



ARP
Colin Monroe



Table of Contents:

Definition.....	2
Question 1.....	3
Question 2.....	3
Question 3.....	3
Question 4.....	3
Question 5.....	4
Question 6.....	4
Question 7.....	4
Question 8.....	4
Question 9.....	5
Question 10.....	5
Question 11.....	6
Question 12.....	6
Question 13.....	7
Question 14.....	8
Question 15.....	8
Extra Credit.....	9
Appendice.....	10
Reference.....	11

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?

6	0.028614	192.168.2.42	128.119.245.12	HTTP	596 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
7	0.057698	128.119.245.12	192.168.2.42	TCP	60 80 → 50400 [ACK] Seq=1 Ack=543 Win=30336 Len=0

>	Frame 6: 596 bytes on wire (4768 bits), 596 bytes captured (4768 bits) on interface 0
▼	Ethernet II, Src: Apple_52:2e:60 (28:f0:76:52:2e:60), Dst: Tp-LinkT_01:a6:eb (d4:6e:0e:01:a6:eb)
>	Destination: Tp-LinkT_01:a6:eb (d4:6e:0e:01:a6:eb)
>	Source: Apple_52:2e:60 (28:f0:76:52:2e:60)
	Type: IPv4 (0x0800)

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?

d4	6e	0e	01	a6	eb	28	f0	76	52	2e	60	08	00	45	00	.n....(. vR. ^ ..E.
02	46	1d	fe	40	00	80	06	a2	5d	c0	a8	02	2a	80	77	.F..@... .]...*.w
f5	0c	c4	fd	00	50	1c	82	c4	06	aa	73	4e	8e	50	18P.. ...sN.P.
01	02	b5	77	00	00	47	45	54	20	2f	77	69	72	65	73	...w..GE T /wires

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?

3	0.026958	128.119.245.12	192.168.2.42	TCP	60 80 → 50387 [ACK]
4	0.028410	128.119.245.12	192.168.2.42	TCP	66 80 → 50400 [SYN,

```

> Frame 3: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▼ Ethernet II, Src: Tp-LinkT_01:a6:eb (d4:6e:0e:01:a6:eb), Dst: Apple_52:2e:60 (28:f0:76:52:2e:60)
  > Destination: Apple_52:2e:60 (28:f0:76:52:2e:60)
  > Source: Tp-LinkT_01:a6:eb (d4:6e:0e:01:a6:eb)
  Type: IPv4 (0x0800)

```

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?

No.	Time	Source	Destination	Protocol	Length	Info
3	0.261152	192.168.2.42	192.168.2.250	TCP	66	50191 → 445 [ACK] Seq=1 Ack=2 Win=256 Len=0 SLE=1 S
4	0.365117	192.168.2.38	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
5	1.205443	192.168.2.42	128.119.245.12	TCP	66	50614 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=
6	1.232208	128.119.245.12	192.168.2.42	TCP	66	80 → 50614 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 M
7	1.232257	192.168.2.42	128.119.245.12	TCP	54	50614 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
8	1.232383	192.168.2.42	128.119.245.12	TCP	483	50614 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66048 Len=429
9	1.259134	128.119.245.12	192.168.2.42	TCP	60	80 → 50614 [ACK] Seq=1 Ack=430 Win=30336 Len=0
10	1.259134	128.119.245.12	192.168.2.42	TCP	1434	80 → 50614 [ACK] Seq=1 Ack=430 Win=30336 Len=1380

```

> Frame 10: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface 0
▼ Ethernet II, Src: Netgear_8e:1c:dc (a0:04:60:8e:1c:dc), Dst: Apple_52:2e:60 (28:f0:76:52:2e:60)
  > Destination: Apple_52:2e:60 (28:f0:76:52:2e:60)
  > Source: Netgear_8e:1c:dc (a0:04:60:8e:1c:dc)

```

```

0000  28 f0 76 52 2e 60 a0 04 60 8e 1c dc 08 00 45 00  (.vR.`..`.....E.
0010  05 8c d2 ab 40 00 f9 06 71 69 80 77 f5 0c c0 a8  ....@...qi.w....
0020  02 2a 00 50 c5 b6 28 be bb 4f a7 34 c5 82 50 10  ..*.P..(. .O.4..P.
0030  00 ed 35 df 00 00 48 54 54 50 2f 31 2e 31 20 32  ..5...HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75  00 OK...D ate: Thu

```

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?

```
C:\Users\cislab.INFOSECLAB>arp -a

Interface: 192.168.2.42 --- 0xd
Internet Address      Physical Address      Type
192.168.2.1           d4-6e-0e-01-a6-eb    dynamic
192.168.2.13          8c-2d-aa-56-a8-41    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
224.0.0.251           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

C:\Users\cislab.INFOSECLAB>
```

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?

```
C:\WINDOWS\system32>arp -d
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
224.0.0.22            01-00-5e-00-00-16    static

C:\WINDOWS\system32>
```

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?

