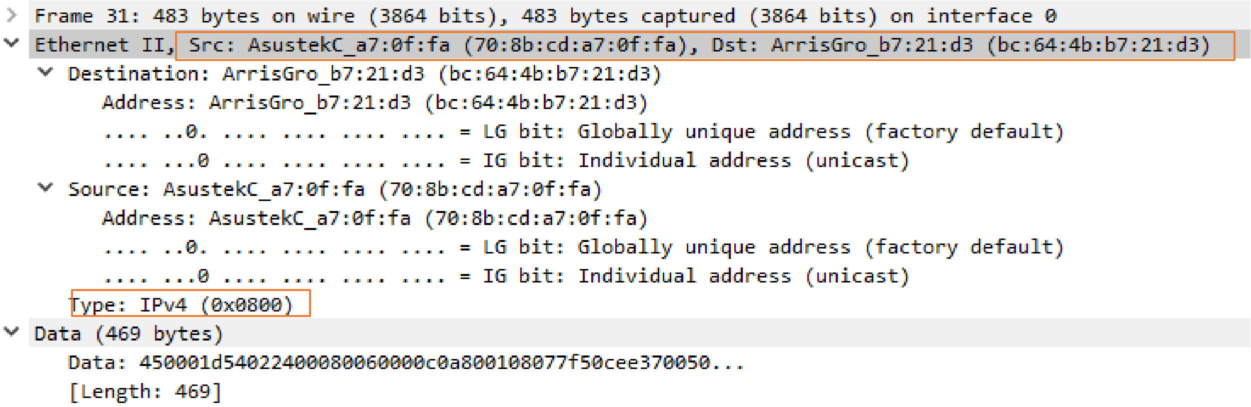
Erin Alltop
CS372 – Spring 2018
Lab 5



```
> Frame 31: 483 bytes on wire (3864 bits), 483 bytes captured (3864 bits) on interface 0
v Ethernet II, Src: AsustekC_a7:0f:fa (70:8b:cd:a7:0f:fa), Dst: ArrisGro_b7:21:d3 (bc:64:4b:b7:21:d3)
  v Destination: ArrisGro_b7:21:d3 (bc:64:4b:b7:21:d3)
      Address: ArrisGro_b7:21:d3 (bc:64:4b:b7:21:d3)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: AsustekC_a7:0f:fa (70:8b:cd:a7:0f:fa)
      Address: AsustekC_a7:0f:fa (70:8b:cd:a7:0f:fa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Data (469 bytes)
    Data: 450001d5402240008006000c0a800108077f50cee370050...
    [Length: 469]
```

Fig 1 – Ethernet GET request. Used to answer questions 1 - 3

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

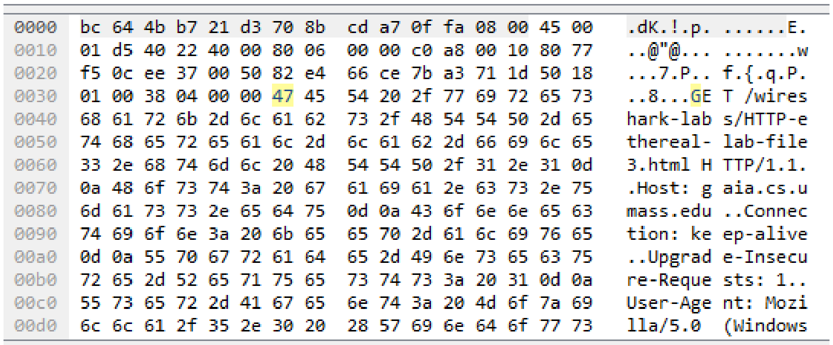
The 48-bit Ethernet address of my computer is 70:8b:cd:a7:0f:fa

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? What device has this as its Ethernet address?

The 48-bit destination address in the Ethernet frame (above) is bc:64:4b:b7:21:d3. It is not the Ethernet address of gaia.cs.umass.edu. It is the Ethernet address of my router which is the link off of the subnet.

3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
The value for the Frame type field is 0x0800.

