

计算机网络 Lab8

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>

选中包含HTTP GET消息的以太网帧，回答以下问题：

No.	Time	Source	Destination	Protocol	Length	Info
390	11.333328	192.168.3.119	101.126.4.197	HTTP/3...	743	PUT /api/v1/device HTTP/1.1, JSON (application/json)
398	11.399561	101.126.4.197	192.168.3.119	HTTP/3...	384	HTTP/1.1 200 OK, JSON (application/json)
404	11.423583	101.126.4.197	192.168.3.119	HTTP/3...	74	HTTP/1.1 200 OK, JSON (application/json)
645	17.276153	192.168.3.119	128.119.245.12	HTTP	576	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
652	17.611470	128.119.245.12	192.168.3.119	HTTP	835	HTTP/1.1 200 OK (text/html)
660	17.858386	192.168.3.119	128.119.245.12	HTTP	522	GET /favicon.ico HTTP/1.1
664	18.083104	128.119.245.12	192.168.3.119	HTTP	538	HTTP/1.1 404 Not Found (text/html)
704	20.126932	240e:46d:5600:1426:e07d:b3e9:43b0:db02	2600:1406:4e00:16::1738:6da8	HTTP	229	GET /connecttest.txt HTTP/1.1
707	20.128025	240e:46d:5600:1426:e07d:b3e9:43b0:db02	2600:1406:4e00:16::1738:6da8	HTTP	229	GET /connecttest.txt HTTP/1.1
710	20.128406	192.168.3.119	23.204.80.239	HTTP	208	GET /connecttest.txt HTTP/1.1
713	20.160042	240e:46d:5600:1426:e07d:b3e9:43b0:db02	2600:1406:4e00:16::1738:6da8	HTTP	229	GET /connecttest.txt HTTP/1.1
718	20.228492	192.168.3.119	23.204.80.239	HTTP	208	GET /connecttest.txt HTTP/1.1
720	20.288441	2600:1406:4e00:16::1738:6da8	240e:46d:5600:1426:e07d:b3e9:43b0:db02	HTTP	261	HTTP/1.1 200 OK (text/plain)

Frame 645: 576 bytes on wire (4608 bits), 576 bytes captured (4608 bits) on interface \Device\NPF{D...}

Ethernet II, Src: Intel 74:7d:db (54:6c:eb:74:7d:db), Dst: 12:ff:66:9a:ed:ba (12:ff:66:9a:ed:ba)

Destination: 12:ff:66:9a:ed:ba (12:ff:66:9a:ed:ba)

...1. = LG bit: Locally administered address (this is NOT the factory d

...0. = IG bit: Individual address (unicast)

Source: Intel 74:7d:db (54:6c:eb:74:7d:db)

...0. = LG bit: Globally unique address (factory default)

...0. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

[Stream index: 0]

Internet Protocol Version 4, Src: 192.168.3.119, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 60979, Dst Port: 80, Seq: 1, Ack: 1, Len: 522

Hypertext Transfer Protocol

0000 12 ff 66 9a ed ba 54 6c eb 74 7d db 00 00 45 00 ...f..l..t)..E

0010 02 32 75 c6 40 00 80 05 48 5c c0 a8 03 77 80 77 ...2v@..H\..w.w

0020 f5 0c ee 33 00 50 1b 7e 17 40 97 64 18 25 50 18 ...3P~.dXP

0030 02 03 21 cf 00 00 47 45 54 20 2f 77 69 72 65 73 ...f..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 4b 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-Reqre 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

- 你的电脑的mac地址是多少？

我的电脑的mac地址是54:6c:eb:74:7d:db

- 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12:ff:66:9a:ed:ba。不是gaia.cs.umass.edu的mac地址

