# 

# **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:**

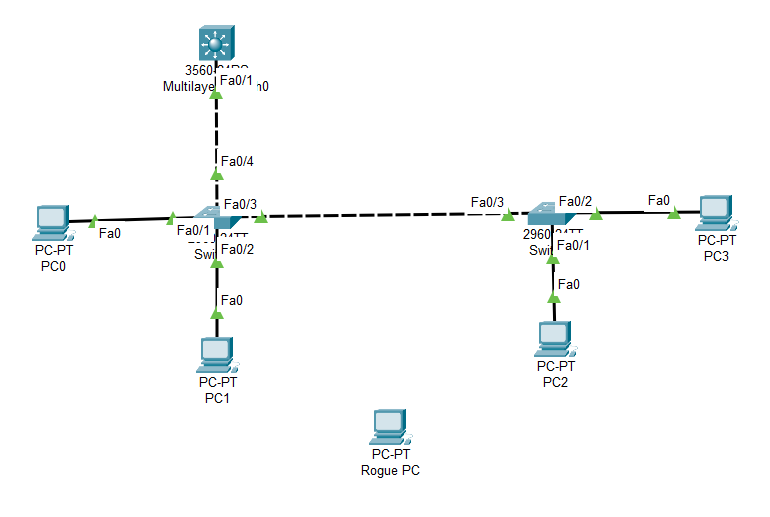
It mirrors traffic from one port to another port. The packets from one port are copied and sent to another port, where a packet analyzer is connected. This packet analyzer can be a purpose-built hardware or it can be an application like Wireshark or an Intrusion Detection System (IDS) running on a host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

