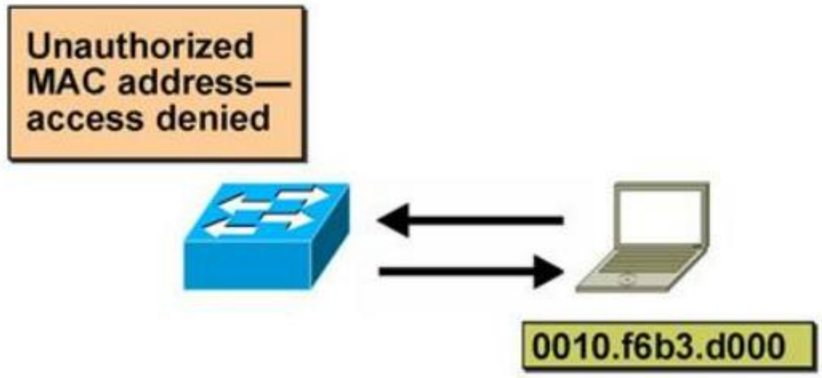
Introduction :

Switch is a network device, which is configured to connect and maintain communication channel between various devices. Ethernet ports are present on a switch, which are used to connect devices, such as Router, computer system and Laptop in the network. To connect all these networks, Ethernet cables are used. MAC address of these connected devices is used by switch to identify them and provide them with the requested service. It is a crucial task to secure these ports, so that only authorized users are able to connect their systems into the network through a switch. Before configuration of any switch in an organizational network, port security is considered, as it ensures that authentic and authorized user is connected within the network. This security feature of Cisco IOS Switches can only be configured on access ports and by default, this feature is disabled.



Port security restricts port access by MAC address.

Objectives :

Part 1: Configure Port Security

Part 2: Verify Port Security

Background :

In this activity, you will configure and verify port security on a switch. Port security allows you to restrict a port’s ingress traffic by limiting the MAC addresses that are allowed to send traffic into the port.

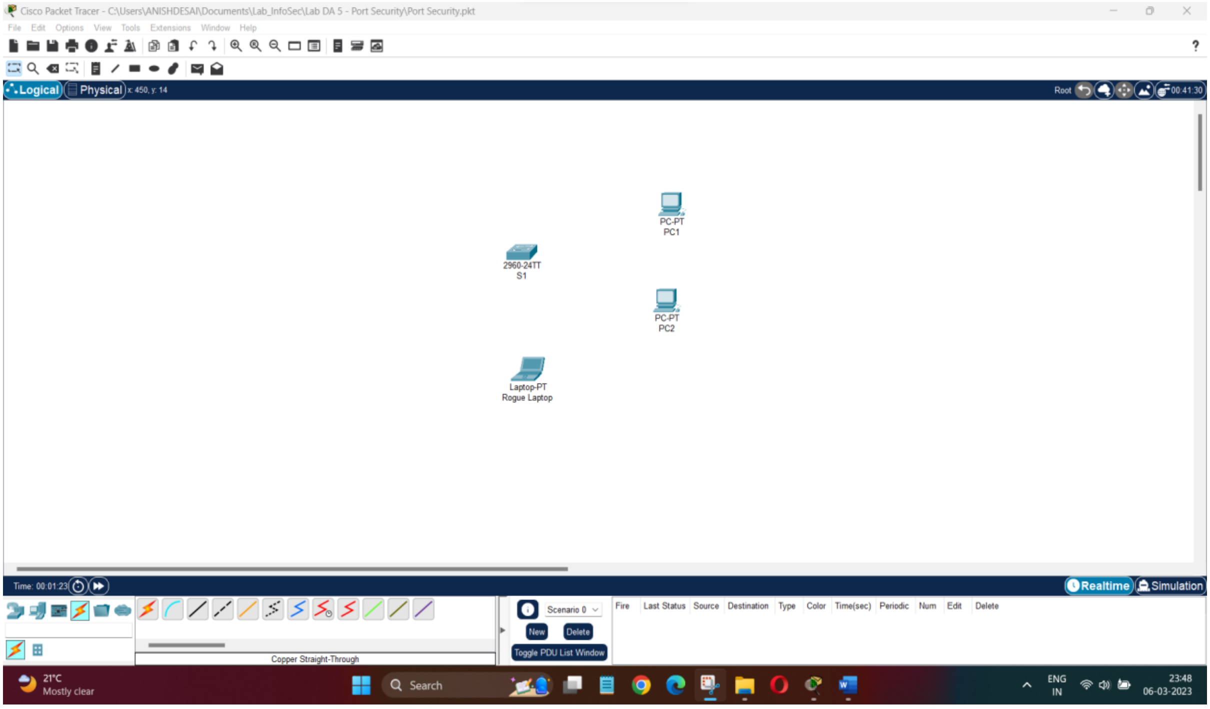
Configuration of Port Security using CISCO Packet Tracer

Note : For all the demonstrations, timestamp is provided at the bottom-right of the screen snapshots.

Step 1 : Outlining the components and their connections

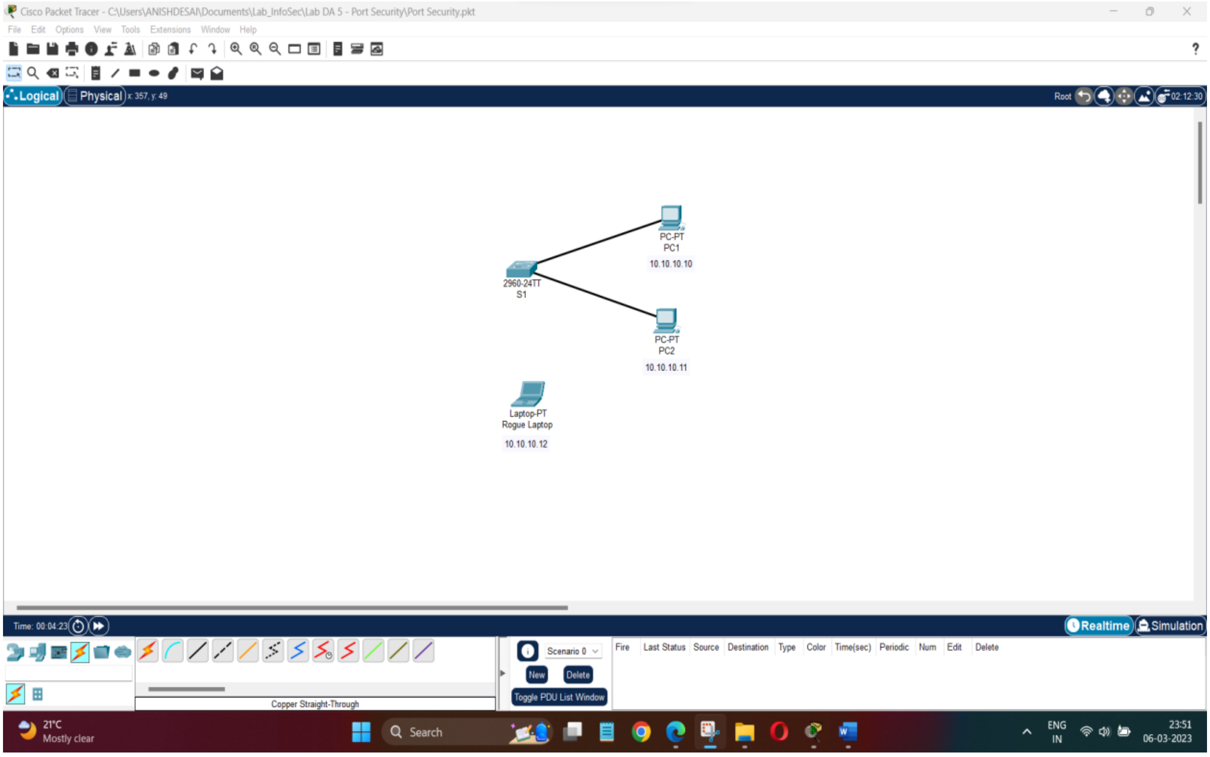
Components used include :

1. Switch 2960-24TT : S1
2. PCs : PC1 and PC2
3. Laptop – Rogue Laptop



Step 2 : Making Topology and Assigning IP Addresses

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	10.10.10.2	255.255.255.0
PC1	Fa0	10.10.10.10	255.0.0.0
PC2	Fa0	10.10.10.11	255.0.0.0
Rogue Laptop	Fa0	10.10.10.12	255.0.0.0

