

# WEEK 4 ASSIGNMENT 1:

## VLANs AND SECURE SWITCH CONFIGURATION

RENE OLUOCH  
CS-CNS09-25030

### Contents

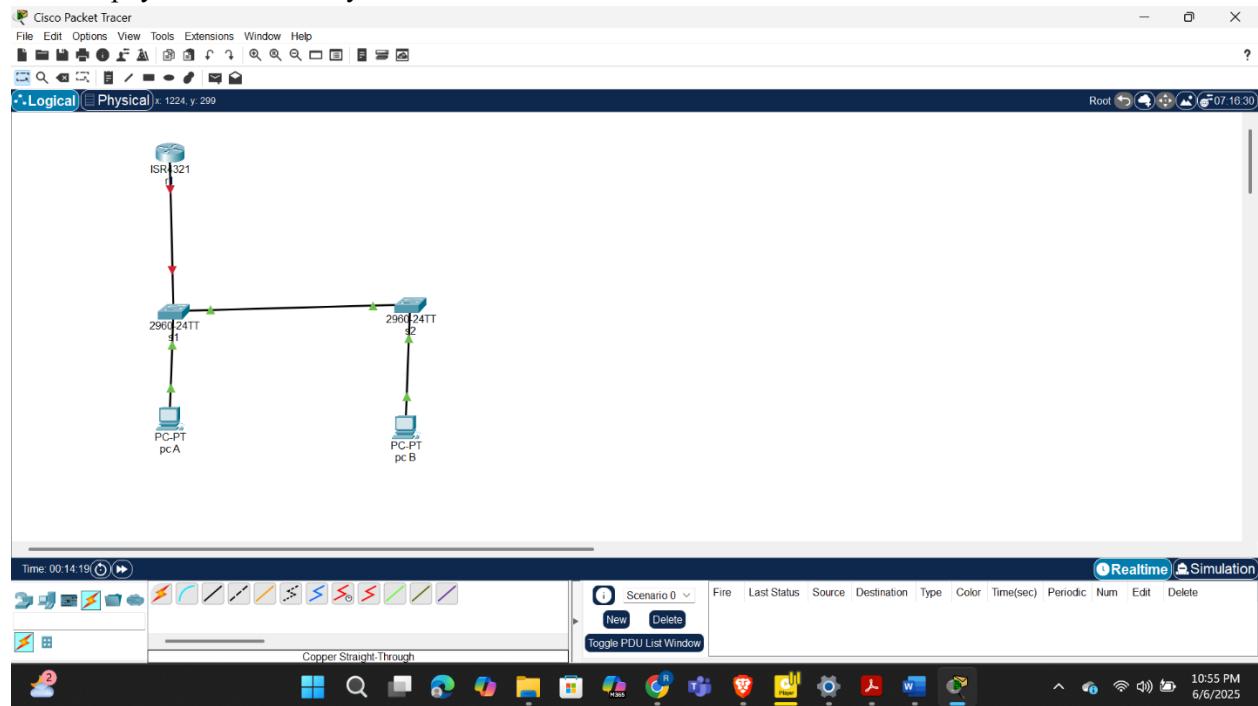
|   |    |
|---|----|
| Introduction.....                               | 2  |
| Cabling the network.....                        | 2  |
| Configuring Router R1 .....                     | 3  |
| Configuring VLANs on Switches .....             | 4  |
| Configuring VLAN 10 .....                       | 4  |
| Configuring the SVI for VLAN 10 .....           | 4  |
| Configuring VLAN 333 (Native VLAN).....         | 5  |
| Configuring VLAN 999 (Parking Lot) .....        | 5  |
| Configuring Switch Security.....                | 7  |
| Implement 802.1Q trunking.....                  | 7  |
| Configuring access points .....                 | 10 |
| Securing and disabling unused switchports ..... | 12 |
| Implementing port security features. ....       | 14 |
| Implementing dhcp snooping security .....       | 16 |
| Implementing PortFast and BPDU guard. ....      | 17 |
| Verifying end-to-end connectivity.....          | 19 |
| Reflection.....                                 | 21 |
| Conclusion .....                                | 23 |

## Introduction

In this lab, I undertook a comprehensive hands-on exercise to design, configure, and secure a network using Cisco switches and routers. The focus was on implementing Virtual LANs (VLANs), inter-VLAN routing, trunking protocols, DHCP services, and critical Layer 2 security features. Through a structured approach, I configured devices, assigned IP addressing, created and verified VLANs, enabled 802.1Q trunking, and deployed advanced switch security mechanisms such as port security, DHCP snooping, and BPDU guard. This practical experience not only reinforced my understanding of theoretical concepts but also enhanced my troubleshooting skills and my ability to manage real-world networking environments securely and efficiently.

## Cabling the network

I started by physically cabling the network according to the provided topology. I connected the router's GigabitEthernet0/0/1 interface to Switch S1's FastEthernet0/5 port, which serves as the gateway for devices on the network. Then, I connected Switch S1's FastEthernet0/1 to Switch S2's FastEthernet0/1 — this link was later configured as a trunk. For end devices, PC-A was connected to S1's F0/6, and PC-B to S2's F0/18. Once connected, I powered on all devices and verified that the link lights were green to confirm physical connectivity.



*Fig 1.0 setting up the topology*

## Configuring Router R1

On the router, I began by changing its hostname to R1 for clarity. I then disabled DNS lookup to avoid unnecessary delay from mistyped commands triggering name resolution.

Next, I configured IP address exclusions to reserve the router's own IP address (192.168.10.1) and the two switch management addresses (192.168.10.201 and .202) so they wouldn't be handed out by the DHCP server.

I then created a DHCP pool named "Students", assigning it the 192.168.10.0/24 subnet. I specified the default gateway as 192.168.10.1 and assigned a domain name "secure.com" for DHCP clients. This configuration allows dynamic IP assignment to both PCs.

After that, I created a Loopback0 interface with the IP address 10.10.1.1/24. This interface simulates a remote internal network or a test point for routing verification.

Finally, I configured the GigabitEthernet0/0/1 interface with the IP address 192.168.10.1, enabled it, and marked it as a trusted source for DHCP relay. This interface connects to Switch S1 and serves as the default gateway for the rest of the network.

