VLANs and Secure Switch Configuration

INTRODUCTION

This lab report presents the configuration and security setup of a small enterprise switched network. The aim was to implement VLAN segmentation, secure switchports, and enable DHCP snooping and port security features to mitigate common Layer 2 attacks. Using Cisco Packet Tracer and adhering to Cisco best practices, the network was segmented into multiple VLANs, and key security mechanisms such as port security, BPDU guard, and DHCP snooping were configured and validated

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.

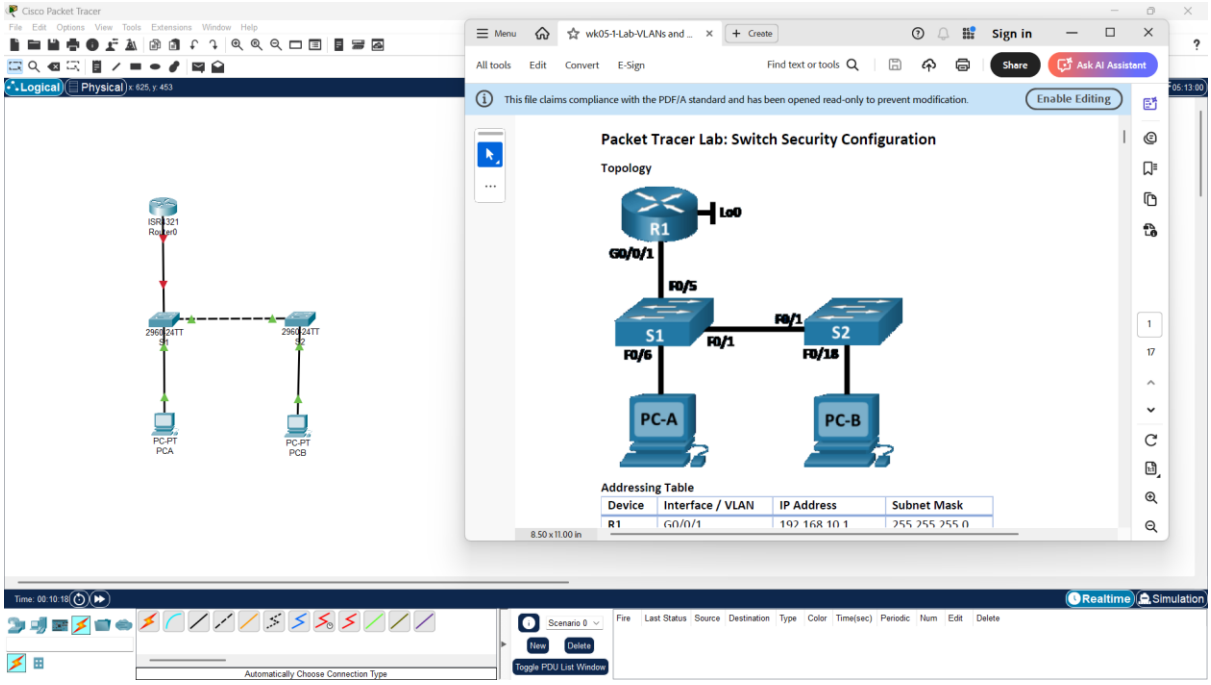
• Implement PortFast and BPDU guard.

• Verify end-to-end-connectivity.

Part 1: Configure the Network Devices.

Step1: Cabling the network.

I started by cabling the Network as indicated in the instructions:



Step2: Configuring R1

I proceeded to configuring R1 using the given commands in the following steps:

Command-by-command with explanation:

hostname R1

- **Purpose:** Sets the router's name to R1. This name will appear in the command prompt and is used to identify the device in a network.

---

no ip domain lookup

- **Purpose:** Disables DNS lookup when an unrecognized command is entered in the CLI.
- **Why:** Without this, the router will try to resolve unknown commands as hostnames, causing delays while it waits for a DNS response.

---

ip dhcp excluded-address 192.168.10.1 192.168.10.9

ip dhcp excluded-address 192.168.10.201 192.168.10.202

- **Purpose:** Prevents the DHCP server from assigning these IP addresses.
- **Why:** Reserved for static use (e.g., router interface, servers, or printers). Ensures they are not assigned dynamically.

---

ip dhcp pool Students

- **Purpose:** Creates a DHCP pool named "Students" for assigning IPs to clients.

Inside the DHCP Pool:

network 192.168.10.0 255.255.255.0

- **Purpose:** Defines the subnet from which IPs will be allocated.

default-router 192.168.10.1

- **Purpose:** Specifies the default gateway for DHCP clients (usually the router's own interface).

domain-name secure.com

- **Purpose:** Sets the domain name for the DHCP clients. This is used in DNS settings for name resolution.

---

interface Loopback0

ip address 10.10.1.1 255.255.255.0

- **Purpose:** Creates a virtual interface with the given IP.
- **Why:** Often used for testing, management, or routing protocol IDs (like OSPF Router-ID).

---

interface GigabitEthernet0/0/1

description Link to S1 Port 5

- **Purpose:** Adds a description to the interface, helping admins know what it's connected to.

ip dhcp relay information trusted

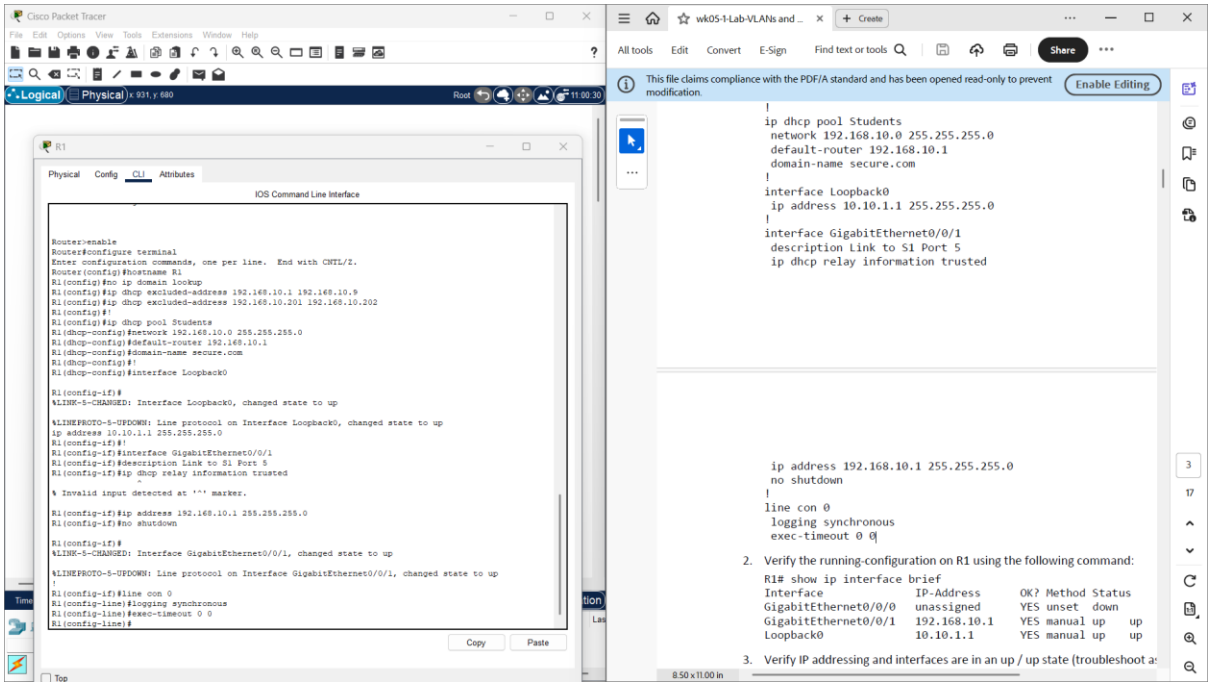
- **Purpose:** Tells the router to trust DHCP relay information from this interface.
- **Why:** Prevents DHCP snooping-related drops when relaying DHCP messages.

ip address 192.168.10.1 255.255.255.0

- **Purpose:** Assigns an IP address and subnet mask to the interface.
- **Why:** This is also the default gateway defined in the DHCP pool.

no shutdown

- **Purpose:** Enables the interface (brings it up).
- **Why:** Interfaces are administratively down by default until this is issued.



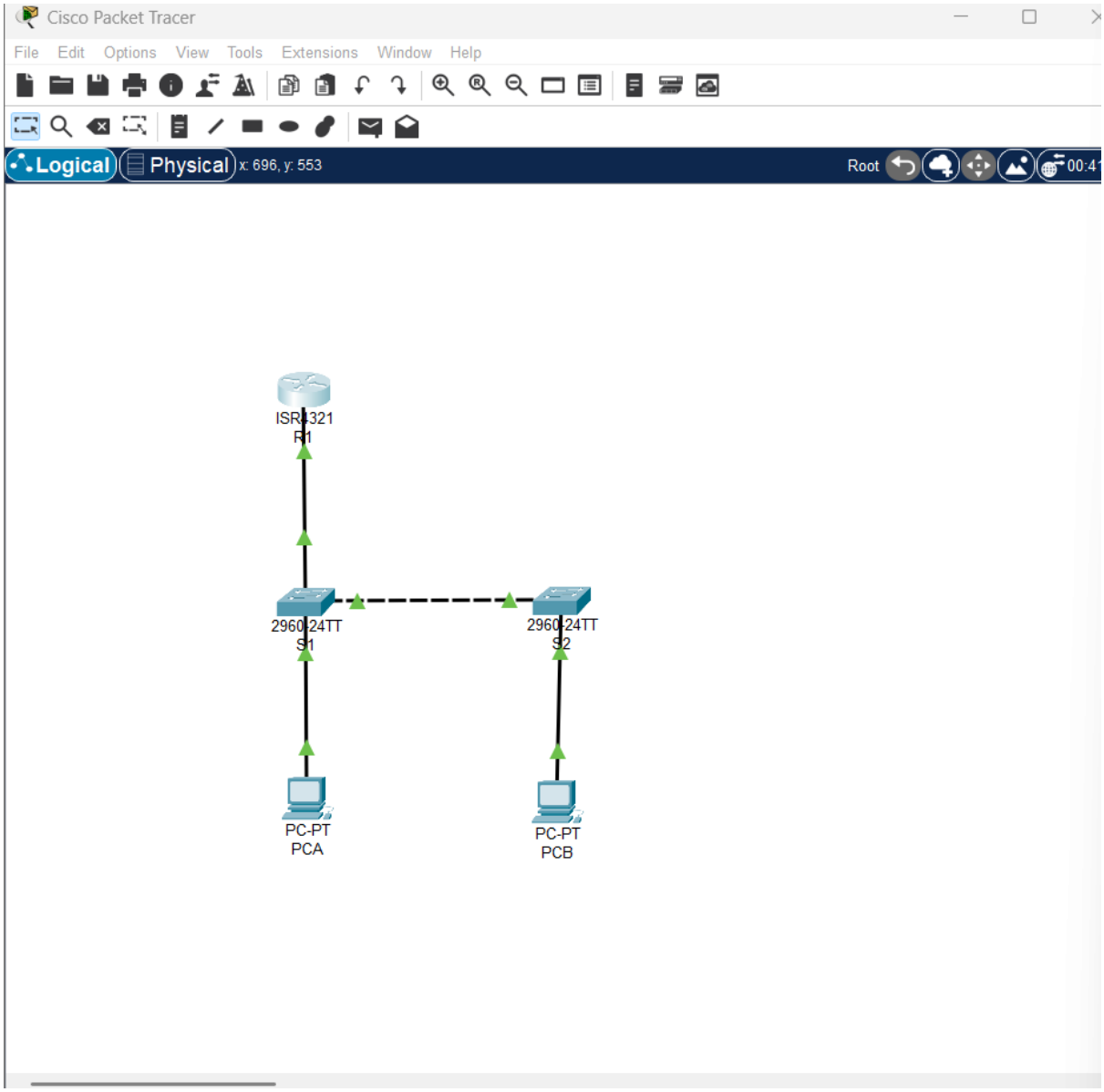
This configuration:

- Sets a recognizable hostname.
- Disables annoying DNS lookups from typos.
- Configures a DHCP server to serve clients in the 192.168.10.0/24 network.
- Excludes IPs that should not be dynamically assigned.
- Sets up a loopback for internal router use.
- Configures a gigabit interface with IP, trust settings for DHCP relay, and ensures it's operational.

To check the progress so far, I used the “show ip interface brief” command:

```
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#
```

On the topology:



Step3: Configuring and verifying basic switch settings

In this step I started by Configuring the hostname for switches S1 and S2.

