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: Hasin Mahtab Alvee
Student ID: 210042174
Section: SWE - B (Even)
Semester: 4th (Summer)
Academic Year: 2023-24

Date of Submission: March 24th, 2024

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

Objective:

1. Understand and configure Switchport security in networks
2. Implement different kinds of port security
3. Understand and configure port mirroring
4. Implement SPAN (Cisco Switch Port Analyzer)

Devices/ software Used:

1. Cisco Packet Tracer

Theory:

Port Mirroring:

Port mirroring is a method of copying and sending network packets transmitted as input from a port to another port of a monitoring computer/switch/device. It is a network monitoring technique implemented on network switches and similar devices.

Port mirroring is also known as switched port analyzer (SPAN) and roving analysis port (RAP).

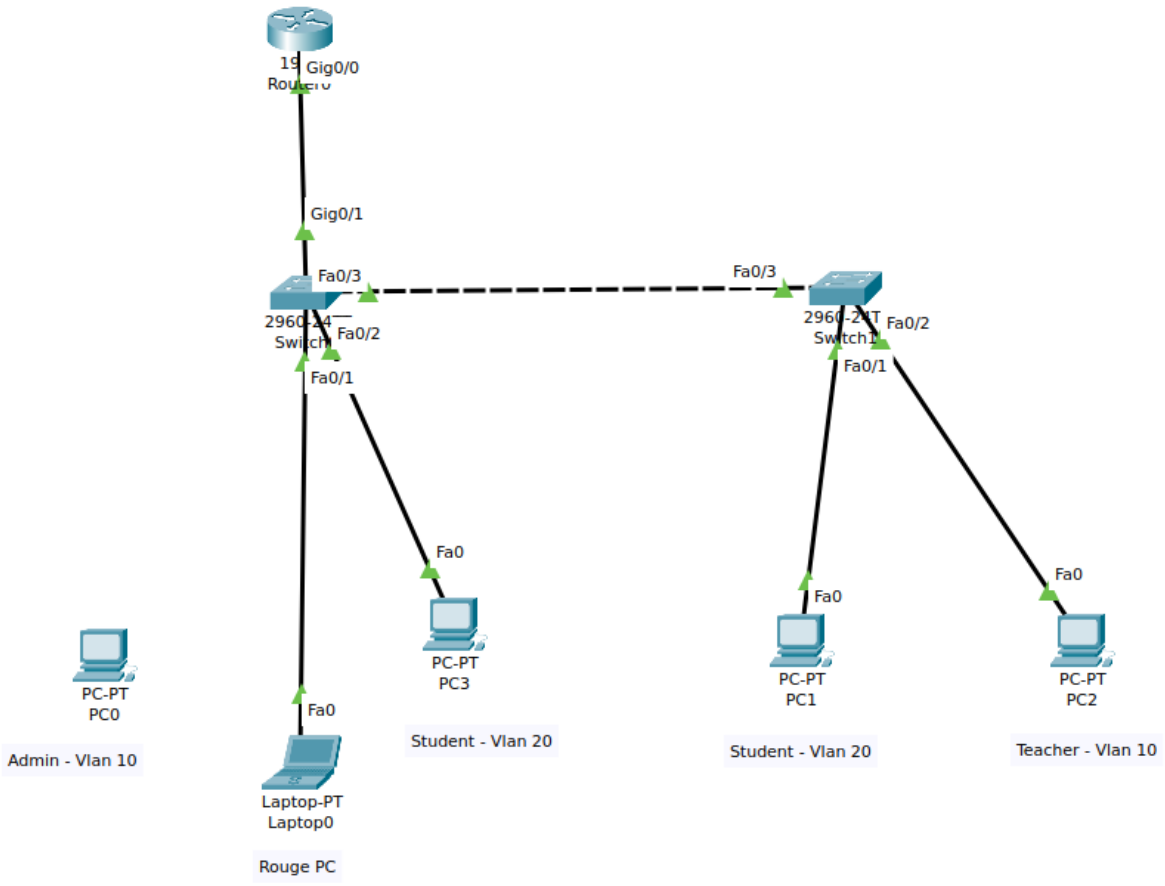
Local SPAN:

Switch Port Analyzer (SPAN) is a mechanism which provide port/vlan analyze by mirroring one port/vlan traffic to another. There are three types SPAN. These are: Local SPAN (SPAN), Remote SPAN (RSPAN) and Encapsulated Remote SPAN (ERSPAN). Local SPAN is the SPAN type in which, both source and destination ports reside in the same switch.

