Assignment 1: VLANs and Secure Switch Configuration

Report by: Tonny Odhiambo, CS-CNS06-24028

Introduction.

In today's networked world, securing infrastructure components such as switches is paramount to maintaining the integrity and availability of network services. Switches play a crucial role in connecting various network devices and managing data traffic efficiently. However, they can also be vulnerable to a range of security threats, from unauthorized access to network attacks such as MAC address flooding, DHCP spoofing, and STP manipulations.

This report outlines a comprehensive approach to configuring switch security using Cisco Packet Tracer, demonstrating step-by-step how to implement VLANs, port security, DHCP snooping, and other critical security features to protect a network.

Objectives

Part 1: Configure the Network Devices.

- Cable the network.
- Configure R1.
- Configure and verify basic switch settings.

Part 2: Configure VLANs on Switches.

- Configure VLAN 10.
- Configure the SVI for VLAN 10.
- Configure VLAN 333 with the name Native on S1 and S2.
- Configure VLAN 999 with the name ParkingLot on S1 and S2.

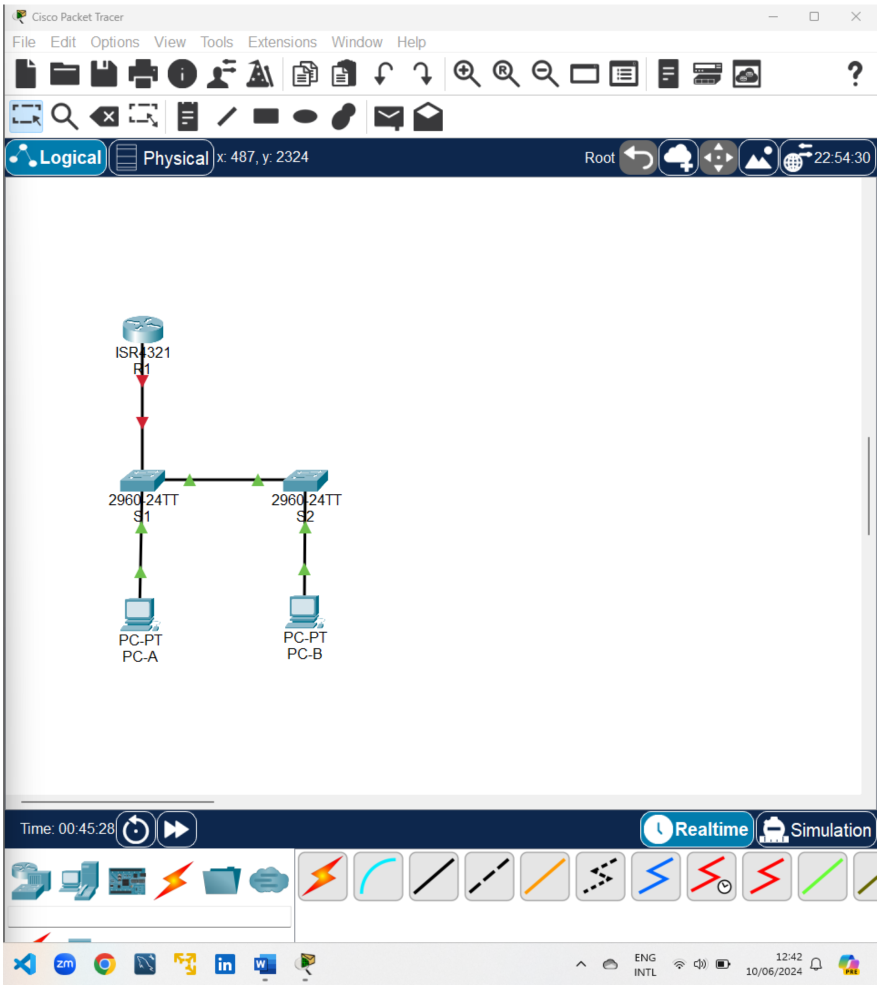
Part 3: Configure Switch Security.

- Implement 802.1Q trunking.
- Configure access ports.
- Secure and disable unused switchports.
- Document and implement port security features.

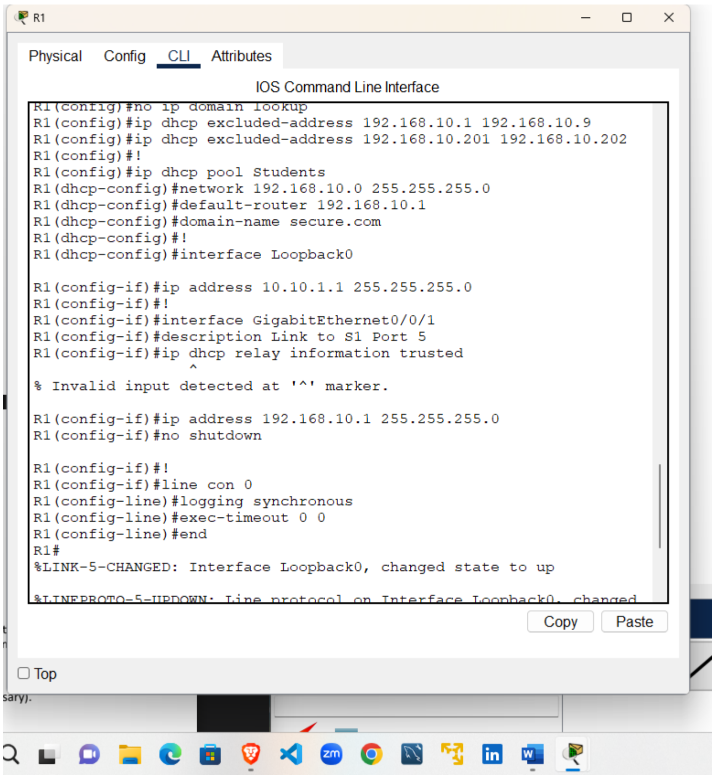
- Implement DHCP snooping security.
- Implement PortFast and BPDU guard.
- Verify end-to-end-connectivity.

Part 1: Configuration the Network Devices.

Step 1: Cable the network.

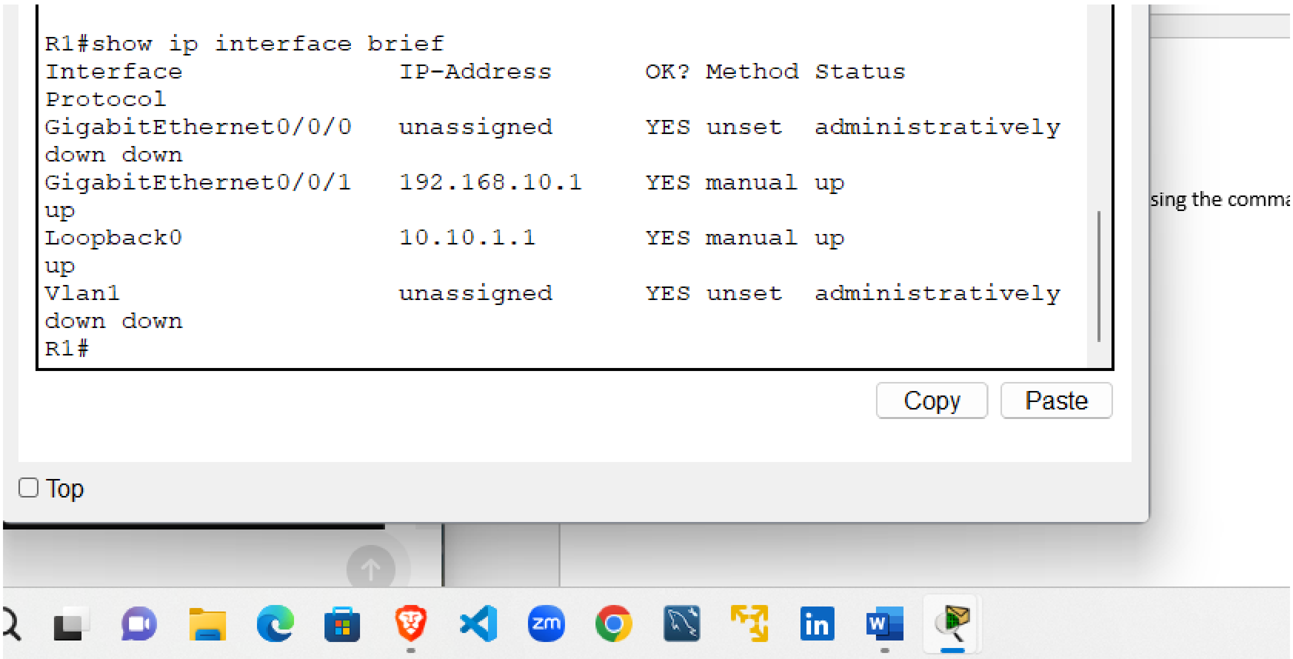


Step 2: Configuration of R1.



```
R1(config)#no ip domain lookup
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)#ip dhcp excluded-address 192.168.10.201 192.168.10.202
R1(config)#!
R1(config)#ip dhcp pool Students
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#domain-name secure.com
R1(dhcp-config)#!
R1(dhcp-config)#interface Loopback0

R1(config-if)#ip address 10.10.1.1 255.255.255.0
R1(config-if)#!
R1(config-if)#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)#!
R1(config-if)#line con 0
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 0 0
R1(config-line)#end
R1#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed
```

Verification of the running-configuration on R1 using the command: **show ip interface brief**

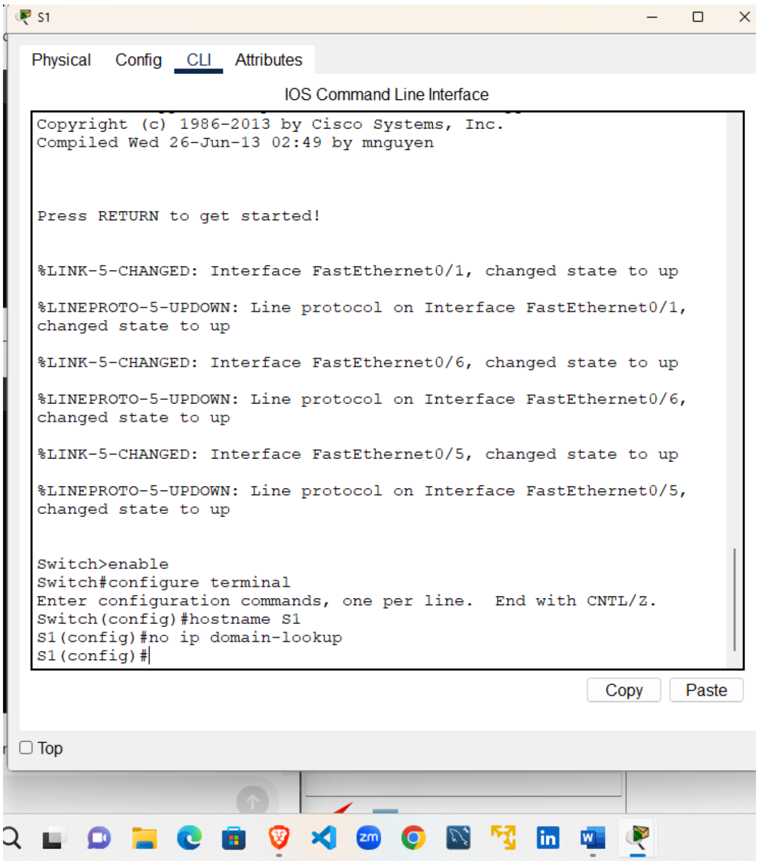


```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively
down down
GigabitEthernet0/0/1   192.168.10.1    YES manual up
up
Loopback0              10.10.1.1       YES manual up
up
Vlan1         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

Step 3: Configuration and Verification of Basic Switch Settings

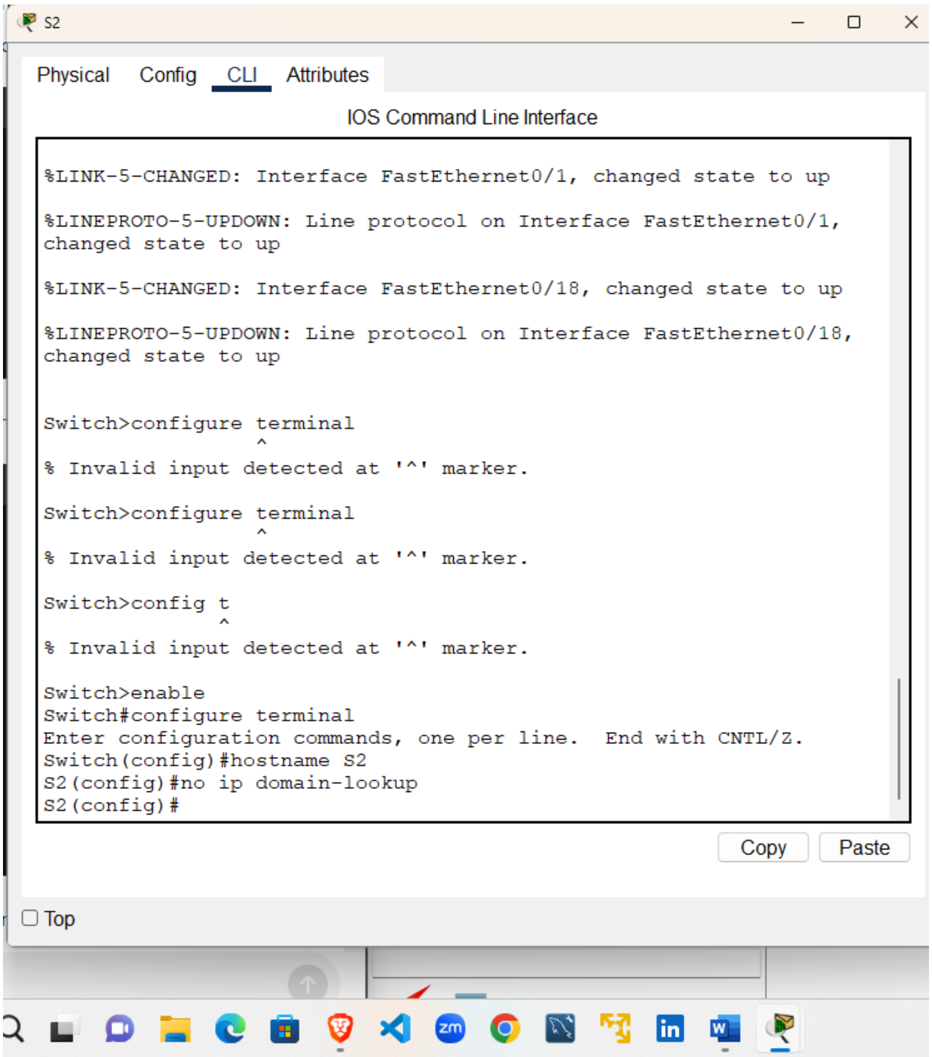
1. **Configuration of the hostname for switches S1 and S2:**

S1 Configuration



