**COURSE: CLOUD AND NETORK SECURITY**

**NAME: DENISE SOPHY ONDISO MUTAYI**

**STUDENT NO: CS-CN09-25047**

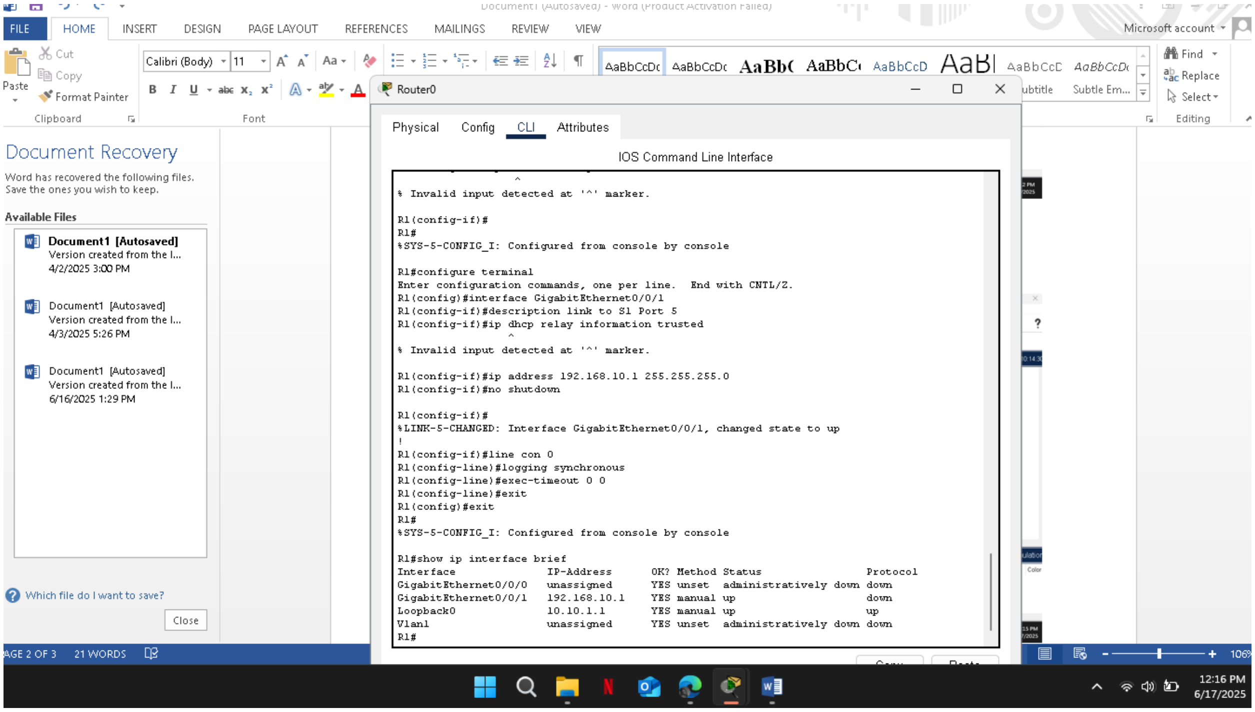
# VLANS AND SECURE SWITCH CONFIGURATION

# Contents

# INTRODUCTION

This report documents the step-by-step configuration and verification of key Layer 2 security, VLAN management, and interface settings on Cisco switches and routers using Cisco Packet Tracer. The objective was to establish a secure and well-structured small enterprise network that includes proper VLAN segmentation, port security implementation, trunking configuration, DHCP snooping, and spanning-tree protocol optimizations.

Two switches (S1 and S2) and one router (R1) were configured with essential services to support secure and efficient network operations. Tasks included assigning hostnames, disabling unwanted DNS lookups, configuring access and trunk ports, setting up switch virtual interfaces (SVIs) for VLAN 10, and implementing strict port security on active ports. DHCP snooping was enabled to prevent rogue DHCP servers, and BPDU Guard and PortFast were applied to edge ports to safeguard the spanning-tree topology.



Document Recovery

Word has recovered the following files. Save the ones you wish to keep.

Available Files

Document1 [Autosaved]
Version created from the l...
4/2/2025 3:00 PM

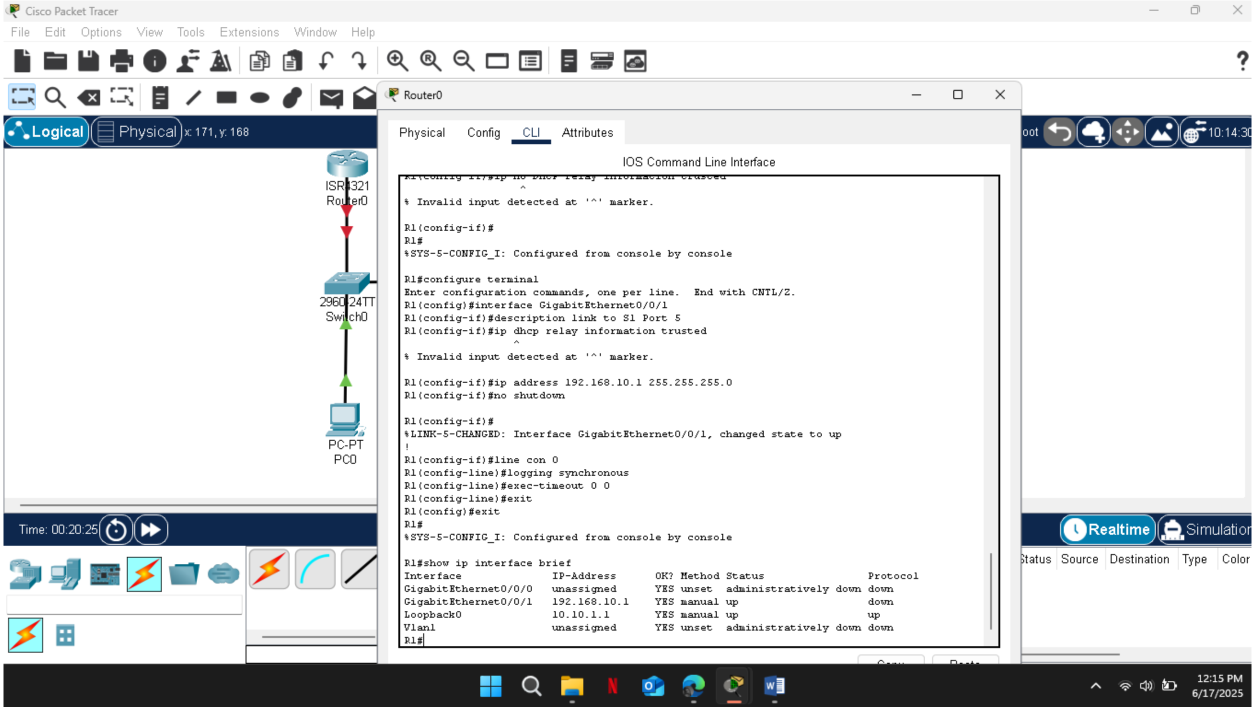
Document1 [Autosaved]
Version created from the l...
4/3/2025 5:26 PM

Document1 [Autosaved]
Version created from the l...
6/16/2025 1:29 PM

Which file do I want to save?

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

R1(config-if)#
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface GigabitEthernet0/0/1
R1(config-if)#description link to S1 Port 5
R1(config-if)#ip dhcp relay information trusted
                   ^
% Invalid input detected at '^' marker.

R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
!
R1(config-if)#line con 0
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 0 0
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down down
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    down
Loopback0              10.10.1.1       YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

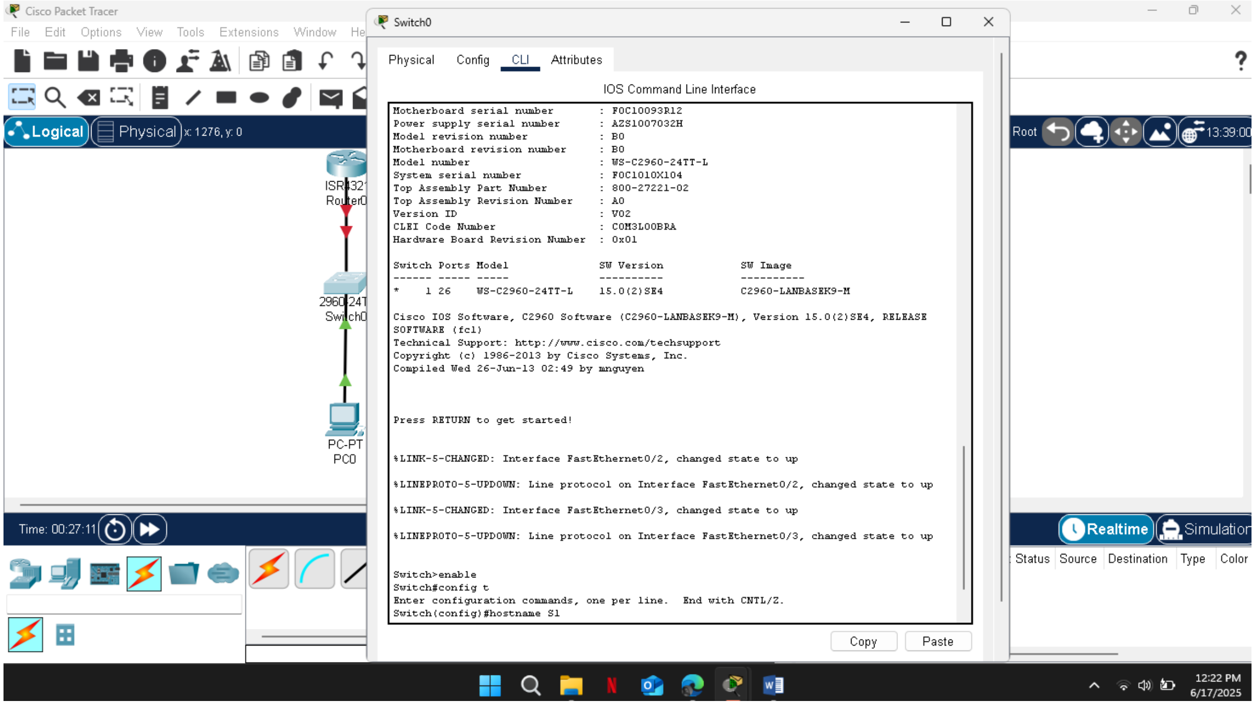
Configuration of the router and Verifying  the running-configuration on R1



