Department of Computer Science and Engineering

Islamic University of Technology (IUT)

A subsidiary organ of OIC

Laboratory Report

CSE 4512: Computer Networks Lab

Name: Md Farhan Ishmam

Student ID: 180041120

Section: CSE-1

Semester: Fifth

Academic Year: 2021

Date of Submission: 23-08-21

Title: Configuring Switch Port Analyzer (SPAN) in Cisco Devices

Objective:

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

Devices/ software Used:

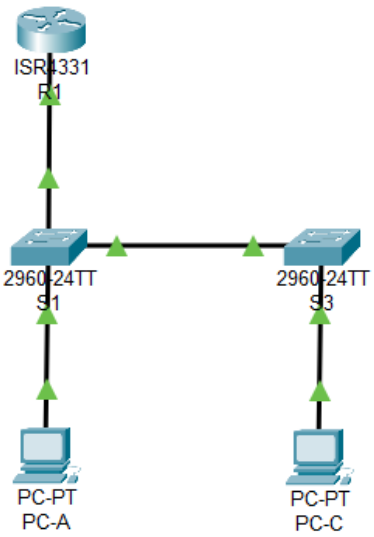
1. Device: Windows PC
2. Software: Cisco Packet Tracer 7.3.0

Theory:

Port Mirroring: Port mirroring mirrors traffic from one port to another by copying the packets from one port and sending it to another one where a packet analyzer is connected. A packet analyzer can be either purpose-built hardware or application-like software. As the port is a switch-port, the mirrored packets are Ethernet frames.

Local SPAN: When traffic on a switch port is mirrored to another port on that same switch then it's called Local SPAN.

Diagram of the experiment(s):



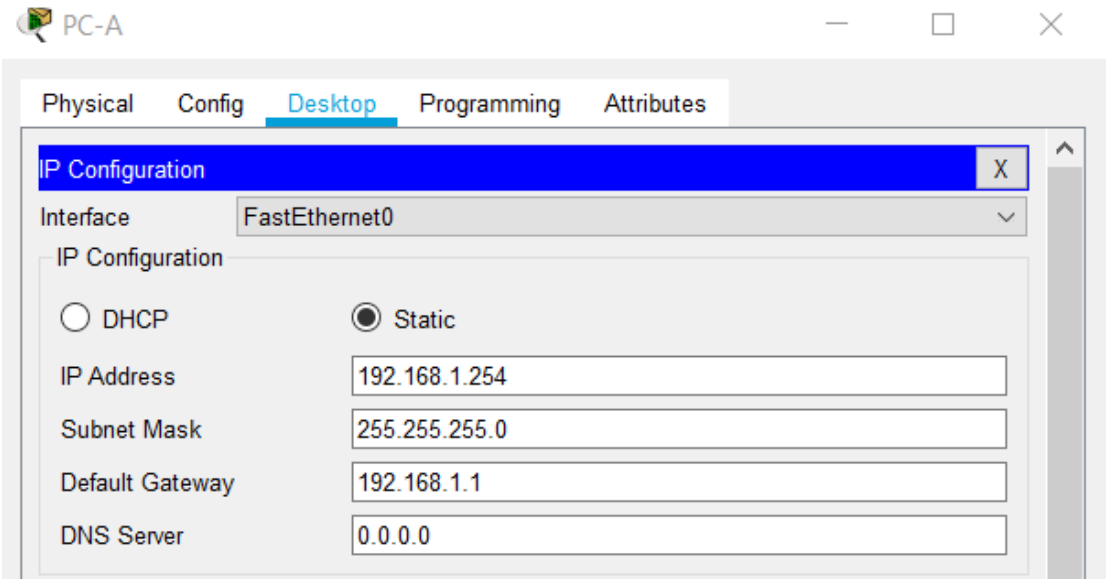
Working Procedure:

