计算机网络实验报告_Ethernet-ARP

PB20000219 李蔚林

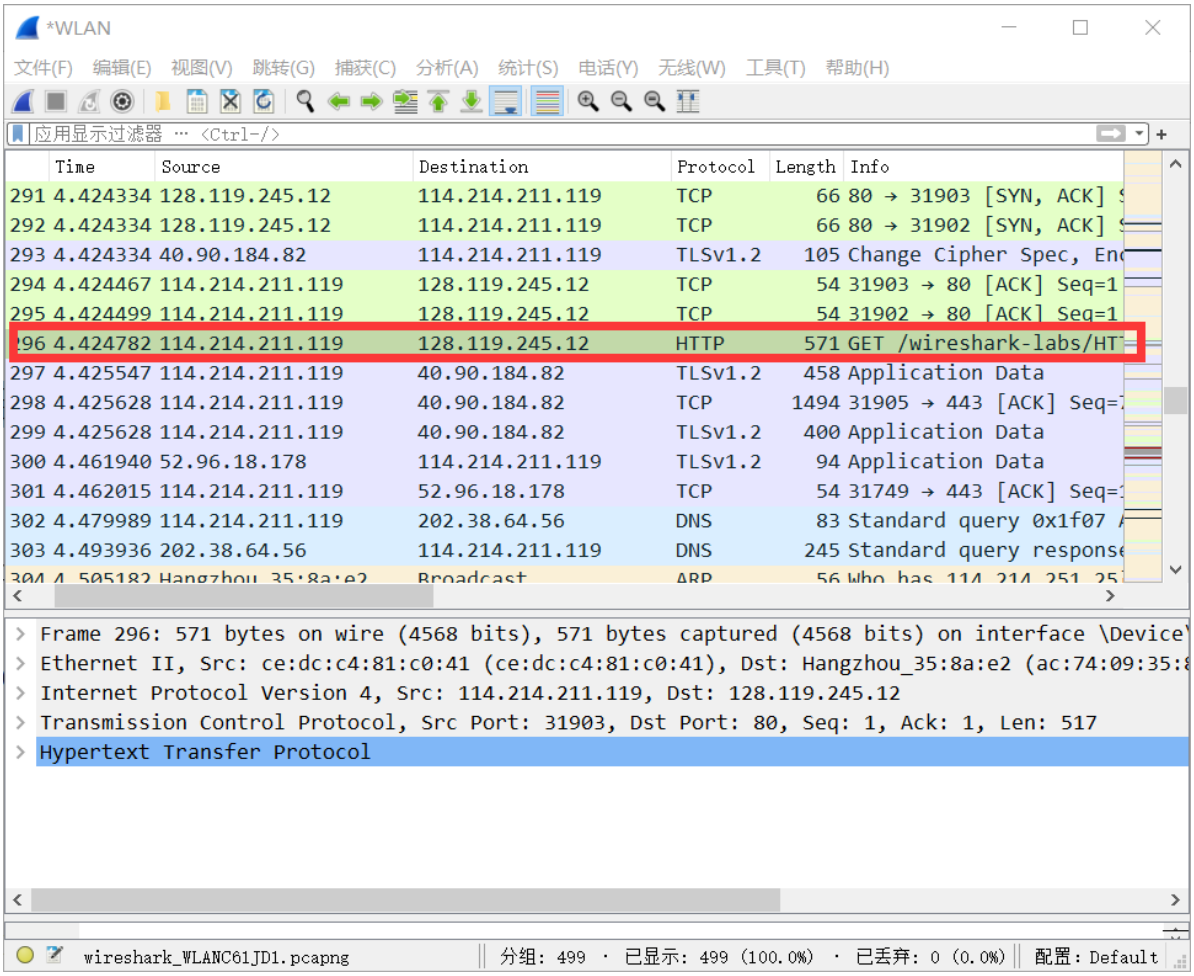
实验目的

1. 复习巩固链路层相关知识
2. 复习巩固ARP协议
3. 复习巩固以太网相关知识

实验过程及题目

PART1 Capturing and analyzing Ethernet frames

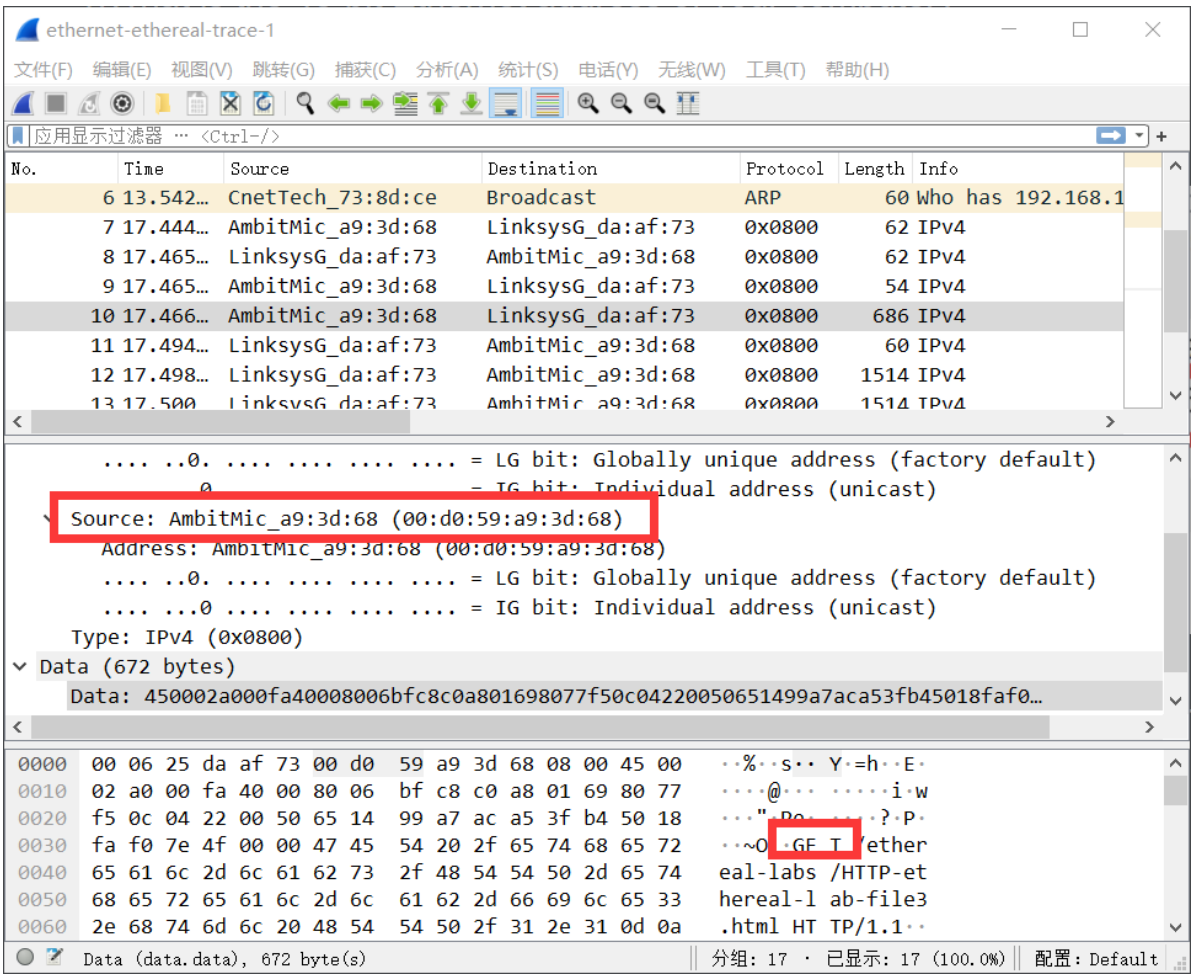
首先开启wireshark软件并用浏览器(已清除cookies)打开网址:http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html.结束抓包,wireshark界面如下:



由于自己抓的包特别乱,(好像是因为后台挂着下载任务的问题),所以下面我们分析作者抓的包.

