Department of Computer Science and Engineering

Islamic University of Technology (IUT)

A subsidiary organ of OIC

Laboratory Report

CSE 4412: Data Communication and Networking Lab

Name: Namisa Najah Raisa
Student ID: 210042112
Section: B(Even)
Semester: 4th(Summer)
Academic Year: 2022-2023

Date of Submission: March 22, 2024

Title: Configuring Switch Port Security and Switch Port Analyzer (SPAN) in Cisco Devices

Objective:

1. Describe the concept of Switch Port Security
2. Explain importance of Switch Port Security in securing an organization
3. Configure Switch Port Security in CISCO devices
4. Use Switch Port Security feature to achieve varying degrees of protection
5. Describe the concept of port mirroring
6. Implement port mirroring using Cisco Switch Port Analyzer (SPAN)
7. Explain use cases of SPAN in real-life

Devices/ software Used:

1. Cisco Packet Tracer

Theory:

Port Mirroring:

It mirrors traffic from one port to another port. The packets from one port are copied and sent to another port, where a packet analyzer is connected. This packet analyzer can be a purpose-built hardware or it can be an application like Wireshark or an Intrusion Detection System (IDS) running on a host device. Technically, these are Ethernet frames which will be mirrored.

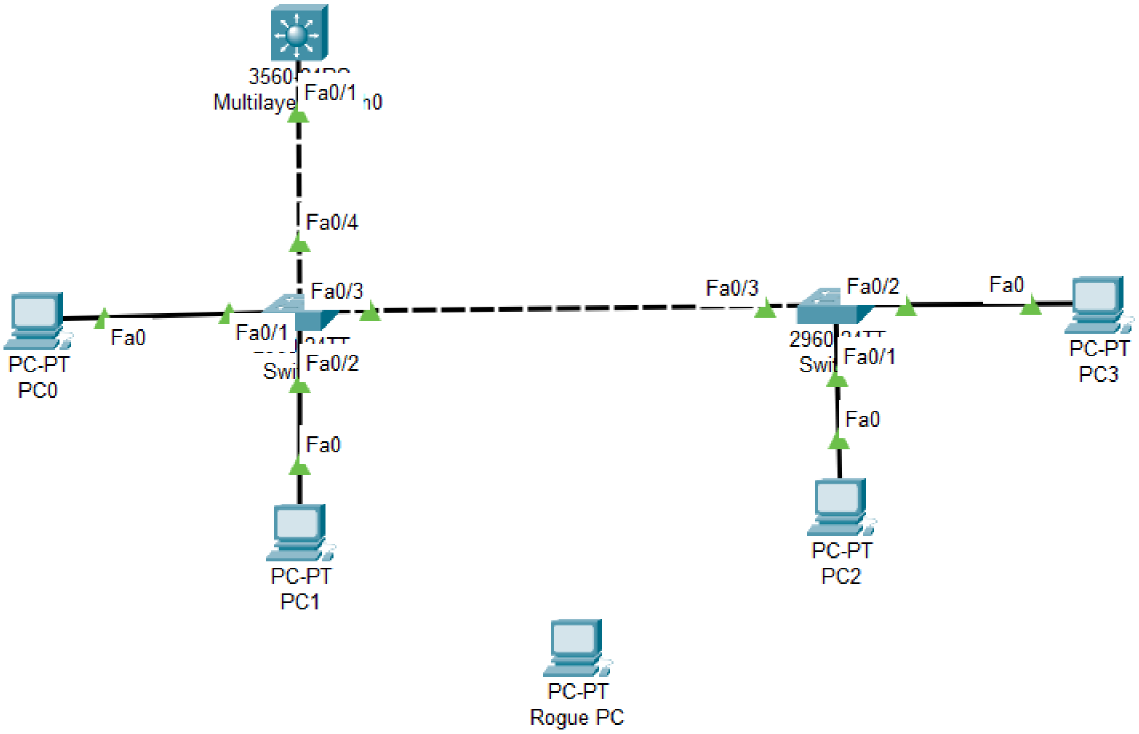
Local SPAN:

When traffic on a switch port is mirrored to another port on that switch, then it's Local SPAN.

Diagram of the experiment(s):

(Provide screenshot of the final network topology. Make sure to label the network components.)

