

计算机网络与通信实验报告（四）			
学 号	姓 名	班 级	报告日期
202221139	杨涛	2211106	2024.11.4
实验内容	利用分组嗅探器分析数据链路层协议		
实验目的	了解数据链路层协议构造，掌握对其进行分析的能力		
实验预备知识	<div data-bbox="450 667 1123 846"></div> <p>图4-3 用于以太网的ARP请求或应答分组格式</p> <p>以太网报头中的前两个字段是以太网的源地址和目的地址。目的地址为全 1 的特殊地址是广播地址。电缆上的所有以太网接口都要接收广播的数据帧。</p> <p>两个字节长的以太网帧类型表示后面数据的类型。对于 ARP 请求或应答来说，该字段的值为 0x0806。</p> <p>hardware（硬件）和 protocol（协议）用来描述 ARP 分组中的各个字段。例如，一个 ARP 请求分组询问协议地址（这里是 IP 地址）对应的硬件地址（这里是以太网地址）。</p> <p>硬件类型字段表示硬件地址的类型。它的值为 1 即表示以太网地址。协议类型字段表示要映射的协议地址类型。它的值为 0x0800 即表示 IP 地址。它的值与包含 IP 数据报的以太网数据帧中的类型字段的值相同，这是有意设计的。</p> <p>接下来的两个 1 字节的字段，硬件地址长度和协议地址长度分别指出硬件地址和协议地址的长度，以字节为单位。对于以太网上 IP 地址的 ARP 请求或应答来说，它们的值分别为 6 和 4。</p> <p>操作字段指出四种操作类型，它们是 ARP 请求（值为 1）、ARP 应答（值为 2）、R ARP 请求（值为 3）和 R ARP 应答（值为 4）。这个字段必需的，因为 ARP 请求和 ARP 应答的帧类型字段值是相同的。</p> <p>接下来的四个字段是发送端的硬件地址（在本例中是以太网地址）、发送</p>		

	<p>端的协议地址（IP 地址）、目的端的硬件地址和目的端的协议地址。注意，这里有一些重复信息：在以太网的数据帧报头中和 ARP 请求数据帧中都有发送端的硬件地址。</p> <p>对于一个 ARP 请求来说，除目的端硬件地址外的所有其他的字段都有填充值。当系统收到一份目的端为本机的 ARP 请求报文后，它就把硬件地址填进去，然后用两个目的端地址分别替换两个发送端地址，并把操作字段置为 2，最后把它发送回去。</p>																					
实验过程描述	<p>一、以太网帧分析</p> <p>(1) 清空浏览器缓存。</p> <p>(2) 启动分组捕获软件，开始分组俘获。</p> <p>(3) 在浏览器的地址栏中输入：<a href="http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file3.html">http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file3.html</a>，浏览器将显示冗长的美国权力法案。</p> <p>(4) 停止分组俘获。首先，找到你的主机向服务器 <a href="http://gaia.cs.umass.edu">gaia.cs.umass.edu</a> 发送的 HTTP GET 报文的分组序号，以及服务器发送到你主机上的 HTTP 响应报文的序号。</p> <p>选择“Analyze-&gt;Enabled Protocols”，取消对 IP 复选框的选择，单击 OK。</p> <p>(5) 选择包含 HTTP GET 报文的以太网帧，在分组详细信息窗口中，展开 Ethernet II 信息部分。</p> <p>(6) 选择包含 HTTP 响应报文第一个字节的以太网帧。</p> <table><tr><th>No.</th><th>Time</th><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr><tr><td>156</td><td>2.851998</td><td>192.168.105.161</td><td>128.119.245.12</td><td>HTTP</td><td>524</td><td>GET /ethereal-labs/HTTP-ethereal-file3.html HTTP/1.1</td></tr><tr><td>168</td><td>2.466008</td><td>128.119.245.12</td><td>192.168.105.161</td><td>HTTP</td><td>835</td><td>HTTP/1.1 200 OK (text/html)</td></tr></table> <p>二、ARP 分析</p> <p>(1) 利用 MS-DOS 命令：arp 或 c:\windows\system32\arp 查看主机上 ARP 缓存的内容。</p> <p>(2) 利用 MS-DOS 命令：arp-d * 清除主机上 ARP 缓存的内容。</p> <p>(3) 清除浏览器缓存。</p> <p>(4) 启动分组捕获软件，开始分组俘获。</p> <p>(5) 在浏览器的地址栏中输入：<a href="http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-lab-file3.html">http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-lab-file3.html</a>，浏览器显示冗长的美国权力法案。</p> <p>(6) 停止分组俘获。选择“Analyze-&gt;Enabled Protocols”，取消对 IP 复选框的选择，单击 OK。</p>	No.	Time	Source	Destination	Protocol	Length	Info	156	2.851998	192.168.105.161	128.119.245.12	HTTP	524	GET /ethereal-labs/HTTP-ethereal-file3.html HTTP/1.1	168	2.466008	128.119.245.12	192.168.105.161	HTTP	835	HTTP/1.1 200 OK (text/html)
No.	Time	Source	Destination	Protocol	Length	Info																
156	2.851998	192.168.105.161	128.119.245.12	HTTP	524	GET /ethereal-labs/HTTP-ethereal-file3.html HTTP/1.1																
168	2.466008	128.119.245.12	192.168.105.161	HTTP	835	HTTP/1.1 200 OK (text/html)																