After the configuration, I verified interface statuses to ensure both G0/0/1 and Loopback0 were up and operational.

Physical Config **CLI** Attributes

IOS Command Line Interface

```
Router#show version
Cisco ISR4321/K9 (IRQ) processor with 1687137K/6147K bytes of memory.
Processor ID FIMC041WEND
2 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3223351K bytes of flash memory at bootflash:.

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: n

Press RETURN to get started!

Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface g0/0/0/1
% Invalid input detected at '^' marker.

Router(config)#
Router(config)#hostname R1
R1(config)#interface GigabitEthernet0/0/1
% Invalid input detected at '^' marker.

R1(config)#
R1(config)#hostname R1
R1(config)#interface GigabitEthernet0/0/1
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
R1(config-if)#LINEPROTO-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

 
```

```

R1>en
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no ip domain lookup
R1(config)ip dhcp excluded-address 192.168.10.1 192.168.10.5
R1(config)ip dhcp pool students
R1(config-dhcp)#range address 192.168.10.201 192.168.10.202
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)#interface Loopback0
R1(config-if)#
LINK-5-CHANGED: Interface Loopback0, changed state to up
LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
R1(config-if)#ip address 10.10.1.1 255.255.255.0
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 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)#line con 0
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 0 0
R1(config-line)#
R1#
$S1-5-CONFIG I: Configured from console by console
R1#s
R1#
R1#show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
GigabitEthernet0/0/0 unassigned      YES unset administratively down down

```

*Figs 1.1 configuring the router*

## Configuring VLANs on Switches

For both switches, I first renamed their hostnames to S1 and S2 to differentiate them clearly in the CLI and network monitoring tools. I disabled DNS lookup to prevent delays from mistyped commands being interpreted as hostnames.

I then added interface descriptions on both switches to label the purpose of each port — for example, marking F0/1 as "Link to S2" and F0/5 as "Link to R1." This step improves readability and management of the configuration, especially during troubleshooting.

After that, I set the default gateway of both switches to 192.168.10.1 — the router's IP — so that they can communicate with devices outside their VLAN. This is crucial for remote management (e.g., via SSH or Telnet).

## Configuring VLAN 10

I created VLAN 10 on both S1 and S2 and assigned it the name "Management". This VLAN is used for management purposes, including accessing the switch remotely. Using a dedicated VLAN helps in segregating administrative traffic from user data traffic, improving security and monitoring.

## Configuring the SVI for VLAN 10

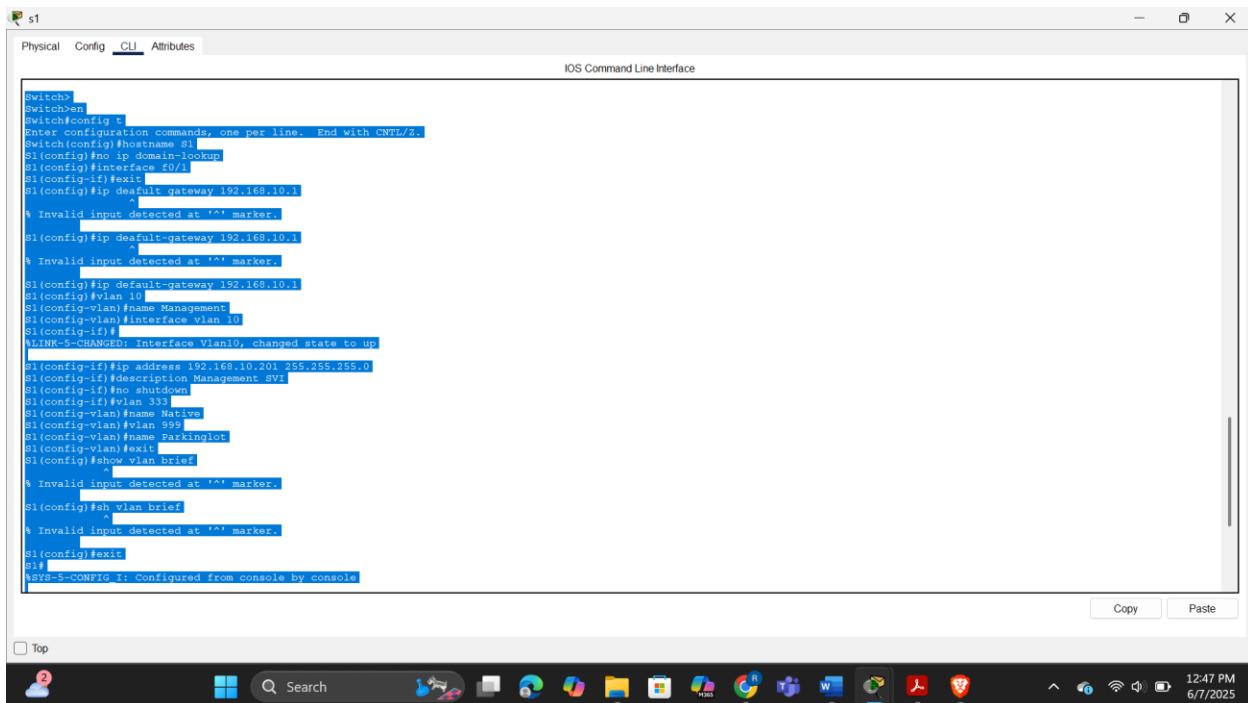
I then configured a Switched Virtual Interface (SVI) for VLAN 10 on both switches. On S1, I assigned the IP address 192.168.10.201, and on S2, 192.168.10.202. I added a description to each SVI indicating it is for management purposes and then enabled the interfaces. These IP addresses allow me to remotely access and manage each switch through VLAN 10.

## Configuring VLAN 333 (Native VLAN)

Next, I created VLAN 333 on both switches and named it "Native." This VLAN is assigned as the native VLAN for trunk ports between S1 and S2. The native VLAN is used for untagged traffic, and setting a custom native VLAN (rather than leaving it at VLAN 1) adds a layer of security to prevent VLAN hopping attacks.

