

计算机网络以太网和 ARP 实验报告

姓名：陈鹤影

学号：PB21061287

日期：2022.12.4

一、 实验目的：

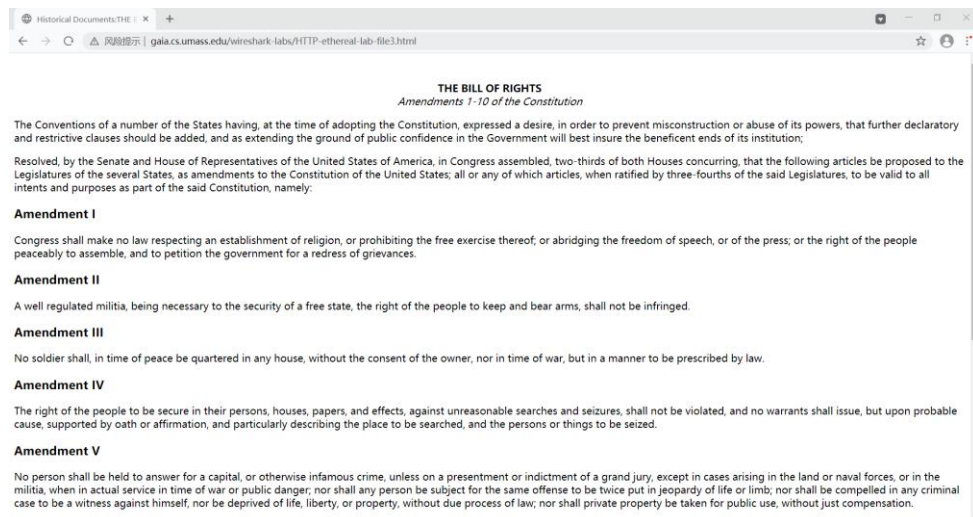
1. 了解以太网协议及 ARP 协议。
2. 学会分析 ARP 请求和响应报文。
3. 学会分析链路层帧的结构。
4. 了解 MAC 地址与 IP 地址各自的功能。
5. 学会使用 arp 命令查看和修改 ARP 缓存。

二、 实验流程及问题回答：

Part 1: Capturing and analyzing Ethernet frames

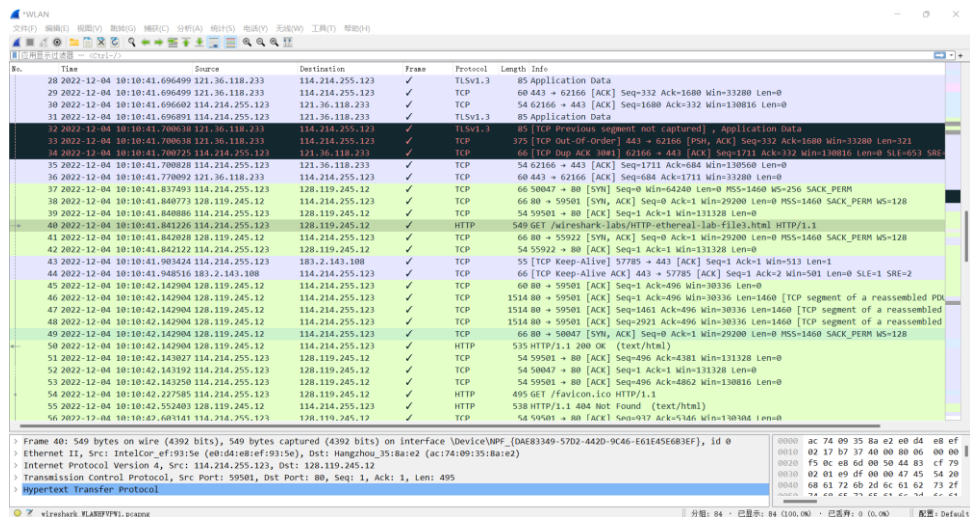
1. 实验流程：

- 1) 清除浏览器缓存，打开 Wireshark 抓包。
- 2) 输入 URL：<http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>
显示界面如图：



