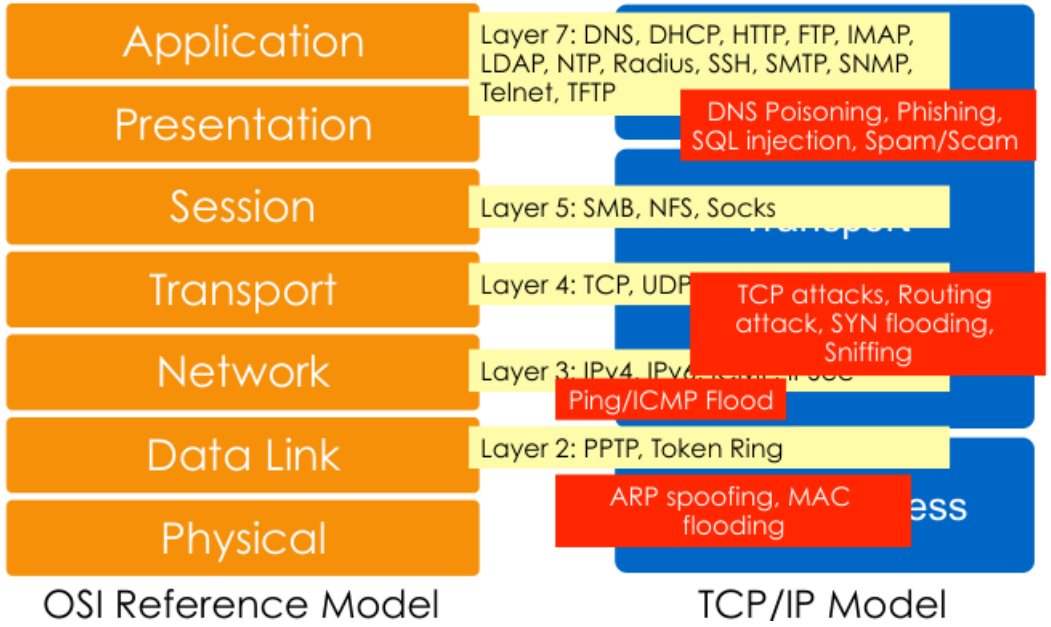
BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM INTERNET VIỆT NAM

# BẢO MẬT HẠ TẦNG MẠNG
# LAYER 2 MÔ HÌNH OSI

# PHẦN 1
# NHỮNG KIỂU TẤN CÔNG PHỔ BIẾN & CÁCH PHÒNG CHỐNG

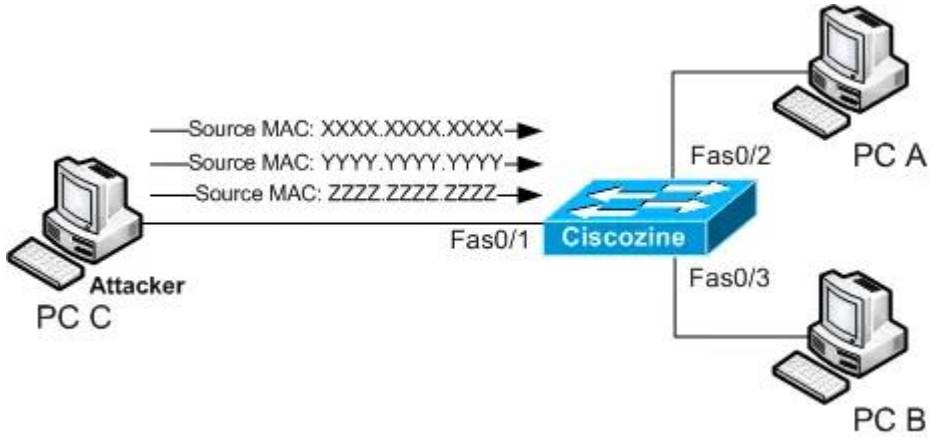
# Tấn công bảo mật ở các Layer

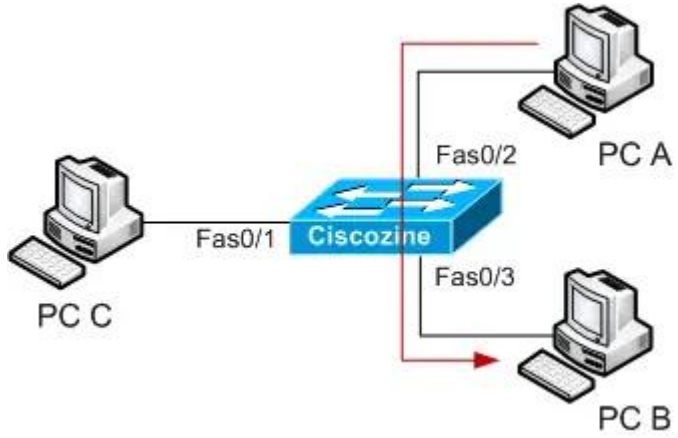
- Mô hình OSI (và TCP/IP) gồm nhiều tầng khác nhau, mỗi tầng hoạt động độc lập không cần biết chi tiết công việc của nhau.
- Việc tấn công bảo mật có thể xảy ra ở bất kỳ tầng nào của mô hình OSI. Khi một tầng bị tấn công thì các tầng khác không nhận biết điều này và có thể bị tác động.
- Vì thế cần bảo mật đối với tất cả các tầng, đầu tiên từ tầng 2 vì nếu tầng này bị tấn công thì các tầng phía trên chắc chắc bị ảnh hưởng, đặc biệt tấn công DoS.
- Để bảo vệ hạ tầng mạng, cần tập trung phòng chống từ Layer 2 đến 4.

