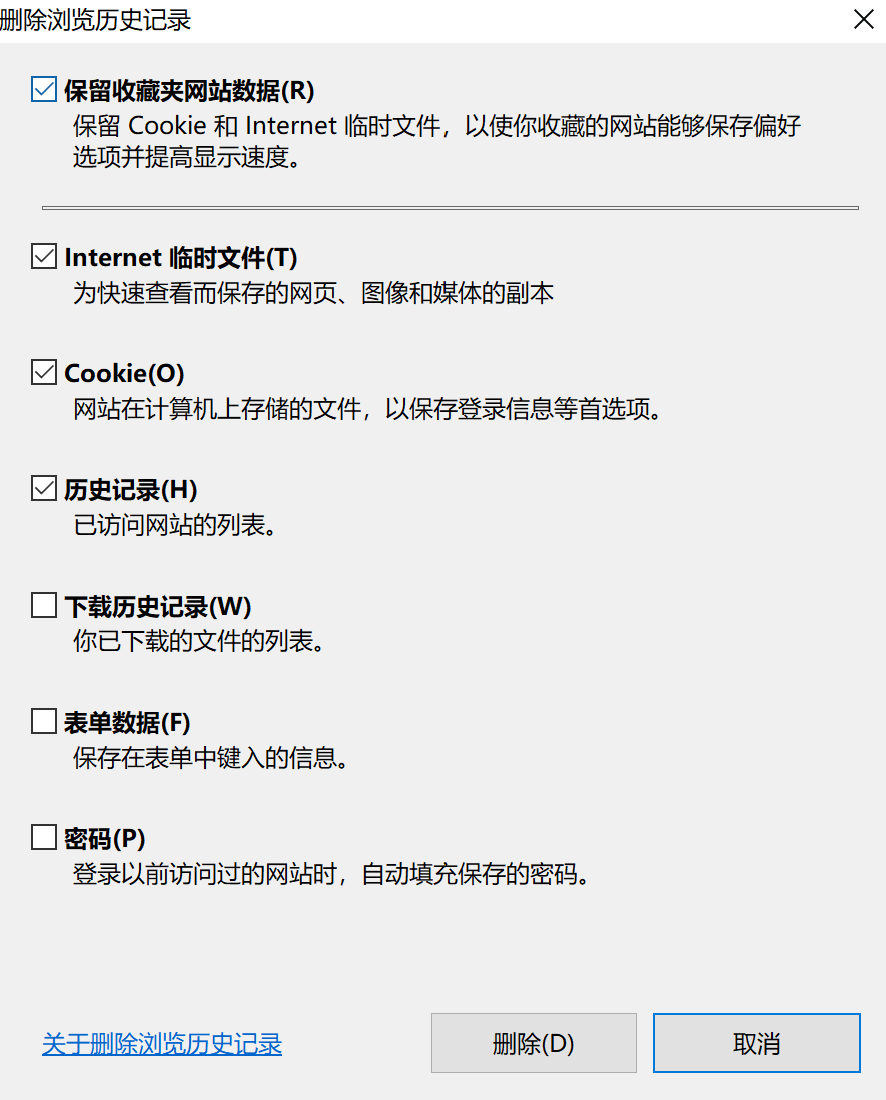
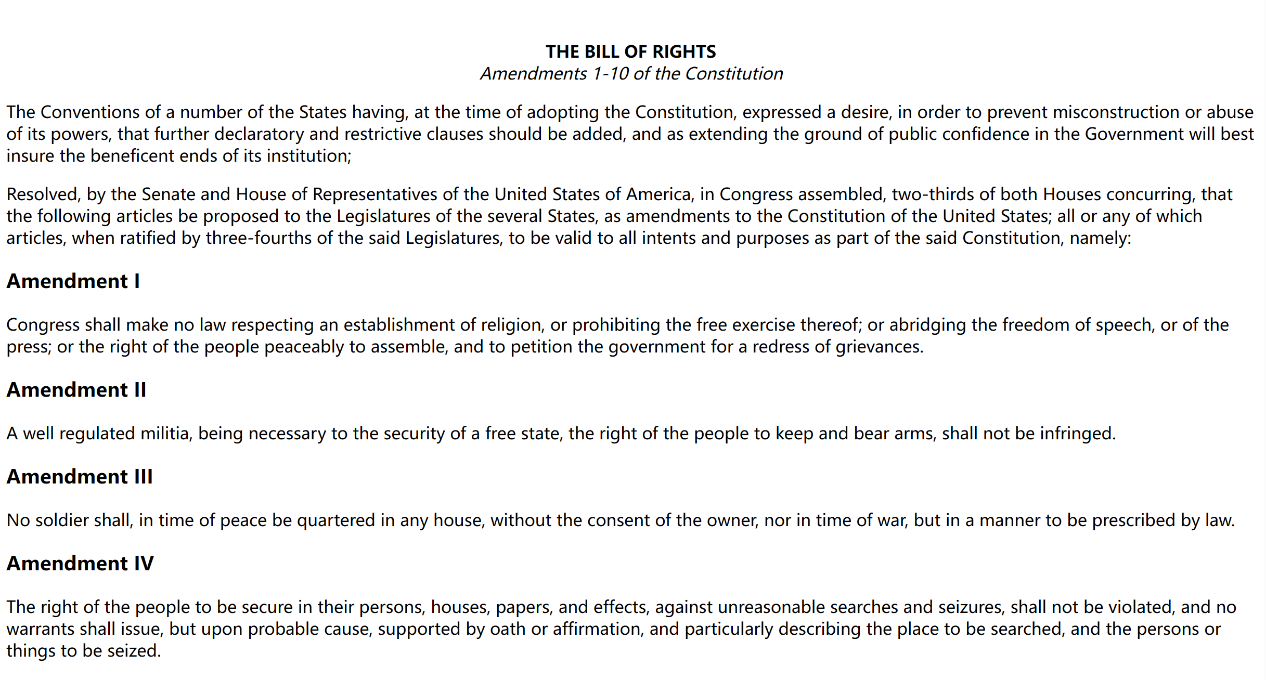
**实验6：ARP实验**

