

# 计算机网络实验报告\_Ethernet-ARP

---

PB20000219 李蔚林

## 计算机网络实验报告\_Ethernet-ARP

实验目的

实验过程及题目

PART1 Capturing and analyzing Ethernet frames

PART2 The Address Resolution Protocol

EX-1. The arp command

EX-2.

实验收获

## 实验目的

---

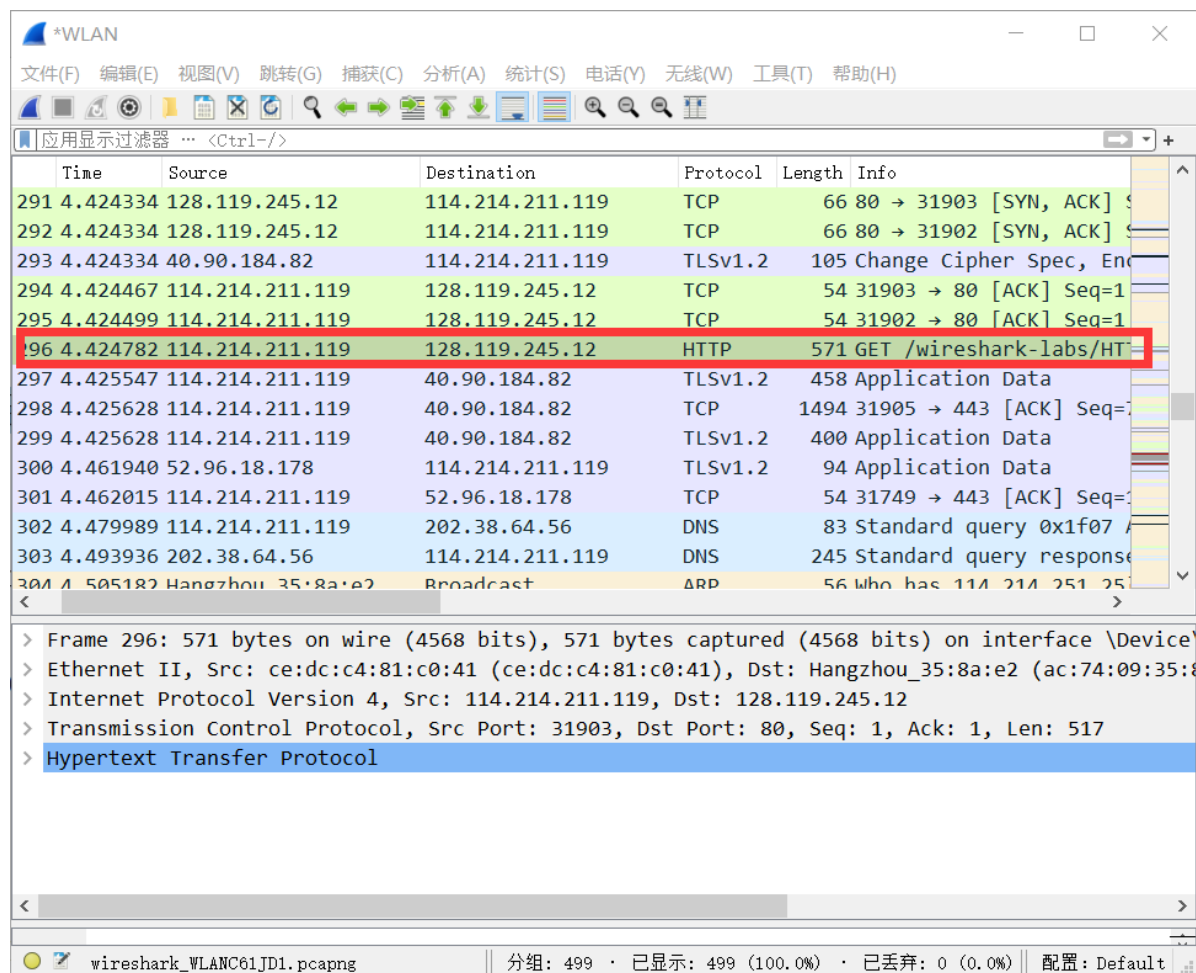
1. 复习巩固链路层相关知识
2. 复习巩固ARP协议
3. 复习巩固以太网相关知识

## 实验过程及题目

---

### PART1 Capturing and analyzing Ethernet frames

首先开启wireshark软件并用浏览器(已清除cookies)打开网址:<http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html>.结束抓包,wireshark界面如下:



由于自己抓的包特别乱,(好像是因为后台挂着下载任务的问题),所以下面我们分析作者抓的包.