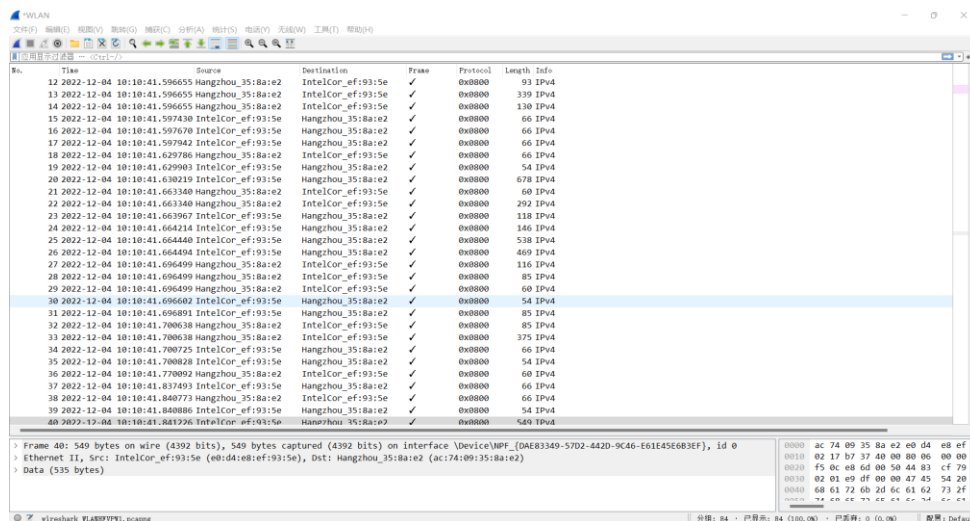
(图 1-1 输入网址显示界面)

- 3) 停止抓包。找到 HTTP GET (Num = 40) 及响应 (Num = 46) 报文，显示如下：



(图 1-2 Wireshark 抓包界面)

- 4) 更改 Wireshark 的“捕获包列表”窗口，使其仅显示 IP 以下协议的信息。更改后显示界面如下：



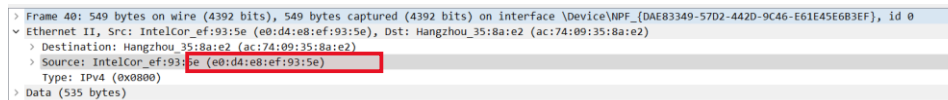
(图 1-3 更改显示界面)

2. 问题回答：

下面根据包含 HTTP GET 报文的以太网帧的内容，回答问题：

1. What is the 48-bit Ethernet address of your computer?

Ans: e0:d4:e8:ef:93:5e。(在前述步骤中已经找到 HTTP GET 对应的 Num = 40)。



2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]

Ans: Destination address: ac:74:09:35:8a:e2;

这不是 gaia.cs.umass.edu 的以太网地址。

这是主机所在子网的网关 MAC 地址。对应网关路由器拥有该地址。

```
> Frame 40: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
  Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
    > Destination: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
    > Source: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
    Type: IPv4 (0x0800)
  Data (535 bytes)
```

3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

Ans: 0x0800, 与之相对应的上层协议为 IPv4。

```
> Frame 40: 549 bytes on wire (4392 bits), 549 bytes captured (4392 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
  Ethernet II, Src: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
    > Destination: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
    > Source: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
    Type: IPv4 (0x0800)
  Data (535 bytes)
```

4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

Ans: 出现在第 55 个字节。

0000	ac 74 09 35 8a e2 e0 d4 e8 ef 93 5e 08 00 45 00	.t.5.... ^..E.
0010	02 17 b7 37 40 00 80 06 00 00 72 d6 ff 7b 80 77	...7@... .r...{.w
0020	f5 0c e8 6d 00 50 44 83 cf 79 5a 0e d2 ba 50 18	...m.PD. .yZ...P.
0030	02 01 e9 df 00 00 47 45 54 20 2f 77 69 72 65 73GET/wires
0040	68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 65	hark-lab s/HTTP-e
0050	74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65	thereal- lab-file
0060	33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d	3.html H TTP/1.1.
0070	0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75	.Host: g aia.cs.u
0080	6d 61 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63	mass.edu ..Connec
0090	74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65	tion: ke ep-alive
00a0	0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75	..Upgrad e-Insecu
00b0	72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a	re-Reque sts: 1..
00c0	55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69	User-Age nt: Mozi
00d0	6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73	lla/5.0 (Windows
00e0	20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b	NT 10.0 ; win64;
00f0	20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4b 69	x64) Ap pleWebKi

下面根据包含 HTTP 响应消息的第一个字节的以太网帧的内容，回答问题：

5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

Ans: 上述过程已记录首个 HTTP response 报文的 Num = 46。则可知 Ethernet source address 为：ac:74:09:35:8a:e2；