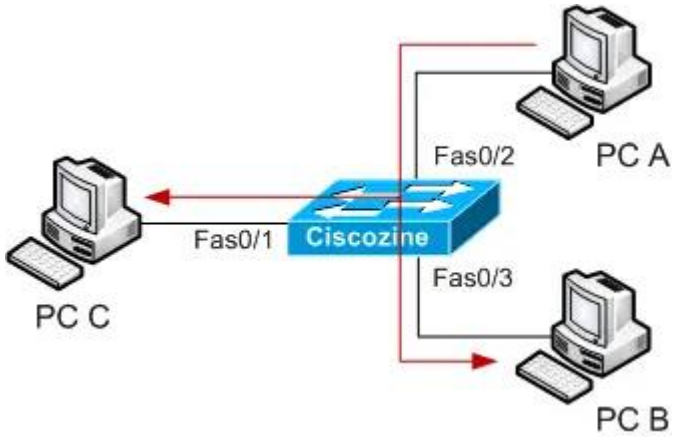


# Kiểu tấn công MAC Flooding

- Bình thường Switch sẽ chuyển mạch bản tin giữa các cổng mạng thông quan bảng MAC Table (bảng CAM).
- Máy tính tấn công sẽ gửi số lượng lớn địa chỉ MAC giả mạo nhằm làm đầy MAC Table của Switch.
- Lúc này Switch khi nhận được bản tin sẽ gửi ra tất cả các cổng (hoạt động giống Hub) nên máy tấn công có thể nghe lén các bản tin.

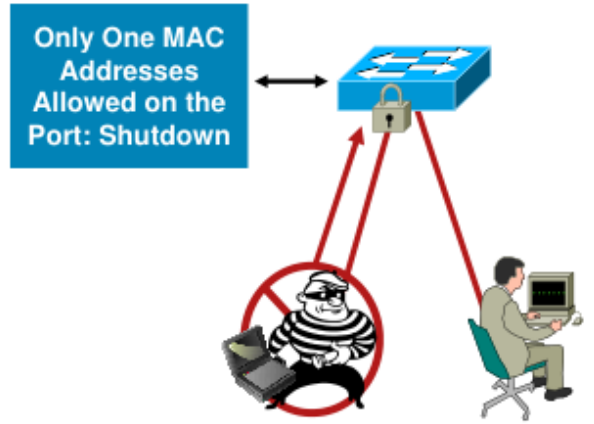


- Tính năng Port-Security giúp hạn chế số lượng MAC học trên mỗi cổng, khai báo địa chỉ MAC tĩnh và hành động xử lý khi xảy ra vi phạm.

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)# switchport port-security mac-address bbbb.bbbb.bbbb
Switch(config-if)# switchport port-security mac-address sticky
```




| Switch Port Action during Port Security Violation | Protect | Restrict | Shutdown |
|---|---|---|---|
| Discards offending traffic | Yes | Yes | Yes |
| Sends log and SNMP messages | No | Yes | Yes |
| Disables the interface by putting it in an err-disabled state, discarding all traffic | No | No | Yes |

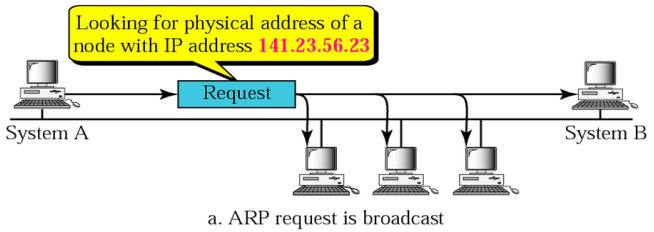
```
SwitchA# show port-security interface fa0/1
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Restrict
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

**Solution:**

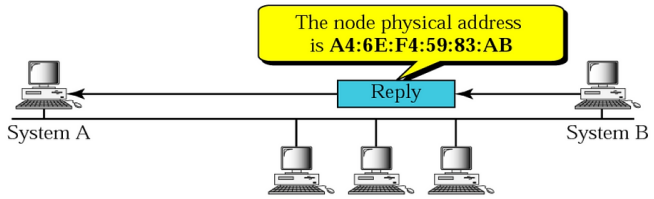
- Port security limits MAC flooding attack and locks down port and sends an SNMP trap

# Kiểu tấn công ARP Spoofing (Poisoning)

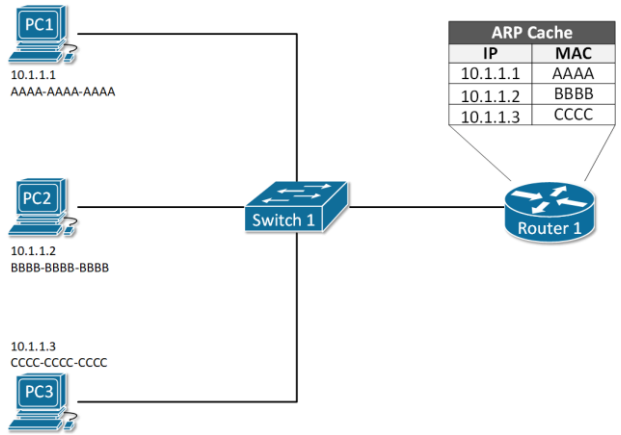
- Đây là cách tấn công giả mạo địa chỉ MAC nhằm đổi hướng truyền dữ liệu nhằm nghe lén hay can thiệp luồng dữ liệu (Session Hijacking). Còn có tên gọi là ARP Poisoning hoặc Man-in-The-Middle (MiTH).
-Việc tấn công thông qua bản tin gratuitous arp.
- Còn một cách tấn công khác là ARP Flooding làm tràn bộ nhớ ARP Cache của một máy tính hoặc Switch.