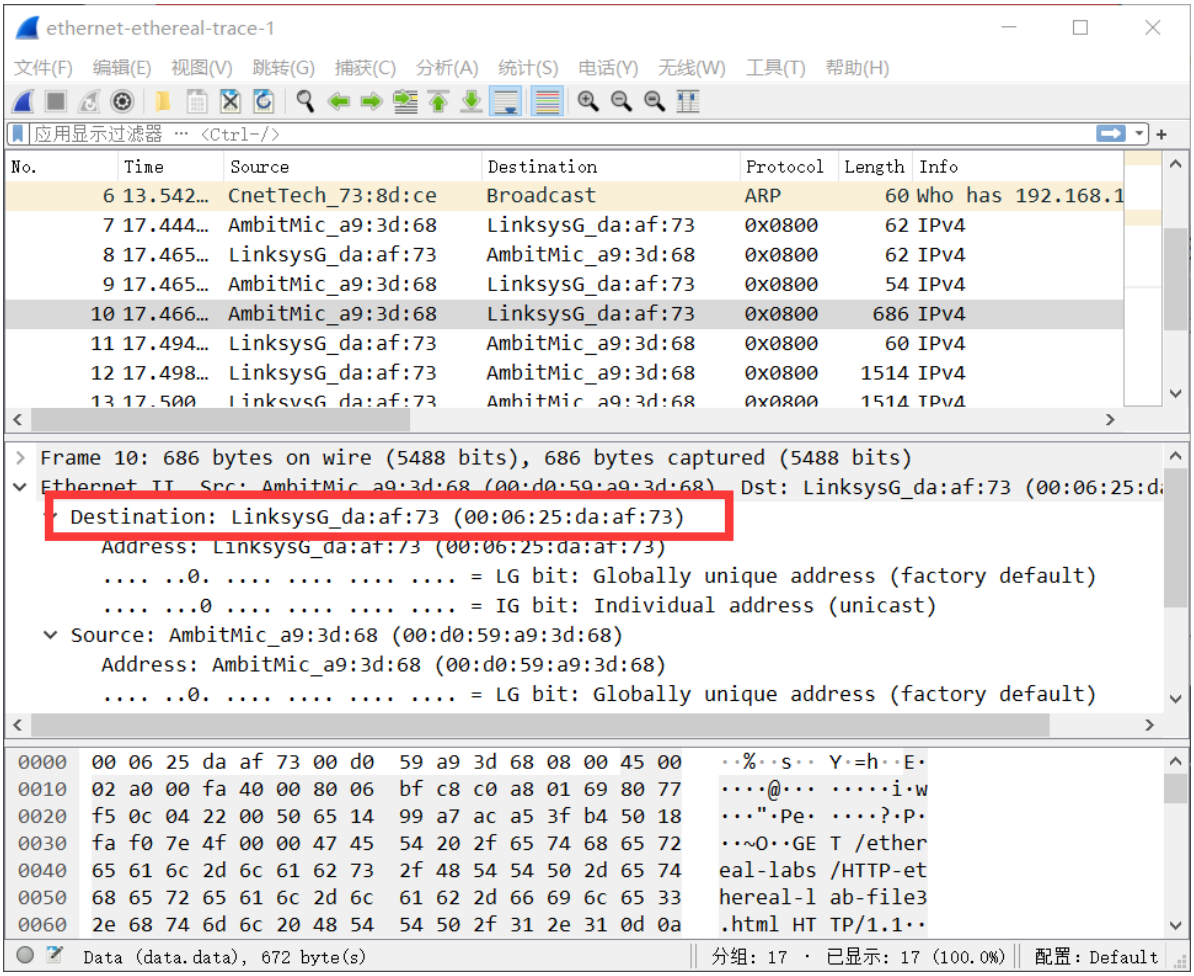
1.What is the 48-bit Ethernet address of your computer?

作者抓的包的自己的Ethernet address为: 00:d0:59:a9:3d:68.



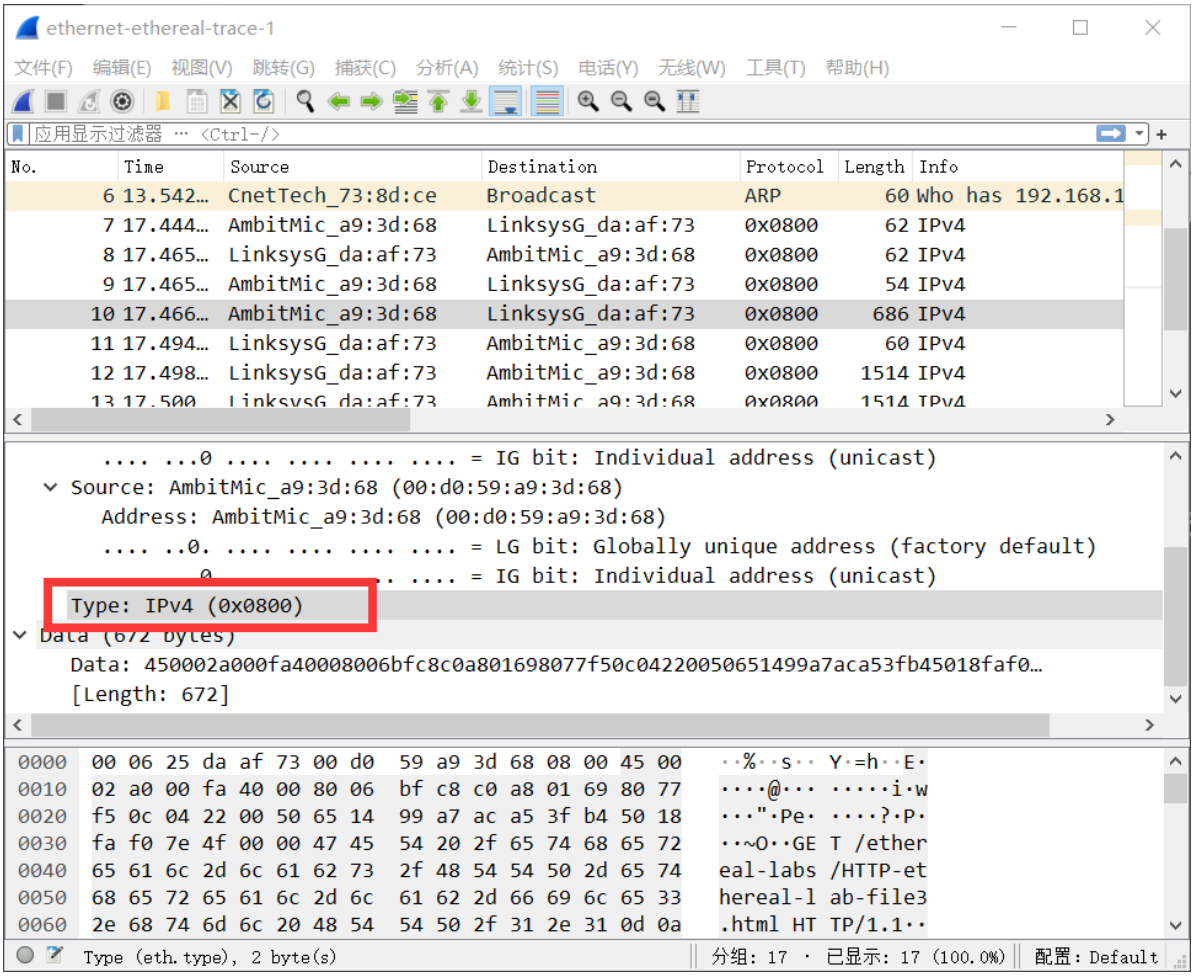
2.What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address?

