

## Week 4 Assignment 1

Course: [Cloud and Network Security - C1-2026](#)

Student Name: [Bussllus Bertrand](#)

Student Number: [CS-CNS11-26004](#)

Thursday, February 12, 2026

**Week four Assignment one:**

**Class exercise: VLANs and Secure Switch Configuration**

## Contents

Introduction .....	2
Topology.....	3
Addressing Table .....	3
Objectives .....	4
Part 1: Configure the Network Devices. ....	4
Part 2: Configure VLANs on Switches. ....	4
Part 3: Configure Switch Security. ....	4
Background / Scenario .....	5
Instructions .....	5
Part 1: Configure the Network Devices. ....	5
Part 2: Configure VLANs on Switches. ....	11
Part 3: Configure Switch Security. ....	13
Reflection Questions .....	35
Conclusion .....	36

## Introduction

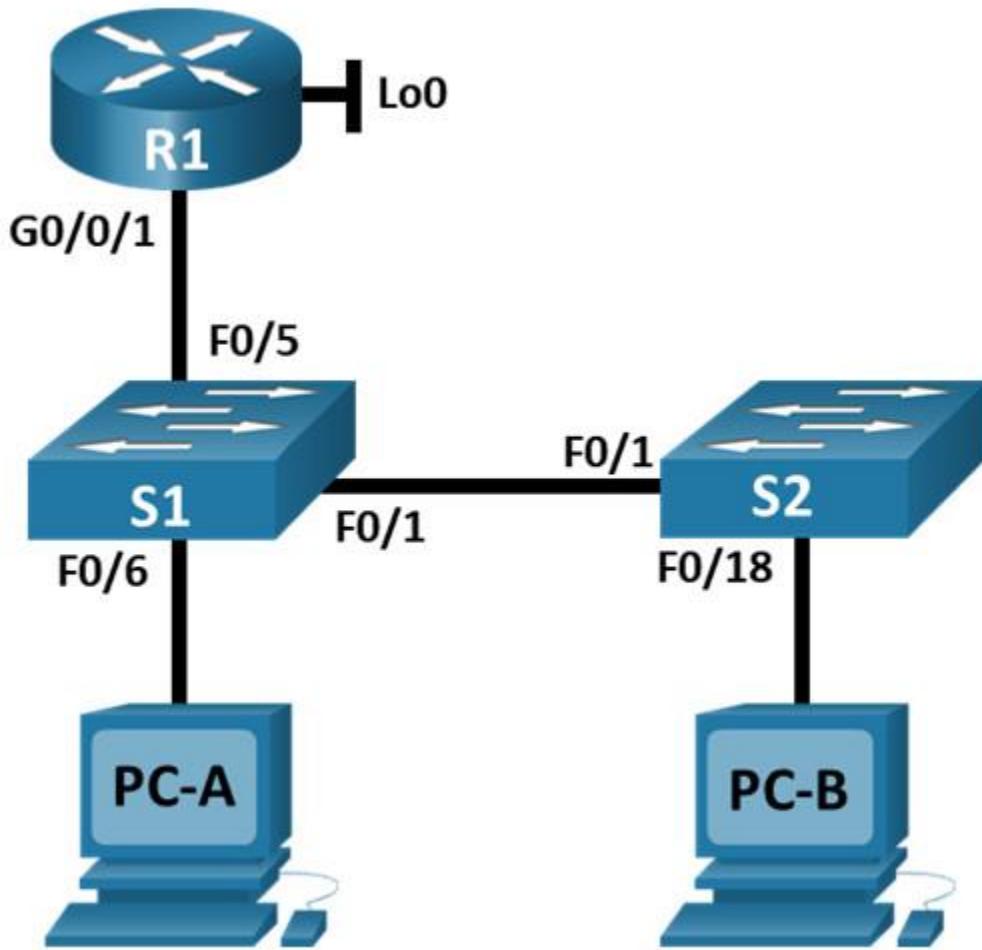
In this comprehensive lab, VLANs and Secure Switch Configuration, we focus on hardening Layer 2 network infrastructure by reviewing and implementing essential security features. The primary objective is to transform a basic network topology consisting of a router, switches, and workstations into a secure, segmented environment.

Throughout this exercise, we will move beyond initial device initialization to advanced configuration tasks. This includes the creation and management of VLANs to segment traffic, specifically establishing distinct Management, Native, and "Parking Lot" VLANs to organize and isolate network resources. A significant portion of this lab is dedicated to implementing robust

## Week 4 Assignment 1

switch security measures. We will configure 802.1Q trunking, secure access ports using Port Security features like sticky MAC addresses, and defend against common network attacks by deploying DHCP Snooping, PortFast, and BPDU Guard. By the end of this session, the network will be configured not just for connectivity, but for resilience against unauthorized access and Layer 2 vulnerabilities.

### Topology



### Addressing Table

Device	Interface / VLAN	IP Address	Subnet Mask
R1	G0/0/1	192.168.10.1	255.255.255.0
	Loopback 0	10.10.1.1	255.255.255.0

## Week 4 Assignment 1

Device	Interface / VLAN	IP Address	Subnet Mask
S1	VLAN 10	192.168.10.201	255.255.255.0
S2	VLAN 10	192.168.10.202	255.255.255.0
PC – A	NIC	DHCP	255.255.255.0
PC – B	NIC	DHCP	255.255.255.0

### 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.

## Week 4 Assignment 1

- Verify end-to-end-connectivity.

### Background / Scenario

This is a comprehensive lab to review previously covered Layer 2 security features.

**Note:** The routers used with CCNA hands-on labs are Cisco 4221 with Cisco IOS XE Release 16.9.3 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used.

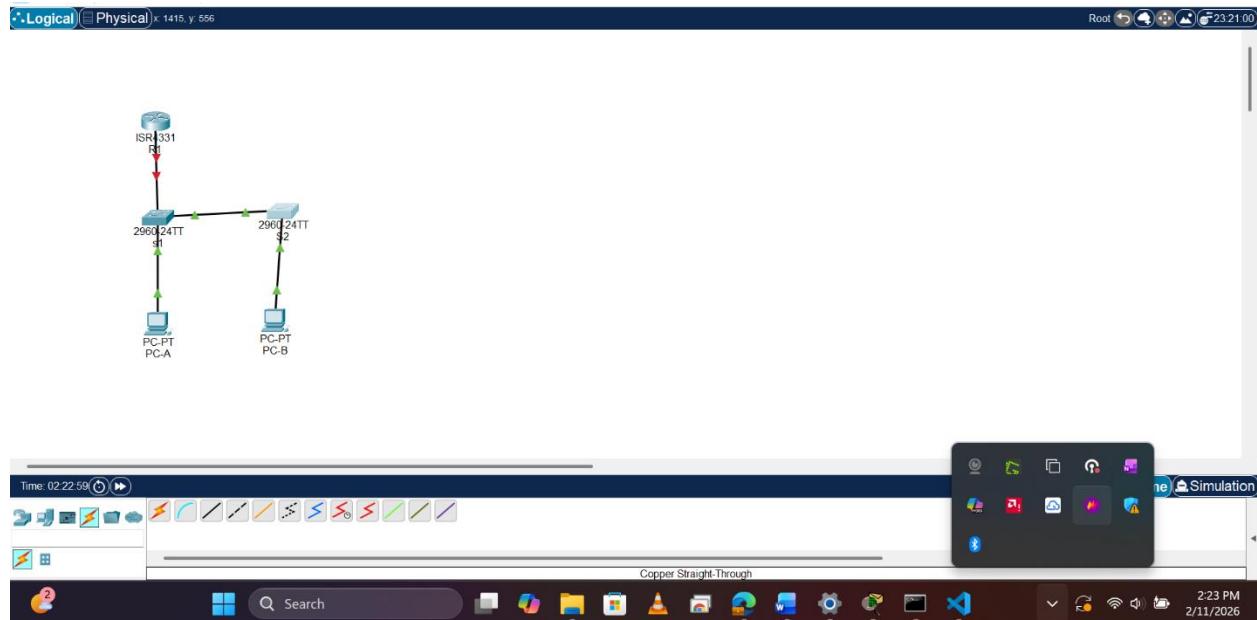
**Note:** Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

### Instructions

#### Part 1: Configure the Network Devices.

##### *Step 1: Cable the network.*

- Cable the network as shown in the topology.



- Initialize the devices.

##### *Step 2: Configure R1.*

- Load the following configuration script on R1.

```
enable
```

```
configure terminal
```

## Week 4 Assignment 1

```
hostname R1
no ip domain lookup
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.201 192.168.10.202
!
ip dhcp pool Students
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
domain-name CCNA2.Lab-11.6.1
!
interface Loopback0
ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet0/0/1
description Link to S1 Port 5
ip dhcp relay information trusted
ip address 192.168.10.1 255.255.255.0
no shutdown
!
line con 0
logging synchronous
exec-timeout 0 0
```