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

作者抓的包的自己的Ethernet address为: 00:d0:59:a9:3d:68.

ethernet-ethereal-trace-1

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
6	13.542...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1
7	17.444...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
11	17.494...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	17.498...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	17.500...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4

.... ..0. .... = LG bit: Globally unique address (factory default)  
 .... ..0. .... = IG bit: Individual address (unicast)  
 Source: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)  
 Address: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)  
 .... ..0. .... = LG bit: Globally unique address (factory default)  
 .... ..0. .... = IG bit: Individual address (unicast)  
 Type: IPv4 (0x0800)  
 Data (672 bytes)  
 Data: 450002a000fa40008006bfc8c0a801698077f50c04220050651499a7aca53fb45018faf0...

0000	00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00	..%..s.. Y=h..E.
0010	02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69 80 77	....@... ..i.w
0020	f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4 50 18	..."De...?..P.
0030	fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72	...~O..GF.T ether
0040	65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74	eal-labs /HTTP-et
0050	68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33	hereal-l ab-file3
0060	2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a	.html HT TP/1.1..

Data (data.data), 672 byte(s) | 分组: 17 · 已显示: 17 (100.0%) | 配置: Default

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?

是00:06:25:da:af:73.这不是 gaia.cs.umass.edu 的以太网地址。应该是作者使用的设备的默认路由地址。  
 (个人想法:事实上可以打开cmd,输入ipconfig /all找到默认路由ip,接下来 arp -a,找到该ip对应的MAC应该就是本题所求的结果)

ethernet-ethereal-trace-1

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
6	13.542...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1
7	17.444...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
11	17.494...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	17.498...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	17.500...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4

> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)

▼ Ethernet II, Src: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG\_da:af:73 (00:06:25:da:af:73)

Destination: LinksysG\_da:af:73 (00:06:25:da:af:73)

Address: LinksysG\_da:af:73 (00:06:25:da:af:73)

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

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

▼ Source: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

Address: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

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

0000	00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00	..%.s..Y=h..E.
0010	02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69 80 77	....@...i.w
0020	f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4 50 18	..."Pe....?P.
0030	fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72	..~O..GE T /ether
0040	65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74	eal-labs /HTTP-et
0050	68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33	hereal-l ab-file3
0060	2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a	.html HT TP/1.1..

Data (data.data), 672 byte(s) || 分组: 17 · 已显示: 17 (100.0%) || 配置: Default

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

0x0800.对应的是IPv4协议。

ethernet-ethereal-trace-1

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
6	13.542...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1
7	17.444...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
11	17.494...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	17.498...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	17.500...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4

.... 00000000 = IG bit: Individual address (unicast)  
 Source: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)  
 Address: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)  
 .... 00000000 = IG bit: Globally unique address (factory default)  
 .... 00000000 = IG bit: Individual address (unicast)  
 Type: IPv4 (0x0800)  
 Data (672 bytes)  
 Data: 450002a000fa40008006bfc8c0a801698077f50c04220050651499a7aca53fb45018faf0...  
 [Length: 672]

Offset	Hex	ASCII
0000	00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00	..%.s..Y+=h..E.
0010	02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69 80 77	....@...i.w
0020	f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4 50 18	..."Pe....?.P.
0030	fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72	...~O...GE T /ether
0040	65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74	eal-labs /HTTP-et
0050	68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33	hereal-l ab-file3
0060	2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a	.html HT TP/1.1..

Type (eth. type), 2 byte(s) | 分组: 17 · 已显示: 17 (100.0%) | 配置: Default

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

如图所示，一共55个字节。

ethernet-ethereal-trace-1

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
6	13.542...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1
7	17.444...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
11	17.494...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	17.498...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	17.500...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4

.... 00000000 = IG bit: Individual address (unicast)  
 Source: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)  
 Address: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)  
 .... 00000000 = IG bit: Globally unique address (factory default)  
 .... 00000000 = IG bit: Individual address (unicast)  
 Type: IPv4 (0x0800)  
 Data (672 bytes)  
 Data: 450002a000fa40008006bfc8c0a801698077f50c04220050651499a7aca53fb45018faf0...  
 [Length: 672]

0000	00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00	..%.s..Y=h..E.
0010	02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69 80 77	...@... ..i.w
0020	f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4 50 18	..."Pe. ....?.P.
0030	fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72	...0..Ge T /ether
0040	65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74	ea1-lab5 /HTTP-et
0050	68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33	hereal-l ab-file3
0060	2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a	.html HT TP/1.1..

