PHỤ LỤC 3

**HƯỚNG DẪN PHÂN TÍCH HOẠT ĐỘNG CỦA GIAO THỨC IP và ARP**

**Mục tiêu:**

Cung cấp cho sinh viên các kỹ năng cơ bản để phân tích hoạt động của giao thức IP và ARP:

* Thiết lập các thông số địa chỉ IP cho máy trạm
* Hiển thị thông tin bảng ánh xạ địa chỉ của giao thức ARP trên máy trạm
* Sử dụng công cụ để quan sát hoạt động của giao thức ARP
* Sử dụng công cụ phân tích gói tin IP

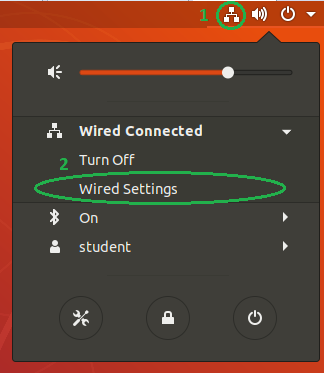
**Môi trường:** Hệ điều hành Ubuntu 18.04

**Nội dung**

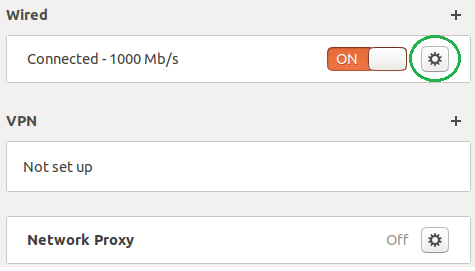
***Lưu ý: Trước khi thực hiện các nội dung thực hành sau đây, nên tắt các ứng dụng mạng đang sử dụng***

**1. Cấu hình các thông số địa chỉ IP cho máy trạm**

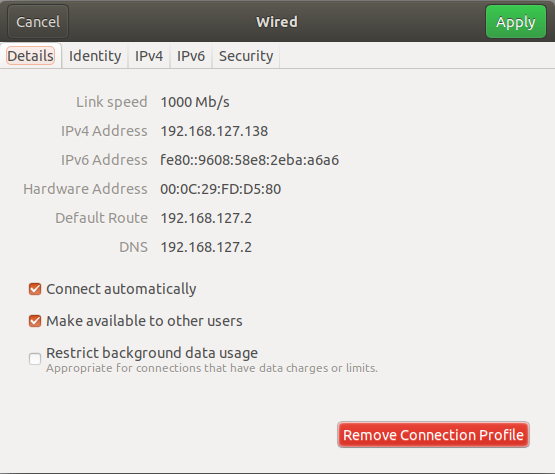
- **Bước 1:** Để không làm gián đoạn kết nối mạng của máy trạm, trước tiên ta tìm xem máy trạm đang sử dụng địa chỉ IP nào.Chọn biểu tượng kết nối mạng ở góc trên bên phải của màn hình. Chọn tiếp mục Wired Settings



- **Bước 2**: Nhấn vào biểu tượng Setting trong mục Wired



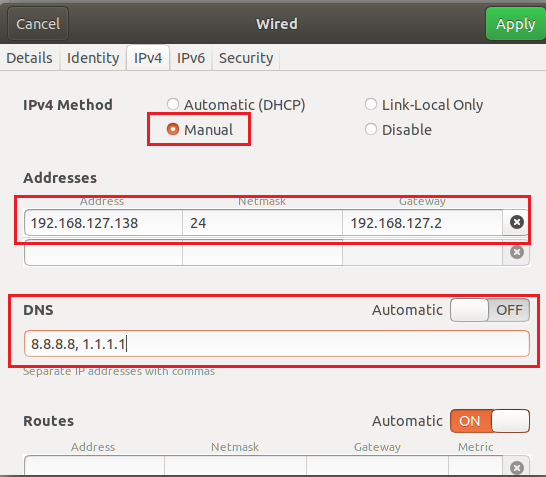
- **Bước 3**: Chúng ta có thể thấy các thông số địa chỉ IP mà máy tính đang sử dụng. Ví dụ minh họa như hình dưới đây.



