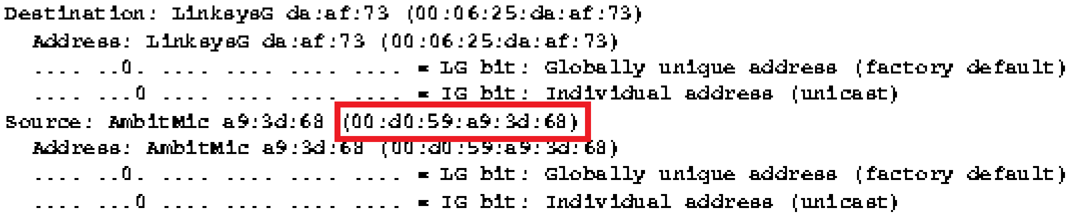
Assignment 6.01 - Wireshark Lab: Ethernet and ARP

Packet trace taken from author

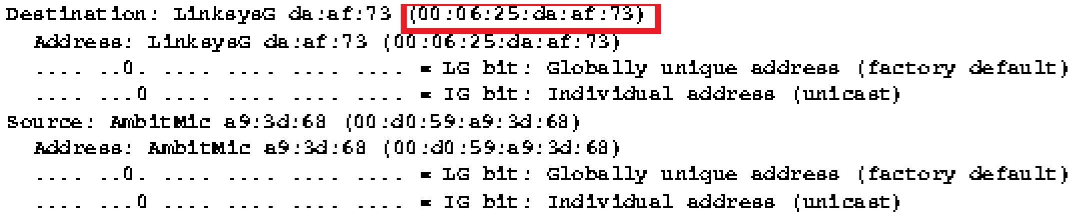
Answer 1:



```
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)
```

The 48 bit Ethernet address of the computer is **00:d0:59:a9:3d:68**

Answer 2:

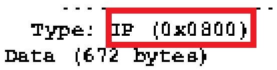


```
Destination: LinksysG da:af:73 (00:06:25:da:af:73)
  Address: LinksysG da:af:73 (00:06:25:da:af:73)
  .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: AmbitMic a9:3d:68 (00:d0:59:a9:3d:68)
  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)
```

The 48 bit destination address in Ethernet frame is **00:06:25:da:af:73**

No from the IP address of gaia.cs.umass.edu it's clear that it's in a different subnet. ARP tables are created for a subnet and the source subnet will not be aware of the Ethernet address of the destination that resides on a different subnet. The network interface of the router connecting to gaia.cs.umass.edu subnet is most likely the device to have this Ethernet address.

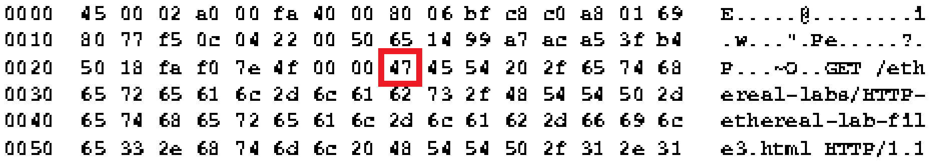
Answer 3:



```
  Type: IP (0x0800)
Data (672 bytes)
```

The two-byte frame type field is **0x0800 .** It corresponds to IP v4 protocol.

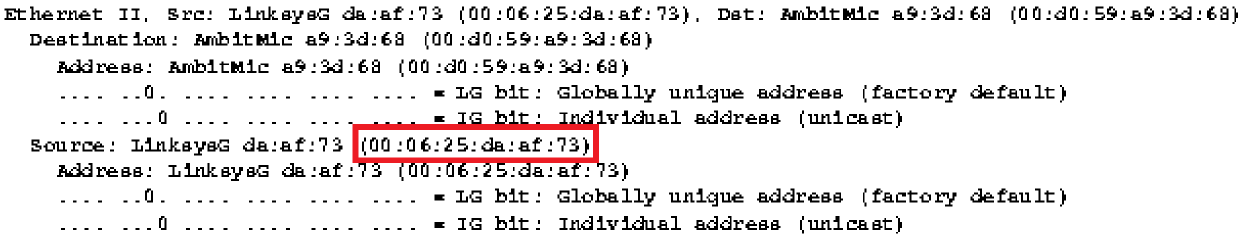
Answer 4:



```
0000  45 00 02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69   E.....@........i
0010  80 77 f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4   .w...".Pe.....?.
0020  50 18 fa f0 7e 4f 00 00 47 45 54 20 2f 65 74 68   P...~O..GET /eth
0030  65 72 65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d   ereal-labs/HTTP-
0040  65 74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c   ethereal-lab-fil
0050  65 33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31   e3.html HTTP/1.1
```

