ARP

Colin Monroe

Table of Contents:

Definition:

Address Resolution Protocol (ARP):

ARP is a protocol which operates between layer 2, Data Link, and layer 3, Network, of the OSI model (Gary Fairhurst, 2005). It is specifically used by the IPv4 protocol, Internet Protocol version 4, to chart the different IP addresses with the physical, Media Access Control (MAC), addresses (Gary Fairhurst, 2005).

Questions:

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

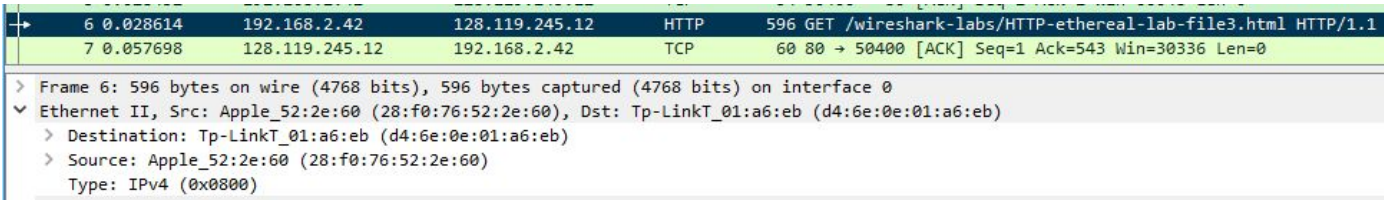


Figure 1.

In Figure 1. It can be seen that the 48-bit Ethernet address of my computer, source, is 28:f0:76:52:2e:60

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.]

In Figure 1. It can be seen that the 48-bit Ethernet address of the destination address is d4:6e:0e:01:a6:eb . The device that has this Ethernet address is the router.

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

In Figure 1. In the “Type:” field you can see the hex value for the Frame type field is 0x0800. The EtherType 0x0800 is associated with the IPv4 protocol.
http://standards-oui.ieee.org/ethertype/eth.txt

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

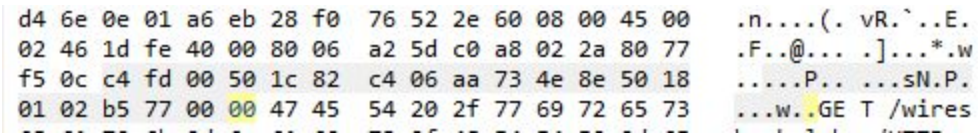


Figure 2.

In Figure 2. It can be seen that there are 54 bytes in the Ethernet frame before the ASCII “G” in “GET” appears. This is due to the fact that the:
Ethernet header = 14 bytes max size
IP header = 20 bytes max size
TCP Header = 20-40 bytes

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?

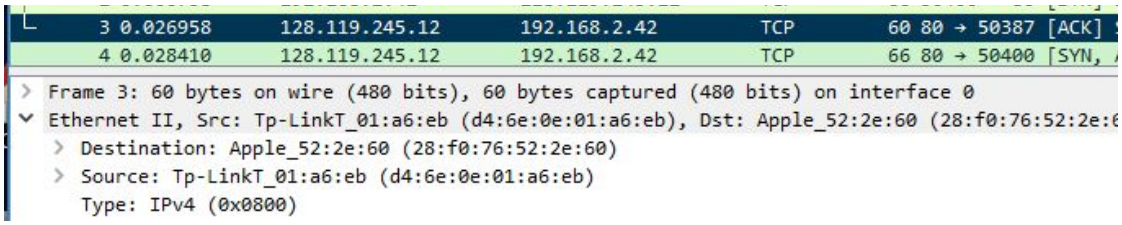


Figure 3.

In Figure 3. It can be seen that the value of the Ethernet source address is: d4:6e:0e:01:a6:eb which is the physical address of the router.

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

In Figure 3. It can be seen that the value of the Ethernet destination address is: 28:f0:76:52:2e:60 which is the physical address of my computer.

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

In Figure 3. It can be seen that the hex value for the Frame type field is 0x0800. The EtherType 0x0800 is associated with the IPv4 protocol.

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?