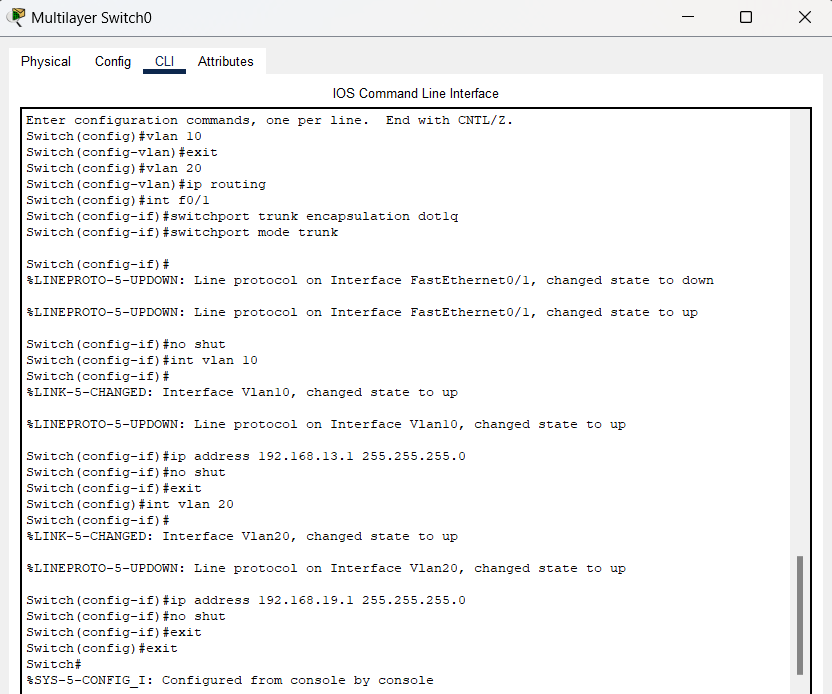
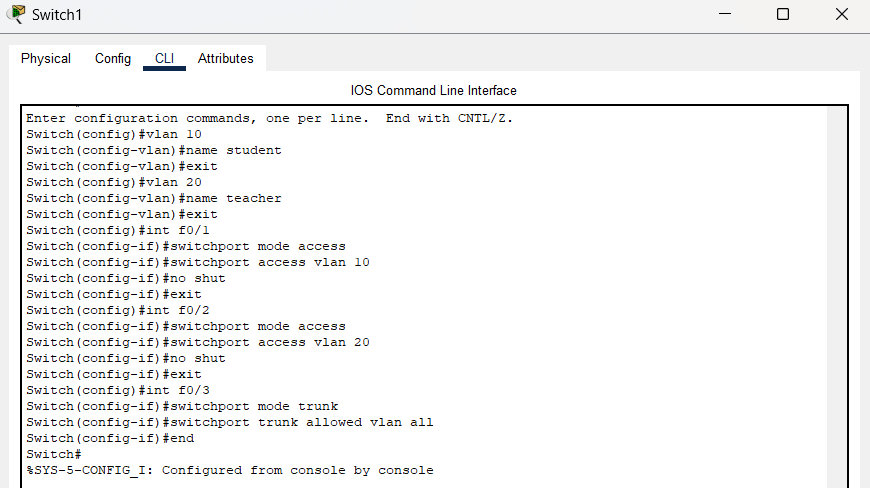
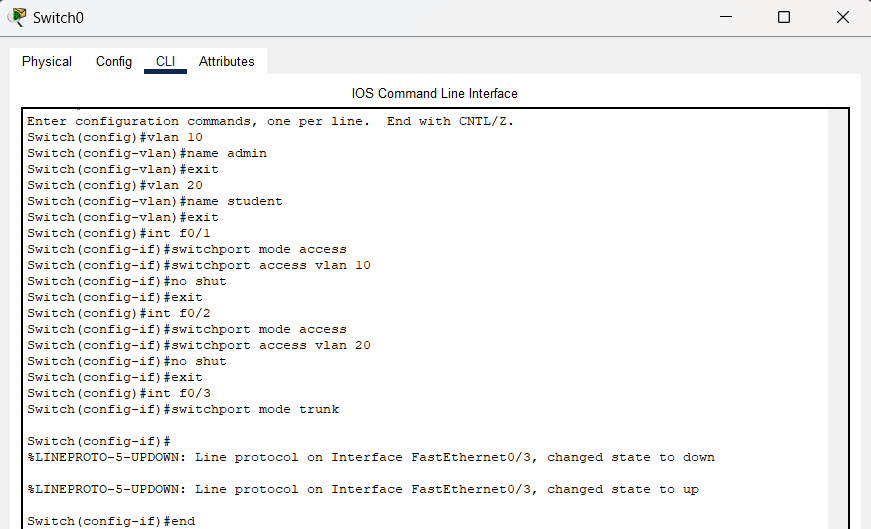
**Task1:**