I opened configuration window for S1

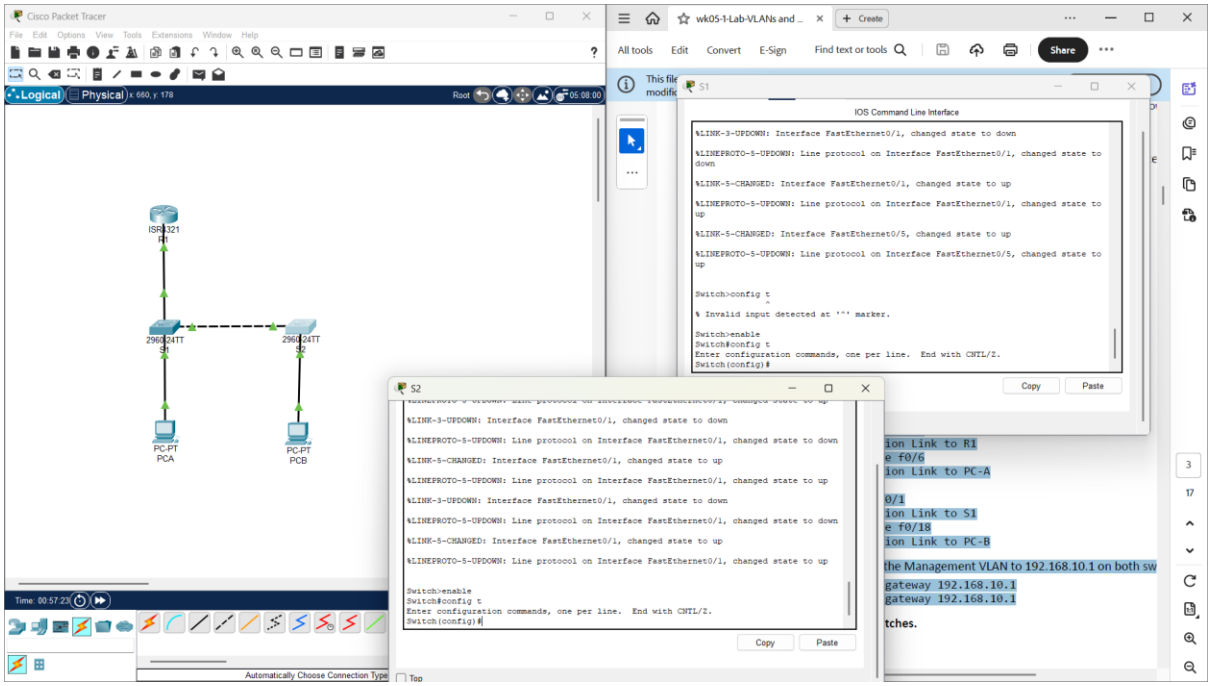
Switch# config t

Switch(config)# hostname S1

Then for S2:

Switch# config t

Switch(config)# hostname S2



I then proceeded to Prevent unwanted DNS lookups on both switches.

S1(config)# no ip domain-lookup

S2(config)# no ip domain-lookup

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

For S1:

S1(config)# interface f0/1

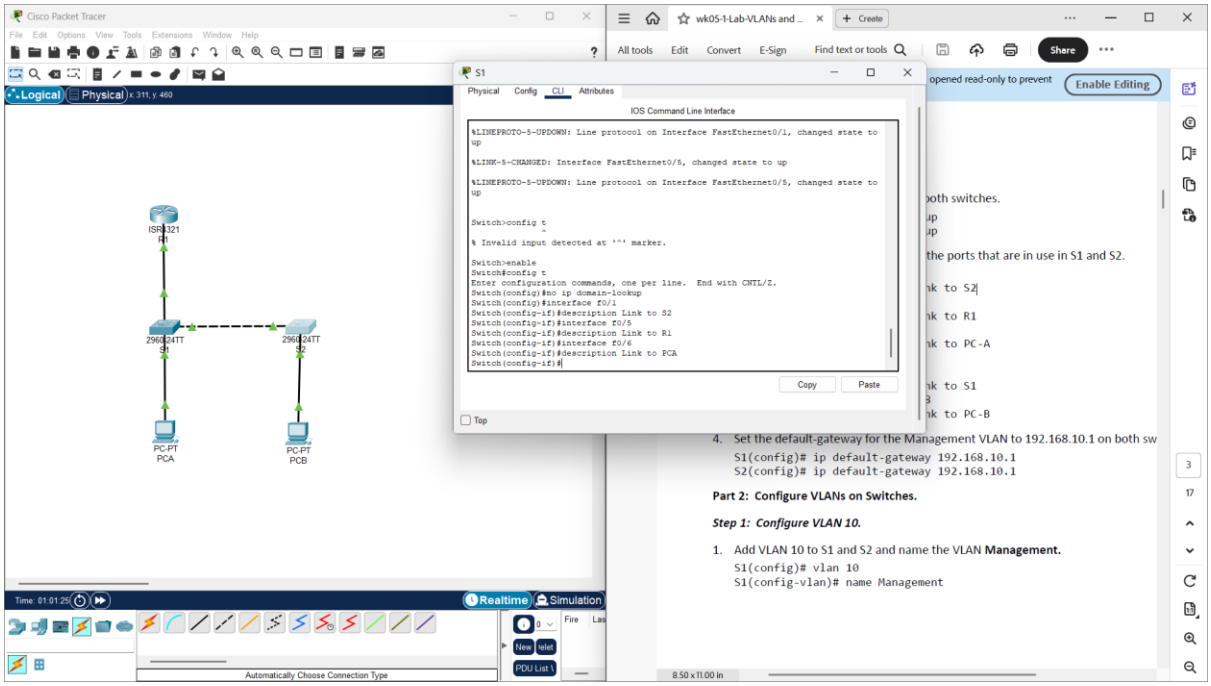
S1(config-if)# description Link to S2

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



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

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

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

```
S1(config)# ip default-gateway 192.168.10.1
S2(config)# ip default-gateway 192.168.10.1
```

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(config)# vlan 10
S1(config-vlan)# name Management
```

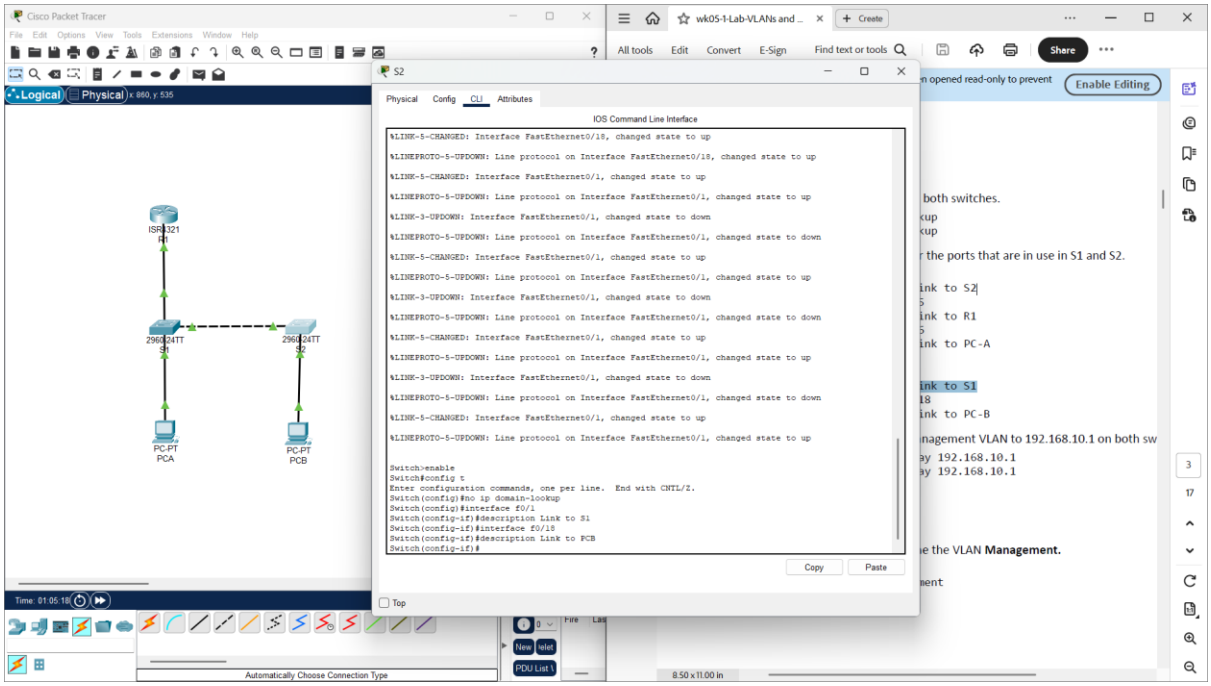
For S2:

S2(config)# interface f0/1

S2(config-if)# description Link to S1

S2(config–if)# interface f0/18

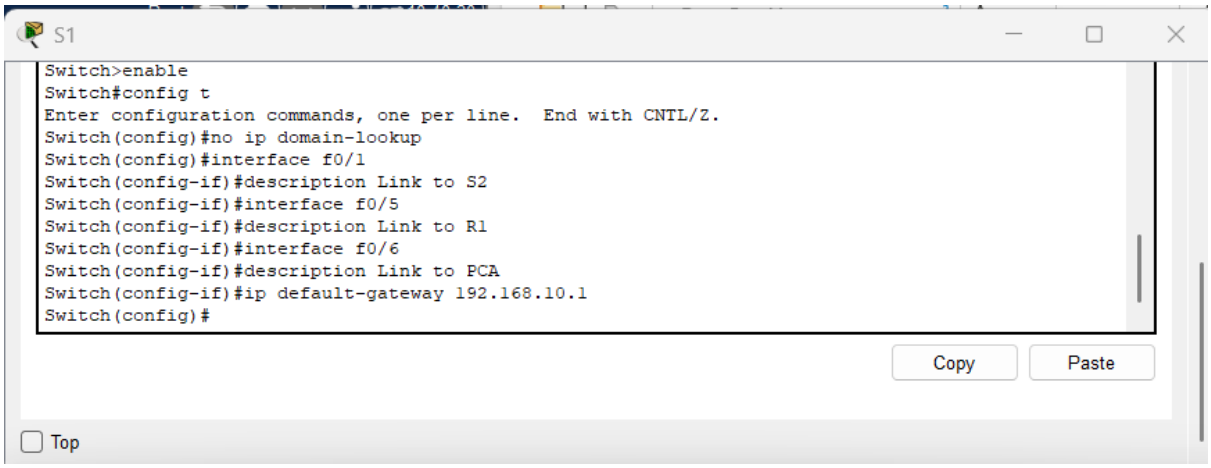
S2(config-if)# description Link to PC-B



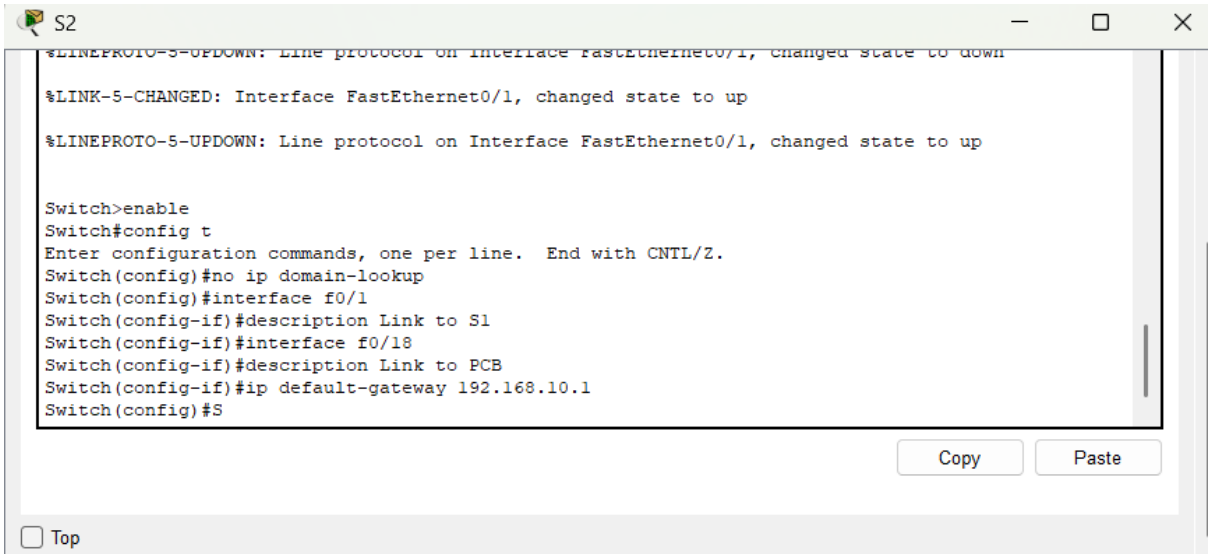
```
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, 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-3-UPDOWN: Interface FastEthernet0/1, changed state to down

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

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

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

%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

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

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

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

%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down

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

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

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


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

Once done I 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



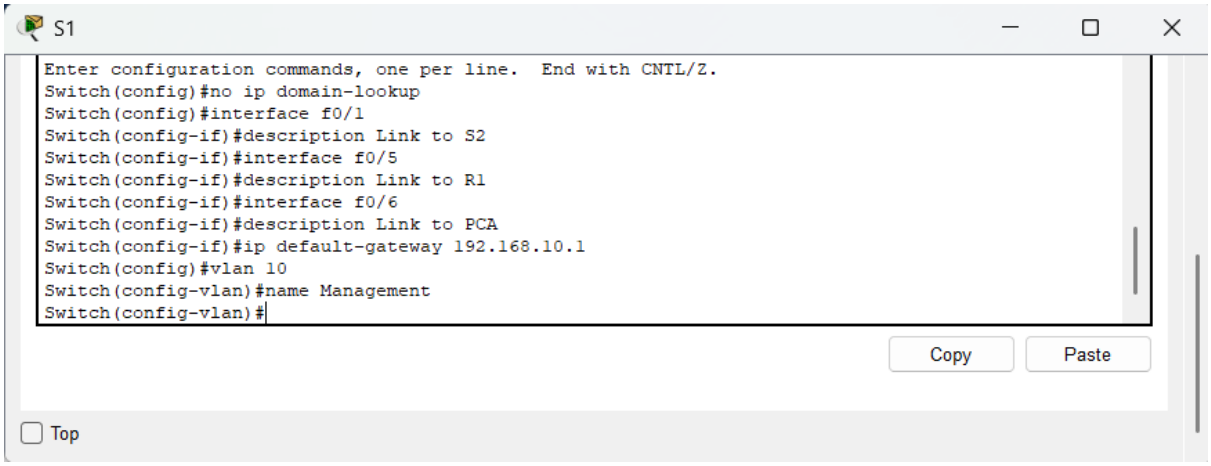
Part 2: Configure VLANs on Switches.