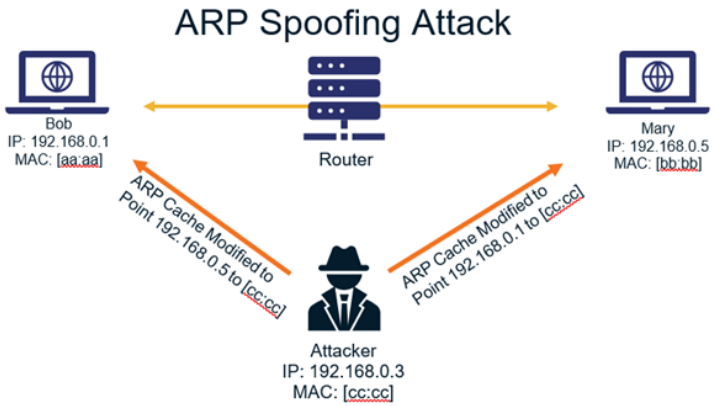


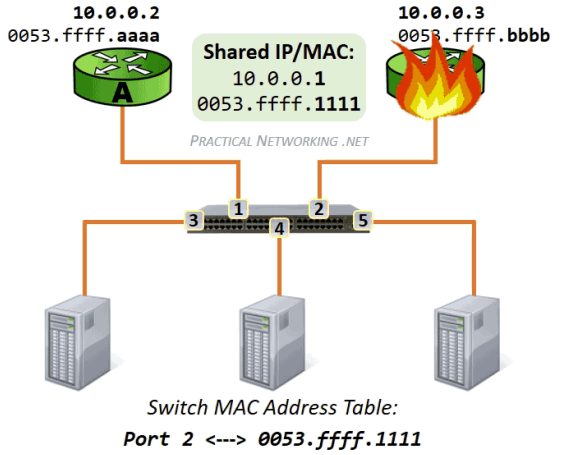
a. ARP request is broadcast



b. ARP reply is unicast

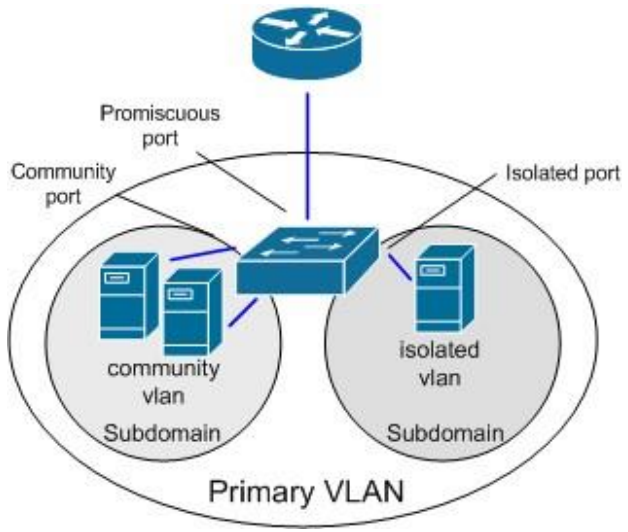


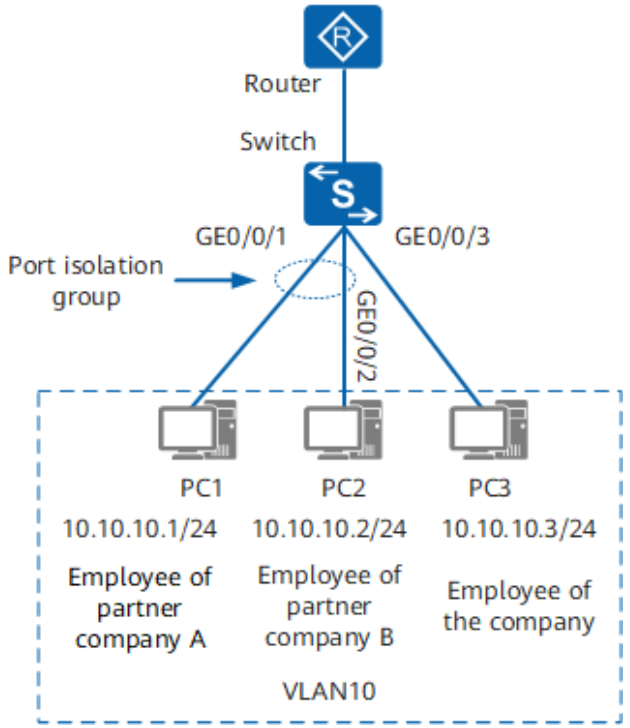



# Cách phòng chống tấn công ARP Spoofing

- Ngoài việc khai báo Port-Security cần khai báo thêm tính năng Private-VLAN hoặc Port-Isolation.
- Ngoài ra còn có thể sử dụng kỹ thuật Static ARP hoặc Dynamic ARP Inspection (DAI) kết hợp với DHCP Snooping.



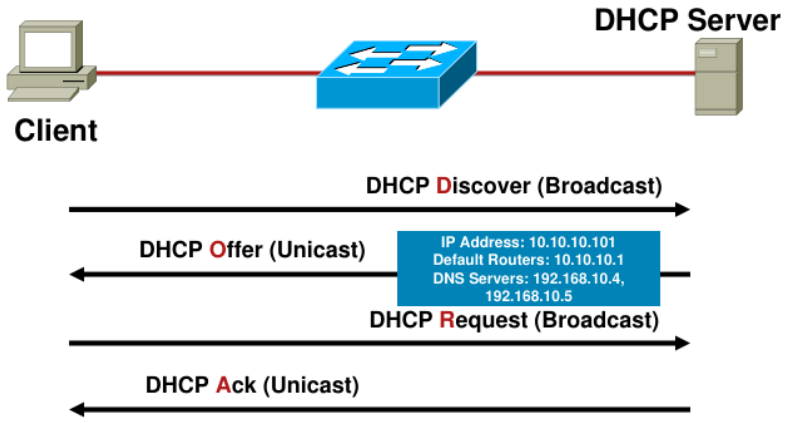

```
interface range fa0/1 - 2
 switchport mode private-vlan host
 switchport private-vlan host-association 500 501
interface fa0/24
 switchport mode private-vlan promiscuous
switchport private-vlan mapping 500 501
```



