SWITCH SECURITY CONFIGURATION REPORT

PACKET TRACER LAB

BY

YUNIS MOHAMED

Contents

Introduction

This packet tracer lab is designed to help practices and review the layer 2 security practices. Activities performed in this lab include designing of the topology, creating of vlans and assigning ports such as access ports and trunks ports to the respective vlan.switch and port security is the last task covered in this lab. This include implementing portfast and bpdu guards on ports to help secure them and prevent intruders from using the ports.

Part 1: Configure the Network Devices

Cable and design the topology

The first step was to design and cable the network topology with the given devices which include:

1 Router (Cisco 4221 with Cisco IOS XE Release 16.9.3 universal image or comparable) • 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable) • 2 PCs (Windows with a terminal emulation program, such as Tera Term) • Console cables to configure the Cisco IOS devices via the console ports.

The addressing table used is the one below.

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

The diagram of the designed topology is the one below.

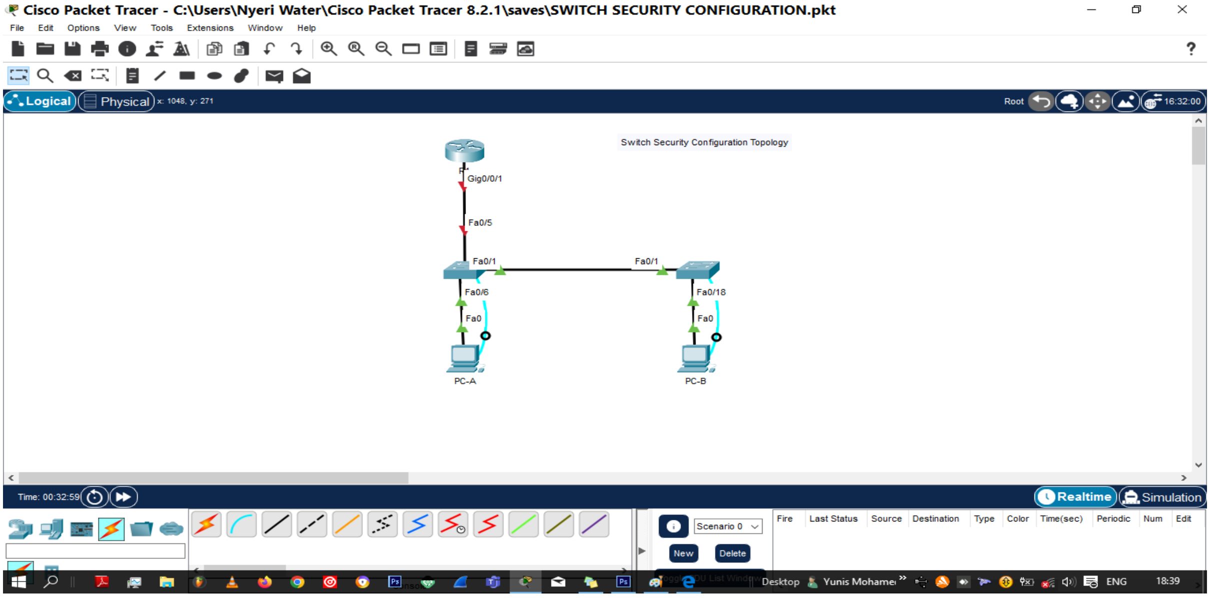
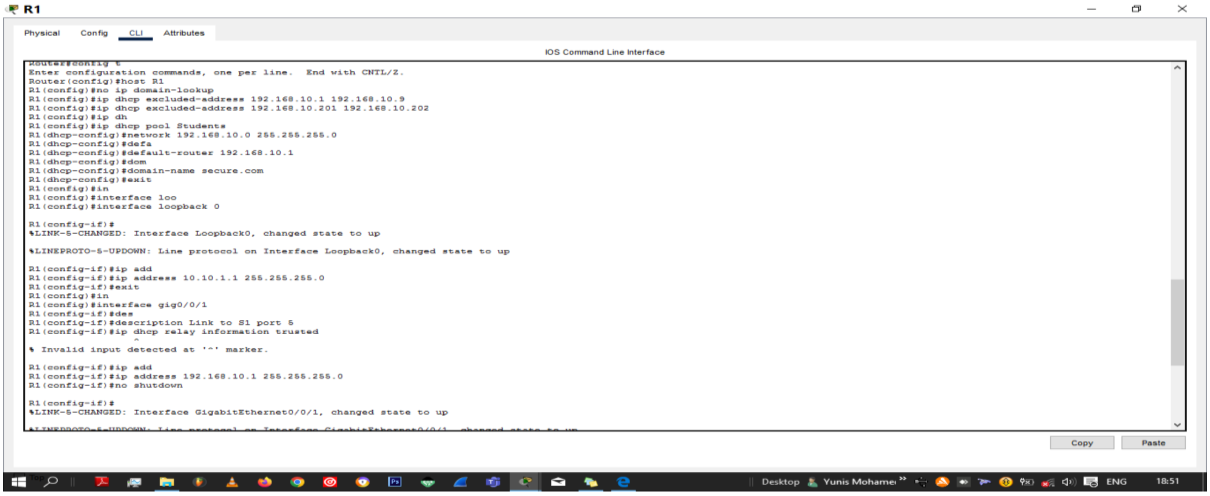


Figure 1 topology diagram

Configure the R1 Router

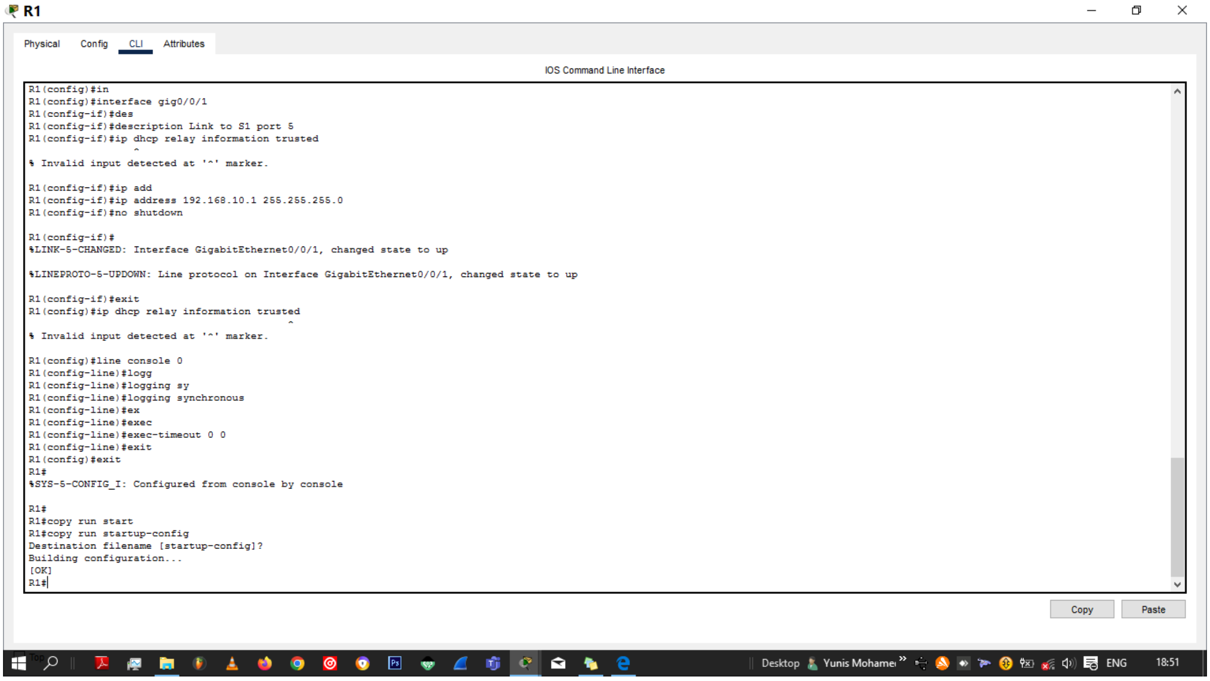
The second step was to configure the R1 router with the following:

1. Hostname R1.
2. Disable the IP domain-lookup.
3. Configure the router with DHCP with the following parameters so the devices can obtain IP addresses automatically: dhcp pool **Students,** network **192.168.10.0 255.255.255.0,** default-router **192.168.10.1,** domain-name secure.com.
4. Configure the loopback address: **10.10.1.1 255.255.255.0.**
5. Configure the IP DHCP relay information as trusted.
6. Turn up the GigabitEthernet0/0/1, configure its IP address and give it a description.
7. Secure the console line with logging synchronous and exec-timeout command.



```
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#host R1
R1(config)#no ip domain-lookup
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)#ip dhcp excluded-address 192.168.10.201 192.168.10.202
R1(config)#ip dh
R1(config)#ip dhcp pool Students
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#defa
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#dom
R1(dhcp-config)#domain-name secure.com
R1(dhcp-config)#exit
R1(config)#in
R1(config)#interface loo
R1(config)#interface loopback 0

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 add
R1(config-if)#ip address 10.10.1.1 255.255.255.0
R1(config-if)#exit
R1(config)#in
R1(config)#interface gig0/0/1
R1(config-if)#des
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 add
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
```

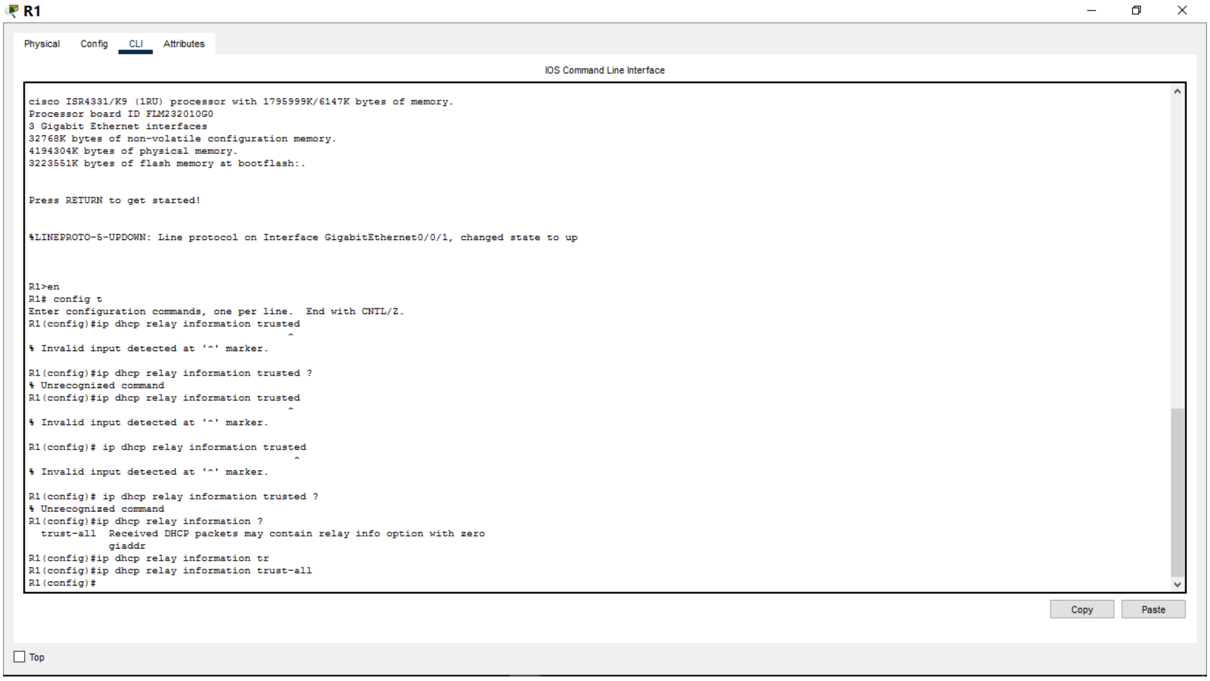
Figure 2 configure R1 (a)



```
R1(config)#in
R1(config)#interface gig0/0/1
R1(config-if)#des
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 add
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R1(config-if)#exit
R1(config)#ip dhcp relay information trusted
                                          ^
% Invalid input detected at '^' marker.

R1(config)#line console 0
R1(config-line)#logg
R1(config-line)#logging sy
R1(config-line)#logging synchronous
R1(config-line)#ex
R1(config-line)#exec
R1(config-line)#exec-timeout 0 0
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
R1#copy run start
R1#copy run startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Figure 3 configure R1 (b)

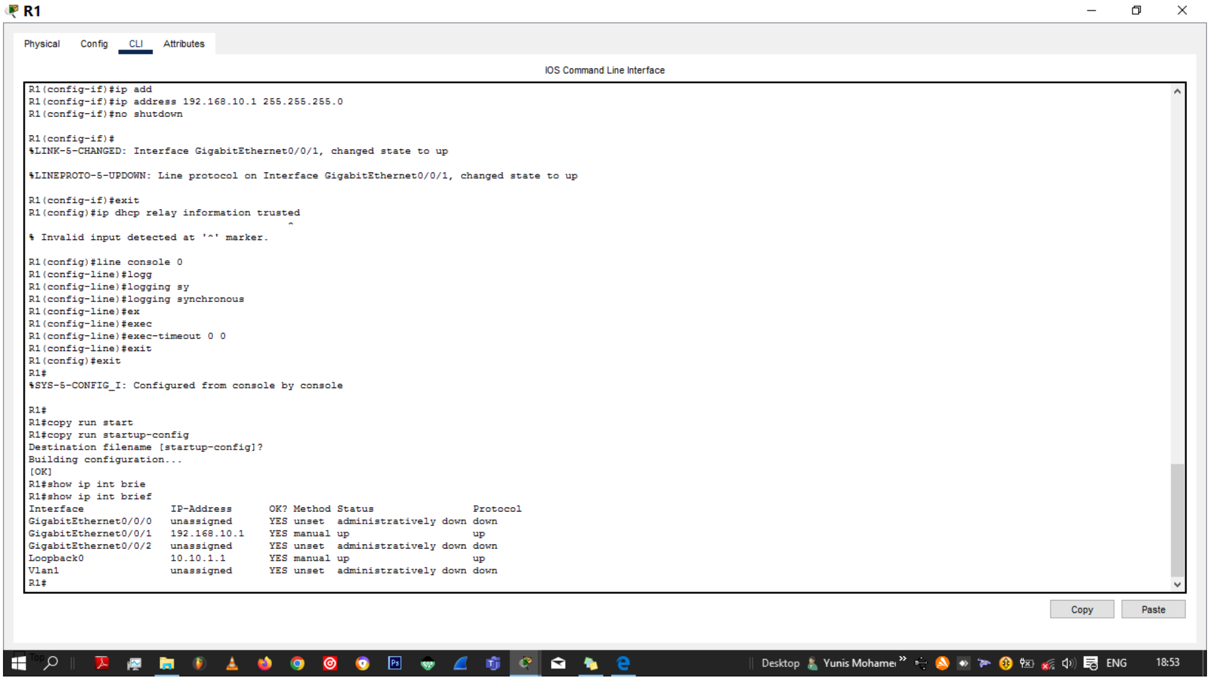
Configure ip dhcp relay information as trusted



```
cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.
Processor board ID FLM232010G0
3 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3223551K bytes of flash memory at bootflash:.


Press RETURN to get started!


%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)#ip dhcp relay information trusted
                                          ^
% Invalid input detected at '^' marker.

R1(config)#ip dhcp relay information trusted ?
% Unrecognized command
R1(config)#ip dhcp relay information trusted
                                          ^
% Invalid input detected at '^' marker.

R1(config)# ip dhcp relay information trusted
                                           ^
% Invalid input detected at '^' marker.