Step1: Configuring VLAN 10

On this step I added VLAN 10 to S1 and S2 and named the VLAN **Management.**

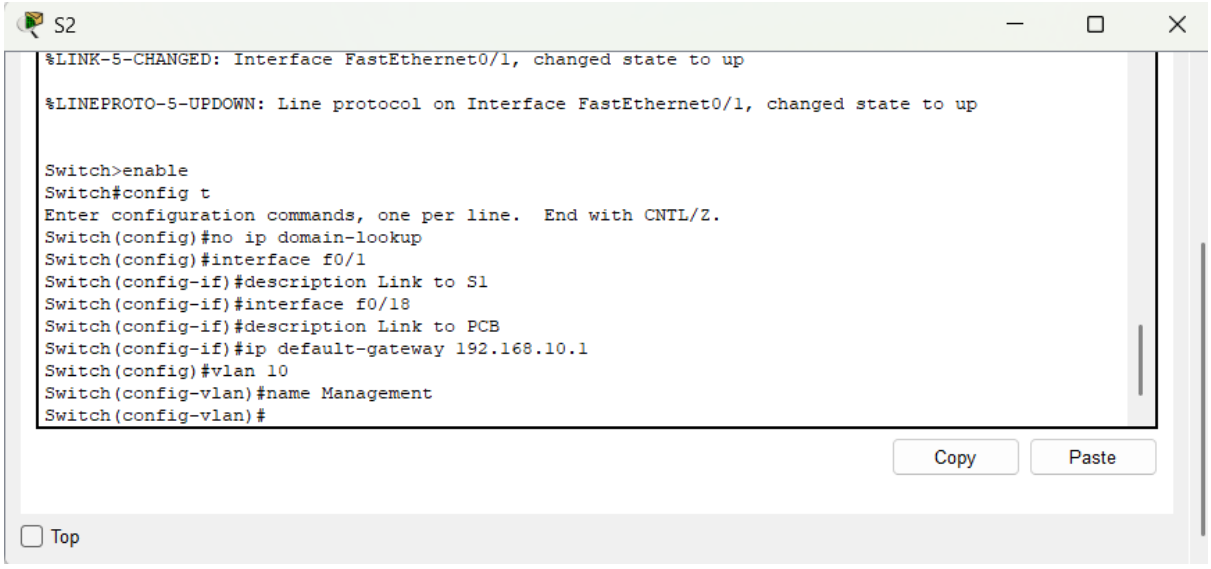
S1(config)# vlan 10

S1(config-vlan)# name Management



S2(config)# vlan 10

S2(config-vlan)# name Management



Step2: Configuring the SVI for VLAN 10.

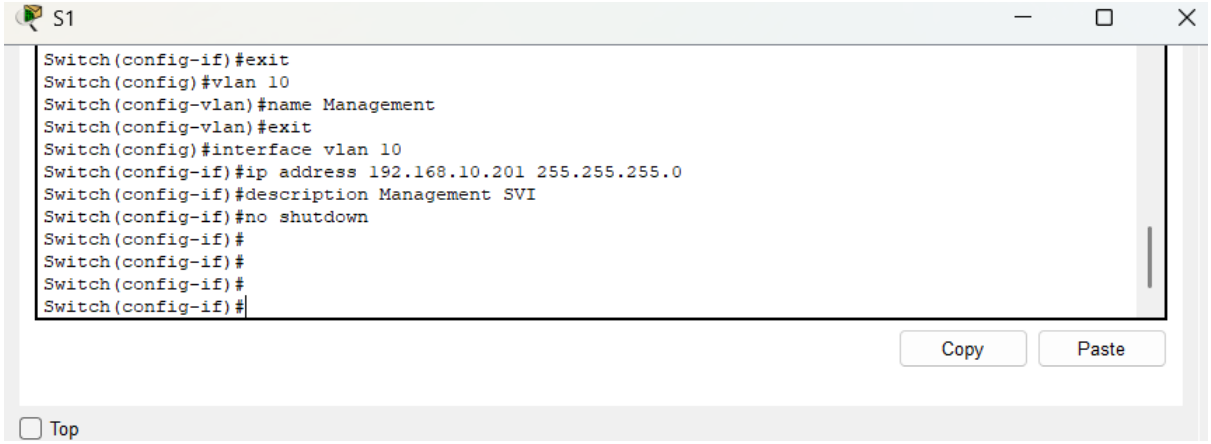
In this step my major task was to configure the IP address according to the Addressing Table for SVI for VLAN 10 on S1 and S2. Then to enable the SVI interfaces and provide a description for the interface.

S1(config)# 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

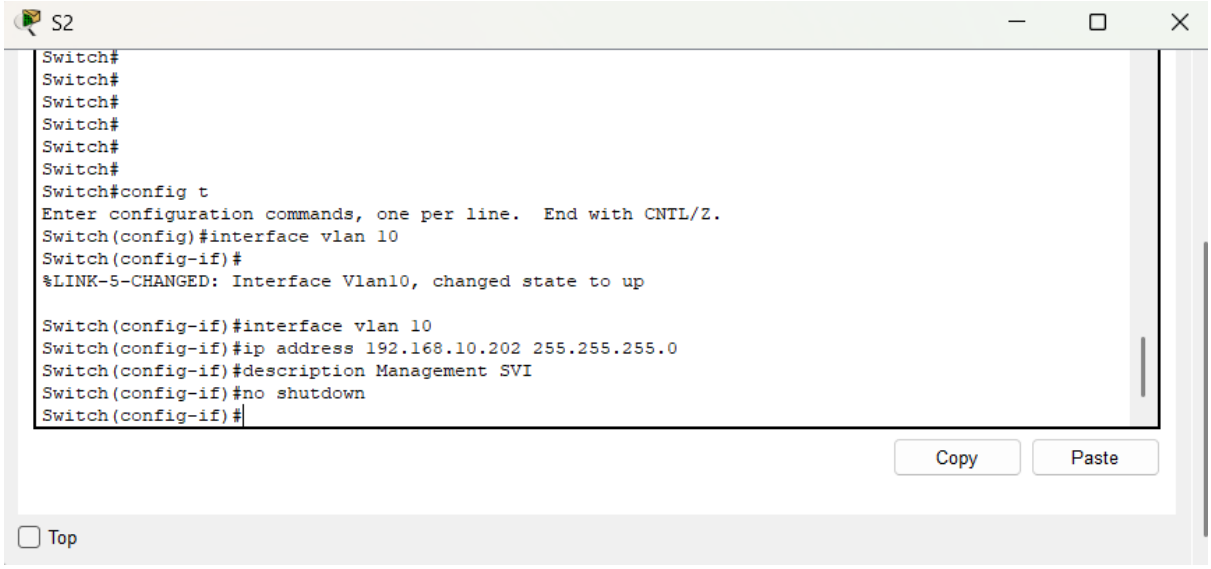


S2(config)# interface vlan 10

S2(config-if)# ip address 192.168.10.202 255.255.255.0

2S1(config-if)# description Management SVI

S2(config-if)# no shutdown



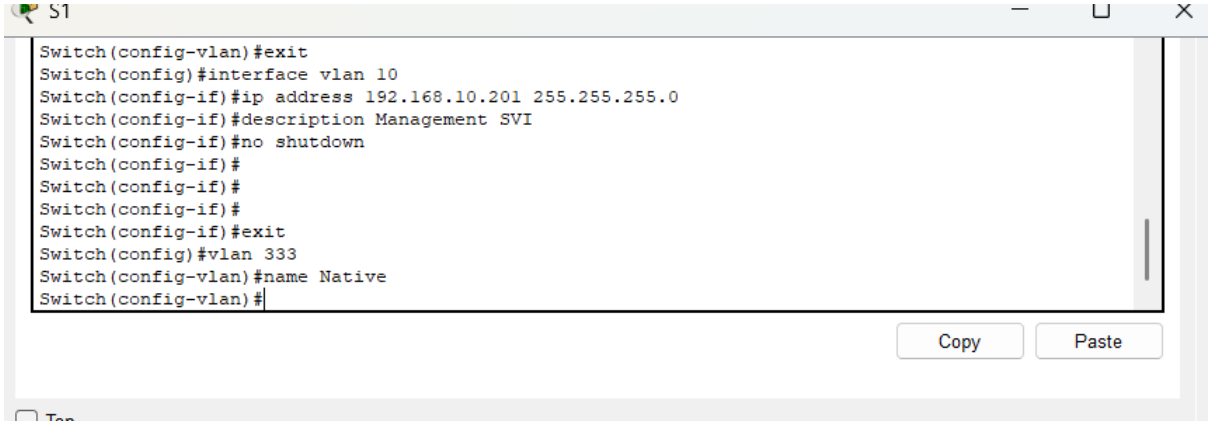
Step3: Configuring VLAN 333 with the name Native on S1 and S2.

In this step I configured VLAN 333 and gave it the Name Native, with the following steps:

Entring S1 CLI console and typing the commands:

S1(config)# vlan 333

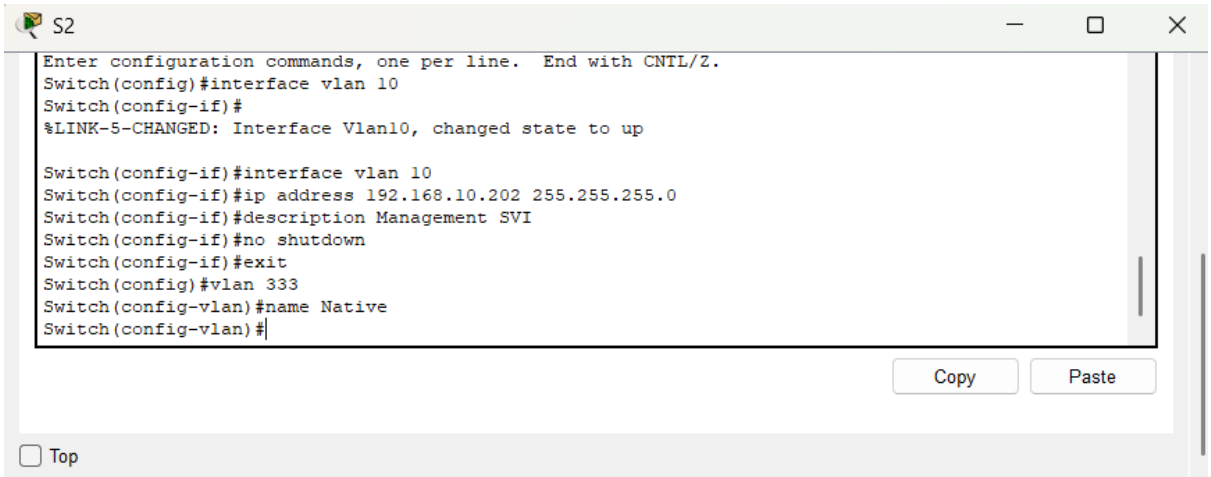
S1(config-vlan)# name Native



Entering the S2 CLI Console and typing the commnds:

S2(config)# vlan 333

S2(config-vlan)# name Native

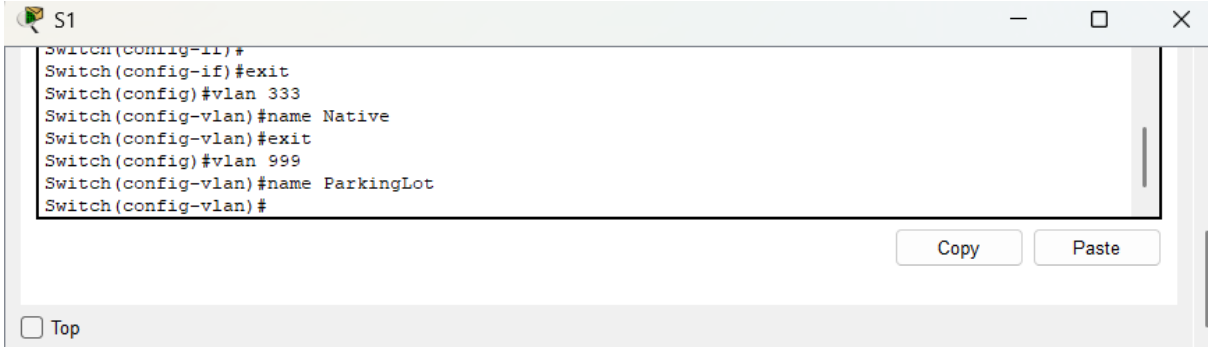


Step4: Configuring VLAN 999 with the name ParkingLot on S1 and S2.