学号：PB21000224 姓名：陈鸿绪 日期：12.11.2023

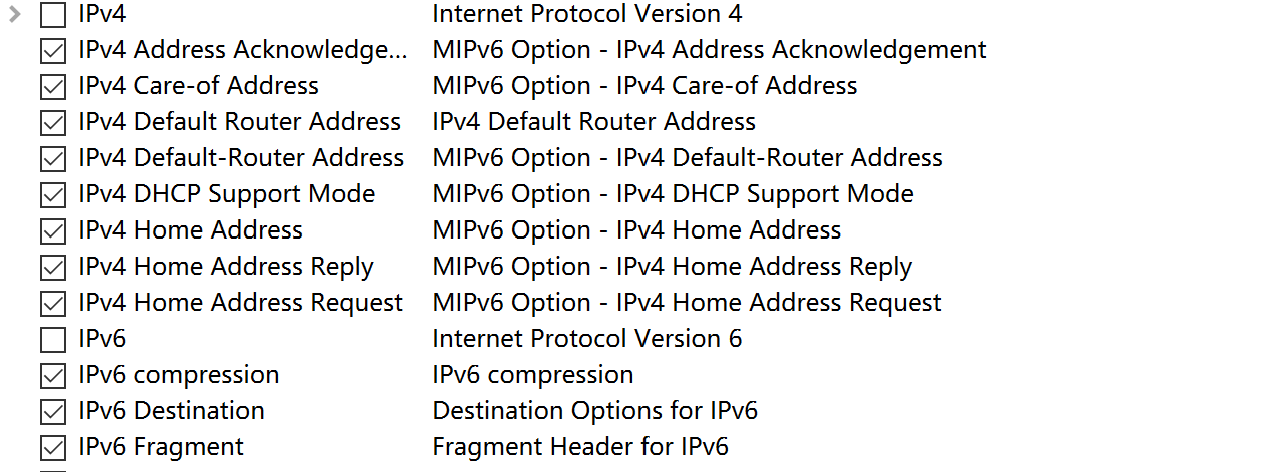
清除记录：

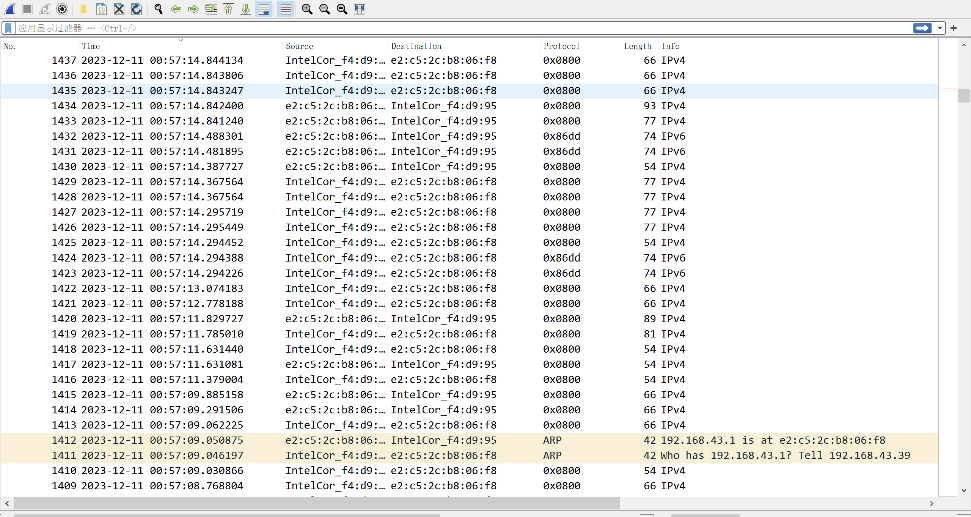


上指定网站：

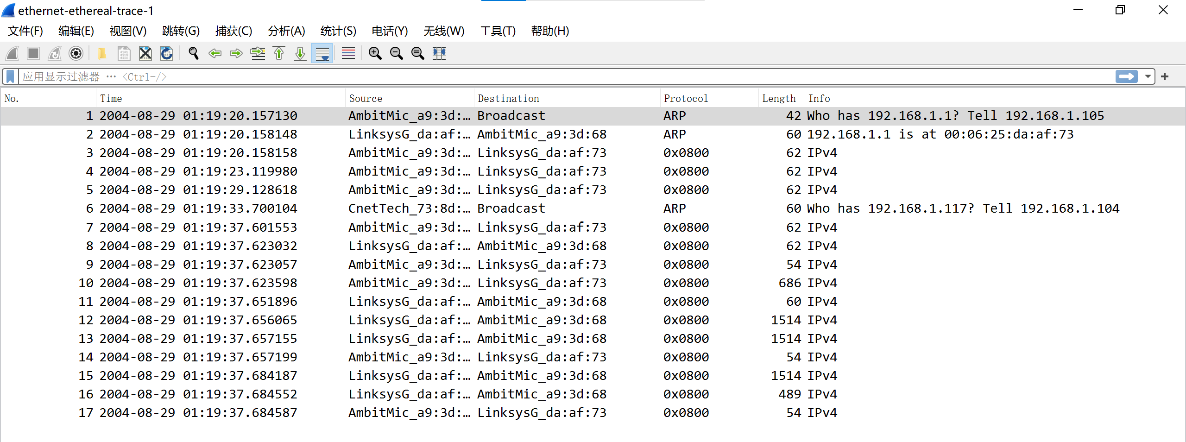


修改捕获数据包的协议类型，仅显示IP以下协议信息：





由于抓包干扰较多，采取文档提供的包：



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





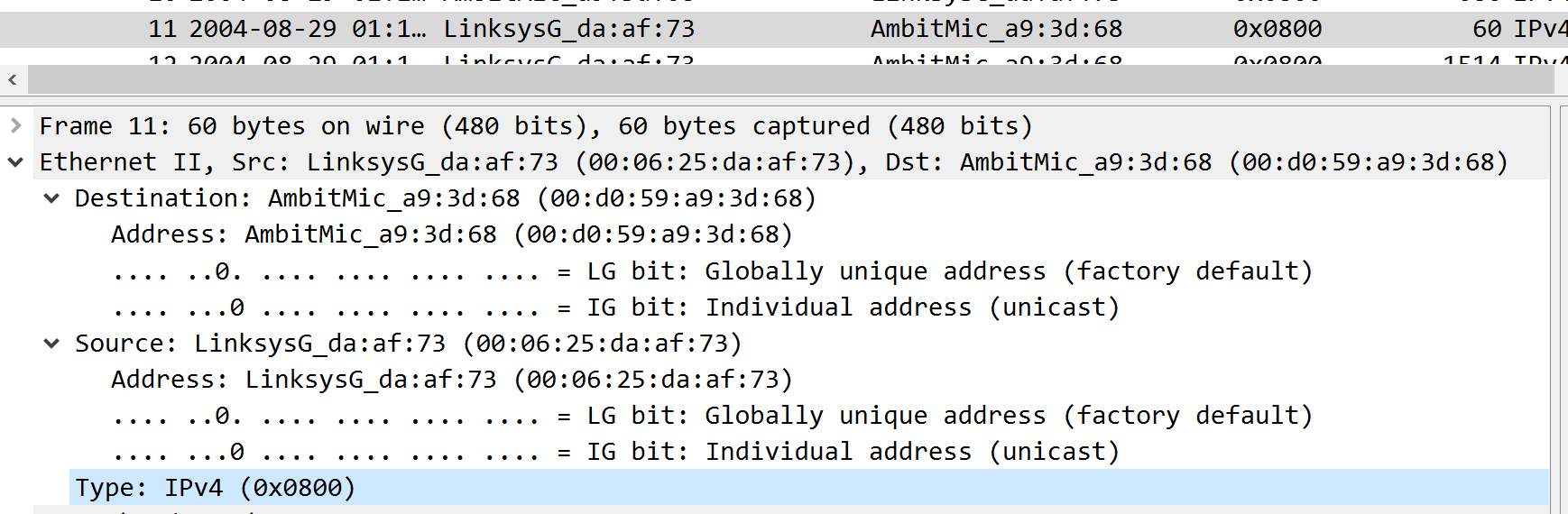
Ethernet address：AmbitMic\_a9:3d:68(00:d0:59:a9:3d:68)

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.]