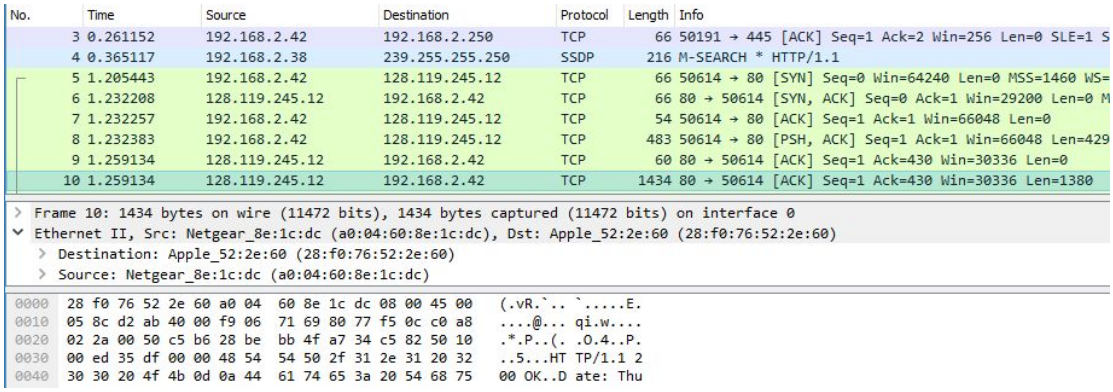


Figure 4.

As shown in Figure 4. There are 67 bytes from the very start of the Ethernet frame before the "O" in "OK".

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

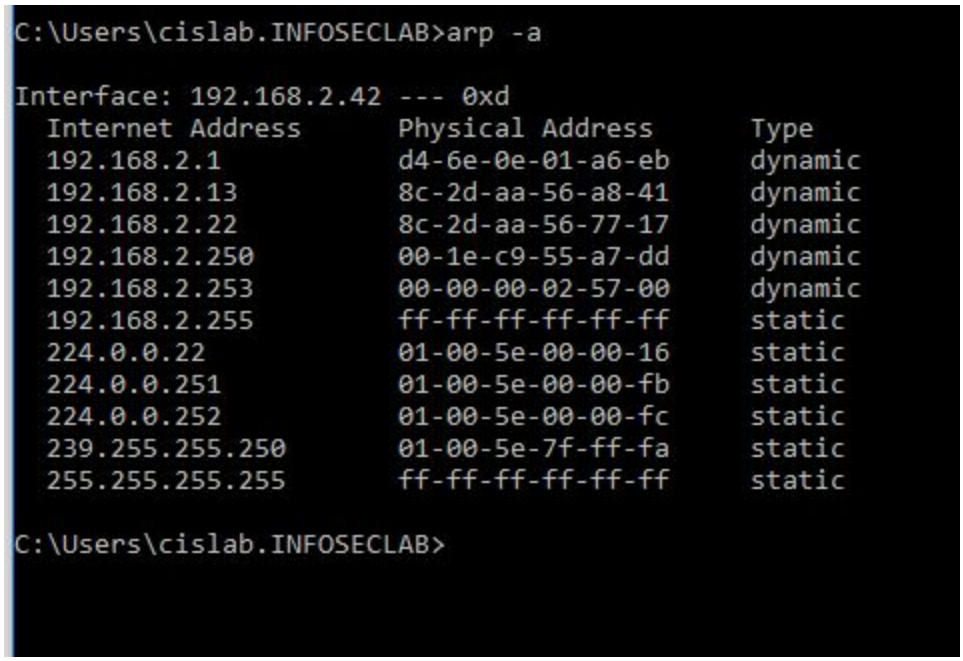


Figure 5.

IP addresses **MAC Addresses** **Types**

Figure 5. Shows the ARP table. Internet Protocol, Media Access Control, and Dynamic or Static Type are the categories for the ARP table.

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

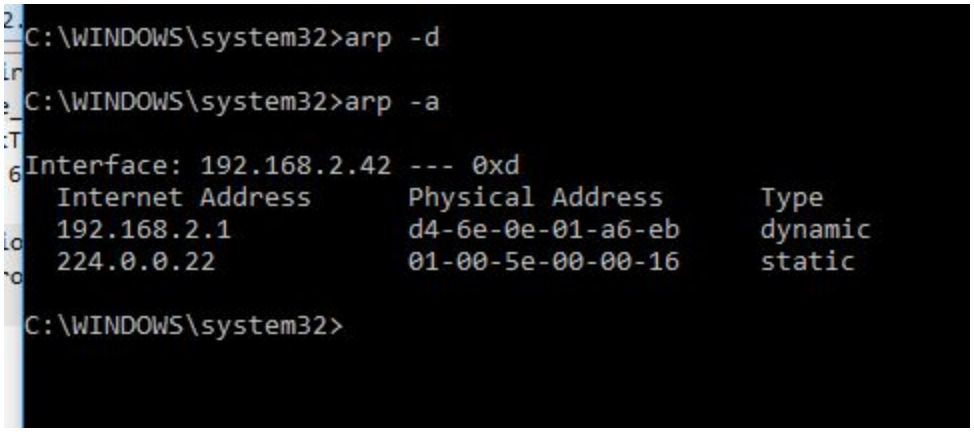


Figure 6.