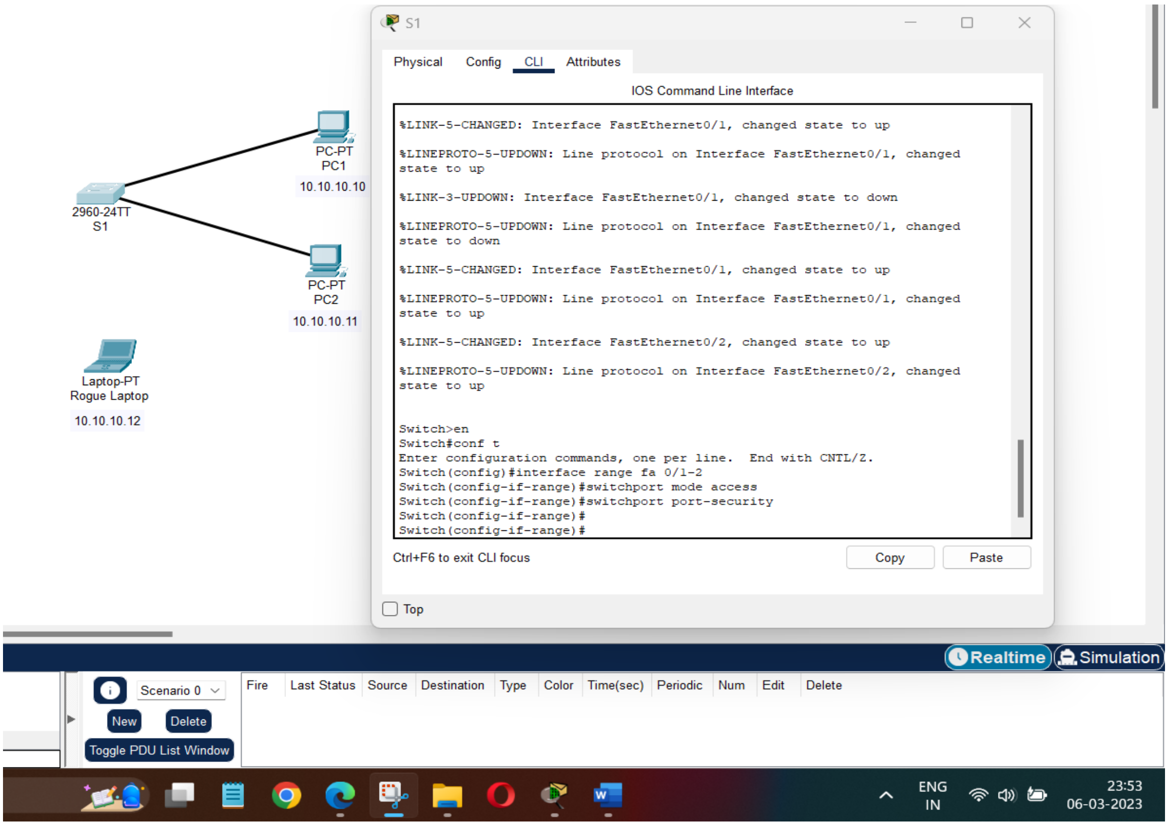


Part 1 : Configure Port Security

Step 1 : Enable Port Security

Access the command line for S1 and enable port security on Fast Ethernet ports 0/1 and 0/2.

```
S1(config)# interface range f0/1 – 2
S1(config-if-range)#switchport mode access
S1(config-if-range)# switchport port-security
```

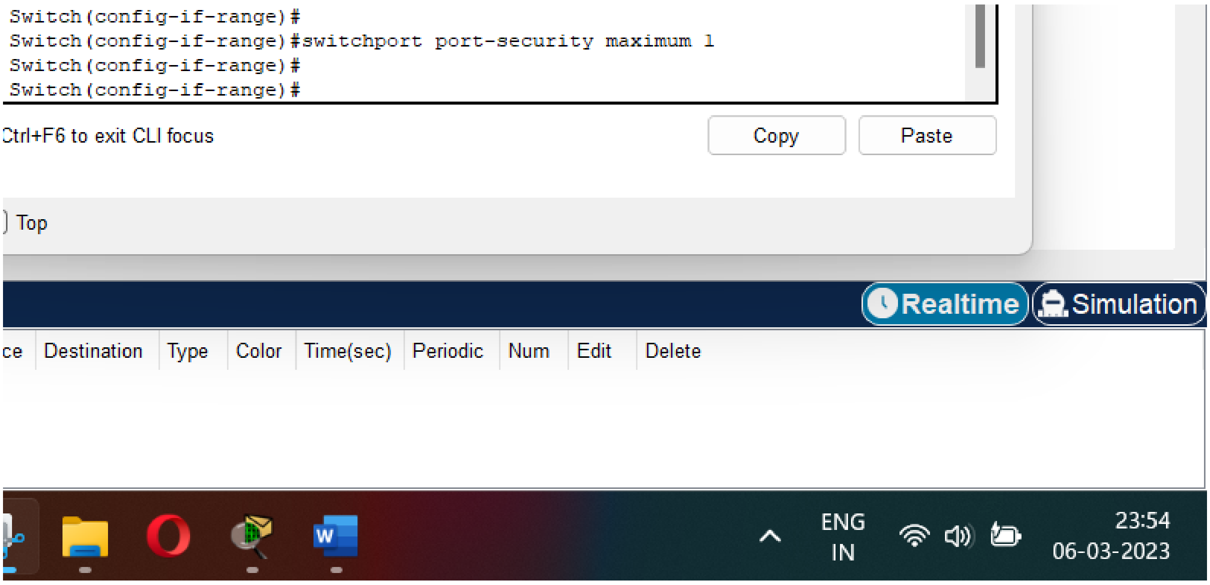


```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

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

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

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

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

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

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

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
state to up


Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fa 0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#
Switch(config-if-range)#
```

Step 2 : Set maximum

Set the maximum so that only one device can access the Fast Ethernet ports 0/1 and 0/2.

S1(config-if-range)# switchport port-security maximum 1

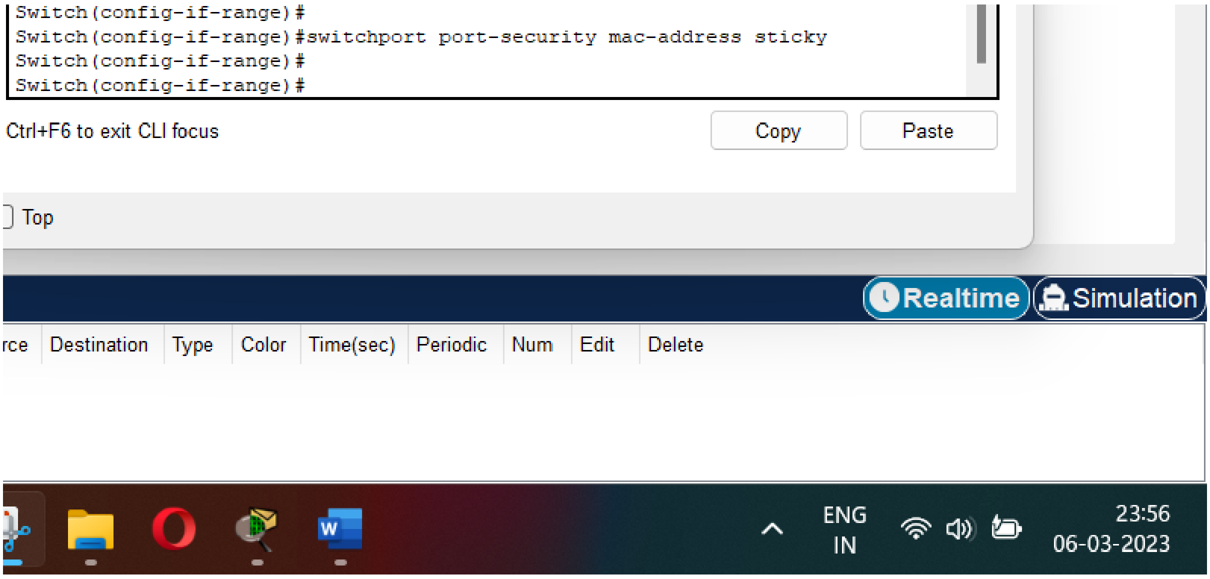


```
Switch(config-if-range)#
Switch(config-if-range)#switchport port-security maximum 1
Switch(config-if-range)#
Switch(config-if-range)#
```

Step 3 : Secure the ports

Secure the ports so that the MAC address of a device is dynamically learned and added to the running configuration.