不是gaia.cs.umass.edu的Ethernet address，该地址有可能是连接该子网的路由器。

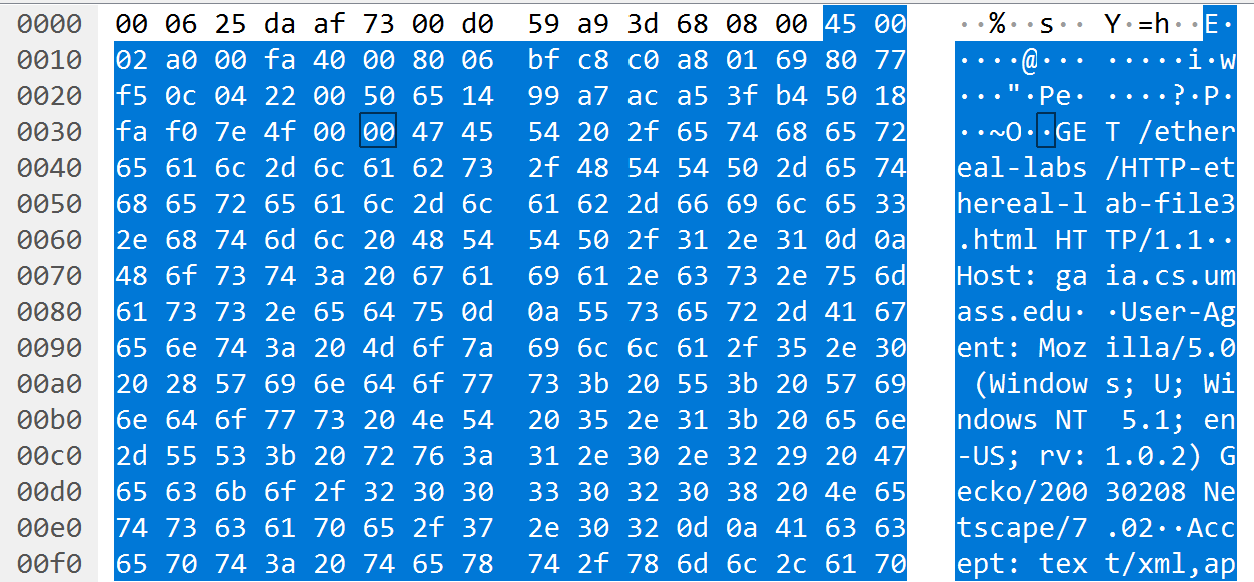
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?



hexadecimal value：0x0800

协议：IPv4

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



由图，前面有三行，所以是48个，G之前的第四行有6个，所以G之前有54字节（不包括G，如果包括则为55）。

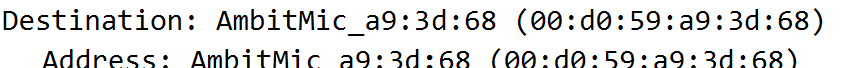
5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?



