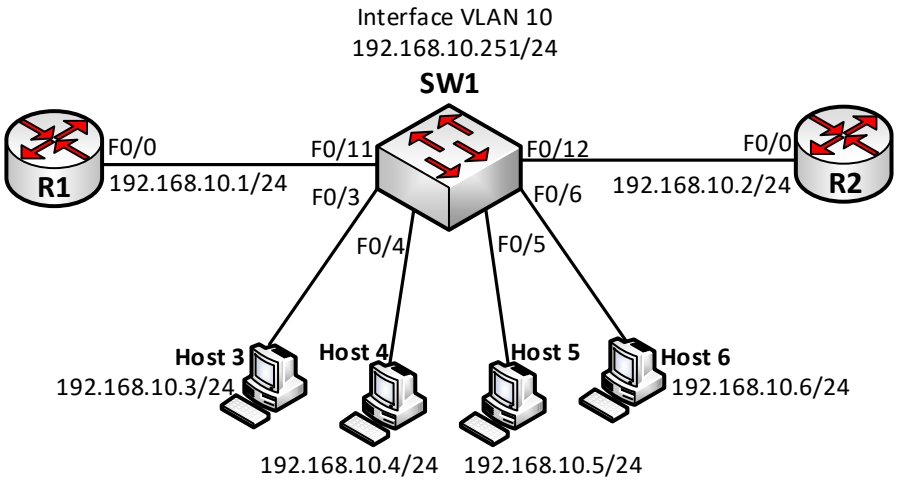
# Lab 1 – Security trên Switch

**Sơ đồ:**




*Hình 1 – Sơ đồ bài Lab*

**Mô tả:**

Bài lab gồm 2 Router 2811, 1 Switch 2960 và các PC được đấu nối với nhau như hình. Bài Lab này có thể được dựng trên lab ảo hoá sử dụng các IOL Router L3-ADVENTERPRISEK9-M-15.4-2T, IOL Switch i86bi_linux_l2-advipservicesk9, các vPC.

Trong bài lab này học viên thực hiện một số tính năng security trên switch.

**Yêu cầu:**

**1. Cấu hình ban đầu**

- Trên SW1 thực hiện tạo VLAN 10 và gán tất cả các cổng Fast Ethernet trên Switch vào VLAN 10.
- Thực hiện cấu hình địa chỉ IP trên các interface của các thiết bị theo quy hoạch IP được chỉ ra trên hình 1.

***Cấu hình:***

Trên SW1:

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

SW1(config)#interface range f0/1 - 24
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#exit

SW1(config)#interface vlan 10
SW1(config-if)#ip address 192.168.10.251 255.255.255.0
SW1(config-if)#exit
```

Trên R1:

```
R1(config)#interface f0/0
R1(config-if)#no shutdown
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#exit
```

Trên R2:

```
R2(config)#interface f0/0
R2(config-if)#no shutdown
R2(config-if)#ip address 192.168.10.2 255.255.255.0
R2(config-if)#exit
```

***Kiểm tra:***

Trên SW1 VLAN 10 đã được tạo ra và các cổng Fast Ethernet đều đã được gán vào VLAN 10 (bài Lab được thực hiện trên Switch 3560 có 24 cổng Fast Ethernet):

```
SW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/1, Gi0/2
10   VLAN0010                         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, Fa0/24
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Interface VLAN 10 của SW1 đã active (up/up):

```
SW1#show ip interface brief vlan 10
Interface              IP-Address      OK? Method Status                Protocol
Vlan10                 192.168.10.251  YES manual up                    up
```

Các địa chỉ IP của các Host trên VLAN 10 đã có thể đi đến nhau được:

```
R1#ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#ping 192.168.10.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.251, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R2#ping 192.168.10.251
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.251, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

**2. VLAN Access – List (VACL)**

Sử dụng VACL trên VLAN 10 để thực hiện chính sách như sau:

- Giả thiết R1 là một web Server dành riêng. Thực hiện cấm mọi hoạt động truy nhập web đến Server R1, ngoại trừ các hoạt động truy nhập web xuất phát từ địa chỉ 192.168.10.2.
- Cấm mọi session telnet đến R2, ngoại trừ các session telnet đến từ địa chỉ 192.168.10.1 của R1.
- R1 và R2 không được phép chạy định tuyến bằng giao thức OSPF qua VLAN 10.
- R1 có thể ping được R2 nhưng R2 không thể ping được R1.
- Mọi hoạt động trao đổi dữ liệu khác qua VLAN 10 không bị ảnh hưởng bởi VACL đã xây dựng.

***Cấu hình:***

Cấu hình một access – list với tên gọi "WEB_TO_R1" đề cập đến ("permit") mọi lưu lượng web đi đến Server 192.168.10.1 và thực hiện loại trừ ra ("deny") lưu lượng web xuất phát từ địa chỉ 192.168.10.2:

```
SW1(config)#ip access-list extended WEB_TO_R1
SW1(config-ext-nacl)#deny tcp host 192.168.10.2 host 192.168.10.1 eq 80
SW1(config-ext-nacl)#permit tcp any host 192.168.10.1 eq 80
SW1(config-ext-nacl)#exit
```

Các lưu lượng được permit trong access – list vừa tạo sẽ được áp hành động "drop" trong VLAN Access – map:

```
SW1(config)#vlan access-map VLAN10
SW1(config-access-map)#match ip address WEB_TO_R1
SW1(config-access-map)#action drop
SW1(config-access-map)#exit
```

Tiếp theo, viết một access – list có tên gọi "TELNET_TO_R2" đề cập đến ("permit") mọi lưu lượng telnet đi đến địa chỉ 192.168.10.2 của R2 và thực hiện loại trừ ra ("deny") lưu lượng telnet xuất phát từ địa chỉ 192.168.10.1 của R1:

```
SW1(config)#ip access-list extended TELNET_TO_R2
SW1(config-ext-nacl)#deny tcp host 192.168.10.1 host 192.168.10.2 eq 23
SW1(config-ext-nacl)#permit tcp any host 192.168.10.2 eq 23
SW1(config-ext-nacl)#exit
```

Các lưu lượng được permit trong access – list vừa tạo sẽ được áp hành động "drop" trong VLAN Access – map:

```
SW1(config)#vlan access-map VLAN10 20
SW1(config-access-map)#match ip address TELNET_TO_R2
SW1(config-access-map)#action drop
SW1(config-access-map)#exit
```

Tiếp theo, viết một access – list đề cập đến ("permit") hoạt động định tuyến OSPF giữa R1 và R2:

```
SW1(config)#ip access-list extended OSPF_R1_R2
SW1(config-ext-nacl)#permit 89 any any <- Protocol - ID của OSPF là 89
SW1(config-ext-nacl)#exit
```

Lưu lượng OSPF được đề cập đến (permit) trong access – list vừa tạo sẽ được áp hành động drop trong VLAN Access – map:

```
SW1(config)#vlan access-map VLAN10 30
SW1(config-access-map)#match ip address OSPF_R1_R2
SW1(config-access-map)#action drop
SW1(config-access-map)#exit
```

Tiếp theo, viết một access – list permit các gói ICMP Echo Request phát đi từ R2 đến R1 và áp hành động drop với các gói này trong VLAN Access – map:

```
SW1(config)#ip access-list extended ICMP_R2_TO_R1
SW1(config-ext-nacl)#permit icmp host 192.168.10.2 host 192.168.10.1 echo
SW1(config-ext-nacl)#exit

SW1(config)#vlan access-map VLAN10 40
SW1(config-access-map)#match ip address ICMP_R2_TO_R1
SW1(config-access-map)#action drop
SW1(config-access-map)#exit
```

Tiếp theo, viết một entry dưới cùng của VLAN Access – map thực hiện hành động forward cho mọi lưu lượng còn lại:

```
SW1(config)#vlan access-map VLAN10 50
SW1(config-access-map)#action forward
SW1(config-access-map)#exit
```

Cuối cùng, áp VLAN Access – map vừa xây dựng lên VLAN 10:

```
SW1(config)#vlan filter VLAN10 vlan-list 10
```

***Kiểm tra:***

Kiểm tra lại VLAN Access – map vừa tạo:

```
SW1#show vlan access-map VLAN10
Vlan access-map "VLAN10"  10
  Match clauses:
    ip  address: WEB_TO_R1
```