R1(config)# ip dhcp relay information trusted ?
% Unrecognized command
R1(config)#ip dhcp relay information ?
  trust-all  Received DHCP packets may contain relay info option with zero
             giaddr
R1(config)#ip dhcp relay information tr
R1(config)#ip dhcp relay information trust-all
R1(config)#
```

Figure 4 configure relay agent as trusted

Verify the running-configuration on R1 using the show ip interface brief.

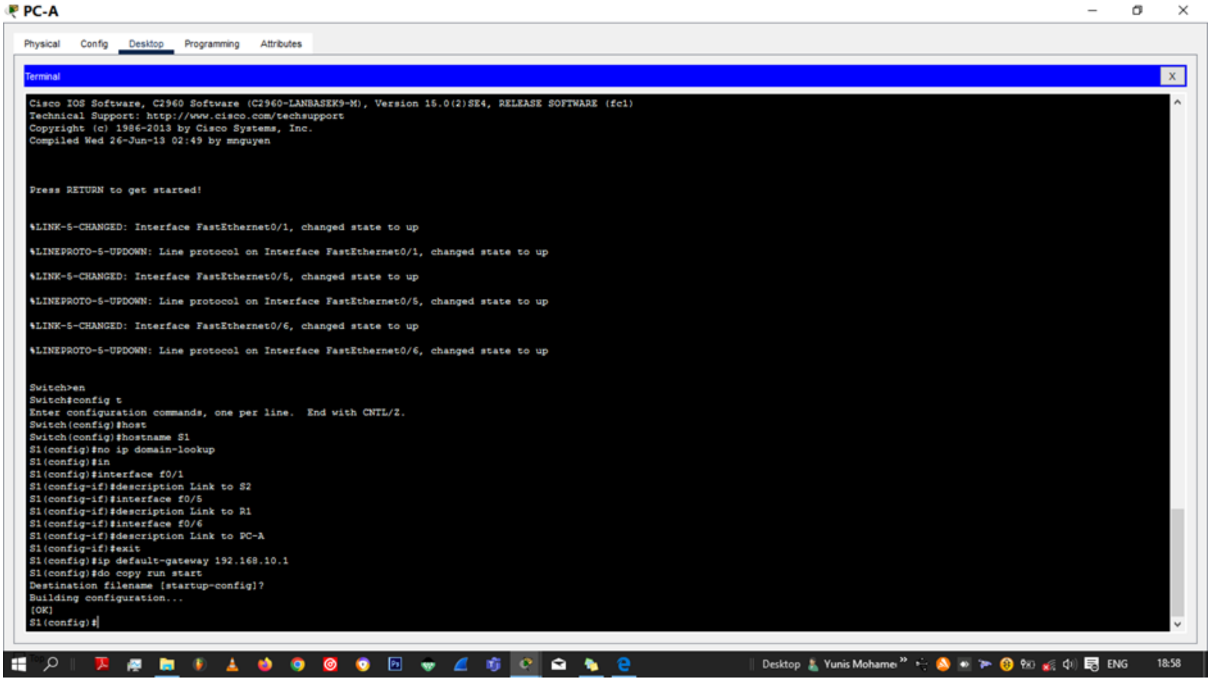


```
R1(config-if)#ip add
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R1(config-if)#exit
R1(config)#ip dhcp relay information trusted
                                         ^
% Invalid input detected at '^' marker.

R1(config)#line console 0
R1(config-line)#logg
R1(config-line)#logging sy
R1(config-line)#logging synchronous
R1(config-line)#ex
R1(config-line)#exec
R1(config-line)#exec-timeout 0 0
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
R1#copy run start
R1#copy run startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#show ip int brie
R1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down down
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Loopback0              10.10.1.1       YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

Figure 5 verify running-config on R1

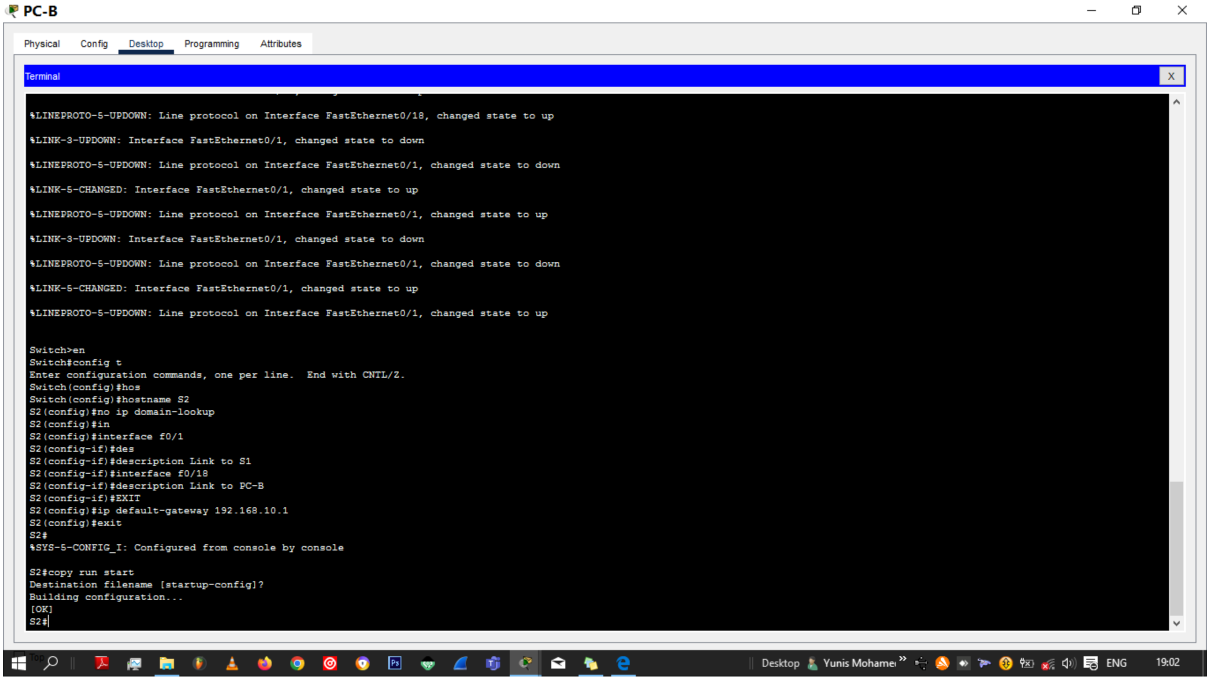
Configure and verify basic switch settings.

1. Configure the hostname for switches S1 and S2.
2. Prevent unwanted DNS lookups on both switches.
3. Configure interface descriptions for the ports that are in use in S1 and S2.
4. Set the default-gateway for the Management VLAN to 192.168.10.1 on both switches.



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



Press RETURN to get started!


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

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

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

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

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

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


Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#host
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#in
S1(config)#interface f0/1
S1(config-if)#description Link to S2
S1(config-if)#interface f0/5
S1(config-if)#description Link to R1
S1(config-if)#interface f0/6
S1(config-if)#description Link to PC-A
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.10.1
S1(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1(config)#
```

Figure 6 basic S1 configuration



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

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

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

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

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

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

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

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

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


Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hos
Switch(config)#hostname S2
S2(config)#no ip domain-lookup
S2(config)#in
S2(config)#interface f0/1
S2(config-if)#des
S2(config-if)#description Link to S1
S2(config-if)#interface f0/18
S2(config-if)#description Link to PC-B
S2(config-if)#EXIT
S2(config)#ip default-gateway 192.168.10.1
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S2#
```

Figure 7 basic S2 configuration

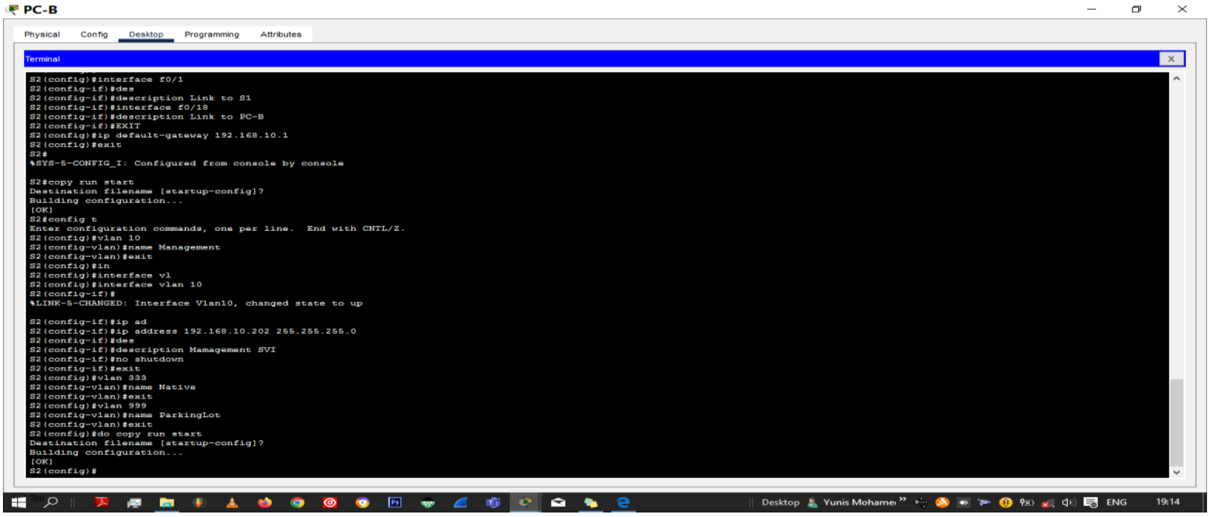
Part 2: Configure VLANs on Switches

1. Configure the following VLANS on both **S1** and **S2**:

   VLAN 10, name **Management.**

   VLAN 333, name **Native**.

   VLAN 999, name **ParkingLot.**



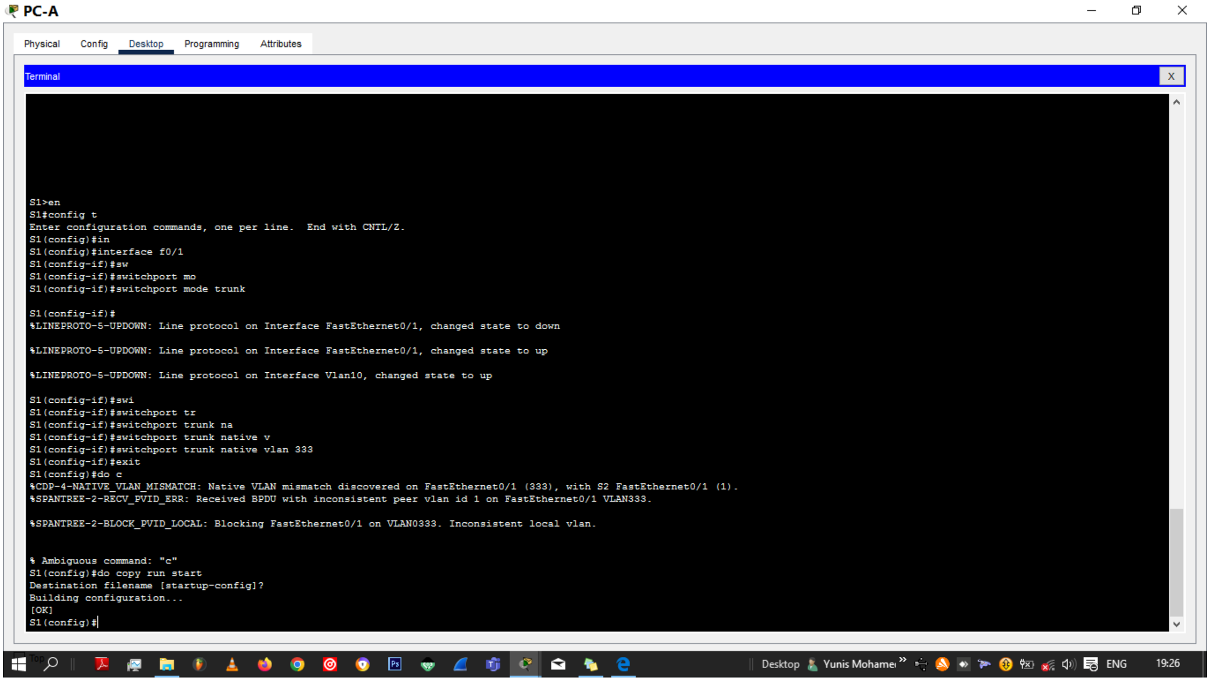
```
S2(config)#interface f0/1
S2(config-if)#des
S2(config-if)#description Link to S1
S2(config-if)#interface f0/18
S2(config-if)#description Link to PC-B
S2(config-if)#EXIT
S2(config)#ip default-gateway 192.168.10.1
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#vlan 10
S2(config-vlan)#name Management
S2(config-vlan)#exit
S2(config)#in
S2(config)#interface vl
S2(config)#interface vlan 10
S2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

S2(config-if)#ip ad
S2(config-if)#ip address 192.168.10.202 255.255.255.0
S2(config-if)#des
S2(config-if)#description Mamagement SVI
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#vlan 333
S2(config-vlan)#name Native
S2(config-vlan)#exit
S2(config)#vlan 999
S2(config-vlan)#name ParkingLot
S2(config-vlan)#exit
S2(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S2(config)#
```

Figure 8 configure vlans SVI on S2

Part 3: Configure Switch Security.

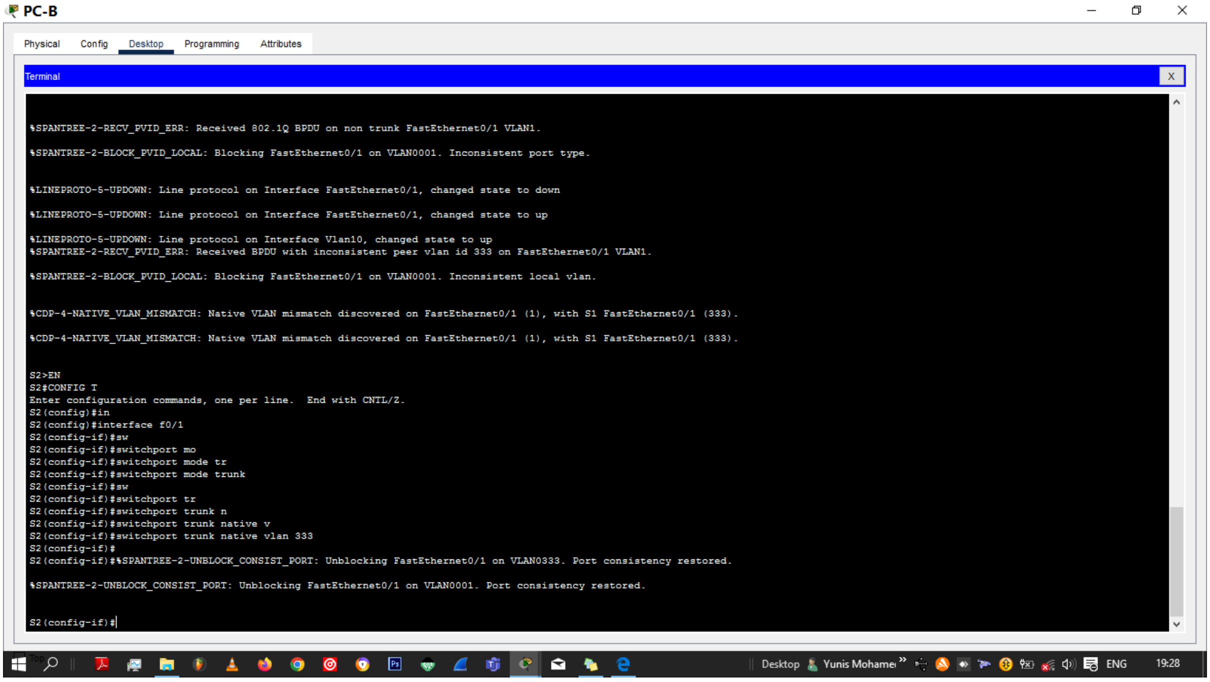
Implement 802.1Q trunking.

