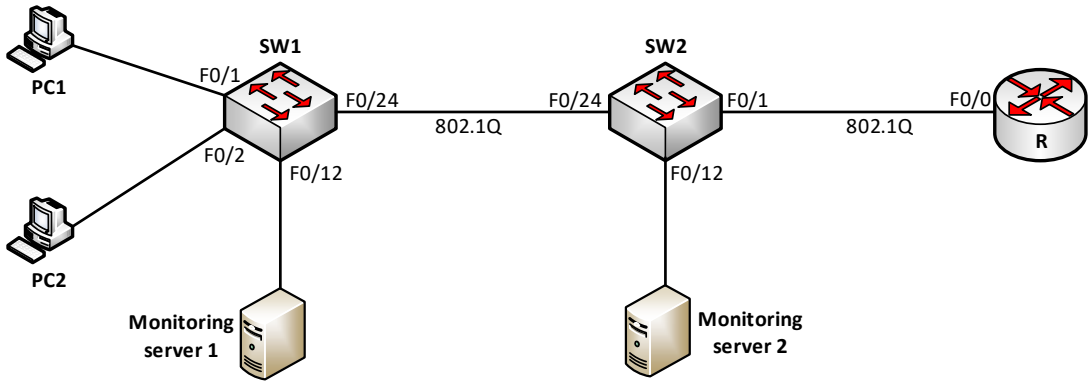
SPAN và RSPAN

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Bài lab gồm các router và các PC được kết nối với nhau như hình 1. Trong các PC tham gia bài lab, hai PC được sử dụng với vai trò Monitoring server.
- Trong bài lab này, học viên sẽ thực tập cấu hình tính năng SPAN và RSPAN trên các switch.

Yêu cầu:

1. Cấu hình trunking:

- Thực hiện thiết lập đường trunk kết nối giữa SW1 và SW2.
- Đường trunk này sử dụng kỹ thuật trunking Dot1Q, thiết lập tĩnh, tắt DTP.

2. Cấu hình VTP và VLAN:

- Thực hiện cấu hình VTP trên hai switch theo yêu cầu sau:
  - VTP domain: waren, VTP password: cisco.
  - SW1: server, SW2: client.
- Trên SW1 thực hiện cấu hình các VLAN 10 và 20. Kiểm tra xác nhận rằng cấu hình VLAN này đã được lan truyền đến SW2.
- Trên SW1 thực hiện gán cổng F0/1 vào VLAN 10 và F0/2 vào VLAN 20.

3. Định tuyến VLAN trên router:

- Cấu hình router R định tuyến giữa hai VLAN 10 và 20 theo các thông số theo bảng sau:

Cổng	*VLAN kết nối*	*Địa chỉ IP*
F0/0.10	10	192.168.10.1/24
F0/0.20	20	192.168.20.1/24

Bảng 1 – Thông tin định tuyến VLAN.

4. SPAN:

- Cấu hình tính năng SPAN để SW1 thực hiện sao lưu tất cả dữ liệu ra/vào cổng F0/1 đến Monitoring server 1 đặt trên cổng F0/12.

5. RSPAN:

- Cấu hình tính năng RSPAN để SW1 thực hiện sao lưu tất cả dữ liệu đi qua VLAN 20 đến Monitoring server 2 đặt trên cổng F0/12 của SW2.
- VLAN 30 được tạo thêm để hoàn thành yêu cầu này.

Thực hiện:

1. Cấu hình trunking:

Trên SW1 và SW2:

```
SW1-2(config)#interface f0/24
SW1-2(config-if)#switchport trunk encapsulation dot1q
SW1-2(config-if)#switchport mode trunk
SW1-2(config-if)#switchport nonegotiate
SW1-2(config-if)#exit
```

2. Cấu hình VTP và VLAN:

Cấu hình VTP:

```
SW1(config)#vtp domain waren
SW1(config)#vtp password cisco

SW2(config)#vtp domain waren
SW2(config)#vtp password cisco
SW2(config)#vtp mode client
```

Tạo VLAN trên SW1:

```
SW1(config)#vlan 10
SW1(config-vlan)#exit

SW1(config)#vlan 20
SW1(config-vlan)#exit
```

Gán cổng vào các VLAN vừa tạo theo yêu cầu:

```
SW1(config)#interface f0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 10
SW1(config-if)#exit

SW1(config)#interface f0/2
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 20
SW1(config-if)#exit
```

3. Định tuyến VLAN trên router:

Trên SW2:

```
SW2(config)#interface f0/1
SW2(config-if)#switchport trunk encapsulation dot1q
SW2(config-if)#switchport mode trunk
SW2(config-if)#switchport nonegotiate
SW2(config-if)#exit
```

Trên R:

```
R(config)#interface f0/0
R(config-if)#no shutdown
R(config-if)#exit

R(config)#interface f0/0.10
R(config-subif)#encapsulation dot1Q 10
R(config-subif)#ip address 192.168.10.1 255.255.255.0
R(config-subif)#exit

R(config)#interface f0/0.20
R(config-subif)#encapsulation dot1Q 20
R(config-subif)#ip address 192.168.20.1 255.255.255.0
R(config-subif)#exit
```

4. SPAN:

- Cấu hình tính năng SPAN để SW1 thực hiện sao lưu tất cả dữ liệu ra/vào cổng F0/1 đến Monitoring server 1 đặt trên cổng F0/12.

Ghi chú:

Tính năng SPAN (Switchport Analyzer) được sử dụng để sao lưu dữ liệu đang trao đổi trên một cổng hoặc một VLAN của một switch đến một cổng khác trên cùng switch ấy nhằm mục đích phân tích dữ liệu này. Thiết bị phân tích gắn trên cổng khác ấy có thể là một thiết bị bắt gói (packet sniffer) hoặc một IPS (Instrusion Prevention Sensor),.v.v…

Để cấu hình SPAN, chúng ta cần làm hai thao tác:

- Thao tác đầu tiên là chỉ ra cổng hoặc VLAN mà ta muốn theo dõi dữ liệu:

  Switch(config)#monitor *session-id* **source {vlan** *vlan-list* **| interface** *tên_cổng***} [tx | rx | both]**

  Trong đó:
  - *session-id:* là số hiệu của hoạt động monitor của chúng ta. Tùy theo dòng switch được sử dụng mà ta có thể khai báo được bao nhiêu monitor sesstion.
  - VLAN hay cổng cần theo dõi dữ liệu được chỉ ra trong phần khai báo "`source vlan`" hay "`source interface`" của câu lệnh.
  - Trên VLAN hoặc interface được theo dõi, ta có thể giám sát dữ liệu đi ra (`tx`), đi vào (`rx`) hoặc cả hai chiều (`both`).

- Thao tác tiếp theo là chỉ ra cổng đích đến mà ta có gắn thiết bị phân tích:

```
Switch(config)#monitor session-id destination interface tên_cổng [ingress vlan vlan-id]
```

Ta chỉ ra cổng mà monitor session sẽ phải gửi dữ liệu đến đó để giám sát và phân tích trong phần khai báo "**destination interface**" của câu lệnh. Mặc định, khi một cổng trở thành monitor port, switch sẽ drop bỏ mọi lưu lượng đi vào cổng đó và như vậy host thực hiện nhiệm vụ bắt gói và giám sát trên cổng monitor sẽ không thể gửi dữ liệu đi đâu được nữa. Ta có thể thay đổi ứng xử mặc định này bằng cách khai báo thêm tham số "**ingress vlan** *vlan-id*" cho cổng. Với tham số này được khai báo, host giám sát có thể gửi được lưu lượng vào switch và lưu lượng này sẽ được đưa vào VLAN *vlan-id* đã chỉ ra trong câu lệnh.

Cấu hình:

Trên SW1:

```
SW1(config)#monitor session 1 source interface f0/1 both
SW1(config)#monitor session 1 destination interface f0/12
```

Kiểm tra:

Kiểm tra cấu hình đã thực hiện trên SW1:

```
SW1#sh monitor session 1
Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Fa0/1
Destination Ports      : Fa0/12
    Encapsulation      : Native
          Ingress      : Disabled
```

Cổng F0/12 của SW1 hiện đã trở thành monitoring port và không còn có thể sử dụng cho hoạt động truyền dữ liệu thông thường:

```
SW1#show ip interface brief f0/12
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/12       unassigned      YES unset  up                    down

SW1#show interface f0/12 status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/12                       monitoring   1          a-full  a-100 10/100BaseTX
```

Để kiểm tra hoạt động capture dữ liệu, thực hiện telnet từ PC1 đến router R. Toàn bộ dữ liệu telnet giữa PC1 và router sẽ được bắt gói trên monitoring server. Có thể sử dụng phần mềm Wireshark trên server để kiểm chứng điều này.

