Vlad Predovic

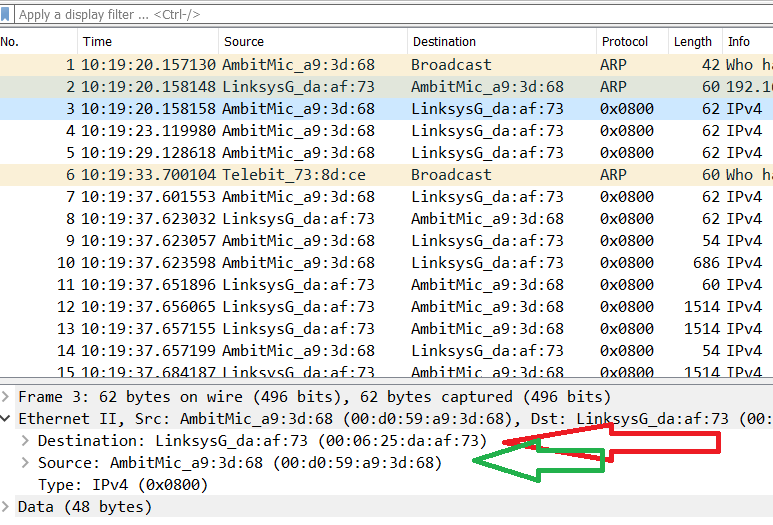
CS 372  
Summer 2016

Lab 4: Wireshark Lab: Ethernet and ARP

*NOTE: Used ethernet-ethereal-trace-1 for homework*

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

Address: 00:d0:59:a9:3d:68 (green arrow)



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.]

Address: 00:06:25da:af:73 , it is the address of the router, used to get out of the internal network. (subnet?)

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

Hex value: 0x0800, The IP protocol

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

It appears after 52 bytes.

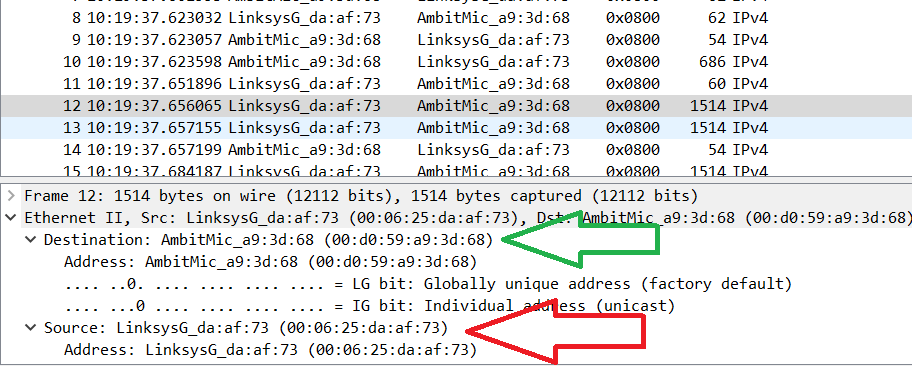
Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

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?

Address: 00:06:25da:af:73 , it is the address of the router, used to get out of the internal network.

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

The destination address is 00:d0:59:a9:3d:68 (my computer)



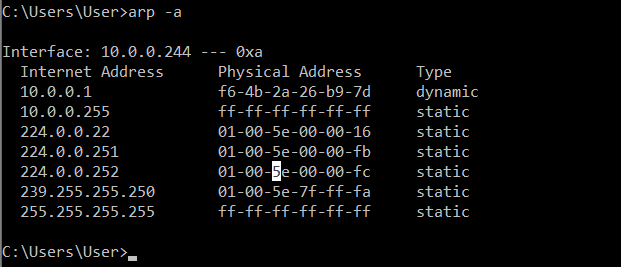
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

Hex value: 0x0800, The IP protocol

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?

52 Bytes into the frame.

9. Write down the contents of your computer’s ARP cache. What is the meaning of each column value? *NOTE: THIS QUESTION WAS DONE USING MY PC*



Internet Address: IP address

Physical Address: MAC address

Type: Protocol type

Answer the following questions:

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

Source Address (hex): 00:d0:59:a9:3d:68

Destination Address(hex): 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?

Value: ARP (0x0806) Corresponds to ARP protocol.