Task1:



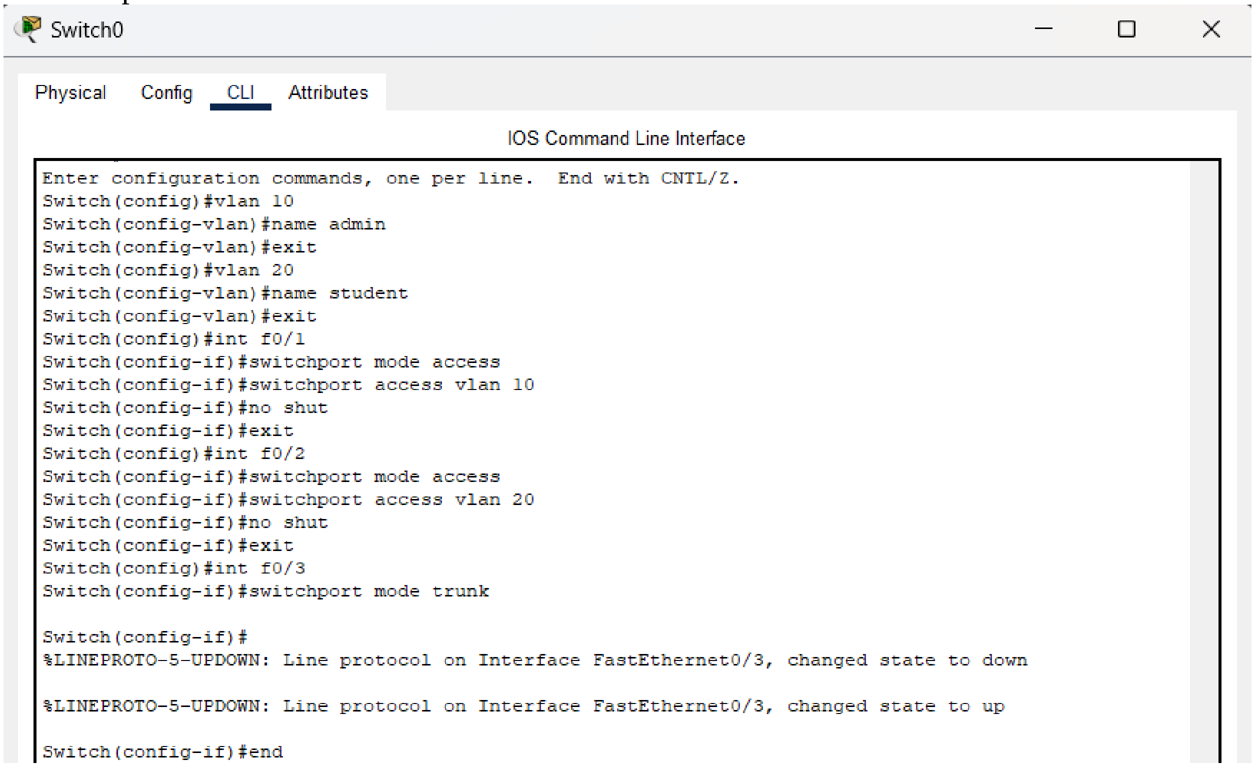
Task2:(same as Task1)

Working Procedure:

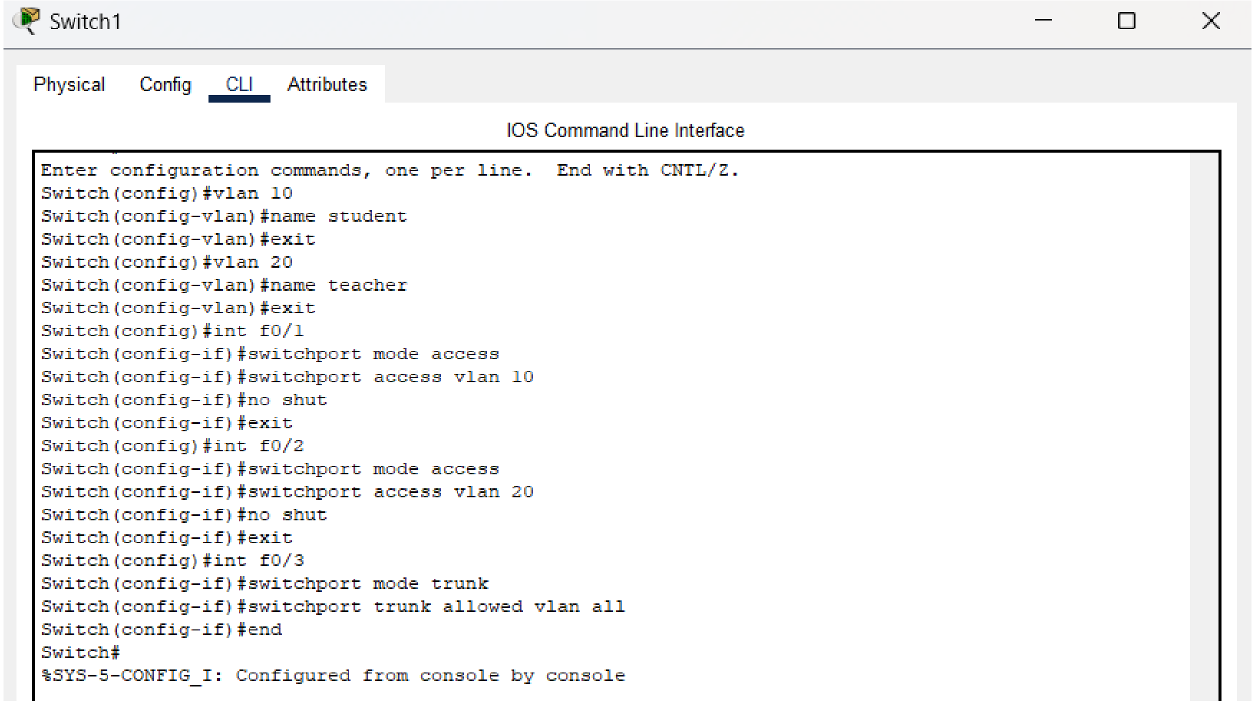
(Explain in brief how you completed the tasks. Provide necessary screenshots of used commands for each task.)