```
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 FastEthernet0/6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6,
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>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#
```

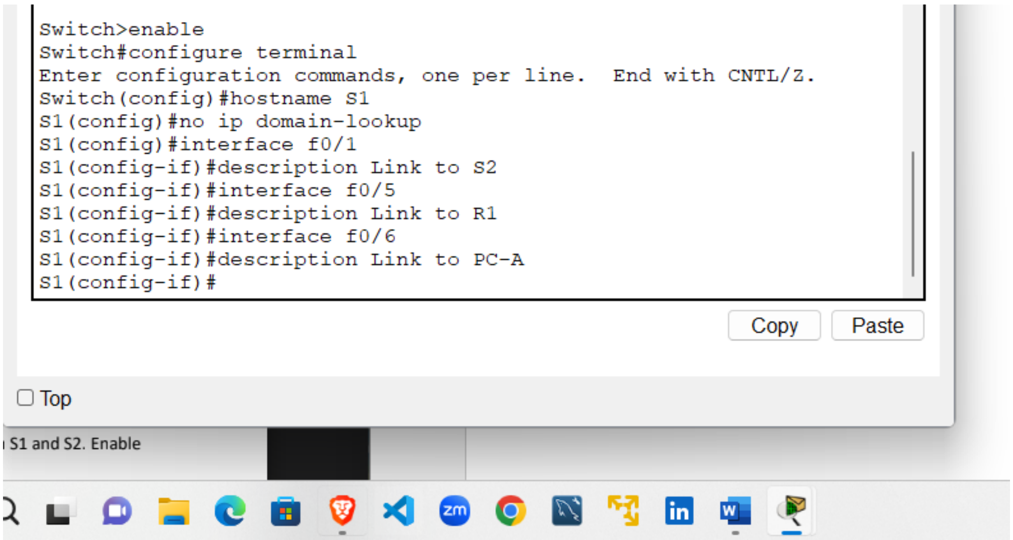
S2 Configuration



```
%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 FastEthernet0/18, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18,
changed state to up


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

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

Switch>config t
              ^
% Invalid input detected at '^' marker.

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#
```

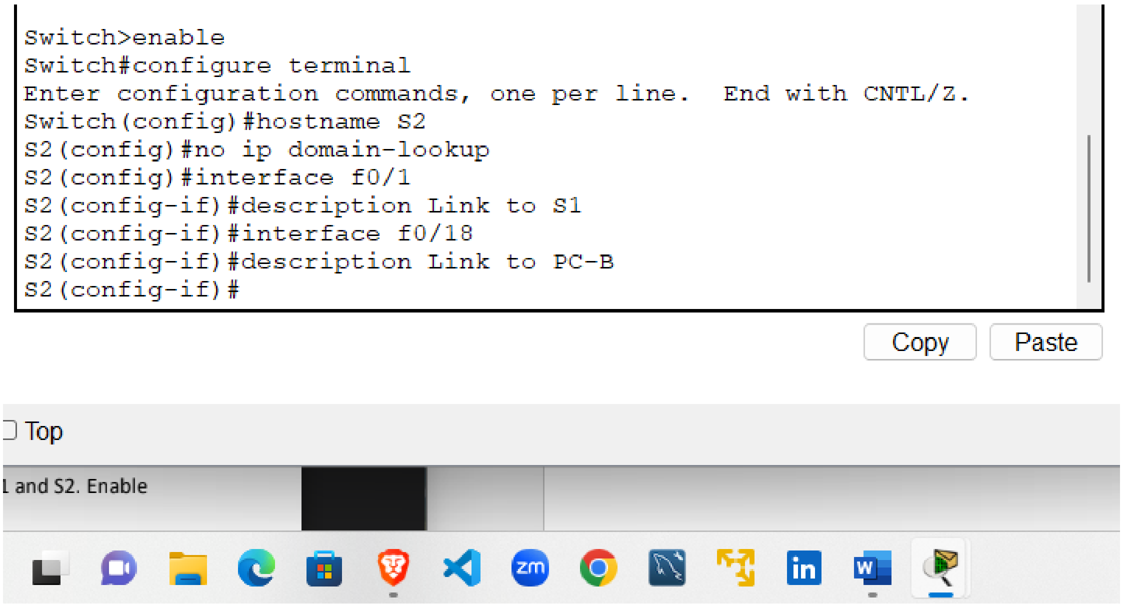
2. Configuration of interface descriptions for the ports in use:

S1 Configuration



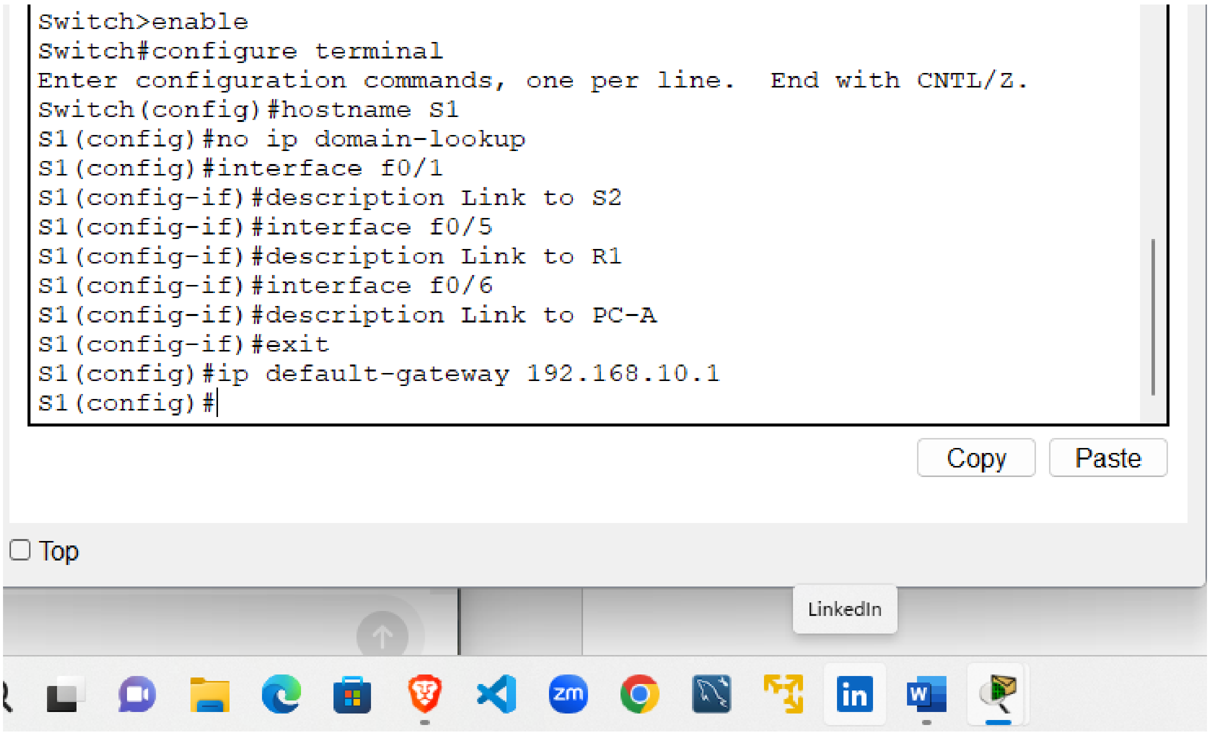
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#interface f0/1
S1(config-if)#description Link to S2
S1(config-if)#interface f0/5
S1(config-if)#description Link to R1
S1(config-if)#interface f0/6
S1(config-if)#description Link to PC-A
S1(config-if)#
```

S2 Configuration



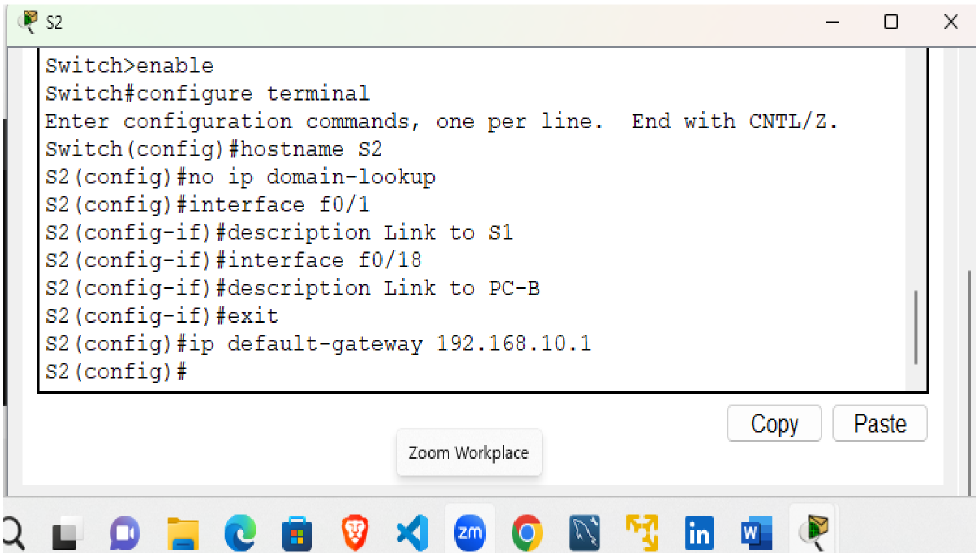
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#interface f0/1
S2(config-if)#description Link to S1
S2(config-if)#interface f0/18
S2(config-if)#description Link to PC-B
S2(config-if)#
```

3. **Setting the default gateway for the Management VLAN to 192.168.10.1 on both switches:**
S1



```
Switch>enable
Switch#configure terminal
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)#exit
S1(config)#ip default-gateway 192.168.10.1
S1(config)#
```

S2



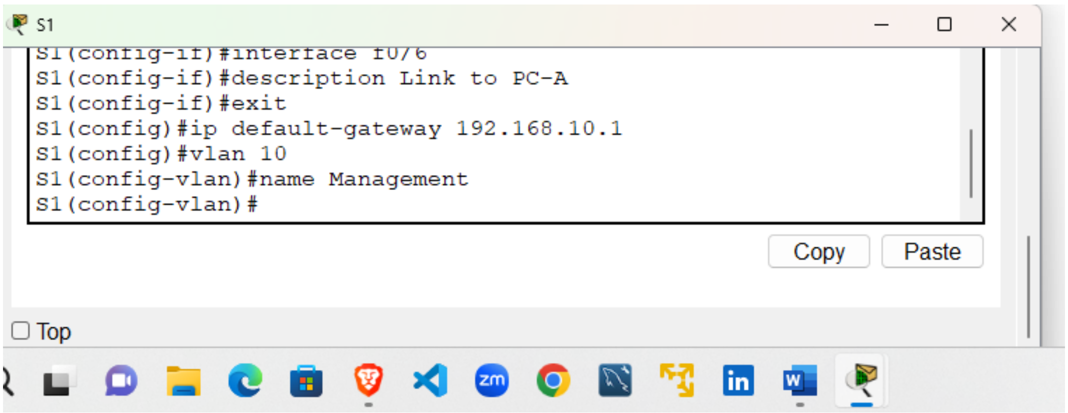
```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#interface f0/1
S2(config-if)#description Link to S1
S2(config-if)#interface f0/18
S2(config-if)#description Link to PC-B
S2(config-if)#exit
S2(config)#ip default-gateway 192.168.10.1
S2(config)#
```

Part 2: Configuration of VLANs on Switches

Step 1: Configuration of VLAN 10

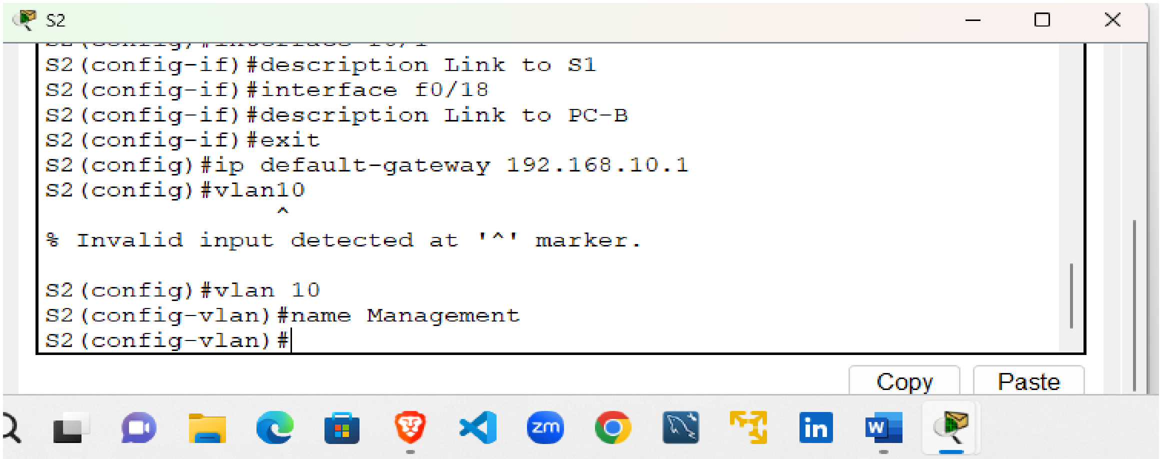
a) **Add VLAN 10 to S1 and S2:**

S1



```
S1(config-if)#interface f0/6
S1(config-if)#description Link to PC-A
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.10.1
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#
```

S2

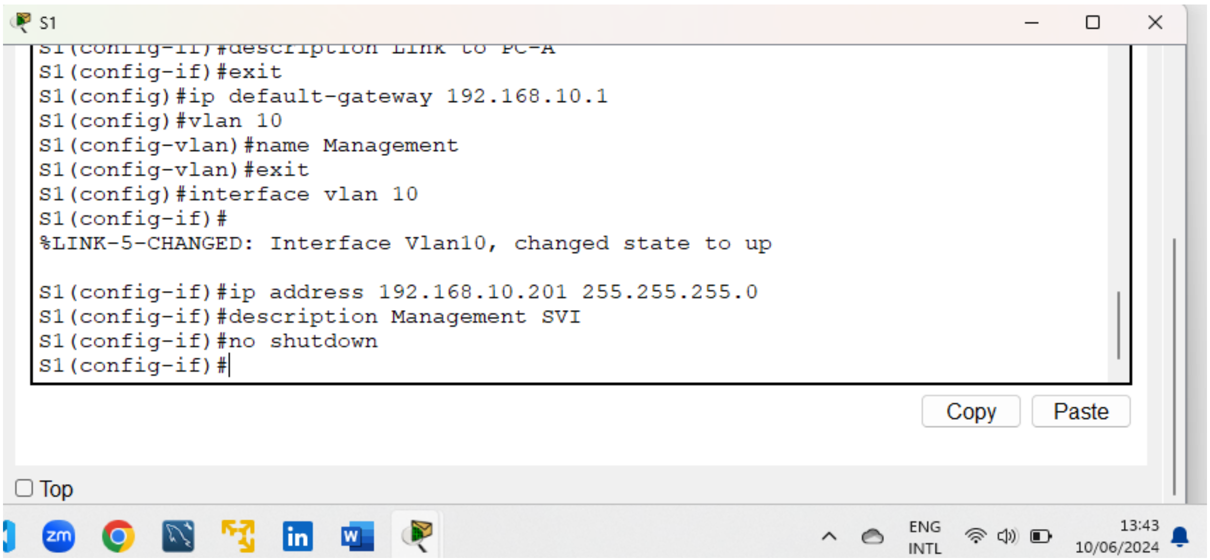


```
S2(config)#interface f0/1
S2(config-if)#description Link to S1
S2(config-if)#interface f0/18
S2(config-if)#description Link to PC-B
S2(config-if)#exit
S2(config)#ip default-gateway 192.168.10.1
S2(config)#vlan10
                ^
% Invalid input detected at '^' marker.