## Configuring VLAN 999 (Parking Lot)

Lastly, I configured VLAN 999 on both switches and named it "ParkingLot." This VLAN is used to isolate unused ports, effectively neutralizing them from unauthorized access or accidental connections. Assigning unused ports to an unused VLAN and disabling them is a common security best practice.



The screenshot shows a Windows desktop environment with a Cisco IOS CLI window open. The window title is 's1'. The tabs at the top are 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. Below the tabs is the text 'IOS Command Line Interface'. The main area of the window displays the following configuration commands:

```
Switch>
Switch#en
Switch(config)#
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)#exit
S1(config)#ip default-gateway 192.168.10.1
          ^
% Invalid input detected at '^' marker.
S1(config)#ip default-gateway 192.168.10.1
          ^
% Invalid input detected at '^' marker.
S1(config)#ip default-gateway 192.168.10.1
S1(config)#vlan 10
S1(config-vlan)#name Management
S1(config-vlan)#interface vlan 10
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up
S1(config-if)#ip address 192.168.10.201 255.255.255.0
S1(config-if)#description Management svr
S1(config-if)#no shutdown
S1(config-if)#vlan 333
S1(config-vlan)#name Native
S1(config-vlan)#vlan 999
S1(config-vlan)#name Parkinglot
S1(config-vlan)#exit
S1(config)#show vlan brief
          ^
% Invalid input detected at '^' marker.
S1(config)#sh vlan brief
          ^
% Invalid input detected at '^' marker.
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

At the bottom of the window, there are 'Copy' and 'Paste' buttons. The taskbar at the bottom of the screen shows various application icons, and the system tray indicates the date and time as 12:47 PM on 6/7/2025.

Fig 1.2 configuring s1

s1

Physical Config CLI Attributes

IOS Command Line Interface

```

Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname s1
Switch(config)#interface vlan 10
Switch(config-if)#description Management SVI
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#name Management
Switch(config)#exit
Switch#Configured from console by console

S1#show vlan brief
VLAN Name          Status    Ports
-- -- --
1   default         active   Fa0/1, Fa0/2, Fa0/3, Fa0/4
                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                           G1g0/1, G1g0/2

10  Management      active
33  Native          active
999 Parkinglot     active
1002 fddi0-default  active
1003 token-ring-default active
1004 fddi1-default  active
1005 trnet-default  active
S1#

```

Top

Copy Paste

12:48 PM  
6/7/2025

Fig 1.3 s1 vlan interfaces

s2

Physical Config CLI Attributes

IOS Command Line Interface

```

Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname s2
Switch(config)#interface vlan 10
Switch(config-if)#description Management
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config-vlan)#configure interface vlan 10
Switch(config-vlan)#ip address 192.168.10.202 255.255.255.0
Switch(config-vlan)#ip address 192.168.10.202 255.255.255.0
Switch(config-vlan)#ip address 192.168.10.202 255.255.255.0
Switch(config-vlan)#ip address 192.168.10.202 255.255.255.0
Switch(config-vlan)#interface vlan 10
Switch(config-if)#description Management SVI
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config-vlan)#name Management
Switch(config-vlan)#exit
Switch#Configured from console by console

S2#show vlan brief
VLAN Name          Status    Ports
-- -- --
1   default         active   Fa0/1, Fa0/2, Fa0/3, Fa0/4
                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                           G1g0/1, G1g0/2

10  Management      active
33  Native          active
999 Parkinglot     active
1002 fddi0-default  active
1003 token-ring-default active
1004 fddi1-default  active
1005 trnet-default  active
S2#

```

Top

Copy Paste

12:57 PM  
6/7/2025

Fig 1.4 configuring s2

*Fig 1.5 s2 vlan interfaces*

## Configuring Switch Security.

Implement 802.1Q trunking.

To enable VLAN communication across switches, I configured 802.1Q trunking on the inter-switch link (F0/1) between S1 and S2. I set both interfaces to trunk mode and assigned VLAN 333 as the native VLAN. This ensures that untagged frames (often management or legacy traffic) are handled securely on a dedicated VLAN.

To further harden the trunk, I disabled DTP (Dynamic Trunking Protocol) on both trunk interfaces using the nonegotiate option. This forces the trunk configuration to be static, preventing a rogue device from negotiating trunking automatically — a common attack vector.

Afterward, I verified trunking using the show interfaces trunk command and confirmed that VLANs 1, 10, 333, and 999 were allowed and active on the trunk link, and the native VLAN was correctly set to 333.

```

S1>
S1>n
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
S1(config-if)#switchport trunk native vlan 333
S1(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with s2 FastEthernet0/1 (1).
S1(config-if)#exit
S1(config)#
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#n
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#
S1(config)#interface f0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#

```

Fig 1.6 implementing 802.1Q trunking to s1

```

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
S1(config-if)#switchport trunk native vlan 333
S1(config-if)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with s2 FastEthernet0/1 (1).
S1(config-if)#exit
S1(config)#
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#n
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1#
S1(config)#
S1(config)#interface f0/1
S1(config-if)#switchport nonegotiate
S1(config-if)#
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#show interface f0/1 switchport | include Negotiation
Negotiation of Trunking: off
S1#

```

Fig 1.7 disabling dtp on s1

```

s2#en
s2#config t
Enter configuration commands, one per line. End with CNTL/Z.
s2(config)#
s2(config)#interface f0/1
s2(config-if)#switchport mode trunk
s2(config-if)#switchport trunk native vlan 333
s2(config-if)##SPAN TREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0333. Port consistency restored.
%SPAN TREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0001. Port consistency restored.

s2(config-if)#
s2(config-if)#exit
s2(config)#
s2#
%SYS-5-CONFIG_I: Configured from console by console

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    1,10,33,999

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1,10,33,999

s2#
s2#config t
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)#
%SYS-5-CONFIG_I: Configured from console by console

s2#show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: off
s2#

```

Fig 1.8 implementing 802.1Q trunking to s2

```

s2#en
s2#config t
Enter configuration commands, one per line. End with CNTL/Z.
s2(config)#
s2(config)#interface f0/1
s2(config-if)#switchport mode trunk
s2(config-if)#switchport trunk native vlan 333
s2(config-if)##SPAN TREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0333. Port consistency restored.
%SPAN TREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0001. Port consistency restored.

s2(config-if)#
s2(config-if)#exit
s2(config)#
s2#
%SYS-5-CONFIG_I: Configured from console by console

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    1,10,33,999

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1,10,33,999

s2#
s2#config t
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)#
%SYS-5-CONFIG_I: Configured from console by console

s2#show interfaces f0/1 switchport | include Negotiation
Negotiation of trunking: off
s2#

```

*Fig 1.9 disabling dtp on s1*

```
s2#config t
Enter configuration commands, one per line. End with CNTL/Z.
s2(config)#interface f0/1
s2(config-if)#switchport mode trunk
s2(config-if)#switchport trunk native vlan 333
s2(config-if)##SPAN TREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0333. Port consistency restored.

