
10/10/2024

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

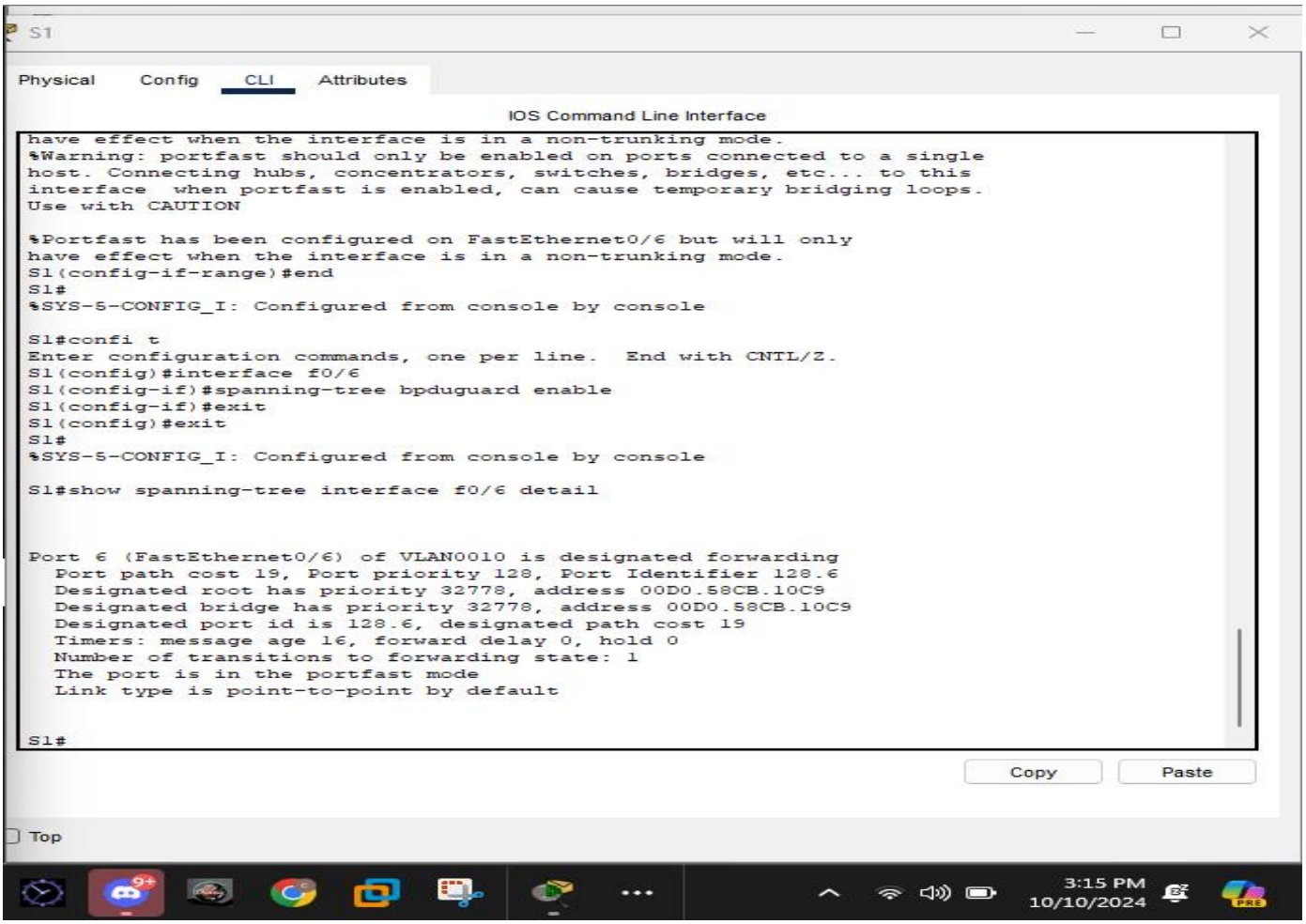
```
S2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type
VLAN  Interface
------------------  ---------------  ----------  -------------
----  -----------------
Total number of bindings: 0
S2#
```

