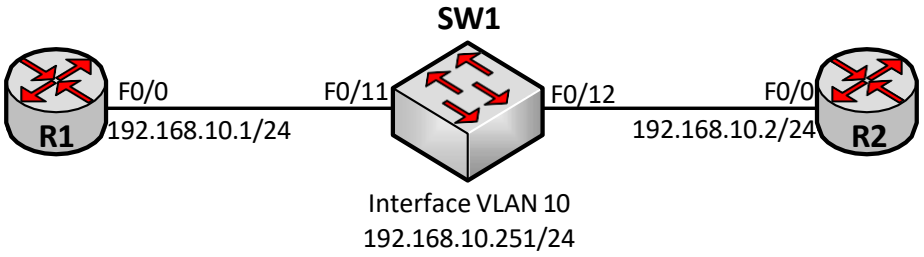
LAB - DHCP SNOOPING, DAI

I. Sơ đồ



Hình 1: Sơ đồ bài Lab

II. Yêu cầu

2.1. Cấu hình ban đầu

- Trên SW1 tạo VLAN 10 và thực hiện gán tất cả các cổng Fast Ethernet của switch vào VLAN 10 vừa tạo.

- Thực hiện cấu hình các địa chỉ IP trên các interface của các thiết bị như 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 upup
```

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
```

2.2. DHCP snooping

- Cấu hình để R1 đóng vai trò DHCP server cấp phát IP cho tất cả các host thuộc VLAN 10 (VLAN 10 được quy hoạch subnet IP 192.168.10.0/24).

- Cấu hình tính năng DHCP snooping trên VLAN 10 của SW1 đảm bảo ngăn chặn tất cả các hoạt động tấn công giả mạo DHCP server diễn ra trên VLAN này.

Cấu hình:

Thực hiện cấu hình R1 thành DHCP server cấp phát IP cho VLAN 10:

```
R1(config)#ip dhcp excluded-address 192.168.10.1
R1(config)#ip dhcp excluded-address 192.168.10.251
```

```
R1(config)#ip dhcp pool VLAN10
R1(dhcp-config)#network 192.168.10.0 /24
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#exit
```

Cấu hình tính năng DHCP snooping cho VLAN 10 trên SW1:

```
SW1(config)#ip dhcp snooping
SW1(config)#ip dhcp snooping vlan 10

SW1(config)#interface f0/11
SW1(config-if)#ip dhcp snooping trust
SW1(config-if)#exit

SW1(config)#no ip dhcp snooping information option
```

Ghi chú:

Cấu hình DHCP snooping đã thực hiện ở trên có thể được giải thích ngắn gọn như sau:

- Tính năng DHCP Snooping được sử dụng để ngăn chặn phương thức tấn công giả mạo DHCP (DHCP Spoofing) trên một VLAN. Với phương thức tấn công này, kẻ tấn công dựng lên một DHCP server giả để rót thông tin IP sai lệch xuống cho người dùng cùng VLAN từ đó gây ảnh hưởng đến việc truy nhập mạng hoặc đánh cắp thông tin từ người dùng. Tính năng này được bật trên một VLAN của một switch bằng các lệnh:

```
SW1(config)#ip dhcp snooping ← Bật DHCP snooping trên SW1
SW1(config)#ip dhcp snooping vlan 10 ← Áp dụng cho VLAN 10
```

- Khi tính năng DHCP snooping được bật trên VLAN, các cổng thuộc VLAN được chia thành hai loại: *trusted port* và *untrusted port*.

+ Trên *trusted port*, thiết bị kết nối được quyền gửi vào port tất cả các loại gói tin DHCP. Các trusted port là các port kết nối đến DHCP server hoặc các port uplink.

+ Trên *untrusted port*, thiết bị chỉ được phép gửi vào port các loại gói tin DHCP do client gửi lên server và không được gửi vào port các loại gói tin mà DHCP server gửi xuống cho client. Các untrusted port được dùng để kết nối đến các end - user trong VLAN. Khi được kết nối vào untrusted port, end - user không thể dựng DHCP server giả vì mọi gói tin cấp phát IP đến từ DHCP server giả mạo của end - user sẽ bị chặn khi đi đến untrusted port.

+ Mặc định, các cổng thuộc VLAN được áp DHCP snooping sẽ hoạt động ở chế độ untrusted. Người quản trị phải chỉ định tường minh các cổng trusted bằng lệnh "`ip dhcp snooping trust`" trên các cổng kết nối đến DHCP server hoặc uplink.

