Wireshark Lab: Ethernet and ARP v7.0

实验步骤：

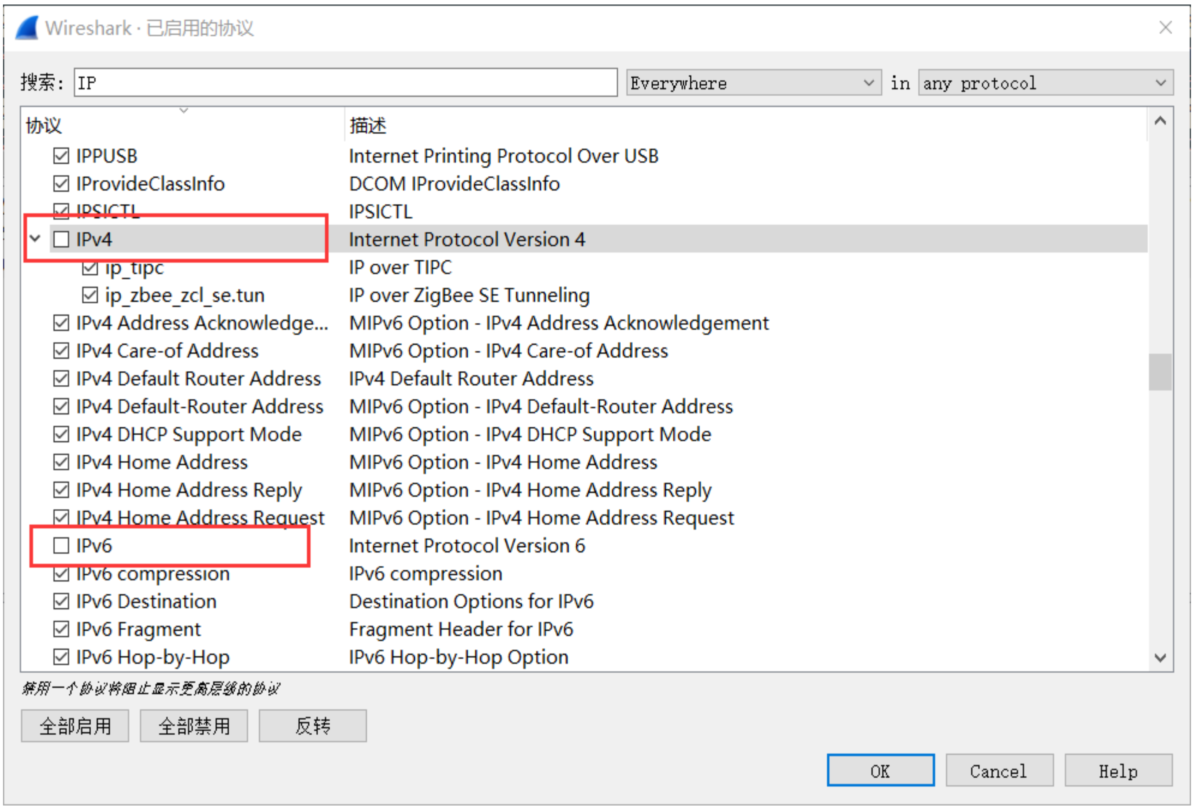
1.清空浏览器的cache

2.开始抓包

3.进入http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html

4.停止抓包

5.由于不关心IP和更高层的协议，故点击 分析-->启用的协议，取消选中IP框再选择OK



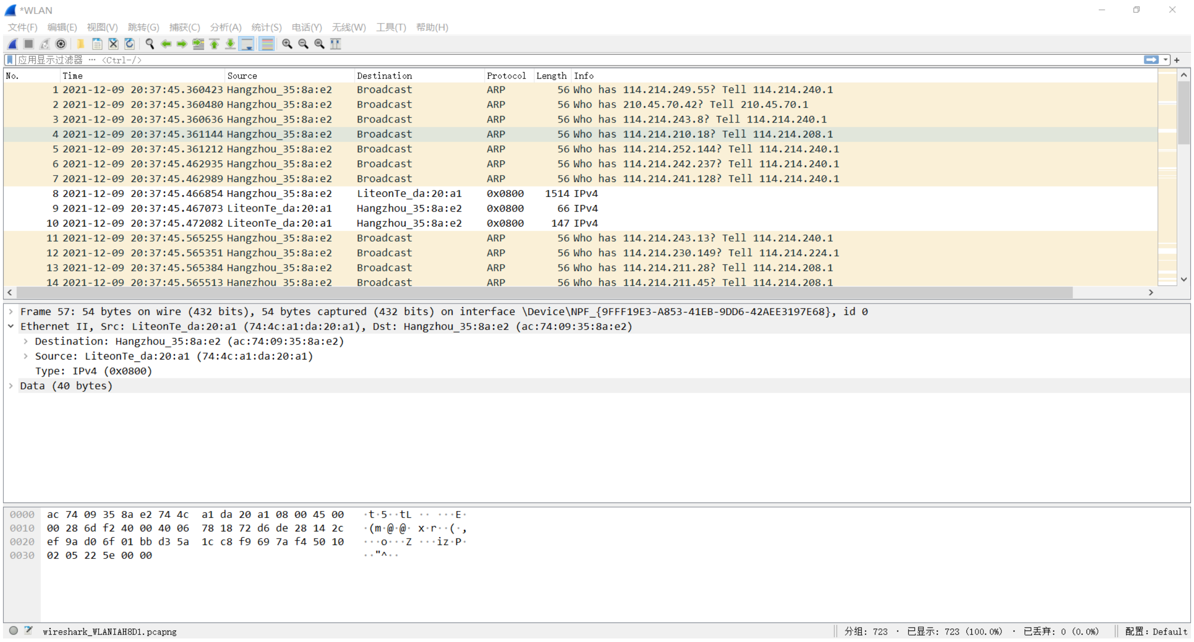
Wireshark · 已启用的协议

搜索： IP   Everywhere   in   any protocol

协议	描述
☑ IPPUSB	Internet Printing Protocol Over USB
☑ IProvideClassInfo	DCOM IProvideClassInfo
☑ IPSICTL	IPSICTL
☐ IPv4	Internet Protocol Version 4
☑ ip_tipc	IP over TIPC
☑ ip_zbee_zcl_se.tun	IP over ZigBee SE Tunneling
☑ 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
☑ IPv6 Hop-by-Hop	IPv6 Hop-by-Hop Option

禁用一个协议将阻止显示更高层级的协议

得到的页面如下：


*WLAN
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
      1 2021-12-09 20:37:45.360423 Hangzhou_35:8a:e2  Broadcast          ARP        56 Who has 114.214.249.55? Tell 114.214.240.1
      2 2021-12-09 20:37:45.360480 Hangzhou_35:8a:e2  Broadcast          ARP        56 Who has 210.45.70.42? Tell 210.45.70.1
      3 2021-12-09 20:37:45.360636 Hangzhou_35:8a:e2  Broadcast          ARP        56 Who has 114.214.243.8? Tell 114.214.240.1
      4 2021-12-09 20:37:45.361144 Hangzhou_35:8a:e2  Broadcast          ARP        56 Who has 114.214.210.18? Tell 114.214.208.1
      5 2021-12-09 20:37:45.361212 Hangzhou_35:8a:e2  Broadcast          ARP        56 Who has 114.214.252.144? Tell 114.214.240.1
      6 2021-12-09 20:37:45.462935 Hangzhou_35:8a:e2  Broadcast          ARP        56 Who has 114.214.242.237? Tell 114.214.240.1
      7 2021-12-09 20:37:45.462989 Hangzhou_35:8a:e2  Broadcast          ARP        56 Who has 114.214.241.128? Tell 114.214.240.1
      8 2021-12-09 20:37:45.466854 Hangzhou_35:8a:e2  LiteonTe_da:20:a1  0x0800   1514 IPv4
      9 2021-12-09 20:37:45.467073 LiteonTe_da:20:a1  Hangzhou_35:8a:e2  0x0800     66 IPv4
     10 2021-12-09 20:37:45.472082 LiteonTe_da:20:a1  Hangzhou_35:8a:e2  0x0800    147 IPv4
     11 2021-12-09 20:37:45.565255 Hangzhou_35:8a:e2  Broadcast          ARP        56 Who has 114.214.243.13? Tell 114.214.240.1
     12 2021-12-09 20:37:45.565351 Hangzhou_35:8a:e2  Broadcast          ARP        56 Who has 114.214.230.149? Tell 114.214.224.1
     13 2021-12-09 20:37:45.565384 Hangzhou_35:8a:e2  Broadcast          ARP        56 Who has 114.214.211.28? Tell 114.214.208.1
     14 2021-12-09 20:37:45.565513 Hangzhou_35:8a:e2  Broadcast          ARP        56 Who has 114.214.211.45? Tell 114.214.208.1
```