S1(config-if-range)# switchport port-security mac-address sticky

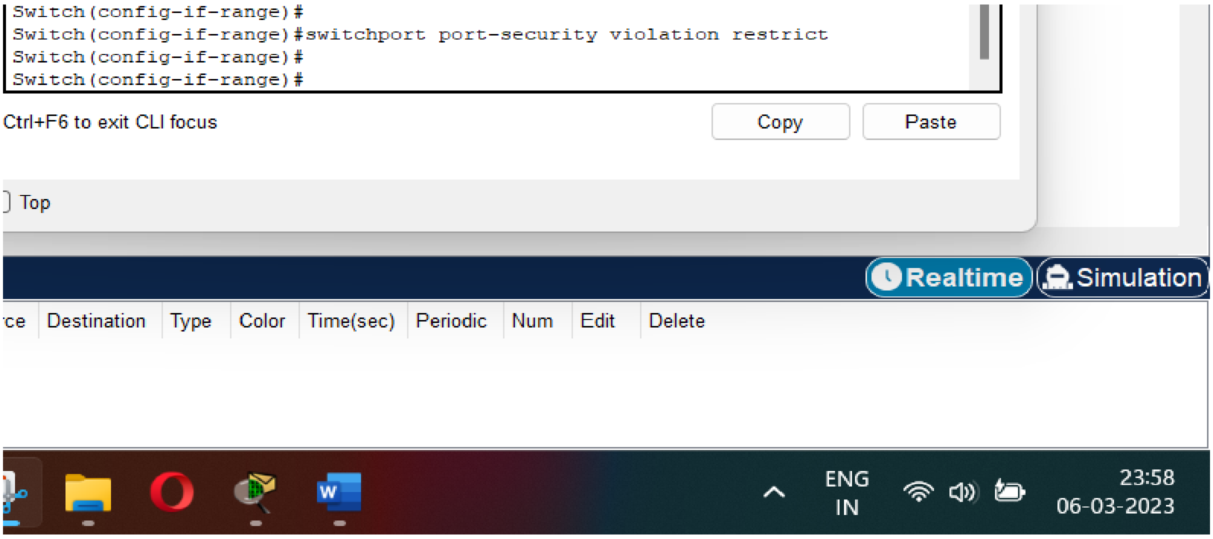


```
Switch(config-if-range)#
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#
Switch(config-if-range)#
```

Step 4 : Set violation mode

Set the violation mode so that the Fast Ethernet ports 0/1 and 0/2 are not disabled when a violation occurs, but a notification of the security violation is generated and packets from the unknown source are dropped.

S1(config-if-range)# switchport port-security violation restrict



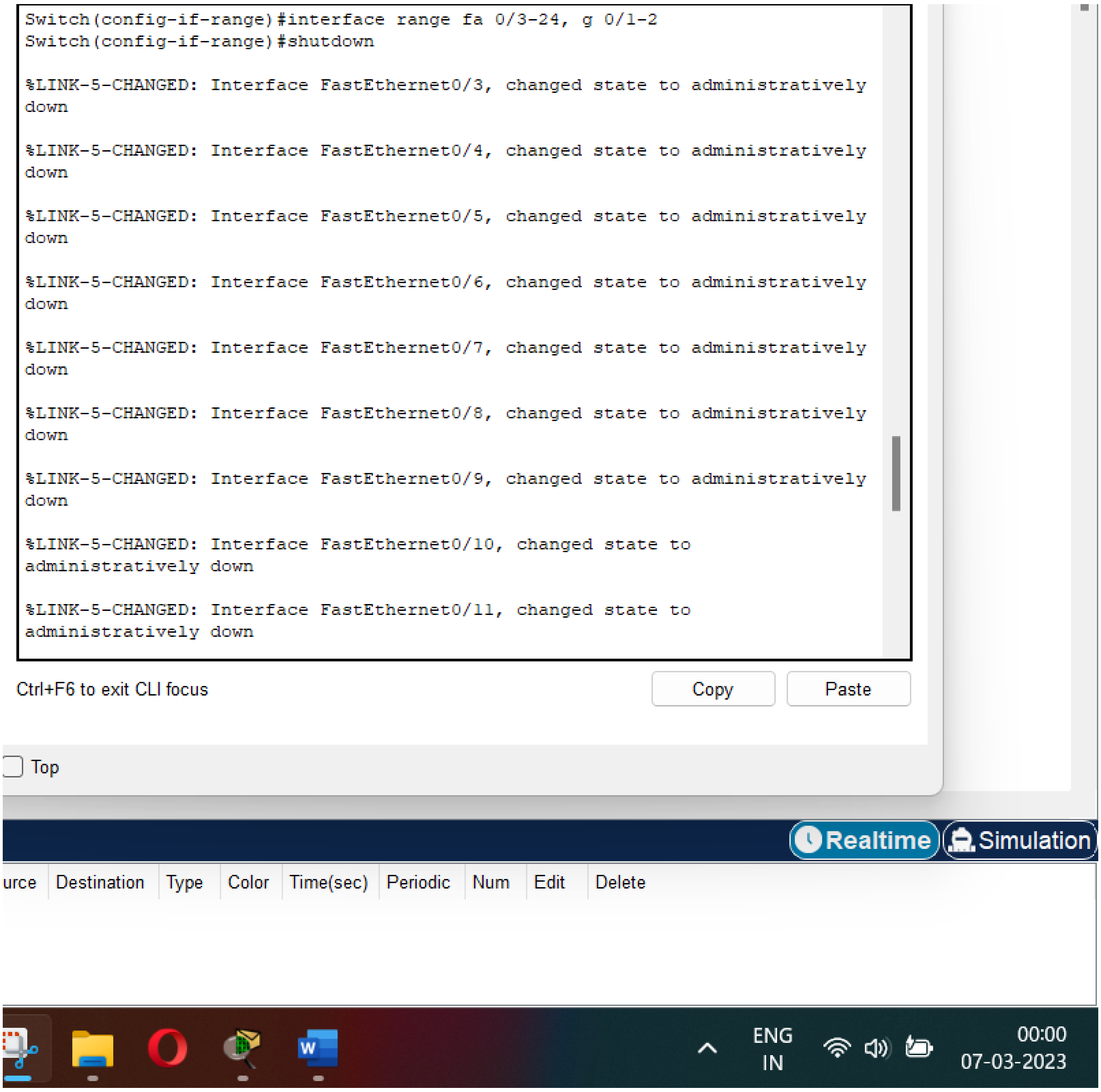
```
Switch(config-if-range)#
Switch(config-if-range)#switchport port-security violation restrict
Switch(config-if-range)#
Switch(config-if-range)#
```

Step 5 : Disable unused ports

Disable all the remaining unused ports. Use the range keyword to apply this configuration to all the ports simultaneously.

