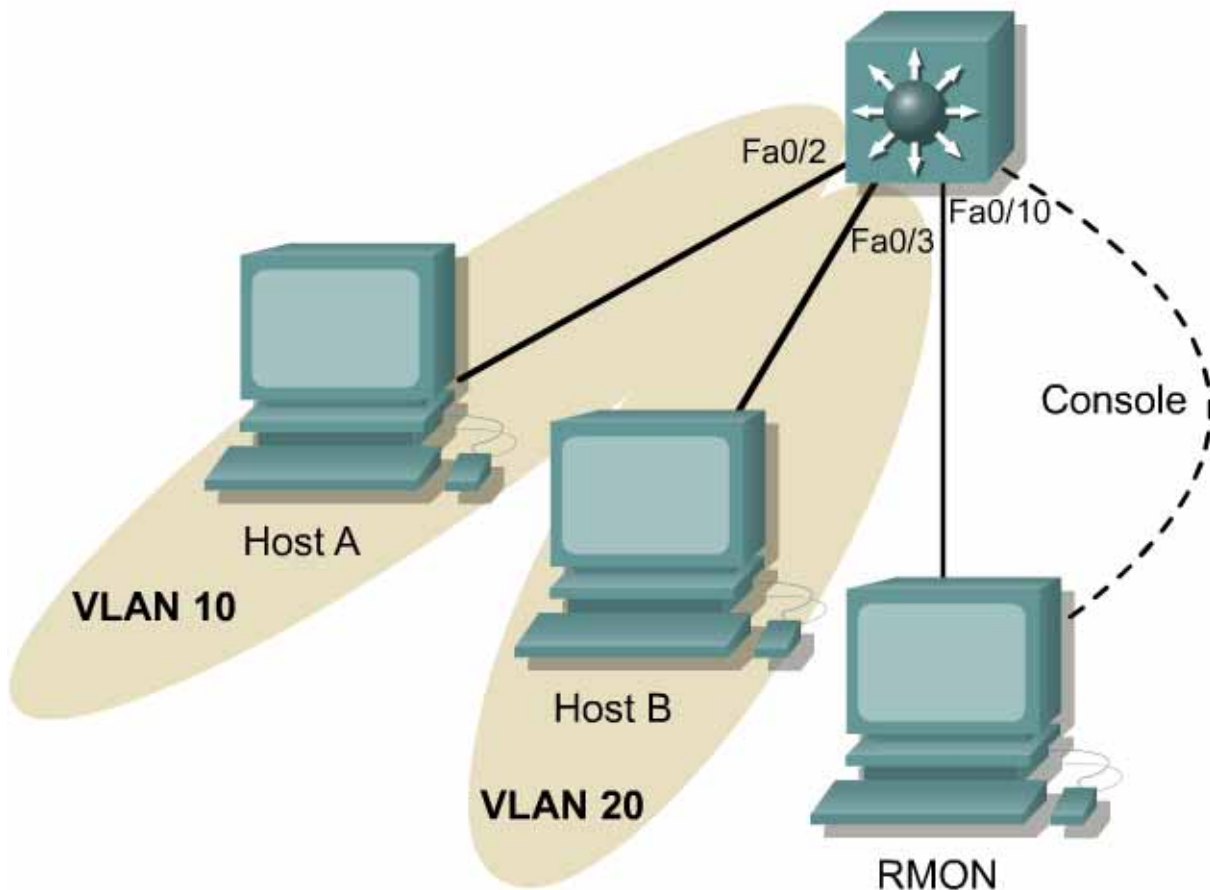


Lab 7.5.9.2 Creating a VSPAN Session



Objective

In this lab a VLAN Switchport Analyzer (VSPAN) session is created to remotely monitor network traffic.

Scenario

Effective monitoring of network traffic in fully switched networks can be challenging. However, it can be made easier with the inclusion of VSPAN in 3550 and 6500 switches. Using VSPAN, the LAN traffic received or transmitted by single or multiple VLANs can be copied and forwarded to a monitoring port. This mirrored traffic can then be captured and analyzed.

