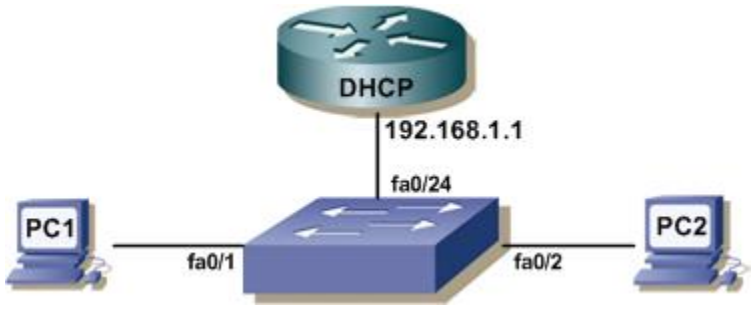
LAB – DHCP Snooping, DAI và IP Source Guard



1. Cấu hình DHCP Snooping

Kích hoạt tính năng DHCP Snooping

```
SW(config)#ip dhcp snooping

SW(config)#no ip dhcp snooping information option

SW(config)#ip dhcp snooping vlan 1

SW(config)#interface fa0/24

SW(config-if)#ip dhcp snooping trust
```

Kiểm tra

Địa chỉ IP được cấp trên Server DHCP

```
DHCP# sh ip dhcp binding
IP address       Hardware address        Lease expiration        Type
192.168.1.3      0100.1bfc.36ec.e4       Mar 02 1993 12:43 AM    Automatic
192.168.1.4      0100.1bfc.36ec.dd       Mar 02 1993 12:43 AM    Automatic
```

Switch xây dựng bảng cơ sở dữ liệu dựa vào thông tin của DHCP Request và Reply

```
Sw#sh ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:1B:FC:36:EC:DD   192.168.1.4      86399       dhcp-snooping   1     FastEthernet0/1
00:1B:FC:36:EC:E4   192.168.1.3      86399       dhcp-snooping   1     FastEthernet0/2
Total number of bindings: 2
```

Thông tin cổng tin cậy

```
Sw#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
DHCP snooping is configured on the following Interfaces:

Insertion of option 82 is disabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted     Rate limit (pps)
-------------------------  -------     ----------------
FastEthernet0/24           yes         unlimited
```

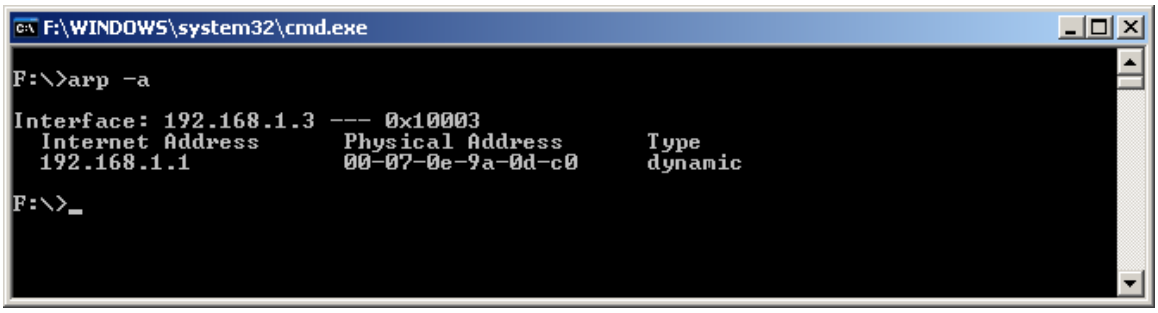
Trong một số trường hợp kẻ tấn công có thể thực hiện DHCP Request với địa chỉ MAC giả, sử dụng hết dãy địa chỉ trên Server DHCP. Và Server DHCP không còn địa chỉ để cấp cho người dùng khác . Để hạn chế DHCP Snooping cho phép giới hạn tốc độ gói Request được gởi

```
SW(config)#interface range fa0/1 - 2

SW(config-if-range)#ip dhcp snooping limit rate 10
```

```
SW#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
DHCP snooping is configured on the following Interfaces:

Insertion of option 82 is disabled
   circuit-id format: vlan-mod-port
    remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted     Rate limit (pps)
------------------------   -------     ----------------
FastEthernet0/1            no          10
FastEthernet0/2            no          10
FastEthernet0/24           yes         unlimited
```