S1(config-if-range)# interface range f0/3 - 24, g0/1 - 2

S1(config-if-range)# shutdown

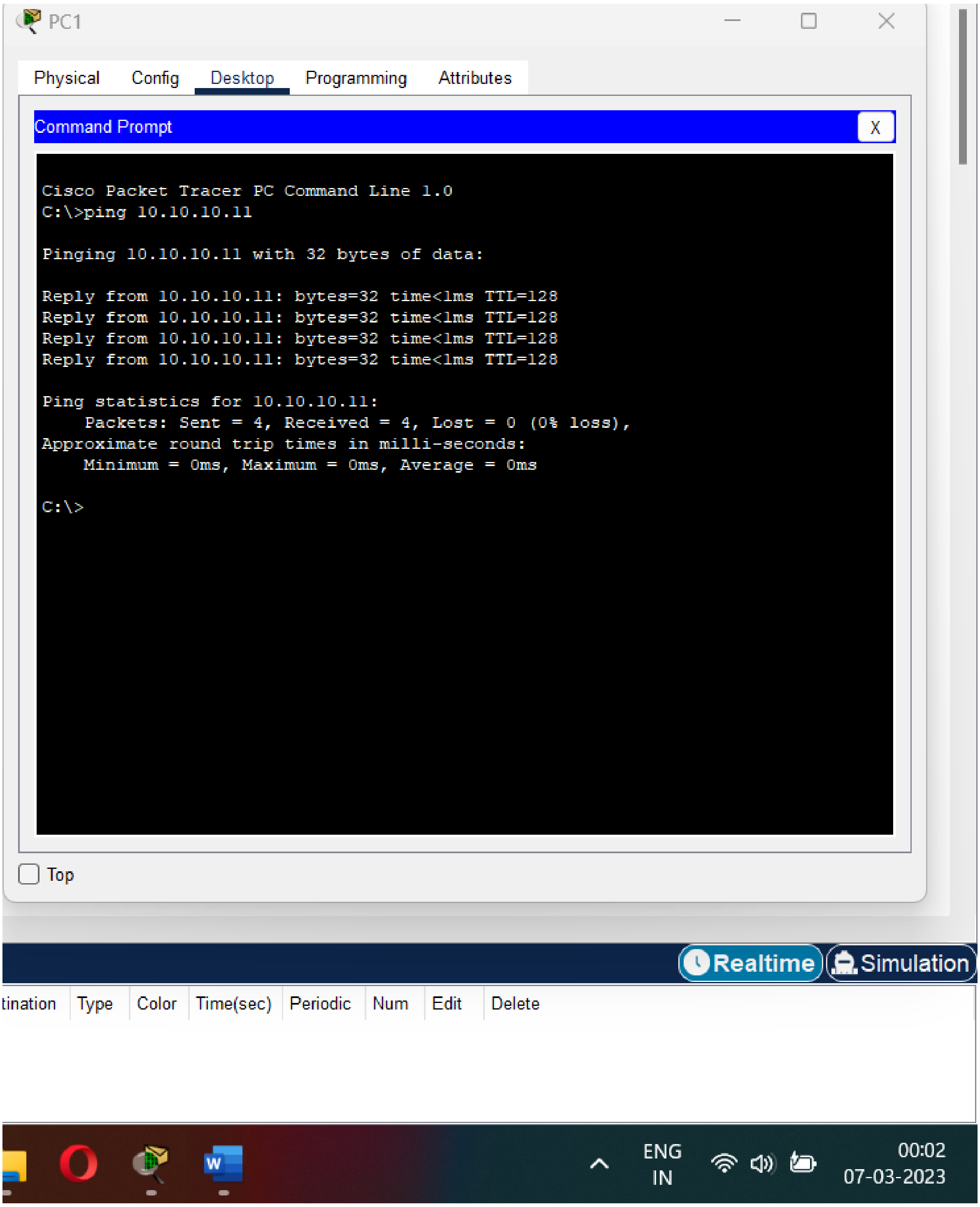


```
Switch(config-if-range)#interface range fa 0/3-24, g 0/1-2
Switch(config-if-range)#shutdown

%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
```

Part 2 : Verify Port Security

Step 1 : Ping

From PC1, ping PC2.

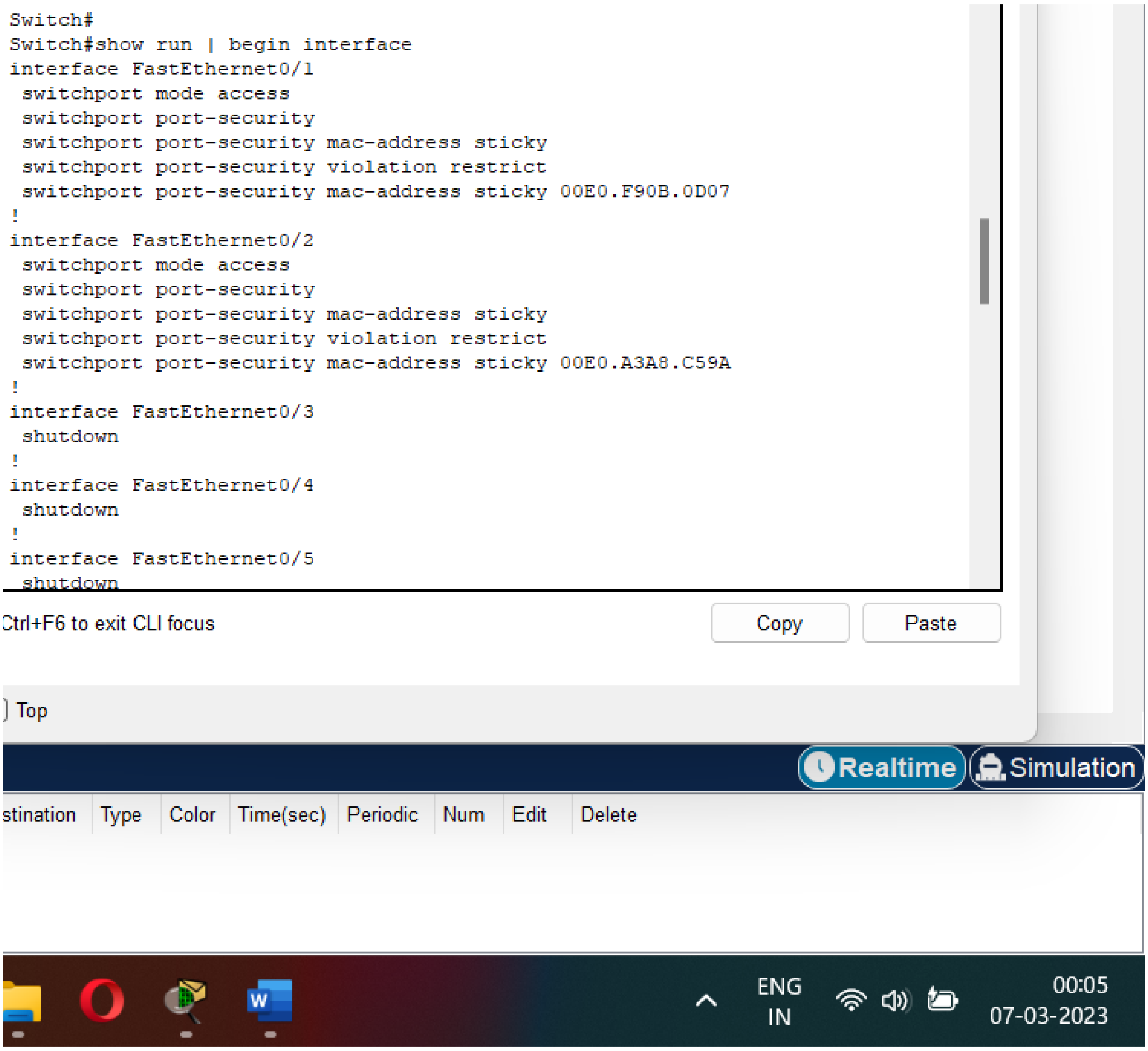


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.11

Pinging 10.10.10.11 with 32 bytes of data:

Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Step 2 : Verify enabled port security

Verify that port security is enabled and the MAC addresses of PC1 and PC2 were added to the running configuration.

S1# show run | begin interface



```
Switch#
Switch#show run | begin interface
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00E0.F90B.0D07
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security mac-address sticky 00E0.A3A8.C59A
!
interface FastEthernet0/3
 shutdown
!
interface FastEthernet0/4
 shutdown
!
interface FastEthernet0/5
 shutdown
```