是00:06:25:da:af:73.这不是 gaia.cs.umass.edu 的以太网地址。应该是作者使用的设备的默认路由地址.(个人想法:事实上可以打开cmd,输入ipconfig /all找到默认路由ip,接下来 arp -a,找到该ip对应的MAC应该就是本题所求的结果)



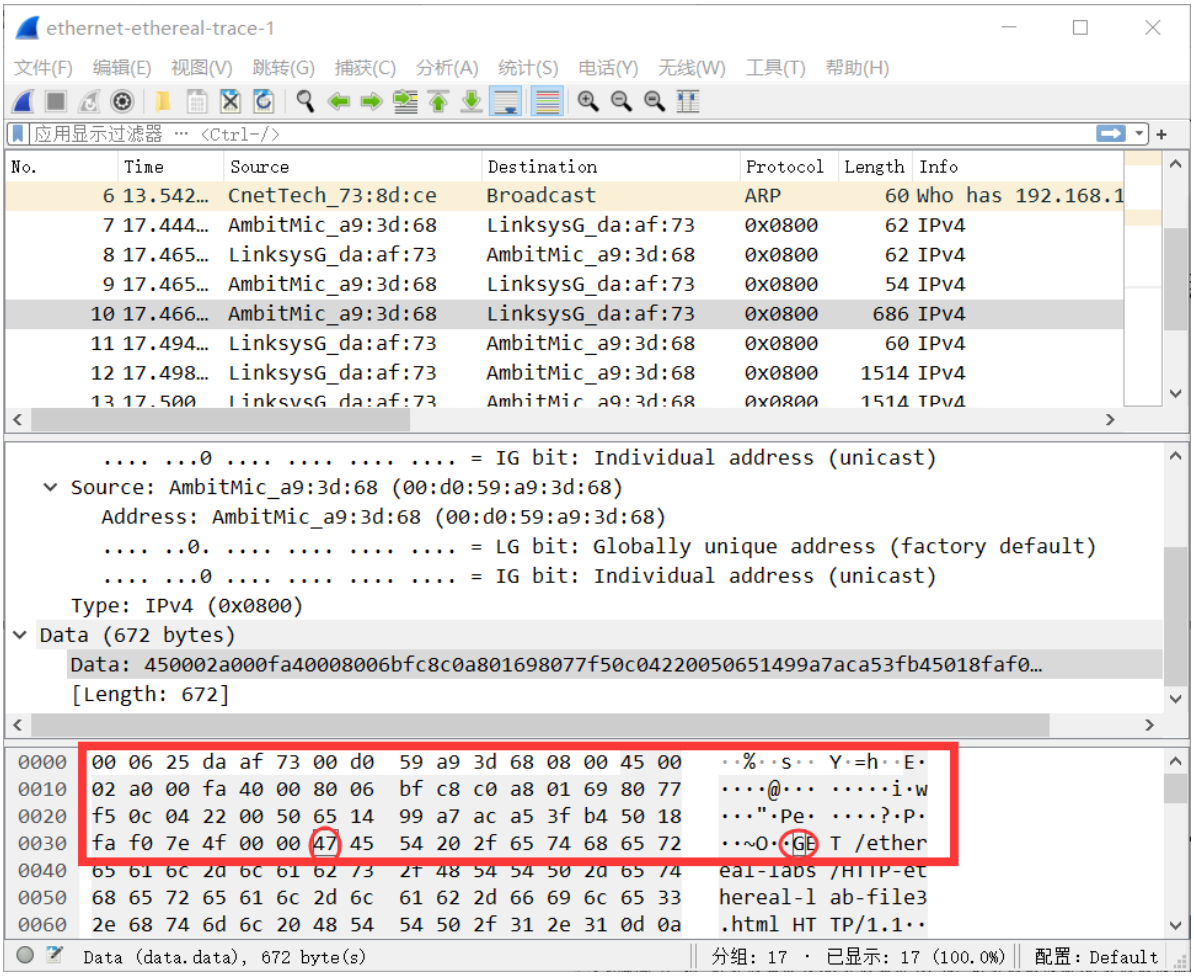
3.Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

0x0800.对应的是IPv4协议。



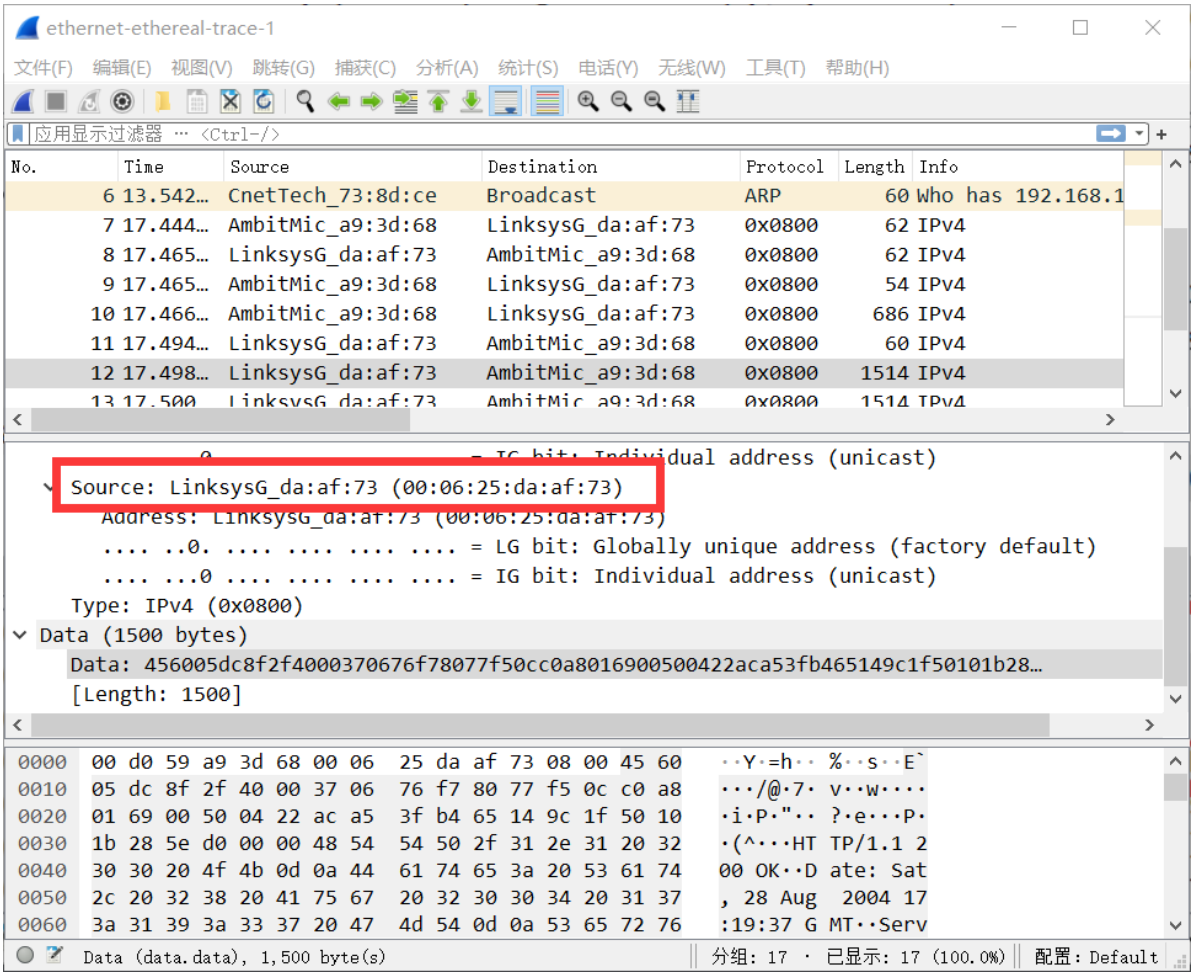
4.How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

如图所示，一共55个字节.



