

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC BÁCH KHOA
KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH



MẠNG MÁY TÍNH TN (CO3094)

LAB 6

Wireshark: Ethernet và ARP v8.0

HK: 241 - LỚP: L09

GVHD: Bùi Xuân Giang

Sinh viên thực hiện

Nguyễn Tấn Tài : 2212990

Thành phố Hồ Chí Minh, tháng 11 năm 2024

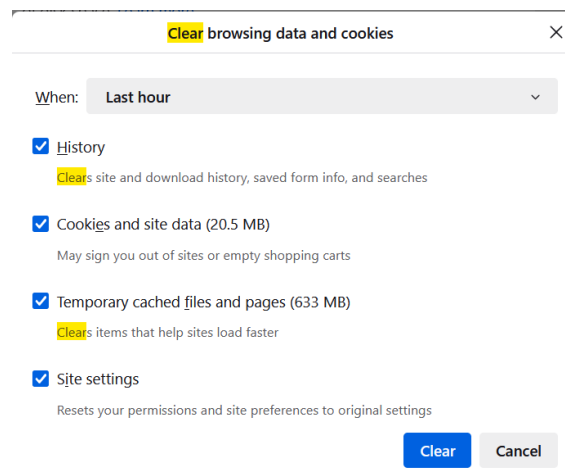
Ethernet và ARP v8.0

Trong thí nghiệm này, chúng ta sẽ điều tra giao thức Ethernet và giao thức ARP. Trước khi bắt đầu phòng thí nghiệm này, nên xem lại các phần 6.4.1 (Định địa chỉ lớp liên kết và ARP) và 6.4.2 (Ethernet) trong sách giáo khoa. RFC 826 ([link](#)) chứa các chi tiết chi tiết về giao thức ARP, được sử dụng bởi một thiết bị IP để xác định địa chỉ IP của một giao diện từ xa mà địa chỉ Ethernet của nó đã được biết.

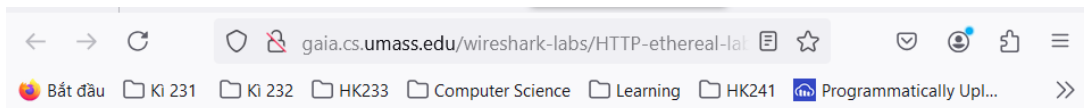
1. Thu thập và phân tích các khung Ethernet

Hãy bắt đầu bằng cách thu một tập hợp các khung Ethernet để nghiên cứu. Thực hiện các bước sau:

- Trước tiên, hãy đảm bảo rằng bộ nhớ đệm của trình duyệt của bạn đã được xóa. Để thực hiện việc này trong Mozilla Firefox V3, chọn Tools -> Clear Recent History và đánh dấu vào ô Cache. Đối với Internet Explorer, chọn Tools -> Internet Options -> Delete Files. Bắt đầu Wireshark để thu gói tin.



- Nhập URL sau vào trình duyệt của bạn: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>. Trình duyệt của bạn sẽ hiển thị một văn bản khá dài của Tuyên Ngôn Quyền Lợi Hoa Kỳ.



THE BILL OF RIGHTS

Amendments 1-10 of the Constitution

The Conventions of a number of the States having, at the time of adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added, and as extending the ground of public confidence in the Government will best insure the beneficent ends of its institution;

Resolved, by the Senate and House of Representatives of the United States of America, in Congress assembled, two-thirds of both Houses concurring, that the following articles be proposed to the Legislatures of the several States, as amendments to the Constitution of the United States; all or any of which articles, when ratified by three-fourths of the said Legislatures, to be valid to all intents and purposes as part of the said Constitution, namely:

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment II

A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed.

Amendment III

No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.

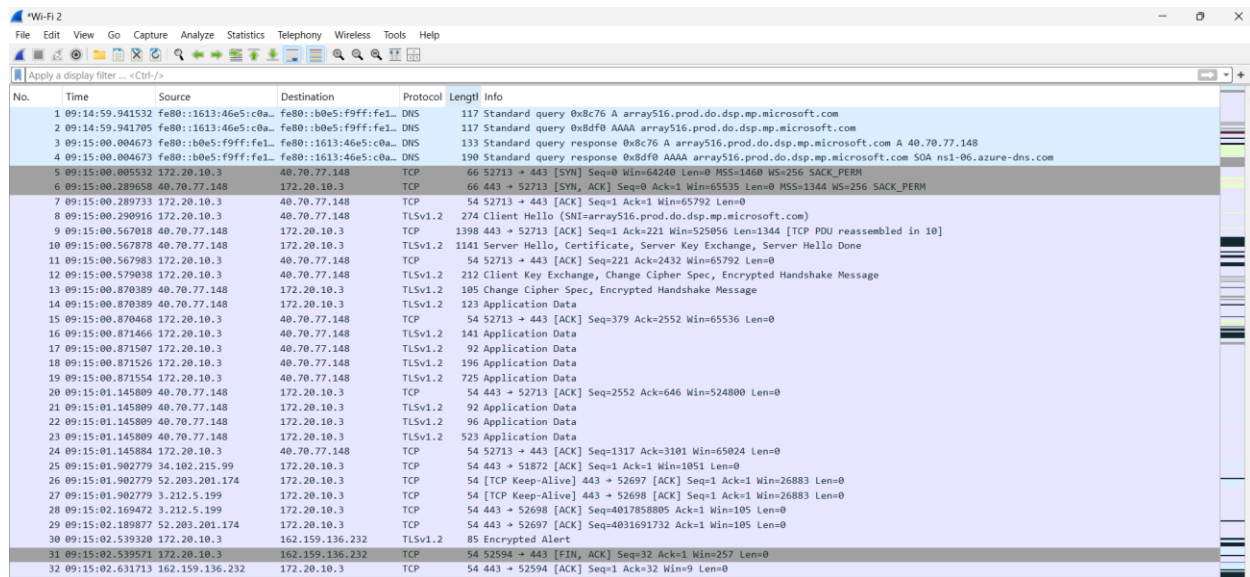
Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Amendment V

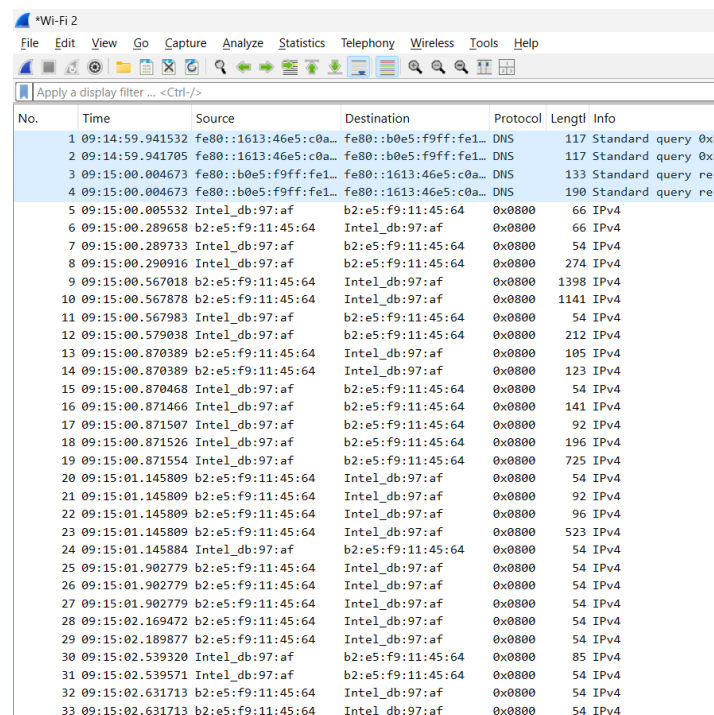
No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

- Dừng Wireshark khi hoàn tất thu gói tin. Đầu tiên, tìm số thứ tự gói tin (cột ngoài cùng bên trái trong cửa sổ Wireshark) của thông điệp HTTP GET được gửi từ máy tính của bạn tới gaia.cs.umass.edu, cũng như phần đầu của thông điệp phản hồi HTTP được gửi tới máy tính của bạn bởi gaia.cs.umass.edu. Màn hình của bạn sẽ trông giống như hình dưới đây (gói tin số 4 trong ảnh chụp màn hình bên dưới chứa thông điệp HTTP GET).



