山东大学 计算机 学院

计算机网络 课程实验报告

学号：	姓名：	班级：
实验题目： Ethernet and ARP		
实验学时：2h	实验日期： 2023.05.08	
实验目的： 学习有关 Ethernet 和 ARP 的相关知识		
硬件环境： Windows10 家庭版		
软件环境： Wireshark		

实验步骤与内容：

实验内容：

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

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.

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

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

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?

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

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

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?

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

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame

containing the ARP request message?

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

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?

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?

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

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

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?

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?

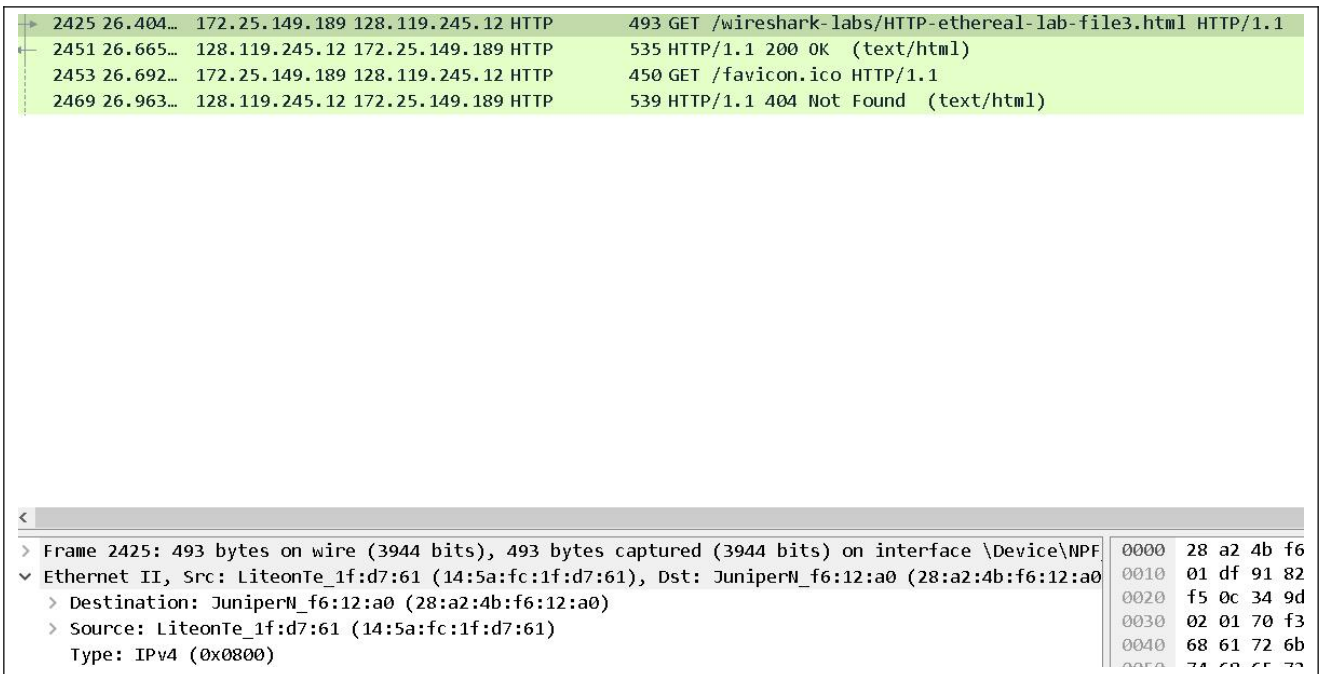
c) Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

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

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?

