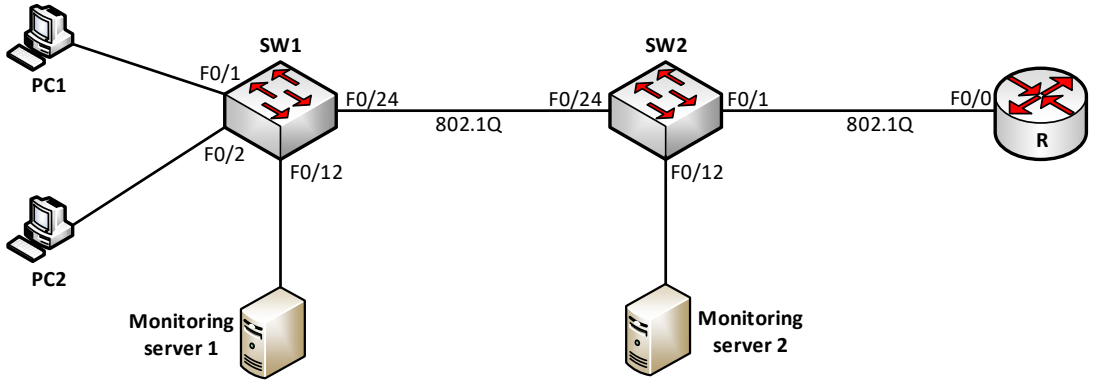
Lab – SPAN và RSPAN

Sơ đồ:



Hình 1 – Sơ đồ bài Lab

Mô tả:

- Bài Lab gồm các Router 2811, các Switch 3560 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. Bài lab này có thể được thực hiện trên LAB giả lập sử dụng các IOL Router L3-ADVENTERPRISEK9-M-15.4-2T, Qemu Switch: viosl2-adventerprisek9-m.SSA.high_iron và các Qemu Windows: win-7-x86-IPCC.
- Trong bài Lab, học viên sẽ thực hành 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.

Cấu hình:

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
```

Kiểm tra:

Kiểm tra đường trunk theo yêu cầu đã được thiết lập giữa hai Switch:

```
SW1#show interfaces trunk
Port        Mode             Encapsulation  Status        Native vlan
Fa0/24      on               802.1q         trunking      1
(…)
```

```
SW2#show interfaces trunk
Port        Mode             Encapsulation  Status        Native vlan
Fa0/24      on               802.1q         trunking      1
(…)
```

2. Cấu hình VTP và VLAN

- Thực hiện cấu hình VTP trên hai Switch theo yêu cầu sau:
  - VTP domain: vnpro, 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.

Cấu hình:

Cấu hình VTP:

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

SW2(config)#vtp domain vnpro
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
```

Kiểm tra:

VTP đã được thiết lập theo yêu cầu:

```
SW1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : vnpro
VTP Pruning Mode                : Disabled
```

```
VTP Traps Generation            : Disabled
Device ID                       : 0011.936a.2580
Configuration last modified by 0.0.0.0 at 3-1-93 01:13:19
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 7
Configuration Revision          : 2
MD5 digest                      : 0xFC 0xD0 0x8C 0x33 0x8D 0xD9 0xE3 0x65
                                  0x76 0x47 0x44 0x10 0xFE 0x67 0xCB 0xE5
SW1#show vtp password
VTP Password: cisco

SW2#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : vnpro
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 001c.b1c5.ce80
Configuration last modified by 0.0.0.0 at 3-1-93 01:13:19

Feature VLAN:
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 7
Configuration Revision          : 2
MD5 digest                      : 0xFC 0xD0 0x8C 0x33 0x8D 0xD9 0xE3 0x65
                                  0x76 0x47 0x44 0x10 0xFE 0x67 0xCB 0xE5
SW2#show vtp password
VTP Password: cisco
```

Cấu hình VLAN đã được đồng nhất giữa hai Switch:

```
SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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    Fa0/1
20   VLAN0020                         active    Fa0/2
1002 fddi-default                     act/unsup
```

```
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

```
SW2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, 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
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Kết quả show cũng cho thấy các cổng trên SW1 đã được gán vào các VLAN đúng theo yêu cầu.