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

s2(config-if)#
s2(config-if)#exit
s2(config)#
s2#
%SYS-5-CONFIG_I: Configured from console by console

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#config t
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)#
%SYS-5-CONFIG_I: Configured from console by console

s2#show interfaces f0/1 switchport | include Negotiation
Negotiation of trunking: Off
s2#
```

*Fig 2.0 Disabling dtp on s2*

After completing the trunk implementation, I proceeded to verify the entire VLAN and trunk configuration to ensure that all settings were applied correctly and were functioning as expected. Using the show vlan brief command on both switches, I confirmed the presence of VLAN 10, VLAN 333 (named Native), and VLAN 999 (named ParkingLot). VLAN 10 appeared as active, and the appropriate ports were correctly assigned to it. VLAN 333 was confirmed as the native VLAN, and VLAN 999 was observed to be assigned to unused ports, serving its purpose as the designated parking lot VLAN. I then issued the show interfaces trunk command and verified that 802.1Q trunking was operational between the switches S1 and S2, with VLAN 333 correctly set as the native VLAN and VLAN 10 allowed across the trunk. Finally, the show interfaces status command allowed me to confirm that all interfaces were in the expected state, matching the configuration plans. This verification step gave me confidence that the VLAN segmentation and inter-switch communication were implemented correctly and securely.

### Configuring access points

I configured access ports for the end devices. On Switch S1, I set F0/5 and F0/6 as access ports in VLAN 10, used for PC-A and the router connection respectively. On Switch S2, I configured F0/18 as an access port for PC-B, also in VLAN 10. Assigning these ports to the correct VLAN ensures that client devices can obtain IP addresses via DHCP and communicate within the correct broadcast domain.

The screenshot shows a Windows desktop environment with a terminal window titled 's1'. The window has tabs for 'Physical', 'Config', 'CLI' (which is selected), and 'Attributes'. The title bar also says 'IOS Command Line Interface'. The terminal window displays the following configuration command:

```
S1>
S1#con0
S1(config)#
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#
S1(config)#interface range f0/5 6
      ^
% Invalid input detected at '' marker.

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)#

S1 con0 is now available

Press RETURN to get started.
```

At the bottom right of the terminal window, there are 'Copy' and 'Paste' buttons. Below the terminal window, the Windows taskbar is visible, showing various icons for applications like File Explorer, Microsoft Edge, and others. The system tray indicates the date and time as 6/7/2025 at 4:24 PM.

Fig 2.1 Config access point s1

The screenshot shows a Windows desktop environment with a terminal window titled 's2'. The window has tabs for 'Physical', 'Config', 'CLI' (selected), and 'Attributes'. The title bar says 'IOS Command Line Interface'. The terminal window displays the following configuration command:

```
s2>
s2>
s2>
s2#con0
s2(config)#
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)#

s2 con0 is now available

Press RETURN to get started.
```

At the bottom right of the terminal window, there are 'Copy' and 'Paste' buttons. Below the terminal window, the Windows taskbar is visible, showing various icons for applications like File Explorer, Microsoft Edge, and others. The system tray indicates the date and time as 6/7/2025 at 4:27 PM.

Fig 2.1.1 Config access point s2

## Securing and disabling unused switchports

To improve security, I identified all unused switchports on both S1 and S2. I moved these ports into VLAN 999 (ParkingLot), which is a non-functional VLAN. This effectively isolates unused ports and prevents them from passing traffic. I then administratively shut down these interfaces to prevent unauthorized access or rogue device connections.

After this, I verified port statuses using the show interfaces status command. All unused ports appeared as "disabled" and assigned to VLAN 999, as expected.



```
s2>
s2#conf t
s2#
s2#config t
Enter configuration commands, one per line. End with CNTL/Z.
s2(config)#
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
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
```

Fig 2.2 Disabling unused sw ports s2

```
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
s2#s2#
%SYS-5-CONFIG_I: Configured from console by console

s2#show interfaces status
Port    Name      Status   Vlan   Duplex Speed Type
Fast0/1  connected auto    auto   full-duplex
Fast0/2  disabled  999    auto   auto   10/100BaseTX
Fast0/3  disabled  999    auto   auto   10/100BaseTX
Fast0/4  disabled  999    auto   auto   10/100BaseTX
Fast0/5  disabled  999    auto   auto   10/100BaseTX
Fast0/6  disabled  999    auto   auto   10/100BaseTX
Fast0/7  disabled  999    auto   auto   10/100BaseTX
Fast0/8  disabled  999    auto   auto   10/100BaseTX
Fast0/9  disabled  999    auto   auto   10/100BaseTX
Fast0/10  disabled  999    auto   auto   10/100BaseTX
Fast0/11  disabled  999    auto   auto   10/100BaseTX
Fast0/12  disabled  999    auto   auto   10/100BaseTX
Fast0/13  disabled  999    auto   auto   10/100BaseTX
Fast0/14  disabled  999    auto   auto   10/100BaseTX
Fast0/15  disabled  999    auto   auto   10/100BaseTX
Fast0/16  disabled  999    auto   auto   10/100BaseTX
Fast0/17  disabled  999    auto   auto   10/100BaseTX
Fast0/18  connected 10    auto   auto   10/100BaseTX
Fast0/19  disabled  999    auto   auto   10/100BaseTX
Fast0/20  disabled  999    auto   auto   10/100BaseTX
Fast0/21  disabled  999    auto   auto   10/100BaseTX
Fast0/22  disabled  999    auto   auto   10/100BaseTX
Fast0/23  disabled  999    auto   auto   10/100BaseTX
Fast0/24  disabled  999    auto   auto   10/100BaseTX
Gig0/1   disabled  999    auto   auto   10/100BaseTX
Gig0/2   disabled  999    auto   auto   10/100BaseTX
```

*Fig 2.3 Verifying the disabled ports*

```
s1#s1#config t
Enter configuration commands, one per line. End with CNTL/Z.
s1(config)#interface range f0/2-21, f0/7-24, q0/1-2
s1(config-if-range)#switchport mode access
s1(config-if-range)#switchport access vlan 995
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
%LINK-5-CHANGED: Interface FastEthernet0/13, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/14, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/16, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
```

*fig 2.4 Disabling unused ports s1*

```

%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S1(config-if-range)#show interfaces status
^
% Invalid input detected at '^' marker.

