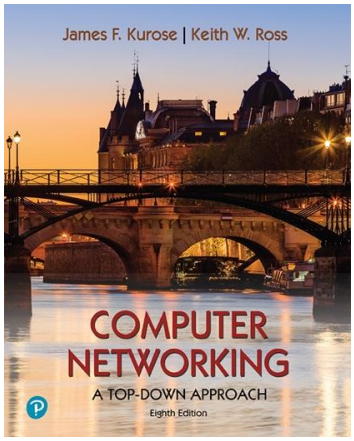
Wireshark Lab:
Ethernet and ARP v8.0

Supplement to *Computer Networking: A Top-Down Approach, 8th ed.*, J.F. Kurose and K.W. Ross



"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

---

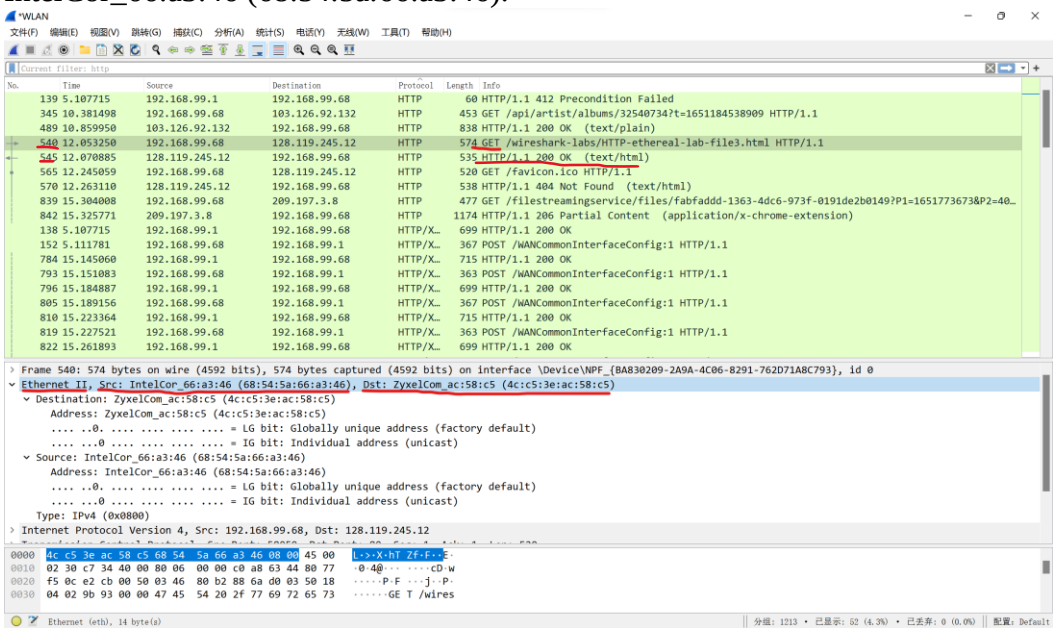
0. Academic integrity

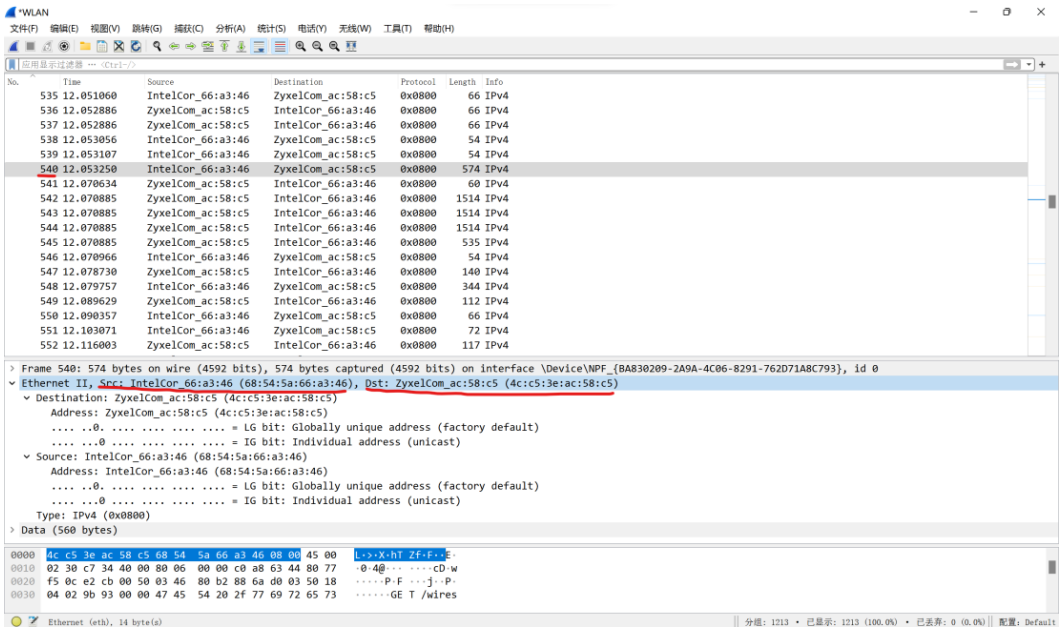
I have read and understood the course academic integrity policy.

1. Capturing and analyzing Ethernet frames

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

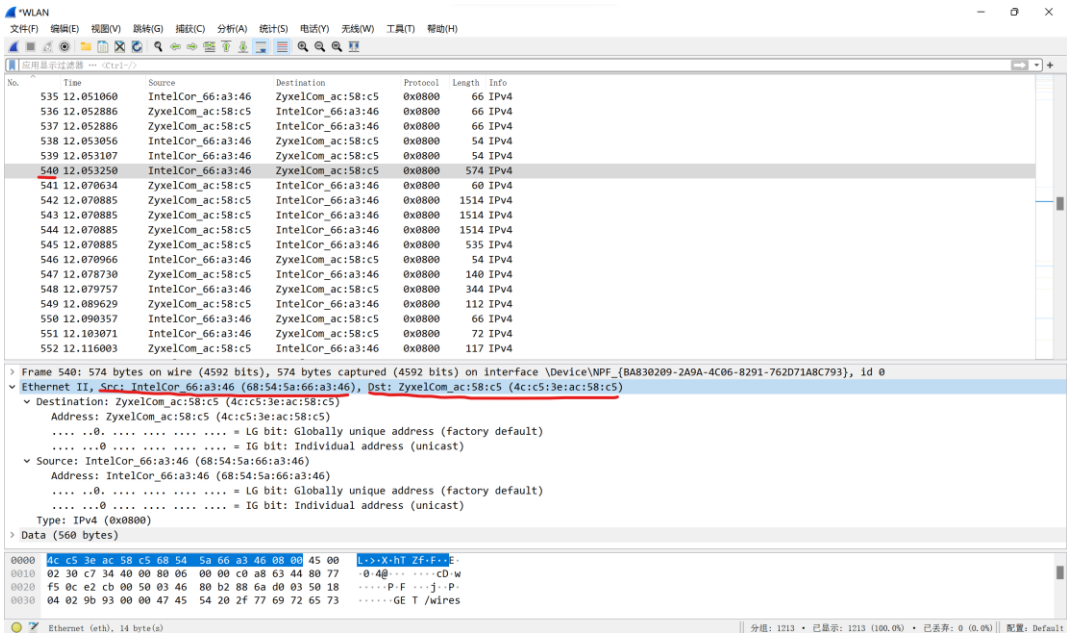
   IntelCor_66:a3:46 (68:54:5a:66:a3:46).