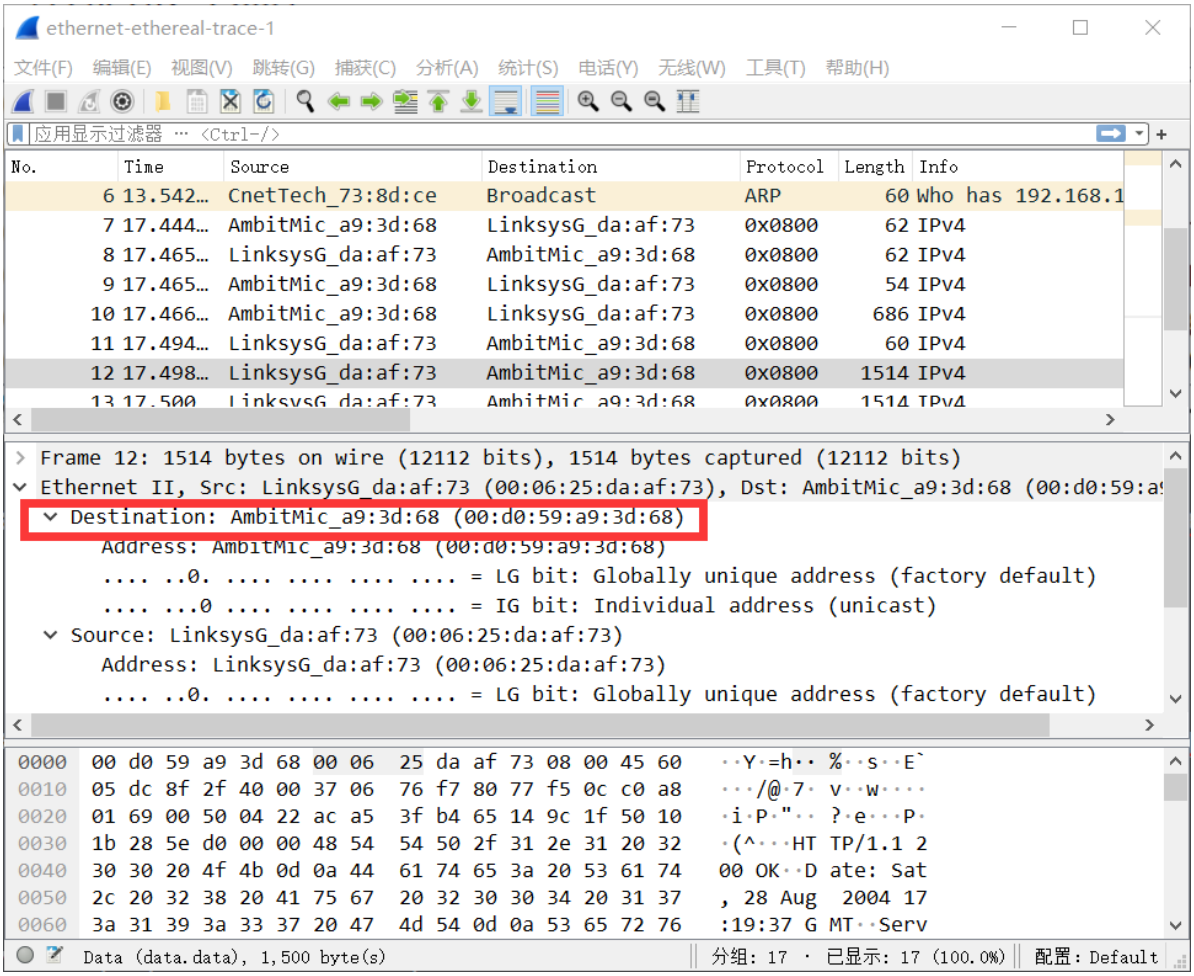
5.What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

00:06:25:da:af:73.两个都不是.如前面分析,这是作者使用设备的默认路由地址.



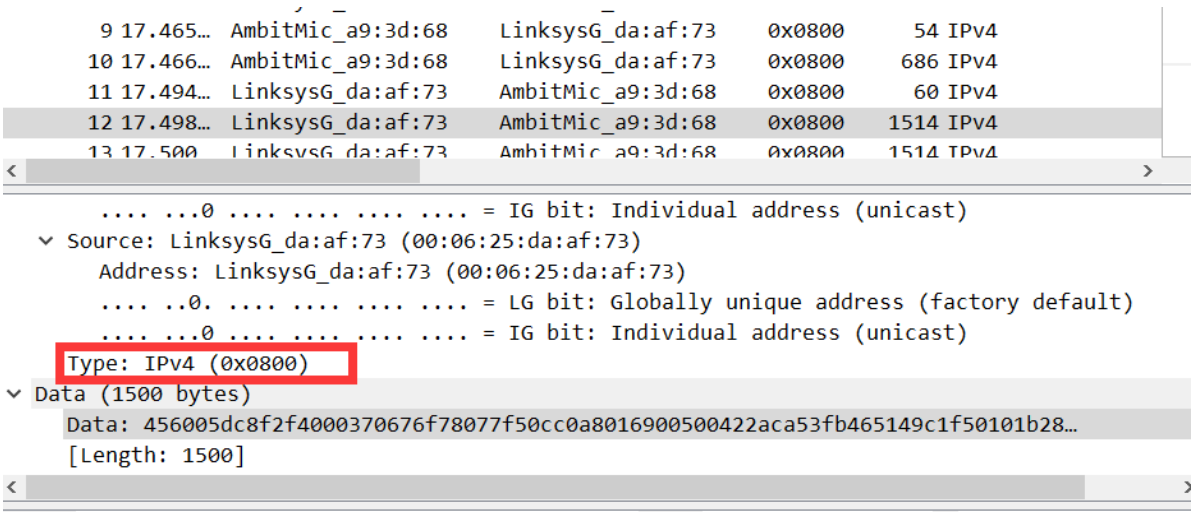
6.What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

00:d0:59:a9:3d:68.是作者使用的设备自己的地址



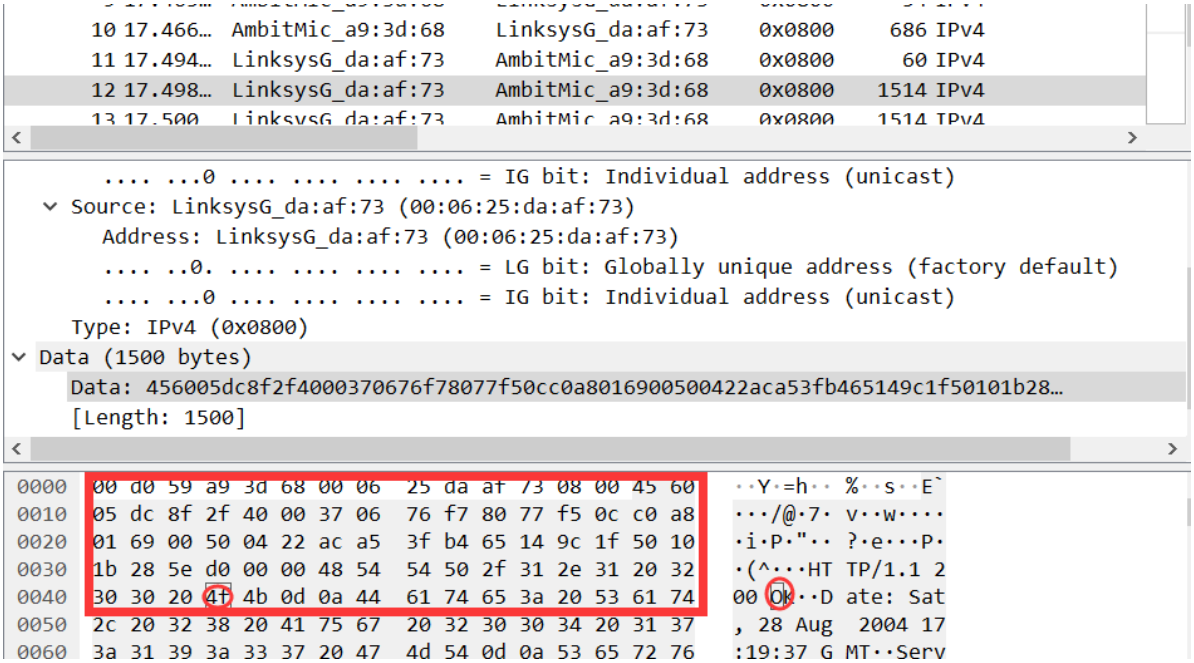
7.Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

0x0800.对应的是IPv4协议。



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?