```
  Action:
    drop
Vlan access-map "VLAN10"  20
  Match clauses:
    ip  address: TELNET_TO_R2
  Action:
    drop
Vlan access-map "VLAN10"  30
  Match clauses:
    ip  address: OSPF_R1_R2
  Action:
    drop
Vlan access-map "VLAN10"  40
  Match clauses:
    ip  address: ICMP_R2_TO_R1
  Action:
    drop
Vlan access-map "VLAN10"  50
  Match clauses:
  Action:
    forward

SW1#show vlan filter
VLAN Map VLAN10 is filtering VLANs:
  10
```

Trước hết kiểm tra kết quả thực hiện với lưu lượng web.

Thực hiện bật HTTP Server trên R1 để giả lập R1 là một Web Server:

```
R1(config)#ip http server
```

R2 có thể truy nhập web đến R1:

```
R2#telnet 192.168.10.1 80
Trying 192.168.10.1, 80 ... Open <- Truy nhập thành công
hhh
HTTP/1.1 400 Bad Request
Date: Thu, 19 May 2016 10:18:29 GMT
Server: cisco-IOS
Accept-Ranges: none

400 Bad Request
[Connection to 192.168.10.1 closed by foreign host]
R2#
```

Thực hiện đổi lại địa chỉ IP trên R2:

```
R2(config)#interface f0/0
R2(config-if)#ip address 192.168.10.22 255.255.255.0
R2(config-if)#exit
```

Lúc này, hoạt động truy nhập Web đến R1 không còn thành công nữa:

```
R2#telnet 192.168.10.1 80
Trying 192.168.10.1, 80 ...
% Connection timed out; remote host not responding
```

Sau khi thực hiện kiểm tra xong, trả lại IP trên R2 lại như cũ:

```
R2(config)#interface f0/0
R2(config-if)#ip address 192.168.10.2 255.255.255.0
R2(config-if)#exit
```

Tiếp theo, thực hiện kiểm tra với hoạt động Telnet qua VLAN 10.

Thực hiện cấu hình telnet trên Router R2:

```
R2(config)#line vty 0 4
R2(config-line)#password vnpro
R2(config-line)#login
R2(config-line)#exit
```

Từ địa chỉ 192.168.10.1 của R1 có thể thực hiện telnet đến R2:

```
R1#telnet 192.168.10.2
Trying 192.168.10.2 ... Open


User Access Verification

Password:
R2>
```

Thực hiện đổi lại địa chỉ IP trên R1 thành một địa chỉ không được phép telnet đến R2:

```
R1(config)#interface f0/0
R1(config-if)#ip address 192.168.10.11 255.255.255.0
R1(config-if)#exit
```

Lúc này, R1 không thể telnet R2 được nữa:

```
R1#telnet 192.168.10.2
Trying 192.168.10.2 ...
% Connection timed out; remote host not responding
```

Sau khi kiểm tra xong, thực hiện trả lại IP cho R1 như cũ:

```
R1(config)#interface f0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#exit
```

Tiếp theo, thực hiện kiểm tra với giao thức định tuyến.

Thực hiện bật định tuyến EIGRP trên cổng F0/0 của R1 và R2:

```
R1(config)#router eigrp 100
```

```
R1(config-router)#no auto-summary
R1(config-router)#network 192.168.10.0
R1(config-router)#exit

R2(config)#router eigrp 100
R2(config-router)#no auto-summary
R2(config-router)#network 192.168.10.0
R2(config-router)#exit
```

Hai Router chạy định tuyến EIGRP thành công qua VLAN 10 và thiết lập được quan hệ láng giềng với nhau:

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.10.2            Fa0/0             12 00:00:38  237  1422  0  3

R2#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
0   192.168.10.1            Fa0/0             11 00:00:49  346  2076  0  3
```

Gỡ bỏ EIGRP và thực hiện chạy định tuyến OSPF trên hai Router:

```
R1(config)#no router eigrp 100
R1(config)#router ospf 1
R1(config-router)#network 192.168.10.1 0.0.0.0 area 0
R1(config-router)#exit

R2(config)#no router eigrp 100
R2(config)#router ospf 1
R2(config-router)#network 192.168.10.2 0.0.0.0 area 0
R2(config-router)#exit
```

OSPF đã bị chặn trên VLAN 10 nên hai Router không thể thiết lập quan hệ láng giềng OSPF với nhau:

```
R1#show ip ospf neighbor

R2#show ip ospf neighbor
```

