

Daniel McDonough (dmcdonough)
10/5/2018
Lab 3

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

My Ethernet address is Address: (00:d0:59:a9:3d:68)

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? (2 points)

The destination address is 00:06:25:da:af:73. This is not the Ethernet address of gaia.cs.umass.edu but rather the Ethernet address of the router we used to send the info.

3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to? (2 points)

0x0800 which is the IPv4 protocol

4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame? (1 point)

52 bytes before the G. 14 bytes for Ethernet header, 20bytes for each IP and TCP.

The image shows a Wireshark packet capture window titled 'ethernet.pcap'. The packet list pane shows several packets, with packet 10 selected. The packet details pane shows the structure of the selected packet, which is an Ethernet II frame. The frame contains an ARP request (protocol 0x0800) from source 00:d0:59:a9:3d:68 to destination 00:06:25:da:af:73. The data field shows the raw bytes of the ARP request, which includes the source and target MAC addresses and the source and target IP addresses. The packet bytes pane shows the raw bytes of the packet, with the source MAC address 00:d0:59:a9:3d:68 highlighted in red. The status bar at the bottom shows 'Packets: 17 - Displayed: 17 (100.0%) - Load time: 0:0.0' and 'Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	13.542974	Telebit_73:0d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4
11	17.494766	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	17.498935	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	17.500625	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
14	17.500669	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
15	17.527057	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
16	17.527422	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489	IPv4
17	17.527457	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4

Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits) on interface 0
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
Address: LinksysG_da:af:73 (00:06:25:da:af:73)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Data: 450002a00fa40008006bfc0a801698077f50c04220050...
[Length: 672]

0000 00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 00 45 00 ...%..S..Y..E.
0010 02 a0 00 fa 40 00 80 90 bf c8 c9 a5 01 09 80 77@.....i.W
0020 f5 0c 04 22 00 50 05 14 99 a7 ac a5 3f b4 50 18 ...".Pe....?..P.
0030 fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68 65 72 ...-O...GE T /ether
0040 65 01 6c 2d 6c 61 62 73 2f 48 54 54 2d 65 74 eal-labs /HTTP-et
0050 08 05 72 65 61 6c 2d 6c 61 62 2d 60 09 6c 65 33 herael-l ab-file03
0060 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HT TP/1.1..
0070 48 0f 73 74 3a 20 67 61 09 61 2e 63 73 2e 75 6d Host: ga ia.cs.um
0080 61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 67 ass.edu. User-Ag
0090 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Moz illa/5.0
00a0 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20 57 69 (Window s; U; Wi
00b0 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20 65 6e ndows NT 5.1; en
00c0 2d 55 53 3b 20 72 76 3a 31 2e 30 2e 32 29 20 47 -US; rv:1.0.2) G
00d0 65 63 6b 6f 2f 32 30 30 33 30 32 30 38 20 4e 65 ecko/200 30208 Ne
00e0 74 73 63 61 70 65 2f 37 2e 30 32 0d 0a 41 63 63 tscape/7 .02..Acc

Source Hardware Address (eth.src), 6 bytes
Packets: 17 - Displayed: 17 (100.0%) - Load time: 0:0.0
Profile: Default
cache on your computer. Run the *arp* command.

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? (2 points)

The source is: 00:06:25:da:af:73 which is again the Ethernet address of the router used.

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer? (2 points)

00:d0:59:a9:3d:68 is the destination and my Ethernet Address.

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to? (2 points)

0x0800 which is 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? (1 point)

54 bytes until the “O” .14 bytes for Ethernet header, 20bytes for each IP and TCP.

The image shows a Wireshark packet capture of an Ethernet frame. The packet list pane shows 17 packets. Packet 12 is selected, showing details of an Ethernet II frame. The source MAC address is 00:06:25:da:af:73 (LinksysG_da:af:73) and the destination MAC address is 00:d0:59:a9:3d:68 (AmbitMic_a9:3d:68). The frame type is 0x0800 (IPv4). The packet bytes pane shows the raw data of the frame, with the ASCII text "OK" visible at the beginning of the data field.

No.	Time	Source	Destination	Protocol	Length	Info
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	13.542974	Telnet_73:bd:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	17.466408	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	606	IPv4
11	17.494766	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	60	IPv4
12	17.498935	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
13	17.500025	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
14	17.500069	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
15	17.527057	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	1514	IPv4
16	17.527422	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	489	IPv4
17	17.527457	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4

Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
Source: LinksysG_da:af:73 (00:06:25:da:af:73)
Address: LinksysG_da:af:73 (00:06:25:da:af:73)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Data (1500 bytes)
Data: 45605dc8f2f40037067f78077f50cc0a801690509422...
[Length: 1500]