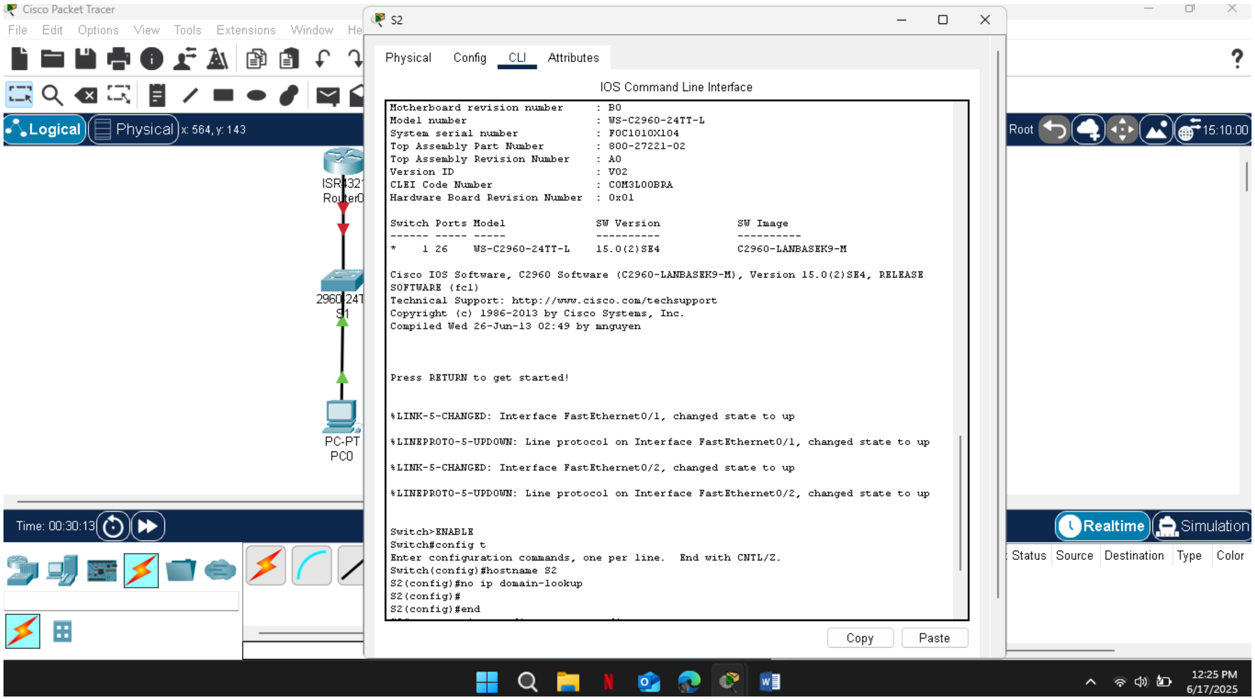
```
R1(config-if)#ip no dhcp relay information trusted
                    ^
% Invalid input detected at '^' marker.

R1(config-if)#
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface GigabitEthernet0/0/1
R1(config-if)#description link to S1 Port 5
R1(config-if)#ip dhcp relay information trusted
                   ^
% Invalid input detected at '^' marker.

R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
!
R1(config-if)#line con 0
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 0 0
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down down
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    down
Loopback0              10.10.1.1       YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

Verify IP addressing and interfaces are in an up

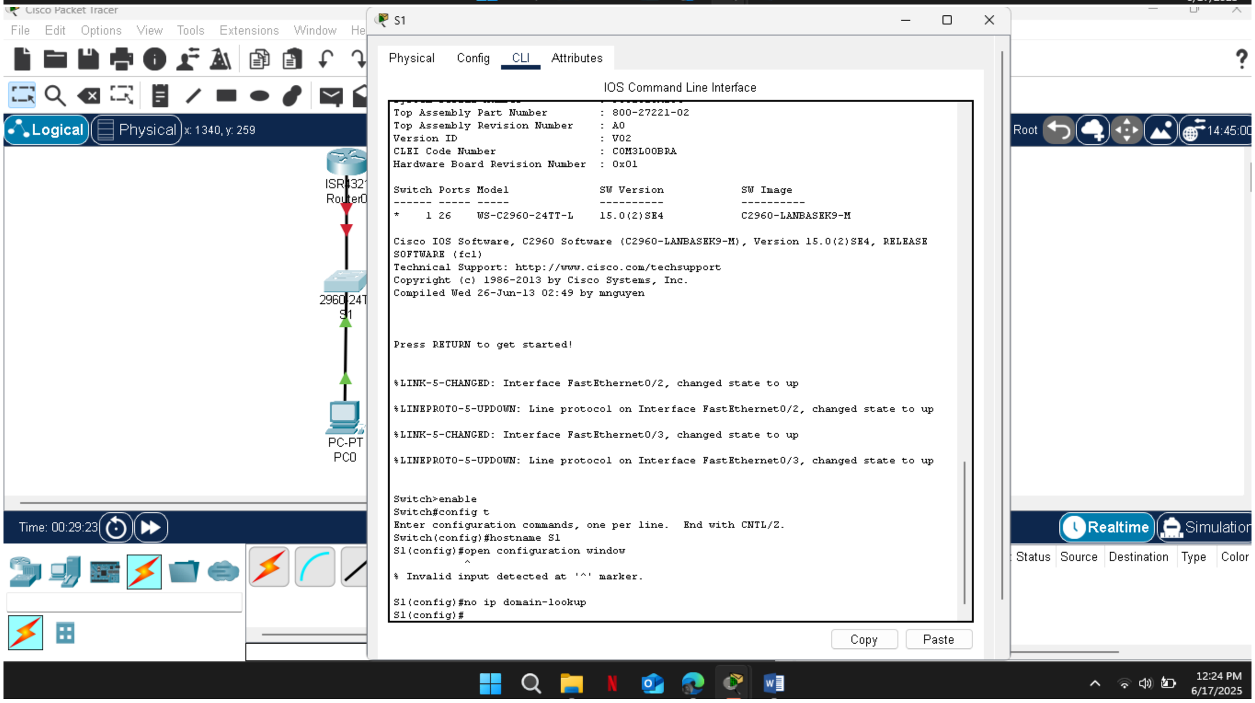
Configure the hostname for switches S1 and S2.



```
Motherboard serial number        : FOC10093R12
Power supply serial number       : AZS1007032H
Model revision number            : B0
Motherboard revision number      : B0
Model number                     : WS-C2960-24TT-L
System serial number             : FOC1010X104
Top Assembly Part Number         : 800-27221-02
Top Assembly Revision Number     : A0
Version ID                       : V02
CLEI Code Number                 : COM3L00BRA
Hardware Board Revision Number   : 0x01

Switch Ports Model               SW Version           SW Image
------ ----- -----               ----------           ----------
*    1 26    WS-C2960-24TT-L     15.0(2)SE4           C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen



Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

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

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
```

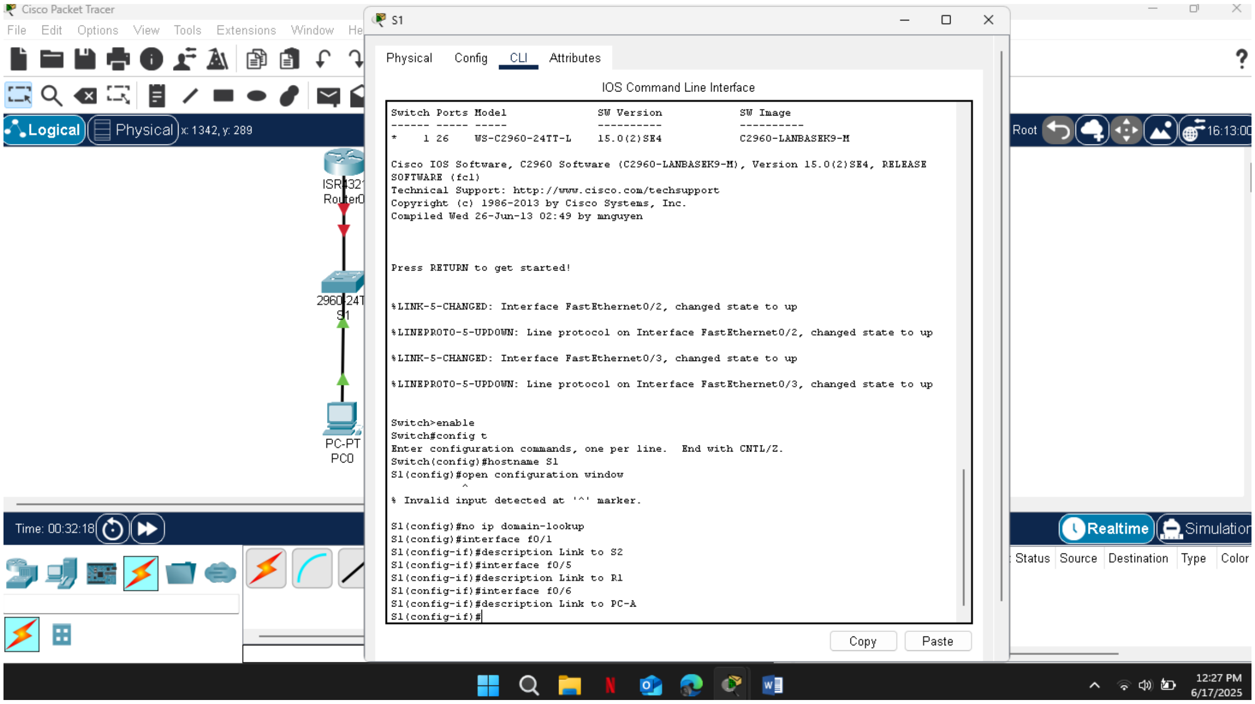


```
Motherboard revision number       : B0
Model number                      : WS-C2960-24TT-L
System serial number              : FOC1010X104
Top Assembly Part Number          : 800-27221-02
Top Assembly Revision Number      : A0
Version ID                        : V02
CLEI Code Number                  : COM3L00BRA
Hardware Board Revision Number    : 0x01

Switch Ports Model                SW Version            SW Image
------ ----- -----                ----------            ----------
*    1 26    WS-C2960-24TT-L      15.0(2)SE4            C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen



Press RETURN to get started!


%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 FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, 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)#
S2(config)#end
```



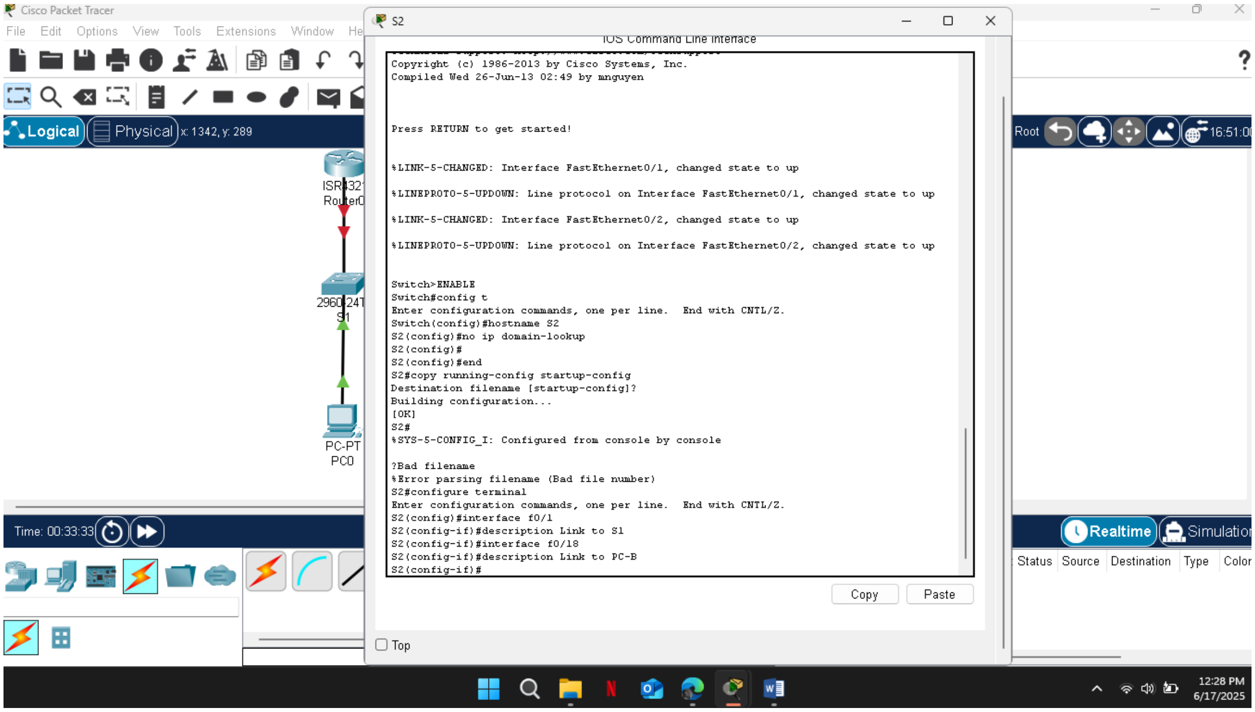
```
Top Assembly Part Number          : 800-27221-02
Top Assembly Revision Number      : A0
Version ID                        : V02
CLEI Code Number                  : COM3L00BRA
Hardware Board Revision Number    : 0x01

Switch Ports Model                SW Version            SW Image
------ ----- -----                ----------            ----------
*    1 26    WS-C2960-24TT-L      15.0(2)SE4            C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen



Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

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

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#open configuration window
           ^
% Invalid input detected at '^' marker.

