



Başkent Üniversitesi
Elektrik - Elektronik Mühendisliği Bölümü

EEM 438

Deney No: 5

1. Capturing and analyzing Ethernet frames

The image shows a Wireshark capture window titled "(Untitled) - Wireshark". The main pane displays a list of captured packets. The first packet is an Ethernet II frame from Netgear_61:8e:6d to LinksysG_45:90:a8. The packet details pane shows the frame structure: Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: LinksysG_45:90:a8 (00:0c:41:45:90:a8). The packet type is IP (0x0800). The packet data pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	Netgear_61:8e:6d	LinksysG_45:90:a8	0x0800	IP
2	0.000000	LinksysG_45:90:a8	Netgear_61:8e:6d	0x0800	IP
3	0.000000	LinksysG_45:90:a8	LinksysG_45:90:a8	0x0800	IP
4	0.055906	Netgear_61:8e:6d	LinksysG_45:90:a8	0x0800	IP
5	0.128700	LinksysG_45:90:a8	Netgear_61:8e:6d	0x0800	IP
6	0.134167	LinksysG_45:90:a8	Netgear_61:8e:6d	0x0800	IP
7	0.150302	LinksysG_45:90:a8	Netgear_61:8e:6d	0x0800	IP
8	0.150487	Netgear_61:8e:6d	LinksysG_45:90:a8	0x0800	IP
9	0.213639	LinksysG_45:90:a8	Netgear_61:8e:6d	0x0800	IP
10	0.213639	Netgear_61:8e:6d	LinksysG_45:90:a8	0x0800	IP
11	0.232143	Netgear_61:8e:6d	LinksysG_45:90:a8	0x0800	IP
12	0.320470	Netgear_61:8e:6d	LinksysG_45:90:a8	0x0800	IP
13	0.403428	LinksysG_45:90:a8	Netgear_61:8e:6d	0x0800	IP
14	0.579522	Netgear_61:8e:6d	LinksysG_45:90:a8	0x0800	IP
15	3.383584	Netgear_61:8e:6d	LinksysG_45:90:a8	0x0800	IP
16	9.392197	Netgear_61:8e:6d	LinksysG_45:90:a8	0x0800	IP
17	10.389131	LinksysG_45:90:a8	Netgear_61:8e:6d	0x0800	IP
18	10.389258	Netgear_61:8e:6d	LinksysG_45:90:a8	0x0800	IP

Frame 4 (506 bytes on wire, 506 bytes captured)

Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: LinksysG_45:90:a8 (00:0c:41:45:90:a8)

- Destination: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
Address: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
.....0..... = IG bit: Individual address (unicast)
.....0..... = LG bit: Globally unique address (factory default)
- Source: Netgear_61:8e:6d (00:09:5b:61:8e:6d)
Address: Netgear_61:8e:6d (00:09:5b:61:8e:6d)
.....0..... = IG bit: Individual address (unicast)
.....0..... = LG bit: Globally unique address (factory default)

Type: IP (0x0800)
Data (492 bytes)

0000 00 0c 41 45 90 a8 00 09 5b 61 8e 6d 08 00 45 00 ..AE... [a.m..E.
0010 01 ec 87 e9 40 00 80 06 38 65 c0 a8 02 91 80 77@...8e....w
0020 f5 0c 07 f6 00 50 7a 74 c4 58 7d a6 27 90 50 18 Pzt.X).P.
0030 ff ff 3a 9c 00 00 47 45 54 20 2f 77 69 72 65 73 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

Ethernet (eth), 14 bytes P: 21 D: 21 M: 0 Drops: 0

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

Ethernet Adresi: 00:09:5b:61:8e:6d

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as Ethernet address?

Destination adres: 00:0c:41:45:90:a8 gaia.cs.umass.edu.'nun Ethernet Adresi değildir. Bu adres, Linksys router'imin adresidir.

3. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field?

Two – byte Frame type field'in hexadecimal değeri 0x0800' dir.

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

ASCII “G”, ethernet frame'in başından itibaren 52 byte olarak görülmektedir. 14byte Ethernet frame, 20 byte IP header, 20 byte TCP header'dır.

5. What is the hexadecimal value of the CRC field in this Ethernet frame?

Ethernet frame'indeki CRC field'in hexadecimal karşılığı 0x0d0a0d0a.

6. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

Destination adres: 00:0c:41:45:90:a8 gaia.cs.umass.edu.'nun Ethernet Adresi değildir. Bu adres, Linksys router'ının adresidir.

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

Ethernet frame'in destination adresi 00:09:5b:61:8e:6d. Bu adres aynı zamanda benim bilgisayarımın adresi.

8. Give the hexadecimal value for the two-byte Frame type field. What do the bit(s) whose value is 1 mean within the flag field?

Frame type field'in hexadecimal değeri 0x0800'dir.

9. 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?

ASCII “O” da ASCII “G” ile aynıdır. Yani; ethernet frame'in başından itibaren 52 byte olarak görülmektedir. 14byte Ethernet frame, 20 byte IP header, 20 byte TCP header'dır.