<p>实验结果</p>	<p>(1)你的主机的 48 位以太网地址是多少？</p> <p>bc:6e:e2:8d:f5:13</p> <pre>▼ Ethernet II, Src: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13), Dst: a6:9c:cc:1a:46:2d (a6:9c:cc:1a:46:2d)   ▶ Destination: a6:9c:cc:1a:46:2d (a6:9c:cc:1a:46:2d)   ▶ Source: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)   Type: IPv4 (0x0800)   [Stream index: 0]</pre> <p>(2)是 gaia.cs.umass.edu 服务器的地址吗？如不是，该地址是什么设备的以太网地址？</p> <p>不是，这是局域网路由器网关的以太网地址。</p> <p>(3)给出两种帧类型字段的十六进制值。标志字段的值是 1 的含义是什么？</p> <pre>▼ Ethernet II, Src: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13), Dst: a6:9c:cc:1a:46:2d (a6:9c:cc:1a:46:2d)   ▶ Destination: a6:9c:cc:1a:46:2d (a6:9c:cc:1a:46:2d)   ▶ Source: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)   Type: IPv4 (0x0800)   [Stream index: 0]</pre> <p>对于 IP 报文来说，该字段值是 0x0800。对于 ARP 信息来说，以太类型字段的值是 0x0806。</p> <pre>▼ Ethernet II, Src: a6:9c:cc:1a:46:2d (a6:9c:cc:1a:46:2d), Dst: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)   ▶ Destination: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)     ... .. = LG bit: Globally unique address (factory default)     ... .. = IG bit: Individual address (unicast)   ▶ Source: a6:9c:cc:1a:46:2d (a6:9c:cc:1a:46:2d)     ... .. = LG bit: Locally administered address (this is NOT the factory default)     ... .. = IG bit: Individual address (unicast)   Type: IPv4 (0x0800)   [Stream index: 0]</pre> <p>LG 标志位置 1 表示：由本地管理的 mac 地址，而非出厂时默认设置。</p> <p>IG 标志位置 1 表示：组地址，多播或广播地址。</p> <p>TCP 中也含有标志字段。</p> <p>URG 表示紧急数据</p> <p>ACK 表示确认字段的值有效</p> <p>PSH 表示接收方应立即将数据交给上层</p> <p>RST 表示重建连接</p> <p>SYN 表示连接建立的第一次握手</p> <p>FIN 表示连接拆除的第一次握手</p> <p>(4)在包含 “get” 以太网帧中，从该帧的起始处开始一共有多少个 ASCII 字符 “G” ？</p> <p>包含两个 G。</p>
-------------	--

```

a6 9c cc 1a 46 2d bc 6e e2 8d f5 13 08 00 45 00 ... F-n ... E-
01 fe 56 51 40 00 40 06 00 00 c0 a8 69 a1 80 77 ... VQ@ @ ... i w
f5 0c e1 ed 00 50 ab e9 f9 5e d2 03 31 ce 50 18 ... P ... ^ ... 1 P
02 03 a1 be 00 00 47 45 54 20 2f 65 74 68 65 72 ... GI T /ether
65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74 eal-labs /HTTP-et
68 65 72 65 61 6c 2d 66 69 6c 65 33 2e 68 74 6d hereal-f ile3.htm
6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 l HTTP/1 .1 Host
3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 73 73 2e : gaia.c s.umass.
65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a edu Con nection:
20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 keep-al ive Upg
72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 rade-Ins ecure-Re
71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d quests: 1 User-
41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent: M ozilla/5
2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 .0 (Wind ows NT 1
30 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 0.0; Win 64; x64)
20 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 AppleWe bKit/537
2e 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 36 (KHT ML, like
20 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 Gecko) Chrome/1
33 30 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 2f 30.0.0 Safari/
35 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 3a 20 537.36 Accept:
74 65 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 text/htm l,applic
61 74 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c ation/xh tml+xml,
61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b applicat ion/xml;
71 3d 30 2e 39 2c 69 6d 61 67 65 2f 61 76 69 66 q=0.9,im age/avif
2c 69 6d 61 67 65 2f 77 65 62 70 2c 69 6d 61 67 ,image/w ebp,imag
65 2f 61 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e 38 e/apng,* /*;q=0.8
2c 61 70 70 6c 69 63 61 74 69 6f 6e 2f 73 69 67 ,applica tion/sig
6e 65 64 2d 65 78 63 68 61 6e 67 65 3b 76 3d 62 ned-exch ange;v=b
33 3b 71 3d 30 2e 37 0d 0a 41 63 63 65 70 74 2d 3;q=0.7 Accept-
45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 Encoding : gzip,
64 65 66 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d deflate Accept-
4c 61 6e 67 75 61 67 65 3a 20 7a 68 2d 43 4e 2c Language : zh-CN,
7a 68 3b 71 3d 30 2e 39 0d 0a 0d 0a zh;q=0.9

