

山东大学 计算机科学与技术 学院

新兴网络技术与实践 课程实验报告

学号：202300130183	姓名：宋浩宇	班级：23 级智能班
实验题目：Wireshark Lab: Ethernet and ARP v8.0		
实验学时：4	实验日期：2025/5/14	
实验目的：学习了解 Ethernet 和 ARP		
实验结果：		
1. What is the 48-bit Ethernet address of your computer?		
<div><div>▼ Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)</div><div>> Destination: LinksysGroup_da:af:73 (00:06:25:da:af:73)</div><div>> Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)</div><div>Type: IPv4 (0x0800)</div><div>[Stream index: 1]</div></div>		
如图，是 00:d0:59:a9:3d:68		
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.]		
<div><div>▼ Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)</div><div>▼ Destination: LinksysGroup_da:af:73 (00:06:25:da:af:73)</div><div>.... ..0. = LG bit: Globally unique address (factory default)</div><div>.... ..0. = IG bit: Individual address (unicast)</div><div>> Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)</div><div>Type: IPv4 (0x0800)</div><div>[Stream index: 1]</div></div>		
如图，是 00:06:25:da:af:73，不是 gaia.cs.umass.edu 的地址，是本地网关的地址。		

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

```
Frame 10: 1460 bytes on wire (11680 bits), 1460 bytes captured (11680 bits) on 0
Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)
  Destination: LinksysGroup_da:af:73 (00:06:25:da:af:73)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    Type: IPv4 (0x0800)
    [Stream index: 1]
  Internet Protocol Version 4, Src: 192.168.1.105, Dst: 128.119.245.12
```

如图，值是 0x0800，表示 IPv4 上层协议

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

```
000  00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00  ..%..s..Y.=h..E.
010  02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69 80 77  ....@...i.w
020  f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4 50 18  ...".Pe....?.P.
030  fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72  ..~O:GET/ether
040  65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74  eal-labs/HTTP-et
050  68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33  hereal-l ab-file3
060  7a 68 74 6d 6c 2d 48 54 54 50 2f 31 2a 31 0d 0a  html HT TP/1 1..
```

如图，应该是第 55 字节（从 1 开始计数）

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?

```
Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
  Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 1]
```

如图，源地址是 00:06:25:da:af:73，这个不是 gaia.cs.umass.edu 的地址，是本地网关的地址。

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

```
Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
  Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 1]
  Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105
```

如图，目标地址是 00:d0:59:a9:3d:68，这是本地计算机的地址。

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

```

Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
  Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 1]

```

如图，值是 0x0800，上层协议是 IPv4

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?

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 53 61 74 2c 20 32 38 20 41	Date: Sat, 28 Aug 2004 17:19:37
0020	75 67 20 32 30 30 34 20 31 37 3a 31 39 3a 33 37	GMT Server: Apache/2.0.40 (Red Hat Linux) Last-Modified: Sat, 28 Aug 2004 17:18:53 GMT
0030	20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70	ETag: "1ba5c-1194-69ed940" Accept-Ranges: bytes Content-Length: 450
0040	61 63 68 65 2f 32 2e 30 2e 34 30 20 28 52 65 64	Keep-Alive: timeout=10, max=100 Connection: Keep-Alive
0050	20 48 61 74 20 4c 69 6e 75 78 29 0d 0a 4c 61 73	Content-Type: text/html; charset=ISO-8859-1
0060	74 2d 4d 6f 64 69 66 69 65 64 3a 20 53 61 74 2c	<html><head><title>Historical Documents: THE BILL OF RIGHTS</title></head><body bgcolor="#ffffff" link="#330000" vlink="#666633">
0070	20 32 38 20 41 75 67 20 32 30 30 34 20 31 37 3a	
0080	31 38 3a 35 33 20 47 4d 54 0d 0a 45 54 61 67 3a	
0090	20 22 31 62 61 35 63 2d 31 31 39 34 2d 36 39 65	
00a0	64 39 34 30 22 0d 0a 41 63 63 65 70 74 2d 52 61	
00b0	6e 67 65 73 3a 20 62 79 74 65 73 0d 0a 43 6f 6e	
00c0	74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 34 35 30	
00d0	30 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 3a 20 74	
00e0	69 6d 65 6f 75 74 3d 31 30 2c 20 6d 61 78 3d 31	
00f0	30 30 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20	
0100	4b 65 65 70 2d 41 6c 69 76 65 0d 0a 43 6f 6e 74	
0110	65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68	
0120	74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 49 53 4f	
0130	2d 38 38 35 39 2d 31 0d 0a 0d 0a 3c 68 74 6d 6c	
0140	3e 3c 68 65 61 64 3e 20 0a 3c 74 69 74 6c 65 3e	
0150	48 69 73 74 6f 72 69 63 61 6c 20 44 6f 63 75 6d	
0160	65 6e 74 73 3a 54 48 45 20 42 49 4c 4c 20 4f 46	
0170	20 52 49 47 48 54 53 3c 2f 74 69 74 6c 65 3e 3c	
0180	2f 68 65 61 64 3e 0a 0a 0a 3c 62 6f 64 79 20 62	
0190	67 63 6f 6c 6f 72 3d 22 23 66 66 66 66 66 22	
01a0	20 6c 69 6e 6b 3d 22 23 33 33 30 30 30 30 22 20	
01b0	76 6c 69 6e 6b 3d 22 23 36 36 36 36 33 33 22 3e	