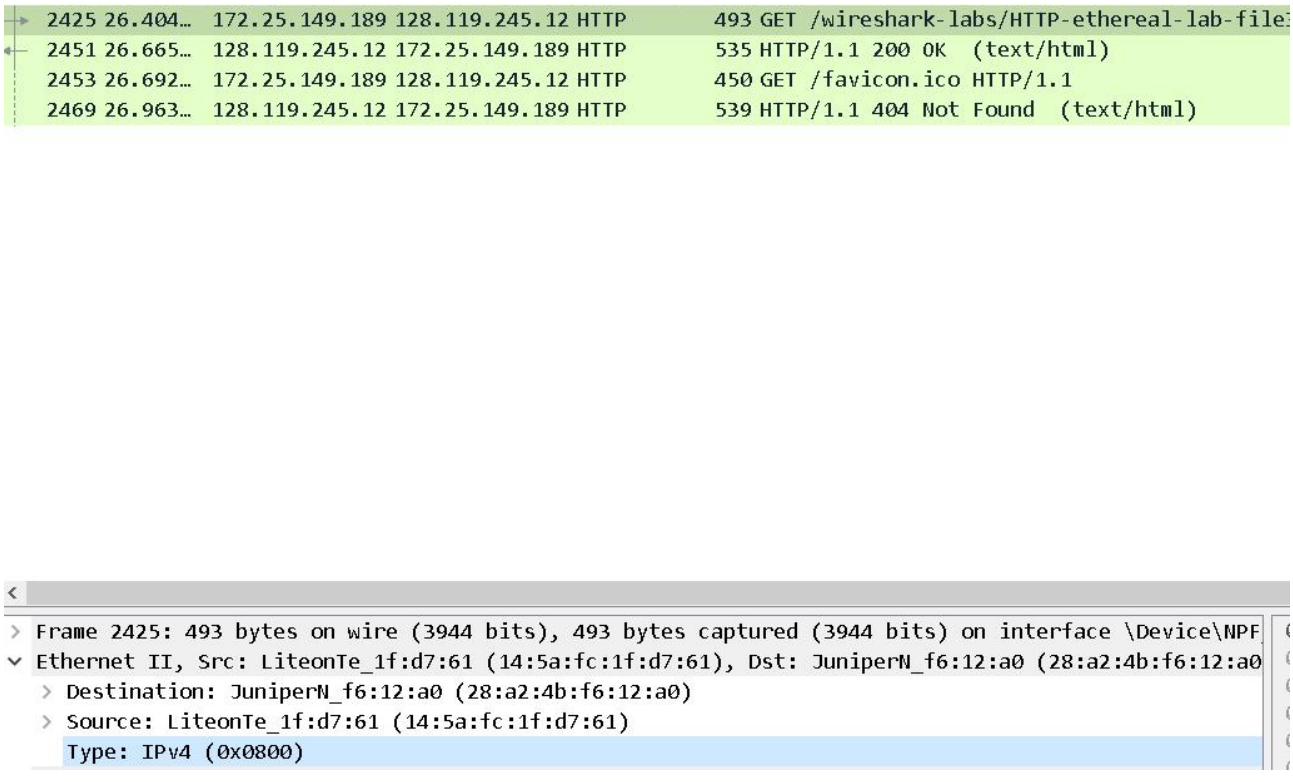
实验步骤：
根据实验指导书进行抓包，并查看相应的封包，本实验主要学习 ARP 的内容，在命令行中输入 arp -a 可以查看相关缓存信息。

