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: Adib Sakhawat
Student ID: 210042106
Section: B
Semester: Summer (4th)
Academic Year: 2022 - 23

Date of Submission: 24 March 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. Laptop
2. PC
3. Cisco Packet Tracer

Theory:

Port Mirroring:
port mirroring refers to the capability of duplicating the traffic from one port (the source port) and sending it to another port (the destination port) for analysis or monitoring purposes. This feature is commonly used for network troubleshooting, security analysis, or performance monitoring.

When port mirroring is configured on a Cisco switch, all traffic that enters or exits the source port is copied and forwarded to the destination port without affecting the original traffic flow. This allows network administrators to monitor the network traffic passing through the source port in real-time without disrupting normal network operations.

Local SPAN:
Local SPAN, or Local Switched Port Analyzer, is a feature commonly found in Cisco switches that allows network administrators to monitor traffic on a single switch. With Local SPAN, you can mirror traffic from one or more source ports to a designated destination port on the same switch. This feature is particularly useful for troubleshooting network issues, monitoring network traffic for security purposes, or analyzing network performance.

1. Source Ports: These are the ports from which you want to mirror the traffic. You can select one or more source ports on the switch.

2. Destination Port: This is the port to which the mirrored traffic is sent. The destination port is where the monitoring device, such as a network analyzer or a monitoring server, is connected to capture and analyze the mirrored traffic.

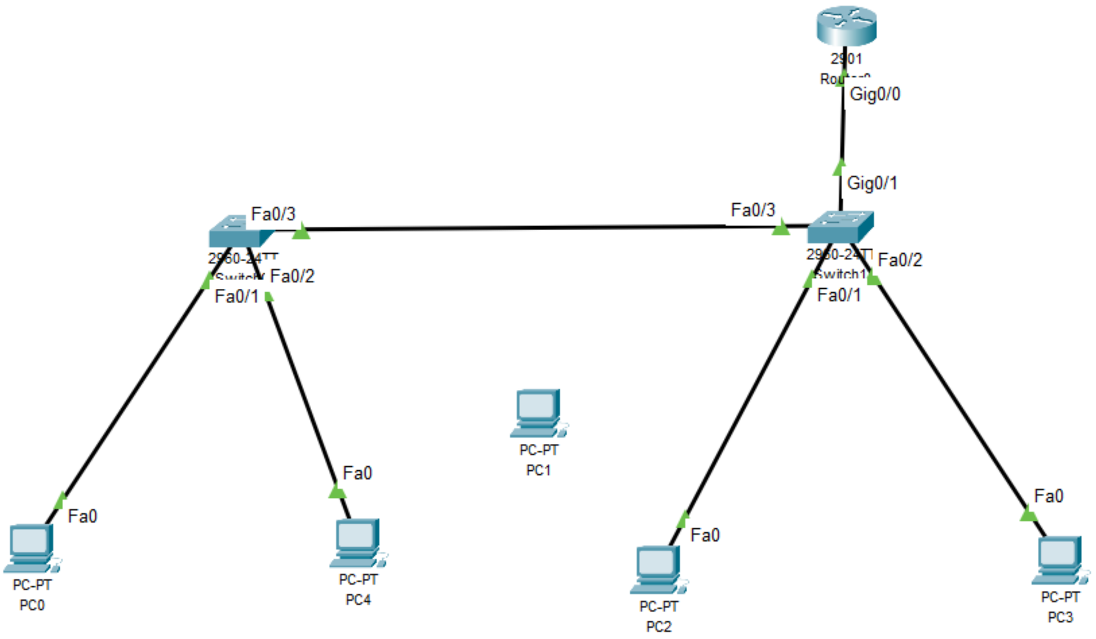
3. Mirroring Traffic: When Local SPAN is configured, the switch copies all traffic from the specified source ports and forwards it to the destination port. This allows the monitoring device connected to the destination port to receive and analyze the mirrored traffic without disrupting the original traffic flow.