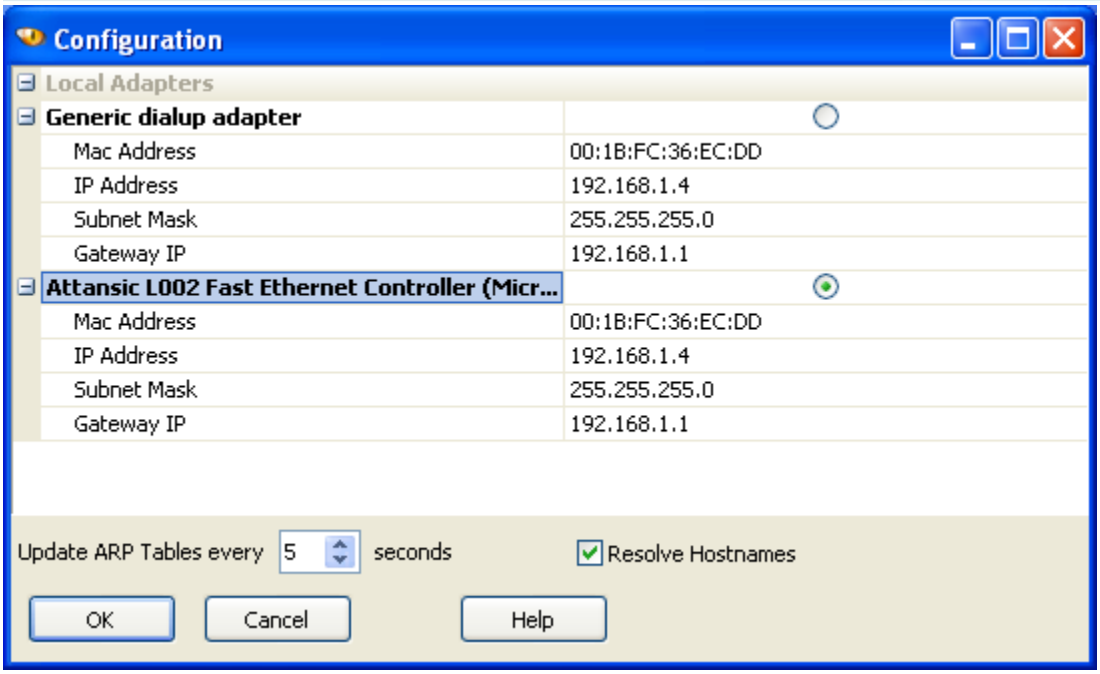
2. Cấu hình Dynamic ARP Inspection

Trạng thái bảng ARP trên PC2



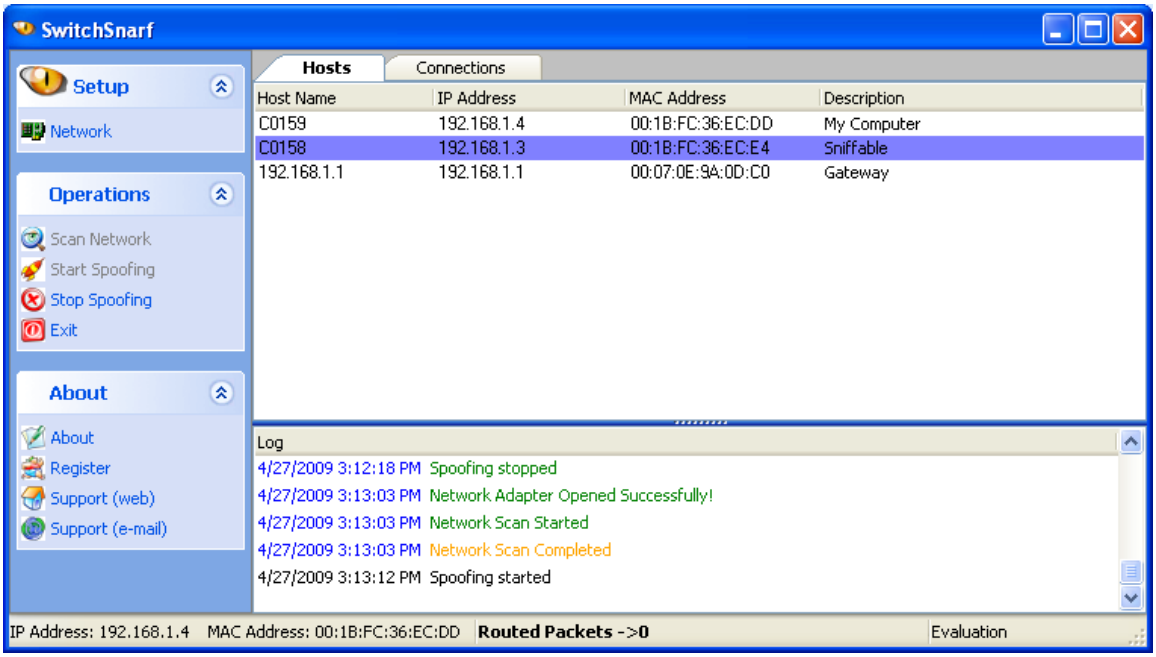
Thực hiện ARP spoofing với ứng dụng **Switchsnarf** trên PC1