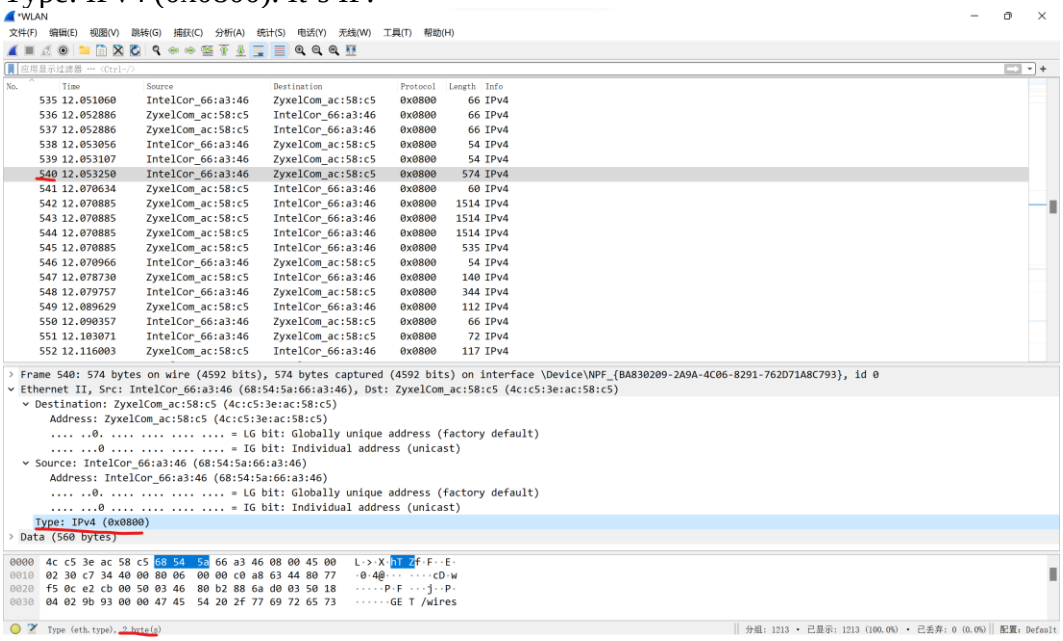
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]?

   ZyxelCom_ac:58:c5 (4c:c5:3e:ac:58:c5). No, it isn't, it's an adjacent router's address.



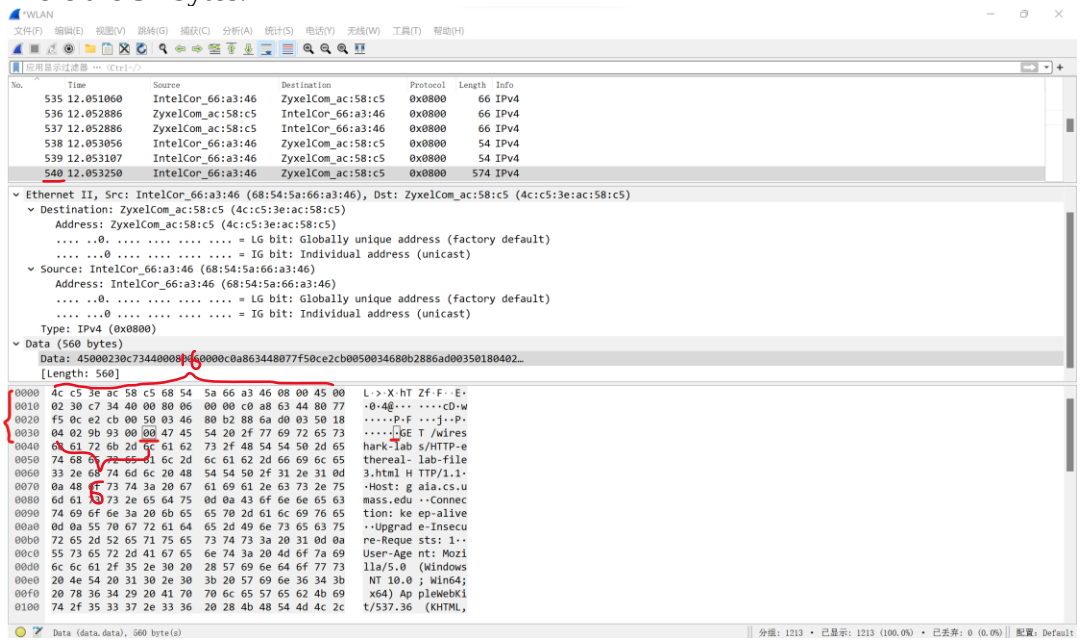
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

Type: IPv4 (0x0800). It’s IP.