1. 本机的 48 位以太网地址是 14:5a:fc:1f:d7:61。

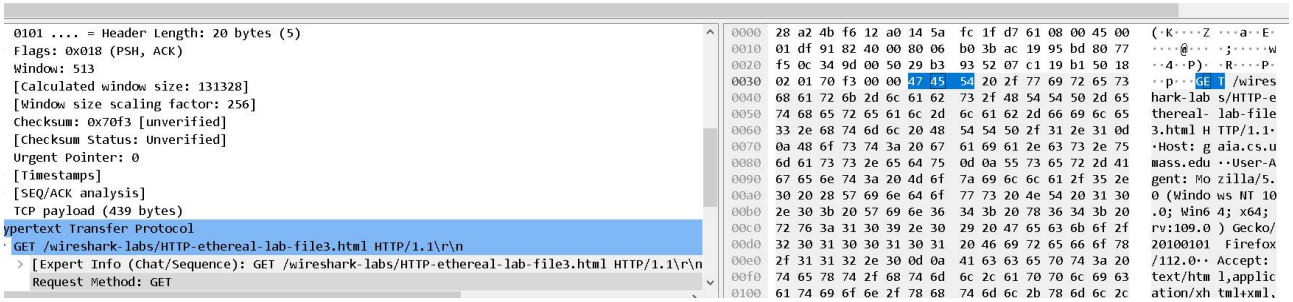


2. 以太网帧中的目标地址是 28:a2:4b:f6:12:a0，并不是 gaia.cs.umass.edu 的以太网地址，而是我们连接该子网路由器的 MAC 地址。