No.	Time	Source	Destination	Protocol	Length	Info
1	09:14:59.941532	fe80::1613:46e5:c0a...	fe80::b0e5:f9ff:fe1...	DNS	117	Standard query 0x8c76 A array516.prod.do.dsp.mp.microsoft.com
2	09:14:59.941705	fe80::1613:46e5:c0a...	fe80::b0e5:f9ff:fe1...	DNS	117	Standard query 0x8df0 AAAA array516.prod.do.dsp.mp.microsoft.com
3	09:15:00.004673	fe80::b0e5:f9ff:fe1...	fe80::1613:46e5:c0a...	DNS	133	Standard query response 0x8c76 A array516.prod.do.dsp.mp.microsoft.com A 40.70.77.148
4	09:15:00.004673	fe80::b0e5:f9ff:fe1...	fe80::1613:46e5:c0a...	DNS	190	Standard query response 0x8df0 AAAA array516.prod.do.dsp.mp.microsoft.com SOA ns1-06.azure-dns.com
5	09:15:00.005532	172.20.10.3	40.70.77.148	TCP	66	52713 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
6	09:15:00.289658	40.70.77.148	172.20.10.3	TCP	66	443 → 52713 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1344 WS=256 SACK_PERM
7	09:15:00.289733	172.20.10.3	40.70.77.148	TCP	54	52713 → 443 [ACK] Seq=1 Ack=1 Win=65792 Len=0
8	09:15:00.290916	172.20.10.3	40.70.77.148	TLSv1.2	274	Client Hello (SHI=array516.prod.do.dsp.mp.microsoft.com)
9	09:15:00.567018	40.70.77.148	172.20.10.3	TCP	1398	443 → 52713 [ACK] Seq=1 Ack=221 Win=525056 Len=1344 [TCP PDU reassembled in 10]
10	09:15:00.567878	40.70.77.148	172.20.10.3	TLSv1.2	1141	Server Hello, Certificate, Server Key Exchange, Server Hello Done
11	09:15:00.567983	172.20.10.3	40.70.77.148	TCP	54	52713 → 443 [ACK] Seq=221 Ack=2432 Win=65792 Len=0
12	09:15:00.579038	172.20.10.3	40.70.77.148	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
13	09:15:00.870389	40.70.77.148	172.20.10.3	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
14	09:15:00.870389	40.70.77.148	172.20.10.3	TLSv1.2	123	Application Data
15	09:15:00.870468	172.20.10.3	40.70.77.148	TCP	54	52713 → 443 [ACK] Seq=379 Ack=2552 Win=65536 Len=0
16	09:15:00.871466	172.20.10.3	40.70.77.148	TLSv1.2	141	Application Data
17	09:15:00.871507	172.20.10.3	40.70.77.148	TLSv1.2	92	Application Data
18	09:15:00.871526	172.20.10.3	40.70.77.148	TLSv1.2	196	Application Data
19	09:15:00.871554	172.20.10.3	40.70.77.148	TLSv1.2	725	Application Data
20	09:15:01.145809	40.70.77.148	172.20.10.3	TCP	54	443 → 52713 [ACK] Seq=2552 Ack=646 Win=524800 Len=0
21	09:15:01.145809	40.70.77.148	172.20.10.3	TLSv1.2	92	Application Data
22	09:15:01.145809	40.70.77.148	172.20.10.3	TLSv1.2	96	Application Data
23	09:15:01.145809	40.70.77.148	172.20.10.3	TLSv1.2	523	Application Data
24	09:15:01.145884	172.20.10.3	40.70.77.148	TCP	54	52713 → 443 [ACK] Seq=1317 Ack=3101 Win=65024 Len=0
25	09:15:01.902779	34.102.215.99	172.20.10.3	TCP	54	443 → 51872 [ACK] Seq=1 Ack=1 Win=1051 Len=0
26	09:15:01.902779	52.203.201.174	172.20.10.3	TCP	54	[TCP Keep-Alive] 443 → 52697 [ACK] Seq=1 Ack=1 Win=26883 Len=0
27	09:15:01.902779	3.212.5.199	172.20.10.3	TCP	54	[TCP Keep-Alive] 443 → 52698 [ACK] Seq=1 Ack=1 Win=26883 Len=0
28	09:15:02.169472	3.212.5.199	172.20.10.3	TCP	54	443 → 52698 [ACK] Seq=401785800 Ack=1 Win=105 Len=0
29	09:15:02.189877	52.203.201.174	172.20.10.3	TCP	54	443 → 52697 [ACK] Seq=4031691732 Ack=1 Win=105 Len=0
30	09:15:02.539320	172.20.10.3	162.159.136.232	TLSv1.2	85	Encrypted Alert
31	09:15:02.539571	172.20.10.3	162.159.136.232	TCP	54	52594 → 443 [FIN, ACK] Seq=32 Ack=1 Win=257 Len=0
32	09:15:02.631713	162.159.136.232	172.20.10.3	TCP	54	443 → 52594 [ACK] Seq=1 Ack=32 Win=9 Len=0

Vì thí nghiệm này tập trung vào Ethernet và ARP, chúng ta không quan tâm đến các giao thức IP hoặc lớp cao hơn. Hãy thay đổi Wireshark để chỉ hiển thị thông tin về các giao thức bên dưới IP. Để làm việc này, chọn Analyze -> Enabled Protocols. Sau đó bỏ chọn hộp IP và nhấn OK. Bạn sẽ thấy cửa sổ Wireshark trông như sau:



No.	Time	Source	Destination	Protocol	Length	Info
1	09:14:59.941532	fe80::1613:46e5:c0a...	fe80::b0e5:f9ff:fe1...	DNS	117	Standard query 0x8c76 A array516.prod.do.dsp.mp.microsoft.com
2	09:14:59.941705	fe80::1613:46e5:c0a...	fe80::b0e5:f9ff:fe1...	DNS	117	Standard query 0x8df0 AAAA array516.prod.do.dsp.mp.microsoft.com
3	09:15:00.004673	fe80::b0e5:f9ff:fe1...	fe80::1613:46e5:c0a...	DNS	133	Standard query response 0x8c76 A array516.prod.do.dsp.mp.microsoft.com A 40.70.77.148
4	09:15:00.004673	fe80::b0e5:f9ff:fe1...	fe80::1613:46e5:c0a...	DNS	190	Standard query response 0x8df0 AAAA array516.prod.do.dsp.mp.microsoft.com SOA ns1-06.azure-dns.com
5	09:15:00.005532	Intel_db:97:af	b2:e5:f9:11:45:64	IPv4	66	IPv4
6	09:15:00.289658	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	66	IPv4
7	09:15:00.289733	Intel_db:97:af	b2:e5:f9:11:45:64	IPv4	54	IPv4
8	09:15:00.290916	Intel_db:97:af	b2:e5:f9:11:45:64	IPv4	274	IPv4
9	09:15:00.567018	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	1398	IPv4
10	09:15:00.567878	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	1141	IPv4
11	09:15:00.567983	Intel_db:97:af	b2:e5:f9:11:45:64	IPv4	54	IPv4
12	09:15:00.579038	Intel_db:97:af	b2:e5:f9:11:45:64	IPv4	212	IPv4
13	09:15:00.870389	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	105	IPv4
14	09:15:00.870389	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	123	IPv4
15	09:15:00.870468	Intel_db:97:af	b2:e5:f9:11:45:64	IPv4	54	IPv4
16	09:15:00.871466	Intel_db:97:af	b2:e5:f9:11:45:64	IPv4	141	IPv4
17	09:15:00.871507	Intel_db:97:af	b2:e5:f9:11:45:64	IPv4	92	IPv4
18	09:15:00.871526	Intel_db:97:af	b2:e5:f9:11:45:64	IPv4	196	IPv4
19	09:15:00.871554	Intel_db:97:af	b2:e5:f9:11:45:64	IPv4	725	IPv4
20	09:15:01.145809	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	54	IPv4
21	09:15:01.145809	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	92	IPv4
22	09:15:01.145809	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	96	IPv4
23	09:15:01.145809	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	523	IPv4
24	09:15:01.145884	Intel_db:97:af	b2:e5:f9:11:45:64	IPv4	54	IPv4
25	09:15:01.902779	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	54	IPv4
26	09:15:01.902779	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	54	IPv4
27	09:15:01.902779	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	54	IPv4
28	09:15:02.169472	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	54	IPv4
29	09:15:02.189877	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	54	IPv4
30	09:15:02.539320	Intel_db:97:af	b2:e5:f9:11:45:64	IPv4	85	IPv4
31	09:15:02.539571	Intel_db:97:af	b2:e5:f9:11:45:64	IPv4	54	IPv4
32	09:15:02.631713	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	54	IPv4
33	09:15:02.631713	b2:e5:f9:11:45:64	Intel_db:97:af	IPv4	54	IPv4

Để trả lời các câu hỏi sau, bạn sẽ cần xem chi tiết gói tin và nội dung của khung Ethernet (cửa sổ hiển thị chi tiết và nội dung gói tin ở giữa và dưới của Wireshark).