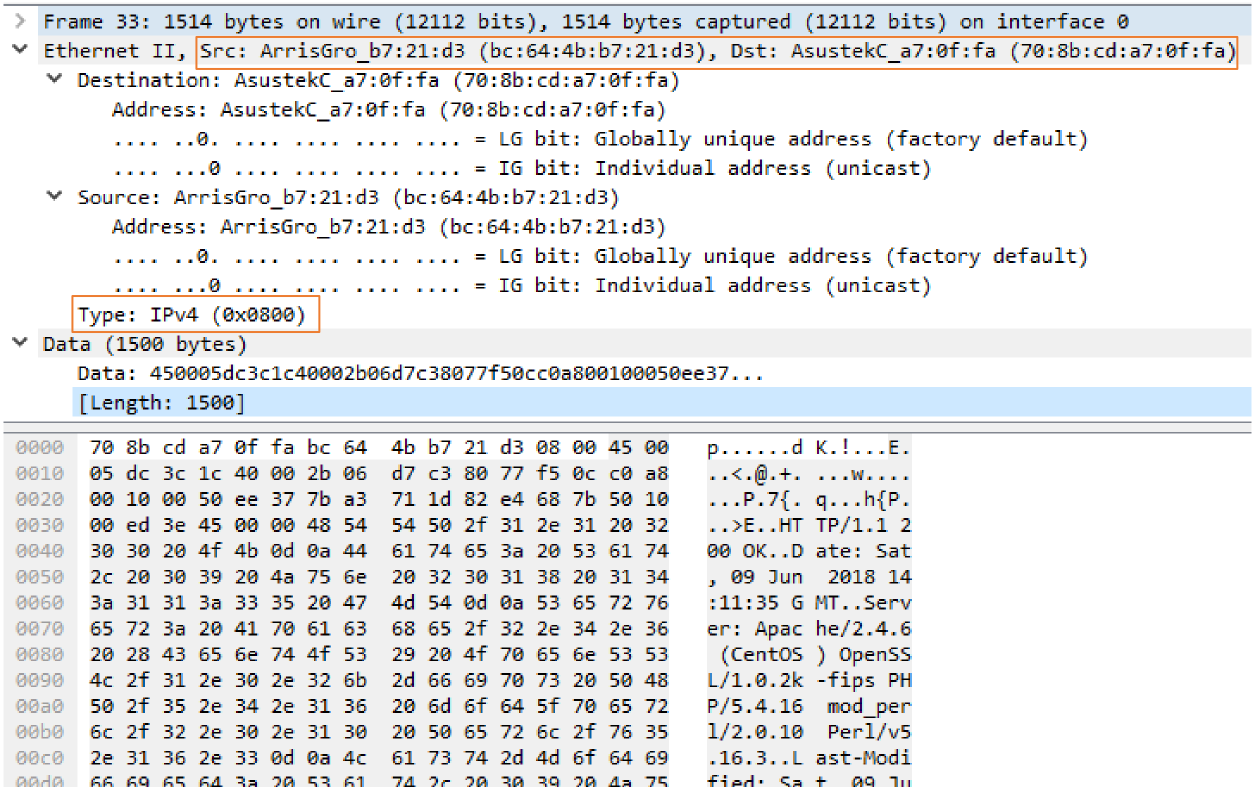
4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?



```
0000  bc 64 4b b7 21 d3 70 8b  cd a7 0f fa 08 00 45 00   .dK.!.p. ......E.
0010  01 d5 40 22 40 00 80 06  00 00 c0 a8 00 10 80 77   ..@"@... .......w
0020  f5 0c ee 37 00 50 82 e4  66 ce 7b a3 71 1d 50 18   ...7.P.. f.{.q.P.
0030  01 00 38 04 00 00 47 45  54 20 2f 77 69 72 65 73   ..8...GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-lab s/HTTP-e
0050  74 68 65 72 65 61 6c 2d  6c 61 62 2d 66 69 6c 65   thereal- lab-file
0060  33 2e 68 74 6d 6c 20 48  54 54 50 2f 31 2e 31 0d   3.html H TTP/1.1.
0070  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   .Host: g aia.cs.u
0080  6d 61 73 73 2e 65 64 75  0d 0a 43 6f 6e 6e 65 63   mass.edu ..Connec
0090  74 69 6f 6e 3a 20 6b 65  65 70 2d 61 6c 69 76 65   tion: ke ep-alive
00a0  0d 0a 55 70 67 72 61 64  65 2d 49 6e 73 65 63 75   ..Upgrad e-Insecu
00b0  72 65 2d 52 65 71 75 65  73 74 73 3a 20 31 0d 0a   re-Reque sts: 1..
00c0  55 73 65 72 2d 41 67 65  6e 74 3a 20 4d 6f 7a 69   User-Age nt: Mozi
00d0  6c 6c 61 2f 35 2e 30 20  28 57 69 6e 64 6f 77 73   lla/5.0  (Windows
```