S1(config)#no ip domain-lookup
S1(config)#
```

Prevent unwanted DNS lookups on both switches.


Cisco Packet Tracer
File Edit Options View Tools Extensions Window He
S1
Physical Config CLI Attributes
IOS Command Line Interface
Logical Physical x: 1342, y: 289
ISR4321 Router0
2960-24TT S1
PC-PT PC0
Time: 00:32:18
Root 16:13:00
Realtime Simulation
Status Source Destination Type Color
Copy Paste
12:27 PM 6/17/2025

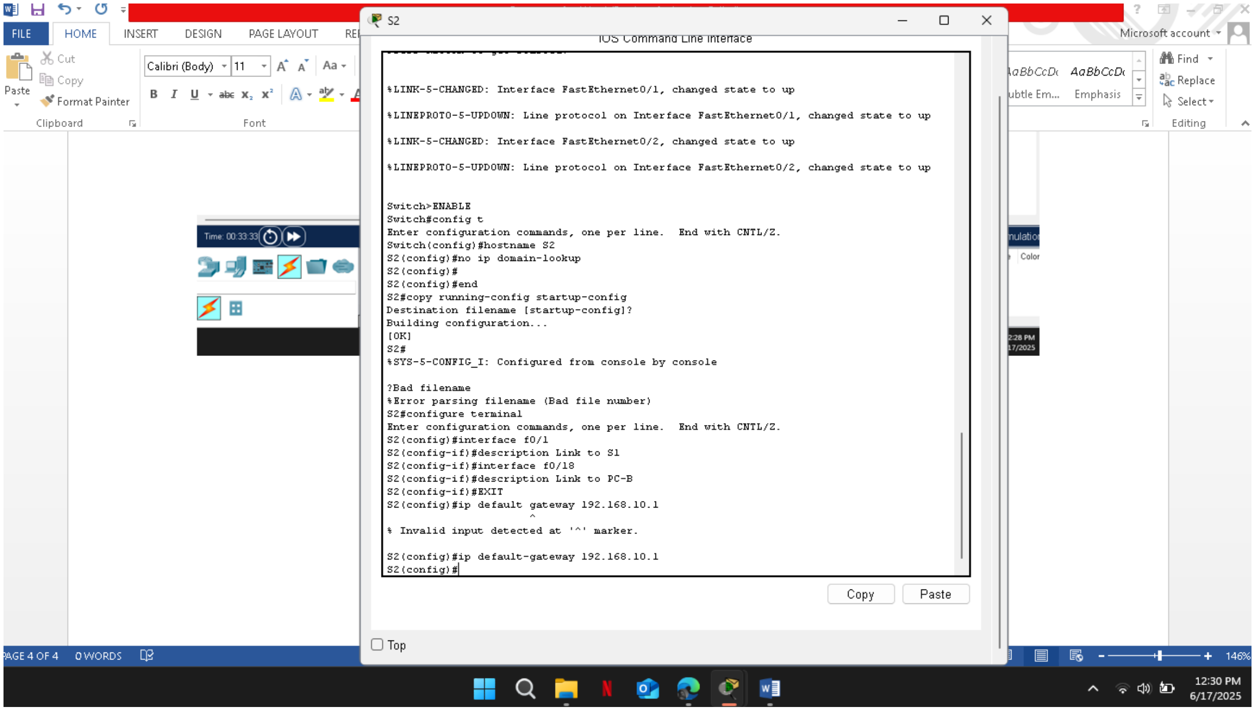
```
Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 26    WS-C2960-24TT-L    15.0(2)SE4            C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen



Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

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

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#open configuration window
          ^
% Invalid input detected at '^' marker.

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)#
```

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

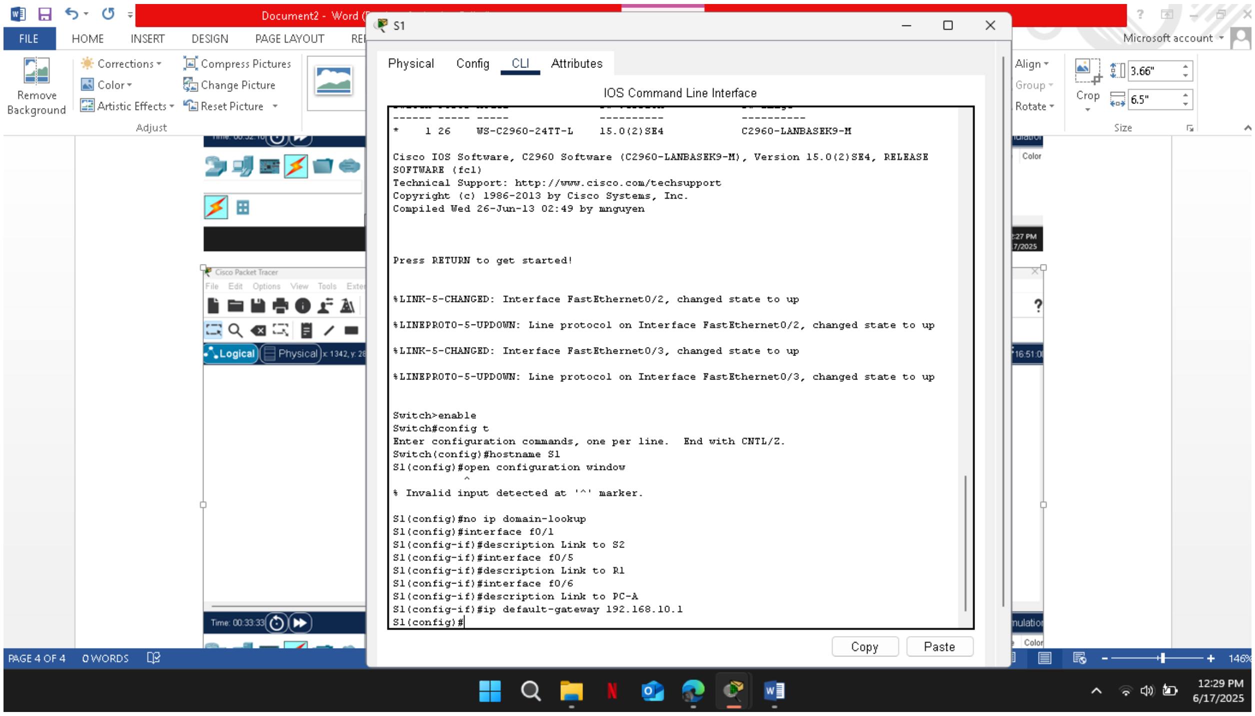

Cisco Packet Tracer
File Edit Options View Tools Extensions Window He
S2
IOS Command Line Interface
Logical Physical x: 1342, y: 289
ISR4321 Router0
2960-24TT S1
PC-PT PC0
Time: 00:33:33
Root 16:51:00
Realtime Simulation
Status Source Destination Type Color
Copy Paste
Top
12:28 PM 6/17/2025

```
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen



Press RETURN to get started!


%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 FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, 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)#
S2(config)#end
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
%SYS-5-CONFIG_I: Configured from console by console

?Bad filename
%Error parsing filename (Bad file number)
S2#configure terminal
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)#
```

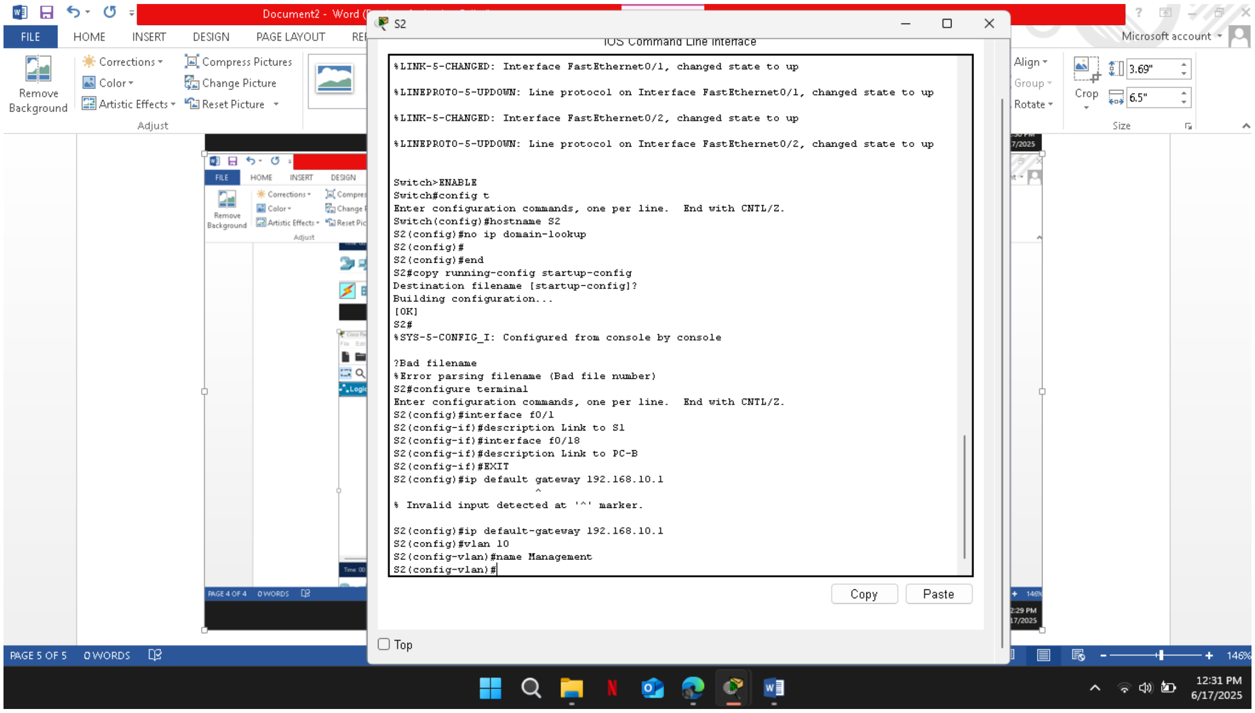
Set the default-gateway for the Management VLAN to 192.168.10.1 on both switches.



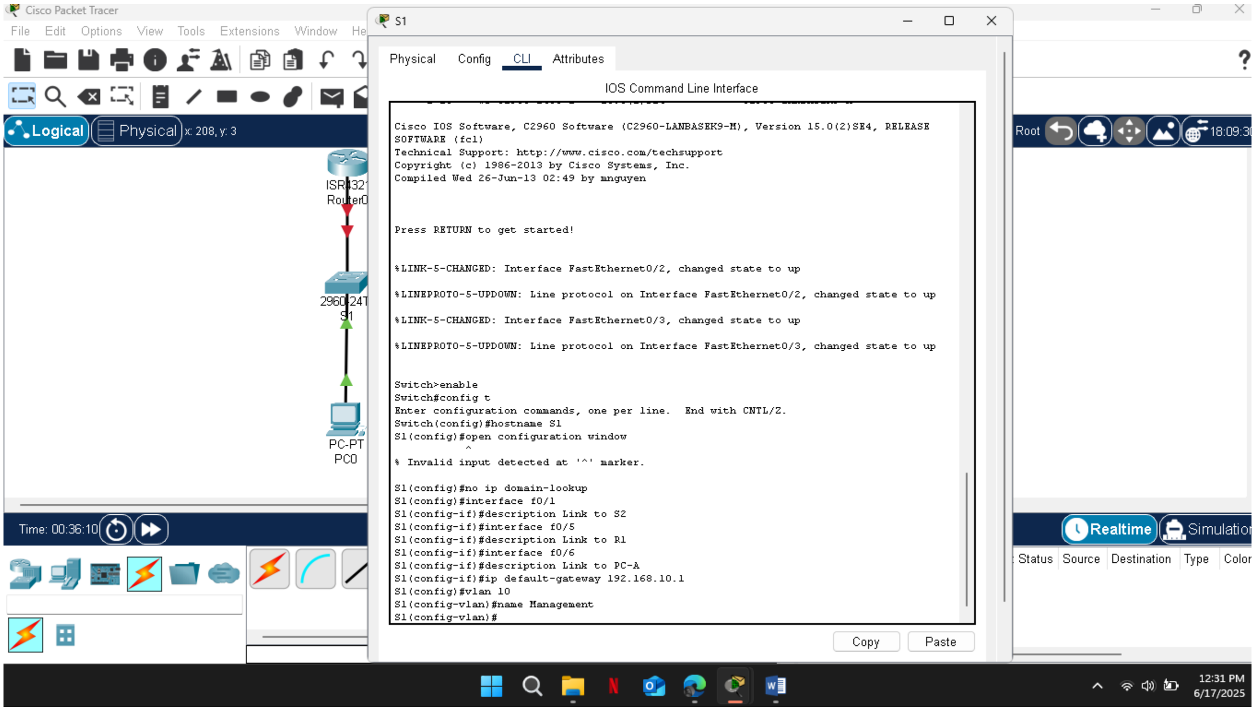
```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, 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)#
S2(config)#end
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
%SYS-5-CONFIG_I: Configured from console by console

?Bad filename
%Error parsing filename (Bad file number)
S2#configure terminal
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)#EXIT
S2(config)#ip default gateway 192.168.10.1
                      ^
% Invalid input detected at '^' marker.