In this step I Configured VLAN 999 with the name ParkingLot on S1 and S2:

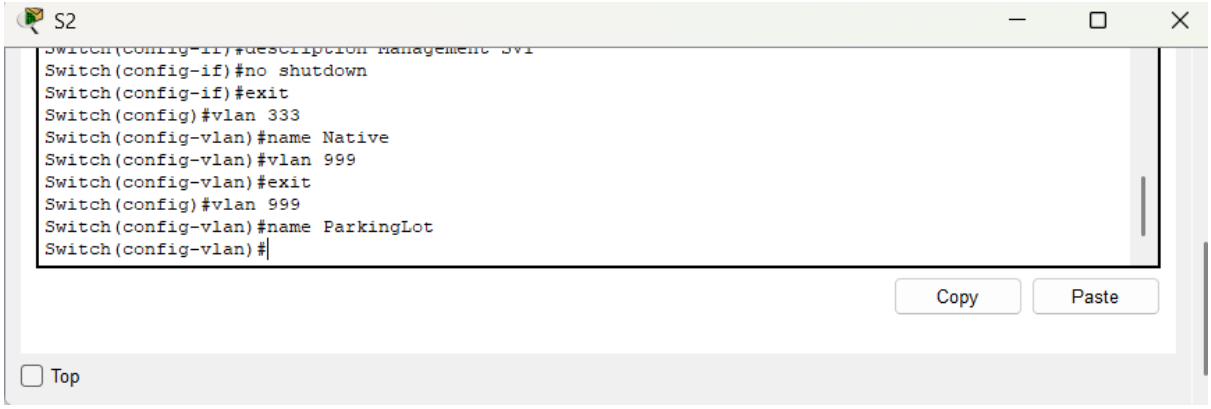
S1(config-vlan)# vlan 999

S1(config-vlan)# name ParkingLot



S2(config-vlan)# vlan 999

S2(config-vlan)# name ParkingLot



Part 3: Configure Switch Security.

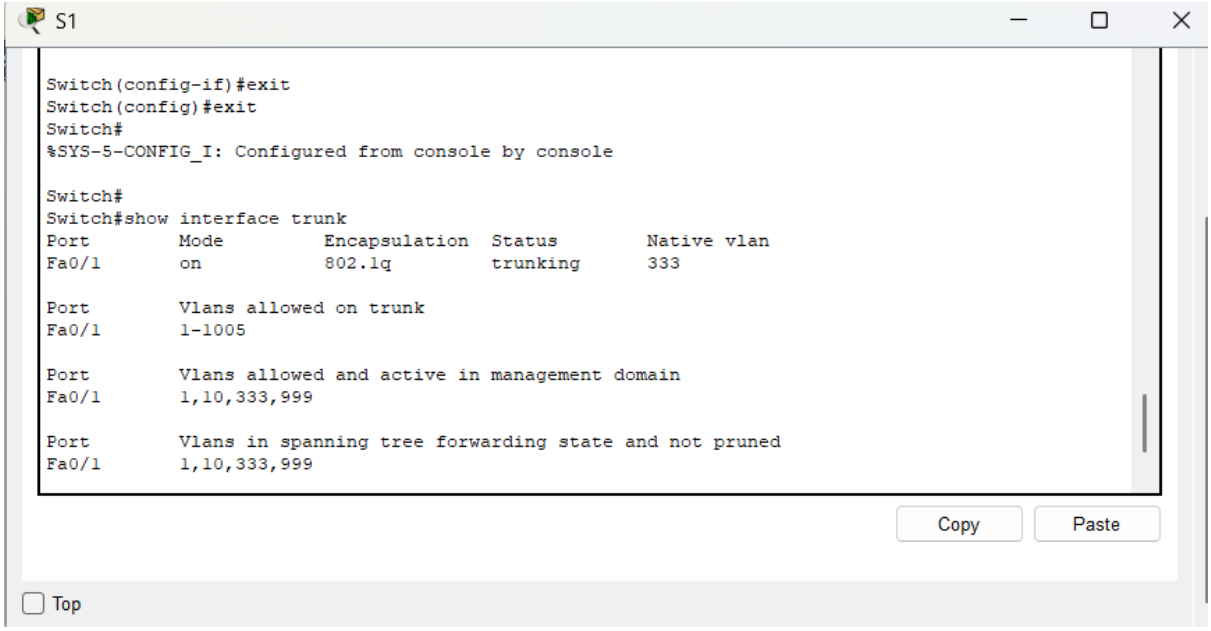
Step1: Implement 802.1Q trunking.

On both switches, I configured trunking on F0/1 to use VLAN 333 as the native VLAN and verified the configuration using “show interface trunk” command.

S1(config)# interface f0/1

S1(config-if)# switchport mode trunk

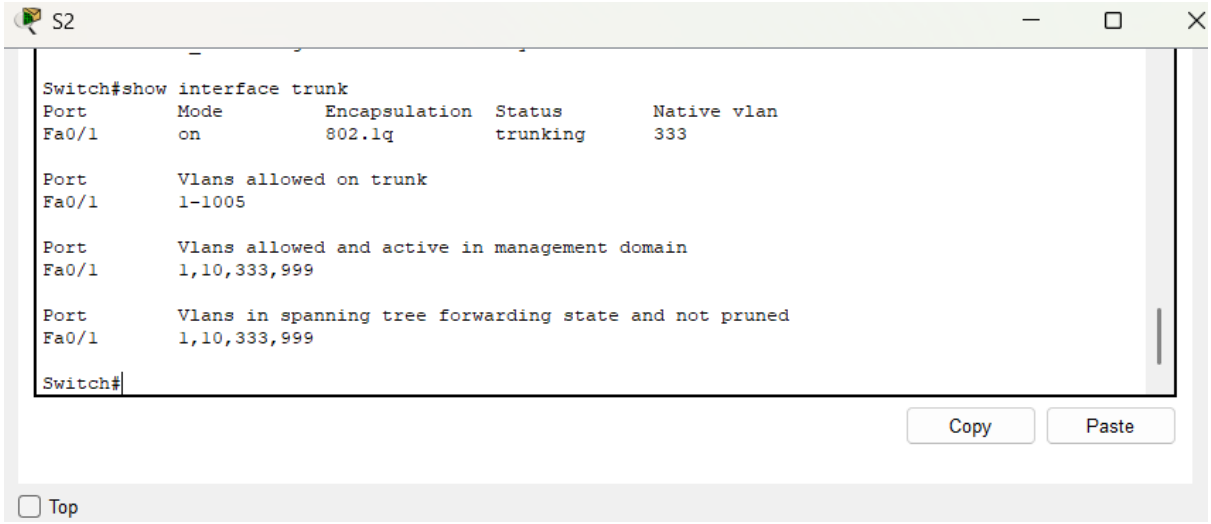
S1(config-if)# switchport trunk native vlan 333



S2(config)# interface f0/1

S2(config-if)# switchport mode trunk

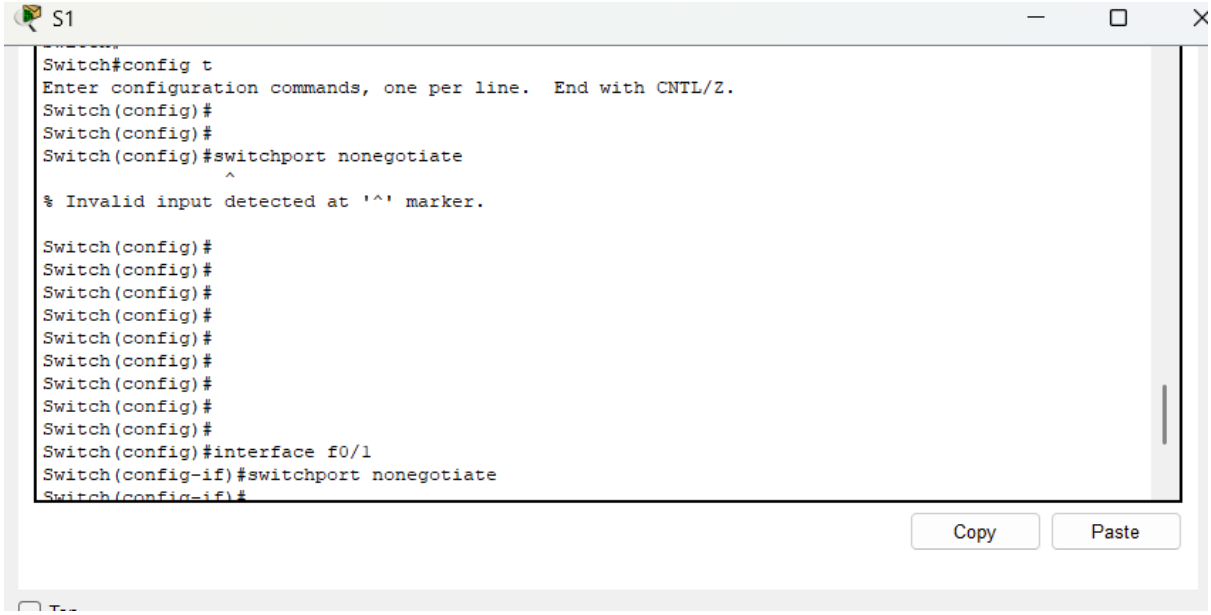
S2(config-if)# switchport trunk native vlan 333



Next step was to disable DTP negotiation on F0/1 on S1 and S2.