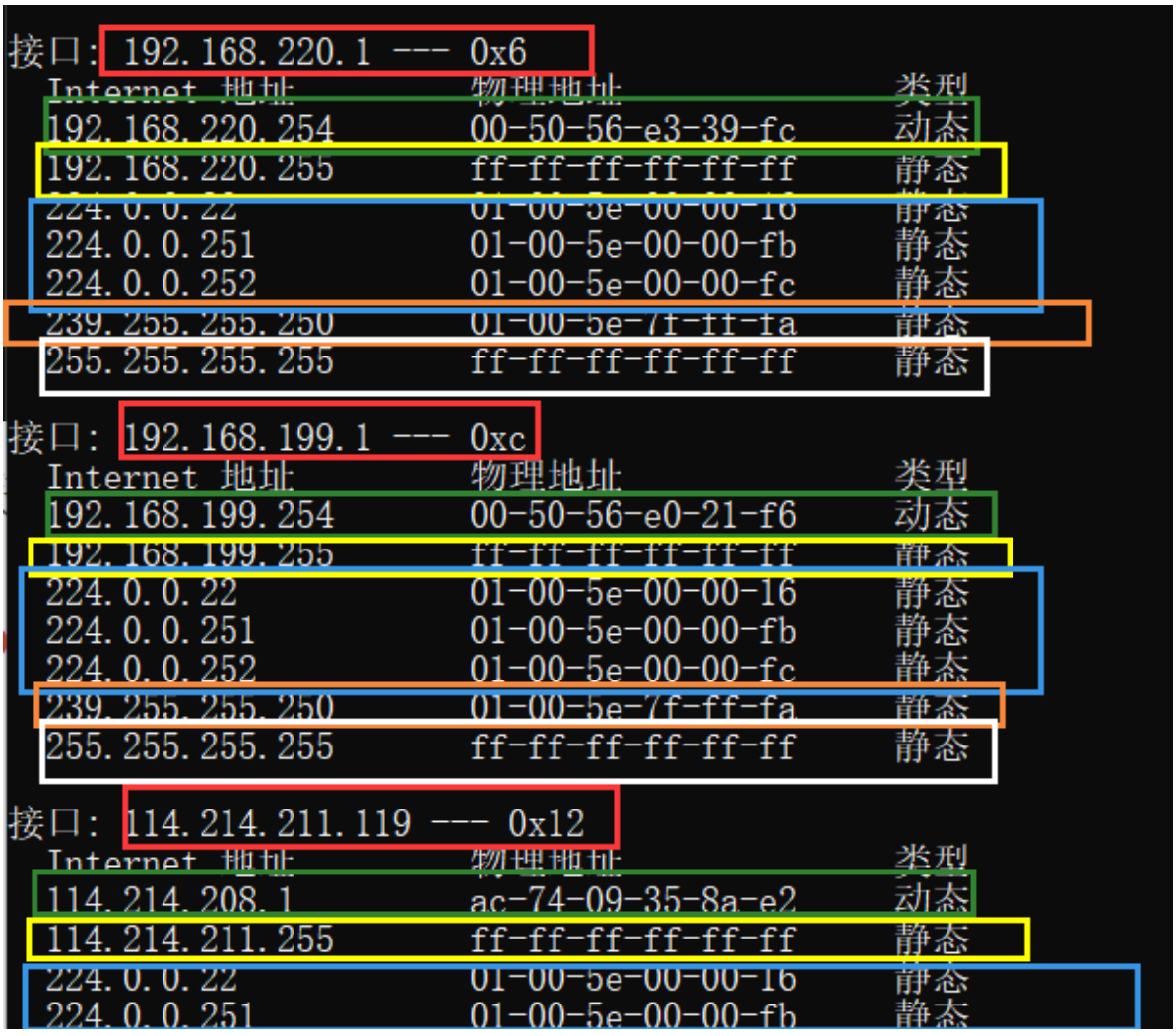
如图所示，一共68个字节.



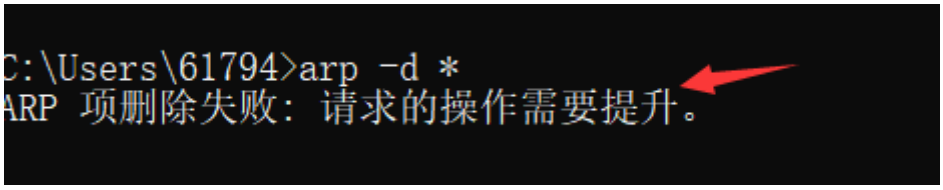
PART2 The Address Resolution Protocol

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

如下图:红色是指接口(对应不同的IP和MAC),绿色对应的是其路由地址和路由MAC,黄色和白色对应广播地址,蓝色和橙色对应组播地址.



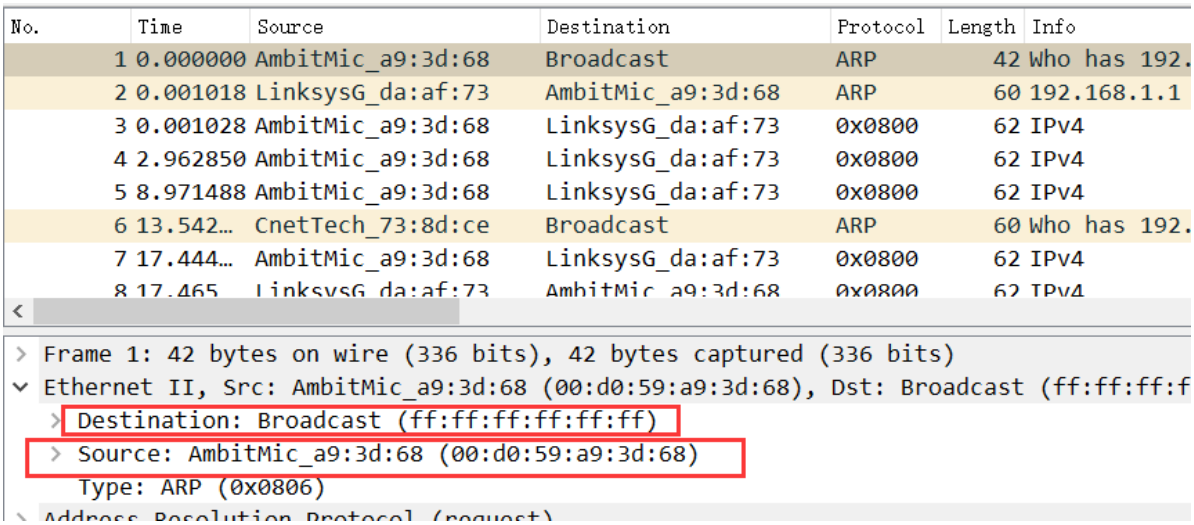
下面的问题由于清理ARP缓存需要root权限,故用作者抓的包进行分析.



