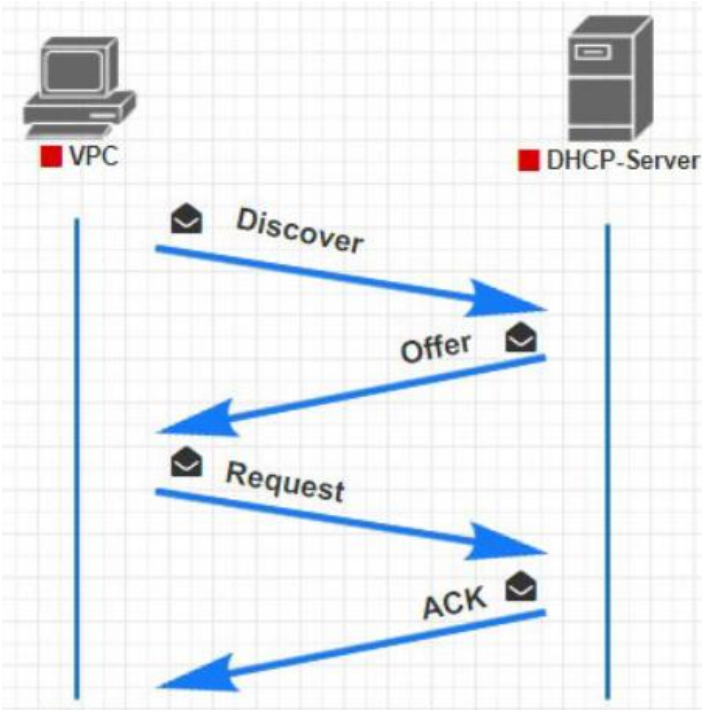
DHCP SNOOPING

DHCP Snooping là 1 tính năng bảo mật thuộc lớp 2, hoạt động giống như 1 firewall giữa các server DHCP, giúp chúng ta có thể ngăn chặn các DHCP Server giả mạo trong mạng. DHCP Snooping là 1 tính năng chuẩn quốc tế, do vậy thì các bạn có thể cấu hình nó trên tất cả các thiết bị hỗ trợ. Nó chỉ khác nhau về mặt cấu hình, còn hoạt động thì tương tự nhau.

DHCP Snooping thì hoạt động dựa trên VLAN, do vậy khi cấu hình các bạn cần phải kích hoạt trên từng VLAN, hoặc trên tất cả các VLAN đang có trong mạng.

Hoạt động của DHCP

Trước tiên chúng ta sẽ cùng tìm hiểu về hoạt động của DHCP trong mạng trước nhé.



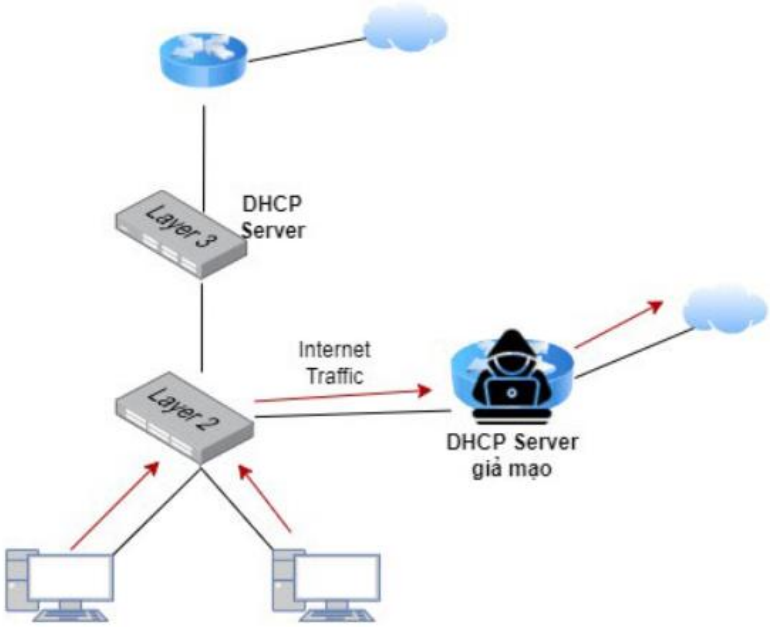
Ban đầu khi 1 thiết bị kết nối vào mạng, nó sẽ gửi ra 1 bản tin DHCP **Discover** ra toàn mạng. Khi đó toàn bộ các thiết bị trong LAN sẽ đều nhận được. Tuy nhiên chỉ các thiết bị có bật tính năng DHCP Server sẽ xử lý gói tin này và phản hồi lại 1 gói tin khác là DHCP **Offer**. Còn lại các thiết bị khác sẽ drop gói tin này. Gói tin DHCP Offer sẽ chứa thông tin địa chỉ IP và các tùy chọn khác mà các bạn cấu hình trên DHCP Server. Địa chỉ IP này sẽ là địa chỉ IP chưa được sử dụng trong mạng.