Chọn khung Ethernet chứa thông điệp HTTP GET. (Lưu ý rằng thông điệp HTTP GET được chứa bên trong một đoạn TCP, đoạn này được chứa trong một datagram IP, datagram IP được chứa trong một khung Ethernet; nếu bạn thấy cấu trúc này hơi phức tạp, hãy xem lại phần 1.5.2 trong sách giáo khoa). Mở rộng thông tin Ethernet II trong cửa sổ chi tiết gói tin. Lưu ý rằng nội dung của khung Ethernet (cả phần tiêu đề và phần tải) được hiển thị trong cửa sổ nội dung gói tin.

Trả lời các câu hỏi sau, dựa trên nội dung của khung Ethernet chứa thông điệp HTTP GET:

Câu 1: Địa chỉ Ethernet 48-bit của máy tính của bạn là gì?

```

[Capturing rule string: http || tcp.port == 80 || !tcp2]
Ethernet II, Src: Intel_db:97:af (00:93:37:db:97:af), Dst: b2:e5:f9:11:45:64 (b2:e5:f9:11:45:64)
Destination: b2:e5:f9:11:45:64 (b2:e5:f9:11:45:64)
.... 1. .... = LG bit: Locally administered address (this is NOT the factory default)
.... 0 .... = IG bit: Individual address (unicast)
Source: Intel_db:97:af (00:93:37:db:97:af)
.... 0. .... = LG bit: Globally unique address (factory default)
.... 0 .... = IG bit: Individual address (unicast)
Type: IPv6 (0x86dd)
[Stream index: 0]
Internet Protocol Version 6, Src: 2401:d800:9d1:bf47:7c07:9908:6990:3290, Dst: 2402:800:6353:1::7dea:334b
0110 .... = Version: 6
.... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... 0000 00.. .... = Differentiated Services Codepoint: Default (0)
.... ..00 .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
.... 0111 0111 0101 0001 0011 = Flow Label: 0x77513
Payload Length: 175
Next Header: TCP (6)
Hop Limit: 64
Source Address: 2401:d800:9d1:bf47:7c07:9908:6990:3290
[Address Space: Global Unicast]
Destination Address: 2402:800:6353:1::7dea:334b
[Address Space: Global Unicast]
[Stream index: 11]

```

Trong phần Ethernet II của gói tin HTTP GET, trường Source sẽ là địa chỉ MAC của máy tính. Trong ảnh, địa chỉ này là b2:e5:f9:11:45:64.

Câu 2: Địa chỉ đích 48-bit trong khung Ethernet là gì? Đây có phải là địa chỉ Ethernet của gaia.cs.umass.edu không? (Gợi ý: câu trả lời là không). Thiết bị nào có địa chỉ Ethernet này? [Lưu ý: đây là một câu hỏi quan trọng, và đôi khi sinh viên trả lời sai. Xem lại trang 468-469 trong sách giáo khoa và đảm bảo bạn hiểu rõ câu trả lời ở đây.]

Trường Destination trong phần Ethernet II của gói tin HTTP GET không phải là địa chỉ của máy chủ mà tôi đang truy cập mà thường là địa chỉ của router trong mạng. Trong

ảnh, địa chỉ đích là 00:0c:41:45:90. Đây là địa chỉ của router hoặc thiết bị chuyển mạch (switch) mà máy tính của tôi kết nối đến, chứ không phải địa chỉ của máy chủ đích.

Bước 1: Xác định Địa chỉ IP và MAC của Gateway

Sử dụng lệnh ipconfig để xác định Default Gateway: Kết quả lệnh ipconfig chỉ ra rằng địa chỉ Default Gateway của adapter Wi-Fi là 172.20.10.1. Điều này cho thấy rằng tất cả các gói tin ra ngoài mạng cục bộ từ adapter Wi-Fi của tôi (có địa chỉ IPv4 là 172.20.10.3) sẽ đi qua gateway này.

```
Wireless LAN adapter Wi-Fi 2:

Connection-specific DNS Suffix . : 
IPv6 Address. . . . . : 2401:d800:9d1:b47:6ffc:62a:52ae:106f
Temporary IPv6 Address. . . . . : 2401:d800:9d1:b47:7c07:9908:6990:329
0
Link-local IPv6 Address . . . . . : fe80::1613:46e5:c0a9:5240%18
IPv4 Address. . . . . : 172.20.10.3
Subnet Mask . . . . . : 255.255.255.240
Default Gateway . . . . . : fe80::b0e5:f9ff:fe11:4564%18
                          172.20.10.1
```

Sử dụng lệnh arp -a để tìm địa chỉ MAC của Gateway: Kết quả của lệnh arp -a cho thấy địa chỉ IP 172.20.10.1 có địa chỉ MAC là b2-e5-f9-11-45-64. Đây là địa chỉ MAC của router hoặc gateway mà máy tính tôi kết nối để ra ngoài Internet.

```
Interface: 172.20.10.3 --- 0x12
Internet Address      Physical Address      Type
172.20.10.1          b2-e5-f9-11-45-64    dynamic
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250      01-00-5e-7f-ff-fa    static
255.255.255.255      ff-ff-ff-ff-ff-ff    static
```

Bước 2: So sánh với Địa chỉ MAC Đích trong Gói Tin HTTP GET

Trong Wireshark, tôi đã bắt gói tin HTTP GET và kiểm tra phần Ethernet II. Địa chỉ đích (Destination) trong gói tin này là b2-e5-f9-11-45-64. Địa chỉ MAC này trùng khớp với địa chỉ MAC của gateway 172.20.10.1 mà tôi đã xác định được từ lệnh arp -a. Điều

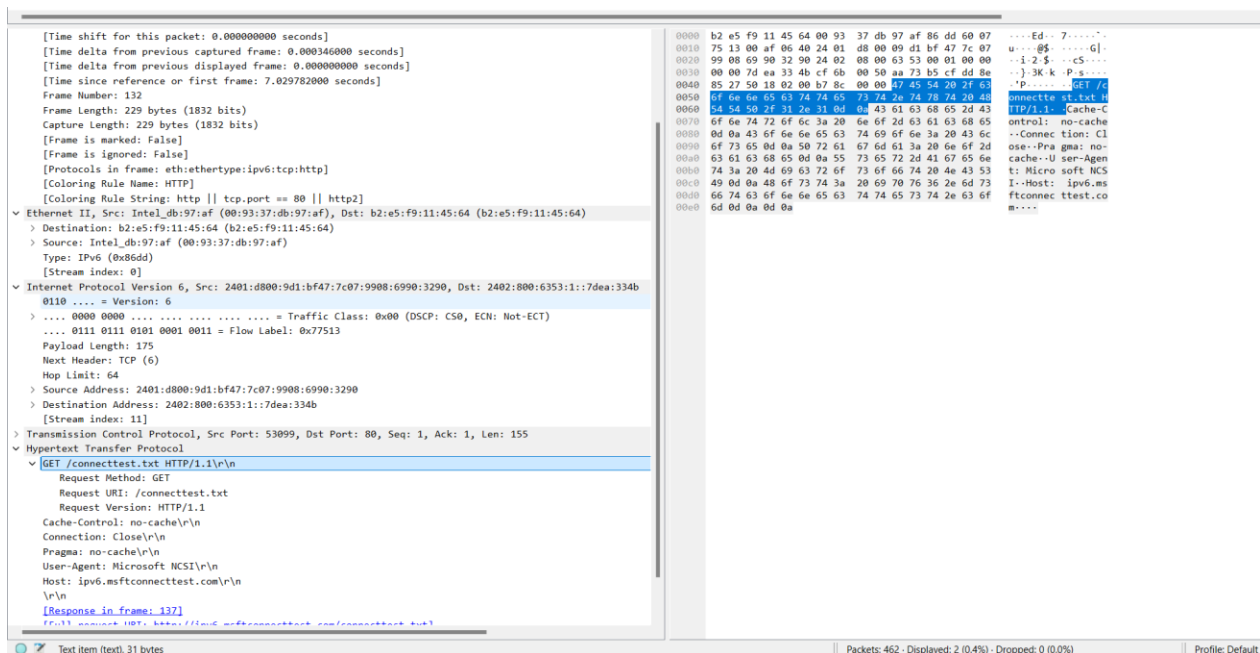
này xác nhận rằng gói tin HTTP GET được gửi đến địa chỉ MAC của gateway, chứ không phải địa chỉ MAC của máy chủ đích.