Fig 2. The portion of the GET data request

There are 14 bytes in the ethernet frame (destination address, source address, and frame type). There are 20 bytes in the IP header. And there are 20 bytes in the TCP header. In total, there are 54 byes from the very start of the Ethernet frame that the "G" in "GET" appears.



```
> Frame 33: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
v Ethernet II, Src: ArrisGro_b7:21:d3 (bc:64:4b:b7:21:d3), Dst: AsustekC_a7:0f:fa (70:8b:cd:a7:0f:fa)
  v Destination: AsustekC_a7:0f:fa (70:8b:cd:a7:0f:fa)
      Address: AsustekC_a7:0f:fa (70:8b:cd:a7:0f:fa)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: ArrisGro_b7:21:d3 (bc:64:4b:b7:21:d3)
      Address: ArrisGro_b7:21:d3 (bc:64:4b:b7:21:d3)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Data (1500 bytes)
    Data: 450005dc3c1c40002b06d7c38077f50cc0a800100050ee37...
    [Length: 1500]

0000  70 8b cd a7 0f fa bc 64  4b b7 21 d3 08 00 45 00   p......d K.!...E.
0010  05 dc 3c 1c 40 00 2b 06  d7 c3 80 77 f5 0c c0 a8   ..<.@.+. ...w....
0020  00 10 00 50 ee 37 7b a3  71 1d 82 e4 68 7b 50 10   ...P.7{. q...h{P.
0030  00 ed 3e 45 00 00 48 54  54 50 2f 31 2e 31 20 32   ..>E..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 30 39 20 4a 75 6e  20 32 30 31 38 20 31 34   , 09 Jun  2018 14
0060  3a 31 31 3a 33 35 20 47  4d 54 0d 0a 53 65 72 76   :11:35 G MT..Serv
0070  65 72 3a 20 41 70 61 63  68 65 2f 32 2e 34 2e 36   er: Apac he/2.4.6
0080  20 28 43 65 6e 74 4f 53  29 20 4f 70 65 6e 53 53    (CentOS ) OpenSS
0090  4c 2f 31 2e 30 2e 32 6b  2d 66 69 70 73 20 50 48   L/1.0.2k -fips PH
00a0  50 2f 35 2e 34 2e 31 36  20 6d 6f 64 5f 70 65 72   P/5.4.16  mod_per
00b0  6c 2f 32 2e 30 2e 31 30  20 50 65 72 6c 2f 76 35   l/2.0.10  Perl/v5
00c0  2e 31 36 2e 33 0d 0a 4c  61 73 74 2d 4d 6f 64 69   .16.3..L ast-Modi
00d0  66 69 65 64 3a 20 53 61  74 2c 20 30 39 20 4a 75   fied: Sa t, 09 Ju
```

Fig 3 – The HTTP response message. Used to answer questions 5 - 8

5. What is the value of the Ethernet source address? Is this the address of your computer or of gaia.cs.umass.edu? What device has this as its Ethernet address?

The value of the Ethernet source address is bc:64:4b:b7:21:d3. No, this is not the address of my computer or gaia.cs.umass.edu. It is the address of my router, used to get off the subnet.

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

The destination address in the Ethernet frame is 70:8b:cd:a7:0f:fa. Yes, this is the Ethernet address of my computer.

