

实验名称: Lab 8: 链路层观察

实验人: 谢志康

学号: 22307110187

时间: 24.12.12 – 24.12.13

一、实验任务一: Ethernet 帧观察

捕获以太网帧

- step1: 清空浏览器缓存
- step2: wireshark 抓包
- step3: 访问 <http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>

No.	Time	Source	Destination	Protocol	Length	Info
14	8.261208	192.168.31.146	128.119.245.12	HTTP	720	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
20	9.698226	192.168.31.146	183.47.121.98	HTTP	967	POST /mtti/08067ef8 HTTP/1.1 (application/octet-stream)
22	9.646493	183.47.121.98	192.168.31.146	HTTP	369	HTTP/1.1 200 OK (application/octet-stream)
54	19.045320	192.168.31.146	128.119.245.12	HTTP	633	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
68	21.058913	192.168.31.146	128.119.245.12	HTTP	720	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
69	21.316888	128.119.245.12	192.168.31.146	HTTP	294	HTTP/1.1 304 Not Modified
82	25.452073	192.168.31.146	23.211.178.227	HTTP	165	GET /connecttest.txt HTTP/1.1
85	25.454370	192.168.31.146	23.211.178.227	HTTP	165	GET /connecttest.txt HTTP/1.1
87	25.521946	23.211.178.227	192.168.31.146	HTTP	241	HTTP/1.1 200 OK (text/plain)
92	25.526716	23.211.178.227	192.168.31.146	HTTP	241	HTTP/1.1 200 OK (text/plain)
106	26.329995	192.168.31.146	23.211.178.224	HTTP	165	GET /connecttest.txt HTTP/1.1
108	26.481834	23.211.178.224	192.168.31.146	HTTP	241	HTTP/1.1 200 OK (text/plain)
184	85.418420	192.168.31.146	128.119.245.12	HTTP	720	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
188	85.416684	128.119.245.12	192.168.31.146	HTTP	294	HTTP/1.1 304 Not Modified

访问后 wireshark 抓包信息 (部分) 如上。

选中包含 HTTP GET 消息的以太网帧, 回答以下问题:

- 你的电脑的 mac 地址是多少?

```
✓ Ethernet II, Src: Intel_15:ff:31 (20:c1:9b:15:ff:31), Dst: XiaomiMobile_e5:95:10 (24:cf:24:e5:95:10)
  Destination: XiaomiMobile_e5:95:10 (24:cf:24:e5:95:10)
    ... ..0. .... = LG bit: Globally unique address (factory default)
    ... ..0. .... = IG bit: Individual address (unicast)
  Source: Intel_15:ff:31 (20:c1:9b:15:ff:31)
    ... ..0. .... = LG bit: Globally unique address (factory default)
    ... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 0]
```

我的电脑的 mac 地址也就是源 mac 地址是 **20:c1:9b:15:ff:31**

- 以太网帧的目标 mac 地址是多少? 这个地址是 gaia.cs.umass.edu 的 mac 地址吗?

目标 mac 地址是 **24:cf:24:e5:95:10**

但它并不是该网址的 mac 地址。目标 mac 地址为局域网中的设备地址, 可能是网络网关的地址, 用于将数据包转发到 gaia.cs.umass.edu。而 gaia.cs.umass.edu 是互联网上的远程主机, 其 mac 地址在本地网络中不可见。

- 以太网帧 EtherType 字段值是多少, 对应着什么协议?

EtherType 字段值是 0x0800, 对应的协议是 IPv4。

- 从以太网帧的开始到 "GET" 中的 'G' 出现, 有多少字节?

以太网的头部长是 14 字节 (Ethernet II Header)。

IPv4 头部长是 20 字节。

```
✓ Internet Protocol Version 4, Src: 192.168.31.146, Dst: 128.119.245.12
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 706
  Identification: 0xc5f3 (50675)
```

TCP 头部长是 20 字节

```

Transmission Control Protocol, Src Port: 1898, Dst Port: 80, Seq: 1, Ack: 1, Len: 666
  Source Port: 1898
  Destination Port: 80
  [Stream index: 18]
  [Stream Packet Number: 4]
  > [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 666]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 1872722300
  [Next Sequence Number: 667 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 2274882999
  0101 .... = Header Length: 20 bytes (5)