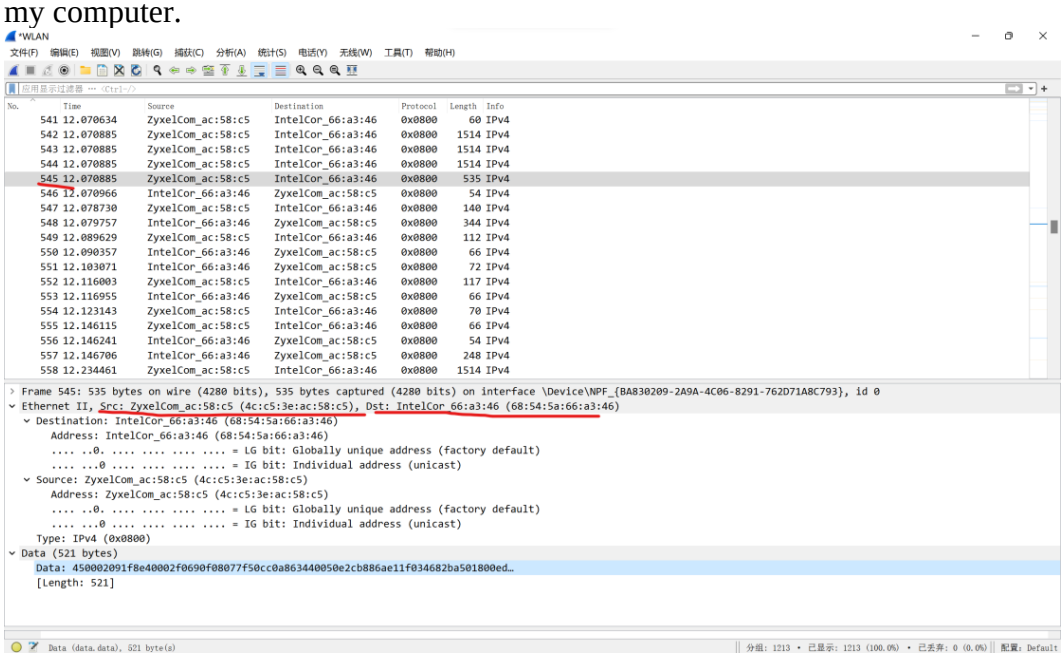
4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

There are 54 bytes.



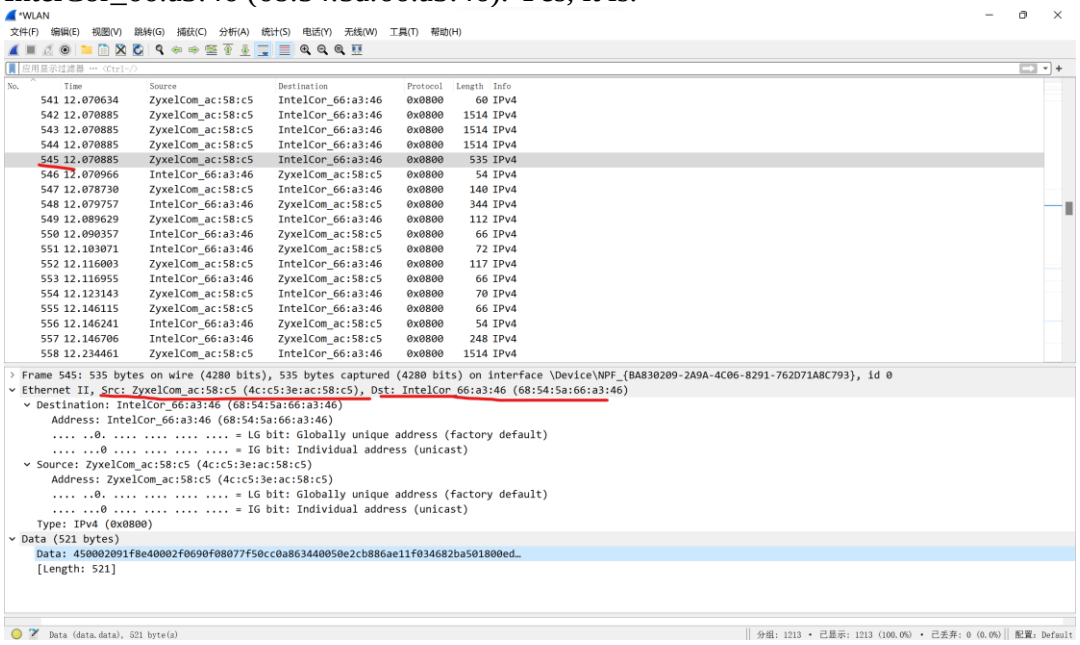
5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

ZyxelCom_ac:58:c5 (4c:c5:3e:ac:58:c5). It’s an adjacent router’s address, near my computer.



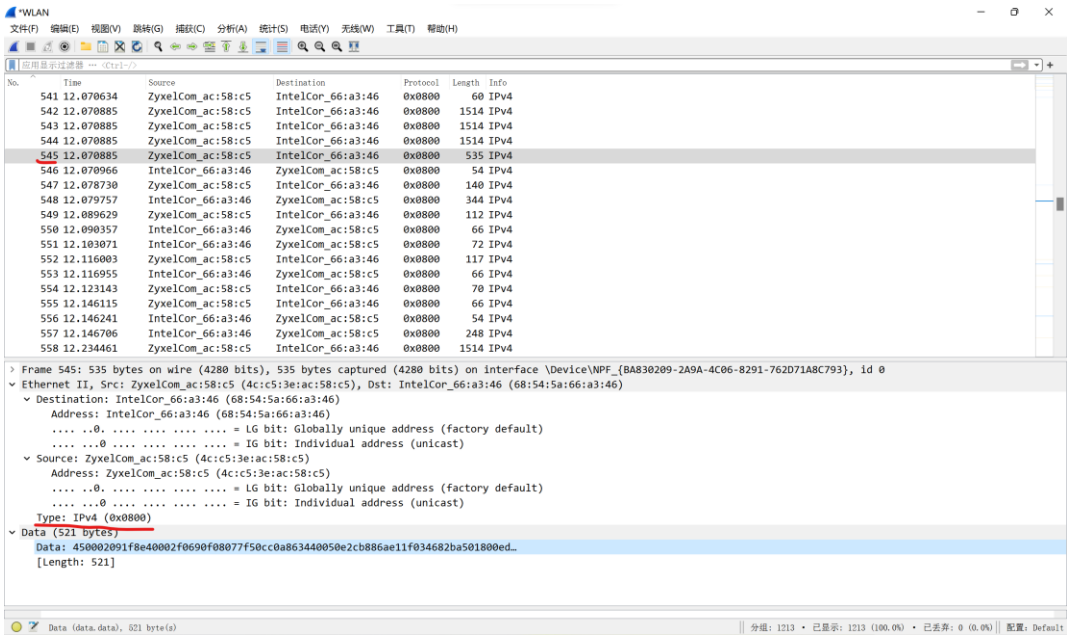
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

IntelCor_66:a3:46 (68:54:5a:66:a3:46). Yes, it is.