S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#
```

Step 2: Configure the SVI for VLAN 10

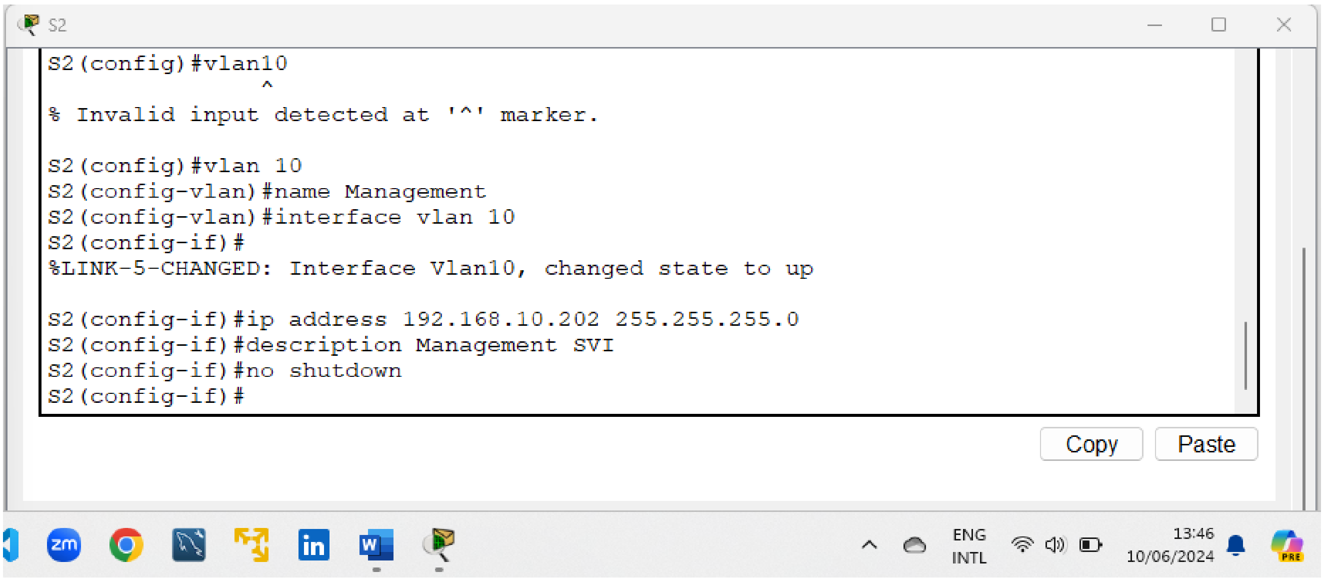
a) **Configure the IP address and enable the SVI interfaces on S1 and S2:**

S1



```
S1(config-if)#description Link to PC-A
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.10.1
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config)#interface vlan 10
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

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

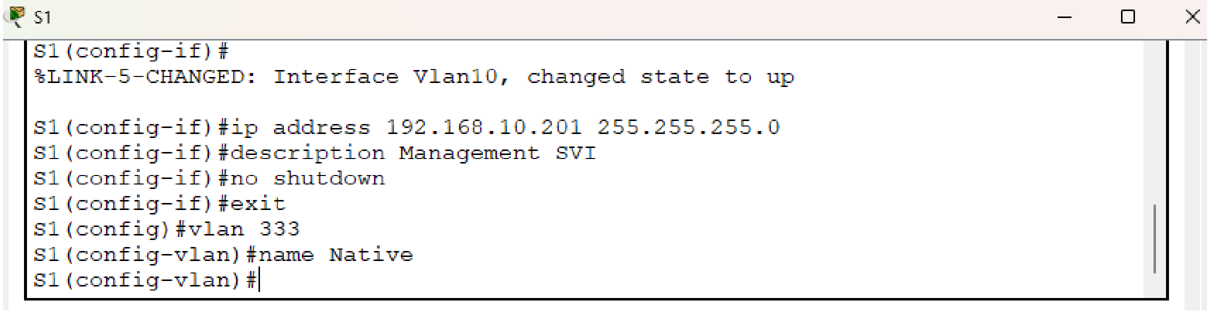
S2



```
S2(config)#vlan10
                 ^
% Invalid input detected at '^' marker.

S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#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)#
```

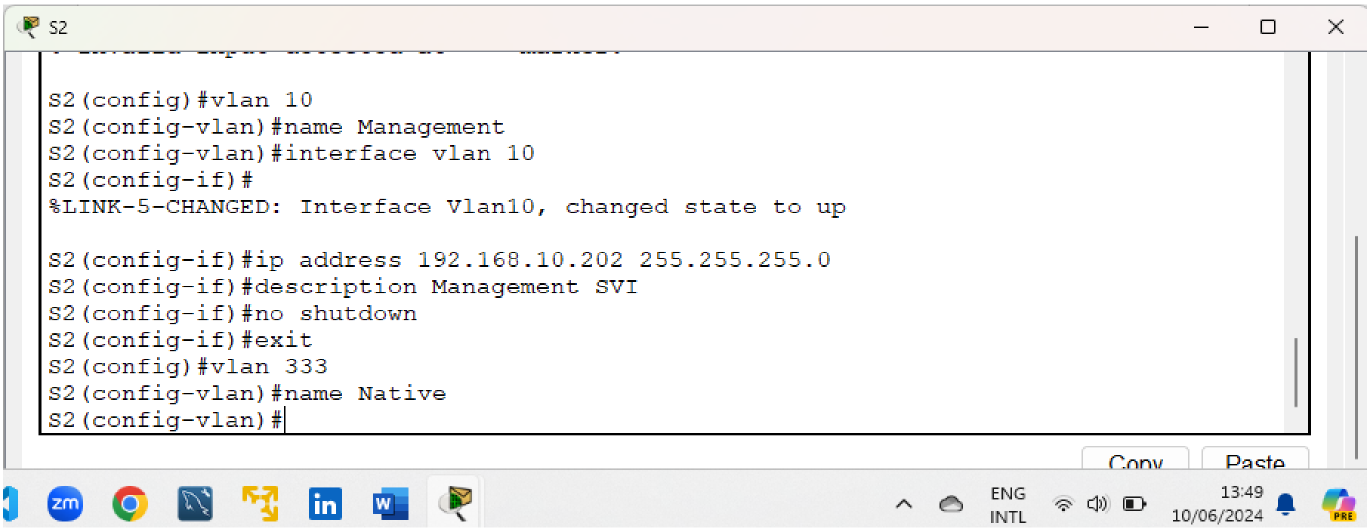
Step 3: Configure VLAN 333 with the Name Native

S1



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

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)#exit
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#
```

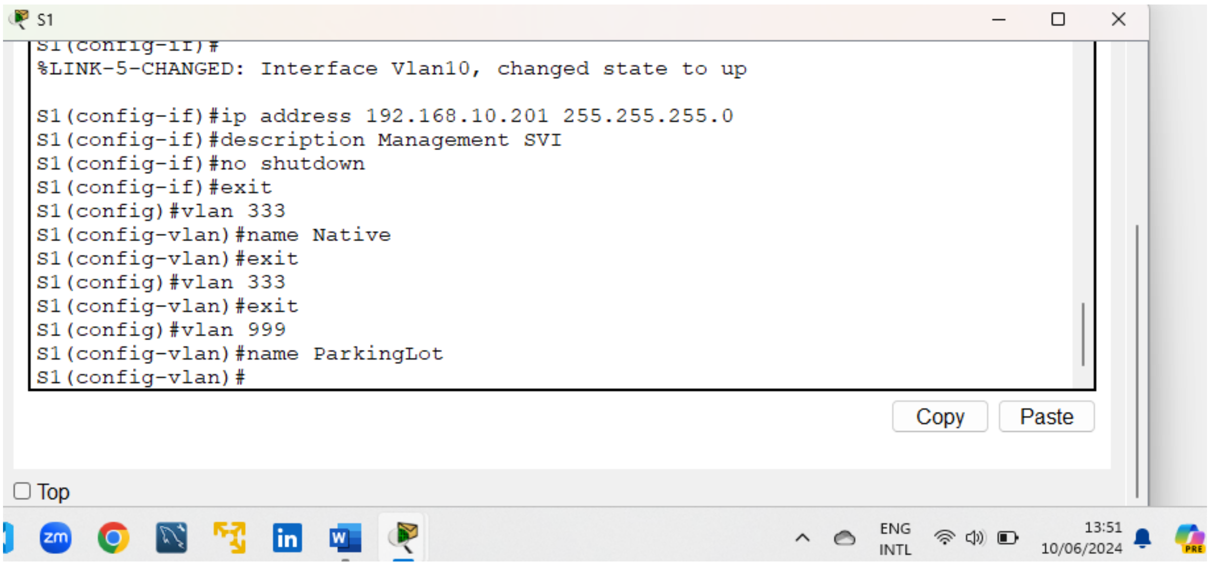
S2



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

S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#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)#exit
S2(config)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#
```

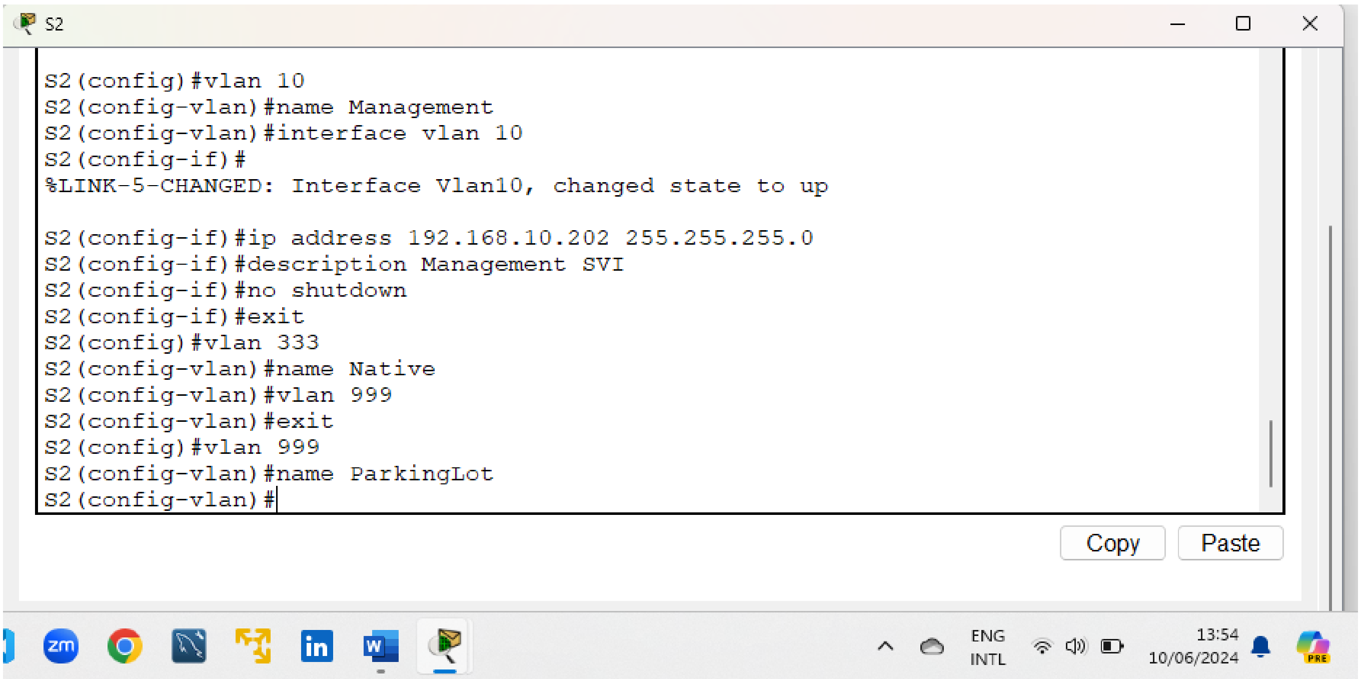
Step 4: Configure VLAN 999 with the Name ParkingLot

S1



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

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)#exit
S1(config)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#exit
S1(config)#vlan 333
S1(config-vlan)#exit
S1(config)#vlan 999
S1(config-vlan)#name ParkingLot
S1(config-vlan)#
```

S2



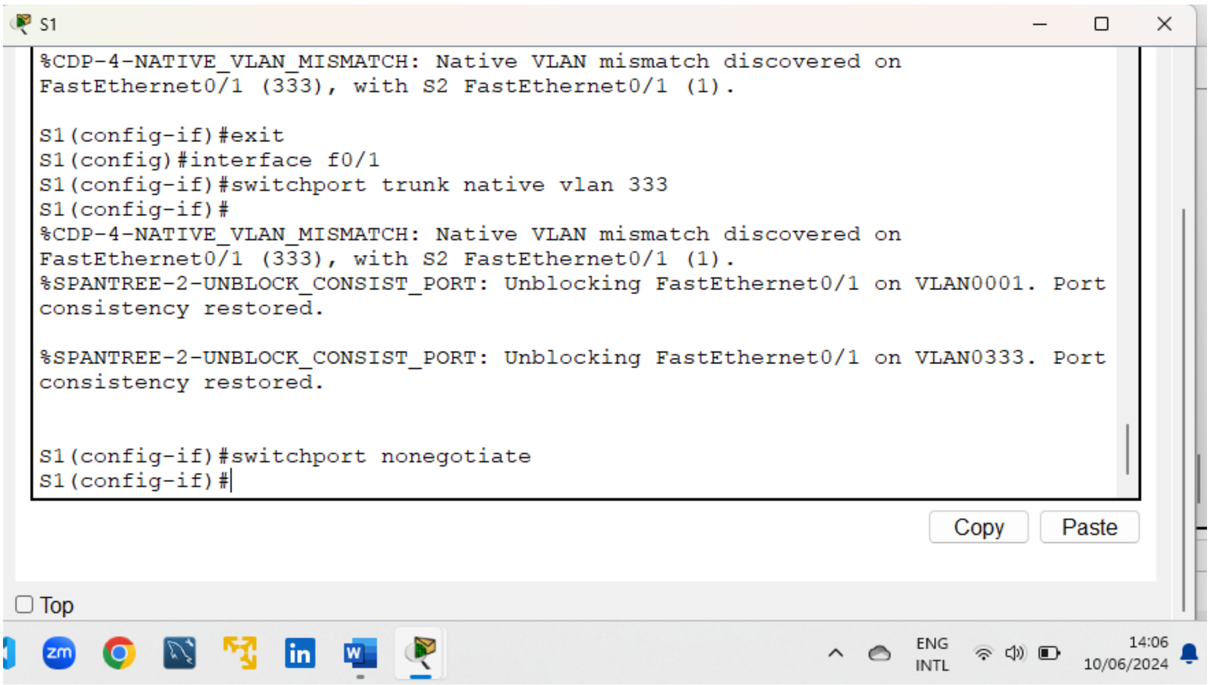
```
S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#interface vlan 10
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