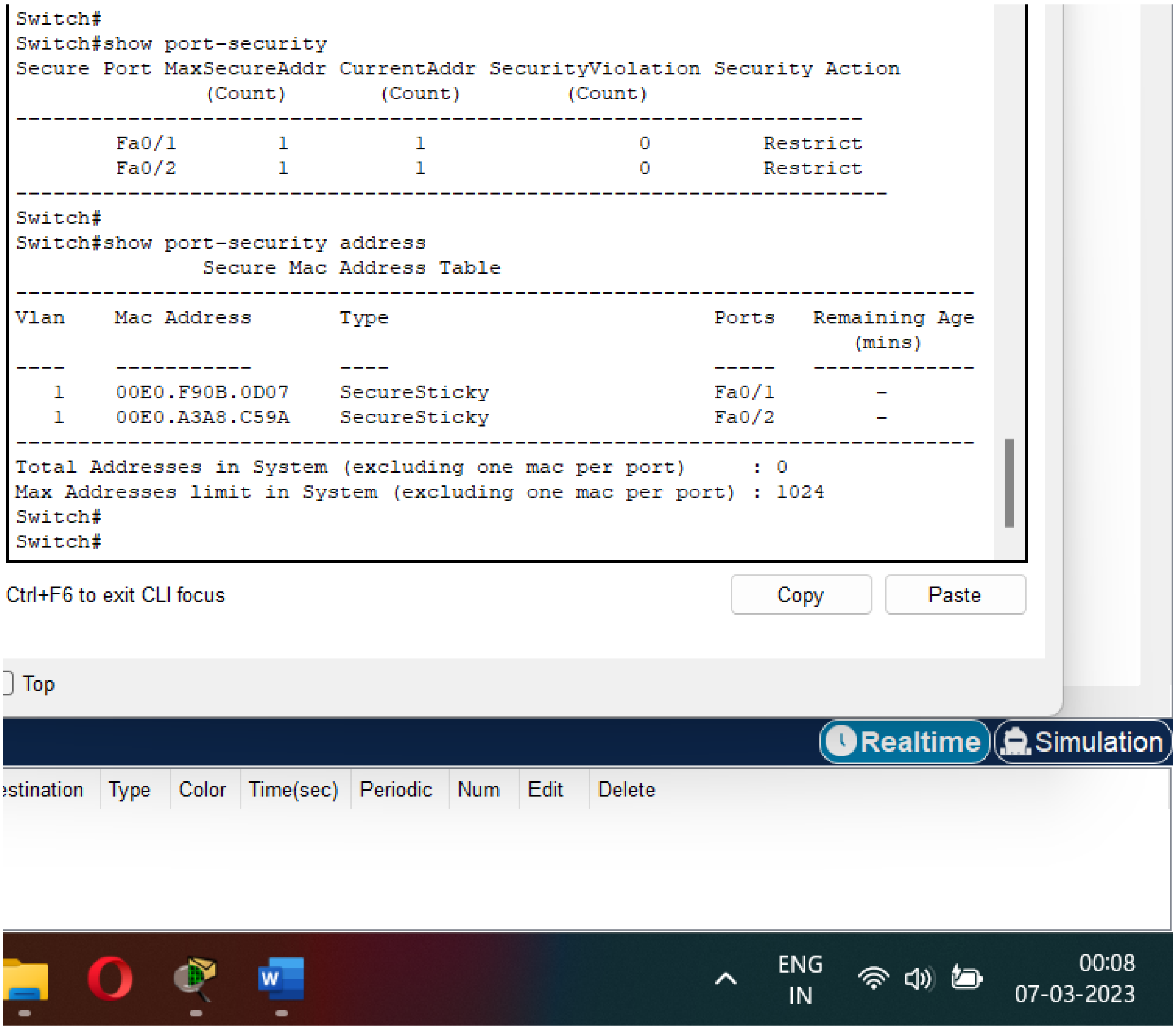
As we can notice, port security has been enabled and MAC addresses of interfaces fa0/1 and fa0/2 (essentially PC1 and PC2) have been added.

Step 3 : Review configuration information

Use port-security show commands to display configuration information.

S1# show port-security

S1# show port-security address

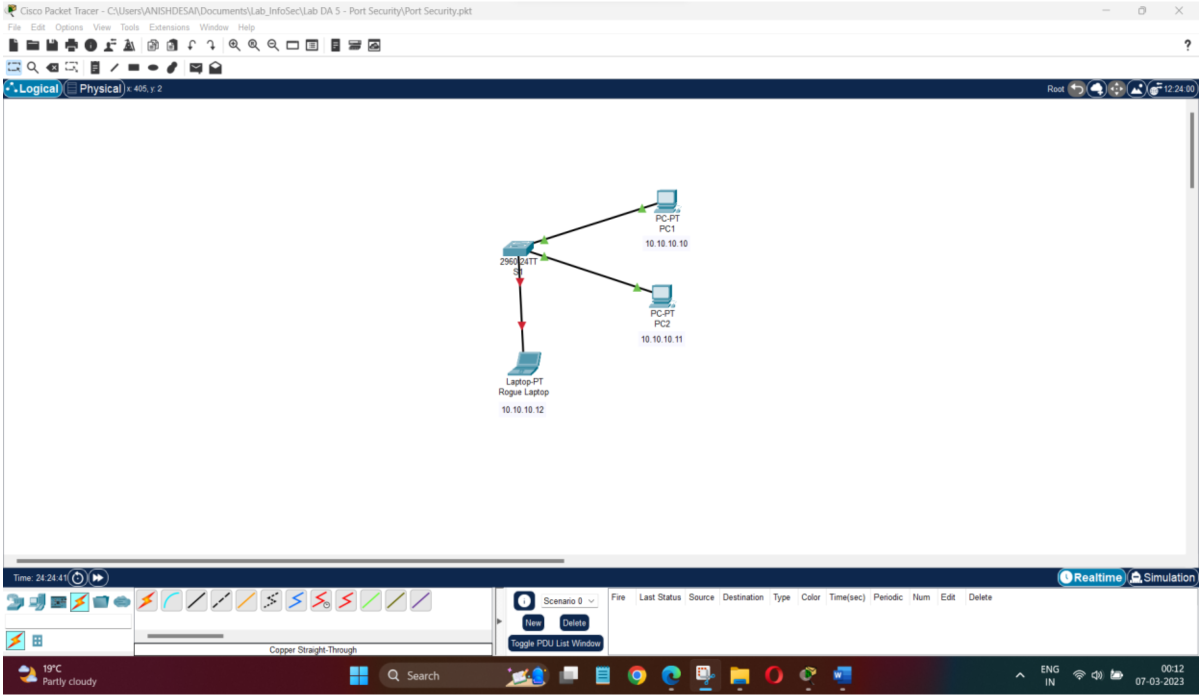


```
Switch#
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
--------------------------------------------------------------------
        Fa0/1        1          1                 0         Restrict
        Fa0/2        1          1                 0         Restrict
----------------------------------------------------------------------
Switch#
Switch#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
   1    00E0.F90B.0D07    SecureSticky                  Fa0/1        -
   1    00E0.A3A8.C59A    SecureSticky                  Fa0/2        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
Switch#
Switch#
```

As we can see, Maximum and Current address are 1 and No security violations as of now. Mode is Restrict as set. Further, we can see MAC addresses of both the PCs and the ports connected.

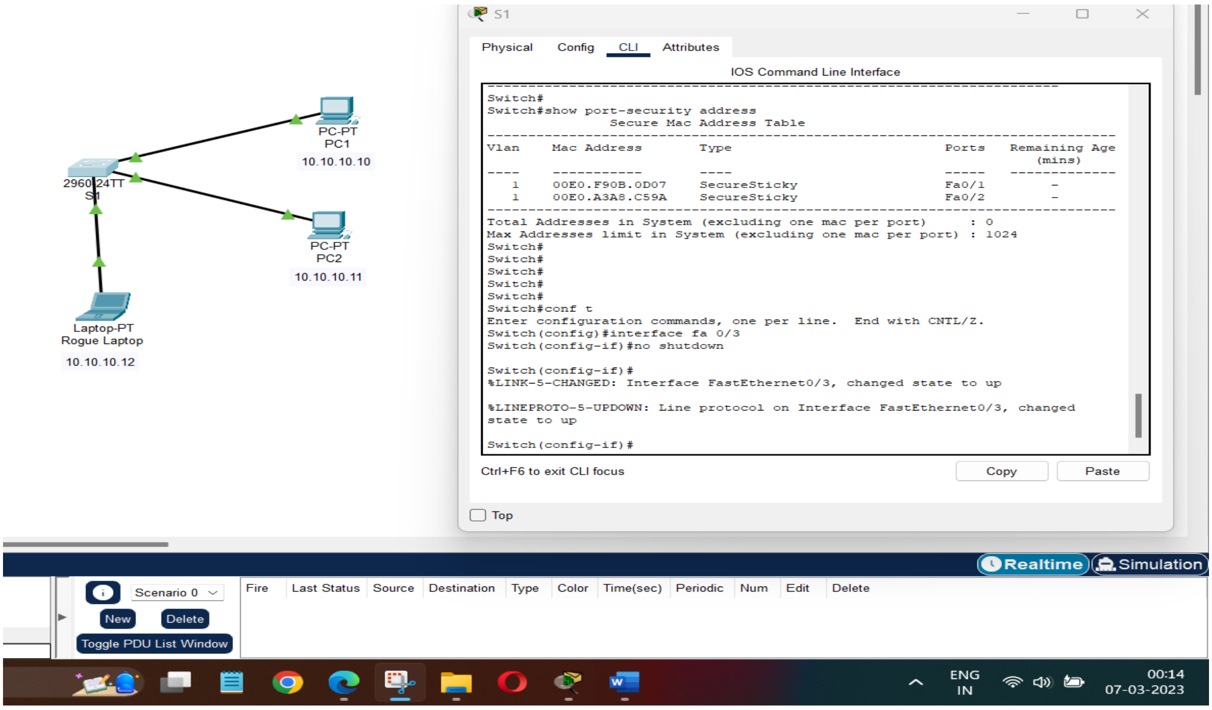
Step 4 : Review using Rogue Laptop

Attach Rogue Laptop to any unused switch port and notice that the link lights are red.