Câu 3: Giá trị dưới dạng hệ thập lục phân cho trường loại hai byte của khung là gì? Trường này tương ứng với giao thức lớp trên nào?

```
Ethernet II, Src: Intel_db:97:af (00:93:37:db:97:af), Dst: b2:e5:f9:11:45:64 (b2:e5:f9:11:45:64)
  Destination: b2:e5:f9:11:45:64 (b2:e5:f9:11:45:64)
    ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
    ....0 .... = IG bit: Individual address (unicast)
  Source: Intel_db:97:af (00:93:37:db:97:af)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0 .... = IG bit: Individual address (unicast)
  Type: IPv6 (0x86dd)
  [Stream index: 0]
Internet Protocol Version 6, Src: 2401:d800:9d1:bf47:7c07:9908:6990:3290, Dst: 2402:800:6353:1::7dea:334b
  0110 .... = Version: 6
  .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0000 00. .... = Differentiated Services Codepoint: Default (0)
  .... ..00 .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  .... 0111 0111 0101 0001 0011 = Flow Label: 0x77513
  Payload Length: 175
  Next Header: TCP (6)
  Hop Limit: 64
  Source Address: 2401:d800:9d1:bf47:7c07:9908:6990:3290
    [Address Space: Global Unicast]
  Destination Address: 2402:800:6353:1::7dea:334b
    [Address Space: Global Unicast]
  [Stream index: 11]
```

Trường này chỉ ra giao thức lớp trên. Trong gói tin, nó được liệt kê là 0x86dd, có nghĩa là đây là giao thức Ipv6.

Câu 4: Có bao nhiêu byte từ đầu của khung Ethernet tới khi ký tự ASCII “G” trong “GET” xuất hiện trong khung Ethernet?



The image shows a Wireshark packet capture analysis. The packet list on the left shows a packet of type Ethernet II. The packet details pane on the right shows the following information:

- Ethernet II, Src: Intel_db:97:af (00:93:37:db:97:af), Dst: b2:e5:f9:11:45:64 (b2:e5:f9:11:45:64)
 - Destination: b2:e5:f9:11:45:64 (b2:e5:f9:11:45:64)
 - Source: Intel_db:97:af (00:93:37:db:97:af)
 - Type: IPv6 (0x86dd)
 - [Stream index: 0]
- Internet Protocol Version 6, Src: 2401:d800:9d1:bf47:7c07:9908:6990:3290, Dst: 2402:800:6353:1::7dea:334b
 - Version: 6
 - Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Differentiated Services Codepoint: Default (0)
 - Explicit Congestion Notification: Not ECN-Capable Transport (0)
 - Flow Label: 0x77513
 - Payload Length: 175
 - Next Header: TCP (6)
 - Hop Limit: 64
 - Source Address: 2401:d800:9d1:bf47:7c07:9908:6990:3290
 - Destination Address: 2402:800:6353:1::7dea:334b
 - [Stream index: 11]
- Transmission Control Protocol, Src Port: 53099, Dst Port: 80, Seq: 1, Ack: 1, Len: 155
 - Hypertext Transfer Protocol
 - GET /connecttest.txt HTTP/1.1
 - Request Method: GET
 - Request URI: /connecttest.txt
 - Request Version: HTTP/1.1
 - Cache-Control: no-cache
 - Connection: Close
 - Pragma: no-cache
 - User-Agent: Microsoft NCSI
 - Host: ipv6.msftconnecttest.com
 - [Response in frame: 137]

The packet bytes pane on the right shows the raw data of the packet, including the Ethernet II header and the IPv6 packet payload.

Vị trí của ký tự “G”: Ta có thể thấy ký tự “G” trong GET bắt đầu ở phần dữ liệu gói tin. Trong phần Packet Bytes (cửa sổ hiển thị dữ liệu dạng hexadecimal và ASCII bên dưới), ta có thể thấy ký tự "G" xuất hiện ngay tại byte đầu tiên của chuỗi "GET /connecttest.txt HTTP/1.1\r\n".

Đếm số byte từ đầu khung Ethernet: Bắt đầu từ phần Ethernet II trong dữ liệu gói tin, đếm từng byte (mỗi cặp hexadecimal đại diện cho một byte) cho đến khi ta tới ký tự “G”. Trong trường hợp này, ký tự "G" xuất hiện tại byte thứ 47 từ đầu của khung Ethernet (đếm từ đầu khung). ➔ Ký tự "G" trong "GET" xuất hiện tại byte thứ 47 trong khung Ethernet của gói tin.

Tiếp theo, trả lời các câu hỏi sau, dựa trên nội dung của khung Ethernet chứa byte đầu tiên của thông điệp phản hồi HTTP:

Câu 5: Giá trị của địa chỉ Ethernet nguồn là gì? Đây có phải là địa chỉ của máy tính của bạn, hay của gaia.cs.umass.edu (Gợi ý: câu trả lời là không). Thiết bị nào có địa chỉ Ethernet này?

```

No.    Time    Source                Destination            Protocol Length Info
132 09:22:20.809448 2401:d800:9d1:bf47:7c07:9908:6990:3290 2402:800:6353:1::7dea:334b HTTP 229 GET /connecttest.txt HT
Frame 132: 229 bytes on wire (1832 bits), 229 bytes captured (1832 bits) on interface \Device\NPF_{E8972303-5AC7-4ADA-9205-681936D705B5}
Section number: 1
Interface id: 0 (\Device\NPF_{E8972303-5AC7-4ADA-9205-681936D705B5})
Interface name: \Device\NPF_{E8972303-5AC7-4ADA-9205-681936D705B5}
Interface description: Wi-Fi 2
Encapsulation type: Ethernet (1)
Arrival Time: Nov 16, 2024 09:22:20.809448000 SE Asia Standard Time
UTC Arrival Time: Nov 16, 2024 02:22:20.809448000 UTC
Epoch Arrival Time: 1731723740.809448000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000346000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 7.029782000 seconds]
Frame Number: 132
Frame Length: 229 bytes (1832 bits)

```

```

Wireless LAN adapter Wi-Fi 2:

Connection-specific DNS Suffix . : 
IPv6 Address. . . . . : 2401:d800:9d1:bf47:6ffe:c2a:52ae:10cf
Temporary IPv6 Address. . . . . : 2401:d800:9d1:bf47:7c07:9908:6990:3290
Link-Local IPv6 Address . . . . . : fe80::1613:46e5:c0a9:5240%18
IPv4 Address. . . . . : 172.20.10.3
Subnet Mask . . . . . : 255.255.255.240
Default Gateway . . . . . : fe80::b0e5:f9ff:fe11:4564%18
                             172.20.10.1

```


Trong phần Ethernet II của gói tin HTTP GET, địa chỉ nguồn (Source) là địa chỉ MAC của máy tính, có giá trị 2401:d800:9d1:bf47:7c07:9908:6990:3290. Địa chỉ này không phải là của gaia.cs.umass.edu; đây là địa chỉ của card mạng (network interface card) của máy tính đang sử dụng.

