**Switchport Analyzer**

Table of Contents

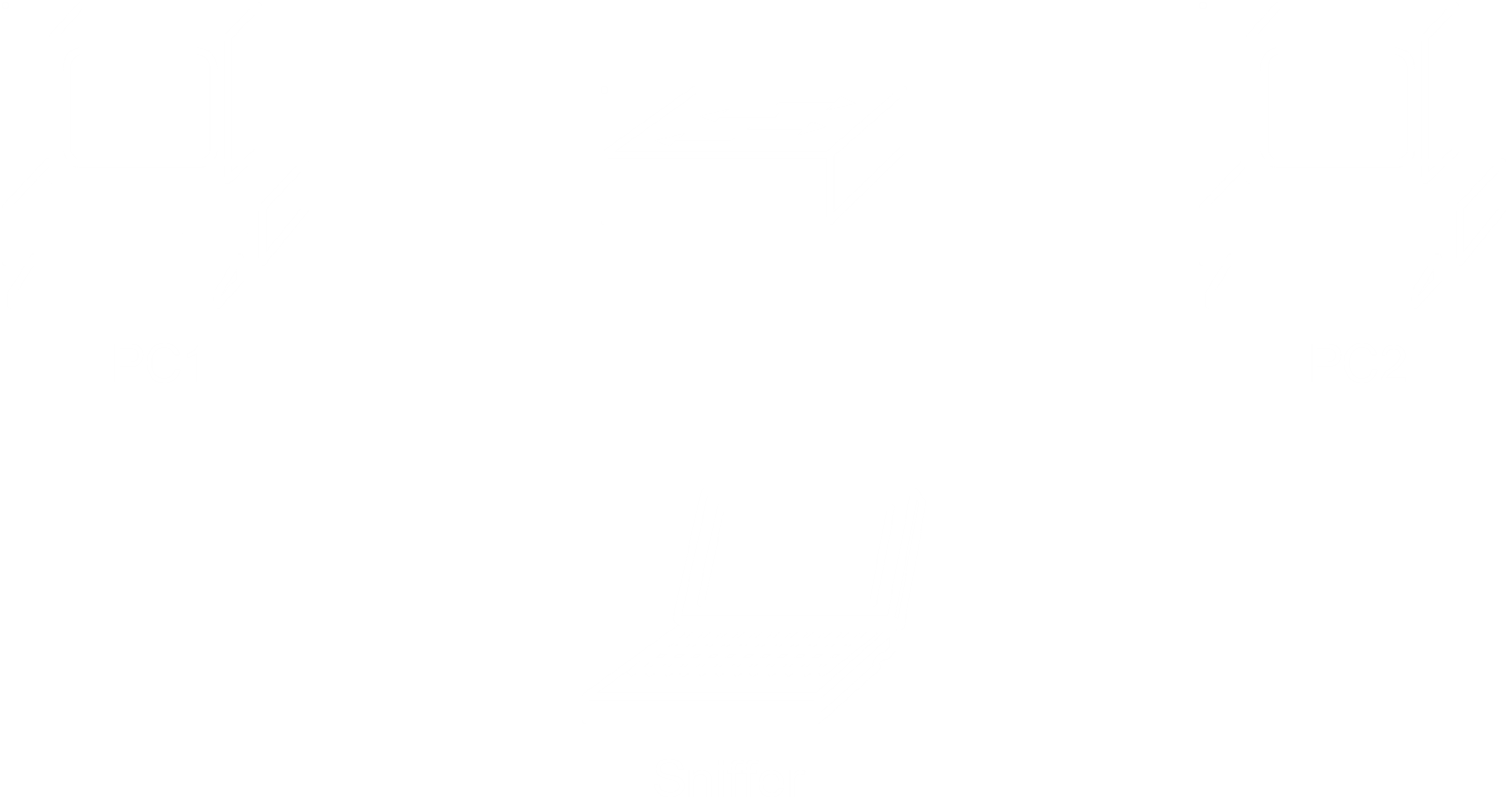
[Configuration 3](#_Toc87293969)

[Sessions 3](#_Toc87293970)

[Verification 3](#_Toc87293971)

[Simulation Mode 4](#_Toc87293972)

Imagine a scenario where we want to know what one device is send or receiving as traffic. This may be because for monitory or security purposes. This is possible through the concept of **Port Mirroring**.



In the above diagram, PC1 is communicating with PC2. We also have another device, the **sniffer**, attached to a different port in the switch. The switch can now be configured so that all the data that is sent out from the port connected to PC1 and all the data that is received at the port connected to PC1 is copied and sent to the sniffer as well. Note that this does not affect the normal communication between PC1 and PC2 and neither PC is made aware of the fact that there is a sniffer in between. However, the sniffer cannot be used for normal communication purposes.

In Cisco, the concept of port mirror is used in a feature called **Switchport Analyzer**, or **SPAN**. SPAN can work either with devices that are on the same switch, called **Local SPAN**, or with devices that are on a different switch, called **Remote SPAN**.

## Configuration

There is only a single command required to setup SPAN on a switch.

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

CLI

### Sessions

Notice that in the command to setup SPAN, there is a **session number**. Every association we create between a set of source ports, which can be an individual port, multiple ports or even a VLAN, and a destination port is called a session. Each session must be given a different number. The number of destination ports in a session varies from device to device.

In a session, we can mirror the traffic **entering** a port, called the **ingress traffic**, or the traffic **leaving** a port, called the **egress traffic**. By default, both are mirrored.