1. Implement 802.1Q trunking by configuring trunk ports to native VLAN.



```
S1>en
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#in
S1(config)#interface f0/1
S1(config-if)#sw
S1(config-if)#switchport mo
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)#swi
S1(config-if)#switchport tr
S1(config-if)#switchport trunk na
S1(config-if)#switchport trunk native v
S1(config-if)#switchport trunk native vlan 333
S1(config-if)#exit
S1(config)#do c
%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 vlan id 1 on FastEthernet0/1 VLAN333.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0333. Inconsistent local vlan.


% Ambiguous command: "c"
S1(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1(config)#
```

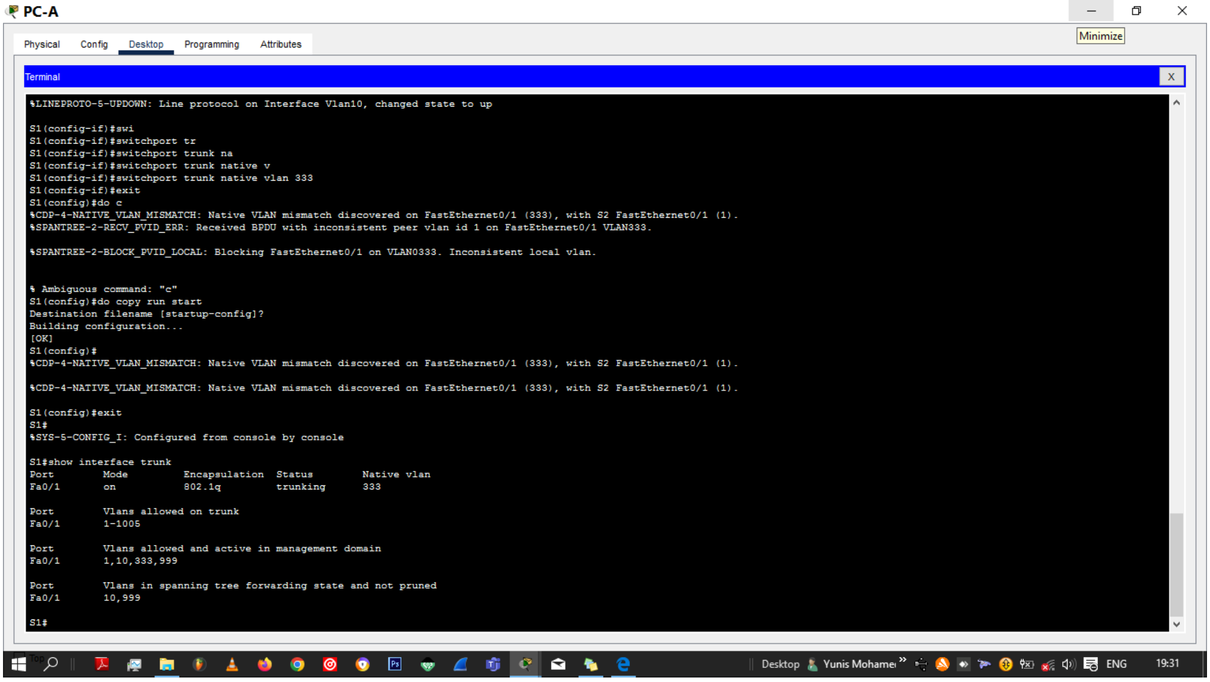
Figure 9 trunk ports S1



```
%SPANTREE-2-RECV_PVID_ERR: Received 802.1Q BPDU on non trunk FastEthernet0/1 VLAN1.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0001. Inconsistent port type.


%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
%SPANTREE-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 333 on FastEthernet0/1 VLAN1.

%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>EN
S2#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#in
S2(config)#interface f0/1
S2(config-if)#sw
S2(config-if)#switchport mo
S2(config-if)#switchport mode tr
S2(config-if)#switchport mode trunk
S2(config-if)#sw
S2(config-if)#switchport tr
S2(config-if)#switchport trunk n
S2(config-if)#switchport trunk native v
S2(config-if)#switchport trunk native vlan 333
S2(config-if)#
S2(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0333. Port consistency restored.

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


S2(config-if)#
```

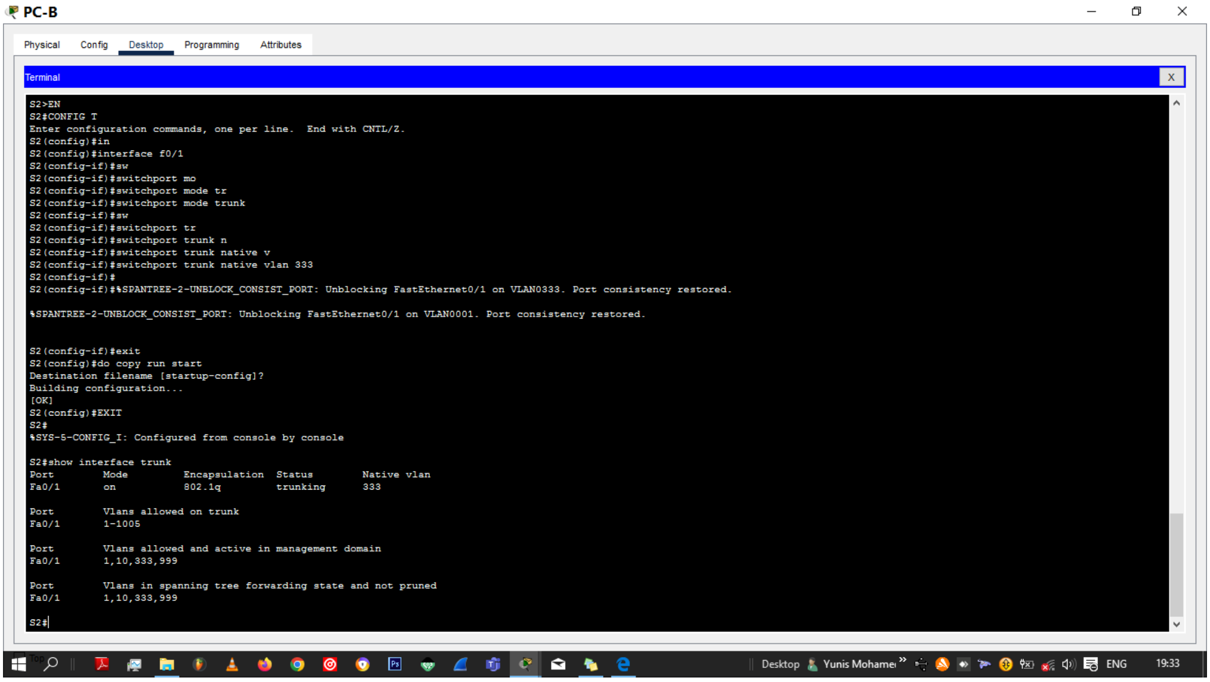
Figure 10 trunk ports S2

2. Verify that trunking is configured on both switches.



```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

S1(config-if)#swi
S1(config-if)#switchport tr
S1(config-if)#switchport trunk na
S1(config-if)#switchport trunk native v
S1(config-if)#switchport trunk native vlan 333
S1(config-if)#exit
S1(config)#do c
%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 vlan id 1 on FastEthernet0/1 VLAN333.

%SPANTREE-2-BLOCK_PVID_LOCAL: Blocking FastEthernet0/1 on VLAN0333. Inconsistent local vlan.


% Ambiguous command: "c"
S1(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2 FastEthernet0/1 (1).

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

S1(config)#exit
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       10,999

S1#
```

Figure 11 trunk verification S1

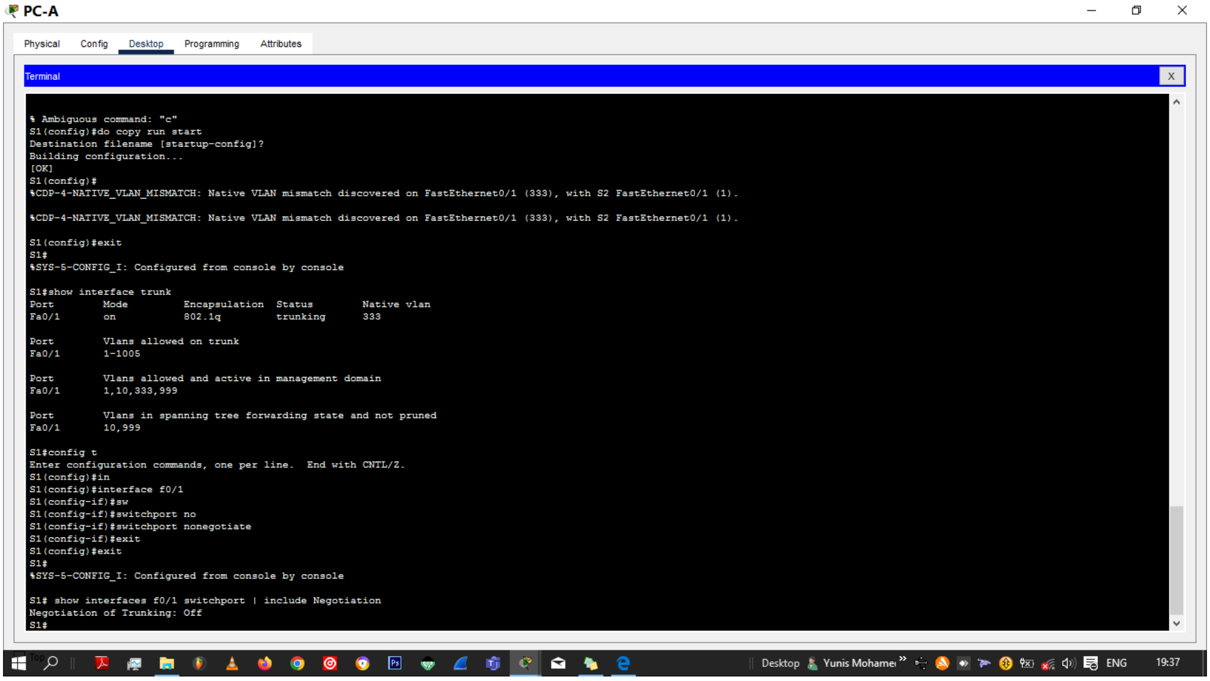


```
S2>EN
S2#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#in
S2(config)#interface f0/1
S2(config-if)#sw
S2(config-if)#switchport mo
S2(config-if)#switchport mode tr
S2(config-if)#switchport mode trunk
S2(config-if)#sw
S2(config-if)#switchport tr
S2(config-if)#switchport trunk n
S2(config-if)#switchport trunk native v
S2(config-if)#switchport trunk native vlan 333
S2(config-if)#
S2(config-if)#%SPANTREE-2-UNBLOCK_CONSIST_PORT: Unblocking FastEthernet0/1 on VLAN0333. Port consistency restored.

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


S2(config-if)#exit
S2(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S2(config)#EXIT
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#
```

Figure 12 trunk verification S2

3. Disable DTP negotiation of F0/1 on S1 on S2 by issuing the switchport nonegotiate command.

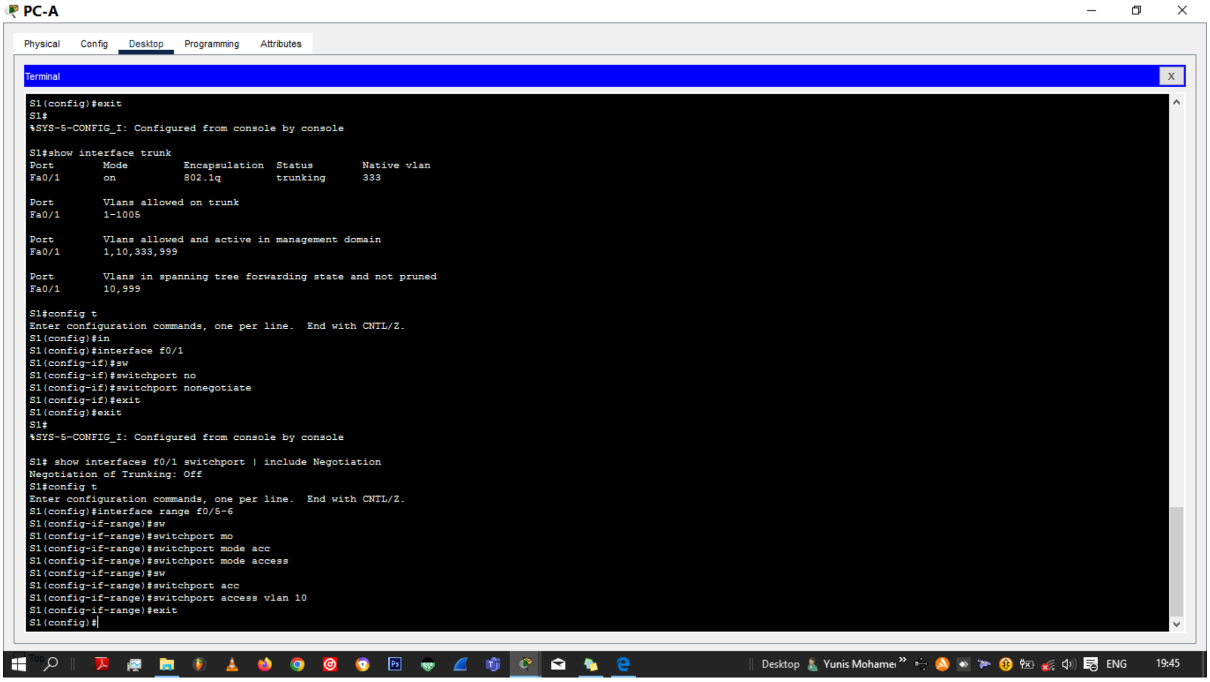
4. Verifying that DTP negotiation is of on both switches.



```
% Ambiguous command: "c"
S1(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (333), with S2 FastEthernet0/1 (1).

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

S1(config)#exit
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       10,999

S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#in
S1(config)#interface f0/1
S1(config-if)#sw
S1(config-if)#switchport no
S1(config-if)#switchport nonegotiate
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

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

Configure access ports.

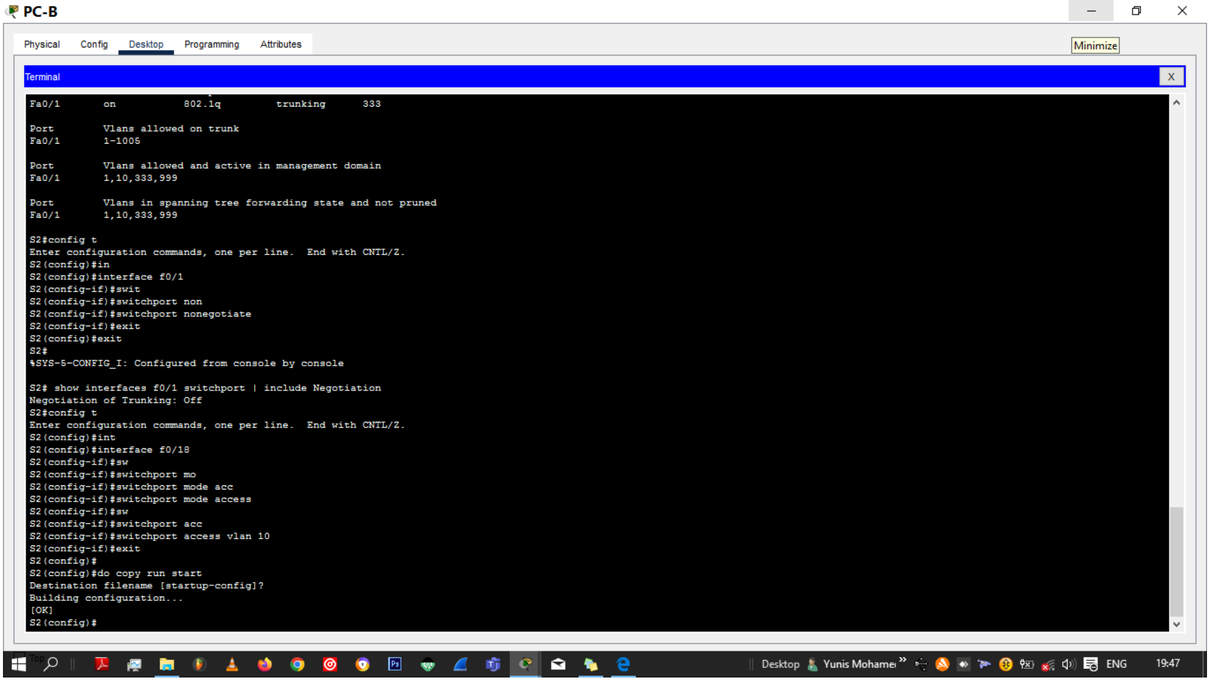
1. On S1, configure F0/5 and F0/6 as access ports that are associated with VLAN 10.



