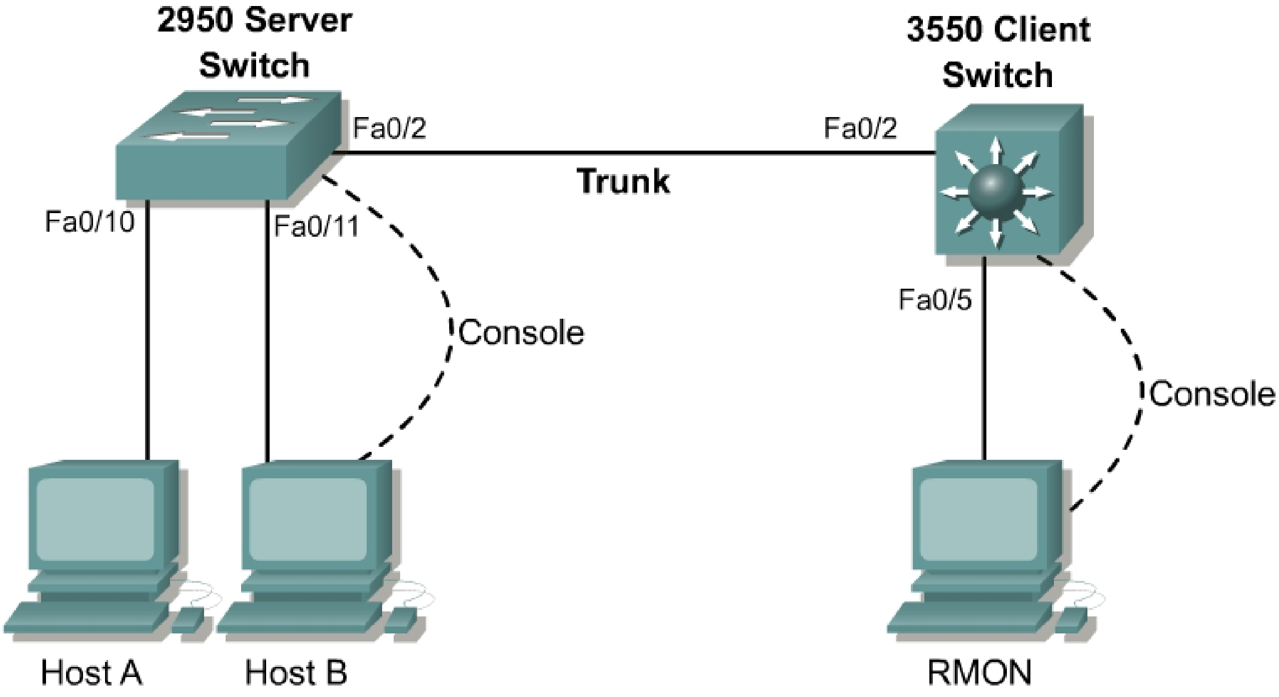
Lab 7.5.9.3 Creating a RSPAN Session



Objective

In this lab a Remote Switchport Analyzer (RSPAN) session will be created on two switches to remotely monitor network traffic.

Scenario

Effective monitoring of network traffic in fully switched networks can be challenging. However, the process can be made easier with the inclusion of RSPAN in 2950, 3550, and 6500 series switches. Using RSPAN, LAN traffic received or transmitted by switchports or VLANs can be copied and forwarded to a monitoring port on a remote switch. This mirrored traffic can then be captured and analyzed.

A company has recently upgraded to fully switched network architecture. In order to optimize network performance, it has been decided that network traffic should be monitored for analysis purposes. After trying SPAN sessions and VSPAN sessions on a single switch it is now time to progress to RSPAN session trials. This will occur by monitoring traffic generated on one switch and using a remote switch port as the destination for the monitored traffic.

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

Step 1

Cable the network devices according to the diagram and configure the hostname **Server** for the 2950 switch and **Client** for the 3550 switch.

Step 2

Enter global configuration mode in the Server switch IOS. Clear any previous monitor sessions:

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

Step 3

From privileged mode, enter the VLAN database and create a VTP server and domain name so that VLAN information can be propagated from the Server switch to the attached Client switch.

```
Server#vlan database
Server(vlan)#vtp server
Server(vlan)#vtp domain CORP
```

On the Client 3550 enter the VLAN database and create a Virtual Terminal Protocol (VTP) client in the same domain:

```
Client#vlan database
Client(vlan)#vtp client
Client(vlan)#vtp domain CORP

Server#vlan database
Server(vlan)#vtp server
Device mode already VTP SERVER.
Server(vlan)#vtp domain CORP
Changing VTP domain name from NULL to CORP
Server(vlan)#exit
APPLY completed.
Exiting....

Server#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 250
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : CORP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x9D 0xEF 0x7A 0x6D 0xE0 0x6C 0xE1 0xDE
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Client#vlan database
Client(vlan)#vtp client
Setting device to VTP CLIENT mode.
Client(vlan)#exit
In CLIENT state, no apply attempted.
Exiting....

Client#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
```

```
VTP Operating Mode              : Client
VTP Domain Name                 : CORP
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x9D 0xEF 0x7A 0x6D 0xE0 0x6C 0xE1 0xDE
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

Step 4

Create a unique VLAN for the RSPAN session. This VLAN will be forwarded through a VLAN trunk to its destination port in exactly the same way as normal traffic. The RSPAN VLAN must be a unique VLAN. It cannot be a native VLAN of any of the active switch ports:

```
Server(config)#vlan 901
Server(config-vlan)#remote-span
Server(config-vlan)#exit
```

Step 5

Create the trunk between the Server switch and Client switch. Perform the same procedure on both the Server switch and Client switch:

```
Server(config)#interface fastethernet 0/2
Server(config-if)#switchport trunk native vlan 99
Server(config-if)#switchport mode trunk
Server(config-if)#^Z

Client3350(config)#interface fastethernet 0/2
Client3350(config-if)#switchport trunk native vlan 99
Client3350(config-if)#switchport trunk encapsulation dot1q
Client3350(config-if)#switchport mode trunk
Client3350(config-if)#^Z
```

Step 6

Verify that the trunks are set correctly at both ends using the **show interface fastethernet 0/2 trunk** command. Output for both switches should indicate that the RSPAN VLAN is present on both switches as an allowed VLAN in the CORP management domain.

