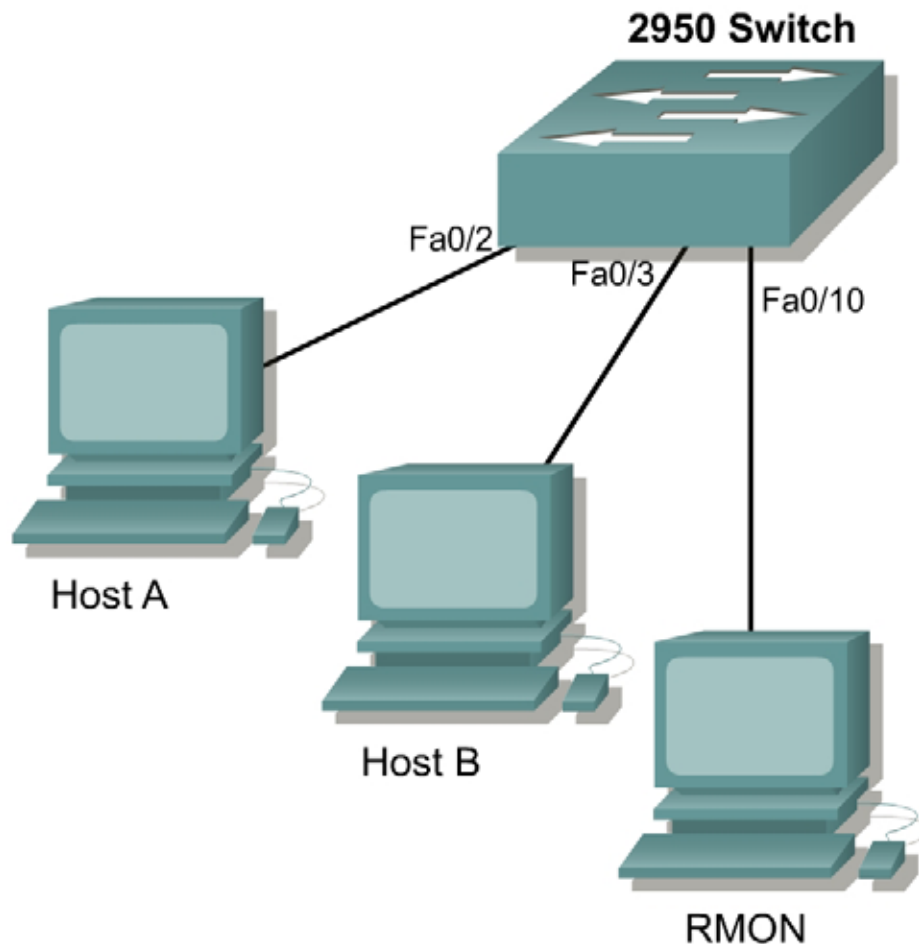


Lab 7.5.9.1 Creating a Switched Port Analyzer (SPAN) Session



Objective

In this lab a Switched Port Analyzer (SPAN) session will be created to remotely monitor network traffic.

Scenario

The effective monitoring of network traffic in a fully switched network can be challenging. SPAN is included in the 2950, 3550 and 6500 switches. Therefore, the LAN traffic received or transmitted by single or multiple switch ports can be copied and forwarded to a monitoring port. This mirrored traffic can then be captured and analyzed.

A company has recently upgraded to fully switched network architecture. To optimize network performance, network traffic will be monitored for analysis purposes. The SPAN features of Cisco switches will be used to enable this process. A SPAN session will initially be implemented on an access layer 2950 switch to test the potential of port-centric traffic monitoring.

Protocol analysis software such as Protocol Inspector or Optiview Protocol Expert should be loaded and running on a host that will act as the Remote Monitor (RMON). Two hosts must be configured with IP addresses in the same subnet to be able to share network traffic.