```
S1(config)#exit
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       10,999

S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#in
S1(config)#interface f0/1
S1(config-if)#sw
S1(config-if)#switchport no
S1(config-if)#switchport nonegotiate
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1# show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range f0/5-6
S1(config-if-range)#sw
S1(config-if-range)#switchport mo
S1(config-if-range)#switchport mode acc
S1(config-if-range)#switchport mode access
S1(config-if-range)#sw
S1(config-if-range)#switchport acc
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#exit
S1(config)#
```

Figure 13 access ports S1

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

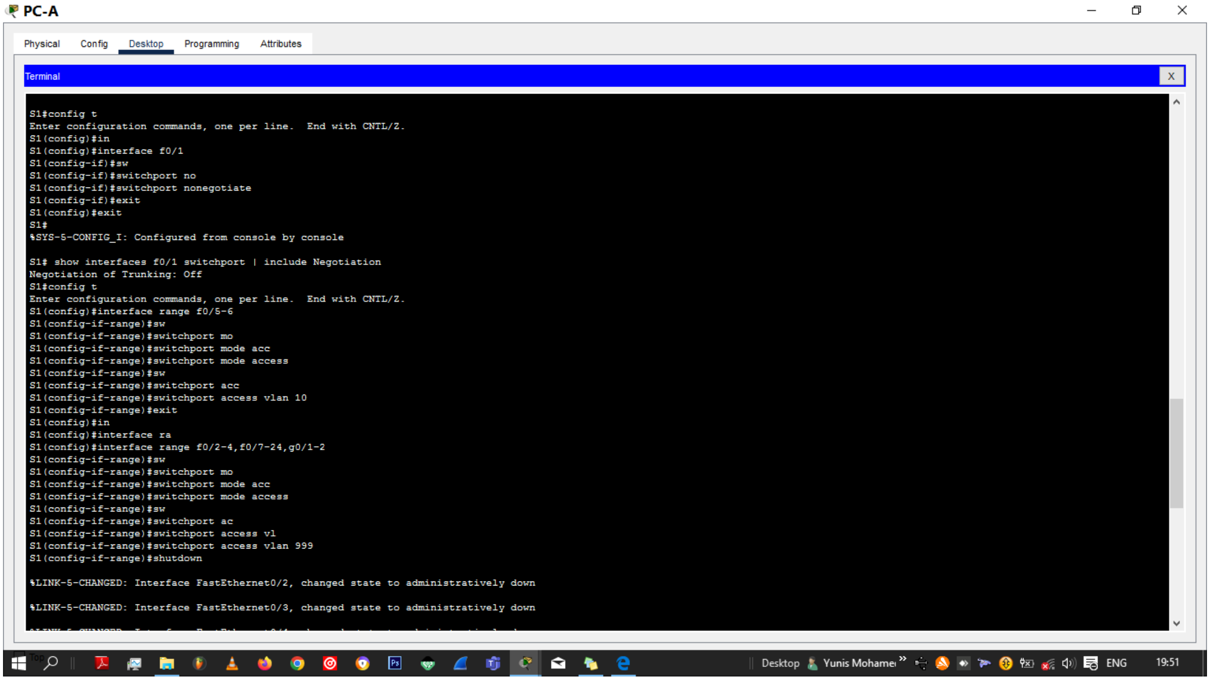


```
Fa0/1       on          802.1q        trunking      333

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)#in
S2(config)#interface f0/1
S2(config-if)#swit
S2(config-if)#switchport non
S2(config-if)#switchport nonegotiate
S2(config-if)#exit
S2(config)#exit
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2# show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#int
S2(config)#interface f0/18
S2(config-if)#sw
S2(config-if)#switchport mo
S2(config-if)#switchport mode acc
S2(config-if)#switchport mode access
S2(config-if)#sw
S2(config-if)#switchport acc
S2(config-if)#switchport access vlan 10
S2(config-if)#exit
S2(config)#
S2(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S2(config)#
```

Figure 14 access ports S2

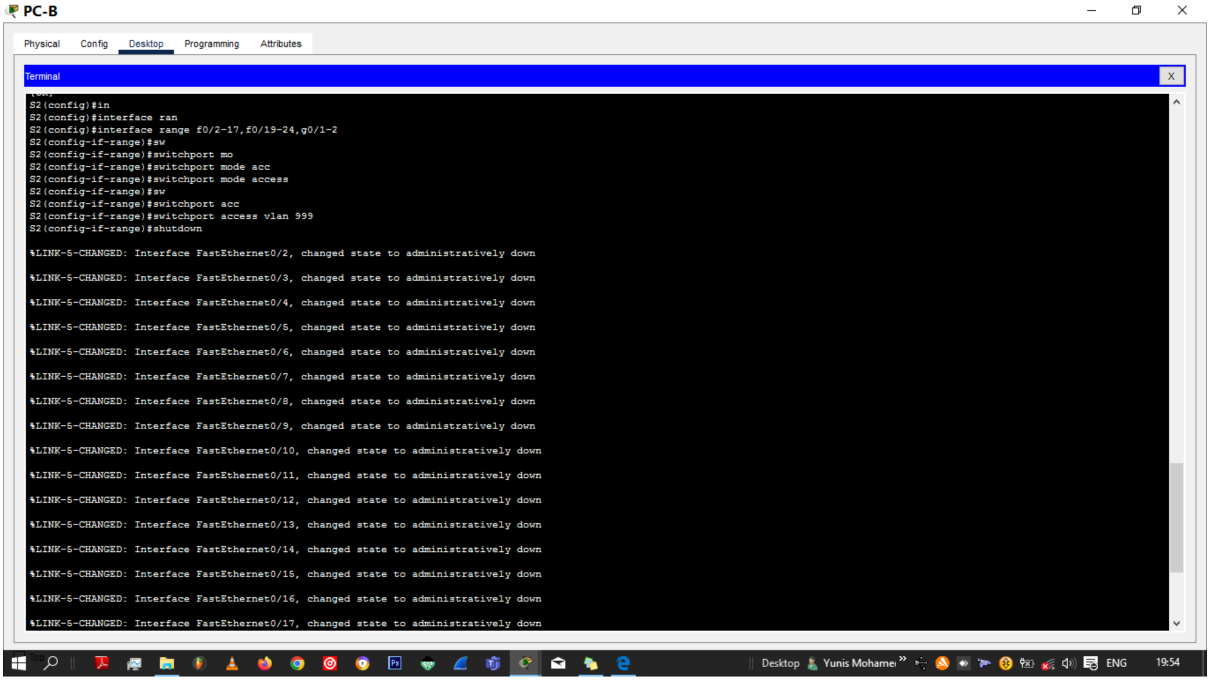
Secure and disable unused switchport.

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



```
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#in
S1(config)#interface f0/1
S1(config-if)#sw
S1(config-if)#switchport no
S1(config-if)#switchport nonegotiate
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1# show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface range f0/5-6
S1(config-if-range)#sw
S1(config-if-range)#switchport mo
S1(config-if-range)#switchport mode acc
S1(config-if-range)#switchport mode access
S1(config-if-range)#sw
S1(config-if-range)#switchport acc
S1(config-if-range)#switchport access vlan 10
S1(config-if-range)#exit
S1(config)#in
S1(config)#interface ra
S1(config)#interface range f0/2-4,f0/7-24,g0/1-2
S1(config-if-range)#sw
S1(config-if-range)#switchport mo
S1(config-if-range)#switchport mode acc
S1(config-if-range)#switchport mode access
S1(config-if-range)#sw
S1(config-if-range)#switchport ac
S1(config-if-range)#switchport access vl
S1(config-if-range)#switchport access vlan 999
S1(config-if-range)#shutdown

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

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

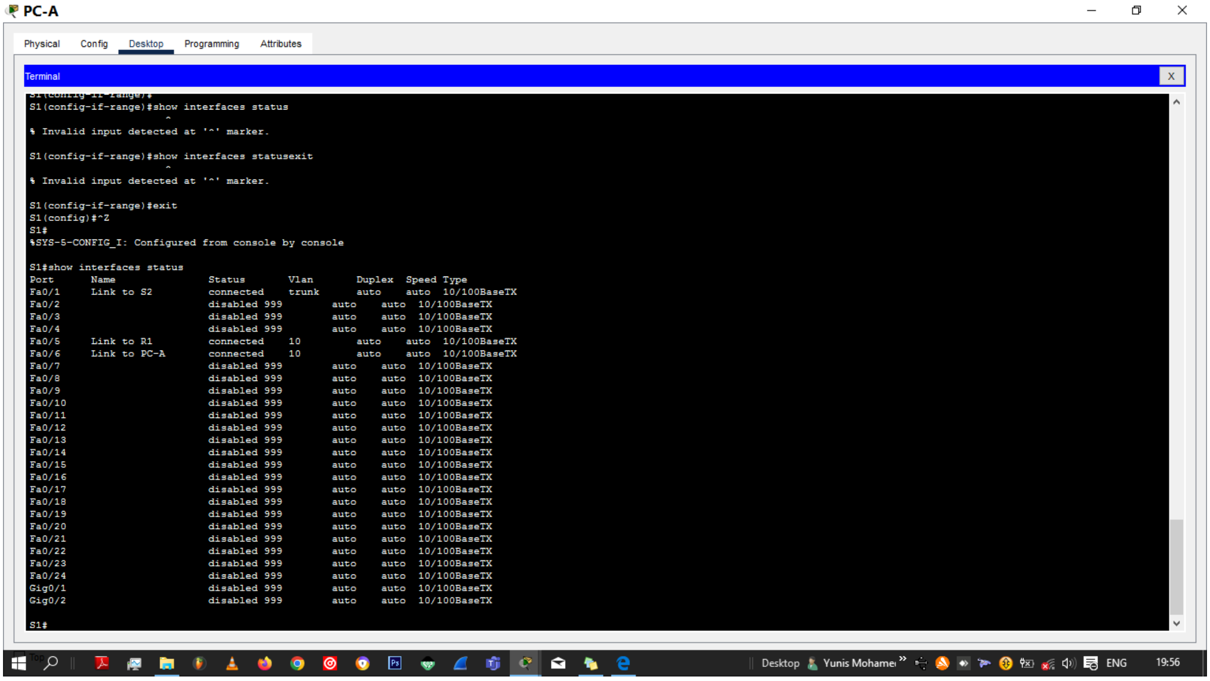
Figure 15 unused ports S1



```
S2(config)#in
S2(config)#interface ran
S2(config)#interface range f0/2-17,f0/19-24,g0/1-2
S2(config-if-range)#sw
S2(config-if-range)#switchport mo
S2(config-if-range)#switchport mode acc
S2(config-if-range)#switchport mode access
S2(config-if-range)#sw
S2(config-if-range)#switchport acc
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

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
```

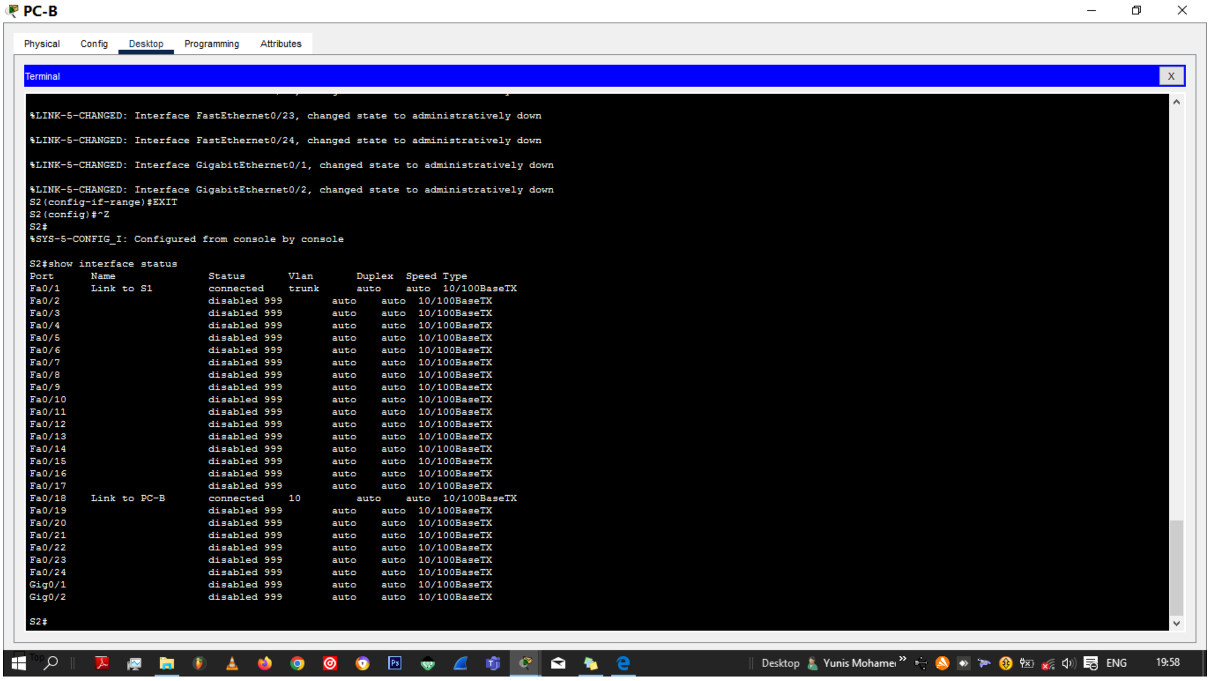
Figure 16 unused ports S2

2. Verify that unused ports are disabled and associated with VLAN 999.



```
S1(config-if-range)#
S1(config-if-range)#show interfaces status
                      ^
% Invalid input detected at '^' marker.

S1(config-if-range)#show interfaces statusexit
                      ^
% Invalid input detected at '^' marker.

S1(config-if-range)#exit
S1(config)#^Z
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
Fa0/22                       disabled 999        auto    auto  10/100BaseTX
Fa0/23                       disabled 999        auto    auto  10/100BaseTX
Fa0/24                       disabled 999        auto    auto  10/100BaseTX
Gig0/1                       disabled 999        auto    auto  10/100BaseTX
Gig0/2                       disabled 999        auto    auto  10/100BaseTX

S1#
```

Figure 17 S1 unused ports

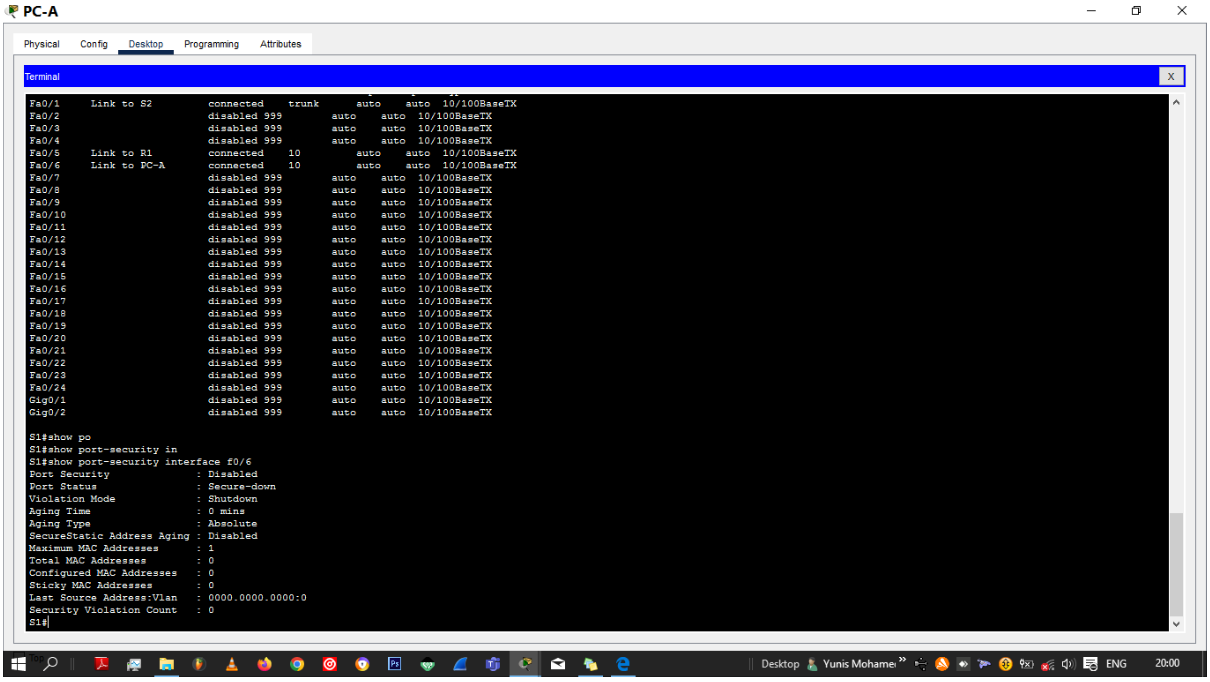


```
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down

%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(config-if-range)#EXIT
S2(config)#^Z
S2#
%SYS-5-CONFIG_I: Configured from console by console

S2#show interface status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1     Link to S1         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                        disabled 999        auto    auto  10/100BaseTX
Fa0/6                        disabled 999        auto    auto  10/100BaseTX
Fa0/7                        disabled 999        auto    auto  10/100BaseTX
Fa0/8                        disabled 999        auto    auto  10/100BaseTX
Fa0/9                        disabled 999        auto    auto  10/100BaseTX
Fa0/10                       disabled 999        auto    auto  10/100BaseTX
Fa0/11                       disabled 999        auto    auto  10/100BaseTX
Fa0/12                       disabled 999        auto    auto  10/100BaseTX
Fa0/13                       disabled 999        auto    auto  10/100BaseTX
Fa0/14                       disabled 999        auto    auto  10/100BaseTX
Fa0/15                       disabled 999        auto    auto  10/100BaseTX
Fa0/16                       disabled 999        auto    auto  10/100BaseTX
Fa0/17                       disabled 999        auto    auto  10/100BaseTX
Fa0/18    Link to PC-B       connected    10         auto    auto  10/100BaseTX
Fa0/19                       disabled 999        auto    auto  10/100BaseTX
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
Gig0/1                       disabled 999        auto    auto  10/100BaseTX
Gig0/2                       disabled 999        auto    auto  10/100BaseTX

S2#
```

Figure 18 S2 unused ports

Document and implement port security features.