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)#exit
S2(config)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#vlan 999
S2(config-vlan)#exit
S2(config)#vlan 999
S2(config-vlan)#name ParkingLot
S2(config-vlan)#
```

Part 3: Configure Switch Security

Step 1: Implement 802.1Q Trunking

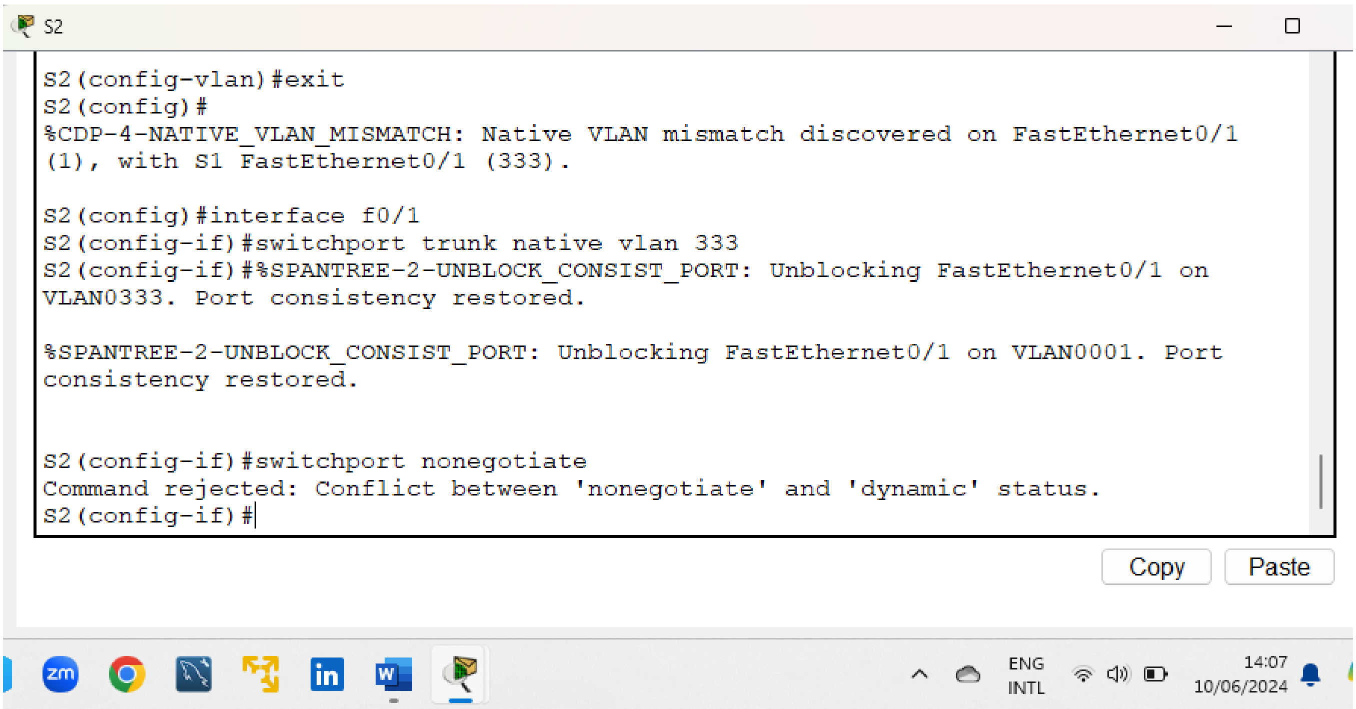
a) **Configure trunking on F0/1 to use VLAN 333 as the native VLAN:**

S1



```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/1 (333), with S2 FastEthernet0/1 (1).

S1(config-if)#exit
S1(config)#interface f0/1
S1(config-if)#switchport trunk native vlan 333
S1(config-if)#
%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)#switchport nonegotiate
S1(config-if)#
```

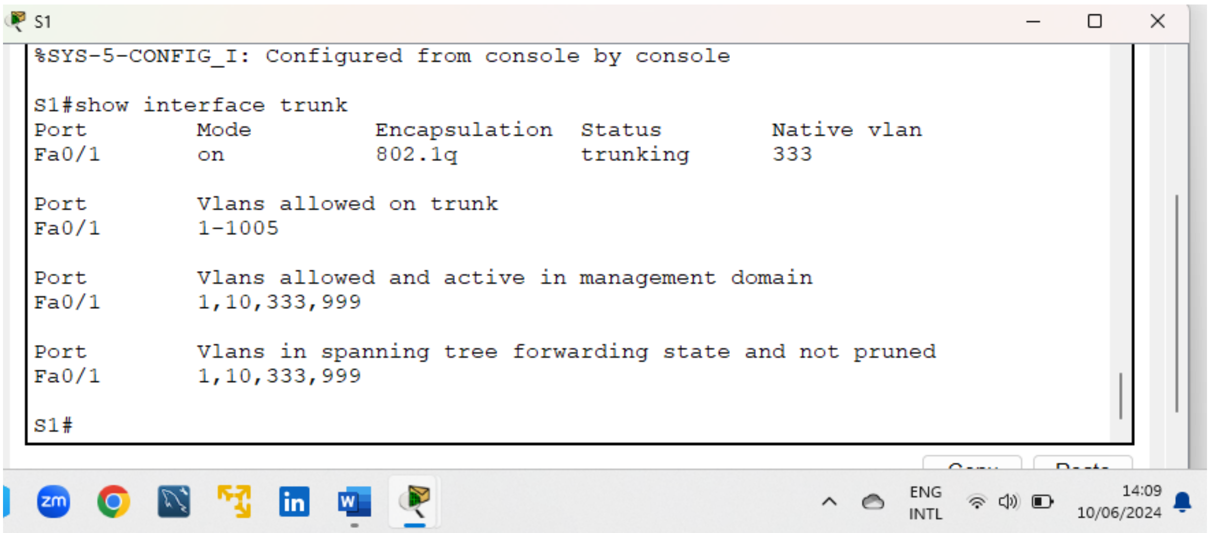
S2



```
S2(config-vlan)#exit
S2(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1
(1), with S1 FastEthernet0/1 (333).

S2(config)#interface f0/1
S2(config-if)#switchport trunk native vlan 333
S2(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on
VLAN0333. Port consistency restored.

%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0001. Port
consistency restored.


S2(config-if)#switchport nonegotiate
Command rejected: Conflict between 'nonegotiate' and 'dynamic' status.
S2(config-if)#
```

b) Verify trunking configuration:

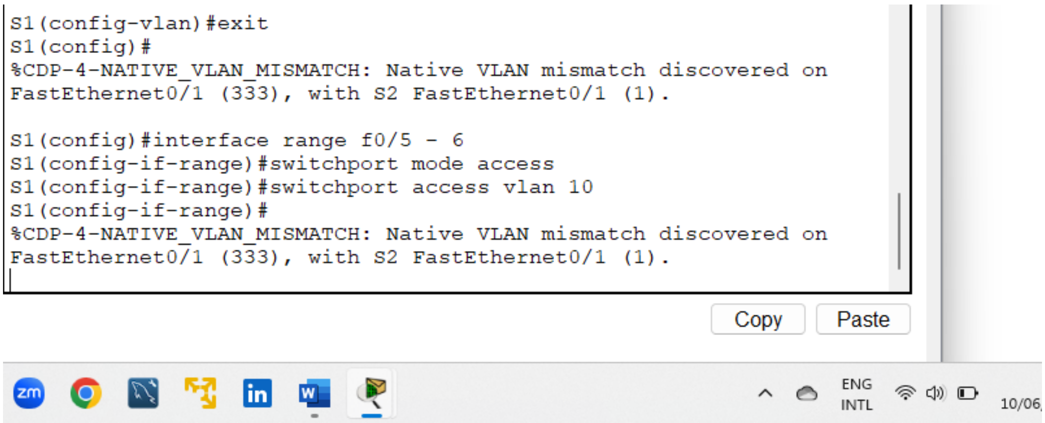
S1



```
%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#
```

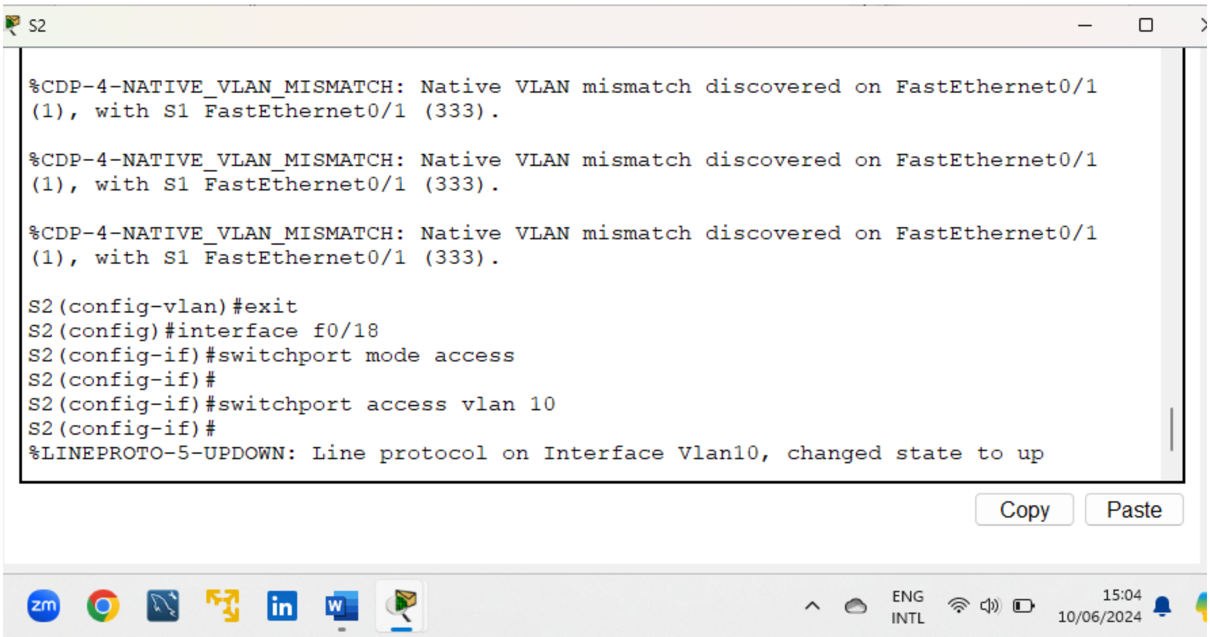
Step 2: Configure Access Ports

a) **Configure F0/5 and F0/6 as access ports on S1:**



```
S1(config-vlan)#exit
S1(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/1 (333), with S2 FastEthernet0/1 (1).

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)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on
FastEthernet0/1 (333), with S2 FastEthernet0/1 (1).
```

b) **Configure F0/18 as an access port on S2:**

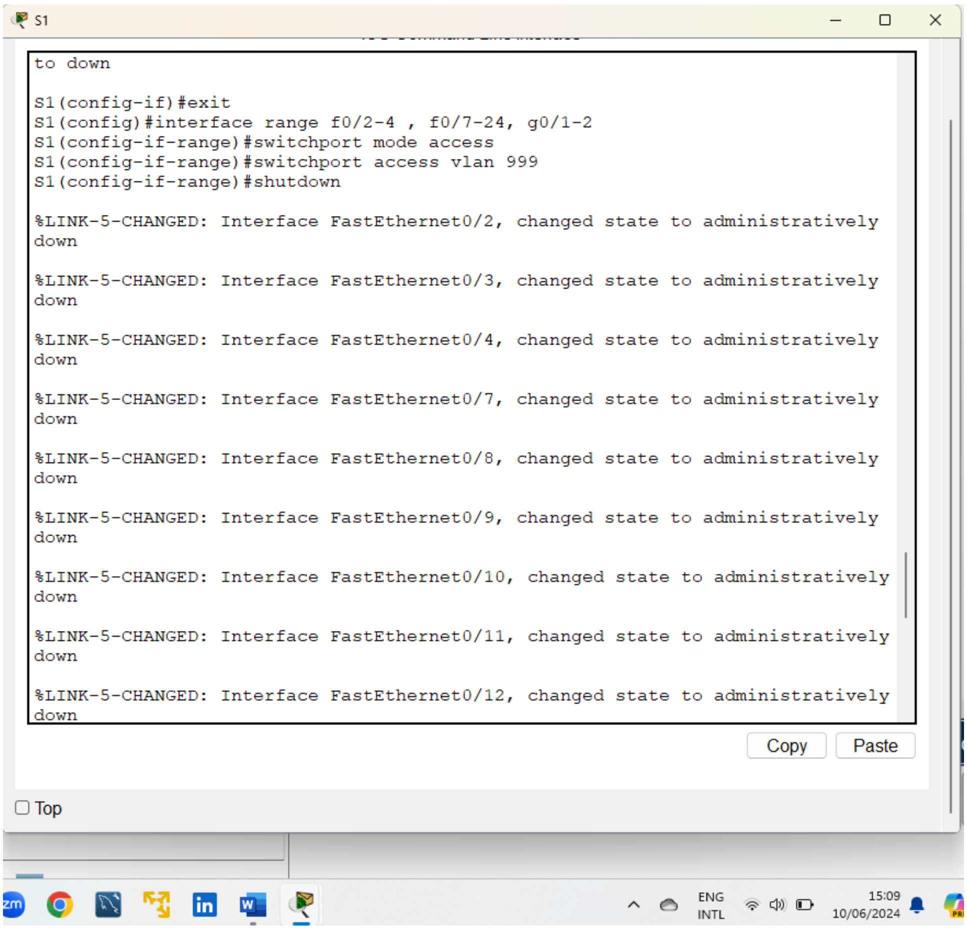


```
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1
(1), with S1 FastEthernet0/1 (333).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1
(1), with S1 FastEthernet0/1 (333).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1
(1), with S1 FastEthernet0/1 (333).