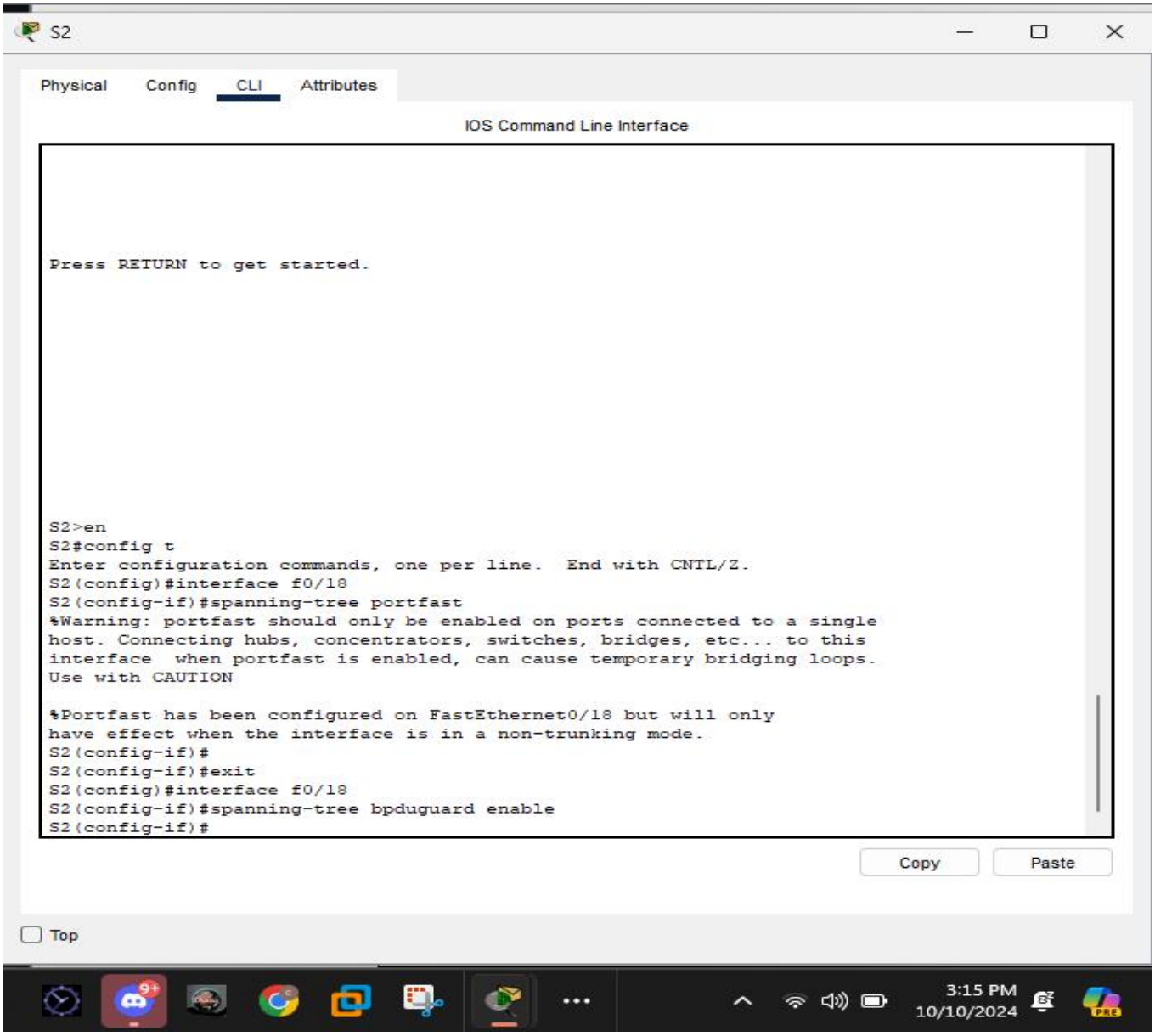
Copy Paste

Top

Step 6: Implement PortFast and BPDU guard.