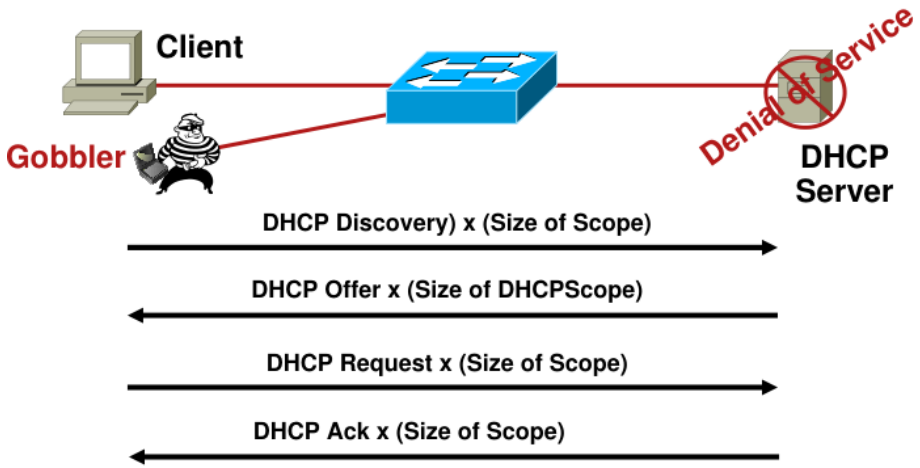

```
#
interface Gi0/0/1
 port link-type access
 port default vlan 10
 port-isolate enable group 3
#
interface Gi0/0/2
 port link-type access
 port default vlan 10
 port-isolate enable group 3
#
interface Gi0/0/3
 port link-type access
 port default vlan 10
#
```

# Kiểu tấn công DHCP Starvation

- Kẻ tấn công sử dụng nhiều địa chỉ MAC nguồn khác nhau và gửi yêu cầu địa cấp địa chỉ động đến DHCP Server là cạn kiệt dãy IP của Server làm cho các máy tính khác không có IP để truy cập mạng.
- Đây còn được gọi là kiểu tấn công từ chối dịch vụ DOS (Denial Of Service).



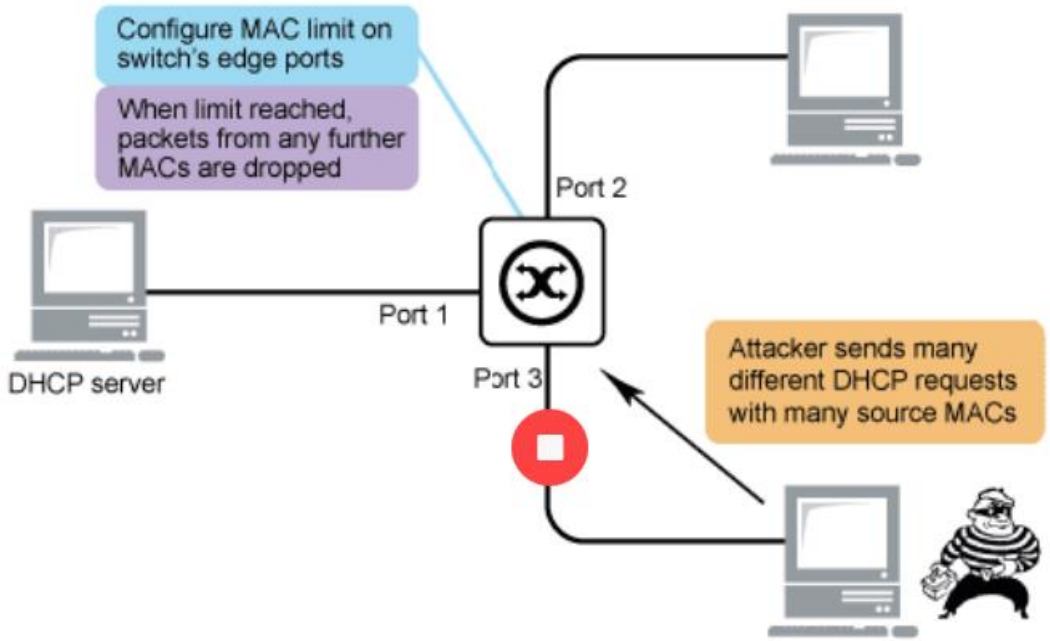

- DHCP Defined by RFC 2131




- Gobbler/DHCPx looks at the entire DHCP scope and tries to lease all of the DHCP addresses available in the DHCP scope
- This is a Denial of Service DoS attack using DHCP leases

# Cách phòng chống tấn công DHCP Starvation

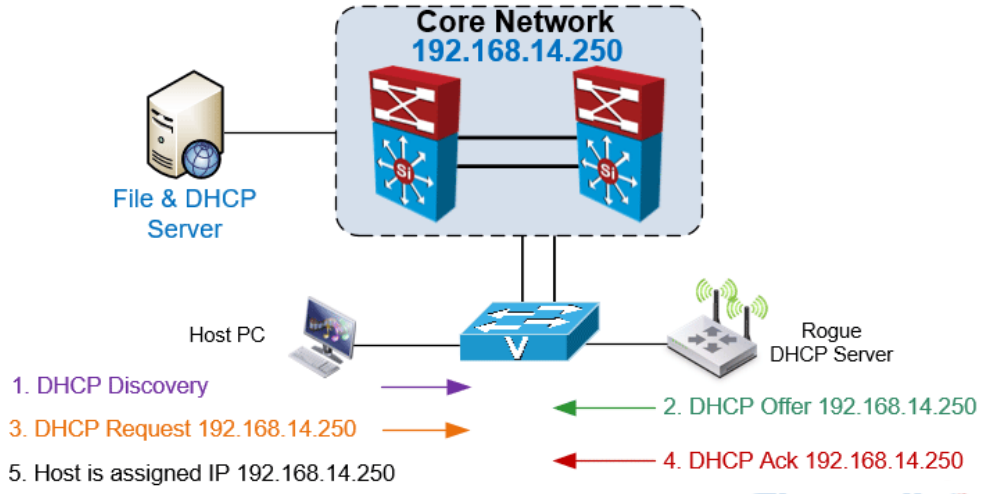
- Vì kẻ tấn công giả mạo nhiều địa chỉ MAC khác nhau để gửi yêu cầu đến máy chủ DHCP nên cần phải giới hạn số lượng MAC học được trên mỗi Port thông qua tính năng Port-Security (như trường hợp sMAC Flooding).
- Kiểm tra trạng thái của Port-Security để xác định vị trí Port của máy tính tấn công.