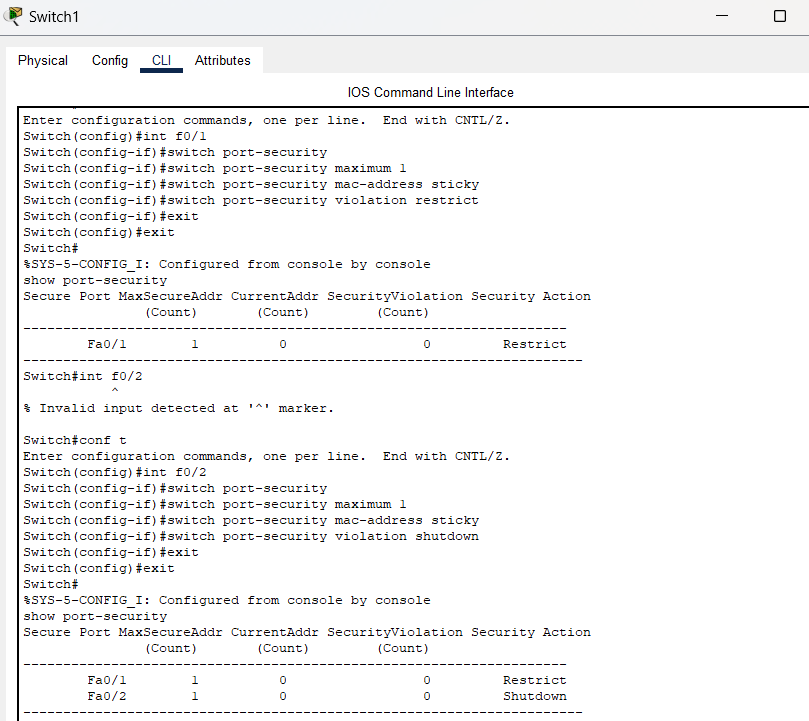
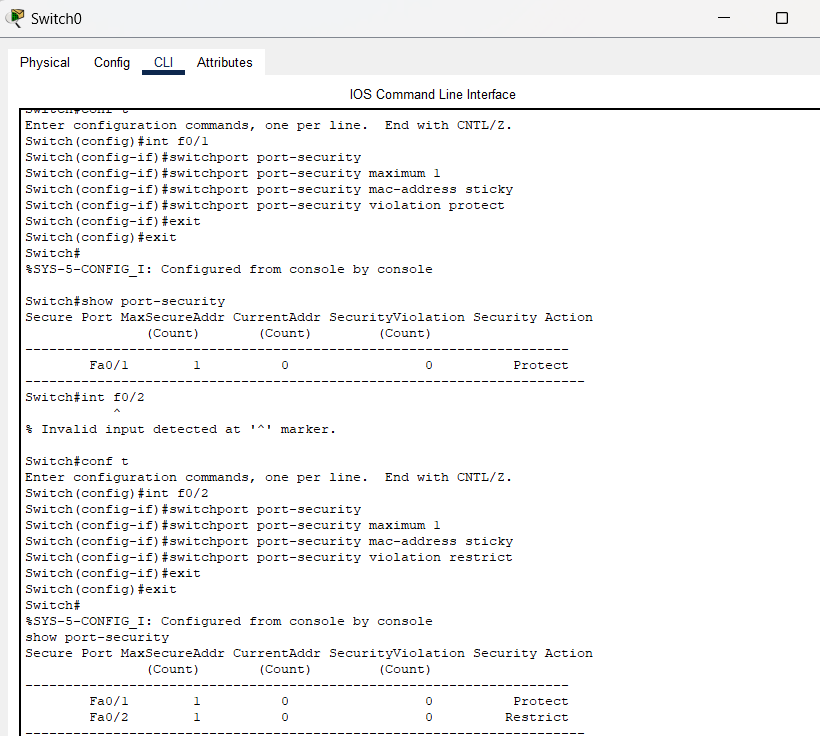
Task2:(same as Task1)

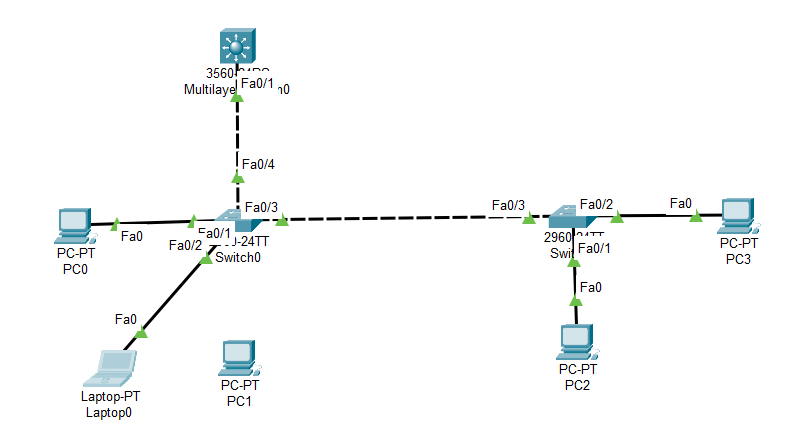
### **Working Procedure:**

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

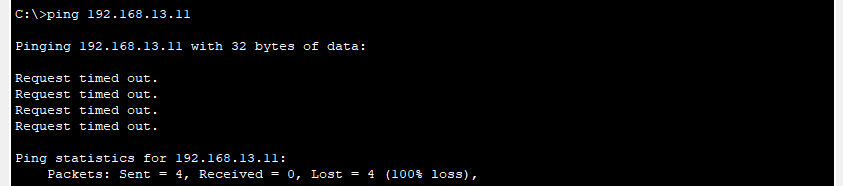
Task1:

First setup the inter-VLAN with the L3 switch:

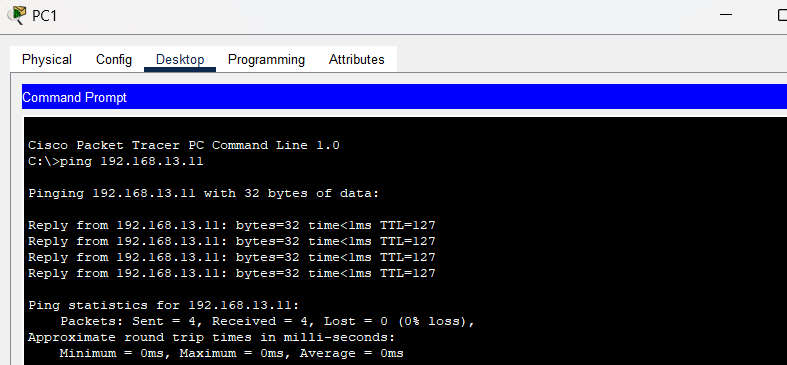
Configuring the port security of the two switches:

Connecting the rogue laptop in the place of PC1:

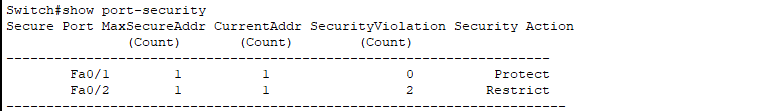
Pinging from the laptop to PC0:



After disconnecting the laptop and reconnecting the PC2:

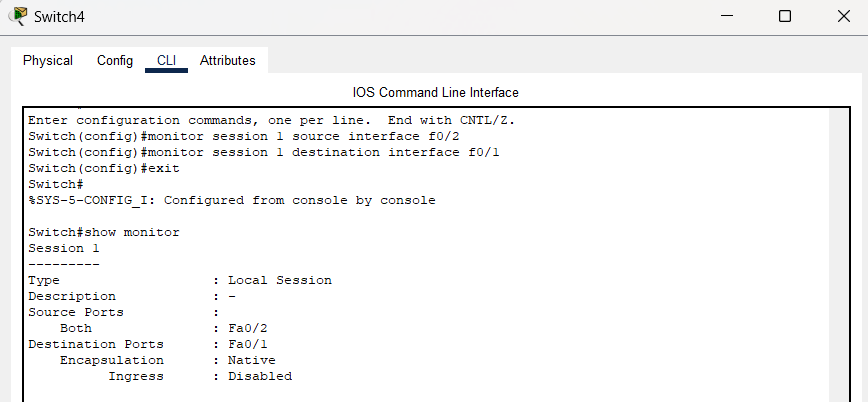


Port-security restriction violation:(Z=2)



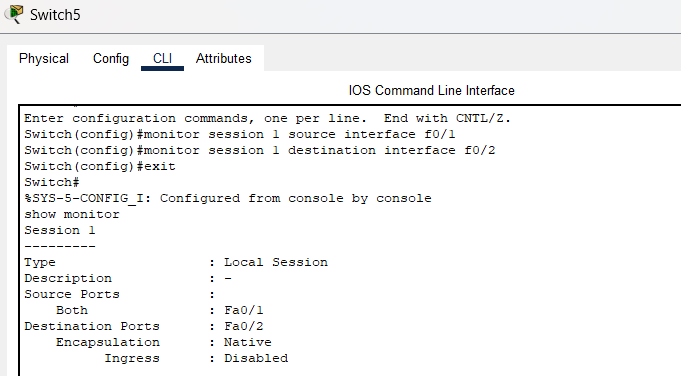
Task2:

First switch:



Second switch:

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



### **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.