```
> Frame 57: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{9FFF19E3-A853-41EB-9DD6-42AEE3197E68}, id 0
v Ethernet II, Src: LiteonTe_da:20:a1 (74:4c:a1:da:20:a1), Dst: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
  > Destination: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2)
  > Source: LiteonTe_da:20:a1 (74:4c:a1:da:20:a1)
    Type: IPv4 (0x0800)
> Data (40 bytes)
```

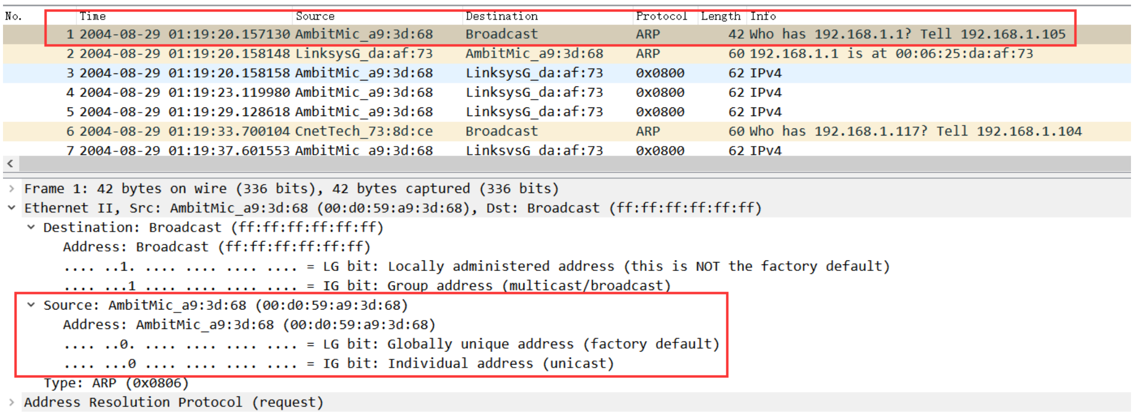
```
0000  ac 74 09 35 8a e2 74 4c  a1 da 20 a1 08 00 45 00   ·t·5··tL ·· ···E·
0010  00 28 6d f2 40 00 40 06  78 18 72 d6 de 28 14 2c   ·(m·@·@· x·r··(·,
0020  ef 9a d0 6f 01 bb d3 5a  1c c8 f9 69 7a f4 50 10   ···o···Z ···iz·P·
0030  02 05 22 5e 00 00                                  ··"^··
```

wireshark_WLANIAH8D1.pcapng　分组：723 · 已显示：723 (100.0%) · 已丢弃：0 (0.0%)　配置：Default

以下用的是作者抓的包

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

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

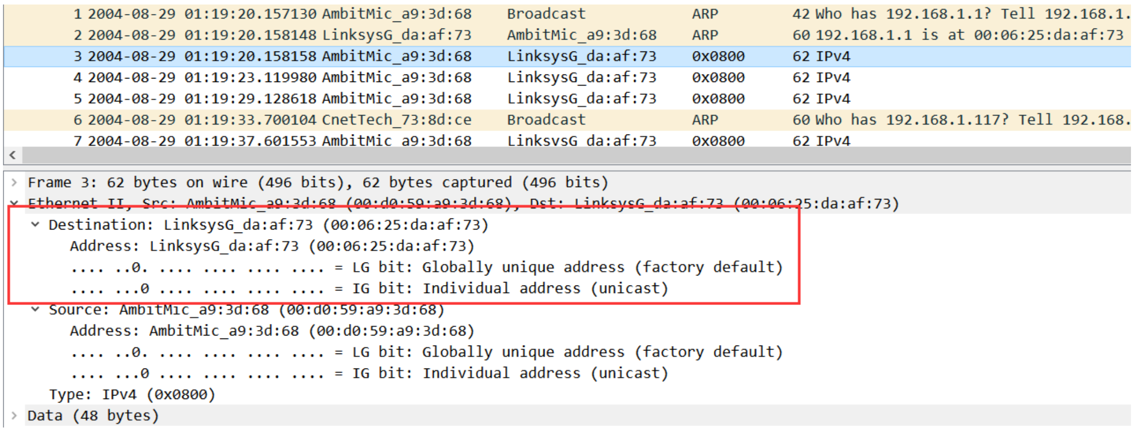


```
No.     Time                       Source              Destination        Protocol Length Info
      1 2004-08-29 01:19:20.157130 AmbitMic_a9:3d:68   Broadcast          ARP        42 Who has 192.168.1.1? Tell 192.168.1.105
      2 2004-08-29 01:19:20.158148 LinksysG_da:af:73   AmbitMic_a9:3d:68  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:68   LinksysG_da:af:73  0x0800     62 IPv4
      4 2004-08-29 01:19:23.119980 AmbitMic_a9:3d:68   LinksysG_da:af:73  0x0800     62 IPv4
      5 2004-08-29 01:19:29.128618 AmbitMic_a9:3d:68   LinksysG_da:af:73  0x0800     62 IPv4
      6 2004-08-29 01:19:33.700104 CnetTech_73:8d:ce   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:68   LinksysG_da:af:73  0x0800     62 IPv4
```

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
v Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v 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)
> Address Resolution Protocol (request)
```

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.]**

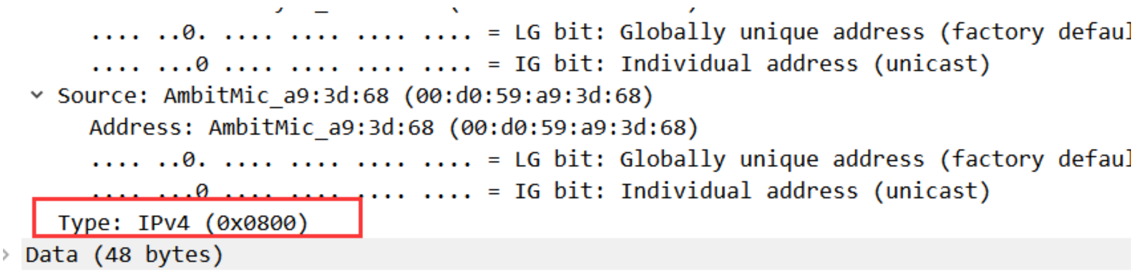
   00:06:25:da:af:73，不是，这可能是连接该子网的路由器的IP地址。



```
1 2004-08-29 01:19:20.157130 AmbitMic_a9:3d:68    Broadcast          ARP      42 Who has 192.168.1.1? Tell 192.168.1.
2 2004-08-29 01:19:20.158148 LinksysG_da:af:73    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:68    LinksysG_da:af:73  0x0800   62 IPv4
4 2004-08-29 01:19:23.119980 AmbitMic_a9:3d:68    LinksysG_da:af:73  0x0800   62 IPv4
5 2004-08-29 01:19:29.128618 AmbitMic_a9:3d:68    LinksysG_da:af:73  0x0800   62 IPv4
6 2004-08-29 01:19:33.700104 CnetTech_73:8d:ce    Broadcast          ARP      60 Who has 192.168.1.117? Tell 192.168.
7 2004-08-29 01:19:37.601553 AmbitMic_a9:3d:68    LinksysG_da:af:73  0x0800   62 IPv4

> Frame 3: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
v Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
  v 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)
  v 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 (48 bytes)
```

