Julia Diliberto
CST 311
Lab 8
June 16, 2015

```
No.     Time                   Source                Destination
Protocol Length Info
     14 17:13:45.640030000 LiteonTe_a1:7d:de     Netgear_c7:80:e8
0x0800   442    IP

Frame 14: 442 bytes on wire (3536 bits), 442 bytes captured (3536 bits) on
interface 0
Ethernet II, Src: LiteonTe_a1:7d:de (ac:b5:7d:a1:7d:de), Dst:
Netgear_c7:80:e8 (00:22:3f:c7:80:e8)
    Destination: Netgear_c7:80:e8 (00:22:3f:c7:80:e8)
    Source: LiteonTe_a1:7d:de (ac:b5:7d:a1:7d:de)
    Type: IP (0x0800)
Data (428 bytes)

0000  45 00 01 ac 6b c9 40 00 80 06 0d f5 0a 00 00 0a   E...k.@.........
0010  80 77 f5 0c cb ee 00 50 5c 23 e4 93 4a af 67 7d   .w.....P\#..J.g}
0020  50 18 01 00 13 44 00 00 47 45 54 20 2f 77 69 72   P....D..GET /wir
0030  65 73 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50   eshark-labs/HTTP
0040  2d 65 74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69   -ethereal-lab-fi
0050  6c 65 33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e   le3.html HTTP/1.
0060  31 0d 0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73   1..Host: gaia.cs
0070  2e 75 6d 61 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e   .umass.edu..Conn
0080  65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69   ection: keep-ali
0090  76 65 0d 0a 41
```

1. ac:b5:7d:a1:7d:de
2. 00:22:3f:c7:80:e8; No, the router interface on the same subnet as my computer.
3. 0800; IP
4. Seems like it should be after 54 bytes of header, but I can't find it in the data.

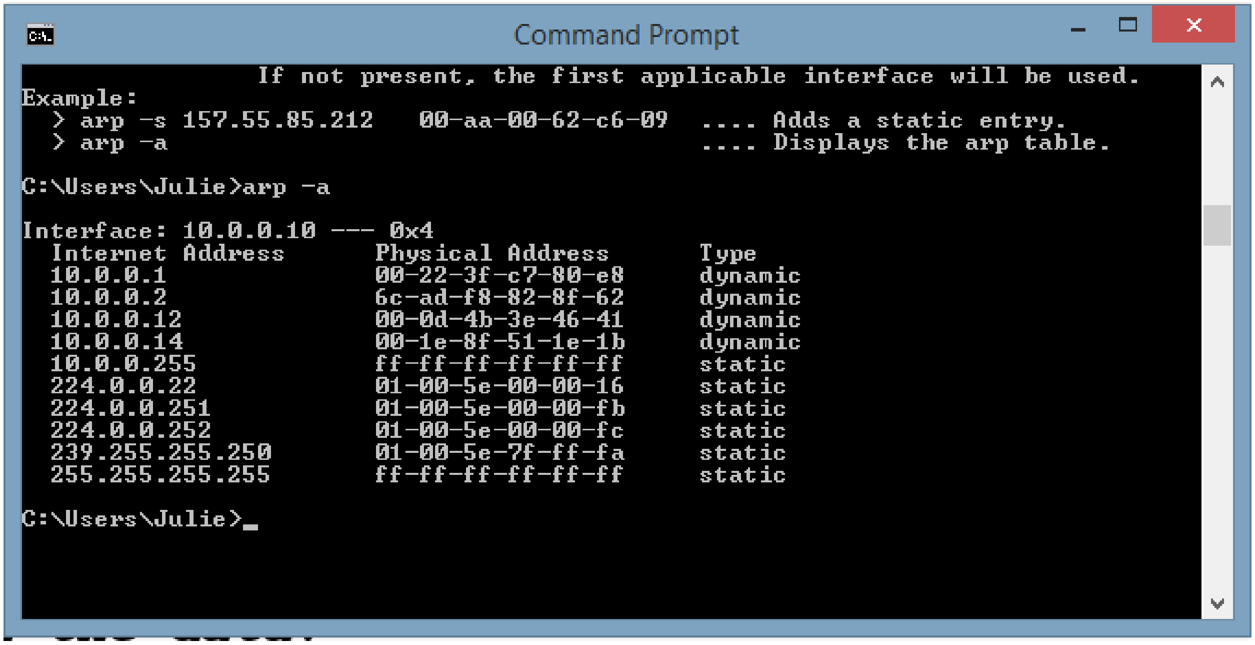
```
No.     Time                   Source                Destination
Protocol Length Info
     20 17:13:45.751002000 Netgear_c7:80:e8      LiteonTe_a1:7d:de
0x0800   537    IP

Frame 20: 537 bytes on wire (4296 bits), 537 bytes captured (4296 bits) on
interface 0
Ethernet II, Src: Netgear_c7:80:e8 (00:22:3f:c7:80:e8), Dst:
LiteonTe_a1:7d:de (ac:b5:7d:a1:7d:de)
    Destination: LiteonTe_a1:7d:de (ac:b5:7d:a1:7d:de)
    Source: Netgear_c7:80:e8 (00:22:3f:c7:80:e8)
    Type: IP (0x0800)
Data (523 bytes)

0000  45 00 02 0b a2 63 40 00 2e 06 28 fc 80 77 f5 0c   E....c@...(..w..
0010  0a 00 00 0a 00 50 cb ee 4a af 78 99 5c 23 e6 17   .....P..J.x.\#..
```

```
0020   50 18 00 7b d7 c9 00 00 69 73 68 6d 65 6e 74 73   P..{....ishments
0030   20 69 6e 66 6c 69 63 74 65 64 2e 0a 0a 3c 2f 70    inflicted...</p
0040   3e 3c 70 3e 3c 61 20 6e 61 6d 65 3d 22 39 22 3e   ><p><a name="9">
0050   3c 73 74 72 6f 6e 67 3e 3c 68 33 3e 41 6d 65 6e   <strong><h3>Amen
0060   64 6d 65 6e 74 20 49 58 3c 2f 68 33 3e 3c 2f 73   dment IX</h3></s
0070   74 72 6f 6e 67 3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c   trong></a>..<p><
0080   2f 70 3e 3c 70 3e 54 68 65 20 65 6e 75 6d 65 72   /p><p>The enumer
0090   61 74 69 6f 6e 20 69 6e 20 74 68 65 20 43 6f 6e   ation in the Con
00a0   73 74 69 74 75 74 69 6f 6e 2c 20 6f 66 20 63 65   stitution, of ce
00b0   72 74 61 69 6e 20 72 69 67 6
```