Part 1: Build the Network and Verify Connectivity

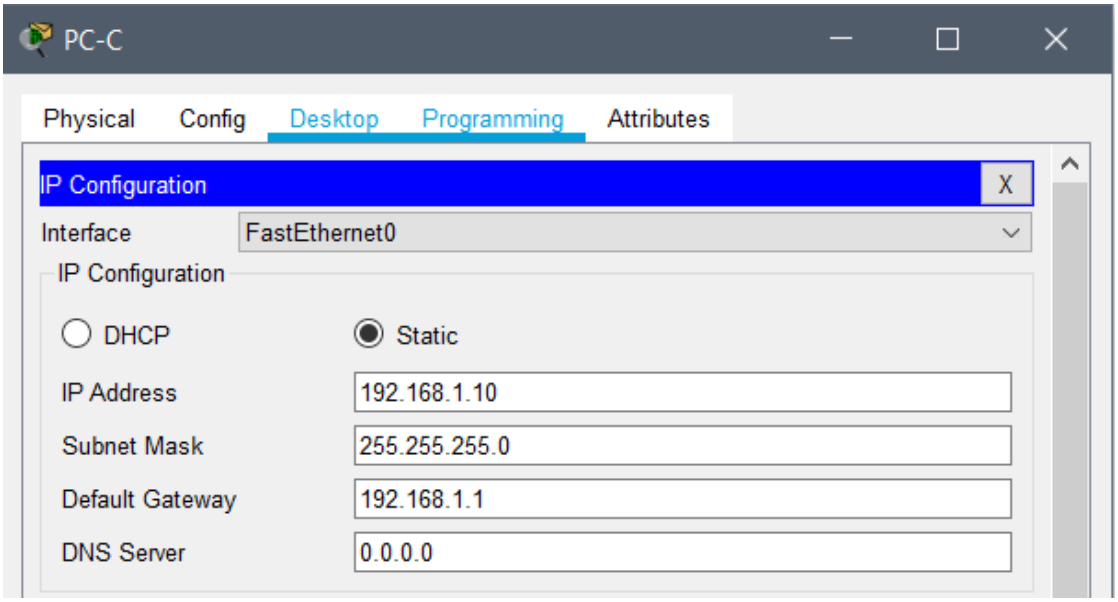
Step 1: Cable the network as shown in the topology.

Step 2: Configure PC hosts

PC-A



PC-C



Step 3: Initialize and reload the routers and switches as necessary.
Step 4: Configure basic settings for the router.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ho R1
R1(config)#no ip domain-lookup
R1(config)#int g0/0/1
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R1(config-if)#en secret class
% Ambiguous command: "en secret class"
R1(config)#enable secret class
R1(config)#con 0
R1(config)#password cisco
             ^
% Invalid input detected at '^' marker.

R1(config)#line con 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#vty 0 15
           ^
% Invalid input detected at '^' marker.

R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#transport input telnet
R1(config-line)#line console 0
R1(config-line)#logging sync
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Step 5: Configure basic settings for each switch

S1:

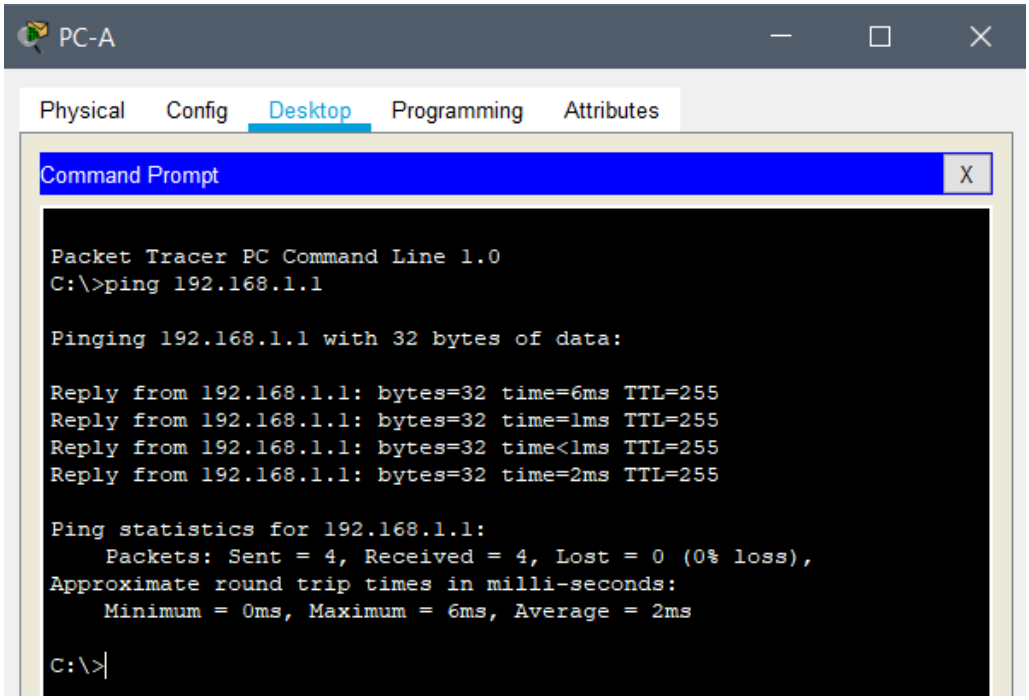
```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ho S1
S1(config)#no ip domain lookup
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#logging sync
S1(config-line)#exit
S1(config)#vty 0 15
             ^
% Invalid input detected at '^' marker.

S1(config)#line vty 0 15
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#int vlan 1
S1(config-if)#ip add 192.168.1.2 255.255.255.0
S1(config-if)#no shut

S1(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S1(config-if)#int vlan 1
S1(config-if)#ip default gateway 192.168.1.1
                 ^
% Invalid input detected at '^' marker.

S1(config-if)#ip default-gateway 192.168.1.1
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

S3:

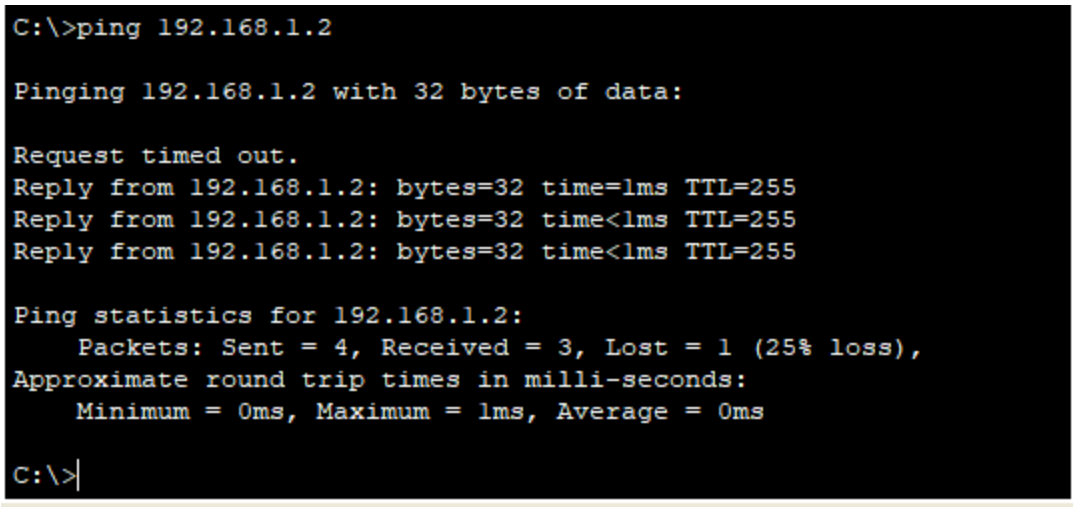
```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ho S3
S3(config)#no ip domain-lookup
S3(config)#en secret class
% Ambiguous command: "en secret class"
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#logging sync
S3(config-line)#exit
S3(config)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#int vlan 1
S3(config-if)#ip add 192.168.1.3 255.255.255.0
S3(config-if)#no shut

S3(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

S3(config-if)#
S3(config-if)#ip default-gateway 192.168.1.1
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Step 6: Verify connectivity