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

   0x0800，IPv4



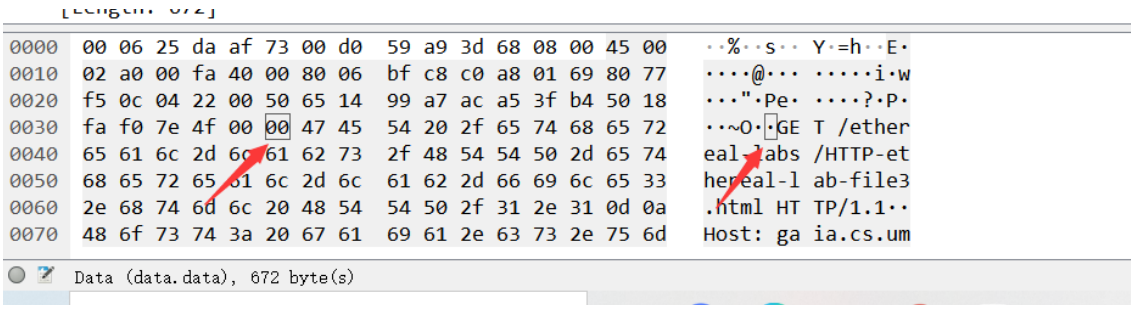
```
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defaul
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory defaul
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Data (48 bytes)
```

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

   图中每两个十六进制字符表示8比特，即一个字节，故

   不包括GE : 3*16+6=54 byte

   包括GE : 3*16+7=55 byte

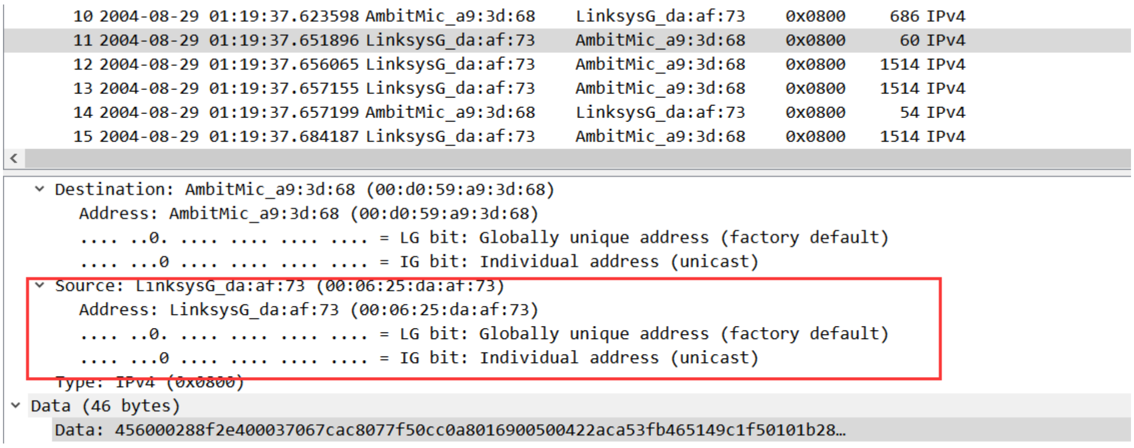


```
    [Length: 672]
0000  00 06 25 da af 73 00 d0  59 a9 3d 68 08 00 45 00   ··%··s·· Y·=h··E·
0010  02 a0 00 fa 40 00 80 06  bf c8 c0 a8 01 69 80 77   ····@··· ·····i·w
0020  f5 0c 04 22 00 50 65 14  99 a7 ac a5 3f b4 50 18   ···"·Pe· ····?·P·
0030  fa f0 7e 4f 00 00 47 45  54 20 2f 65 74 68 65 72   ··~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

Data (data.data), 672 byte(s)
```

Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

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?**

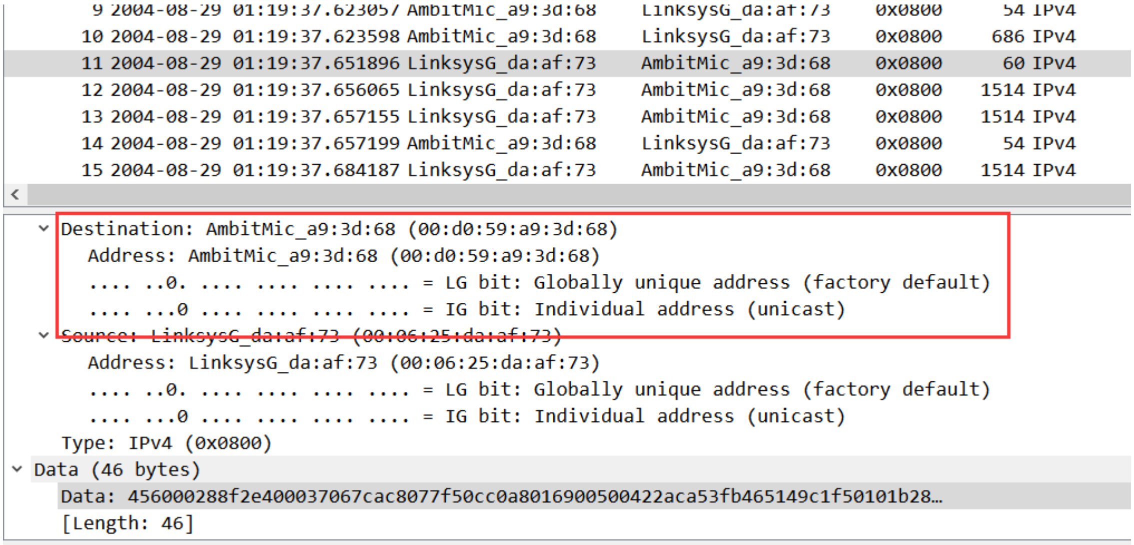
   00:06:25:da:af:73，不是，这是连接此子网的路由器的IP地址。



```
10 2004-08-29 01:19:37.623598 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800    686 IPv4
11 2004-08-29 01:19:37.651896 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800     60 IPv4
12 2004-08-29 01:19:37.656065 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800   1514 IPv4
13 2004-08-29 01:19:37.657155 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800   1514 IPv4
14 2004-08-29 01:19:37.657199 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800     54 IPv4
15 2004-08-29 01:19:37.684187 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800   1514 IPv4

  ˅ 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)
˅ Data (46 bytes)
    Data: 456000288f2e400037067cac8077f50cc0a8016900500422aca53fb465149c1f50101b28…
```

