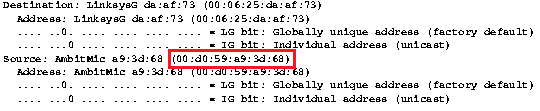
**Assignment 6.01 - Wireshark Lab: Ethernet and ARP**

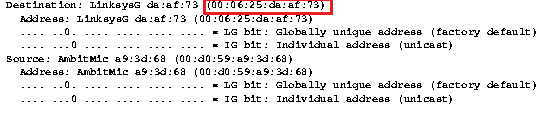
**Packet trace taken from author**

**Answer 1:**

****

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

**Answer 2:**

****

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

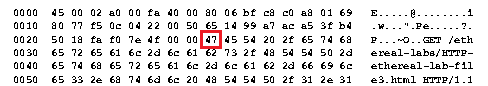
No from the IP address of gaia.cs.umass.edu it’s clear that it’s in a different subnet. ARP tables are created for a subnet and the source subnet will not be aware of the Ethernet address of the destination that resides on a different subnet. The network interface of the router connecting to gaia.cs.umass.edu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

**Answer 3:**

****

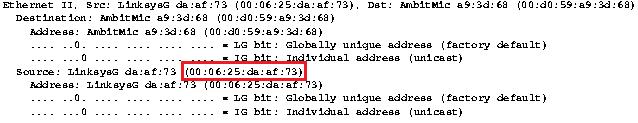
The two-byte frame type field is **0x0800 .** It corresponds to IP v4 protocol.

**Answer 4:**

****

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

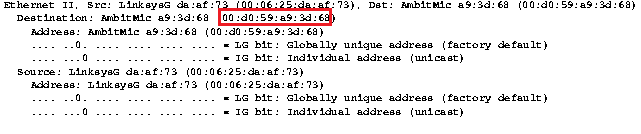
**Answer 5:**

****

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:**

****

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

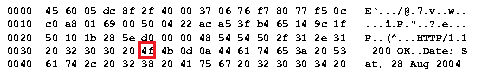
Yes it’s the Ethernet address of the computer

**Answer 7:**

****

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

**Answer 8:**

****

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:**

****

The source and destination address in the Ethernet frame are –

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

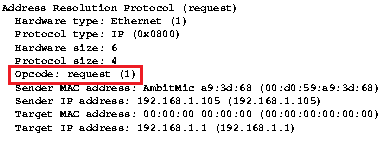
Destination address – **ff:ff:ff:ff:ff:ff**

**Answer 11:**

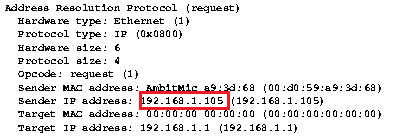
****

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

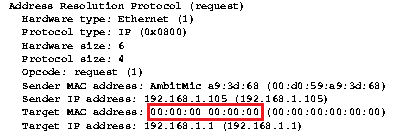
**Answer 12:**

****

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

****

Yes the ARP message contains the senders IP address.

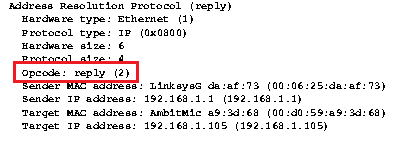


The question appears in the Target Mac address field and this is supported by the *opcode* which is 1(=request)

**Answer 13.**

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

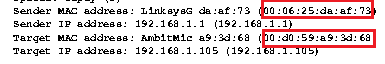
b.



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.**



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.**

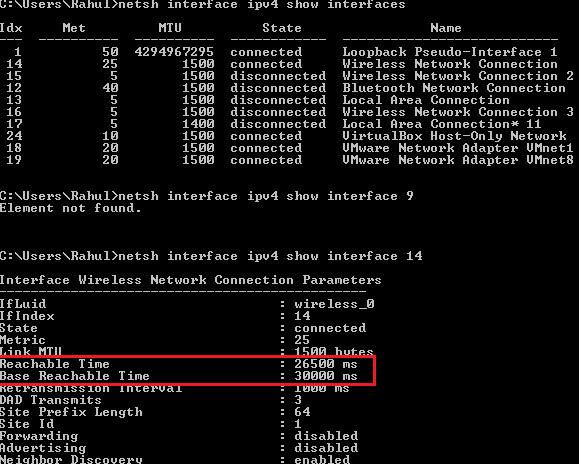
Putting the wrong address sometimes gives strange results. I found that by just configuring some IP addresses MAC address we can still get away because there are other hosts that will help propagate the packet. But for a personal site where none of participating routers and hosts have no entry, it can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



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