Trong câu lab này, cổng F0/11 kết nối đến DHCP server R1 được chỉ định là trusted port:

```
SW1(config)#interface f0/11
SW1(config-if)#ip dhcp snooping trust
SW1(config-if)#exit
```

Khi tính năng DHCP snooping được bật trên switch, switch tự động thực hiện chèn thêm option - 82 cho các gói tin DHCP đi đến DHCP server.

Option 82 là một loại option được sử dụng để cung cấp thêm thông tin về Agent đến cho DHCP server. Các gói tin DHCP mà có chèn thêm option 82 thường có trường "giaddr" nhận giá trị khác 0 vì trường này được sử dụng để mang theo địa chỉ của DHCP relay agent.

+ Tuy nhiên, trong tình huống sử dụng DHCP snooping, switch thực hiện chèn vào option 82 nhưng nó lại không phải là DHCP relay agent nên trường "giaddr" phải nhận giá trị là 0. Điều này dẫn đến DHCP server sẽ coi gói DHCP nhận được là bị lỗi (xuất hiện option 82 nhưng lại có giaddr = 0) và loại bỏ gói này khiến cho các client sẽ không nhận được cấu hình IP.

+ Để khắc phục vấn đề vừa nêu, khi cấu hình DHCP snooping trên switch, cần phải thực hiện tắt thao tác chèn option 82 hoặc cấu hình DHCP server chấp nhận các gói tin có option 82 nhưng trường giaddr lại bằng 0.

+ Để tắt option 82 với DHCP snooping trên switch, sử dụng lệnh:

```
SW(config)#no ip dhcp snooping information option
```

+ Để DHCP server chấp nhận các gói tin DHCP với option 82 nhưng lại có giaddr = 0, sử dụng lệnh:

```
R(config)#ip dhcp relay information trust-all
```

+ Hoặc câu lệnh ở mode interface:

```
R(config-if)#ip dhcp relay information trusted
```

+ Trong câu lab này, cách tắt option 82 trên switch được lựa chọn để thực hiện:

```
SW1(config)#no ip dhcp snooping information option
```

Kiểm tra:

Thực hiện kiểm tra các thông số của DHCP snooping trên switch:

```
SW1#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
DHCP snooping is operational on following VLANs:
10
Smartlog is configured on following VLANs:
none
Smartlog is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is disabled
   circuit-id default format: vlan-mod-port
   remote-id: a40c.c304.9d00 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface              Trusted    Allow option    Rate limit (pps)
-----------------------    ----------    ------------------------------    ---------------
FastEthernet0/11yes    yes        unlimited
  Custom circuit-ids:
```

Thực hiện chuyển R2 thành một client xin cấp phát IP từ DHCP server R1:

```
R2(config)#interface f0/0
R2(config-if)#no ip address
R2(config-if)#ip address dhcp
R2(config-if)#end
R2#
```

```
*May    13    07:27:30.763:    %DHCP-6-ADDRESS_ASSIGN:    Interface
FastEthernet0/0    assigned    DHCP    address    192.168.10.2,    mask
255.255.255.0, hostname R2
```

Có thể thấy rằng R2 đã được cấp phát động địa chỉ IP 192.168.10.2/24.

Tính năng DHCP snooping bên cạnh chống giả mạo DHCP còn tiến hành theo dõi mọi gói tin DHCP đi ngang qua switch để xây dựng bảng DHCP snooping dùng cho các tính năng DAI và IP sourceguard. Thực hiện kiểm tra bảng DHCP snooping binding trên switch:

```
SW1#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN
Interface
-----------------------    --------------    ----------------------    ----------    ----
00:00:11:11:22:22  192.168.10.2     86382       dhcp-snooping  10
FastEthernet0/12
Total number of bindings: 1
```

Từ kết quả show có thể thấy, switch đã giám sát được hoạt động cấp phát IP bằng DHCP cho các client. Với mỗi client, switch biết được rằng client có địa chỉ MAC là gì, được DHCP server cấp phát cho địa chỉ IP nào và đang được kết nối vào interface nào của VLAN 10. *Ví dụ:* Hiện nay client với MAC 0000.1111.2222 kết nối vào cổng F0/12 thuộc VLAN 10 đã được cấp địa chỉ IP là 192.168.10.2.

Tiếp theo, thực hiện kiểm tra hoạt động chống tấn công giả mạo DHCP server của DHCP snooping bằng cách chuyển cổng F0/11 nối đến R1 thành untrusted port. Lúc này R1 sẽ bị coi là DHCP giả mạo và không thể cấp phát IP cho các end - user thuộc VLAN 10 được nữa.