Data (data.data), 672 byte(s) | 分组: 17 · 已显示: 17 (100.0%) | 配置: Default

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?

00:06:25:da:af:73.两个都不是.如前面分析,这是作者使用设备的默认路由地址.

ethernet-ethereal-trace-1

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
6	13.542...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1
7	17.444...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
11	17.494...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	17.498...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	17.500...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4

Source: LinksysG\_da:af:73 (00:06:25:da:af:73)  
 Address: LinksysG\_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)  
 Data (1500 bytes)  
 Data: 456005dc8f2f4000370676f78077f50cc0a8016900500422aca53fb465149c1f50101b28...  
 [Length: 1500]

0000	00 d0 59 a9 3d 68 00 06 25 da af 73 08 00 45 60	..Y.=h..%.s..E`
0010	05 dc 8f 2f 40 00 37 06 76 f7 80 77 f5 0c c0 a8	.../@.7. v...w....
0020	01 69 00 50 04 22 ac a5 3f b4 65 14 9c 1f 50 10	.i.P."..?.e...P.
0030	1b 28 5e d0 00 00 48 54 54 50 2f 31 2e 31 20 32	.(^...HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74	00 OK..D ate: Sat
0050	2c 20 32 38 20 41 75 67 20 32 30 30 34 20 31 37	, 28 Aug 2004 17
0060	3a 31 39 3a 33 37 20 47 4d 54 0d 0a 53 65 72 76	:19:37 G MT..Serv

Data (data.data), 1,500 byte(s) || 分组: 17 · 已显示: 17 (100.0%) || 配置: Default

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

00:d0:59:a9:3d:68.是作者使用的设备自己的地址

ethernet-ethereal-trace-1

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
6	13.542...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1
7	17.444...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
11	17.494...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	17.498...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	17.500	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4

> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 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)

▼ Destination: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

Address: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

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

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

▼ Source: LinksysG\_da:af:73 (00:06:25:da:af:73)

Address: LinksysG\_da:af:73 (00:06:25:da:af:73)

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

0000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 00 45 60 ..Y.=h..%..s..E`

0010 05 dc 8f 2f 40 00 37 06 76 f7 80 77 f5 0c c0 a8 .../@.7. v..w....

0020 01 69 00 50 04 22 ac a5 3f b4 65 14 9c 1f 50 10 .i.P."..?.e...P.

0030 1b 28 5e d0 00 00 48 54 54 50 2f 31 2e 31 20 32 .(^...HT TP/1.1 2

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74 00 OK..D ate: Sat

0050 2c 20 32 38 20 41 75 67 20 32 30 30 34 20 31 37 , 28 Aug 2004 17

0060 3a 31 39 3a 33 37 20 47 4d 54 0d 0a 53 65 72 76 :19:37 G MT..Serv

Data (data.data), 1,500 byte(s) | 分组: 17 · 已显示: 17 (100.0%) | 配置: Default

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

0x0800.对应的是IPv4协议。

9	17.465...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
11	17.494...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	17.498...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	17.500	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4

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

▼ Source: LinksysG\_da:af:73 (00:06:25:da:af:73)

Address: LinksysG\_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)

▼ Data (1500 bytes)