LinksysG\_da:af:73 (00:06:25:da:af:73)

不是address of my computer 或者 gaia.cs.umass.edu，是连接子网的路由器地址。

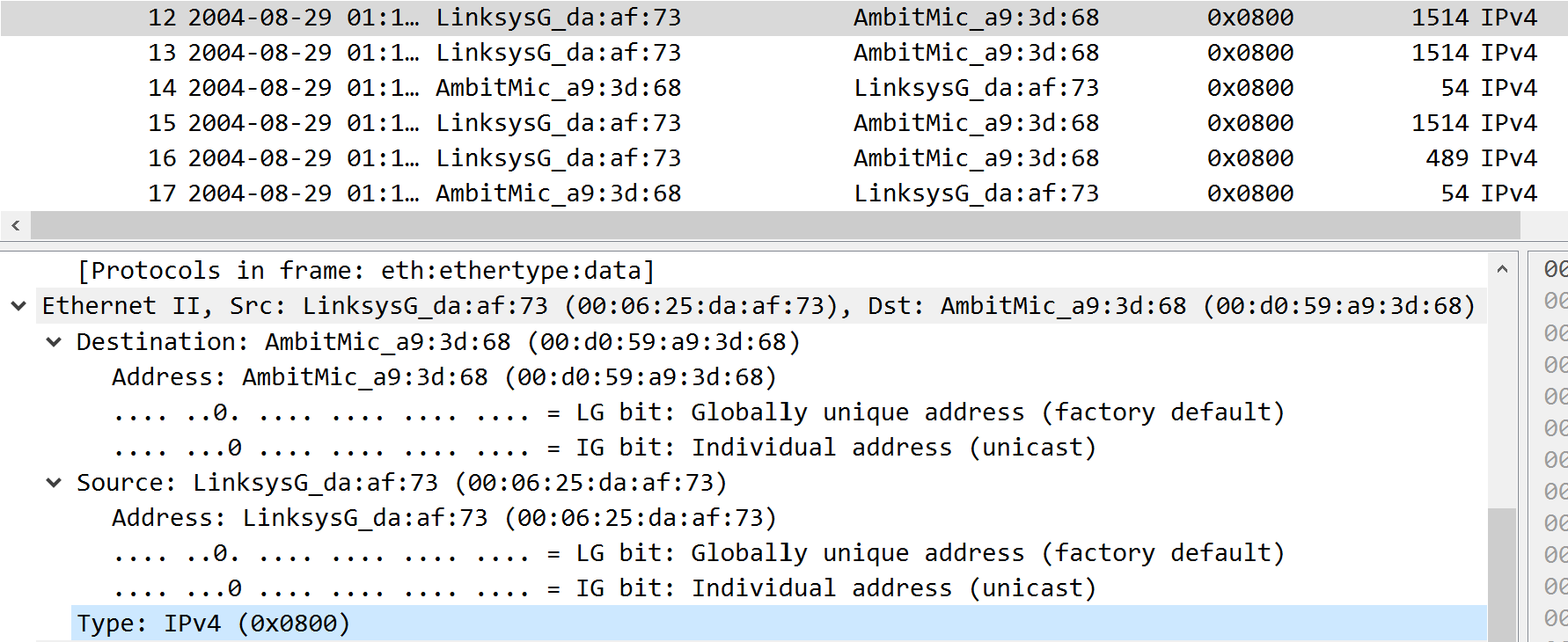
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?



AmbitMic\_a9:3d:68(00:d0:59:a9:3d:68)

