Ethernet ARP 实验报告

PB20111689 蓝俊玮

我使用的是实验所提供的包 http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip 中的 ethernet--ethereal-trace-1。

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.105
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	192.168.1.105	199.2.53.206	TCP	62 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	2.962850	192.168.1.105	199.2.53.206	TCP	62 [TCP Retransmission] [TCP Port numbers reused] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
5	8.971488	192.168.1.105	199.2.53.206	TCP	62 [TCP Retransmission] [TCP Port numbers reused] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	13.542974	CnetTech_73:8d:ce	Broadcast	ARP	60 Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62 1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	17.465902	128.119.245.12	192.168.1.105	TCP	62 80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	17.465927	192.168.1.105	128.119.245.12	TCP	54 1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686 GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.498935	128.119.245.12	192.168.1.105	TCP	1514 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
13	17.500025	128.119.245.12	192.168.1.105	TCP	1514 80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
14	17.500069	192.168.1.105	128.119.245.12	TCP	54 1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0
15	17.527057	128.119.245.12	192.168.1.105	TCP	1514 80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
16	17.527422	128.119.245.12	192.168.1.105	HTTP	489 HTTP/1.1 200 OK (text/html)
17	17.527457	192.168.1.105	128.119.245.12	TCP	54 1058 → 80 [ACK] Seq=633 Ack=4816 Win=64240 Len=0

1. Capturing and analyzing Ethernet frames

其中 HTTP GET 所对应的报文是序号为 10 的报文。

1. 我（包中）计算机的以太网地址为 **00:d0:59:a9:3d:68**。

10 17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686 IPv4
11 17.494766	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60 IPv4
12 17.498935	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514 IPv4
13 17.500025	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514 IPv4
14 17.500069	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54 IPv4
15 17.527057	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514 IPv4
16 17.527422	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489 IPv4
17 17.527457	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54 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
    > 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)
> Data (672 bytes)
```

2. 目的地址为 **00:06:25:da:af:73**，它不是 gaia.cs.umass.edu 的以太网地址，这个是我（包中）计算机用来获取子网的路由器地址。

10 17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686 IPv4
11 17.494766	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60 IPv4
12 17.498935	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514 IPv4
13 17.500025	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514 IPv4
14 17.500069	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54 IPv4
15 17.527057	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514 IPv4
16 17.527422	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489 IPv4
17 17.527457	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54 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:7
    > 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)
> Data (672 bytes)
```

3. Frame Type 字段的值为 **0x0800**，指示着上层协议为 **IPv4** 协议

```
10 17.466468    AmbitMic_a9:3d:68      LinksysG_da:af:73    0x0800    686 IPv4
11 17.494766    LinksysG_da:af:73      AmbitMic_a9:3d:68    0x0800     60 IPv4
12 17.498935    LinksysG_da:af:73      AmbitMic_a9:3d:68    0x0800   1514 IPv4
13 17.500025    LinksysG_da:af:73      AmbitMic_a9:3d:68    0x0800   1514 IPv4
14 17.500069    AmbitMic_a9:3d:68      LinksysG_da:af:73    0x0800     54 IPv4
15 17.527057    LinksysG_da:af:73      AmbitMic_a9:3d:68    0x0800   1514 IPv4
16 17.527422    LinksysG_da:af:73      AmbitMic_a9:3d:68    0x0800    489 IPv4
17 17.527457    AmbitMic_a9:3d:68      LinksysG_da:af:73    0x0800     54 IPv4
```

```
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
v Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:
   > 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)
> Data (672 bytes)
```

4. 在 "G" 出现之前有 **54** 个字节（即 "G" 出现在第 **55** 个字节）。可以视为有 14 字节的以太网帧字段，20 字节的 IP 首部和 20 字节的 TCP 首部。


```
10 17.466468    AmbitMic_a9:3d:68      LinksysG_da:af:73    0x0800    686
11 17.494766    LinksysG_da:af:73      AmbitMic_a9:3d:68    0x0800     60
12 17.498935    LinksysG_da:af:73      AmbitMic_a9:3d:68    0x0800   1514
13 17.500025    LinksysG_da:af:73      AmbitMic_a9:3d:68    0x0800   1514
14 17.500069    AmbitMic_a9:3d:68      LinksysG_da:af:73    0x0800     54
15 17.527057    LinksysG_da:af:73      AmbitMic_a9:3d:68    0x0800   1514
16 17.527422    LinksysG_da:af:73      AmbitMic_a9:3d:68    0x0800    489
17 17.527457    AmbitMic_a9:3d:68      LinksysG_da:af:73    0x0800     54
```

```
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Type: IPv4 (0x0800)
v Data (672 bytes)
    Data: 450002a000fa40008006bfc8c0a801698077f50c04220050651499a7aca53fb4
    [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 ba 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··
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
```