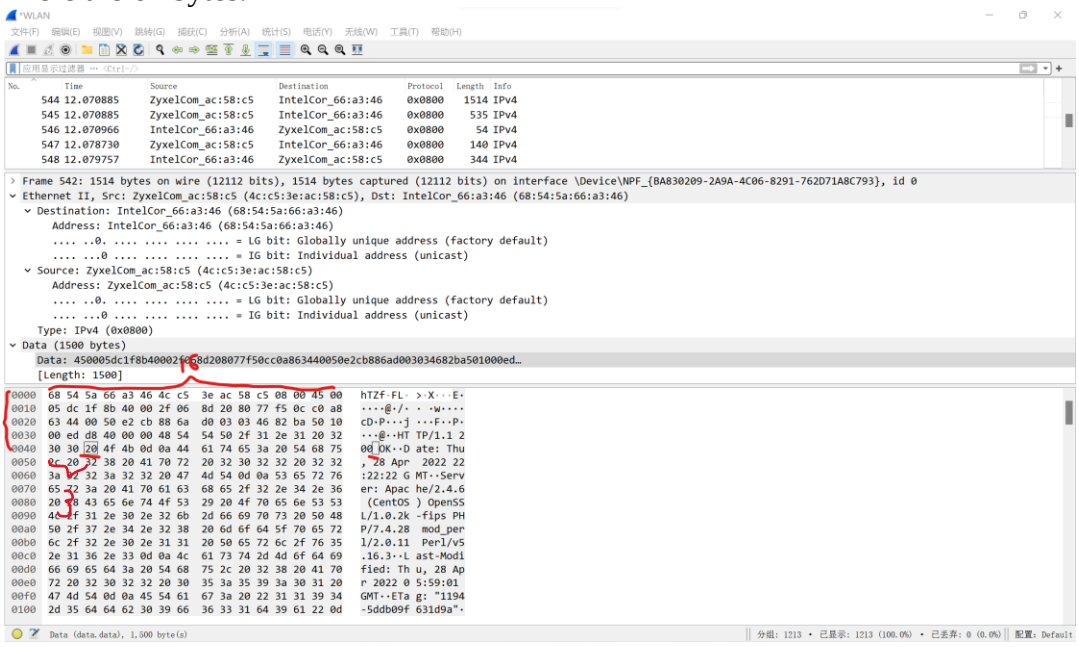
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

Type: IPv4 (0x0800). It’s IP.



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?

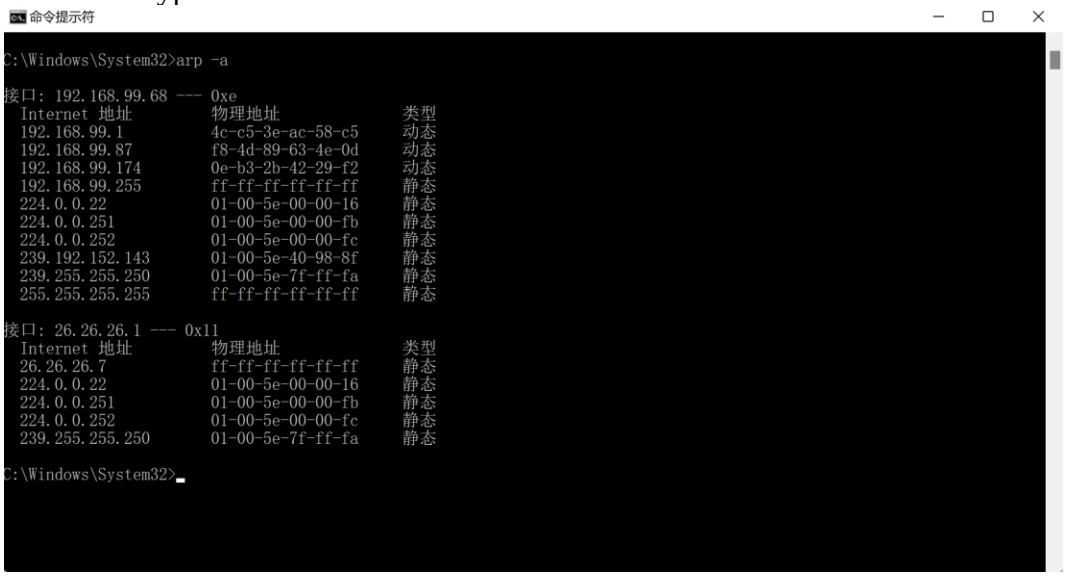
There are 67 bytes.



2. The Address Resolution Protocol

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

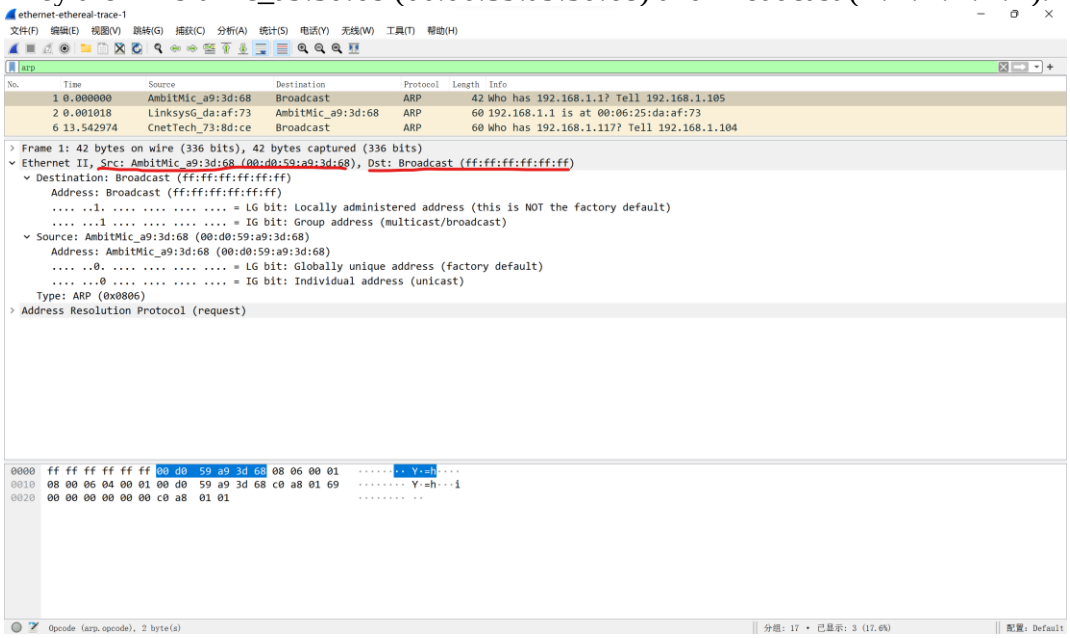
The first column is IP address, the second column is MAC address and the third column is Type.