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

S1#show interfaces status
Port      Name           Status    Vlan   Duplex  Speed  Type
Fast0/1   connected    trunk    auto   auto   10/100BaseTX
Fast0/2   disabled     999     auto   auto   10/100BaseTX
Fast0/3   disabled     999     auto   auto   10/100BaseTX
Fast0/4   disabled     999     auto   auto   10/100BaseTX
Fast0/5   connected    10      auto   auto   10/100BaseTX
Fast0/6   connected    10      auto   auto   10/100BaseTX
Fast0/7   disabled     999     auto   auto   10/100BaseTX
Fast0/8   disabled     999     auto   auto   10/100BaseTX
Fast0/9   disabled     999     auto   auto   10/100BaseTX
Fast0/10  disabled     999     auto   auto   10/100BaseTX
Fast0/11  disabled     999     auto   auto   10/100BaseTX
Fast0/12  disabled     999     auto   auto   10/100BaseTX
Fast0/13  disabled     999     auto   auto   10/100BaseTX
Fast0/14  disabled     999     auto   auto   10/100BaseTX
Fast0/15  disabled     999     auto   auto   10/100BaseTX
Fast0/16  disabled     999     auto   auto   10/100BaseTX
Fast0/17  disabled     999     auto   auto   10/100BaseTX
Fast0/18  disabled     999     auto   auto   10/100BaseTX
Fast0/19  disabled     999     auto   auto   10/100BaseTX
Fast0/20  disabled     999     auto   auto   10/100BaseTX
Fast0/21  disabled     999     auto   auto   10/100BaseTX
--More--

```

Copy      Paste

Top

Fig 2.5 Verifying disabled s1 ports

Implementing port security features.

To prevent MAC flooding or unauthorized device access, I enabled port security on F0/6. I configured the port to allow a maximum of 3 MAC addresses, which is helpful for scenarios like VoIP phones + workstations sharing a port.

I set the violation mode to restrict, which silently drops unauthorized traffic but logs the violation. I also enabled MAC address aging — specifically inactivity-based aging, which removes MACs from the table after 60 minutes of no activity.

I verified this using the show port-security command, which confirmed that port security was active, the violation mode was restrict, and the aging policy was in place.

- ◆ On S2 (Port F0/18 for PC-B):

On S2, I enabled sticky MAC address learning on F0/18, allowing the switch to dynamically learn MAC addresses and write them into the running configuration.

I limited the port to two MAC addresses, and configured the violation action as protect, meaning any unknown MAC will be silently dropped, without shutting down the port or generating alerts.

This is a stricter form of control suitable for stable endpoint environments. After setup, I validated the configuration and confirmed that the MAC address for PC-B was stored as a sticky entry.

s1

Physical Config **CLI** Attributes

IOS Command Line Interface

```
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S1(config-if-range)#show interfaces status
^
% Invalid input detected at '^' marker.

S1(config-if-range)##2
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#show interfaces status
Port Name Status Vlan Duplex Speed Type
Fast0/1 connected trunk auto auto 10/100BaseTX
Fast0/2 disabled 999 auto auto 10/100BaseTX
Fast0/3 disabled 999 auto auto 10/100BaseTX
Fast0/4 disabled 999 auto auto 10/100BaseTX
Fast0/5 connected 10 auto auto 10/100BaseTX
Fast0/6 connected 10 auto auto 10/100BaseTX
Fast0/7 disabled 999 auto auto 10/100BaseTX
Fast0/8 disabled 999 auto auto 10/100BaseTX
Fast0/9 disabled 999 auto auto 10/100BaseTX
Fast0/10 disabled 999 auto auto 10/100BaseTX
Fast0/11 disabled 999 auto auto 10/100BaseTX
Fast0/12 disabled 999 auto auto 10/100BaseTX
Fast0/13 disabled 999 auto auto 10/100BaseTX
Fast0/14 disabled 999 auto auto 10/100BaseTX
Fast0/15 disabled 999 auto auto 10/100BaseTX
Fast0/16 disabled 999 auto auto 10/100BaseTX
Fast0/17 disabled 999 auto auto 10/100BaseTX
Fast0/18 disabled 999 auto auto 10/100BaseTX
Fast0/19 disabled 999 auto auto 10/100BaseTX
Fast0/20 disabled 999 auto auto 10/100BaseTX
Fast0/21 disabled 999 auto auto 10/100BaseTX
--More--

```

Top

Copy Paste

4:38 PM  
6/7/2025

Fig 2.6 Showing port security

s2

Physical Config **CLI** Attributes

IOS Command Line Interface

```
s2#show port-security interface f0/18
Port Security : Disabled
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#config t
Enter configuration commands, one per line. End with CNTL/Z.
s2(config)#int f0/18
s2(config-if)#port security
^
% Invalid input detected at '^' marker.

s2(config-if)#switchport port-security
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)##2
S2#
%SYS-5-CONFIG_I: Configured from console by console
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#

```

Top

Copy Paste

5:12 PM  
6/7/2025

Fig 2.7 Enabling port security and verifying s2

## Implementing dhcp snooping security

To defend against rogue DHCP servers, I enabled DHCP snooping globally and specifically on VLAN 10, which is the client VLAN.

I marked the trunk port (F0/1) on S2 as a trusted port, because it connects to other infrastructure devices. The access port F0/18 (connected to PC-B) was left untrusted and limited to 5 DHCP messages per second. This prevents DHCP starvation or exhaustion attacks.

I tested the setup by releasing and renewing PC-B's IP address, which succeeded, indicating that DHCP snooping was allowing legitimate traffic. I confirmed that the MAC and IP binding appeared in the DHCP snooping table, verifying the feature was working correctly.

The screenshot shows the CLI interface of a Cisco router. The command-line history is displayed in the terminal window, showing the configuration of DHCP snooping on interface F0/18. The configuration includes enabling DHCP snooping on VLAN 10, marking F0/1 as a trusted interface, and setting a rate limit of 5 DHCP messages per second on F0/18. The terminal also displays the output of the 'show ip dhcp snooping' command, which shows that DHCP snooping is enabled on VLAN 10 and provides a table of MAC-to-IP bindings. The taskbar at the bottom shows various Windows icons, and the system tray indicates the date and time as 12:16 PM on 6/8/2025.