Sau khi Client nhận được gói tin Offer với thông tin IP, nó sẽ gửi lại 1 gói tin **Request** về Server đã gửi Offer cho nó, cũng với thông tin IP mà Server đã gửi cho.

Cuối cùng là DHCP Server sẽ gửi lại bản tin **ACK** để xác nhận, chưa các thông tin IP mà 2 bên đã trao đổi, sau đó Client có thể sử dụng IP đó để giao tiếp trong mạng.

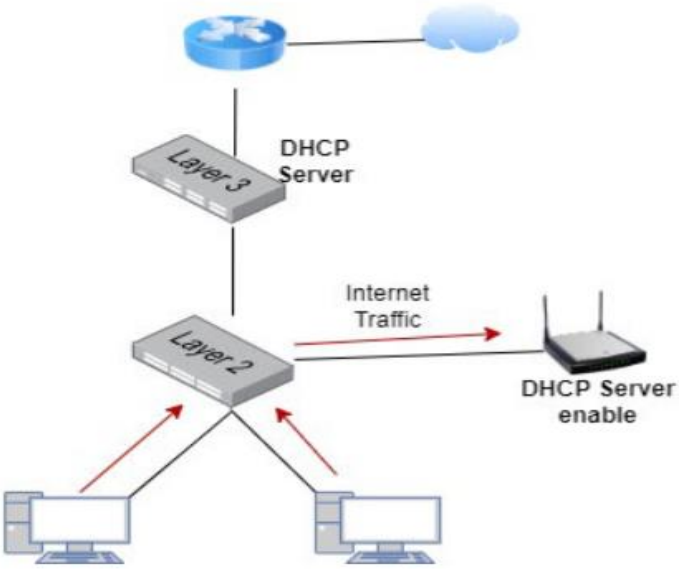
Các vấn đề thường xảy ra với DHCP Server

- Trường hợp 1: nếu có 1 hacker nào đó giả mạo 1 DHCP Server trong mạng của bạn với gateway chính là router của hacker. Khi đó thì toàn bộ traffic đi ra sẽ qua router hoặc switch của hacker, và hacker này có thể đọc được toàn bộ dữ liệu của người dùng. Router của Hacker vẫn có Internet nên người dùng hoàn toàn không biết về vấn đề này, do họ vẫn truy cập Internet bình thường. Nếu các thông tin nhạy cảm như các dữ liệu nội bộ, các thông tin



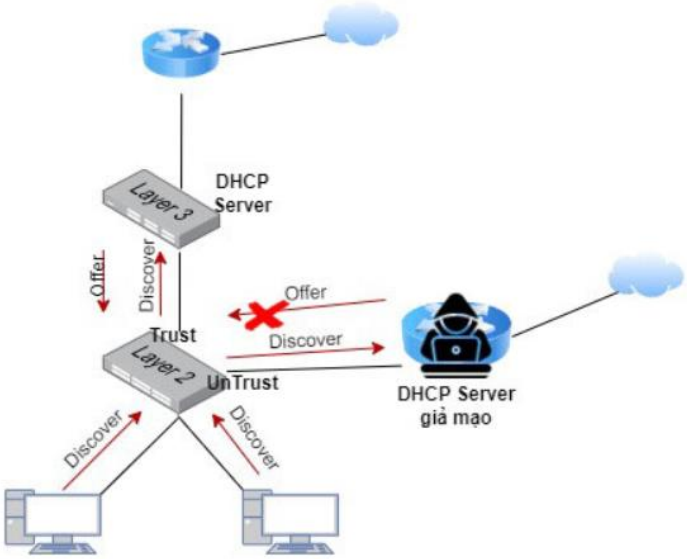
giao dịch bị lộ ra ngoài thì rất nguy hiểm.