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

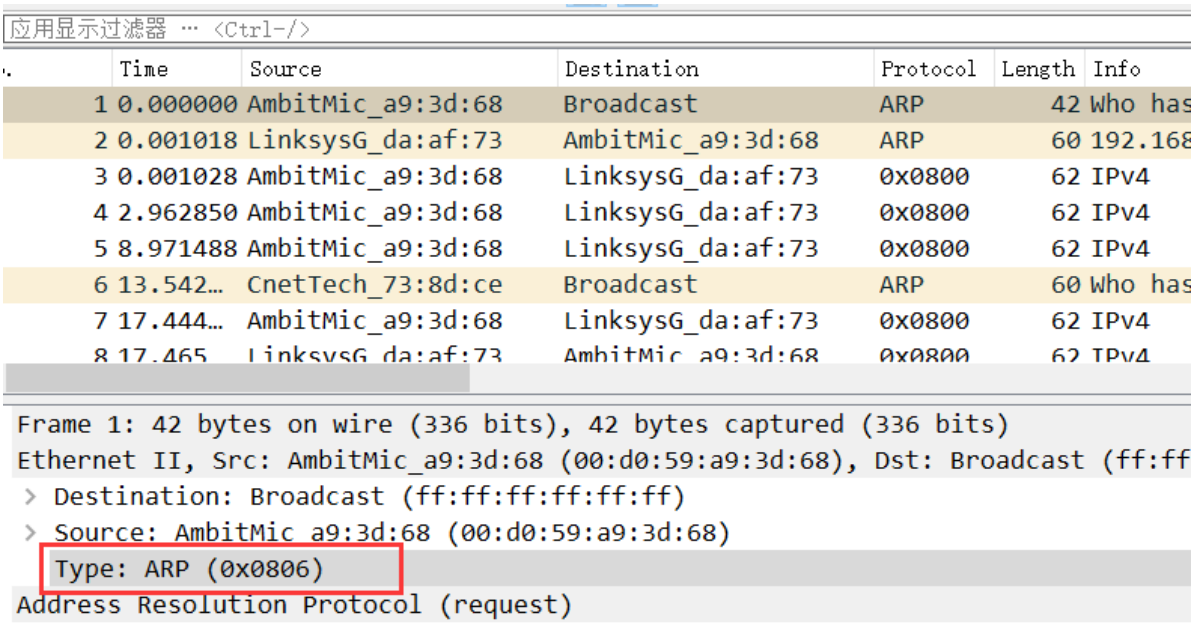
source: 00:d0:59:a9:3d:68

destination: ff:ff:ff:ff:ff:ff



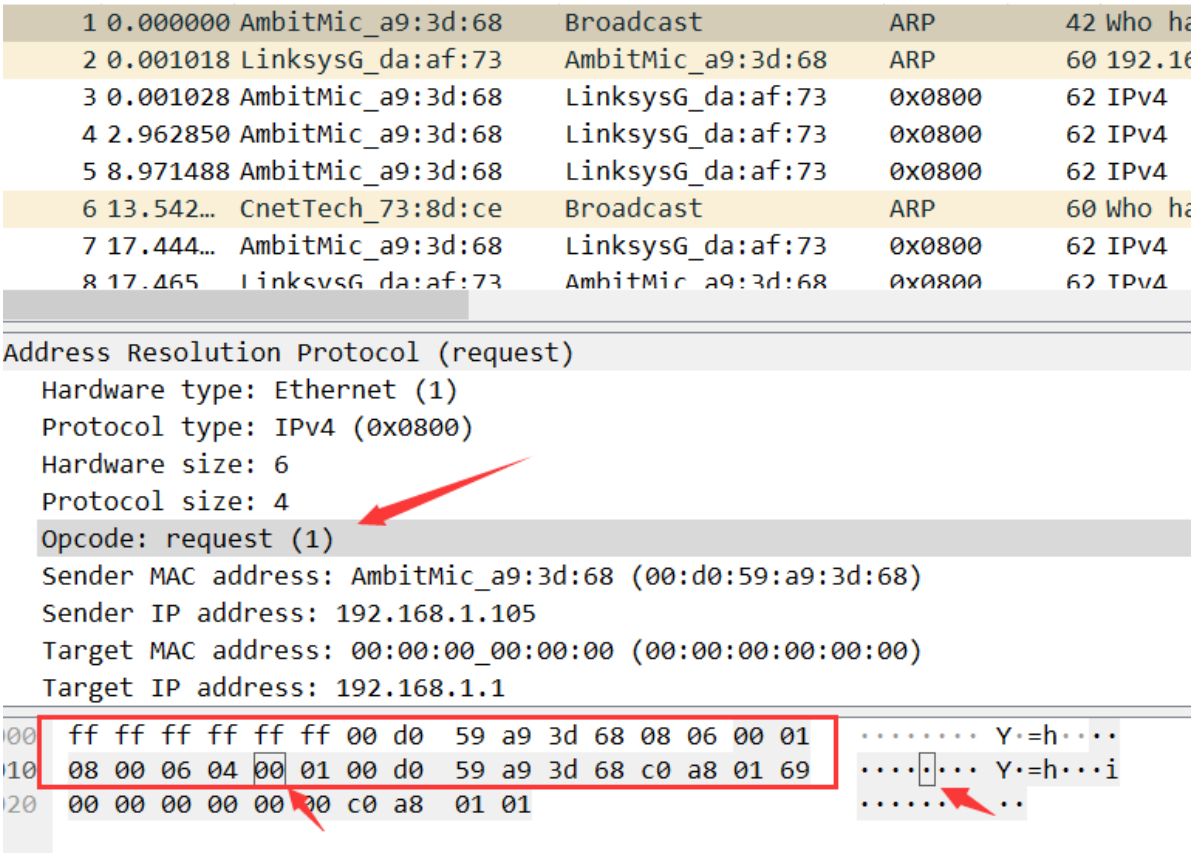
11.Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
以太网帧上层协议16 进制值是什么?

0x0806,ARP协议.



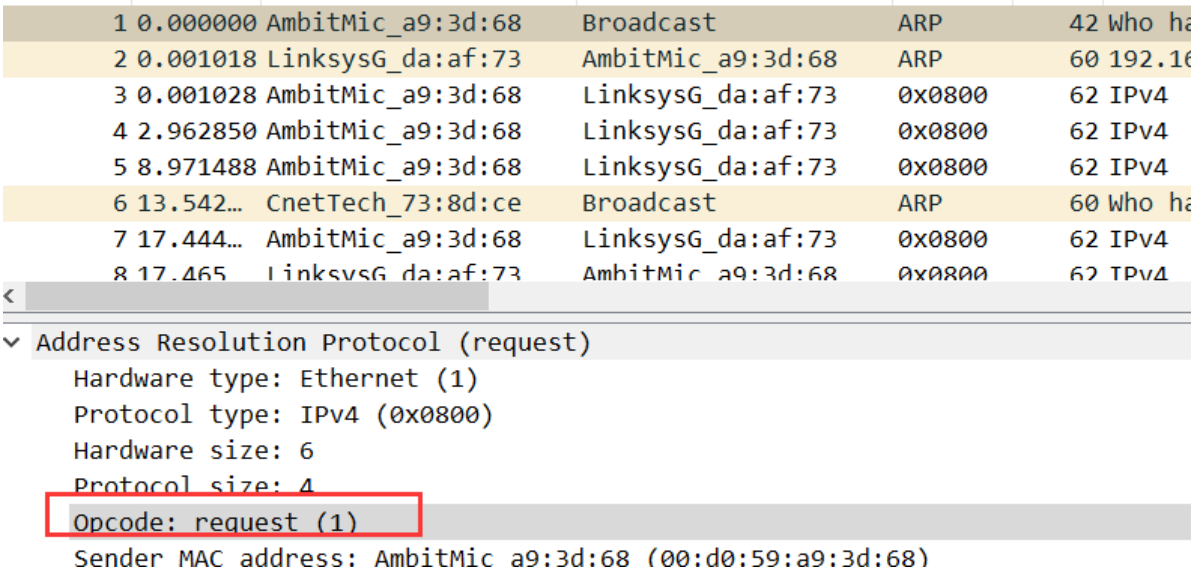
12.
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

21字节.



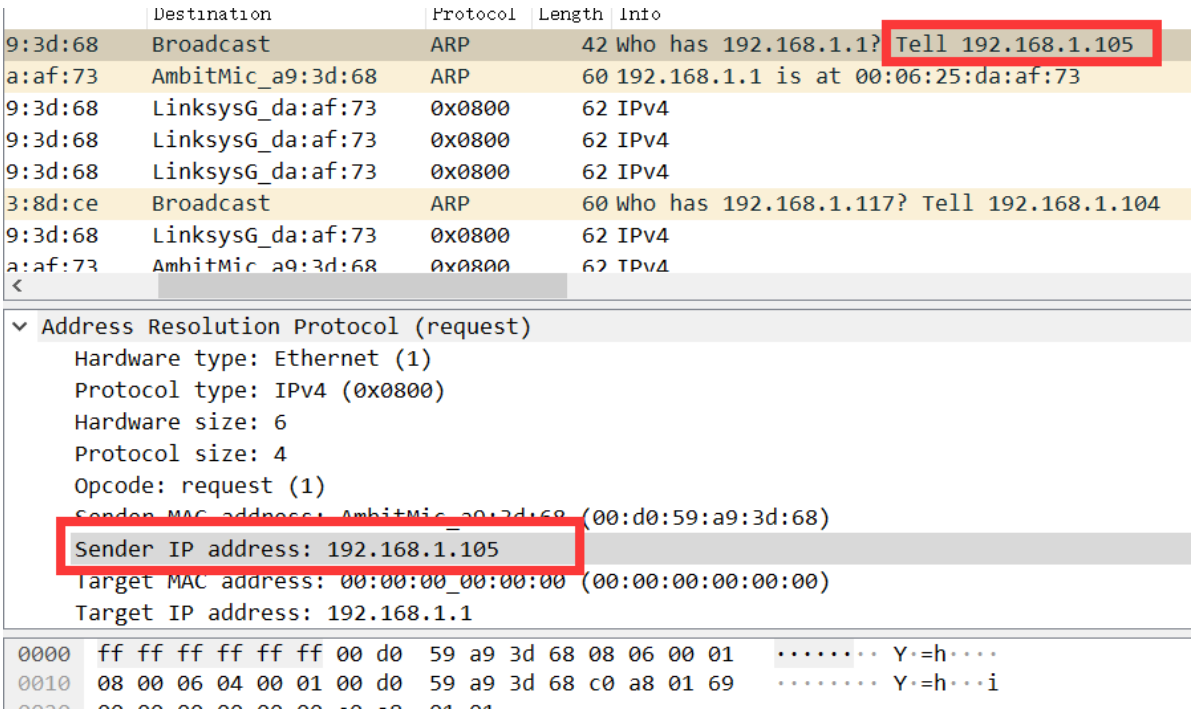
12.b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

opcode是1.



