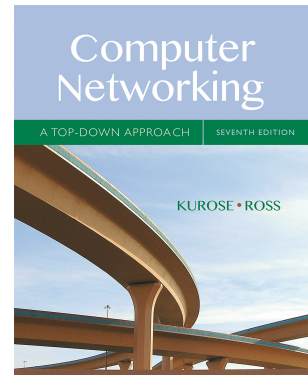


Wireshark Lab: Ethernet & ARP **SOLUTION**

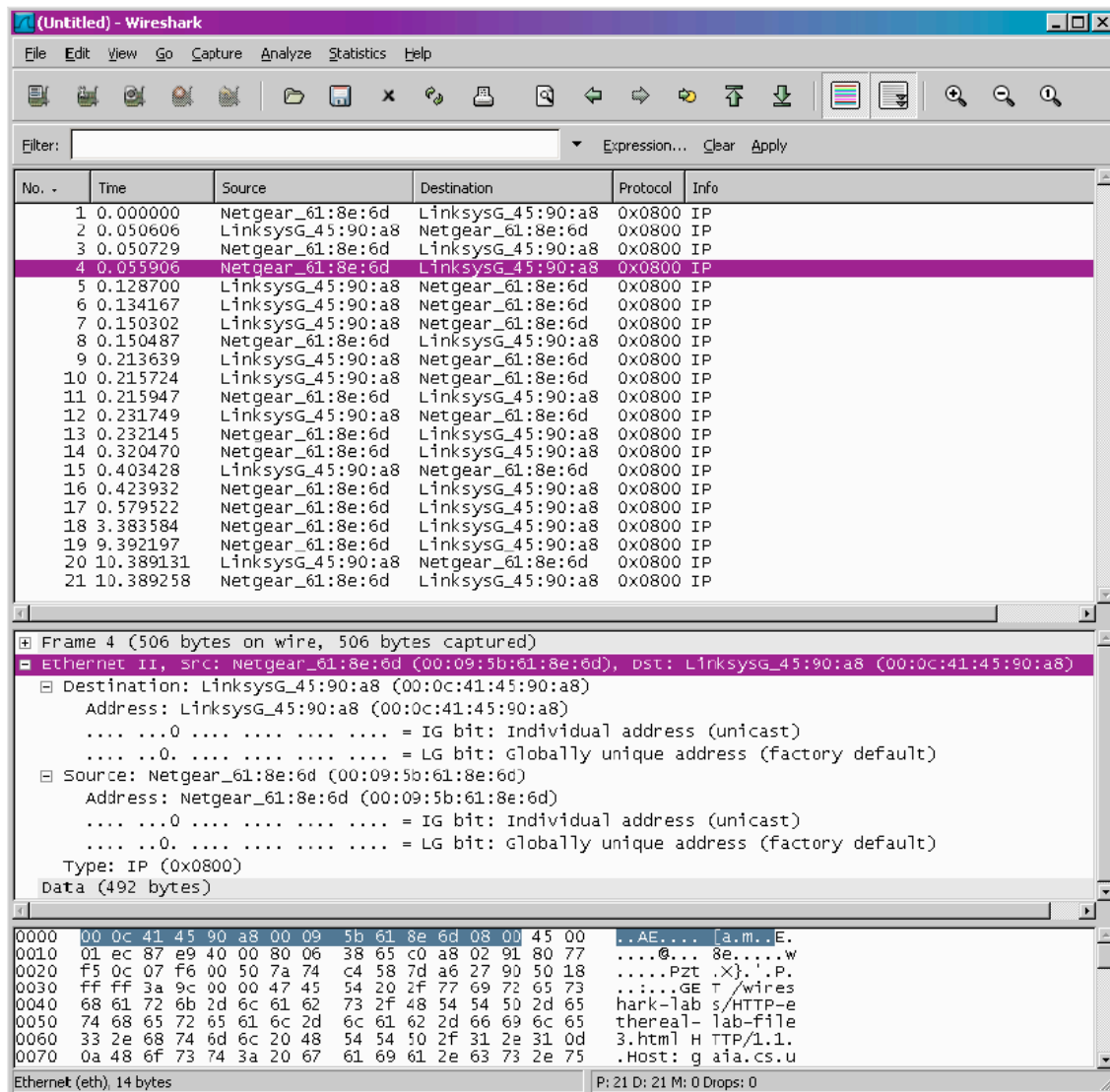
Supplement to *Computer Networking: A Top-Down Approach*, 7th ed., J.F. Kurose and K.W. Ross

© 2005-2016, J.F Kurose and K.W. Ross, All Rights Reserved



The solutions below are based on the trace file *ethernet--ethereal-trace-1* in the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> .