S2(config)#ip default-gateway 192.168.10.1
S2(config)#
```



```
------ ----- -----              ----------            ----------
*    1 26    WS-C2960-24TT-L    15.0(2)SE4            C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen



Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

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

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#open configuration window
           ^
% Invalid input detected at '^' marker.

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)#
```

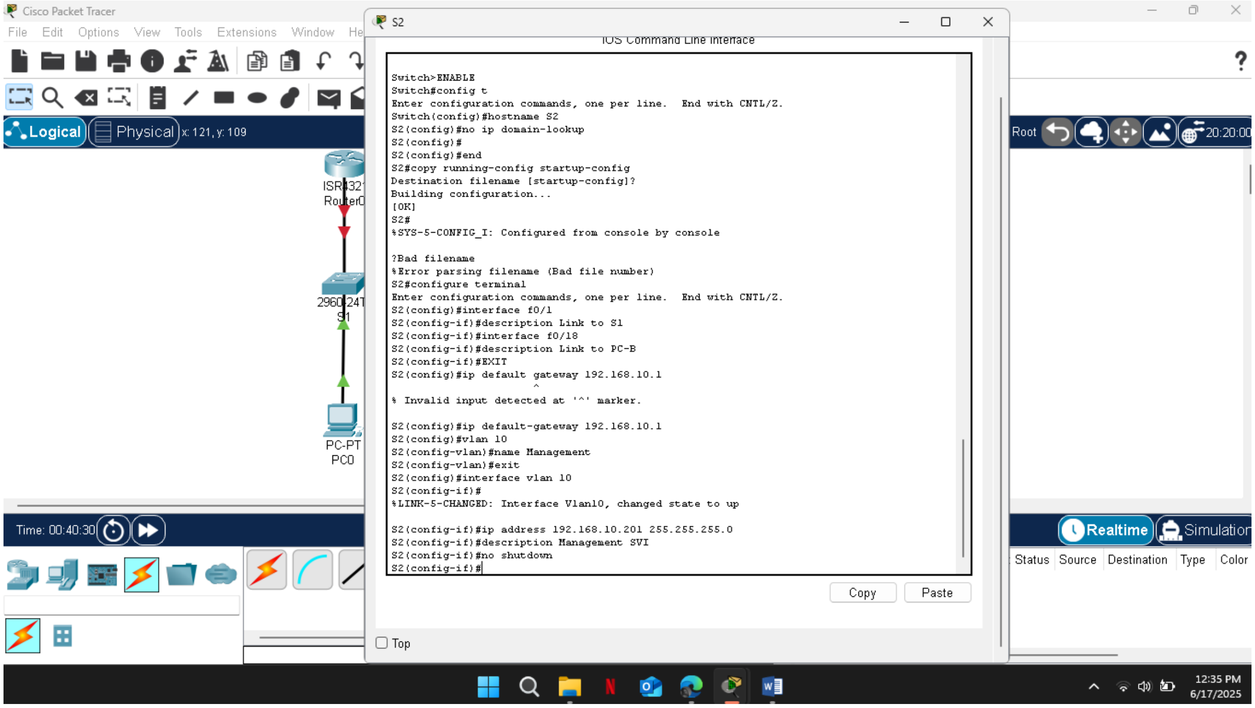


```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, 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)#
S2(config)#end
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
%SYS-5-CONFIG_I: Configured from console by console

?Bad filename
%Error parsing filename (Bad file number)
S2#configure terminal
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)#EXIT
S2(config)#ip default gateway 192.168.10.1
                      ^
% Invalid input detected at '^' marker.

S2(config)#ip default-gateway 192.168.10.1
S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#
```

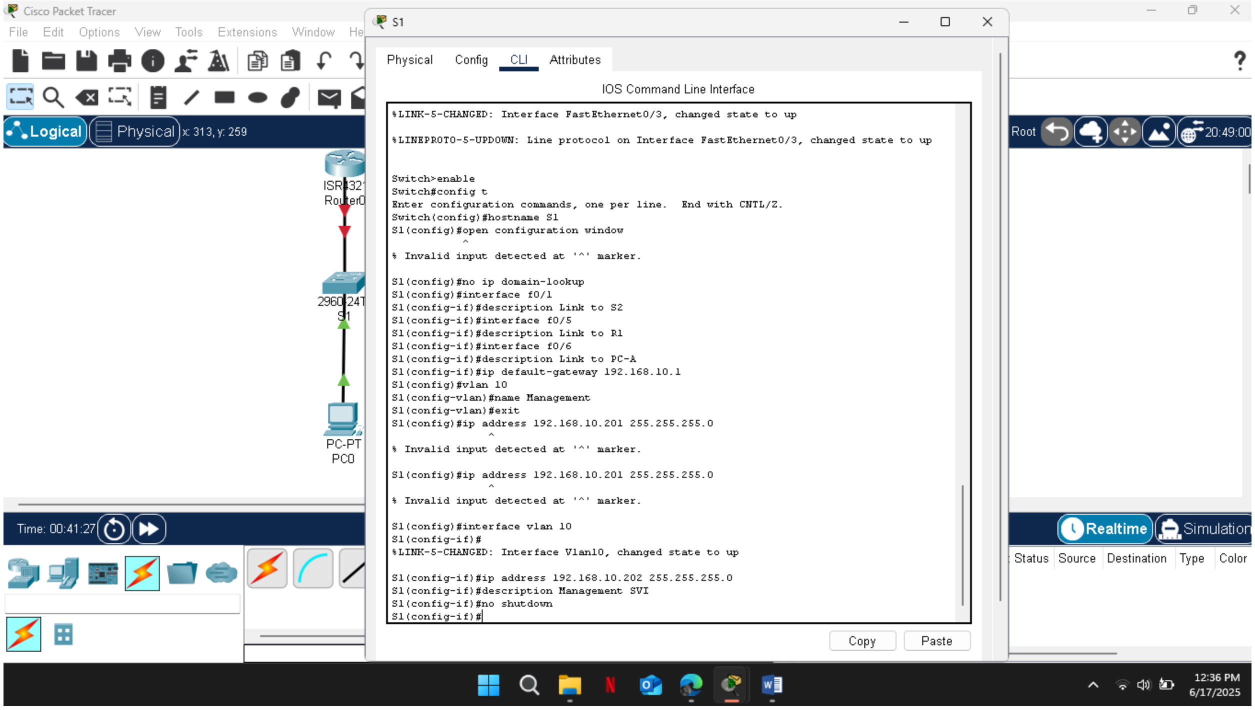


```
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen



Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

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

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#open configuration window
           ^
% Invalid input detected at '^' marker.

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)#
```

## Configure VLANs on Switches.

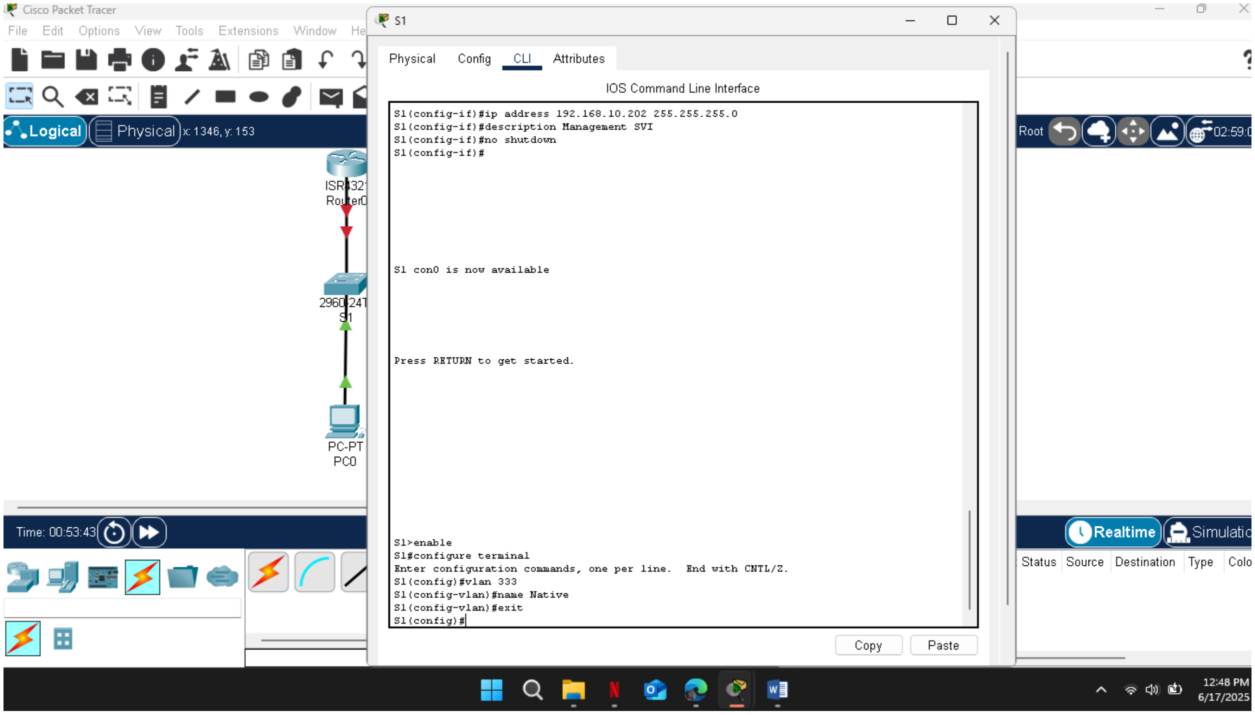


```
Switch>ENABLE
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#
S2(config)#end
S2#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
%SYS-5-CONFIG_I: Configured from console by console

?Bad filename
%Error parsing filename (Bad file number)
S2#configure terminal
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)#EXIT
S2(config)#ip default gateway 192.168.10.1
                      ^
% Invalid input detected at '^' marker.

