Computer Network 1

LAB 6

Wireshark lab Ethernet and ARP

Student Name: Alexandre Rousseau

Student ID: 1952001

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

The Ethernet address of my computer is 00:22:75:af:71:6b.

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?

00:16:cb:c1:5f:50. This is the Ethernet address of my external router.

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

0x0800 means that this frame is of the IP Protocol type.

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

53 bytes from the start.

5) What is the value of the Ethernet source address? What device has this as its Ethernet address

00:16:cb:c1:5f:50. It is the address of neither. It the address of my external router.

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

00:22:75:af:71:6b. It is the Ethernet address of my wireless USB adapter, so yes.

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

0x0800. The bits signify that this is an IP Protocol frame.

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

66 bytes from the start.

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

Address	HWtype	HWaddress	Flags	Mask	Iface
Base–Station–N.local	ether	00:16:cb:c1:5f:50	C		wlan0

Address: A named reference to the MAC address of the network router.

HWtype: The type of hardware address.

HWaddress: The actual hardware address.

Flags: Flags attached to the address. C means Cached.

Mask: What this address could be hidden as.

Iface: The interface on which this address resides.

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

Source: 00:22:75:af:71:6b. Destination: ff:ff:ff:ff:ff:ff.

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

0x0806. Its specifics that this packet is using the ARP protocol.

12)

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

21 Bytes after the beginning.

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?

0x0001 (Request).

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

Yes. It is 10.0.1.20.

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

Starting at byte 33 and going till byte 39. It comes just after the sender Ethernet address and IP address is listed.

```
No.     Time        Source                Destination           Protocol
    Length Info
     17 14.979987   BelkinIn_af:71:6b     Broadcast             ARP
        42      Who has 10.0.1.1?  Tell 10.0.1.20

Frame 17: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: BelkinIn_af:71:6b (00:22:75:af:71:6b), Dst: Broadcast
    (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Source: BelkinIn_af:71:6b (00:22:75:af:71:6b)
    Type: ARP (0x0806)
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: False]
    Sender MAC address: BelkinIn_af:71:6b (00:22:75:af:71:6b)
    Sender IP address: 10.0.1.20 (10.0.1.20)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.0.1.1 (10.0.1.1)

0000   ff ff ff ff ff ff 00 22 75 af 71 6b 08 06 00 01    .......”u.qk....
0010   08 00 06 04 00 01 00 22 75 af 71 6b 0a 00 01 14    .......”u.qk....
0020   00 00 00 00 00 00 0a 00 01 01                      ..........
```

13)

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

21 bytes after the 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?

0x0002 (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?

7 bytes after the opcode. The 6 bytes after the opcode is used for the Ethernet address of the queried machine.

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

Source: 00:16:cb:c1:5f:50. Destination: 00:22:75:af:71:6b.

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

There is no ARP reply sent because the Ethernet address in the request does not match the local machines hardware address.

```
No.     Time        Source                Destination           Protocol
   Length Info
     18 14.992318   AppleCom_c1:5f:50     BelkinIn_af:71:6b     ARP      42
            10.0.1.1 is at 00:16:cb:c1:5f:50

Frame 18: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50), Dst: BelkinIn_af:71:6b
   (00:22:75:af:71:6b)
    Destination: BelkinIn_af:71:6b (00:22:75:af:71:6b)
    Source: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50)
    Type: ARP (0x0806)
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    [Is gratuitous: False]
    Sender MAC address: AppleCom_c1:5f:50 (00:16:cb:c1:5f:50)
    Sender IP address: 10.0.1.1 (10.0.1.1)
    Target MAC address: BelkinIn_af:71:6b (00:22:75:af:71:6b)
    Target IP address: 10.0.1.20 (10.0.1.20)

0000  00 22 75 af 71 6b 00 16 cb c1 5f 50 08 06 00 01    ."u.qk...._P....
0010  08 00 06 04 00 02 00 16 cb c1 5f 50 0a 00 01 01    ..........._P....
0020  00 22 75 af 71 6b 0a 00 01 14                      ."u.qk....
```

EXTRA CREDIT:

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?

It disables that interface. All outbound requests go nowhere.

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

60 seconds. It can be found in /proc/sys/net/ipv4/neigh/wlan0/ gc stale time.