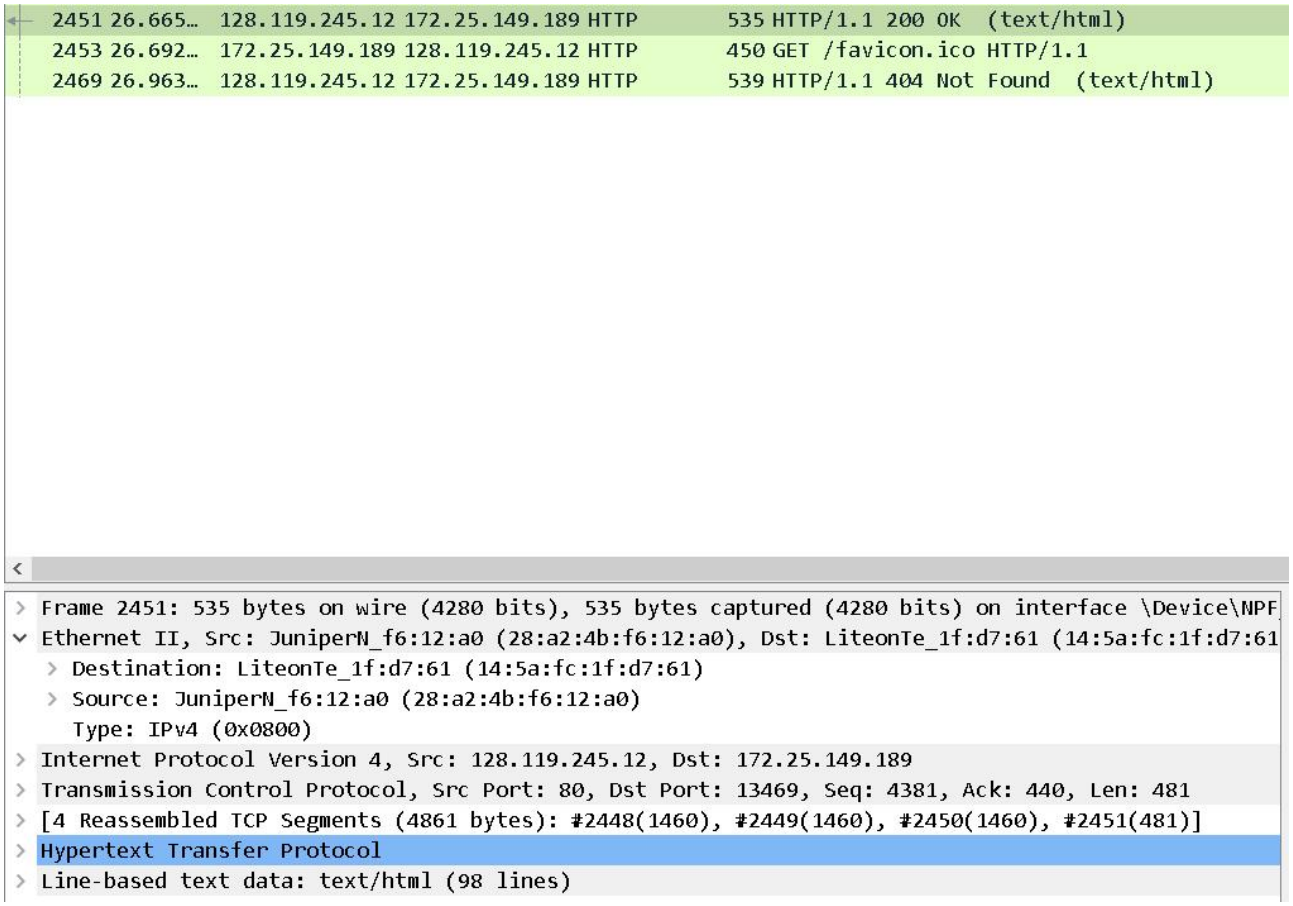
3. 16 进制的值是 0x0800，对应的上层协议是 IPv4。



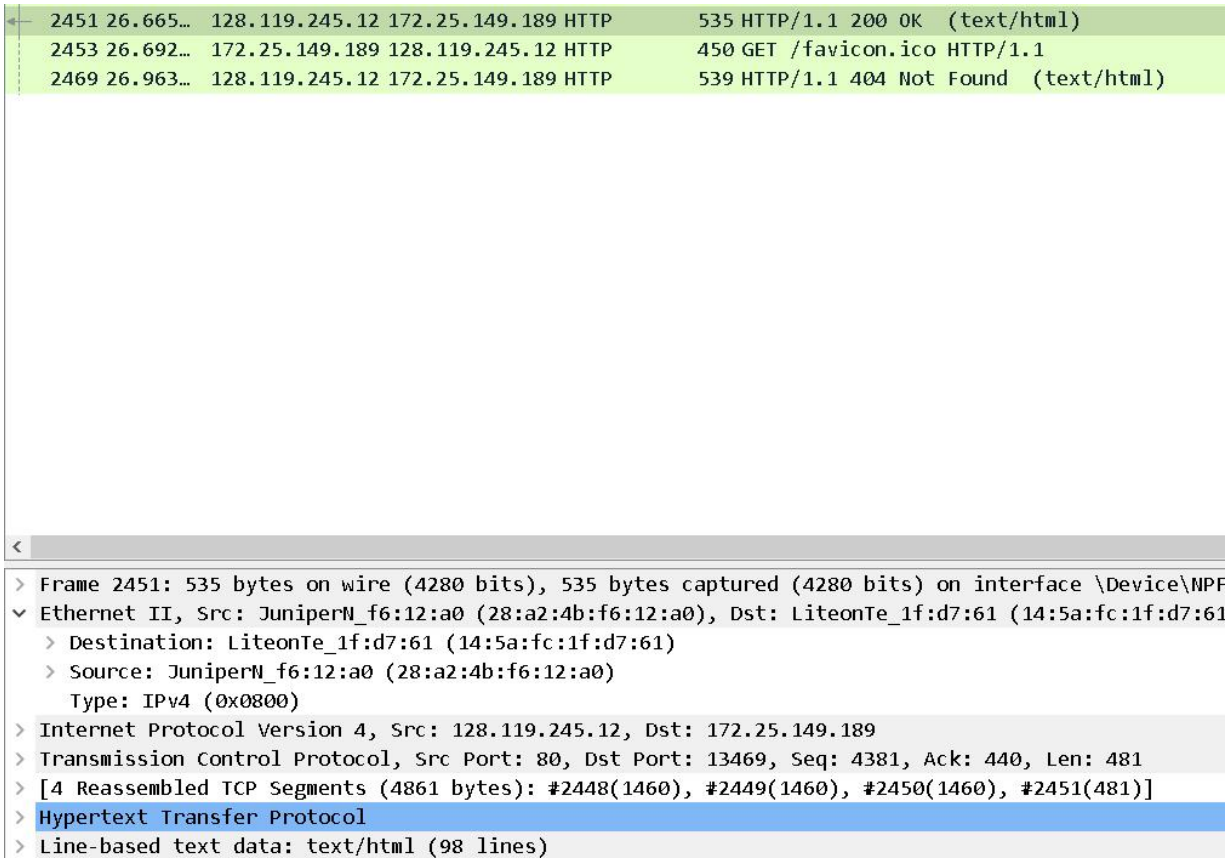
4. 可以看到 GET 前面有 16*3+6=54 个字节，而 G 出现在以太网帧中的 55 个字节。