如图，应该是第 489 + 14 = 503 字节（从 1 开始计数）

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


```

C:\Users\23676>arp -a

Interface: 192.168.126.1 --- 0x5
  Internet Address      Physical Address      Type
  192.168.126.254      00-50-56-e9-94-06    dynamic
  192.168.126.255      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
  239.192.152.143      01-00-5e-40-98-8f    static
  239.255.255.250      01-00-5e-7f-ff-fa    static
  255.255.255.255      ff-ff-ff-ff-ff-ff    static

Interface: 192.168.153.1 --- 0x6
  Internet Address      Physical Address      Type
  192.168.153.254      00-50-56-eb-80-07    dynamic
  192.168.153.255      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
  239.192.152.143      01-00-5e-40-98-8f    static
  239.255.255.250      01-00-5e-7f-ff-fa    static
  255.255.255.255      ff-ff-ff-ff-ff-ff    static

Interface: 192.168.56.1 --- 0xc
  Internet Address      Physical Address      Type
  192.168.56.255      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
  239.192.152.143      01-00-5e-40-98-8f    static
  239.255.255.250      01-00-5e-7f-ff-fa    static

Interface: 2.0.0.1 --- 0x11
  Internet Address      Physical Address      Type
  2.0.0.255            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
  239.192.152.143      01-00-5e-40-98-8f    static
  239.255.255.250      01-00-5e-7f-ff-fa    static

Interface: 172.25.178.105 --- 0x18
  Internet Address      Physical Address      Type
  172.25.255.254      28-a2-4b-f6-12-a0    dynamic
  172.25.255.255      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
  239.192.152.143      01-00-5e-40-98-8f    static
  239.255.255.250      01-00-5e-7f-ff-fa    static
  255.255.255.255      ff-ff-ff-ff-ff-ff    static

C:\Users\23676>_

```

如图，这是我的电脑的 ARP 缓存。

每一列的含义分别是：Internet 地址、物理地址、类型。

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

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
  Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), 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: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    [Stream index: 0]
```

如图，源地址是 00:d0:59:a9:3d:68，目标地址是 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?

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
  Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), 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: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
      ....0. .... = LG bit: Globally unique address (factory default)
      ....0. .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    [Stream index: 0]
  Address Resolution Protocol (request)
```

如图，值是 0x0806，上层协议是 ARP

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?

0000	ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01 Y=h...
0010	08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69 Y=h...i
0020	00 00 00 00 00 00 c0 a8 01 01

如图，是第 22 字节（从 1 开始计数）

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?

```

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: AmbitMicrosy_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

```

如图，操作码是 1

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

```

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on 0
v Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), 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)
  v Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)

```

如图，是包含的。

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

```

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: AmbitMicrosy_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

```

如图，在 Target MAC address 字段

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?

```

0000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 06 00 01  ..Y.=h..%.s...
0010 08 00 06 04 00 02 00 06 25 da af 73 c0 a8 01 01  ....02..%.s...
0020 00 d0 59 a9 3d 68 c0 a8 01 69 00 00 00 00 00 00  ..Y.=h..i.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....