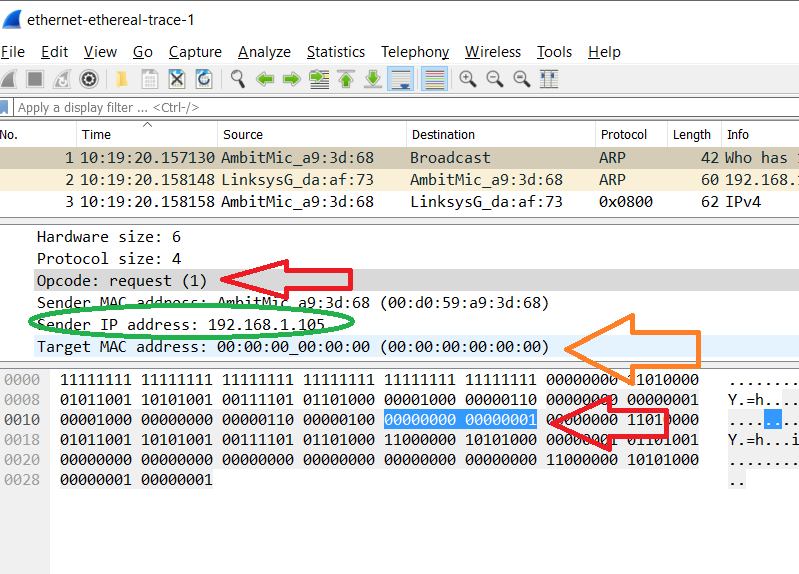


12. Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.

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

--20 bytes from beginning of frame

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?



The value is 0x0001 as noted above by the red arrows.

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

Yes it does as noted by the green circle above, 192.168.1.105

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

It would appear in the target in the target MAC 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?

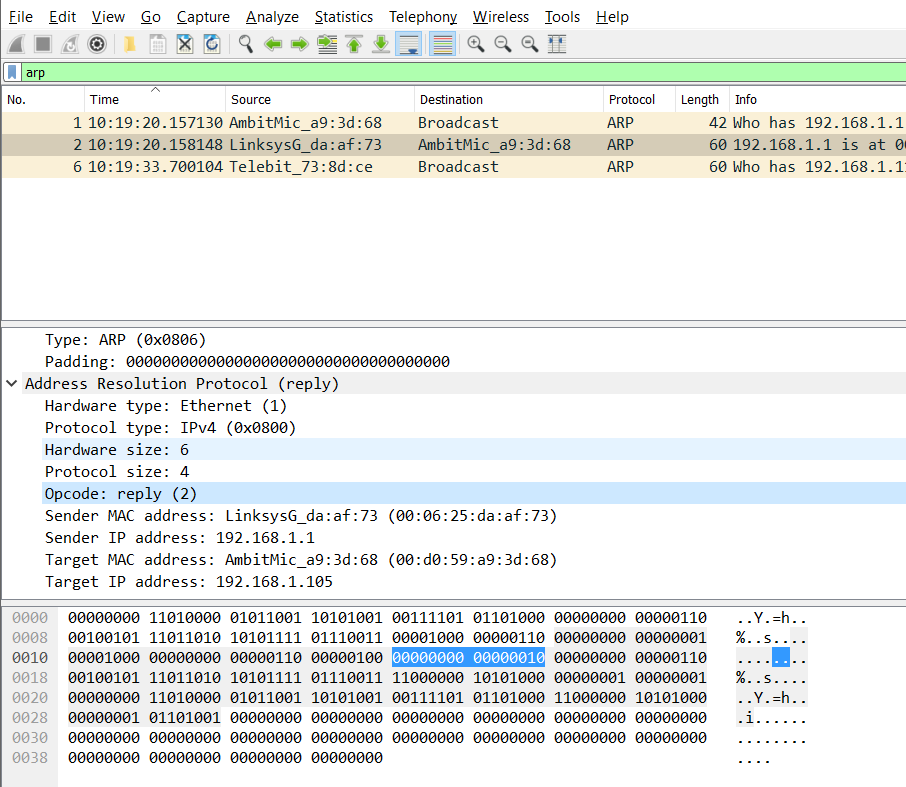
Again, 20 bytes from the beginning of the ethernet frame.

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?

The value is (2) which is the designated value for a reply.

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?

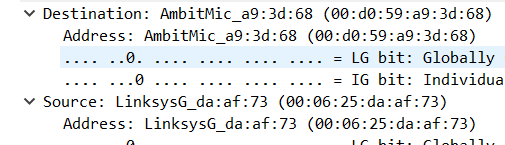
It appears under sender MAC address.



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. 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?

AS seen in the picture above question 14, the third request is a broadcast. Therefore, when the reply Is sent, it goes directly to that machine. Because that is not the computer I am on, the packet sniffer running on our machine does not pick up the response.