S2(config)#ip default-gateway 192.168.10.1
S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#exit
S2(config)#interface vlan 10
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S2(config-if)#ip address 192.168.10.201 255.255.255.0
S2(config-if)#description Management SVI
S2(config-if)#no shutdown
S2(config-if)#
```

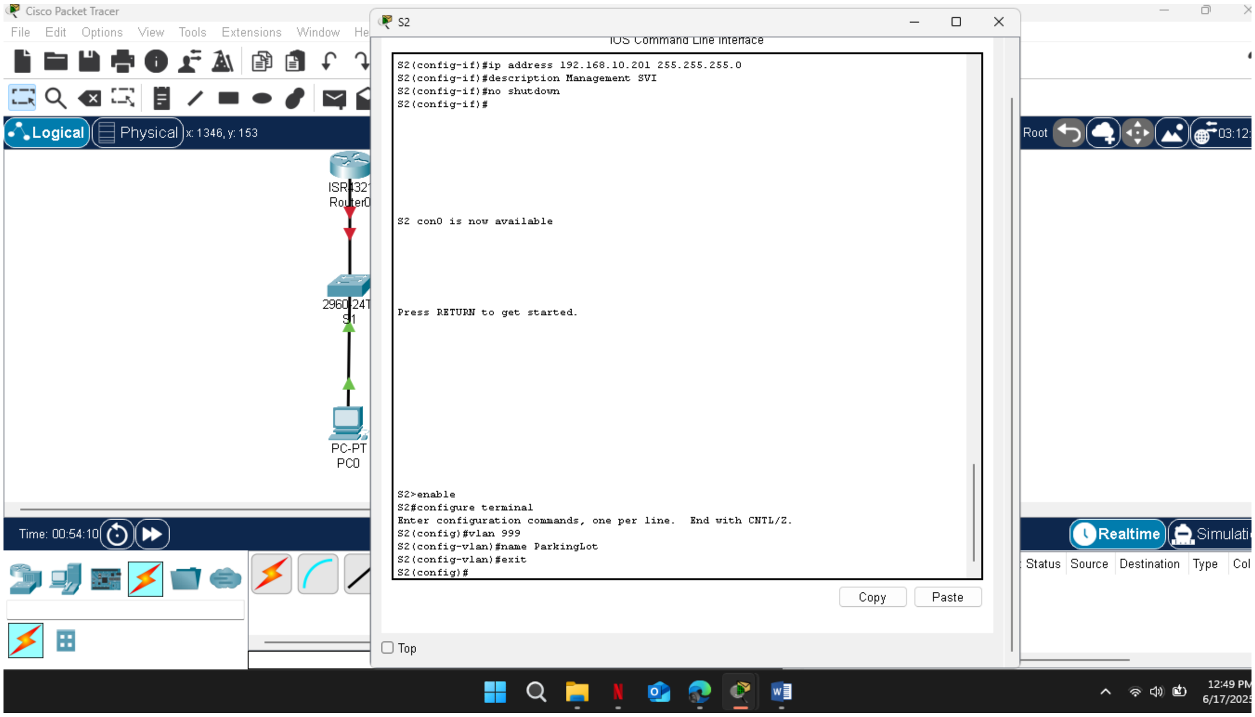


```
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up


Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#open configuration window
           ^
% Invalid input detected at '^' marker.

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)#exit
S1(config)#ip address 192.168.10.201 255.255.255.0
               ^
% Invalid input detected at '^' marker.

S1(config)#ip address 192.168.10.201 255.255.255.0
               ^
% Invalid input detected at '^' marker.

S1(config)#interface vlan 10
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S1(config-if)#ip address 192.168.10.202 255.255.255.0
S1(config-if)#description Management SVI
S1(config-if)#no shutdown
S1(config-if)#
```

Configure the SVI for VLAN 10 for VLAN 10 on S1 and S2.

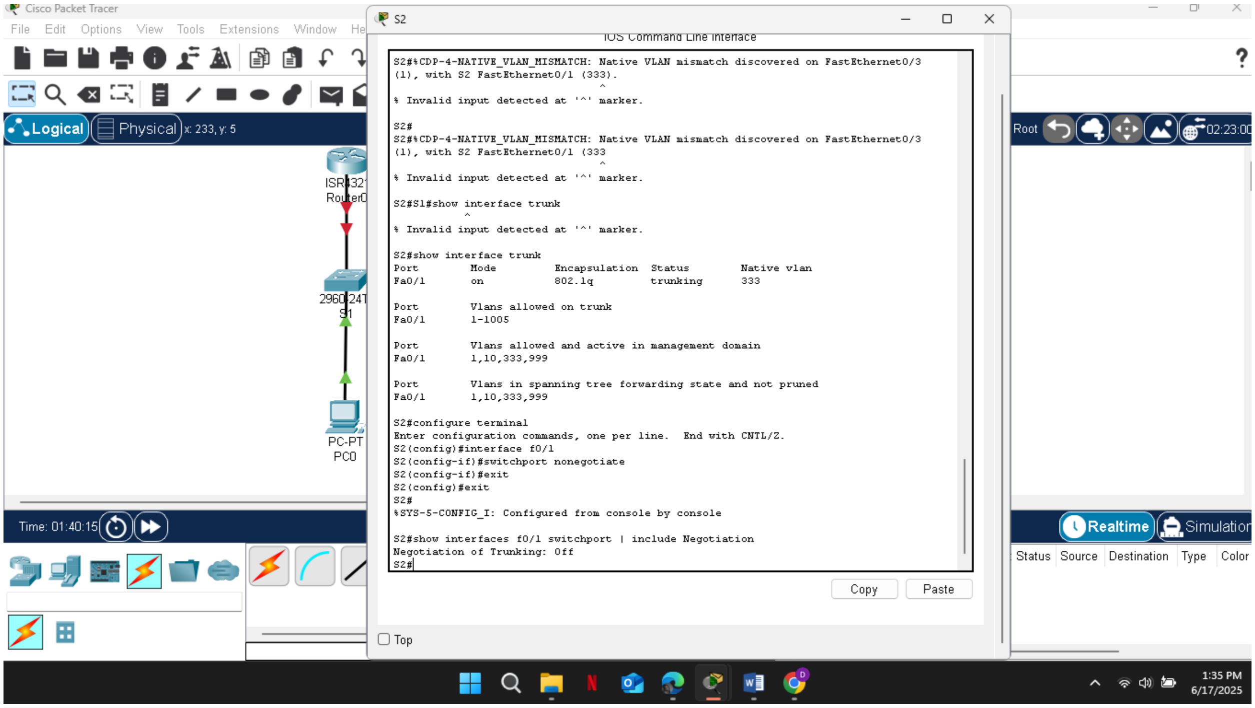


```
S1(config-if)#ip address 192.168.10.202 255.255.255.0
S1(config-if)#description Management SVI
S1(config-if)#no shutdown
S1(config-if)#




S1 con0 is now available




Press RETURN to get started.









S1>enable
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#
```

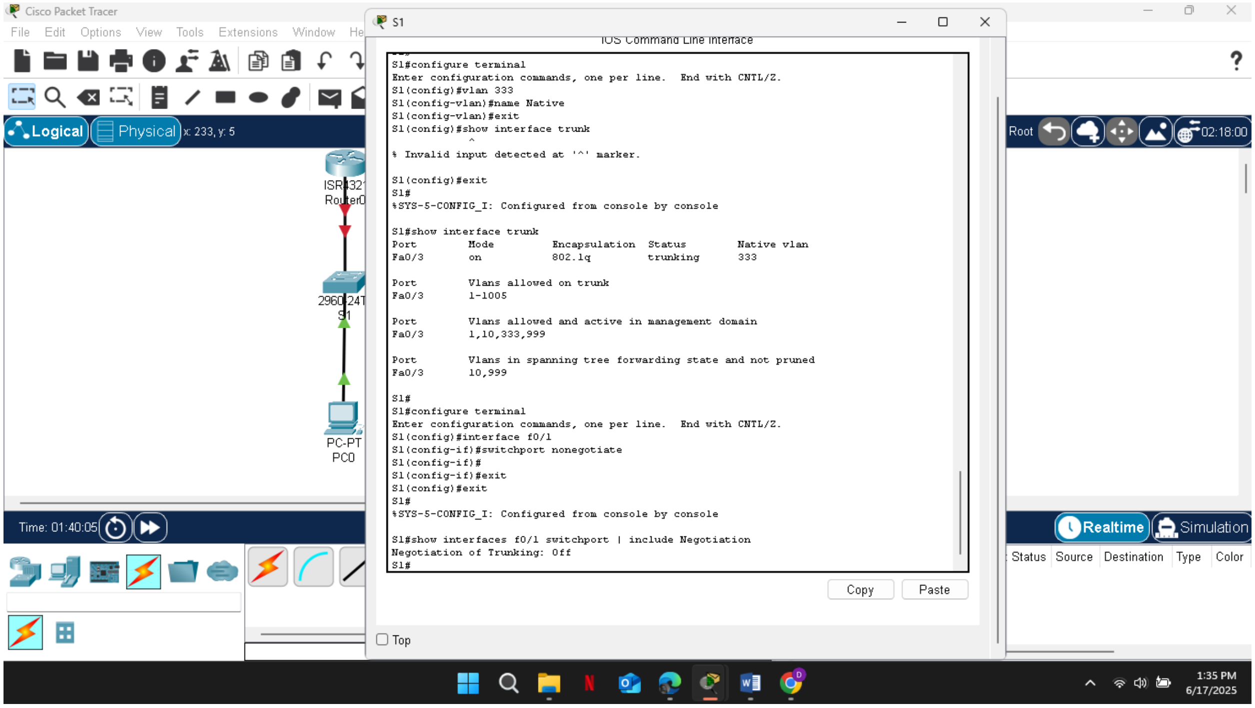


```
S2(config-if)#ip address 192.168.10.201 255.255.255.0
S2(config-if)#description Management SVI
S2(config-if)#no shutdown
S2(config-if)#




S2 con0 is now available




Press RETURN to get started.









S2>enable
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 999
S2(config-vlan)#name ParkingLot
S2(config-vlan)#exit
S2(config)#
```

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

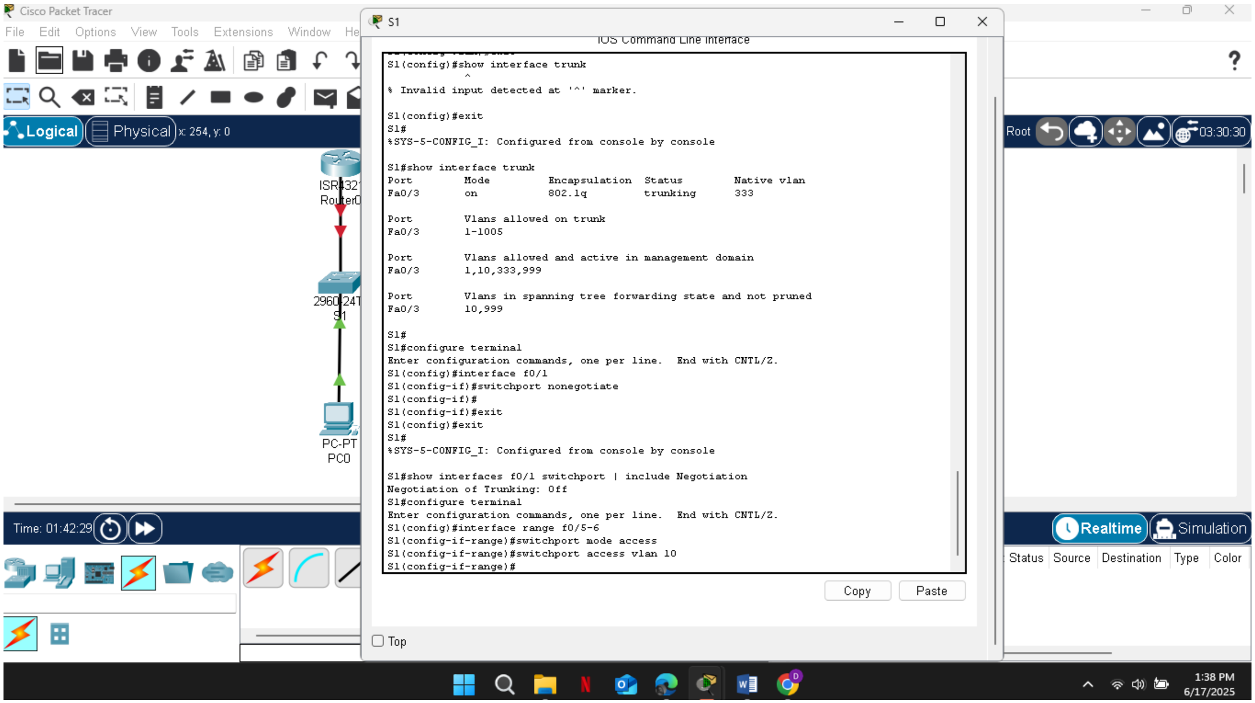


```
S2#%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3
(1), with S2 FastEthernet0/1 (333).
                                ^
% Invalid input detected at '^' marker.