(The following answers are based on the pre-captured trace in Question 15)

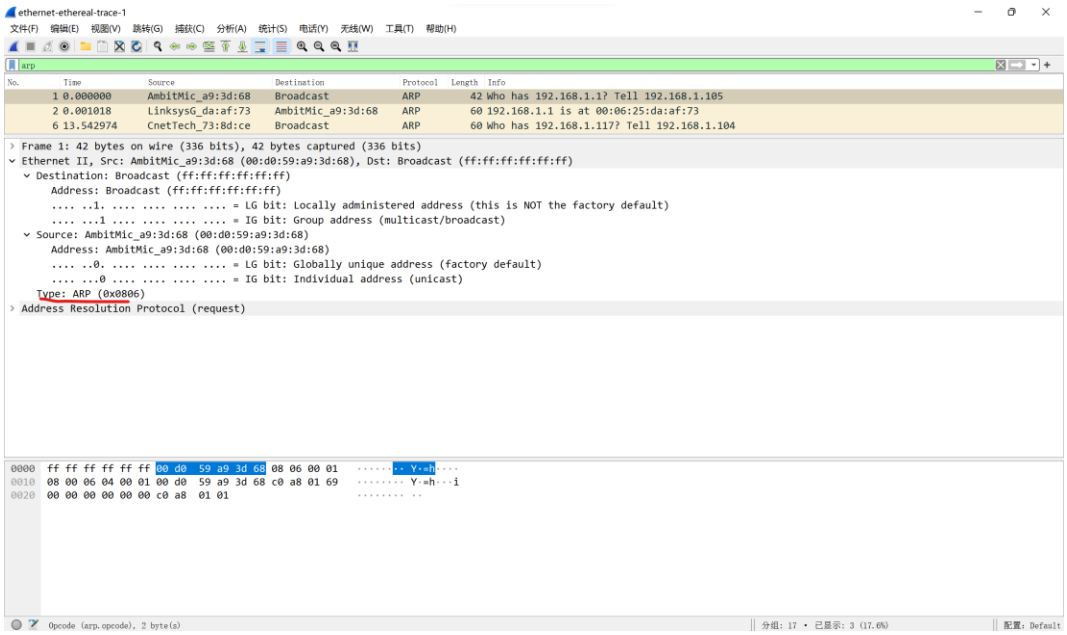
10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

They are AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) and Broadcast (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?

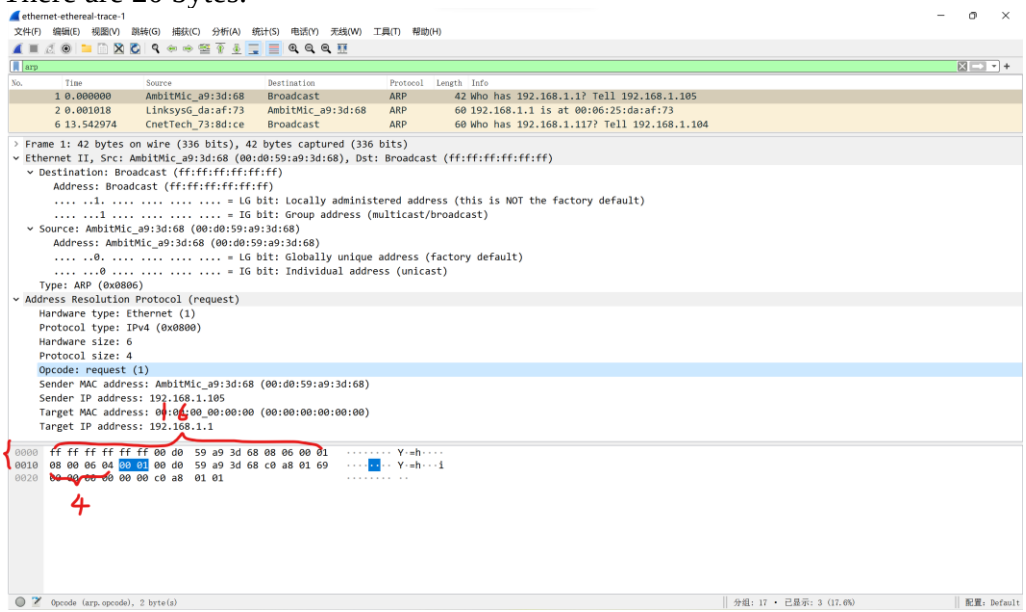
Type: ARP (0x0806). It’s ARP.



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.

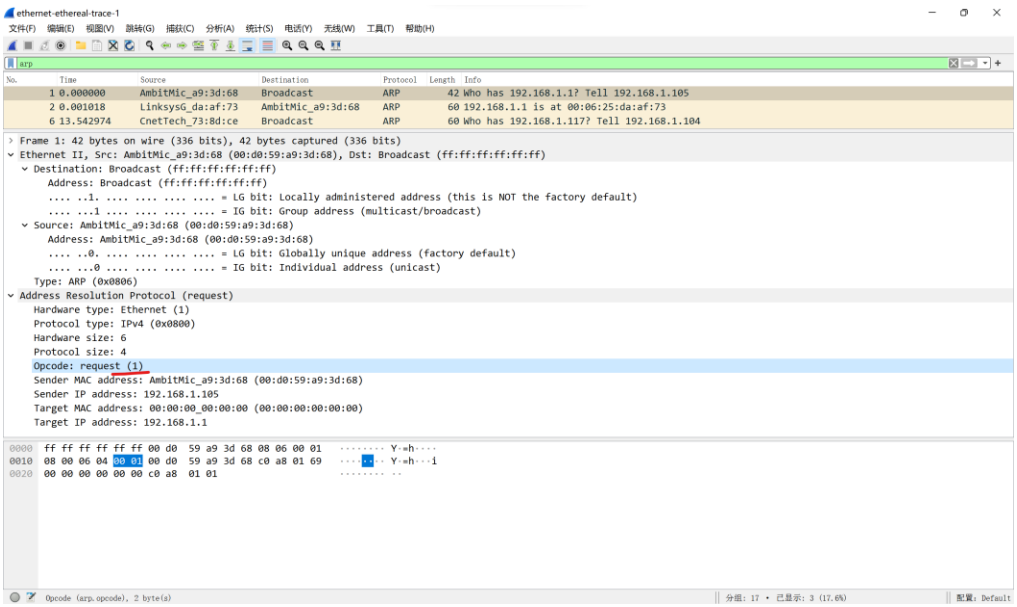
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

There are 20 bytes.



