

计网实验6

PB21111723 王涵

PS: 使用实验提供的的ethernet-ethereal-trace-1来回答问题完成实验报告

Q1

您的计算机的48位以太网地址是什么？

10	17.4664...	192.168.1.105	128.119.245.12	HT...	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HT
11	17.4947...	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.4989...	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [T
13	17.5000...	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460

>	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)
>	Source: AmbitMic_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
>	Transmission Control Protocol, Src Port: 1058, Dst Port: 80, Seq: 1, Ack: 1, Len: 632
>	Hypertext Transfer Protocol

得到以太网地址是 00:d0:59:a9:3d:68

Q2

以太网帧中的 48 位目标地址是什么？这是 gaia.cs.umass.edu 的以太网地址吗？（提示：答案是否定的）。那么它是什么？注意这一题可能会犯错，请阅读 468-469(中文版 305-308 页)然后理解它。

10	17.4664...	192.168.1.105	128.119.245.12	HT...	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HT
11	17.4947...	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.4989...	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [T
13	17.5000...	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460

>	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)
>0 = IG bit: Individual address (unicast)
>	Type: IPv4 (0x0800)
>	Internet Protocol Version 4, Src: 192.168.1.105, Dst: 128.119.245.12
>	Transmission Control Protocol, Src Port: 1058, Dst Port: 80, Seq: 1, Ack: 1, Len: 632
>	Hypertext Transfer Protocol

- 以太网帧中的 48 位目标地址是 00:06:25:da:af:73
- 该地址不是gaia.cs.umass.edu的以太网地址。
- 它是路由器的地址，这是用于出子网的链路，属于主机连接到路由器的接口。

Q3

以太网帧上层协议 16 进制值是什么?这对应的上层协议是什么?

```
> Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
> Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  Type: IPv4 (0x0800)
```

- 16进制值是0x800
- 对应上层协议IPv4

Q4

从以太帧的开始，一直到“GET”中的 ASCII“G”出现在以太网帧中为止，有多少字节?

00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00	..%..s.. Y.=h..E.
02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69 80 77@... ..i.w
f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4 50 18	...".Pe.?.P.
fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72	..~0..G E 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 6c 61 62 2d 66 69 6c 65 33	hereal-l ab-file3
2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a	.html HT TP/1.1..
48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d	Host: ga ia.cs.um
61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67	ass.edu. ·User-Ag
65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30	ent: Moz illa/5.0
20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69	(Window s; U; Wi
6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65 6e	ndows NT 5.1; en
2d 55 53 3b 20 72 76 3a 31 2e 30 2e 32 29 20 47	-US; rv: 1.0.2) G
65 63 6b 6f 2f 32 30 30 33 30 32 30 38 20 4e 65	ecko/200 30208 Ne

- G 的ASCII码是 47
- 47 出现在第55bytes的位置
- 那么 G 之前已经有了54bytes

Q5

这个以太网帧中，以太网源地址的值是多少？这是你的计算机的地址，还是gaia.cs.umass.edu 的地址（提示：答案是否定的）。拥有这个以太网地址的设备是什么？

```
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)
> Source: LinksysG_da:af:73 (00:06:25:da:af:73)
  Type: IPv4 (0x0800)
```

- 以太网源地址的值是 00:06:25:da:af:73
- 不是计算机的地址，也不是gaia.cs.umass.edu 的地址
- 这是主机的子网路由器地址

Q6

以太网帧中的目的地址是什么？这是您的计算机的以太网地址吗？

```
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)
> Source: LinksysG_da:af:73 (00:06:25:da:af:73)
  Type: IPv4 (0x0800)
```

- 以太网帧中的目的地址是 00:d0:59:a9:3d:68
- 这是计算机的以太网地址

Q7

以太网帧上层协议 16 进制值是什么？这对应的上层协议是什么？

```
Ethernet II, Src: 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)
  Type: IPv4 (0x0800)
```

- 以太网帧上层协议 16 进制值：0x800
- IPv4协议

Q8

从以太帧的开始，一直到“OK”中的 ASCII“O”出现在以太网帧中为止，有多少字节？

00 d0 59 a9 3d 68 00 06 25 da af 73 08 00 45 60	..Y.=h.. %..s..E`
05 dc 8f 2f 40 00 37 06 76 f7 80 77 f5 0c c0 a8	.../@.7. v..w....
01 69 00 50 04 22 ac a5 3f b4 65 14 9c 1f 50 10	.i.P.".. ?..e...P.
1b 28 5e d0 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 53 61 74	00 OK..D ate: Sat
2c 20 32 38 20 41 75 67 20 32 30 30 34 20 31 37	, 28 Aug 2004 17
3a 31 39 3a 33 37 20 47 4d 54 0d 0a 53 65 72 76	:19:37 G MT..Serv
65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34	er: Apac he/2.0.4
30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 78	0 (Red H at Linux
29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64)..Last- Modified
3a 20 53 61 74 2c 20 32 38 20 41 75 67 20 32 30	: Sat, 2 8 Aug 20
30 34 20 31 37 3a 31 38 3a 35 33 20 47 4d 54 0d	04 17:18 :53 GMT.
0a 45 54 61 67 3a 20 22 31 62 61 35 63 2d 31 31	.ETag: " 1ba5c-11
39 34 2d 36 39 65 64 39 34 30 22 0d 0a 41 63 63	94-69ed9 40" ..Acc

