

实验 6：ARP 实验

学号：PB21000224 姓名：陈鸿绪 日期：12. 11. 2023

清除记录：

删除浏览历史记录

☒保留收藏夹网站数据(R)
保留 Cookie 和 Internet 临时文件，以使你收藏的网站能够保存偏好选项并提高显示速度。

☒Internet 临时文件(T)
为快速查看而保存的网页、图像和媒体的副本

☒Cookie(O)
网站在计算机上存储的文件，以保存登录信息等首选项。

☒历史记录(H)
已访问网站的列表。

☐下载历史记录(W)
你已下载的文件列表。

☐表单数据(F)
保存在表单中键入的信息。

☐密码(P)
登录以前访问过的网站时，自动填充保存的密码。

[关于删除浏览历史记录](#)

删除(D)

取消

上指定网站：

THE BILL OF RIGHTS

Amendments 1-10 of the Constitution

The Conventions of a number of the States having, at the time of adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory and restrictive clauses should be added, and as extending the ground of public confidence in the Government will best insure the beneficent ends of its institution;

Resolved, by the Senate and House of Representatives of the United States of America, in Congress assembled, two-thirds of both Houses concurring, that the following articles be proposed to the Legislatures of the several States, as amendments to the Constitution of the United States; all or any of which articles, when ratified by three-fourths of the said Legislatures, to be valid to all intents and purposes as part of the said Constitution, namely:

Amendment I

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Amendment II

A well regulated militia, being necessary to the security of a free state, the right of the people to keep and bear arms, shall not be infringed.

Amendment III

No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.

Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

修改捕获数据包的协议类型，仅显示 IP 以下协议信息：

- ☐ IPv4 Internet Protocol Version 4
- ☒ IPv4 Address Acknowledge... MIPv6 Option - IPv4 Address Acknowledgement
- ☒ IPv4 Care-of Address MIPv6 Option - IPv4 Care-of Address
- ☒ IPv4 Default Router Address IPv4 Default Router Address
- ☒ IPv4 Default-Router Address MIPv6 Option - IPv4 Default-Router Address
- ☒ IPv4 DHCP Support Mode MIPv6 Option - IPv4 DHCP Support Mode
- ☒ IPv4 Home Address MIPv6 Option - IPv4 Home Address
- ☒ IPv4 Home Address Reply MIPv6 Option - IPv4 Home Address Reply
- ☒ IPv4 Home Address Request MIPv6 Option - IPv4 Home Address Request
- ☐ IPv6 Internet Protocol Version 6
- ☒ IPv6 compression IPv6 compression
- ☒ IPv6 Destination Destination Options for IPv6
- ☒ IPv6 Fragment Fragment Header for IPv6

No.	Time	Source	Destination	Protocol	Length	Info
1433	2023-12-11 00:57:14.844134	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	66	IPv4
1436	2023-12-11 00:57:14.843806	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	66	IPv4
1435	2023-12-11 00:57:14.843267	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	66	IPv4
1434	2023-12-11 00:57:14.842400	e2:c5:2c:b8:06:f8	IntelCor_f4:d9:95	0x0800	93	TpV4
1433	2023-12-11 00:57:14.841240	e2:c5:2c:b8:06:f8	IntelCor_f4:d9:95	0x0800	77	TpV4
1432	2023-12-11 00:57:14.488301	e2:c5:2c:b8:06:f8	IntelCor_f4:d9:95	0x06dd	74	IPv6
1431	2023-12-11 00:57:14.481895	e2:c5:2c:b8:06:f8	IntelCor_f4:d9:95	0x06dd	74	IPv6
1430	2023-12-11 00:57:14.387727	e2:c5:2c:b8:06:f8	IntelCor_f4:d9:95	0x0800	54	IPv4
1429	2023-12-11 00:57:14.367564	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	77	IPv4
1428	2023-12-11 00:57:14.367564	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	77	IPv4
1427	2023-12-11 00:57:14.295719	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	77	IPv4
1426	2023-12-11 00:57:14.295449	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	77	IPv4
1425	2023-12-11 00:57:14.294452	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	54	IPv4
1424	2023-12-11 00:57:14.294388	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x06dd	74	IPv6
1423	2023-12-11 00:57:14.294226	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x06dd	74	IPv6
1422	2023-12-11 00:57:13.074183	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	66	IPv4
1421	2023-12-11 00:57:12.778188	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	66	IPv4
1420	2023-12-11 00:57:11.829727	e2:c5:2c:b8:06:f8	IntelCor_f4:d9:95	0x0800	89	IPv4
1419	2023-12-11 00:57:11.785010	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	81	IPv4
1418	2023-12-11 00:57:11.631440	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	54	IPv4
1417	2023-12-11 00:57:11.631081	e2:c5:2c:b8:06:f8	IntelCor_f4:d9:95	0x0800	54	IPv4
1416	2023-12-11 00:57:11.379004	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	54	IPv4
1415	2023-12-11 00:57:09.885158	e2:c5:2c:b8:06:f8	IntelCor_f4:d9:95	0x0800	66	IPv4
1414	2023-12-11 00:57:09.291506	e2:c5:2c:b8:06:f8	IntelCor_f4:d9:95	0x0800	66	IPv4
1413	2023-12-11 00:57:09.062225	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	66	IPv4
1412	2023-12-11 00:57:09.050975	e2:c5:2c:b8:06:f8	IntelCor_f4:d9:95	ARP	42	192.168.43.1 is at e2:c5:2c:b8:06:f8
1411	2023-12-11 00:57:09.046197	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	ARP	42	Who has 192.168.43.1? Tell 192.168.43.39
1410	2023-12-11 00:57:09.030866	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	54	IPv4
1409	2023-12-11 00:57:08.768804	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	66	IPv4