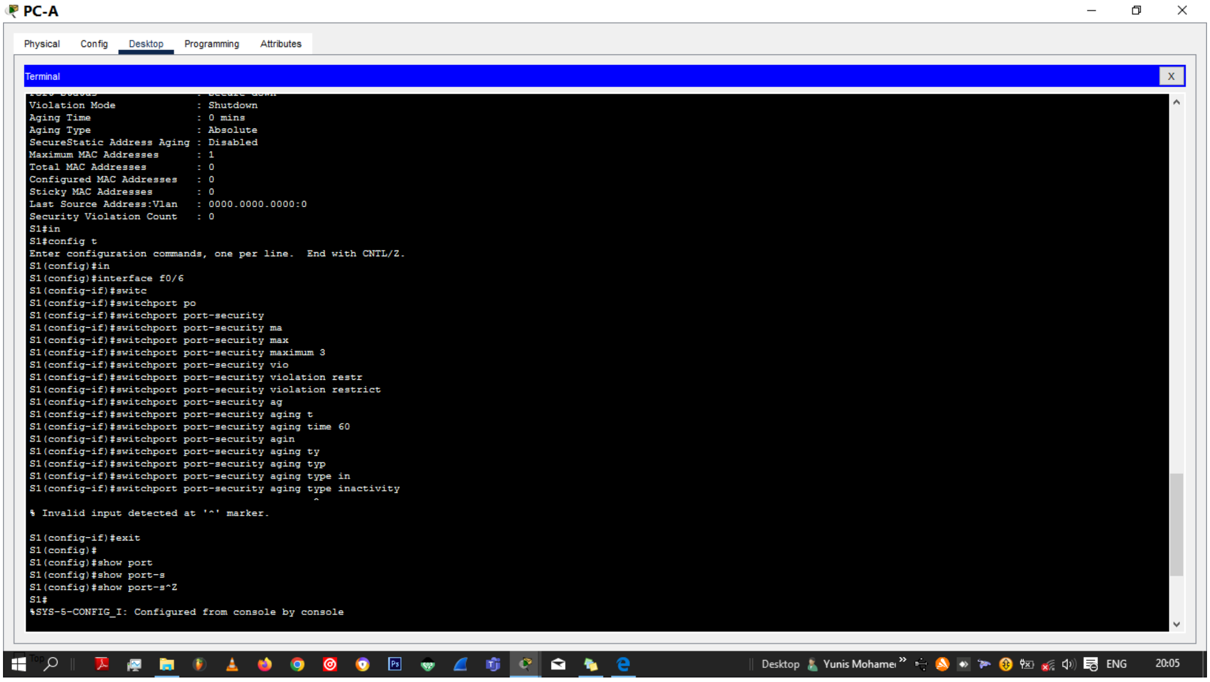
1. On S1, issue the show port-security interface f0/6 command to display the default port security settings for interface F0/6.



```
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
Fa0/22                       disabled 999        auto    auto  10/100BaseTX
Fa0/23                       disabled 999        auto    auto  10/100BaseTX
Fa0/24                       disabled 999        auto    auto  10/100BaseTX
Gig0/1                       disabled 999        auto    auto  10/100BaseTX
Gig0/2                       disabled 999        auto    auto  10/100BaseTX

S1#show po
S1#show port-security in
S1#show port-security interface f0/6
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

Figure 19 verify f0/6 security setting

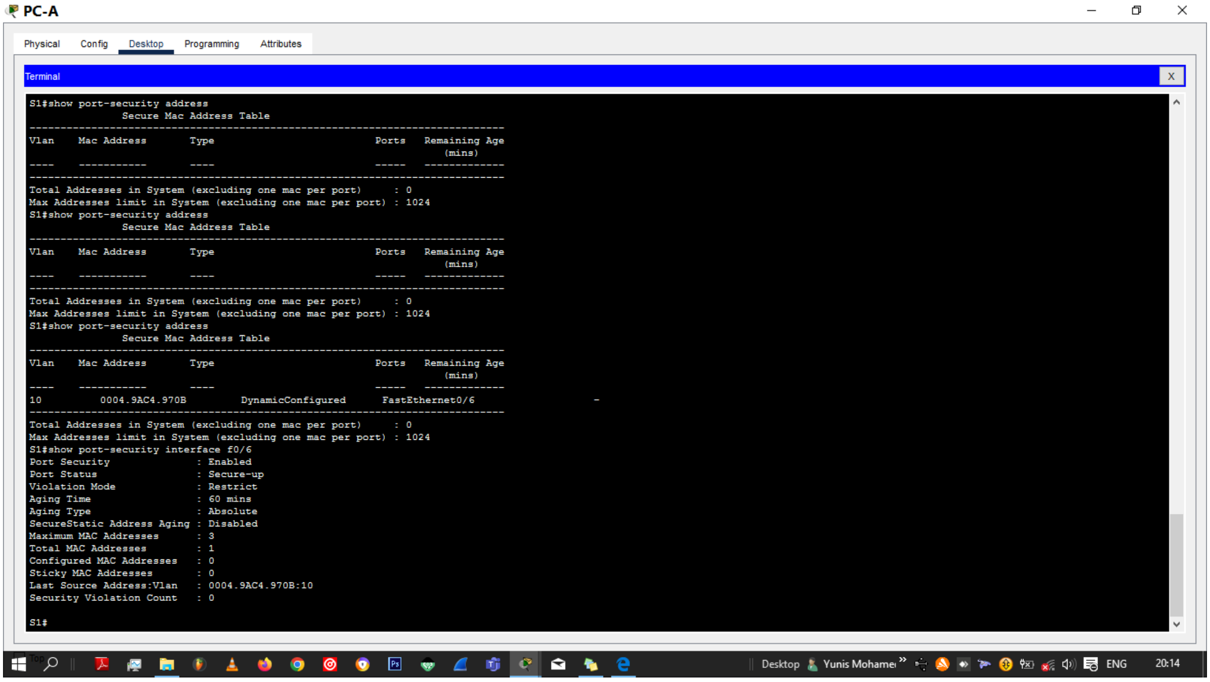
2. On S1, enable port security on F0/6 with the following settings:
   - Maximum number of MAC addresses: 3
   - Violation type: restrict
   - Aging time: 60 min
   - Aging type: inactivity



```
Port Status                 : Secure-down
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses       : 1
Total MAC Addresses         : 0
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 0
Last Source Address:Vlan    : 0000.0000.0000:0
Security Violation Count    : 0
S1#in
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#in
S1(config)#interface f0/6
S1(config-if)#switc
S1(config-if)#switchport po
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security ma
S1(config-if)#switchport port-security max
S1(config-if)#switchport port-security maximum 3
S1(config-if)#switchport port-security vio
S1(config-if)#switchport port-security violation restr
S1(config-if)#switchport port-security violation restrict
S1(config-if)#switchport port-security ag
S1(config-if)#switchport port-security aging t
S1(config-if)#switchport port-security aging time 60
S1(config-if)#switchport port-security agin
S1(config-if)#switchport port-security aging ty
S1(config-if)#switchport port-security aging typ
S1(config-if)#switchport port-security aging type in
S1(config-if)#switchport port-security aging type inactivity
                                              ^
% Invalid input detected at '^' marker.

S1(config-if)#exit
S1(config)#
S1(config)#show port
S1(config)#show port-s
S1(config)#show port-s^Z
S1#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 20 S1 enable port security f0/6

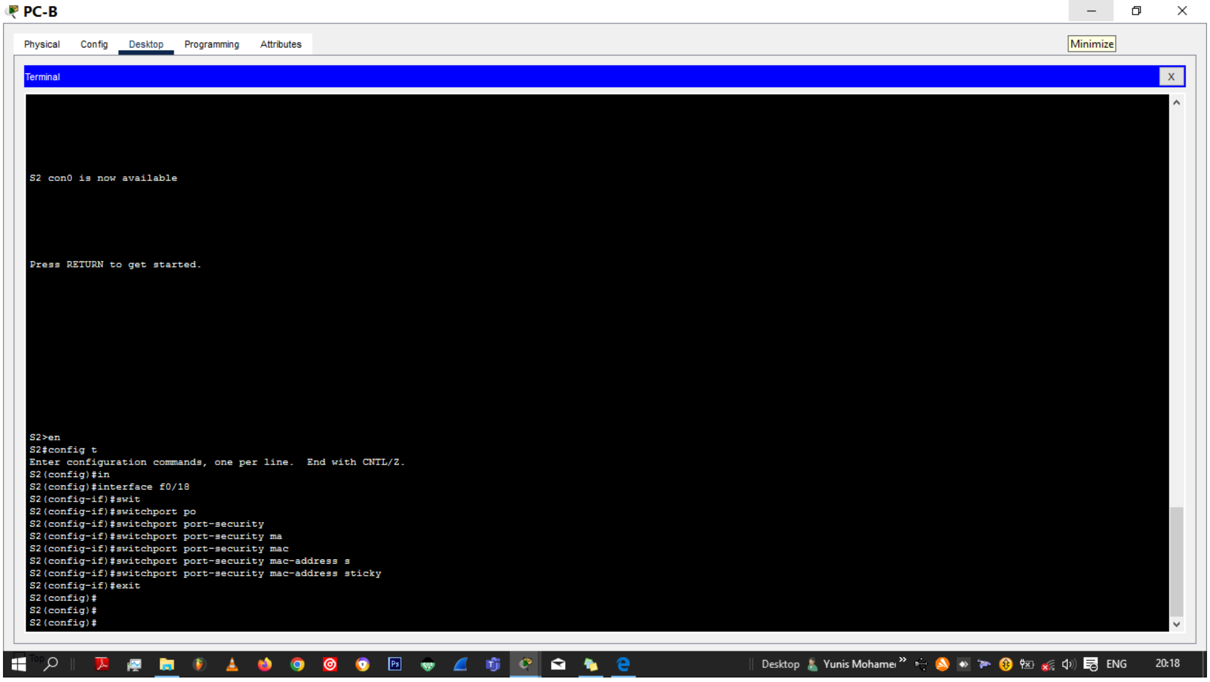
3. Verify port security on S1 F0/6.



```
S1#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S1#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S1#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
10          0004.9AC4.970B          DynamicConfigured      FastEthernet0/6                  -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S1#show port-security interface f0/6
Port Security               : Enabled
Port Status                 : Secure-up
Violation Mode              : Restrict
Aging Time                  : 60 mins
Aging Type                  : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses       : 3
Total MAC Addresses         : 1
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 0
Last Source Address:Vlan    : 0004.9AC4.970B:10
Security Violation Count    : 0

S1#
```

Figure 21 verify port security S1

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

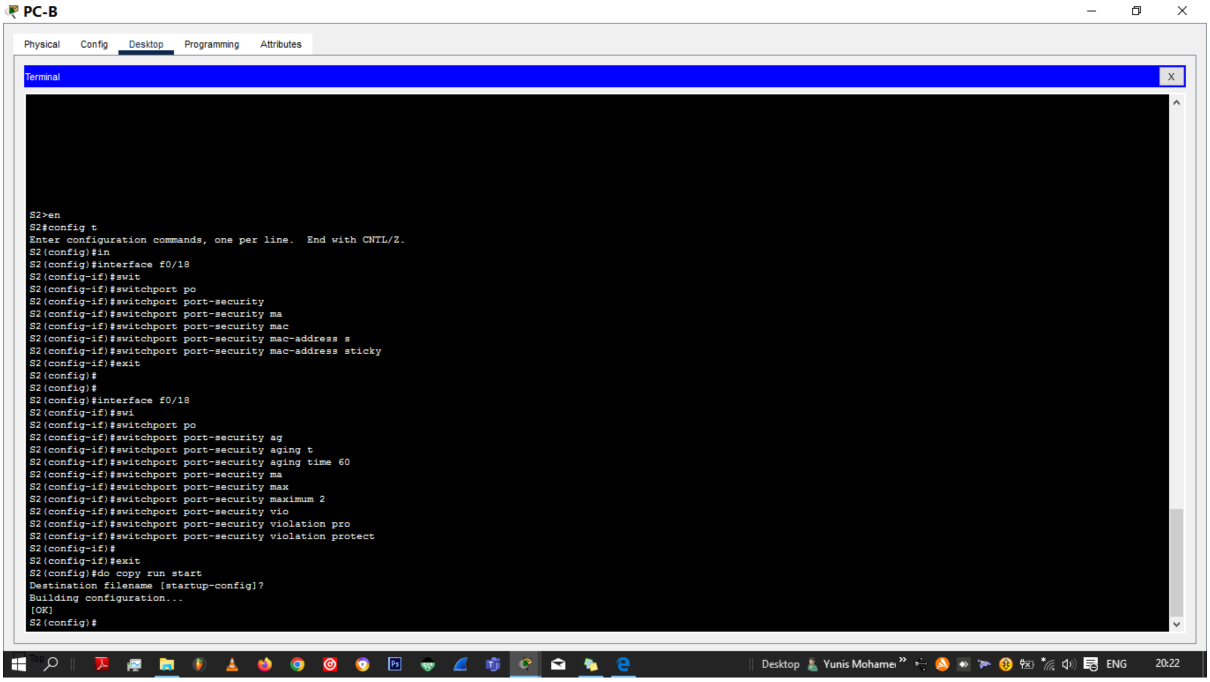


```
S2 con0 is now available



Press RETURN to get started.



S2>en
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#in
S2(config)#interface f0/18
S2(config-if)#swit
S2(config-if)#switchport po
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security ma
S2(config-if)#switchport port-security mac
S2(config-if)#switchport port-security mac-address s
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#exit
S2(config)#
S2(config)#
S2(config)#
```

Figure 22 enable port-security F0/18 S2

5. Configure the following port security settings on S2 F/18:
   - Maximum number of MAC addresses: 2
   - Violation type: Protect

