**BÀI THỰC HÀNH 1**

**I. Mở Wireshark và chọn giao diện mạng**

1. Mở Wireshark.
2. Chọn giao diện mạng đang sử dụng (Ethernet hoặc Wi-Fi).
3. Nhấn Start để bắt gói tin.

Sau khi lọc được các gói tin, ta có hình ảnh bắt được các gói tin Ethernet như sau:

**A screenshot of a computer

AI-generated content may be incorrect.**

**II. Chụp ảnh 1 gói tin hoàn chỉnh và đánh dấu các trường quan trọng.**

**Sau đây ảnh là 1 gói tin hoàn chỉnh**

A screenshot of a computer

AI-generated content may be incorrect.

Đánh dấu các trường quan trọng

* Địa chỉ MAC đích (Destination MAC): **58:ce:2a:68:83:d7**. o Chức năng: Xác định thiết bị nhận gói tin trong mạng LAN.
* Địa chỉ MAC nguồn (Source MAC): **cc:71:90:6d:db:24.**
  + Chức năng: Xác định thiết bị gửi gói tin.
* EtherType: 0x0800 (IPv4).
* Chức năng: Cho biết loại giao thức bên trong gói tin, ở đây là IPv4.

Trả lời các câu hỏi:

Câu 1: Địa chỉ MAC nguồn và đích trong gói tin của Anh/Chị là gì?

Ethernet II (Lớp liên kết dữ liệu - Layer 2)

* Địa chỉ MAC nguồn (Src MAC):**VietnamPostA\_6d:db:24 (cc:71:90:6d:db:24)**
* Địa chỉ MAC đích (Dst MAC): **58:ce:2a:68:83:d7**
* Ý nghĩa: Gói tin này đang được truyền từ **cc:71:90:6d:db:24 đến 58:ce:2a:68:83:d7**

Câu 2. Gói tin này sử dụng giao thức nào ở tầng trên (IPv4, IPv6, ARP,...)?

Gói tin này sử dụng giao thức:

* EtherType: 0x0800 (IPv4)

Câu 3. Có trường Padding không? Nếu có, nó có tác dụng gì?

Dựa vào hình ảnh Wireshark, ta thấy tổng độ dài của gói tin là 52 bytes. Trong đó:

* Ethernet Header: 14 bytes
* IPv4 Header: 20 bytes
* TCP Header: 20 bytes
* Payload (Dữ liệu): 0 bytes (ACK, không chứa dữ liệu)

Do tổng dữ liệu không nhỏ hơn 46 bytes, nên gói tin này không có trường Padding.

Trong trường hợp gói tin có Payload < 46 bytes, Ethernet yêu cầu tổng độ dài tối thiểu 64 bytes (bao gồm cả Ethernet Header và CRC) để tránh lỗi. Nếu không đủ, Padding sẽ được thêm vào:

Đảm bảo frame Ethernet đạt đủ kích thước tối thiểu 64 bytes, tránh bị loại bỏ trên mạng.

Giúp card mạng xử lý chính xác gói tin, tránh lỗi trong quá trình truyền tải.

Không ảnh hưởng đến dữ liệu, vì Padding chỉ chứa các byte rỗng (0x00) và không được xử lý bởi tầng trên.

Câu 4. Kiểm tra CRC của gói tin có hợp lệ không?

Sau khi kiểm tra CRC thì không có gói tin nào bị lỗi, CRC hợp lệ.

**BÀI THỰC HÀNH 2**

**I. Chọn frame đầu tiên của giao thức ARP, quan sát chi tiết nội dung frame và trả lời các câu hỏi sau:**

# a) Đây là frame đầu tiên của giao thức ARP

A screenshot of a computer

AI-generated content may be incorrect.

1. **Địa chỉ đích (Target - Máy nhận ARP Request)**
   * MAC Address**:** ff:ff:ff:ff:ff:ff
   * NIC Manufacturer**:** Không có (Vì đây là địa chỉ Broadcast)
   * NIC Serial Number**:** Không có
2. **Địa chỉ nguồn (Sender - Máy gửi ARP Request)**
   * MAC Address**:** 58:ce:2a:68:83:d7
   * NIC Manufacturer: Intel Corporation (Dựa trên phần đầu MAC 58:ce:2a)
   * NIC Serial Number: 68:83:d7 (phần còn lại của địa chỉ MAC)

**II. Chọn frame thứ hai của giao thức ARP hiển thị ở cửa sổ Packet List, hãy trả lời các câu hỏi sau:**

# b) Đây là frame thứ hai của giao thức ARP hiển thị ở cửa sổ Packet List

A screenshot of a computer

AI-generated content may be incorrect.

1. **Địa chỉ MAC đích:** 
   * MAC Address: ff:ff:ff:ff:ff:ff (Broadcast)
   * NIC Manufacturer: Broadcast không thuộc về nhà sản xuất cụ thể.
   * NIC Serial Number: Không áp dụng.
2. **Địa chỉ MAC nguồn:** 
   * MAC Address: 58:ce:2a:68:83:d7
   * NIC Manufacturer: Intel Corporation (Dựa trên phần đầu MAC 58:ce:2a)
   * NIC Serial Number: 68:83:d7 (phần còn lại của địa chỉ MAC)

Bài tập: thực hiện lệnh ping đến một server ngoài Internet đồng thời bắt gói (chẳng hạn www.uneti.edu.vn). Dựa vào việc thu thập thông tin trong các gói tin bắt được có thể biết được địa chỉ MAC của server này không? Tại sao?

A computer screen with white text

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Khi thực hiện lệnh ping đến một server ngoài Internet, chẳng hạn www.uneti.edu.vn, và bắt gói tin bằng Wireshark, ta không thể xác định được địa chỉ MAC của server đó. Điều này xuất phát từ cách hoạt động của giao thức ICMP và nguyên tắc truyền dữ liệu trên mạng.

Giao thức ICMP hoạt động ở lớp 3 (Network Layer - IP) của mô hình OSI. Khi một gói tin ICMP Echo Request được gửi từ máy tính đến địa chỉ IP của server, server sẽ phản hồi bằng gói tin ICMP Echo Reply. Tuy nhiên, địa chỉ MAC chỉ có ý nghĩa trong phạm vi mạng LAN, giúp các thiết bị trong cùng một mạng nhận diện và giao tiếp với nhau. Khi gói tin rời khỏi mạng nội bộ để đi qua Internet, nó phải đi qua router (gateway). Router sẽ thay đổi địa chỉ MAC của gói tin để chuyển tiếp đến bước tiếp theo trong hành trình của nó, nhưng vẫn giữ nguyên địa chỉ IP đích.

Trong dữ liệu bắt được bằng Wireshark, địa chỉ MAC đích không phải của server mà là của router/gateway của nhà cung cấp dịch vụ mạng (ISP). Điều này cho thấy Wireshark chỉ có thể hiển thị địa chỉ MAC của thiết bị mạng gần nhất trong phạm vi mạng LAN của người dùng. Vì vậy, dù có bắt được các gói tin ICMP trao đổi với server, ta vẫn không thể xác định được địa chỉ MAC thực sự của server đó.