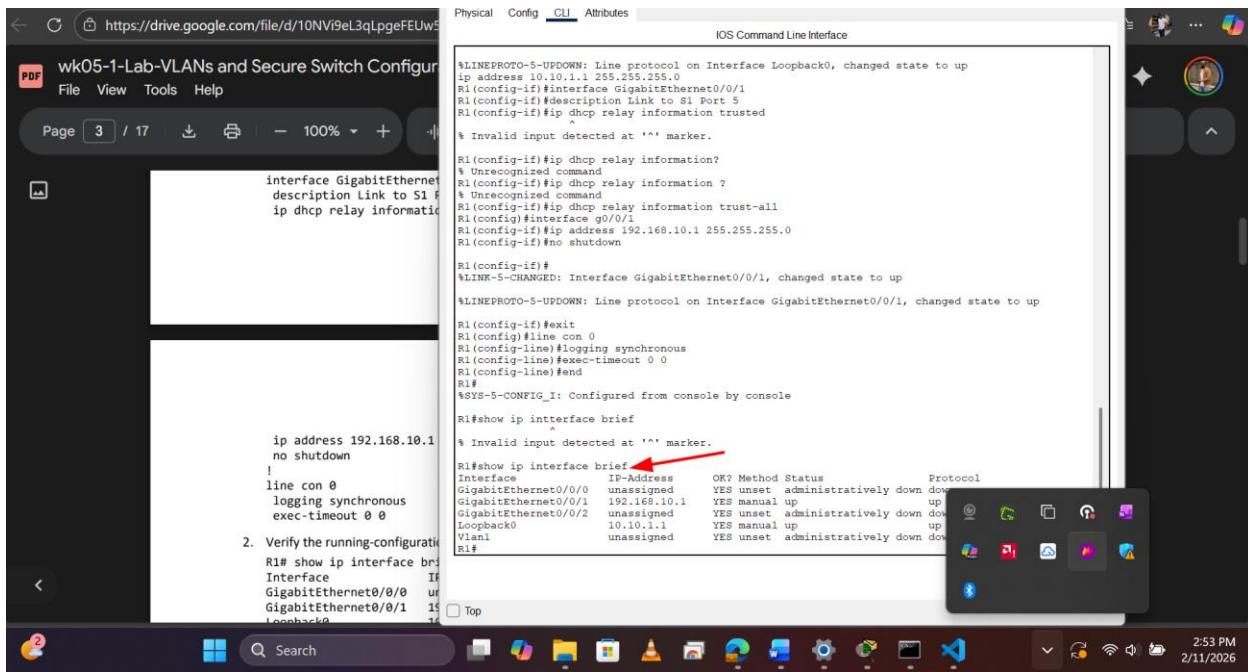
## Week 4 Assignment 1

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

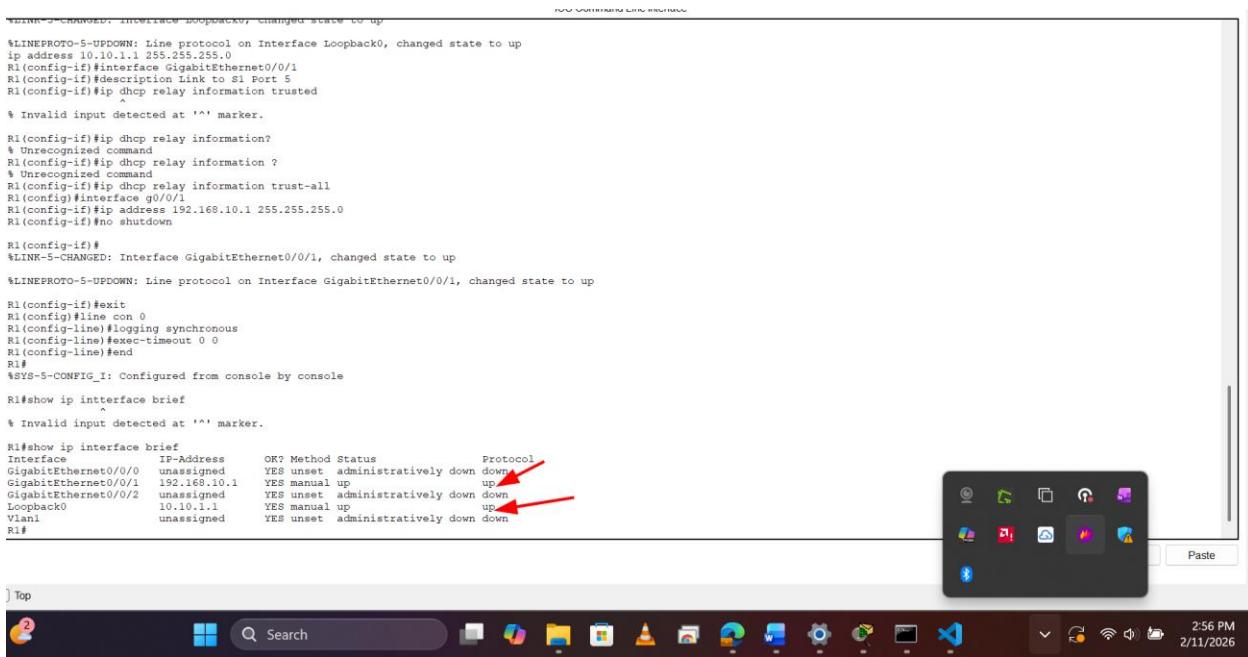
R1# show ip interface brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0/0	unassigned	YES	unset	down	down
GigabitEthernet0/0/1	192.168.10.1	YES	manual	up	up
Loopback0	10.10.1.1	YES	manual	up	up

## Week 4 Assignment 1



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



### *Step 3: Configure and verify basic switch settings.*

a. Configure the hostname for switches S1 and S2.

Switch# config t

Switch(config)# hostname S1

## Week 4 Assignment 1

Switch# config t

```
Switch(config)# hostname S2
```

b. Prevent unwanted DNS lookups on both switches.

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

```
S2(config)# no ip domain-lookup
```

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

## Week 4 Assignment 1

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

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

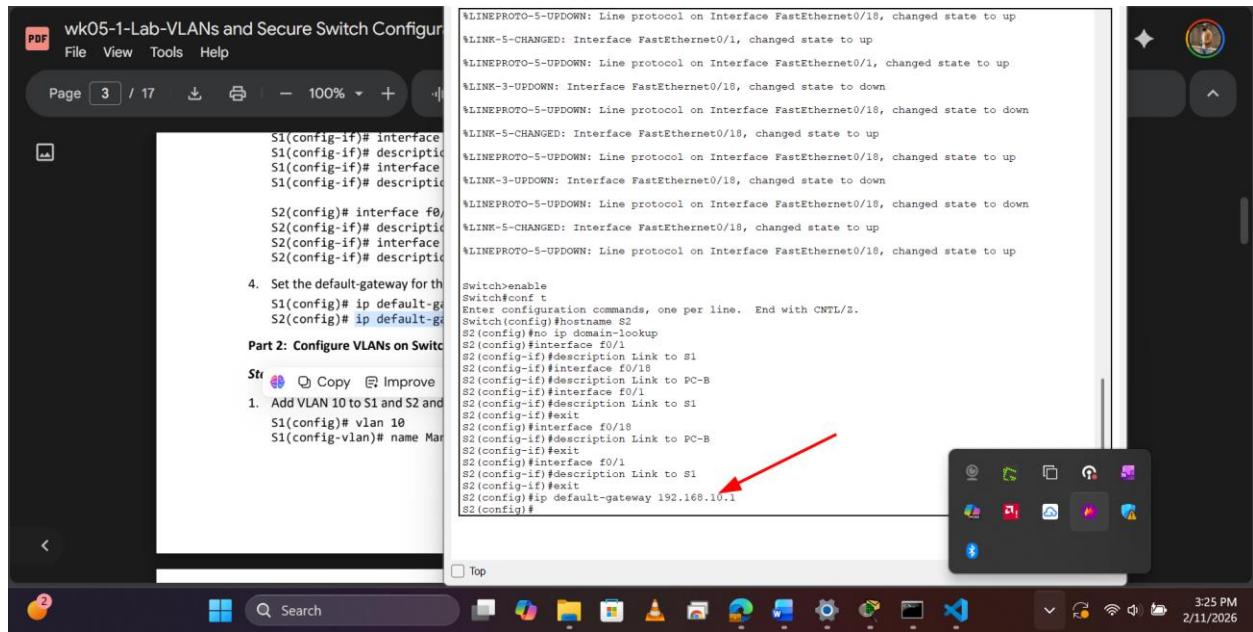
The screenshot shows a Mac desktop environment. A browser window is open to a Google Drive URL, displaying a PDF titled "wk05-1-Lab-VLANs and Secure Switch Configuration". The PDF contains configuration steps for two switches, S1 and S2. The terminal window is titled "IOS Command Line Interface" and shows the actual CLI commands being entered. The terminal session starts with the configuration mode of S2, followed by interface configurations for f0/1, f0/5, f0/18, and f0/6, each with a descriptive name. It also includes setting the default gateway for the Management VLAN. The terminal window has a dark theme, and the desktop background is a dark space-themed image.

d. 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

## Week 4 Assignment 1



The screenshot shows a Windows desktop environment. On the left, a PDF viewer window displays the first page of a document titled "wk05-1-Lab-VLANs and Secure Switch Configuration". The page contains configuration commands for two switches, S1 and S2, including interface descriptions and VLAN configurations. A red arrow points from the bottom right of the PDF window towards the taskbar. On the taskbar, there are several pinned icons for Microsoft applications like File Explorer, Edge, and Power BI, along with other standard icons for file operations and system status.

```
%LINK-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up  
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up  
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up  
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down  
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to down  
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up  
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up  
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down  
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to down  
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to up  
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up  
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down  
%LINKPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to down  
4. Set the default-gateway for the management interface.  
S1(config)# ip default-gateway 192.168.10.1  
S2(config)# ip default-gateway 192.168.10.1  
Part 2: Configure VLANs on Switches  
Str ⌂ Copy ⌂ Improve  
1. Add VLAN 10 to S1 and S2 and name the VLAN Management.  
S1(config)# vlan 10  
S1(config-vlan)# name Management  
S2(config)# vlan 10  
S2(config-vlan)# name Management  
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 192.168.10.1 255.255.255.0  
S2(config-if)# description Management SVI  
S2(config-if)# no shutdown
```

### Part 2: Configure VLANs on Switches.

#### Step 1: Configure VLAN 10.

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

```
S1(config)# vlan 10
```

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

```
S2(config)# vlan 10
```

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

#### Step 2: Configure the SVI for VLAN 10.

Configure the IP address according to the Addressing Table for SVI for VLAN 10 on S1 and S2.