S2#
S2#%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3
(1), with S2 FastEthernet0/1 (333
                                ^
% Invalid input detected at '^' marker.

S2#S1#show interface trunk
           ^
% Invalid input detected at '^' marker.

S2#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

S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#switchport nonegotiate
S2(config-if)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S2#
```

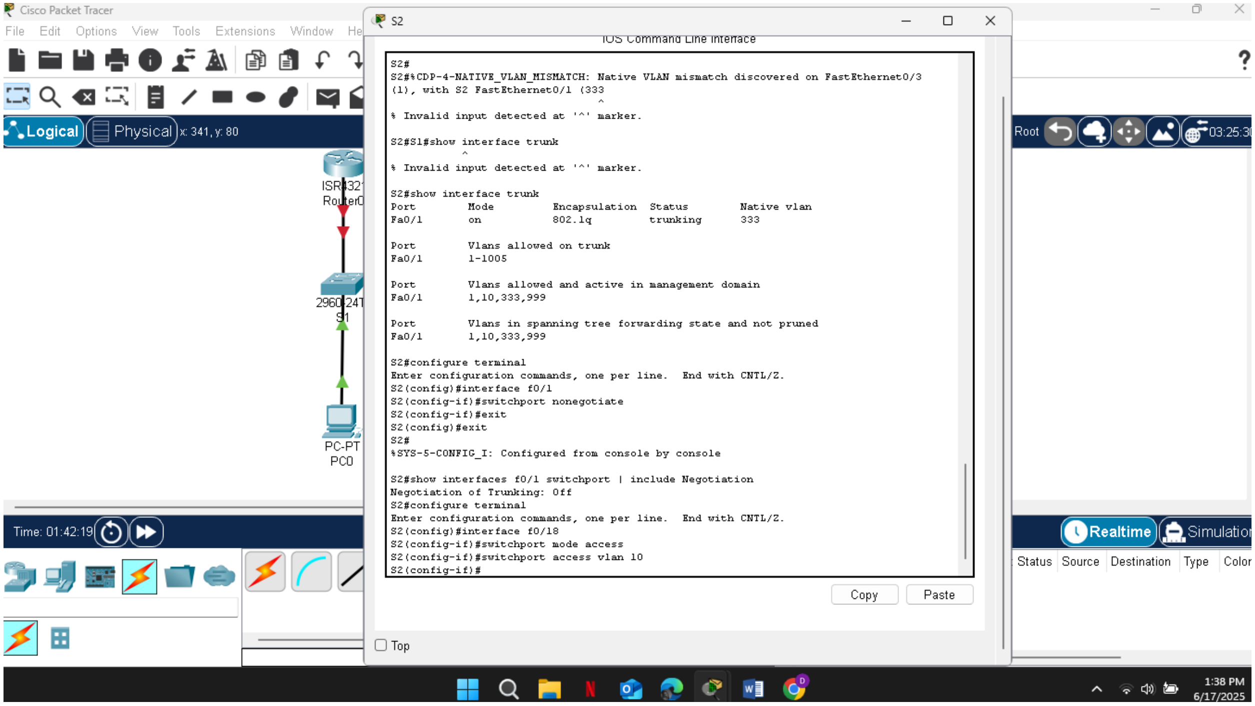


```
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#show interface trunk
            ^
% Invalid input detected at '^' marker.

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

S1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/3       on           802.1q         trunking      333

Port        Vlans allowed on trunk
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/3       1,10,333,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/3       10,999

S1#
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

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

Configure Switch Security by Implementing 802.1Q trunking then Verify that trunking is configured on both switches and Disable DTP negotiation on F0/1 on S1 and S2.

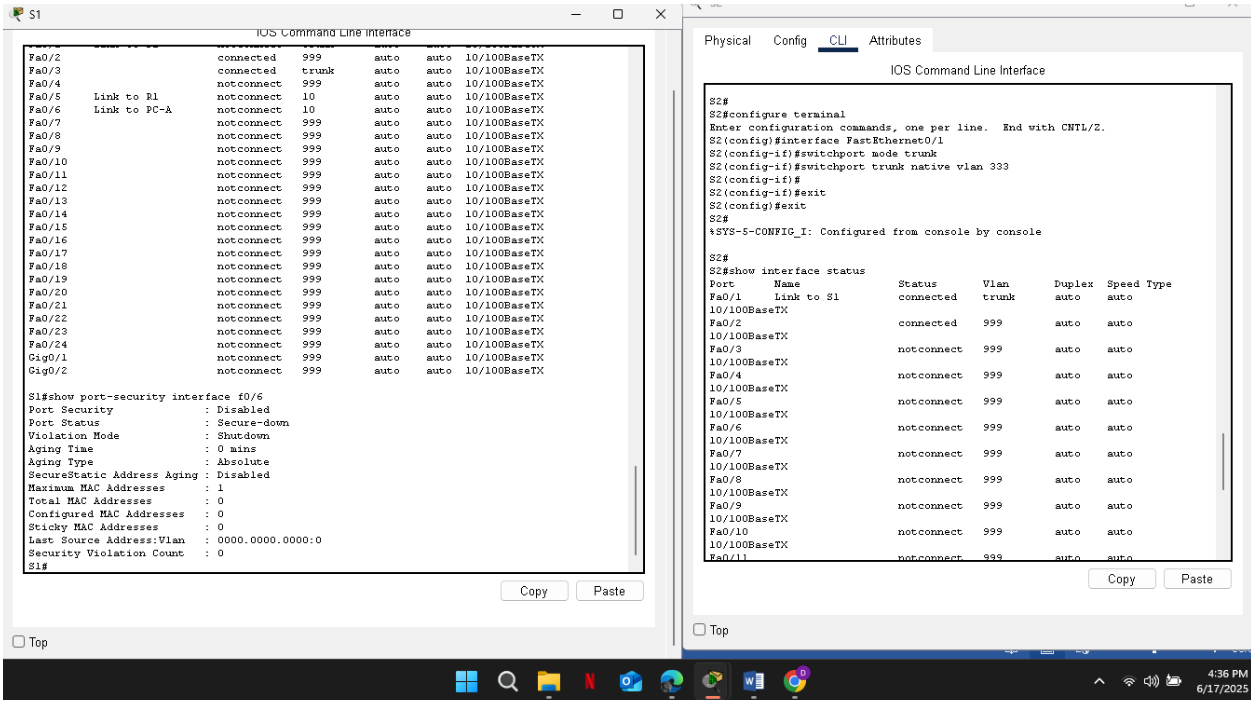


```
S1(config)#show interface trunk
            ^
% Invalid input detected at '^' marker.

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

S1#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/3       on           802.1q         trunking      333

Port        Vlans allowed on trunk
Fa0/3       1-1005

Port        Vlans allowed and active in management domain
Fa0/3       1,10,333,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/3       10,999

S1#
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S1#configure terminal
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)#
```



```
S2#
S2#%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/3
(1), with S2 FastEthernet0/1 (333
                                 ^
% Invalid input detected at '^' marker.

S2#S1#show interface trunk
           ^
% Invalid input detected at '^' marker.

S2#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

S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/1
S2(config-if)#switchport nonegotiate
S2(config-if)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
S2(config-if)#
```

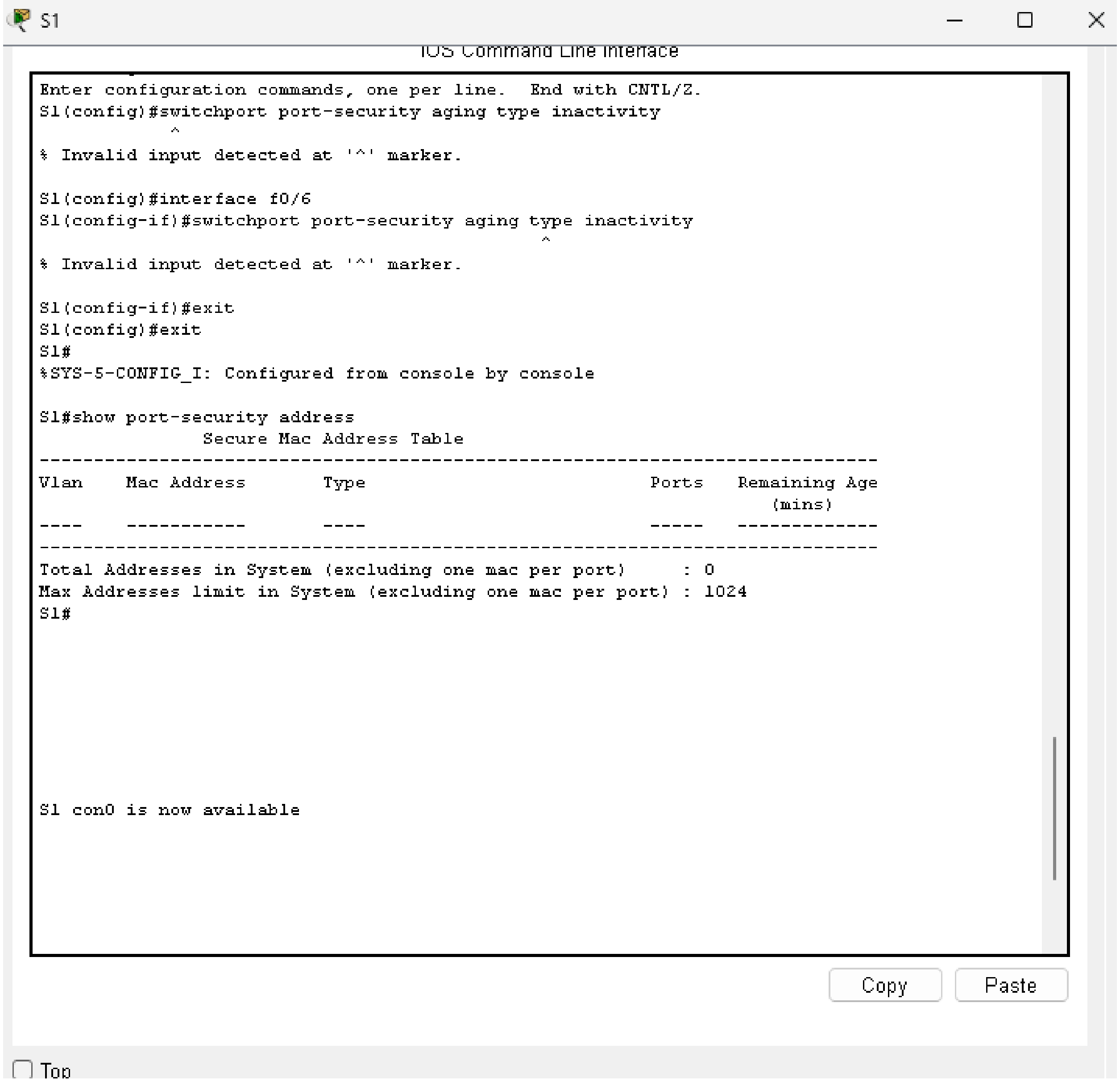
Configure access ports that are associated with VLAN 10 on both s1 and s2, Secure and disable unused switchports.