这既不是主机地址也不是 gaia.cs.umass.edu 的地址，这是主机所在子网的网关 MAC 地址。对应网关路由器拥有该地址。

```
> Frame 46: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{DAE83349-57D2-442D-9C46-E61E45E6B3EF}, id 0
  Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
    > Destination: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
    > Source: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
    Type: IPv4 (0x0800)
  Data (1500 bytes)
    Data: 450005dca68d4002006c6b88077f50c72d6ff7b0050e86d5a0ed2ba4483d168501000ed...
    [Length: 1500]
```

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

Ans: Destination address: e0:d4:e8:ef:93:5e;

这是我主机的以太网地址。

```

> Frame 46: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{DAE8334
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
  > Destination: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
  > Source: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
  Type: IPv4 (0x0800)
  > Data (1500 bytes)
    Data: 450005dca68d40002006c6b88077f50c72d6ff7b0050e86d5a0ed2ba4483d168501000ed...
    [Length: 1500]

```

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

Ans: 0x0800, 与之相对应的上层协议为 IPv4。

```

> Frame 46: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{DAE8334
Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
  > Destination: IntelCor_ef:93:5e (e0:d4:e8:ef:93:5e)
  > Source: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
  Type: IPv4 (0x0800)
  > Data (1500 bytes)
    Data: 450005dca68d40002006c6b88077f50c72d6ff7b0050e86d5a0ed2ba4483d168501000ed...
    [Length: 1500]

```

8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?

Ans: 出现在第 68 个字节。

0000	e0 d4 e8 ef 93 5e ac 74 09 35 8a e2 08 00 45 00^..t..5.....E..
0010	05 dc a6 8d 40 00 20 06 c6 b8 80 77 f5 0c 72 d6@..w...r..
0020	ff 7b 00 50 e8 6d 5a 0e d2 ba 44 83 d1 68 50 10	..{.P..mZ.. ..D...hP..
0030	00 ed d9 21 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... ate: Sun
0050	2c 20 30 34 20 44 65 63 20 32 30 32 32 20 30 32	, 04 Dec 2022 02
0060	3a 31 30 3a 34 31 20 47 4d 54 0d 0a 53 65 72 76	:10:41 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	l/2.0.11 Perl/v5
00c0	2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69	.16.3...L ast-Modi
00d0	66 69 65 64 3a 20 53 61 74 2c 20 30 33 20 44 65	fied: Sa t, 03 De
00e0	63 20 32 30 32 32 20 30 36 3a 35 39 3a 30 31 20	c 2022 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

Part 2: The Address Resolution Protocol

1. 实验内容:

研究 ARP 协议的运行。

注意区分 arp 命令及 ARP 协议。arp 命令用于显示和修改地址解析协议 (ARP)使用的“IP 到物理”地址转换表。ARP 缓存中包含一个或多个表，它们用于存储 IP 地址及其经过解析的以太网或令牌环物理地址。

2. 实验流程及问题回答:

- 1) 打开 MS-DOS command line 输入“c:\windows\system32\arp”。
- 2) 没有参数的 Windows arp 命令将显示计算机上 arp 缓存的内容。运行 arp 命令，显示如下：

```
命令提示符

显示和修改地址解析协议(ARP)使用的“IP 到物理”地址转换表。

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          通过询问当前协议数据，显示当前 ARP 项。
             如果指定 inet_addr，则只显示指定计算机
             的 IP 地址和物理地址。如果不止一个网络
             接口使用 ARP，则显示每个 ARP 表的项。
-g          与 -a 相同。
-v          在详细模式下显示当前 ARP 项。所有无效项
             和坏回接口上的项都将显示。
inet_addr   指定 Internet 地址。
-N if_addr  显示 if_addr 指定的网络接口的 ARP 项。
-d          删除 inet_addr 指定的主机。inet_addr 可
             以是通配符 *，以删除所有主机。
-s          添加主机并且将 Internet 地址 inet_addr
             与物理地址 eth_addr 相关联。物理地址是用
             连字符分隔的 6 个十六进制字节。该项是永久的。
eth_addr    指定物理地址。
if_addr     如果存在，此项指定地址转换表应修改的接口
             的 Internet 地址。如果不存在，则使用第一
             个适用的接口。

示例：
> arp -s 157.55.85.212 00-aa-00-62-c6-09... 添加静态项。
> arp -a          .... 显示 ARP 表。

C:\Users\华为>
```

(图 1-4 arp 命令显示界面)