The ASCII 'G' appears at the **55th** byte position from the start of the frame

Answer 5:

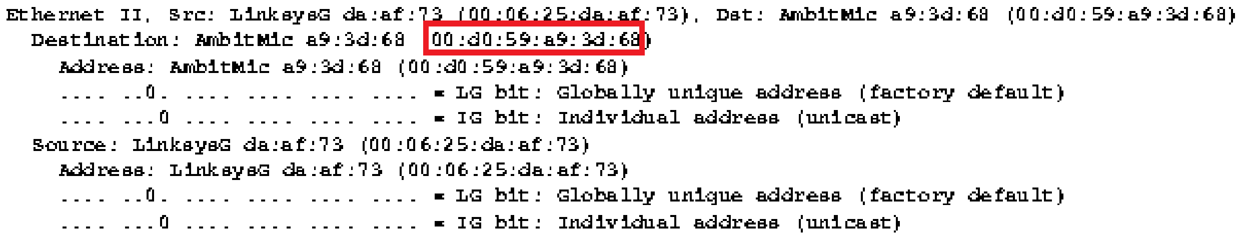


```
Ethernet II, Src: LinksysG da:af:73 (00:06:25:da:af:73), Dst: AmbitMic a9:3d:68 (00:d0:59:a9:3d:68)
  Destination: AmbitMic a9:3d:68 (00:d0:59:a9:3d:68)
    Address: AmbitMic a9:3d:68 (00:d0:59:a9:3d:68)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...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)
```

The value of the Ethernet source address is **00:06:25:da:af:73**

No this the Ethernet source address is of the router interface that is sending the frame to our subnet

Answer 6:

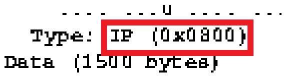


```
Ethernet II, Src: LinksysG da:af:73 (00:06:25:da:af:73), Dst: AmbitMic a9:3d:68 (00:d0:59:a9:3d:68)
  Destination: AmbitMic a9:3d:68 (00:d0:59:a9:3d:68)
    Address: AmbitMic a9:3d:68 (00:d0:59:a9:3d:68)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...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)
```

The destination address in the Ethernet frame is **00:d0:59:a9:3d:68**

Yes it’s the Ethernet address of the computer

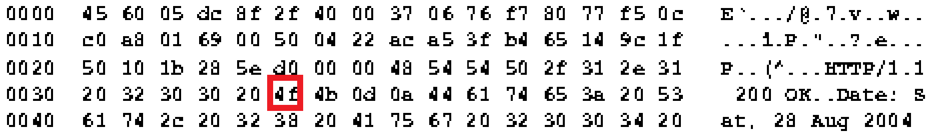
Answer 7:



```
    .... ...0 .... ...
  Type: IP (0x0800)
Data (1500 bytes)
```

The hexadecimal value for the two-byte frame type field is **0x0800** . It corresponds to IPv4 Protocol.

Answer 8:



```
0000  45 60 05 dc 8f 2f 40 00 37 06 76 f7 80 77 f5 0c   E`.../@.7.v..w..
0010  c0 a8 01 69 00 50 04 22 ac a5 3f b4 65 14 9c 1f   ...i.P."..?.e...
0020  50 10 1b 28 5e d0 00 00 48 54 54 50 2f 31 2e 31   P..(^...HTTP/1.1
0030  20 32 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53    200 OK..Date: S
0040  61 74 2c 20 32 38 20 41 75 67 20 32 30 30 34 20   at, 28 Aug 2004
```

The ASCII ‘O’ appears at the **68th** byte position from the start of the frame

Answer 9:

Following are the contents of ARP cache of my computer

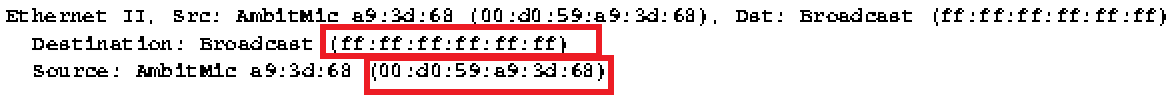
Internet Address	Physical Address	Type
172.16.192.1	00-00-5e-00-01-53	dynamic
172.16.198.35	28-cf-da-d7-6b-78	dynamic
172.16.199.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
224.0.1.60	01-00-5e-00-01-3c	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Column 1 signifies **IP address** of the interface

Column 2 signifies **Physical address(Mac address)** of the interface

Column 3 signifies **Type of entry , static cache or dynamic cache**

Answer 10:



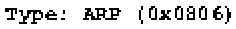
```
Ethernet II, Src: AmbitMic a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: AmbitMic a9:3d:68 (00:d0:59:a9:3d:68)
```

The source and destination address in the Ethernet frame are –

Source address – **00:d0:59:a9:3d:68**

Destination address – **ff:ff:ff:ff:ff:ff**

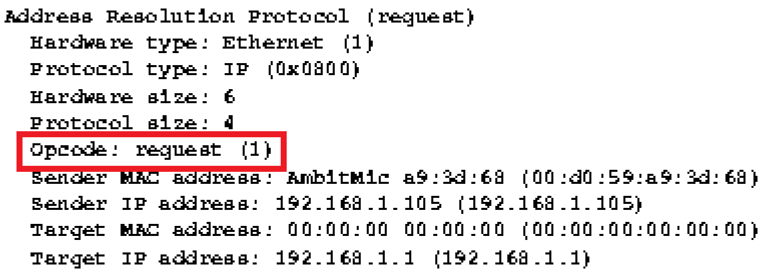
Answer 11:



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

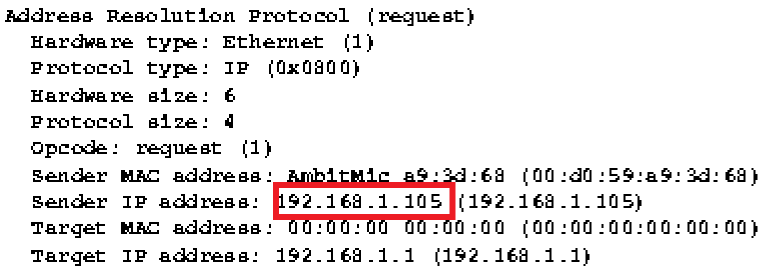
The hexadecimal value for the two-byte Ethernet frame type field is **0x0806** .It corresponds to ARP protocol.

Answer 12:



```
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)
```

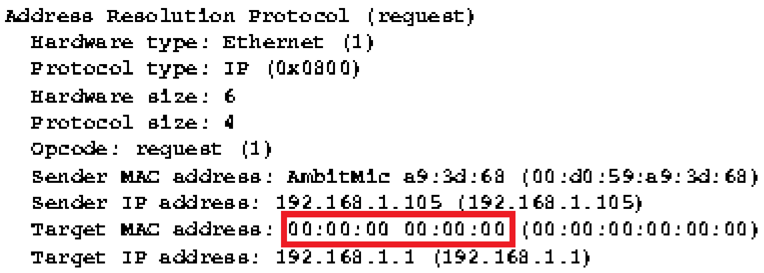
a. The *opcode* begins at the **22nd byte** from the Ethernet frame start.
b. The value of the *opcode* in the ARP payload is **1(request)**
c.



```
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)
```

Yes the ARP message contains the senders IP address.

d.