S2(config-vlan)#exit
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#
S2(config-if)#switchport access vlan 10
S2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
```

Step 3: Secure and Disable Unused Switchports

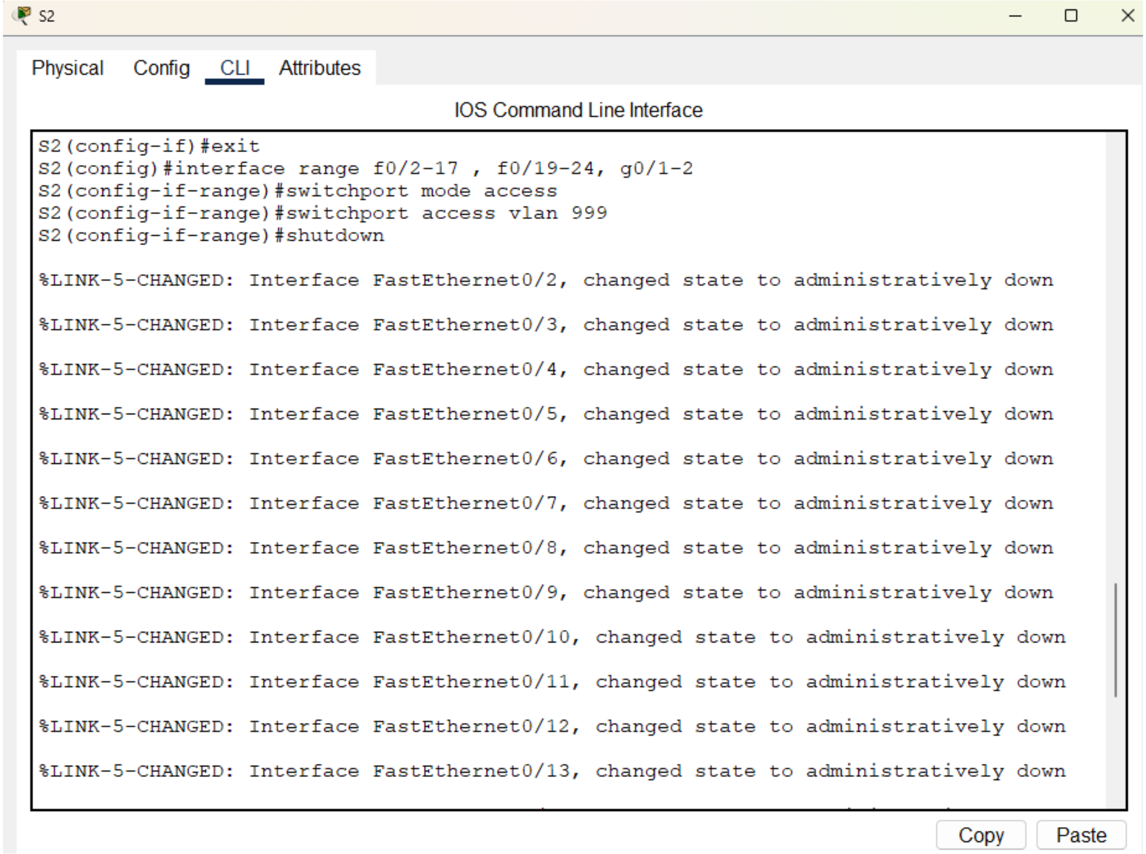
a) Move unused ports to VLAN 999 and disable them.

S1



```
to down

S1(config-if)#exit
S1(config)#interface range f0/2-4 , f0/7-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#shutdown

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

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

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively
down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively
down
```

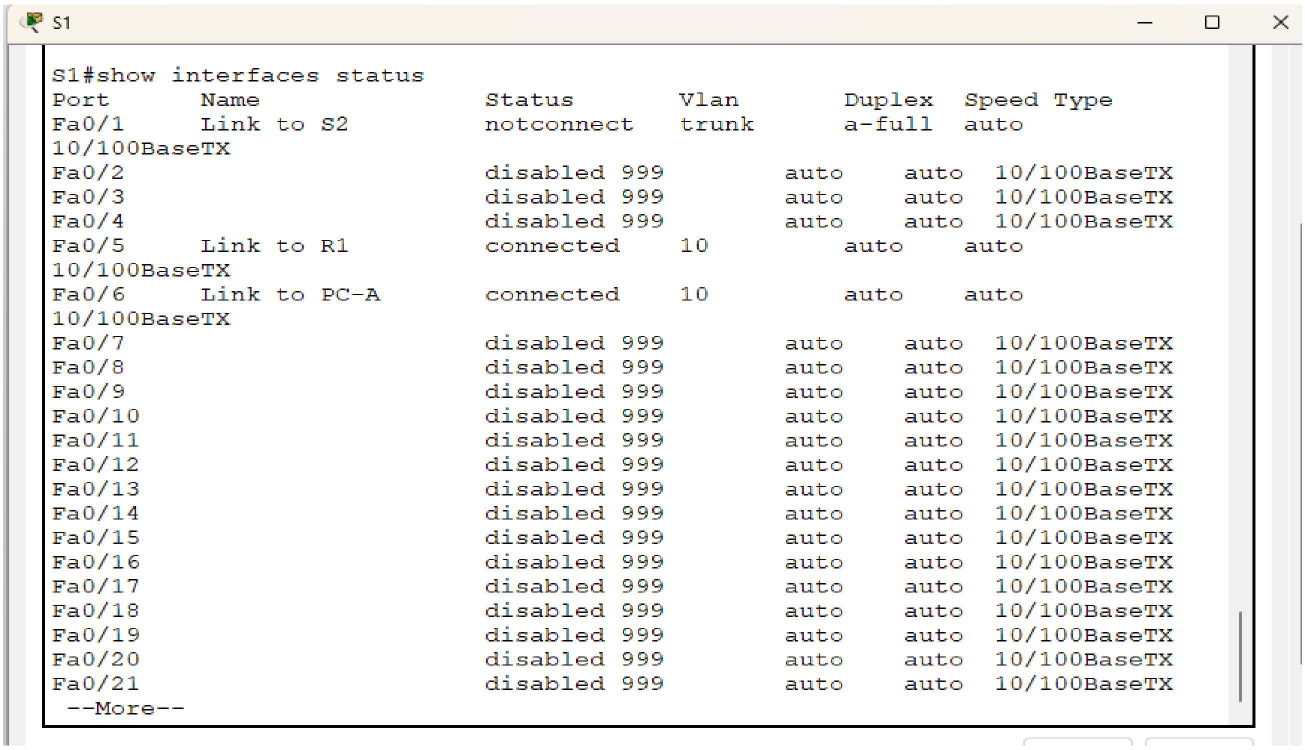
S2



```
S2(config-if)#exit
S2(config)#interface range f0/2-17 , f0/19-24, g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 999
S2(config-if-range)#shutdown

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

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

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/12, changed state to administratively down

%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
```

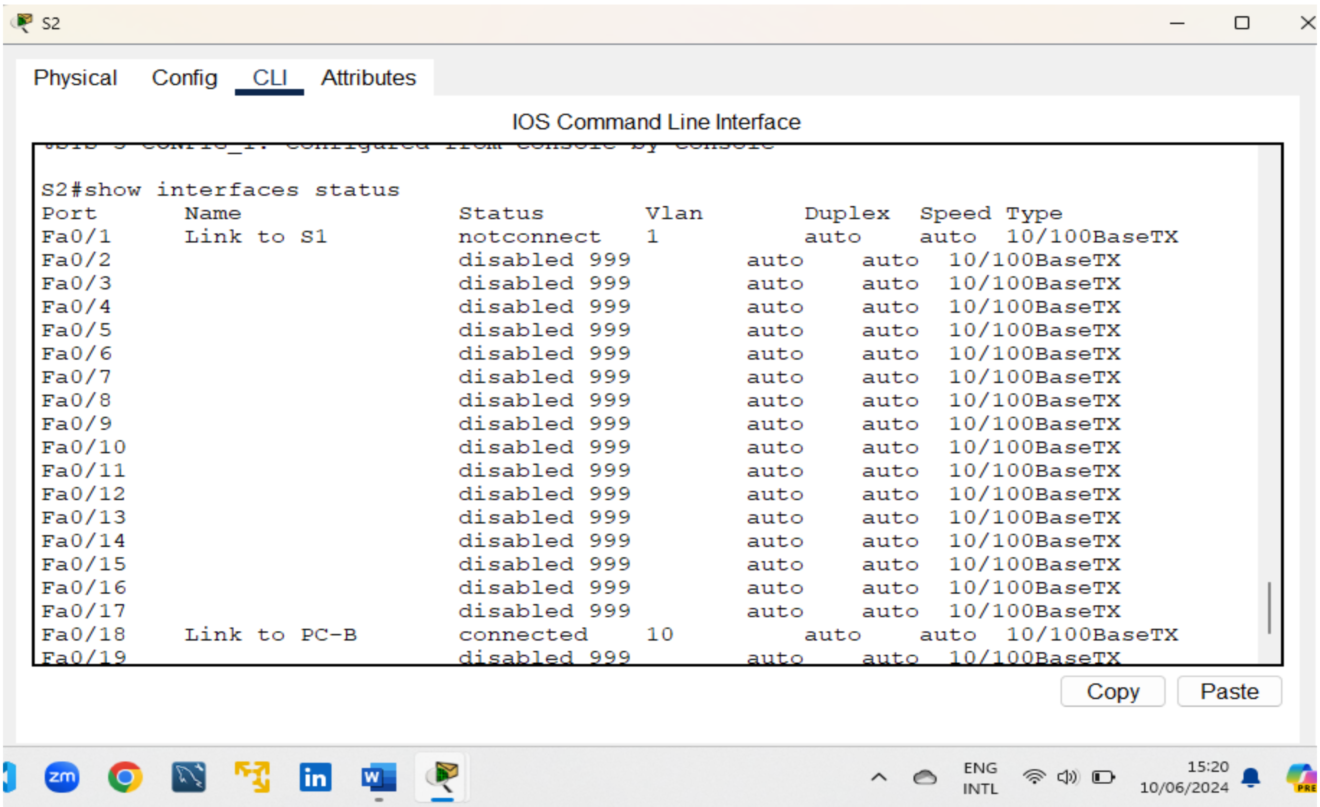
b) Verify the configuration:

S1



```
S1#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Link to S2         notconnect   trunk      a-full  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--
```

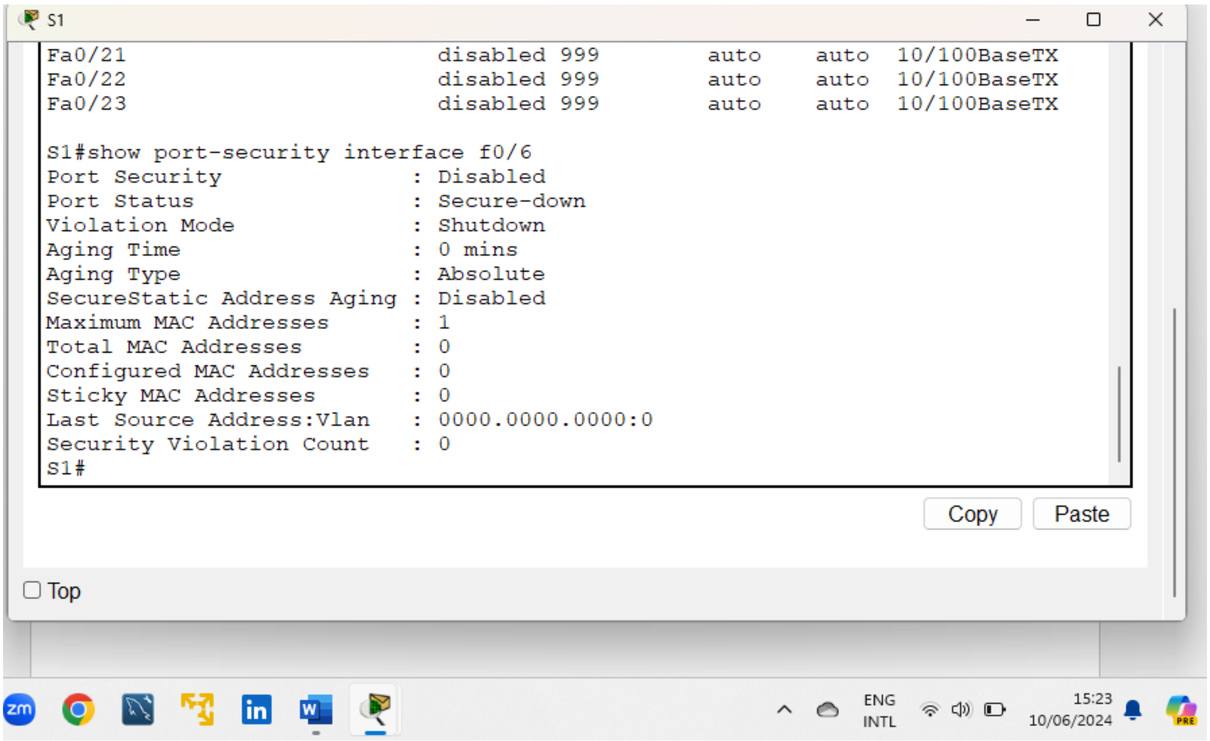
S2