- 以太网帧EtherType字段值是多少，对应着什么协议？

以太网帧的EtherType字段值是 0x0800，这对应着IPv4协议

- 从以太网帧的开始到“GET”中的‘G’出现，有多少字节？

根据wireshark抓包，前三行总共48个字节，第四行到G总共有7个字节，总共55个字节。

选中第一个包含HTTP响应消息的以太网帧，回答以下问题：

No.	Time	Source	Destination	Protocol	Length	Info
390	11.333328	192.168.3.119	101.126.4.197	HTTP/1.1	743	PUT /api/v1/device HTTP/1.1, JSON (application/json)
398	11.399561	101.126.4.197	192.168.3.119	HTTP/1.1	384	HTTP/1.1 200 OK, JSON (application/json)
404	11.423583	101.126.4.197	192.168.3.119	HTTP/1.1	74	HTTP/1.1 200 OK, JSON (application/json)
645	17.276153	192.168.3.119	128.119.245.12	HTTP	576	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
652	17.611470	128.119.245.12	192.168.3.119	HTTP	835	HTTP/1.1 200 OK (text/html)
660	17.858386	192.168.3.119	128.119.245.12	HTTP	522	GET /favicon.ico HTTP/1.1
664	18.083104	128.119.245.12	192.168.3.119	HTTP	538	HTTP/1.1 404 Not Found (text/html)
704	20.126932	240e:46d:5600:1426:e07d:b3e9:43b0:db02	2600:1406:4e00:16::1738:6da8	HTTP	229	GET /connecttest.txt HTTP/1.1
707	20.128025	240e:46d:5600:1426:e07d:b3e9:43b0:db02	2600:1406:4e00:16::1738:6da8	HTTP	229	GET /connecttest.txt HTTP/1.1
710	20.128406	192.168.3.119	23.204.80.239	HTTP	208	GET /connecttest.txt HTTP/1.1
713	20.160042	240e:46d:5600:1426:e07d:b3e9:43b0:db02	2600:1406:4e00:16::1738:6da8	HTTP	229	GET /connecttest.txt HTTP/1.1
718	20.228492	192.168.3.119	23.204.80.239	HTTP	208	GET /connecttest.txt HTTP/1.1
720	20.288441	2600:1406:4e00:16::1738:6da8	240e:46d:5600:1426:e07d:b3e9:43b0:db02	HTTP	261	HTTP/1.1 200 OK (text/plain)

▶ Frame 652: 835 bytes on wire (6680 bits), 835 bytes captured (6680 bits) on interface \Device\NPF{D...}

▶ Ethernet II, Src: 12:ff:66:9a:ed:ba (12:ff:66:9a:ed:ba), Dst: Intel_74:7d:db (54:6c:eb:74:7d:db)

Destination: Intel_74:7d:db (54:6c:eb:74:7d:db)

...0... = LG bit: Globally unique address (factory default)

...0... = IG bit: Individual address (unicast)

Source: 12:ff:66:9a:ed:ba (12:ff:66:9a:ed:ba)

...1... = LG bit: Locally administered address (this is NOT the factory default)

...0... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

[Stream index: 0]

▶ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.3.119

▶ Transmission Control Protocol, Src Port: 80, Dst Port: 60979, Seq: 4081, Ack: 523, Len: 781

▶ [4 Reassembled TCP Segments (4861 bytes): #649(1360), #650(1360), #651(1360), #652(781)]

▶ Hypertext Transfer Protocol

▶ Line-based text data: text/html (98 lines)

- 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？

12:ff:66:9a:ed:ba拥有这个以太网地址的设备是我电脑连接热点的手机。

- 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？

54:6c:eb:74:7d:db拥有这个以太网地址的设备是我的电脑主机。

- 以太网帧EtherType字段值是多少，对应着什么协议？

以太网帧的EtherType字段值是 0x0800，这对应着IPv4协议

- 从以太网帧的开始到“OK”中的‘O’出现，有多少字节？

根据wireshark抓包，到o总共有14个字节。

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?
 1. **接口**: 显示了ARP缓存对应的网络接口的IP地址。
 2. **Internet 地址**: 这是与物理地址关联的IP地址。
 3. **物理地址**: 这是与IP地址关联的MAC地址。
 4. **类型**: 表示条目的类型, 可以是“动态”或“静态”。动态条目是通过ARP请求和响应自动学习的, 而静态条目是手动配置的。

```
C:\Users\IScream>arp -a
```

接口: 192.168.227.1 --- 0x3	Internet 地址	物理地址	类型
	192.168.227.254	00-50-56-ff-77-cd	动态
	192.168.227.255	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
	255.255.255.255	ff-ff-ff-ff-ff-ff	静态

接口: 192.168.56.1 --- 0x4	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

接口: 192.168.229.1 --- 0x17	Internet 地址	物理地址	类型
	192.168.229.254	00-50-56-eb-c1-56	动态
	192.168.229.255	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
	255.255.255.255	ff-ff-ff-ff-ff-ff	静态