```

到'G'开头总共是 14 + 20 + 20 = 54 字节。字符'G'是第 55 个字节
或直接看底下: 0x30==48, G 在第 55 个。

```

0000 dc 99 14 f2 be 11 20 c1 9b 15 ff 31 08 00 45 00 .....1..E-
0010 02 c2 3d 1c 40 00 80 06 00 00 0a db 8f 9d 80 77 ...=@.....W
0020 f5 0c 67 6a 00 50 6f 9f 79 7c 87 97 f5 b7 50 18 ...jPo.y|...P
0030 02 01 12 b1 00 00 47 45 54 20 2f 77 69 72 65 73 .....GET/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 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a ..Cache- Control:
00b0 20 6d 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 max-age =0..Upgr
00c0 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 ade-Inse cure-Req

```

所以, 从以太网帧的开始到"GET"中的'G'出现一共有 55 个字节 (包括 G)

选中第一个包含 HTTP 响应消息的以太网帧, 回答以下问题:

54	19.045320	192.168.31.146	128.119.245.12	HTTP	633	GET /wiresark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
68	21.058913	192.168.31.146	128.119.245.12	HTTP	728	GET /wiresark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
69	21.316808	128.119.245.12	192.168.31.146	HTTP	294	HTTP/1.1 304 Not Modified
82	25.452073	192.168.31.146	23.211.178.227	HTTP	165	GET /connecttest.txt HTTP/1.1
85	25.454370	192.168.31.146	23.211.178.227	HTTP	165	GET /connecttest.txt HTTP/1.1
87	25.521946	23.211.178.227	192.168.31.146	HTTP	241	HTTP/1.1 200 OK (text/plain)
92	25.526776	23.211.178.227	192.168.31.146	HTTP	241	HTTP/1.1 200 OK (text/plain)
106	26.329995	192.168.31.146	23.211.178.224	HTTP	165	GET /connecttest.txt HTTP/1.1
108	26.408334	23.211.178.224	192.168.31.146	HTTP	241	HTTP/1.1 200 OK (text/plain)
184	85.418420	192.168.31.146	128.119.245.12	HTTP	728	GET /wiresark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
188	85.615684	128.119.245.12	192.168.31.146	HTTP	295	HTTP/1.1 304 Not Modified
241	122.130155	192.168.31.146	183.47.121.90	HTTP	851	POST /mnt/00000006 HTTP/1.1 (application/octet-stream)

- 这个以太网帧中, 源 mac 地址是多少? 拥有这个以太网地址的设备是什么?

```

Ethernet II, Src: XiaomiMobile_e5:95:10 (24:cf:24:e5:95:10), Dst: Intel_15:ff:31 (20:c1:9b:15:ff:31)
  Destination: Intel_15:ff:31 (20:c1:9b:15:ff:31)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Source: XiaomiMobile_e5:95:10 (24:cf:24:e5:95:10)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 0]

```

由上图信息可知: 源 mac 地址是 24:cf:24:e5:95:10

设备标识为 XiaomiMobile_e5:95:10, 是一个小米移动设备的 mac 地址。

- 这个以太网帧中, 目的 mac 地址是多少? 拥有这个以太网地址的设备是什么?

目的 mac 地址为 20:c1:9b:15:ff:31

设备标识为 Intel_15:ff:31, 这是一个 Intel 设备的 mac 地址。

- 以太网帧 EtherType 字段值是多少, 对应着什么协议?

0x0800, 对应 IPv4

- 从以太网帧的开始到"OK"中的'O'出现, 有多少字节?

```

  Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  > Content-Length: 22\r\n
  Date: Thu, 12 Dec 2024 10:01:08 GMT\r\n
  Connection: close\r\n
  Content-Type: text/plain\r\n
  Cache-Control: max-age=30, must-revalidate\r\n
  \r\n
  [Request in frame: 82]
  [Time since request: 0.069873000 seconds]
0000 20 c1 9b 15 ff 31 24 cf 24 e5 95 10 08 00 45 00 .....1$ $.....E
0010 00 e3 99 67 40 00 31 06 04 bd 17 d3 b2 e3 c0 a8 ...g@1.....
0020 1f 92 00 50 28 84 e6 ff 69 34 b9 ba 66 01 50 18 ...P(...i4..f.P
0030 01 f6 c5 3f 00 00 48 54 54 50 2f 31 2e 31 20 32 ...?..HT TP/1.1 2
0040 30 30 20 4f 4e 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 00 OK..C ontent-L
0050 65 6e 67 74 68 3a 20 32 32 0d 0a 44 61 74 65 3a ..enthy: 2 2..Date:
0060 20 54 68 75 2c 20 31 32 20 44 65 63 20 32 30 32 Thu, 12 Dec 202
0070 34 20 31 30 3a 30 31 3a 30 38 20 47 4d 54 0d 0a 4 10:01: 08 GMT..
0080 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 Connecti on: clos
0090 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a e..Conte nt-Type:
00a0 20 74 65 78 74 2f 70 6c 61 69 6e 0d 0a 43 61 63 text/pl ain..Cac
00b0 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d he-Contr ol: max-
00c0 61 67 65 3d 33 30 2c 20 6d 75 73 74 2d 72 65 76 age=30, must-rev
00d0 61 6c 69 64 61 74 65 0d 0a 0d 0a 4d 69 63 72 6f alidate- ...Micro
00e0 73 6f 66 74 20 43 6f 6e 6e 65 63 74 20 54 65 73 soft Con nect Tes
00f0 74 t