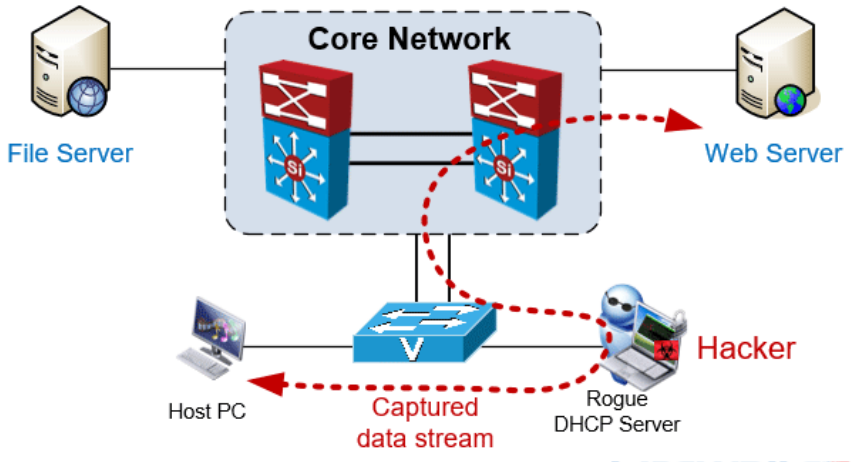



```
SW1(config)# Interface Fa0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport port-security
SW1(config-if)# switchport port-security mac-address AAAA.AAAA.AAAA
SW1(config-if)# exit
SW1(config)# interface Fa0/2
SW1(config-if)# switchport mode access
SW1(config-if)# switchport port-security
SW1(config-if)# switchport port-security maximum 2
SW1(config-if)# switchport port-security violation restrict
```

# Kiểu tấn công DHCP Rogue Server

- Kẻ tấn công sẽ dựng lên một DHCP Server giả mạo, cung cấp thông tin sai lệch nhằm điều hướng dữ liệu đi sang máy tính tấn công để đánh cắp hay thay đổi dữ liệu.
- Đây còn được gọi là kiểu tấn công Man-in-The-Middle (MiTM) như ARP Spoofing.

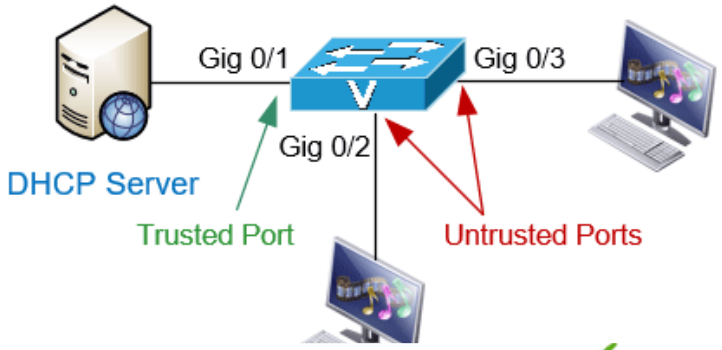


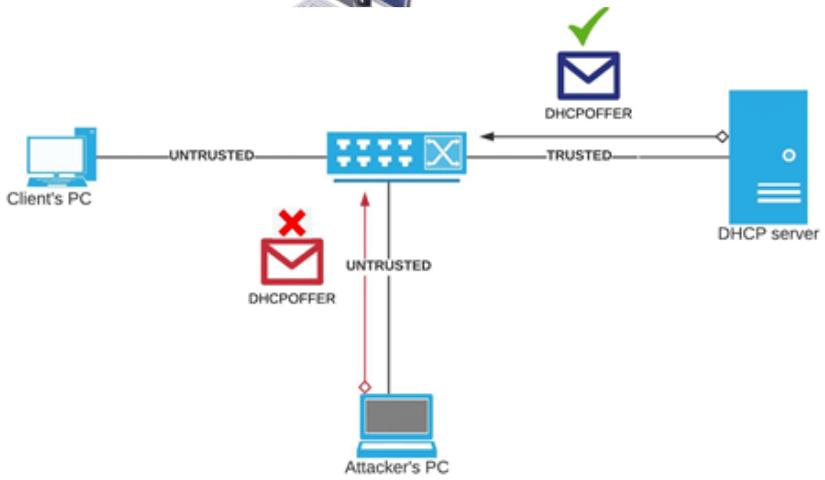




- **Wrong default gateway** - The rogue server provides an invalid gateway or the IP address of its host to create a man-in-the-middle attack. This may go entirely undetected as the intruder intercepts the data flow through the network.
- **Wrong DNS server** - The rogue server provides an incorrect DNS server address pointing the user to a nefarious website.
- **Wrong IP address** - The rogue server provides an invalid IP address effectively creating a DoS attack on the DHCP client.

# Cách phòng chống tấn công DHCP Rogue Server

- Tính năng DHCP Snooping cho phép chỉ định Port trên Switch là Trusted hay là Untrusted và lắng nghe các bản tin DHCP.
- Port ở chế độ Untrusted sẽ không chấp nhận các bản tin DHCP Offer, ACK nên DHCP Server giả mạo không thể hoạt động.
- Port nối với DHCP Server thực sự sẽ được khai báo chế độ Trusted.