Câu 6: Địa chỉ đích trong khung Ethernet là gì? Đây có phải là địa chỉ Ethernet của máy tính của bạn không?

```
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Intel_db:97:af (00:93:37:db:97:af), Dst: b2:e5:f9:11:45:64 (b2:e5:f9:11:45:64)
Destination: b2:e5:f9:11:45:64 (b2:e5:f9:11:45:64)
.... 1. .... = LG bit: Locally administered address (this is NOT the factory default)
.... 0. .... = IG bit: Individual address (unicast)
Source: Intel_db:97:af (00:93:37:db:97:af)
.... 0. .... = LG bit: Globally unique address (factory default)
.... 0. .... = IG bit: Individual address (unicast)
Type: IPv6 (0x86dd)
[Stream index: 0]
Internet Protocol Version 6, Src: 2401:d800:9d1:bf47:7c07:9908:6990:3290, Dst: 2402:800:6353:1::7dea:334b
0110 .... = Version: 6
.... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... 0000 00.. .... = Differentiated Services Codepoint: Default (0)
.... ..00 .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
.... 0111 0111 0101 0001 0011 = Flow Label: 0x77513
Payload Length: 175
Next Header: TCP (6)
Hop Limit: 64
Source Address: 2401:d800:9d1:bf47:7c07:9908:6990:3290
[Address Space: Global Unicast]
Destination Address: 2402:800:6353:1::7dea:334b
[Address Space: Global Unicast]
[Stream index: 111]
```

Địa chỉ đích (Destination) trong phần Ethernet II của gói tin là b2-e5-f9-11-45-64. Đây không phải là địa chỉ MAC của máy tính. Thay vào đó, đây là địa chỉ của router/gateway trong mạng (đã chứng minh ở trên). Địa chỉ MAC này đại diện cho gateway mà máy tính đang sử dụng để kết nối với các máy chủ bên ngoài mạng LAN, bao gồm gaia.cs.umass.edu.

Câu 7: Giá trị dưới dạng hệ thập lục phân cho trường loại hai byte của khung là gì? Trường này tương ứng với giao thức lớp trên nào?

```

[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Intel_db:97:af (00:93:37:db:97:af), Dst: b2:e5:f9:11:45:64 (b2:e5:f9:11:45:64)
Destination: b2:e5:f9:11:45:64 (b2:e5:f9:11:45:64)
.... 1. .... = LG bit: Locally administered address (this is NOT the factory default)
.... 0 .... = IG bit: Individual address (unicast)
Source: Intel_db:97:af (00:93:37:db:97:af)
.... 0. .... = LG bit: Globally unique address (factory default)
.... 0 .... = IG bit: Individual address (unicast)
Type: IPv6 (0x86dd)
[Stream index: 0]
Internet Protocol Version 6, Src: 2401:d800:9d1:bf47:7c07:9908:6990:3290, Dst: 2402:800:6353:1::7dea:334b
0110 .... = Version: 6
.... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... 0000 00.. .... = Differentiated Services Codepoint: Default (0)
.... .... 00 .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
.... 0111 0111 0101 0011 = Flow Label: 0x77513
Payload Length: 175
Next Header: TCP (6)
Hop Limit: 64
Source Address: 2401:d800:9d1:bf47:7c07:9908:6990:3290
[Address Space: Global Unicast]
Destination Address: 2402:800:6353:1::7dea:334b
[Address Space: Global Unicast]
[Stream index: 11]

```

Giá trị thập lục phân của trường Frame Type trong phần Ethernet II là 0x86dd, giá trị này chỉ ra rằng gói tin sử dụng giao thức Ipv6 làm giao thức lớp trên.

Câu 8: Có bao nhiêu byte từ đầu của khung Ethernet tới khi ký tự ASCII “O” trong “OK” (tức là mã phản hồi HTTP) xuất hiện trong khung Ethernet?

Ký tự "G" trong "GET" xuất hiện ở byte thứ 47 tính từ đầu khung Ethernet (đã chứng minh ở trên).

2. Giao thức Phân giải Địa chỉ (ARP)

Trong phần này, chúng ta sẽ quan sát giao thức ARP trong hành động. Chúng tôi khuyến nghị bạn nên đọc lại mục 6.4.1 trong sách trước khi tiếp tục.

ARP Caching

Hãy nhớ rằng giao thức ARP thường duy trì một bộ đệm (cache) của các cặp dịch địa chỉ IP thành địa chỉ Ethernet trên máy tính của bạn. Lệnh arp (cả trên MSDOS và Linux/Unix) được sử dụng để xem và thao tác với nội dung của bộ đệm này. Do lệnh arp và giao thức ARP có tên giống nhau, rất dễ nhầm lẫn giữa chúng. Nhưng hãy lưu ý rằng chúng khác nhau - lệnh arp được sử dụng để xem và thao tác với nội dung bộ đệm ARP, trong khi giao thức ARP định nghĩa định dạng và ý nghĩa của các thông điệp được gửi và nhận, đồng thời xác định các hành động được thực hiện khi truyền và nhận thông điệp.

Hãy xem nội dung của bộ đệm ARP trên máy tính của bạn:

- **MS-DOS:** Lệnh arp nằm trong c:\windows\system32, do đó nhập vào dòng lệnh MS-DOS arp hoặc c:\windows\system32\arp (không có dấu ngoặc kép).
- **Linux/Unix/MacOS:** Tập thực thi cho lệnh arp có thể nằm ở nhiều nơi khác nhau. Vị trí phổ biến là /sbin/arp (trên Linux) và /usr/etc/arp (đối với một số biến thể Unix).

Lệnh arp trên Windows không có tham số sẽ hiển thị nội dung của bộ đệm ARP trên máy tính của bạn. Hãy chạy lệnh arp.

Câu 9: Ghi lại nội dung của bộ đệm ARP trên máy tính của bạn. Ý nghĩa của mỗi giá trị cột là gì?

```

Windows PowerShell
PS D:\HCMUT\[HK241]\CO3093-Computer-Networks-HK241\Lab\Lab_03\src> arp -a

Interface: 192.168.220.1 --- 0x6
Internet Address      Physical Address      Type
192.168.220.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 172.20.10.3 --- 0x12
Internet Address      Physical Address      Type
172.20.10.1           b2-e5-f9-11-45-64    dynamic
172.20.10.15          ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static

Interface: 192.168.253.1 --- 0x15
Internet Address      Physical Address      Type
192.168.253.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 172.20.112.1 --- 0x3b
Internet Address      Physical Address      Type
172.20.114.189        00-15-5d-33-0f-54    dynamic
172.20.127.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
239.255.255.250       01-00-5e-7f-ff-fa    static

```

Giải thích ý nghĩa của từng cột:

- **Interface (Giao diện):** Giao diện mạng trên máy tính mà địa chỉ IP và MAC được liên kết. Ví dụ: 192.168.220.1, 172.20.10.3.
- **Internet Address (Địa chỉ Internet):** Đây là địa chỉ IP của các thiết bị khác mà máy tính của bạn đã liên lạc gần đây.

- Physical Address (Địa chỉ Vật lý): Địa chỉ MAC của thiết bị tương ứng với địa chỉ IP.
- Type (Loại): Cho biết loại mục nhập ARP. Dynamic nghĩa là được tạo tự động thông qua giao thức ARP, còn Static nghĩa là được thêm vào thủ công và cố định.

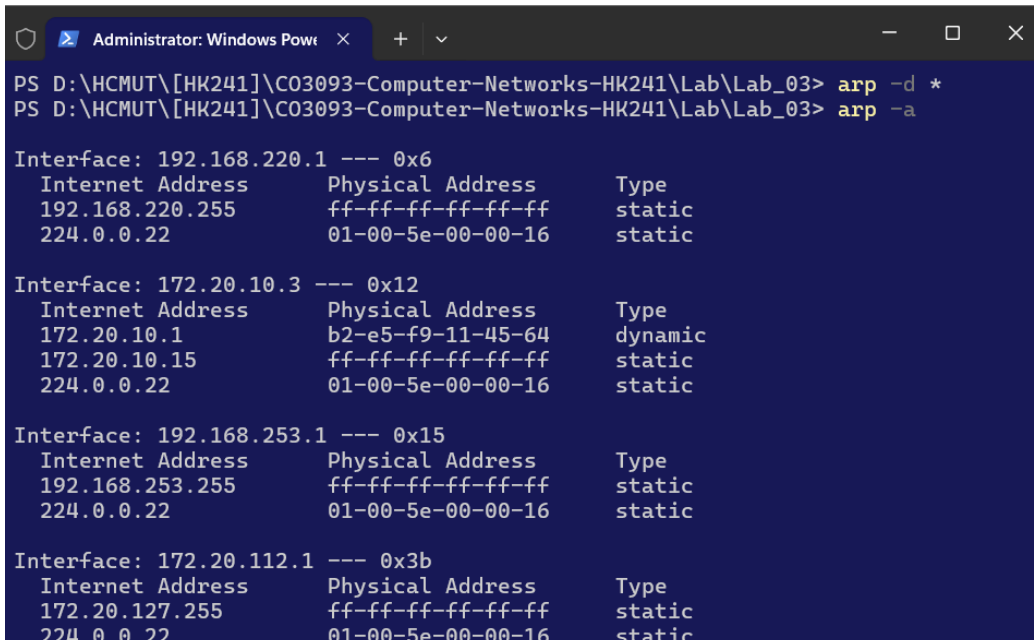
Để quan sát máy tính của bạn gửi và nhận các thông điệp ARP, chúng ta cần xóa bộ đệm ARP, bởi nếu không thì máy tính của bạn có khả năng tìm thấy một cặp dịch địa chỉ IP-Ethernet cần thiết trong bộ đệm và do đó không cần phải gửi ra một thông điệp ARP.

