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.

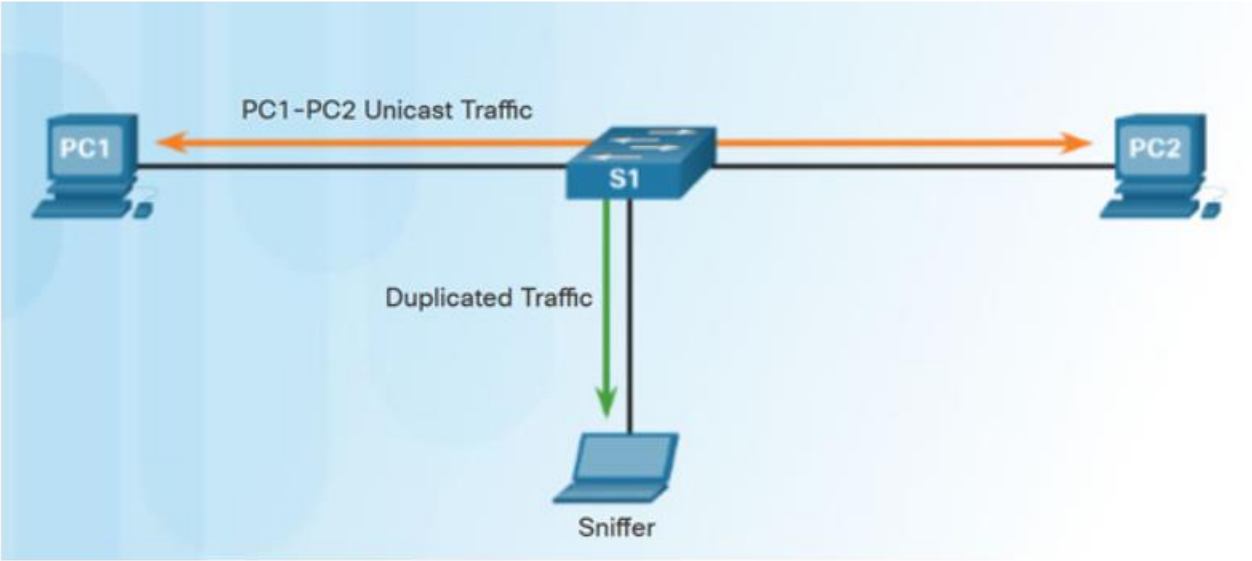


Fig: Port Mirroring

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.

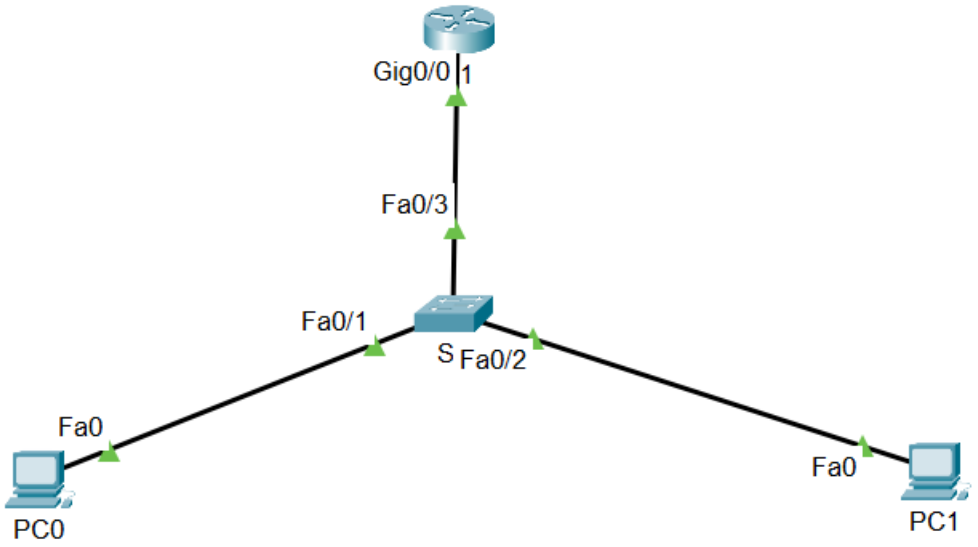
When configuring SPAN, an association between the *source ports* (the port whose traffic would be copied/mirrored) and the *destination port* (the port through which the copied/mirrored traffic will be sent) is made. In SPAN terminology, this association is known as a *session*. You can mirror traffic 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

