

# BÀI TẬP THỰC HÀNH SỐ 6

## MÔN HỌC: NHẬP MÔN MẠNG MÁY TÍNH

MSSS: 21521935

Họ và Tên: Ngô Vũ Minh Đạt

### 1. Địa chỉ Ethernet 48 bit của máy tính chúng ta?

Address:LCFCHeFe\_ad:c1:cc(84:a9:38:ad:c1:cc)

The screenshot displays two windows. The left window is Wireshark, showing a packet capture on the 'Ethernet' interface. The selected packet (No. 352) is an Ethernet II frame from LCFCHeFe\_ad:c1:cc (84:a9:38:ad:c1:cc) to Cambrldg\_fd:ef:90 (a8:5b:a0:fd:ef:90). The right window is a Command Prompt showing the output of the 'ipconfig /all' command for the Ethernet adapter. The physical address is highlighted as 84-A9-38-AD-C1-CC, which matches the source MAC address in the Wireshark packet.

```
Autoconfiguration Enabled . . . . . : Yes

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : 
   Description . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . : 84-A9-38-AD-C1-CC
   DHCP Enabled. . . . . : Yes
   Autoconfiguration Enabled . . . . . : Yes
   IPv6 Address. . . . . : 2405:4882:9176:b100:eelb:3c5f:cf6d:b090(Preferred)
   IPv6 Address. . . . . : 2405:4882:9176:b100:ffff:ffff:ffff:ffff(Preferred)
   Lease Obtained. . . . . : Sunday, 1 January, 2023 8:06:33 PM
   Lease Expires . . . . . : Sunday, 1 January, 2023 8:24:34 PM
```

### 2. Địa chỉ đích (Ethernet 48 bit) trong Ethernet frame? Đó có phải là địa chỉ của gaia.cs.umass.edu hay không (Gợi ý: là không). Địa chỉ đó là của thiết bị nào? (trang 468-469 trong giáo trình)

Nó không phải là địa chỉ của trang web, mà là địa chỉ MAC của router.

```

[... Ethernet II, Src: LCFCHefe_ad:c1:cc (84:a9:38:ad:c1:cc), Dst: Cambridg_fd:6f:90 (a8:58:40:fd:6f:90)]
  Destination: Cambridg_fd:6f:90 (a8:58:40:fd:6f:90)
    Address: Cambridg_fd:6f:90 (a8:58:40:fd:6f:90)
      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ...0 .... = IG bit: Individual address (unicast)
  Source: LCFCHefe_ad:c1:cc (84:a9:38:ad:c1:cc)
    Address: LCFCHefe_ad:c1:cc (84:a9:38:ad:c1:cc)
      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ...0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  Data (557 bytes)

```

3. Giá trị hệ 16 của trường Frame type (2 byte). Giao thức tầng trên tương ứng là gì?

```

      .... ..0. .... = LG bit: Globally unique address (factory default)
      .... ...0 .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  Data (557 bytes)

```

Giá trị hệ 16: 0x0800

Giao thức tầng trên tương ứng là Ipv4

4. Tính từ ký tự “G” (GET) trong frame đến hết frame có bao nhiêu byte?

52 bytes

5. Địa chỉ nguồn trong Ethernet frame? Có phải là địa chỉ của máy tính chúng ta hay của gaia.cs.umass.edu? (Gợi ý: là không). Địa chỉ đó của thiết bị nào?

Apply a display filter - Ctrl+H						
Packet bytes	Narrow & Wide	Case sensitive	String	get		
No.	Time	Source	Destination	Protocol	Length	Info
353	3.447016	Cambridg_fd:6f:90	LCFChEfE_ad:c1:cc	0x0000	66	IPv4
354	3.447092	LCFChEfE_ad:c1:cc	Cambridg_fd:6f:90	0x0000	54	IPv4
355	3.576121	LCFChEfE_ad:c1:cc	Cambridg_fd:6f:90	0x0000	55	IPv4
356	3.639293	Cambridg_fd:6f:90	LCFChEfE_ad:c1:cc	0x0000	66	IPv4
357	3.639403	LCFChEfE_ad:c1:cc	Cambridg_fd:6f:90	0x0000	54	IPv4
358	3.684393	Cambridg_fd:6f:90	LCFChEfE_ad:c1:cc	0x0000	66	IPv4
359	3.709288	Cambridg_fd:6f:90	LCFChEfE_ad:c1:cc	0x0000	64	IPv4
360	3.710321	Cambridg_fd:6f:90	LCFChEfE_ad:c1:cc	0x0000	1466	IPv4
361	3.712392	Cambridg_fd:6f:90	LCFChEfE_ad:c1:cc	0x0000	1466	IPv4