4. Configuration: Local SPAN is typically configured through the switch's command-line interface (CLI) or web-based management interface. Administrators can specify the source ports and the destination port, as well as additional parameters such as the direction of traffic (ingress, egress, or both) and the type of traffic to be mirrored (e.g., all traffic or specific VLANs).

5. Monitoring and Analysis: Once Local SPAN is configured, the monitoring device connected to the destination port can capture and analyze the mirrored traffic in real-time. This allows administrators to troubleshoot network issues, detect security threats, or monitor network performance without disrupting normal network operations.

Diagram of the experiment(s):

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



Working Procedure:

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

Step 1 : Creating the network structure

- Taking 2 *2960 switches* and connecting them using the port `fastEthernet 0/3`
- Placing 4 PCs on their place and connecting each of them with respective switches.
- Assigning IP addresses to the PCs
  - PC – 0 : 192.168.7.10
  - PC – 4 : 192.168.13.30
  - PC – 2 : 192.168.7.20
  - PC – 3 : 192.168.13.20
- Taking a router and connecting it to switch 2 for `interVlan` communication

Step 2 : Creating Vlan

- Giving following commands on switch 1 cli.

```
» conf t
» vlan 10
» name student
» exit
»
» vlan 20
» name admin
» exit
»
» interface fastEthernet 0/1
» switchport mode access
» switchport access vlan 10
» no shutdown
» exit
»
» interface fastEthernet 0/2
» switchport mode access
» switchport access vlan 20
» no shutdown
» exit
»
» interface fastEthernet 0/3
» switchport mode trunk
» switchport trunk allowed vlan all
» no shutdown
» exit
```

- Giving following commands on switch 2 cli.

```
» conf t
» vlan 10
» name student
» exit
»
» vlan 20
» name admin
» exit
»
» interface fastEthernet 0/1
» switchport mode access
» switchport access vlan 10
» no shutdown
» exit
»
» interface fastEthernet 0/2
» switchport mode access
» switchport access vlan 20
» no shutdown
» exit
»
» interface fastEthernet 0/3
» switchport mode trunk
» switchport trunk allowed vlan all
» no shutdown
» exit
»
» interface gigabitEthernet 0/1
» switchport mode trunk
» switchport trunk allowed vlan all
» no shutdown
» exit
```

- Giving following commands on router cli.

```
» conf t
» interface gigabitEthernet 0/0
» no shutdown
» exit
»
» interface gigabitEthernet 0/0.10
» encapsulation dot1Q 10
» ip address 192.168.7.1 255.255.255.0
» exit
»
```

```
» interface gigabitEthernet 0/0.20
» encapsulation dot1Q 10
» ip address 192.168.13.1 255.255.255.0
» exit
```

Now interVlan Communication of the network is set.

Step 3 : Creating `port security` for switch 1

- Giving following commands to switch 1

```
» interface range fastEthernet 0/1-2
» switchport port-security
» switchport port-security maximum 1
» switchport port-security mac-address sticky
» switchport port-security violation restrict
» exit
```

- Giving following commands to switch 2

```
» Interface fastEthernet 0/1
» switchport port-security
» switchport port-security maximum 1
» switchport port-security mac-address sticky
» switchport port-security violation protect
» exit
»
» Interface fastEthernet 0/2
» switchport port-security
» switchport port-security maximum 1
» switchport port-security mac-address sticky
» switchport port-security violation shutdown
» exit
```

Step 4 : Introducing a rough PC

- creating a rough pc in the system.
- Assigning its ip address – `192.168.13.10`
- Connecting the rough PC to the system through `interface fastEthernet 0/2`
- Trying to send data from rough PC to any other pc on network
- Status is failed. Port is Secured

