Wireshark Lab 5: Ethernet and ARP

Trevor Bramwell
CS372 - Introduction to Computer Networks
Professor Bechir Hamdaoui

June 5, 2012

1 Capturing and analyzing Ethernet frames

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

   Answer 00:22:75:af:71:6b

2. **Question** 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.]

   Answer 00:16:cb:c1:5f:50. This is the Ethernet address of my external router.

3. **Question** Give the hexadecimal value for the two-byte Frame type field. What do the bits(s) whose value is 1 mean within the flag field?

   Answer 0x0800 means that this frame is of the IP Protocol type.

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

   Answer 53 bytes from the start.

5. **Question** What is the hexadecimal value of the CRC field in this Ethernet frame?

   Answer 0x0d 0x0a 0x0d 0x0a

```
No.     Time           Source                Destination           Protocol
    Length Info
     76 1.300951       BelkinIn_af:71:6b     AppleCom_c1:5f:50     0x0800
         483     IP

Frame 76: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits)
Ethernet II, Src: BelkinIn_af:71:6b (00:22:75:af:71:6b), Dst: AppleCom_c1:5f
    :50 (00:16:cb:c1:5f:50)
     Destination: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50)
     Source: BelkinIn_af:71:6b (00:22:75:af:71:6b)
     Type: IP (0x0800)
Data (469 bytes)

0000  45 00 01 d5 34 8e 40 00 40 06 83 fd 0a 00 01 14   E...4.@.@.......
0010  80 77 f5 0c 8d 9d 00 50 bb 18 b1 c9 d3 88 9f dc   .w.....P........
0020  80 18 01 c9 20 8b 00 00 01 01 08 0a 00 28 85 5e   .... ........(.^
0030  ff 99 94 11 47 45 54 20 2f 77 69 72 65 73 68 61   ....GET /wiresha
0040  72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74 68   rk-labs/HTTP-eth
0050  65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33 2e   ereal-lab-file3.
0060  68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48   html HTTP/1.1..H
0070  6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61   ost: gaia.cs.uma
0080  73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69   ss.edu..Connecti
0090  6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a   on: keep-alive..
00a0  55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69   User-Agent: Mozi
00b0  6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b 20 4c 69   lla/5.0 (X11; Li
00c0  6e 75 78 20 78 38 36 5f 36 34 29 20 41 70 70 6c   nux x86_64) Appl
00d0  65 57 65 62 4b 69 74 2f 35 33 35 2e 31 31 20 28   eWebKit/535.11 (
00e0  4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b   KHTML, like Geck
00f0  6f 29 20 43 68 72 6f 6d 65 2f 31 37 2e 30 2e 39   o) Chrome/17.0.9
0100  36 33 2e 37 39 20 53 61 66 61 72 69 2f 35 33 35   63.79 Safari/535
0110  2e 31 31 0d 0a 41 63 63 65 70 74 3a 20 74 65 78   .11..Accept: tex
0120  74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69   t/html,applicati
0130  6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70   on/xhtml+xml,app
0140  6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30   lication/xml;q=0
0150  2e 39 2c 2a 2f 2a 3b 71 3d 30 2e 38 0d 0a 41 63   .9,*/*;q=0.8..Ac
0160  63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a 20 67   cept-Encoding: g
0170  7a 69 70 2c 64 65 66 6c 61 74 65 2c 73 64 63 68   zip,deflate,sdch
0180  0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67   ..Accept-Languag
0190  65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e   e: en-US,en;q=0.
01a0  38 0d 0a 41 63 63 65 70 74 2d 43 68 61 72 73 65   8..Accept-Charse
01b0  74 3a 20 49 53 4f 2d 38 38 35 39 2d 31 2c 75 74   t: ISO-8859-1,ut
01c0  66 2d 38 3b 71 3d 30 2e 37 2c 2a 3b 71 3d 30 2e   f-8;q=0.7,*;q=0.
01d0  33 0d 0a 0d 0a                                    3....
```

6. **Question** 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?

   Answer 00:16:cb:c1:5f:50. It is the address of neither. It the address of my extenal router.

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

   Answer 00:22:75:af:71:6b. It is the Ethernet address of my wireless usb adapter, so yes.

8. **Question** Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field?

   Answer 0x0800. The bits signify that this is an IP Protocol frame.

9. **Question** 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?

   Answer 66 bytes from the start.

10. **Question** What is the hexadecimal value of the CRC field in this Ethernet frame ?

