Alex Banning

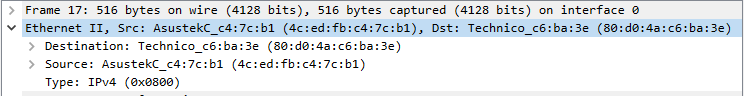
Wireshark Lab 3 – December 1st, 2019

**PART 1: Ethernet**

**Answer the following questions about the packet containing the HTTP GET message:**

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

Source: AsustekC\_c4:7c:b1 **(4c:ed:fb:c4:7c:b1)**

Destination: Technico\_c6:ba:3e (80:d0:4a:c6:ba:3e)

1. **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: Technico\_c6:ba:3e **(80:d0:4a:c6:ba:3e)**

This is the address of the TP link router that my computer is connected to (Gateway to Internet)

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

Hexadecimal for Type: IPv4 is 0x0800

1. **After how many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame? (Ignore the 8-byte preamble since by default Wireshark does not include it in the content of the Ethernet frame).**

The index in the figure below indicate that the ASCII G appears in the frame after 54 bytes.

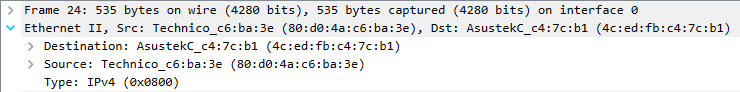


**Answer the following questions about the HTTP packet containing the response (OK) message:**

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

Source: Technico\_c6:ba:3e **(80:d0:4a:c6:ba:3e)**

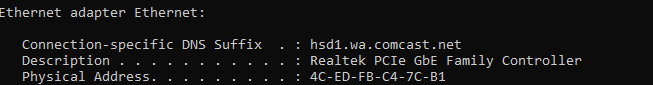
This is the address of my router.



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

Destination: AsustekC\_c4:7c:b1 **(4c:ed:fb:c4:7c:b1)**

**Confirmation:**



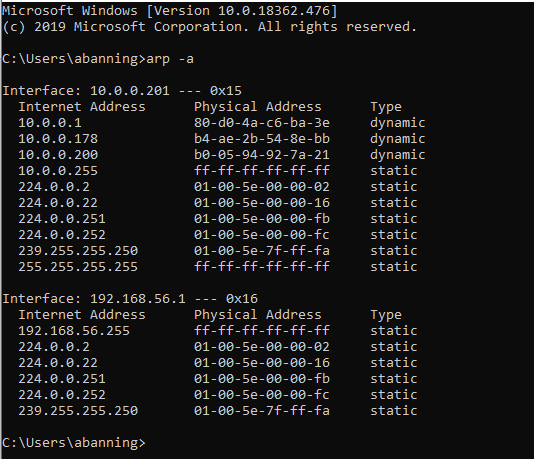
This is the address of my computer.

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

Type: IPv4 (0x0800)

**PART 2: APR**

1. **Provide a screenshot of the contents of the ARP cache on your computer.**



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

Src: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

Dst: Broadcast (ff:ff:ff:ff:ff:ff)



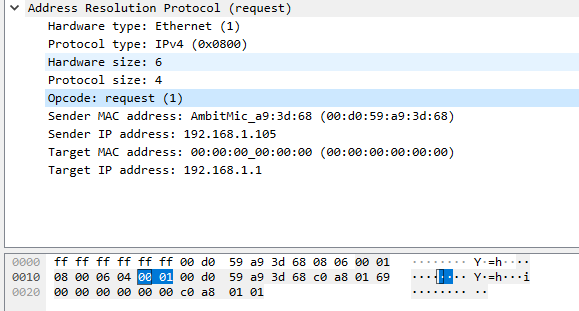
1. **Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?**

Type: ARP (0x0806)



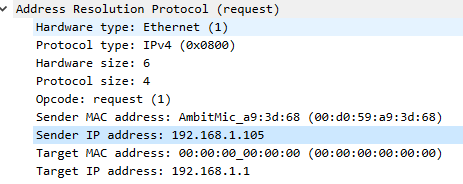
1. **How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?**

Opcode begins on the 21st byte



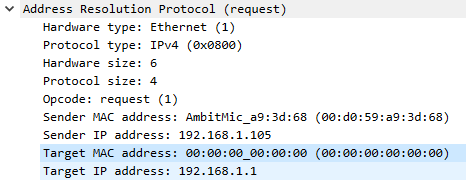
1. **Does the ARP message contain the IP address of the sender?**

Yes: 192.168.1.105



1. **What is the opcode field value for the ARP request message?**

Opcode field is 0x0001 as seen highlighted above.

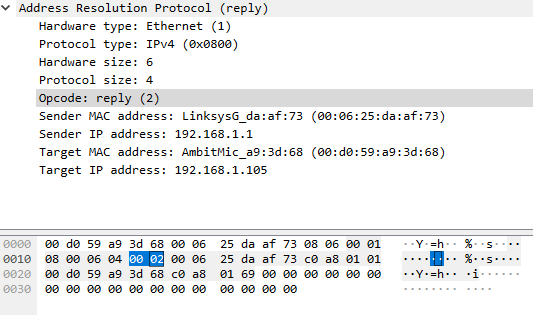
1. **How in the ARP request message does the target MAC address “in question” appear?**

All 0s

**Now find the ARP reply that was sent in response to the ARP request.**

1. **What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?**

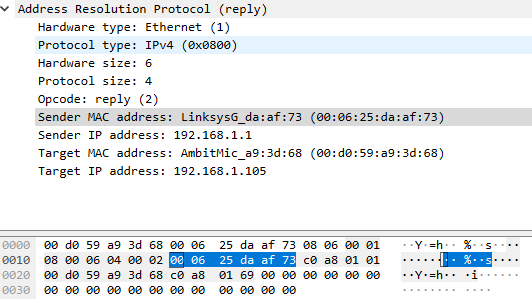
Opcode = 0x0002



1. **Where in the ARP message does the “answer” to the earlier ARP request appear?**

Sender IP Address and Sender MAC Address answer the request

They appear at byte 23



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

Src: LinksysG\_da:af:73 (00:06:25:da:af:73)

Dst: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)



1. **There is yet another computer on the network of the Wireshark trace, 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 the Wireshark trace because replies are not broadcast, so only the sender of the request will receive a reply.