Enable the SVI interfaces and provide a description for the interface.

```
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
```

## Week 4 Assignment 1

S2(config-if)# ip address 192.168.10.202 255.255.255.0

S2(config-if)# description Management SVI

S2(config-if)# no shutdown

wk05-1-Lab-VLANs and Secure Switch Configuration

Page 4 / 17

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch#hostname S1
S1(config)#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)#interface F0/1
S1(config-if)#description Link to S2
S1(config-if)#exit
S1(config)#interface F0/5
S1(config-if)#description Link to R1
S1(config-if)#exit
S1(config)#interface F0/6
S1(config-if)#description Link to PC-A
S1(config-if)#exit
S1(config-if)#ip default-gateway 192.168.10.1
S1(config-if)#name Management
S1(config-vlan)#name Management
S1(config-vlan)#exit
S1(config-if)#description Management SVI
S1(config-if)#no shutdown
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)#

```

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

S1(config)# vlan 333

S1(config-vlan)# name Native

S2(config)# vlan 333

S2(config-vlan)# name Native

*Step 4: Configure 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

## Week 4 Assignment 1

## Part 3: Configure Switch Security.

### *Step 1: Implement 802.1Q trunking.*

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

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
```

## Week 4 Assignment 1

The screenshot shows a Windows desktop environment. On the left, a PDF viewer window titled "wk05-1-Lab-VLANs and Secure Switch Configuration" is open, showing configuration steps for two switches (S1 and S2) including VLAN creation and security settings. On the right, a terminal window is running Cisco IOS commands. Red arrows point from the terminal window to specific lines of code: one arrow points to the command "switchport mode trunk" on S1, and another points to the command "switchport trunk native vlan 333" on S1. The terminal window also displays interface status messages like "LINEPROTO-5-UPDOWN". The taskbar at the bottom shows various application icons.

```
S2(config)# vlan 333
S2(config-vlan)# name Nat
Step 4: Configure VLAN 999
S1(config-vlan)# vlan 999
S1(config-vlan)# name Park

S2(config-vlan)# vlan 999
S2(config-vlan)# name Park

Part 3: Configure Switch Security
Step 1: Implement 802.1Q trunking
1. On both switches, configure trunking on interface F0/1
S1(config)# interface F0/1
S1(config-if)# switchport
S1(config-if)# switchport mode trunk

S2(config)# interface F0/1
S2(config-if)# switchport
S2(config-if)# switchport mode trunk

2. Verify that trunking is configured correctly
S1# show interface trunk
Port      Mode       Encapsulation  Status      Native vlan
Fa0/1    on        802.1q        trunking    333

S1# show interface trunk
Port      Vlans allowed on trunk
Fa0/1    1-4094

S1# show interface trunk
Port      Vlans allowed and active in management domain
Fa0/1    1,10,333,999

S1# show interface trunk
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1,10,333,999
```

b. Verify that trunking is configured on both switches.

**S1# show interface trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	333

Port Vlans allowed on trunk

Fa0/1 1-4094

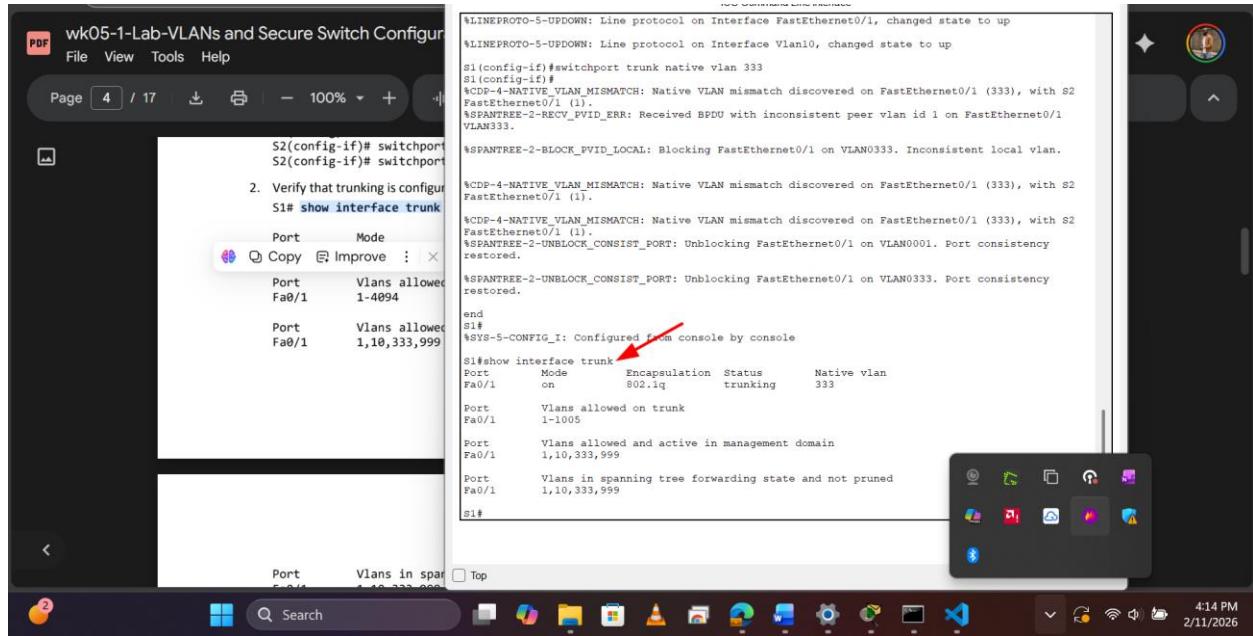
Port Vlans allowed and active in management domain

Fa0/1 1,10,333,999

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,10,333,999

## Week 4 Assignment 1



The screenshot shows a Windows desktop environment. A terminal window is open, displaying Cisco IOS configuration output. The output includes messages about line protocol changes, native VLAN mismatch errors, and port consistency restored. It also shows the result of the command `show interface trunk`. A red arrow points to the word "trunk" in the output. The taskbar at the bottom shows various application icons, and the system tray indicates the date and time as 4:14 PM on 2/11/2026.

```
%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
S1(config-if)#switchport
2. Verify that trunking is configured
S1# show interface trunk
Port      Mode          Encapsulation Status      Native vlan
Fa0/1    on           802.1q        trunking     333
Port      Vlans allowed on trunk
Fa0/1    1-4094
Port      Vlans allowed 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#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
S1(config-if)#switchport trunk native vlan 333
S1(config-if)#switchport
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2
FastEthernet0/1 (1).
%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlad id 1 on FastEthernet0/1
VLAN333.
%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0333. Inconsistent local vlan.
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2
FastEthernet0/1 (1).
%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0001. Port consistency
restored.
end
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#
```

**S2# show interface trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/1	on	802.1q	trunking	333

Port	Vlans allowed on trunk
Fa0/1	1-4094

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

## Week 4 Assignment 1

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 333 on FastEthernet0/1
%VLANI.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent local vlan.

%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-if)# switchport
S2(config-if)# switchport
2. Verify that trunking is configured
S1# show interface trunk
Port Mode
Port Vlans allowed
Fa0/1 1-4094
Port Vlans allowed
Fa0/1 1,10,333,999
S2# Copy ⌂ Improve : < >
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#

```

c. 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

```
%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent local vlan.

%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 f0/1
S2(config-if)# switchport mode trunk
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.

end
S2#
%SYS-5-CONFIG_I: Configured from console by console
S2#
S2#
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#
Step 2: Configure access ports.
1. On S1, configure F0/5 and F0/1
S1(config)# interface range f0/5-f0/1
S1(config-if)# switchport
S1(config-if)# switchport
2. On S2, configure F0/18 as an access port
S2(config)# interface f0/18
S2(config-if)# switchport
S2(config-if)# switchport
S2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
S2(config-if)#

```

## Week 4 Assignment 1

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

```
S1# show interfaces f0/1 switchport | include Negotiation
```

## Negotiation of Trunking: Off

wk05-1-Lab-VLANs and Secure Switch Configuration

File View Tools Help

Page 5 / 17

Fa0/1 1,10,333,999  
Port Vlans in spanning tree forwarding state and not pruned  
Fa0/1 1,10,333,999

Si#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Si(config)#interface f0/1  
Si(config-if)#switchport negotiate  
Si(config-if)#show interfaces f0/1 switchport

% Invalid input detected at '^' marker.

Si(config-if)#end  
Si#  
\$SYS-5-CONFIG\_I: Configured from console by console

Si#  
Si#  
Si#show interfaces f0/1 switchport  
Name: Fa0/1  
Switchport: Enabled  
Administrative Mode: trunk  
Operational Mode: trunk  
Administrative Trunking Encapsulation: dot1q  
Operational Trunking Encapsulation: dot1q  
Mode: Trunk  
Medium: Unknown  
Access Mode VLAN 1 (Native)  
Trunking Native Mode VLAN: 333 (Native)  
Voice VLAN: none  
Administrative private-vlan host-association: none  
Administrative private-vlan mapping: none  
Administrative private-vlan trunk native VLAN: none  
Administrative private-vlan trunk encapsulation: dot1q  
Administrative private-vlan trunk normal VLANs: none  
Administrative private-vlan trunk private VLANs: none  
Operational private-vlan: none  
Trunking VLANs Enabled: All  
Port Trunking Enabled: 2-1001  
Capture Mode Disabled  
Capture VLANs Allowed: ALL  
Protected: false  
--More--

Copy Improve

Step 2: Configure access ports.

1. On S1, configure F0/5 and F0/1  
S1(config)# interface range f0/5-1  
S1(config-if)# switchport  
S1(config-if)# switchport

2. On S2, configure F0/18 as an access port  
S2(config)# interface f0/18  
S2(config-if)# switchport

Top

S2# show interfaces f0/1 switchport | include Negotiation

## Negotiation of Trunking: Off

wk05-1-Lab-VLANs and Secure Switch Configuration

File View Tools Help

Page 5 / 17

S2>conf t  
% Invalid input detected at '^' marker.

S2>enable

S2#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
S2(config)#end

S2#  
\$SYS-5-CONFIG\_I: Configured from console by console

S2#  
S2#  
\$#show interfaces Fa0/1 switchport  
Name: Fa0/1  
Switchport: Enabled  
Administrative Mode: trunk  
Operational Mode: trunk  
Administrative Trunking Encapsulation: dot1q  
Operational Trunking encapsulation: dot1q  
Negotiation of Trunking: Off (highlighted)

Access Mode VLAN: 1 (default)  
Trunking Native Mode VLAN: 333 (Native)  
Voice VLAN: none  
Administrative private-vlan host-association: none  
Administrative private-vlan mapping: none  
Administrative private-vlan trunk native VLAN: none  
Administrative private-vlan trunk encapsulation: dot1q  
Administrative private-vlan trunk normal VLANs: none  
Administrative private-vlan trunk private VLANs: none  
Operational private-vlan: none  
Trunking VLANs Enabled: ALL  
Private VLAN Mapping: z=1001  
Capture Mode Disabled  
Capture VLANs Allowed: ALL  
Protected: false  
--More--

Step 2: Configure access ports.

1. On S1, configure Fa0/5 and Fa0/6 as trunk ports.  
S1(config)# interface range Fa0/5-6  
S1(config-if)# switchport  
S1(config-if)# switchport

2. On S2, configure Fa0/18 as an access port.  
S2(config)# interface Fa0/18  
S2(config-if)# switchport

Copy Improve : X

Top



4:42 PM  
2/11/2026

## Week 4 Assignment 1

### Step 2: Configure access ports.

- On S1, configure 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, configure 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
```

```
wk05-1-Lab-VLANs and Secure Switch Configuration
File View Tools Help
Page 5 / 17
S2>enable
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#end
S2#
4SIS-5-CONFIG_I: Configured from console by console
S2#
S2#
S2#show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 333 (Native)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 2-1001
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

4. Verify with the show interface
S1# show interfaces f0/1
Negotiation of Trunking:
S2# show interfaces f0/1
Negotiation of Trunking:
Step 2: Configure access ports.
1. On S1, configure F0/5 and F0/6
S1(config)# interface range f0/5-6
S1(config-if)# switchport
S1(config-if)# switchport
2. On S2, configure F0/18 as an access port
S2(config)# interface f0/18
S2(config-if)# switchport
S2(config-if)# switchport
Step 3: Secure and disable unused ports
1. On S1, copy and impr
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 f0/1-17
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 10
S2(config-if-range)# shutdown

S2>conf t
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)#
```

### Step 3: Secure and disable unused switchports.

- On S1 and S2, move the unused ports from VLAN 1 to VLAN 999 and disable the unused ports.