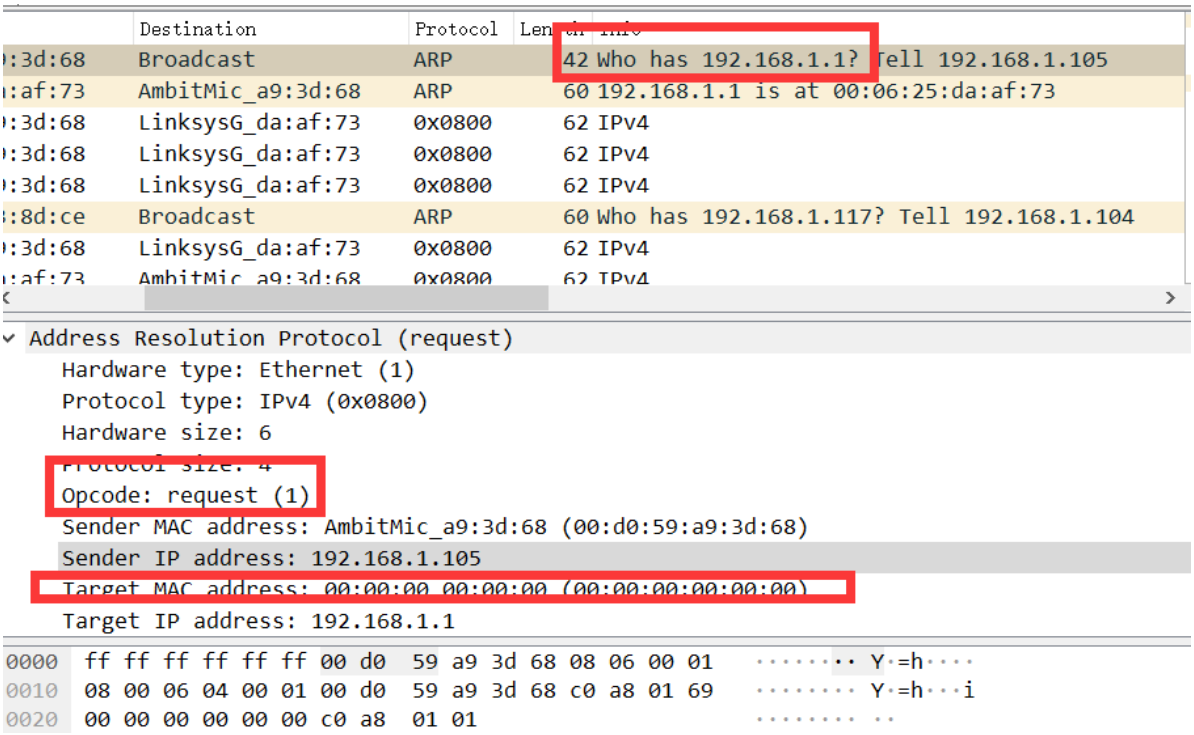
12.
c) Does the ARP message contain the IP address of the sender?

包含,如图:192.168.1.105



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

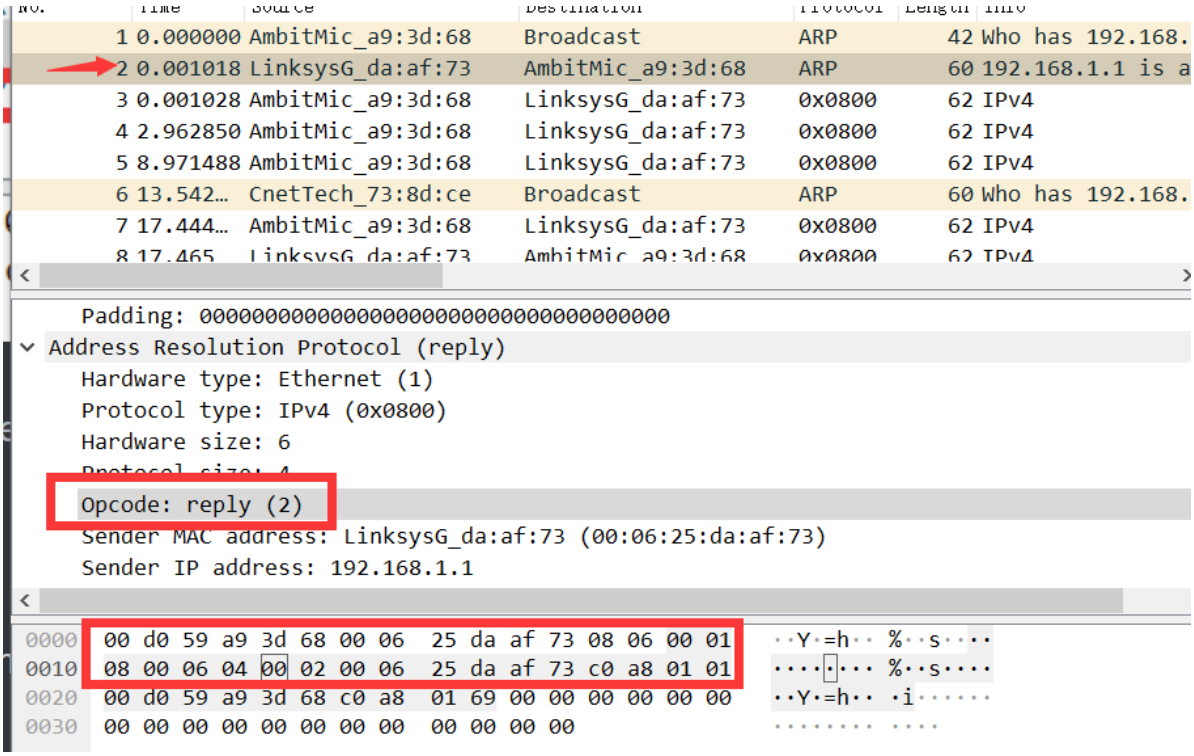
如图,操作数为1代表是询问MAC地址.同时info栏有问题"Who has 192.168.1.1",且目标MAC为空.



13.

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

21字节.