▼ Frame 360: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface \Dev

Section number: 1

> Interface id: 0 {Device\NPF\_{D6FE4618-0178-479C-882E-19A186A8B061}}

Encapsulation type: Ethernet (1)

Arrival Time: Jan 1, 2023 19:15:11.636915000 SE Asia Standard Time

Epoch Time: 1672575311.636915000 seconds

[Time delta from previous captured frame: 0.001033000 seconds]

[Time delta from previous displayed frame: 0.001033000 seconds]

[Time since reference or first frame: 3.710321000 seconds]

Frame Number: 360

Frame Length: 1466 bytes (11728 bits)

Capture Length: 1466 bytes (11728 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: ethertype:data]

Ethernet II, Src: Cambridg\_fd:6f:90 (a8:58:40:fd:6f:90), Dst: LCFChEfE\_ad:c1:cc (84:a9:38:ad:c1:cc)

Destination: LCFChEfE\_ad:c1:cc (84:a9:38:ad:c1:cc)

Address: LCFChEfE\_ad:c1:cc (84:a9:38:ad:c1:cc)

.....0..... = LG bit: Globally unique address (factory default)

.....0..... = IG bit: Individual address (unicast)

Source: Cambridg\_fd:6f:90 (a8:58:40:fd:6f:90)

Address: Cambridg\_fd:6f:90 (a8:58:40:fd:6f:90)

.....0..... = LG bit: Globally unique address (factory default)

.....0..... = IG bit: Individual address (unicast)

Type: IPv4 (0x0000)

Data (1452 bytes)

[Length: 1452]

0000 84 a9 38 ad c1 cc a8 58 40 fd 6f 90 08 00 45 48 08 00

Nó không phải là địa chỉ của máy tính hay địa chỉ của trang web, mà là địa

MAC của router, dùng để chuyển gói vào lớp mạng

6. Địa chỉ đích của Ethernet frame? Có phải đó là địa chỉ của máy tính chúng ta hay không?

No.	Time	Source	Destination	Protocol	Length	Info
353	3.447016	Cambridg_fd:6f:90	LCFCHefe_ad:c1:cc	0x0800	66	IPv4
354	3.447092	LCFCHefe_ad:c1:cc	Cambridg_fd:6f:90	0x0800	54	IPv4
355	3.576121	LCFCHefe_ad:c1:cc	Cambridg_fd:6f:90	0x0800	55	IPv4
356	3.639293	Cambridg_fd:6f:90	LCFCHefe_ad:c1:cc	0x0800	66	IPv4
357	3.639403	LCFCHefe_ad:c1:cc	Cambridg_fd:6f:90	0x0800	54	IPv4
358	3.684393	Cambridg_fd:6f:90	LCFCHefe_ad:c1:cc	0x0800	66	IPv4
359	3.709288	Cambridg_fd:6f:90	LCFCHefe_ad:c1:cc	0x0800	64	IPv4
360	3.710321	Cambridg_fd:6f:90	LCFCHefe_ad:c1:cc	0x0800	1466	IPv4
361	3.712392	Cambridg_fd:6f:90	LCFCHefe_ad:c1:cc	0x0800	1466	IPv4

  

▼

Frame 360: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface \Dev

Section number: 1

> Interface id: 0 (\Device\NPF\_{D6FE461B-0178-479C-882E-19A186AB8061})

Encapsulation type: Ethernet (1)

Arrival Time: Jan 1, 2023 19:15:11.636915000 SE Asia Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1672575311.636915000 seconds

[Time delta from previous captured frame: 0.001033000 seconds]

[Time delta from previous displayed frame: 0.001033000 seconds]

[Time since reference or first frame: 3.710321000 seconds]

Frame Number: 360

Frame Length: 1466 bytes (11728 bits)

Capture Length: 1466 bytes (11728 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:data]

▼ Ethernet II, Src: Cambridg\_fd:6f:90 (a8:58:40:fd:6f:90), Dst: LCFCHefe\_ad:c1:cc (84:a9:38:ad:c1:cc)

Destination: LCFCHefe\_ad:c1:cc (84:a9:38:ad:c1:cc)

Address: LCFCHefe\_ad:c1:cc (84:a9:38:ad:c1:cc)

... .. = LG bit: Globally unique address (factory default)

... .. = IG bit: Individual address (unicast)

▼ Source: Cambridg\_fd:6f:90 (a8:58:40:fd:6f:90)

Address: Cambridg\_fd:6f:90 (a8:58:40:fd:6f:90)

... .. = LG bit: Globally unique address (factory default)

... .. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

▼ Data (1452 bytes)

...