```

(5)在该以太网帧中 CRC 字段的十六进制值是多少？

分组被 Ethereal 捕获时网卡已经把以太网的 CRC 校验字段给剥除了，故没有显示。

(6)以太网源地址是多少？该地址是你主机的地址吗？是 gaia.cs.umass.edu 服务器的地址吗？如果不是，该地址是什么设备的以太网地址？

```

▼ Ethernet II, Src: a6:9c:cc:1a:46:2d (a6:9c:cc:1a:46:2d), Dst: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)
  ► Destination: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)
  ► Source: a6:9c:cc:1a:46:2d (a6:9c:cc:1a:46:2d)
    Type: IPv4 (0x0800)
    [Stream index: 0]

```

```

接口: 192.168.105.161 --- 0x17
Internet 地址      物理地址      类型
192.168.105.87      a6-9c-cc-1a-46-2d      动态
192.168.105.255      ff-ff-ff-ff-ff-ff      静态
224.0.0.2            01-00-5e-00-00-02      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
239.192.152.143      01-00-5e-40-98-8f      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


```

以太网源地址是 a6:9c:cc:1a:46:2d，不是主机地址，也不是目标 gaia.cs.umass.edu 服务器的地址，是 192.168.105.87 的动态以太网地址。



(7)以太网帧的 48 位目的地址是多少？该地址是你主机的地址吗？

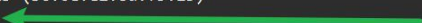
```
▼ Ethernet II, Src: a6:9c:cc:1a:46:2d (a6:9c:cc:1a:46:2d), Dst: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)
  ▶ Destination: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)
  ▶ Source: a6:9c:cc:1a:46:2d (a6:9c:cc:1a:46:2d)
  Type: IPv4 (0x0800)
  [Stream index: 0]
```



以太网帧的 48 位目的地址是 bc:6e:e2:8d:f5:13，该地址是我的主机地址。

(8)给出两种帧类型字段的十六进制值。标志字段的值是 1 的含义是什么？

```
▼ Ethernet II, Src: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13), Dst: a6:9c:cc:1a:46:2d (a6:9c:cc:1a:46:2d)
  ▶ Destination: a6:9c:cc:1a:46:2d (a6:9c:cc:1a:46:2d)
  ▶ Source: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)
  Type: IPv4 (0x0800)
  [Stream index: 0]
```