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:

Bảng 1 – Thông tin định tuyến VLAN

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

Cấu hình:

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/IDS (Instrusion Prevention Sensor/Instrution Detection Sensor),.v.v…

Để cấu hình SPAN, các bước sau cần được thực hiện:

- Khai báo cổng hoặc VLAN cần phải capture dữ liệu:

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

  Trong đó:
  - *session-id:* Số hiệu của hoạt động monitor. Số lượng monitor session thay đổi tùy theo dòng Switch được sử dụng.
  - "`source vlan`" hay "`source interface`": VLAN hay cổng cần capture dữ liệu của câu lệnh.
  - VLAN hoặc interface được theo dõi, có thể capture dữ liệu đi ra (`tx`), đi vào (`rx`) hoặc cả hai chiều (`both`).
- Khai báo cổng đích đến có gắn thiết bị phân tích:

  Switch(config)#monitor *session-id* **destination interface** *tên_cổng*

  Mặc định, khi một cổng trở thành monitor port, Switch sẽ drop bỏ mọi lưu lượng đi vào cổng đó và như vậy thiết bị thực hiện nhiệm vụ bắt gói và giám sát trên cổng monitor sẽ không thể truy nhập mạng.

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:

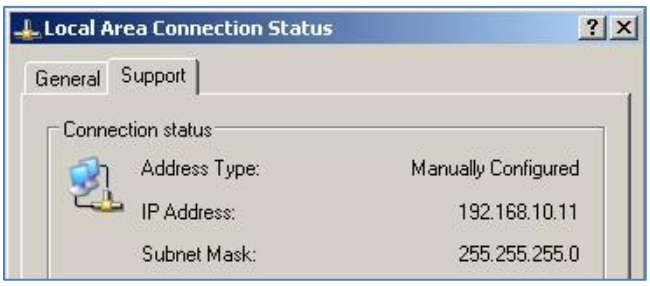
```
SW1#show ip interface brief f0/12
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/12       unassigned      YES unset  up                    down

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. Thực hiện:

Đặt IP trên PC1 thuộc dải IP của VLAN 10 (cổng F0/1 được gán vào VLAN 10):



Hình 2 – IP trên PC1

Cấu hình telnet trên Router R, sử dụng password telnet là "vnpro", password enable là "cisco":

```
R(config)#line vty 0 4
R(config-line)#password vnpro
R(config-line)#login
R(config-line)#exit

R(config)#enable password cisco
```

Từ PC1 thực hiện telnet đến Router R và thực hiện một vài thao tác trên cửa sổ telnet:

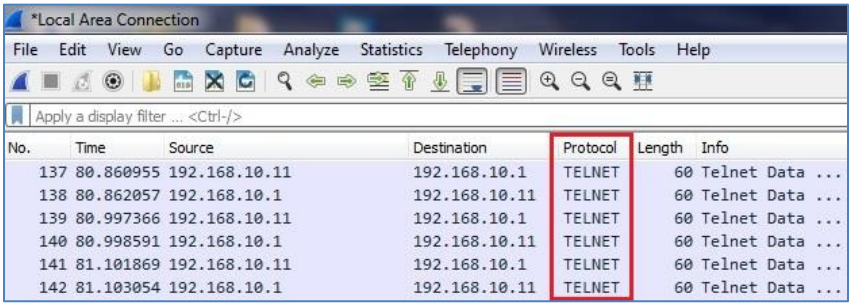
```
C:\>telnet 192.168.10.1 <- Telnet đến địa chỉ của router R