- Trường hợp 2 : là trường hợp rất hay xảy ra, mà thường là do vô tình. Đó là trường hợp mà 1 nhân viên trong phòng ban nào đó mang 1 thiết bị router wifi vào cắm trong mạng để sử dụng wifi cá nhân. Nhưng vô tình thì router wifi đó được enable DHCP lên, và họ cắm dây mạng vào cổng LAN nên DHCP Server này sẽ cấp ngược IP vào mạng LAN của các bạn. Khi đó thì những thiết bị nào nhận được IP từ bộ router wifi này đều mất mạng do bộ Router wifi này sẽ không có kết nối Internet trên dải mạng riêng của Wifi. Và nếu tại các địa điểm như bệnh viện, hay các nhà xưởng có nhiều tòa nhà thì chúng ta sẽ rất mất thời gian để tìm ra.



Hoạt động của DHCP Snooping

Ban đầu Client gửi ra các gói tin **Discover** là dạng broadcast tới toàn LAN, sau đó các Server sẽ trả về gói **Offer**.



Khi đó trên switch chạy DCHP Snooping sẽ chia các port role là **Trust** và **Untrust**. Chỉ có các cổng trust mới cho các gói tin DHCP **Offer** đi qua, như vậy thì các DHCP server giả mạo trên các cổng untrust sẽ không thể cấp ngược được IP vào mạng do gói tin DHCP Offer sẽ bị drop ngay trên switch.

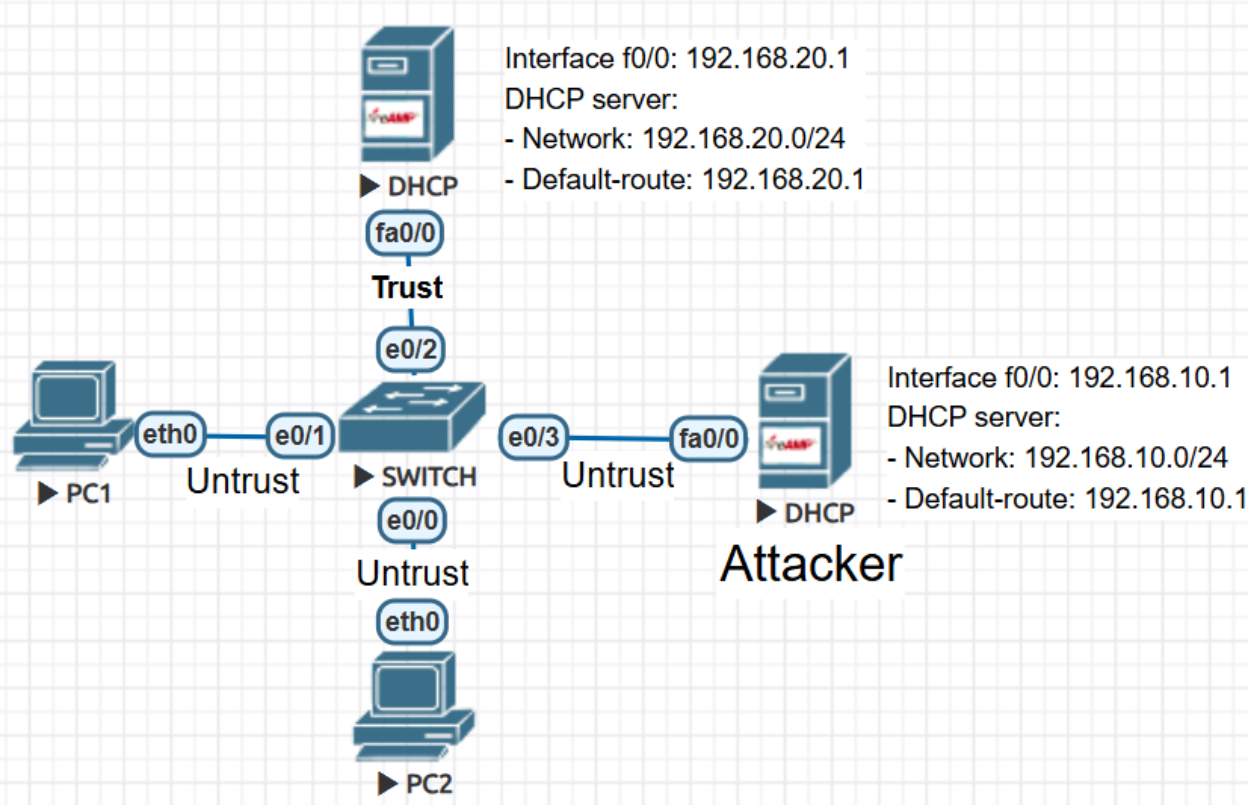
Các bạn chỉ cần cấu hình cổng nối lên DHCP Server của VnPro là cổng trust là xong, còn lại mặc định các cổng khi bật DHCP Snooping lên thì các cổng đều là untrust.