```
%SYS-5-CONFIG_I: Configured from console by console

S2#show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Link to S1         notconnect   1          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                        disabled 999        auto    auto  10/100BaseTX
Fa0/6                        disabled 999        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    Link to PC-B       connected    10         auto    auto  10/100BaseTX
Fa0/19                       disabled 999        auto    auto  10/100BaseTX
```

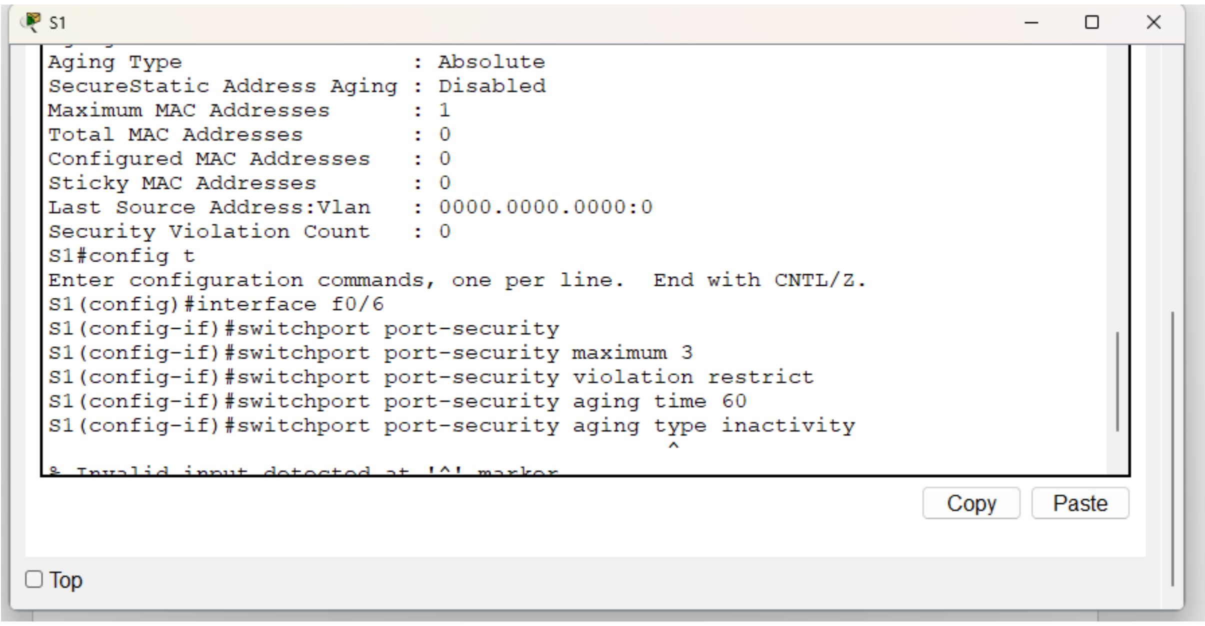
Step 4: Document and Implement Port Security Features

a) **Verify default port security settings for F0/6 on S1**



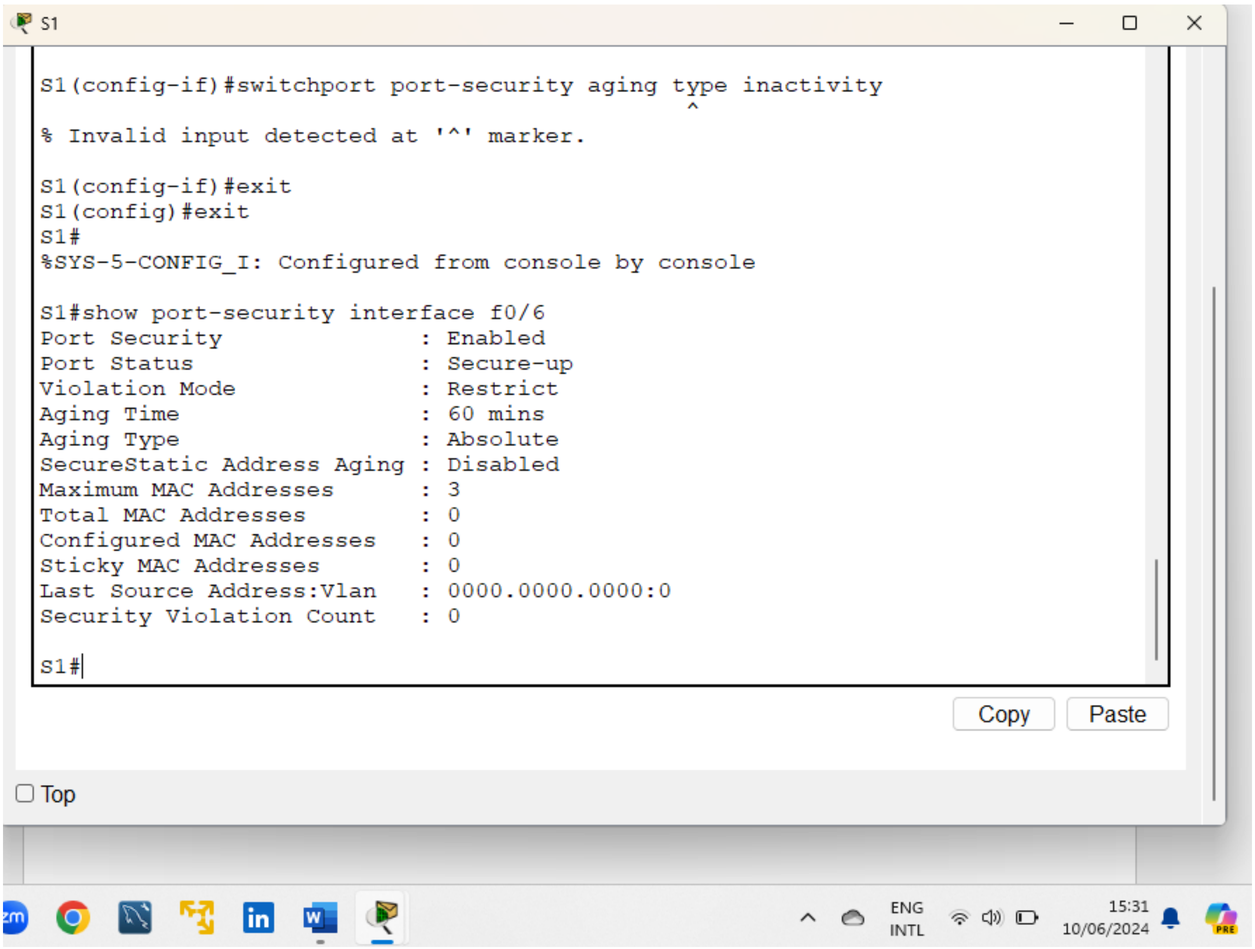
```
Fa0/21                       disabled 999        auto    auto  10/100BaseTX
Fa0/22                       disabled 999        auto    auto  10/100BaseTX
Fa0/23                       disabled 999        auto    auto  10/100BaseTX

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#
```

b) **Configure port security on S1 F0/6:**

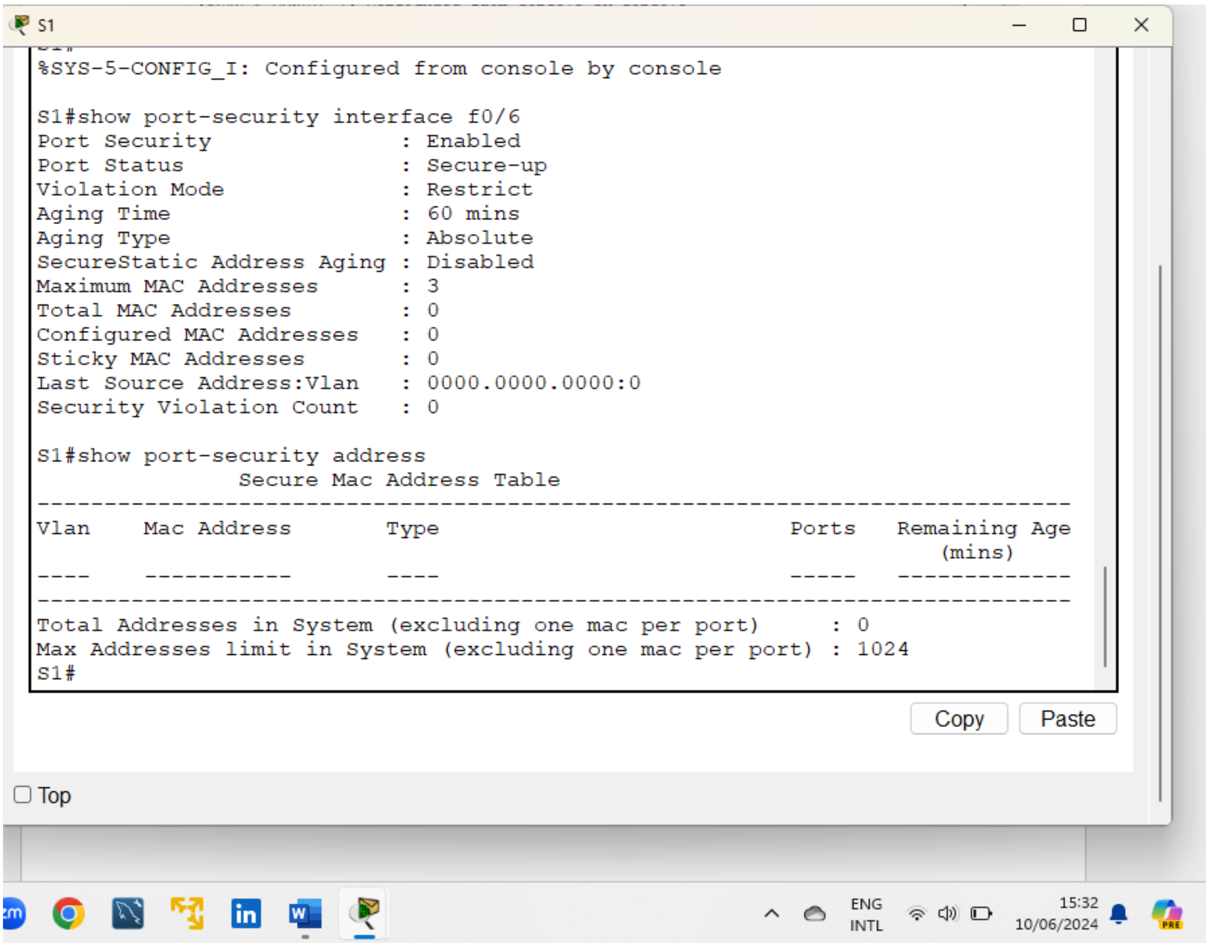


```
Aging Type                  : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses       : 1
Total MAC Addresses         : 0
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 0
Last Source Address:Vlan    : 0000.0000.0000:0
Security Violation Count    : 0
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/6
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3
S1(config-if)#switchport port-security violation restrict
S1(config-if)#switchport port-security aging time 60
S1(config-if)#switchport port-security aging type inactivity
                                                     ^
% Invalid input detected at '^' marker.
```

c) **Verify port security on S1 F0/6:**

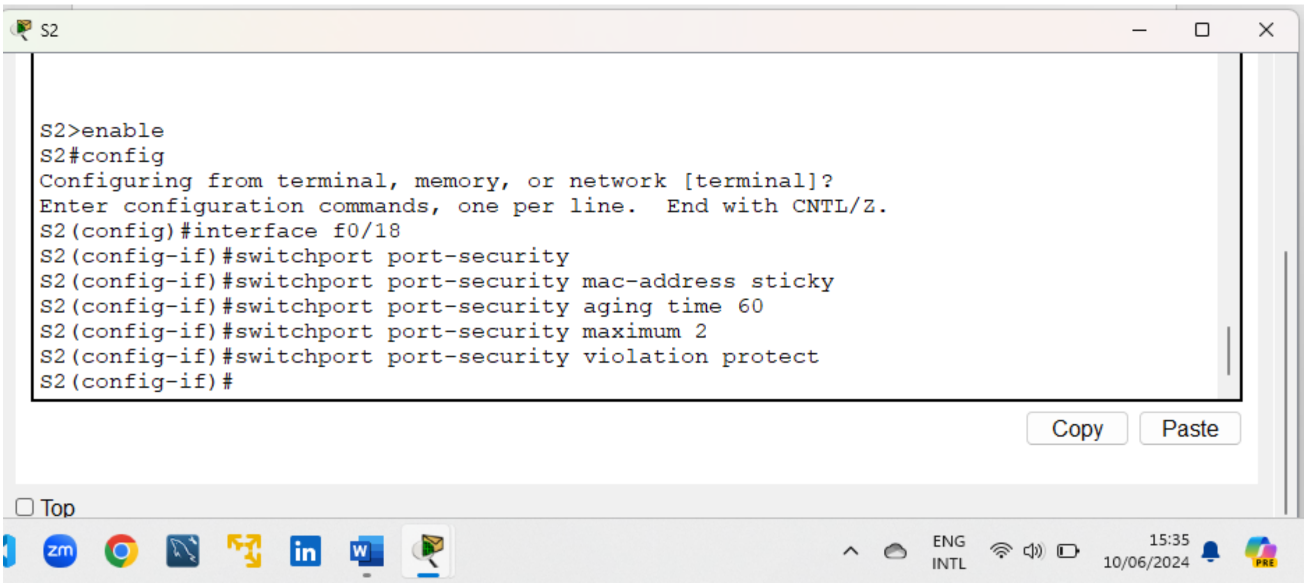


```
S1(config-if)#switchport port-security aging type inactivity
                                                     ^
% Invalid input detected at '^' marker.