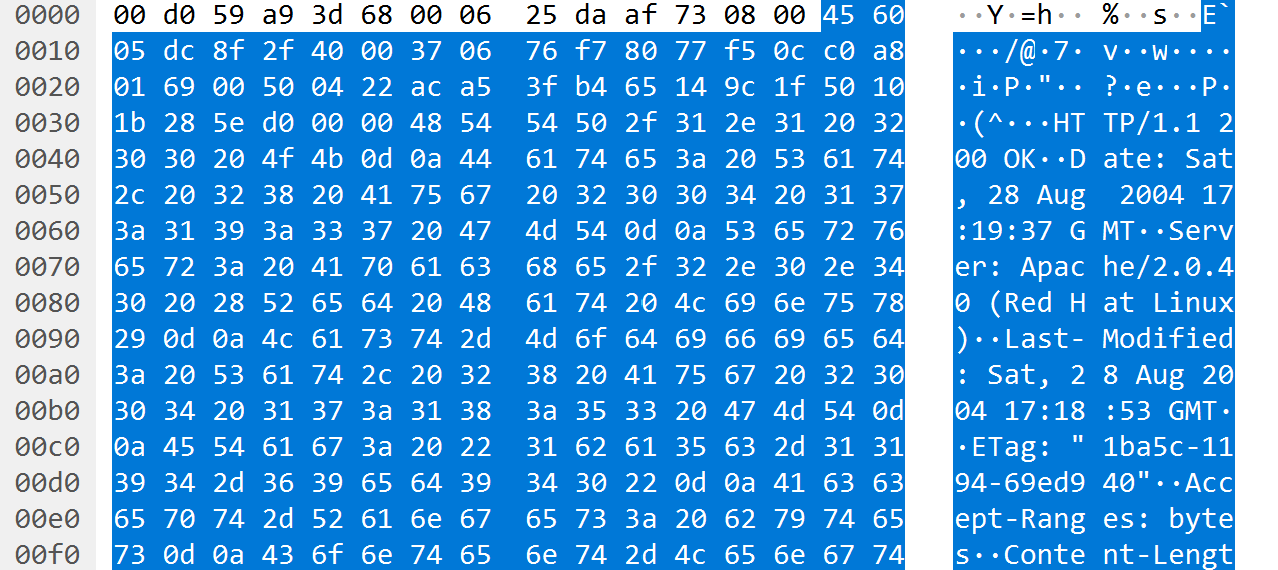
是the Ethernet address of my computer

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



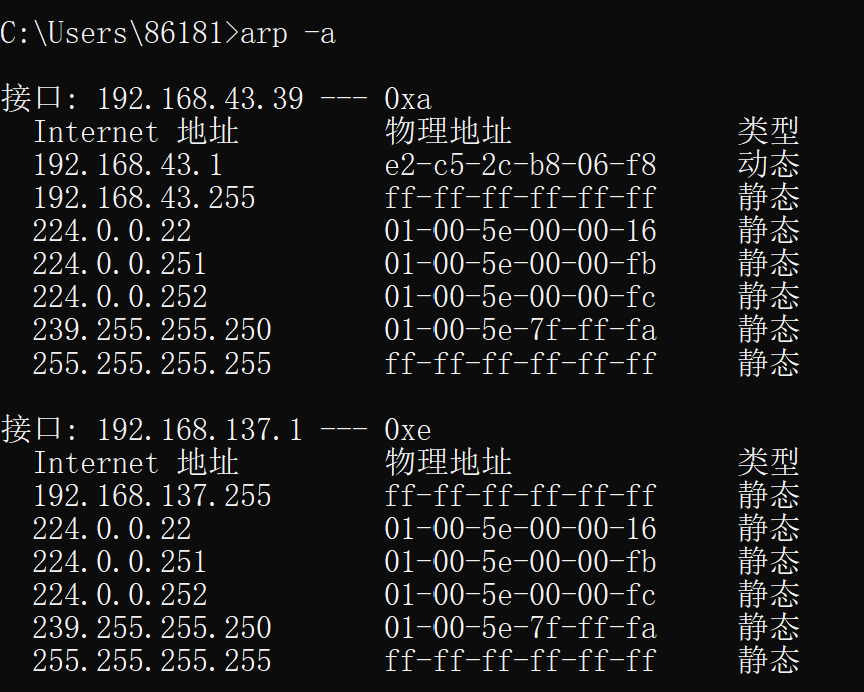
答案：0x0800，IPv4

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?