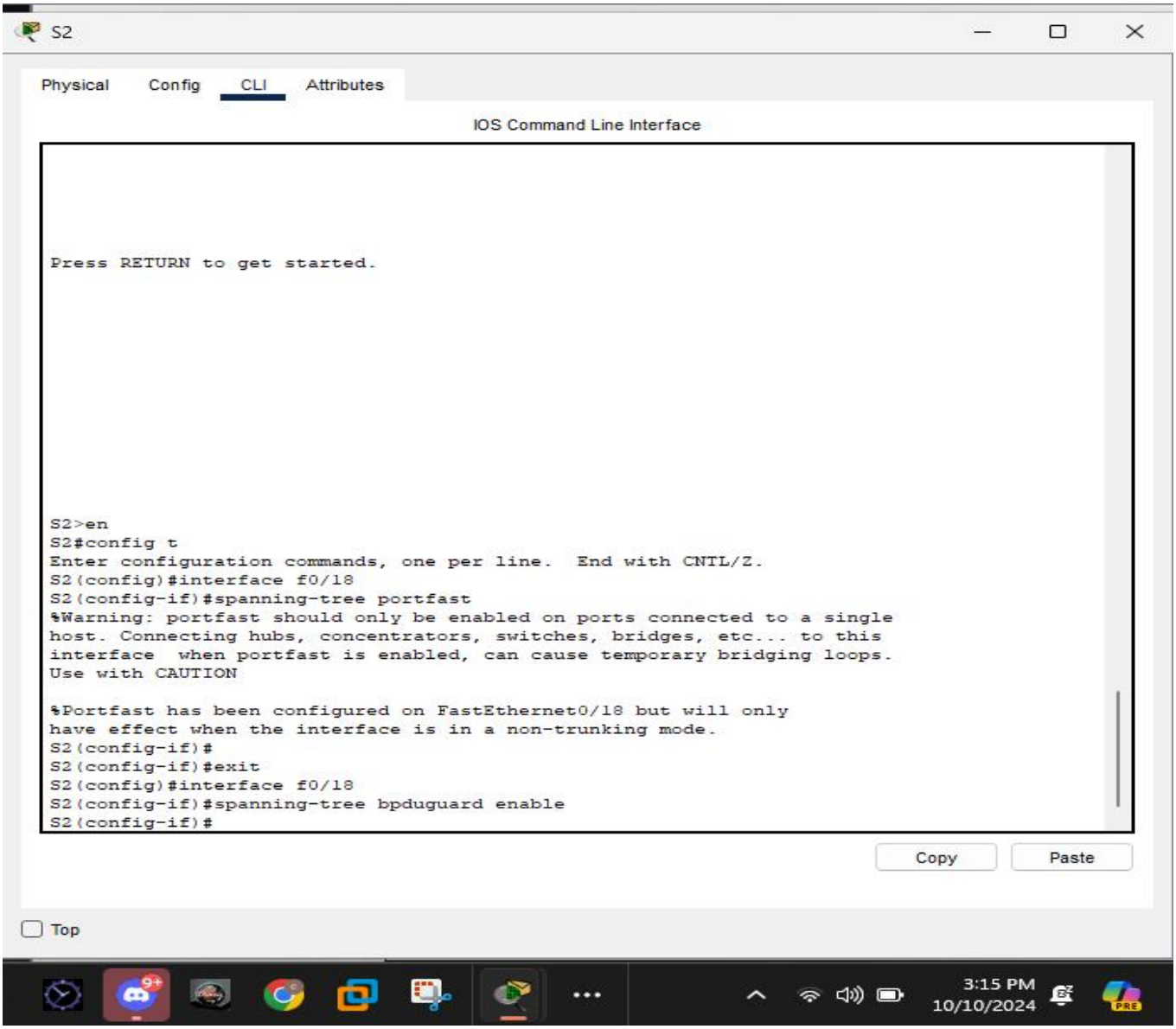
1. Configure PortFast on all the access ports that are in use on both switches.