Task1:

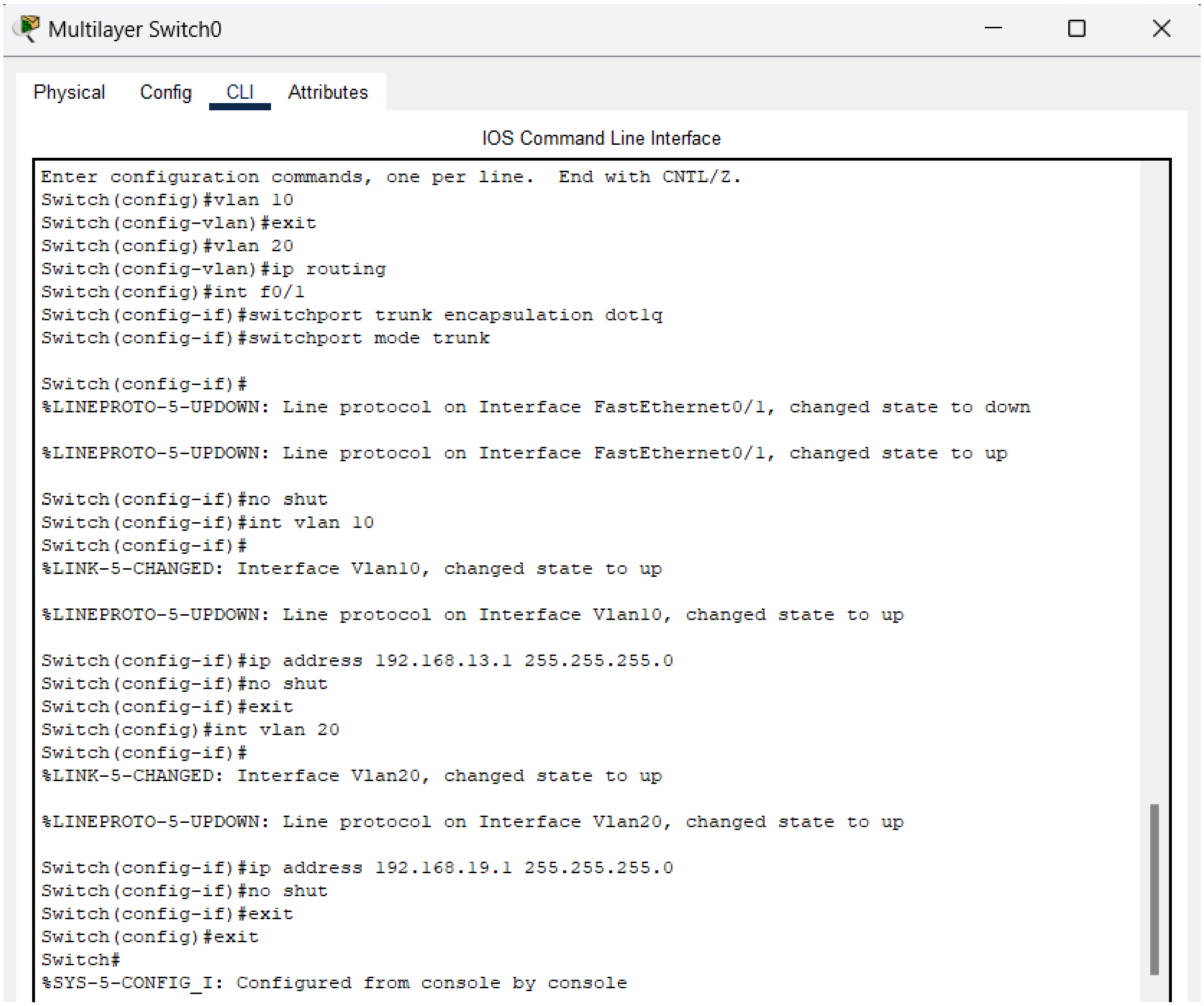
First setup the inter-VLAN with the L3 switch:



```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name admin
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name student
Switch(config-vlan)#exit
Switch(config)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#int f0/3
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

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

Switch(config-if)#end
```