4\*16 + 3 =67 （不包括“O”，包括“O”则为68）

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

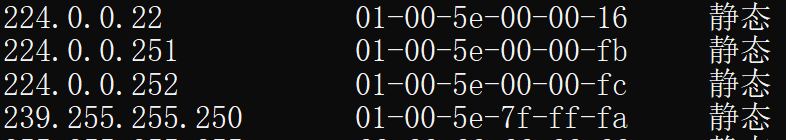


网卡：192.168.43.39

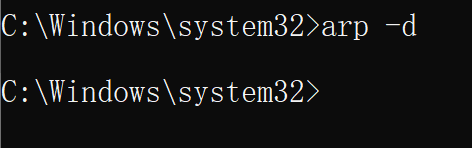
路由IP：

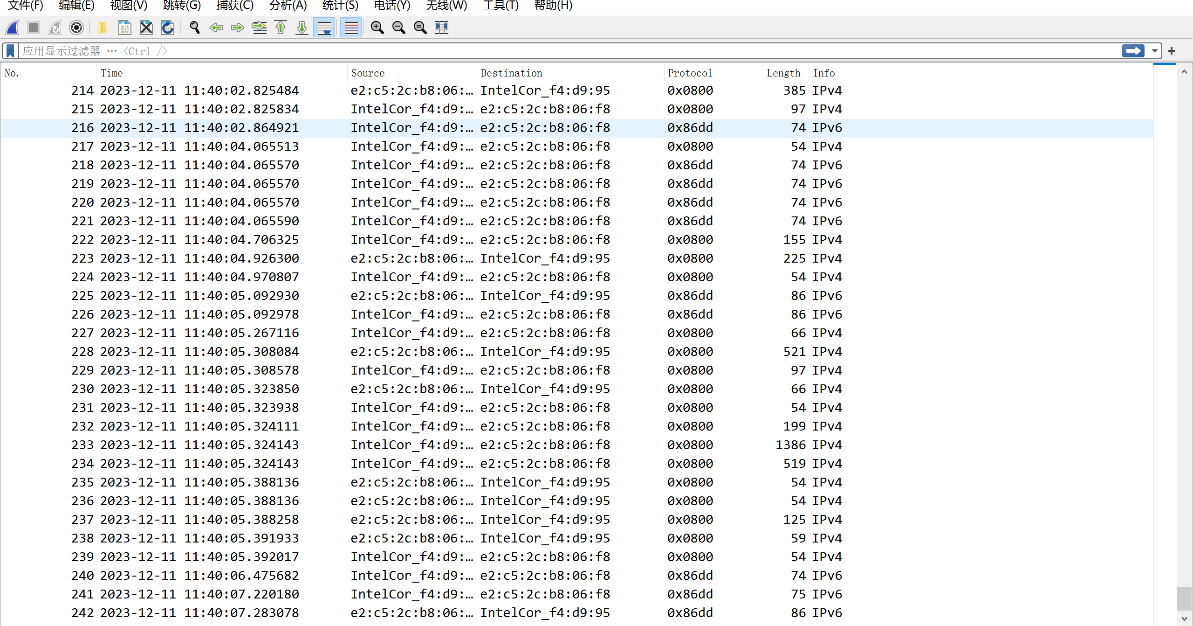
组播地址：

MAC地址：

广播地址：

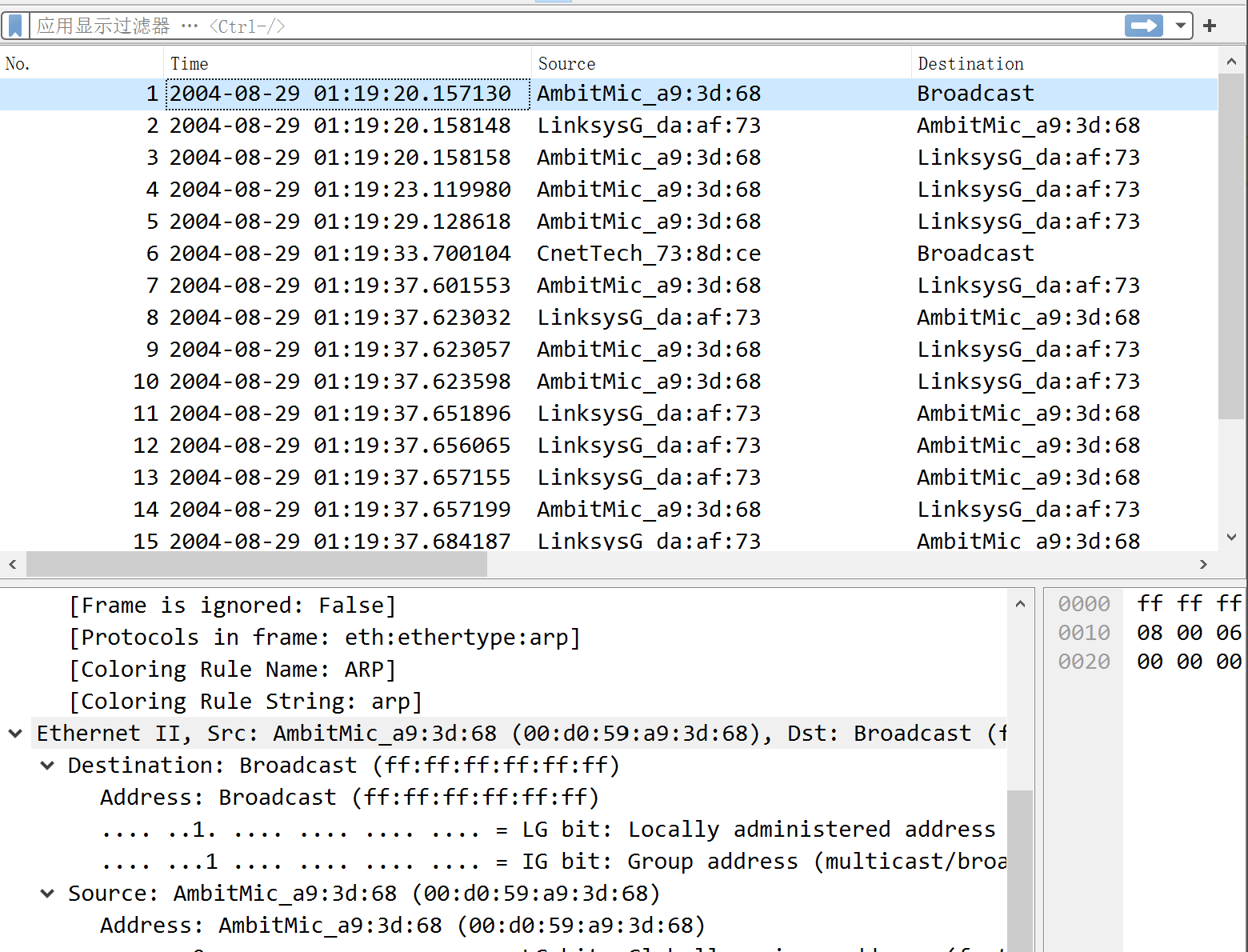
进行如下操作：

1. clear arp缓存：
2. 清空浏览器缓存
3. wireshark抓包
4. 打开停止抓包
5. 抓包界面如下（只有比IP低层的协议）



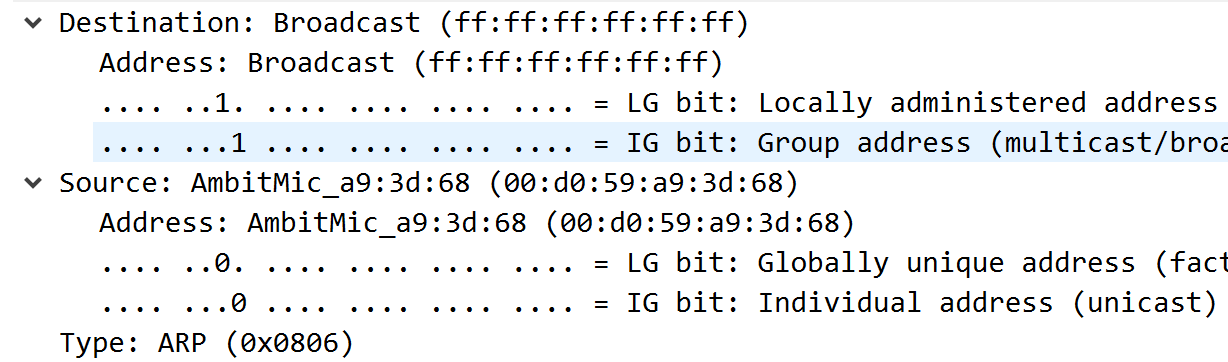
使用作者的包进行回答问题。

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



destination : Broadcast (ff:ff:ff:ff:ff:ff)source : AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

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

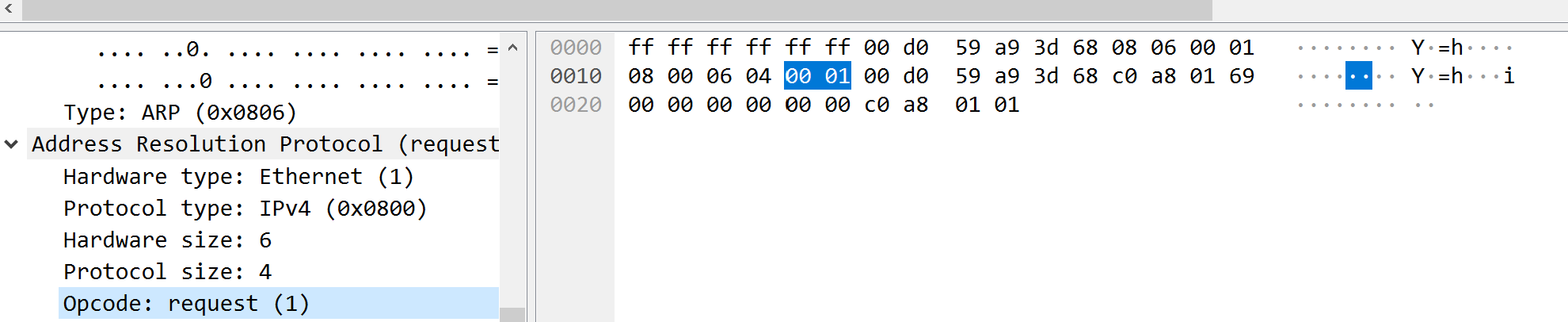


ARP(0x0806)

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>.

1. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

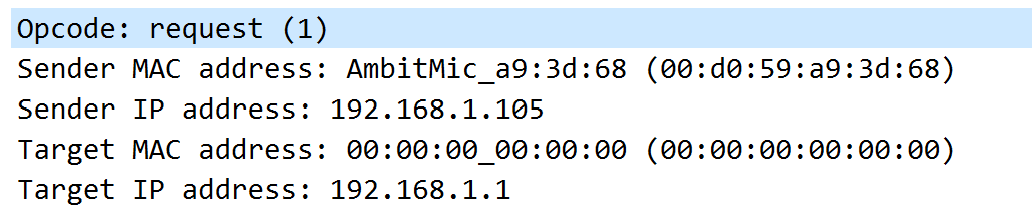


20bytes(如果包括opcode的开头就是21)

1. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

如上图0x0001

1. Does the ARP message contain the IP address of the sender?

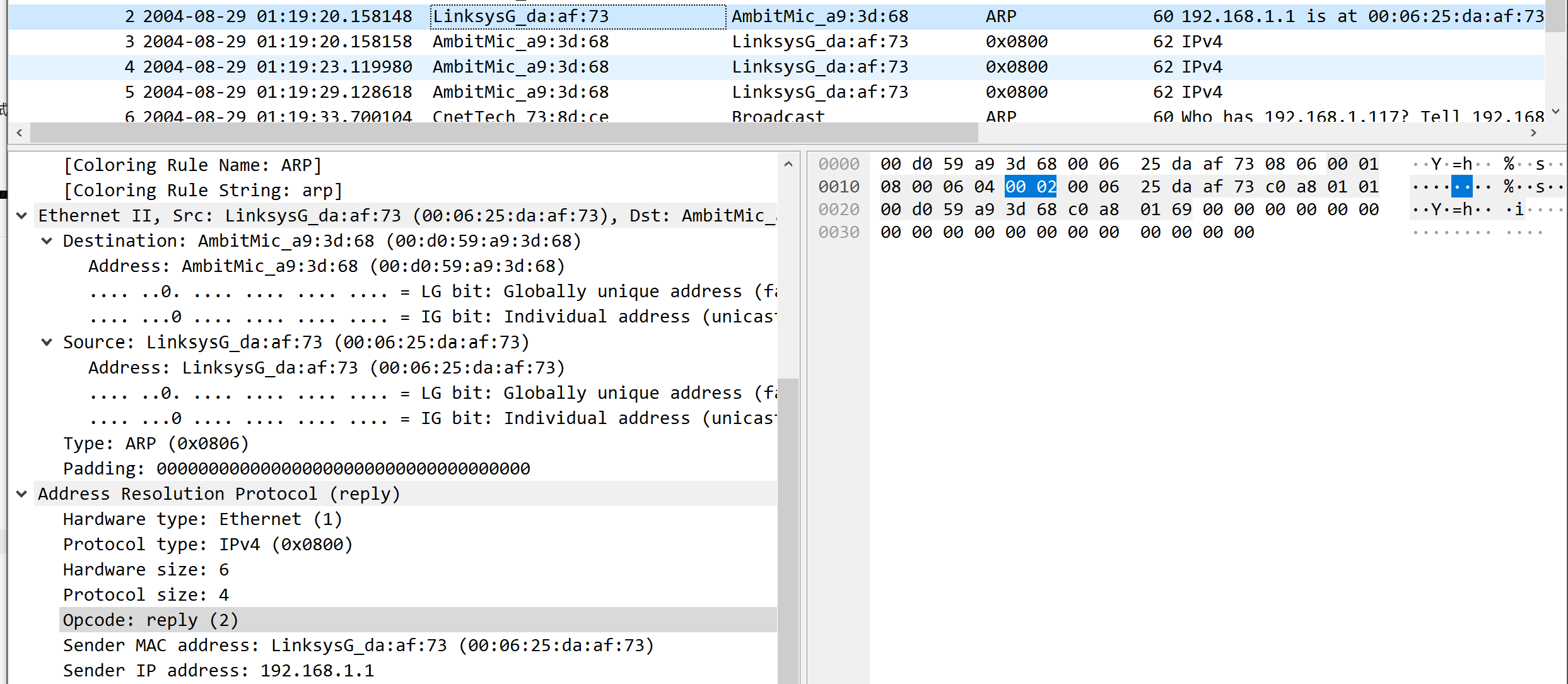


包含the IP address of the sender

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

Opcode告诉我们是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? 

20bytes(如果包括opcode的开头就是21)

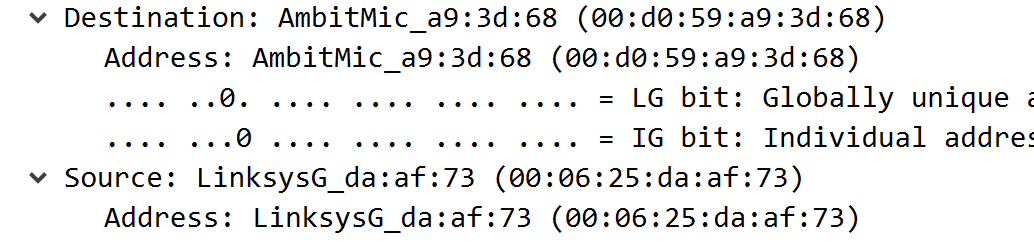
b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