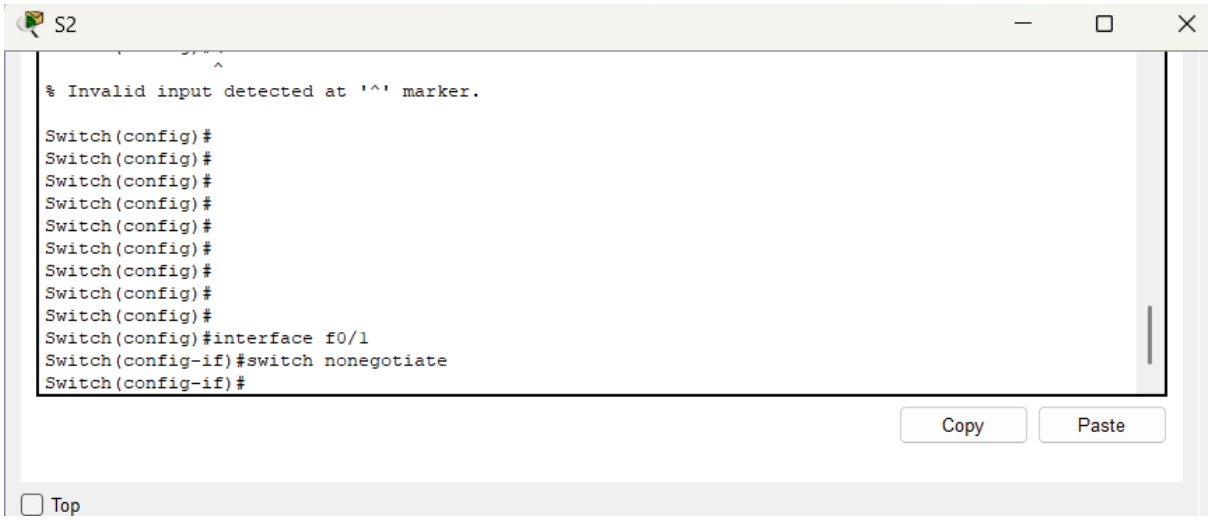
S1(config)# interface f0/1

S1(config-if)# switchport nonegotiate



S2(config)# interface f0/1

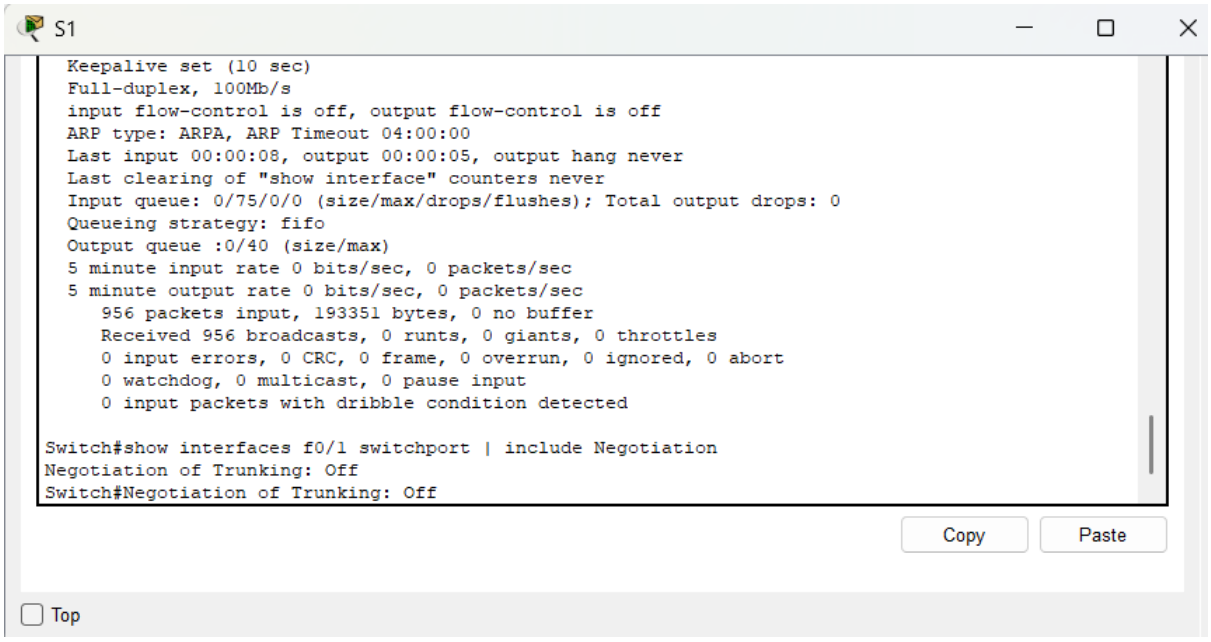
S2(config-if)# switchport nonegotiate



4. Verify with the **show interfaces** command.

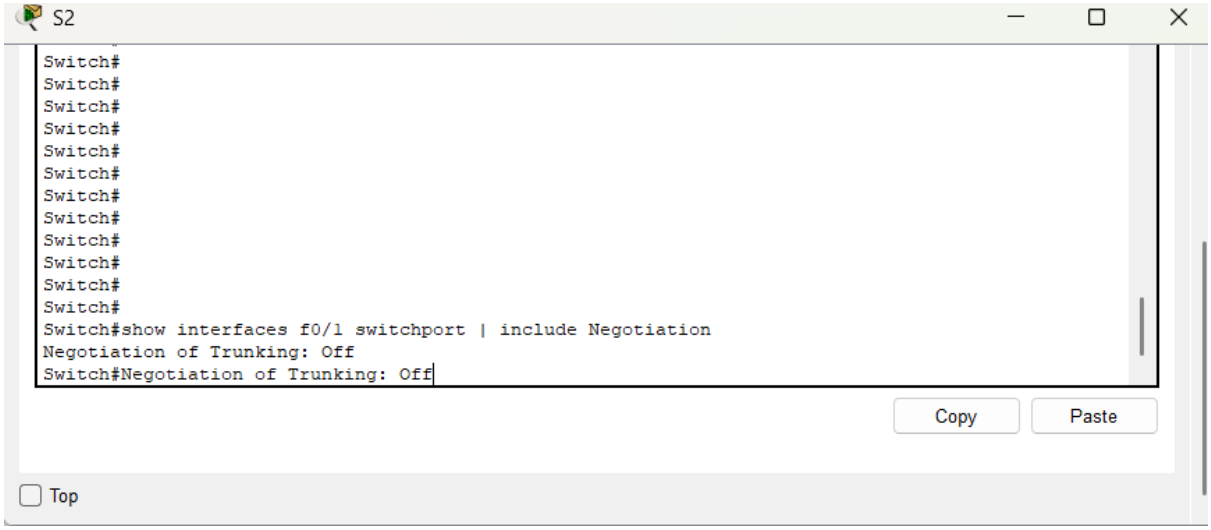
S1# show interfaces f0/1 switchport | include Negotiation

Negotiation of Trunking: Off



S2# show interfaces f0/1 switchport | include Negotiation

Negotiation of Trunking: Off



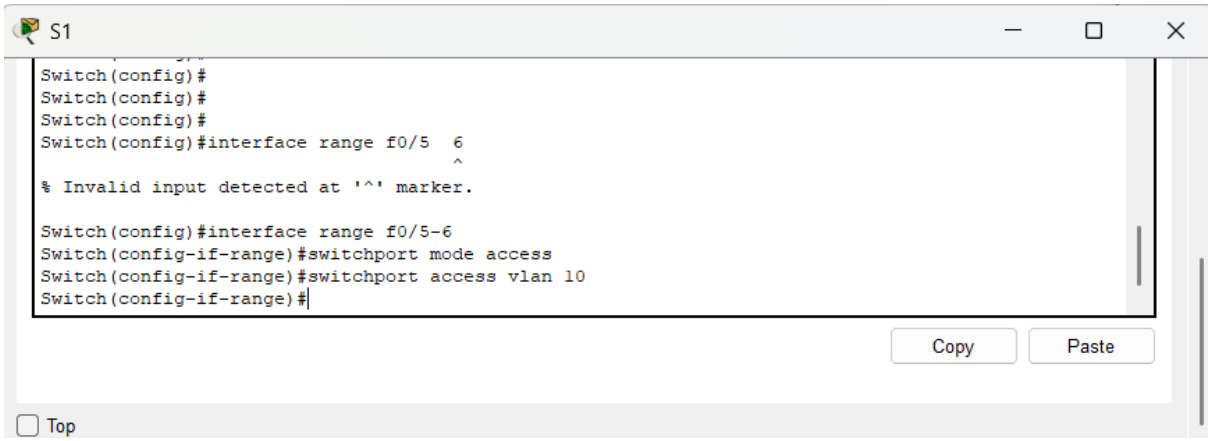
Step2: Configure access ports.

On S1, I configured F0/5 and F0/6 as access ports that are associated with VLAN 10.

S1(config)# interface range f0/5 – 6

S1(config-if)# switchport mode access

S1(config-if)# switchport access vlan 10

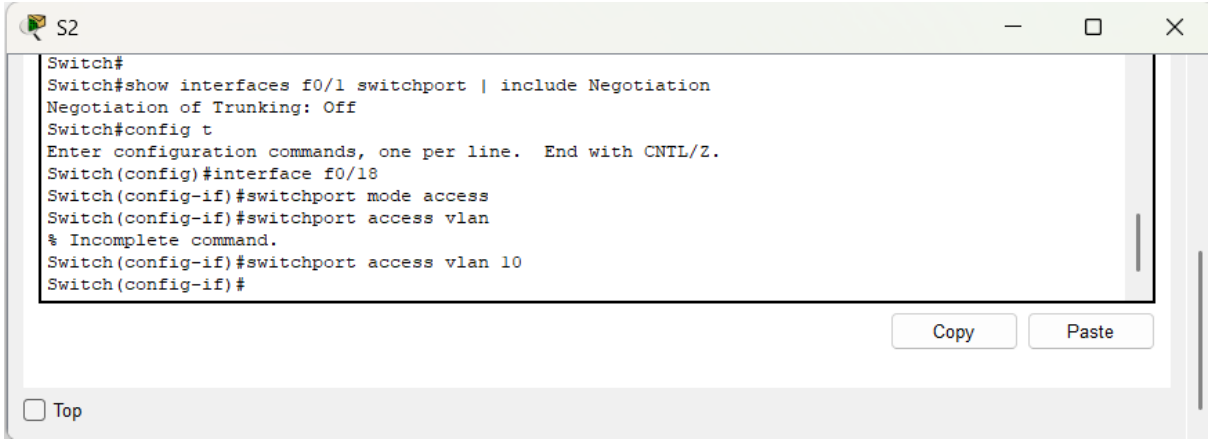


On S2, I configured F0/18 as an access port that is associated with VLAN 10.

S2(config)# interface f0/18

S2(config-if)# switchport mode access

S2(config-if)# switchport access vlan 10



Step3: Secure and disable unused switchports.

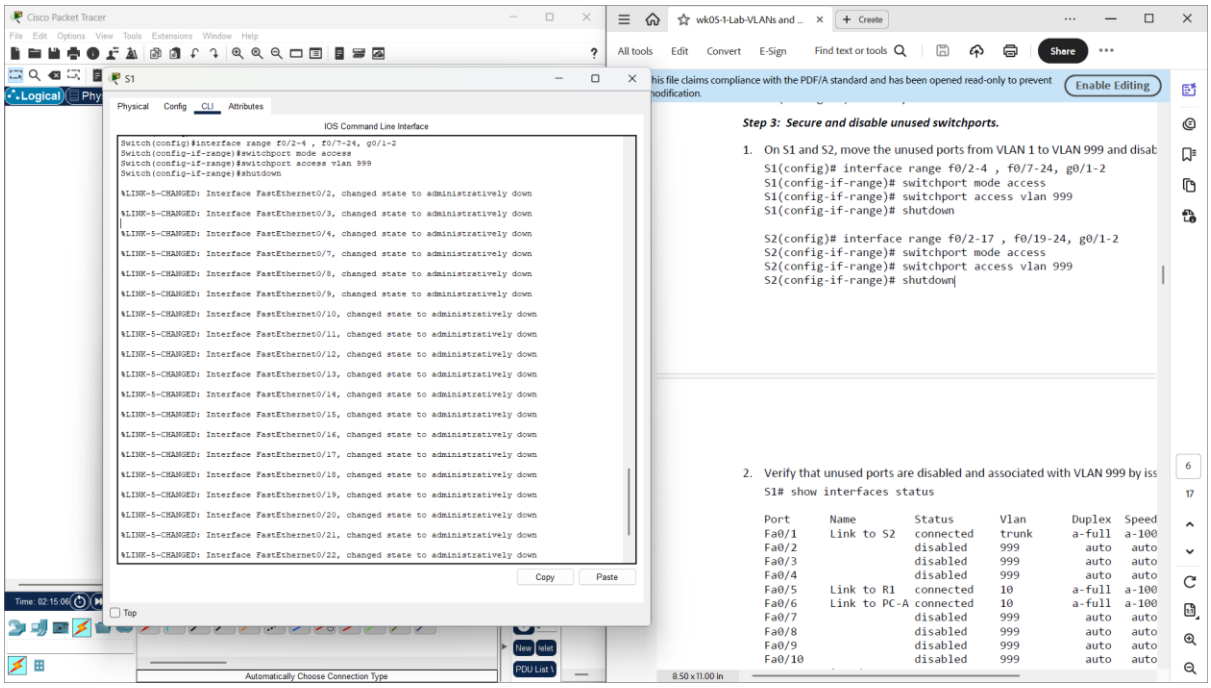
On S1 and S2, I moved the unused ports from VLAN 1 to VLAN 999 and disabled the unused ports.