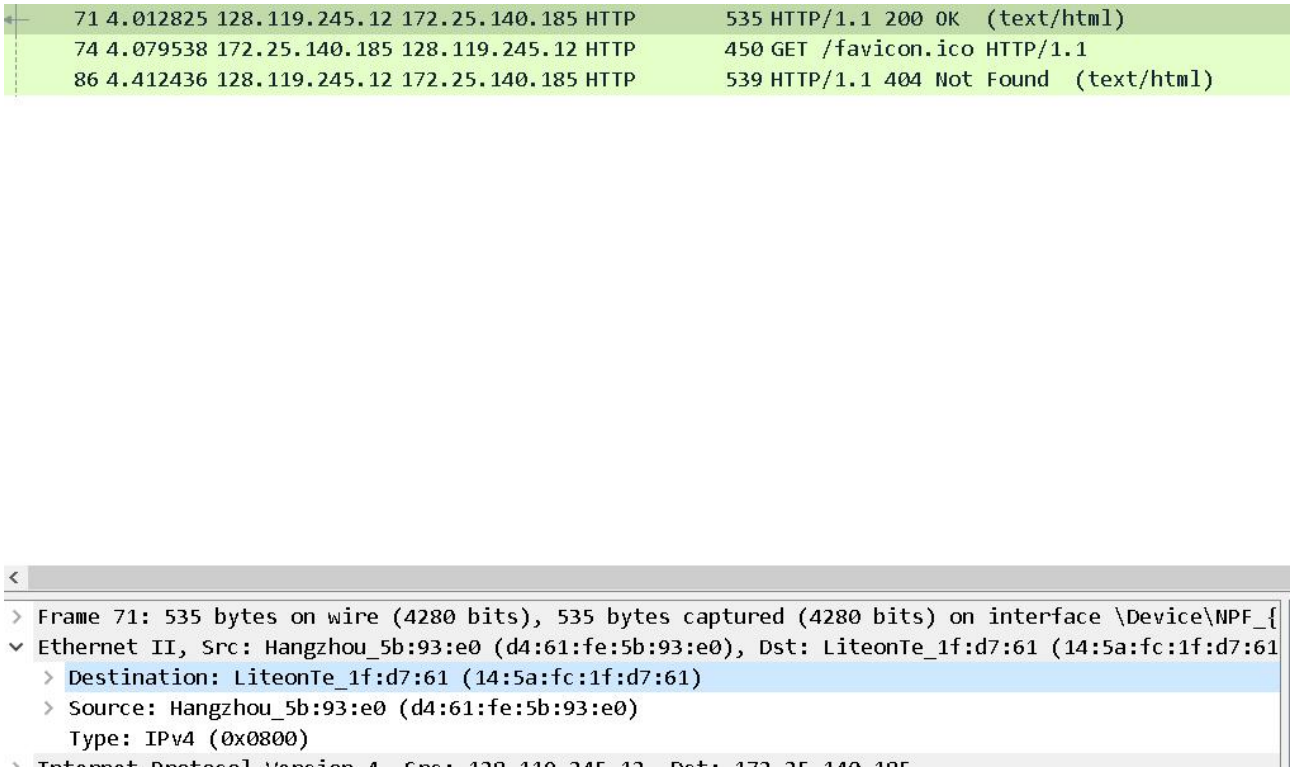
5. 以太网源地址的值是 28:a2:4b:f6:12:a0，这是连接该子网的路由器的 MAC 地址。