由于抓包干扰较多，采取文档提供的包：

No.	Time	Source	Destination	Protocol	Length	Info
1	2004-08-29 01:19:20.157130	AmbitMic_a9:3d:...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	2004-08-29 01:19:20.158148	LinksysG_da:af:...	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	2004-08-29 01:19:20.158158	AmbitMic_a9:3d:...	LinksysG_da:af:73	0x0800	62	IPv4
4	2004-08-29 01:19:23.119980	AmbitMic_a9:3d:...	LinksysG_da:af:73	0x0800	62	IPv4
5	2004-08-29 01:19:29.128618	AmbitMic_a9:3d:...	LinksysG_da:af:73	0x0800	62	IPv4
6	2004-08-29 01:19:33.700104	CnetTech_73:8d:...	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	2004-08-29 01:19:37.601553	AmbitMic_a9:3d:...	LinksysG_da:af:73	0x0800	62	IPv4
8	2004-08-29 01:19:37.623032	LinksysG_da:af:...	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	2004-08-29 01:19:37.623057	AmbitMic_a9:3d:...	LinksysG_da:af:73	0x0800	54	IPv4
10	2004-08-29 01:19:37.623598	AmbitMic_a9:3d:...	LinksysG_da:af:73	0x0800	686	IPv4
11	2004-08-29 01:19:37.651896	LinksysG_da:af:...	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	2004-08-29 01:19:37.656065	LinksysG_da:af:...	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	2004-08-29 01:19:37.657155	LinksysG_da:af:...	AmbitMic_a9:3d:68	0x0800	1514	IPv4
14	2004-08-29 01:19:37.657199	AmbitMic_a9:3d:...	LinksysG_da:af:73	0x0800	54	IPv4
15	2004-08-29 01:19:37.684187	LinksysG_da:af:...	AmbitMic_a9:3d:68	0x0800	1514	IPv4
16	2004-08-29 01:19:37.684552	LinksysG_da:af:...	AmbitMic_a9:3d:68	0x0800	489	IPv4
17	2004-08-29 01:19:37.684587	AmbitMic_a9:3d:...	LinksysG_da:af:73	0x0800	54	IPv4

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

AmbitMic_a9:3d:68 LinksysG_da:af:73 0x0800 62 IPv4

AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

Ethernet address: AmbitMic_a9:3d:68(00:d0:59:a9:3d:68)

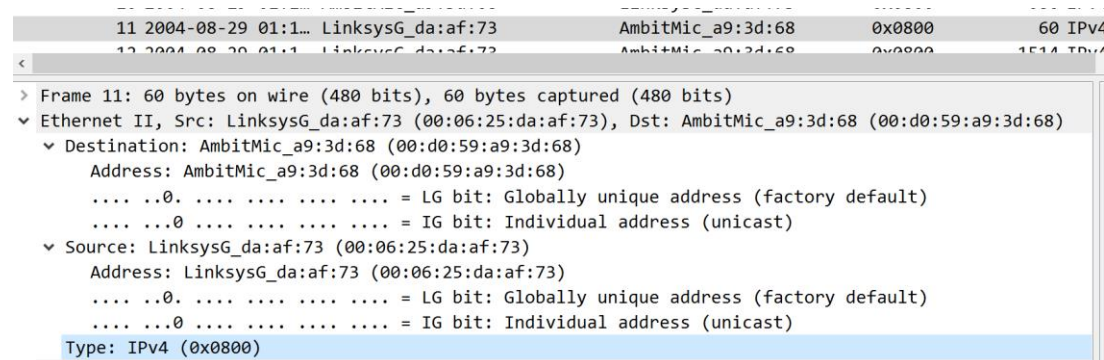
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure

you understand the answer here.]