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

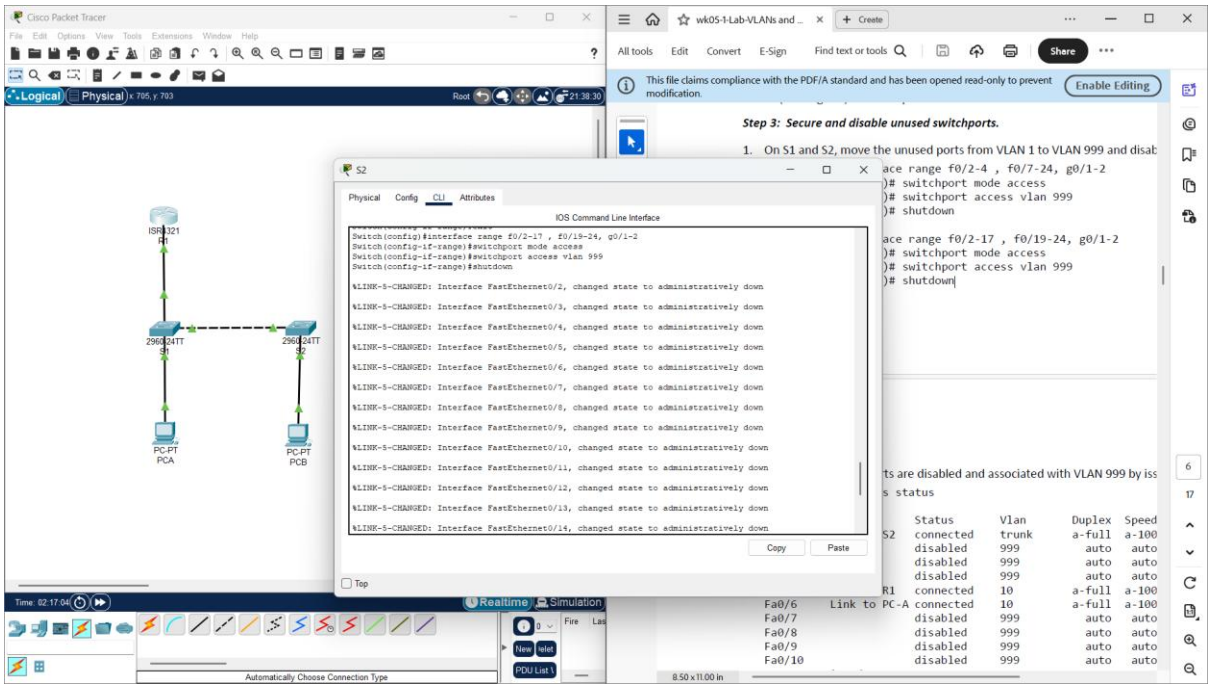


S2(config)# interface range f0/2-17 , f0/19-24, g0/1-2

S2(config-if-range)# switchport mode access

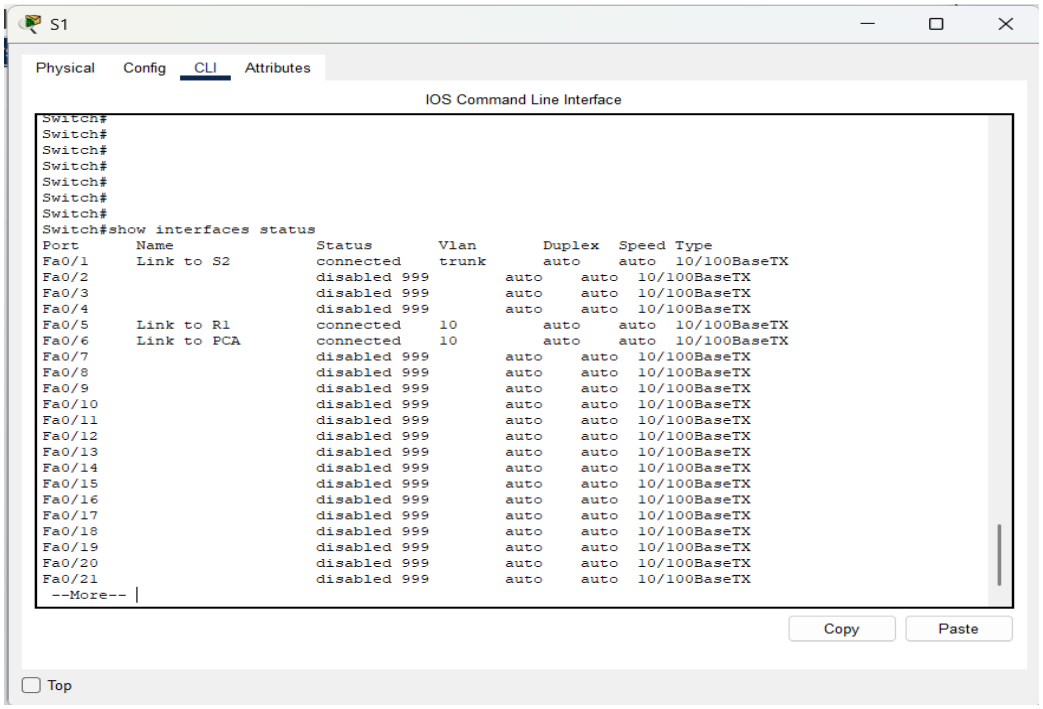
S2(config-if-range)# switchport access vlan 999

S2(config-if-range)# shutdown

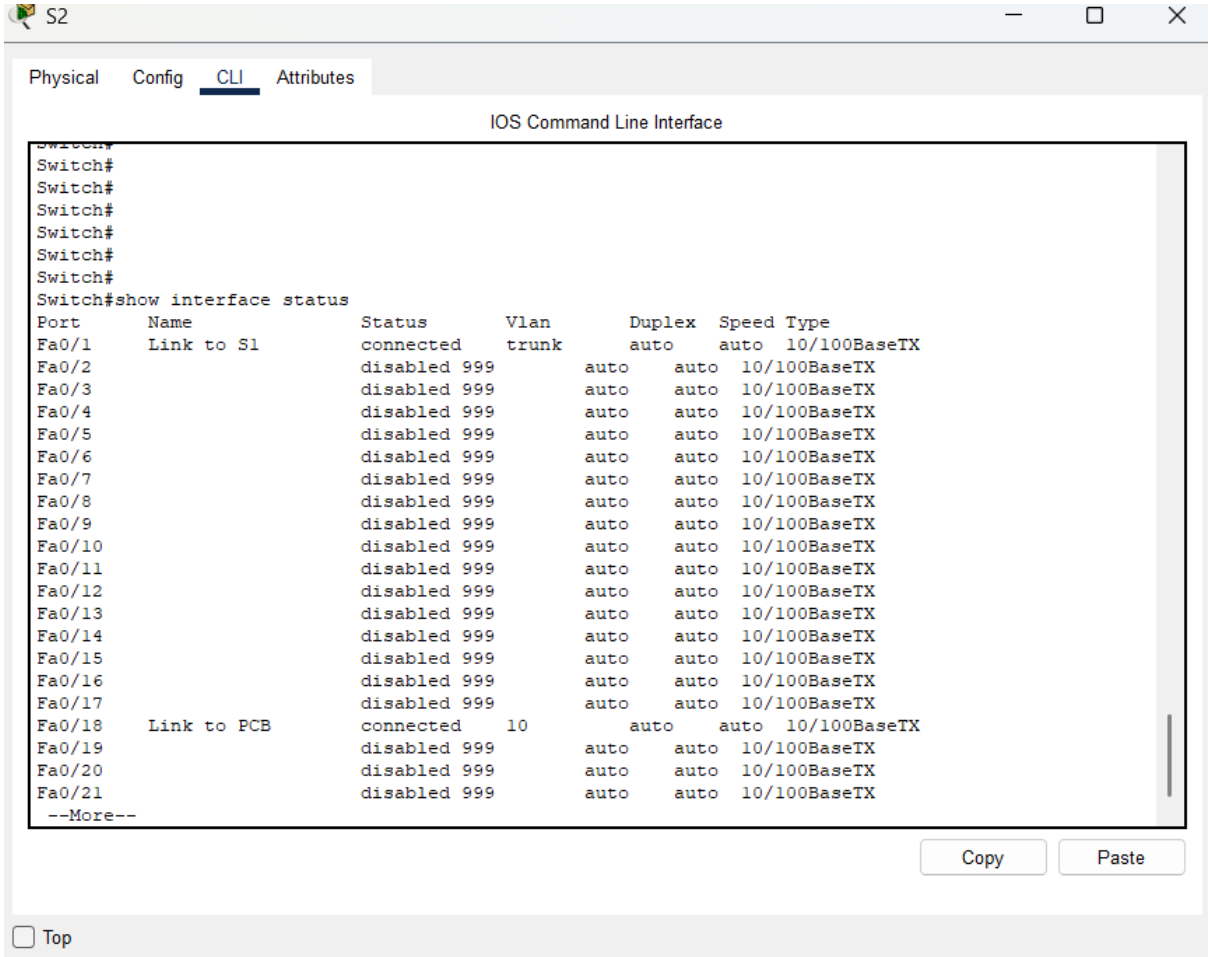


Verify that unused ports are disabled and associated with VLAN 999 by issuing the **show** command.

S1# show interfaces status



S2# show interfaces status

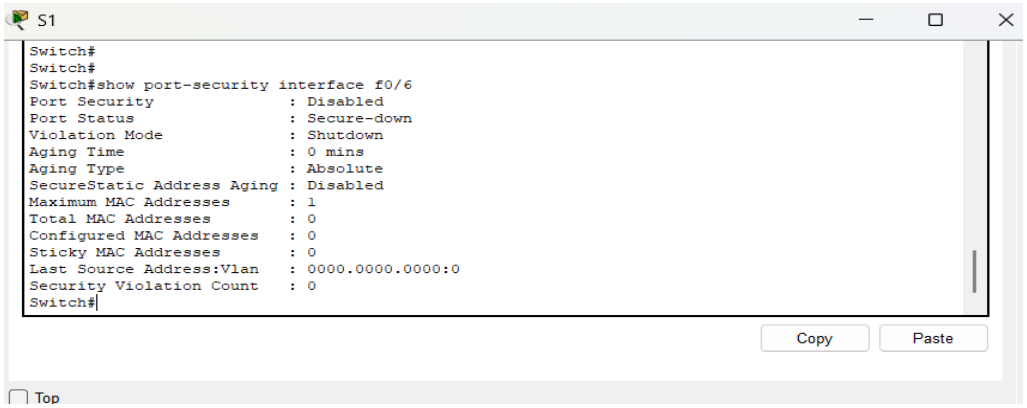


Step4: Document and implement port security features.

The interfaces F0/6 on S1 and F0/18 on S2 are configured as access ports. In this step, I will also configure port security on these two access ports.

1. On S1, I issued the **show port-security interface f0/6** command to display the default port security settings for interface F0/6. I recorded my answers in the table below

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 Agine	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

2. On S1, I enabled 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

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

```
Switch(config-if)#exit
Switch(config)#interface f0/6
Switch(config-if)#switchport port mode access
                                         ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 3
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#switchport port-security aging time 60
Switch(config-if)#switchport port-security aging type inactivity
                                                       ^
% Invalid input detected at '^' marker.

Switch(config-if)#switchport port-security aging type inactivity
```