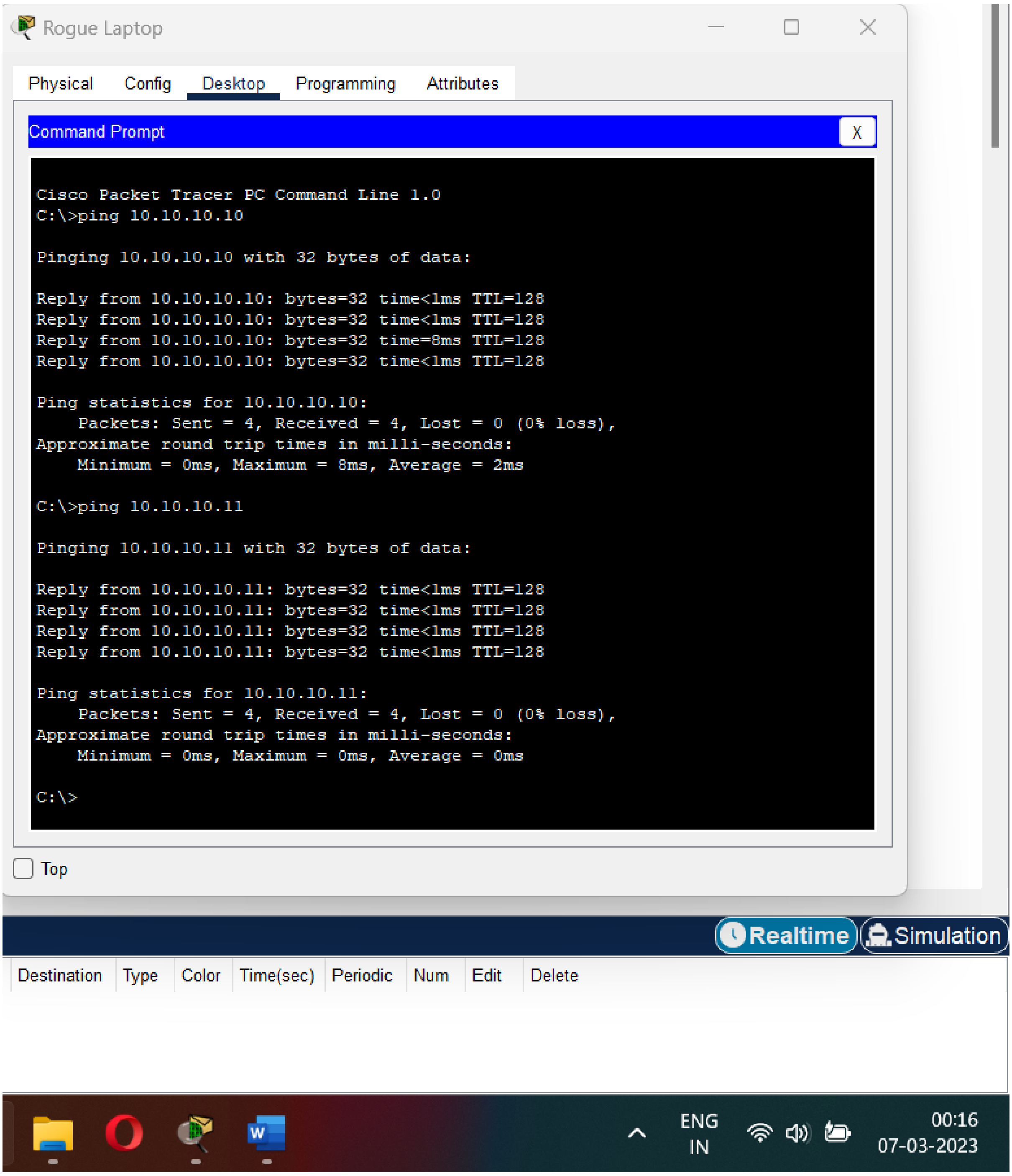


Step 5 : Verify using Rogue Laptop

Enable the port and verify that Rogue Laptop can ping PC1 and PC2. After verification, shut down the port connected to Rogue Laptop.