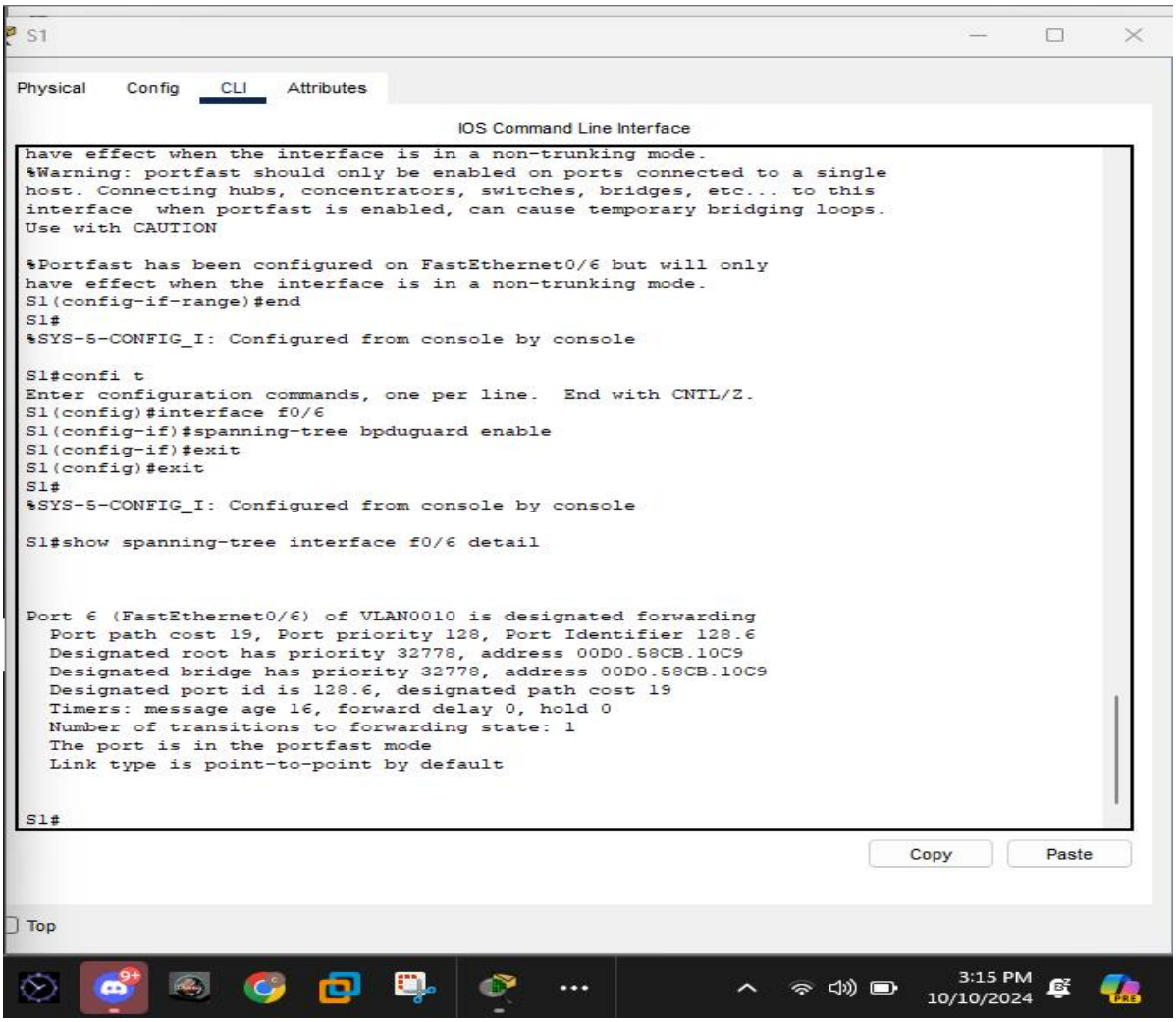


2.

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



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



Step 7: Verify end-to-end connectivity.

Verify PING connectivity between all devices in the IP Addressing Table. If the pings fail, you may need to disable the firewall on the PC hosts.