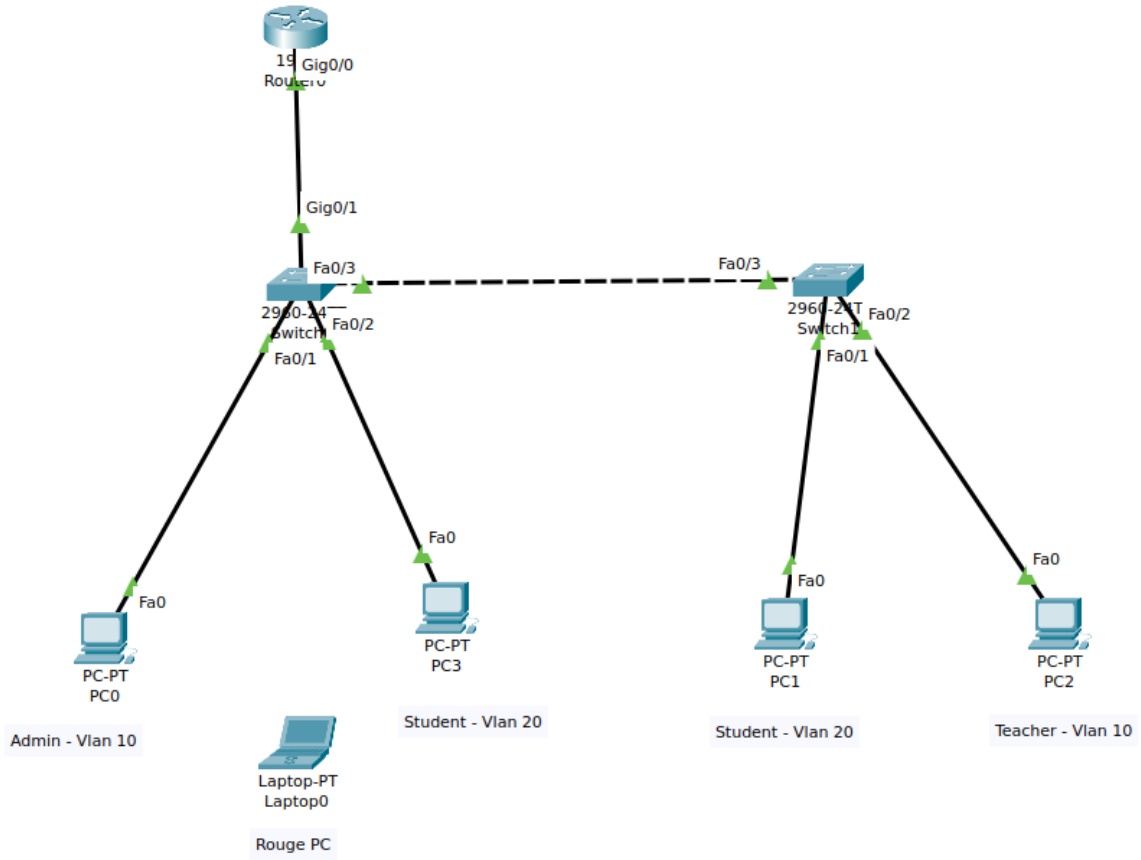
Diagram of the experiment(s):

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

Task 1


Gig0/0
Gig0/1
Fa0/3
Fa0/3
Fa0/2
Fa0/1
Fa0/2
Fa0/1
Fa0
Fa0
Fa0
Fa0
PC-PT
PC0
PC-PT
PC3
PC-PT
PC1
PC-PT
PC2
Admin - Vlan 10
Student - Vlan 20
Student - Vlan 20
Teacher - Vlan 10
Laptop-PT
Laptop0
Rouge PC

Task 2


Gig0/0
Gig0/1
Fa0/3
Fa0/3
Fa0/2
Fa0/1
Fa0/2
Fa0/1
Fa0
Fa0
Fa0
Fa0
PC-PT
PC0
PC-PT
PC3
PC-PT
PC1
PC-PT
PC2
Admin - Vlan 10
Student - Vlan 20
Student - Vlan 20
Teacher - Vlan 10
Laptop-PT
Laptop0
Rouge PC

Working Procedure:

1. At first, I had to set up vlan 10 and 20, where 20 is for the students and 10 is for the admin and teachers.
2. Then I had to ensure Router on a stick configuration by setting the trunk of the first switch to a router connected to that switch.
3. I set IP addresses for the vlans to 192.168.75.1 and 192.168.81.1. Then also set up respective IP addresses for the host devices.
4. After all this, now I set up the port security on both switches. I set a restrict and a protect violation to the first switch and a restrict and a shutdown violation for the second switch.

```
sl(config)#interface fa
sl(config)#interface fastEthernet 0/2
sl(config-if)#
sl(config-if)#swi
sl(config-if)#switchport por
sl(config-if)#switchport port-security ?
  aging        Port-security aging commands
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode
  <cr>
sl(config-if)#switchport port-security
sl(config-if)#switchport port-security max
sl(config-if)#switchport port-security maximum 1
sl(config-if)#swi
sl(config-if)#switchport mac
sl(config-if)#switchport mac-
sl(config-if)#switchport po
sl(config-if)#switchport port-security mac
sl(config-if)#switchport port-security mac-address st
sl(config-if)#switchport port-security mac-address sticky
sl(config-if)#
sl(config-if)#swi
sl(config-if)#switchport por
sl(config-if)#switchport port-security viol
sl(config-if)#switchport port-security violation pro
sl(config-if)#switchport port-security violation protect
sl(config-if)#
sl(config-if)#
sl(config-if)#exit
sl(config)#exit
sl#
%SYS-5-CONFIG_I: Configured from console by console

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

5. After setting up the port security, I had to send messages from the devices to ensure the connection which made the current address count to 1 from 0.

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

6. After this, I connected a rouge Laptop in the place of the admin PC, to check the violation count. As soon as I connected the rouge laptop and assigned the right IP address for it, the violation count was 3, as it was already connected to the other 3 devices. To make the count 4, which is my last digit, I had to send another message to any one of the devices and the count was then 4.

```
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
        Fa0/1        1          1                3         Restrict
        Fa0/2        1          1                0          Protect
---------------------------------------------------------------------
sl#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
        Fa0/1        1          1                4         Restrict
        Fa0/2        1          1                0          Protect
---------------------------------------------------------------------
```

7. Now, we can set up port mirroring for the configured topology. I disconnect the rouge laptop and reconnect the Admin PC to ensure the mirroring. For mirroring, I used the admin and the student vlan.

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

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

Observation:

This task shows how to implement port security to a VLAN configuration. Using the port security, we can manage the devices we want to be connected to the network and this ensures that no outside device can take control even if they are directly connected.

Challenges (if any):

- I could not increment the Current address count in the port security at first. Then I had to send messages from host devices to see the security count increase.