Ethernet and ARP Lab

In this lab, you will analyze Ethernet and ARP traffic using Wireshark. Follow the instructions below and answer each question in detail. Be sure to include screenshots or listings where appropriate.

Opening the Wireshark Trace File

To analyze the Ethernet and ARP traffic in this lab, you need to open the provided trace file `ethernet-ether` in Wireshark.

1. Download the `wireshark-traces.zip` file from the course materials on Canvas.
2. Unzip the file, which should include the trace file `ethernet-ethereal-trace-1`.
3. In Wireshark, go to `File -> Open` and navigate to the directory where the unzipped trace files are located. Select the file `ethernet-ethereal-trace-1` and click `Open`.

Lab Questions

Q1: **Packet 10**

(a) What is the 48-bit Ethernet address of the source computer? Who is the manufacturer of this device?
`00:d0:59:a9:3d:68` - Ambit Microsystems Corp.

(b) What is the 48-bit destination address in the Ethernet frame? Who is the manufacturer of this device?
`00:06:25:da:af:73` - The Linksys Group, Inc.

(c) Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
`0x0800` - IPv4

(d) How many bytes from the very start of the Ethernet frame does the ASCII character G in GET appear in the Ethernet frame?
55 bytes in.

Q2: **Packet 12**

(a) What is the value of the Ethernet source address?
`00:06:25:da:af:73`

(b) What is the destination address in the Ethernet frame?
`00:d0:59:a9:3d:68`

(c) Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
`0x0800` - IPv4

(d) How many bytes from the very start of the Ethernet frame does the ASCII character O in OK (i.e., the HTTP response code) appear in the Ethernet frame?
68

Q3: **ARP Cache**

(a) In your terminal, run the `arp` command (`arp -n`) and write down the contents of your computer's ARP cache. What is the meaning of each column value?

```
Address                     HWtype  HWaddress
140.160.137.1               ether   54:51:de:c8:51:bf
140.160.137.30              ether   02:42:8c:a0:89:1e
```

Address Is the destination IPv4 address that we are caching

HWtype Is presumably the type of communication used to get it

HWaddress Is the cached hardware address of the IPv4

Q4: **Ethernet Frame with ARP Request**

(a) What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message? What is this message doing?
`00:d0:59:a9:3d:68` -> `ff:ff:ff:ff:ff:ff`
This message is asking for the hardware address of `192.168.1.1`.

(b) Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
`0x0806` - ARP

Q5: **ARP Specification**

(a) Refer to this discussion of ARP or the slides.

(i) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
21

(ii) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?
`0x0001`

(iii) Does the ARP message contain the IP address of the sender?
Yes

(iv) Where in the ARP request does the "question" appear — the Ethernet address of the machine whose corresponding IP address is being queried?
The very end of the message- or the last 4 bytes.

Q6: **ARP Reply**

(a) Find the ARP reply sent in response to the ARP request.

(i) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
21

(ii) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?
`0x0002`

(iii) 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 is stored in the sender's hardware address in the ARP packet.

(b) What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?
`00:06:25:da:af:73` -> `00:d0:59:a9:3d:68`

Q7: **Unanswered ARP Request**

(a) The first and second ARP packets correspond to an ARP request and ARP reply. Packet 6 contains another ARP request. Why is there no ARP reply in response to the request in packet 6?
One possibility is that there was an error in sending or receiving the message to the machine that was at the destination address. Another possibility is that the machine itself is not connected (which, technically, could be considered an error).

Q8: **Wireshark Statistics**

(a) Browse through the different Statistics options in Wireshark (`Statistics -> Capture File Properties`). What does the Packet size limit refer to: IP or Ethernet?
65535 bytes, which refers to the IP limit.

Q9: **Wireshark 802.11 Trace**

(a) Open the `Wireshark 802.11` trace file. Find the smallest and largest packets at layer 2. What protocol is used for the smallest frame? What protocol is used for the largest frame? (Not the code, but the name of the layer 2 protocol.)

Both the smallest and largest packets are using the 802.11 protocol.

Q10: **ARP Cache Timeout**

(a) What is the default amount of time that an entry remains in your ARP cache before being removed in seconds? Do this by running this command:

```
cat /proc/sys/net/ipv4/neigh/default/base_reachable_time_ms
```

30,000 milliseconds → 30 seconds