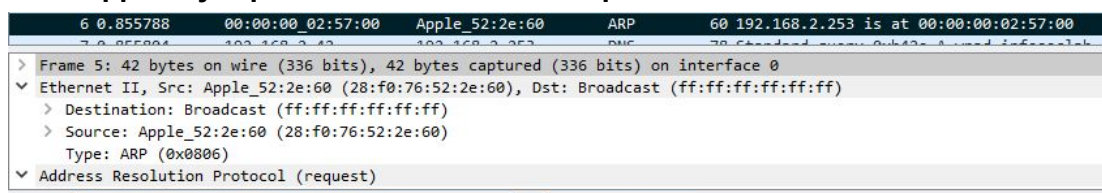


Figure 8.

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?

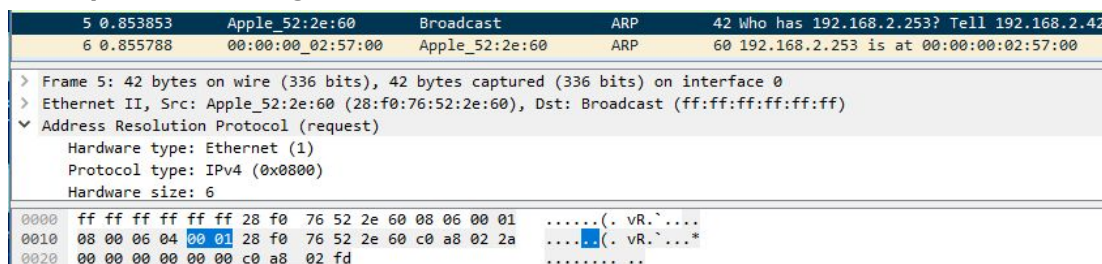


Figure 9.

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?

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

```

Opcode: request (1)
Sender MAC address: Apple_52:2e:60 (28:f0:76:52:2e:60)
Sender IP address: 192.168.2.42
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.2.253

```

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?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.42	172.217.10.227	SSL	55	Continuation Data
2	0.021037	172.217.10.227	192.168.2.42	TCP	66	443 → 50370 [ACK] Seq=1 Ack=2 Win=176 Len=0
3	0.823789	173.194.175.189	192.168.2.42	TLSv1.2	113	Application Data
4	0.851825	192.168.2.42	128.119.245.12	TCP	66	50429 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
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

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?

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.42	172.217.10.227	SSL	55	Continuation Data
2	0.021037	172.217.10.227	192.168.2.42	TCP	66	443 → 50370 [ACK] Seq=1 Ack=2 Win=176 Len=0 SLE=1...
3	0.823789	173.194.175.189	192.168.2.42	TLSv1.2	113	Application Data
4	0.851825	192.168.2.42	128.119.245.12	TCP	66	50429 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W...
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 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: 00:00:00_02:57:00 (00:00:00:02:57:00), Dst: Apple_52:2e:60 (28:f0:76:52:2e:60)
  Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    0000 28 f0 76 52 2e 60 00 00 00 02 57 00 08 06 00 01 (.vR... ..W....
    0010 08 00 06 04 00 02 00 00 00 02 57 00 c0 a8 02 fd .... ..W....
    0020 28 f0 76 52 2e 60 c0 a8 02 2a 00 00 00 00 00 00 (.vR... *......
    0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

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:

No.	Time	Source	Destination	Protocol	Length	Info
15	0.878972	192.168.2.42	128.119.245.12	HTTP	596	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/

1.1 **Capture Time** **Source and Destination Internet Protocol Address** **Hypertext Transfer Protocol**
Packet Number

Frame 15: 596 bytes on wire (4768 bits), 596 bytes captured (4768 bits) on interface 0
Ethernet II, Src: Apple_52:2e:60 (28:f0:76:52:2e:60), Dst: Tp-LinkT_01:a6:eb (d4:6e:0e:01:a6:eb)
Destination: Tp-LinkT_01:a6:eb (d4:6e:0e:01:a6:eb) **Router MAC address in hexadecimal**
Source: Apple_52:2e:60 (28:f0:76:52:2e:60) **My Computer MAC address in hexadecimal**
Type: IPv4 (0x0800) **Two-byte Frame Type**

Internet Protocol Version 4, Src: 192.168.2.42, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50429, Dst Port: 80, Seq: 1, Ack: 1, Len: 542
Hypertext Transfer Protocol

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\(v=technet.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc958841(v=technet.10))