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

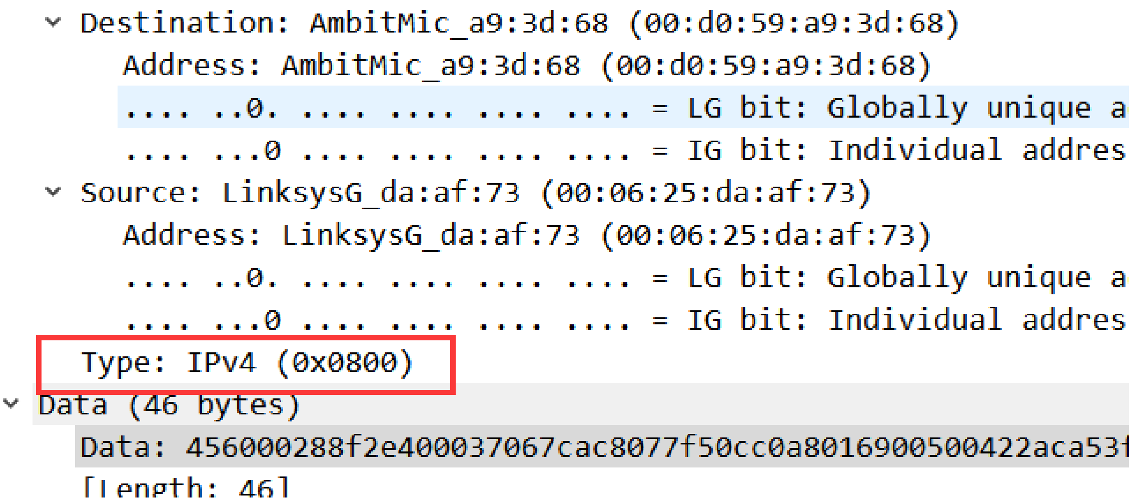
00:d0:59:a9:3d:68，是作者计算机的MAC地址。



```
 9 2004-08-29 01:19:37.623057 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800     54 IPv4
10 2004-08-29 01:19:37.623598 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800    686 IPv4
11 2004-08-29 01:19:37.651896 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800     60 IPv4
12 2004-08-29 01:19:37.656065 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800   1514 IPv4
13 2004-08-29 01:19:37.657155 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800   1514 IPv4
14 2004-08-29 01:19:37.657199 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800     54 IPv4
15 2004-08-29 01:19:37.684187 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800   1514 IPv4

  ˅ 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)
˅ Data (46 bytes)
    Data: 456000288f2e400037067cac8077f50cc0a8016900500422aca53fb465149c1f50101b28…
    [Length: 46]
```

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

0x0800，IPv4

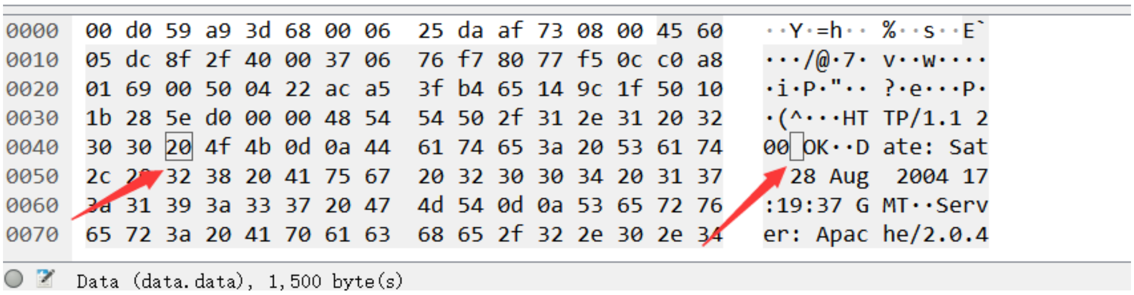


```
  ˅ Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique a
      .... ...0 .... .... .... .... = IG bit: Individual addres
  ˅ Source: LinksysG_da:af:73 (00:06:25:da:af:73)
      Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique a
      .... ...0 .... .... .... .... = IG bit: Individual addres
    Type: IPv4 (0x0800)
˅ Data (46 bytes)
    Data: 456000288f2e400037067cac8077f50cc0a8016900500422aca53f
    [Length: 46]
```

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?**

不包括OK : 4*16+3=67 byte

包括OK : 4*16+4=68 byte



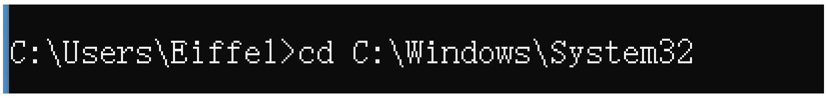
```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 00 45 60   ··Y·=h·· %··s··E`
0010  05 dc 8f 2f 40 00 37 06  76 f7 80 77 f5 0c c0 a8   ···/@·7· v··w····
0020  01 69 00 50 04 22 ac a5  3f b4 65 14 9c 1f 50 10   ·i·P·"·· ?·e···P·
0030  1b 28 5e d0 00 00 48 54  54 50 2f 31 2e 31 20 32   ·(^···HT TP/1.1 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
```

Data (data.data), 1,500 byte(s)

The Address Resolution Protocol

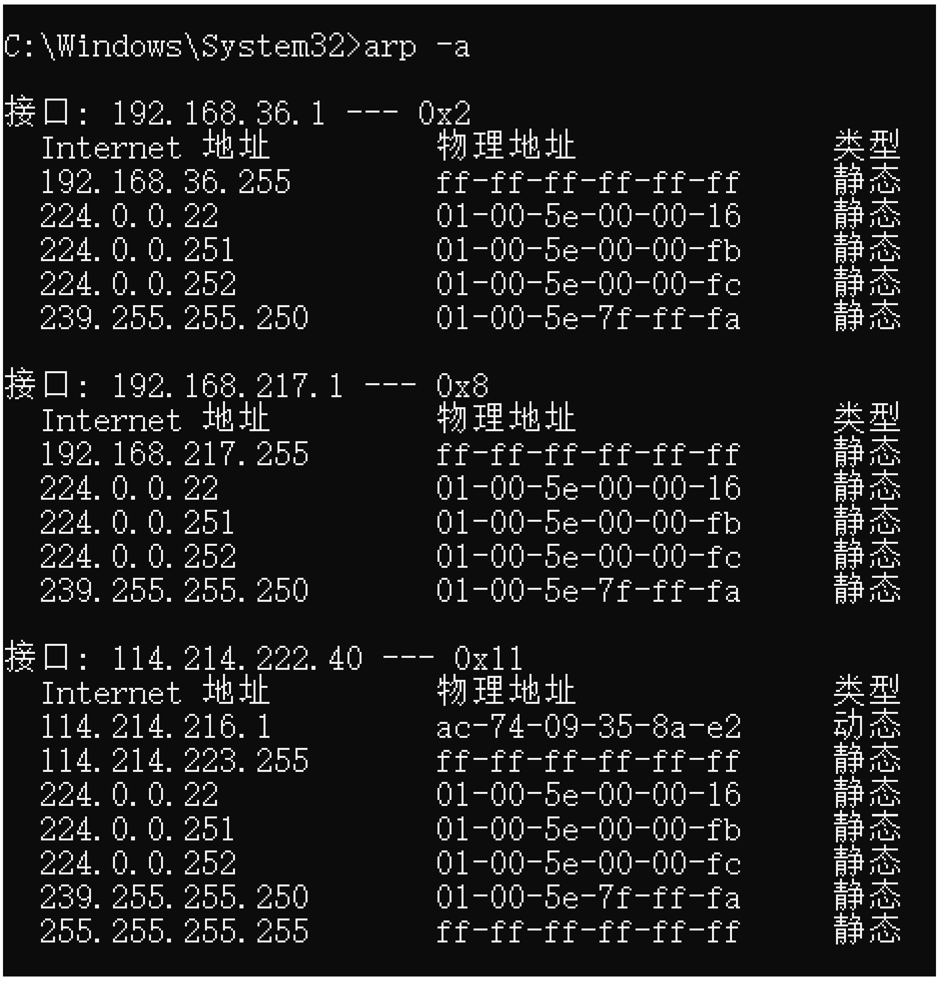
实验步骤

1.进入目录C:\Windows\System32



```
C:\Users\Eiffel>cd C:\Windows\System32
```

2.输入 arp -a



```
C:\Windows\System32>arp -a

接口: 192.168.36.1 --- 0x2
  Internet 地址         物理地址              类型
  192.168.36.255        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

接口: 192.168.217.1 --- 0x8
  Internet 地址         物理地址              类型
  192.168.217.255       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

接口: 114.214.222.40 --- 0x11
  Internet 地址         物理地址              类型
  114.214.216.1         ac-74-09-35-8a-e2     动态
  114.214.223.255       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
```