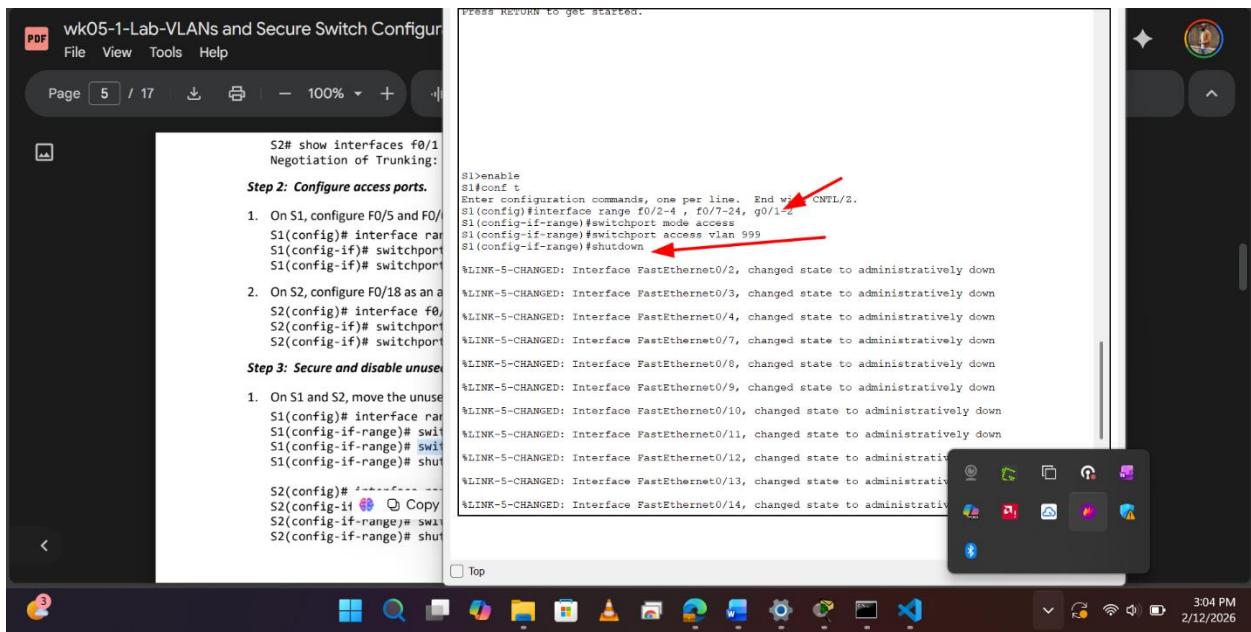
```
S1(config)# interface range f0/2-4 , f0/7-24, g0/1-2
```

```
S1(config-if-range)# switchport mode access
```

```
S1(config-if-range)# switchport access vlan 999
```

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

## Week 4 Assignment 1



S2# show interfaces f0/1  
Negotiation of Trunking:

**Step 2: Configure access ports.**

1. On S1, configure F0/5 and F0/19-24:  
S1(config)# interface range f0/5-19, f0/24, g0/1-2  
S1(config-if-range)# switchport mode access  
S1(config-if-range)# switchport access vlan 999  
S1(config-if-range)# shutdown
2. On S2, configure F0/18 as an access port:  
S2(config)# interface f0/18  
S2(config-if)# switchport mode access  
S2(config-if)# switchport access vlan 999

**Step 3: Secure and disable unused ports.**

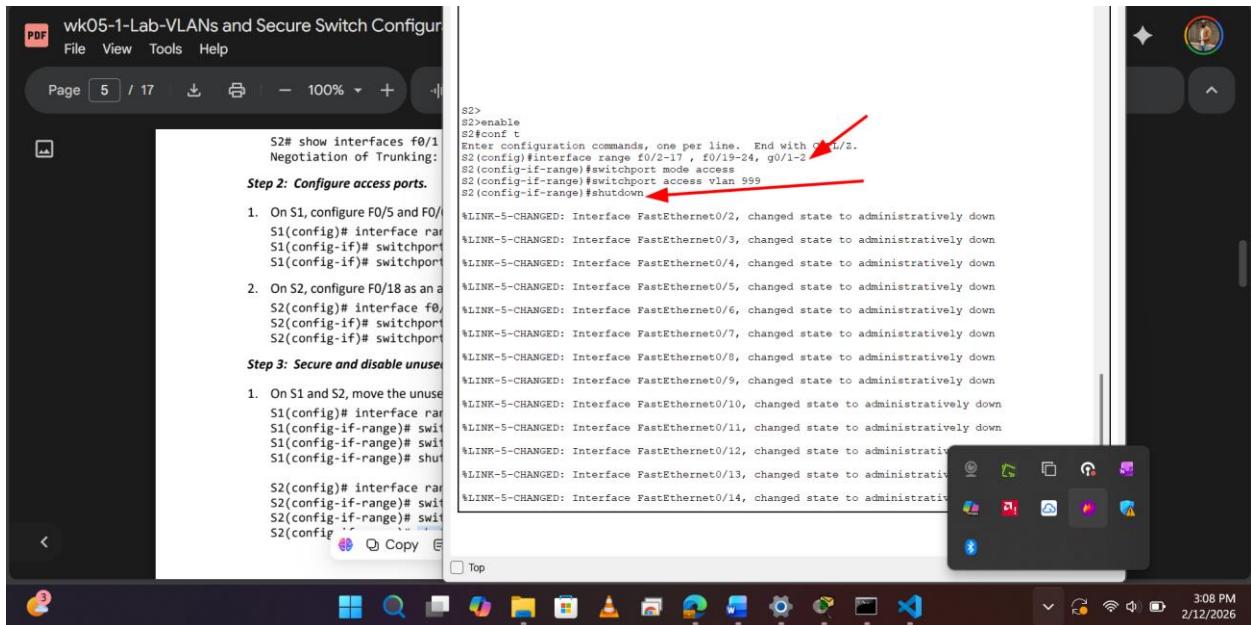
1. On S1 and S2, move the unused ports to shutdown:  
S1(config)# interface range f0/2-17, f0/19-24, g0/1-2  
S1(config-if-range)# switchport mode access  
S1(config-if-range)# switchport access vlan 999  
S1(config-if-range)# shutdown  
S2(config)# interface range f0/2-17, f0/19-24, g0/1-2  
S2(config-if-range)# switchport mode access  
S2(config-if-range)# switchport access vlan 999  
S2(config-if-range)# shutdown

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



S2# show interfaces f0/1  
Negotiation of Trunking:

**Step 2: Configure access ports.**

1. On S1, configure F0/5 and F0/19-24:  
S1(config)# interface range f0/5-19, f0/24, g0/1-2  
S1(config-if-range)# switchport mode access  
S1(config-if-range)# switchport access vlan 999  
S1(config-if-range)# shutdown
2. On S2, configure F0/18 as an access port:  
S2(config)# interface f0/18  
S2(config-if)# switchport mode access  
S2(config-if)# switchport access vlan 999

**Step 3: Secure and disable unused ports.**

1. On S1 and S2, move the unused ports to 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

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

## Week 4 Assignment 1

### S1# show interfaces status

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1	Link to S2	connected	trunk	a-full	a-100	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	a-full	a-100	10/100BaseTX
Fa0/6	Link to PC-A	connected	10	a-full	a-100	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