Shown below is the screen shot expanding the view of the Ethernet frame carrying the HTTP GET:

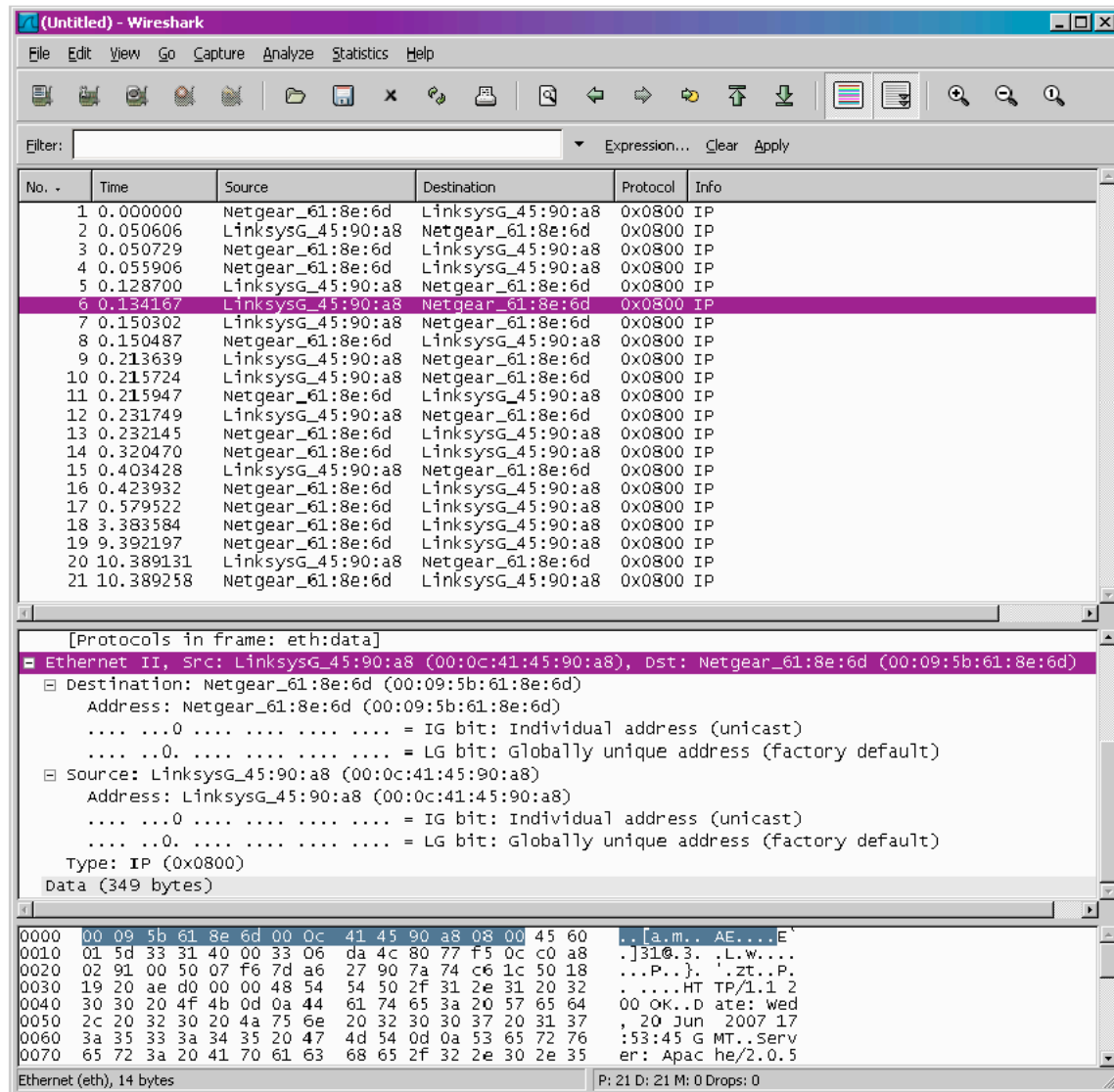


1. What is the 48-bit Ethernet address of your computer? *The Ethernet address of my computer is 00:09:5b:61:8e:6d*
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [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.] *The destination address 00:0c:41:45:90:a8 is not the Ethernet address of gaia.cs.umass.edu. It is the address of my Linksys router, which is the link used to get off the subnet.*
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to? *The hex value for the Frame type field is 0x0800. This corresponds to the IP protocol (the frame type field indicates that the next layer above IP – the layer to which the payload of this Ethernet frame will*