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

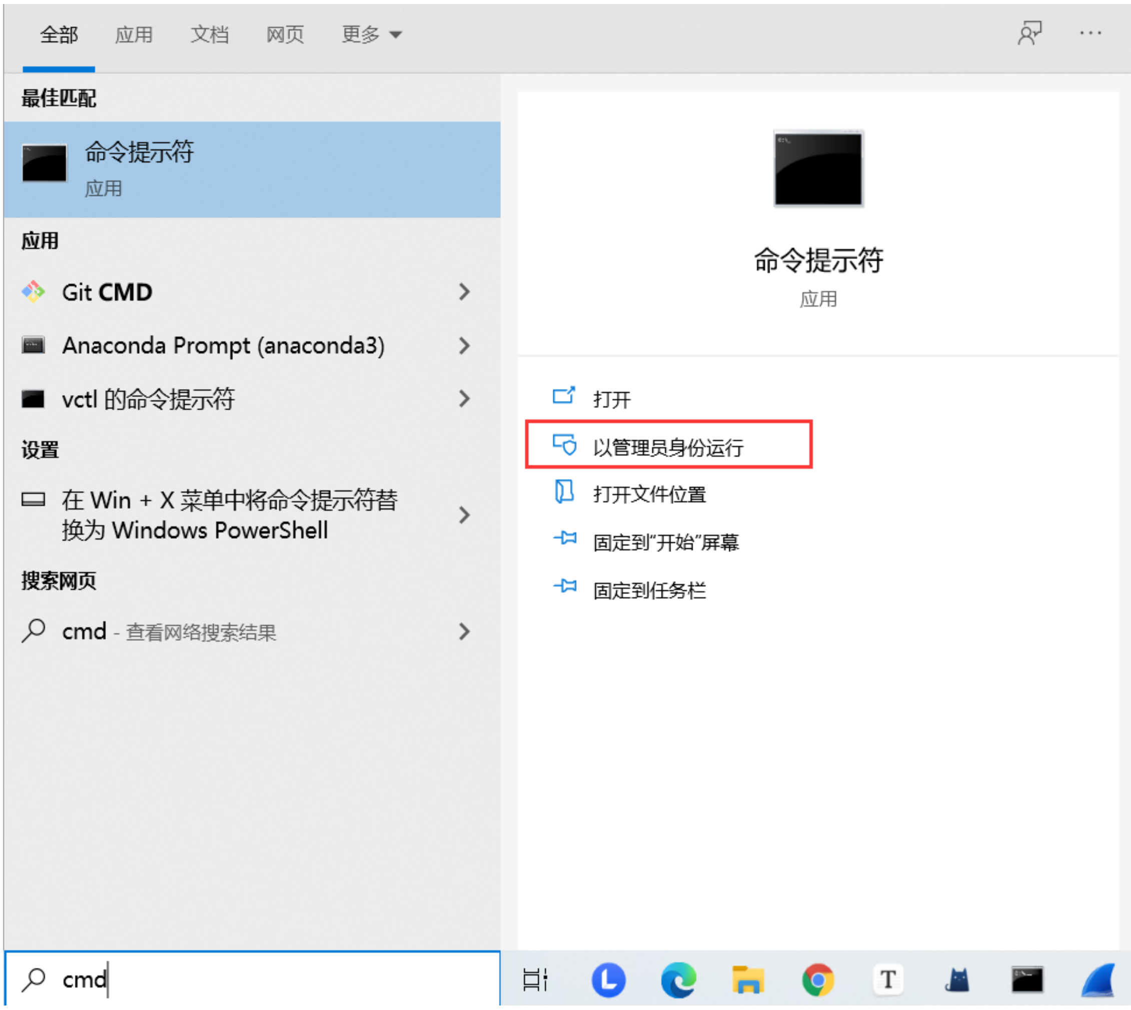
   从第一列到第三列依次是 IP地址、MAC地址、类型。

Observing ARP in action

实验步骤:

1.进入目录C:\Windows\System32，用命令`arp -d *`清空ARP cache

清空cache时，遇到了"ARP项目删除失败：请求的操作需要提升"，此时解决方法是，在电脑搜索框中搜索cmd，选择以管理员身份运行即可。



2.清空浏览器的缓存。

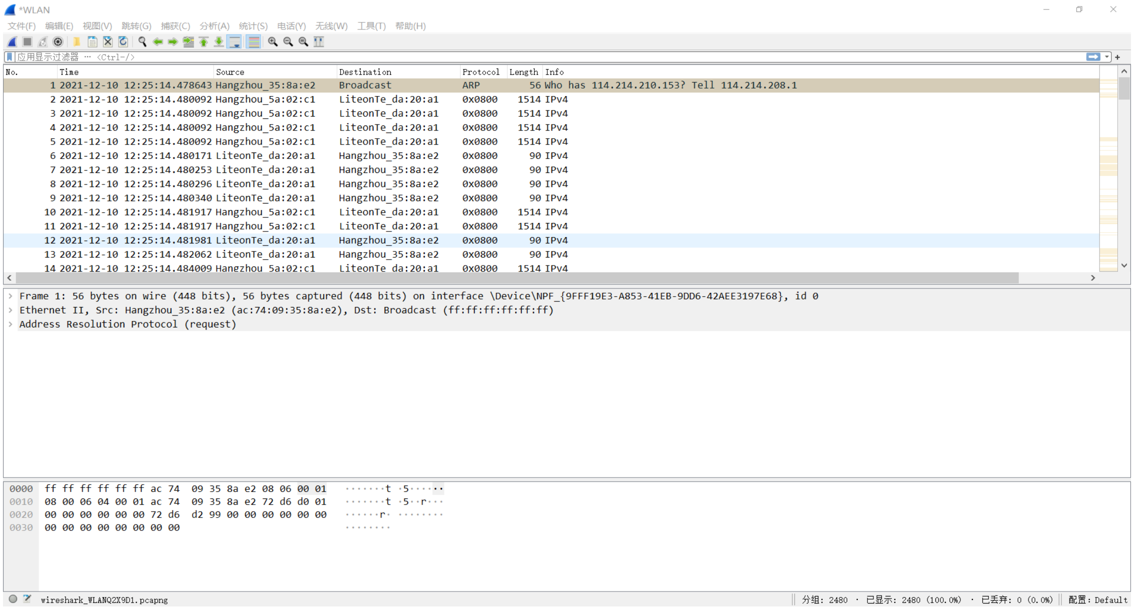
3.开始抓包

4.进入http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html

5.停止抓包

6.由于不关心IP和更高层的协议，故点击 分析-->启用的协议，取消选中IP框再选择OK

抓到的包的页面如下:



*WLAN

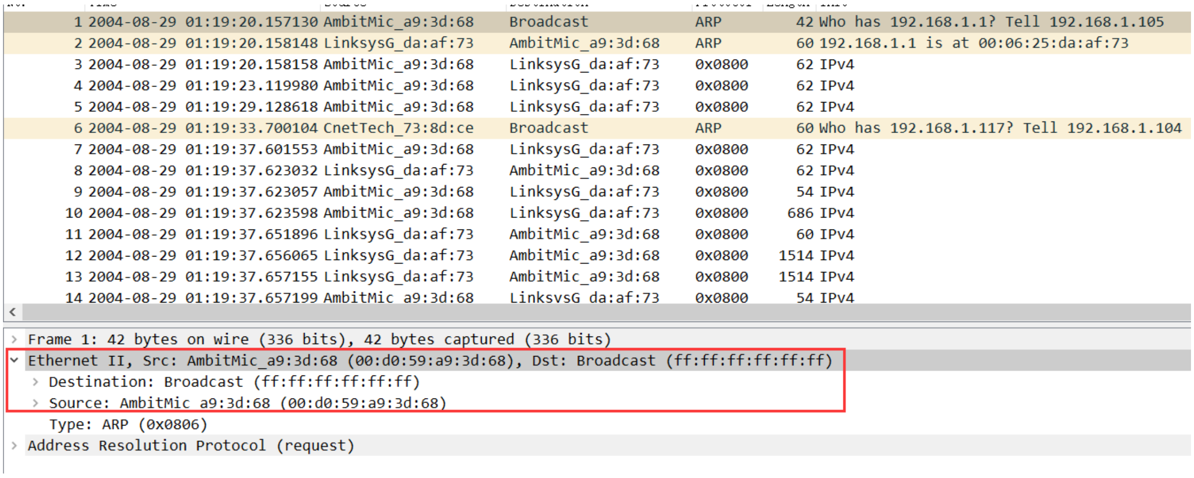
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.   Time                       Source              Destination         Protocol Length Info
    1 2021-12-10 12:25:14.478643 Hangzhou_35:8a:e2   Broadcast           ARP        56 Who has 114.214.210.153? Tell 114.214.208.1
    2 2021-12-10 12:25:14.480092 Hangzhou_5a:02:c1   LiteonTe_da:20:a1   0x0800   1514 IPv4
    3 2021-12-10 12:25:14.480092 Hangzhou_5a:02:c1   LiteonTe_da:20:a1   0x0800   1514 IPv4
    4 2021-12-10 12:25:14.480092 Hangzhou_5a:02:c1   LiteonTe_da:20:a1   0x0800   1514 IPv4
    5 2021-12-10 12:25:14.480092 Hangzhou_5a:02:c1   LiteonTe_da:20:a1   0x0800   1514 IPv4
    6 2021-12-10 12:25:14.480171 LiteonTe_da:20:a1   Hangzhou_35:8a:e2   0x0800     90 IPv4
    7 2021-12-10 12:25:14.480253 LiteonTe_da:20:a1   Hangzhou_35:8a:e2   0x0800     90 IPv4
    8 2021-12-10 12:25:14.480296 LiteonTe_da:20:a1   Hangzhou_35:8a:e2   0x0800     90 IPv4
    9 2021-12-10 12:25:14.480340 LiteonTe_da:20:a1   Hangzhou_35:8a:e2   0x0800     90 IPv4
   10 2021-12-10 12:25:14.481917 Hangzhou_5a:02:c1   LiteonTe_da:20:a1   0x0800   1514 IPv4
   11 2021-12-10 12:25:14.481917 Hangzhou_5a:02:c1   LiteonTe_da:20:a1   0x0800   1514 IPv4
   12 2021-12-10 12:25:14.481981 LiteonTe_da:20:a1   Hangzhou_35:8a:e2   0x0800     90 IPv4
   13 2021-12-10 12:25:14.482062 LiteonTe_da:20:a1   Hangzhou_35:8a:e2   0x0800     90 IPv4
   14 2021-12-10 12:25:14.484009 Hangzhou_5a:02:c1   LiteonTe_da:20:a1   0x0800   1514 IPv4

> Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{9FFF19E3-A853-41EB-9DD6-42AEE3197E68}, id 0
> Ethernet II, Src: Hangzhou_35:8a:e2 (ac:74:09:35:8a:e2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)

0000  ff ff ff ff ff ff ac 74  09 35 8a e2 08 06 00 01   ·······t ·5······
0010  08 00 06 04 00 01 ac 74  09 35 8a e2 72 d6 d0 01   ·······t ·5··r···
0020  00 00 00 00 00 00 72 d6  d2 99 00 00 00 00 00 00   ······r· ········
0030  00 00 00 00 00 00 00 00                            ········

wireshark_WLANQ2X9D1.pcapng    分组: 2480 · 已显示: 2480 (100.0%) · 已丢弃: 0 (0.0%)  配置: Default
```

以下用作者抓到的包进行回答：

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

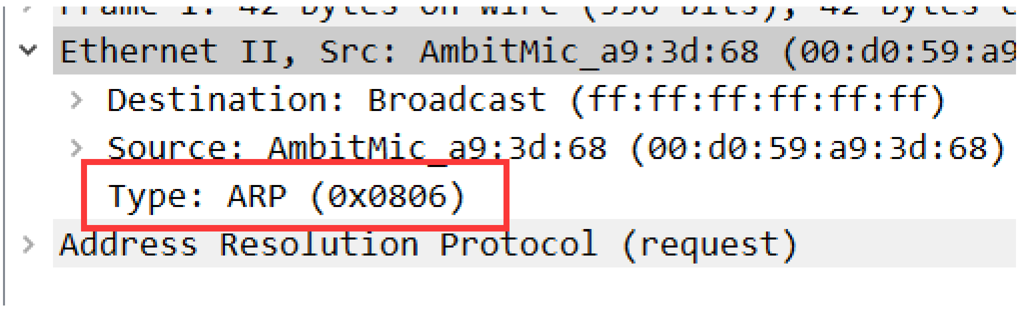
src : 00:d0:59:a9:3d:68   dst : ff : ff : ff : ff : ff : ff



```
    1 2004-08-29 01:19:20.157130 AmbitMic_a9:3d:68 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:73 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:68 LinksysG_da:af:73 0x0800   62 IPv4
    4 2004-08-29 01:19:23.119980 AmbitMic_a9:3d:68 LinksysG_da:af:73 0x0800   62 IPv4
    5 2004-08-29 01:19:29.128618 AmbitMic_a9:3d:68 LinksysG_da:af:73 0x0800   62 IPv4
    6 2004-08-29 01:19:33.700104 CnetTech_73:8d:ce 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:68 LinksysG_da:af:73 0x0800   62 IPv4
    8 2004-08-29 01:19:37.623032 LinksysG_da:af:73 AmbitMic_a9:3d:68 0x0800   62 IPv4
    9 2004-08-29 01:19:37.623057 AmbitMic_a9:3d:68 LinksysG_da:af:73 0x0800   54 IPv4
   10 2004-08-29 01:19:37.623598 AmbitMic_a9:3d:68 LinksysG_da:af:73 0x0800  686 IPv4
   11 2004-08-29 01:19:37.651896 LinksysG_da:af:73 AmbitMic_a9:3d:68 0x0800   60 IPv4
   12 2004-08-29 01:19:37.656065 LinksysG_da:af:73 AmbitMic_a9:3d:68 0x0800 1514 IPv4
   13 2004-08-29 01:19:37.657155 LinksysG_da:af:73 AmbitMic_a9:3d:68 0x0800 1514 IPv4
   14 2004-08-29 01:19:37.657199 AmbitMic_a9:3d:68 LinksysG_da:af:73 0x0800   54 IPv4

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
v 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?**

0x0806，ARP



```
v Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9
  > 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)
```

