

LAB6

牛庆源 PB21111733

1.

依据source可知：

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMicrosy_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1 is at
2	0.001018	LinksysGroup_da:af:73	AmbitMicrosy_a9:3d:68	ARP	60	192.168.1.1 is at
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] Seq=0
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] Seq=0
6	13.542974	CnetTechnolo_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.1 is at

> Frame 3: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0

> Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)

> Destination: LinksysGroup_da:af:73 (00:06:25:da:af:73)

> Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)

> Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.1.105, Dst: 199.2.53.206

> Transmission Control Protocol, Src Port: 1057, Dst Port: 631, Seq: 0, Len: 0

2.

依据destination可知：

00:06:25:da:af:73

不是gaia.cs.umass.edu的以太网地址，是距离本机最近的路由器地址

3.

由Type：IPv4 (0x0800)可知

双字节帧类型字段的十六进制值为：0x0800，对应的上层协议为IPv4

4.

由下图GET中G的位置出现在0x0037即第55byte，前面有54bytes

No.	Time	Source	Destination	Protocol	Length	Info
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-...

> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits) on interface 0

> Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)

> Destination: LinksysGroup_da:af:73 (00:06:25:da:af:73)

> Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)

> Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.1.105, Dst: 128.119.245.12

> Hypertext Transfer Protocol, Src Port: 80, Dst Port: 80

> GET /ethereal-labs/HTTP-ethereal-lab-... HTTP/1.1

5.

依据source可知：

源地址的值是00:06:25:da:af:73

不是电脑地址也不是gaia.cs.umass.edu的地址，是最近路由器的地址

> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

> Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)

> Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)

> Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)

> Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105

> Transmission Control Protocol, Src Port: 80, Dst Port: 1058, Seq: 1, Ack: 633, Len: 1460

• 6.

依据destination可知：
目的地址是00:d0:59:a9:3d:68
是我电脑的以太地址

• 7.

由Type: IPv4 (0x0800)
双字节帧类型字段中的十六进制值为0x0800，上层协议为IPv4

• 8.

200 OK中OK第一次出现在frame 12的0x0044即68byte，前面有67bytes

> Frame 12: 1514 bytes on wire (12112 bits), 1	0000	00 d0 59 a9 3d 68 00 06	25 da af 73 08 00 45 60	..Y.=h.. %..s..E`
Ethernet II, Src: LinksysGroup_da:af:73 (00:	0010	05 dc 8f 2f 40 00 37 06	76 f7 80 77 f5 0c c0 a8	.../@.7. v..w....
> Destination: AmbitMicrosy_a9:3d:68 (00:d0:	0020	01 69 00 50 04 22 ac a5	3f b4 65 14 9c 1f 50 10	..i.P.."... ?..e...P.
> Source: LinksysGroup_da:af:73 (00:06:25:c	0030	1b 28 5e d0 00 00 48 54	54 50 2f 31 2e 31 20 32	..(^...HT TP/1.1 2
Type: IPv4 (0x0800)	0040	30 30 20 4f 4b 0d 0a 44	61 74 65 3a 20 53 61 74	00 OK..D ate: Sat
Internet Protocol Version 4, Src: 128.119.24	0050	2c 20 32 38 20 41 75 67	20 32 30 30 34 20 31 37	, 28 Aug 2004 17
0100 = Version: 4	0060	3a 31 39 3a 33 37 20 47	4d 54 0d 0a 53 65 72 76	:19:37 G MT...Serv
.... 0101 = Header Length: 20 bytes (5)	0070	65 72 3a 20 41 70 61 63	68 65 2f 32 2e 30 2e 34	er: Apac he/2.0.4
Differentiated Services Field: 0x60 (DSCP	0080	30 20 28 52 65 64 20 48	61 74 20 4c 69 6e 75 78	0 (Red H at Linux
Total Length: 1500	0090	29 0d 0a 4c 61 73 74 2d	4d 6f 64 69 66 69 65 64)..Last- Modified
Identification: 0x8f2f (36655)	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

• 9.