Xác định cổng mà gói ARP giả mạo sẽ được gởi

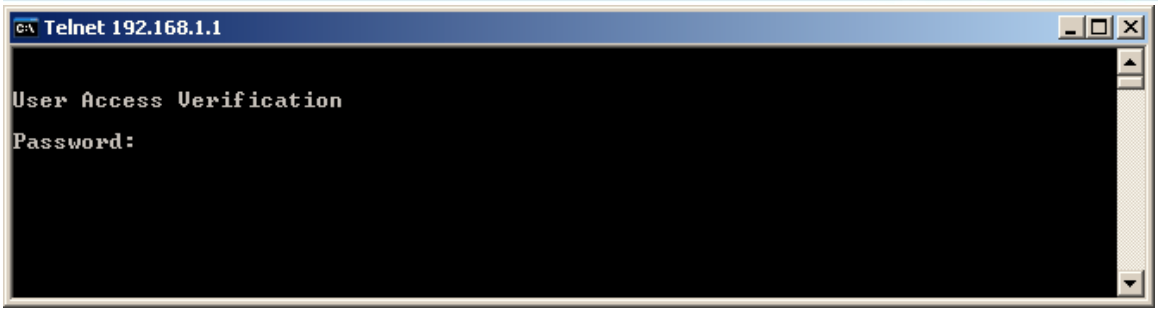


Chọn Scan Network để tìm PC trên mạng

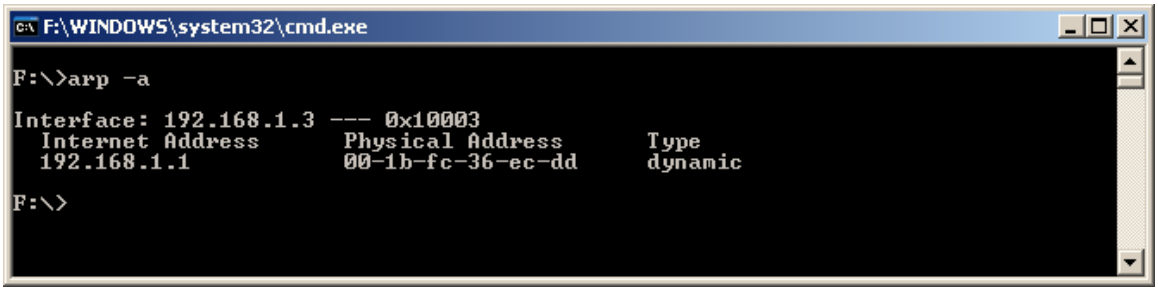
Chọn PC mà có phần **Description** là **Sniffable**, chọn **Start Spoofing**