6. 以太网帧中的目标地址是 14:5a:fc:1f:d7:61，是本机的以太网地址。



7. 16 进制的值是 0x0800，对应的上层协议是 IPv4 协议。



8. OK 前面有 13 个字节，OK 出现在以太网帧中的 14 个字节。

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 4d  6f 6e 2c 20 30 38 20 4d   ·Date: M on, 08 M
0020  61 79 20 32 30 32 33 20  30 36 3a 31 39 3a 31 38   ay 2023  06:19:18
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.4.
0070  33 33 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   33 mod_p erl/2.0.
0080  31 31 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   11 Perl/ v5.16.3·
0090  0a 4c 61 73 74 2d 4d 6f  64 69 66 69 65 64 3a 20   ·Last-Mo dified:
00a0  4d 6f 6e 2c 20 30 38 20  4d 61 79 20 32 30 32 33   Mon, 08  May 2023
00b0  20 30 35 3a 35 39 3a 30  31 20 47 4d 54 0d 0a 45    05:59:0 1 GMT··E
00c0  54 61 67 3a 20 22 31 31  39 34 2d 35 66 62 32 38   Tag: "11 94-5fb28
00d0  35 35 64 65 34 32 62 63  22 0d 0a 41 63 63 65 70   55de42bc "··Accep
00e0  74 2d 52 61 6e 67 65 73  3a 20 62 79 74 65 73 0d   t-Ranges : bytes·
00f0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
```

9. 第一列的值是 IP 地址，第二列的值是 MAC 地址，而第三列的值则是类型。

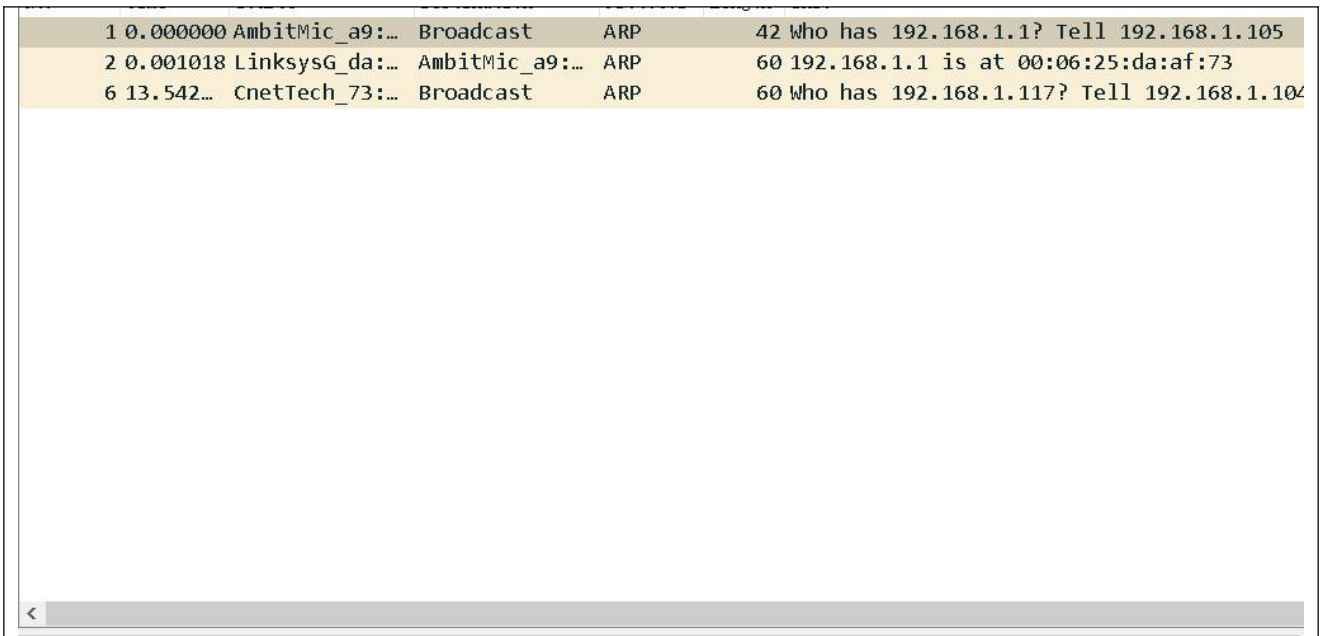
```
接口: 172.25.149.189 --- 0x3
  Internet 地址         物理地址              类型
  172.25.255.254        28-a2-4b-f6-12-a0     动态
  172.25.255.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态