- 3) 由于版本系统并不完全相同，在我的电脑上运行没有参数的 Windows arp 命令并不会显示计算机上 arp 缓存的内容。需要运行 arp -a 命令，显示如下：

```
命令提示符

C:\Users\华为>arp -a

接口: 192.168.133.1 --- 0x10
Internet 地址 物理地址 类型
192.168.133.255 ff-ff-ff-ff-ff-ff 静态
224.0.0.22 01-00-5e-00-00-16 静态
224.0.0.251 01-00-5e-00-00-fb 静态
224.0.0.252 01-00-5e-00-00-fc 静态
239.255.255.250 01-00-5e-7f-ff-fa 静态

接口: 192.168.118.1 --- 0x11
Internet 地址 物理地址 类型
192.168.118.255 ff-ff-ff-ff-ff-ff 静态
224.0.0.22 01-00-5e-00-00-16 静态
224.0.0.251 01-00-5e-00-00-fb 静态
224.0.0.252 01-00-5e-00-00-fc 静态
239.255.255.250 01-00-5e-7f-ff-fa 静态

接口: 114.214.255.123 --- 0x14
Internet 地址 物理地址 类型
114.214.216.1 ac-74-09-35-8a-e2 动态
114.214.240.1 ac-74-09-35-8a-e2 动态
114.214.255.255 ff-ff-ff-ff-ff-ff 静态
224.0.0.22 01-00-5e-00-00-16 静态
224.0.0.251 01-00-5e-00-00-fb 静态
224.0.0.252 01-00-5e-00-00-fc 静态
239.255.255.250 01-00-5e-7f-ff-fa 静态
255.255.255.255 ff-ff-ff-ff-ff-ff 静态

C:\Users\华为>
```

(图 1-5 ARP 缓存显示界面)

9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?

Ans:

接口: 192.168.133.1 --- 0x10

Internet 地址	物理地址	类型
192.168.133.255	ff-ff-ff-ff-ff-ff	静态
224.0.0.22	01-00-5e-00-00-16	静态
224.0.0.251	01-00-5e-00-00-fb	静态
224.0.0.252	01-00-5e-00-00-fc	静态
239.255.255.250	01-00-5e-7f-ff-fa	静态

接口: 192.168.118.1 --- 0x11

Internet 地址	物理地址	类型
192.168.118.255	ff-ff-ff-ff-ff-ff	静态
224.0.0.22	01-00-5e-00-00-16	静态

224.0.0.251	01-00-5e-00-00-fb	静态
224.0.0.252	01-00-5e-00-00-fc	静态
239.255.255.250	01-00-5e-7f-ff-fa	静态

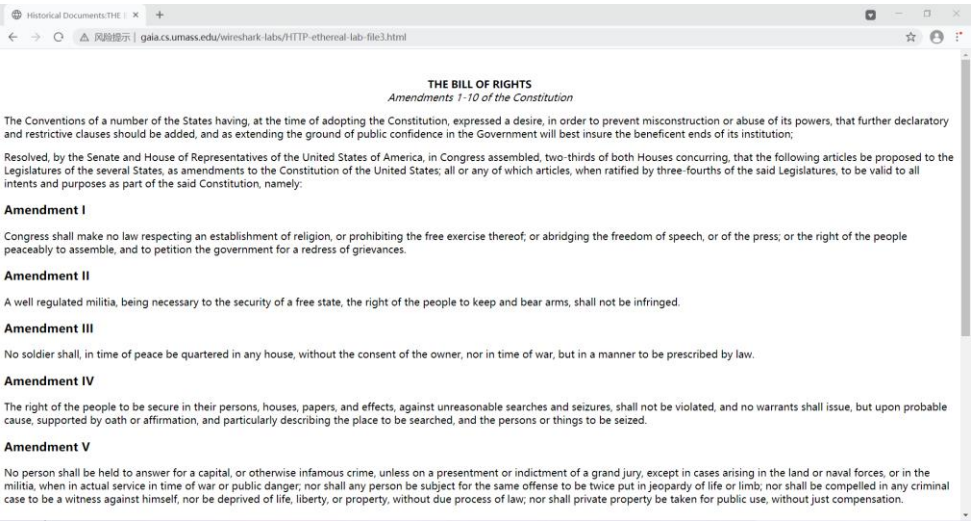
接口: 114.214.255.123 --- 0x14

Internet 地址	物理地址	类型
114.214.216.1	ac-74-09-35-8a-e2	动态
114.214.240.1	ac-74-09-35-8a-e2	动态
114.214.255.255	ff-ff-ff-ff-ff-ff	静态
224.0.0.22	01-00-5e-00-00-16	静态
224.0.0.251	01-00-5e-00-00-fb	静态
224.0.0.252	01-00-5e-00-00-fc	静态
239.255.255.250	01-00-5e-7f-ff-fa	静态
255.255.255.255	ff-ff-ff-ff-ff-ff	静态