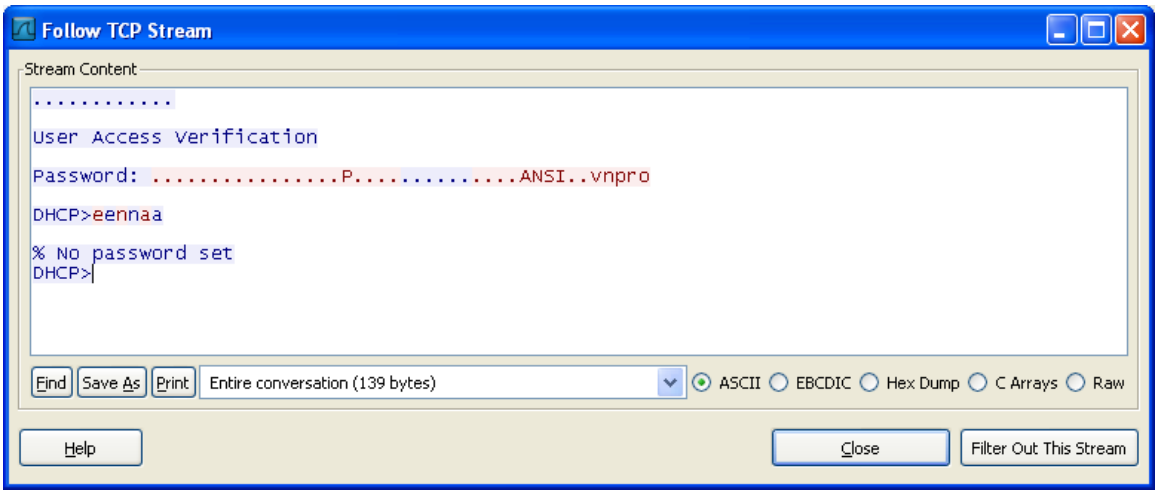
Thực hiện Telnet từ PC2



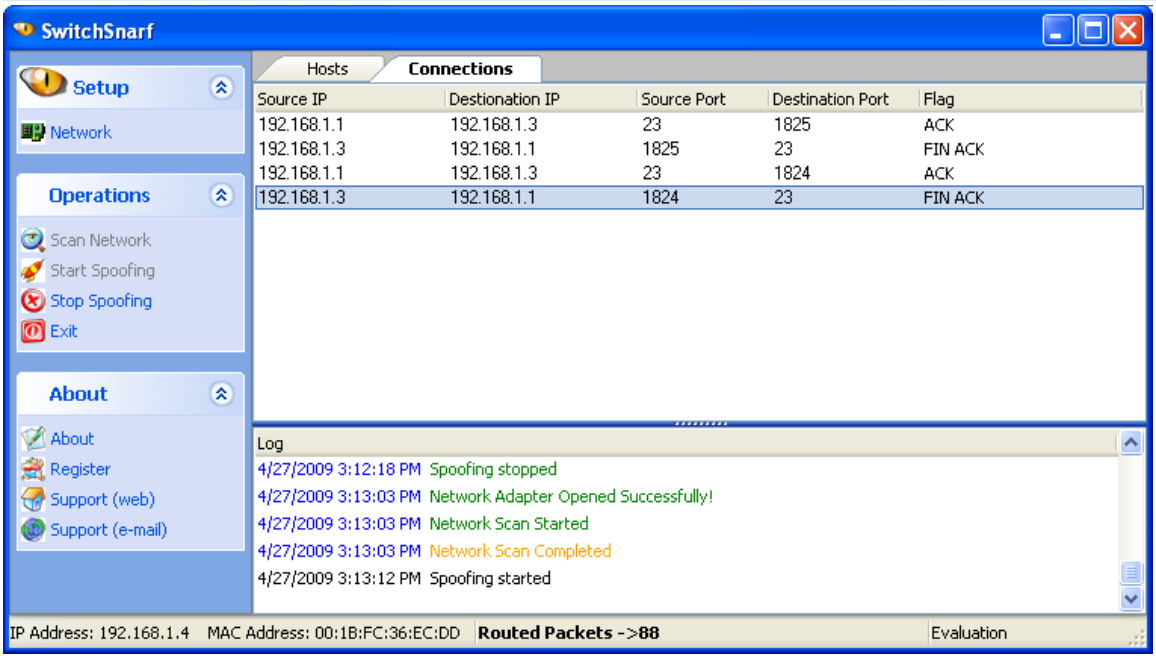
Bảng ARP trên PC2 bị thay đổi



Dùng Wireshark để thực hiện phân tích nội dung gói



Gói Telnet gởi đến PC1 trước khi đến Router



Trong trường hợp nếu DHCP Snooping đã được cấu hình trước đó, bạn chỉ cần xác định VLAN sử dụng tính năng DAI

```
SW(config)#ip arp inspection vlan 1

Xác định cổng tin cậy (tất cả các cổng còn lại là không tin cậy)

SW(config)#interface fa0/24

SW(config-if)#ip arp inspection trust
```

Kiểm tra

Chạy lại ứng dụng **Switchsnarf** trên PC1, thông tin log cho biết gói ARP Reply không hợp lệ bị loại bỏ

*00:54:51: **%SW_DAI-4-DHCP_SNOOPING_DENY**: 1 Invalid ARPs (Res) on Fa0/1, vlan 1.([001b.fc36.ecdd/192.168.1.3/0007.0e9a.0dc0/192.168.1.1/00:54:51 UTC Mon Mar 1 1993])*

*00:54:51: **%SW_DAI-4-DHCP_SNOOPING_DENY**: 1 Invalid ARPs (Res) on Fa0/1, vlan 1.([001b.fc36.ecdd/192.168.1.1/001b.fc36.ece4/192.168.1.3/00:54:51 UTC Mon Mar 1 1993])*