be passed – is IP.

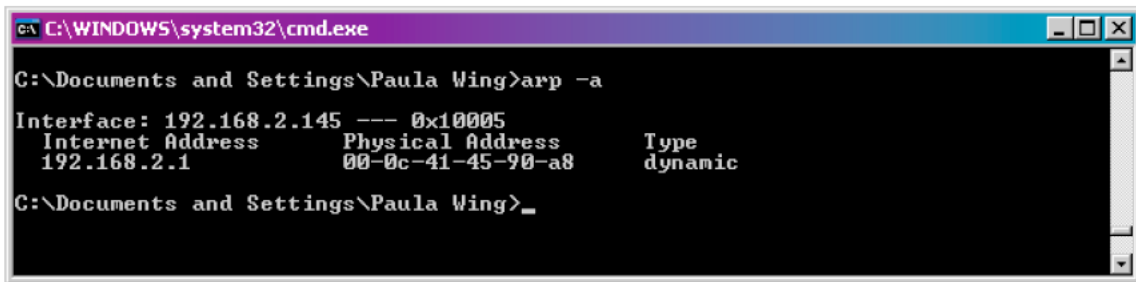
- How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame? *The ASCII “G” appears 52 bytes from the start of the Ethernet frame. There are 14 B Ethernet frame, and then 20 bytes of IP header followed by 20 bytes of TCP header before the HTTP data is encountered.*

Here is a screenshot of the Ethernet frame containing the HTTP OK response:



- 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? *The source address 00:0c:41:45:90:a8 is neither the Ethernet address of gaia.cs.umass.edu nor the address of my computer. It is the address of my Linksys router, which is the link used to get onto my subnet.*