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

S1#show port-security 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#
```



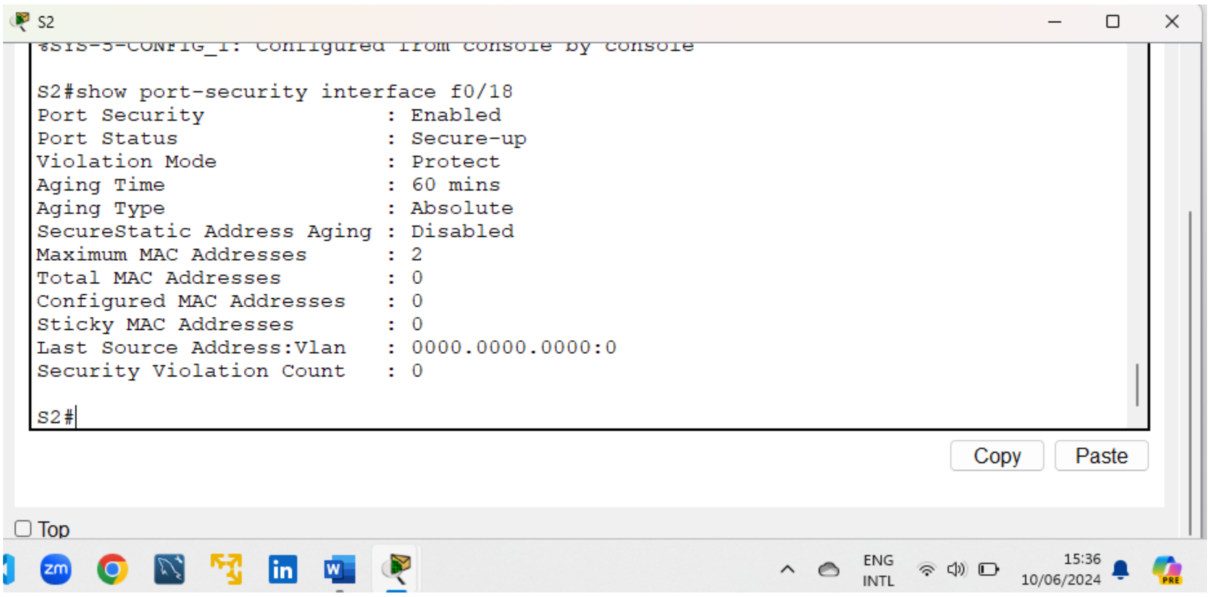
```
%SYS-5-CONFIG_I: Configured from console by console

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 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#
```

d) Enable port security for F0/18 on S2:

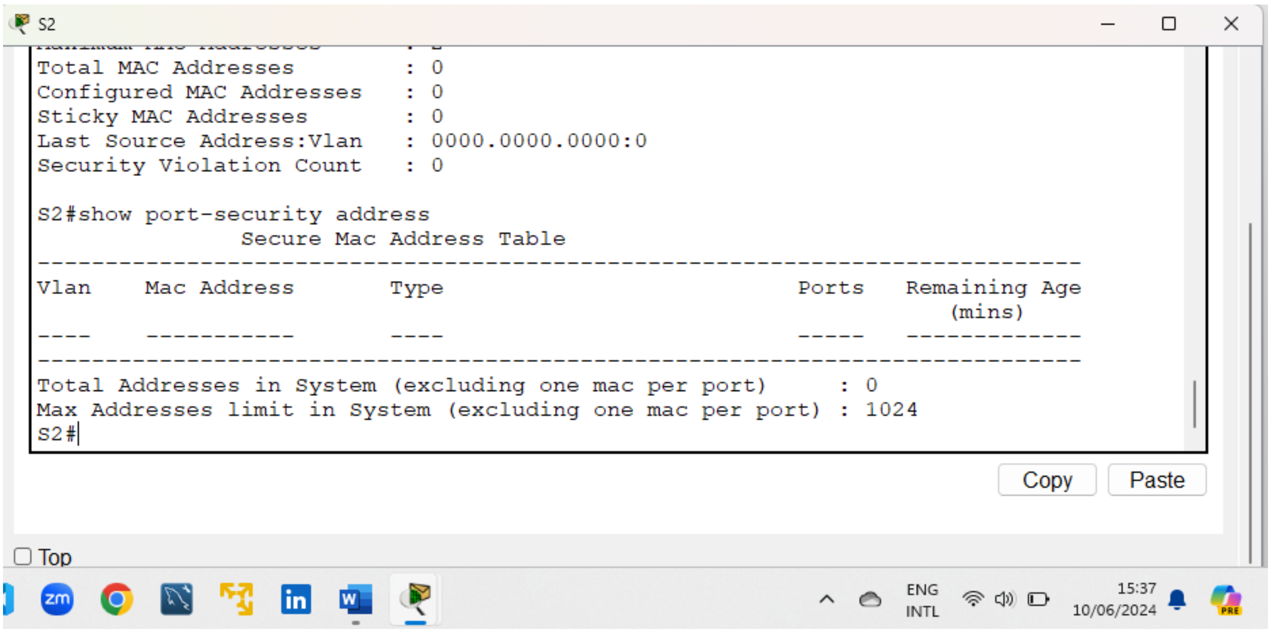


```
S2>enable
S2#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface f0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#switchport port-security aging time 60
S2(config-if)#switchport port-security maximum 2
S2(config-if)#switchport port-security violation protect
S2(config-if)#
```

e) Verifying port security on S2 F0/18:



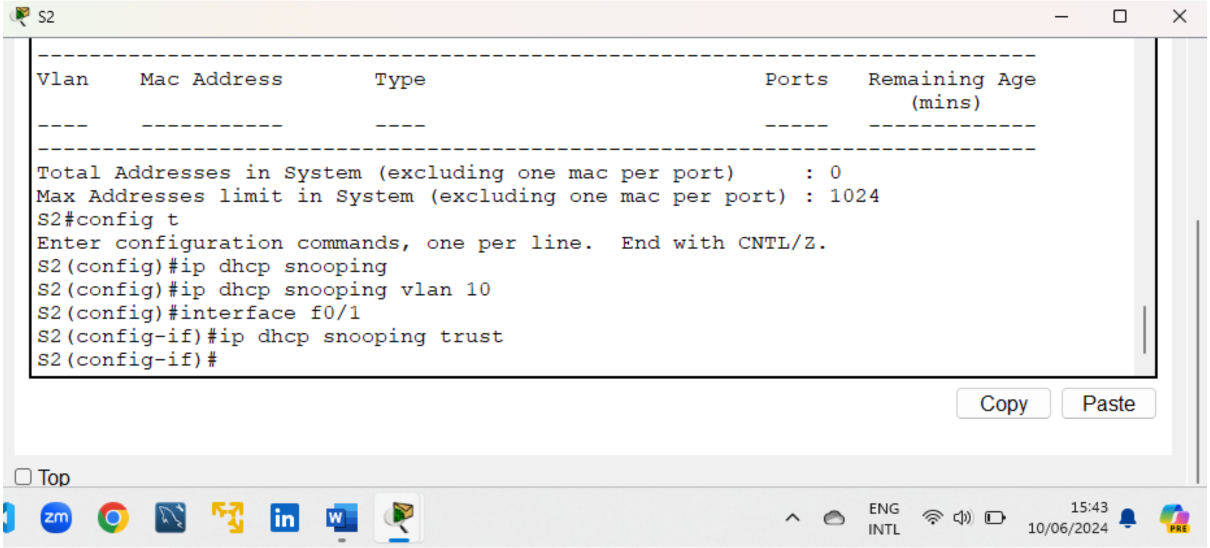
```
%SYS-5-CONFIG_I: Configured from console by console

S2#show port-security interface f0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Protect
Aging Time                 : 60 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

S2#
```



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

S2#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S2#
```

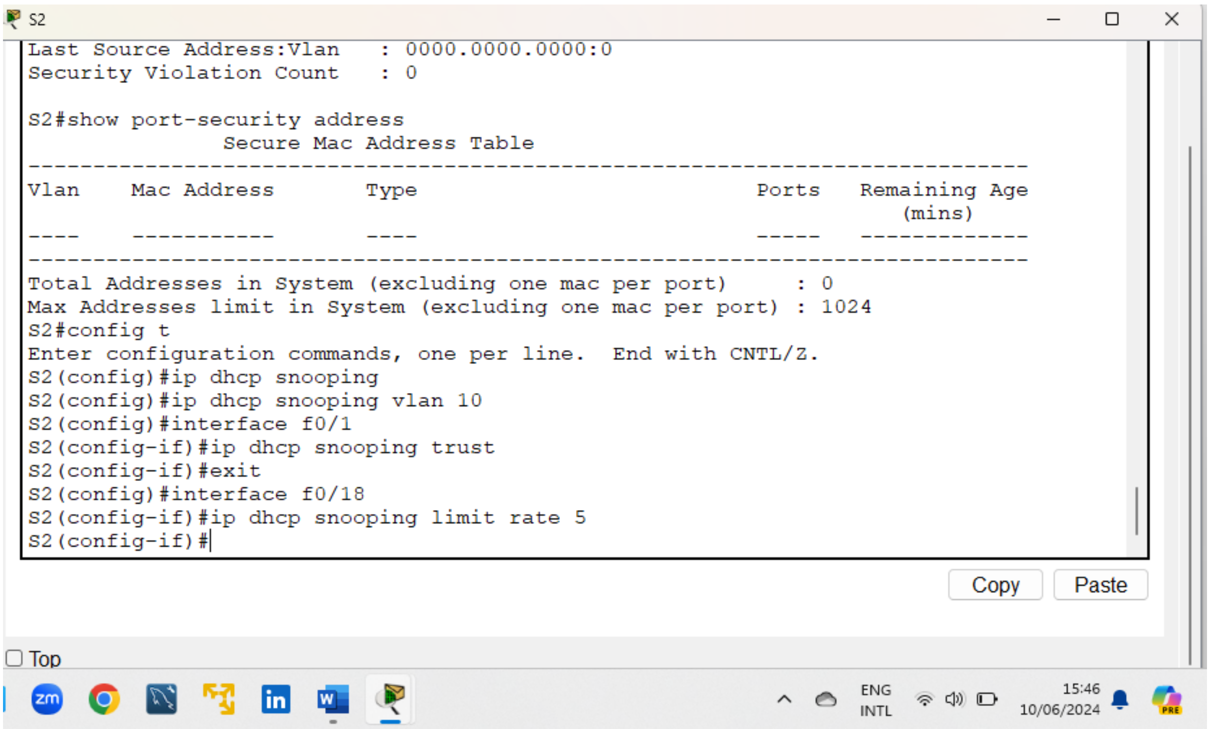
Step 5: Implementing DHCP Snooping Security

a) Enable DHCP snooping on S2 and configure it for VLAN 10: And configuration of the trunk port on s2 as a trusted port



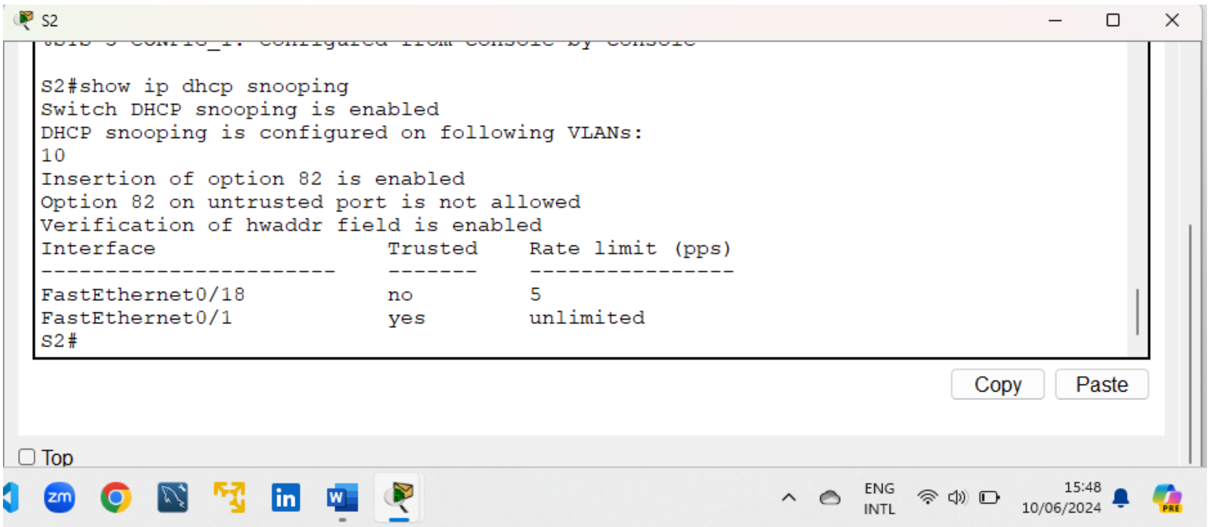
```
-------------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
-------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S2#config 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)#interface f0/1
S2(config-if)#ip dhcp snooping trust
S2(config-if)#
```

b) Limitation of untrusted port F0/18 to five DHCP packets per second:



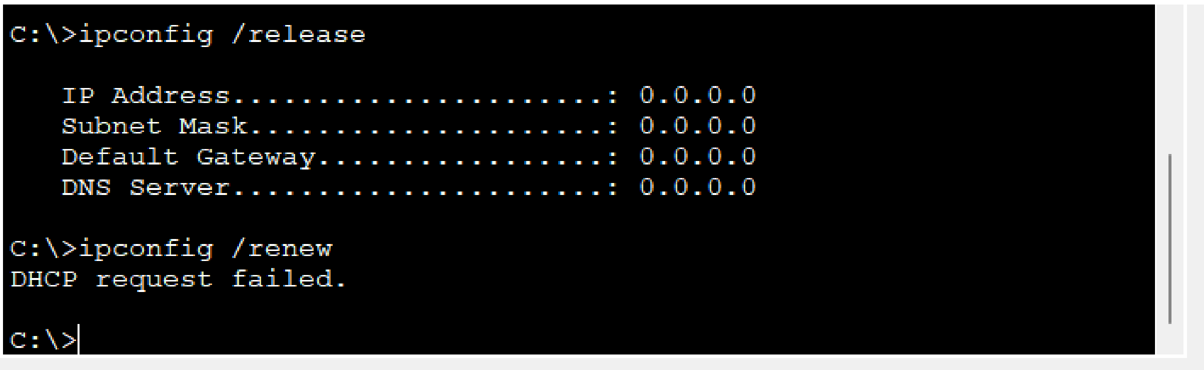
```
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

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#config 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)#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)#
```

c) **Verification of DHCP snooping configuration:**



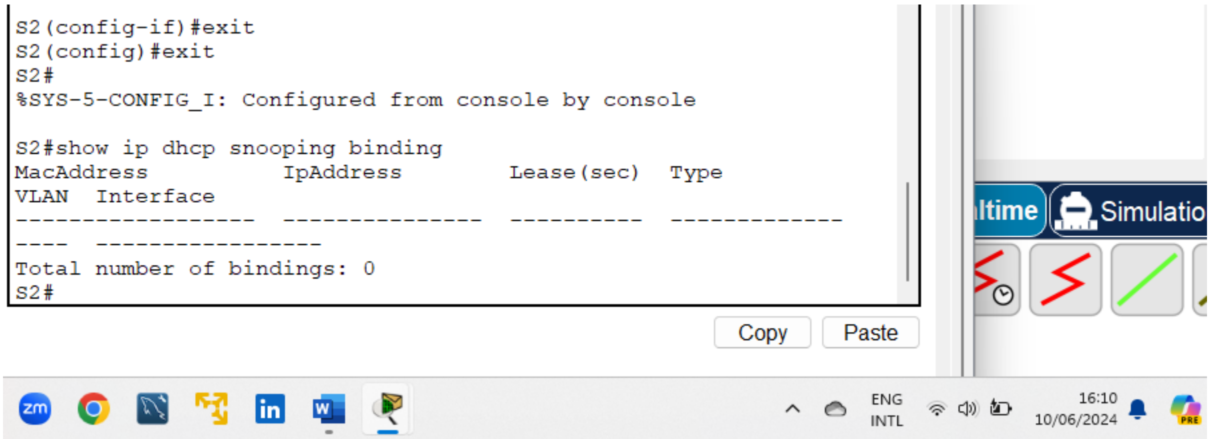
```
%SYS-5-CONFIG_I: Configured from console by console

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#
```

d) **Release and renew the IP address on PC-B:**



```
C:\>ipconfig /release

   IP Address......................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: 0.0.0.0
   DNS Server......................: 0.0.0.0

C:\>ipconfig /renew
DHCP request failed.

C:\>
```