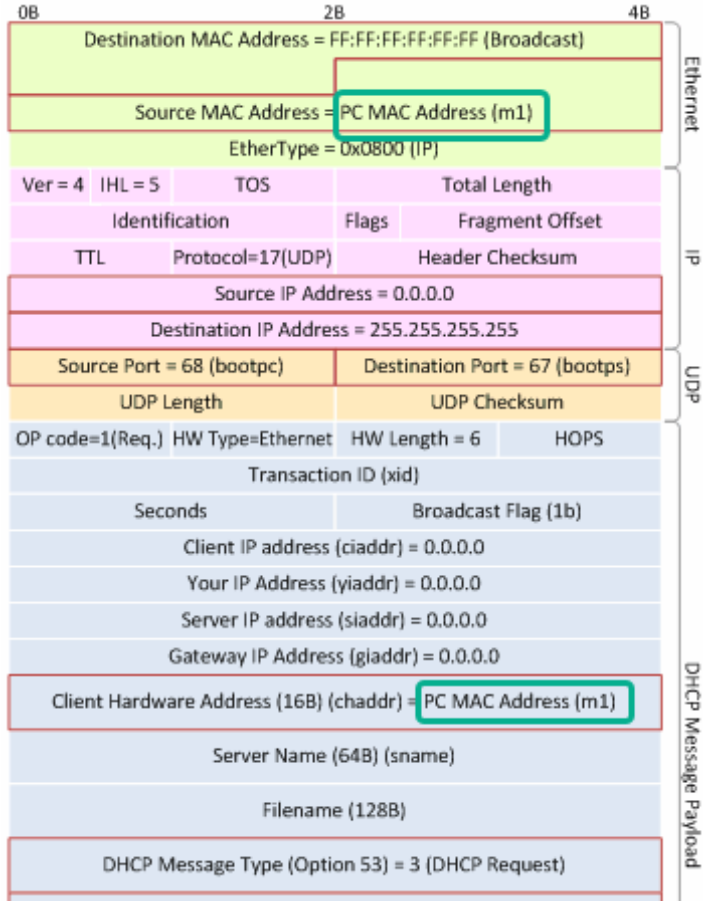



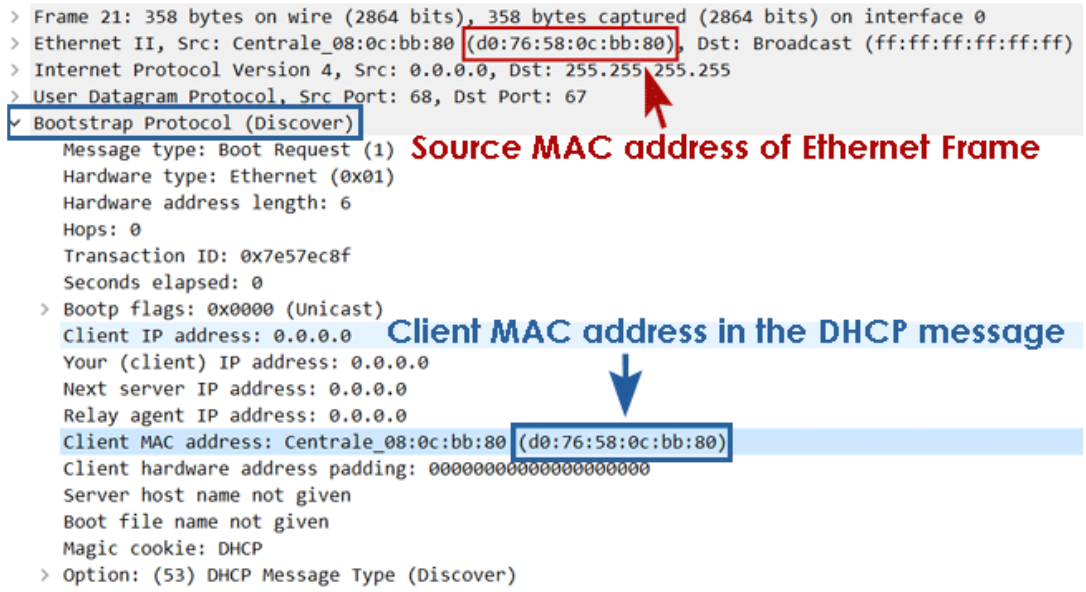

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# interface Fastethernet 0/5
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 10

Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
Insertion of option 82 is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/5              yes         unlimited
```