接口: 10.223.122.88 --- 0x18	Internet 地址	物理地址	类型
	10.223.0.1	10-c1-72-83-c8-1b	动态
	10.223.127.255	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
	255.255.255.255	ff-ff-ff-ff-ff-ff	静态

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>

抓取并观察ARP包，回答以下问题：

No.	Time	Source	Destination	Protocol	Length	Info
1218	42.716102	Intel_74:7d:db	Broadcast	ARP	42	Who has 192.168.3.97? Tell 192.168.3.119
1219	42.809722	12:ff:66:9a:ed:ba	Intel_74:7d:db	ARP	42	192.168.3.97 is at 12:ff:66:9a:ed:ba
1326	48.120890	12:ff:66:9a:ed:ba	Intel_74:7d:db	ARP	42	Who has 192.168.3.119? Tell 192.168.3.97
1327	48.120129	Intel_74:7d:db	12:ff:66:9a:ed:ba	ARP	42	192.168.3.119 is at 54:6c:eb:74:7d:db
1822	73.793091	12:ff:66:9a:ed:ba	Intel_74:7d:db	ARP	42	Who has 192.168.3.119? Tell 192.168.3.97
1830	73.793183	Intel_74:7d:db	12:ff:66:9a:ed:ba	ARP	42	192.168.3.119 is at 54:6c:eb:74:7d:db
2748	99.767636	12:ff:66:9a:ed:ba	Intel_74:7d:db	ARP	42	Who has 192.168.3.119? Tell 192.168.3.97
2749	99.767650	Intel_74:7d:db	12:ff:66:9a:ed:ba	ARP	42	192.168.3.119 is at 54:6c:eb:74:7d:db
3075	124.698451	12:ff:66:9a:ed:ba	Intel_74:7d:db	ARP	42	Who has 192.168.3.119? Tell 192.168.3.97
3076	124.698469	Intel_74:7d:db	12:ff:66:9a:ed:ba	ARP	42	192.168.3.119 is at 54:6c:eb:74:7d:db
3259	153.463237	12:ff:66:9a:ed:ba	Intel_74:7d:db	ARP	42	Who has 192.168.3.119? Tell 192.168.3.97
3260	153.463269	Intel_74:7d:db	12:ff:66:9a:ed:ba	ARP	42	192.168.3.119 is at 54:6c:eb:74:7d:db
3519	183.064894	Intel_74:7d:db	Broadcast	ARP	42	Who has 192.168.3.97? Tell 192.168.3.119

<p>Frame 1218: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D623...}</p> <p>Ethernet II, Src: Intel_74:7d:db (54:6c:eb:74:7d:db), Dst: Broadcast (ff:ff:ff:ff:ff:ff)</p> <p>Destination: Broadcast (ff:ff:ff:ff:ff:ff)</p> <p>...1 ... = LG bit: Locally administered address (this is NOT the factory d</p> <p>... .. = IG bit: Group address (multicast/broadcast)</p> <p>Source: Intel_74:7d:db (54:6c:eb:74:7d:db)</p> <p>...0 ... = LG bit: Globally unique address (factory default)</p> <p>...0 ... = IG bit: Individual address (unicast)</p> <p>Type: ARP (0x0806)</p> <p>[Stream index: 1]</p> <p>Address Resolution Protocol (request)</p> <p>Hardware type: Ethernet (1)</p> <p>Protocol type: IPv4 (0x0800)</p> <p>Hardware size: 6</p> <p>Protocol size: 4</p> <p>Opcode: request (1)</p> <p>Sender MAC address: Intel_74:7d:db (54:6c:eb:74:7d:db)</p> <p>Sender IP address: 192.168.3.119</p> <p>Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)</p> <p>Target IP address: 192.168.3.97</p>	<p>0000 ff ff ff ff 54 6c eb 74 7d db 08 06 00 01 ...t...t}</p> <p>0010 08 00 06 00 00 00 54 6c eb 74 7d db c0 a8 03 77 ...t...t}...w</p> <p>0020 00 00 00 00 00 00 c0 a8 03 61a</p>
--	--