<output omitted>

The screenshot shows a Microsoft Word document with a red arrow pointing from the text "S1# show interfaces status" to the corresponding command output. The output displays the status of various interfaces on a Cisco router, including Fa0/1 through Fa0/10, Fa0/12 through Fa0/21, and Fa0/23 through Fa0/25. The document also includes configuration commands like %LINK-5-CHANGED and %SYS-5-CONFIG\_I, and a note about being configured from the console.

```
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%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
S1(config-if-range)#
S1(config-if-range)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

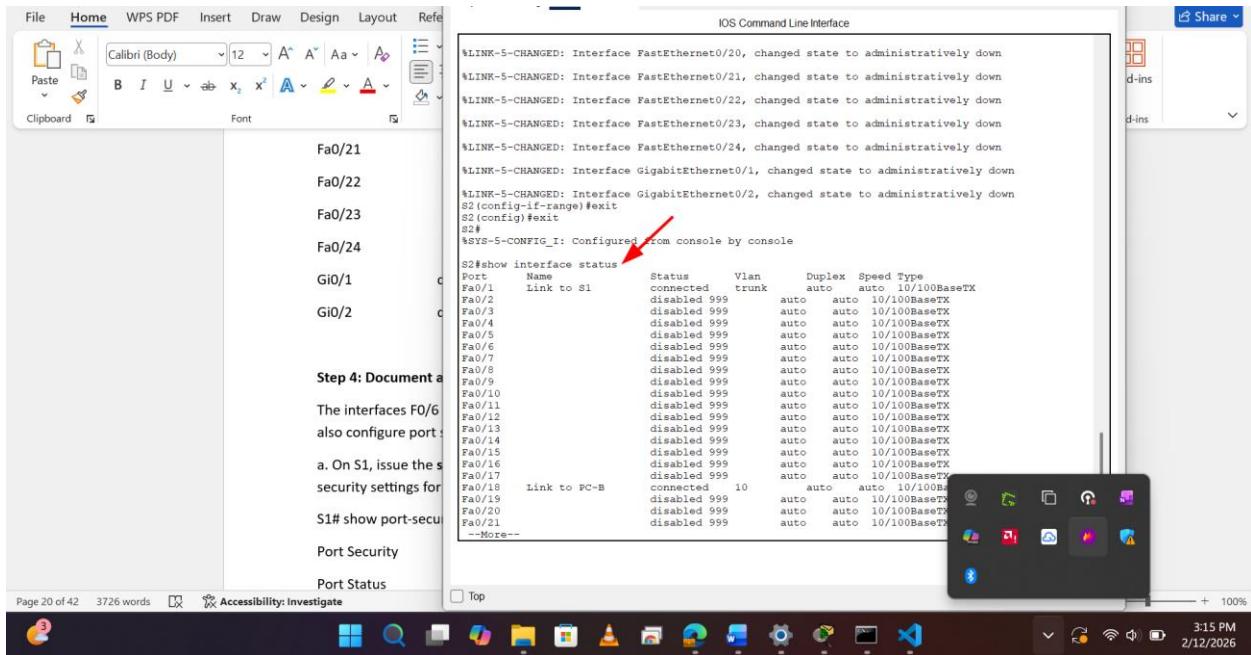
S1#show interfaces status
Port      Name           Status      Vlan      Duplex    Speed   Type
Fa0/1     Link to S2    connected   trunk    auto     auto   10/100BaseTX
Fa0/2     disabled      999       auto     auto   10/100BaseTX
Fa0/3     disabled      999       auto     auto   10/100BaseTX
Fa0/4     disabled      999       auto     auto   10/100BaseTX
Fa0/5     Link to R1    connected   10      auto     auto   10/100BaseTX
Fa0/6     Link to PC-A   connected   10      auto     auto   10/100BaseTX
Fa0/7     disabled      999       auto     auto   10/100BaseTX
Fa0/8     disabled      999       auto     auto   10/100BaseTX
Fa0/9     disabled      999       auto     auto   10/100BaseTX
Fa0/10    disabled      999       auto     auto   10/100BaseTX
Fa0/11    disabled      999       auto     auto   10/100BaseTX
Fa0/12    disabled      999       auto     auto   10/100BaseTX
Fa0/13    disabled      999       auto     auto   10/100BaseTX
Fa0/14    disabled      999       auto     auto   10/100BaseTX
Fa0/15    disabled      999       auto     auto   10/100BaseTX
Fa0/16    disabled      999       auto     auto   10/100BaseTX
Fa0/17    disabled      999       auto     auto   10/100BaseTX
Fa0/18    disabled      999       auto     auto   10/100BaseTX
Fa0/19    disabled      999       auto     auto   10/100BaseTX
Fa0/20    disabled      999       auto     auto   10/100BaseTX
Fa0/21    disabled      999       auto     auto   10/100BaseTX
--More--
```

### S2# show interfaces status

## Week 4 Assignment 1

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1	Link to S1	connected	trunk	a-full	a-100	10/100BaseTX
Fa0/2		disabled	999	auto	auto	10/100BaseTX
Fa0/3		disabled	999	auto	auto	10/100BaseTX
<output omitted>						
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	a-full	a-100	10/100BaseTX
Fa0/19		disabled	999	auto	auto	10/100BaseTX
Fa0/20		disabled	999	auto	auto	10/100BaseTX
Fa0/21		disabled	999	auto	auto	10/100BaseTX
Fa0/22		disabled	999	auto	auto	10/100BaseTX
Fa0/23		disabled	999	auto	auto	10/100BaseTX
Fa0/24		disabled	999	auto	auto	10/100BaseTX
Gi0/1		disabled	999	auto	auto	10/100/1000BaseTX
Gi0/2		disabled	999	auto	auto	10/100/1000BaseTX

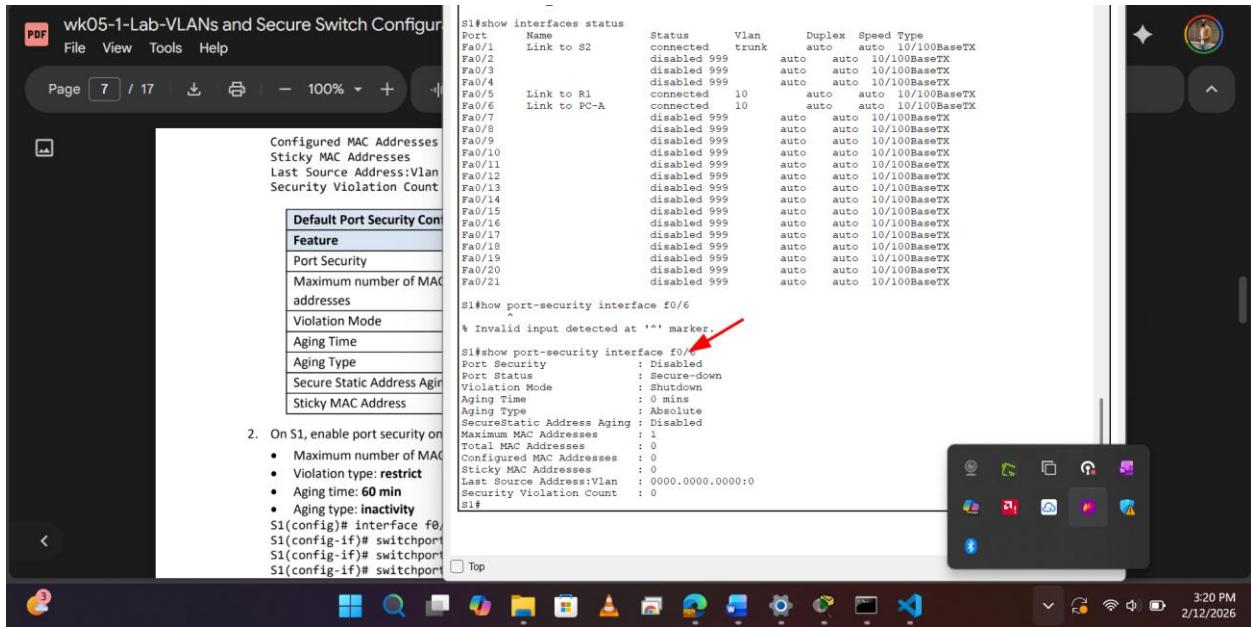
# Week 4 Assignment 1



## Step 4: 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, you will also configure port security on these two access ports.

- On S1, issue the **show port-security interface f0/6** command to display the default port security settings for interface F0/6. Record your answers in the table below.



S1# show port-security interface f0/6

Port Security : Disabled

## Week 4 Assignment 1

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

Default Port Security Configuration	
Feature	Default Setting
Port Security	Disabled
Maximum number of MAC addresses	1
Violation Mode	Shutdown
Aging Time	0 mins
Aging Type	Absolute
Secure Static Address Aging	Disabled
Sticky MAC Address	0

b. On S1, enable port security on F0/6 with the following settings:

- Maximum number of MAC addresses: 3

## Week 4 Assignment 1

- Violation type: **restrict**
- Aging time: **60 min**
- Aging type: **inactivity**

```
S1(config)# interface f0/6
```

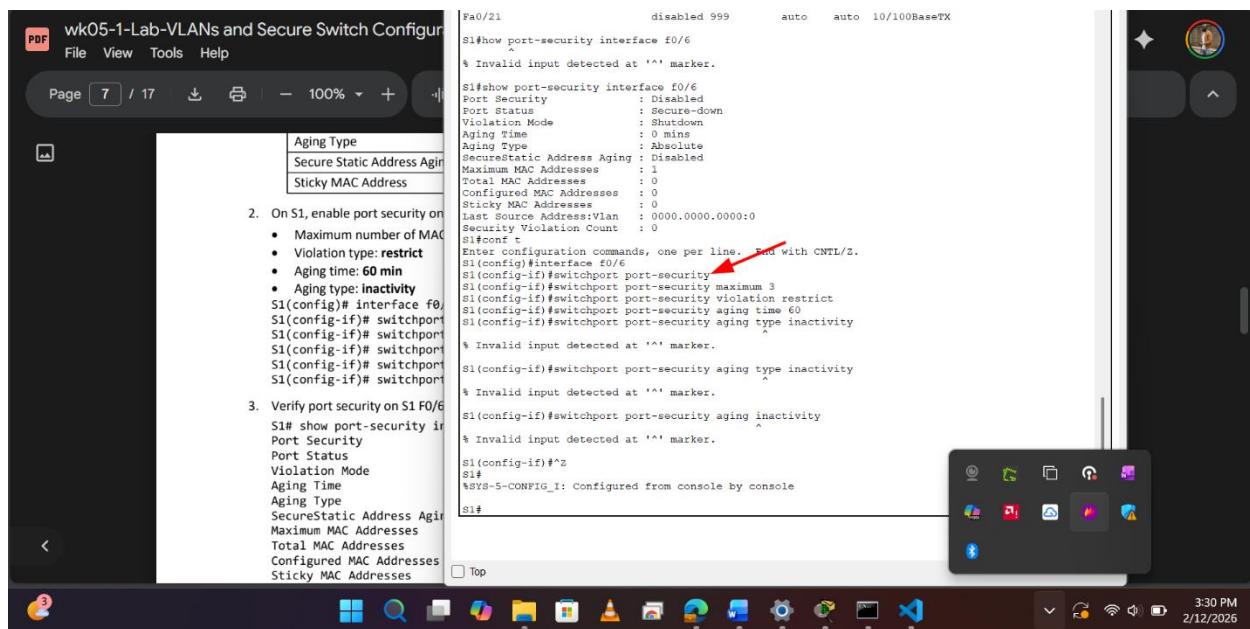
```
S1(config-if)# switchport port-security
```

```
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
```



```
Fa0/21           disabled 999      auto    auto  10/100BaseTX
S1#how port-security interface f0/6
% Invalid input detected at '^' marker.

S1#show port-security interface f0/6
Port Security       : Disabled
Port Status         : Secure-down
Violation Mode     : None
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#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#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.

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

S1(config-if)#^Z
S1#
$S73-5-CONFIG_I: Configured from console by console

S1#
```

c. Verify port security on S1 F0/6.

```
S1# show port-security interface f0/6
```