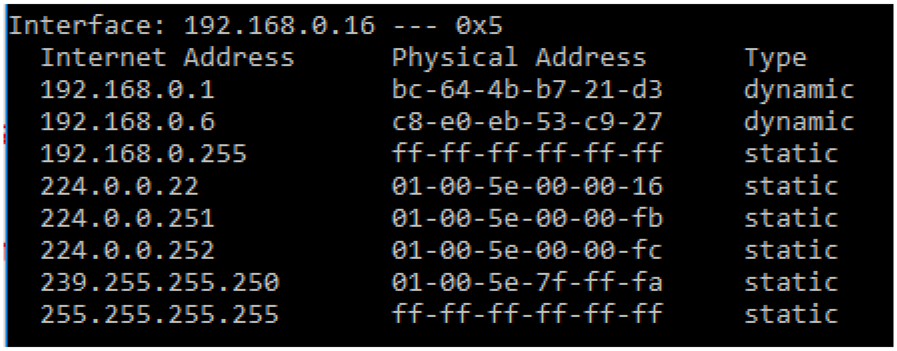
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

The hexadecimal value for the two-byte Frame type field is 0x0800. This corresponds to the IP upper layer protocol.

8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” appear in the Ethernet frame?

There are 14 bytes in the ethernet frame (destination address, source address, and frame type). There are 20 bytes in the IP header. And there are 20 bytes in the TCP header. In total, there are 54 byes from the very start of the Ethernet frame that the “O” in “OK” appears.

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

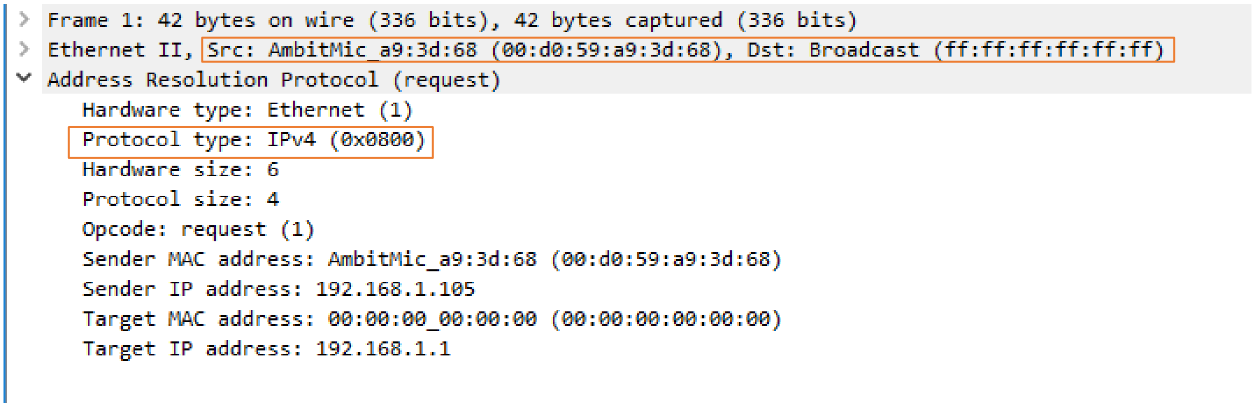


```
Interface: 192.168.0.16 --- 0x5
  Internet Address      Physical Address      Type
  192.168.0.1           bc-64-4b-b7-21-d3     dynamic
  192.168.0.6           c8-e0-eb-53-c9-27     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  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
```

The columns of the ARP cache are – Internet Address: IPv4 address. Physical Address: MAC address. Type: Protocol type