5. RSPAN:

Ghi chú:

- Nếu tính năng SPAN đã trình bày ở mục trước chỉ cho phép đặt host monitor lên một cổng thuộc về cùng switch với các thành phần bị giám sát bị giám sát (VLAN hoặc port) thì tính năng RSPAN cho phép host giám sát được đặt trên một switch khác với switch có các thành phần bị giám sát từ đó mở rộng phạm vi giám sát mạng và tập trung việc giám sát về một điểm cố định trong hệ thống mạng.
- Để cấu hình tính năng RSPAN, chúng ta thực hiện các bước như sau:
  - Cấu hình tạo một VLAN để chuyên chở thông tin được sao lưu từ các thành phần bị giám sát đi đến switch đích đến có gắn thiết bị giám sát. Vì VLAN này là đường trung chuyển thông tin nên nó cần phải được tạo ra trên tất cả các switch nằm trên đường đi từ nơi bị giám sát đến nơi đặt thiết bị giám sát.
    Ta thực hiện cấu hình VLAN này trên các switch bằng cách sử dụng lệnh tạo VLAN như thông thường và khai báo thêm tính chất RSPAN cho VLAN mới tạo bằng lệnh "`remote-span`".

    ```
    Switch(config)#vlan vlan-id
    Switch(config-vlan)#remote-span
    ```

    Ta không sử dụng VLAN này cho các mục đích truyền dữ liệu thông thường. Mọi cổng access được gán vào VLAN RSPAN sẽ bị disable và chuyển sang trạng thái down/down.
  - Trên các switch chứa các thành phần bị giám sát (source switch), chúng ta khai báo các monitor session. Việc khai báo source của các monitor session hoàn toàn giống như với tính năng SPAN đã thực hiện ở mục trước. Với khai báo destination, chúng ta sử dụng destination là remote VLAN chứ không phải interface như với SPAN:

    ```
    Switch(config)#monitor session session-id destination remote vlan vlan-id
    ```

  - Cuối cùng, trên switch đích đến có gắn sensor, chúng ta cấu hình RSPAN với source chính là RSPAN VLAN và destination là interface có gắn thiết bị Sensor.

    ```
    Switch(config)#monitor session session-id source remote vlan vlan-id
    Switch(config)#monitor session session-id destination interface Tên_cổng
    [ingress vlan vlan-id]
    ```

    Giống như với SPAN, tham số "`ingress vlan`" cho phép thiết bị sensor có thể gửi dữ liệu vào cổng và dữ liệu này được chuyển đến VLAN *vlan-id*.

Cấu hình:

Trên SW1 tạo VLAN 30 và thiết lập VLAN này trở thành RSPAN VLAN:

```
SW1(config)#vlan 30
SW1(config-vlan)#remote-span
SW1(config-vlan)#exit
```

Vì hệ thống switch trong bài lab đang chạy VTP nên cấu hình RSPAN VLAN trên SW1 sẽ được tự động lan truyền qua SW2:

```
SW2#show vlan br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
```

```
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Gi0/1, Gi0/2
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active

SW2#show vlan remote-span

Remote SPAN VLANs
------------------------------------------------------------------------------
30
```

Trên SW1 cấu hình monitor session thứ hai để thực hiện bắt gói lưu lượng đi qua VLAN 20 và gửi dữ liệu bắt gói vào VLAN 30 để đi qua SW2:

```
SW1(config)#monitor session 2 source vlan 20 both
SW1(config)#monitor session 2 destination remote vlan 30
```

Trên SW2 cấu hình một monitor session để chuyển dữ liệu bắt gói nhận được từ VLAN 30 đến interface F0/12 nối đến monitoring server:

```
SW2(config)#monitor session 1 source remote vlan 30
SW2(config)#monitor session 1 destination interface f0/12
```

Kiểm tra:

Kiểm tra cấu hình đã thực hiện trên SW1 và SW2:

```
SW1#show monitor session 2
Session 2
---------
Type                   : Remote Source Session
Source VLANs           :
    Both               : 20
Dest RSPAN VLAN        : 30

SW2#show monitor session 1
Session 1
---------
Type                   : Remote Destination Session
Source RSPAN VLAN      : 30
Destination Ports      : Fa0/12
    Encapsulation      : Native
          Ingress      : Disabled
```

Tương tự như ở bước 4, có thể thực hiện telnet từ PC2 đến router R và sử dụng chương trình bắt gói trên monitoring server 2 để kiểm tra kết quả cấu hình RSPAN đã thực hiện.