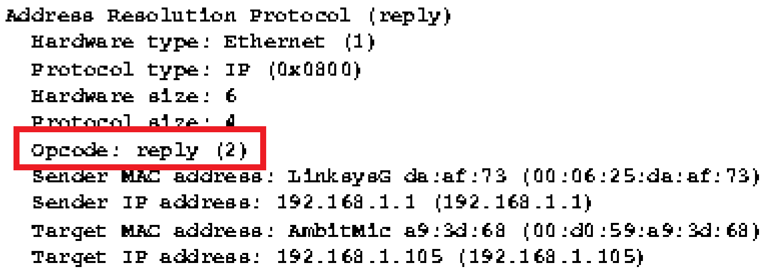
```
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: AmbitMic a9:3d:68 (00:d0:59:a9:3d:68)
  Sender IP address: 192.168.1.105 (192.168.1.105)
  Target MAC address: 00:00:00 00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.1.1 (192.168.1.1)
```

The question appears in the Target Mac address field and this is supported by the *opcode* which is 1(=request)

Answer 13.

a. The *opcode* begins at the **22nd byte** from the Ethernet frame start.

b.

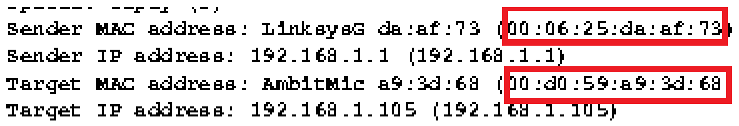


```
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: LinksysG da:af:73 (00:06:25:da:af:73)
  Sender IP address: 192.168.1.1 (192.168.1.1)
  Target MAC address: AmbitMic a9:3d:68 (00:d0:59:a9:3d:68)
  Target IP address: 192.168.1.105 (192.168.1.105)
```

The value of the *opcode* within the ARP-payload part of the Ethernet frame is **2(=reply)**

c. The answer is located in the Sender Mac Address.

Answer 14.



```
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)
```

The hexadecimal values for the source and destination addresses in the ARP reply message are –

Source - **00:06:25:da:af:73**

Destination – **00:d0:59:a9:3d:68**

Answer 15.

For the Packet number 6, the only reason for the ARP reply not received could be that the device has disconnected itself from the network and the ARP tables are have been cleared after the timeout. Therefore there is no reply by any of the participating hosts of the subnet to the ARP request.

EXTRA CREDIT

EX-1.

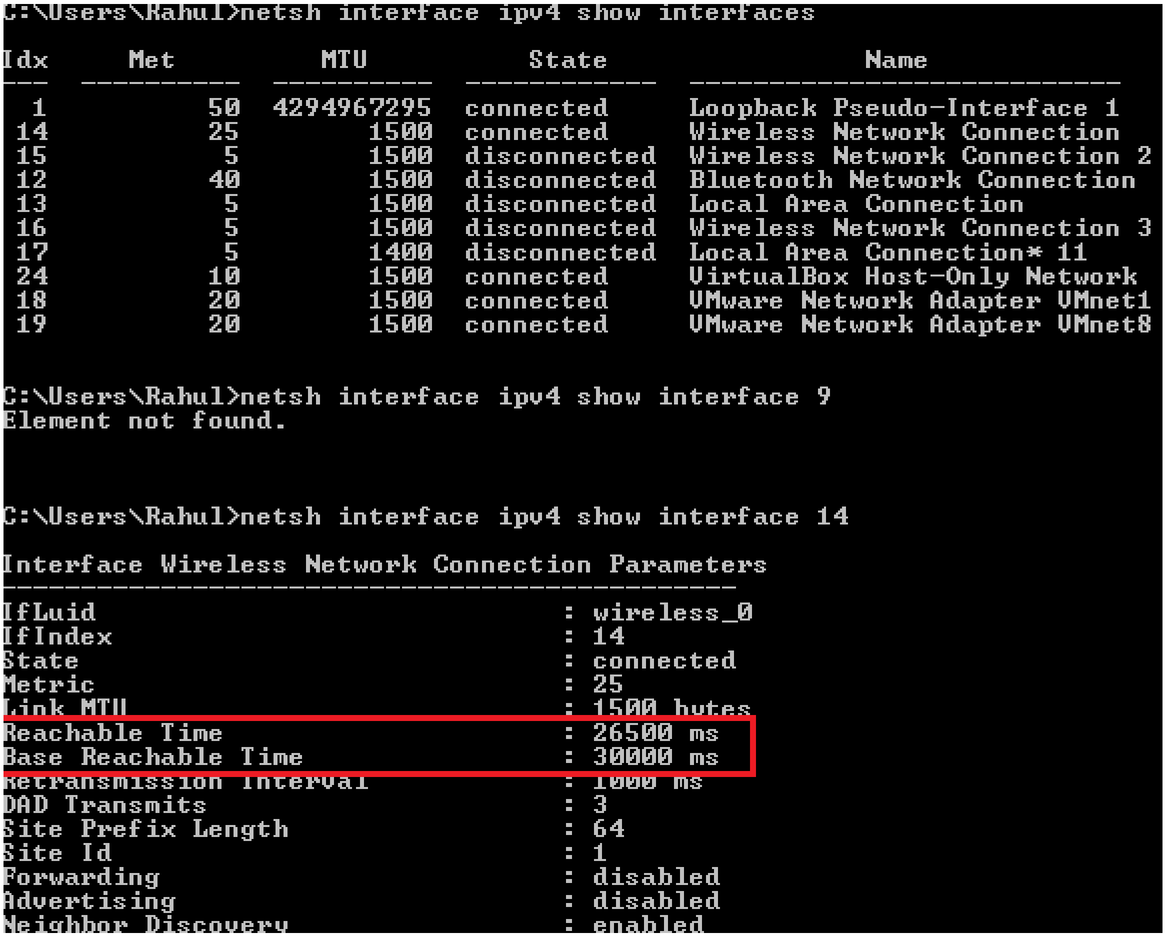
Putting the wrong address sometimes gives strange results. I found that by just configuring some IP addresses MAC address we can still get away because there are other hosts that will help propagate the packet. But for a personal site where none of participating routers and hosts have no entry, it can be blocked by adding an invalid MAC address .