Trong trường hợp nếu như PC2 khai báo địa chỉ tĩnh, Switch sẽ không có thông tin để kiểm tra, bạn có thể xây dựng thông tin tĩnh để kiểm tra sự giả mạo

```
SW(config)#arp access-list ARPINSPECT

SW(config-arp-nacl)#permit ip host 192.168.1.3 mac host 001B.FC36.ECE4

SW(config)#ip arp inspection filter ARPINSPECT vlan 1
```

```
Sw#sh ip arp inspection

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan      Configuration    Operation   ACL Match          Static ACL
 ----      -------------    ---------   ---------          ----------
    1      Enabled          Active      ARPINSPECT         No
```

Mặc định DAI chỉ kiểm sự vi phạm dựa vào nội dung của gói ARP, mà không kiểm tra giá trị của header của gói ARP. Thực hiện câu lệnh sau khi cần kiểm tra thêm giá trị header của gói ARP

```
SW(config)#ip arp inspection validate ?

   dst-mac  Validate destination MAC address

   ip       Validate IP addresses

   src-mac  Validate source MAC address
```

```
Frame 691 (42 bytes on wire, 42 bytes captured)
Ethernet II, Src: AsustekC_36:ec:dd (00:1b:fc:36:ec:dd), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: AsustekC_36:ec:dd (00:1b:fc:36:ec:dd)
  Type: ARP (0x0806)
Address Resolution Protocol (request)
  Hardware type: Ethernet (0x0001)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (0x0001)
  Sender MAC address: AsustekC_36:ec:dd (00:1b:fc:36:ec:dd)
  Sender IP address: 192.168.1.4 (192.168.1.4)
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.1.1 (192.168.1.1)
```

- **Src-mac**: Kiểm tra đại chỉ MAC nguồn trong header Ethernet với địa chỉ MAC của người gởi trong gói ARP Reply
- **Det-mac**: Kiểm tra địa chỉ MAC đích trong Ethernet header với địa chỉ MAC đích trong gói ARP Reply
- **IP**: Kiểm tra địa chỉ IP của người gởi trong tất cả các gói ARP Request, kiểm tra địa chỉ IP của thiết bị gởi với địa chỉ IP đích trong tất cả gói ARP Reply

3. Cấu hình IP Source Guard

Xác định cổng và kích hoạt tính năng IP Source Guard

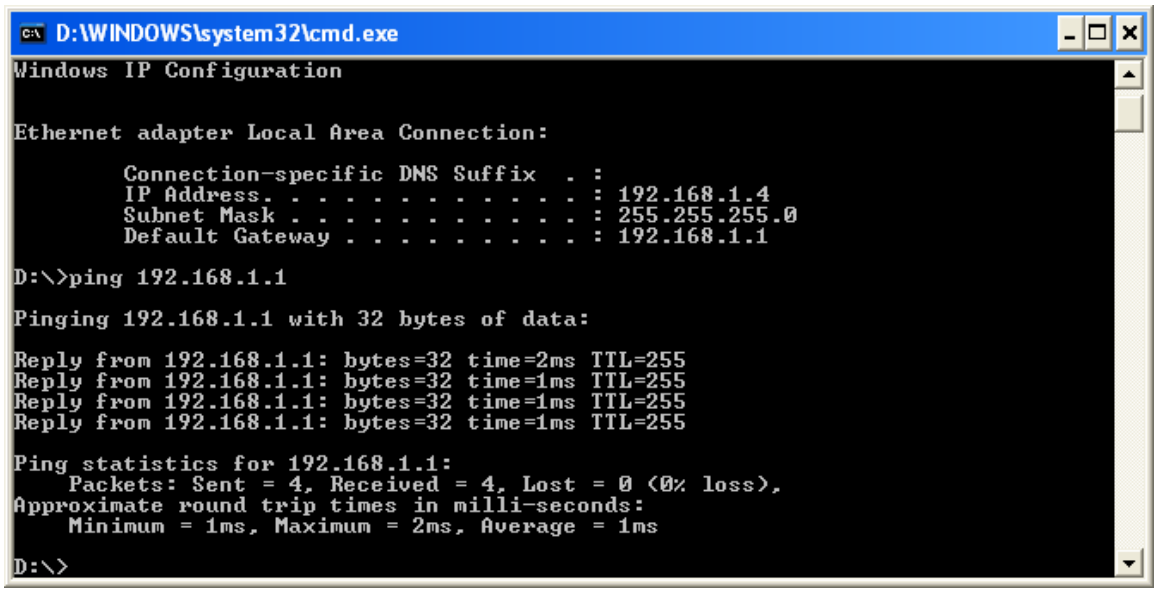
```
SW(config)#interface range fa0/1 - 2

SW(config-if-range)#ip verify source
```

