# Computer Networks Lab, Assignment 11

Suyash Gaurav

210010054

---

## 1 Part-1: Capturing and analyzing Ethernet frames

---

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

The 48-bit Ethernet address of my computer is: **(c4:41:1e:75:b1:52)**

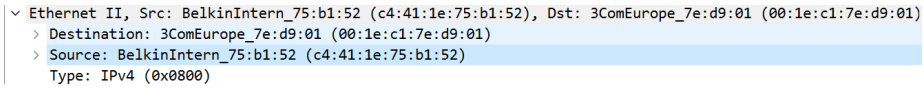


Figure 1: Q1. 48-bit Ethernet address

**2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of *gaia.cs.umass.edu*? What device has this as its Ethernet address?**

Destination 48 bit address: $(00:1e:c1:7e:d9:01)$ This address does not belong to *gaia.cs.umass.edu*. It belongs to router.

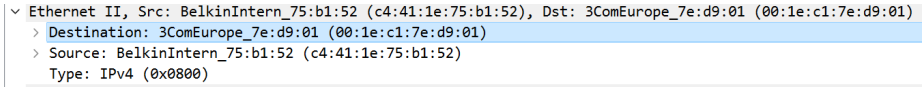


Figure 2: Q2. 48-bit Ethernet address

**3. What is the hexadecimal value for the two-byte Frame type field in the Ethernet frame carrying the HTTP GET request? What upper layer protocol does this correspond to?**

The hexadecimal value for the two-byte Frame type field in the Ethernet frame is **0x0800**. It corresponds to the **IPv4** layer protocol.

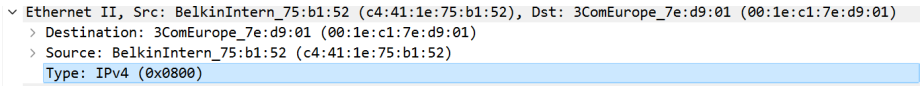


Figure 3: Q3. hexadecimal value

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

The ASCII "G" in GET appears 66 times in the Ethernet frame

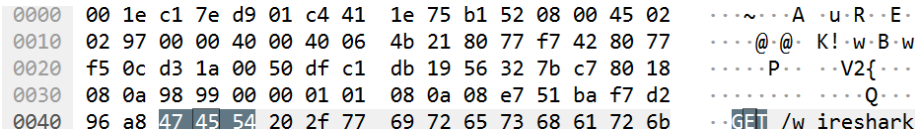


Figure 4: Q4. ASCII "G"

**5. What is the value of the Ethernet source address? Is this the address of your computer, or gaia.cs.umass.edu? What device has this as its Ethernet address?**

The value of the Ethernet source address is $(00 : 1e : c1 : 7e : d9 : 01)$ This address does not belong to *gaia.cs.umass.edu*. It belongs to router.

**6. What is the destination address in the Eth-**

**ernet frame? Is this the Ethernet address of your computer?**

The destination address in the Ethernet frame is ($c4:41:1e:75:b1:52$). It belongs to my computer.

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

The hexadecimal value for the two-byte Frame type field in the Ethernet frame is **0x0800**. It corresponds to the **IPv4** layer protocol.

**8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" appear? After how many bytes in the HTTP does the "O" in "OK" appear?**

The ASCII "O" in "OK" appears in the 13 bytes from the very start of the Ethernet frame. No. of entries in ARP cache is 2

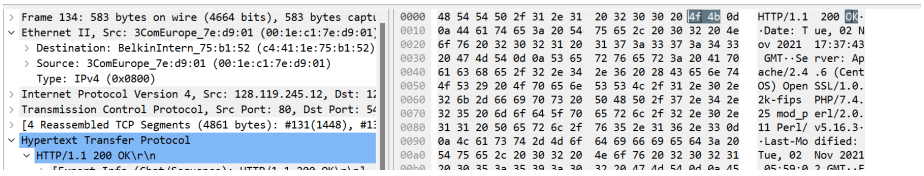


Figure 5: Q8

**9. How many Ethernet frames (each containing an IP datagram, each containing a TCP segment) carry data that is part of the complete HTTP "OK 200 ..." reply message?**

No of Ethernet frames carry the data that is part of the complete HTTP "OK 200..." reply message is **4**.

No. of entries in ARP cache is 2

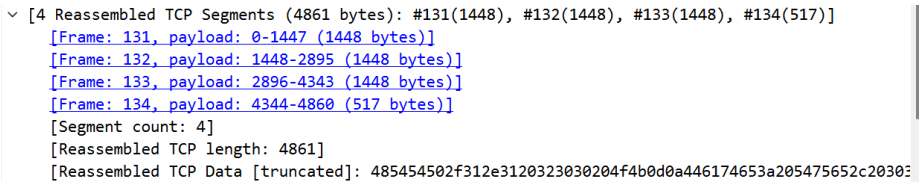


Figure 6: Q9

---

## 2 Part-2: The Address Resolution Protocol

---

**1. How many entries are stored in your ARP cache?**

No. of entries in ARP cache is 2

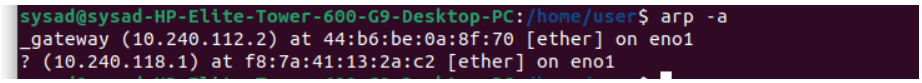


Figure 7: Q1. ARP cache

**2. What is contained in each displayed entry of the ARP cache?**

Each entry in the ARP cache contains a mapping between an IP address and a corresponding MAC address. Static ARP tables are user-configured entries within the ARP cache.