```

'O'是第 0x40 行的第四个，也就是 64 + 4 = 68，'O'是第 68 byte，所以，从以太网帧的开始到"OK"中的'O'出现共有 68 字节（包括 O）

二、实验任务二：ARP

查看计算机上 ARP 缓存： MS-DOS: arp -a ； Linux/Unix/MacOS: arp
回答以下问题：

- 列出 ARP 缓存的内容(截图)，每列表示什么意思？

```

接口: 192.168.31.146 --- 0xa
Internet 地址      物理地址      类型
192.168.31.1      24-cf-24-e5-95-10 动态
192.168.31.255    ff-ff-ff-ff-ff-ff 静态
224.0.0.2         01-00-5e-00-00-02 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

接口: 192.168.232.1 --- 0xc
Internet 地址      物理地址      类型
192.168.232.255   ff-ff-ff-ff-ff-ff 静态
224.0.0.2         01-00-5e-00-00-02 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

接口: 192.168.29.1 --- 0xd
Internet 地址      物理地址      类型
192.168.29.255    ff-ff-ff-ff-ff-ff 静态
224.0.0.2         01-00-5e-00-00-02 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

接口: 192.168.56.1 --- 0x10
Internet 地址      物理地址      类型
192.168.56.255    ff-ff-ff-ff-ff-ff 静态
224.0.0.2         01-00-5e-00-00-02 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

```

每列分别表示 Internet 地址(即 IP 地址)、物理地址(即 mac 地址)、类型(动态表示如果某

个表项在一定的时间内没有被用到就会被删除，静态则是永久保存)。

清除计算机上 ARP 缓存： MS-DOS: arp -d ； Linux/Unix/MacOS: arp -ad

抓取 ARP 包：

- step1: 清空 ARP 缓存
- step2: 清空浏览器缓存
- step3: wireshark 抓包
- step4: 访问 <http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>

```
C:\Windows\System32>arp -d
C:\Windows\System32>arp -a

接口: 192.168.31.146 --- 0xa
Internet 地址      物理地址      类型
224.0.0.22         01-00-5e-00-00-16 静态

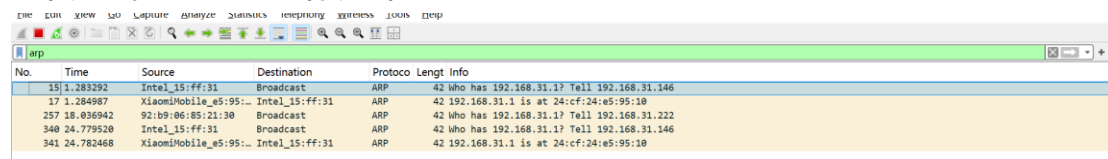
接口: 192.168.232.1 --- 0xc
Internet 地址      物理地址      类型
224.0.0.22         01-00-5e-00-00-16 静态

接口: 192.168.29.1 --- 0xd
Internet 地址      物理地址      类型
224.0.0.22         01-00-5e-00-00-16 静态

接口: 192.168.56.1 --- 0x10
Internet 地址      物理地址      类型
224.0.0.22         01-00-5e-00-00-16 静态
```

清除缓存后只剩下静态的了

抓取并观察 ARP 包，回答以下问题：



No.	Time	Source	Destination	Protocol	Length	Info
15	1.283292	Intel_15:ff:31	Broadcast	ARP	42	Who has 192.168.31.1? Tell 192.168.31.146
17	1.284987	XiaomiMobile_e5:95:...	Intel_15:ff:31	ARP	42	192.168.31.1 is at 24:cf:24:e5:95:10
257	18.036942	92:b9:06:85:21:30	Broadcast	ARP	42	Who has 192.168.31.1? Tell 192.168.31.222
340	24.779520	Intel_15:ff:31	Broadcast	ARP	42	Who has 192.168.31.1? Tell 192.168.31.146
341	24.782468	XiaomiMobile_e5:95:...	Intel_15:ff:31	ARP	42	192.168.31.1 is at 24:cf:24:e5:95:10