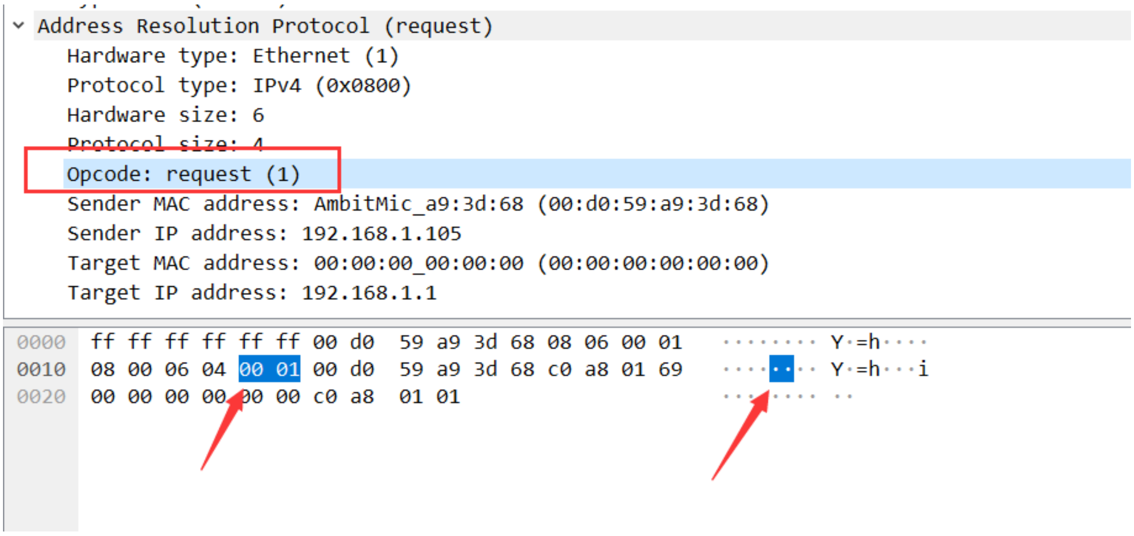
实验步骤和之前的类似，只不过进入的网站不同

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?

不包括Opcode : 16+4=20 byte

包括Opcode : 16+6=22 byte



```
∨ 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
```

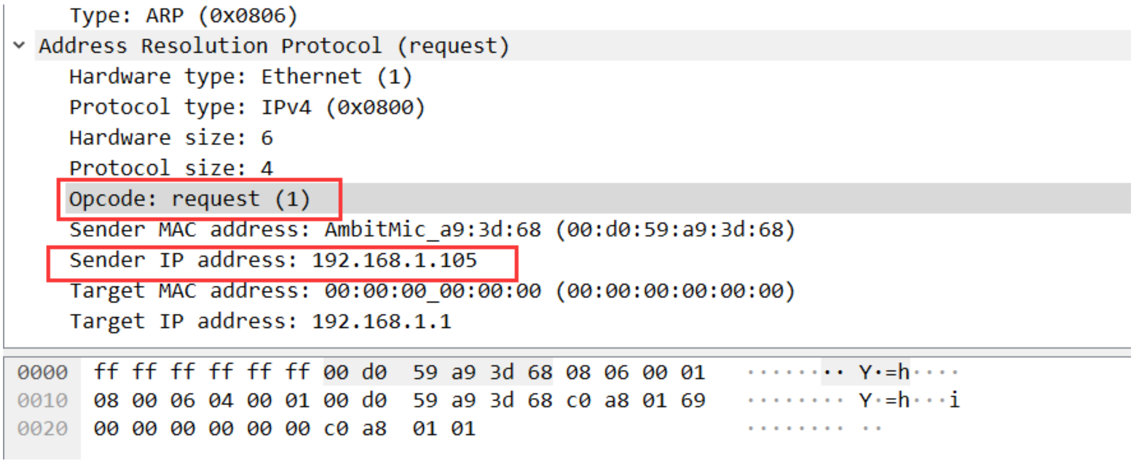
```
0000  ff ff ff ff ff ff 00 d0  59 a9 3d 68 08 06 00 01   ········ Y·=h····
0010  08 00 06 04 00 01 00 d0  59 a9 3d 68 c0 a8 01 69   ········ Y·=h···i
0020  00 00 00 00 00 00 c0 a8  01 01                     ········ ··
```

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?

由上面的图可知，opcode的值为0x0001

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

包含了，sender IP addr : 192.168.1.105



```
    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
```

```
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                     ········ ··
```

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

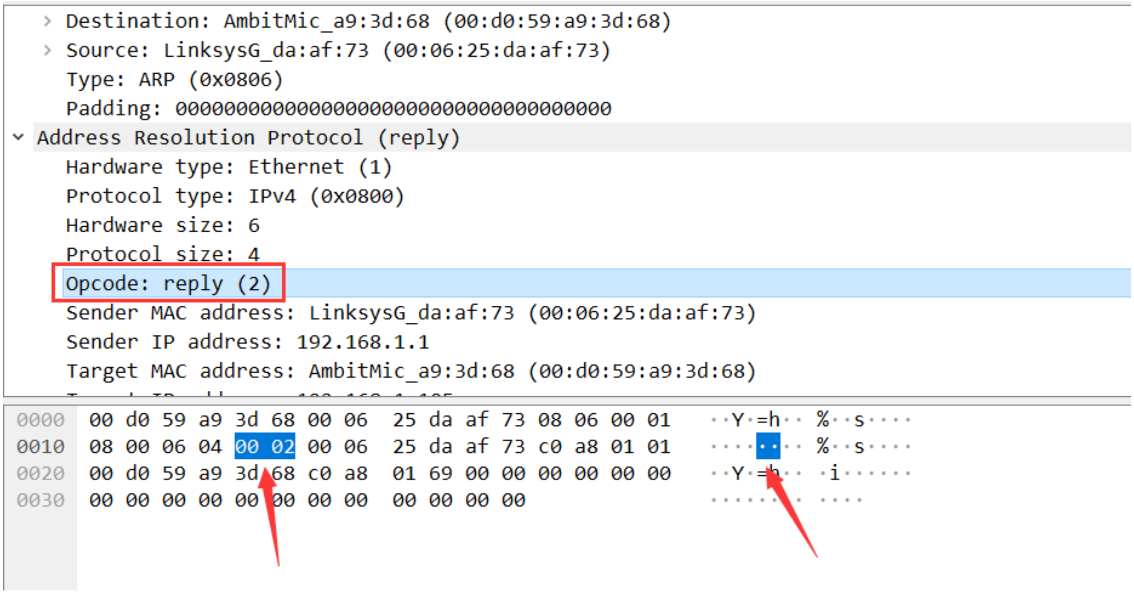
由上图可得，opcode的值为1，表示为request

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?

不包括Opcode : 16+4=20 byte

包括Opcode : 16+6=22 byte



```
  > 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
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)

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               ········ ····
```

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?