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: reply(2)，是reply

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



destination : AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)  
source : LinksysG\_da:af:73 (00:06:25:da:af:73)

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

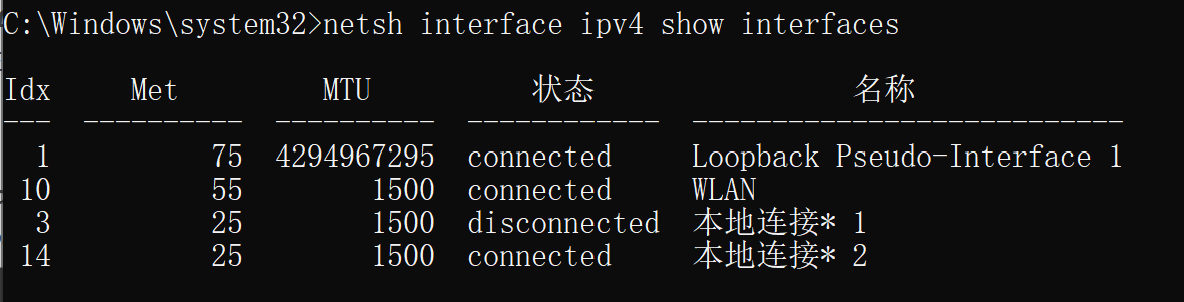
ARP查询报文通过广播帧传播，而响应ARP通过一个标准帧发送，所以响应ARP只有请求ARP的结点才可以接受，

Extra Credit

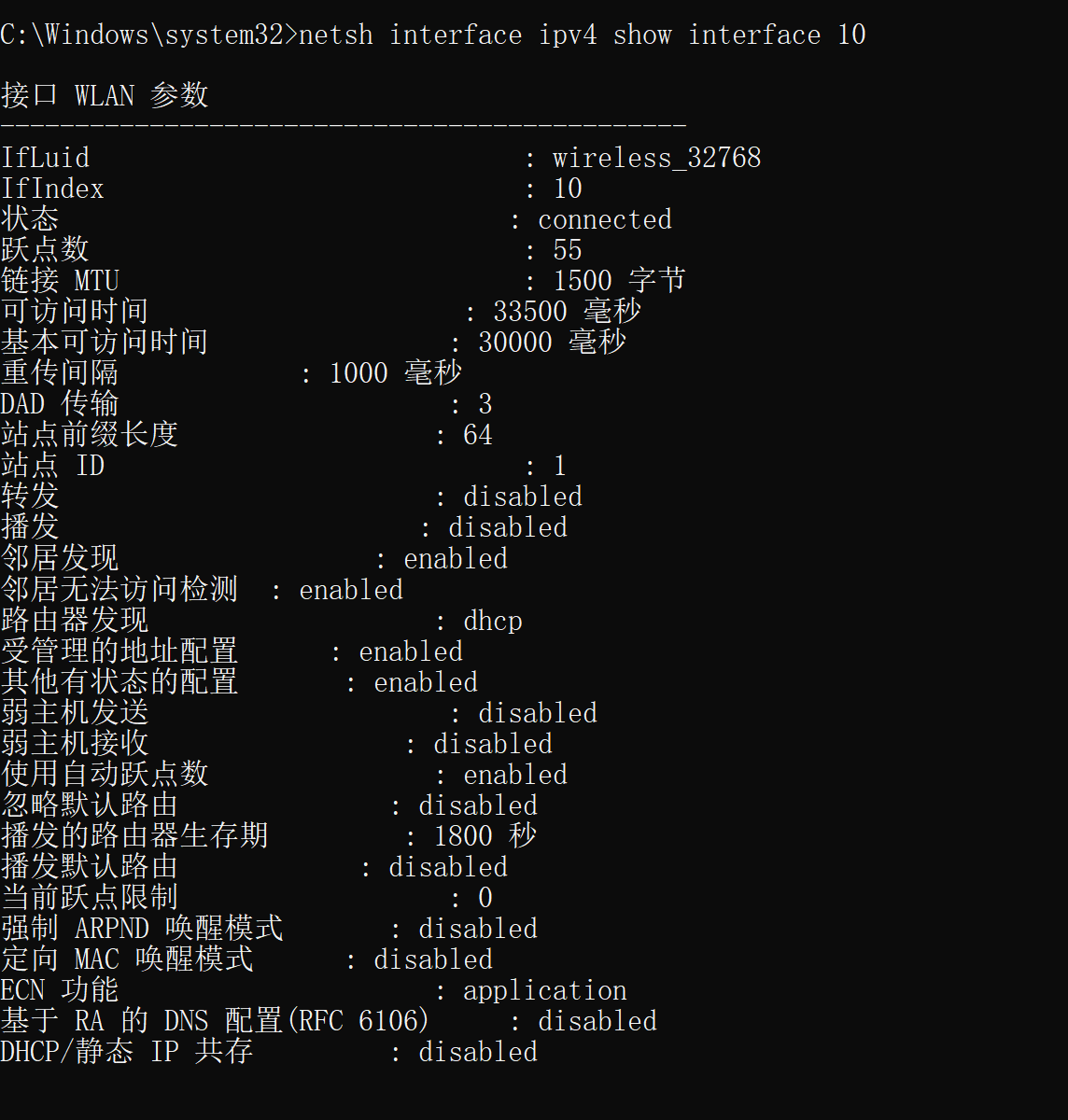
EX-1. The arp command: arp -s InetAddr EtherAddr allows you to manually add an entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for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

如果输入了正确的IP地址，但输入了与该远程接口不匹配的错误的以太网地址，会导致通信失败：系统将尝试使用该错误的以太网地址与远程接口进行通信，但是由于以太网地址不匹配，通信将会失败。将无法与具有正确IP地址的远程主机建立连接。

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.



Idx=10 对应WLAN：



基本可访问时间为 30000 毫秒，所以ARP cache TTL为30000