- 第一个包含ARP请求信息的以太网帧中，源和目的mac地址为？
源mac地址54:6c:eb:74:7d:db
目的mac地址ff:ff:ff:ff:ff:ff
- 以太网帧EtherType字段值是多少，对应着什么协议？
0x0806，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？
第21个字节
- 进行ARP请求的以太网帧中，ARP负载部分操作字段值是多少？
0001
- ARP消息是否包含发送方的IP地址？
包含。

- 在ARP请求中从哪里看出我们想查询相应IP的mac地址？

ARP请求的操作字段为01，表示是一个查询请求(request)。

找到ARP请求对应的回应包，回答以下问题：

No.	Time	Source	Destination	Protocol	Length	Info
1218	42.716102	Intel_74:7d:db	Broadcast	ARP	42	Who has 192.168.3.97? Tell 192.168.3.119
1219	42.809722	12:ff:66:9a:ed:ba	Intel_74:7d:db	ARP	42	192.168.3.97 is at 12:ff:66:9a:ed:ba
1326	48.128090	12:ff:66:9a:ed:ba	Intel_74:7d:db	ARP	42	Who has 192.168.3.119? Tell 192.168.3.97
1327	48.128129	Intel_74:7d:db	12:ff:66:9a:ed:ba	ARP	42	192.168.3.119 is at 54:6c:eb:74:7d:db
1822	73.793091	12:ff:66:9a:ed:ba	Intel_74:7d:db	ARP	42	Who has 192.168.3.119? Tell 192.168.3.97
1830	73.793183	Intel_74:7d:db	12:ff:66:9a:ed:ba	ARP	42	192.168.3.119 is at 54:6c:eb:74:7d:db
2748	99.767636	12:ff:66:9a:ed:ba	Intel_74:7d:db	ARP	42	Who has 192.168.3.119? Tell 192.168.3.97
2749	99.767650	Intel_74:7d:db	12:ff:66:9a:ed:ba	ARP	42	192.168.3.119 is at 54:6c:eb:74:7d:db
3075	124.698451	12:ff:66:9a:ed:ba	Intel_74:7d:db	ARP	42	Who has 192.168.3.119? Tell 192.168.3.97
3076	124.698469	Intel_74:7d:db	12:ff:66:9a:ed:ba	ARP	42	192.168.3.119 is at 54:6c:eb:74:7d:db
3259	153.463237	12:ff:66:9a:ed:ba	Intel_74:7d:db	ARP	42	Who has 192.168.3.119? Tell 192.168.3.97
3260	153.463269	Intel_74:7d:db	12:ff:66:9a:ed:ba	ARP	42	192.168.3.119 is at 54:6c:eb:74:7d:db
3510	183.064894	Intel_74:7d:db	Broadcast	ARP	42	Who has 192.168.3.97? Tell 192.168.3.119

Frame 1219: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{D623...}	0000	54 6c eb 74 7d db 12 ff 66 9a ed ba 08 06 00 01	T1 t1 ... f
Ethernet II, Src: 12:ff:66:9a:ed:ba (12:ff:66:9a:ed:ba), Dst: Intel_74:7d:db (54:6c:eb:74:7d:db)	0010	08 00 06 04 00 02 12 ff 66 9a ed ba c0 a8 03 61 f
Destination: Intel_74:7d:db (54:6c:eb:74:7d:db)	0020	54 6c eb 74 7d db c0 a8 03 77	T1 t1 ... w
... ..0 ... = IG bit: Globally unique address (factory default)			
... ..0 ... = IG bit: Individual address (unicast)			
Source: 12:ff:66:9a:ed:ba (12:ff:66:9a:ed:ba)			
... ..1 ... = LG bit: Locally administered address (this is NOT the factory d			
... ..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			
Opcodes: reply (2)			
Sender MAC address: 12:ff:66:9a:ed:ba (12:ff:66:9a:ed:ba)			
Sender IP address: 192.168.3.97			
Target MAC address: Intel_74:7d:db (54:6c:eb:74:7d:db)			
Target IP address: 192.168.3.119			

- ARP操作字段在以太网帧的第几个字节？

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？

0002

- ARP回应之前请求信息的内容？

192.168.3.97 is at 12:ff:66:9a:ed:ba

- 包含ARP回应信息的以太网帧中，源和目的mac地址为？

源mac地址:12:ff:66:9a:ed:ba

目的mac地址:54:6c:eb:74:7d:db