Chuyển cổng F0/11 thành untrusted port:

```
SW1(config)#interface f0/11
SW1(config-if)#no ip dhcp snooping trust
```

R2 thực hiện xin cấp phát lại IP nhưng không còn xin được IP từ R1:

```
R2(config)#interface f0/0
R2(config-if)#no ip address
R2(config-if)#ip address dhcp
R2(config-if)#end
R2#show ip interface brief f0/0
Interface          IP-Address      OK? Method  Status    Protocol
FastEthernet0/0    unassigned      YES DHCP    up        up
```

Chuyển lại F0/11 thành trusted port, R2 lại nhận được IP cấp phát tự động từ R1:

```
SW1(config)#interface f0/11
SW1(config-if)#ip dhcp snooping trust

R2#
*May    13    07:56:29.207:    %DHCP-6-ADDRESS_ASSIGN:    Interface
FastEthernet0/0   assigned   DHCP   address   192.168.10.2,   mask
255.255.255.0, hostname R2
```

2.3. IP Source - guard

- Cấu hình tính năng IP source guard trên các cổng thuộc VLAN 10 đảm bảo các user kết nối vào các cổng thuộc VLAN 10 phải sử dụng địa chỉ IP được cấp phát bởi DHCP.

- Nếu sử dụng IP cấu hình tĩnh, user sẽ không thể trao đổi dữ liệu.

Cấu hình:

Bật IP source – guard trên tất cả các cổng thuộc VLAN 10 của SW1:

```
SW1(config)#interface range f0/1 - 24
SW1(config-if-range)#ip verify source
```

Kiểm tra:

Hiện nay R2 đang sử dụng IP động 192.168.10.2 được cấp phát bởi DHCP:

```
R2#show ip interface brief f0/0
Interface          IP-Address      OK? Method Status    Protocol
FastEthernet0/0    192.168.10.2    YES DHCP   up        up
```

Điều này được SW1 ghi nhận trong bảng DHCP snooping binding:

```
SW1#show ip dhcp snooping binding
MacAddress          IpAddress       Lease Type           VLAN Interface
                                    (sec)
------------------- --------------- ---------- ------------- ---- --------------------
00:00:11:11:22:22   192.168.10.2    86233 dhcp-snooping 10   FastEthernet0/12
Total number of bindings: 1
```

Nếu tiếp tục sử dụng IP cấp phát động này, R2 được phép gửi dữ liệu vào cổng F0/12 (cột "IpAddress" hiển thị địa chỉ được phép "192.168.10.2"):

```
SW1#show ip verify source interface f0/12
Interface  Filter-type  Filter-mode  IP-address     Mac-address  Vlan  Log
---------- ------------ ------------ -------------- ------------ ----- ---
Fa0/12     ip           active       192.168.10.2                10    disabled
```

R2 có thể đi đến được các host khác:

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

Tiếp theo, thực hiện cấu hình tĩnh một IP nào đó trên cổng F0/0 của R2 (ví dụ: 192.168.10.22) thay cho IP động đã nhận từ DHCP:

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

Khi R2 cấu hình tĩnh địa chỉ mới thay thế cho IP cũ nhận từ DHCP, tiến trình DHCP trên R2 gửi cập nhật về điều này lên DHCP server R1 để từ bỏ địa chỉ IP đã được cấp phát. SW1 theo dõi các gói tin DHCP đến từ R2, biết được điều này và xóa bỏ thông tin tương ứng ra khỏi bảng DHCP snooping binding:

```
SW1#show ip dhcp snooping binding
MacAddress  IpAddress  Lease(sec)  Type  VLAN  Interface
--------------  ---------------------  ----------  --------  ----  ------------
Total number of bindings: 0
```

Tiếp đó, SW1 cũng đồng thời ngăn chặn mọi IP trên cổng F0/12 kết nối đến R2 (cột "IPAddress" hiển thị "deny-all"):

```
SW1#show ip verify source interface f0/12
Interface   Filter-type  Filter-mode  IP-address   Mac-address  Vlan
------------  ---------------  --------------  -----------------  ---------------  ----
Fa0/12      ip           active       deny-all                    10
```

R2 không thể gửi dữ liệu đi tiếp được nữa:

```
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)
```