Sau đó switch sẽ lưu lại 1 bảng DHCP Snooping Database, DHCP Snooping database cũng có thể được sử dụng cho các tính năng như Dynamic ARP inspection hoặc IP Source Guard để tăng bảo mật cho mạng.

Theo nguyên lý thì các switch sẽ drop gói tin DHCP Offer đi qua các cổng Untrust, nghĩa là ban đầu gói tin Discover sẽ vẫn gửi ra toàn mạng. Tuy nhiên thì trên switch Cisco hành vi sẽ khác. Các switch được bật DHCP Snooping sẽ chỉ chuyển tiếp gói tin Discover ra các cổng trust ngay từ đầu, do đó thì nó ngăn chặn các DHCP Server giả mạo nhận được ngay từ đầu. Do vậy nó sẽ tối ưu được cả traffic trong mạng, giúp giảm đáng kể các gói tin DHCP Discover.

LAB THỰC HIỆN TRÊN EVE

(VnPro đã thực hiện và kiểm tra thành công)



VnPro sẽ cấu hình DHCP server cho các PC bên dưới

Router>enable

Router#configure terminal

Router(config)#hostname DHCP-server

DHCP-server (config)#ip dhcp pool DHCP1

DHCP-server (dhcp-config)# network 192.168.20.0 255.255.255.0

DHCP-server (dhcp-config)# default-router 192.168.20.1

Bây giờ thì cả 2 PC bên dưới mạng LAN sẽ nhận được IP từ DHCP server cấp xuống, thuộc dải 192.168.20.0/24.

Giả sử bây giờ VnPro có 1 DHCP khác trong mạng, sẽ cấu hình trên switch Hacker, trong thực tế thì nó thường là các bộ router wifi mà người dùng lắp vào. VnPro sẽ cấu hình cho nó cấp 1 dải mạng khác là 192.168.10.0/24.

Router>enable

Router#configure terminal

Router(config)#hostname DHCP-Attacker

DHCP-Attacker(config)#ip dhcp pool DHCP-Attacker

DHCP-Attacker(dhcp-config)# network 192.168.10.0 255.255.255.0

DHCP-Attacker(dhcp-config)# default-router 192.168.10.1

Bây giờ khi các PC nhận IP thì nó sẽ nhận ngẫu nhiên giữa 2 Server này, server nào gửi lại gói DHCP Offer trước thì các PC sẽ nhận IP từ server đó.

Trên PC:

```
VPCS> ip dhcp
DORA IP 192.168.20.2/24 GW 192.168.20.1

VPCS> ip dhcp
DORA IP 192.168.10.4/24 GW 192.168.10.1
```

Các bạn có thể thấy PC đã nhận ngẫu nhiên IP, có lúc nhận IP từ hacker, có lúc nhận từ DHCP server. Vấn đề này chúng ta không control được do nó phục thuộc vào đường truyền mạng, server có đang xử lý nhiều gói tin không… DHCP Server nào gần client hơn, hoặc tài nguyên còn nhiều hơn thì khả năng cao sẽ cấp IP cho client đó.

Trong trường hợp này VnPro sẽ bật **DHCP Snooping** cho VLAN 1 trên SW-Access, và cấu hình cổng e0/0 là cổng **Trust**, còn các cổng khác mặc định sẽ là **Untrust**. Khi đó thì chỉ DHCP server kết nối với cổng e0/2 của switch access mới có thể gửi gói tin DHCP Offer qua.