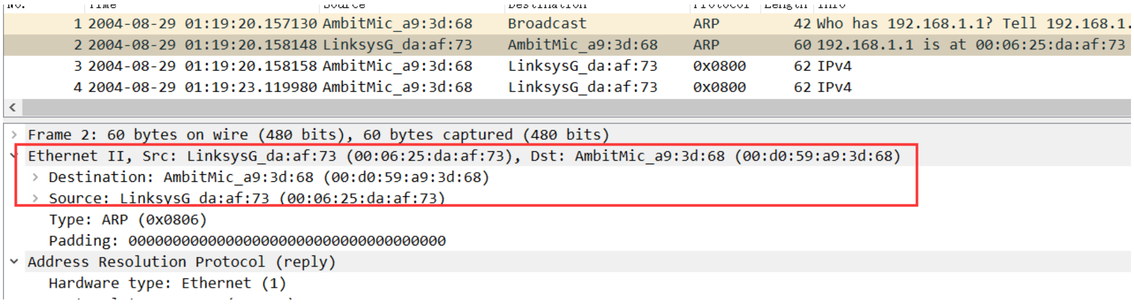
由上图可得，opcode的值为0x0002

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的值为2，表示reply

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

src : 00:06:25:da:af:73   dst : 00:d0:59:a9:3d:68



```
No.   Time                       Source              Destination         Protocol  Length Info
    1 2004-08-29 01:19:20.157130 AmbitMic_a9:3d:68   Broadcast           ARP           42 Who has 192.168.1.1? Tell 192.168.1.
    2 2004-08-29 01:19:20.158148 LinksysG_da:af:73   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:68   LinksysG_da:af:73   0x0800        62 IPv4
    4 2004-08-29 01:19:23.119980 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800        62 IPv4

> 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: 000000000000000000000000000000000000
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
```

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

因为查询ARP报文是在广播帧发送的，此子网的所有节点都能收到，而响应ARP在一个标准帧中发送，只有请求ARP的那个节点才能收到。

Extra Credit

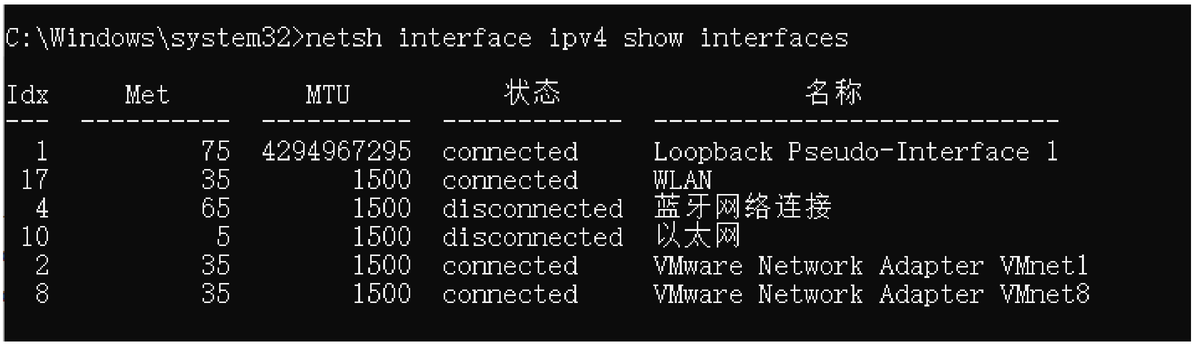
EX-1. The arp command: arp -s InetAddr EtherAddr allows you to manually add an entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

这样会使自己的电脑和那个IP地址对应的节点建立不了连接

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.

30000毫秒

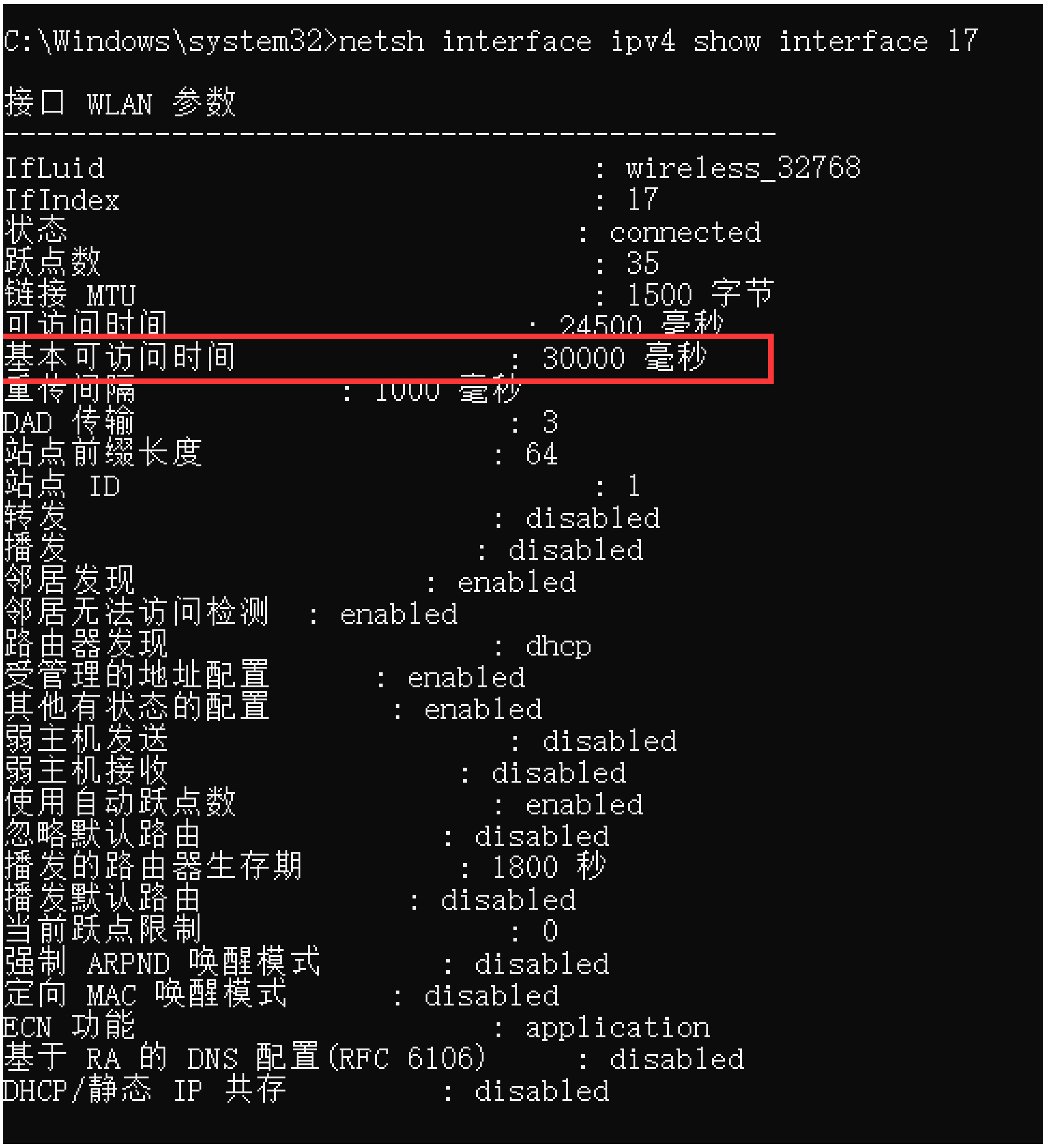
在终端中，先输入`netsh interface ipv4 show interfaces`得到系统网络接口的信息：



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

Idx     Met         MTU          状态                名称
---  ----------  ----------  ------------  ---------------------------
  1          75  4294967295  connected     Loopback Pseudo-Interface 1
 17          35        1500  connected     WLAN
  4          65        1500  disconnected  蓝牙网络连接
 10           5        1500  disconnected  以太网
  2          35        1500  connected     VMware Network Adapter VMnet1
  8          35        1500  connected     VMware Network Adapter VMnet8
```

由图可得Idx为17所对应的是WLAN

再输入`netsh interface ipv4 show interface 17`得到Idx为17所对应的接口的信息，由图可得，基本可访问时间为30000毫秒，故ARP cache条目的TTL为30000



```
C:\Windows\system32>netsh interface ipv4 show interface 17

接口 WLAN 参数
----------------------------------------------
IfLuid                             : wireless_32768
IfIndex                            : 17
状态                               : connected
跃点数                             : 35
链接 MTU                           : 1500 字节
可访问时间                         : 24500 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
```