A company has recently upgraded to a fully switched network architecture. In order to optimize network performance it has been decided that network traffic should be monitored for analysis purposes. The VSPAN features of Cisco switches will be used to enable this process. A VSPAN session will be implemented on a distribution layer 3550 switch, to explore the potential of VLAN based 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) for this session. Two hosts, Host A and Host B, will also need to be configured with IP addresses in different subnets, to represent hosts in different VLANs.

Step 1

On the Catalyst 3550 switch, enter global configuration mode. Create a VLAN containing FastEthernet port 0/2 called VLAN 10:

```
Switch(config)#interface fastethernet 0/2
Switch(config-if)#switchport access vlan 10
```

Next, create a VLAN containing FastEthernet port 0/3 called VLAN 20:

```
Switch(config)#interface fastethernet 0/3
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
```

Step 2

It is important to ensure that previous SPAN based sessions are cleared from the switch.

In global configuration mode enter the following command:

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

Step 3

Configure routing between VLAN 10 and VLAN 20. This is achieved by creating switch virtual interfaces (SVIs) for VLAN10 and VLAN 20. Assign IP addresses within VLAN 10 and VLAN 20 to the respective interfaces and enable **ip routing** in global configuration mode. Remember to configure the Host A and Host B network interface card (NIC) default gateway with the SVI IP addresses of their respective VLAN interfaces.

```
Switch#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface vlan 10
Switch(config-if)#ip add 192.168.1.1 255.255.255.0
Switch(config-if)#interface vlan 20
Switch(config-if)#ip add 192.168.2.1 255.255.255.0
Switch(config-if)#ip routing
Switch(config)#^Z
Switch#
```

Test connectivity by pinging between the VLANs and troubleshoot where necessary.

What does this do to the amount of traffic received by the VSPAN destination port?

Step 4

Create a monitor session on the switch by defining the source VLAN of a monitor session called session 1:

```
Switch(config)#monitor session 1 source VLAN 10 rx
```

The **rx** is specified because VSPAN sessions can only occur based on traffic received by the VLAN switch ports.

Step 5

Create a destination port, which will receive the mirrored traffic being sent to source ports within VLAN 10:

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

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

An option exists to take into account any encapsulation when trunking has been configured on a switch. The full command syntax, which will not be used in this lab, is as follows:

```
Switch(config)#monitor session session_number destination interface  
module/interface encapsulation [isl|dot1q]
```

Step 6

To check that the session has been correctly configured, use the following command:

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

The following output should be displayed:

```
Switch#show monitor session 1 detail
Session 1
-----
Type                : Local Session
Source Ports        :
    RX Only         : None
    TX Only         : None
    Both            : None
Source VLANs        :
    RX Only         : 10
    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#
```

Ping continuously from Host A to Host B.

2. Are packets being received by the RMON?

Step 7

An additional VLAN will be added to the session for mirroring onto the destination port:

```
Switch(config)#monitor session 1 source VLAN 10 , 20 rx
```

Multiple VLANs can be added to a monitoring session by inserting a space and comma after the previous VLAN, followed by a further space and then the subsequent VLAN. A continuous series of VLANs could be added by using a dash (–) instead of a comma, separating the initial and final VLAN in a sequence.

Use the **show monitor session 1** command to verify VLANs 10 and 20 are now being monitored.

```
Switch#show monitor session 1 detail
Session 1
-----
Type                : Local Session
Source Ports        :
    RX Only         : None
    TX Only         : None
    Both            : None
Source VLANs        :
    RX Only         : 10,20
    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#
```

3. Does the amount of ICMP traffic collected by the RMON change? Why?

Step 8

Remove VLAN 20 from the monitored port list:

```
Switch(config)#no monitor session 1 source VLAN 20 rx
```

Step 9

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

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

4. How has removing VLAN 20 from the monitor session affected the amount of data captured?