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

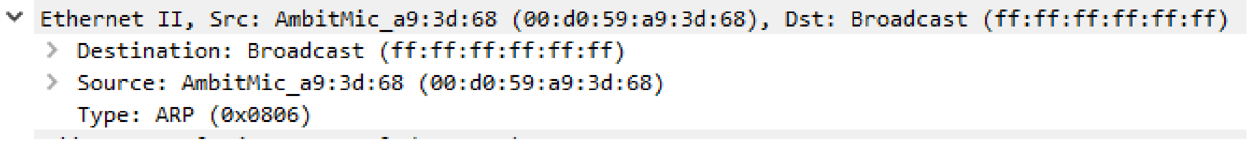
NOTE: I had trouble getting the Address Resolution Protocol to appear in my Wireshark trace so I am using the ethernet-ethereal-trace-1 file that was provided to answer these questions.



```
> 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)
v Address Resolution Protocol (request)
     Hardware type: Ethernet (1)
     Protocol type: IPv4 (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
     Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
     Target IP address: 192.168.1.1
```

The source and destination addresses are 00:d0:59:a9:3d:68 and ff:ff:ff:ff:ff:ff (broadcast address), respectively.

11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?



```
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)
```

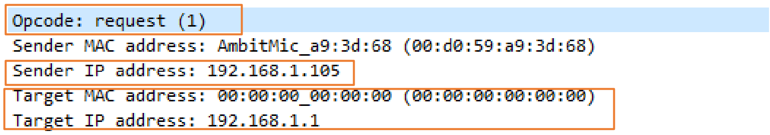
The hexadecimal value for the two-byte Ethernet Frame type field is 0x0806 which corresponds to the ARP protocol.

12.

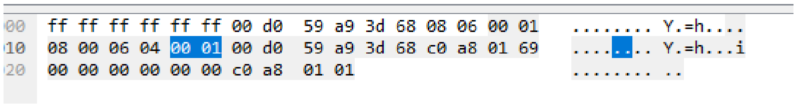
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

The opcode field begins 20 bytes from the very beginning of the Ethernet frame.

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?



```
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
```



```
00  ff ff ff ff ff ff 00 d0  59 a9 3d 68 08 06 00 01   ........ Y.=h....
10  08 00 06 04 00 01 00 d0  59 a9 3d 68 c0 a8 01 69   ........ Y.=h...i
20  00 00 00 00 00 00 c0 a8  01 01                    ........ ..
```

The hex value for the opcode field within the ARP-payload part of the Ethernet frame is 0x0001.

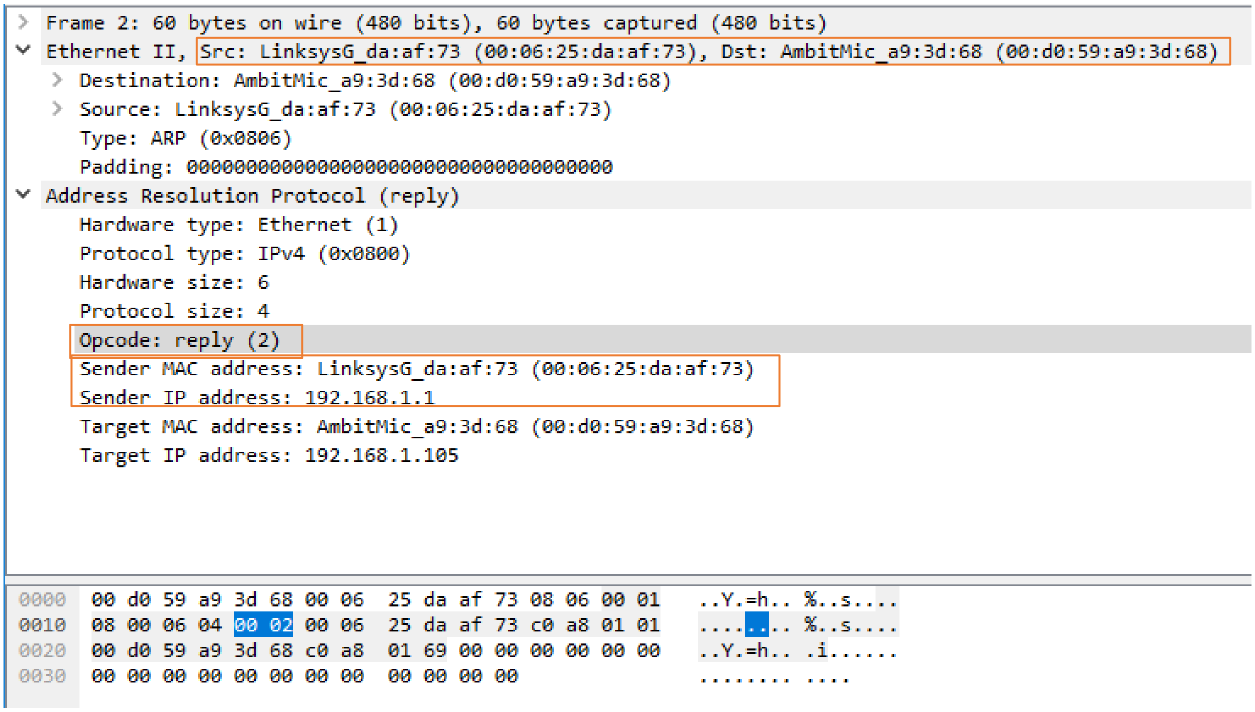
c) Does the ARP message contain the IP address of the sender?