Tiếp theo, cấu hình để R2 sử dụng trở lại IP nhận từ DHCP thay cho IP tĩnh:

```
R2(config)#interface f0/0
R2(config-if)#no ip address
R2(config-if)#ip address dhcp
R2(config-if)#end
R2#
*Jan       1    01:01:27.039:    %DHCP-6-ADDRESS_ASSIGN:    Interface
FastEthernet0/0    assigned    DHCP    address    192.168.10.3,    mask
255.255.255.0, hostname R2
```

Thông tin này được SW1 cập nhật vào bảng DHCP snooping binding:

```
SW1#show ip dhcp snooping binding
MacAddressIpAddress           Lease Type           VLAN  Interface
                              (sec)
------------------------------------------------------------------ ---------- ---------- ------  -------
00:00:11:11:22:22192.168.10.3  86286 dhcp-snooping   10    FastEthernet0/12
Total number of bindings: 1
```

Tính năng IP source - guard cho phép IP 192.168.10.3 được đi vào cổng F0/12:

```
SW1#show ip verify source interface f0/12
Interface Filter-type Filter-mode IP-address Mac-address Vlan Log
--------- ----------- ----------- ---------- ----------- ---- ---
Fa0/12    ip          active      192.168.10.3            10   disabled
```

R2 đã có thể giao tiếp trở lại với các host khác:

```
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 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
```

Như vậy, một host kết nối vào VLAN 10 chỉ có thể giao tiếp với các host khác nếu nó sử dụng IP động được cấp phát bởi DHCP.

2.4. DAI - Dynamic ARP Inspection

- Tiếp tục cấu hình bổ sung thêm tính năng DAI trên VLAN 10 để ngăn chặn hoạt động tấn công giả mạo ARP trên VLAN này.

Cấu hình:

Thực hiện bật tính năng DAI cho VLAN 10 trên SW1:

```
SW1(config)#ip arp inspection vlan 10
```

Khi tính năng DAI được bật lên, switch sẽ chia các cổng thuộc VLAN 10 thành hai loại trusted port và untrusted port (tương tự như DHCP snooping ở trên). Mọi gói tin ARP Reply do các host kết nối trên các untrusted port gửi vào switch sẽ đều được kiểm tra. Nếu kết quả phân giải IP - MAC ghi trên các gói này không khớp với thông tin IP - MAC tương ứng trong bảng DHCP snooping binding đã xây dựng trước đó, gói ARP Reply sẽ bị loại bỏ, không được chuyển đi tiếp. Điều này sẽ giúp ngăn chặn mọi cuộc tấn công giả mạo ARP xuất phát từ các end - user.

Mặc định, tất cả các cổng thuộc VLAN bật DAI sẽ được để ở chế độ untrusted. Với các cổng kết nối đến các thiết bị có độ tin cậy cao (như các server hay các thiết bị uplink), có thể chuyển cổng về chế độ trusted:

```
SW1(config)#interface f0/11
SW1(config-if)#ip arp inspection trust
SW1(config-if)#exit
```

Các gói tin ARP đến từ các cổng trusted sẽ không bị kiểm tra khi đi vào switch.

Kiểm tra:

Bảng DHCP snooping binding đã xây dựng trước đó của SW1:

```
SW1#show ip dhcp snooping binding
MacAddressIpAddress          Lease Type          VLAN Interface
                             (sec)
-------------------------------------------------- ------- ----------------- ------ --------------------------------------

00:00:11:11:22:22192.168.10.3 86286 dhcp-snooping  10    FastEthernet0/12
Total number of bindings: 1
```

Bảng này chỉ rõ rằng IP 192.168.10.3 đã được cấp phát cho host có MAC 0000.1111.2222 trên cổng F0/12. Do đó, kết quả phân giải ARP trả về từ host này bắt buộc phải là một sự tương quan giữa IP 192.168.10.3 và MAC 0000.1111.2222; nếu sự phân giải không khớp với sự tương quan này gói tin ARP Reply trả về từ host sẽ bị SW1 drop bỏ. Điều này ngăn chặn việc giả mạo kết quả phân giải ARP.

Tiếp theo, thực hiện kiểm tra hoạt động của DAI bằng cách khảo sát ứng xử của switch khi kết quả phân giải ARP được trả về khi đúng và khi sai với thông tin trong bảng DHCP snooping binding.