```
%LINK-3-UPDOWN: Interface Vlan10, changed state to down
%LINK-5-CHANGED: Interface Vlan10, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, 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

s2>
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)#ip dhcp snooping fast
s2(config-if)#ip dhcp snooping trust
s2(config-if)#ip interface F0/18
s2(config-if)#ip dhcp snooping limit rate 5
s2(config-if)#
s2#
s2#SIS-5-CONFIG : Configured from console by console
s2#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
Interface          Trusted      Rate limit (pps)
FastEthernet0/1     yes         unlimited
FastEthernet0/18    no          5
s2#
```

Fig 2.8 implementing dhcp snooping security

```

S2 Physical Config CLI Attributes
IOS Command Line Interface

%LINK-5-CHANGED: Line protocol on interface Vlan10, changed state to up
%LINK-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

s2>
s2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
s2(config)#ip dhcp snooping
s2(config)#ip dhcp snooping vlan 10
s2(config)#interface f0/1
s2(config-if)#ip dhcp snooping trust
s2(config-if)#interface f0/18
s2(config-if)#ip dhcp snooping limit rate 5
s2(config-if)#Z
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
Inspection of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface      Trusted     Rate limit (pps)
FastEthernet0/1    yes      unlimited
FastEthernet0/18   no       5
s2#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
Inspection 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#

```

*Fig 2.9 verifying implemented dhcp snooping security*

### Implementing PortFast and BPDU guard.

To reduce startup delay for access ports, I enabled PortFast on the access interfaces in use (F0/5 and F0/6 on S1, F0/18 on S2). This allows ports to immediately enter the forwarding state, rather than wait through STP's learning/listening phases.

I also enabled BPDU Guard on the same access ports. This adds protection against rogue switches — if a BPDU is received on any of these ports, the port will automatically shut down to protect the spanning tree topology.

I verified both features using show spanning-tree interface detail, which showed that PortFast and BPDU Guard were enabled, and the ports were in forwarding state.

```

S1>
S1#en
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface range f0/6-6
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)#interface F0/18
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 FastEthernet0/18 but will only have effect when the interface is in a non-trunking mode.
S1(config-if)#interface F0/6
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#interface F0/18
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#
S1#
SYS-5-CONFIG_I: Configured from console by console
S1#show spanning-tree interface f0/6 detail

```

Top

Copy Paste

12:36 PM  
6/8/2025

Fig 3.0 Implementing portFast and bpdu guard

```

Port 6 (FastEthernet0/6) of VLAN018 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 129.6
  Designated root has priority 32778, address 0001.9728.58E6
  Designated bridge has priority 32778, address 0001.9728.58E6
  Designated port id is 128.6, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  State: listening (forwarding state)
  The port is in the portfast mode
  Link type is point-to-point by default

S1#

```

Top

Copy Paste

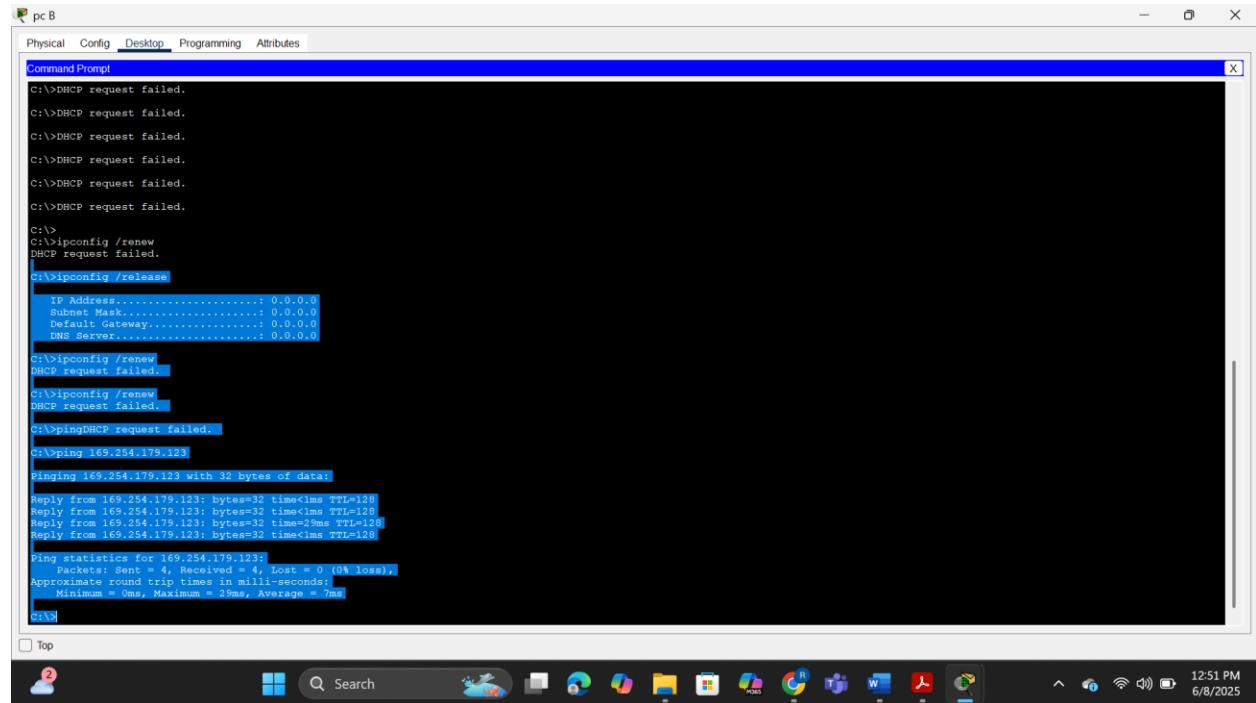
12:41 PM  
6/8/2025

Fig 3.1 Verifying implemented portFast and bpdu guard

## Verifying end-to-end connectivity.

Finally, I verified end-to-end IP connectivity by pinging from PC-A to PC-B, from both PCs to the router gateway (192.168.10.1), and from the switches to the loopback interface (10.10.1.1). All pings were successful.

This confirmed that VLANs, trunking, DHCP, and routing were properly configured, and security features did not interfere with legitimate traffic.



The screenshot shows a Windows Command Prompt window titled "pc B". The window contains the following command-line session:

```
C:\>ping -t 192.168.10.1
Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time<1ms TTL=128

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

The taskbar at the bottom of the window shows various pinned icons and the system clock indicating 12:51 PM on 6/8/2025.

fig 3.2 Pinging pc b from pc a

```

pc B
Physical Config Desktop Programming Attributes
Command Prompt
C:\>DHCP request failed.
C:\>
C:\>ipconfig /renew
DHCP request failed.
DHCP request failed.

C:\>DHCP request failed.

C:\>
C:\>
C:\>pingspi
Invalid Command.

C:\>
C:\>ping 169.254.179.123
pinging 169.254.179.123 with 32 bytes of data:
Reply from 169.254.179.123: bytes=32 time<1ms TTL=128
Ping statistics for 169.254.179.123:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

```

Fig 3.4 Pinging pc b from pc a

```

s2
Physical Config CLI Attributes
Verification of incoming traffic is enabled
IOS Command Line Interface
Interface          Trusted      Rate limit (pps)
FastEthernet0/1     yes         unlimited
FastEthernet0/0/8   no          5
s2#
s2>
s2>ccon0 is now available

Press RETURN to get started.

s2>en
s2#ping 192.168.10.201
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.201, timeout is 2 seconds:
!!!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

```

Fig 3.5 Pinging s1 from s2

```
s2 con0 is now available

Press RETURN to get started.

s2>en
s2#ping 192.168.10.201
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.201, timeout is 2 seconds:
.....!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms
s2#ping 192.168.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
.....!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
s2#
```

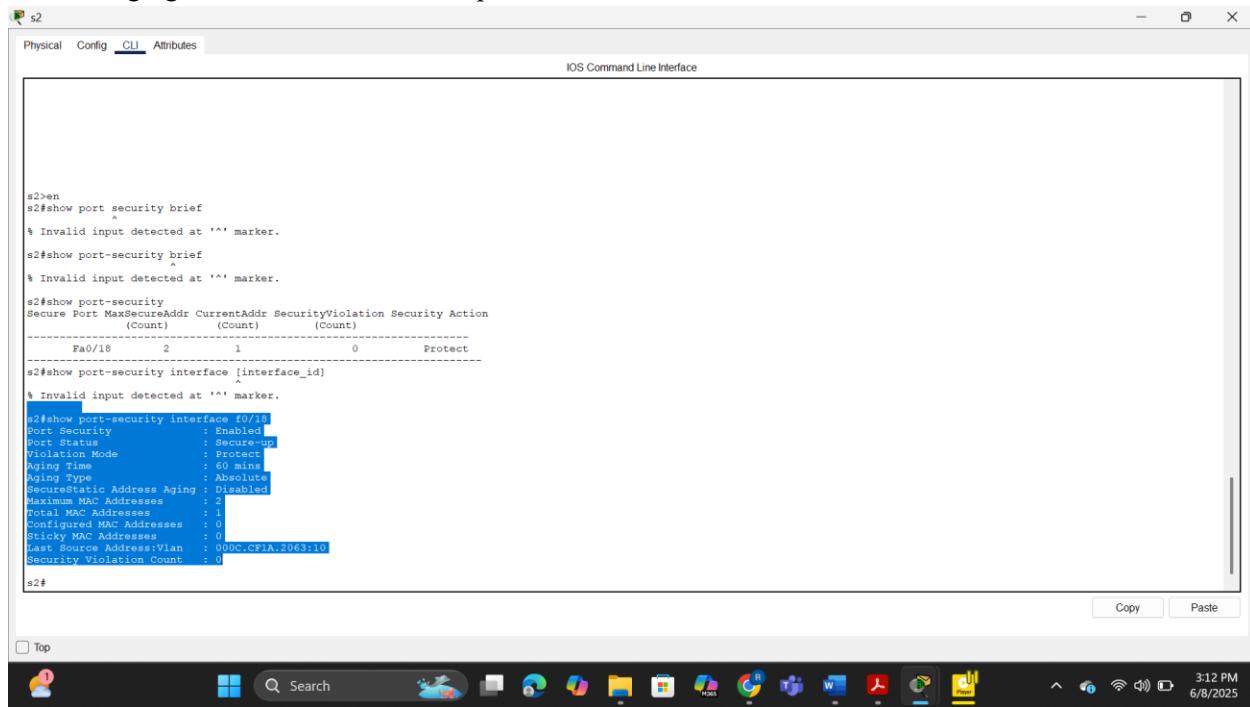
Fig 3.6 Pinging pc a from s2

## Reflection

While configuring port security with sticky MAC learning on S2 (specifically on interface F0/18), I noticed that the remaining age for the sticky MAC address did not show a timer value. This was an interesting discovery, and it helped me learn that sticky MAC addresses do not age out by default.

The aging mechanism does not apply unless explicitly configured for non-sticky secure dynamic addresses. Sticky MAC addresses are written into the running configuration and persist until manually removed or until the switch is rebooted — unless the sticky aging type is supported and enabled, which was not the case on this device.

So, I learned that not all switches support aging of sticky MACs, and even when sticky learning is enabled, aging behavior can be device-specific.