Yes, the ARP message contains the IP address of the sender – 192.168.1.105.

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

The "question" appears in the "Target MAC address" field of the ARP request. It is querying the "Target IP address" 192.168.1.1.

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



```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
v 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)
  > Source: LinksysG_da:af:73 (00:06:25:da:af:73)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (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
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 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               ........ ....
```

ARP Reply

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

The opcode field begins 20 bytes from the very beginning of the Ethernet frame.

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?

The hex value of the opcode field within the ARP-payload part of the Ethernet frame is 0x0002, for the reply.

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?

The answer in the ARP message can be found in the "Sender MAC Address" field with the "Sender IP address" of 192.168.1.1.

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

The source and destinations addresses in the Ethernet frame containing the ARP reply message are 00:06:25:da:af:73 and 00:d0:59:a9:3d:68 respectively.

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

There is no reply in this packet trace because the ARP request is broadcast, but the ARP reply is sent back directly to the sender's Ethernet address. Because we are not at the machine that sent the request, we will not be able to see the reply.

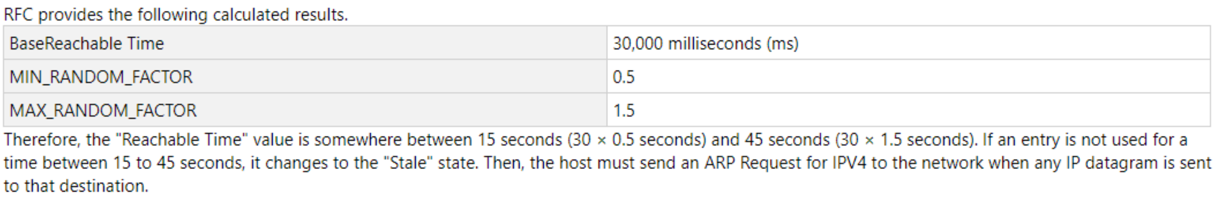
EX-1. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

Whether or not we entered the correct IP address, the router would remove the IP address from the Ethernet frame and would get the correct MAC address of the destination using ARP.

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

I found documentation on ARP caching in Windows Vista and later (including my OS). It can be found here: https://support.microsoft.com/en-us/help/949589/description-of-address-resolution-protocol-arp-caching-behavior-in-win

The TCP/IP stack implementation complies with RFC4861 protocol for IPv6 and IPv4 Neighbor Discovery process. In the new implementation, hosts create the neighbor cache entries when there is no matching entry in the neighbor cache. If an entry is used and it stays in the cache longer than its "Reachable Time" value, the entry changes to the "Stale" state and removed from the cache.



RFC provides the following calculated results.

BaseReachable Time	30,000 milliseconds (ms)
MIN_RANDOM_FACTOR	0.5
MAX_RANDOM_FACTOR	1.5

Therefore, the "Reachable Time" value is somewhere between 15 seconds (30 × 0.5 seconds) and 45 seconds (30 × 1.5 seconds). If an entry is not used for a time between 15 to 45 seconds, it changes to the "Stale" state. Then, the host must send an ARP Request for IPV4 to the network when any IP datagram is sent to that destination.

Screenshot from above source.