Xóa ARP cache hiện tại trên R1 bằng cách shutdown rồi no shutdown cổng F0/0 của R1:

```
R1(config)#interface f0/0
R1(config-if)#shutdown
R1(config-if)#
*May 13 09:03:25.891: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*May 13 09:03:26.891: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
R1(config-if)#no shutdown
R1(config-if)#
*May 13 09:03:32.539: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*May 13 09:03:33.539: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

Từ R1 thực hiện ping địa chỉ 192.168.10.3 của R2:

```
R1#ping 192.168.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
R1#show ip arp
Protocol Address      Age (min) Hardware Addr  Type Interface
Internet 192.168.10.1         - 0000.1111.1111  ARPA FastEthernet0/0
Internet 192.168.10.3         0 0000.1111.2222  ARPA FastEthernet0/0
```

ARP cache đã bị xóa nên R1 phải thực hiện lại thao tác gửi đi ARP request để tìm ra địa chỉ MAC tương ứng với địa chỉ IP 192.168.10.3 của R2. Vì ARP Reply trả về từ R2 có IP và MAC đúng với thông tin đã lưu trên bảng DHCP snooping binding nên thông tin này được cập nhật vào bảng ARP của R1. Phân giải ARP đã được thực hiện thành công nên ping thành công.

Tiếp theo, thực hiện lại việc xóa ARP cache trên R1:

```
R1(config)#interface f0/0
R1(config-if)#shutdown
R1(config-if)#
*May 14 03:42:27.411: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
*May 14 03:42:28.411: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
R1(config-if)#no shutdown
R1(config-if)#
*May 14 03:42:33.123: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*May 14 03:42:34.123: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1#show ip arp
Protocol Address    Age (min) Hardware Addr  Type Interface
Internet 192.168.10.1-  0000.1111.1111 ARPA FastEthernet0/0
```

Đổi lại địa chỉ MAC trên cổng F0/0 của R2 để giả lập hoạt động phân giải sai địa chỉ MAC cho IP 192.168.10.3:

```
R2(config)#interface f0/0
R2(config-if)#mac-address 0000.1111.3333 ← Trước đó là 0000.1111.2222
SW1(config)#int f0/12
SW1(config-if)#no switchport port-security mac-address 0000.1111.2222 ← Gỡ bỏ port-security cho địa chỉ 0000.1111.2222 đã cấu hình trước đó để cổng F0/12 của SW1 chấp nhận địa chỉ MAC mới thay đổi của R2
```

Từ R1 thực hiện ping lại địa chỉ 192.168.10.3:

```
R1#ping 192.168.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Hoạt động ping diễn ra không thành công. Điều này xảy ra do phân giải ARP đã không thể hoàn tất:

```
R1#show ip arp
Protocol Address     Age (min) Hardware Addr  Type Interface
Internet 192.168.10.1        -  0000.1111.1111 ARPA FastEthernet0/0
Internet 192.168.10.3        0  Incomplete     ARPA
```

SW1 đã chặn lại các gói ARP Reply đến từ R2 vì thông tin phân giải không đúng với nội dung đã lưu trong bảng DHCP snooping binding: địa chỉ 192.168.10.3 đáng lẽ phải được phân giải thành MAC 0000.1111.2222 thì lại được phân giải thành MAC 0000.1111.3333. Điều này được thể hiện qua các thông điệp syslog do SW1 phát ra:

```
SW1#
*Mar  1 01:13:18.096: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs
(Res)                  on                  Fa0/12,                  vlan
10.([0000.1111.3333/192.168.10.3/0000.1111.1111/192.168.10.1/01:1
3:17 UTC Mon Mar 1 1993])
SW1#
*Mar  1 01:13:20.109: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs
(Res)                  on                  Fa0/12,                  vlan
10.([0000.1111.3333/192.168.10.3/0000.1111.1111/192.168.10.1/01:1
3:19 UTC Mon Mar 1 1993])
SW1#
*Mar  1 01:13:22.123: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs
(Res)                  on                  Fa0/12,                  vlan
10.([0000.1111.3333/192.168.10.3/0000.1111.1111/192.168.10.1/01:1
3:21 UTC Mon Mar 1 1993])
```

Thực hiện đổi lại địa chỉ MAC trên cổng F0/0 về lại thành địa chỉ 0000.1111.2222 đúng như thông tin trong bảng DHCP snooping binding:

```
R2(config)#interface f0/0
R2(config-if)#mac-address 0000.1111.2222
```

Lúc này R1 đã ping được đến R2 vì hoạt động phân giải ARP đã diễn ra thành công:

```
R1#ping 192.168.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.3, timeout is 2 seconds:
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms

R1#show ip arp

Protocol  Address          Age (min)  Hardware Addr   Type   Interface

Internet   192.168.10.1                  -     0000.1111.1111    ARPA
FastEthernet0/0

Internet   192.168.10.3                  0     0000.1111.2222    ARPA
FastEthernet0/0
```