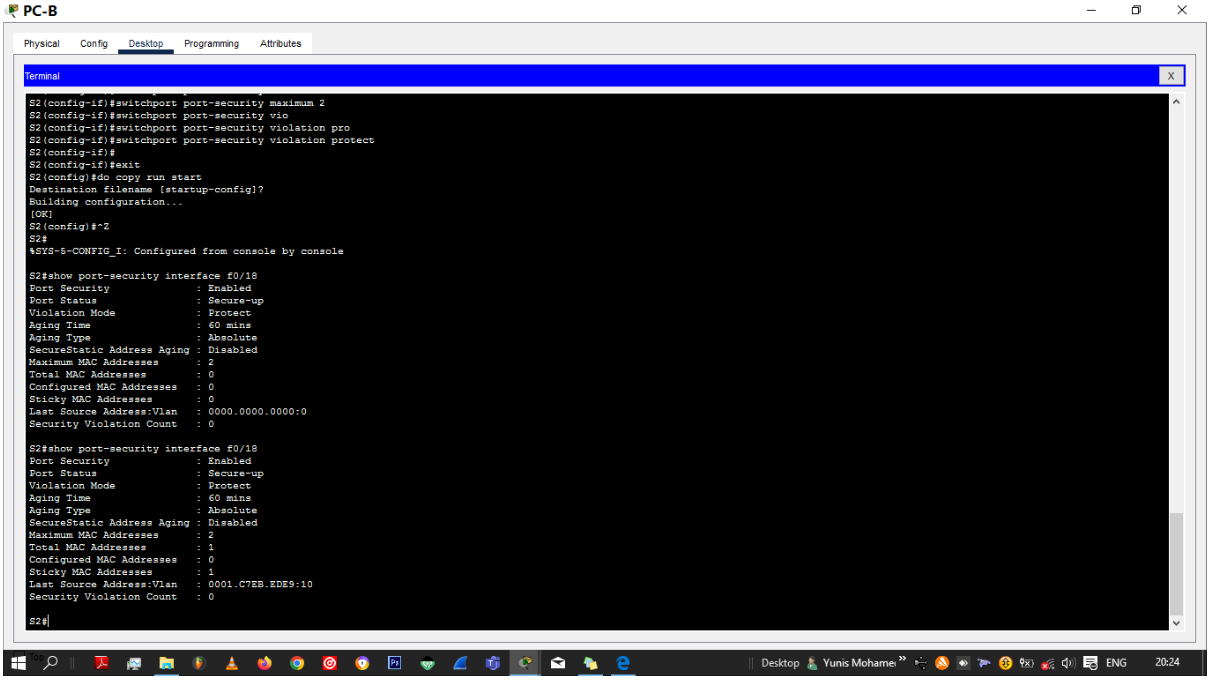
- Aging time: 60 min



```
S2>en
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#in
S2(config)#interface f0/18
S2(config-if)#swit
S2(config-if)#switchport po
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security ma
S2(config-if)#switchport port-security mac
S2(config-if)#switchport port-security mac-address s
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#exit
S2(config)#
S2(config)#
S2(config)#interface f0/18
S2(config-if)#swi
S2(config-if)#switchport po
S2(config-if)#switchport port-security ag
S2(config-if)#switchport port-security aging t
S2(config-if)#switchport port-security aging time 60
S2(config-if)#switchport port-security ma
S2(config-if)#switchport port-security max
S2(config-if)#switchport port-security maximum 2
S2(config-if)#switchport port-security vio
S2(config-if)#switchport port-security violation pro
S2(config-if)#switchport port-security violation protect
S2(config-if)#
S2(config-if)#exit
S2(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S2(config)#
```

Figure 23configure port security S2 f0/18

6. Verify port security on S2 F0/18.

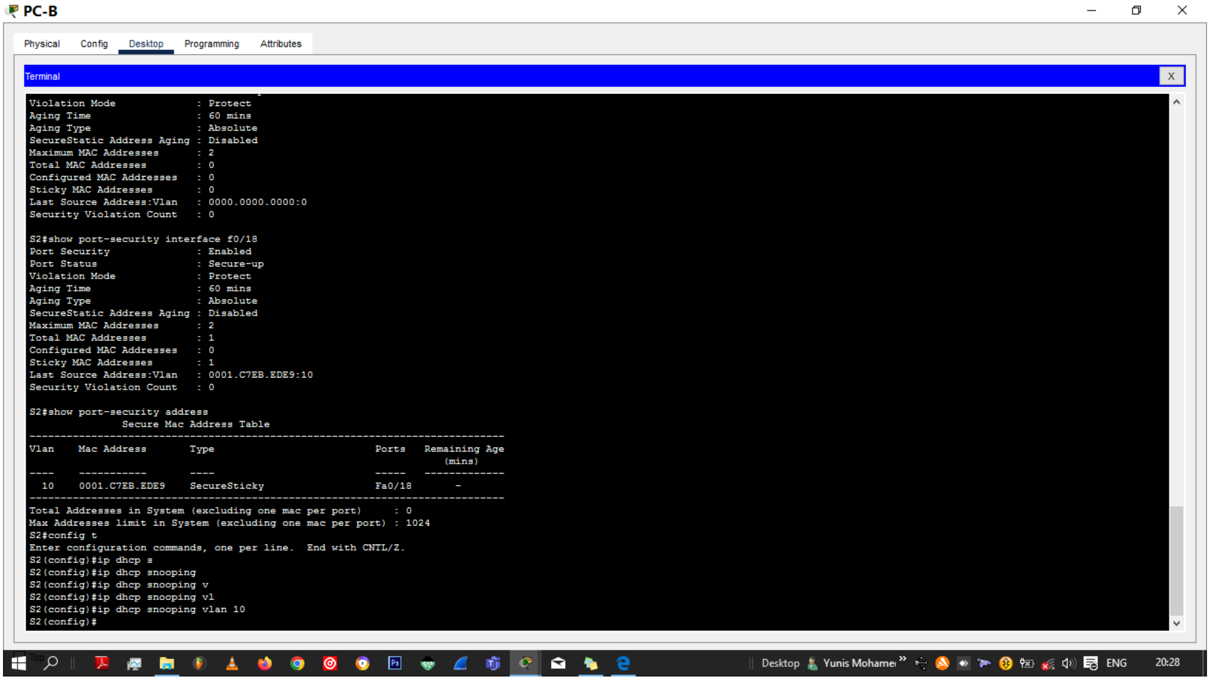


```
S2(config-if)#switchport port-security maximum 2
S2(config-if)#switchport port-security vio
S2(config-if)#switchport port-security violation pro
S2(config-if)#switchport port-security violation protect
S2(config-if)#
S2(config-if)#exit
S2(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S2(config)#^Z
S2#
%SYS-5-CONFIG_I: Configured from console by console

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

S2#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       : 1
Last Source Address:Vlan   : 0001.C7EB.EDE9:10
Security Violation Count   : 0

S2#
```

Figure 24 verify port security S2 f0/18

Implement DHCP snooping security.

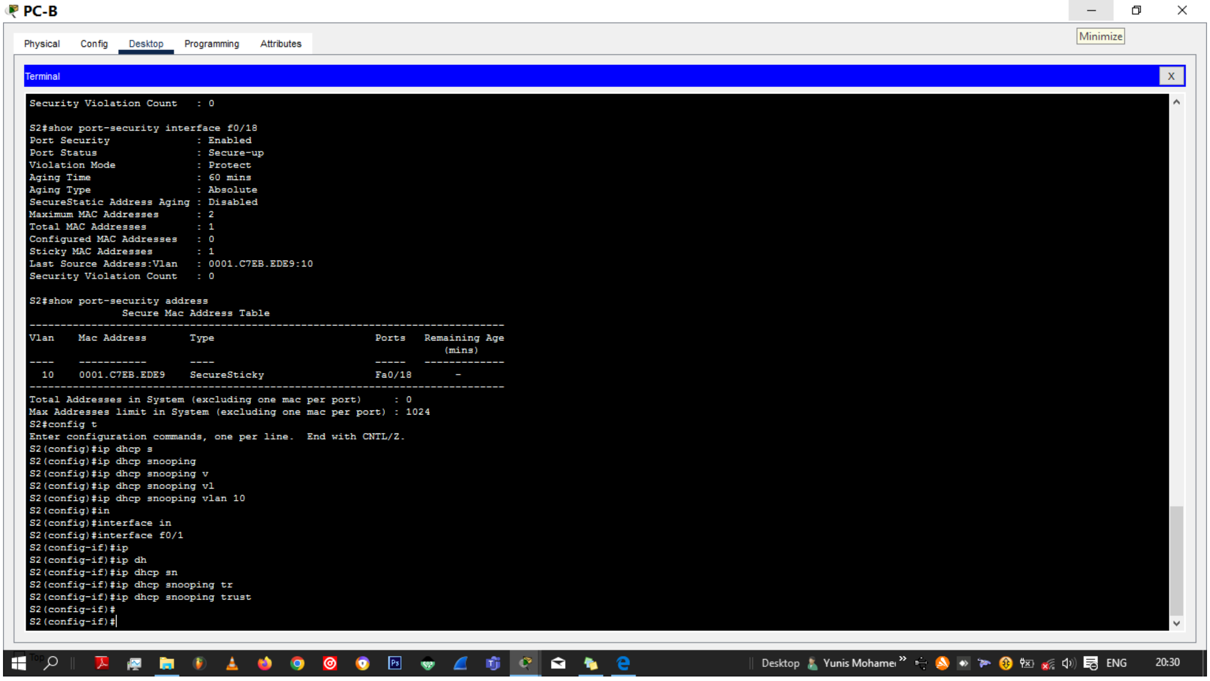
1. On S2, enable DHCP snooping and configure DHCP snooping on VLAN 10.



```
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 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       : 1
Last Source Address:Vlan   : 0001.C7EB.EDE9:10
Security Violation Count   : 0

S2#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
  10    0001.C7EB.EDE9    SecureSticky                  Fa0/18        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#ip dhcp s
S2(config)#ip dhcp snooping
S2(config)#ip dhcp snooping v
S2(config)#ip dhcp snooping vl
S2(config)#ip dhcp snooping vlan 10
S2(config)#
```

Figure 25 S2 enable dhcp snooping

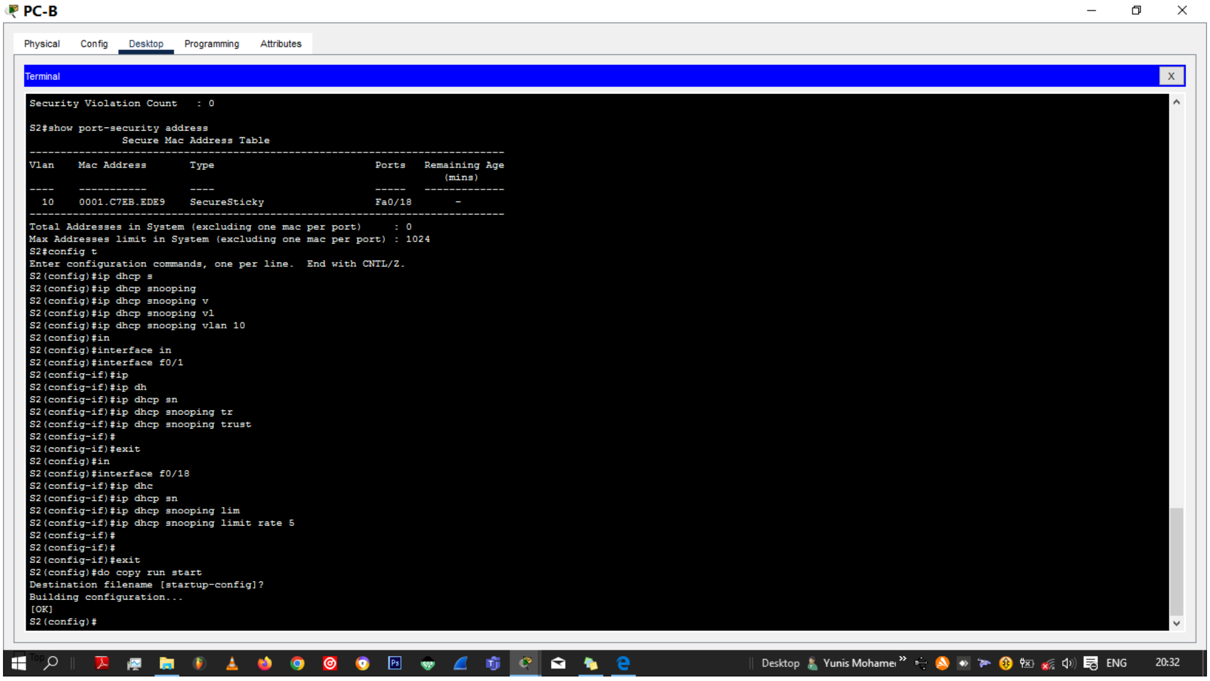
2. Configure the trunk port on S2 as a trusted port.



```
Security Violation Count   : 0

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       : 1
Last Source Address:Vlan   : 0001.C7EB.EDE9:10
Security Violation Count   : 0

S2#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
  10    0001.C7EB.EDE9    SecureSticky                  Fa0/18        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#ip dhcp s
S2(config)#ip dhcp snooping
S2(config)#ip dhcp snooping v
S2(config)#ip dhcp snooping vl
S2(config)#ip dhcp snooping vlan 10
S2(config)#in
S2(config)#interface in
S2(config)#interface f0/1
S2(config-if)#ip
S2(config-if)#ip dh
S2(config-if)#ip dhcp sn
S2(config-if)#ip dhcp snooping tr
S2(config-if)#ip dhcp snooping trust
S2(config-if)#
S2(config-if)#
```

Figure 26 S2 trunkport as trusted

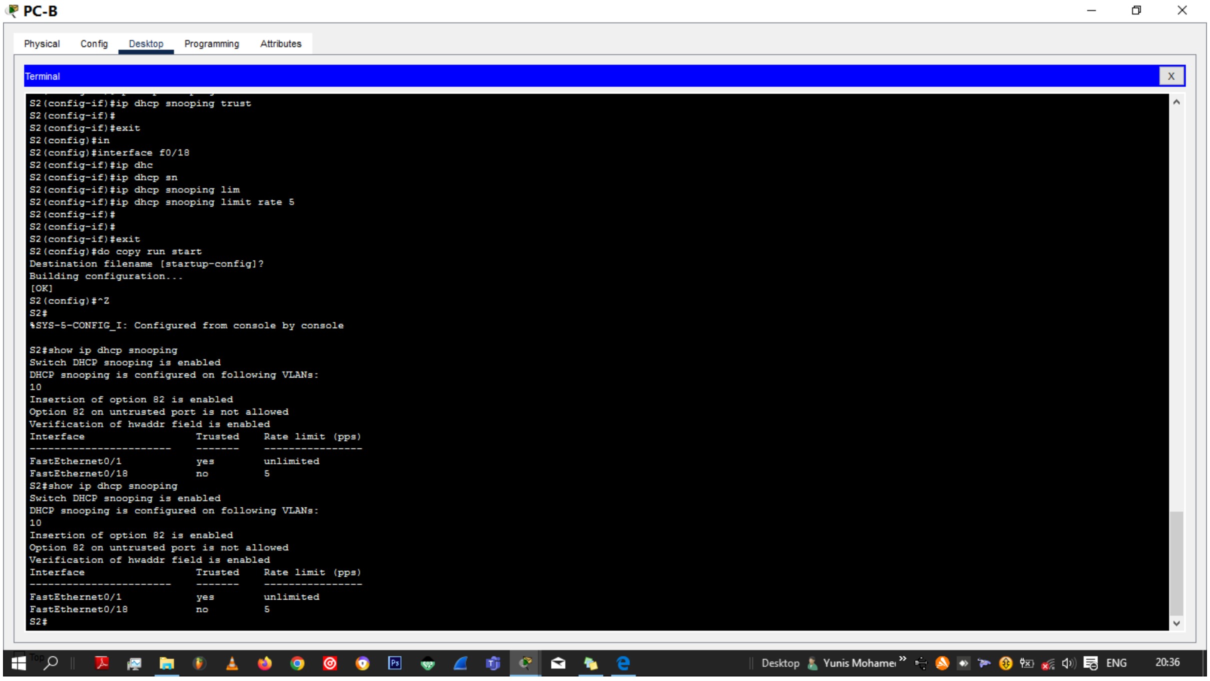
3. Limit the untrusted port, F18 on S2, to five DHCP packets per second.



```
Security Violation Count   : 0

S2#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
  10    0001.C7EB.EDE9    SecureSticky                  Fa0/18        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#ip dhcp s
S2(config)#ip dhcp snooping
S2(config)#ip dhcp snooping v
S2(config)#ip dhcp snooping vl
S2(config)#ip dhcp snooping vlan 10
S2(config)#in
S2(config)#interface in
S2(config)#interface f0/1
S2(config-if)#ip
S2(config-if)#ip dh
S2(config-if)#ip dhcp sn
S2(config-if)#ip dhcp snooping tr
S2(config-if)#ip dhcp snooping trust
S2(config-if)#
S2(config-if)#exit
S2(config)#in
S2(config)#interface f0/18
S2(config-if)#ip dhc
S2(config-if)#ip dhcp sn
S2(config-if)#ip dhcp snooping lim
S2(config-if)#ip dhcp snooping limit rate 5
S2(config-if)#
S2(config-if)#
S2(config-if)#exit
S2(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S2(config)#
```