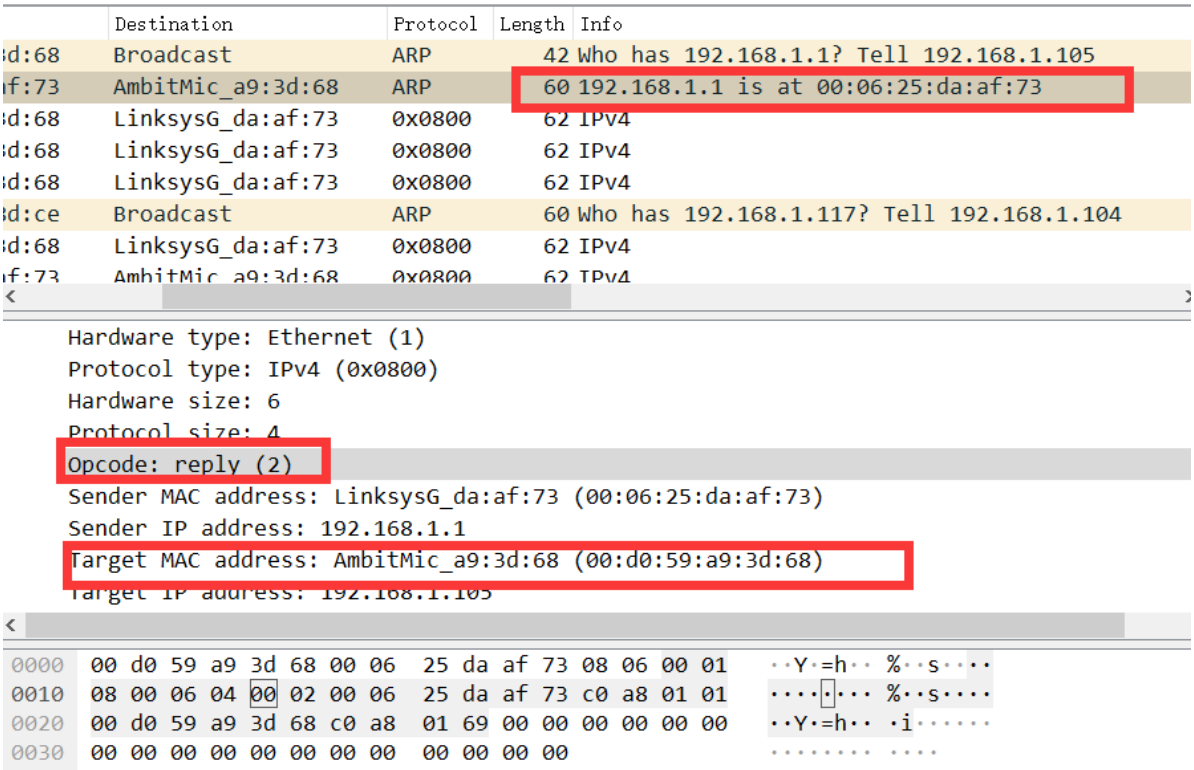


13.b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

由a)中图可以知道opcode = 2.

13.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?

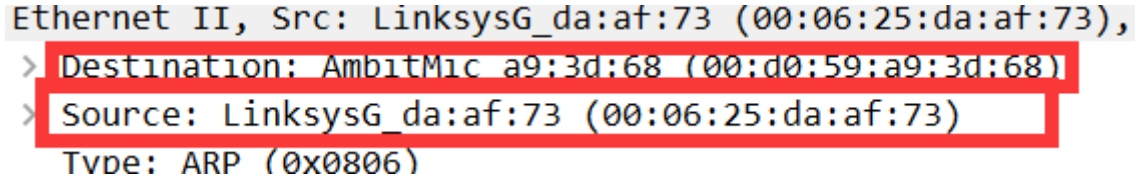
如图,info栏有:"192.168.1.1 is at 00:06:25:da:af:73",操作数为2,且有Target MAC address.



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

source:00:06:25:da:af:73

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



15.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?

因为获取目标地址是广播的.但是回复仅仅传回进行询问的主机.

EX-1. The arp command

如果按照题目所说,那么在添加了正确IP地址而错误的MAC地址后,尝试ping该ip地址将会无法连接(超时).这是因为链路层无法对该信息进行正确传输导致的.由于需要高级权限,本题无法实验.

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.

我们查询相应的Windows操作系统文档,发现似乎并没有默认的有效时间.但是找到论一个计算公式如下图.

在 Vista TCP/IP 堆栈Windows中，当邻接缓存中不存在匹配的条目时，主机将创建邻接缓存条目。 IPv4 的 ARP 缓存条目是邻接缓存条目的一个示例。 在邻接缓存中成功创建条目后，如果条目满足特定条件，该条目可能会更改为"Reachable"状态。 如果条目为"Reachable"状态，Windows Vista TCP/IP 主机不会向网络发送 ARP 请求。 因此，Windows Vista TCP/IP 主机使用缓存中的信息。 如果未使用条目，并且其保持"可到达"状态的时间超过其"可到达时间"值，则条目将更改为"过时"状态。 如果某个条目的状态为"过时"，vista TCP/IP Windows必须发送 ARP 请求以到达该目标。

"Reachable Time"值的计算公式如下：

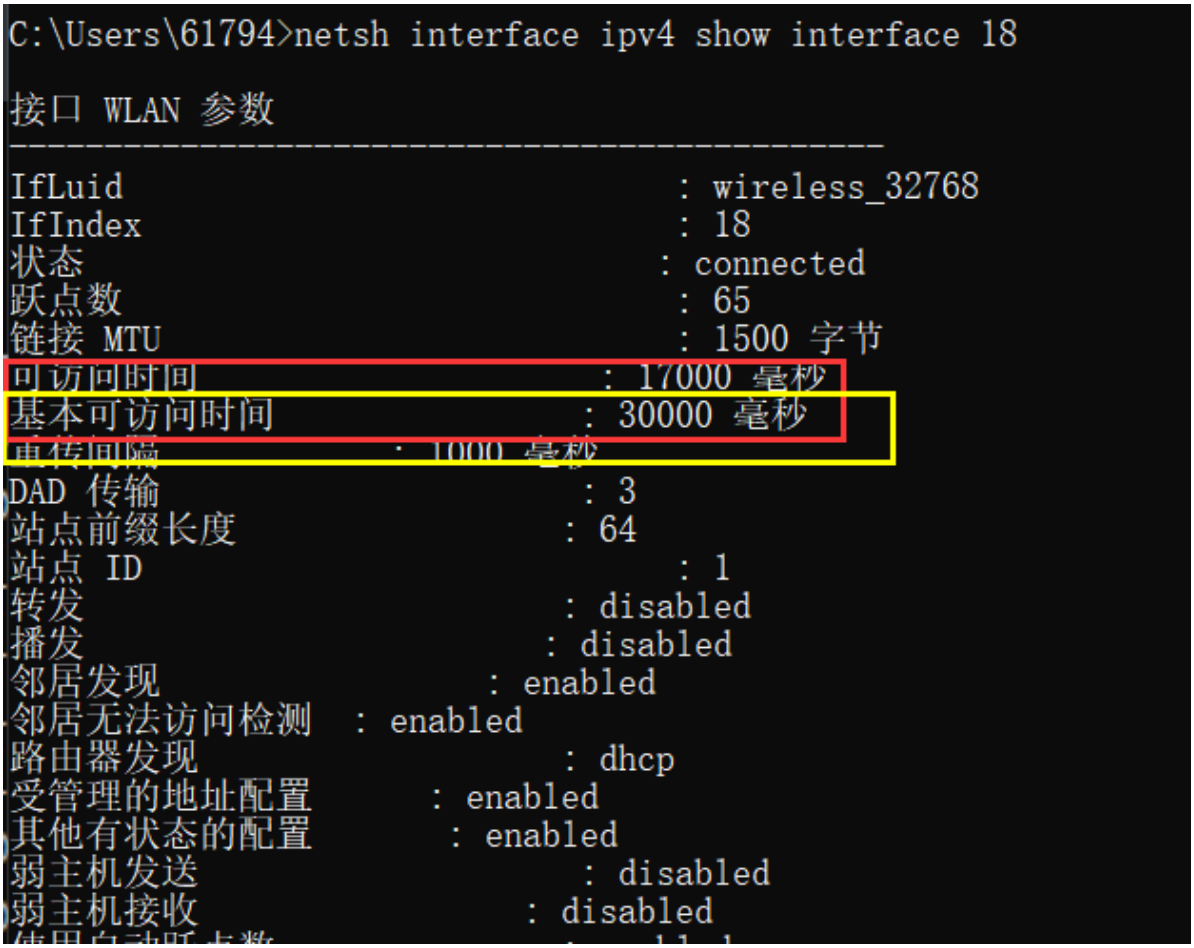
Reachable Time = BaseReachable Time × (A random value between MIN_RANDOM_FACTOR and MAX_RANDOM_FACTOR)

RFC 提供以下计算结果。

BaseReachable 时间	30，000 毫秒 (毫秒)
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) 到 45 秒之间 (30 × 1.5 秒) 。 如果某个条目在 15 到 45 秒之间没有使用，它将进入"过时"状态。 然后，当向目标发送任何 IP 数据报时，主机必须将 IPV4 的 ARP 请求发送到网络。

查看本电脑ARP地址缓存保存时间可以得到:



实验收获

本次实验学习并巩固了ARP,以太网相关的链路层知识,同时学习了实践层面如何对计算机发出的MAC请求和回复帧进行抓包,在附加实验中了解到了更多知识,收益匪浅.