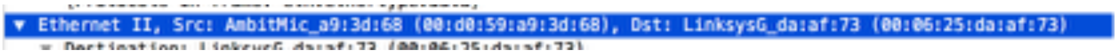
Benjamin Fondell

CS 372

December 1, 2017

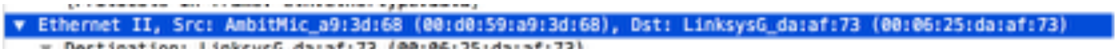
Lab 5

NOTE: I am using the provided trace for the lab as my network was unable to provide the needed information at the time.



```
▼ 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)
```

1. The computers ip is: 00:d0:59:a9:3d:68

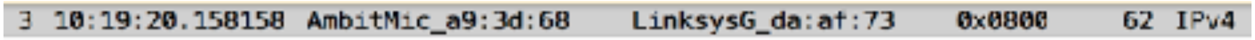


```
▼ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
  ▼ Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
```

2. Destination is: 00:06:25:da:af:73

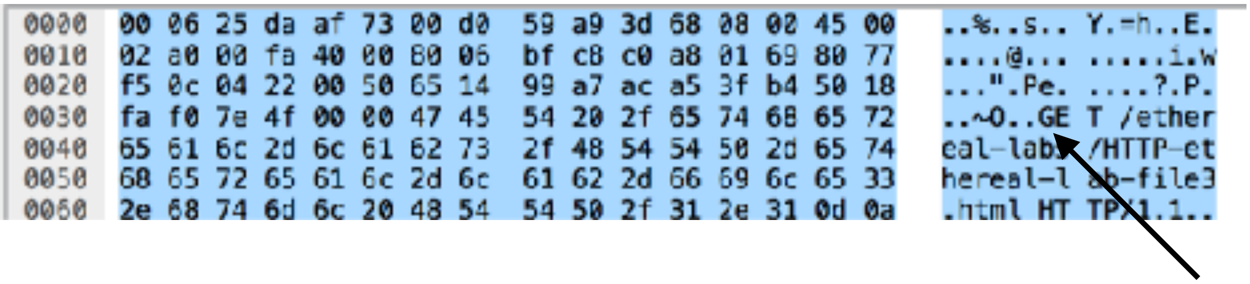
This is not the address of gaia.cs.umas.edu.

It is the address of a linksys router. This link is taken to get off the subnet.



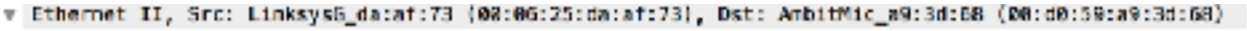
```
3  10:19:20.158158  AmbitMic_a9:3d:68    LinksysG_da:af:73    0x0800     62  IPv4
```

3. The hex value in the frame type field is 0x0800. This represents IP v4. The bits suggest it is an IP protocol frame. The one suggests to not fragment.



```
0000  00 06 25 da af 73 00 d0  59 a9 3d 68 08 02 45 00   ..%..s.. Y.=h..E.
0010  02 a0 00 fa 40 00 80 06  bf c8 c0 a8 01 69 80 77   ....@... .....i.w
0020  f5 0c 04 22 00 50 65 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 61 6c 2d 6c 61 62 73  2f 48 54 54 50 2d 65 74   eal-labs /HTTP-et
0050  68 65 72 65 61 6c 2d 6c  61 62 2d 66 69 6c 65 33   hereal-l ab-file3
0060  2e 68 74 6d 6c 20 48 54  54 50 2f 31 2e 31 0d 0a   .html HT TP/1.1..
```

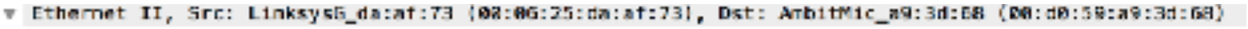
4. The ASCII "G" appears 54 bytes from the start of the ethernet data frame.



```
▼ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
```

5. Value of ethernet source is: 00:06:25:da:af:73

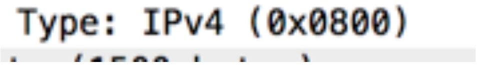
It is the address of a linksys router. This link is taken to get off the subnet. It is the router responsible for sending from the UMASS host which is within the subnet.



```
▼ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
```

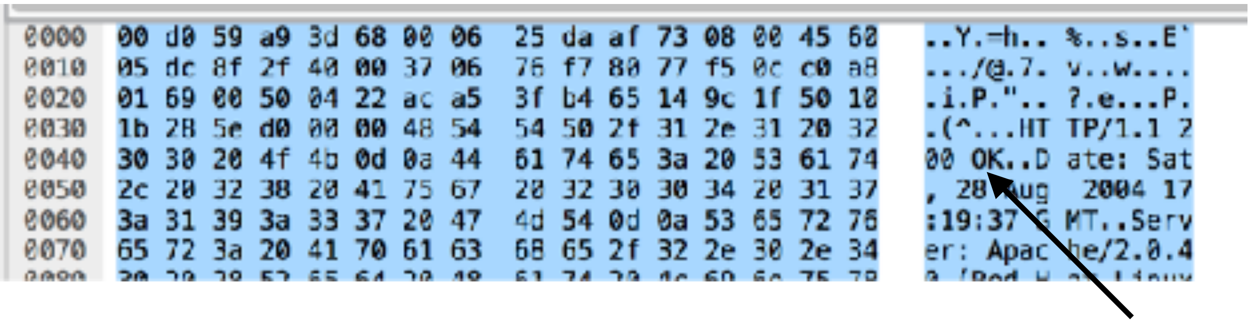
6. The destination address is 00:d0:59:a9:3d:68

This is the address of home computer that is sending the request.