3. Verify port security on S1 F0/6.

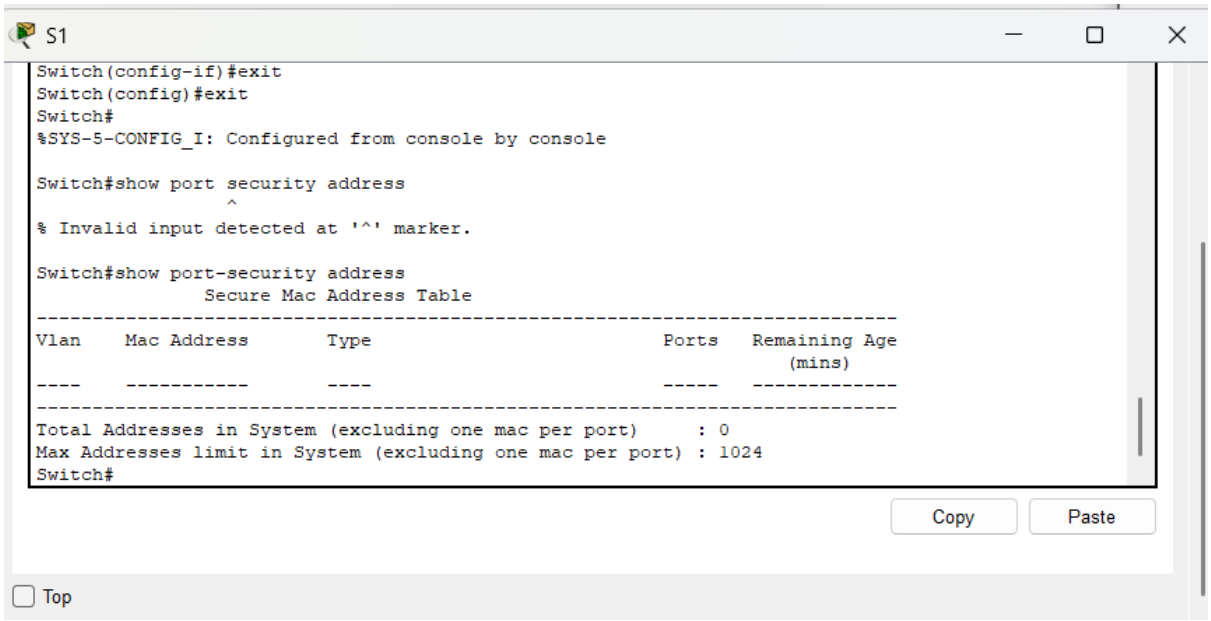
S1# show port-security interface f0/6

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

Switch#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

Switch#config t'
              ^
```

According to the output the switch 2960 does not support inactivity-type configuration

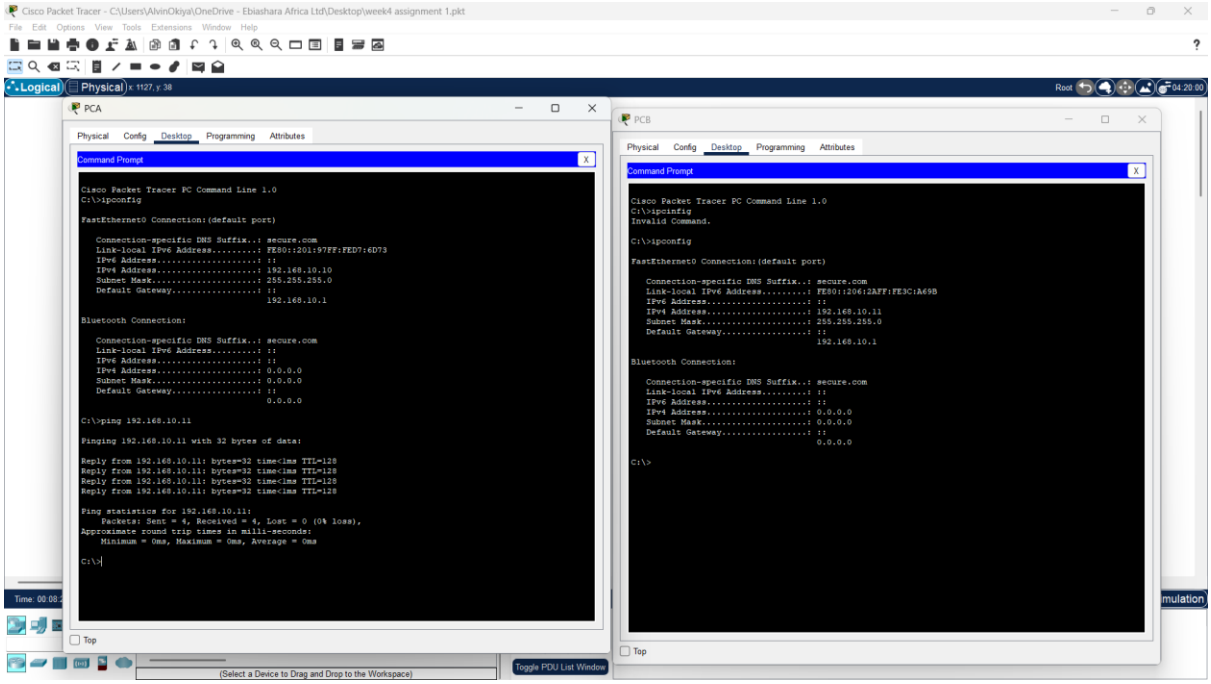
```
Switch(config)#interface f0/6
Switch(config-if)#switchport port-security aging ?
  time  Port-security aging time
Switch(config-if)#
```

Show port security address:

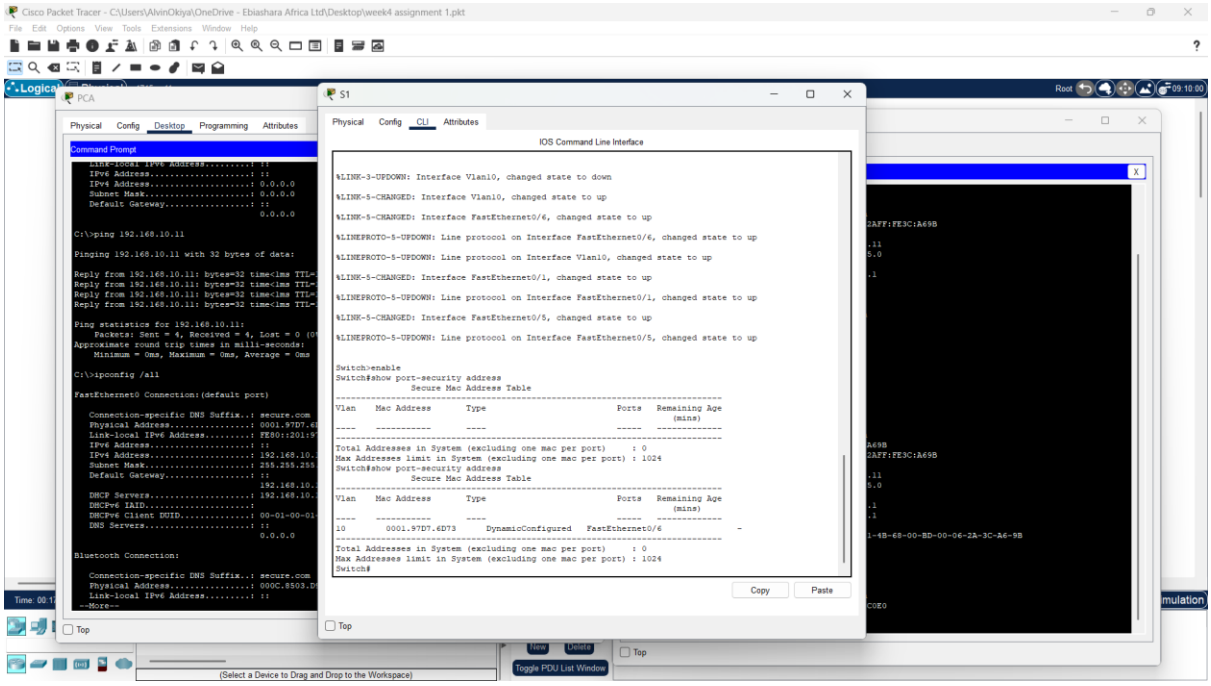


However this wasn't the expected output. This is because the command gives us an empty output.

The reason for this was because Port-security only learns MAC addresses when a device sends frames (like ARP or ICMP). If a device (like a PC) is connected but idle or powered off, no MAC will be learned. I therefore opened configurations for each pc and enabled DHCP for them to obtain ip addresses automatically, used the ipconfig on their cli and pinged one of them as shown:



This confirmed that the two devices were communicating. I hence checked the switch's "show port-security address" and one mac address had reflected. For the sender of the ICMP packets.



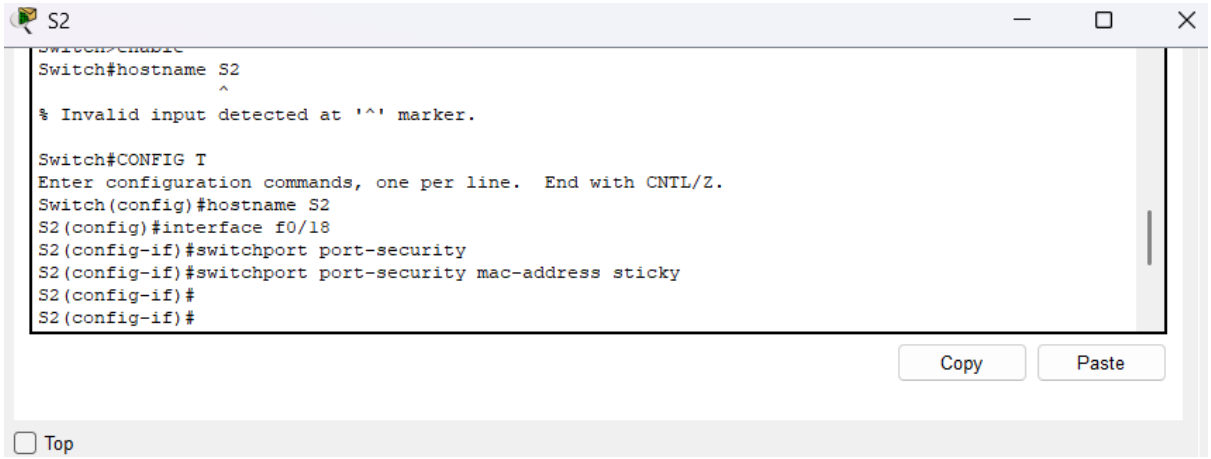
This was the result as the switch didn't allow configuration of aging type hence secure dynamic is replaced with dynamic configured.

4.Next was to enable port security for F0/18 on S2. Configure the port to add MAC addresses learned on the port automatically to the running configuration.

S2(config)# interface f0/18

S2(config-if)# switchport port-security

S2(config-if)# switchport port-security mac-address sticky



5. I then Configured the following port security settings on S2 F/18:

• Maximum number of MAC addresses: 2

• Violation type: **Protect**

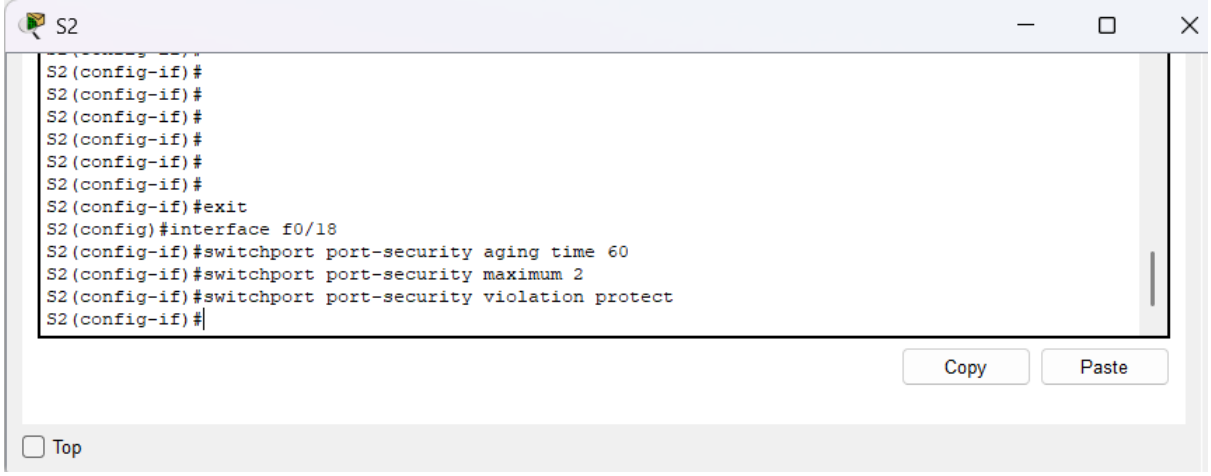
• Aging time: **60 min**

S2(config)# interface f0/18

S2(config-if)# switchport port-security aging time 60

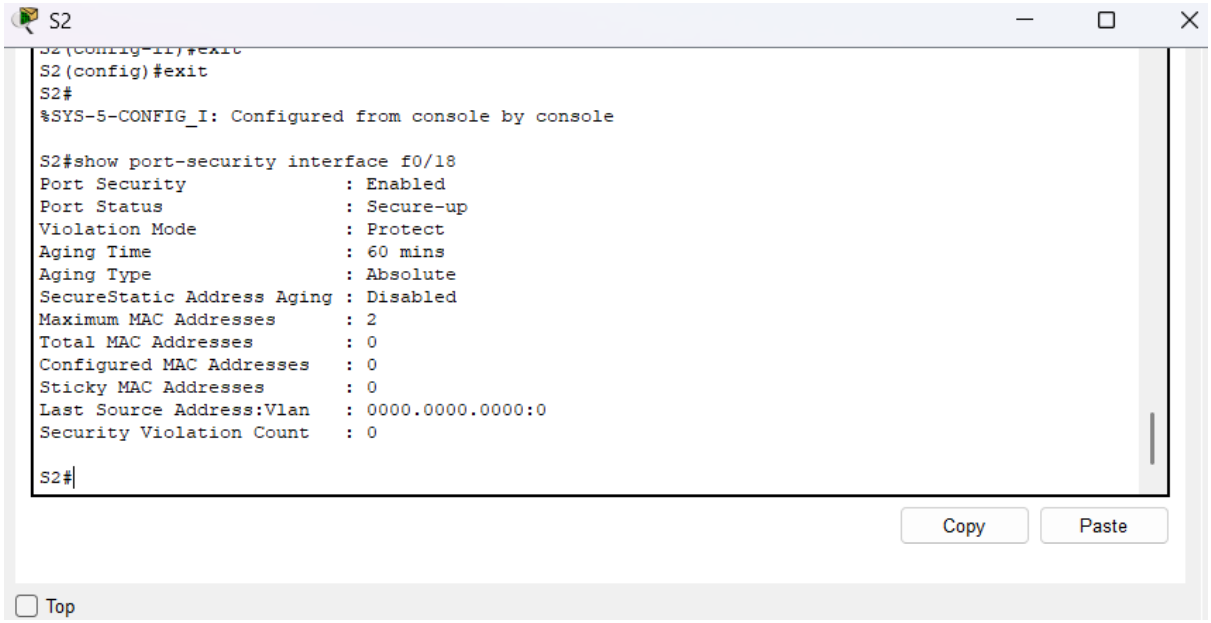
S2(config-if)# switchport port-security maximum 2

S2(config-if)# switchport port-security violation protect



6. Verify port security on S2 F0/18.

S2# show port-security interface f0/18



After pinging PCB from PCA, the switch learned PCB Macs address and the “show port-security address” command outputted this which is PCBs mac address:

```
S2
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#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
  10    0006.2A3C.A69B    SecureSticky                  Fa0/18       -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S2#S
```

Step5: Implement DHCP snooping security.

1. On S2, I enabled DHCP snooping and configured DHCP snooping on VLAN 10.

S2(config)# ip dhcp snooping

S2(config)# ip dhcp snooping vlan 10

```
S2
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)#
S2(config)#
S2(config)#
S2(config)#
```

2. I then Configured the trunk port on S2 as a trusted port.

S2(config)# interface f0/1

S2(config-if)# ip dhcp snooping trust

```
S2
S2(config)#
S2(config)#interface f0/1
S2(config-if)#if dhcp snooping trust
                ^
% Invalid input detected at '^' marker.