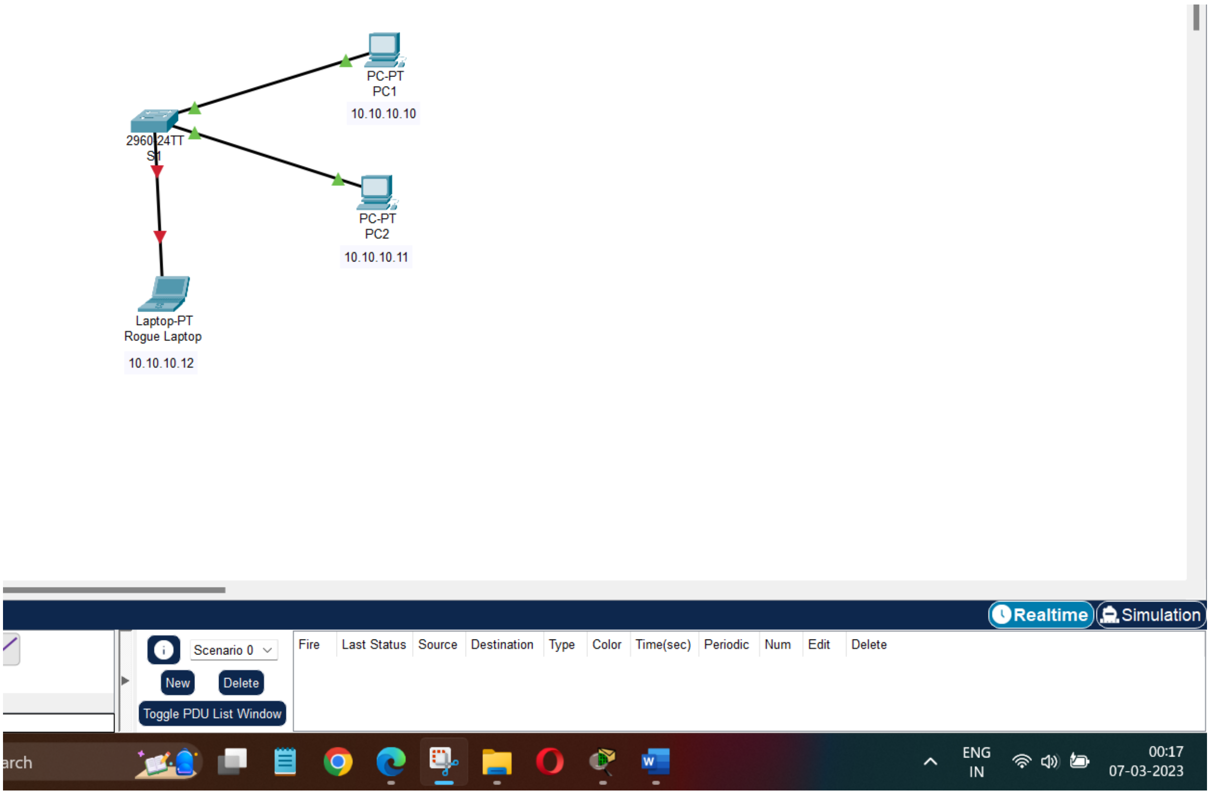
```
Switch#
Switch#show port-security address
               Secure Mac Address Table
-----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
   1    00E0.F90B.0D07    SecureSticky                  Fa0/1        -
   1    00E0.A3A8.C59A    SecureSticky                  Fa0/2        -
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa 0/3
Switch(config-if)#no shutdown

Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

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

Switch(config-if)#
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time=8ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 8ms, Average = 2ms

C:\>ping 10.10.10.11

Pinging 10.10.10.11 with 32 bytes of data:

Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128
Reply from 10.10.10.11: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

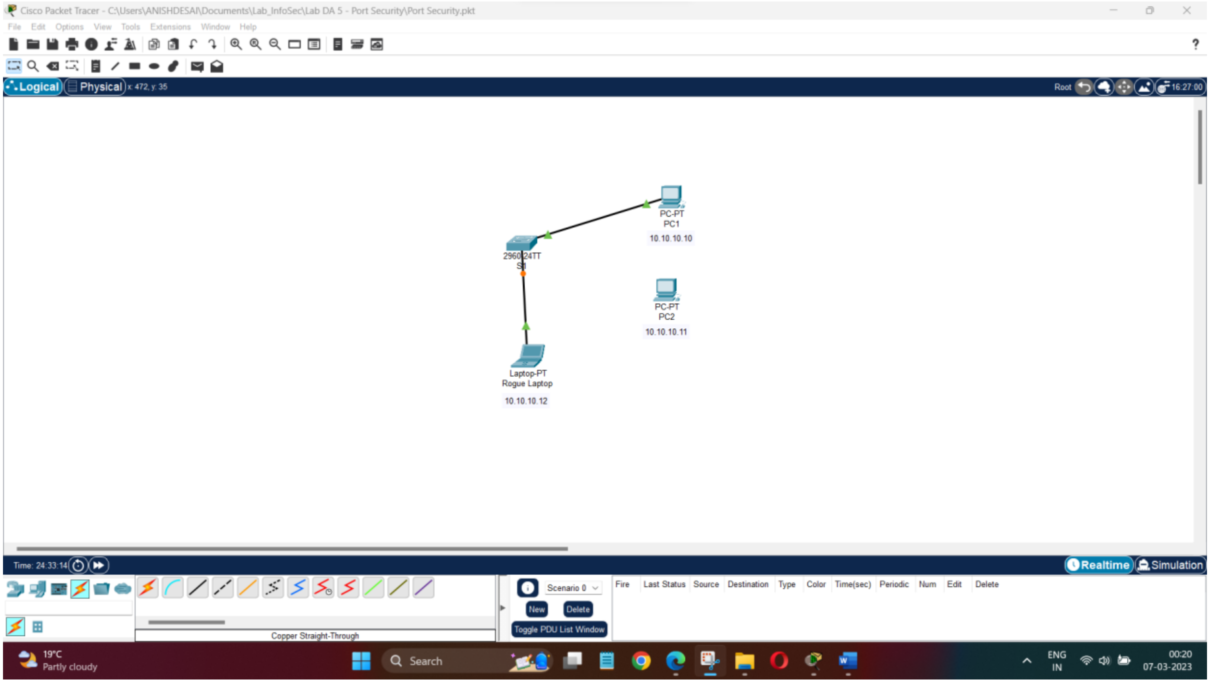
Ping to PC1 and PC2 from Rogue Laptop successful.

Shutdown the interface now.

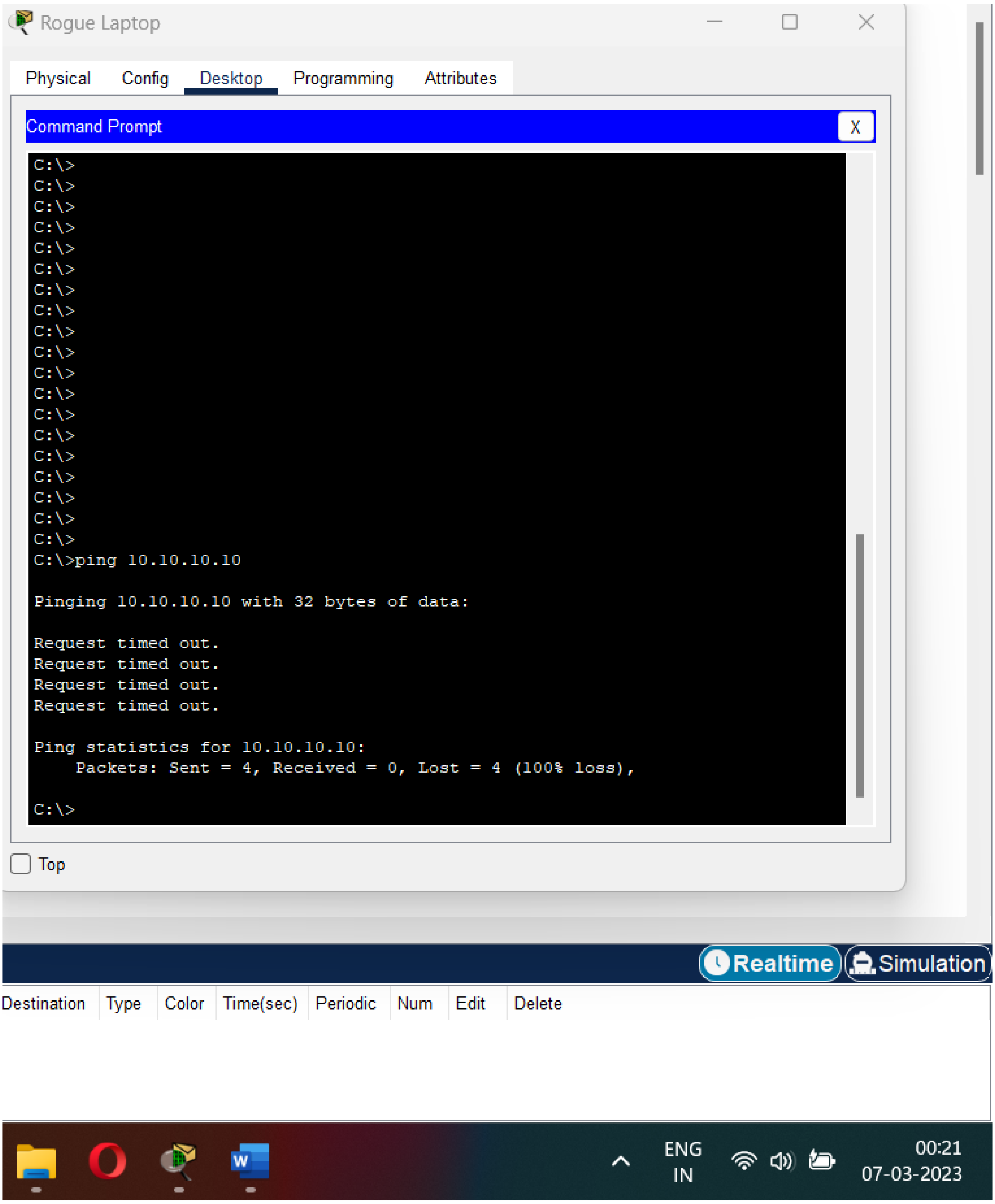


Step 6 : Verify using Rogue Laptop in place of PC2

Disconnect PC2 and connect Rogue Laptop to F0/2, which is the port to which PC2 was originally connected. Verify that Rogue Laptop is unable to ping PC1.



PC2 disconnected and Rogue Laptop connected to port Fa0/2 in which PC2 was originally connected.



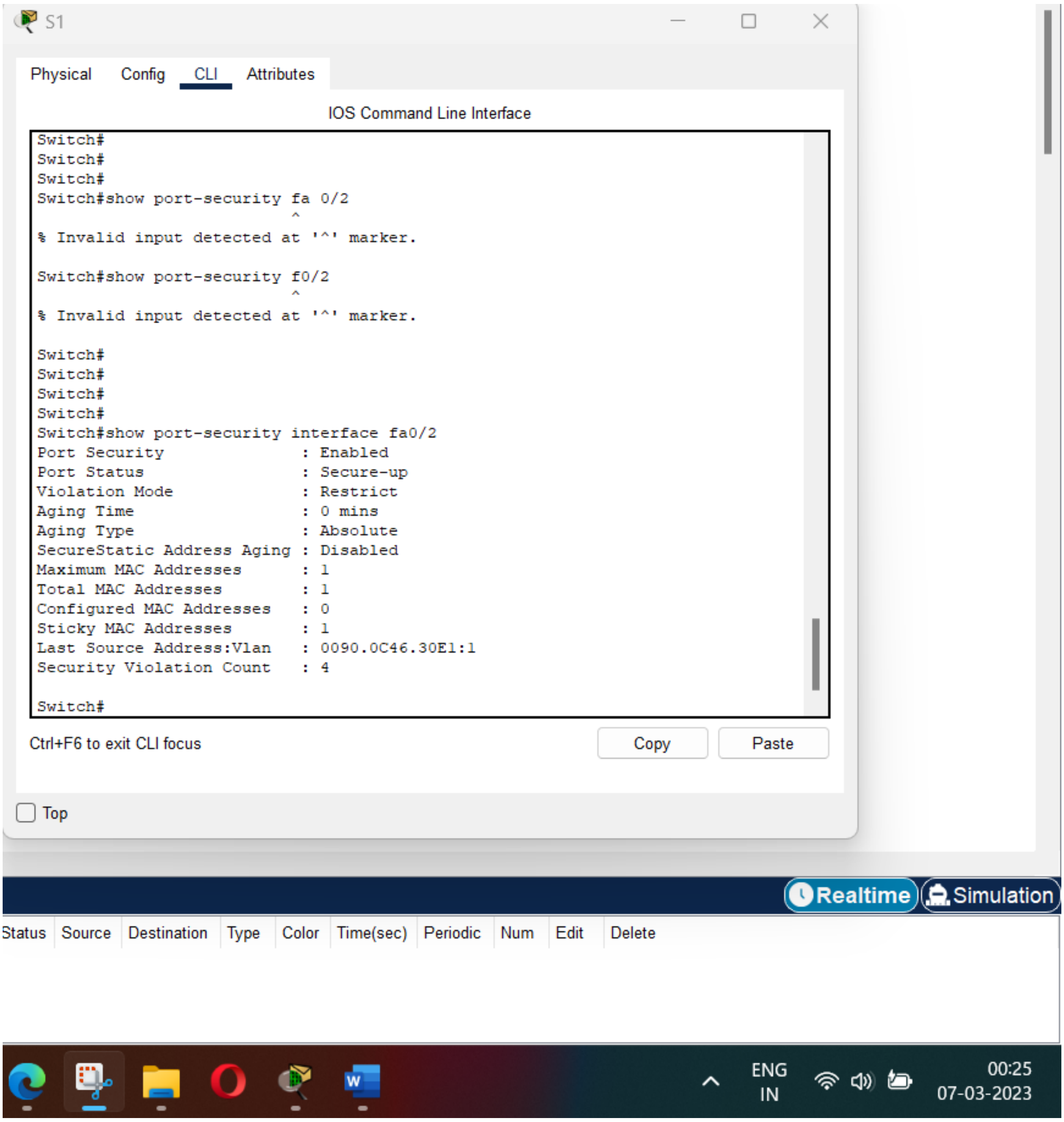
```
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Rogue Laptop unable to ping PC1 since only PC2 is allowed to connect to port Fa0/2.