Port Security : Enabled

Port Status : Secure-up

Violation Mode : Restrict

Aging Time : 60 mins

Aging Type : Inactivity

## Week 4 Assignment 1

SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 3

Total MAC Addresses : 1

Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0022.5646.3411:10

Security Violation Count : 0

wk05-1-Lab-VLANs and Secure Switch Configuration Guide

Physical Config **CLI** Attributes

IOS Command Line Interface

```
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#^Z
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.
S1(config-if)#switchport port-security aging type inactivity
% Invalid input detected at '^' marker.
S1(config-if)#switchport port-security aging inactivity
% Invalid input detected at '^' marker.
S1(config-if)^Z
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 : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
S1#
```

S1# show port-security address

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
10	0022.5646.3411	SecureDynamic	Fa0/6	60 (I)

Total Addresses in System (excluding one mac per port) : 0

## Week 4 Assignment 1

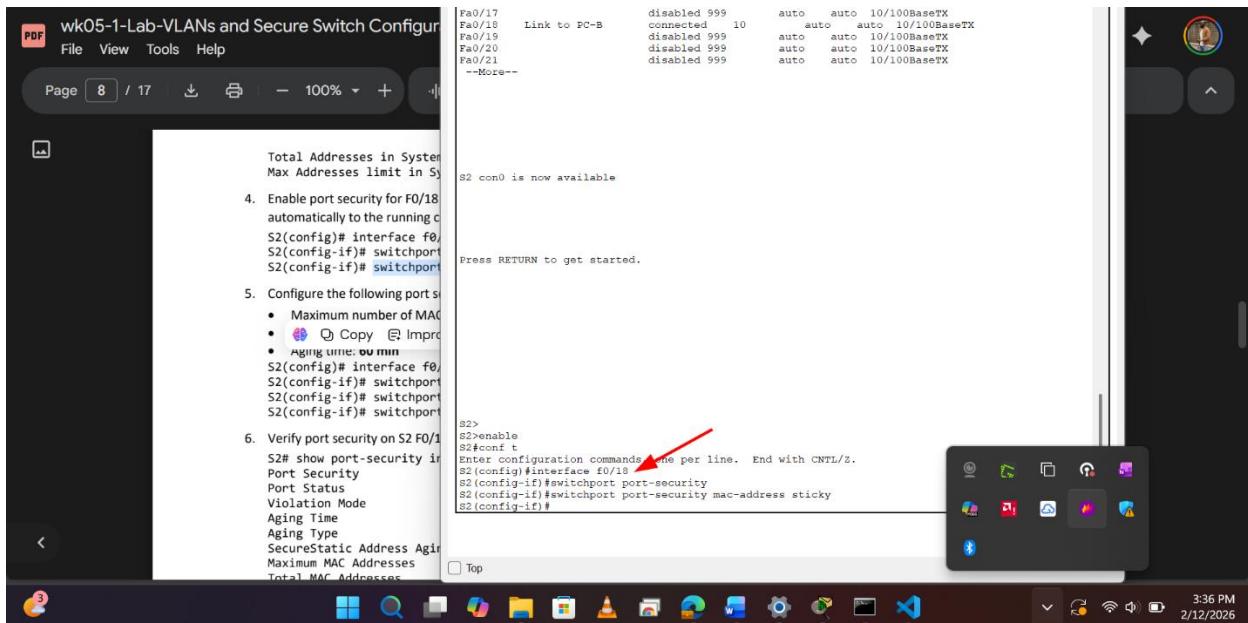
Max Addresses limit in System (excluding one mac per port) : 8192

d. 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
```



e. Configure the following port security settings on S2 F/18:

- Maximum number of MAC addresses: **2**
- Violation type: **Protect**
- Aging time: **60 min**

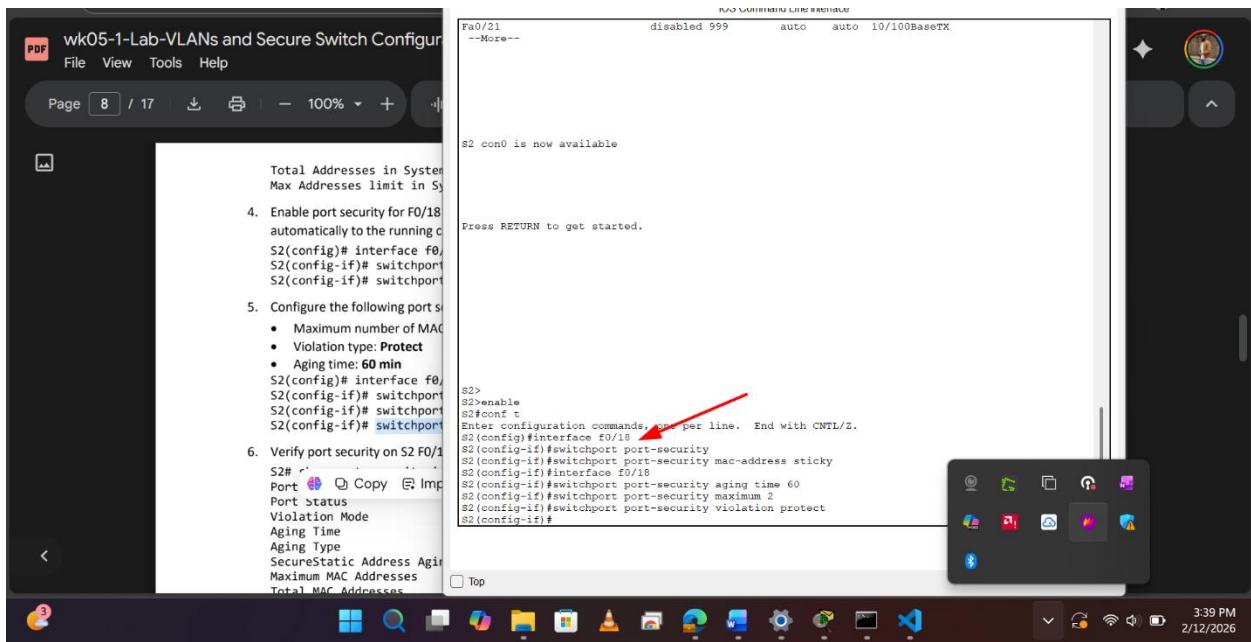
```
S2(config)# interface f0/18
```

```
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
```

## Week 4 Assignment 1



f. Verify port security on S2 F0/18.

**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 : 1

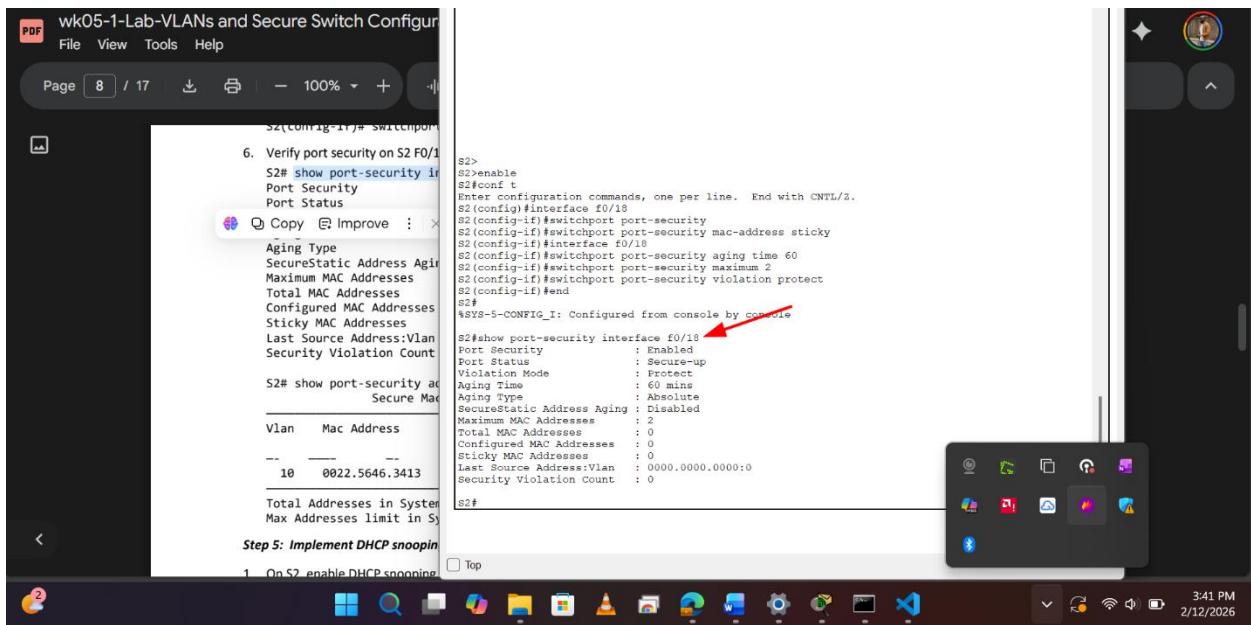
Configured MAC Addresses : 0

Sticky MAC Addresses : 0

Last Source Address:Vlan : 0022.5646.3413:10

Security Violation Count : 0

## Week 4 Assignment 1



```
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# show port-security address**

Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
10	0022.5646.3413	SecureSticky	Fa0/18	-

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 8192

### *Step 5: Implement DHCP snooping security.*

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

S2(config)# ip dhcp snooping

S2(config)# ip dhcp snooping vlan 10

## Week 4 Assignment 1

```
S2>
S2#enable
S2#conf t
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)#interface f0/18
S2(config-if)#switchport port-security aging time 60
S2(config-if)#switchport port-security maximum 2
S2(config-if)#switchport port-security violation protect
S2(config-if)#end
S2#
$SYS-5-CONFIG_I: Configured from console by console

Step 5: Implement DHCP snooping
1. On S2, enable DHCP snooping
S2(config)# ip dhcp snooping
S2(config)#
2. Configure the trunk port on S2
S2(config)# interface f0/18
S2(config-if)#
Copy Improve

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#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)#

Top
```