Destination: LinksysG_da:af:73 (00:06:25:da:af:73)

不是 gaia.cs.umass.edu 的 Ethernet address, 该地址有可能是连接该子网的路由器。

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



hexadecimal value: 0x0800

协议: IPv4

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

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	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..
0070	48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d	Host: ga ia.cs.um
0080	61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67	ass.edu. ·User-Ag
0090	65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30	ent: Moz illa/5.0
00a0	20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69	(Window s; U; Wi
00b0	6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65 6e	ndows NT 5.1; en
00c0	2d 55 53 3b 20 72 76 3a 31 2e 30 2e 32 29 20 47	-US; rv: 1.0.2) G
00d0	65 63 6b 6f 2f 32 30 30 33 30 32 30 38 20 4e 65	ecko/200 30208 Ne
00e0	74 73 63 61 70 65 2f 37 2e 30 32 0d 0a 41 63 63	tscape/7 .02..Acc
00f0	65 70 74 3a 20 74 65 78 74 2f 78 6d 6c 2c 61 70	ept: tex t/xml,ap

由图, 前面有三行, 所以是 48 个, G 之前的第四行有 6 个, 所以 G 之前有 54 字节 (不包括 G, 如果包括则为 55)。

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?

Source: LinksysG_da:af:73 (00:06:25:da:af:73)

LinksysG_da:af:73 (00:06:25:da:af:73)

不是 address of my computer 或者 gaia.cs.umass.edu, 是连接子网的路由器地址。

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

Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

是 the Ethernet address of my computer

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

12	2004-08-29 01:1...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514 IPv4
13	2004-08-29 01:1...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514 IPv4
14	2004-08-29 01:1...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54 IPv4
15	2004-08-29 01:1...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514 IPv4
16	2004-08-29 01:1...	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489 IPv4
17	2004-08-29 01:1...	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54 IPv4

[Protocols in frame: eth:ethertype:data]					
▼	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)				
0. = IG bit: Individual address (unicast)				
	Type: IPv4 (0x0800)				

答案: 0x0800, IPv4

8. How many bytes from the very start of the Ethernet frame does the ASCII “0” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?

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
0070	65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34	er: Apac he/2.0.4
0080	30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 78	0 (Red H at Linux
0090	29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64)..Last- Modified
00a0	3a 20 53 61 74 2c 20 32 38 20 41 75 67 20 32 30	: Sat, 2 8 Aug 20
00b0	30 34 20 31 37 3a 31 38 3a 35 33 20 47 4d 54 0d	04 17:18 :53 GMT.
00c0	0a 45 54 61 67 3a 20 22 31 62 61 35 63 2d 31 31	.ETag: " 1ba5c-11
00d0	39 34 2d 36 39 65 64 39 34 30 22 0d 0a 41 63 63	94-69ed9 40"..Acc
00e0	65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65	ept-Rang es: byte
00f0	73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74	s..Conte nt-Lengt

4*16 + 3 =67 （不包括“0”，包括“0”则为68）

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

```
C:\Users\86181>arp -a

接口: 192.168.43.39 --- 0xa
Internet 地址      物理地址      类型
192.168.43.1      e2-c5-2c-b8-06-f8  动态
192.168.43.255    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
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: 192.168.137.1 --- 0xe
Internet 地址      物理地址      类型
192.168.137.255   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
239.255.255.250   01-00-5e-7f-ff-fa  静态
255.255.255.255   ff-ff-ff-ff-ff-ff  静态
```

网卡: 192.168.43.39

路由 IP: 192.168.43.1 e2-c5-2c-b8-06-f8 动态

组播地址: 255.255.255.255 ff-ff-ff-ff-ff-ff 静态

MAC 地址: 192.168.43.255 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
广播地址: 239.255.255.250 01-00-5e-7f-ff-fa 静态

进行如下操作:

```
C:\Windows\system32>arp -d

C:\Windows\system32>
```

1. clear arp 缓存:
2. 清空浏览器缓存
3. wireshark 抓包
4. 打开停止抓包
5. 抓包界面如下 (只有比 IP 低层的协议)