不同接口指示不同的网卡对应的 IP 地址；Internet 地址对应目的 IP 地址；物理地址表示 IP 地址对应的 MAC 地址；类型指示该条目的获取方式：类型列的“动态”表示使用 ARP 请求广播动态获取到的条目，“静态”表示是手工配置和维护的 ARP 表。

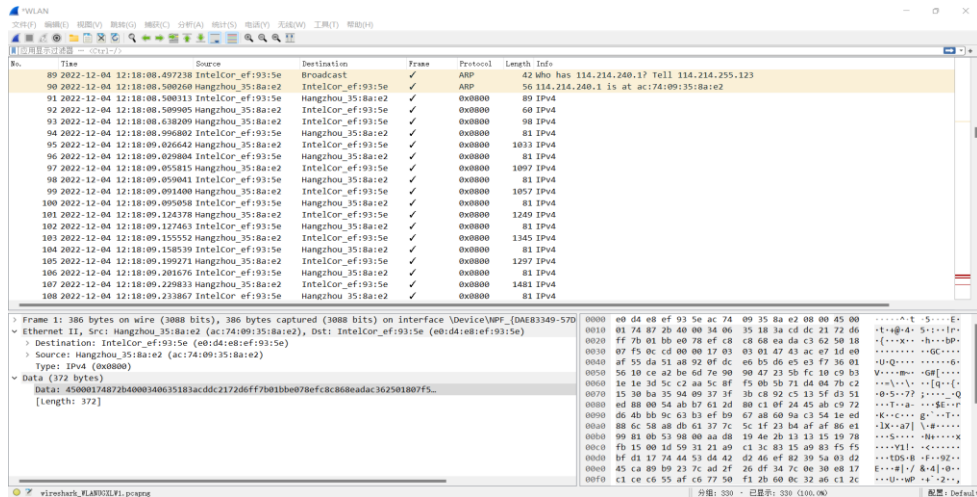
- 4) 运行 `arp -d` 命令清除 arp 缓存。
- 5) 清除浏览器缓存，开启 Wireshark 抓包。
- 6) 输入 URL: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>

显示界面如图：



(图 1-6 输入网址显示界面)

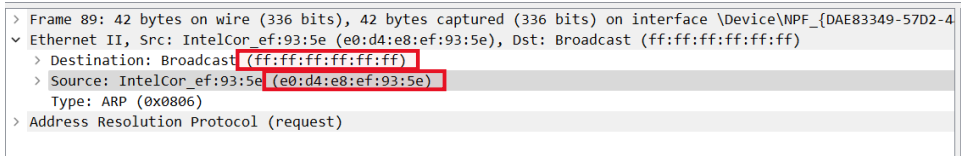
- 7) 停止抓包。更改 Wireshark 的“捕获包列表”窗口，使其仅显示 IP 以下协议的信息。更改后显示界面如下：



(图 1-7 Wireshark 抓包界面)

10. 10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

Ans: Source address: e0:d4:e8:ef:93:5e;
Destination address: ff:ff:ff:ff:ff:ff;



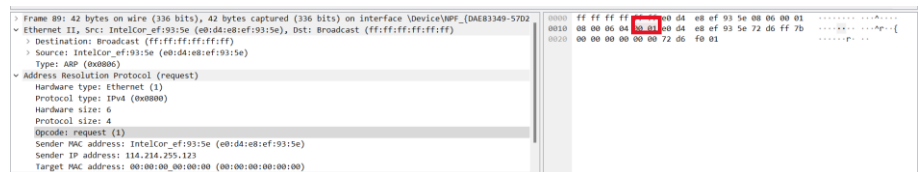
11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

Ans: 0x0806, 对应的上层协议为 ARP 协议;

12. Download the ARP specification from <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>.

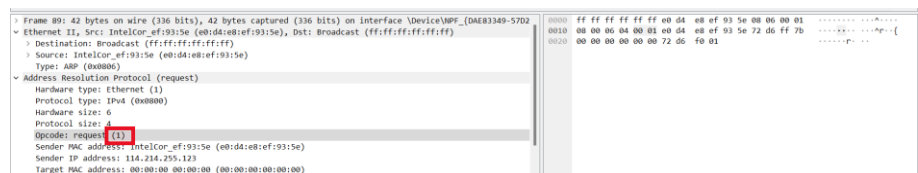
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