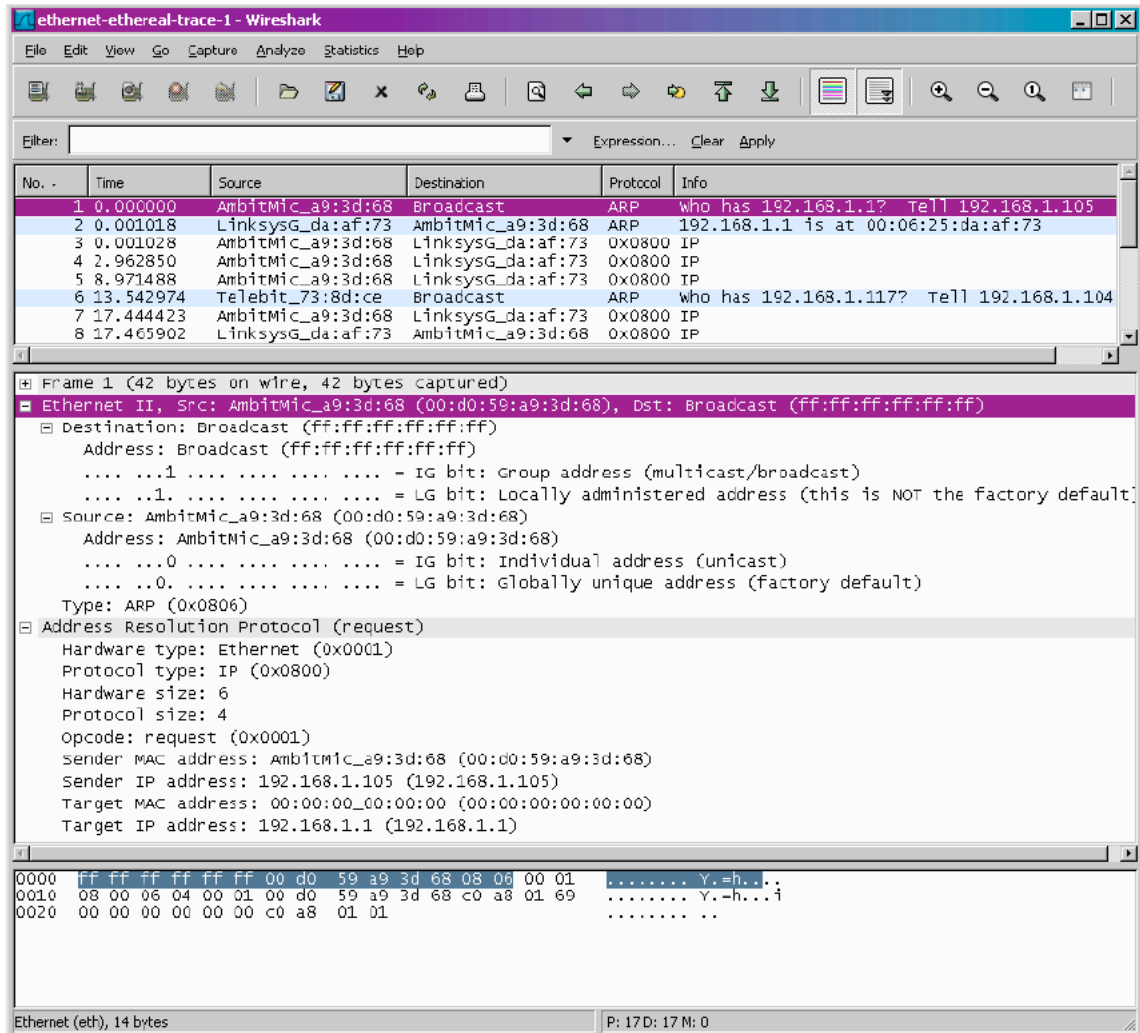
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer? *The destination address 00:09:5b:61:8e:6d is the address of my computer.*
7. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field? *The hex value for the Frame type field is 0x0800. This value corresponds to the IP protocol (see also answer to 3. above).*
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? *The ASCII “O” appears 52 bytes from the start of the Ethernet frame. Again, there are 14 bytes of Ethernet frame, and then 20 bytes of IP header followed by 20 bytes of TCP header before the HTTP data is encountered.*