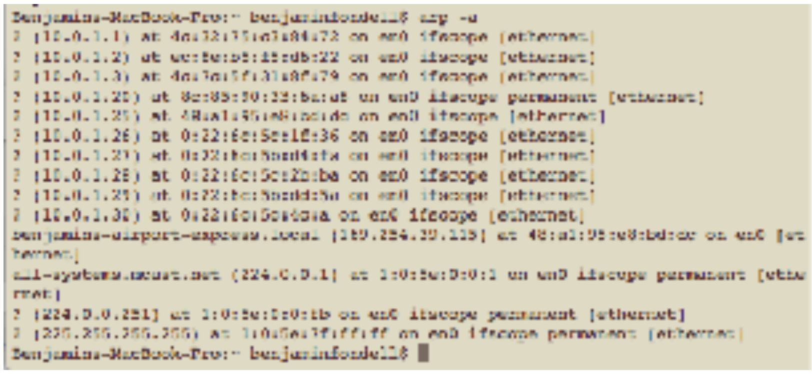
```
Type: IPv4 (0x0800)
```

7. The hex value for the frame type field is 0x0800 which corresponds to IPv4



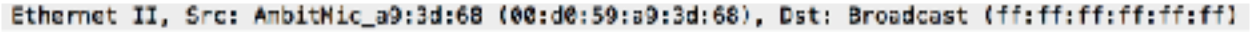
```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 00 45 60   ..Y.=h.. %..s..E`
0010  05 dc 8f 2f 40 00 37 06  76 f7 80 77 f5 0c c0 a8   .../@.7. v..w....
0020  01 69 00 50 04 22 ac a5  3f b4 65 14 9c 1f 50 10   .i.P.".. ?.e...P.
0030  1b 28 5e d0 00 00 48 54  54 50 2f 31 2e 31 20 32   .(^...HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 61 74   00 OK..D ate: 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
```

8. The hexadecimal ASCII “O” is 67 bytes from the start of the ethernet data frame.



```
Benjamins-MacBook-Pro:~ benjaminfondell$ arp -a
? (10.0.1.1) at 4c:32:75:a1:84:72 on en0 ifscope [ethernet]
? (10.0.1.2) at ac:fe:05:15:db:22 on en0 ifscope [ethernet]
? (10.0.1.3) at 4c:3c:5f:31:8f:79 on en0 ifscope [ethernet]
? (10.0.1.20) at 8c:85:90:33:ba:a8 on en0 ifscope permanent [ethernet]
? (10.0.1.25) at 48:a1:95:e8:bd:dc on en0 ifscope [ethernet]
? (10.0.1.26) at 0:22:6c:5e:1f:36 on en0 ifscope [ethernet]
? (10.0.1.27) at 0:22:6c:5e:d4:fa on en0 ifscope [ethernet]
? (10.0.1.28) at 0:22:6c:5c:2b:ba on en0 ifscope [ethernet]
? (10.0.1.29) at 0:22:6c:5e:dd:5a on en0 ifscope [ethernet]
? (10.0.1.30) at 0:22:6c:5e:4e:a on en0 ifscope [ethernet]
benjamins-airport-express.local (169.254.39.115) at 48:a1:95:e8:bd:dc on en0 [et
hernet]
all-systems.mcast.net (224.0.0.1) at 1:0:5e:0:0:1 on en0 ifscope permanent [ethe
rnet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
Benjamins-MacBook-Pro:~ benjaminfondell$ 
```

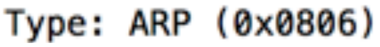
9. The first column is the the internet address of the computer then the the physical address. Then the last column of information is the type.



```
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
```

10. Source: 00:d0:59:a9:3d:68

Destination: ff:ff:ff:ff:ff:ff (broadcast address)



```
Type: ARP (0x0806)
```

11. The hex value is 0x0806

This corresponds to ARP .

12.

a) 20 bytes from beginning of ethernet frame.

b) Value in the ARP payload is 0x0001for requests

c) Yes

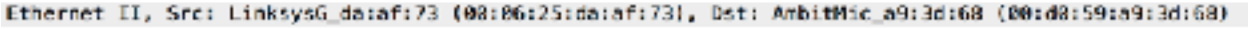
d) Target MAC ADRESS is used to question the host destination IP address

13.

a) 20 bytes from start

b) 0x0002 for replies

c) in the Sender MAC Address field, it contains the ip address of the sending router.



```
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
```

14. Source: 00:06:25:da:af:73

Destination: 00:d0:59:a9:3d:68

15. Because the machine being used receives the reply. If running a trace on that machine that a request was sent to then you would see a reply. The reason for multiple requests is that we must send a broadcast message to find the the router.

EX1: We entered the wrong MAC address and the router has recieved the destination IP address. The router will remove the IP address from the frame and use ARP to find the correct hardware address of the destination.

https://apple.stackexchange.com/questions/38545/when-does-the-arp-cache-get-emptied

For mac OS….

EX2: Default time is 20min. Every 20 min the ARP table values are refreshed. This allows for up to date tables for neighbor devices that may join or leave a network.