Ans: ARP opcode 域从第 21 字节开始;



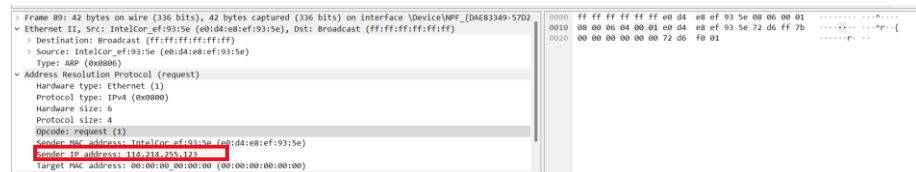
b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

Ans: ARP 请求中 ARP opcode 域的值为 1;



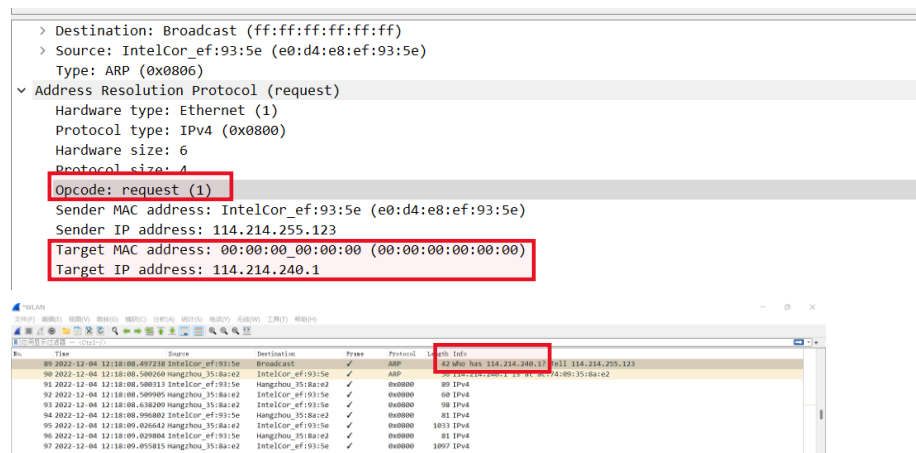
c) Does the ARP message contain the IP address of the sender?

Ans: 包含，发送方 IP 地址为 114.214.255.123;



- d) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

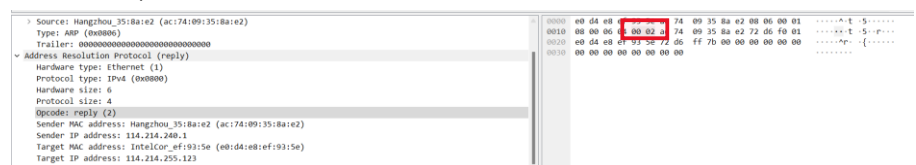
Ans: Opcode 的值为 1，代表查询 MAC 地址，且 Target MAC address 为空。
(也可以从 info 里看出):



13. Now find the ARP reply that was sent in response to the ARP request.

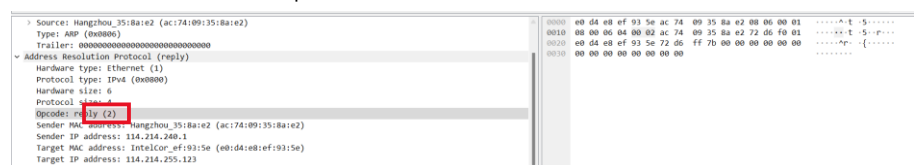
- a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

Ans: ARP opcode 域从第 21 字节开始;



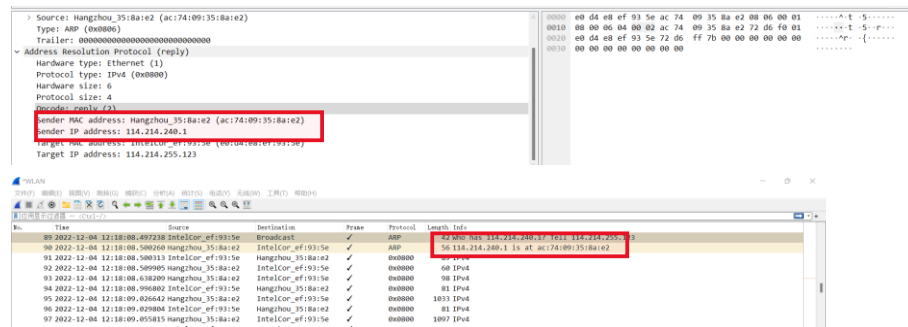
- b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