接口: 2.0.0.1 --- 0x9
  Internet 地址         物理地址              类型
  2.0.0.255             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: 192.168.182.1 --- 0xd
  Internet 地址         物理地址              类型
  192.168.182.254       00-50-56-e7-9f-33     动态
  192.168.182.255       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: 192.168.213.1 --- 0x14
  Internet 地址         物理地址              类型
  192.168.213.254       00-50-56-f4-e1-be     动态
  192.168.213.255       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
```

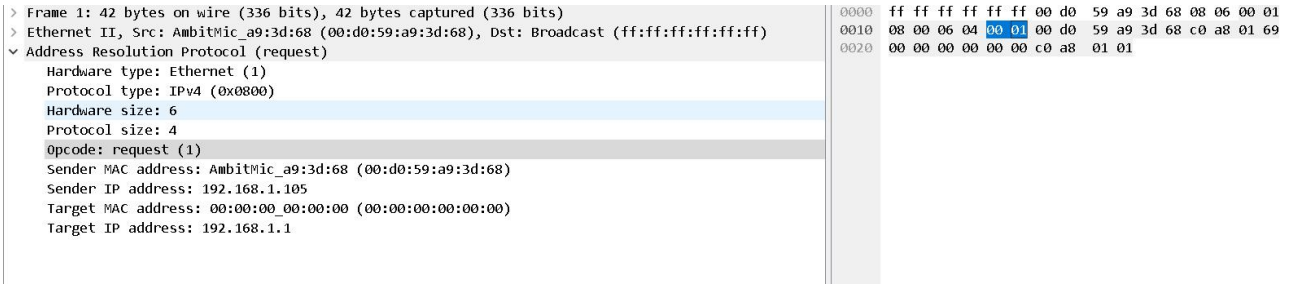
10. 源地址是 00:d0:59:a9:3d:68，目标地址是 ff:ff:ff:ff:ff:ff。



11. 十六进制的值是 0x0806，对应的上层协议是 ARP。

12.

（1）从最开头开始 20 个字节。



（2）操作码字段的值是 1。

（3）包括了发送方的 IP 地址。

```
     1 0.000000 AmbitMic_a9:… Broadcast      ARP         42 Who has 192.168.1.1? Tell 192.168.1.105
     2 0.001018 LinksysG_da:… AmbitMic_a9:… ARP         60 192.168.1.1 is at 00:06:25:da:af:73
     6 13.542… CnetTech_73:… Broadcast      ARP         60 Who has 192.168.1.117? Tell 192.168.1.104
```

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Sender IP address: 192.168.1.105
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1
```

（4）从操作码的值可以看出，值为 1 表示 ARP 请求，也就是查询响应 IP 的以太网地址。

13.

（1）最开头开始的 20 个字节。

```
     2 0.001018 LinksysG_da:… AmbitMic_a9:… ARP         60 192.168.1.1 is at 00:06:25:da:af:73
     6 13.542… CnetTech_73:… Broadcast      ARP         60 Who has 192.168.1.117? Tell 192.168.1.104
```