Kiểm tra

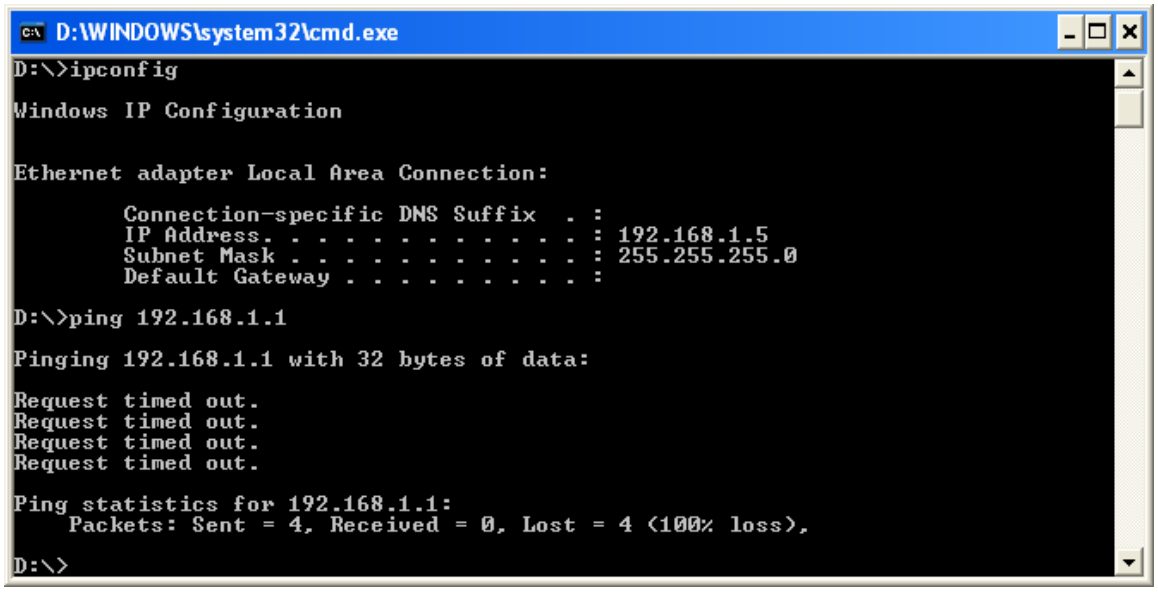
Địa chỉ của gói được nhận trên cổng phải khớp với thông tin có được từ DHCP Snooping

```
Sw#sh ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Fa0/1      ip           active       192.168.1.4                         1
Fa0/2      ip           active       192.168.1.3                         1
```

Thực hiện kiểm tra sự hợp lệ với PC1



Thay đổi địa chỉ bằng cách gán tĩnh trên PC1, gói sẽ bị loại bỏ do không hợp lệ



Trong trường hợp bạn muốn kiểm tra thêm địa chỉ MAC của gói

```
SW(config-if-range)#ip verify source port-security
```

```
Sw#sh ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Fa0/1      ip-mac       active       192.168.1.4      permit-all         1
Fa0/2      ip-mac       active       192.168.1.3      permit-all         1
```

Tuy nhiên trong trường hợp này tất cả địa chỉ MAC lại được cho phép, bạn cần dùng kết hợp với port-security để xác định địa chỉ IP và MAC cụ thể được cho phép

```
SW(config)#interface range fa0/1 - 2

SW(config-if-range)#switchport mode access

SW(config-if-range)#switchport port-security
```

```
Sw#sh ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Fa0/1      ip-mac       active       192.168.1.4      00:1B:FC:36:EC:DD  1
Fa0/2      ip-mac       active       192.168.1.3      00:1B:FC:36:EC:E4  1
```

Trong trường hợp không sử dụng dữ liệu của DHCP Snooping bạn có thể xây dựng dữ liệu tĩnh

```
SW(config)#ip source binding 001B.FC36.ECE4 vlan 1 192.168.1.3 interface
fa0/2
```

```
Sw#sh ip source binding static
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:1B:FC:36:EC:E4   192.168.1.3      infinite    static         1     FastEthernet0/2
Total number of bindings: 1
```