其中含有 HTTP 响应报文第一个字节所对应的报文是序号为 12 的报文。

5. 源以太网地址是 **00:06:25:da:af:73**，这个不是我（包中）计算机的地址也不是 gaia.cs.umass.edu 的以太网地址，这个是我（包中）计算机用来获取子网的路由器地址。这个是**路由器**的以太网地址。


```
12 17.498935    LinksysG_da:af:73      AmbitMic_a9:3d:68    0x0800
13 17.500025    LinksysG_da:af:73      AmbitMic_a9:3d:68    0x0800
<
> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12
v Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Ambi
   > 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)
```

6. 这个以太帧的目的地址是 **00:d0:59:a9:3d:68**，是我（包中）电脑的以太网地址。


```
12 17.498935    LinksysG_da:af:73      AmbitMic_a9:3d:68    0x0800
13 17.500025    LinksysG_da:af:73      AmbitMic_a9:3d:68    0x0800
<
> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (121
v Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Ambit
   > 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)
v Data (1500 bytes)
    Data: 456005dc8f2f4000370676f78077f50cc0a8016900500422aca53fb465
    [Length: 1500]
```

7. Frame Type 字段的值为 **0x0800**，指示着上层协议为 **IPv4** 协议

8. 在 "O" 出现之前有 **67** 个字节（即 "O" 出现在第 **68** 个字节）。可以视为有 14 字节的以太网帧字段，20 字节的 IP 首部，20 字节的 TCP 首部和 13 个字节的 HTTP 的状态行，包括：版本字段（8 个字节），状态码（3 个字节）和两个空格（2 个字节）。

2. The Address Resolution Protocol

ARP Caching

9. ARP 缓存中有 3 列。Internet 地址表示的是 IP 地址，物理地址表示的是以太网 MAC 地址，类型表示的是 IP 地址是动态的还是静态的。

Observing ARP in action

10. ARP 请求报文的源地址是 **00:d0:59:a9:3d:68**，目标地址是 **ff:ff:ff:ff:ff:ff**。它们分别是我（包中）计算机的以太网地址和广播地址。

```
> 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. Frame Type 字段的值为 **0x0806**，指示着上层协议为 **ARP** 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 (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. ○ ARP *opcode* 字段前面共有 20 个字节（即它从第 21 个字节开始）。因为在 ARP 帧中它前面有 6 个字节，以及还有 14 个字节的以太网帧字段。

   ○ ARP *opcode* 字段的值为 **1** (request)

```
> 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: Broad
   > 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)
     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
```

   ○ 有，在这里显示出发送者的 IP 地址为 192.168.1.105

```
> 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: Broad
   > 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)
     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
```

   ○ "question" 出现在目的 MAC 地址 Target MAC address，它被设置为全 0 来向目的 IP 地址 192.168.1.1 请求查询。

```
> 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)
     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
```

13. APR 响应报文在序号为 2 的报文。

- ARP *opcode* 字段前面共有 **20** 个字节（即它从第 **21** 个字节开始）。因为在 ARP 帧中它前面有 6 个字节，以及还有 14 个字节的以太网帧字段。

- ARP *opcode* 字段的值为 **2** (reply)

```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
∨ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Ambit
    > 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: 000000000000000000000000000000000000
∨ 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)
```

- "answer" 出现在发送 MAC 地址 Sender MAC address，返回了之前请求 IP 地址 192.168.1.1 所对应的 MAC 地址 00:06:25:da:af:73。

```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
∨ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: Ambit
    > 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: 000000000000000000000000000000000000
∨ 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)
```

14. ARP 响应报文的源地址是 **00:06:25:da:af:73**，目标地址是 **00:d0:59:a9:3d:68**。它们分别是路由器的以太网地址和我（包中）计算机的以太网地址。

```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
∨ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_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: 000000000000000000000000000000000000
> Address Resolution Protocol (reply)
```

15. 因为 ARP 响应报文不会使用广播地址，而响应报文中的目的 IP 地址肯定是 192.168.1.104，与我（包中）计算机的 IP 地址 192.168.1.105 不匹配，同时响应报文是不会通过广播地址向子网内所有的主机都发送，因此我们不会接收到 ARP 响应报文。

```
   6 13.542974   CnetTech_73:8d:ce    Broadcast          ARP     60 Who has 192.168.1.117? Tell 192.168.1.104
   7 17.444423   AmbitMic_a9:3d:68    LinksysG_da:af:73  0x0800  62 IPv4
   8 17.465902   LinksysG_da:af:73    AmbitMic_a9:3d:68  0x0800  62 IPv4
   9 17.465927   AmbitMic_a9:3d:68    LinksysG_da:af:73  0x0800  54 IPv4
<
∨ Ethernet II, Src: CnetTech_73:8d:ce (00:80:ad:73:8d:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    > Source: CnetTech_73:8d:ce (00:80:ad:73:8d:ce)
      Type: ARP (0x0806)
      Padding: 000000000000000000000000000000000000
∨ Address Resolution Protocol (request)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: request (1)
      Sender MAC address: CnetTech_73:8d:ce (00:80:ad:73:8d:ce)
      Sender IP address: 192.168.1.104
      Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
      Target IP address: 192.168.1.117
```