Cuối cùng, thực hiện kiểm tra R1 có thể ping được R2 nhưng R2 không thể ping được R1:

```
R1#ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R2#ping 192.168.10.1
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

### 3. Protected port

- Sử dụng tính năng protected port đảm bảo Host 3 và Host 4 không thể trao đổi được dữ liệu với nhau nhưng hai Host này vẫn có thể đi đến được các thiết bị khác.

***Cấu hình:***

Thực hiện cấu hình tính năng protected port trên các cổng F0/2 và F0/3 kết nối đến các Host 2 và Host 3:

```
SW1(config)#interface range f0/3,f0/4
SW1(config-if-range)#switchport protected
SW1(config-if-range)#exit
```

Nhắc lại rằng các cổng được bật chế độ protected sẽ không thể trao đổi được dữ liệu với nhau nhưng vẫn có thể trao đổi dữ liệu với các cổng không bật chế độ này. Mặc định chế độ này được tắt trên các cổng.

Tính năng này giúp người quản trị giới hạn việc trao đổi dữ liệu giữa các cổng thuộc cùng VLAN *trên nội bộ một Switch*. Nếu muốn giới hạn việc trao đổi giữa các cổng thuộc cùng một VLAN nhưng được đặt trên nhiều Switch, cần phải sử dụng kỹ thuật Private VLAN.

***Kiểm tra:***

Kiểm tra Host 3 không thể đi đến được Host 4:

```
C:\>ping 192.168.10.4
Pinging 192.168.10.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

(Các Host 3, 4, 5,6 có thể là các PC chạy hệ điều hành Window được kết nối vào các cổng tương ứng trên Switch để thực hiện kiểm tra Lab).

Tuy nhiên, Host 3 vẫn có thể đi đến được các Host nằm trên các cổng khác của Switch:

```
C:\>ping 192.168.10.1
Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=2ms TTL=255
Reply from 192.168.10.2: bytes=32 time=1ms TTL=255
Reply from 192.168.10.2: bytes=32 time=1ms TTL=255
Reply from 192.168.10.2: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

## 4. Private VLAN

- Gỡ bỏ cấu hình protected port đã thực hiện ở yêu cầu 3.
- Sử dụng tính năng Private VLAN trên SW1 thực hiện chính sách như sau:
  - Các Host 3 và Host 4 không được phép trao đổi dữ liệu với các Host 5 và Host 6.
  - Host 5 và Host 6 vẫn có thể trao đổi được dữ liệu với nhau; Host 3 và Host 4 không thể trao đổi được dữ liệu với nhau.
  - Tất cả các Host 3, 4, 5, 6 đều có thể đi đến được các Router cũng như đi đến được IP trên interface VLAN 10 của SW1.

***Cấu hình:***

Gỡ bỏ cấu hình protected port trên các cổng F0/3 và F0/4 đã thực hiện:

```
SW1(config)#interface range f0/3,f0/4
SW1(config-if-range)#no switchport protected
SW1(config-if-range)#exit
```

Thực hiện cấu hình Private VLAN trên SW1 để đáp ứng các yêu cầu đặt ra theo các bước dưới đây.

Trước hết, cần chuyển SW1 sang hoạt động ở mode Transparent vì Private VLAN chỉ được hỗ trợ trên Transparent Switch:

```
SW1(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
```

Tạo ra VLAN 34 là một secondary VLAN. VLAN này sẽ được sử dụng để kết nối các Host 3 và 4. Căn cứ yêu cầu đặt ra, VLAN 34 sẽ là một Isolated VLAN:

```
SW1(config)#vlan 34
SW1(config-vlan)#private-vlan isolated
SW1(config-vlan)#exit
```

Tiếp theo, thực hiện tạo VLAN 56, là một secondary VLAN dành cho các Host 5 và 6. Căn cứ theo yêu cầu, VLAN 56 là một community VLAN:

```
SW1(config)#vlan 56
SW1(config-vlan)#private-vlan community
SW1(config-vlan)#exit
```

VLAN 10 được khai báo thành Primary VLAN hỗ trợ hai secondary VLAN vừa cấu hình:

```
SW1(config)#vlan 10
SW1(config-vlan)#private-vlan primary
SW1(config-vlan)#private-vlan association 34,56
SW1(config-vlan)#exit
```

Tiếp theo, thực hiện khai báo các cổng kết nối đến các Host 3, 4, 5, 6 thành các Host port và gán chúng vào các Secondary VLAN tương ứng:

```
SW1(config)#interface range f0/3,f0/4
SW1(config-if-range)#switchport mode private-vlan host
SW1(config-if-range)#switchport private-vlan host-association 10 34
SW1(config-if-range)#exit

SW1(config)#interface range f0/5,f0/6
SW1(config-if-range)#switchport mode private-vlan host
SW1(config-if-range)#switchport private-vlan host-association 10 56
SW1(config-if-range)#exit
```

Tiếp tục khai báo promiscuous port trên SW1. Cần chú ý thêm thao tác khai báo cho interface VLAN của Primary VLAN:

```
SW1(config)#interface range f0/11,f0/12
SW1(config-if-range)#switchport mode private-vlan promiscuous
SW1(config-if-range)#switchport private-vlan mapping 10 34,56
SW1(config-if-range)#exit

SW1(config)#ip routing

SW1(config)#interface vlan 10
SW1(config-if)#private-vlan mapping 34,56
SW1(config-if)#exit
```

Đến đây, cấu hình Private VLAN theo yêu cầu đặt ra đã hoàn tất.

***Kiểm tra:***

Thực hiện kiểm tra cấu hình Private VLAN đã thực hiện:

```
SW1#show vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ----------------------------------------
10      34        isolated          Fa0/3, Fa0/4, Fa0/11, Fa0/12
10      56        community         Fa0/5, Fa0/6, Fa0/11, Fa0/12
```

Kết quả show cho thấy các Private VLAN đã được cấu hình đúng như yêu cầu.

Tiếp tục kiểm tra chính sách trao đổi dữ liệu giữa các Host đã được thiết lập đúng đắn.

Host 3 không đi đến được Host 4:

```
C:\>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:
Reply from 192.168.10.3: Destination host unreachable.
Reply from 192.168.10.3: Destination host unreachable.
Reply from 192.168.10.3: Destination host unreachable.
Reply from 192.168.10.3: Destination host unreachable.
Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Host 3 không đi đến được các Host 5 và Host 6:

```
C:\>ping 192.168.10.5
Pinging 192.168.10.5 with 32 bytes of data:
Reply from 192.168.10.3: Destination host unreachable.
Reply from 192.168.10.3: Destination host unreachable.
Reply from 192.168.10.3: Destination host unreachable.
Reply from 192.168.10.3: Destination host unreachable.

Ping statistics for 192.168.10.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\>ping 192.168.10.6
Pinging 192.168.10.6 with 32 bytes of data:
Reply from 192.168.10.3: Destination host unreachable.
Reply from 192.168.10.3: Destination host unreachable.
Reply from 192.168.10.3: Destination host unreachable.
Reply from 192.168.10.3: Destination host unreachable.

Ping statistics for 192.168.10.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Host 3 có thể đi đến được các Router R1, R2 và interface VLAN 10 của SW1:

```
C:\>ping 192.168.10.1
Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Reply from 192.168.10.1: bytes=32 time=1ms TTL=255
Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=1ms TTL=255
Reply from 192.168.10.2: bytes=32 time=1ms TTL=255
Reply from 192.168.10.2: bytes=32 time=1ms TTL=255
Reply from 192.168.10.2: bytes=32 time=1ms TTL=255
```

```
Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 192.168.10.251
Pinging 192.168.10.251 with 32 bytes of data:
Reply from 192.168.10.251: bytes=32 time<1ms TTL=255
Reply from 192.168.10.251: bytes=32 time=1ms TTL=255
Reply from 192.168.10.251: bytes=32 time=1ms TTL=255
Reply from 192.168.10.251: bytes=32 time=2ms TTL=255
Ping statistics for 192.168.10.251:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

Host 5 và Host 6 thuộc cùng một Community VLAN có thể đi đến nhau được. Kết quả ping từ Host 5 đến Host 6:

```
C:\>ping 192.168.10.6

Pinging 192.168.10.6 with 32 bytes of data:
Reply from 192.168.10.6: bytes=32 time<1ms TTL=255
Reply from 192.168.10.6: bytes=32 time=1ms TTL=255
Reply from 192.168.10.6: bytes=32 time=1ms TTL=255
Reply from 192.168.10.6: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.10.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Có thể kiểm tra tương tự rằng Host 5 thuộc community VLAN cũng có thể đi đến được R1, R2 và interface VLAN 10 của SW1.