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

```
S2(config)# interface f0/1
```

```
S2(config-if)# ip dhcp snooping trust
```

```
S2>
S2#enable
S2#conf t
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)#interface f0/18
S2(config-if)#switchport port-security aging time 60
S2(config-if)#switchport port-security maximum 2
S2(config-if)#switchport port-security violation protect
S2(config-if)#end
S2#
$SYS-5-CONFIG_I: Configured from console by console

Step 5: Implement DHCP snooping
3. Limit the untrusted port, F18 on S2
S2(config)# interface f0/18
S2(config-if)#
4. Verify DHCP Snooping on S2.
S2# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on interface
  10
DHCP snooping is operational on interface
  10
DHCP snooping is configured on interface
  18
Insertion of option 82 is disabled
  circuit-id default for
    remote-id: 0cd9.96d2.3e
Option 82 on untrusted ports is disabled
Verification of hwaddr file
Verification of giaddr file
DHCP snooping trust/rate
Interface
  FastEthernet0/1
    Custom circuit-id: 0cd9.96d2.3e

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#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-if)#ip dhcp snooping trust
S2(config)#

Top
```

c. Limit 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
```

## Week 4 Assignment 1

PDF wk05-1-Lab-VLANs and Secure Switch Configuration

File View Tools Help

Page 9 / 17

S2>  
S2>enable  
S2#conf t  
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)#end  
S2#  
%SYS-5-CONFIG\_I: Configured from console by console

3. Limit the untrusted port, F18 c  
S2(config)# interface f0/  
S2(config-if)# ip dhcp s  
4. Verify DHCP Snooping on S2.  
S2# show ip dhcp snooping  
Swi 🖥 Copy ⌂ Impr  
DHCP snooping is enabled on 10  
DHCP snooping is operational on 10  
DHCP snooping is configured  
Insertion of option 82 is enabled  
circuit-id default for remote-id: 0cd9.96d2.3  
Option 82 on untrusted ports is disabled  
Verification of haddr is disabled  
Verification of giaddr is disabled  
DHCP snooping trust/rate

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  
Mac-to-IP 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#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 f0/18  
S2(config-if)#switchport port-security limit rate 5  
S2(config-if)#exit  
S2(config)#interface f0/18  
S2(config-if)#ip dhcp snooping limit rate 5  
S2(config-if)#

Interface

FastEthernet0/1

Custom circuit id:

Top



d. Verify DHCP Snooping on S2.

## S2# show ip dhcp snooping

Switch DHCP snooping is enabled

DHCP snooping is configured on following VLANs:

10

DHCP snooping is operational on following VLANs:

10

DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled

circuit-id default format: vlan-mod-port

remote-id: 0cd9.96d2.3f80 (MAC)

Option 82 on untrusted port is not allowed

Verification of hwaddr field is enabled

Verification of giaddr field is enabled

DHCP snooping trust/rate is configured on the following Interfaces:

## Week 4 Assignment 1

Interface	Trusted	Allow option	Rate limit (pps)
-----------	---------	--------------	------------------

FastEthernet0/1 yes yes unlimited

## Custom circuit-ids:

FastEthernet0/18 no no 5

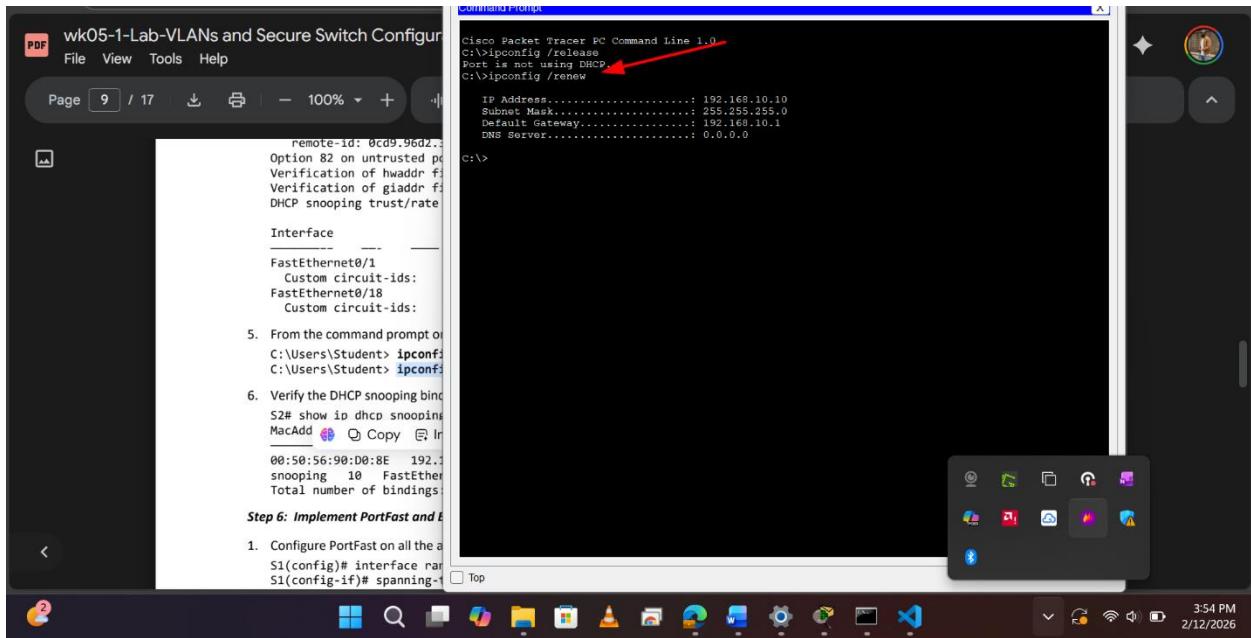
## Custom circuit-ids:

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

C:\Users\Student> ipconfig /release

C:\Users\Student> ipconfig /renew

## Week 4 Assignment 1



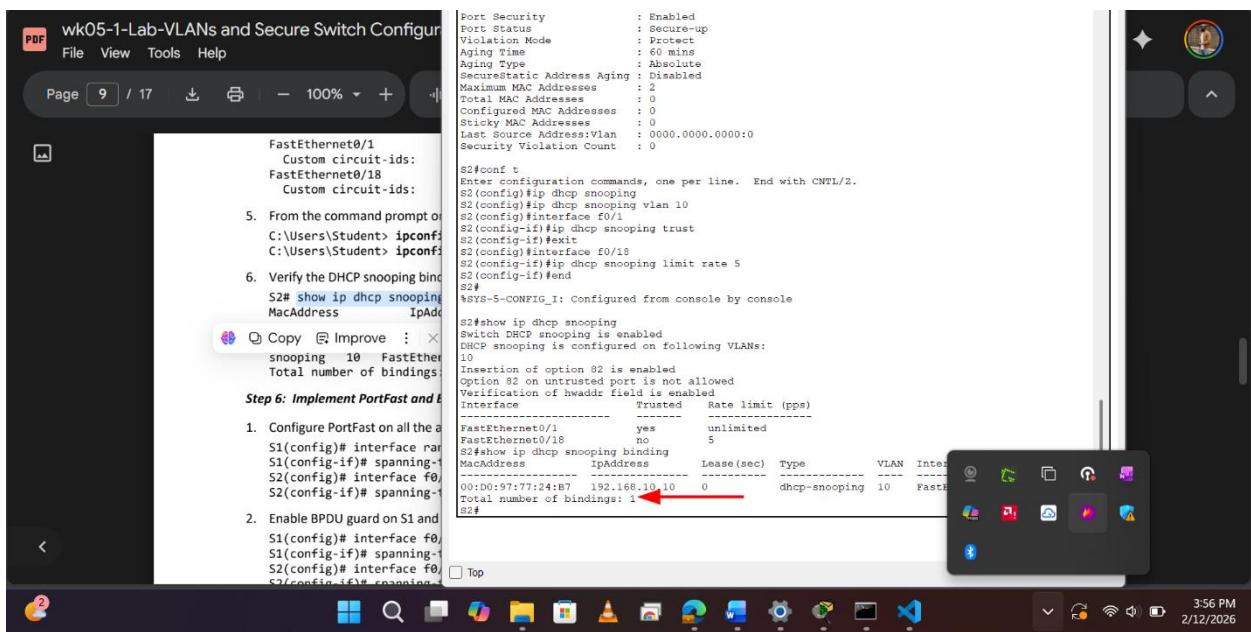
f. Verify the DHCP snooping binding using the **show ip dhcp snooping binding** command.

**S2# show ip dhcp snooping binding**

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
------------	-----------	------------	------	------	-----------

00:50:56:90:D0:8E 192.168.10.11 86213 dhcp-snooping 10 FastEthernet0/18

Total number of bindings: 1



## Week 4 Assignment 1

### Step 6: Implement PortFast and BPDU guard.

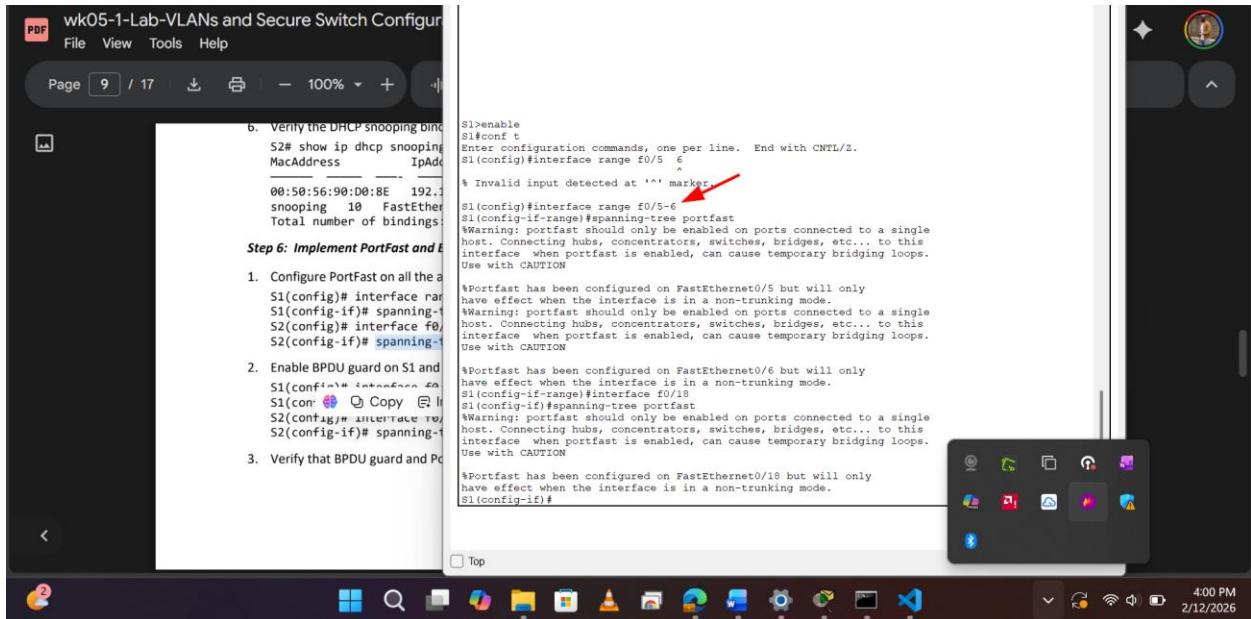
- Configure PortFast on all the access ports that are in use on both switches.

