ARP实验

Q1

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

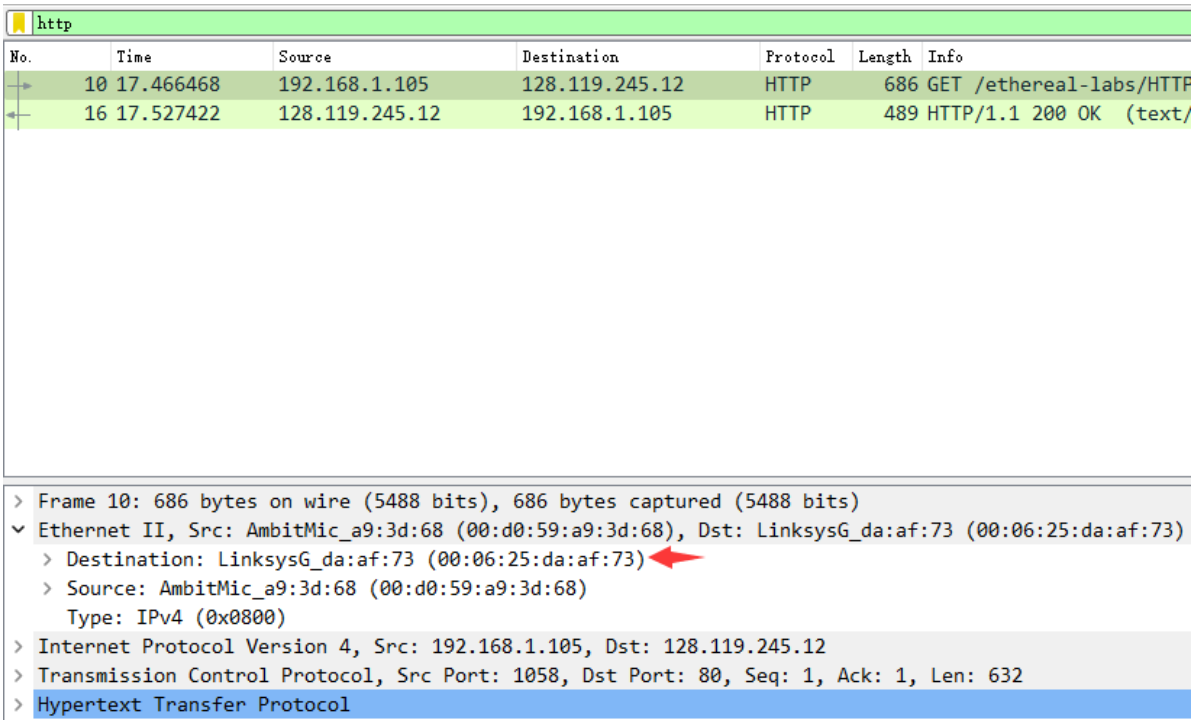
No.	Time	Source	Destination	Protocol	Length	Info
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-e
16	17.527422	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1 200 OK (text/ht

```
> 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: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
```

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

Q2

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.]



目的地址: LinksysG_da:af:73 (00:06:25:da:af:73)

不是gaia.cs.umass.edu的以太网地址

是出子网的路由器接口的地址

Q3

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

No.	Time	Source	Destination	Protocol	Length	Info
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-
16	17.527422	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1 200 OK (text/

```
> 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: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
```

0x0800

表示上层协议是 IPv4

Q4

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

```
> 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: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
```

```
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
```

G对应47，之前一共3*16+6=54字节，算上G出现是55字节

Q5

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?

No.	Time	Source	Destination	Protocol	Length	Info
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-et
16	17.527422	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1 200 OK (text/htm

```
> Frame 16: 489 bytes on wire (3912 bits), 489 bytes captured (3912 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: 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: 4381, Ack: 633, Len: 435
> [4 Reassembled TCP Segments (4815 bytes): #12(1460), #13(1460), #15(1460), #16(435)]
> Hypertext Transfer Protocol
```