Figure 27 S2 limit untrusted ports

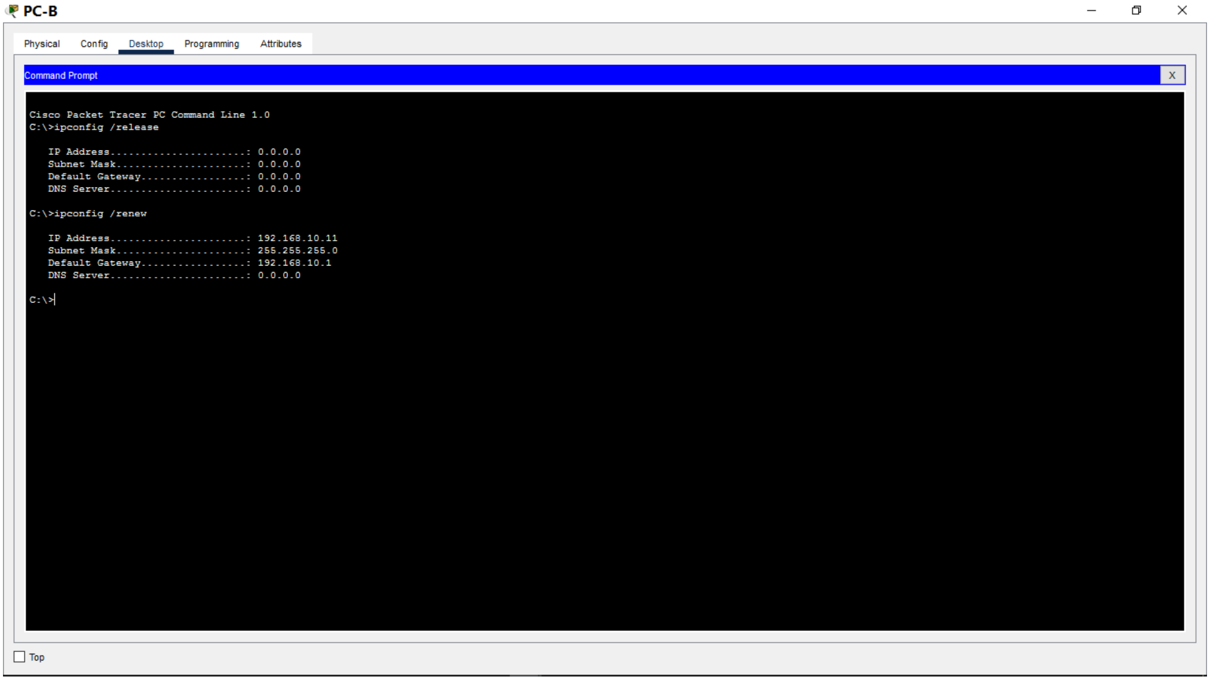
4. Verify DHCP Snooping on S2.



```
S2(config-if)#ip dhcp snooping trust
S2(config-if)#
S2(config-if)#exit
S2(config)#in
S2(config)#interface f0/18
S2(config-if)#ip dhc
S2(config-if)#ip dhcp sn
S2(config-if)#ip dhcp snooping lim
S2(config-if)#ip dhcp snooping limit rate 5
S2(config-if)#
S2(config-if)#
S2(config-if)#exit
S2(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S2(config)#^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
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/1            yes        unlimited
FastEthernet0/18           no         5
S2#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/1            yes        unlimited
FastEthernet0/18           no         5
S2#
```

Figure 28 verify dhcp snooping S2

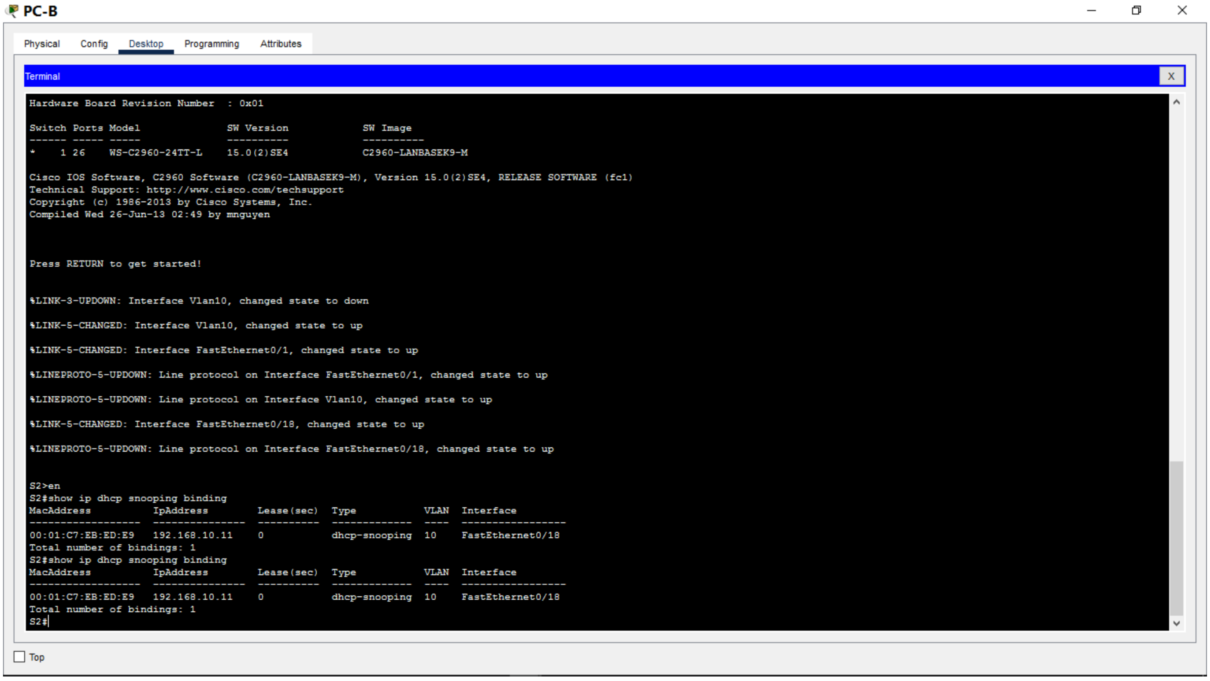
5. From the command prompt on PC-B, release and then renew the IP address.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /release

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

C:\>ipconfig /renew

   IP Address......................: 192.168.10.11
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.10.1
   DNS Server......................: 0.0.0.0

C:\>
```

Figure 29 release and renew ip address

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

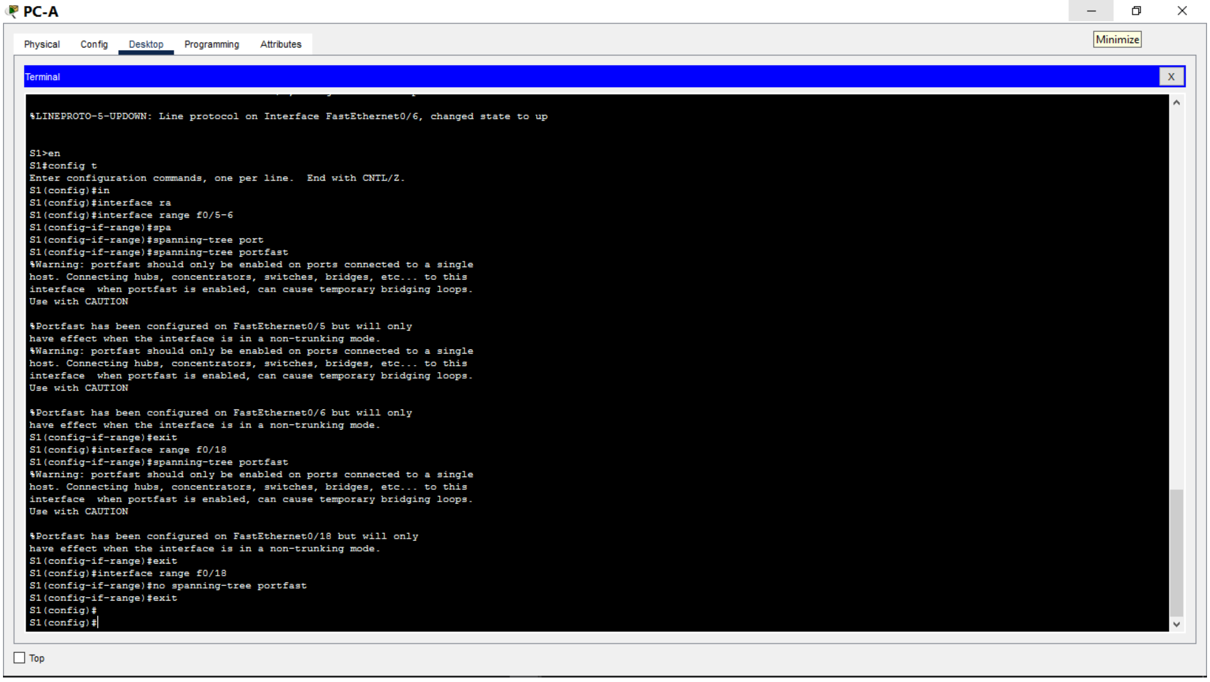


```
Hardware Board Revision Number  : 0x01

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

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



Press RETURN to get started!


%LINK-3-UPDOWN: Interface Vlan10, changed state to down

%LINK-5-CHANGED: 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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

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

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


S2>en
S2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
00:01:C7:EB:ED:E9   192.168.10.11    0           dhcp-snooping  10    FastEthernet0/18
Total number of bindings: 1
S2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
00:01:C7:EB:ED:E9   192.168.10.11    0           dhcp-snooping  10    FastEthernet0/18
Total number of bindings: 1
S2#
```

Figure 30 verify dhcp snooping binding

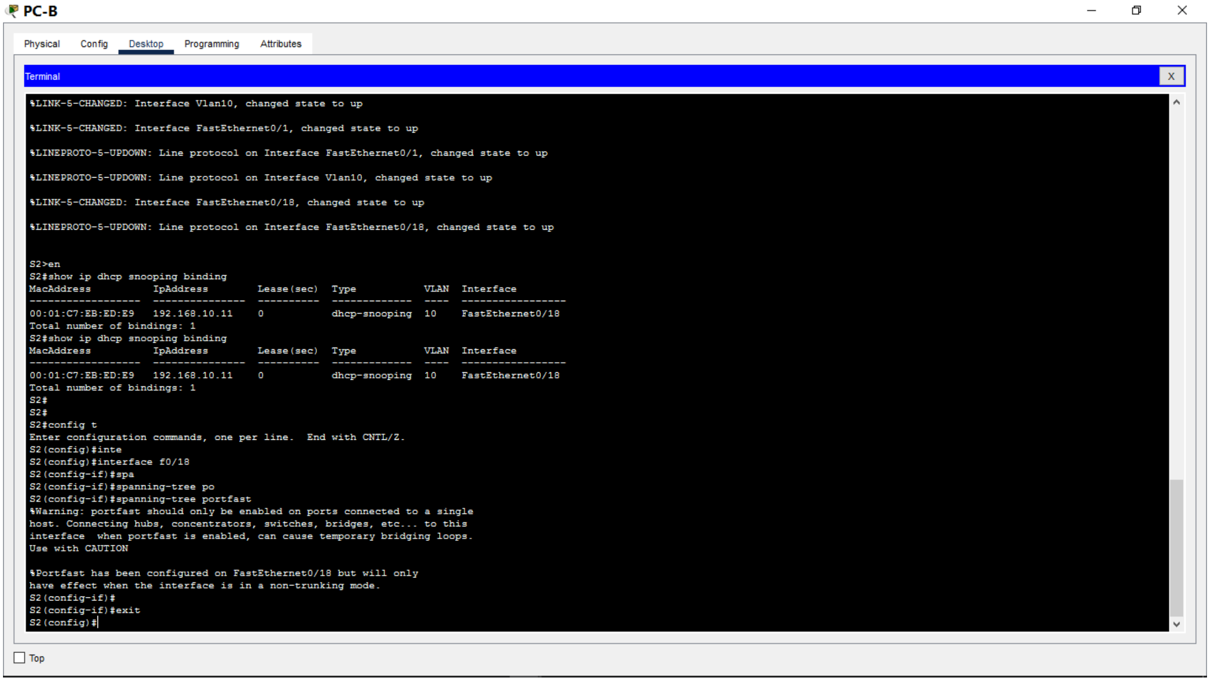
Implement PortFast and BPDU guard.

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



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


S1>en
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#in
S1(config)#interface ra
S1(config)#interface range f0/5-6
S1(config-if-range)#spa
S1(config-if-range)#spanning-tree port
S1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if-range)#exit
S1(config)#interface range 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-range)#exit
S1(config)#interface range f0/18
S1(config-if-range)#no spanning-tree portfast
S1(config-if-range)#exit
S1(config)#
S1(config)#
```

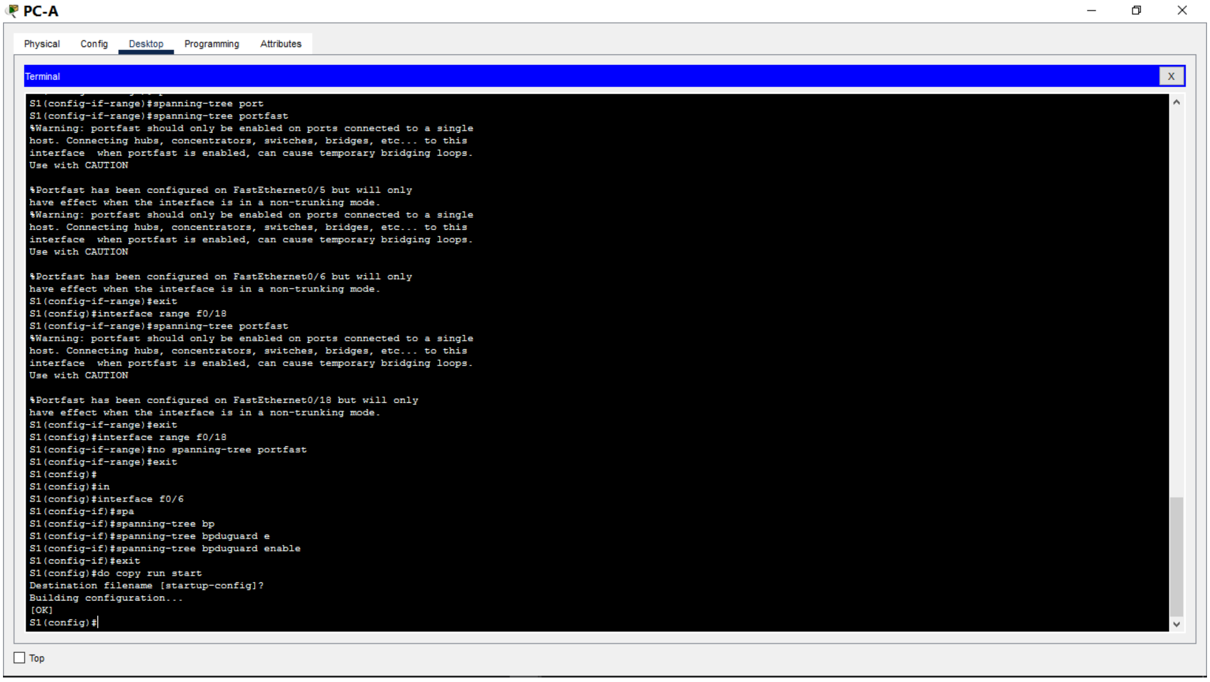
Figure 31 S1 portfast access ports



```
%LINK-5-CHANGED: 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

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

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

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


S2>en
S2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
00:01:C7:EB:ED:E9   192.168.10.11    0           dhcp-snooping  10    FastEthernet0/18
Total number of bindings: 1
S2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
00:01:C7:EB:ED:E9   192.168.10.11    0           dhcp-snooping  10    FastEthernet0/18
Total number of bindings: 1
S2#
S2#
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#inte
S2(config)#interface f0/18
S2(config-if)#spa
S2(config-if)#spanning-tree po
S2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

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

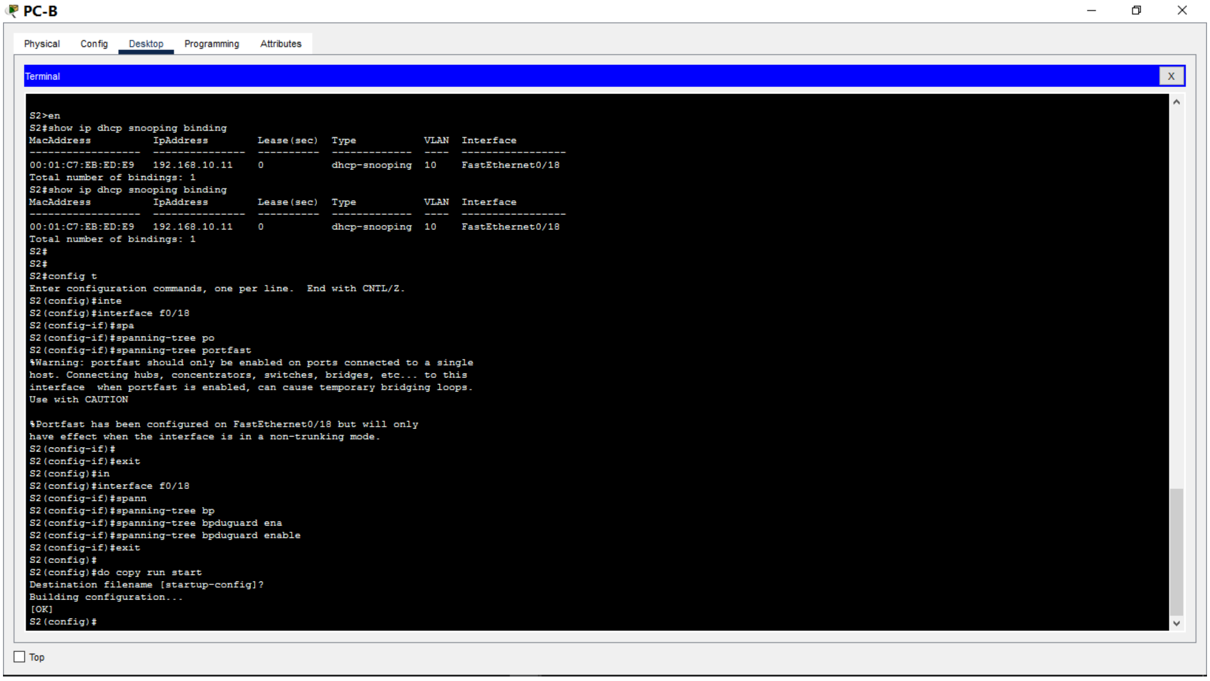
Figure 32 S2 portfast access ports

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



