

Tu Lam

CS 372 Lab

March 6<sup>th</sup>, 2021

## Lab #3

### (ARP)

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

**Answer:** The 48-bit Ethernet address of my computer is  
**F8:DA:0C:75:C4:25.**

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.]*

**Answer:** The 48-bit destination address in the Ethernet frame is **8C:3B:AD:DF:C6:00** and this **is not the Ethernet address** of the gaia.cs.umass.edu. This address is my NetGear router address as the website is using this router to get onto my subnet.

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

**Answer:** The hexadecimal value for the two-byte Frame type field is **0x800**. The upper layer protocol this correspond to is the **IPv4** (Internet Protocol version 4).

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

**Answer:** The ASCII "G" in "GET" appear in the Ethernet frame hold **52** bytes from the very start. Before the "G" is 14 ethernet header + 20 IP header + 20 TCP header.

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?*

**Answer:** The source address value of the Ethernet is **8C:3B:AD:DF:C6:00**. This is **not** the address of my computer nor the gaia.cs.umass.edu, this is my router NetGear's address.

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

**Answer:** The destination address in the Ethernet frame is **F8:DA:0C:75:C4:25** and this is the Ethernet address of my computer.

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

**Answer:** The hexadecimal value is the same as answering in question #3 which is **0x800** and its upper layer protocol it belongs to is **IPv4**.

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?*

**Answer:** The number of bytes from the very start of the Ethernet frame that ASCII "O" in "OK" have **52** bytes. This follow again to what answer in question #4 is 14 ethernet header + 20 IP header + 20 TCP header before the "O".

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

**Answer:** Below is a picture of ARP cache look like from my computer:

```
C:\Users\Tu Lam>arp -a

Interface: 192.168.1.9 --- 0xb
Internet Address      Physical Address      Type
192.168.1.1           8c-3b-ad-df-c6-00    dynamic
192.168.1.2           94-f6-d6-1c-72-b4    dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff    static
224.0.0.2             01-00-5e-00-00-02    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

There are in total **3** column values. The first column is "**Internet Address**" containing the IP address, the second column is "**Physical Address**" containing the MAC address, and the last column is the "**Type**" containing which protocol is using.

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

**Answer:** The hexadecimal values for the source address is **F8:DA:0C:75:C4:25** & the destination address is **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?

**Answer:** The hexadecimal value for the two-type Ethernet Frame is **0x0806** and the upper layer protocol correspond to **ARP**.

**12.** *Download the ARP specification:*

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

**Answer:** The ARP opcode field begin with **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?*

**Answer:** The value of the opcode field within the ARP-payload part of the Ethernet frame is in hexadecimal of **0x0001**.

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

**Answer:** Yes, it does contain the IP address of the sender, the IP address is **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?*

**Answer:** The field "Target MAC address" is set to **00:00:00:00:00:00** to "question" the machine whose corresponding IP address of 192.168.1.1 is being queried.

**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?*

**Answer:** This is the same as answering question #12-part A that it has **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?*

**Answer:** The value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made is hexadecimal **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?*

**Answer:** The 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 when the "answer" in the ARP message.

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

**Answer:** The hexadecimal values for the **source address** for the frame containing the ARP message is **00:06:25:DA:AF:73** and the **destination address** is **F8:DA:0C:75:C4:25**.

*15. Open the ethernet-ethereal-trace-1 trace file. 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?*

**Answer:** There's no reply for this trace as we are not at the machine that send the request since the ARP request is broadcasted, but the ARP reply is sent back directly to the sender's Ethernet address.

**EX-1.** *The arp command allows you to manually add an entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?*

**Answer:** When entering in a correct IP address, but the wrong Ethernet address, it sends as a "static" type protocol but in this case since the wrong Ethernet address is enter, the case of 100% total packet loss could happen as it try to send data through the IP to the Ethernet but since it doesn't exist, it will fail to transmit.