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Paula Wing>arp -a
Interface: 192.168.2.145 --- 0x10005
Internet Address      Physical Address      Type
192.168.2.1           00-0c-41-45-90-a8     dynamic
C:\Documents and Settings\Paula Wing>
```

9. Write down the contents of your computer’s ARP cache. What is the meaning of each column value? *The Internet Address column contains the IP address, the Physical Address column contains the MAC address, and the type indicates the protocol type.*

Here is a screenshot showing the ARP request message:

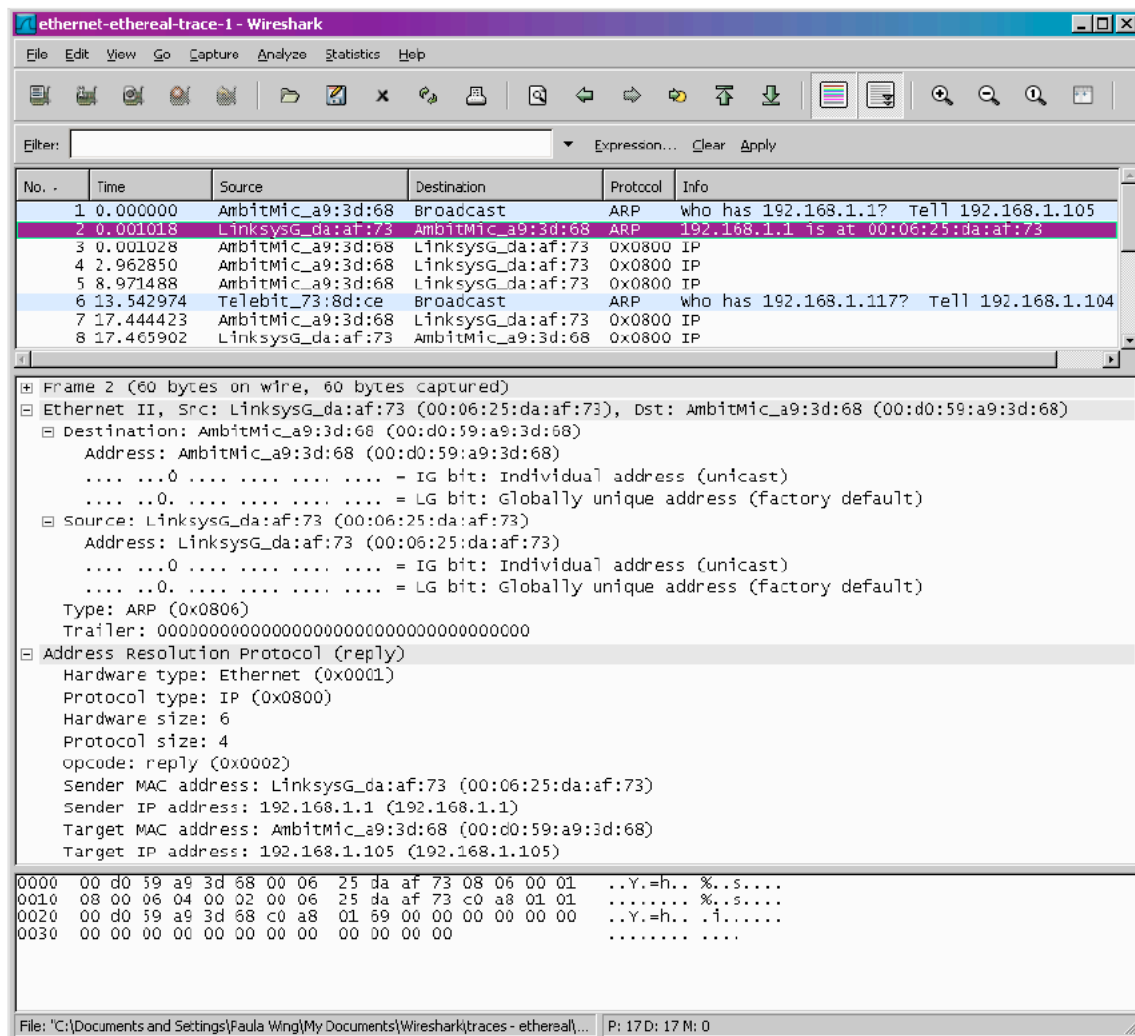


10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message? *The hex value for the source address is 00:d0:59:a9:3d:68. The hex value for the destination address is ff:ff:ff:ff:ff:ff, the broadcast address.*
11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What do the bit(s) whose value is 1 mean within the flag field? The hex value for the Ethernet Frame type field is 0x0806, for ARP.
12. Download the ARP specification from <ftp://ftp.rfc-editor.org/innotes/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? *The ARP opcode field begins 20 bytes from the very 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 request is made? *The hex value for*

opcode field within the ARP-payload of the request is 0x0001, for request.

- c) Does the ARP message contain the IP address of the sender? Yes, the ARP message containing the IP address 192.168.1.105 for 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? The field “Target MAC address” is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.1.1) is being queried.

Here is the screenshot for the ARP reply message:



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? The ARP opcode field begins 20 bytes from the very 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 hex value for

opcode field withing the ARP-payload of the request is 0x0002, for 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? *The answer to the earlier ARP request appears in the “Sender MAC address” field, which contains the Ethernet address 00:06:25:da:af:73 for the sender with IP address 192.168.1.1.*

14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message? *The hex value for the source address is 00:06:25:da:af:73 and for the destination is 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? *There is no reply in this trace, because we are not at the machine that sent the request. The ARP request is broadcast, but the ARP reply is sent back directly to the sender’s Ethernet address.*