PC-A

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=3ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 3ms, Average = 1ms

C:\>ping 192.168.10.201

Pinging 192.168.10.201 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.201: bytes=32 time<1ms TTL=255
Reply from 192.168.10.201: bytes=32 time<1ms TTL=255
Reply from 192.168.10.201: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.201:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Top

```
C:\>ping 192.168.10.202

Pinging 192.168.10.202 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.202: bytes=32 time=1ms TTL=255
Reply from 192.168.10.202: bytes=32 time<1ms TTL=255
Reply from 192.168.10.202: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.202:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Close configuration window

Questions to answer

1. In reference to Port Security on S2, why is there no timer value for the remaining age in minutes when sticky learning was configured? This switch does not support the port security aging of sticky secure addresses.
2. In reference to Port Security on S2, if you load the running-config script on S2, why will PC-B on port 18 never get an IP address via DHCP? Port security is set for only two MAC addresses and port 18 has two “sticky” MAC address bound to the port. Additionally, the violation is protect, which will never send a console/syslog message or increment the violation counter.
3. In reference to Port Security, what is the difference between the absolute aging type and inactivity aging type? If the inactivity type is set, then the secure addresses on the port will be removed only if there is no data traffic from the secure source addresses for the specified time period. If the absolute type is set, then all secure addresses on this port age out exactly after the time specified ends

Device Configurations – Final

S2

Physical Config CLI Attributes

IOS Command Line Interface

```
S2#show running-config
Building configuration...

Current configuration : 3304 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S2
!
!
!
no ip domain-lookup
!
!
ip dhcp snooping vlan 10
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 description Link to S1 Port Fa0/1
 switchport trunk native vlan 333
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 --More--
```

Copy Paste

☐ Top

S1

Physical Config CLI Attributes

IOS Command Line Interface

```
interface FastEthernet0/2
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/3
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/4
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 description Link to R1 Port G0/0/1
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/6
 description Link to PC-A port Fa0/6
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security maximum 3
 switchport port-security violation restrict
 --More--
```

Copy Paste

Top

S1

Physical Config CLI Attributes

IOS Command Line Interface

```
 switchport port-security violation restrict
 switchport port-security aging time 60
 spanning-tree portfast
 spanning-tree bpduguard enable
!
interface FastEthernet0/7
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/8
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/9
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/10
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/11
 switchport access vlan 999
 switchport mode access
 shutdown
```

Copy Paste

☐ Top

S1

Physical Config CLI Attributes

IOS Command Line Interface

```
!
interface FastEthernet0/23
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/24
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface GigabitEthernet0/1
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface GigabitEthernet0/2
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description S1 Management vlan
 ip address 192.168.10.201 255.255.255.0
 --More--
```

Copy Paste

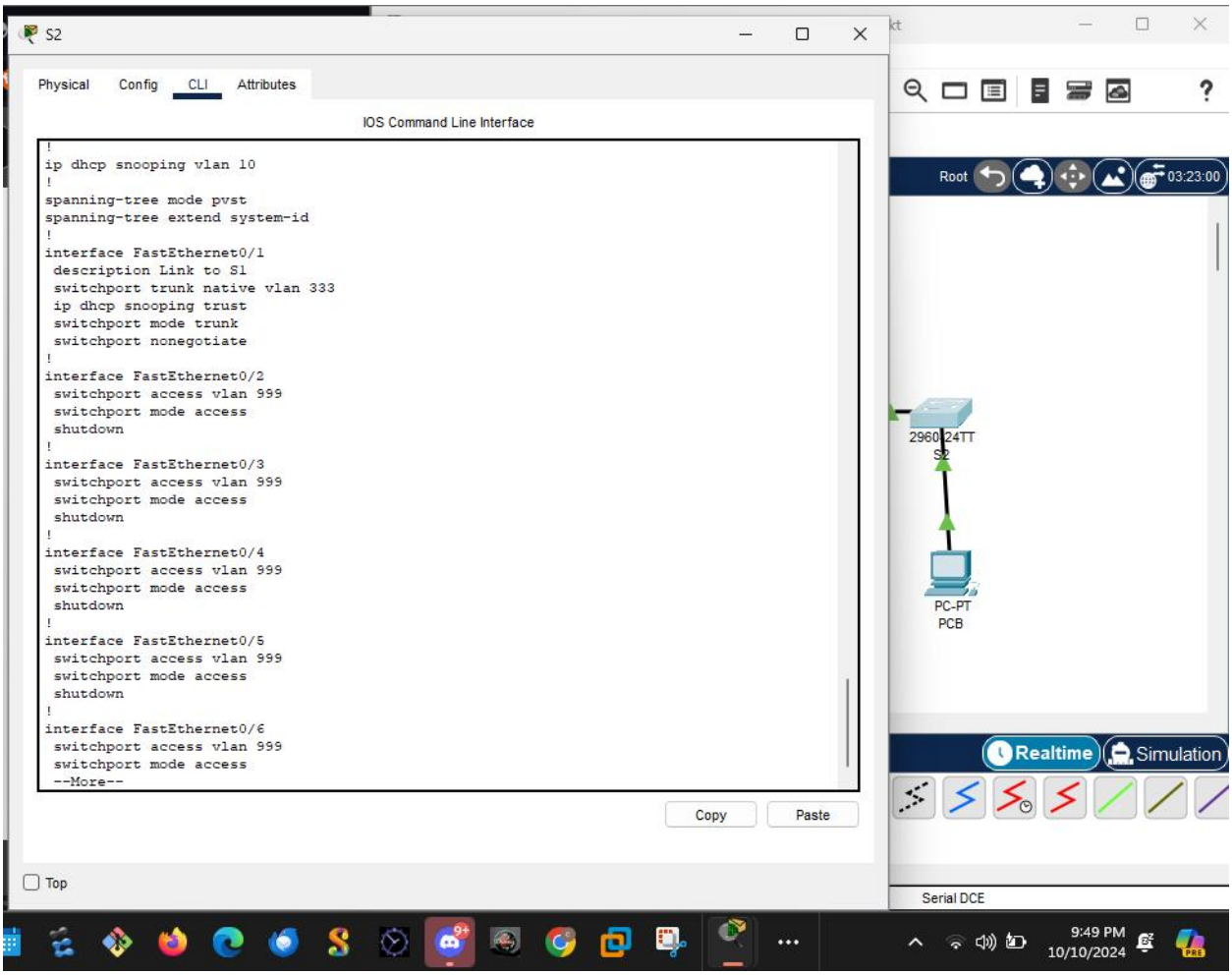
Top

S1

Physical Config CLI Attributes

IOS Command Line Interface