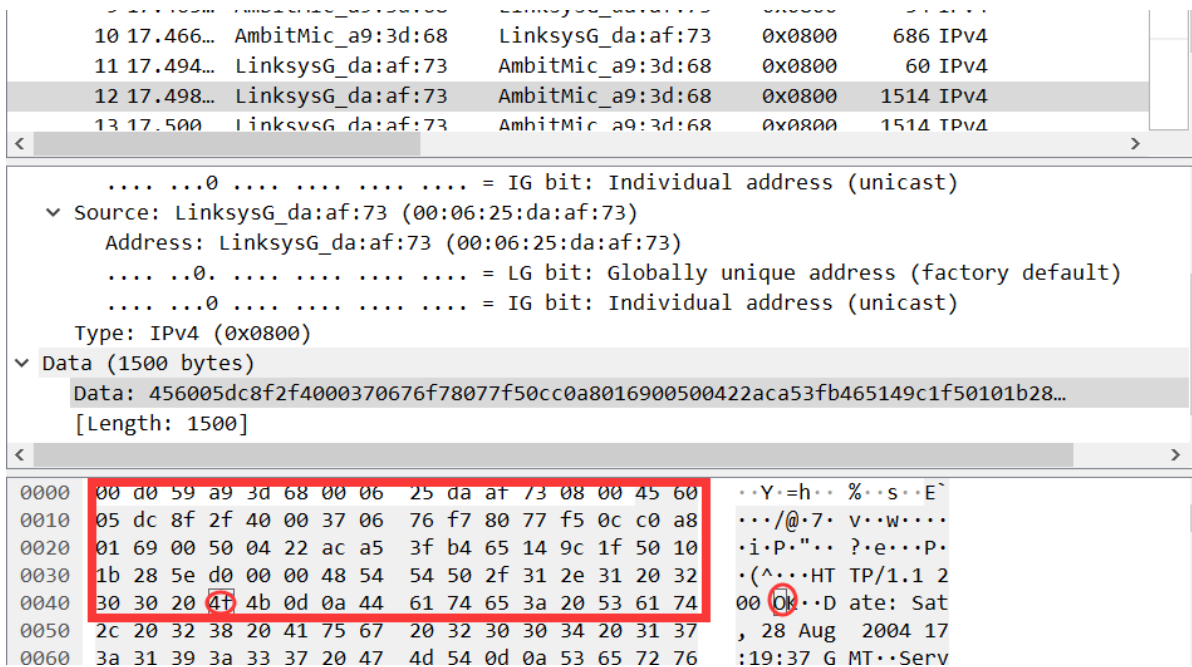
Data: 456005dc8f2f4000370676f78077f50cc0a8016900500422aca53fb465149c1f50101b28...

[Length: 1500]

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?