内容如下：

C:\Users\23186>arp -a		
接口：169.254.94.198 --- 0x6		
Internet 地址	物理地址	类型
169.254.255.255	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
239.192.152.143	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
接口：202.141.181.210 --- 0xa		
Internet 地址	物理地址	类型
202.141.181.1	00-50-56-9f-00-7f	动态
202.141.181.255	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
239.192.152.143	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

两个接口，每个接口有三列内容，分别是

Internet 地址(IP 地址)，物理地址(MAC地址)，类型（静态永久保存，动态没用就删）

- 10.

源地址为00:d0:59:a9:3d:68

目标地址为ff:ff:ff:ff:ff:ff

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on 0
v Ethernet II, Src: AmbitMicrosy_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: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
  Type: ARP (0x0806)
  > Address Resolution Protocol (request)
```

- 11.

由Type: ARP (0x0806)

双字节以太网帧类型字段的十六进制值为0x0806，上层协议为IPv4

- 12.

- a.

由Opcode: request (1)开始对应的位置为0x0015，所以有0x0014即20bytes

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on 0	0000	ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01
v Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)	0010	08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69
> Destination: Broadcast (ff:ff:ff:ff:ff:ff)	0020	00 00 00 00 00 00 c0 a8 01 01
> Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)		
Type: ARP (0x0806)		
v Address Resolution Protocol (request)		
Hardware type: Ethernet (1)		
Protocol type: IPv4 (0x0800)		
Hardware size: 6		
Protocol size: 4		
Opcode: request (1)		
Sender MAC address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)		
Sender IP address: 192.168.1.105		
Target MAC address: Xerox_00:00:00 (00:00:00:00:00:00)		
Target IP address: 192.168.1.1		

- b.

查看右侧内容可知Opcode为0x0001

- c.

包含了，右侧包含了源地址和目标地址

00 d0 59 a9 3d 68

ff ff ff ff ff ff

- d.

Target IP address字段

- 13.

- a.

同Q12，20bytes

> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)	0000	00 d0 59 a9 3d 68 00 06	25 da af 73 08 06 00 01
▼ Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst:	0010	08 00 06 04 00 02 00 06	25 da af 73 c0 a8 01 01
> Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)	0020	00 d0 59 a9 3d 68 c0 a8	01 69 00 00 00 00 00 00
> Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)	0030	00 00 00 00 00 00 00 00	00 00 00 00
Type: ARP (0x0806)			
Padding: 00			
▼ Address Resolution Protocol (reply)			
Hardware type: Ethernet (1)			
Protocol type: IPv4 (0x0800)			
Hardware size: 6			
Protocol size: 4			
Opcode: reply (2)			
Sender MAC address: LinksysGroup_da:af:73 (00:06:25:da:af:73)			
Sender IP address: 192.168.1.1			
Target MAC address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)			
Target IP address: 192.168.1.105			

- o b.
同Q12，找到其位置，内容为00 02即0x0002
- o c.
回答在Sender MAC address，对应IP地址在Sender IP address

• 14.

由Q13图中的Destination和Source可知

源地址：00:06:25:da:af:73

目的地址:00:d0:59:a9:3d:68

• 15.

因为发送ARP请求时是广播，ARP响应是只有对应IP地址的路由器或者主机响应，而数据包6的请求可能没有这样的主机或者路由器，所以没有响应

• Extra Credit

- o EX-1

正常：

```
C:\Windows\System32>arp -s 255.255.255.255 aa-aa-aa-aa-aa-aa

C:\Windows\System32>arp -a

接口: 169.254.94.198 --- 0x6
Internet 地址      物理地址      类型
224.0.0.22         01-00-5e-00-00-16 静态
239.192.152.143    01-00-5e-40-98-8f 静态
255.255.255.255    ff-ff-ff-ff-ff-ff 静态

接口: 202.141.181.210 --- 0xa
Internet 地址      物理地址      类型
202.141.181.1      00-50-56-9f-00-7f 动态
224.0.0.22         01-00-5e-00-00-16 静态
```

- o EX-2

默认时间是2min