5. 00:22:3f:c7:80:e8; No, my first hop router.
6. ac:b5:7d:a1:7d:de; yes
7. 0800; IP
8. Seems like it should be after 54 bytes of header, but I can't find it in the data.
9.



```
              If not present, the first applicable interface will be used.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09   .... Adds a static entry.
  > arp -a                                     .... Displays the arp table.

C:\Users\Julie>arp -a

Interface: 10.0.0.10 --- 0x4
  Internet Address      Physical Address      Type
  10.0.0.1              00-22-3f-c7-80-e8     dynamic
  10.0.0.2              6c-ad-f8-82-8f-62     dynamic
  10.0.0.12             00-0d-4b-3e-46-41     dynamic
  10.0.0.14             00-1e-8f-51-1e-1b     dynamic
  10.0.0.255            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\Julie>_
```

IP address; MAC address; whether this address changes or not

```
No.     Time               Source                Destination
Protocol Length Info
      1 10:19:20.157130 AmbitMic_a9:3d:68     Broadcast               ARP
42     Who has 192.168.1.1?  Tell 192.168.1.105

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Type: ARP (0x0806)
Address Resolution Protocol (request)
```

10. 00:d0:59:a9:3d:68; ff:ff:ff:ff:ff:ff
11. 0806; ARP

```
No.     Time               Source                Destination
Protocol Length Info
      1 10:19:20.157130 AmbitMic_a9:3d:68     Broadcast             ARP
42     Who has 192.168.1.1?  Tell 192.168.1.105

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 28, 2004 10:19:20.157130000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1093713560.157130000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
        Address: Broadcast (ff:ff:ff:ff:ff:ff)
        .... ..1. .... .... .... .... = LG bit: Locally administered
address (this is NOT the factory default)
        .... ...1 .... .... .... .... = IG bit: Group address
(multicast/broadcast)
    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: ARP (0x0806)
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    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 (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 (192.168.1.1)

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

12a. After 20 bytes

12b. 1

12c. Yes,192.168.1.105

12d. In the Target IP Address field - 192.168.1.1

```
No.     Time             Source                Destination
Protocol Length Info
      2 10:19:20.158148 LinksysG_da:af:73     AmbitMic_a9:3d:68     ARP
60     192.168.1.1 is at 00:06:25:da:af:73

Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 28, 2004 10:19:20.158148000 Pacific Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1093713560.158148000 seconds
    [Time delta from previous captured frame: 0.001018000 seconds]
    [Time delta from previous displayed frame: 0.001018000 seconds]
    [Time since reference or first frame: 0.001018000 seconds]
    Frame Number: 2
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
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: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1 (192.168.1.1)
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105 (192.168.1.105)

0000  00 d0 59 a9 3d 68 00 06 25 da af 73 08 06 00 01   ..Y.=h..%..s....
0010  08 00 06 04 00 02 00 06 25 da af 73 c0 a8 01 01   ........%..s....
```

```
0020  00 d0 59 a9 3d 68 c0 a8 01 69 00 00 00 00 00 00   ..Y.=h...i......
0030  00 00 00 00 00 00 00 00 00 00 00 00                ............
```

13a. After 20 bytes

13b. 2

13c. In the Target MAC Address field

14. 00:06:25:da:af:73; 00:d0:59:a9:3d:68

15. The request was made by a different computer than is capturing the packets (192.168.1.104, not 192.168.1.105 like the first request).