Step 7 : Review port security violation

Display the port security violations for the port to which Rogue Laptop is connected.

S1# show port-security interface f0/2



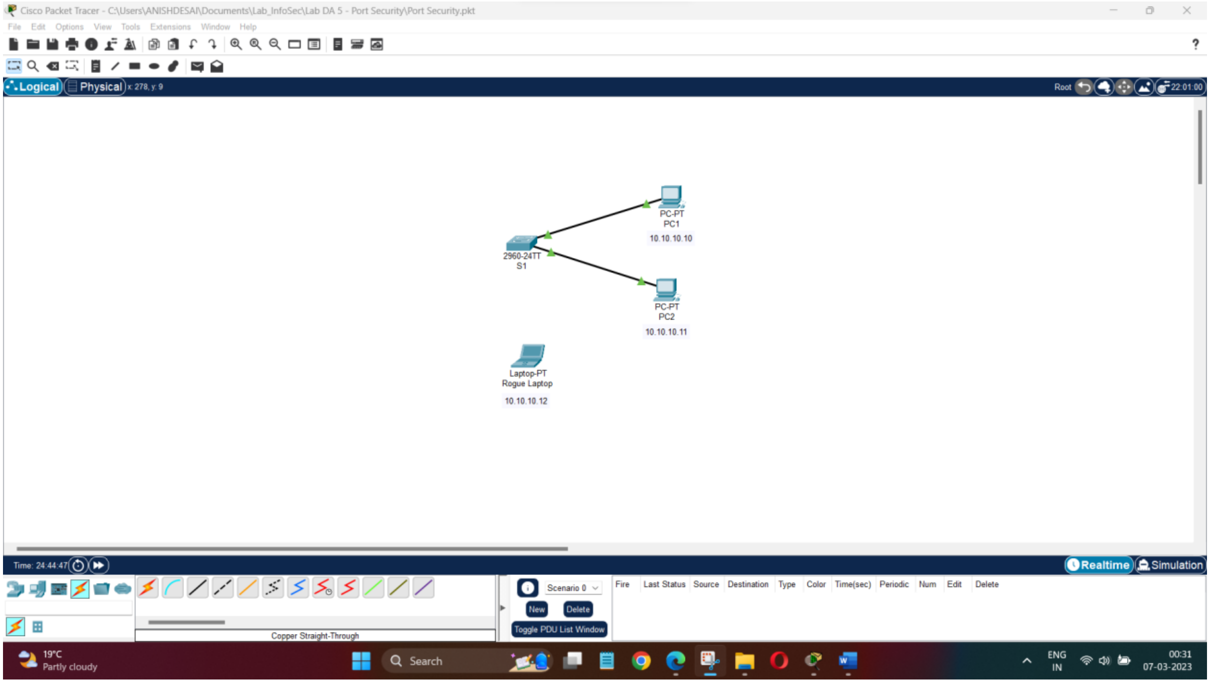
```
Switch#
Switch#
Switch#
Switch#show port-security fa 0/2
                              ^
% Invalid input detected at '^' marker.

Switch#show port-security f0/2
                              ^
% Invalid input detected at '^' marker.

Switch#
Switch#
Switch#
Switch#
Switch#show port-security interface fa0/2
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0090.0C46.30E1:1
Security Violation Count   : 4

Switch#
```

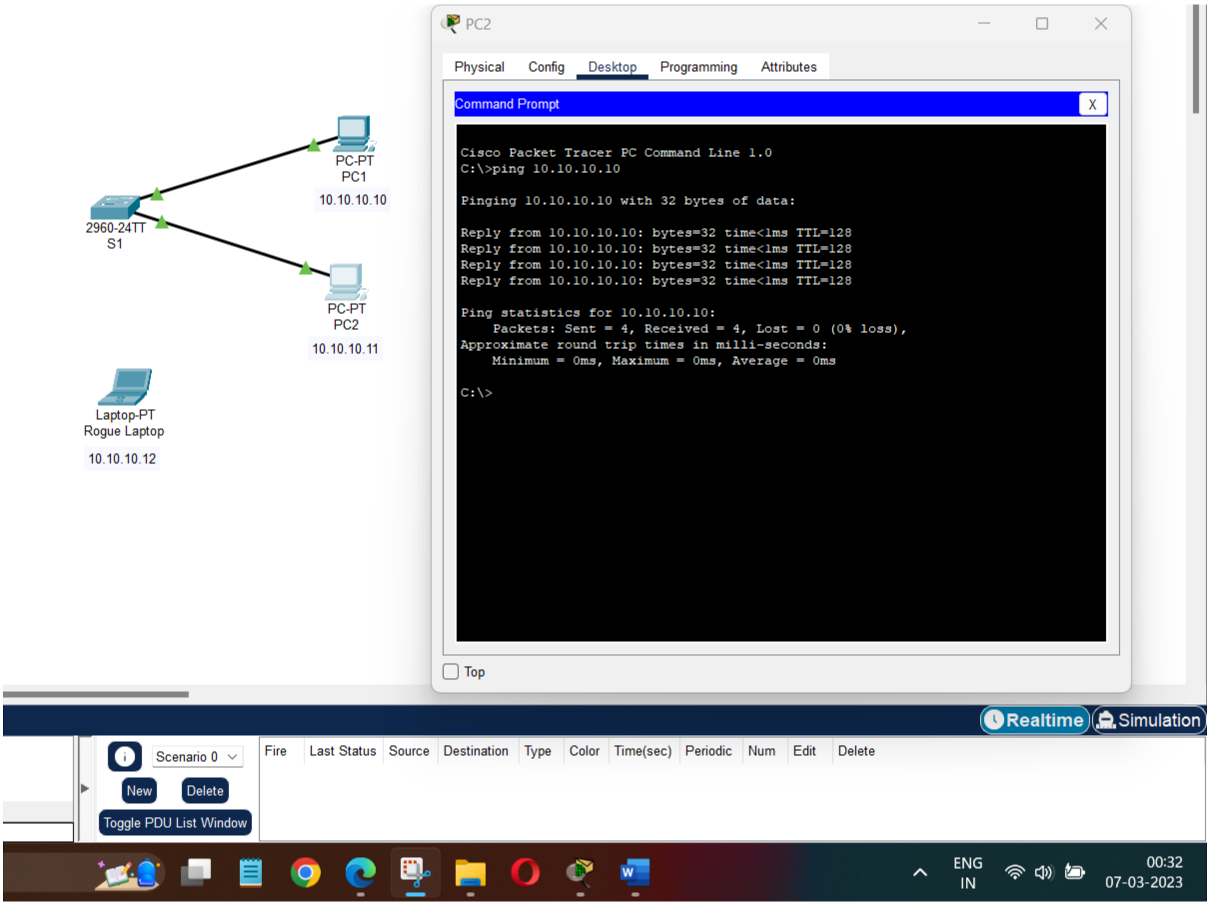
Successfully verified the Security Violation Count.

There should be a violation count of at least four, one for each ping request.

Step 8 : Re-verification using PC2

Disconnect Rouge Laptop and reconnect PC2. Verify PC2 can ping PC1.





```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Successfully verified that PC2 can ping PC1.

The port security that was enabled on the port only allowed the device, whose MAC was learned first, access to the port while preventing all other devices access.

--