- **MS-DOS:** Lệnh `arp -d *` sẽ xóa bộ đệm ARP của bạn. Cờ `-d` chỉ thị thao tác xóa, và `*` là ký tự đại diện nói rằng sẽ xóa tất cả các mục trong bảng.
- **linux/Unix/MacOS:** Lệnh `arp -d *` sẽ xóa bộ đệm ARP của bạn. Để chạy lệnh này bạn sẽ cần quyền root. Nếu bạn không có quyền root và không thể chạy Wireshark trên máy Windows, bạn có thể bỏ qua phần thu thập dấu vết của phần lab này và sử dụng dấu vết đã đề cập ở phần chú thích trước đó.

Quan sát ARP trong hành động

Hãy làm theo các bước sau:

- Xóa bộ đệm ARP của bạn như đã mô tả ở trên.



```

Administrator: Windows PowerShell
PS D:\HCMUT\HK241\C03093-Computer-Networks-HK241\Lab\Lab_03> arp -d *
PS D:\HCMUT\HK241\C03093-Computer-Networks-HK241\Lab\Lab_03> arp -a

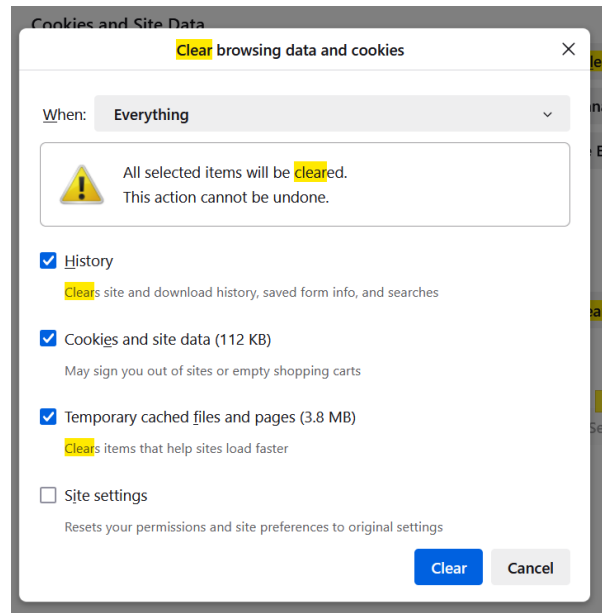
Interface: 192.168.220.1 --- 0x6
Internet Address      Physical Address      Type
192.168.220.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static

Interface: 172.20.10.3 --- 0x12
Internet Address      Physical Address      Type
172.20.10.1           b2-e5-f9-11-45-64    dynamic
172.20.10.15          ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static

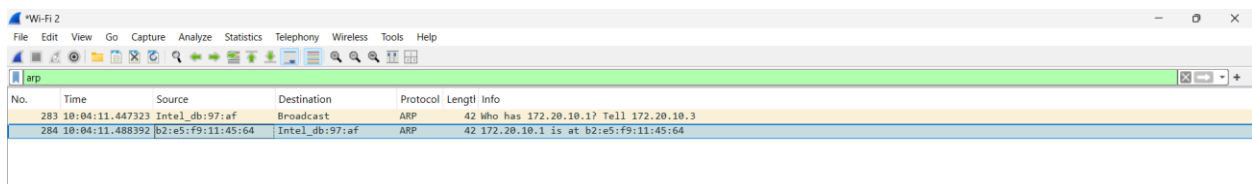
Interface: 192.168.253.1 --- 0x15
Internet Address      Physical Address      Type
192.168.253.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static

Interface: 172.20.112.1 --- 0x3b
Internet Address      Physical Address      Type
172.20.127.255         ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
  
```

- Sau đó, đảm bảo bộ đệm của trình duyệt của bạn là trống. Để làm điều này trên Mozilla Firefox V3, chọn **Tools -> Clear Recent History** và đánh dấu ô Cache. Đối với Internet Explorer, chọn **Tools -> Internet Options -> Delete Files**.



- Khởi động trình bắt gói Wireshark.
- Nhập địa chỉ URL sau vào trình duyệt của bạn:
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html>
Trình duyệt của bạn sẽ hiển thị một bản sao dài của US Bill of Rights.



- Dừng bắt gói Wireshark. Một lần nữa, vì chúng ta không quan tâm đến IP hoặc các giao thức lớp cao hơn, hãy thay đổi cửa sổ "listing of captured packets" của Wireshark để chỉ hiển thị thông tin về các giao thức bên dưới IP. Để làm điều này trong Wireshark, chọn **Analyze -> Enabled Protocols**. Sau đó bỏ chọn ô IP và chọn **OK**. Bây giờ bạn sẽ thấy một cửa sổ Wireshark trông giống như sau:
Trả lời các câu hỏi sau đây

Câu 10: Các giá trị thập lục phân cho địa chỉ nguồn và địa chỉ đích trong khung Ethernet chứa thông điệp yêu cầu ARP là gì?

```

[Capturing rule string: arp]
Ethernet II, Src: Intel_db:97:af (00:93:37:db:97:af), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
... ..1. .... = IG bit: Group address (multicast/broadcast)
Source: Intel_db:97:af (00:93:37:db:97:af)
... ..0. .... = LG bit: Globally unique address (factory default)
... ..0. .... = IG bit: Individual address (unicast)
Type: ARP (0x0806)
[Stream index: 1]

```

Hexadecimal values cho địa chỉ nguồn và đích trong Ethernet frame chứa ARP request:

Địa chỉ nguồn (Source MAC Address): 00:93:37:db:97:af

Địa chỉ đích (Destination MAC Address): ff:ff:ff:ff:ff:ff (đây là địa chỉ broadcast).

Câu 11: Cho giá trị thập lục phân của trường loại khung hai byte (Ethernet Frame type field). Giao thức lớp trên nào tương ứng với giá trị này?

```

[Capturing rule string: arp]
Ethernet II, Src: Intel_db:97:af (00:93:37:db:97:af), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
... ..1. .... = IG bit: Group address (multicast/broadcast)
Source: Intel_db:97:af (00:93:37:db:97:af)
... ..0. .... = LG bit: Globally unique address (factory default)
... ..0. .... = IG bit: Individual address (unicast)
Type: ARP (0x0806)
[Stream index: 1]

```

Giá trị thập lục phân (hexadecimal) cho trường loại hai byte (Frame Type): Trường này cho biết giao thức lớp trên (upper layer protocol). Trong ARP request, giá trị của Frame Type là 0x0806, biểu thị rằng đây là gói ARP (Address Resolution Protocol).

Câu 12: Tải về đặc tả ARP từ <ftp://ftp.rfc-editor.org/in-notes/std/std37.txt>. A readable, detailed discussion of ARP is also at <http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>.

a. Có bao nhiêu byte từ đầu khung Ethernet đến khi trường opcode ARP bắt đầu?

Trường opcode của gói tin ARP thường xuất hiện sau phần địa chỉ phần cứng và địa chỉ giao thức trong tải trọng của gói tin ARP. Nếu ta nhìn từ đầu khung Ethernet, opcode xuất hiện sau phần địa chỉ MAC và IP của sender.