```
 shutdown
!
interface Vlan10
 description S1 Management vlan
 ip address 192.168.10.201 255.255.255.0
!
ip default-gateway 192.168.10.1
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end
```


S2
Physical
Config
CLI
Attributes
IOS Command Line Interface
!
ip dhcp snooping vlan 10
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 description Link to S1
 switchport trunk native vlan 333
 ip dhcp snooping trust
 switchport mode trunk
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/3
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/4
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/5
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/6
 switchport access vlan 999
 switchport mode access
 --More--
Copy
Paste
Top
Root
03:23:00
2960-24TT
S2
PC-PT
PCB
Realtime
Simulation
Serial DCE
9:49 PM
10/10/2024

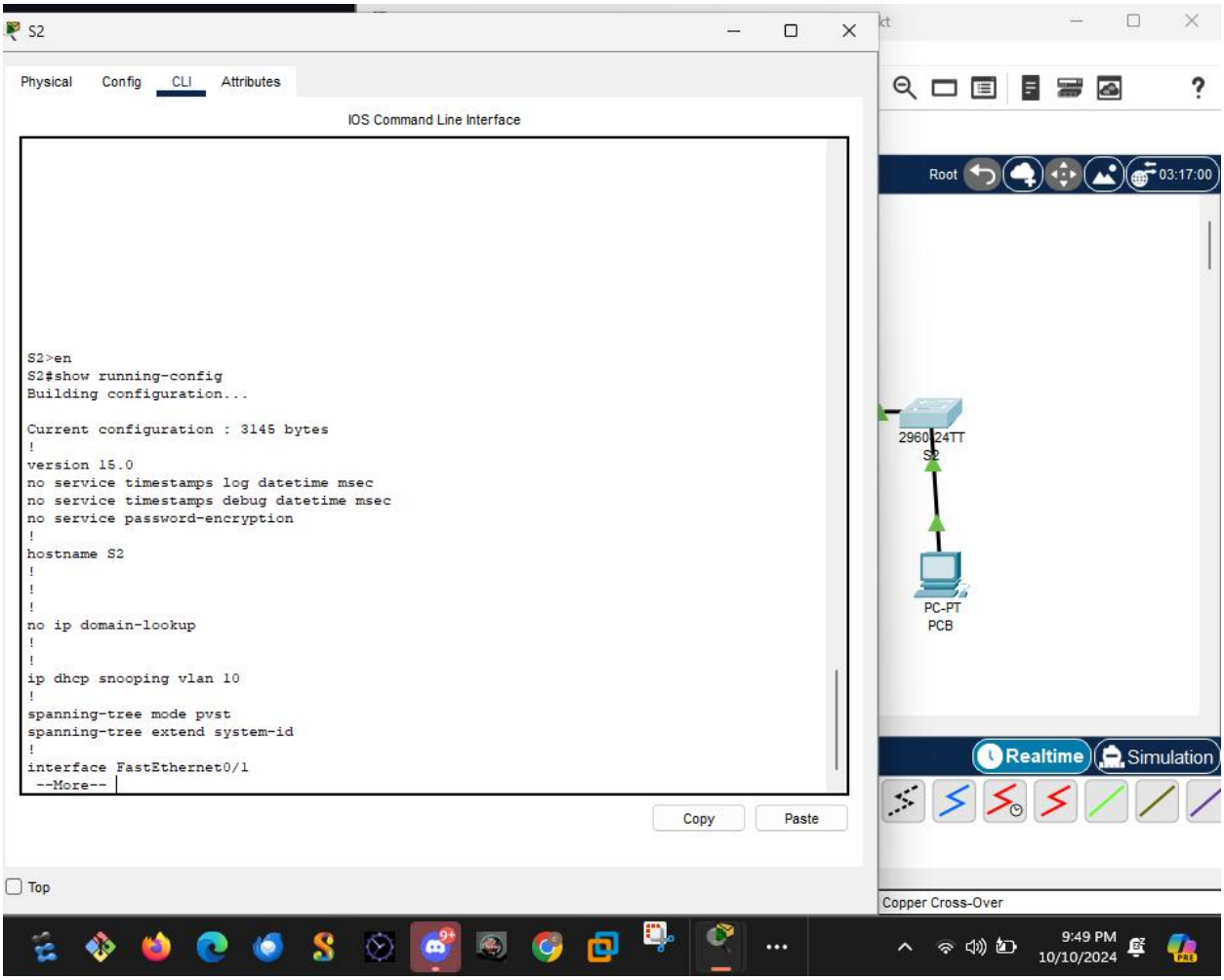
Physical Config CLI Attributes

IOS Command Line Interface