Ans: ARP 请求中 ARP opcode 域的值为 2;



- c) Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

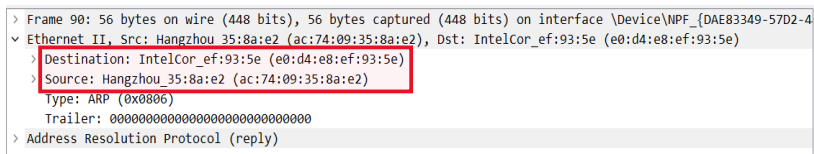
Ans: 在 Sender MAC address 中。(也可以从 info 里看出):



14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

Ans: Source address: ac:74:09:35:8a:e2;

Destination address: e0:d4:e8:ef:93:5e;



15. Open the ethernet-ethereal-trace-1 trace file in <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

Ans: 因为 ARP 请求是广播的，但是 ARP 响应是单播的，只有发送请求的主机可以接收到响应报文。第二次发送 ARP 请求的源不是对应主机，因此无法接收到 ARP 响应信息。

No.	Time	Source	Destination	Frame	Protocol	Length	Info
1	2004-08-29 01:19:20.157130	AmbitMic_a9:3d:68	Broadcast	✓	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	2004-08-29 01:19:20.158148	LinksysG_da:af:73	AmbitMic_a9:3d:68	✓	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	2004-08-29 01:19:20.158158	AmbitMic_a9:3d:68	LinksysG_da:af:73	✓	0x0800	62	IPv4
4	2004-08-29 01:19:23.119980	AmbitMic_a9:3d:68	LinksysG_da:af:73	✓	0x0800	62	IPv4
5	2004-08-29 01:19:29.128440	AmbitMic_a9:3d:68	LinksysG_da:af:73	✓	0x0800	62	IPv4
6	2004-08-29 01:19:33.700004	CnetTech_73:8d:ce	Broadcast	✓	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	2004-08-29 01:19:37.601633	AmbitMic_a9:3d:68	LinksysG_da:af:73	✓	0x0800	62	IPv4
8	2004-08-29 01:19:37.623832	LinksysG_da:af:73	AmbitMic_a9:3d:68	✓	0x0800	62	IPv4
9	2004-08-29 01:19:37.623857	AmbitMic_a9:3d:68	LinksysG_da:af:73	✓	0x0800	54	IPv4
10	2004-08-29 01:19:37.623598	AmbitMic_a9:3d:68	LinksysG_da:af:73	✓	0x0800	686	IPv4
11	2004-08-29 01:19:37.651896	LinksysG_da:af:73	AmbitMic_a9:3d:68	✓	0x0800	60	IPv4
12	2004-08-29 01:19:37.656065	LinksysG_da:af:73	AmbitMic_a9:3d:68	✓	0x0800	1514	IPv4
13	2004-08-29 01:19:37.657155	LinksysG_da:af:73	AmbitMic_a9:3d:68	✓	0x0800	1514	IPv4
14	2004-08-29 01:19:37.657199	AmbitMic_a9:3d:68	LinksysG_da:af:73	✓	0x0800	54	IPv4
15	2004-08-29 01:19:37.684187	LinksysG_da:af:73	AmbitMic_a9:3d:68	✓	0x0800	1514	IPv4
16	2004-08-29 01:19:37.684552	LinksysG_da:af:73	AmbitMic_a9:3d:68	✓	0x0800	489	IPv4
17	2004-08-29 01:19:37.684587	AmbitMic_a9:3d:68	LinksysG_da:af:73	✓	0x0800	54	IPv4

0000	e0 d4 e8 ef 93 5e ac 74 09 35 8a e2 08 00 45 00^..t..5.....E..
0010	05 dc a6 8d 40 00 20 06 c6 b8 80 77 f5 0c 72 d6@..w...r..
0020	ff 7b 00 50 e8 6d 5a 0e d2 ba 44 83 d1 68 50 10	{..P..mZ.. ..D...hP..
0030	00 ed d9 21 00 00 48 54 54 50 2f 31 2e 31 20 32	...!...HT TP/1.1 2
0040	30 30 20 4f 40 0d 0a 44 61 74 65 3a 20 53 75 6e	00 OK... ate: Sun
0050	2c 20 30 34 20 44 65 63 20 32 30 32 32 20 30 32	, 04 Dec 2022 02
0060	3a 31 30 3a 34 31 20 47 4d 54 0d 0a 53 65 72 76	:10:41 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	l/2.0.11 Perl/v5
00c0	2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69	.16.3...L ast-Modi
00d0	66 69 65 64 3a 20 53 61 74 2c 20 30 33 20 44 65	fied: Sa t, 03 Dec
00e0	63 20 32 30 32 32 20 30 36 3a 35 39 3a 30 31 20	c 2022 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