    Answer 0x3e 0x0a 0x0d 0x3c

```
No.     Time           Source                Destination           Protocol
    Length Info
     78 1.616849     AppleCom_c1:5f:50     BelkinIn_af:71:6b     0x0800
        1514    IP

Frame 78: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112
    bits)
Ethernet II, Src: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50), Dst: BelkinIn_af
    :71:6b (00:22:75:af:71:6b)
     Destination: BelkinIn_af:71:6b (00:22:75:af:71:6b)
     Source: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50)
     Type: IP (0x0800)
Data (1500 bytes)

0000   45 20 05 dc cd 94 00 00 2e 06 38 d0 80 77 f5 0c   E ........8..w..
0010   0a 00 01 14 00 50 8d 9d d3 88 9f dc bb 18 b3 6a   .....P.........j
0020   80 10 00 36 26 a9 00 00 01 01 08 0a ff 99 94 a3   ...6&...........
0030   00 28 85 5e 48 54 54 50 2f 31 2e 31 20 32 30 30   .(.^HTTP/1.1 200
0040   20 4f 4b 0d 0a 44 61 74 65 3a 20 54 68 75 2c 20    OK..Date: Thu,
0050   31 35 20 4d 61 72 20 32 30 31 32 20 30 34 3a 35   15 Mar 2012 04:5
0060   34 3a 33 31 20 47 4d 54 0d 0a 53 65 72 76 65 72   4:31 GMT..Server
                  ^^^^^^^^^^^                     ^^^^^^^^^^^

05c0   64 6d 65 6e 74 20 49 3c 2f 68 33 3e 3c 2f 73 74   dment I</h3></st
05d0   72 6f 6e 67 3e 3c 2f 61 3e 0a 0a 3c              rong></a>..<
```

2 The Address Resolution Protocol

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

```
Address                  HWtype  HWaddress           Flags Mask  Iface
Base-Station-N.local     ether   00:16:cb:c1:5f:50   C             wlan0
```

Address A named reference to the MAC address of the network router.

HWtype The type of hardware address.

HWaddress The actual hardware address.

Flags Flags attached to the address. C means Cached.

Mask What this address could be hidden as.

Iface The interface on which this address resides.

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

    Answer Source: 00:22:75:af:71:6b. Destination: ff:ff:ff:ff:ff:ff.

13. **Question** Give the hexadecimal value for the two-byte Ethernet Frame type field. What do the bit(s) whose value is 1 mean within the flag field?

    Answer 0x0806. It specifics that this packet is using the ARP protocol.

14. **Question** Download the ARP specification.

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

    Answer 21 Bytes after the beginning.

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

    Answer 0x0001 (Request).

    (c) **Question** Does the ARP message contain the IP address of the sender?

    Answer Yes. It is 10.0.1.20.

    (d) **Question** Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?

    Answer Starting at byte 33 and going till byte 39. It comes just after the sender Ethernet address and IP address is listed.

```
No.     Time        Source                Destination           Protocol
   Length Info
     17 14.979987   BelkinIn_af:71:6b     Broadcast             ARP
        42      Who has 10.0.1.1?  Tell 10.0.1.20

Frame 17: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: BelkinIn_af:71:6b (00:22:75:af:71:6b), Dst: Broadcast
   (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: BelkinIn_af:71:6b (00:22:75:af:71:6b)
    Type: ARP (0x0806)
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: False]
    Sender MAC address: BelkinIn_af:71:6b (00:22:75:af:71:6b)
    Sender IP address: 10.0.1.20 (10.0.1.20)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.0.1.1 (10.0.1.1)

0000  ff ff ff ff ff ff 00 22 75 af 71 6b 08 06 00 01    .......”u.qk....
0010  08 00 06 04 00 01 00 22 75 af 71 6b 0a 00 01 14    .......”u.qk....
0020  00 00 00 00 00 00 0a 00 01 01                      ..........
```

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

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

    Answer 21 bytes after the beginning of the Ethernet frame.

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

    Answer 0x0002 (Reply).

    (c) **Question** Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address of the machine whose corresponding IP address is being queried?

    Answer 7 bytes after the *opcode*. The 6 bytes after the *opcode* is used for the Ethernet address of the queried machine.

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

    Answer Source: 00:16:cb:c1:5f:50. Destination: 00:22:75:af:71:6b.

17. **Question** Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

    Answer There is no ARP reply sent because the Ethernet address in the request does not match the local machines hardware address.

```
No.     Time        Source                Destination           Protocol
    Length Info
     18 14.992318   AppleCom_c1:5f:50     BelkinIn_af:71:6b     ARP      42
            10.0.1.1 is at 00:16:cb:c1:5f:50

Frame 18: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50), Dst: BelkinIn_af:71:6b
    (00:22:75:af:71:6b)
    Destination: BelkinIn_af:71:6b (00:22:75:af:71:6b)
    Source: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50)
    Type: ARP (0x0806)
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    [Is gratuitous: False]
    Sender MAC address: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50)
    Sender IP address: 10.0.1.1 (10.0.1.1)
    Target MAC address: BelkinIn_af:71:6b (00:22:75:af:71:6b)
    Target IP address: 10.0.1.20 (10.0.1.20)

0000  00 22 75 af 71 6b 00 16 cb c1 5f 50 08 06 00 01   ."u.qk...._P....
0010  08 00 06 04 00 02 00 16 cb c1 5f 50 0a 00 01 01   ..........._P....
0020  00 22 75 af 71 6b 0a 00 01 14                     ."u.qk....
```

3 Extra Credit

1. **Question** 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?

   Answer It disables that interface. All outbound requests go nowhere.

2. **Question** What is the default amount of time that an entry remains in your ARP cache before being removed?

   Answer 60 seconds. It can be found in */proc/sys/net/ipv4/neigh/wlan0/ gc_stale_time*.