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

Copy Paste

Top

3. I then Limited the untrusted port, F18 on S2, to five DHCP packets per second.

S2(config)# interface f0/18

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

```
S2
S2(config-if)#exit
S2(config)#interface f0/1
S2(config-if)#ip dhcp snooping trust
S2(config-if)#
S2(config-if)#
S2(config-if)#
S2(config-if)#interface f0/18
S2(config-if)#ip dhcp snooping limit rate 5
S2(config-if)#
```

Copy Paste

Top

4. Then I Verified DHCP Snooping on S2.

S2# show ip dhcp snooping

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

S2#
S2#
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#
```

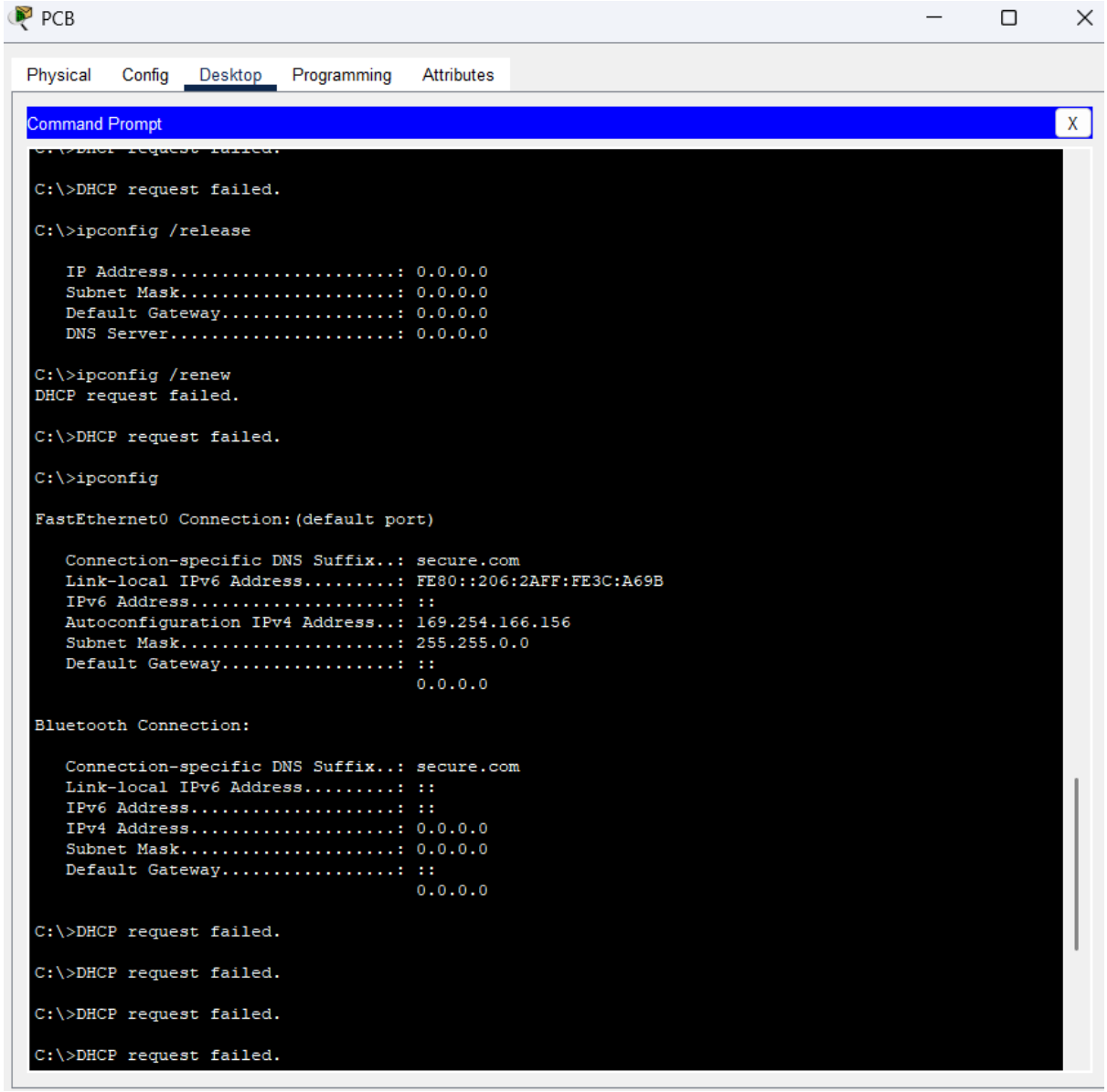
Copy Paste

Top

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

C:\Users\Student> **ipconfig /release**

C:\Users\Student> **ipconfig /renew**

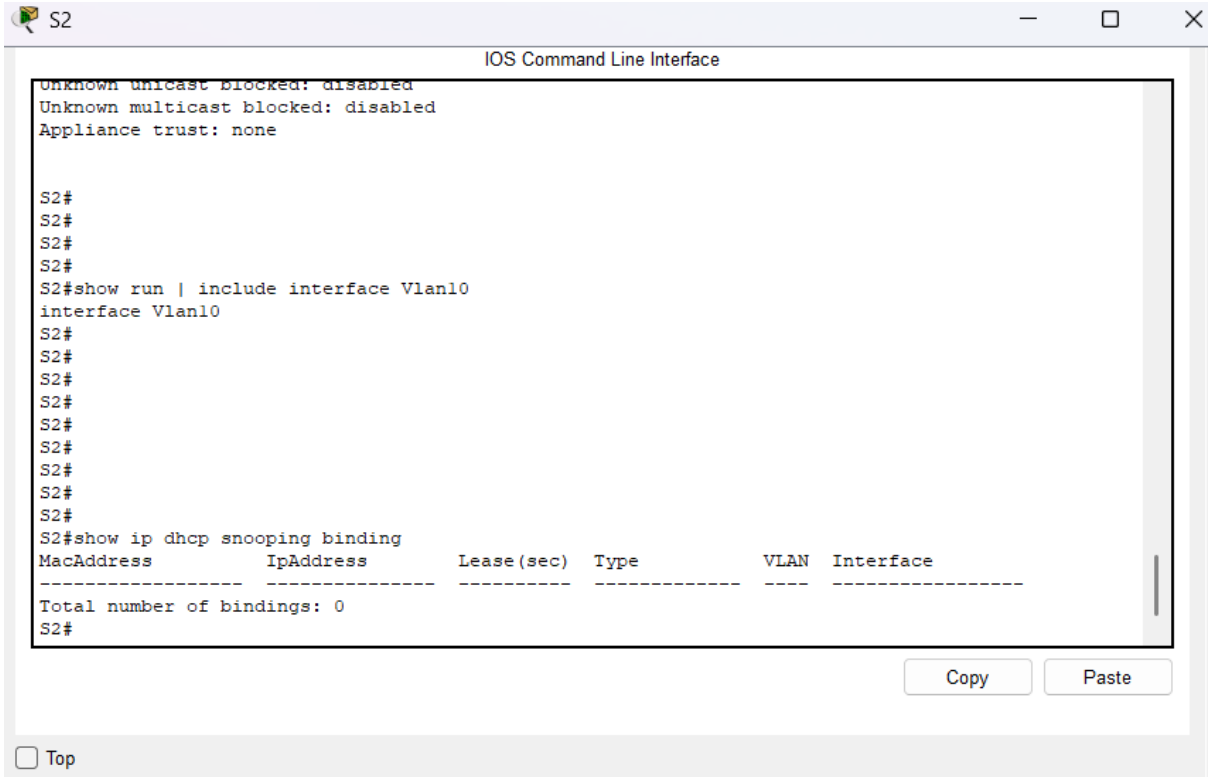


A new ip address cant be assigned because:

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.

6. Verify the DHCP snooping binding using the **show ip dhcp snooping binding** command.

S2# show ip dhcp snooping binding



Step6: Implement PortFast and BPDU guard.

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

S1(config)# interface range f0/5 – 6

S1(config-if)# spanning-tree portfast

S2(config)# interface f0/18

S2(config-if)# spanning-tree portfast

S2

Physical Config CLI Attributes

IOS Command Line Interface

```
S2#
S2#
S2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ------------------
Total number of bindings: 0
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#interface range f0/5-6
S2(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.
S2(config-if-range)#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)#
```

Copy Paste

Top

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

S1(config)# interface f0/6

S1(config-if)# spanning-tree bpduguard enable

S2(config)# interface f0/18

S2(config-if)# spanning-tree bpduguard enable

S2

Physical Config CLI Attributes

IOS Command Line Interface

```
S2(config-if)#spanning-tree bpduguard enable
S2(config-if)#exit
S2(config)#interface f0/18
S2(config-if)#spanning-tree bpduguard enable
S2(config-if)#show spanning-tree interface f0/6 detail
                ^
% Invalid input detected at '^' marker.

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

S2#show spanning-tree interface f0/6 detail


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.C982.E2D0
  Designated bridge has priority 32778, address 0006.2ABE.192E
  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#
```

Copy Paste

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

S1# show spanning-tree interface f0/6 detail

Physical Config CLI Attributes

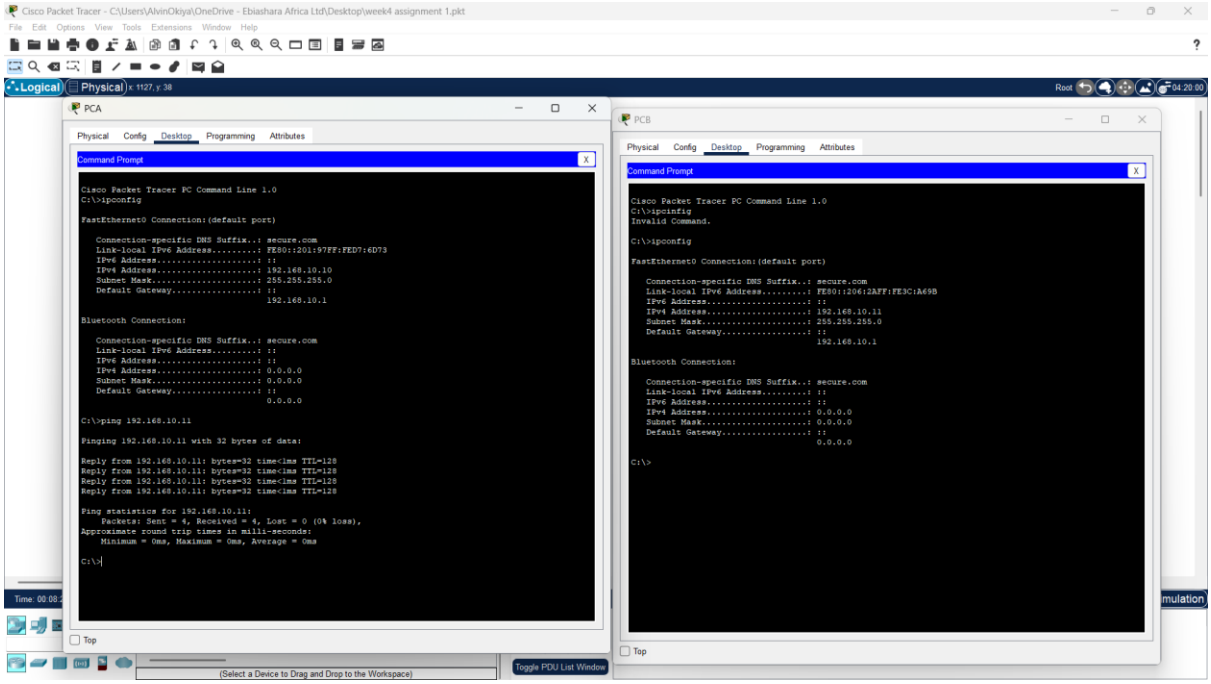
IOS Command Line Interface

```
S1>enable
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/6
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#show spanning tree interface f0/6
                ^
% Invalid input detected at '^' marker.

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

S1#spanning-tree bpduguard enable
                ^
% Invalid input detected at '^' marker.

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 0001.C982.E2D0
  Designated bridge has priority 32778, address 0001.C982.E2D0
  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
  Link type is point-to-point by default


S1#
```

Copy Paste

Step7: 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.



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.

CONCLUSION

Through this hands-on lab, the secure configuration of VLANs and switches was successfully implemented and validated. The network was logically segmented to enhance manageability and security. Critical features including trunking, port security, DHCP snooping, and BPDU guard were applied to mitigate potential threats. This lab reinforces the importance of Layer 2 security in modern networks and demonstrates the practical steps necessary to secure an enterprise-grade switching environment.