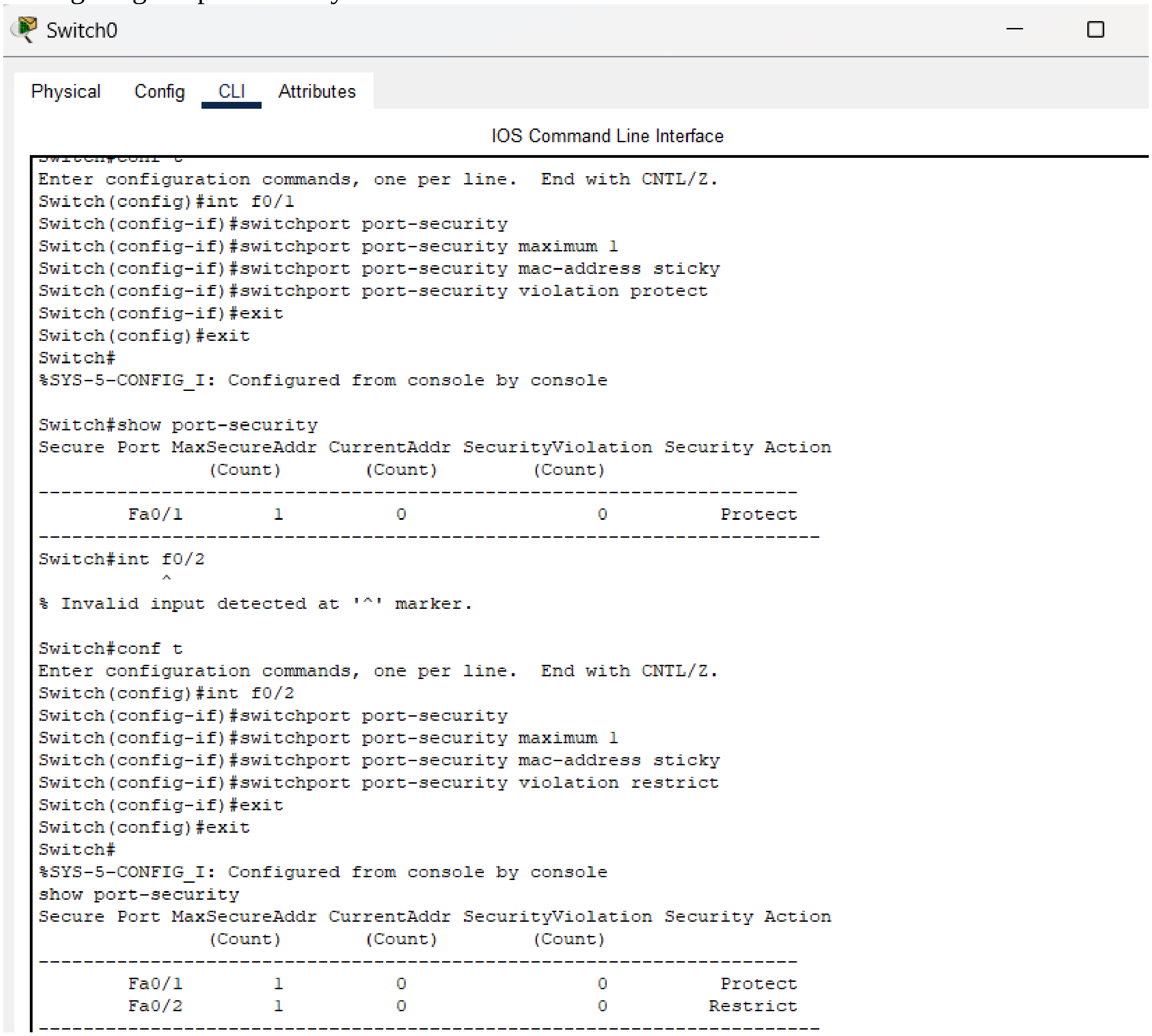


```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name student
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name teacher