PC-A to R1



PC-A to S1



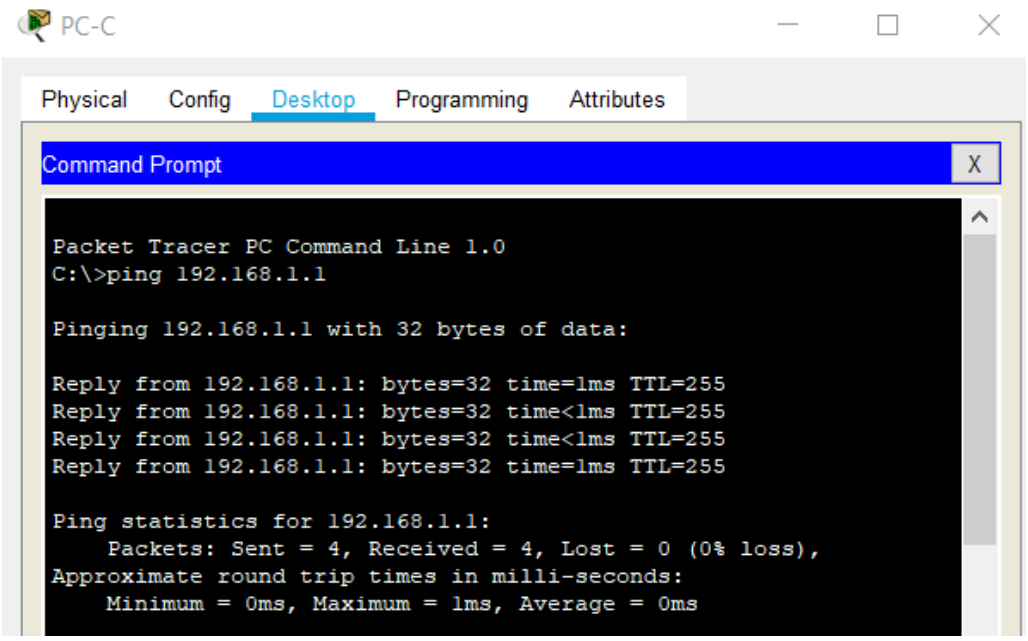
PC-A to S3

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time<1ms TTL=255
Reply from 192.168.1.3: bytes=32 time<1ms TTL=255
Reply from 192.168.1.3: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC-A to PC-C

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time=4ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```

PC-C to R1:



PC-C to S1:

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC-C to S3

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time<1ms TTL=255
Reply from 192.168.1.3: bytes=32 time<1ms TTL=255
Reply from 192.168.1.3: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC-C to PC-A

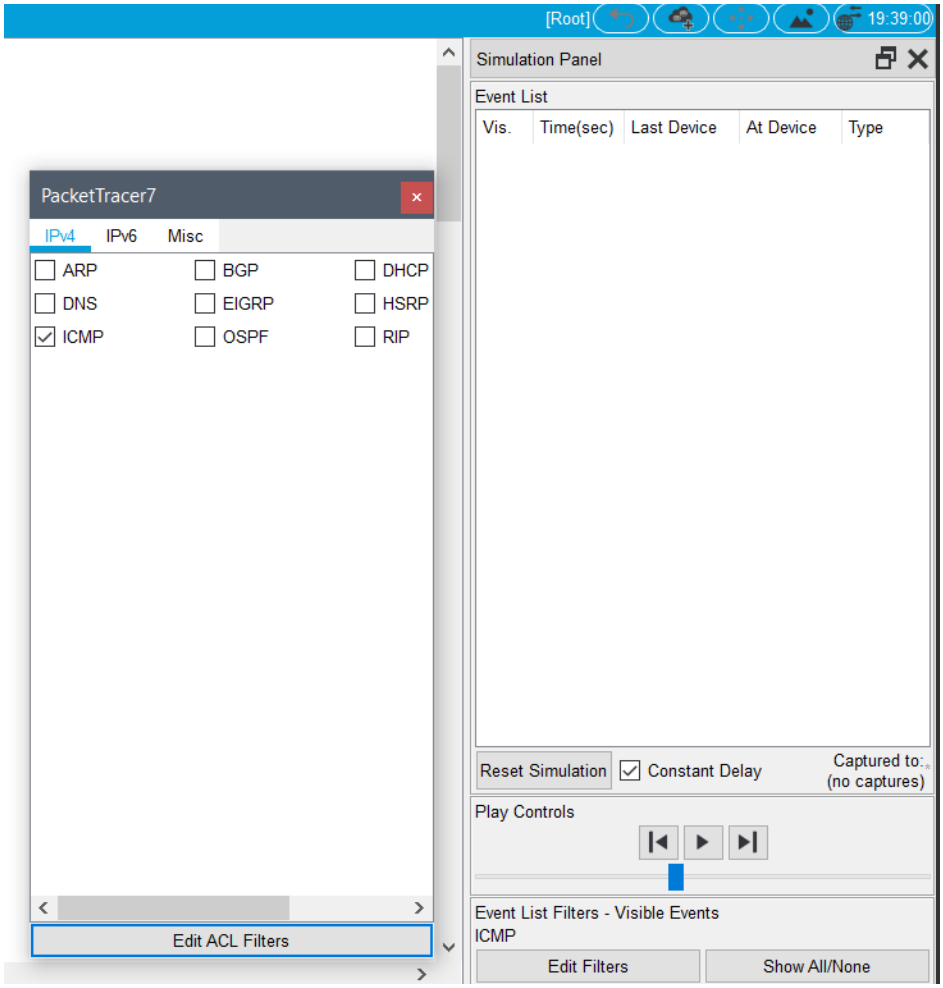
```
C:\>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time=1ms TTL=128
Reply from 192.168.1.254: bytes=32 time<1ms TTL=128
Reply from 192.168.1.254: bytes=32 time<1ms TTL=128
Reply from 192.168.1.254: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Part 2: Configure Local SPAN

Step 1: Configure SPAN on S1