- 0 的ASCII码是 4f
- 4f 出现在第68bytes的位置
- 那么 0 之前已经有了67bytes

Q9

写下计算机 ARP 缓存的内容。每个列值的含义是什么？

```
Microsoft Windows [版本 10.0.22631.2715]
(c) Microsoft Corporation。保留所有权利。

C:\Users\wangh>arp -a

接口: 192.168.203.1 --- 0x8
    Internet 地址      物理地址      类型
    192.168.203.254    00-50-56-f1-a2-e9    动态
    192.168.203.255    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
    255.255.255.255    ff-ff-ff-ff-ff-ff    静态

接口: 202.141.190.179 --- 0xe
    Internet 地址      物理地址      类型
    202.141.190.1      00-50-56-9f-00-7f    动态
    202.141.190.255    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
    255.255.255.255    ff-ff-ff-ff-ff-ff    静态

接口: 192.168.115.1 --- 0x11
    Internet 地址      物理地址      类型
    192.168.115.254    00-50-56-f5-3b-49    动态
    192.168.115.255    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
```

- Internet地址列意即IP地址
- 物理地址列意即MAC地址
- 类型有动态和静态之分：

动态是指在一定的时间内某个表项没有被使用就会被系统删除；静态是指表项会被永久保存。

Q10

包含 ARP 请求消息的以太网帧中源和目标地址的十六进制值是什么？

```

> 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
  > 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)

```

- 源地址是 00:d0:59:a9:3d:68
- 目标地址是 ff:ff:ff:ff:ff:ff

Q11

为双字节以太网帧类型字段提供十六进制值。这对应于什么上层协议？

```

> 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
  > 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)

```

- 0x0806
- ARP协议

Q12

- ARP 操作码字段开始从以太网帧的最开始有多少字节？
- 在进行 ARP 请求的以太网帧的 ARP 负载部分中，操作码字段的值是多少？
- ARP 消息是否包含发送方的 IP 地址？
- 在 ARP 请求中从哪里看出我们要查询相应 IP 的以太网地址？

a)

```

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)

```

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 c0 a8 01 01

距离以太网帧最开始 20 个字节。

- 进行 ARP 请求的以太网帧的 ARP 负载部分中的操作码的值为1
-

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, 如图所示包含发送方的 IP 地址 192.168.1.105

d)

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

如图所示, Target MAC address 字段设置为 00: 00: 00: 00: 00: 00 来对其对应的 IP 地址 192.168.1.1 提问。

Q13

a) ARP 操作码字段开始从以太网帧的最开始有多少字节?

b) 在进行 ARP 响应的以太网帧的 ARP 负载部分中, 操作码字段的值是多少?

c) 在响应 ARP 中从哪里看出现早期 ARP 请求的答案?

a)

Opcode: reply (2)									
0000	00	d0	59	a9	3d	68	00	06	25
0010	08	00	06	04	00	02	00	06	25
0020	da	af	73	08	06	00	01		
0030	00	00	00	00	00	00	00	00	00

ARP 操作码字段开始从以太网帧的最开始有20字节。

b)

> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
v 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)
 > Source: LinksysG_da:af:73 (00:06:25:da:af:73)
 Type: ARP (0x0806)
 Padding: 00000000000000000000000000000000
v 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
 Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 Target IP address: 192.168.1.105

操作码字段2

c)从图中看到,

- Target MAC address 为 00:d0:59:a9:3d:68
- Target IP address 为 192.168.1.105
- 这之前的ARP Sender MAC address、Sender IP address 是照应的

Q14

包含 ARP 回复消息的以太网帧中的源地址和目标地址的十六进制值是多少?

```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on 0
< 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: ARP (0x0806)
    Padding: 00000000000000000000000000000000
< Address Resolution Protocol (reply)
```

- 源地址: 00:06:25:da:af:73
- 目的地址: 00:d0:59:a9:3d:68

Q15

ARP请求是广播的,子网中所有主机都能收到。这个ARP请求没有回复,因为我们不在发送请求的计算机上,回复只能被发送该广播的计算机接受。

EX-1

arp 命令: `arp -s InetAddr EtherAddr` 允许您手动向 ARP 缓存添加一个条目,该条目将 IP 地址 InetAddr 解析为物理地址 EtherAddr。如果在手动添加条目时,输入了正确的 IP 地址,但该远程接口的以太网地址错误,会发生什么情况?

会使本地主机无法访问这个IP地址

EX-2

删除条目之前,条目在 ARP 缓存中保留的默认时间是多少。您可以根据经验(通过监视缓存内容)或通过操作系统文档中查找来确定这一点。指出您如何/在何处确定该值。

我使用的是Windows系统,因此查询Microsoft的官方文档[地址解析协议缓存行为 - Windows Server | Microsoft Learn](#)得到结论:

BaseReachable 时间	30, 000 毫秒 (ms)
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) 和 45 秒之间 (30×1.5 秒)。如果一个条目在 15 到 45 秒之间未使用，它将更改为“过时”状态。然后，当任何 IP 数据报发送到该目标时，主机必须向网络发送 IPv4 的 ARP 请求。

介于15~45s，而接下来通过netsh interface ipv4 show interface 18命令可以查询基本访问时间如下：

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

接口 本地连接* 10 参数
-----
IfLuid                : wireless_32770
IfIndex               : 18
状态                  : disconnected
跃点数                : 25
链接 MTU              : 1500 字节
可访问时间            : 22500 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
```

ARP cache的生存时间，基本可访问时间为 30000 毫秒，即30秒，正好介于15~45s。