Figure 6. Shows the ARP table after it has been reset. All it knows now is my computer's IP and MAC and the Routers IP and MAC.

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.2.42 --- 0xd
  Internet Address      Physical Address      Type
  192.168.2.1           d4-6e-0e-01-a6-eb     dynamic
  192.168.2.22          8c-2d-aa-56-77-17     dynamic
  192.168.2.250         00-1e-c9-55-a7-dd     dynamic
  192.168.2.253         00-00-00-02-57-00     dynamic
  192.168.2.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure 7.

Figure 7. Shows the ARP table after it has broadcasted out and received information allowing it to fill in the table again.

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

```
    6 0.855788    00:00:00_02:57:00    Apple_52:2e:60    ARP    60 192.168.2.253 is at 00:00:00:02:57:00
> Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
v Ethernet II, Src: Apple_52:2e:60 (28:f0:76:52:2e:60), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Apple_52:2e:60 (28:f0:76:52:2e:60)
    Type: ARP (0x0806)
v Address Resolution Protocol (request)
```

Figure 8.

It can be seen in Figure 8. that the hex value for the Frame type field is 0x0806. The EtherType 0x0806 is associated with the ARP protocol.

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

```
    5 0.853853    Apple_52:2e:60    Broadcast         ARP    42 Who has 192.168.2.253? Tell 192.168.2.42
    6 0.855788    00:00:00_02:57:00 Apple_52:2e:60    ARP    60 192.168.2.253 is at 00:00:00:02:57:00

> Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: Apple_52:2e:60 (28:f0:76:52:2e:60), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6

0000  ff ff ff ff ff ff 28 f0  76 52 2e 60 08 06 00 01   ......(. vR.`....
0010  08 00 06 04 00 01 28 f0  76 52 2e 60 c0 a8 02 2a   ......(. vR.`...*
0020  00 00 00 00 00 00 c0 a8  02 fd                     ........ ..
```

Figure 9.

Figure 9. Shows that there are 20 bytes before the ARP opcode field begins.

a) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

As shown in Figure 9. The ARP opcode value is 00 01, (1)

b) Does the ARP message contain the IP address of the sender?

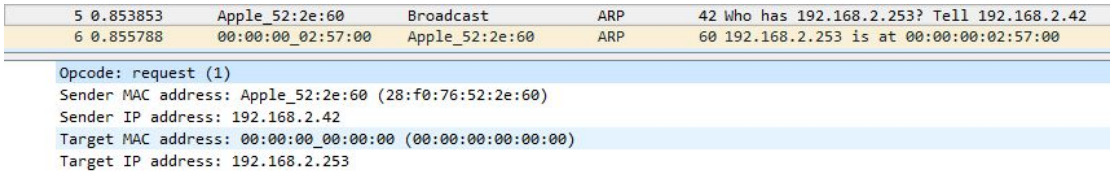


Figure 10.

Yes, as can be seen in Figure 10. The IP address of the sender is included in the ARP packet. In this case it is 192.168.2.42

c) Where in the ARP request does the "question" appear - the Ethernet address of the machine whose corresponding IP address is being queried?

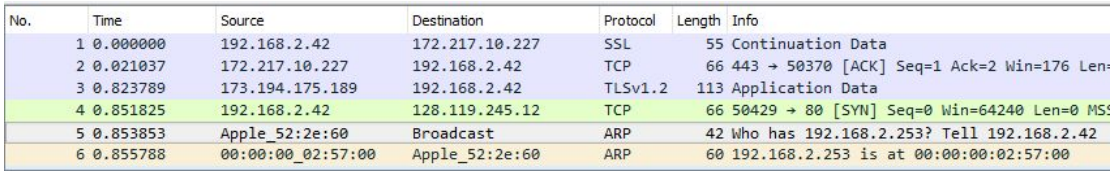


Figure 11.

As shown in Figure 11. The question "Who has" is in the Info section of the query.

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?