0000 84 a9 38 ad c1 cc a8 58 40 fd 6f 90 00 00 45 48 ..X @:..EH

0010 05 ac 04 e6 40 00 23 06 15 41 80 77 f5 0c c0 a8 ...@:..Aw...

0020 01 b1 00 50 c5 8a ea d2 6e cd 38 d2 03 7c 50 10 ...P...n8:]P-

0030 00 ed 1f 00 00 00 48 54 54 50 2f 31 2e 31 20 32 .....HT TP/1.1 2

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 75 6e 00 OK:Date: Sun

0050 2c 20 30 31 20 4a 61 6e 20 32 30 32 33 20 31 32 , 01 Jan 2023 12

0060 3a 31 35 3a 34 32 20 47 4d 54 0d 0a 53 65 72 7e :15:42 G MT:Serv

0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6

0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS ) OpenSS

0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH

00a0 50 2f 37 2e 34 2e 33 30 20 6d 6f 64 5f 70 65 72 P/7.4.30 mod\_per

00b0 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 1/2.0.11 Perl/v5

00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3..last-Modi

00d0 66 69 65 64 3a 20 53 75 6e 2c 20 30 31 20 4a 61 fied: Su n, 01 Ja

00e0 6e 20 32 30 32 33 20 30 36 3a 35 39 3a 30 31 20 n 2023 0 6:59:01

00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 31 31 39 34 GMT: ETa g: "1194

0100 2d 35 66 31 32 65 35 65 39 63 36 33 62 30 22 0d -5f12e5e 9c63b0"

0110 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 -Accept- Ranges:

0120 62 79 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c bytes:Content-L

0130 65 6e 67 74 68 3a 20 34 35 30 30 0d 0a 4b 65 65 length: 4 500: Kee

0140 70 2d 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 p-Alive: timeout

0150 3d 35 2c 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e =S, max= 100: Con

0160 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c nection: Keep-Al

0170 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 ive:Con tent-Typ

0180 65 3a 20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 e: text/ html; ch

0190 61 72 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c arset=UTF-8<<<

01a0 68 74 6d 6c 3e 3c 68 65 61 64 3e 20 0a 3c 74 69 html>che ad <ti

01b0 74 6c 65 3e 48 69 73 74 6f 72 69 63 61 6c 20 44 tle>Hist orical D

01c0 6f 63 75 6d 65 6e 74 73 3a 54 48 45 20 42 49 49 L OF RIG HTS</tit

01d0 4c 20 4f 46 20 52 49 47 48 54 53 3c 2f 74 69 74 le>/hea d><<bo

01e0 6c 65 3e 3c 2f 68 65 61 64 3e 0a 0a 0a 3c 62 6f dy bgcol or="#fff

01f0 64 79 20 62 67 63 6f 6c 6f 72 3d 22 23 66 66 66

0200 66 66 66 22 20 6c 69 6e 6b 3d 22 23 33 33 30 30

Địa chỉ đích này là địa chỉ MAC của máy tính

7. Giá trị hệ 16 của trường Frame type (2 byte). Giao thức tầng trên tương ứng là gì?

Giao thức tầng trên là IPV4

8. Tính từ ký tự “O” (OK) trong frame đến hết frame có bao nhiêu byte?

52 bytes

## 1 ARP

### 1.1 ARP caching

ARP duy trì một bảng ánh xạ giữa IP và MAC (ARP cache). Lệnh *arp* trên Windows và Linux được dùng để xem nội dung của bảng ánh xạ ARP. Tuy lệnh *arp* và giao thức ARP cùng tên nhưng chức năng khác nhau:

- Lệnh arp dùng để xem bảng ánh xạ giữa IP và MAC
- Giao thức ARP định nghĩa định dạng, các thông điệp được gửi và nhận, các hành động khi các thông điệp được gửi và nhận

Quan sát nội dung của ARP cache trên máy tính của chúng ta bằng cách:

- Trên Windows: gõ **arp -a** hoặc “C:\windows\system32\arp - a” trên command line
- Trên Linux/Unix/MacOS: lệnh arp có thể ở các thư mục khác nhau, thông thường là **/sbin/arp** hoặc **/usr/etc/arp**

Trả lời câu hỏi sau:

- Viết nội dung của ARP cache trong máy tính của chúng ta. Giải thích ý nghĩa của từng dòng trong ARP cache?

```
C:\Users\ngovu>arp -a

Interface: 192.168.1.177 --- 0x12
Internet Address      Physical Address      Type
192.168.1.1           a8-58-40-fd-6f-90     dynamic
192.168.1.39          e4-ab-89-18-a9-18     dynamic
192.168.1.70          4c-bd-8f-8b-34-88     dynamic
192.168.1.74          8c-f5-a3-e2-8d-71     dynamic
192.168.1.169         10-82-d7-de-5d-b3     dynamic
192.168.1.186         14-eb-b6-6b-97-3e     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
224.0.0.2             01-00-5e-00-00-02     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
```

IP address: địa chỉ của máy tính

Physical address: địa chỉ MAC của máy tính

Type: loại địa chỉ IP

## 1.2 Quan sát hành vi của ARP

Để quan sát được quá trình gửi và nhận các thông điệp ARP, ta cần phải xóa nội dung của ARP cache, vì nếu máy tính của chúng ta đã có một ánh xạ IP – MAC cần thiết thì ARP không cần được sử dụng.

- Trên Windows: Sử dụng ***arp -d \****
- Trên Linux/Unix/MacOS: Sử dụng ***arp -d \**** nhưng phải có quyền root.

***Chú ý: nếu chúng ta không thể chạy Wireshark trên Internet thật sự thì có thể mở file ethernet-ethereal-trace-1 có sẵn trong thư mục wireshark-traces.***

Thực hiện các bước sau khi có kết nối Internet:

- Xóa ARP cache
- Xóa cache của trình duyệt
- Mở Wireshark và tiến hành bắt gói
- Truy cập trang web <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html>
- Sau khi nội dung của trang web đã được hiển thị, ngưng bắt gói. Vì bài thực hành về ARP nên ta không cần quan tâm đến IP hoặc tầng cao hơn. Để Wireshark chỉ hiển thị các thông tin về giao thức tầng liên kết, chọn Analyze -> Enable Protocol. Bỏ chọn IP hoặc IPv4-> OK. Khi đó, Wireshark sẽ hiển thị như sau

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	LCFCHefe_ad:c1:cc	Broadcast	ARP	42	Who has 192.168.1.75? Tell 192.168.1.177
2	1.000007	LCFCHefe_ad:c1:cc	Broadcast	ARP	42	Who has 192.168.1.75? Tell 192.168.1.177
18	1.787627	TP-Link_b6:97:3e	Broadcast	ARP	60	Who has 192.168.1.74? Tell 192.168.1.186
25	2.787652	TP-Link_b6:97:3e	Broadcast	ARP	60	Who has 192.168.1.39? Tell 192.168.1.186
282	4.722610	LCFCHefe_ad:c1:cc	Broadcast	ARP	42	Who has 192.168.1.75? Tell 192.168.1.177
323	5.496272	LCFCHefe_ad:c1:cc	Broadcast	ARP	42	Who has 192.168.1.75? Tell 192.168.1.177
438	6.495583	LCFCHefe_ad:c1:cc	Broadcast	ARP	42	Who has 192.168.1.75? Tell 192.168.1.177

  

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D... > Ethernet II, Src: LCFCHefe_ad:c1:cc (84:a9:38:ad:c1:cc), Dst: Broadcast (ff:ff:ff:ff:ff:ff) > Address Resolution Protocol (request) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: request (1) Sender MAC address: LCFCHefe_ad:c1:cc (84:a9:38:ad:c1:cc) Sender IP address: 192.168.1.177 Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00) Target IP address: 192.168.1.75	0000 ff ff ff ff ff ff 84 a9 38 ad c1 cc 08 06 00 01 ..... 8..... 0010 08 00 06 04 00 01 84 a9 38 ad c1 cc c0 a8 01 b1 ..... 8..... 0020 00 00 00 00 00 00 c0 a8 01 4b ..... K
--	--

Trả lời các câu hỏi sau:

10. Giá trị hệ 16 của địa chỉ nguồn và đích trong thông điệp ARP request?

Địa chỉ nguồn: Source: LCFCHefe\_ad:c1:cc (84:a9:38:ad:c1:cc)

Địa chỉ đích: Broadcast (ff:ff:ff:ff:ff:ff)

11. Giá trị hệ 16 của trường Frame type (2 byte). Giao thức tầng trên tương ứng là gì?

Type: ARP (0x0806)

12. Download bản miêu tả ARP từ <http://ftp.rfc-editor.org/in-notes/std/std37.txt> . Một bản miêu tả chi tiết khác dễ theo dõi hơn

<http://www.erg.abdn.ac.uk/~gorry/course/inet-pages/arp.html>

Link không vào được nên em không làm được câu này

# Not Found

The requested URL was not found on this server.

Apache/2.4.54 (Debian) Server at erg.abdn.ac.uk Port 443