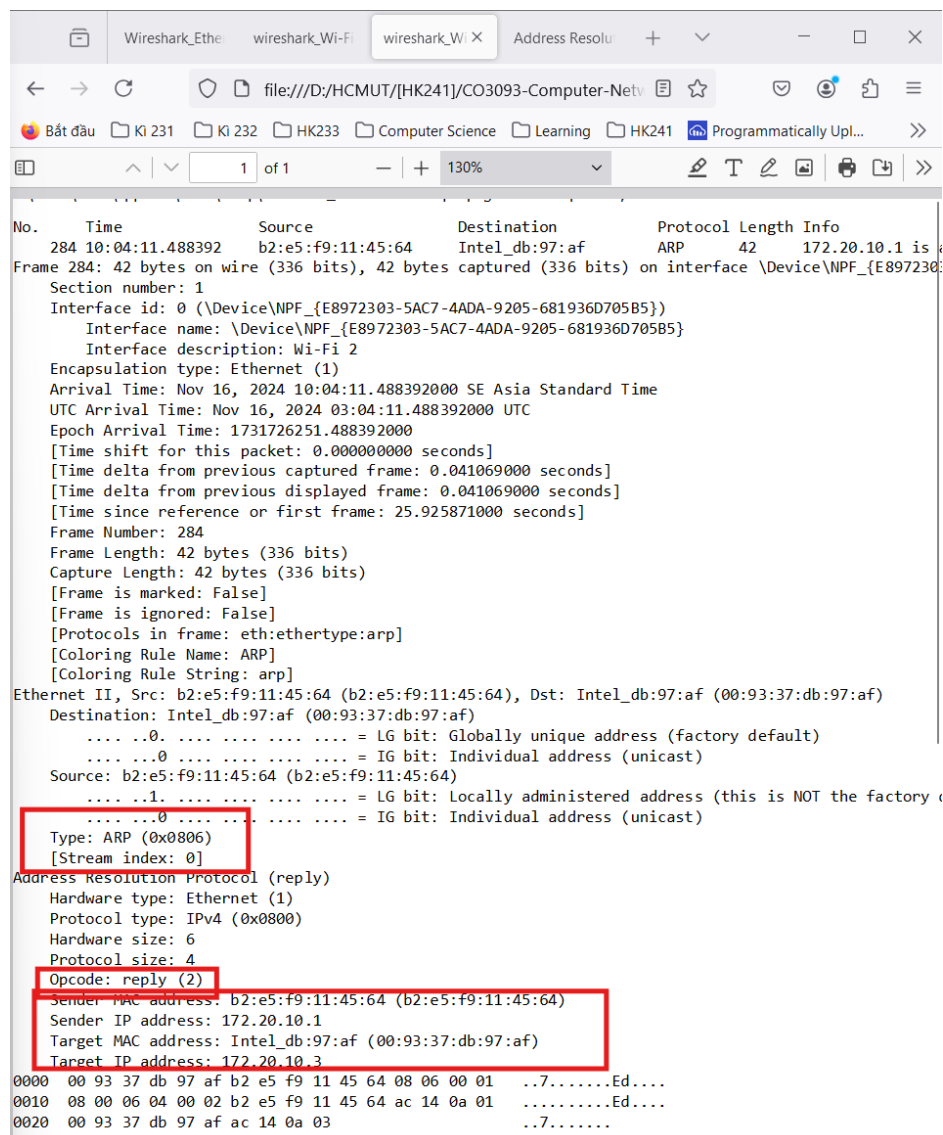
b. Giá trị của trường opcode trong phần tải trọng ARP của khung Ethernet khi một phản hồi ARP được thực hiện là gì?

Theo tài liệu, trường opcode cho một yêu cầu ARP (ARP Request) có giá trị là 0x0001.

c. Thông điệp ARP có chứa địa chỉ IP của người gửi không?

Có, gói tin ARP chứa địa chỉ IP của người gửi trong phần tải trọng của nó. Địa chỉ IP này cho phép người nhận ARP biết địa chỉ IP của máy yêu cầu để có thể gửi phản hồi chính xác.

Câu 13: Bây giờ tìm thông điệp phản hồi ARP đã được gửi để đáp lại yêu cầu ARP.



Wireshark packet capture showing an ARP reply packet. The packet is an Ethernet II frame with destination Intel_db:97:af and source b2:e5:f9:11:45:64. The ARP payload shows "Type: ARP (0x0806)" and "Opcode: reply (2)". The sender IP is 172.20.10.1 and the target IP is 172.20.10.3.

a. Có bao nhiêu byte từ đầu khung Ethernet đến khi trường opcode ARP bắt đầu?

Để xác định vị trí của trường opcode trong gói tin ARP, chúng ta cần tính khoảng cách từ đầu khung Ethernet. Trường opcode sẽ bắt đầu từ byte thứ 20 của khung Ethernet. Điều này bao gồm 6 byte đầu tiên cho địa chỉ MAC đích, 6 byte tiếp theo cho địa chỉ MAC nguồn, và 2 byte cho EtherType (thường là 0x0806 khi chỉ định gói tin ARP), cùng với 6 byte bổ sung cho các trường như loại phần cứng và giao thức, cũng như độ dài của chúng.

b. Giá trị của trường opcode trong phần tải trọng ARP của khung Ethernet khi một phản hồi ARP được thực hiện là gì?

Trong một gói tin phản hồi ARP (ARP Reply), giá trị của trường opcode là 0x0002. Điều này phân biệt một phản hồi ARP với một yêu cầu ARP, vốn có opcode là 0x0001.

c. Trong thông điệp ARP, địa chỉ IP của máy có địa chỉ Ethernet tương ứng đang được truy vấn nằm ở đâu?

Trong gói tin phản hồi ARP, "câu trả lời" cho yêu cầu được chứa trong hai trường chính: Sender MAC Address và Sender IP Address. Những trường này cung cấp địa chỉ MAC và IP của thiết bị trả lời, cho biết rằng địa chỉ IP đã được yêu cầu thuộc về thiết bị với địa chỉ MAC đó.

Câu 14: Các giá trị thập lục phân cho địa chỉ nguồn và đích trong khung Ethernet chứa thông điệp phản hồi ARP là gì?

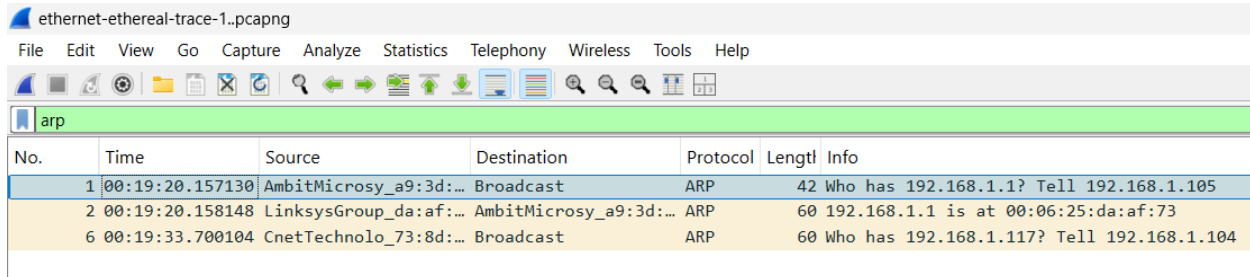
Trong gói tin phản hồi ARP, "câu trả lời" cho yêu cầu được chứa trong hai trường chính: Sender MAC Address và Sender IP Address. Những trường này cung cấp địa chỉ MAC và IP của thiết bị trả lời, cho biết rằng địa chỉ IP đã được yêu cầu thuộc về thiết bị với địa chỉ MAC đó.

Địa chỉ nguồn (Source MAC Address) trong khung Ethernet của phản hồi ARP là b2:e5:f9:11:45:64. Địa chỉ này đại diện cho thiết bị đang trả lời yêu cầu ARP.

Địa chỉ đích (Destination MAC Address) trong khung Ethernet của phản hồi ARP là 00:93:37:db:97:af. Đây là địa chỉ MAC của thiết bị đã gửi yêu cầu ARP.

Câu 15: Mở tệp dấu vết ethernet-ethereal-trace-1 tại <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>. Các gói tin ARP đầu tiên và thứ hai trong dấu vết này tương ứng

với một yêu cầu ARP được gửi bởi máy tính đang chạy Wireshark, và phản hồi ARP được gửi đến máy tính đang chạy Wireshark bởi máy tính với địa chỉ Ethernet được yêu cầu trong ARP. Nhưng có một máy tính khác trên mạng này, như được chỉ ra bởi gói tin 6 - một yêu cầu ARP khác. Tại sao không có phản hồi ARP (được gửi để phản hồi yêu cầu ARP trong gói tin 6) trong dấu vết gói tin?