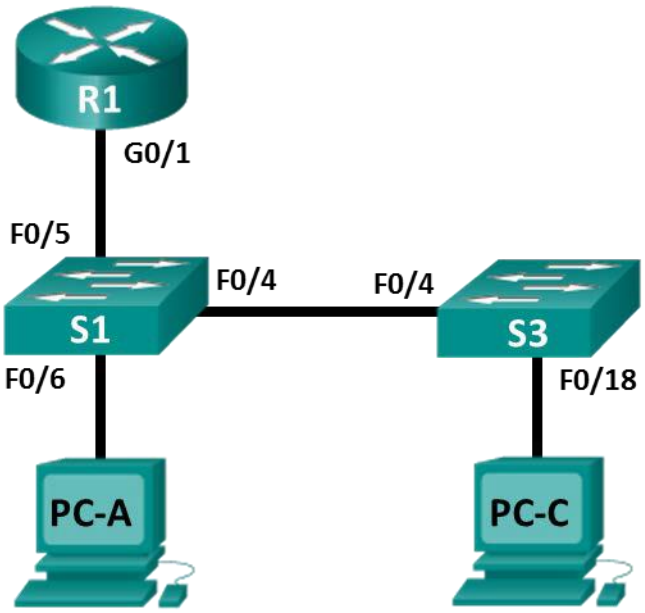
```
S1# show monitor

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.

Lab – Implement Local SPAN

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.1.3	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.254	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure Local SPAN

Background / Scenario

As the network administrator you want to analyze traffic entering and exiting the local network. To do this, you will set up port mirroring on the switch port connected to the router and mirror all traffic to another switch port. In this initial implementation, you will send all mirrored traffic to a PC which will be then verified via the Simulation Window. To set up port mirroring you will use the Switched Port Analyzer (SPAN) feature on the Cisco switch. SPAN is a type of port mirroring that sends copies of a frame entering a portca, out another port on the same switch. It is common to find a device running a packet sniffer or intrusion detection system (IDS) connected to the mirrored port.

© 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.4(3) (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.4(3) universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build the Network and Verify Connectivity

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

Step 1: Cable the network as shown in the topology.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure PC hosts.

Step 3: Initialize and reload the routers and switches as necessary.

Step 4: Configure basic settings for the router.

a. Disable DNS lookup.

b. Configure the device name as shown in the topology.

c. Configure an IP address for the router as listed in the Addressing Table.

d. Assign **class** as the encrypted privileged EXEC mode password.

e. Assign **cisco** for the console and vty password, enable login.

f. Set the vty lines to **transport input telnet**.

g. Configure **logging synchronous** to prevent console messages from interrupting command entry.

h. Copy the running configuration to the startup configuration.

Step 5: Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure the device name as shown in the topology.

c. Assign **class** as the encrypted privileged EXEC mode password.

d. Configure IP addresses for the switches as listed in the Addressing Table.

© 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

e. Configure the default gateway on each switch.

f. Assign **cisco** for the console and vty password and enable login.

g. Configure **logging synchronous** to prevent console messages from interrupting command entry.

h. Copy the running configuration to the startup configuration.

Step 6: Verify connectivity.

a. From PC-A, you should be able to ping the interface on R1, S1, S3, and PC-C. Were all pings successful?

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. From PC-C, you should be able to ping the interface on R1, S1, S3, and PC-A. Were all pings successful?

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Part 2: Configure Local SPAN

To configure Local SPAN you need to configure one or more source ports called monitored ports and a single destination port also called a monitored port for copied or mirrored traffic to be sent out from. SPAN source ports can be configured to monitor traffic in either ingress or egress, or both directions (default).

The SPAN source port will need to be configured on the port that connects to the router on S1 switch port F0/5. This way all traffic entering or exiting the LAN will be monitored. The SPAN destination port will be configured on S1 switch port F0/6 which is connected to PC-A. You'll check in the simulation tool whether the packets are being mirrored to F0/6 or not.

Step 1: Configure SPAN on S1.

a. Console into S1 and configure the source and destination monitor ports on S1. Now all traffic entering or leaving F0/5 will be copied and forwarded out of F0/6

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

Step 2: Open Simulation window and only keep the `ICMP` filter.

© 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Step 3: Telnet into R1 and create ICMP traffic on the LAN.

a. Telnet from S1 to R1.

```
S1# Telnet 192.168.1.1
Trying 192.168.1.1 . . . Open

User Access Verification

Password:
R1>
```

b. From privileged mode, ping PC-C, S1 and S3.

```
R1> enable
Password:
R1# ping 192.168.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1# ping 192.168.1.2
<Output omitted>
R1# ping 192.168.1.3
<Output omitted>
```

Step 4: Verify.

a. Were the pings from R1 to PC-C, S1 and S3 successfully copied and forwarded out f0/6 to PC-A?

b. Was the traffic monitored and copied in both directions?

© 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

outer Interface Summary Table

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

© 2018 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.