**Experiment 3**

**Local SPAN and Ethernet**

**Max group size:** 15

**Objective:**

* Learn how to monitor a connection and sniff packets using Wireshark.
* Analyzing Ethernet Frame.

**Tools and Equipment needed:**

* Cables and connection.
* 15 Cisco switches, 15 PCs.
* Wireshark installed on PC.

**Procedure:**

Setting up monitor session:

* Use the console cable to connect to your switch.
* Load your configuration in the running configuration and startup configuration files from Experiment 2. Make sure that VLAN 1 IP address is set.
* Enter the configuration mode.
* Write the following commands:

SY\_G(config)#monitor session 1 source interface Gi1/0/1

SY\_G(config)#monitor session 1 destination interface Gi1/0/13

These set of command will open a monitoring session with the ID#1, where any packet that pass through interface Gi1/0/1 will be copied, and the copied frame will be sent to Gi1/0/13.

* Go back to the privilege mode and type the command “show monitor session all” to confirm that the session with ID#1 is set correctly.

Q1: show the result of “show monitor session all” command.

Setting up the packet sniffer:

* Make sure to install Wireshark on your PC-S.
* Set the IP and subnet mask as follow.
  + IP: 192.G.Y.5
  + Subnet Mask: 255.255.0.0
* Connect your PC Ethernet port to the Switch Ethernet port Gi 1/0/13.
* Run Wireshark on your PC-S and start capturing on your local area connection or Ethernet.
* Now any frame that travel through Gi1/0/1 will be copied to your PC and Wireshark will present them.

Ethernet Frame analysis (Team work is required):

* Ask one of your team member to connect his PC-T to your switch via Gi1/0/1.

Note: do not change your team member IP address when he connects to your switch.

* On your PC-S make sure that you are capturing packets using Wireshark.
* From your team mate computer PC-T open the Microsoft Windows cmd and type the following command “ping 192.G.Y.2”.

Q2: show a printout proving that the ping has been successful.

* Go back to PC-S and from Wireshark try to find an ICMP packet that have the destination address 192.G.Y.2.

Q3: Expand the Ethernet Frame header and provided it in your report.

Q4: What is the source and destination MAC address?

Q5: Does the source MAC address match with your team member PC-T MAC address?

Q6: What is the frame Length?

PLEASE

reset all startup configuration using the command “write erase” and turn off your devices.

**Lab report (per student):**

The lab report includes the following:

* Present your switch running-config content showing:
  + You have set the IP address of VLAN1.
  + Moniter seession is set
* Answer all questions.