User Access Verification

Password: <- Nhập password là "vnpro"
R>enable
```

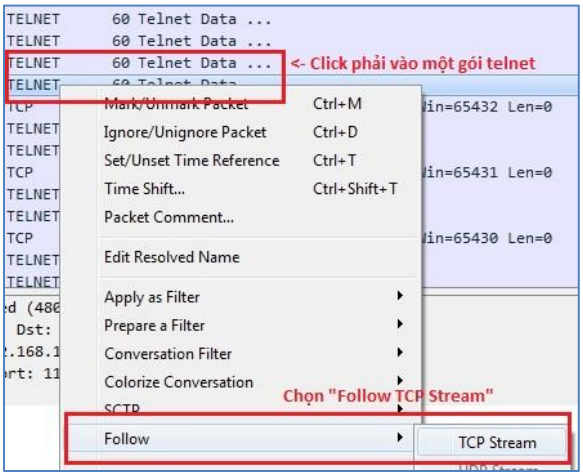
```
Password: <- Nhập password là "cisco"
R#
R#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES NVRAM  up                    up
FastEthernet0/0.10         192.168.10.1    YES NVRAM  up                    up
FastEthernet0/0.20         192.168.20.1    YES NVRAM  up                    up
FastEthernet0/1            unassigned      YES NVRAM  administratively down down
Serial0/0/0                unassigned      YES NVRAM  administratively down down
```

Chương trình bắt gói Wireshark trên monitoring Server đã bắt được dữ liệu telnet trao đổi giữa PC1 và Router R (hình 3):



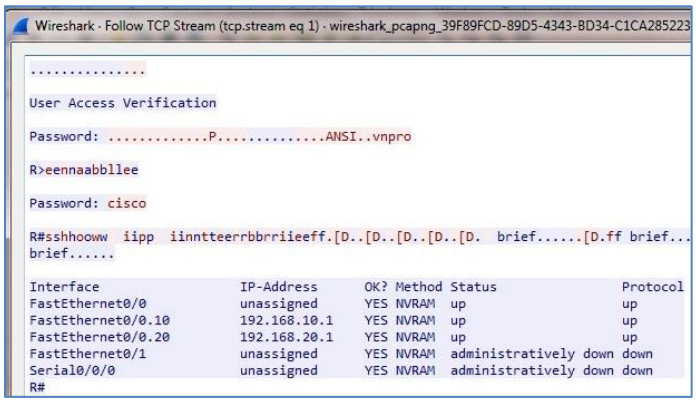
Hình 3 – Kết quả bắt gói bằng Wireshark trên Server

Có thể click phải vào một gói telnet bất kỳ và chọn tùy chọn "Follow TCP Stream" để phân tích dữ liệu telnet bắt được (hình 4):



Hình 4 – Follow TCP Stream

Kết quả phân tích thu được (hình 5):



Hình 5 – Kết quả phân tích dữ liệu Telnet

Như vậy, với tính năng SPAN, người quản trị có thể bắt gói để phân tích lưu lượng đi qua một Switch.

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.

Ghi chú:

Tính năng SPAN chỉ cho phép đặt thiết bị monitor lên một cổng thuộc về cùng Switch với các thành phần bị giám sát (VLAN hoặc port). Để có thể đặt thiết bị giám sát trên một Switch khác cần phải sử dụng tính năng *RSPAN (Remote SPAN)*.

Các bước cấu hình tính năng RSPAN:

- Tạo một VLAN để chuyên chở dữ liệu capture từ các thành phần bị giám sát 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. Cấu hình:

```
Switch(config)#vlan vlan-id
Switch(config-vlan)#remote-span <- Khai báo VLAN này dùng cho RSPAN
```

  VLAN RSPAN này sẽ không còn sử dụng được cho mục đích truyền dữ liệu thông thường nữa. 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 (trong bài Lab này là SW1), thực hiện 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 trên. Với khai báo destination, thực thể được khai báo là remote VLAN chứ không phải interface:

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

- Cuối cùng, trên Switch đích đến có gắn thiết bị giám sát, thực hiện cấu hình monitor session với source là RSPAN VLAN và destination là interface có gắn thiết bị giám sát:

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

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 yêu cầu 5, 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.