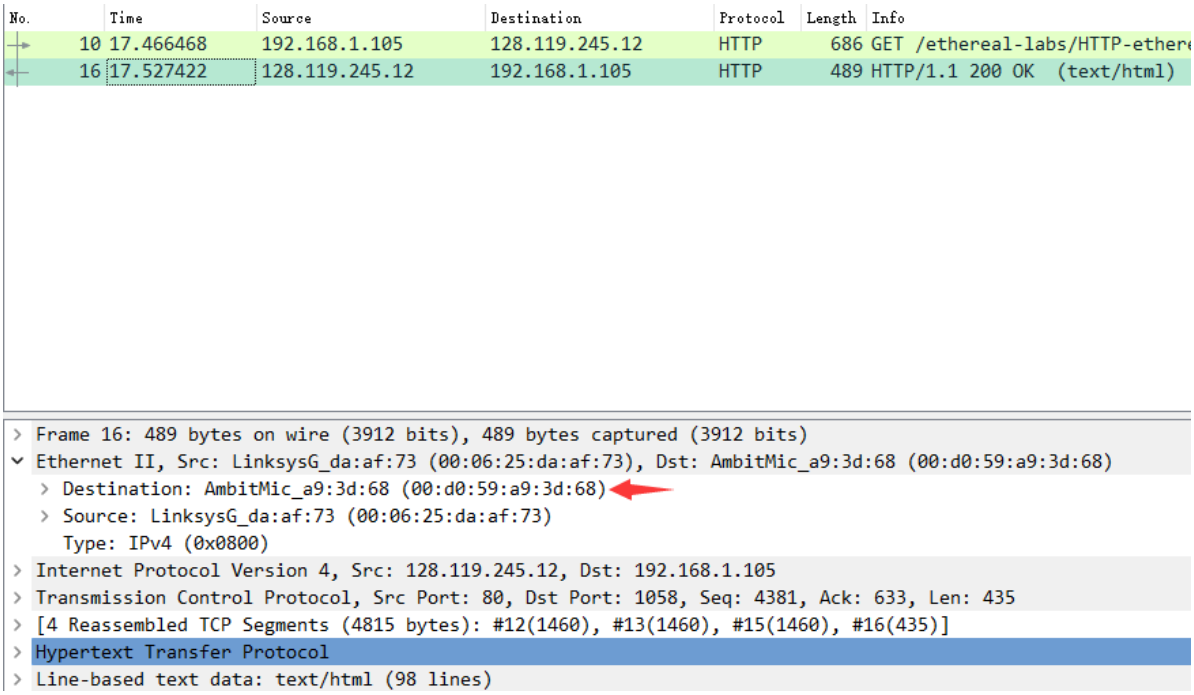
源地址：LinksysG_da:af:73 (00:06:25:da:af:73)

不是

是出子网的路由器的接口地址

Q6

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

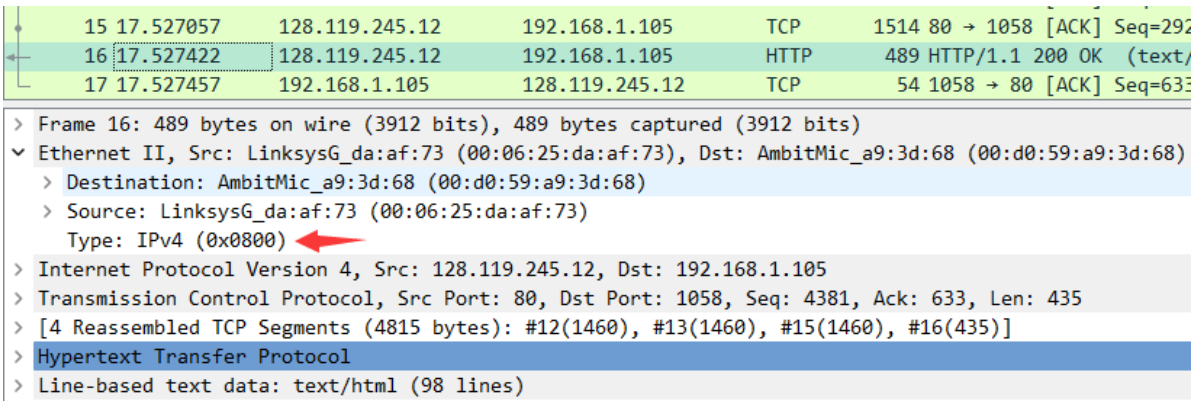


目的地址：AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

是我的计算机的以太网地址

Q7

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



0x0800

表示上层协议是 IPv4

Q8

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?

```
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·
```