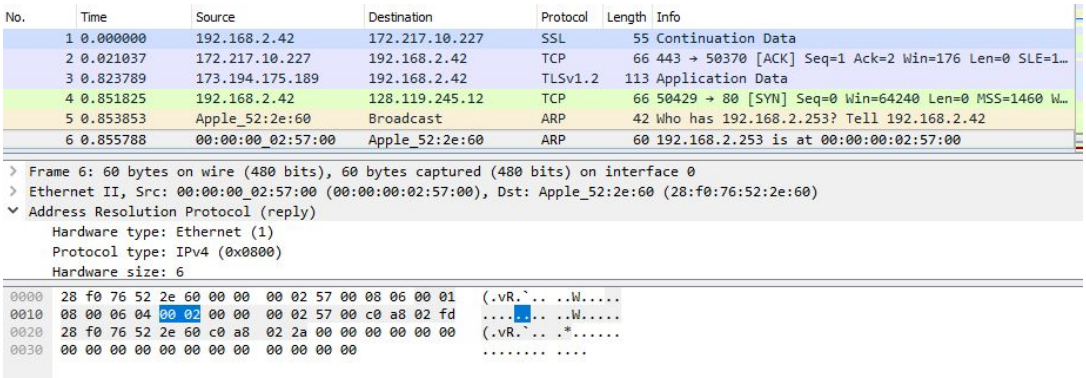


Figure 12.

As shown in Figure 7. There are 20 bytes before the ARP opcode field begins.

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?

As seen in Figure 12. The value of the opcode field within the ARP-payload part of the Ethernet frame is 00 02 (2)

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?

As seen in Figure 12. The ARP "answer" to the earlier ARP request is in the Info section.

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

As shown in Figure 12. The hexadecimal values for Source is: 00:00:00:02:57:00 and Destination is: 28:f0:76:52:2e:60

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?

Telebit is sending it out to broadcast so that is why we can see it initially however we are not the intended target IP address therefore we will not see the response for this.

Extra Credit

EX-1. The *arp* command:

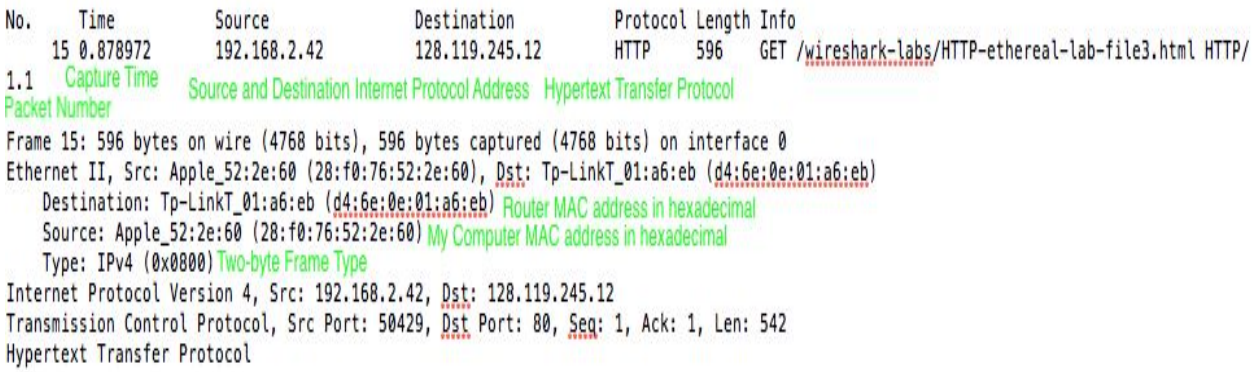
allows you to manually add an entry to the ARP cache that resolves the IP address *InetAddr* to the physical address *EtherAddr*. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

If you entered the wrong Ethernet address in the ARP cache you will probably lose connectivity. This is due to that instead of sending it to your router or the correct place you will then be either broadcasting to another computer or to everyone.

EX-2. What is the default amount of time that an entry remains in your ARP cache before being removed. You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation. Indicate how/where you determined this value.

For Windows 2000 the dynamic ARP cache will timeout after a maximum of 10 minutes time (Microsoft, 2012). If the ARP cache entries are static however then they will not timeout ever (Microsoft, 2012).

Appendice:



References

Fairhurst, G.(January 12, 2005). Address Resolution Protocol (arp). Retrieved on 04/17/18 from http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html

Microsoft, (July 18, 2012). ARP Cache. Retrieved on 04/17/18 from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc958841(v=technet.10)