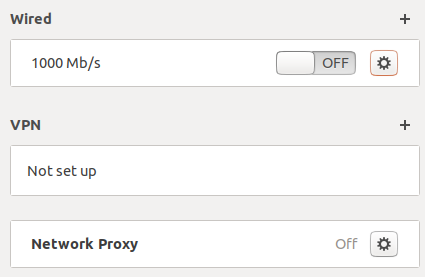
Các thông số này bao gồm:

* IP Address(Địa chỉ IP): 192.168.127.138. Địa chỉ này không kèm mặt nạ mạng nên có thể coi đó là địa chỉ phân lớp. Dễ thấy đây là địa chỉ phân lớp C nên có số bit mặc định của Network ID là 24.
* Default Router (Router mặc định): 192.168.127.2
* DNS (Địa chỉ máy chủ DNS): 192.168.127.2

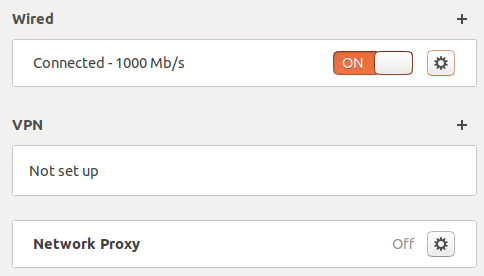
- **Bước 4**: Chọn mục IPv4 của cửa sổ trên và điền các thông số mà chúng ta đã thấy ở bước trên như sau. Nhấn nút Apply sau khi đã thiết lập xong



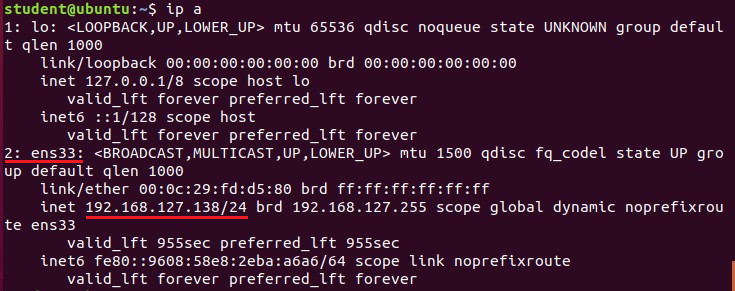
- **Bước 5:** Gạt nút ON/OFF sang vị trí OFF.



Sau đó gạt lại sang vị trí ON để khởi động lại cạc mạng.



- **Bước 6**: Trên cửa sổ Terminal, chúng ta có thể sử dụng lệnh **ip a** để xem thông tin cấu hình địa chỉ IP của máy trạm:



- **Bước 6**: Chúng ta có thể truy cập vào website bất kỳ để kiểm chứng các thiết lập trên là chính xác hay không.

**2. Sử dụng Wireshark để bắt gói tin**

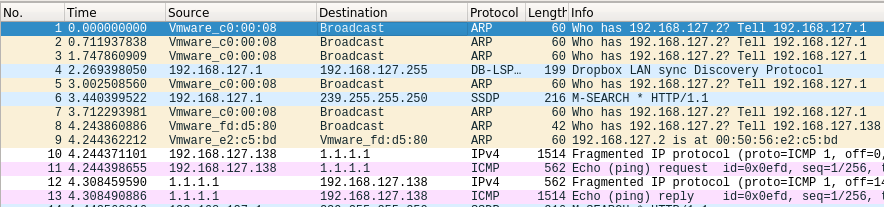
* **Bước 1:** Khởi động công cụ Wireshark từ cửa sổ Terminal với lệnh **sudo wireshark**
* **Bước 3**: Bắt đầu bắt gói tin trên cạc mạng phù họp với Wireshark
* **Bước 4:** Mở cửa sổ Terminal thứ 2 và gõ lệnh sau để xóa bảng ARP Table của máy trạm:



* **Bước 5:** Trên cửa số Terminal thực hiện lệnh ping 1.1.1.1 -s 2000 -c 4 như sau:



Khi lệnh này thực hiện xong, dừng bắt gói tin. Trên cửa sổ của Wireshark, chúng ta sẽ thấy các gói tin tương tự như sau:



* **Bước 6**: Sử dụng lệnh **ip n** để xem thông tin bảng ARP Table



***Lưu ý:***

*- Nếu trên máy học viên không bắt được các gói tin có Protocol là ARP thì nên thực hiện lại từ bước 1.*