No.	Time	Source	Destination	Protocol	Length	Info
214	2023-12-11 11:40:02.825484	e2:c5:2c:b8:06:...	IntelCor_f4:d9:95	0x0800	385	IPv4
215	2023-12-11 11:40:02.825834	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	97	IPv4
216	2023-12-11 11:40:02.864921	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x86dd	74	IPv6
217	2023-12-11 11:40:04.065513	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	54	IPv4
218	2023-12-11 11:40:04.065570	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x86dd	74	IPv6
219	2023-12-11 11:40:04.065570	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x86dd	74	IPv6
220	2023-12-11 11:40:04.065570	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x86dd	74	IPv6
221	2023-12-11 11:40:04.065590	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x86dd	74	IPv6
222	2023-12-11 11:40:04.706325	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	155	IPv4
223	2023-12-11 11:40:04.926300	e2:c5:2c:b8:06:...	IntelCor_f4:d9:95	0x0800	225	IPv4
224	2023-12-11 11:40:04.970807	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	54	IPv4
225	2023-12-11 11:40:05.092930	e2:c5:2c:b8:06:...	IntelCor_f4:d9:95	0x86dd	86	IPv6
226	2023-12-11 11:40:05.092978	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x86dd	86	IPv6
227	2023-12-11 11:40:05.267116	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	66	IPv4
228	2023-12-11 11:40:05.308084	e2:c5:2c:b8:06:...	IntelCor_f4:d9:95	0x0800	521	IPv4
229	2023-12-11 11:40:05.308578	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	97	IPv4
230	2023-12-11 11:40:05.323850	e2:c5:2c:b8:06:...	IntelCor_f4:d9:95	0x0800	66	IPv4
231	2023-12-11 11:40:05.323938	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	54	IPv4
232	2023-12-11 11:40:05.324111	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	199	IPv4
233	2023-12-11 11:40:05.324143	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	1386	IPv4
234	2023-12-11 11:40:05.324143	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	519	IPv4
235	2023-12-11 11:40:05.388136	e2:c5:2c:b8:06:...	IntelCor_f4:d9:95	0x0800	54	IPv4
236	2023-12-11 11:40:05.388136	e2:c5:2c:b8:06:...	IntelCor_f4:d9:95	0x0800	54	IPv4
237	2023-12-11 11:40:05.388258	e2:c5:2c:b8:06:...	IntelCor_f4:d9:95	0x0800	125	IPv4
238	2023-12-11 11:40:05.391933	e2:c5:2c:b8:06:...	IntelCor_f4:d9:95	0x0800	59	IPv4
239	2023-12-11 11:40:05.392017	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x0800	54	IPv4
240	2023-12-11 11:40:06.475682	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x86dd	74	IPv6
241	2023-12-11 11:40:07.220180	IntelCor_f4:d9:...	e2:c5:2c:b8:06:f8	0x86dd	75	IPv6
242	2023-12-11 11:40:07.283078	e2:c5:2c:b8:06:...	IntelCor_f4:d9:95	0x86dd	86	IPv6

使用作者的包进行回答问题。

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

No.	Time	Source	Destination
1	2004-08-29 01:19:20.157130	AmbitMic_a9:3d:68	Broadcast
2	2004-08-29 01:19:20.158148	LinksysG_da:af:73	AmbitMic_a9:3d:68
3	2004-08-29 01:19:20.158158	AmbitMic_a9:3d:68	LinksysG_da:af:73
4	2004-08-29 01:19:23.119980	AmbitMic_a9:3d:68	LinksysG_da:af:73
5	2004-08-29 01:19:29.128618	AmbitMic_a9:3d:68	LinksysG_da:af:73
6	2004-08-29 01:19:33.700104	CnetTech_73:8d:ce	Broadcast
7	2004-08-29 01:19:37.601553	AmbitMic_a9:3d:68	LinksysG_da:af:73
8	2004-08-29 01:19:37.623032	LinksysG_da:af:73	AmbitMic_a9:3d:68
9	2004-08-29 01:19:37.623057	AmbitMic_a9:3d:68	LinksysG_da:af:73
10	2004-08-29 01:19:37.623598	AmbitMic_a9:3d:68	LinksysG_da:af:73
11	2004-08-29 01:19:37.651896	LinksysG_da:af:73	AmbitMic_a9:3d:68
12	2004-08-29 01:19:37.656065	LinksysG_da:af:73	AmbitMic_a9:3d:68
13	2004-08-29 01:19:37.657155	LinksysG_da:af:73	AmbitMic_a9:3d:68
14	2004-08-29 01:19:37.657199	AmbitMic_a9:3d:68	LinksysG_da:af:73
15	2004-08-29 01:19:37.684187	LinksysG_da:af:73	AmbitMic_a9:3d:68