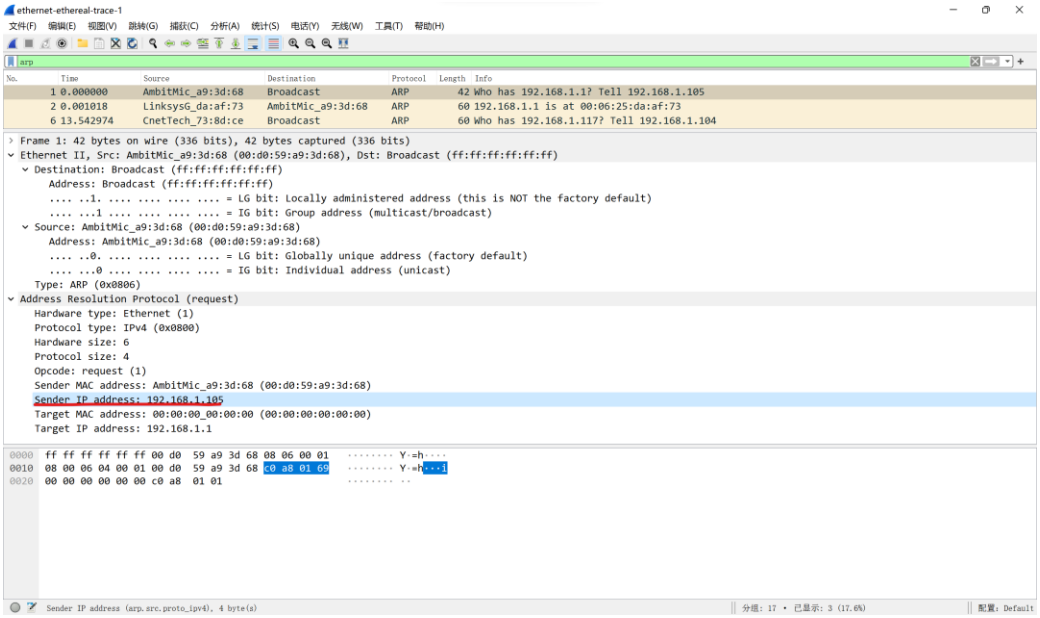
b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

It’s 1.



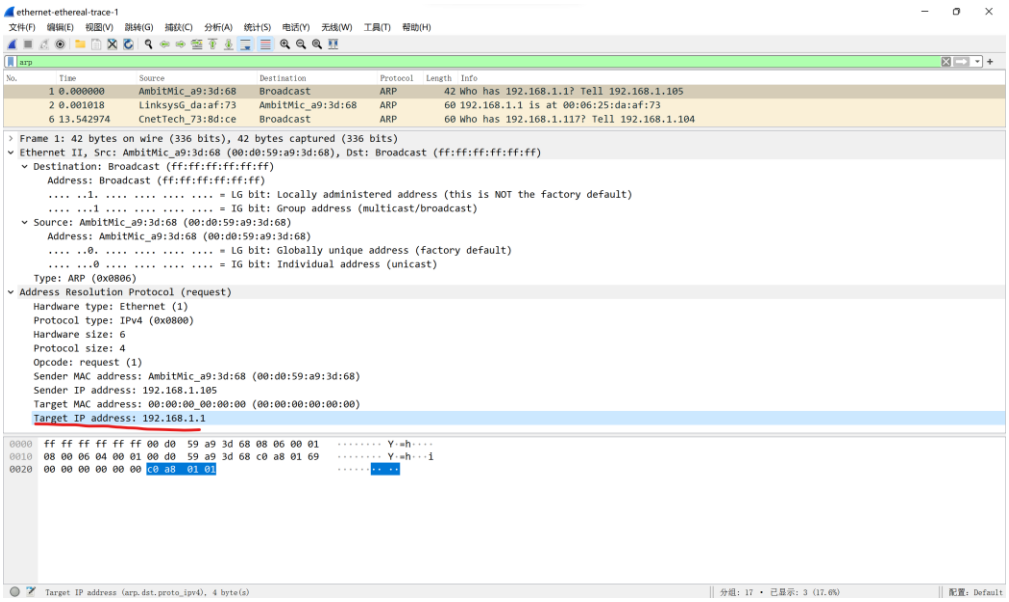
c) Does the ARP message contain the IP address of the sender?

Yes.



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

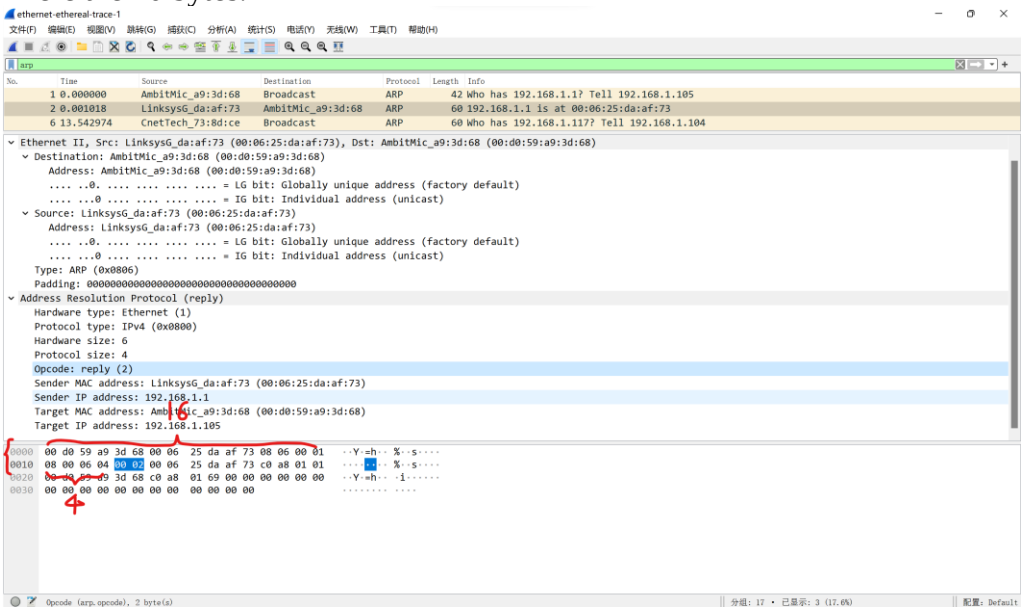
It’s the Target IP address.