### Verification

We can verify that SPAN is enabled.

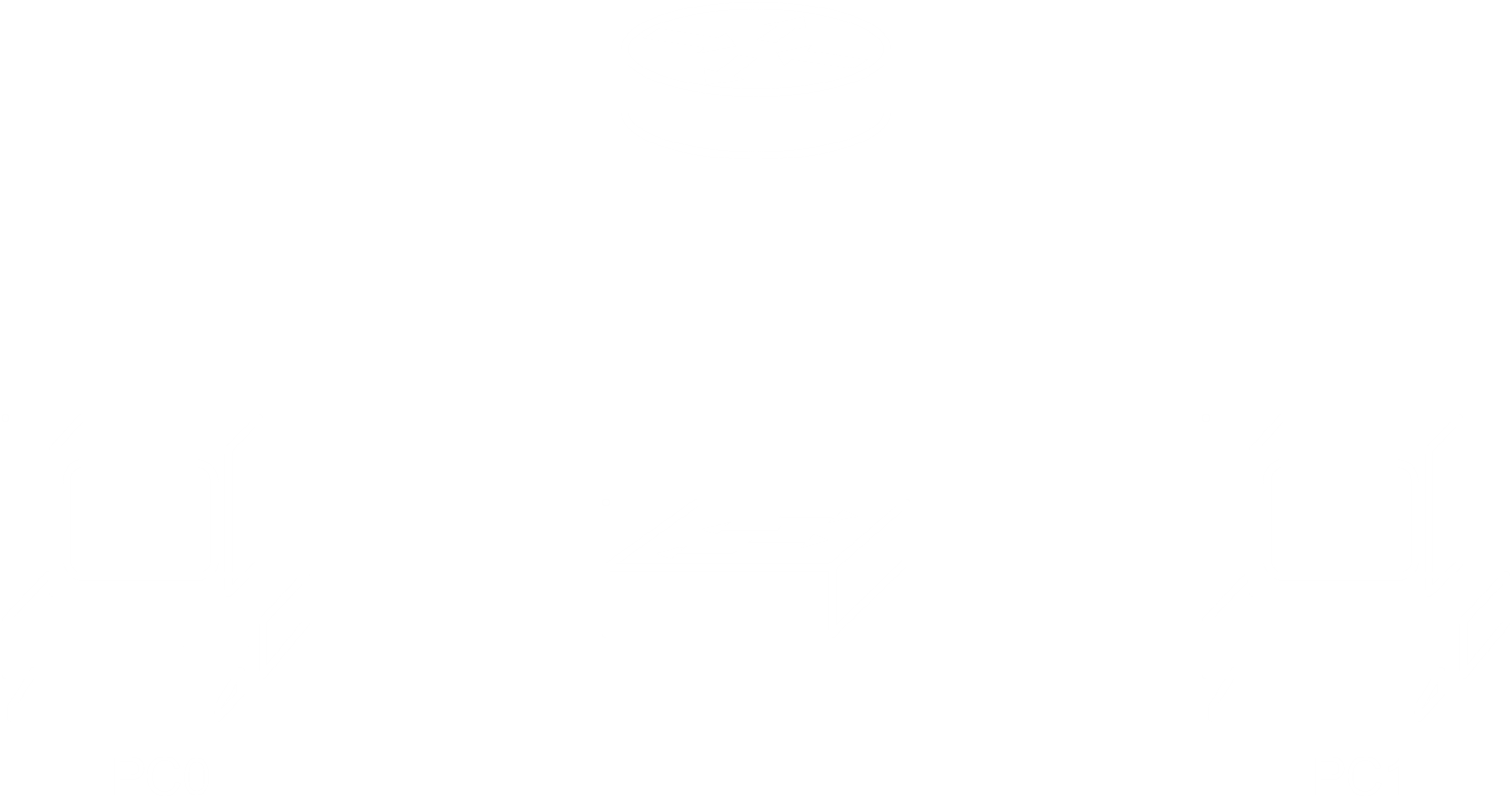
S1# show monitor

CLI

## Simulation Mode

The packets being sent to the sniffer have a different **destination address**, so normally, the sniffer should reject those packets. However, there are special **packet capturing software** that can be used on the sniffer to ensure those packets are not reject and can later be reviewed.

Since we are working with Cisco Packet Tracer, we do not have access to such special software. Instead, in order to make sure SPAN is working, we will be using the **Simulation Mode**.



1. Setup a network similar to the one show above. The details about what IP addresses or interfaces are being used on the devices are not relevant here. Anything is fine.
2. Next, click on the Simulation tab on the bottom right. This brings up a side panel at the bottom of which there is a huge list of filters. Essentially, by default, all packet types are monitored. However, we do not want this. We just want to monitor **ICMP packets**, which are the ones used to send pings. To do this, edit the filters and leave only the ICMP filter checked.
3. Next, click on the Add Simple PDU button from the menu bar. Then click on PC0 and finally on the router. Normally, the packet would start travelling immediately. Since we using Simulation mode however, we need to click on the Play button in the Simulation panel or the Next button to proceed.
4. Notice that the PDU packet travels from PC0 to the switch to the router. We will now setup the switch so that SPAN is enabled. Use the commands specified above to do this.
5. Once SPAN is set up, send another PDU packet under Simulation mode to see how a copy of the packet is sent to the sniffer as well. The sniffer will of course reject the packet, but that is not relevant.