[Frame is ignored: False]	0000	ff ff ff
[Protocols in frame: eth:ethertype:arp]	0010	08 00 06
[Coloring Rule Name: ARP]	0020	00 00 00
[Coloring Rule String: arp]		
▼ 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)		
Address: Broadcast (ff:ff:ff:ff:ff:ff)		
....1. = LG bit: Locally administered address		
....1. = IG bit: Group address (multicast/broadcast)		
▼ Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)		
Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)		

destination : Broadcast (ff:ff:ff:ff:ff:ff)

source : AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

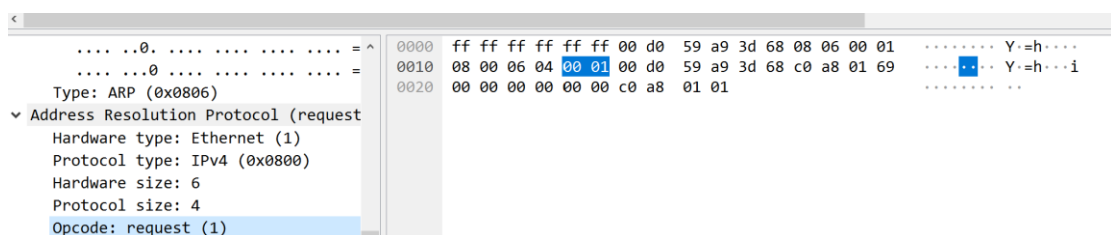
11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

- ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 - Address: Broadcast (ff:ff:ff:ff:ff:ff)
 -1. = LG bit: Locally administered address
 -1 = IG bit: Group address (multicast/broadcast)
- ▼ 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: ARP (0x0806)

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?



20bytes(如果包括 opcode 的开头就是 21)

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?

如上图 0x0001

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

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

包含 the IP address of the sender

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

Opcode 告诉我们是 request

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?

20bytes (如果包括 opcode 的开头就是 21)

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?

值为 0x0002

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?

Opcode: reply(2), 是reply

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

- ▼ 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
0. = IG bit: Individual address
- ▼ Source: LinksysG_da:af:73 (00:06:25:da:af:73)
 Address: LinksysG_da:af:73 (00:06:25:da:af:73)

destination : AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

source : LinksysG_da:af:73 (00:06:25:da:af:73)

15. Open the ethernet-ethereal-trace-1 trace file in <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces>. 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?

ARP 查询报文通过广播帧传播，而响应 ARP 通过一个标准帧发送，所以响应 ARP 只有请求 ARP 的结点才可以接受，

Extra Credit

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?

如果输入了正确的 IP 地址，但输入了与该远程接口不匹配的错误的以太网地址，会导致通信失败：系统将尝试使用该错误的以太网地址与远程接口进行通信，但是由于以太网地址不匹配，通信将会失败。将无法与具有正确 IP 地址的远程主机建立连接。

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.

```
C:\Windows\system32>netsh interface ipv4 show interfaces
```

Idx	Met	MTU	状态	名称
1	75	4294967295	connected	Loopback Pseudo-Interface 1
10	55	1500	connected	WLAN
3	25	1500	disconnected	本地连接* 1
14	25	1500	connected	本地连接* 2

Idx=10 对应 WLAN:

```
C:\Windows\system32>netsh interface ipv4 show interface 10
```

接口 WLAN 参数

```
-----  
IfLuid                        : wireless_32768  
IfIndex                       : 10  
状态                          : connected  
跃点数                        : 55  
链接 MTU                     : 1500 字节  
可访问时间                   : 33500 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  
使用自动跃点数               : enabled  
忽略默认路由                 : disabled  
播发的路由器生存期          : 1800 秒  
播发默认路由                 : disabled  
当前跃点限制                 : 0  
强制 ARPND 唤醒模式          : disabled  
定向 MAC 唤醒模式            : disabled  
ECN 功能                     : application  
基于 RA 的 DNS 配置(RFC 6106) : disabled  
DHCP/静态 IP 共存            : disabled
```

基本可访问时间为 30000 毫秒，所以 ARP cache TTL 为 30000