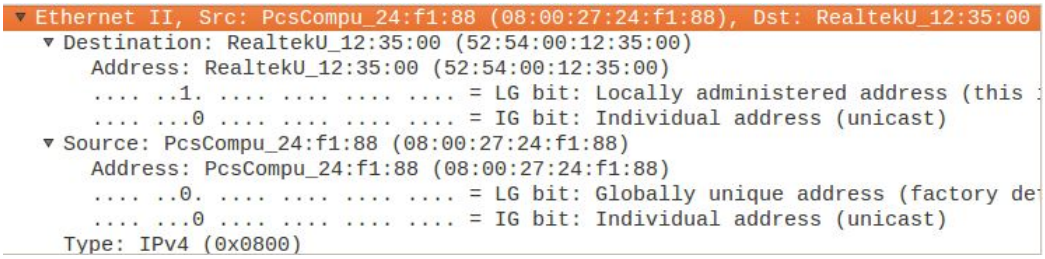
CPS 706 - Wireshark Ethernet ARP



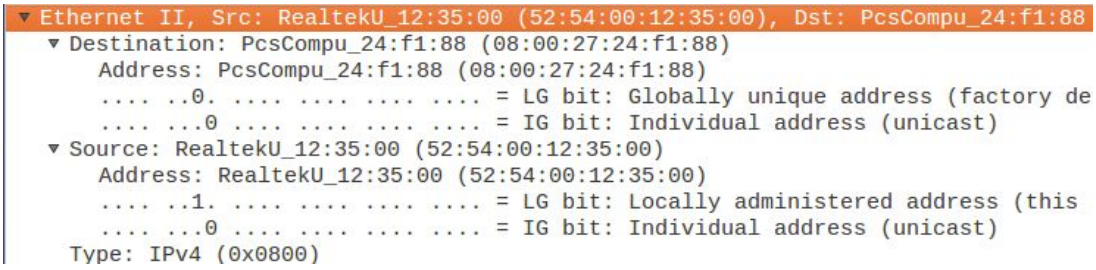
1. *What is the 48-bit Ethernet address of your computer?*
    - 08:00:27:24:f1:88

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?*
    - 52:54:00:12:35:00 (not the ethernet address of gaia.cs.umass.edu)
    - It's the address of Realtek router which connect my home network subnet to ISP

3. *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 of for frame type field is 0x0800
    - It means that the frame has IP protocol type

4. *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 55 bytes from the start of the ethernet frame
    - There are 14 bytes of Ethernet, 20 bytes of IP and 20 bytes of TCP

5. *What is the hexadecimal value of the CRC field in this Ethernet frame?*
    - There is no hexadecimal value of CRC field in ethernet frame



6. *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?*
    - 52:54:00:12:35:00
    - It's not the ethernet address of gaia.cs.umass.edu
    - It's the address of Realtek router which connect ISP to my home network subnet

7. *What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?*
    - 08:00:27:24:f1:88
    - It is the address of my computer

8. *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 of for frame type field is 0x0800
    - It means that the frame has IP protocol type

9. *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 "G" appears 549 bytes from the start of the ethernet frame
    - There are 14 bytes of Ethernet, 20 bytes of IP, 20 bytes of TCP, 481 bytes TCP data, 13 bytes HTTP

10. *What is the hexadecimal value of the CRC field in this Ethernet frame*
    - There is no hexadecimal value of CRC field in ethernet frame

```
3/23/20]seed@VM:~$ arp -a
(10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
(10.0.2.3) at 08:00:27:6f:d1:29 [ether] on enp0s3
```

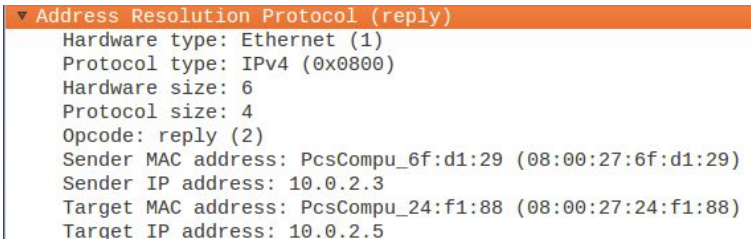
11. *Write down the contents of your computer's ARP cache. What is the meaning of each column value?*
    - The first column represent IP address, the second column represent MAC, the last column represent protocol type

```
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: PcsCompu_24:f1:88 (08:00:27:24:f1:88)
    Sender IP address: 10.0.2.5
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.0.2.3
```

12. *What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?*
    - Source address: 08:00:27:24:f1:88 and Destination address: ff:ff:ff:ff:ff:ff

13. *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 of for frame type field is 0x0806
    - It means that the frame has ARP protocol type

14. *ARP specification*
    a. *How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?*
        - It begins 20 bytes after the beginning of 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?*
        - 0x0001
    c. *Does the ARP message contain the IP address of the sender?*
        - It does, 10.0.2.5
    d. *Where in the ARP request does the "question" appear - the Ethernet address of the machine whose corresponding IP address is being queried*
        - The question appear in the Target MAC address is set to 00:00:00:00:00:00 with the corresponding IP address (10.0.2.3) is being queried



15. *Find 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?*
        - *It begins 20 bytes after the beginning of 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*
        - *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?*
        - The answer appears in Sender MAC address field that is set to 08:00:27:6f:d1:29 with the IP address 10.0.2.3

16. *What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the IP APR reply message*
    - Hex value for source address: 08:00:27:6f:d1:29
    - Hex value for destination address: 08:00:27:24:f1:88

17. *Open the ethernet-ethereal trace. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running wireshark, and ARP reply sent to 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 part 6 - another ARP request. Why is there no ARP reply (sent in my request in packet 6) in the packet trace?*
    - There is no ARP reply in the packet trace because we don't have the Ethernet address of the machine that sent the request. ARP request is a broadcast, but ARP reply is sent back only to the sender's Ethernet address.