对于 IP 报文来说，该字段值是 0x0800。对于 ARP 信息来说，以太类型字段的值是 0x0806。

```
▼ Ethernet II, Src: a6:9c:cc:1a:46:2d (a6:9c:cc:1a:46:2d), Dst: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)
  ▶ Destination: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)
    ... ..0. .... = LG bit: Globally unique address (factory default)
    ... ..0. .... = IG bit: Individual address (unicast)
  ▶ Source: a6:9c:cc:1a:46:2d (a6:9c:cc:1a:46:2d)
    ... ..1. .... = LG bit: Locally administered address (this is NOT the factory default)
    ... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 0]
```

LG 标志位置 1 表示：由本地管理的 mac 地址，而非出厂时默认设置。

IG 标志位置 1 表示：组地址，多播或广播地址。

TCP 中也含有标志字段。

URG 表示紧急数据

ACK 表示确认字段的值有效

PSH 表示接收方应立即将数据交给上层

RST 表示重建连接

SYN 表示连接建立的第一次握手

FIN 表示连接拆除的第一次握手

(9)在包含“OK”以太网帧中，从该帧的起始处开始一共有多少个 ASCII 字符“O”？

一共有 5 个 O。

```

bc 6e e2 8d f5 13 a6 9c cc 1a 46 2d 08 00 45 00 .n . . . . . F . . . E
05 78 c0 01 40 00 2a 06 eb b0 80 77 f5 0c c0 a8 .x .@ . * . . . W . . . .
69 a1 00 50 e1 ed d2 03 31 ce ab e9 fb 34 50 10 i . P . . . . . 1 . . . . 4P .
00 ed 52 0a 00 00 48 54 54 50 2f 31 2e 31 20 32 . . . . . HT TP/1.1 2
30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e 00 OK .D ate: Mon
2c 20 30 34 20 4e 6f 76 20 32 30 32 34 20 30 38 , 04 Nov 2024 08
3a 30 37 3a 31 32 20 47 4d 54 0d 0a 53 65 72 76 :07:12 G MT .Serv
65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (Cen OS ) OpenSS
4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -tips PH
50 2f 37 2e 34 2e 33 33 20 6d 6f 64 5f 70 65 72 P/7.4.33 mod_per
6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 l/2.0.11 Perl/v5
2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3 .L ast-Modi
66 69 65 64 3a 20 4d 6f 6e 2c 20 30 34 20 4e 6f fied: Mo n, 04 No
76 20 32 30 32 34 20 30 36 3a 35 39 3a 30 32 20 v 2024 0 6:59:02
47 4d 54 0d 0a 45 54 61 67 3a 20 22 31 31 39 34 GMT . ETa g: "1194
2d 36 32 36 31 30 64 31 64 38 32 36 66 33 22 0d -62610d1 d826f3"
0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 .Accept- Ranges:
62 79 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c bytes .C ontent-L
65 6e 67 74 68 3a 20 34 35 30 30 0d 0a 4b 65 65 ength: 4 500 .Kee
70 2d 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 p-Alive: timeout
3d 35 2c 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e =5, max= 100 .Con
6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c nection: Keep-Al
69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 ive . Con tent-Typ
65 3a 20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 e: text/ html; ch
61 72 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c arset=UT F-8 . . . . <
68 74 6d 6c 3e 3c 68 65 61 64 3e 20 0a 3c 74 69 html><he ad> .<ti
74 6c 65 3e 48 69 73 74 6f 72 69 63 61 6c 20 44 tle>Hist orical D
6f 63 75 6d 65 6e 74 73 3a 54 48 45 20 42 49 4c ocuments :THE BIL
4c 20 4f 46 20 52 49 47 48 54 53 3c 2f 74 69 74 L OI RIG HTS</tit
6c 65 3e 3c 2f 68 65 61 64 3e 0a 0a 0a 3c 62 6f le></hea d> . . . <bo
64 79 20 62 67 63 6f 6c 6f 72 3d 22 23 66 66 66 dy bgcol or="#fff
66 66 66 22 20 6c 69 6e 6b 3d 22 23 33 33 30 30 fff" lin k="#3300
30 30 22 20 76 6c 69 6e 6b 3d 22 23 36 36 36 36 00" vlin k="#6666
33 33 22 3e 0a 3c 70 3e 3c 62 72 3e 0a 3c 2f 70 33"> .<p> <br> .</p>
3e 0a 3c 70 3e 3c 2f 70 3e 3c 63 65 6e 74 65 72 > .<p></p> ><center
3e 3c 62 3e 54 48 45 20 42 49 4c 4c 20 4f 46 20 ><b>THE BILL OI
52 49 47 48 54 53 3c 2f 62 3e 3c 62 72 3e 0a 20 RIGHTS</ b><br>
20 3c 65 6d 3e 41 6d 65 6e 64 6d 65 6e 74 73 20 <em>Ame ndments
31 2d 31 30 20 6f 66 20 74 68 65 20 43 6f 6e 73 1-10 of the Cons
74 69 74 75 74 69 6f 6e 3c 2f 65 6d 3e 0a 3c 2f titution </em> .</
63 65 6e 74 65 72 3e 0a 0a 3c 70 3e 54 68 65 20 center> . .<p>The
43 6f 6e 76 65 6e 74 69 6f 6e 73 20 6f 66 20 61 Conventi ons of a
20 6e 75 6d 62 65 72 20 6f 66 20 74 68 65 20 53 number of the S
74 61 74 65 73 20 68 61 76 69 6e 67 2c 20 61 74 tates ha ving, at
20 74 68 65 20 74 69 6d 65 20 6f 66 20 61 64 6f the tim e of ado
70 74 69 6e 67 0a 74 68 65 20 43 6f 6e 73 74 69 pting th e Consti
74 75 74 69 6f 6e 2c 20 65 78 70 72 65 73 73 65 tution, expresse
64 20 61 20 64 65 73 69 72 65 2c 20 69 6e 20 6f d a desi re, in o
72 64 65 72 20 74 6f 20 70 72 65 76 65 6e 74 20 rder to prevent
6d 69 73 63 6f 6e 73 74 72 75 63 74 69 6f 6e 0a misconst ruction
6f 72 20 61 62 75 73 65 20 6f 66 20 69 74 73 20 or abuse of its
70 6f 77 65 72 73 2c 20 74 68 61 74 20 66 75 72 powers, that fur
74 68 65 72 20 64 65 63 6c 61 72 61 74 6f 72 79 ther dec laratory
20 61 6e 64 20 72 65 73 74 72 69 63 74 69 76 65 and res trictive
20 63 6c 61 75 73 65 73 0a 73 68 6f 75 6c 64 20 clauses should