如图所示，一共68个字节。

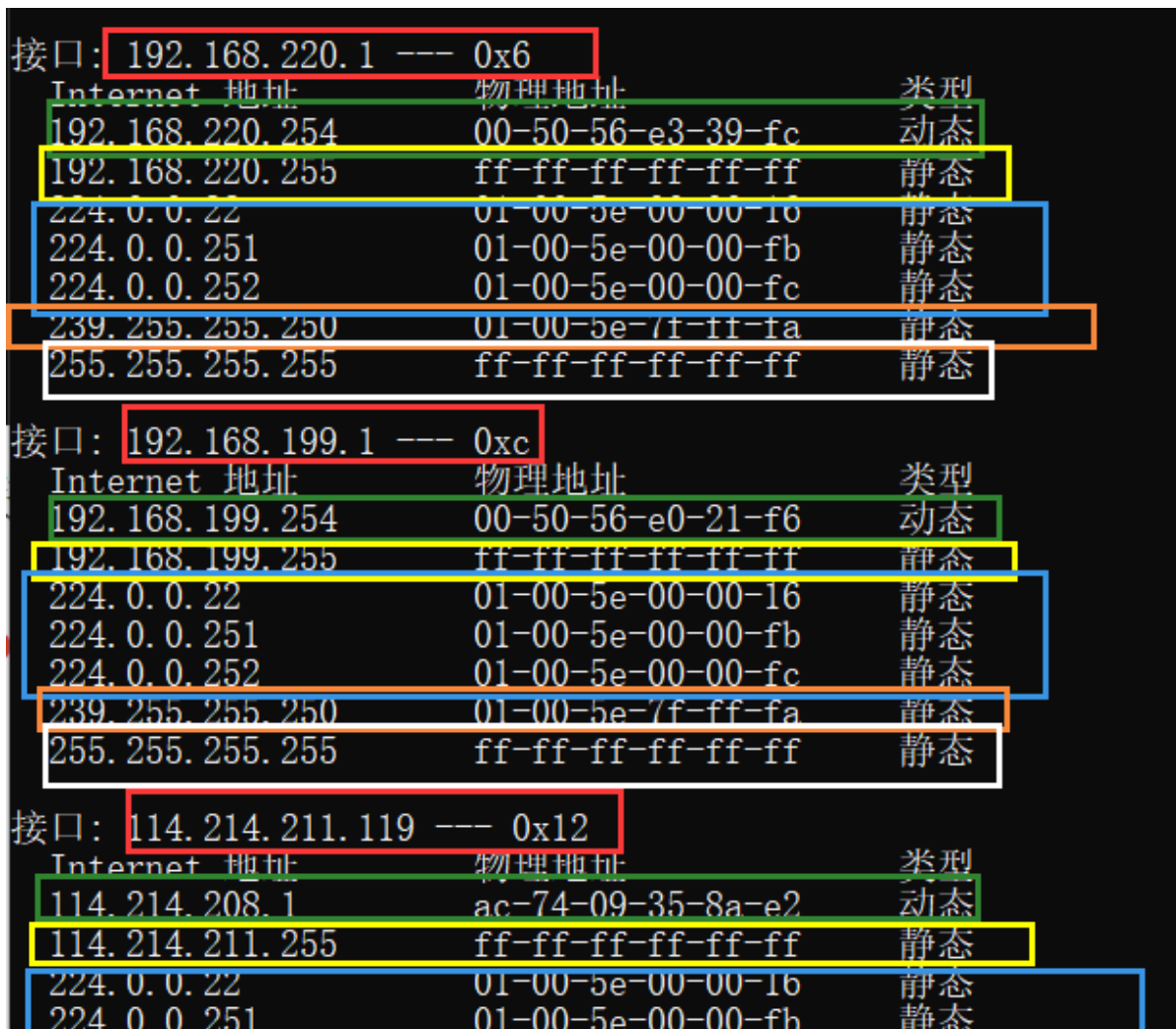




## PART2 The Address Resolution Protocol

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

如下图:红色是指接口(对应不同的IP和MAC),绿色对应的是其路由地址和路由MAC,黄色和白色对应广播地址,蓝色和橙色对应组播地址.



下面的问题由于清理ARP缓存需要root权限,故用作者抓的包进行分析.

```
C:\Users\61794>arp -d *
ARP 项删除失败: 请求的操作需要提升。
```

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

source: 00:d0:59:a9:3d:68

destination: ff:ff:ff:ff:ff:ff

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1
2	0.001018	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1
3	0.001028	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	13.542...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.1
7	17.444...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4

< [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)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff)

> Source: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

Type: ARP (0x0806)

▼ Address Resolution Protocol (request)

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

以太网帧上层协议16进制值是什么?

0x0806, ARP协议.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1
2	0.001018	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1
3	0.001028	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	13.542...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.1
7	17.444...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4

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)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff)

> Source: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

Type: ARP (0x0806)

Address Resolution Protocol (request)

12.

a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

21字节.

1	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who ha
2	0.001018	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.16
3	0.001028	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	13.542...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who ha
7	17.444...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4

#### 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

00	ff	ff	ff	ff	ff	ff	00	d0	59	a9	3d	68	08	06	00	01	.....	Y.=h....
10	08	00	06	04	00	01	00	d0	59	a9	3d	68	c0	a8	01	69	....	Y.=h...i
20	00	00	00	00	00	00	c0	a8	01	01							.....	

12.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?

opcode是1.

1	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who ha
2	0.001018	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.16
3	0.001028	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	13.542...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who ha
7	17.444...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4

#### 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)

12.

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

包含,如图:192.168.1.105

	Destination	Protocol	Length	Info
9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
a:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
3:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
a:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
<				
▼ 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				
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 00 00	00 00 00 00 00 00 00 00	.....	.....

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

如图,操作数为1代表是询问MAC地址,同时info栏有问题"Who has 192.168.1.1",且目标MAC为空.

	Destination	Protocol	Length	Info
9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
a:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
3:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
a:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
<				
▼ 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				
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 00 00	00 00 00 00 00 00 00 00	.....	.....

13.

a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

21字节.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.105 at 00:06:25:da:af:73?
2	0.001018	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	13.542...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.104 at 00:06:25:da:af:73?
7	17.444...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4

Padding: 00000000000000000000000000000000

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

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	....[....%.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	.....

13.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?