The screenshot shows a Windows Command Line Interface window titled "s2". The tab bar at the top has "Physical", "Config", "CLI" (which is selected), and "Attributes". Below the tabs is the text "IOS Command Line Interface". The main area of the window displays the following CLI session:

```
s2>en
s2#show port security brief
%
% Invalid input detected at '^' marker.

s2#show port-security brief
%
% Invalid input detected at '^' marker.

s2#show port-security
Secure Port MaxSeenAddr CurrentAddr SecurityViolation Security Action
(Count) (Count) (Count)
-----+-----+-----+-----+-----+
Fa0/18 2 1 0 Protect
s2#show port-security interface [interface_id]
%
% Invalid input detected at '^' marker.

s2#show port-security interface Fa0/18
Port Security : Enabled
Port Mode : Secure
Violation Mode : Protect
Aging Time : 60 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 2
Total MAC Addresses : 2
Current MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 000C.CF1A.2063:10
Security Violation Count : 0
s2#
```

At the bottom of the window are "Copy" and "Paste" buttons. The taskbar at the bottom of the screen shows various application icons, and the system tray indicates the date and time as 3:12 PM, 6/8/2025.

Fig 3.7 Port security interface

Why will PC-B on port F0/18 never get an IP address via DHCP if the running-config is reloaded?

This situation taught me a very valuable lesson about the interaction between port security and DHCP. When I reloaded the configuration on S2 and tried to reconnect PC-B to port F0/18, it couldn't obtain an IP address from the DHCP server.

After analyzing the settings, I realized that port security on F0/18 was configured with only two sticky MAC addresses, and the violation mode was set to protect. This meant any new device — or even the same PC with a changed NIC/MAC — would not be allowed to communicate on that port. Moreover, the protect mode silently drops unauthorized traffic without incrementing the violation counter or generating alerts, which made it less obvious at first.

The key lesson here was that port security can persist MAC bindings and quietly block traffic, especially with the protect violation mode. I must always remember to clear port security or increase the max MAC count before reconnecting or reconfiguring devices after a reload.

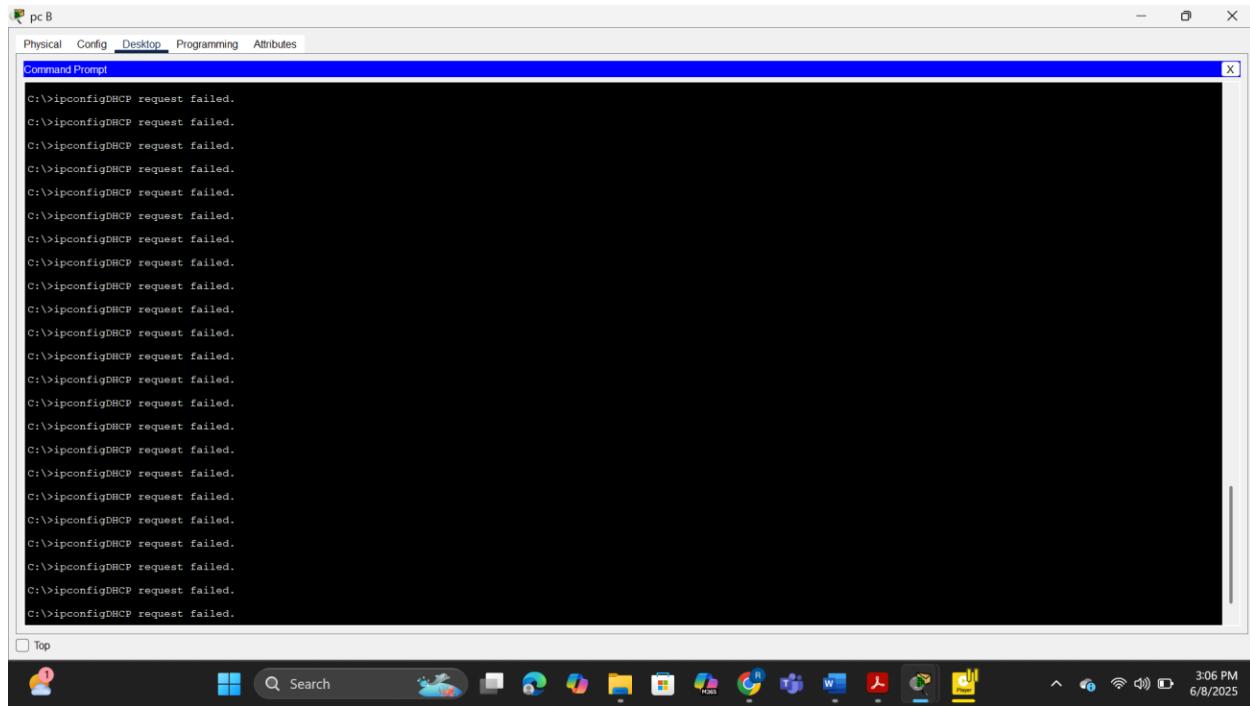


Fig 3.8 Pc b unable to be assigned ip

What is the difference between absolute aging type and inactivity aging type?

This question helped me deepen my understanding of port security aging types. In the lab, I had configured both types:

- Inactivity Aging (used on S1's F0/6): This method removes a secure MAC address only if there is no traffic from the device for the configured aging time (e.g., 60 minutes). It's useful in environments where devices may go idle for extended periods but should retain authorization while active.
- Absolute Aging (the default type): This removes the MAC address after a fixed time, regardless of activity. So even if the device is actively communicating, it will be aged out once the timer expires.

What I learned is that inactivity-based aging is more flexible and user-aware, while absolute aging is more rigid and time-based, potentially leading to service interruptions even for active devices. Choosing between them depends on the network environment and device behavior.

## Conclusion

This lab provided a vital opportunity to apply and reinforce key networking skills in a simulated enterprise environment. I successfully configured the router and switches, established secure trunk links, implemented VLAN segmentation, and enforced multiple security measures on switch ports to protect the network from unauthorized access and potential attacks. Through DHCP snooping and port security, I learned how to control IP address allocation and device authentication at the access layer. Additionally,

enabling PortFast and BPDU guard taught me how to safeguard the spanning-tree topology from rogue switches. Overall, this lab sharpened my configuration proficiency, deepened my understanding of secure Layer 2 practices, and prepared me for future challenges in network infrastructure design and protection.