```

是第 22 字节（从 1 开始计数）

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?

```

  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: LinksysGroup_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105

```

如图，操作码的值是 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?

```

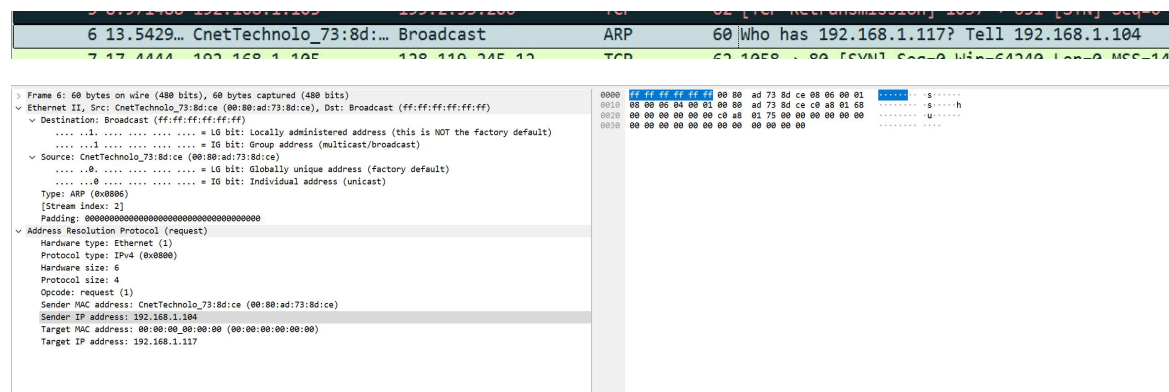
  v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysGroup_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105

```

如图，在 Sender IP address 字段

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



如图，这是那条其他计算机发出的请求。不回复是因为当前计算机的 IP 地址不是 192.168.1.117 EX-1.

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?

手动向 ARP 缓存添加正确 IP 地址但错误以太网地址的条目，会导致网络通信异常，设备按错误以太网地址发送数据帧，目标设备可能无法接收或响应，引发数据包丢失，还可能造成安全风险，需手动修正才能恢复通信。

EX-2.

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.

在 Windows 操作系统中，ARP（Address Resolution Protocol）缓存表的有效时间通常是由网络环境和管理员设置决定的。默认情况下，Windows 的 ARP 缓存项的 TTL 被设置为 2 小时。这意味着，如果一个 ARP 缓存项在 2 小时后没有得到刷新（例如，没有收到新的数据包来更新缓存项），那么这个缓存项就会被清除。实际上，这个值主要与注册表中的 ArpCacheLife 和 ArpCacheMinReferencedLife 这两个项有关。

参考文章：[地址解析协议缓存行为 - Windows Server | Microsoft Learn](#)

问题及收获：

ARP（地址解析协议）和 Ethernet（以太网）是计算机网络底层通信的核心基础：

Ethernet 作为数据链路层协议，定义了局域网内设备间的物理连接和帧传输机制，通过 MAC 地址唯一标识网络设备，实现相邻设备间的可靠数据传输，是构建局域网的主流技术，具有低成本、高兼容性和易于扩展的特点。

ARP 则用于解决 IP 地址与 MAC 地址的映射问题，当设备需要与局域网内其他设备通信时，通过 ARP 协议在本地缓存或网络中查询目标 IP 对应的 MAC 地址，确保数据帧能准确送达目标设备，弥补了 IP 层地址无法直接用于物理传输的不足。

两者结合意义重大：Ethernet 提供了数据传输的物理通道和帧结构，ARP 则打通了 IP 地址与物理地址的转换链路，共同保障了局域网内设备间从逻辑寻址到物理传输的完整通信流程，是 TCP/IP 协议栈实现网络互联的关键环节，也是现代计算机网络稳定运行的基石。