**3. What is the hexadecimal value of the source address in the Ethernet frame containing the first ARP request message sent out by your computer?**

The hexadecimal value of the source address in the Ethernet frame is: c4:41:1e:75:b1:52

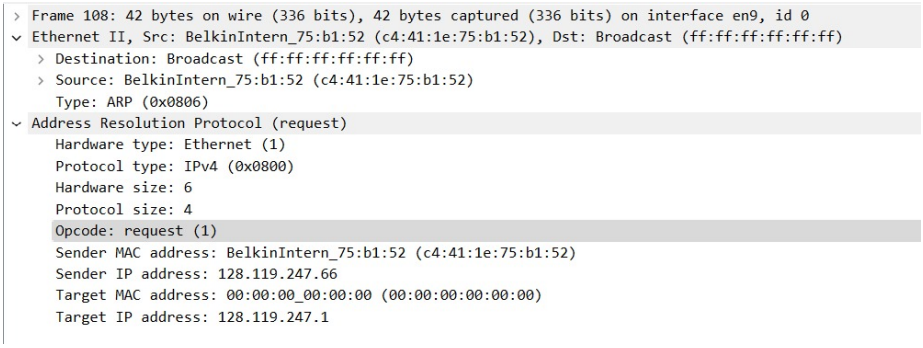


Figure 8: Q3, 4, 5

**4. What is the hexadecimal value of the destination addresses in the Ethernet frame containing the first ARP request message sent out by your computer? And what device (if any) corresponds to that address (e.g., client, server, router, switch or otherwise...)?**

The hexadecimal value of the destination address in the Ethernet frame for the first ARP request is ff:ff:ff:ff:ff:ff, indicating a broadcast address. This address corresponds to no specific device and is used for broadcasting messages to all devices on the network.

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

The hexadecimal value for the two-byte Ethernet Frame type field is 0x0806. The upper layer protocol corresponds to ARP.

**6. How many bytes from the very beginning**

**of the Ethernet frame does the ARP opcode field begin?**

The number of bytes from the very beginning of the Ethernet frame that the ARP opcode field begin with is 20 bytes.

**7. What is the value of the opcode field within the ARP request message sent by your computer?**

The value of the opcode field within the ARP request message sent by my computer is request (1) and its hex value is 0x0001.

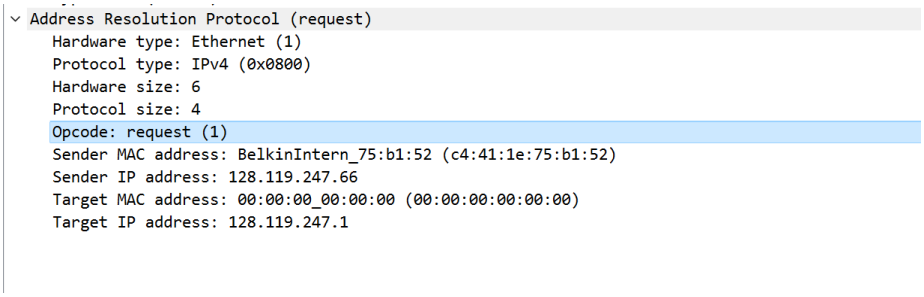


Figure 9: Q7, 8, 9

**8. Does the ARP request message contain the IP address of the sender? If the answer is yes, what is that value?**

Yes, the ARP request message contains the IP address of the sender. The IP address value is 128:119:247:66

**9. What is the IP address of the device whose corresponding Ethernet address is being requested in the ARP request message sent by your computer?**

The IP address of the device whose corresponding Eth-

ernet address is being requested in the ARP request message sent by computer is 128:119:247:1

**10. What is the value of the opcode field within the ARP reply message received by your computer?**

The value of the opcode field within the ARP reply message received by my computer is reply (2) and its hex value is 0x0002

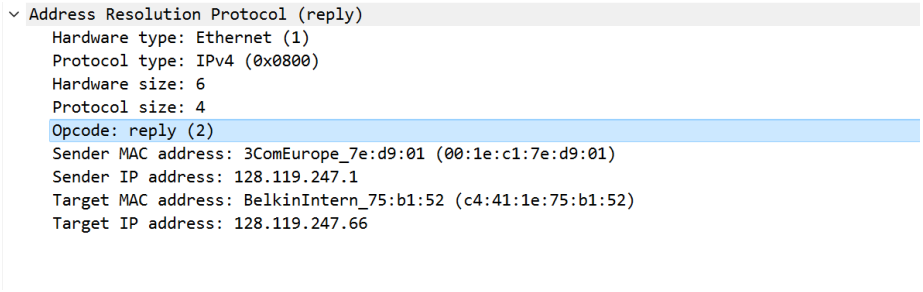


Figure 10: Q10

**11. Finally (!), let's look at the answer to the ARP request message! What is the Ethernet address corresponding to the IP address that was specified in the ARP request message sent by your computer?**

The Ethernet address corresponding to the IP address, specified in the ARP request message sent by computer is 00:1e:c1:7e:d9:01

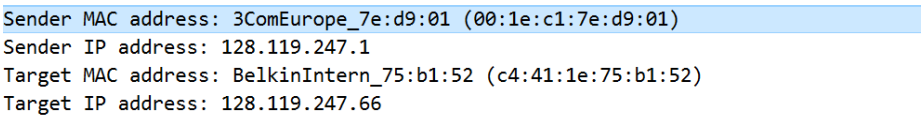


Figure 11: Q11

**12. We've looked at the ARP request message sent by your computer running Wireshark, and the ARP reply message sent in response. But there are other devices in this network that are also sending ARP request messages that you can find in the trace. Why are there no ARP replies in your trace that are sent in response to these other ARP request messages?**

ARP replies are not present in the trace for other ARP request messages because the replies are sent directly to the requesting device's Ethernet address, not to the device capturing the trace.