Switch(config)#ip dhcp snooping

Switch(config)#no ip dhcp snooping information option

Switch(config)#ip dhcp snooping vlan 1

Switch(config)#int e0/2

Switch(config-if)#ip dhcp snooping trust

Switch(config-if)#exit

Switch(config)#int range e0/0-1

Switch(config-if)#ip dhcp snooping limit rate 10

Switch(config-if)#exit

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
DHCP snooping is operational on following VLANs:
1
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is disabled
   circuit-id default format: vlan-mod-port
   remote-id: aabb.cc00.3000 (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)
-----------------------    -------    ------------    ----------------
Ethernet0/0                no         no              10
  Custom circuit-ids:
Ethernet0/1                no         no              10
  Custom circuit-ids:
Ethernet0/2                yes        yes             unlimited
  Custom circuit-ids:
```

Các bạn cũng có thể giới hạn số lượng gói tin DHCP trên các cổng mạng bằng lệnh:

ip dhcp snooping limit rate <1-2048>

Đó là số lượng gói tin DHCP được cho phép trên 1s. Nó sẽ được tính bằng packet per second.

Cấu hình này có thể giúp các bạn phòng chống được các trường hợp tấn công làm cạn kiệt DHCP. Các máy tính của hacker, hoặc các máy bị nhiễm virut sẽ liên tục gửi các yêu cầu DHCP lên server, làm cho cạn IP trên server hoặc làm cho server bị quá tải. Khi đó các máy tính khác trong mạng LAN sẽ không nhận được IP nữa. Các bạn có thể tính dựa trên số lượng Client trong mạng nhân với số lượng gói tin DHCP, sau đó tính dư ra thêm khoảng 1/3 để dự phòng.

Trên các switch bật DHCP Snooping thì các bạn có thể show được thông tin về Client bằng lệnh **show ip dhcp snooping binding**. Bảng này sẽ khác nhau giữa các switch.

Switch#show ip dhcp snooping binding

```
Switch#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:50:79:66:68:05   192.168.20.2     86283       dhcp-snooping  1     Ethernet0/0
Total number of bindings: 1
```

Bảng này sẽ có thông tin về MAC, IP, loại là DHCP Snooping, vlan 1 và cổng kết nối của client.

bật debug trên switch access để các bạn xem hành vi xử lý trên switch Cisco

Switch#debug ip dhcp snooping event

DHCP Snooping Event debugging is on

Switch#debug ip dhcp snooping packet

DHCP Snooping Packet debugging is on

PC2 nhận IP. Trên SW-Access sẽ có các log liên quan đến quá trình xử lý gói tin DHCP.

DHCP | SWITCH | PC2