Switch(config-vlan)#exit
Switch(config)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#int f0/3
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

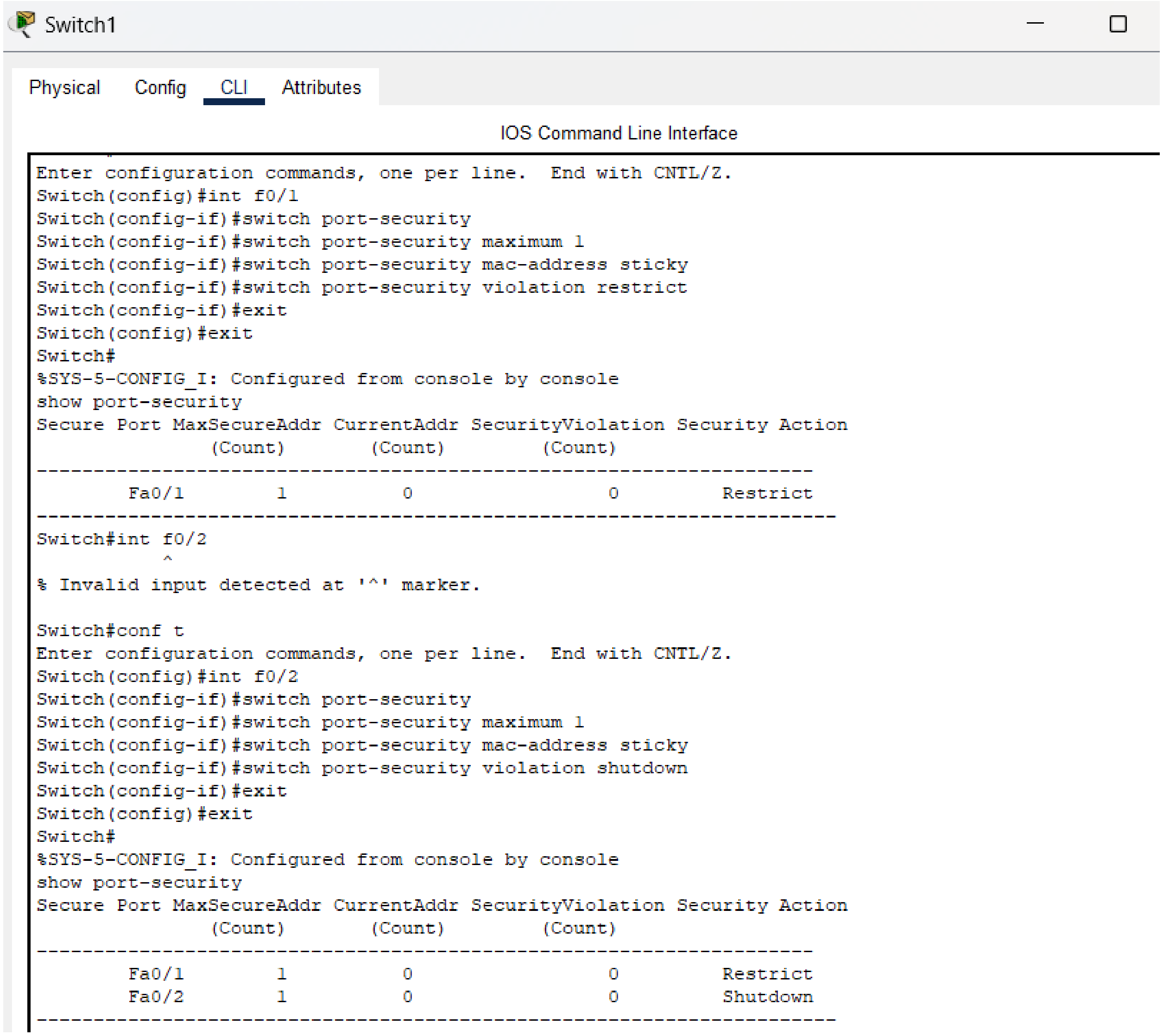