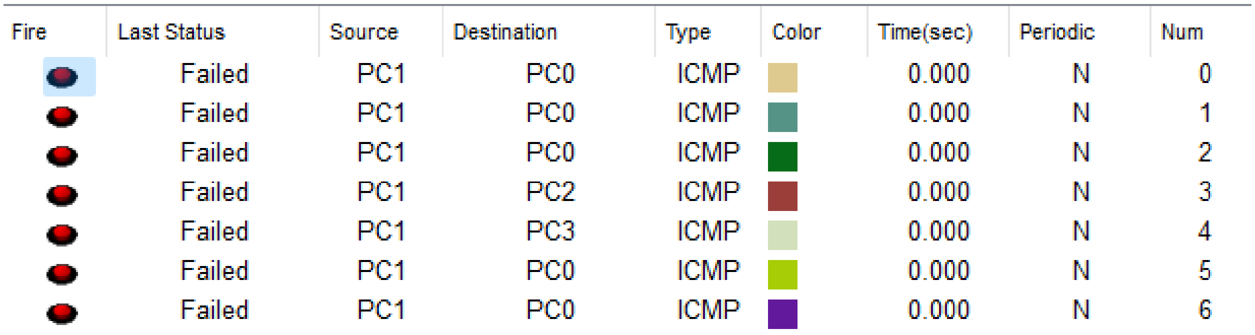
Step 5 : SPAN

- Giving following commands to switch 1

```
» monitor session 1 source interface fastEthernet 0/1
» monitor session 1 destination interface fastEthernet 0/2
```

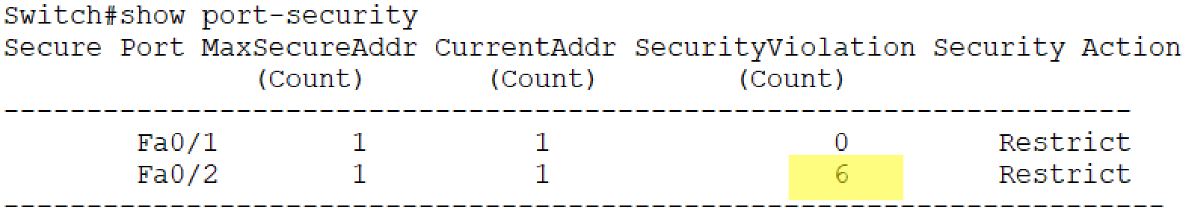
Observation:

Observation 1 : Sending Failed



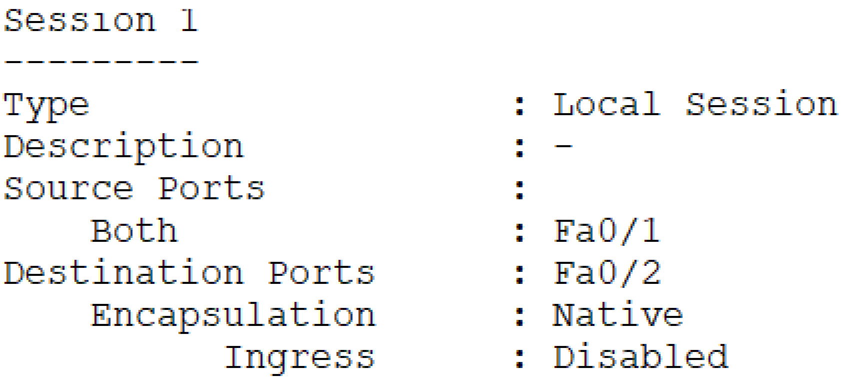
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	Failed	PC1	PC0	ICMP	🟨	0.000	N	0
●	Failed	PC1	PC0	ICMP	🟩	0.000	N	1
●	Failed	PC1	PC0	ICMP	🟩	0.000	N	2
●	Failed	PC1	PC2	ICMP	🟥	0.000	N	3
●	Failed	PC1	PC3	ICMP	🟩	0.000	N	4
●	Failed	PC1	PC0	ICMP	🟩	0.000	N	5
●	Failed	PC1	PC0	ICMP	🟪	0.000	N	6

Observation 2 : Restrict Count 6



```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
                (Count)       (Count)          (Count)
--------------------------------------------------------------------
        Fa0/1        1           1                  0         Restrict
        Fa0/2        1           1                  6         Restrict
----------------------------------------------------------------------
```

Observation 3 : Session Monitor



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