0000 00 00 59 a9 3d 68 00 06 25 da af 73 08 00 45 60 ...Y..t...E
0010 05 dc 8f 2f 40 00 37 06 7f 78 07 7f 50 c0 a8 .../0.7.v.v.w...
0020 01 09 00 50 04 22 ac a5 3f b4 65 14 9c 1f 50 10 .i.P..?e..P.
0030 1b 28 5e d0 00 00 48 54 54 50 2f 31 2e 31 20 32 .(A..HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74 00 OK..Date: Sat
0050 2c 20 32 38 20 41 75 67 20 32 30 30 34 20 31 37 . 28 Aug 2004 17
0060 3a 31 39 3a 33 37 20 47 4d 54 0d 0a 53 65 72 76 :19:37 G MT..Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34 er: Apac he/2.0.4
0080 30 20 20 52 65 64 20 48 61 74 20 4c 69 6e 75 78 0 (Red H at Linux
0090 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64).Last-Modified
00a0 3a 20 53 61 74 2c 20 32 38 20 41 75 67 20 32 30 : Sat, 2 8 Aug 20
00b0 39 34 20 31 37 3a 31 38 3a 35 33 20 47 4d 54 6d 64 17:18 :53 GMT.
00c0 0a 45 5d 61 67 3a 20 22 31 62 61 35 63 2d 31 31 ETag: "1ba5c-11
00d0 39 34 2d 36 39 65 64 39 34 30 22 0d 0a 41 63 63 94-69ed9 40".Acc
00e0 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65 ept-Rang es: byte

Source Hardware Address (eth.src), 6 bytes

Packets: 17 - Displayed: 17 (100.0%) - Load time: 0:0.0

Profile: Default

cache on your computer. Run the *arp* command.

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

Running "arp -a" on linux:

```
autoreg-704614.wifi.wpi.edu (130.215.120.243) at a4:5e:60:ca:7d:4b [ether] on wlp1s0
autoreg-166218.dyn.wpi.edu (130.215.123.157) at ac:bc:32:87:8a:99 [ether] on wlp1s0
autoreg-119838.dyn.wpi.edu (130.215.123.109) at 18:65:90:d3:b9:a5 [ether] on wlp1s0
? (130.215.122.175) at <incomplete> on wlp1s0
autoreg-174531.dyn.wpi.edu (130.215.123.240) at 2c:f0:ee:06:c6:e8 [ether] on wlp1s0
rtr-core-wireless120.inf.wpi.edu (130.215.120.1) at 00:00:5e:00:01:02 [ether] on wlp1s0
? (130.215.121.86) at ac:bc:32:bd:6c:91 [ether] on wlp1s0
autoreg-166699.dyn.wpi.edu (130.215.124.104) at c4:b3:01:99:69:7c [ether] on wlp1s0
autoreg-119337.dyn.wpi.edu (130.215.123.73) at 78:4f:43:81:87:40 [ether] on wlp1s0
autoreg-069184.dyn.wpi.edu (130.215.124.185) at c8:69:cd:91:7c:ec [ether] on wlp1s0
autoreg-170826.dyn.wpi.edu (130.215.122.123) at 8c:85:90:6c:6c:91 [ether] on wlp1s0
autoreg-121018.dyn.wpi.edu (130.215.126.96) at 8c:85:90:25:c8:fa [ether] on wlp1s0
```

This shows the IP address, the MAC address, and the Iface.

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

Source: (00:d0:59:a9:3d:68), Dst: (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? (2 points)

The Type value is 0x00000806 which is ARP

12. Download the ARP specification from <ftp://ftp.rfc-editor.org/in-notes/std/std37.txt>. A readable, detailed discussion of ARP is also at <http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>.

a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin? (1 point)

18 bytes prior to the opt code

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? (1 point)

0x0001 in the request 0x0002 in the response.

c) Does the ARP message contain the IP address of the sender? (1 point)

Yes, 192.168.1.105

ethernet:ethereal-trace-1.p - Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:00:25:da:af:73
3	0.001028	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	62	IPv4
5	8.971480	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	62	IPv4
6	13.542974	Telebit_73:8d:cce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	62	IPv4
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0000	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	54	IPv4
10	17.465408	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	606	IPv4
11	17.494766	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0000	60	IPv4
12	17.498935	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0000	1514	IPv4
13	17.500025	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0000	1514	IPv4
14	17.500069	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	54	IPv4
15	17.527057	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0000	1514	IPv4
16	17.527422	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0000	489	IPv4
17	17.527457	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0000	54	IPv4

Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
0. = LG bit: Globally unique address (factory default)
0. = IG bit: Individual address (unicast)
 Type: ARP (0x0000)
 ▼ Address Resolution Protocol (request)
 Hardware type: Ethernet (1)
 Protocol type: IPv4 (0x0000)
 Hardware size: 6
 Protocol size: 4
 Opcode: request (1)
 Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 Sender IP address: 192.168.1.105
 Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
 Target IP address: 192.168.1.1

0000 ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01 Y..h...
 0010 00 00 00 04 00 00 00 d0 59 a9 3d 68 c0 a8 01 69 Y..h...
 0020 00 00 00 00 00 00 c0 a8 01 01

Opcode (arp.opcode), 2 bytes

Packets: 17 - Displayed: 17 (100.0%) - Load time: 0:0.0

Profile: Default

Target MAC address: Micro-St_66:75:0e (08:c0:8a:66:75:0e)

d) Where in the ARP request does the “question” appear – the Ethernet (1 point) address of the machine whose corresponding IP address is being queried?

The question is in the target IP address as it is 192.168.1.1

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

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?

The reply was sent from the router to that computer. The user's computer would not obtain the reply message from the router that was sent to a different IP. The only reason we see the request is because it is sent through the whole network in order to gain access to it.