Part 3: Extra Credit

1. 问题回答:

16. The arp command: `arp -s InetAddr EtherAddr` allows you to manually add an entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

Ans: 此时主机将无法访问该 IP 地址对应的主机，但是它可以错误 MAC 地址对应的主机通信，直到 TTL 过期。

17. What is the default amount of time that an entry remains in your ARP cache before being removed. You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation. Indicate how/where you determined this value.?

Ans: 查阅华为的系统文档，发现缺省情况下，动态 ARP 表项的老化超时时间为 1200 秒，即 20 分钟。可以使用 `arp expire-time` 命令来设置动态 ARP 表项的老化超时时间以及 `undo arp expire-time` 命令来恢复动态 ARP 表项的老化超时时间为缺省值。（静态条目的生存周期见后文）。

命令功能

`arp expire-time`命令用来设置动态ARP表项的老化超时时间。

`undo arp expire-time`命令用来恢复动态ARP表项的老化超时时间为缺省值。

缺省情况下，动态ARP表项的老化超时时间为1200秒，即20分钟。

命令格式

`arp expire-time expire-time`

`undo arp expire-time`

参数说明

参数	参数说明	取值
<code>expire-time</code>	指定ARP表项的老化超时时间。	整数形式，取值范围是30~62640，单位是秒。缺省值是1200秒，即20分钟。

补充内容:

MAC 表与 ARP 表:

MAC 地址表：

交换机在转发数据前需要知道它的每一个端口所连接的主机的 MAC 地址，构建出一个 MAC 地址表。当交换机从某个端口收到数据帧后，读取数据帧中封装的目的地 MAC 地址信息，然后查阅事先构建的 MAC 地址表，找出和目的地地址相对应的端口，从该端口把数据转发出去，其他端口则不受影响，这样避免了与其它端口上的数据发生碰撞。

ARP 表：

主机发送信息时将包含目标 IP 地址的 ARP 请求广播到局域网络上的所有主机，并接收返回消息，以此确定目标的物理地址。收到返回消息后主机将该 IP 地址和物理地址存入本机 ARP 缓存中并保留一定时间，下次请求时直接查询 ARP 缓存以节约资源，于是就形成了 ARP 表。

无论是主机还是交换机都会有一个用来缓存同一网段设备 IP 地址和 MAC 地址的 ARP 映射表用于数据帧的转发。设备通过 ARP 解析到目的 MAC 之后，将会在自己的 ARP 映射表中增加 IP 地址到 MAC 地址的映射表，以用于后续到同一目的地数据帧的转发。

ARP 静态条目的生命周期：

上述问题中回答了动态条目的生存周期。而静态条目一直保留在 ARP 缓存中，意思是永久生效。但在不同的操作系统中，静态条目的保存方式是不同的。例如，在 Windows XP 系统中，重新启动计算机后该条目失效。而在 Windows 7 中，即使重新启动计算机后，该静态条目仍然保存。

ARP 欺骗攻击：

ARP 是建立在局域网中各个主机互相信任的基础上的，它的诞生使得网络能够更加高效的运行，但由于它没有安全认证机制，本身存在着很多漏洞和不足。

ARP 转换映射表，是依赖于计算机中“高速缓冲存储器”动态更新的，而“高速缓冲存储器”的更新，是受到更新周期的限制的，只能保存最近使用的“地址映射的关系表项”，这使得攻击者有了可乘之机，可以在“高速缓冲存储器”更新表项之前，修改 ARP 转换映射表，以实现攻击。ARP 请求是以广播的形式发送的，局域网上的所有主机，都可以自主地发送 ARP 应答消息，并且当其他主机收到应答消息时，不会检测该消息的真实性，就将其记录在本地的“ARP 缓存表”中。这样攻击者就可以向目标主机发送伪造的“ARP 请求包”（错误的 IP 地址和 MAC 地址的映射关系），从而篡改目标主机的本地“ARP 缓存表”。

ARP 欺骗可以导致目标主机与网关通信失败，更会导致通信重定向，可以使所有的数据均通过攻击者的主机，因此存在极大的安全隐患。