由a)图中可以知道opcode = 2.

13.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?

如图,info栏有:"192.168.1.1 is at 00:06:25:da:af:73",操作数为2,且有Target MAC address.

	Destination	Protocol	Length	Info
d:68	Broadcast	ARP	42	Who has 192.168.1.105 at 00:06:25:da:af:73?
f:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
d:68	LinksysG_da:af:73	0x0800	62	IPv4
d:68	LinksysG_da:af:73	0x0800	62	IPv4
d:68	LinksysG_da:af:73	0x0800	62	IPv4
d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
d:68	LinksysG_da:af:73	0x0800	62	IPv4
f:73	AmbitMic_a9:3d:68	0x0800	62	IPv4

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	..Y.=h..%.s...
0010	08 00 06 04 00 02 00 06 25 da af 73 c0 a8 01 01	....[....%.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	.....

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

source:00:06:25:da:af:73



destination:00:d0:59:a9:3d:68

```
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73),  
> Destination: AmbitM1c a9:3d:68 (00:d0:59:a9:3d:68)  
> Source: LinksysG_da:af:73 (00:06:25:da:af:73)  
Type: ARP (0x0806)
```

15.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?

因为获取目标地址是广播的.但是回复仅仅传回进行询问的主机.

## EX-1. The arp command

如果按照题目所说,那么在添加了正确IP地址而错误的MAC地址后,尝试ping该ip地址将会无法连接(超时).这是因为链路层无法对该信息进行正确传输导致的.由于需要高级权限,本题无法实验.

## 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.

我们查询相应的Windows操作系统文档,发现似乎并没有默认的有效时间.但是找到论一个计算公式如下图.

在 Vista TCP/IP 堆栈Windows中, 当邻接缓存中不存在匹配的条目时, 主机将创建邻接缓存条目。IPv4 的 ARP 缓存条目是邻接缓存条目的一个示例。在邻接缓存中成功创建条目后, 如果条目满足特定条件, 该条目可能会更改为"Reachable"状态。如果条目为"Reachable"状态, Windows Vista TCP/IP 主机不会向网络发送 ARP 请求。因此, Windows Vista TCP/IP 主机使用缓存中的信息。如果未使用条目, 并且其保持"可到达"状态的时间超过其"可到达时间"值, 则条目将更改为"过时"状态。如果某个条目的状态为"过时", vista TCP/IP Windows必须发送 ARP 请求以到达该目标。

"Reachable Time"值的计算公式如下:

Reachable Time = BaseReachable Time × (A random value between MIN\_RANDOM\_FACTOR and MAX\_RANDOM\_FACTOR)

RFC 提供以下计算结果。

BaseReachable 时间	30, 000 毫秒 (毫秒)
MIN_RANDOM_FACTOR	0.5
MAX_RANDOM_FACTOR	1.5

因此, "可到达时间"值介于 15 秒 (30 × 0.5 秒) 到 45 秒之间 (30 × 1.5 秒)。如果某个条目在 15 到 45 秒之间没有使用, 它将进入"过时"状态。然后, 当向目标发送任何 IP 数据报时, 主机必须将 IPV4 的 ARP 请求发送到网络。

查看本电脑ARP地址缓存保存时间可以得到:

```
C:\Users\61794>netsh interface ipv4 show interface 18
```

### 接口 WLAN 参数

```
-----  
IfLuid                      : wireless_32768  
IfIndex                     : 18  
状态                        : connected  
跃点数                      : 65  
链接 MTU                    : 1500 字节  
可访问时间                  : 17000 毫秒  
基本可访问时间              : 30000 毫秒  
重传间隔                    : 1000 毫秒  
DAD 传输                    : 3  
站点前缀长度                : 64  
站点 ID                     : 1  
转发                        : disabled  
播发                        : disabled  
邻居发现                    : enabled  
邻居无法访问检测           : enabled  
路由器发现                  : dhcp  
受管理的地址配置            : enabled  
其他有状态的配置            : enabled  
弱主机发送                  : disabled  
弱主机接收                  : disabled  
使用自动网卡数              : 1
```

## 实验收获

本次实验学习并巩固了ARP,以太网相关的链路层知识,同时学习了实践层面如何对计算机发出的MAC请求和回复帧进行抓包,在附加实验中了解到了更多知识,收益匪浅.