```
Switch#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:01:02:03:04:05   10.0.0.1         86250       dhcp-snooping  10    FastEthernet0/5
```

# Cách phòng chống tấn công DHCP Rogue Server (tt)

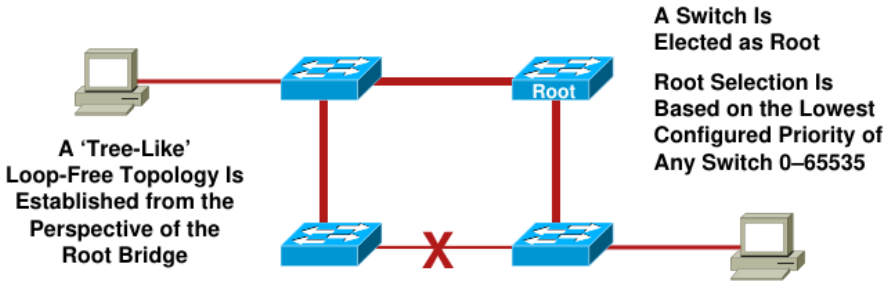
- Một số máy tấn công DHCP không cần giả mạo địa chỉ MAC mà giả mạo thông tin Client Hardware Address (CHADDR) để gửi yêu cầu địa chỉ đến DHCP Server có thể làm cạn kiệt địa chỉ (DHCP Starvation).
- Trong bản tin DHCP có địa chỉ CHADDR và thường trùng với địa chỉ MAC nguồn. DHCP Snooping cho phép kiểm tra trường CHADDR, nếu không trùng thì bản tin DHCP bị loại bỏ, hạn chế tình trạng giả mạo CHADDR.

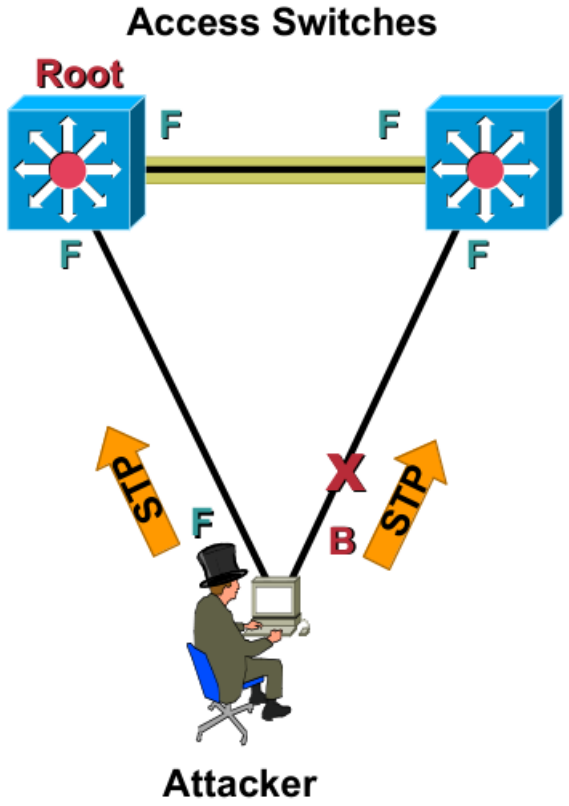


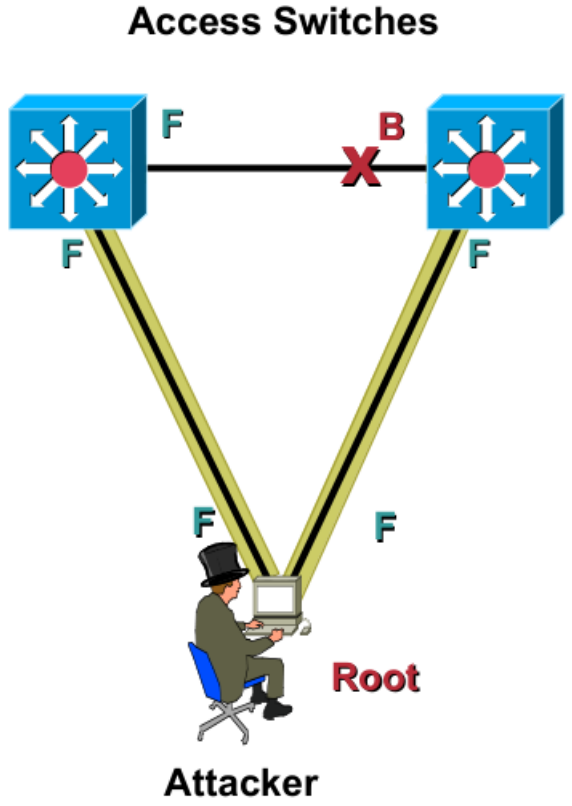



# Kiểu tấn công giao thức STP

- STP là giao thức nhằm bảo đảm dự phòng và chống Loop ở Layer 2, là giao thức được dùng phổ biến.
- Kẻ tấn công có thể giả mạo Switch gửi các bản tin BPDU .

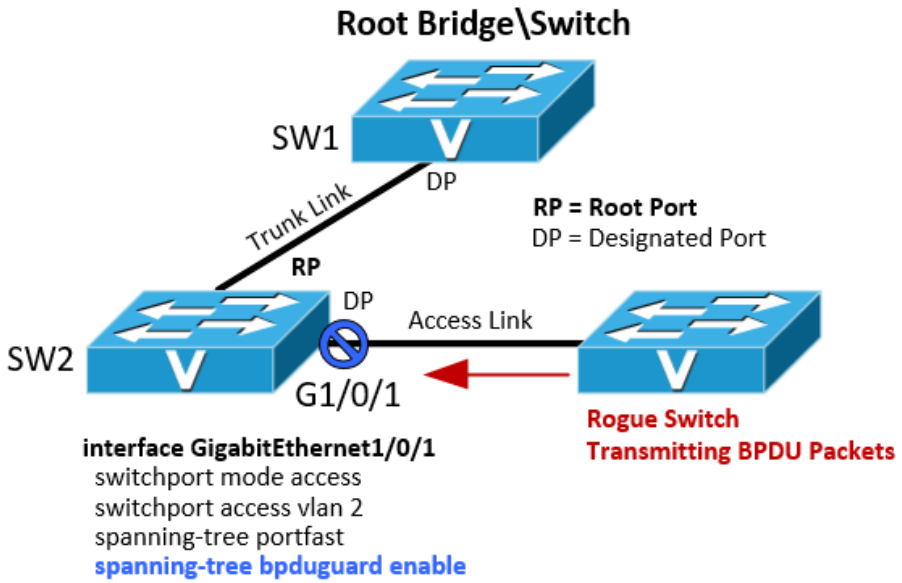


# Cách phòng chống công giao thức STP

- Để phòng chống tấn công STP chúng ta sẽ dùng tính năng Spanning-tree portfast và bpduguard.

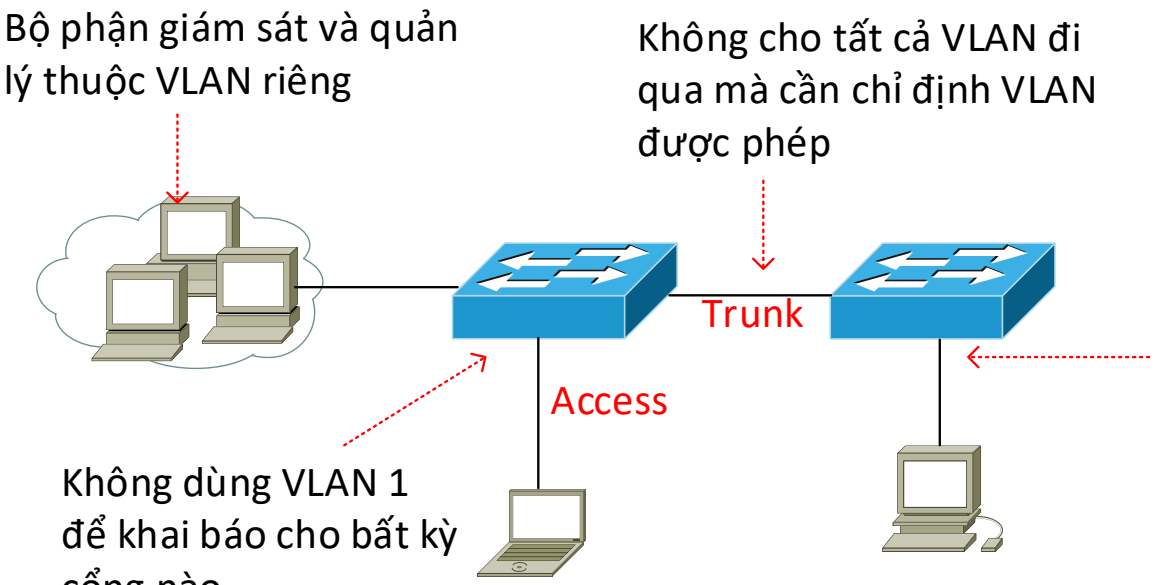