```
Server#show interface fastethernet 0/2 trunk

Port      Mode         Encapsulation  Status        Native vlan
Fa0/2     on           802.1q         trunking      99

Port      Vlans allowed on trunk
Fa0/2     1-4094

Port      Vlans allowed and active in management domain
Fa0/2     1,901

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/2     1,901


Client#show interfaces fastethernet 0/2 trunk

Port      Mode         Encapsulation  Status        Native vlan
Fa0/2     on           802.1q         trunking      99

Port      Vlans allowed on trunk
```

```
Fa0/2     1-4094

Port      Vlans allowed and active in management domain
Fa0/2     1,901

Port      Vlans in spanning tree forwarding state and not pruned

Fa0/2     1,901
```

Step 7

The Server switch will be the source for the RSPAN session. Configure two ports as source ports for mirrored traffic:

- Fastethernet port 0/10 will be monitored for bi-directional traffic
- Fastethernet port 0/11 will only be monitored for received traffic

```
Server(config)#monitor session 1 source interface fastethernet 0/10 both
Server(config)#monitor session 1 source interface fastethernet 0/11 rx
```

Step 8

A reflector port will now be configured on the RSPAN source switch. This is an actual physical port set to loopback mode. In order to redirect copies of the monitored traffic onto the RSPAN VLAN for transport to the destination switch, enter the following commands:

```
Server(config)#monitor session 1 destination remote vlan 901 reflector-port
               fastethernet 0/12
Server(config)#end
```

1. What happened when the above command was entered? Why?

Step 9

Confirm that the RSPAN session has been correctly configured by using the **show monitor session** command:

```
Server#show monitor session 1 detail
Session 1
---------
Type               : Remote Source Session
Source Ports       :
    RX Only        : Fa0/11
    TX Only        : None
    Both           : Fa0/10
Source VLANs       :
    RX Only        : None
    TX Only        : None
    Both           : None
Source RSPAN VLAN  : None
Destination Ports  : None
Reflector Port     : Fa0/12
Filter VLANs       : None
Dest RSPAN VLAN:     901


Server#
```

Step 10

The client switch will act as the RSPAN session destination. It needs to be configured to transfer the RSPAN VLAN traffic from the trunk towards the nominated destination port. The first command identifies the RSPAN source VLAN. The second command defines the port that the RSPAN VLAN traffic should be forwarded to:

```
Client(config)#monitor session 1 source remote vlan 901
Client(config)#monitor session 1 destination interface fastethernet 0/5
Client(config)#end
```

Step11

Confirm that the RSPAN session has been correctly configured. Use the **show monitor session** command:

```
Client#show monitor session 1 detail
Session 1
---------
Type                : Remote Destination Session
Source Ports        :
    RX Only         : None
    TX Only         : None
    Both            : None
Source VLANs        :
    RX Only         : None
    TX Only         : None
    Both            : None
Source RSPAN VLAN : 901
Destination Ports : Fa0/5
    Encapsulation: Native
          Ingress: Disabled
Reflector Port    : None
Filter VLANs      : None
Dest RSPAN VLAN   : None


Client#
```

Generate some pings between Host A and Host B. The Layer 3 traffic generated by Host A should be forwarded to Host C, the remote monitor.

Step 12

The characteristics of one of the source ports, Fastethernet 0/10, will now be altered from monitoring bi-directional traffic to only monitoring sent traffic:

```
Server(config)#no monitor session 1 source interface fastethernet 0/10 both
Server(config)#monitor session 1 source interface fastethernet 0/10 rx
```

In privileged mode, confirm that the monitor session characteristics have changed with the **show monitor session** command. Generate a **ping** from Host A to Host B.

```
Server#show monitor session 1 detail
Session 1
---------
Type                : Remote Source Session
Source Ports        :
    RX Only         : Fa0/10-11
    TX Only         : None
    Both            : None
Source VLANs        :
    RX Only         : None
    TX Only       : None
    Both          : None
Source RSPAN VLAN : None
Destination Ports : None
Reflector Port    : Fa0/12
Filter VLANs      : None
Dest RSPAN VLAN:   901


Server#
```

1. What happened to the volume and types of traffic logged by Host C?

Step 13

Now one of the source ports will be removed from the RSPAN session:

```
Server(config)#no monitor session 1 source interface fastethernet 0/10
Server(config)#end
```

Again, in privileged mode, confirm that the monitor session characteristics have changed with the **show monitor session** command. Generate additional pings from Host A to Host B.

```
Server#show monitor session 1 detail
Session 1
---------
Type              : Remote Source Session
Source Ports      :
    RX Only       : Fa0/11
    TX Only       : None
    Both          : None
Source VLANs      :
    RX Only       : None
    TX Only       : None
    Both          : None
Source RSPAN VLAN : None
Destination Ports : None
Reflector Port    : Fa0/12
Filter VLANs      : None
Dest RSPAN VLAN:   901


Server#
```

2. What happened to the volume and types of traffic logged by Host C?