```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#ip routing
Switch(config)#int f0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk

Switch(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

Switch(config-if)#no shut
Switch(config-if)#int vlan 10
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

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

Switch(config-if)#ip address 192.168.13.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#int vlan 20
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

Switch(config-if)#ip address 192.168.19.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuring the port security of the two switches:

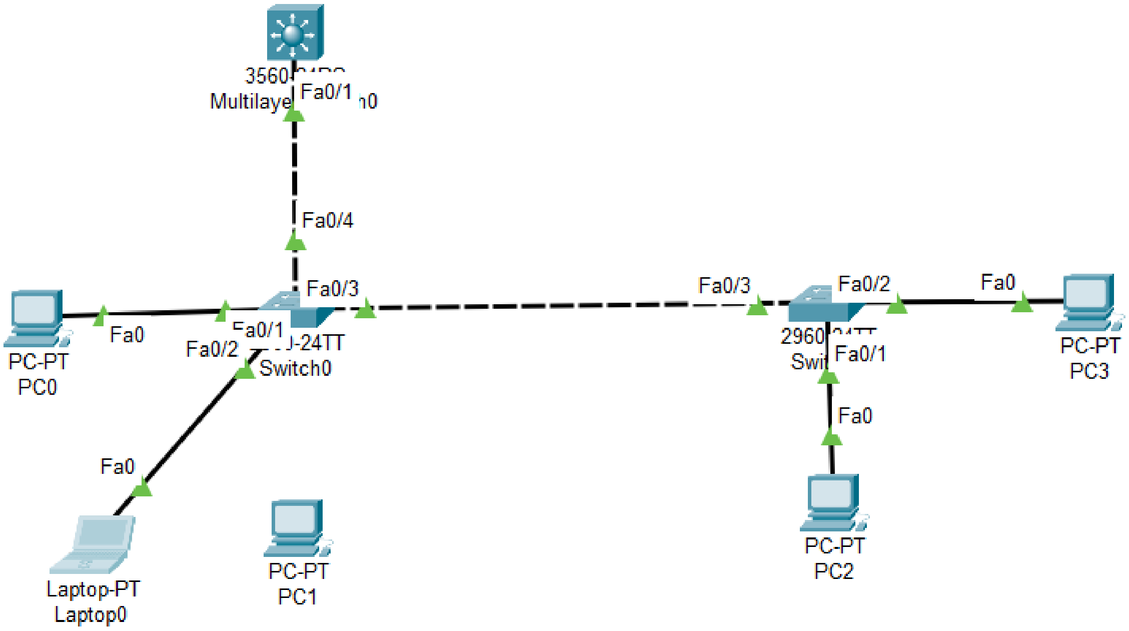


```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int f0/1
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation protect
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/1        1          0                 0          Protect
----------------------------------------------------------------------
Switch#int f0/2
           ^
% Invalid input detected at '^' marker.

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int f0/2
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/1        1          0                 0          Protect
        Fa0/2        1          0                 0         Restrict
----------------------------------------------------------------------
```

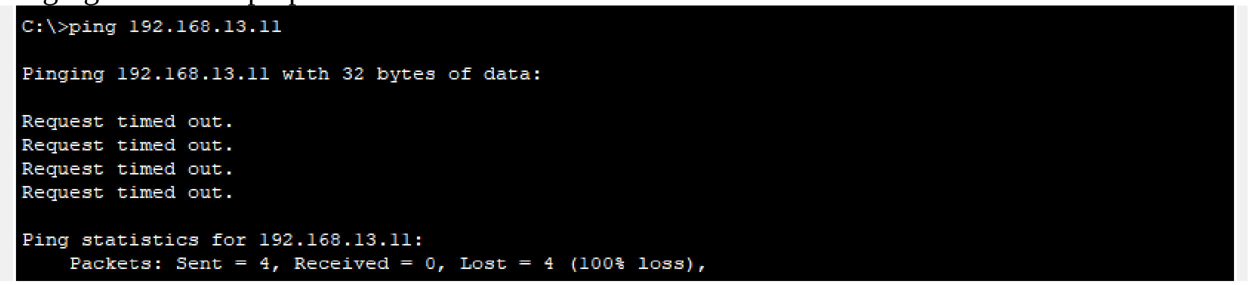


```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int f0/1
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security maximum 1
Switch(config-if)#switch port-security mac-address sticky
Switch(config-if)#switch port-security violation restrict
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/1        1          0                  0         Restrict
----------------------------------------------------------------------
Switch#int f0/2
           ^
% Invalid input detected at '^' marker.

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int f0/2
Switch(config-if)#switch port-security
Switch(config-if)#switch port-security maximum 1
Switch(config-if)#switch port-security mac-address sticky
Switch(config-if)#switch port-security violation shutdown
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/1        1          0                  0         Restrict
        Fa0/2        1          0                  0         Shutdown
----------------------------------------------------------------------
```

Connecting the rogue laptop in the place of PC1:

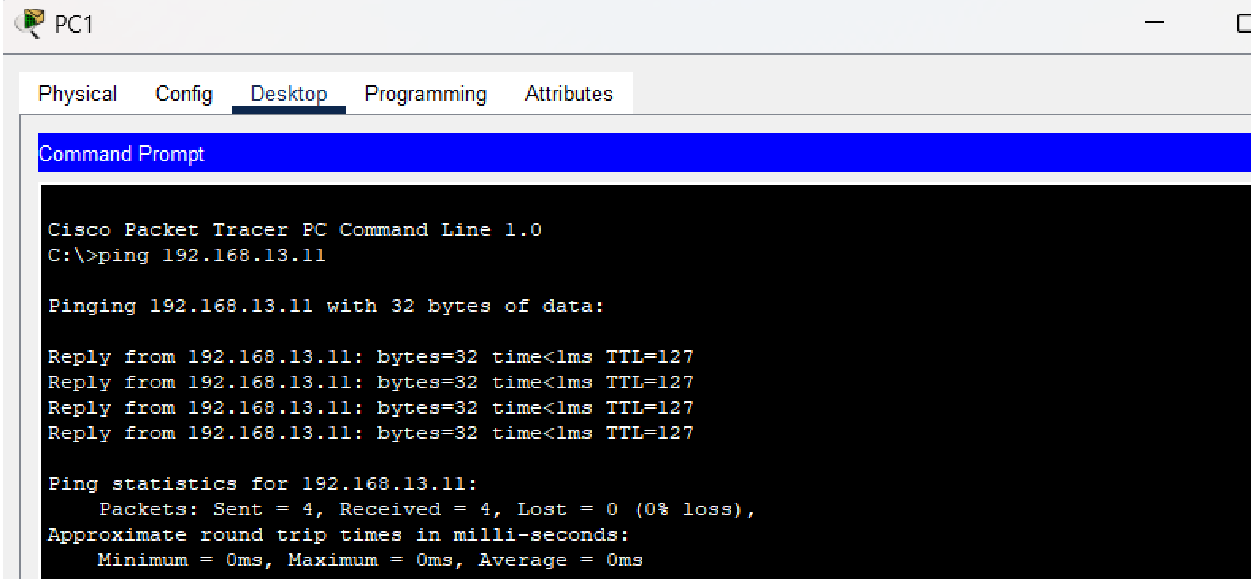


Pinging from the laptop to PC0:



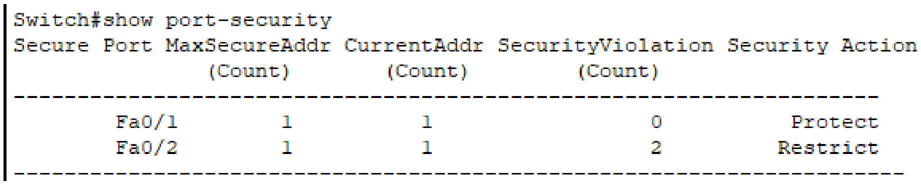
```
C:\>ping 192.168.13.11

Pinging 192.168.13.11 with 32 bytes of data:

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

Ping statistics for 192.168.13.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

After disconnecting the laptop and reconnecting the PC2:



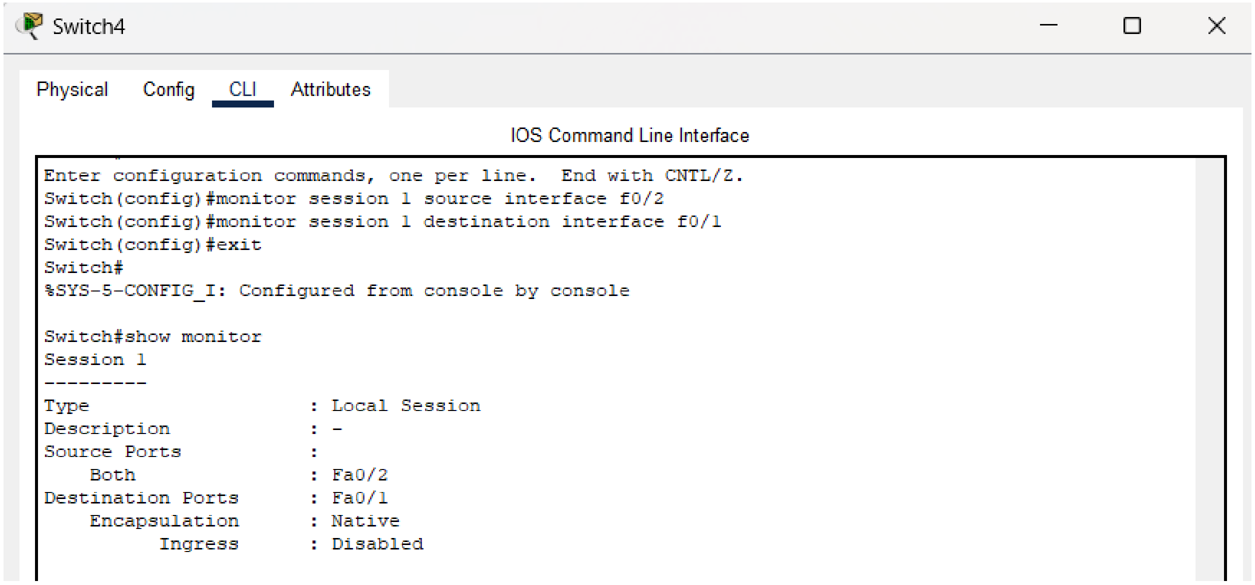
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.13.11

Pinging 192.168.13.11 with 32 bytes of data:

Reply from 192.168.13.11: bytes=32 time<1ms TTL=127
Reply from 192.168.13.11: bytes=32 time<1ms TTL=127
Reply from 192.168.13.11: bytes=32 time<1ms TTL=127
Reply from 192.168.13.11: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.13.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Port-security restriction violation:(Z=2)



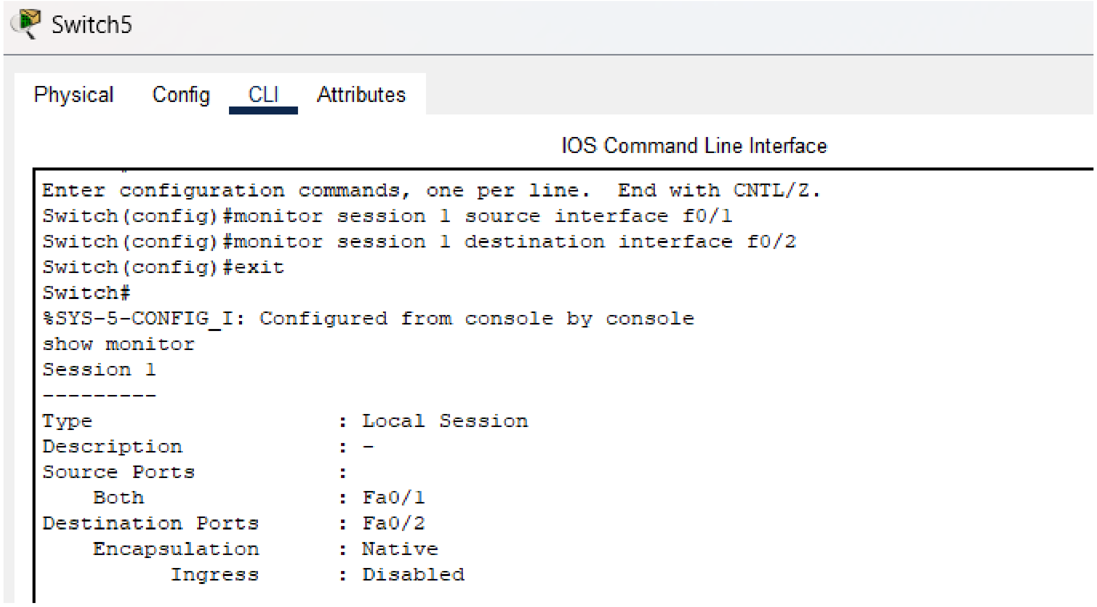
```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
--------------------------------------------------------------------
        Fa0/1        1          1                  0         Protect
        Fa0/2        1          1                  2        Restrict
----------------------------------------------------------------------
```

Task2:
First switch:



```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#monitor session 1 source interface f0/2
Switch(config)#monitor session 1 destination interface f0/1
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show monitor
Session 1
---------
Type                    : Local Session
Description             : -
Source Ports            :
    Both                : Fa0/2
Destination Ports       : Fa0/1
    Encapsulation       : Native
          Ingress       : Disabled
```

Second switch:
(Assuming that in the second switch the teacher vlan is the admin vlan):



```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#monitor session 1 source interface f0/1
Switch(config)#monitor session 1 destination interface f0/2
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
show monitor
Session 1
---------
Type                    : Local Session
Description             : -
Source Ports            :
    Both                : Fa0/1
Destination Ports       : Fa0/2
    Encapsulation       : Native
          Ingress       : Disabled
```

Observation:

Task 1:

Configuring port security with different violation modes (protect, restrict, shutdown) helps in controlling unauthorized access to the network. It ensures that only authorized devices can connect to the network and take appropriate actions when violations occur.

By disconnecting one of the current PCs and introducing a rogue laptop, a security breach scenario is simulated. Continuously testing with rogue PCs allows to evaluate the effectiveness of port security measures in preventing unauthorized access and detecting security violations.

Task 2:

After configuring SPAN, the traffic forwarded to the admin's monitoring port. Monitoring this traffic allows the admin to analyze student activities, identify potential security threats, and take appropriate actions to reduce risks.

Challenges (if any):

The configuration of the port security was complicated. Setting up a rogue laptop and maintaining the VLANs was also confusing.