- 第一个包含 ARP 请求信息的以太网帧中，源和目的 mac 地址为？

```
▼ Ethernet II, Src: Intel_15:ff:31 (20:c1:9b:15:ff:31), 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_15:ff:31 (20:c1:9b:15:ff:31)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  [Stream index: 1]
```

源 mac 地址： 20:c1:9b:15:ff:31

目的 mac 地址： ff:ff:ff:ff:ff:ff

A 要发送帧给 B(B 的 IP 地址已知)， 但 B 的 MAC 地址不在 A 的 ARP 表中时： A 广播包含 B 的 IP 地址的 ARP 查询包， Dest MAC address =FF-FF-FF-FF-FF-FF， LAN 上的所有节点都会收到该查询包。由于前面清空了 ARP 缓存，这里第一个 ARP 包应该是 broadcast。

- 以太网帧 EtherType 字段值是多少， 对应着什么协议？

字段值是 0x0806， 对应 ARP 协议

参考 ARP 规范，回答以下问题：

- ARP 操作字段在以太网帧的第几个字节？

▼ Address Resolution Protocol (request)

Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4

Opcode: request (1)

Sender MAC address: Intel_15:ff:31 (20:c1:9b:15:ff:31)
 Sender IP address: 192.168.31.146
 Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
 Target IP address: 192.168.31.1

0000	ff ff ff ff ff ff 20 c1 9b 15 ff 31 08 06 00 01 1
0010	08 00 06 04 00 01 20 c1 9b 15 ff 31 c0 a8 1f 92 1
0020	00 00 00 00 00 00 c0 a8 1f 01

16+4 = 20, 前面有 20 个字节, 所以操作字段在第 21 字节。

- 进行 ARP 请求的以太网帧中, ARP 负载部分操作字段值是多少?

Opcode: request (1) 值为 1

(操作码: 1 为 ARP 请求, 2 为 ARP 回显, 3 为 RARP 请求, 4 为 RARP 应答。)

- ARP 消息是否包含发送方的 IP 地址?

包含。Sender IP 字段: 192.168.31.1

- 在 ARP 请求中从哪里看出我们想查询相应 IP 的 mac 地址?

Target mac address 字段。

找到 ARP 请求对应的回应包, 回答以下问题:

▼ Ethernet II, Src: XiaomiMobile_e5:95:10 (24:cf:24:e5:95:10), Dst: Intel_15:ff:31 (20:c1:9b:15:ff:31)

▼ Destination: Intel_15:ff:31 (20:c1:9b:15:ff:31)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)

▼ Source: XiaomiMobile_e5:95:10 (24:cf:24:e5:95:10)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)

Type: ARP (0x0806)
 [Stream index: 0]

▼ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0800)
 Hardware size: 6
 Protocol size: 4

Opcode: reply (2)

Sender MAC address: XiaomiMobile_e5:95:10 (24:cf:24:e5:95:10)
 Sender IP address: 192.168.31.1
 Target MAC address: Intel_15:ff:31 (20:c1:9b:15:ff:31)
 Target IP address: 192.168.31.146

0000	20 c1 9b 15 ff 31 24 cf 24 e5 95 10 08 06 00 01 1\$ \$
0010	08 00 06 04 00 02 24 cf 24 e5 95 10 c0 a8 1f 01 \$ \$
0020	20 c1 9b 15 ff 31 c0 a8 1f 92 1

- ARP 操作字段在以太网帧的第几个字节?

同样, 16+5 = 21, 在第 21 个字节。

- 进行 ARP 响应的以太网帧中, ARP 负载部分操作字段值是多少?

2. 表示 reply

- ARP 回应之前请求信息的内容?

所有内容都在上图 ARP 下：

Hardware Type 表示硬件地址的类型。对于以太网，该类型的值为 1。

Protocol Type 表示发送方要映射的协议地址类型。对于 IP 地址，该值为 0x0800。

Hardware size 对于应答报文来说是 6

Protocol size 对于应答报文来说是 4

Opcode: reply(2) 表示是 ARP 应答

Sender MAC address 和 Sender IP address 分别表示源 MAC 地址和源 IP 地址。这两个字段和 ARP 报文首部的以太网源 MAC 地址字段和 IP 字段是相同的信息。

Target 则是目的，与上同理。

所以从 target mac address 也可以看出这是 ARP 回应之前请求信息的内容，reply 的目的 mac 地址也就是 request 的源 mac 地址。

- 包含 ARP 回应信息的以太网帧中，源和目的 mac 地址为？

源：24:cf:24:e5:95:10

目的：20:c1:9b:15:ff:31