```

(10)在该以太网帧中 CRC 字段的十六进制值是多少？

分组被 Ethereal 捕获时网卡已经把以太网的 CRC 校验字段给剥除了，所以未在软件中出现。

(11)写下你主机 ARP 缓存中的内容。其中每一列的含义是什么？



```
PS C:\Users\28678\Desktop> arp -a

接口 : 192.168.33.1 --- 0x8
Internet 地址      物理地址      类型
224.0.0.2          01-00-5e-00-00-02 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
239.192.152.143    01-00-5e-40-98-8f 静态

接口 : 192.168.192.228 --- 0xa
Internet 地址      物理地址      类型
224.0.0.2          01-00-5e-00-00-02 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
239.192.152.143    01-00-5e-40-98-8f 静态

接口 : 192.168.88.1 --- 0xf
Internet 地址      物理地址      类型
224.0.0.2          01-00-5e-00-00-02 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
239.192.152.143    01-00-5e-40-98-8f 静态

接口 : 192.168.105.161 --- 0x17
Internet 地址      物理地址      类型
192.168.105.87     a6-9c-cc-1a-46-2d 动态
224.0.0.2          01-00-5e-00-00-02 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
239.192.152.143    01-00-5e-40-98-8f 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
```

- A.接口：显示当前 ARP 表项所属的网络接口。
- B.Internet 地址：表示设备的 IP 地址或多播地址。
- C.物理地址：表示与该 IP 地址相对应的 MAC 地址。以"01-00-5e"开头的 MAC 地址通常表示多播地址,MAC 地址"ff-ff-ff-ff-ff-ff"表示广播地址。
- D.类型：表示条目的类型，有两种：静态：表示该条目是手动添加或永久保存的。动态：表示该条目是 ARP 协议自动生成的，会定期刷新。

