CSE 4512 [Computer Networks Lab]

Lab # 09

1. Objectives:

- Describe the concept of port mirroring
- Implement port mirroring using Cisco Switch Port Analyzer (SPAN)
- Explain use cases of SPAN in real-life

2. Theory:

Switch Port Analyzer:

One day your boss called you and asked you to monitor if your colleagues are using Facebook during office hours. How do you do it? Or you've been informed of an ongoing cyber attack on your office hosts. How do you know what attacker is doing? All of these and more can be achieved through a CISCO feature known as SPAN or Switch Port Analyzer. SPAN is a port mirroring technique that allows administrators or devices to collect and analyze traffic.

What is this port mirroring actually? The name tells the tale. 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. Remember that these ports we are referring to are Switch Ports that you've seen in last lab (Lab 08). So, technically, these are Ethernet frames which will be mirrored.

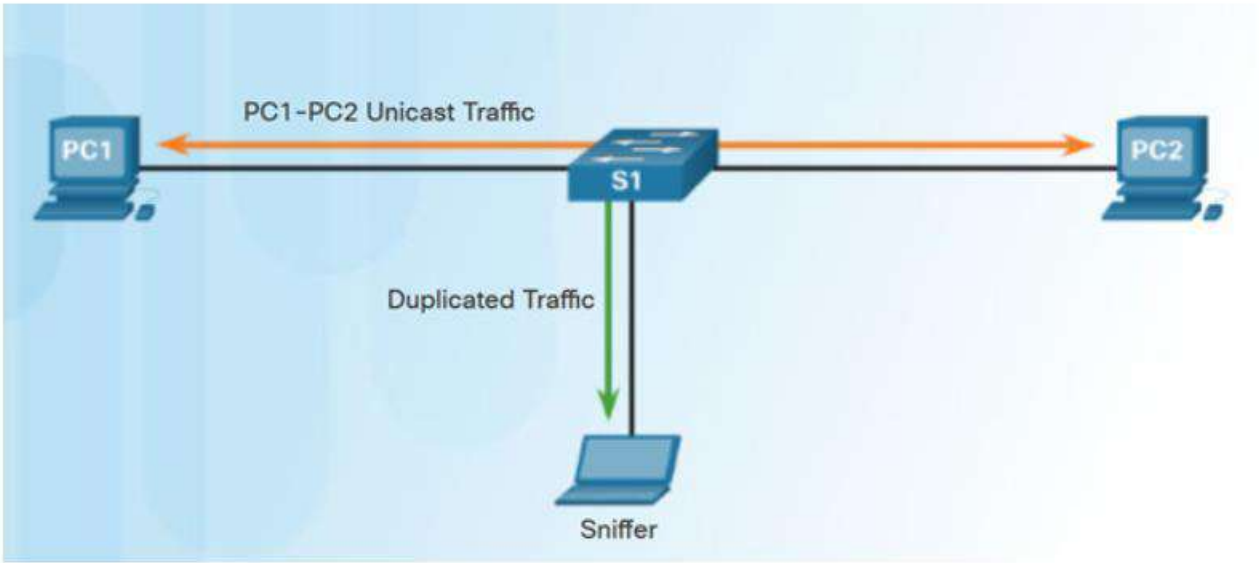


Fig: Port Mirroring

The specific technology that allows this port mirroring in Cisco devices is known as SPAN. There are two types of SPAN: Local SPAN and Remote SPAN. When traffic on a switch port is mirrored to another port on that switch then it's *Local SPAN*. In contrast, when traffic is mirrored to a port on another switch then it's *Remote SPAN*. In this lab, we'll focus only on Local SPAN.

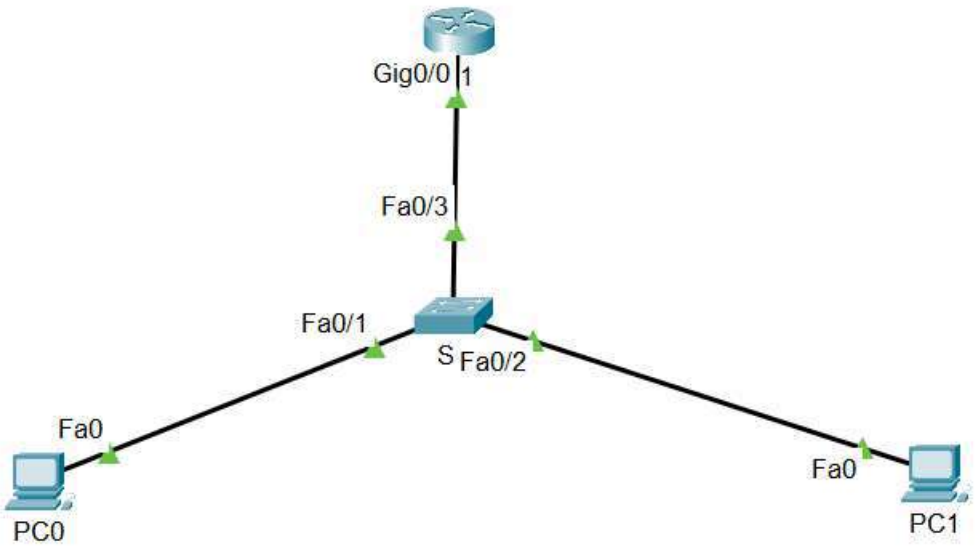
When configuring SPAN, an association between the *source ports* (the port whose traffic would be copied/mirrored) and the *destination port* (the port through which the copied/mirrored traffic will be sent) is made. In SPAN terminology, this association is known as a *session*. You can mirror traffic from multiple source ports or from a source VLAN to a single destination port. The destination port is also known as monitor port. Note that, a destination port can't be a source port or a source port can't be a destination port. It depends on the specific Cisco device as to how many number of destination ports can be there for a single session. And when you configure a normal port as a *destination port*, only mirrored/monitored traffic can pass through it. Other traffic will no longer be able to pass through that port.
There are some other related terminologies in SPAN. The traffic that enters a switch port is called ingress traffic and the traffic that leaves through a switch port is known as egress traffic. The traffic onto a source port can be mirrored/monitored in either ingress or egress mode or in both directions. By default, both ingress and egress traffic are mirrored to the specified destination ports.

Configuration of SPAN is pretty easy. Only a single command format is used. You just have to specify the correct pair of source and destination ports and the mirroring would be enabled in no time. The following two commands are used for enabling SPAN:

```
S1(config)# monitor session 1 source interface f0/5
S1(config)# monitor session 1 destination interface f0/6
```

Here, 1 is the session ID. Each pair of pair of source and destination would belong to a separate session.

3. Configure SPAN:



I. **Configure R1 Interfaces**

```
R1(config)# int g0/0
R1(config-if)# ip address 192.168.0.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1# copy running-config startup-config
```

II. **Enable SPAN on Switch** (source – Fa0/1, dest – Fa0/2)

```
S1(config)# monitor session 1 source interface fa0/1
S1(config)# monitor session 1 destination interface fa0/2
R2# copy running-config startup-config
```

III. Configure PC0

```
IP: 192.168.0.5
Mask: 255.255.255.0
Gateway: 192.168.0.1
```

IV. Configure PC1

```
IP: 192.168.0.10
Mask: 255.255.255.0
Gateway: 192.168.0.1
```

V. Verify

```
S1# show monitor

See in Simulation (Follow Lab demonstration for specific
instructions)
```

4. Tasks:

I. You will configure SPAN following the address configurations and answer the given questions in this task. The task description for this task is provided in the pdf ***Task-1_SPAN***. You're ***not*** provided a .pka file for this task. You need to create the topology on your own.