```
S1(config)# interface range f0/5-6
```

```
S1(config-if)# spanning-tree portfast
```

```
S2(config)# interface f0/18
```

```
S2(config-if)# spanning-tree portfast
```



- 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
```

## Week 4 Assignment 1

The screenshot shows a PDF document titled "wk05-1-Lab-VLANs and Secure Switch Configuration". The document contains several configuration steps and terminal logs. A red arrow points from the terminal log on the right to the configuration command "S1(config-if)# spanning-tree portfast" in the middle of the page.

**Step 6: Implement PortFast and BPDU Guard**

- b. Verify the DHCP snooping binding table:  
S2# show ip dhcp snooping binding  
MacAddress IpAddress  
00:56:90:D0:8E 192.168.1.10 FastEthernet0/5  
Total number of bindings: 1
1. Configure PortFast on all the appropriate interfaces:  
S1(config)# interface range f0/5-6  
S1(config-if)# spanning-tree portfast  
S2(config)# interface f0/0-18  
S2(config-if)# spanning-tree portfast
2. Enable BPDU guard on S1 and S2:  
S1(config)# interface f0/0-18  
S1(config-if)# spanning-tree bpduguard enable  
S2(config)# interface f0/0-18  
S2(config-if)# spanning-tree bpduguard enable
3. Verify that BPDU guard and PortFast are enabled on the appropriate ports:  
S1# show spanning-tree interface f0/6 detail

S1>enable  
S1>conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
S1(config)#interface range f0/5\_6  
% Invalid input detected at '^' marker.  
S1(config)#interface range f0/5-6  
S1(config-if-range)#spanning-tree portfast  
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops.  
Use with CAUTION  
%portfast has been configured on FastEthernet0/5 but will only have effect when the interface is in a non-trunking mode.  
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops.  
Use with CAUTION  
%portfast has been configured on FastEthernet0/6 but will only have effect when the interface is in a non-trunking mode.  
%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 portfast  
S1(config-if)#interface f0/18  
S1(config-if)#spanning-tree portfast  
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause temporary bridging loops.  
Use with CAUTION  
S1(config-if)#spanning-tree bpduguard enable  
S1(config-if)#interface f0/0-18  
S1(config-if)#spanning-tree bpduguard enable  
S1(config-if)#

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

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

Port 8 (FastEthernet0/6) of VLAN0010 is designated forwarding

Port path cost 19, Port priority 128, Port Identifier 128.6.

<output omitted for brevity>

Number of transitions to forwarding state: 1

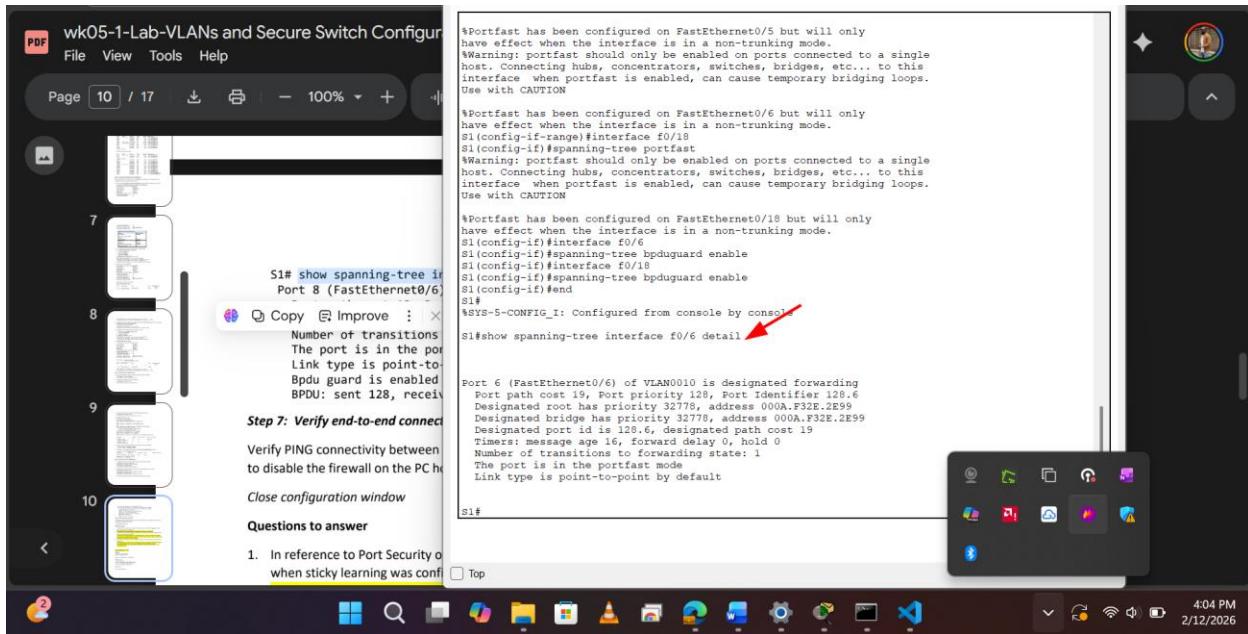
The port is in the portfast mode

Link type is point-to-point by default

Bpdu guard is enabled

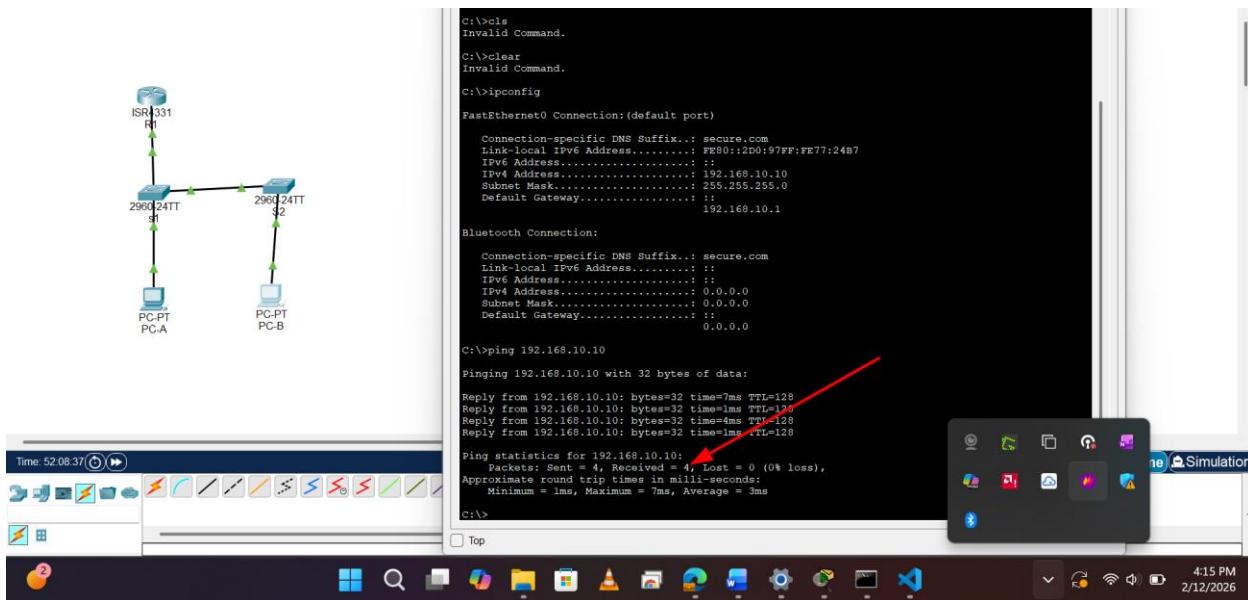
BPDU: sent 128, received 0

## Week 4 Assignment 1



### Step 7: Verify end-to-end connectivity.

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



## Reflection Questions

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.

## Week 4 Assignment 1

### **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

By completing this lab, we have successfully established a secure and optimized Layer 2 network environment. We demonstrated the importance of network segmentation by configuring specific VLANs for management and properly handling unused ports by moving them to a "Parking Lot" VLAN to prevent unauthorized access.

Critically, we reinforced the network's defenses through several key security implementations:

**Trunk Security:** We secured trunk links by manually configuring 802.1Q encapsulation and assigning a dedicated Native VLAN (VLAN 333) to mitigate VLAN hopping attacks.

**Access Control:** We implemented Port Security with specific violation modes (Restrict and Protect) and aging timers, ensuring that only authorized MAC addresses can communicate through the switch ports.

**Threat Mitigation:** We defended the network against DHCP spoofing and starvation attacks by configuring DHCP Snooping and rate-limiting untrusted ports.

**Topology Stability:** Finally, we enhanced the efficiency and security of the Spanning Tree Protocol by enabling PortFast and BPDU Guard on user-facing ports, preventing rogue switches from disrupting the network topology.

This lab confirms that applying these "defense-in-depth" strategies is essential for maintaining network integrity and preventing common LAN-based attacks.