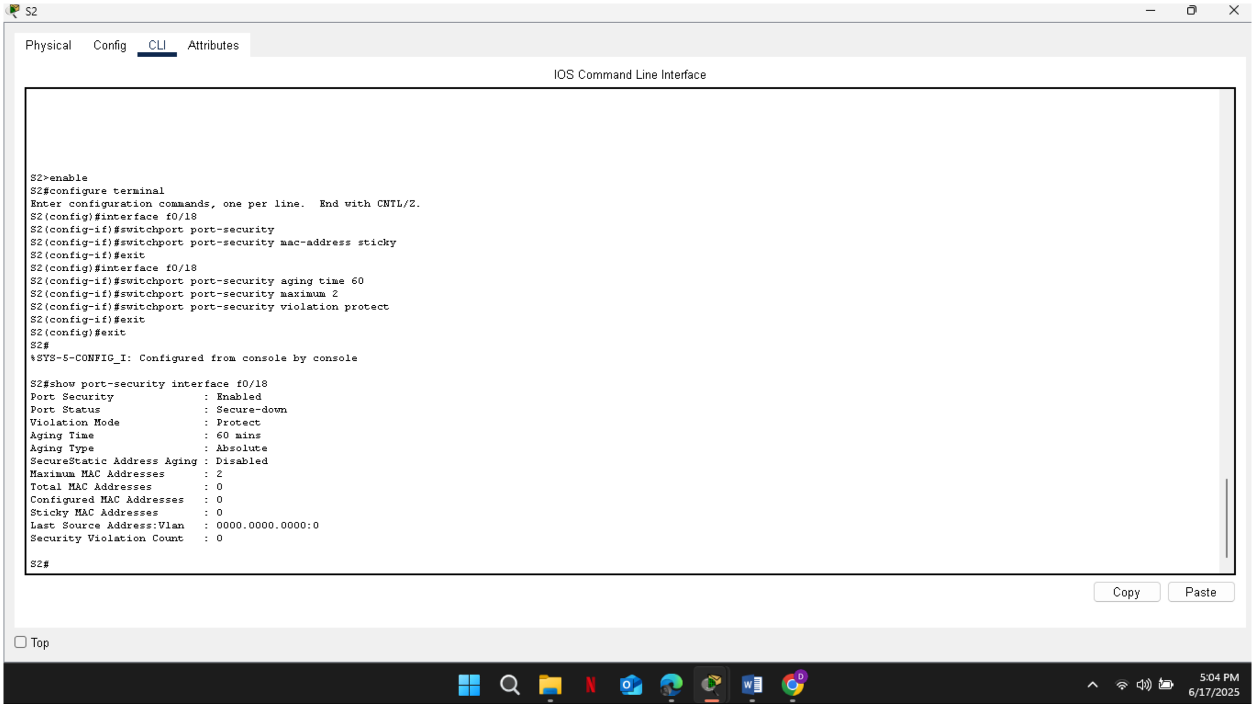
```
Fa0/2                        connected    999        auto    auto   10/100BaseTX
Fa0/3                        connected    trunk      auto    auto   10/100BaseTX
Fa0/4                        notconnect   999        auto    auto   10/100BaseTX
Fa0/5      Link to R1        notconnect   10         auto    auto   10/100BaseTX
Fa0/6      Link to PC-A      notconnect   10         auto    auto   10/100BaseTX
Fa0/7                        notconnect   999        auto    auto   10/100BaseTX
Fa0/8                        notconnect   999        auto    auto   10/100BaseTX
Fa0/9                        notconnect   999        auto    auto   10/100BaseTX
Fa0/10                       notconnect   999        auto    auto   10/100BaseTX
Fa0/11                       notconnect   999        auto    auto   10/100BaseTX
Fa0/12                       notconnect   999        auto    auto   10/100BaseTX
Fa0/13                       notconnect   999        auto    auto   10/100BaseTX
Fa0/14                       notconnect   999        auto    auto   10/100BaseTX
Fa0/15                       notconnect   999        auto    auto   10/100BaseTX
Fa0/16                       notconnect   999        auto    auto   10/100BaseTX
Fa0/17                       notconnect   999        auto    auto   10/100BaseTX
Fa0/18                       notconnect   999        auto    auto   10/100BaseTX
Fa0/19                       notconnect   999        auto    auto   10/100BaseTX
Fa0/20                       notconnect   999        auto    auto   10/100BaseTX
Fa0/21                       notconnect   999        auto    auto   10/100BaseTX
Fa0/22                       notconnect   999        auto    auto   10/100BaseTX
Fa0/23                       notconnect   999        auto    auto   10/100BaseTX
Fa0/24                       notconnect   999        auto    auto   10/100BaseTX
Gig0/1                       notconnect   999        auto    auto   10/100BaseTX
Gig0/2                       notconnect   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#
```

```
S2#
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface FastEthernet0/1
S2(config-if)#switchport mode trunk
S2(config-if)#switchport trunk native vlan 333
S2(config-if)#
S2(config-if)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#
S2#show interface status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Link to S1         connected    trunk      auto    auto
10/100BaseTX
Fa0/2                        connected    999        auto    auto
10/100BaseTX
Fa0/3                        notconnect   999        auto    auto
10/100BaseTX
Fa0/4                        notconnect   999        auto    auto
10/100BaseTX
Fa0/5                        notconnect   999        auto    auto
10/100BaseTX
Fa0/6                        notconnect   999        auto    auto
10/100BaseTX
Fa0/7                        notconnect   999        auto    auto
10/100BaseTX
Fa0/8                        notconnect   999        auto    auto
10/100BaseTX
Fa0/9                        notconnect   999        auto    auto
10/100BaseTX
Fa0/10                       notconnect   999        auto    auto
10/100BaseTX
Fa0/11                       notconnect   999        auto    auto
```

Issue the port security interface f0/6 command that displays the default port security.

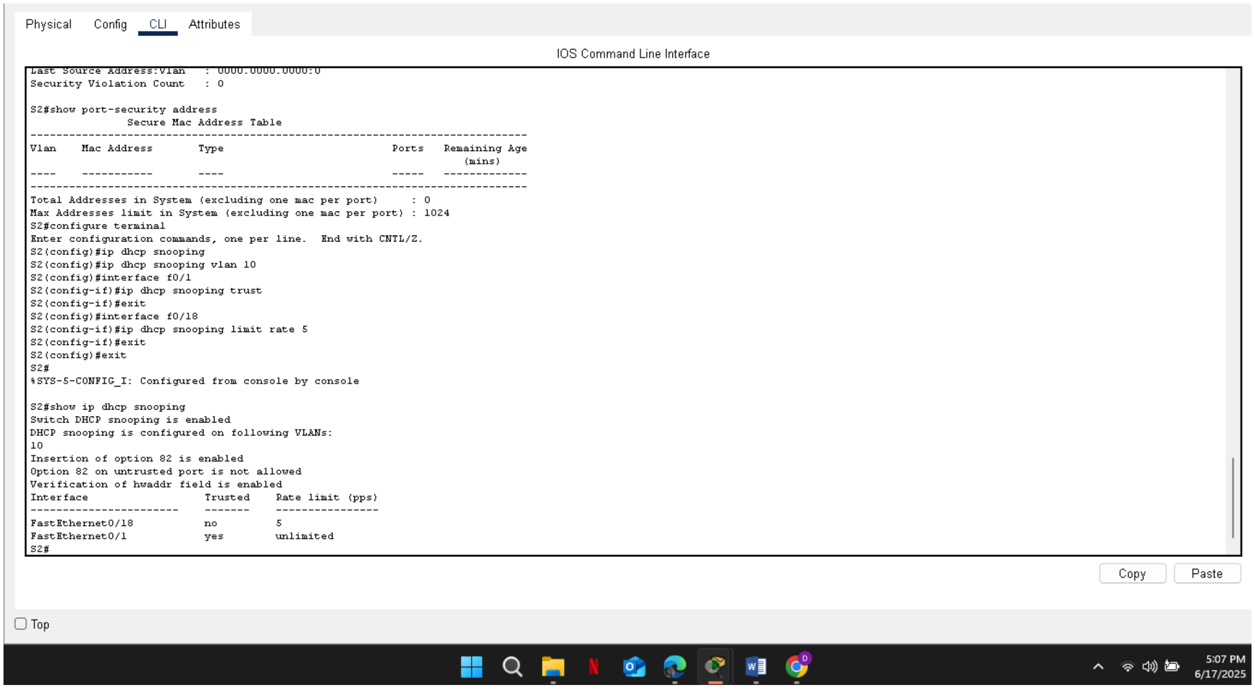


```
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#switchport port-security aging type inactivity
            ^
% Invalid input detected at '^' marker.

S1(config)#interface f0/6
S1(config-if)#switchport port-security aging type inactivity
                                               ^
% Invalid input detected at '^' marker.

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

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#









S1 con0 is now available
```



```
S2>enable
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#exit
S2(config)#interface f0/18
S2(config-if)#switchport port-security aging time 60
S2(config-if)#switchport port-security maximum 2
S2(config-if)#switchport port-security violation protect
S2(config-if)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#show port-security interface f0/18
Port Security              : Enabled
Port Status                : Secure-down
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#
```

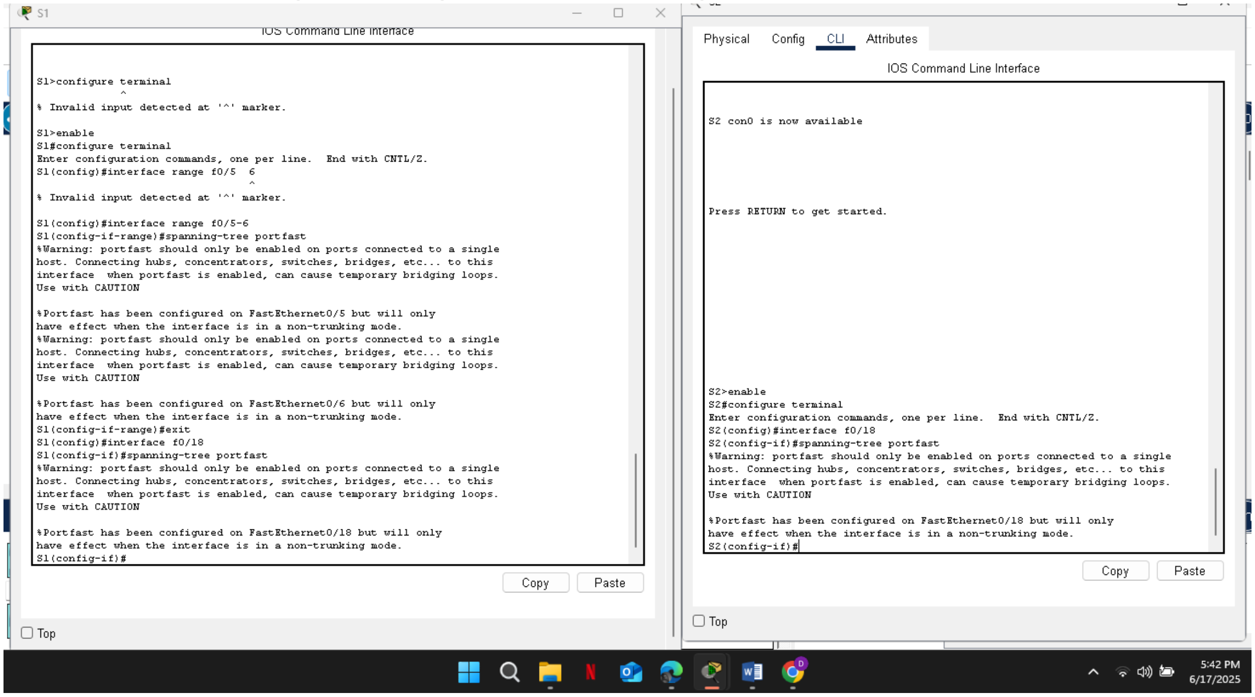
Enable port security for F0/18 on S2. Configure the port to add MAC addresses learned on the port automatically to the running configuration.



```
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#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#ip dhcp snooping
S2(config)#ip dhcp snooping vlan 10
S2(config)#interface f0/1
S2(config-if)#ip dhcp snooping trust
S2(config-if)#exit
S2(config)#interface f0/18
S2(config-if)#ip dhcp snooping limit rate 5
S2(config-if)#exit
S2(config)#exit
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)
-----------------------    -------    ----------------
FastEthernet0/18           no         5
FastEthernet0/1            yes        unlimited
S2#
```

Implement DHCP snooping security.