13. Now find the ARP reply that was sent in response to the ARP request.

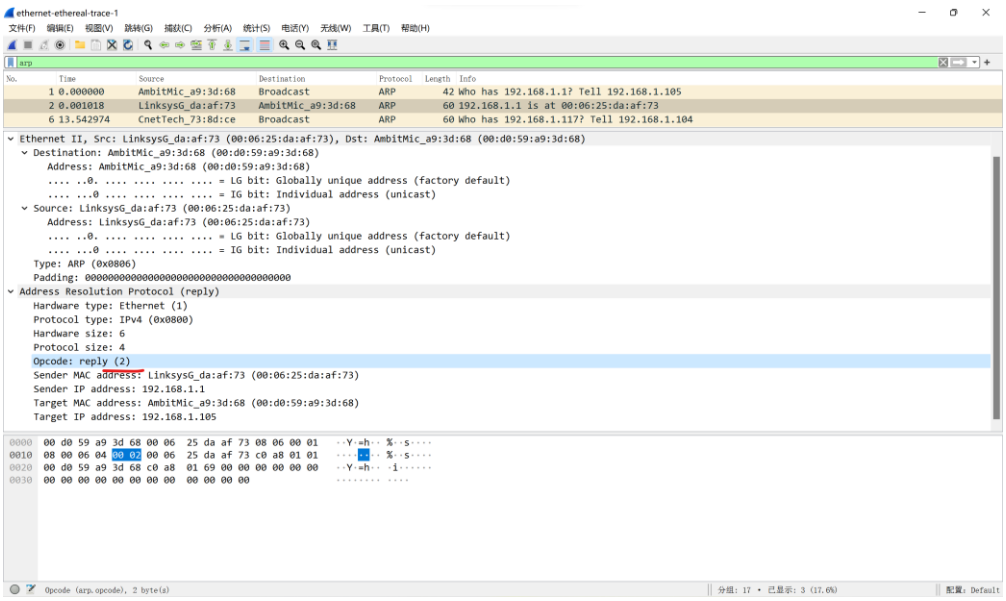
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

There are 20 bytes.



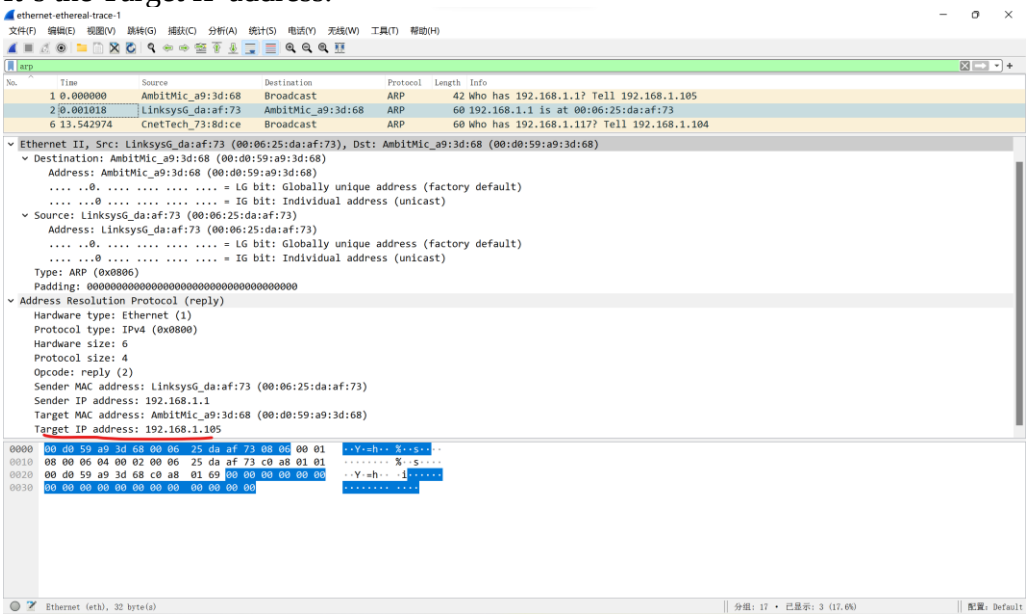
b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

It’s 2.



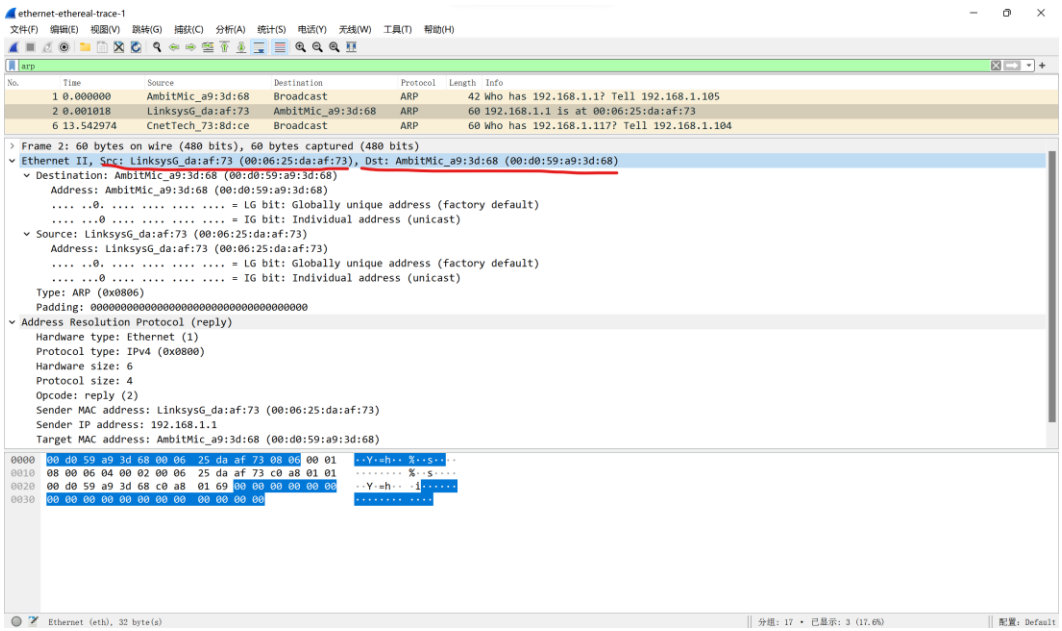
c) Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

It’s the Target IP address.