Step 1

Enter global configuration mode in the switch IOS. Create a monitor session on the switch by defining the source interface of a monitor session called session 1.

```
Switch(config)#monitor session 1 source interface fastethernet 0/2
```

Step 2

Create a destination port, FastEthernet 0/10, which will receive the mirrored traffic being sent to and transmitted from FastEthernet 0/2, which is the source port.

```
Switch(config)#monitor session 1 destination interface fastethernet 0/10
Switch(config)#exit
```

1. What does the switch advertise when switch port FastEthernet 0/10 becomes a destination port?

Step 3

Use the **show monitor** command to verify that the session has been correctly configured.

```
Switch#show monitor session 1
```

The following output should display.

```
Switch#show monitor session 1 detail
Session 1
-----
Type                : Local Session
Source Ports        :
    RX Only         : None
    TX Only         : None
    Both            : Fa0/2
Source VLANs        :
    RX Only         : None
    TX Only         : None
    Both            : None
Source RSPAN VLAN   : None
Destination Ports   : Fa0/10
    Encapsulation   : Native
    Ingress         : Disabled
Reflector Port      : None
Filter VLANs        : None
Dest RSPAN VLAN     : None

Switch#
```

Configure Host A with address 192.168.1.1 and Host B with the address 192.168.1.2. Use the subnet mask 255.255.255.0 for both hosts. The monitoring host attached to the SPAN destination

port can be in any network. Ping continuously from Host A to Host B. The RMON should pick up the ICMP traffic received by FastEthernet port 0/2 and also forwarded by FastEthernet port 0/2 to FastEthernet port 0/3.

2. Are other packets being forwarded to the destination port? If so, what are they?

Step 4

Add an additional port to the session for mirroring onto the destination port.

```
Switch(config)#monitor session 1 source interface fastethernet 0/2 ,
                fastethernet 0/3

Switch#show monitor session 1 detail
Session 1
-----
Type                : Local Session
Source Ports        :
    RX Only         : None
    TX Only         : None
    Both            : Fa0/2-3
Source VLANs        :
    RX Only         : None
    TX Only         : None
    Both            : None
Source RSPAN VLAN   : None
Destination Ports   : Fa0/10
    Encapsulation   : Native
    Ingress         : Disabled
Reflector Port      : None
Filter VLANs        : None
Dest RSPAN VLAN     : None

Switch#
```

An additional port called FastEthernet 0/3 is added to monitoring session 1. Multiple ports can be added by adding a space after the interface number, a comma, another space, and an additional port/port number. A continuous series of ports can be added by using a dash (–) instead of a comma to separate the initial port and the final port in a sequence.

Send another ping from Host A to Host B. Why should the amount of ICMP traffic collected by the RMON increase?

TFTP a file from Host A to Host B and observe the different packet types that are being monitored.

Step 5

Remove port FastEthernet 0/3 from the monitored port list.

```
Switch(config)#no monitor session 1 source interface fastethernet 0/3

Switch#show monitor session 1 detail
Session 1
-----
Type                : Local Session
Source Ports        :
    RX Only         : None
```

```
TX Only      : None
Both         : Fa0/2
Source VLANs :
RX Only      : None
TX Only      : None
Both         : None
Source RSPAN VLAN : None
Destination Ports : Fa0/10
Encapsulation : Native
Ingress      : Disabled
Reflector Port : None
Filter VLANs  : None
Dest RSPAN VLAN : None

Switch#
```

Step 6

Use the **show monitor** command to verify that this has occurred.

```
Switch(config)#show monitor session 1
```

3. Send an additional **ping** from Host A to Host B. How has removing port FastEthernet 0/3 from the monitor session affected the amount of data captured?

Step 7

Remove SPAN monitoring from the switch.

Enter global configuration mode.

```
Switch(config)#no monitor session 1
```

A **show monitor session 1** reveals that the SPAN session has been deleted from the switch.

```
Switch#show monitor session 1

No SPAN configuration is present in the system for session [1].
```