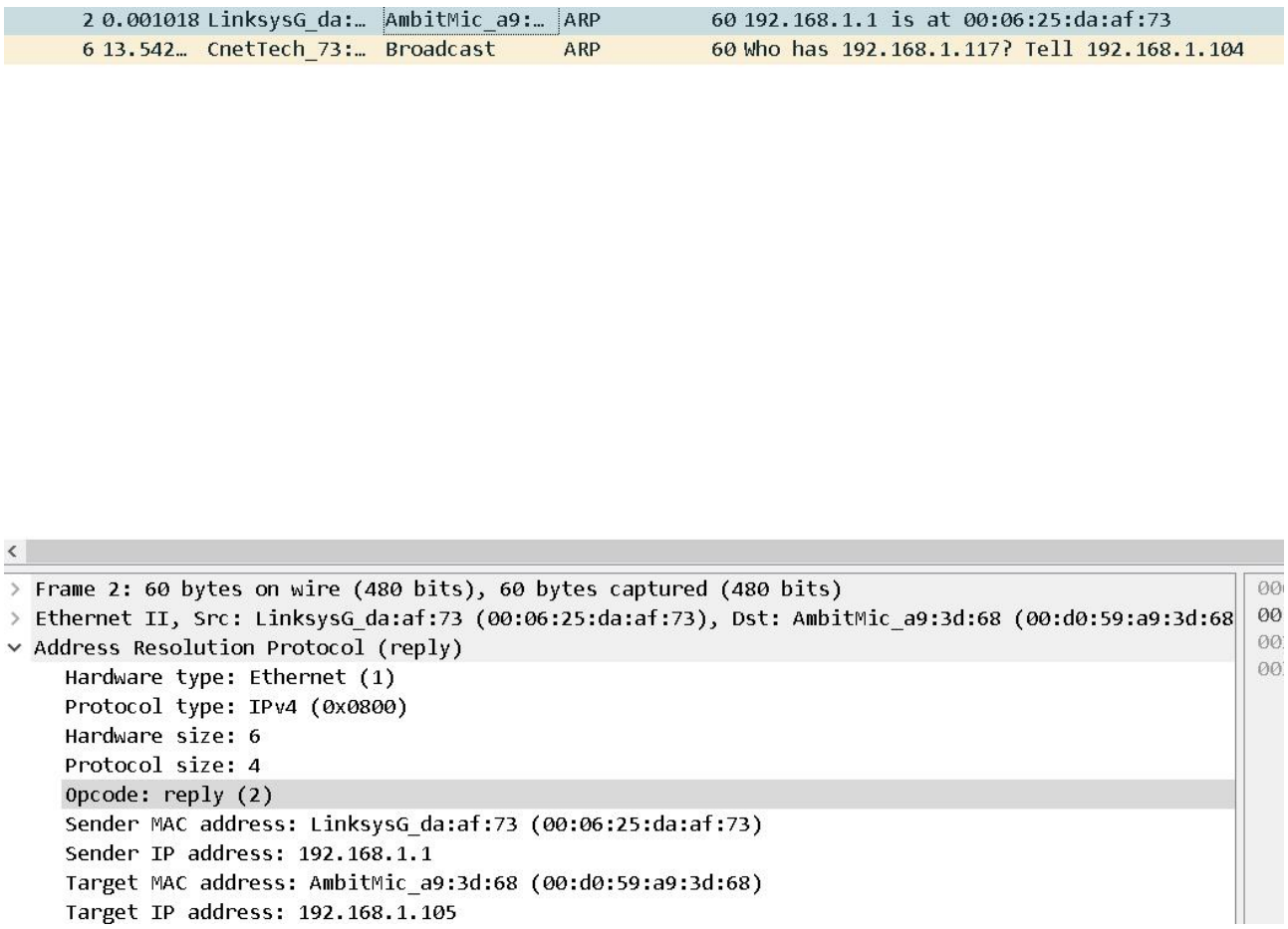
```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105
```

```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01
0010  08 00 06 04 00 02 00 06  25 da af 73 c0 a8 01 01
0020  00 d0 59 a9 3d 68 c0 a8  01 69 00 00 00 00 00 00
0030  00 00 00 00 00 00 00 00  00 00 00 00
```

（2）操作码的值是 2。

（3）放在 Sender MAC address 里面。

14. 源地址的十六进制值是 00:06:25:da:af:73，而目标地址的十六进制值是 00:d0:59:a9:3d:68。



15. 查询 APR 报文是在广播帧中发送的（子网中的所有电脑都能收到），而响应 APR 报文在一个标准帧中发送（只有发送请求的那台电脑能收到），其他的主机发现请求的 IP 地址不匹配会丢弃。

结论分析与体会：

通过本次实验对 ARP 的相关知识有了更多的了解，通过查看相关信息，来学习 ARP 的知识，对以太网以及以太网帧有了更进一步的认知。