O对应4f，之前有16*4+3=67字节，算上O是68字节

Q9

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

```
接口: 192.168.19.1 --- 0x2
  Internet 地址         物理地址              类型
  192.168.19.255        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

接口: 100.64.183.9 --- 0x6
  Internet 地址         物理地址              类型
  100.64.128.1          c8-33-e5-8a-5d-45     动态
  100.64.142.81         c8-33-e5-8a-5d-45     动态
  100.64.147.209        c8-33-e5-8a-5d-45     动态
  100.64.160.209        c8-33-e5-8a-5d-45     动态
  100.64.181.207        c8-33-e5-8a-5d-45     动态
  100.64.188.81         c8-33-e5-8a-5d-45     动态
  100.64.191.255        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: 192.168.75.1 --- 0xb
  Internet 地址         物理地址              类型
  192.168.75.255        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
```

网卡、路由IP和MAC地址、广播地址、组播地址

Q10

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

```
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)
```

源地址　　00:d0:59:a9:3d:68

目标地址　ff:ff:ff:ff:ff:ff

Q11

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

```
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)
```

0x0806

对应上层的ARP协议

Q12

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.

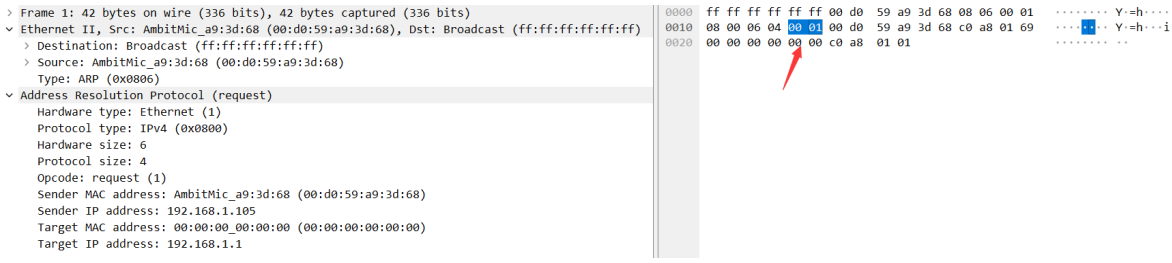
a) How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

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?

c) Does the ARP message contain 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?

a



16+4=20 bytes

b

```
Opcode: request (1)
```

1

代表ARP请求

c

```
Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Sender IP address: 192.168.1.105
```

包含

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
```

opcode可以看出request

Q13

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?
    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?
    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?

a

```
> 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:
  > 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)
    Target IP address: 192.168.1.105

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               ···· ····
```

16+4=20 bytes

b

```
Protocol size: 4
Opcode: reply (2)
Sender MAC address: Link
```

2

代表响应报文

c

```
Opcode: reply (2)
Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
Sender IP address: 192.168.1.1
```

sender MAC address

sender IP address

Q14

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

```
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst:
  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
```

源地址　　00:06:25:da:af:73

目标地址　00:d0:59:a9:3d:68

Q15

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ARP查询报文是广播的，而响应是单播的， 只有对应IP地址的主机才能收到

EX1

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?

```
C:\Windows\System32>arp -s 192.168.75.1 22-22-22-22-22-22

C:\Windows\System32>arp -a

接口: 192.168.19.1 --- 0x2
  Internet 地址         物理地址              类型
  192.168.19.255        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

接口: 100.64.183.9 --- 0x6
  Internet 地址         物理地址              类型
  100.64.128.1          c8-33-e5-8a-5d-45     动态
  100.64.142.81         c8-33-e5-8a-5d-45     动态
  100.64.147.209        c8-33-e5-8a-5d-45     动态
  100.64.160.209        c8-33-e5-8a-5d-45     动态
  100.64.181.207        c8-33-e5-8a-5d-45     动态
  100.64.188.81         c8-33-e5-8a-5d-45     动态
  100.64.191.255        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: 192.168.75.1 --- 0xb
  Internet 地址         物理地址              类型
  192.168.75.1          22-22-22-22-22-22     静态
  192.168.75.255        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
```

管理员权限下可以添加

EX2

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
  6          35        1500  connected     WLAN
  3           5        1500  disconnected  以太网
 14          25        1500  disconnected  本地连接* 1
  7          25        1500  disconnected  本地连接* 10
 13          65        1500  disconnected  蓝牙网络连接
  2          35        1500  connected     VMware Network Adapter VMnet1
 11          35        1500  connected     VMware Network Adapter VMnet8
```

Idx为6对应WLAN

```
C:\Windows\System32>netsh interface ipv4 show interface 6

接口 WLAN 参数
----------------------------------------------
IfLuid                             : wireless_32768
IfIndex                            : 6
状态                               : connected
跃点数                             : 35
链接 MTU                           : 1500 字节
可访问时间                         : 44500 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30000ms，所以ARP cache条目TTL为30000ms