```
SW2(config)# errdisable recovery cause bpduguard
SW2(config)# errdisable recovery interval 30
```

# PHẦN 2
# MỘT SỐ PHƯƠNG ÁN BẢO MẬT KHÁC Ở LAYER 2

# Khuyến cáo chung về khai báo bảo mật

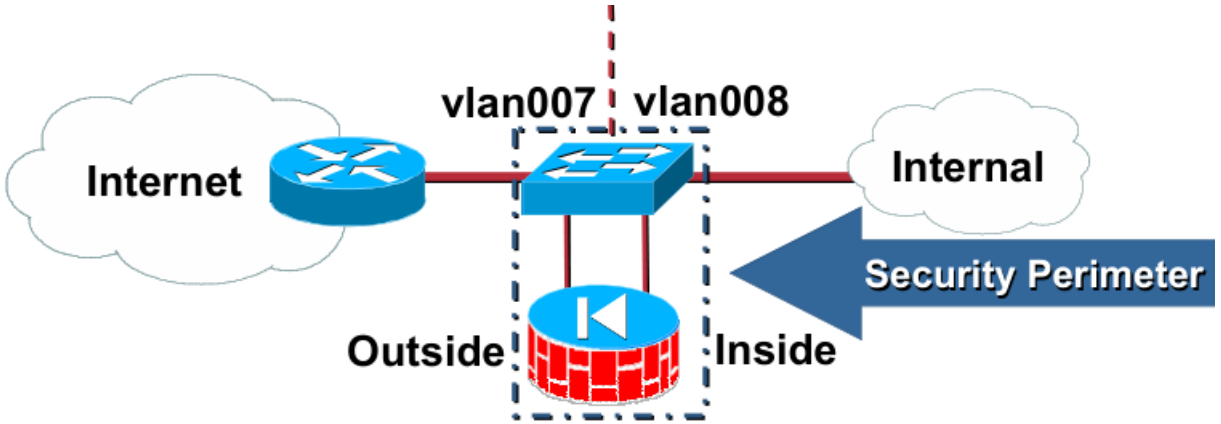
- Đây là những khai báo giúp phòng chống bảo mật ở Layer 2.

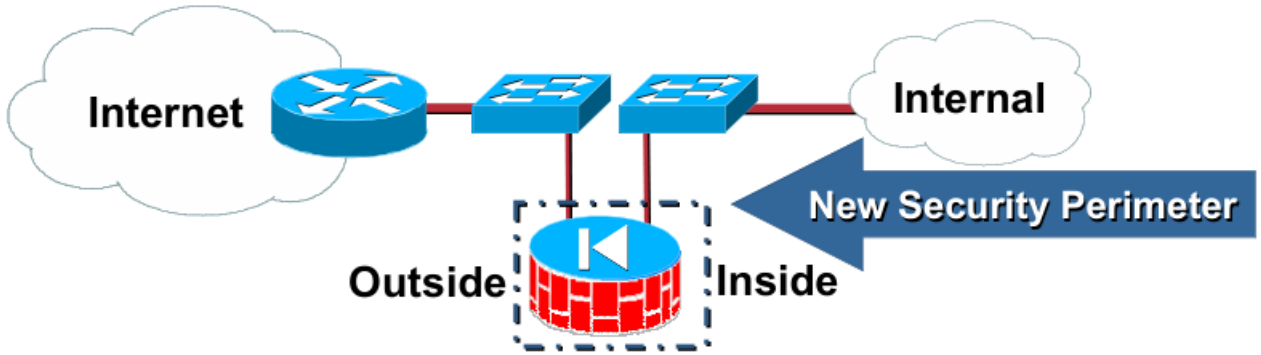



Khai báo cho Port nối với người dùng:
- Port Security
- Portfast & BPDU guard
- Private VLAN (Isolated port)
- DHCP Snooping trusted/ untrusted
- Tắt những Port không dùng

# Khuyến cáo về đấu nối

- Trong trường hợp đấu nối với thiết bị Firewall cần tách vật lý cổng nối bên ngoài và bên trong thay vì dùng VLAN.



VNNIC
Internet for all

.vn
TÊN MIỀN QUỐC GIA VIỆT NAM

VNIX
Viet Nam National Internet eXchange

DNS
National .VN Domain Name System

ASN
Your Net ID

INTERNET SPEED by VNNIC

IP v4 v6
Internet Address

VNIXNOG
VietNam National Internet eXchange
Network Operators Group

VNNIC 2022
INTERNET CONFERENCE
Đà Nẵng
22-25/06/2022

VNNIC
INTERNET ACADEMY

VNNIC
INTERNET ATLAS

Xin trân trọng cám ơn !


**BỘ THÔNG TIN VÀ TRUYỀN THÔNG - TRUNG TÂM INTERNET VIỆT NAM**

**TP. Hà Nội:** Tầng 24, Toà nhà VNTA, Dương Đình Nghệ, Yên Hoà, Cầu Giấy, Hà Nội

**TP. Đà Nẵng:** Lô 21, Đường số 7, KCN An Đồn, Sơn Trà, Đà Nẵng

**TP. Hồ Chí Minh:** Đường số 20, Khu chế xuất Tân Thuận, Quận 7, TP. Hồ Chí Minh

+84 24 3556 4944

webmaster@vnnic.vn

facebook.com/myVNNIC/

https://vnnic.vn/