EX-2 In Microsoft , the table itself classifies the type into Static and Dynamic. The static cache has to be manually updated when network interface equipment changes.

In dynamic cache, the entries for windows 2000 have a default timeout of 10minutes

In Windows 7/Vista – A much robust way of Timeout is implemented. Here once an entry is added it's in a reachable state and a formula helps calculate the reachable time. If the entry exceeds this reachable time, it moves to a stale state. After this state another ARP request is to be sent and if this does not receive a reply then the entry will be removed by the Operating System. The timeout range is somewhere between 15- 45 seconds.

Below is a capture for the Wireless Connection interface on my Laptop



```
C:\Users\Rahul>netsh interface ipv4 show interfaces

Idx     Met         MTU          State                Name
---  ----------  ----------  ------------  ---------------------------
  1          50  4294967295  connected     Loopback Pseudo-Interface 1
 14          25        1500  connected     Wireless Network Connection
 15           5        1500  disconnected  Wireless Network Connection 2
 12          40        1500  disconnected  Bluetooth Network Connection
 13           5        1500  disconnected  Local Area Connection
 16           5        1500  disconnected  Wireless Network Connection 3
 17           5        1400  disconnected  Local Area Connection* 11
 24          10        1500  connected     VirtualBox Host-Only Network
 18          20        1500  connected     VMware Network Adapter VMnet1
 19          20        1500  connected     VMware Network Adapter VMnet8


C:\Users\Rahul>netsh interface ipv4 show interface 9
Element not found.


C:\Users\Rahul>netsh interface ipv4 show interface 14

Interface Wireless Network Connection Parameters
----------------------------------------------
IfLuid                             : wireless_0
IfIndex                            : 14
State                              : connected
Metric                             : 25
Link MTU                           : 1500 bytes
Reachable Time                     : 26500 ms
Base Reachable Time                : 30000 ms
Retransmission Interval            : 1000 ms
DAD Transmits                      : 3
Site Prefix Length                 : 64
Site Id                            : 1
Forwarding                         : disabled
Advertising                        : disabled
Neighbor Discovery                 : enabled
```

There are two parameters here that decide on the state of that Entry and this is configured per interface -

1. Reachable time
2. Base reachable time

Further details found here -> https://support.microsoft.com/en-us/kb/949589