```
S1(config-if-range)#spanning-tree port
S1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/5 but will only
have effect when the interface is in a non-trunking mode.
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/6 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if-range)#exit
S1(config)#interface range 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-range)#exit
S1(config)#interface range f0/18
S1(config-if-range)#no spanning-tree portfast
S1(config-if-range)#exit
S1(config)#
S1(config)#in
S1(config)#interface f0/6
S1(config-if)#spa
S1(config-if)#spanning-tree bp
S1(config-if)#spanning-tree bpduguard e
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#exit
S1(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1(config)#
```

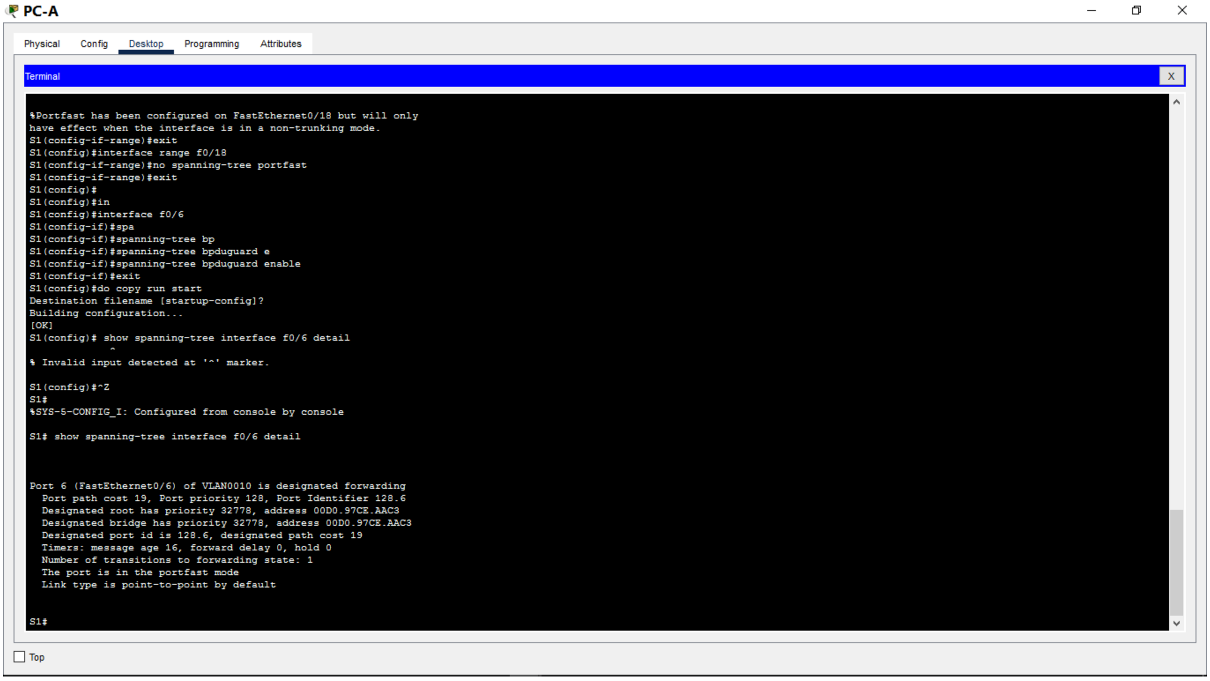
Figure 33 S1 bpdu guard



```
S2>en
S2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
00:01:C7:EB:ED:E9   192.168.10.11    0           dhcp-snooping  10    FastEthernet0/18
Total number of bindings: 1
S2#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  -----------------
00:01:C7:EB:ED:E9   192.168.10.11    0           dhcp-snooping  10    FastEthernet0/18
Total number of bindings: 1
S2#
S2#
S2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S2(config)#inte
S2(config)#interface f0/18
S2(config-if)#spa
S2(config-if)#spanning-tree po
S2(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/18 but will only
have effect when the interface is in a non-trunking mode.
S2(config-if)#
S2(config-if)#exit
S2(config)#in
S2(config)#interface f0/18
S2(config-if)#spann
S2(config-if)#spanning-tree bp
S2(config-if)#spanning-tree bpduguard ena
S2(config-if)#spanning-tree bpduguard enable
S2(config-if)#exit
S2(config)#
S2(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S2(config)#
```

Figure 34 S2 bpdu guard

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

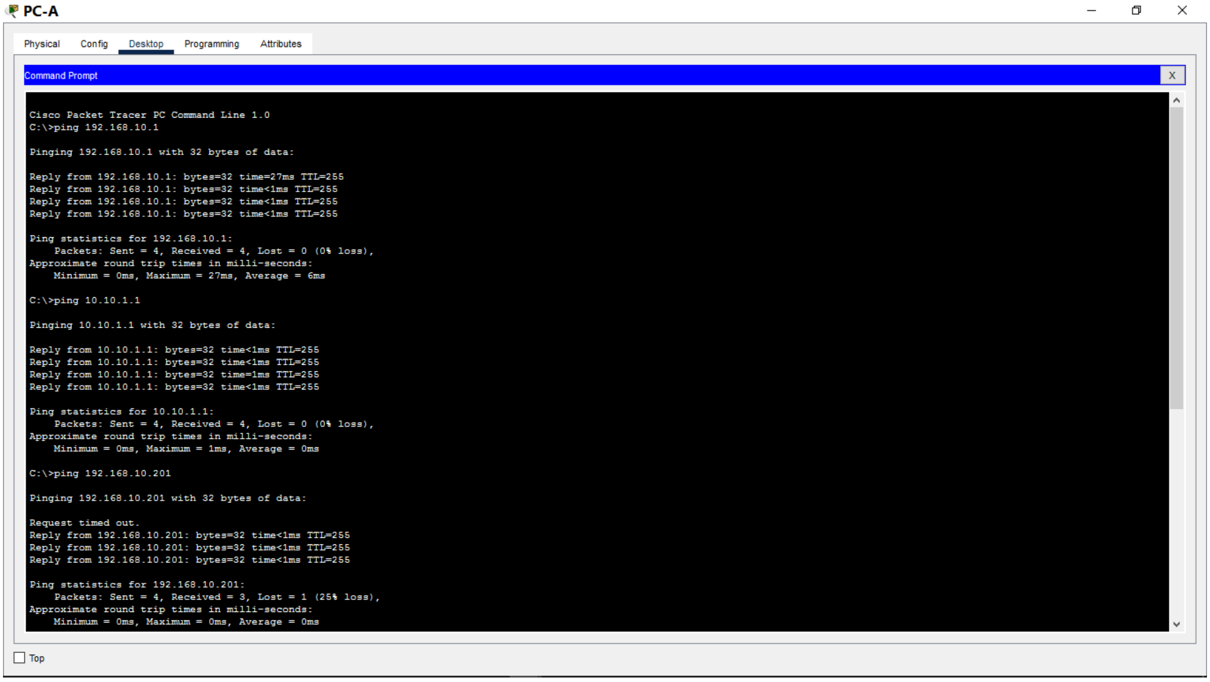


```
%Portfast has been configured on FastEthernet0/18 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if-range)#exit
S1(config)#interface range f0/18
S1(config-if-range)#no spanning-tree portfast
S1(config-if-range)#exit
S1(config)#
S1(config)#in
S1(config)#interface f0/6
S1(config-if)#spa
S1(config-if)#spanning-tree bp
S1(config-if)#spanning-tree bpduguard e
S1(config-if)#spanning-tree bpduguard enable
S1(config-if)#exit
S1(config)#do copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
S1(config)# show spanning-tree interface f0/6 detail
             ^
% Invalid input detected at '^' marker.

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

S1# show spanning-tree interface f0/6 detail



Port 6 (FastEthernet0/6) of VLAN0010 is designated forwarding
  Port path cost 19, Port priority 128, Port Identifier 128.6
  Designated root has priority 32778, address 00D0.97CE.AAC3
  Designated bridge has priority 32778, address 00D0.97CE.AAC3
  Designated port id is 128.6, designated path cost 19
  Timers: message age 16, forward delay 0, hold 0
  Number of transitions to forwarding state: 1
  The port is in the portfast mode
  Link type is point-to-point by default


S1#
```

Figure 35 bpdu and portfast verification

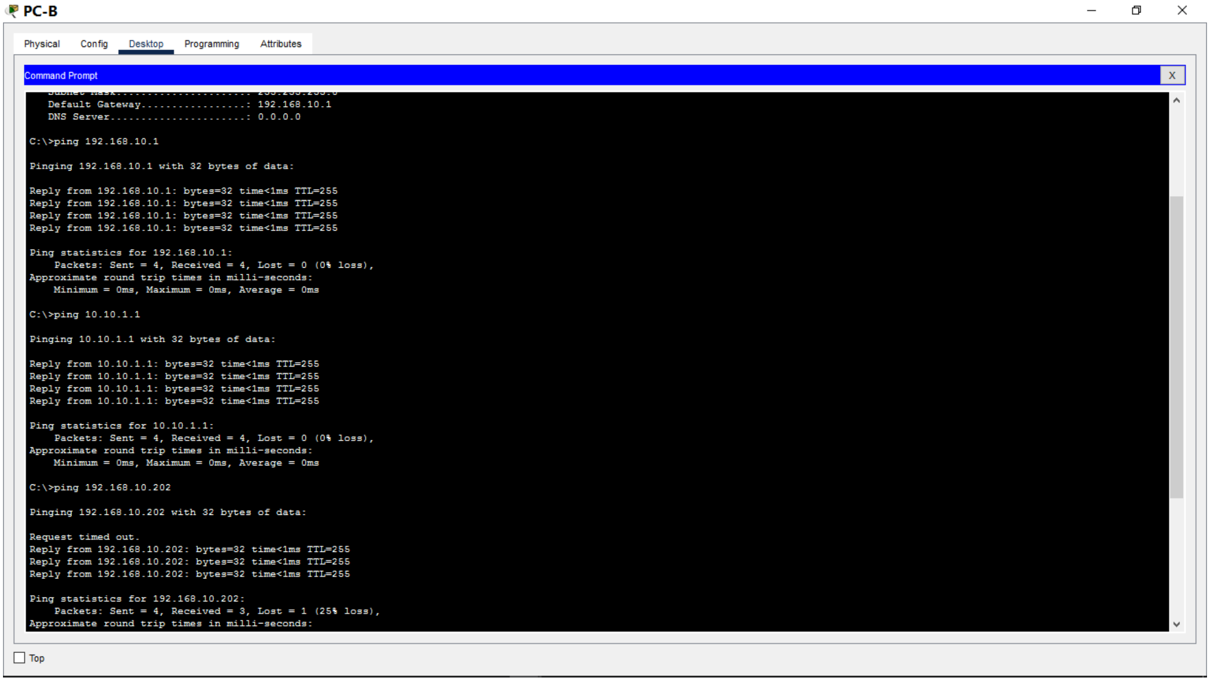
4. Step 7: Verify end-to-end connectivity.

   Conducted pings from PC-A and PC-B to the loopback address and to the vlans interfaces which were successful.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=27ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

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 = 27ms, Average = 6ms

C:\>ping 10.10.1.1

Pinging 10.10.1.1 with 32 bytes of data:

Reply from 10.10.1.1: bytes=32 time<1ms TTL=255
Reply from 10.10.1.1: bytes=32 time<1ms TTL=255
Reply from 10.10.1.1: bytes=32 time=1ms TTL=255
Reply from 10.10.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.10.201

Pinging 192.168.10.201 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.201: bytes=32 time<1ms TTL=255
Reply from 192.168.10.201: bytes=32 time<1ms TTL=255
Reply from 192.168.10.201: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.201:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 36 loopback, S1 S2 ping PC-A



```
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.10.1
   DNS Server......................: 0.0.0.0

C:\>ping 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=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255
Reply from 192.168.10.1: bytes=32 time<1ms TTL=255

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

C:\>ping 10.10.1.1

Pinging 10.10.1.1 with 32 bytes of data:

Reply from 10.10.1.1: bytes=32 time<1ms TTL=255
Reply from 10.10.1.1: bytes=32 time<1ms TTL=255
Reply from 10.10.1.1: bytes=32 time<1ms TTL=255
Reply from 10.10.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.10.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.10.202

Pinging 192.168.10.202 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.202: bytes=32 time<1ms TTL=255
Reply from 192.168.10.202: bytes=32 time<1ms TTL=255
Reply from 192.168.10.202: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.10.202:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
```

Figure 37 loopback, S1 S2 ping PC-B

Conclusion

In conclusion the switch security configuration lab provided me with ample opportunity to enhance and practice skills in securing network switches. I was able to configure vlans on the switches and assign them ports respectively. I came across two types of ports which are trunk and access ports. The trunk ports help provide connection from the router to the switches while the access ports help communication from switches to the client devices i.e. computers. All unused access ports are usually removed from the native vlan and put in another vlan to prevent intruders from using them. The Dynamic trunking protocols (DTP) is turned off or to nonegotiate state to prevent it from automatically establishing trunk links with various neighbouring switches. I was able to configure port security violation modes which define what steps a switch should take when a violation occurs in a port. This mode include protect, restrict and shutdown. Configuring dhcp snooping security help prevent rogue dhcp servers from distributing incorrect or malicious IP configuration. It also provide network visibility by maintaining a DHCP binding database. One can also configure port security by implementing the MAC address sticky feature which learns and bind mac addresses of devices connected to a specific port. Through features like portfast and BPDU guard (bridge protocol data unit), a network administrator can improve network security, prevent potential loops and enhance network performance.