No.	Time	Source	Destination	Protocol	Length	Info
1	00:19:20.157130	AmbitMicrosy_a9:3d:...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	00:19:20.158148	LinksysGroup_da:af:...	AmbitMicrosy_a9:3d:...	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
6	00:19:33.700104	CnetTechnolo_73:8d:...	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104

Trong file ethernet-ethereal-trace-1, các gói tin ARP đầu tiên và thứ hai tương ứng với ARP request do máy tính chạy Wireshark gửi đi. ARP reply được gửi lại tới máy tính chạy Wireshark với địa chỉ Ethernet đã được yêu cầu. Tuy nhiên, ở packet 6, có một ARP request khác từ một máy tính khác trong mạng, yêu cầu địa chỉ MAC của địa chỉ IP 192.168.1.117. Không có ARP reply nào được gửi lại cho yêu cầu này.

Lý do không có ARP reply cho ARP request trong packet 6 có thể là vì:

- Đích không tồn tại trong mạng: Địa chỉ IP 192.168.1.117 có thể không có máy nào sử dụng hoặc không hoạt động tại thời điểm đó.
- Thiết bị không phản hồi: Máy đích (nếu tồn tại) có thể đã ngắt kết nối hoặc không phản hồi lại yêu cầu ARP vào lúc đó.
- Lọc ARP: Một số hệ thống có thể lọc hoặc từ chối các yêu cầu ARP từ các thiết bị không quen thuộc hoặc từ các địa chỉ IP không được xác thực.

Vì vậy, không có ARP reply nào xuất hiện cho ARP request trong packet 6.

3. Extra Credit

Ex1: Lệnh arp: arp -s InetAddr EtherAddr cho phép bạn thủ công thêm một mục vào bộ đệm ARP xác định địa chỉ IP InetAddr tới địa chỉ vật lý EtherAddr. Điều gì sẽ xảy ra nếu, khi bạn thủ công thêm một mục, bạn nhập địa chỉ IP đúng, nhưng sai địa chỉ Ethernet cho giao diện từ xa?

```

Administrator: Windows PowerShell
PS D:\HCMUT\ [HK241] \C03093-Computer-Networks-HK241\Lab\Lab_03> arp -s 192.168.1.50 00-11-22-33-44-55
PS D:\HCMUT\ [HK241] \C03093-Computer-Networks-HK241\Lab\Lab_03> arp -a

Interface: 192.168.220.1 --- 0x6
    Internet Address      Physical Address      Type
    -----
    192.168.220.255       ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 172.20.10.3 --- 0x12
    Internet Address      Physical Address      Type
    -----
    172.20.10.1           b2-e5-f9-11-45-64    dynamic
    172.20.10.15          ff-ff-ff-ff-ff-ff    static
    192.168.1.50          00-11-22-33-44-55    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static
    255.255.255.255       ff-ff-ff-ff-ff-ff    static

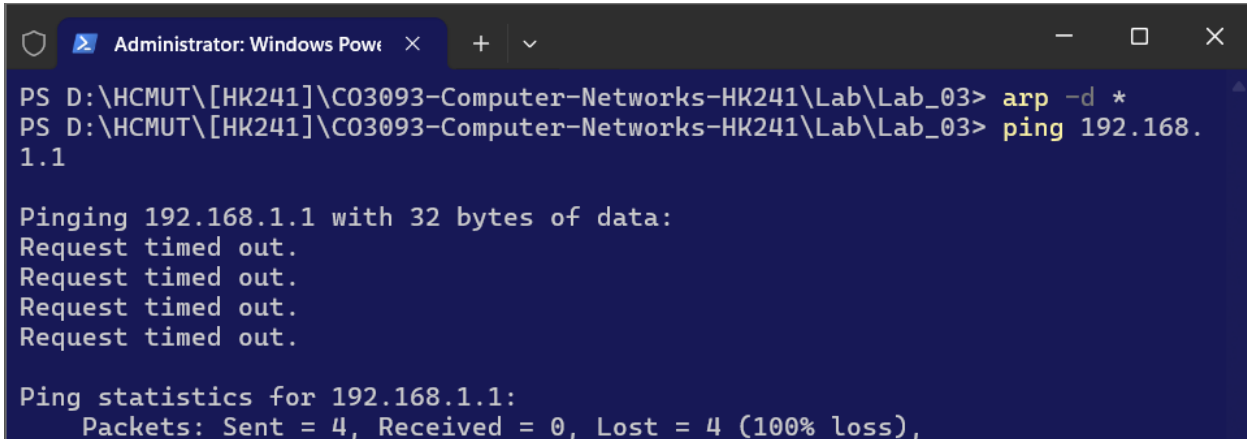
Interface: 192.168.253.1 --- 0x15
    Internet Address      Physical Address      Type
    -----
    192.168.253.255       ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    224.0.0.252           01-00-5e-00-00-fc    static
    239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 172.20.112.1 --- 0x3b
    Internet Address      Physical Address      Type
    -----
    172.20.114.189        00-15-5d-33-0f-54    dynamic
    172.20.127.255        ff-ff-ff-ff-ff-ff    static
    224.0.0.22            01-00-5e-00-00-16    static
    224.0.0.251           01-00-5e-00-00-fb    static
    239.255.255.250       01-00-5e-7f-ff-fa    static
  
```

Bằng cách sử dụng lệnh `arp -s 192.168.1.50 00-11-22-33-44-55`, tôi đã thủ công thêm một mục vào bộ đệm ARP của máy tính với địa chỉ IP 192.168.1.50, nhưng địa chỉ MAC là 00-11-22-33-44-55, thay vì địa chỉ MAC thực của thiết bị tại IP đó. Khi kiểm tra lại bộ đệm ARP bằng lệnh `arp -a`, mục này xuất hiện trong danh sách ARP với giao thức tĩnh (static).

Nếu địa chỉ IP đúng nhưng địa chỉ MAC sai, máy tính sẽ cố gắng gửi các gói tin đến địa chỉ IP đó, nhưng do địa chỉ MAC không khớp, các gói tin sẽ không đến được đúng thiết bị đích. Điều này gây ra lỗi giao tiếp, vì dữ liệu sẽ không được gửi đến thiết bị đúng đắn. Đây là cách mà các vấn đề về cấu hình thủ công có thể dẫn đến lỗi truyền thông trong mạng.

Ex2: Thời gian mặc định mà một mục vẫn tồn tại trong bộ đệm ARP của bạn trước khi bị xóa là bao lâu? Bạn có thể xác định điều này bằng cách thực nghiệm (bằng cách giám sát nội dung bộ đệm) hoặc bằng cách tìm kiếm thông tin này trong tài liệu hệ điều hành của bạn. Chỉ ra cách/bạn xác định giá trị này ở đâu.



```
Administrator: Windows PowerShell
PS D:\HCMUT\HK241\C03093-Computer-Networks-HK241\Lab\Lab_03> arp -d *
PS D:\HCMUT\HK241\C03093-Computer-Networks-HK241\Lab\Lab_03> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Để xác định thời gian một mục tồn tại trong bộ đệm ARP, tôi đã thực hiện xóa toàn bộ các mục trong bộ đệm ARP bằng lệnh `arp -d *`. Sau đó, tôi thực hiện lệnh `ping 192.168.1.1` để kiểm tra xem liệu mục ARP mới có được tạo ra không. Kết quả là toàn bộ các yêu cầu ping đều bị mất (100% loss), cho thấy rằng nếu một mục ARP không có sẵn, kết nối sẽ không thành công, thời gian bị chiếm khoảng 10 giây.

Từ đó, có thể suy ra rằng khi bộ đệm ARP không có thông tin về địa chỉ IP, hệ thống không thể liên lạc với địa chỉ đó cho đến khi mục ARP được cập nhật lại. Thời gian lưu trữ mặc định cho một mục ARP trong bộ đệm phụ thuộc vào cài đặt của hệ điều hành, và có thể được xác minh trong tài liệu hệ điều hành hoặc bằng cách giám sát thời gian mà một mục tự động hết hạn và bị xóa khỏi bộ đệm ARP.