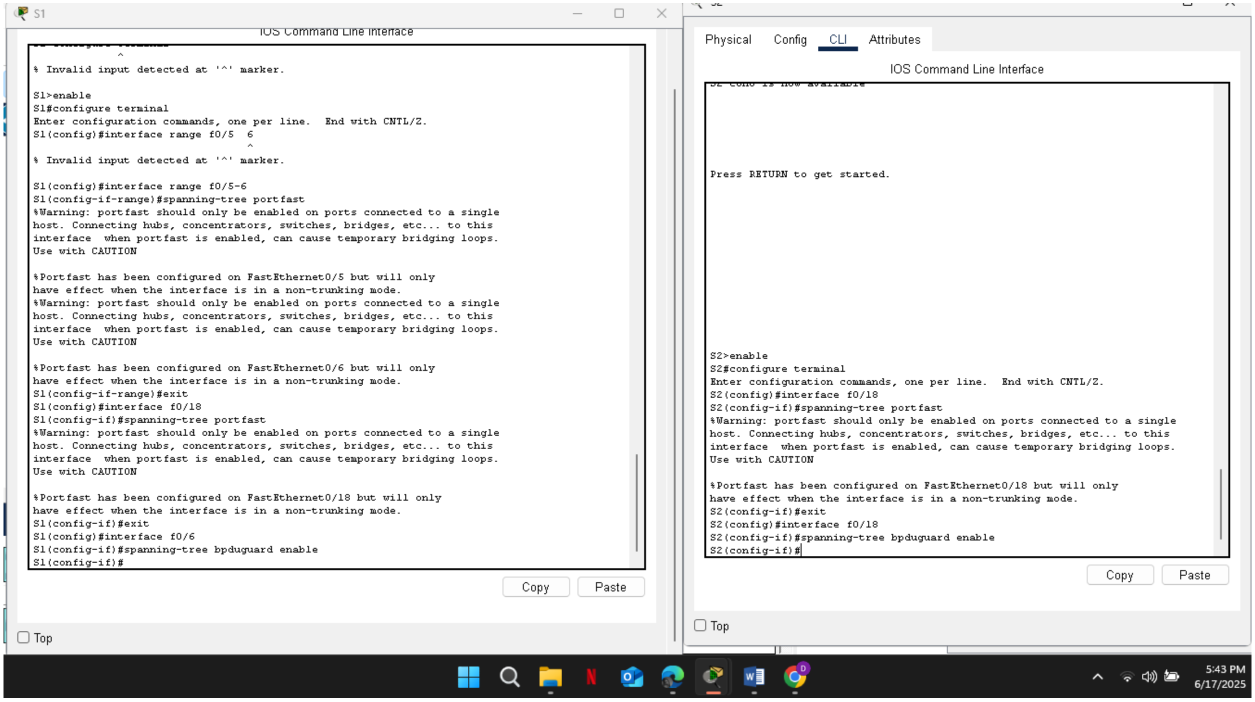
On S2, enable DHCP snooping and configure DHCP snooping on VLAN 10.



```
S1>configure terminal
             ^
% Invalid input detected at '^' marker.

S1>enable
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range f0/5  6
                                 ^
% 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 f0/18
S1(config-if)#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 FastEthernet0/18 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if)#
```

```
S2 con0 is now available




Press RETURN to get started.











S2>enable
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#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 FastEthernet0/18 but will only
have effect when the interface is in a non-trunking mode.
S2(config-if)#
```

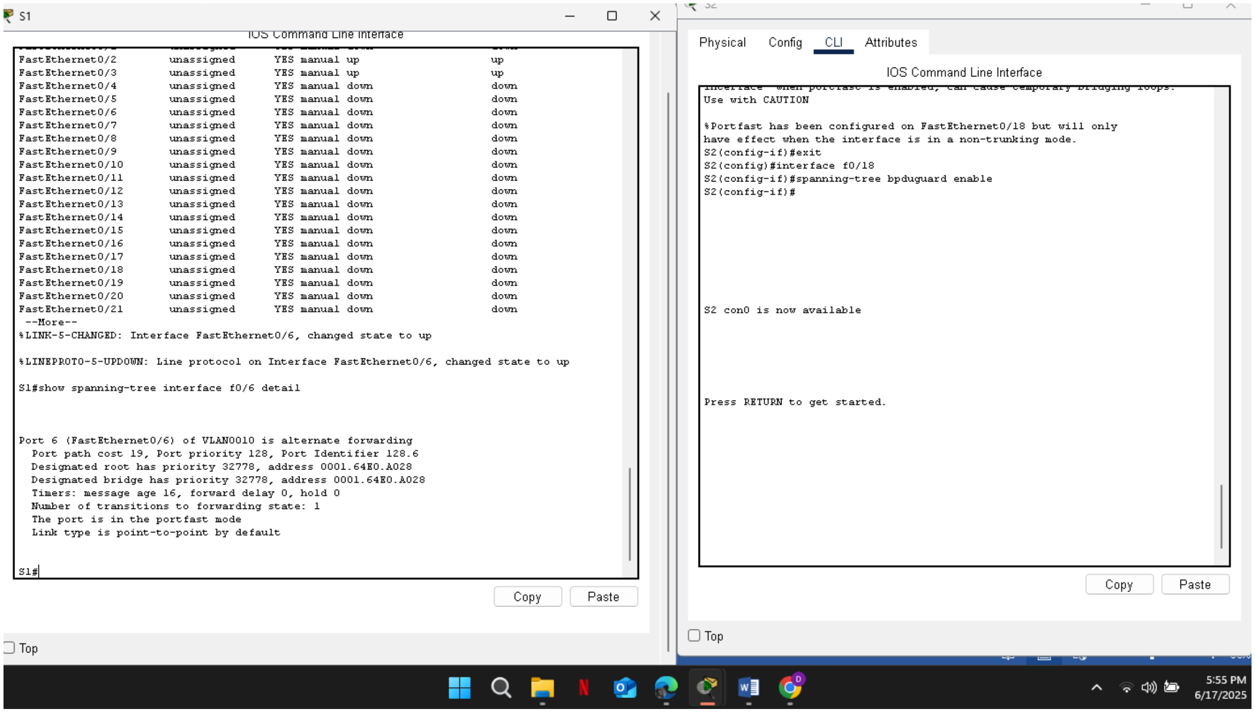
Configure PortFast on all the access ports that are in use on both switches.



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

S1>enable
S1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range f0/5  6
                                 ^
% 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 f0/18
S1(config-if)#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 FastEthernet0/18 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if)#exit
S1(config)#interface f0/6
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#
```

```
Press RETURN to get started.











S2>enable
S2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#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 FastEthernet0/18 but will only
have effect when the interface is in a non-trunking mode.
S2(config-if)#exit
S2(config)#interface f0/18
S2(config-if)#spanning-tree bpduguard enable
S2(config-if)#
```

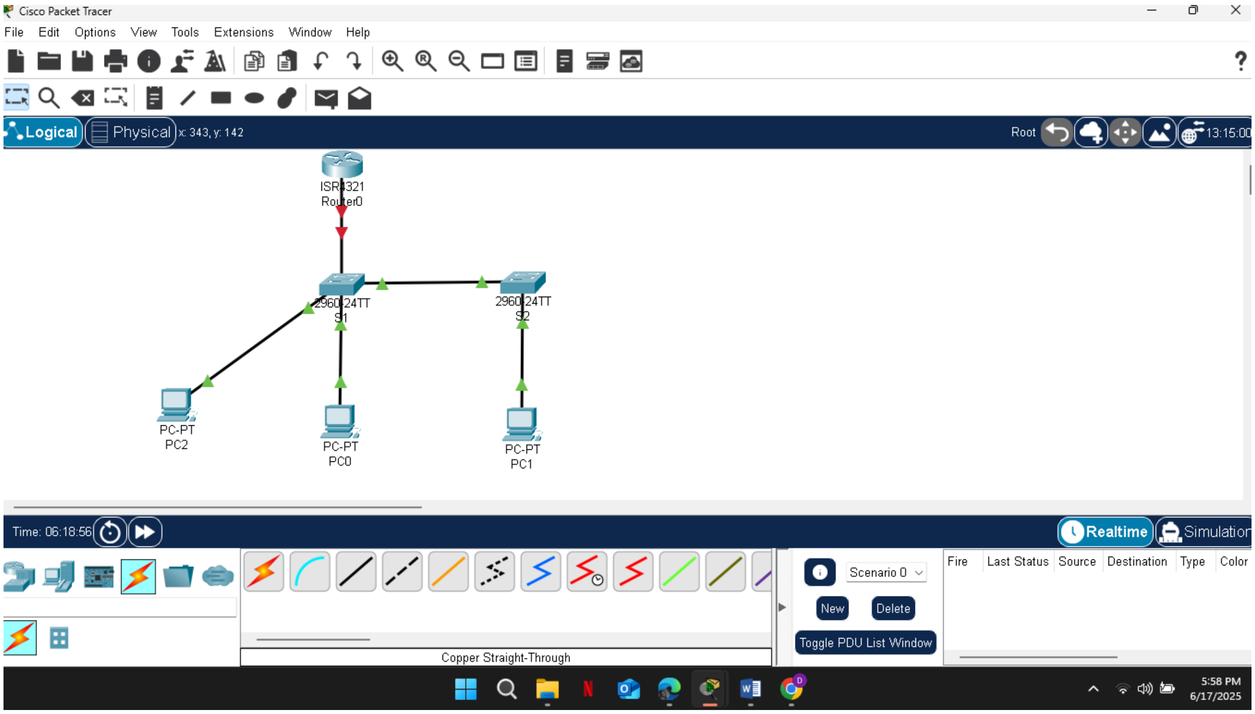
Enable BPDU guard on S1 and S2 VLAN 10 access ports connected to PC-A and PC-B.



```
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual up                    up
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
 --More--
%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to up

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

S1#show spanning-tree interface f0/6 detail



Port 6 (FastEthernet0/6) of VLAN0010 is alternate forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.6
  Designated root has priority 32778, address 0001.64E0.A028
  Designated bridge has priority 32778, address 0001.64E0.A028
  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#
```

```
Use with CAUTION

%Portfast has been configured on FastEthernet0/18 but will only
have effect when the interface is in a non-trunking mode.
S2(config-if)#exit
S2(config)#interface f0/18
S2(config-if)#spanning-tree bpduguard enable
S2(config-if)#








S2 con0 is now available







Press RETURN to get started.
```

Initially the command show spanning-tree interface f0/6 detail didn’t produce output because there is no device connected to it, once we introduce another computer we are able to get an output as shown above



# QUESTIONS

**Why is there no timer for the remaining age when sticky learning is used on S2?**

No timer is shown because aging hasn't been set, and sticky addresses stay in place until the switch is restarted or the port is cleared.

**Why won't PC-B (connected to port 18) get an IP address when the config is loaded on S2?**

PC-B won't get an IP because port 18 is either off, in the wrong VLAN, or blocked by security settings.

**What's the difference between absolute and inactivity aging types in port security?**

Absolute: clears MAC after the timer ends, even if the device is active.

Inactivity: clears MAC **only if** the device is idle for the full timer.

# CONCLUSION

Each component—from VLAN assignments and interface descriptions to advanced port security mechanisms was implemented to align with industry standards for a secure Layer 2 infrastructure.

By carefully applying port security and monitoring features such as DHCP snooping and BPDU Guard, we ensured that the switches are resilient against common threats like MAC flooding and rogue DHCP attacks. The use of sticky learning further allowed for dynamic yet persistent MAC address tracking, enhancing administrative control.