```
!
interface FastEthernet0/14
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/15
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/16
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/17
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface FastEthernet0/18
 description Link to PC-B Port Fa0/18
 switchport access vlan 10
 ip dhcp snooping limit rate 5
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation protect
 --More--
```

Copy Paste

☐ Top


S2
Physical
Config
CLI
Attributes
IOS Command Line Interface
S2>en
S2#show running-config
Building configuration...
Current configuration : 3145 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S2
!
!
!
no ip domain-lookup
!
!
ip dhcp snooping vlan 10
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
--More--
Copy
Paste
Top
Root
03:17:00
2960-24TT
S2
PC-PT
PCB
Realtime
Simulation
Copper Cross-Over
9:49 PM
10/10/2024

Physical Config CLI Attributes

IOS Command Line Interface

```
!
interface FastEthernet0/24
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface GigabitEthernet0/1
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface GigabitEthernet0/2
 switchport access vlan 999
 switchport mode access
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description S2 Management Vlan
 ip address 192.168.10.202 255.255.255.0
!
ip default-gateway 192.168.10.1
!
!
!
!
line con 0
 --More--
```

Copy Paste

☐ Top

Physical Config CLI Attributes

IOS Command Line Interface

```
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description S2 Management Vlan
 ip address 192.168.10.202 255.255.255.0
!
ip default-gateway 192.168.10.1
!
!
!
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
!
!
!
end


S2#
S2#
S2#
```

Copy Paste

☐ Top

CONCLUSION

In this lab, I learned how to configure VLANs on Switches, how to configure Switch Security. After the configurations have been saved, I was able to verify my configuration by testing for network connectivity.

I met a lot of new concepts which were new to me, which made me to research more to ensure I learn a lot on the areas. I surely learnt a lot.