(12)包含 ARP 请求报文的以太网帧的源地址和目的地址的十六进制值各是多少？

```
▼ Ethernet II, Src: RuijieNetwor_a6:8f:09 (58:69:6c:a6:8f:09), 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: RuijieNetwor_a6:8f:09 (58:69:6c:a6:8f:09)
    .... 0. .... = LG bit: Globally unique address (factory default)
    .... 0. .... = IG bit: Individual address (unicast)
Type: ARP (0x0806)
[Stream index: 0]
Padding: 00
```

58:69:6c:a6:8f:09 和 ff:ff:ff:ff:ff:ff

(13)给出两种帧类型字段的十六进制值。标志字段的值是 1 的含义是什么？

对于 IP 报文来说, 该字段值是 0x0800。对于 ARP 信息来说, 以太类型字段的值是 0x0806。

```
▼ Ethernet II, Src: RuijieNetwor_a6:8f:09 (58:69:6c:a6:8f:09), 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
    .... ..1. .... = IG bit: Group address (multicast/broadcast)
  ▼ Source: RuijieNetwor_a6:8f:09 (58:69:6c:a6:8f:09)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
Type: ARP (0x0806)
[Stream index: 0]
Padding: 00
Trailer: 012004c994000000000942db7700000000
```

帧类型字段的十六进制值还可以是 0x0806, 表示数据帧内容为 ARP 请求或响应类型。

LG 标志位置 1 表示: 由本地管理的 mac 地址, 而非出厂时默认设置。

IG 标志位置 1 表示: 组地址, 多播或广播地址。

TCP 中也含有标志字段。

URG 表示紧急数据

ACK 表示确认字段的值有效

PSH 表示接收方应立即将数据交给上层

RST 表示重建连接

SYN 表示连接建立的第一次握手

FIN 表示连接拆除的第一次握手

(14) 形成 ARP 响应报文的以太网帧中 ARP-payload 部分 opcode 字段的值是多少? 在 ARP 报文中是否包含发送方的 IP 地址?

```
▼ Ethernet II, Src: RuijieNetwor_a6:8f:09 (58:69:6c:a6:8f:09), Dst: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)
  ▼ Destination: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  ▼ Source: RuijieNetwor_a6:8f:09 (58:69:6c:a6:8f:09)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
Type: ARP (0x0806)
[Stream index: 1]
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: RuijieNetwor_a6:8f:09 (58:69:6c:a6:8f:09)
  Sender IP address: 10.236.255.254
  Target MAC address: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)
  Target IP address: 10.236.248.40
```

响应报文的 opcode 字段的值是 0x0002。

包含发送方的 IP 地址。

(15) 包含 ARP 回答报文的以太网帧中源地址和目的地址的十六进制值各是多少?

```
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: RuijieNetwor_a6:8f:09 (58:69:6c:a6:8f:09)
  Sender IP address: 10.236.255.254
  Target MAC address: Intel_8d:f5:13 (bc:6e:e2:8d:f5:13)
  Target IP address: 10.236.248.40
```



	源地址为本机的 mac 地址，目的地址为发广播包的主机或路由器的 mac 地址。			
实验当中 问题 及解决方 法	<p>1、执行清楚本机 ARP 缓存时提示需要进行提升 解决方法：采用管理员方式打开 cmd</p> <p>2、 用 Ethereal 所捕的以太网帧没有前导码、CRC。 结论：网卡需要做这样的工作，在物理层上要先去掉前导同步码和帧开始定界符，然后对帧进行 CRC 检验，如果帧校验和错，就丢弃此帧。如果校验和正确，就判断帧的目的硬件地址是否符合自己的接收条件，如果符合，就将帧交“设备驱动程序”做进一步处理。这时我们的捕包软件才能捕到数据。因此，捕包软件捕到的是去掉前导同步码、帧开始分界符和 CRC 检验之外的数据。</p> <p>3、抓包时网络流量过大，捕获不完整 解决方法：使用过滤器减少捕获的包数量，或者将抓包分为多个时间段进行，确保数据不丢失。</p>			
成绩（教师 打分）	优秀	良好	及格	不及格