```
Switch#
*Mar 12 08:22:34.663: DHCP_SNOOPING: checking expired snoop binding entries
Switch#
*Mar 12 08:23:02.610: DHCP_SNOOPING: received new DHCP packet from input interface (Ethernet0/
0)
*Mar 12 08:23:02.610: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, inpu
t interface: Et0/0, MAC da: ffff.ffff.ffff, MAC sa: 0050.7966.6805, IP da: 255.255.255.255, IP
 sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0
.0.0.0, DHCP chaddr: 0050.7966.6805
*Mar 12 08:23:02.610: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, p
acket is flooded to ingress VLAN: (1)
*Mar 12 08:23:02.610: DHCP_SNOOPING_SW: bridge packet send packet to port: Ethernet0/2, vlan 1
.
Switch#
*Mar 12 08:23:03.610: DHCP_SNOOPING: received new DHCP packet from input interface (Ethernet0/
0)
*Mar 12 08:23:03.610: DHCP_SNOOPING: process new DHCP packet, message type: DHCPDISCOVER, inpu
t interface: Et0/0, MAC da: ffff.ffff.ffff, MAC sa: 0050.7966.6805, IP da: 255.255.255.255, IP
 sa: 0.0.0.0, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0
.0.0.0, DHCP chaddr: 0050.7966.6805
*Mar 12 08:23:03.610: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, p
acket is flooded to ingress VLAN: (1)
*Mar 12 08:23:03.610: DHCP_SNOOPING_SW: bridge packet send packet to port: Ethernet0/2, vlan 1
.
*Mar 12 08:23:04.634: DHCP_SNOOPING: received new DHCP packet from input interface (Ethernet0/
2)
*Mar 12 08:23:04.635: DHCP_SNOOPING: process new DHCP packet, message type: DHCPOFFER, input i
nterface: Et0/2, MAC da: 0050.7966.6805, MAC sa: ca01.137c.0000, IP da: 192.168.20.3, IP sa: 1
92.168.20.1, DHCP ciaddr: 0.0.0.0, DHCP yiaddr: 192.168.20.3, DHCP siaddr: 0.0.0.0, DHCP giadd
r: 0.0.0.0, DHCP chaddr: 0050.7966.6805
*Mar 12 08:23:04.635: DHCP_SNOOPING: direct forward dhcp replyto output port: Ethernet0/0.
Switch#
*Mar 12 08:23:06.611: DHCP_SNOOPING: received new DHCP packet from input interface (Ethernet0/
0)
*Mar 12 08:23:06.611: DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST, input
 interface: Et0/0, MAC da: ca01.137c.0000, MAC sa: 0050.7966.6805, IP da: 255.255.255.255, IP
sa: 0.0.0.0, DHCP ciaddr: 192.168.20.3, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giadd
r: 0.0.0.0, DHCP chaddr: 0050.7966.6805
*Mar 12 08:23:06.611: DHCP_SNOOPING_SW: bridge packet send packet to port: Ethernet0/2, vlan 1
.
*Mar 12 08:23:06.621: DHCP_SNOOPING: received new DHCP packet from input interface (Ethernet0/
2)
*Mar 12 08:23:06.621: DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK, input int
erface: Et0/2, MAC da: 0050.7966.6805, MAC sa: ca01.137c.0000, IP da: 192.168.20.3, IP sa: 192
.168.20.1, DHCP ciaddr: 192.168.20.3, DHCP yiaddr: 192.168.20.3, DHCP siaddr: 0.0.0.0, DHCP gi
addr: 0.0.0.0, DHCP chaddr: 0050.7966.6805
*Mar 12 08:23:06.621: DHCP_SNOOPING: add binding on port Ethernet0/0.
*Mar 12 08:23:06.621: DHCP_SNOOPING: added entry to table (index 139)

*Mar 12 08:23:06.621: DHCP_SNOOPING: dump binding entry: Mac=00:50:79:66:68:05 Ip=192.168.20.3
 Lease=86400      Type=dhcp-snooping Vlan=1 If=Ethernet0/0
Switch#
*Mar 12 08:23:06.621: DHCP_SNOOPING_SW no entry found for 0050.7966.6805 0.0.0.1 Ethernet0/0
*Mar 12 08:23:06.622: DHCP_SNOOPING_SW host tracking not found for update add dynamic (192.168
.20.3, 0.0.0.0, 0050.7966.6805) vlan 1
*Mar 12 08:23:06.622: DHCP_SNOOPING: direct forward dhcp replyto output port: Ethernet0/0.
```

Ban đầu switch sẽ nhận được 1 gói tin DHCP Discover từ cổng e0/1 là cổng nối với PC2 với MAC đích là broadcast FFFF.FFFF.FFFF.

Gói tin nhận được từ VLAN 1, nên nó sẽ được chuyển vào VLAN 1, và sau đó nó chỉ gửi gói tin qua port **e0/2**, là cổng **Trust**.

DHCP server nhận được sẽ gửi lại gói tin DHCP Offer qua cổng E0/2 với các thông tin IP, nó là cổng trust nên sẽ được switch cho phép và đẩy qua cổng e0/1 cho PC2.

Và cuối cùng switch sẽ binding địa chỉ IP và port e0/1 với các thông tin của Client. Thông tin này sẽ được sử dụng vào các mục đích khác nhau để chống các loại tấn công liên quan đến giả mạo ARP, giả mạo IP…

Như vậy chúng ta vừa ngăn chặn được các server giả mạo, vừa giảm được các gói tin DHCP Discover trong mạng.

Ngoài ra thì các bạn cũng có thể kết hợp DHCP Snooping cùng với nhiều tính năng bảo mật khác để ngăn chặn việc giả địa chỉ IP hoặc MAC để lấy cắp thông tin trong mạng.

Tác giả : Nguyễn Quang Hòa -PKT VNPRO