```
S1>en
Password:
S1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#monitor session 1 source int f0/5
S1(config)#monitor session 1 dest int f0/6
S1(config)#
```

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

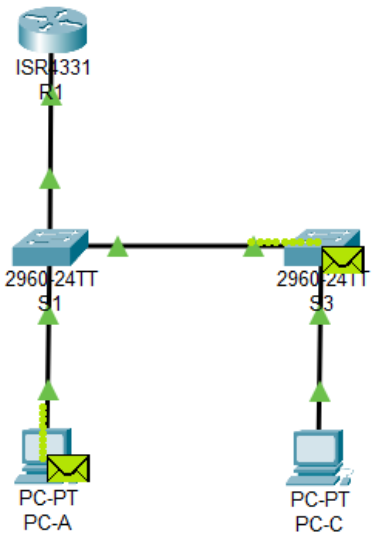


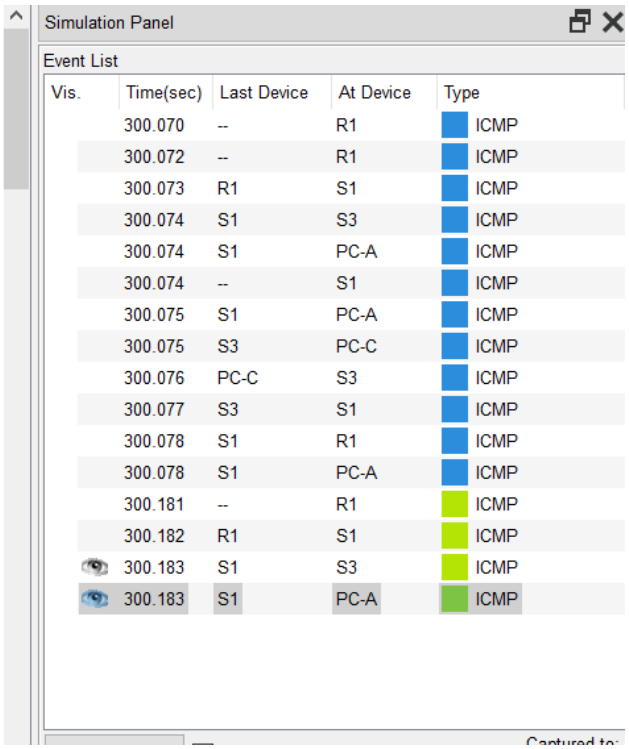
Step 3: Telnet into R1 and create ICMP traffic on the LAN

```
S1#telnet 192.168.1.1
Trying 192.168.1.1 ...Open


User Access Verification

Password:
R1>
```

```
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 = 0/0/3 ms

R1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R1#ping 192.168.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms
```

Step 4: Verify





Questions:

Task # 01:

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

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

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

5. Was the traffic monitored and copied in both directions?
   Ans: Yes