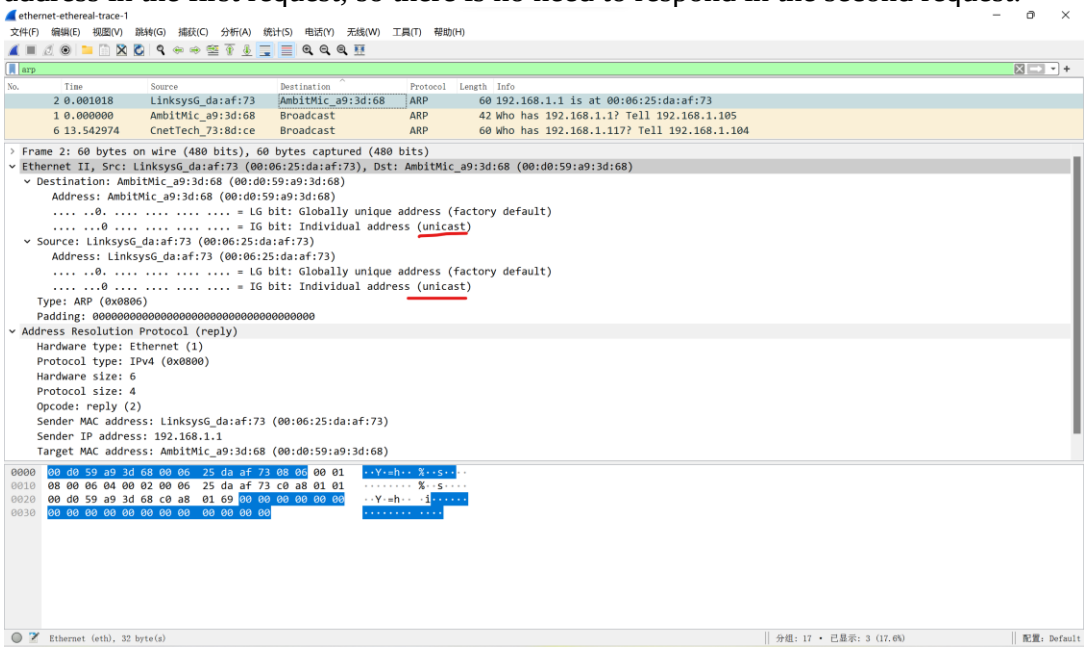
14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

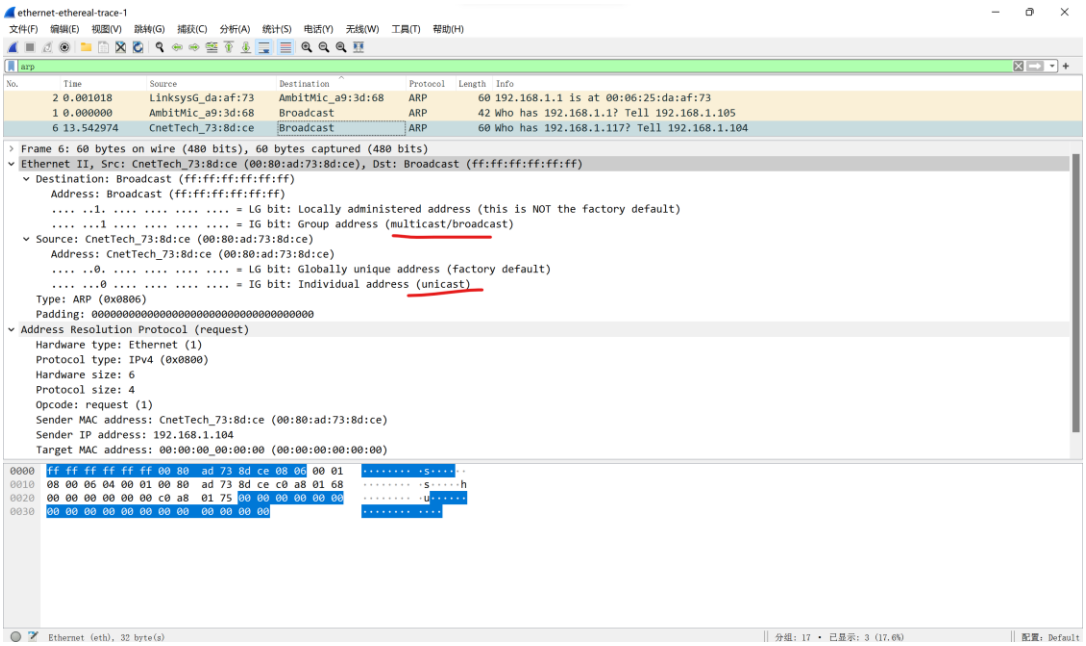
They are LinksysG_da:af:73 (00:06:25:da:af:73) and AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68).



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

    Probably because the nearest router has already recorded the corresponding address in the first request, so there is no need to respond in the second request.




ethernet-ethereal-trace-1
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)
arp
No. Time Source Destination Protocol Length Info
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
1 0.000000 AmbitMic_a9:3d:68 Broadcast ARP 42 Who has 192.168.1.1? Tell 192.168.1.105
6 13.542974 CnetTech_73:8d:ce Broadcast ARP 60 Who has 192.168.1.117? Tell 192.168.1.104
Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
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)
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)
Source: CnetTech_73:8d:ce (00:80:ad:73:8d:ce)
Address: CnetTech_73:8d:ce (00:80:ad:73:8d:ce)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: ARP (0x0806)
Padding: 00000000000000000000000000000000000000
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)
0000 ff ff ff ff ff ff 00 80 ad 73 8d ce 08 06 00 01
0010 08 00 06 04 00 01 00 80 ad 73 8d ce c0 a8 01 68
0020 00 00 00 00 00 00 c0 a8 01 75 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00
Ethernet (eth), 32 byte(s)
分组: 17 • 已显示: 3 (17.6%)
配置: Default