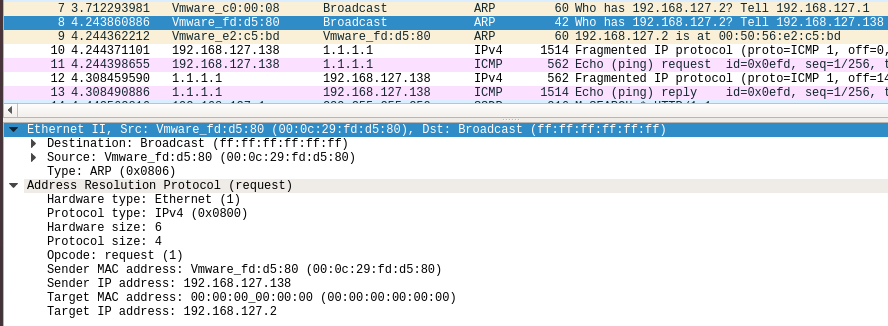
*- Các gói tin bắt được trên máy các bạn có thể sẽ có thông số khác. Điều này là hoàn toàn bình thường và không có ảnh hưởng tới quá trình thực hành*

**3. Phân tích lưu lượng**

*Lưu ý: Các giá trị phân tích dưới đây chỉ mang tính chất minh họa. Với lưu lượng bắt trên máy sinh viên, kết quả có thể sẽ khác. Các bạn có thể download file lưu lượng mẫu tại địa chỉ sau cho nội dung minh họa dưới đây:*

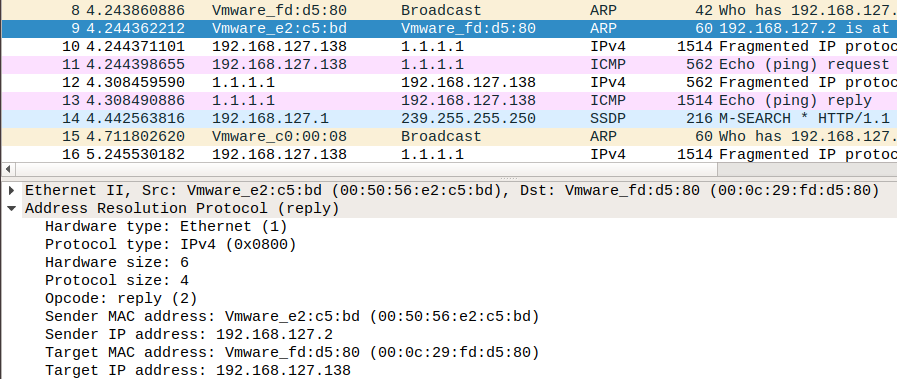
*https://drive.google.com/file/d/1iFg6Y3sk5fS1tC3FdtGHPVPlQhfI3y4Z*

* **Bước 1**: Bạn có thể thấy trên file lưu lượng bắt được một số gói tin có Protocol là ARP và địa chỉ nguồn là địa đích máy của bạn. Mở rộng phần tiêu đề Address Resolution Protocol, chúng ta có thể thấy đây là gói tin ARP Request.

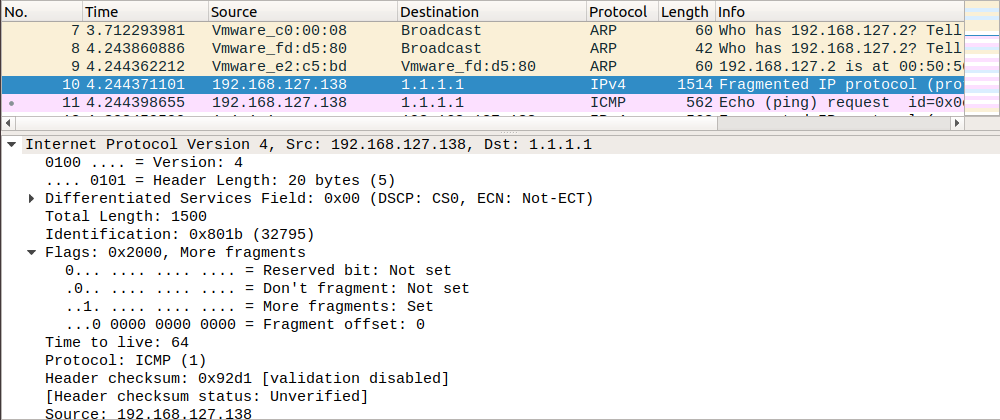


Các thông tin chúng ta đọc được từ phần tiêu đề này gồm có:

* Hardware type: Chuẩn phần cứng sử dụng trong ví dụ này là Ethernet
* Protocol type: giao thức là IPv4
* Hardware size: kích thước phần cứng là 6 byte (địa chỉ MAC)
* Protocol size: địa chỉ giao thức tầng trên là 4 byte
* Sender MAC address: địa chỉ MAC nút nguồn
* Sender IP address: địa chỉ IP của nút nguồn
* Target MAC address: địa chỉ MAC cần tìm kiếm
* Target IP address: địa chỉ IP đã biết
* **Bước 2**: Tiếp theo, bạn sẽ thấy gói tin trả lời là gói tin ARP có địa chỉ đích là địa chỉ MAC máy tính của bạn. Các thông tin trong gói này tương tự ở trên, với điểm khác biệt là địa chỉ Target MAC address đã là địa chỉ cần tìm kiếm. Các bạn có thể thấy rằng, đây cũng chỉ là địa chỉ nguồn của khung tin Ethernet mang theo gói ARP Reply trả lời.

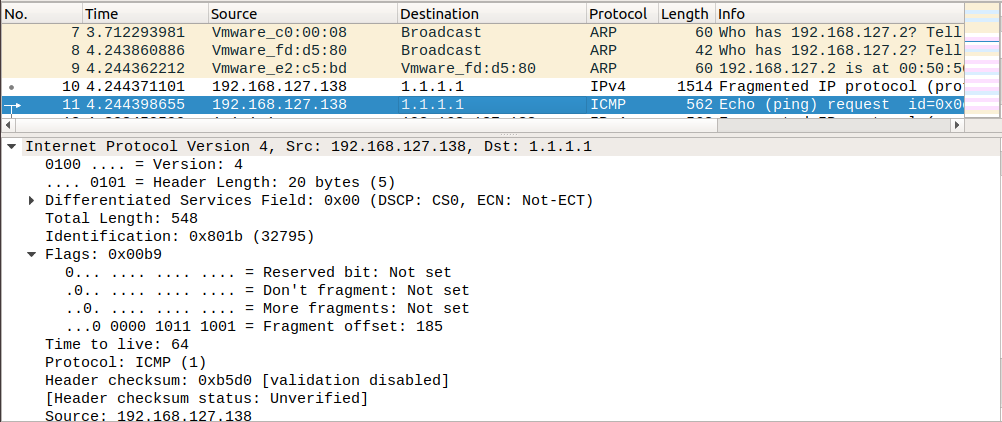


* **Bước 3**: Tìm đến gói tin đầu tiên có địa chỉ nguồn là địa chỉ IP của máy trạm mà chúng ta đã thiết lập ở trên, địa chỉ đích là 1.1.1.1



Mở rộng phần tiêu đề, ta có một số thông tin quan trọng sau:

* Version (phiên bản): 4
* Header Length (kích thước tiêu đề): 20 byte
* Total Length (kích thước cả gói tin): 1500 byte
* Identification: 0x801b
* Flags:
* Don’t fragment: gói tin được phép phân mảnh (giá trị là 0)
* Mỏe fragments: còn các mảnh khác (giá trị là 1)
* Fragment offset = 0 cho thấy đây là mảnh đầu tiên của một gói tin bị phân mảnh
* Time to live: 64
* **Bước 4**: Chọn gói tin thứ hai có địa chỉ nguồn là địa chỉ IP của máy trạm mà chúng ta đã thiết lập ở trên, địa chỉ đích là 1.1.1.1



Mở rộng phần tiêu đề, ta có một số thông tin quan trọng tương tự gói tin trước. Chúng ta chú ý vào các trường sau:

* Identification: 0x801b trùng với gói trên. Như vậy đây là một mảnh cùng một gói tin với mảnh trên.
* Flags:
* Don’t fragment: gói tin được phép phân mảnh (giá trị là 0)
* More fragments: không còn các mảnh khác (giá trị là 0)
* Fragment offset = 185 cho thấy đây là mảnh tiếp theo

**Kết luận**

Với nội dung mà các bạn vừa thực hiện, các bạn đã làm quen được với cách thiết lập các thông số địa chỉ IP cho các máy trạm và phân tích được khuôn dạng gói tin IP, cũng như hoạt động của giao thức ARP.