e) **Verifying DHCP snooping bindings:**

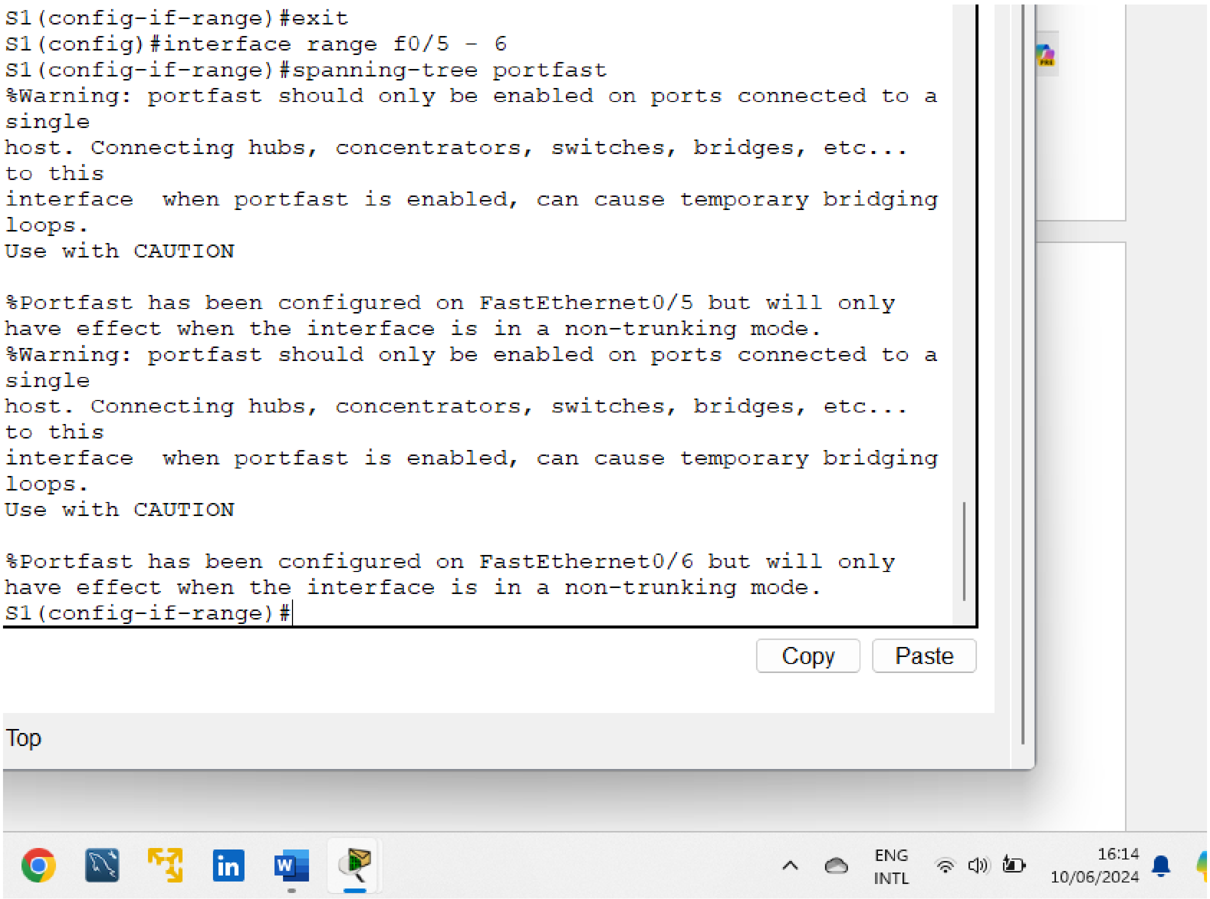


```
S2(config-if)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

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

Step 6: Implementing PortFast and BPDU Guard

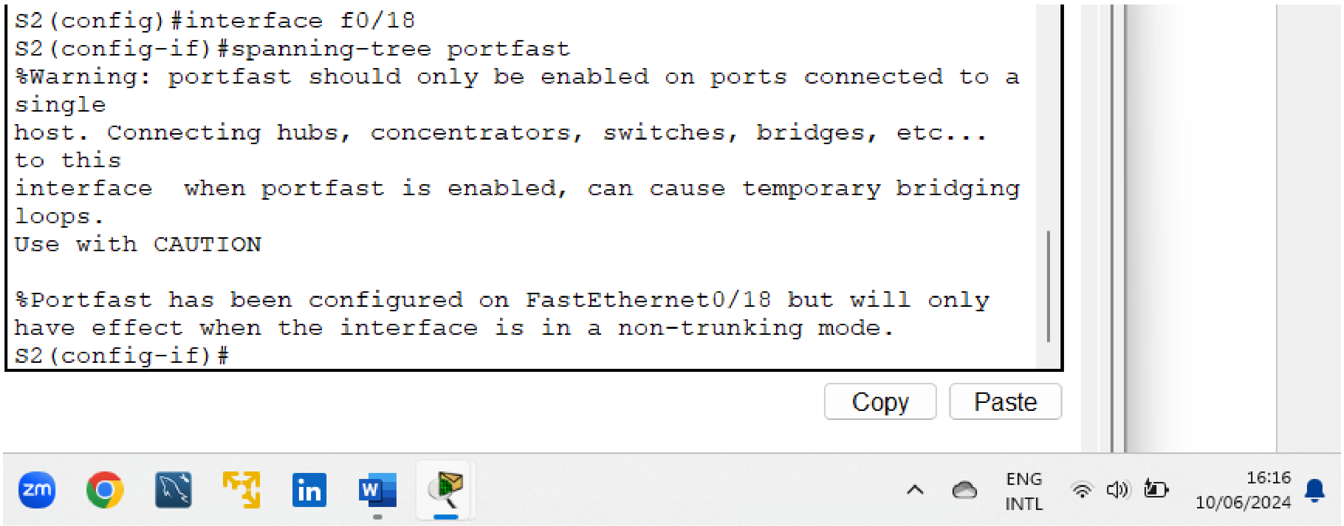
a) **Configuration PortFast on all access ports in use:**

S1



```
S1(config-if-range)#exit
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)#
```

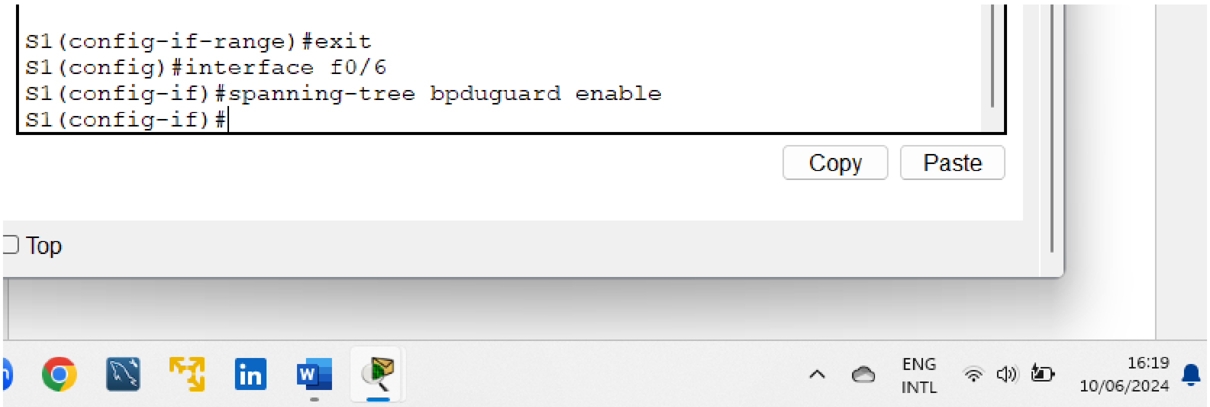
S2



```
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)#
```

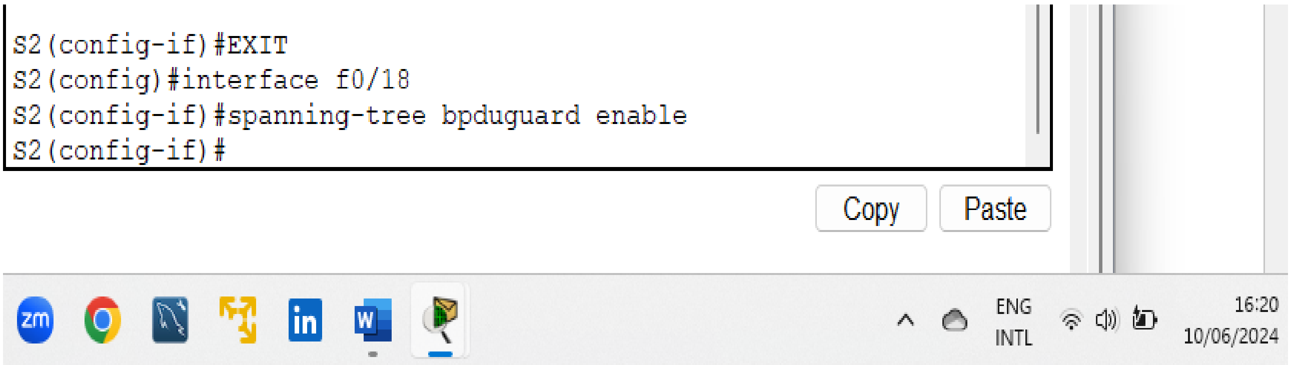
b) **Enabling BPDU guard on VLAN 10 access ports connected to PC-A and PC-B:**

S1



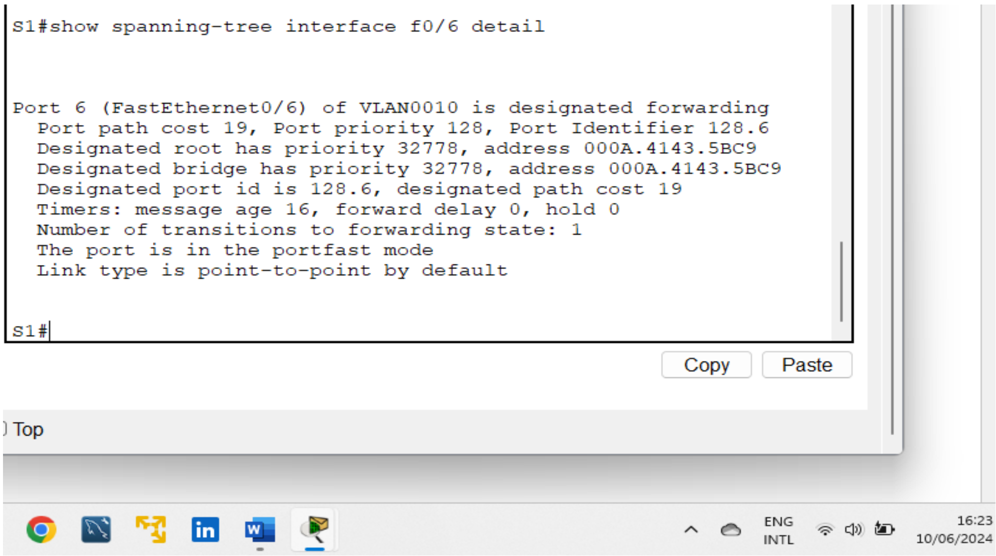
```
S1(config-if-range)#exit
S1(config)#interface f0/6
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#
```

S2



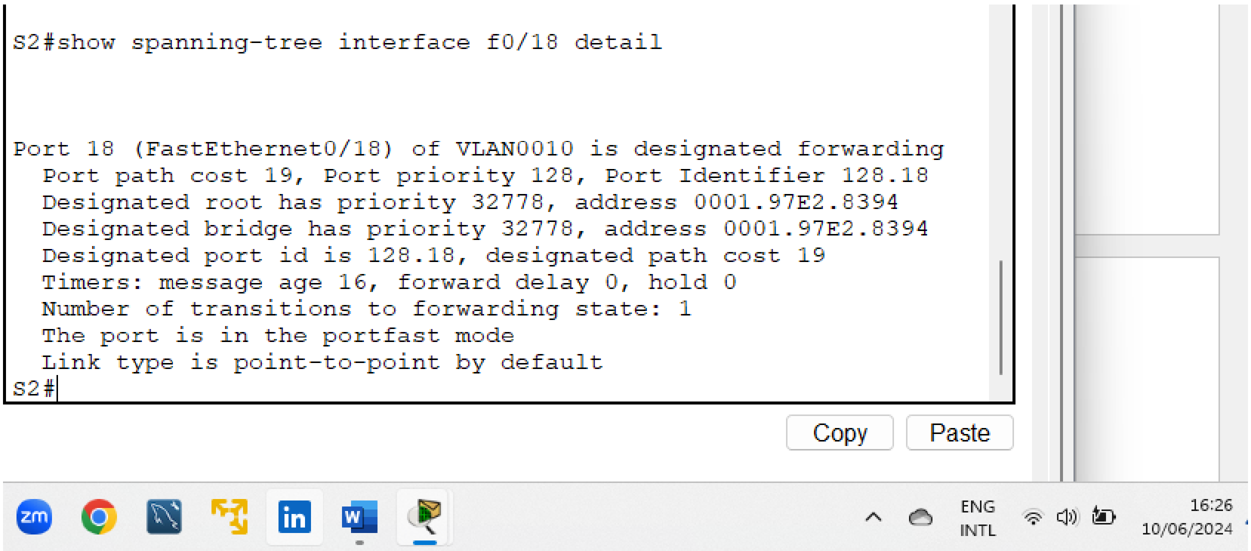
```
S2(config-if)#EXIT
S2(config)#interface f0/18
S2(config-if)#spanning-tree bpduguard enable
S2(config-if)#
```

c) **Verification BPDU guard and PortFast settings:**
S1



```
S1#show spanning-tree interface f0/6 detail


Port 6 (FastEthernet0/6) of VLAN0010 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.6
  Designated root has priority 32778, address 000A.4143.5BC9
  Designated bridge has priority 32778, address 000A.4143.5BC9
  Designated port id is 128.6, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port is in the portfast mode
  Link type is point-to-point by default


S1#
```

S2



```
S2#show spanning-tree interface f0/18 detail


Port 18 (FastEthernet0/18) of VLAN0010 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.18
  Designated root has priority 32778, address 0001.97E2.8394
  Designated bridge has priority 32778, address 0001.97E2.8394
  Designated port id is 128.18, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port is in the portfast mode
  Link type is point-to-point by default
S2#
```

This detailed guide walks through configuring switch security using Packet Tracer, ensuring network devices are secure and correctly configured.

Conclusion

Effective switch security configuration is essential to safeguard network infrastructure against a variety of potential threats. Through the implementation of VLANs, port security, DHCP snooping, and BPDU guard, network administrators can significantly enhance the security posture of their switches. This exercise has demonstrated how to configure these features using Cisco Packet Tracer, providing a practical guide for ensuring network security.

By following these steps, organizations can reduce the risk of unauthorized access, data breaches, and network disruptions, thereby maintaining a robust and secure network environment.