10. What is the hexadecimal value of the CRC field in this Ethernet frame?

Ethernet frame'indeki CRC field'in hexadecimal karşılığı 0x0d0a0d0a.

2. The Address Resolution Protocol

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

```
C:\Windows\system32\command.com
Microsoft(R) Windows DOS
(C)Copyright Microsoft Corp 1990-2001.
C:\USERS\MMT>arp

Adres çözünürlüğü protokolü (ARP) tarafından kullanılan IP-Fiziksel
adrese çevirme tablolarını görüntüler ve değiştirir.

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Geçerli protokol verilerini sorgulayarak
            geçerli ARP girdilerini görüntüler. inet_addr
            belirtilmişse, yalnızca belirtilen bilgisayar için IP ve
            Fiziksel adresler görüntülenir. Birden fazla ağ arabirimi
            ARP kullanıyorsa, her ARP tablosunun girdileri görüntülenir.
            -a ile aynı.
-g          Geçerli ARP girdilerini özet modda görüntüler. Tüm geçersiz
            girdiler ve geri döngü arabirimindeki girdiler gösterilir.
-v          İnternet adresini belirtir.
            if_addr ile belirtilen ağ arabiriminin ARP girdilerini
            görüntüler.
-d          inet_addr ile belirtilen ana bilgisayarını siler. Tüm ana
            bilgisayarları silmek için inet_addr olarak * joker karakteri
            kullanılabilir.
-s          Ana bilgisayar ekler ve inet_addr İnternet adresini eth_addr
            Fiziksel adresiyle ilişkilendirir. Fiziksel adres, kısa
            çizgilerle ayrılmış 6 onaltılı bayttan oluşur. Girdi
            kalıcıdır.
            eth_addr Fiziksel adresi belirtir.
            if_addr Bu kullanılırsa, adres çeviri tablosu değiştirilmesi
            gereken arabirimin İnternet adresini belirtir.
            Bu kullanılmazsa, ilk uygun arabirim kullanılacaktır.

Örnek:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Statik bir girdi ekler.
> arp -a .... ARP tablosunu görüntüler.

C:\USERS\MMT>
```

Buradan arp -a komutunu kullanarak ARP tablosunu görüntüleyebileceğimizi gördük:

```
C:\USERS\MMT>arp -a

Arabirin: 192.168.1.100 --- 0xb
Internet Adresi      Fiziksel Adres      Tipi
192.168.1.1          00-22-6b-e4-ea-08   dinamik
192.168.1.255        ff-ff-ff-ff-ff-ff   statik
224.0.0.22           01-00-5e-00-00-16   statik
224.0.0.252          01-00-5e-00-00-fc   statik
224.0.0.253          01-00-5e-00-00-fd   statik
239.255.255.250      01-00-5e-7f-ff-fa   statik
```

Burada internet adresi sütunu IP adresini, fiziksel adres sütunu MAC adresini ve son olarak tipi sütunu ise protokol tipini içermektedir.

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

```
Frame 1 (42 bytes on wire, 42 bytes captured)
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)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
      ....1.... = IG bit: Group address (multicast/broadcast)
      ....1.... = LG bit: Locally administered address (this is NOT the factory default)
  Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      ....0.... = IG bit: Individual address (unicast)
      ....0.... = LG bit: Globally unique address (factory default)
  Type: ARP (0x0806)
  Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
```

Yukarıda da görüldüğü gibi kaynak adresin onaltılı değeri 00:d0:59:a9:3d:68, varış adresinin onaltılı değeri ise ff:ff:ff:ff:ff:ff dir.

13. Give the hexadecimal value for the two-byte Ethernet Frame type field. What do the bit(s) whose value is 1 mean within the flag field?

ARP'ta ethernet frame type field için onaltılı değer 0x0806'dir.

14. Download the ARP specification from <ftp://ftp.rfc-editor.org/in-notes/std/std37.txt>. A readable, detailed discussion of ARP is also at <http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>.

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

ARP opcode field'ları 20 byte'la başlar.

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?

Davet için olan ARP payload'larının opcode alanının onaltılı değeri 0x0001'dir. Bunun anlamı ARP numarası 10 demektir.

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

ARP mesajları göndericinin IP adresini de içerir bu adres ise 192.168.1.105'dir.

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

ARP davetleri Target MAC adres alanında görülür ve 00:00:00:00:00:00'e ayarlanır. (IP adresi 192.168.1.1'dir.)

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

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

ARP opcode field'ları 20 byte'ya başlar.

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?

Cevap için olan ARP payload'larının opcode alanının onaltılı değeri 0x0002'dir. Bunun anlamı ARP numarası 13 demektir.

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?

ARP mesaj cevapları gönderici MAC adresinde görünür. Bu IP adresi 192.168.1.1 olan gönderici için Ethernet address 00:06:25:da:af:73'dir.

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

Source adresinin hex değeri: 00:06:25:da:af:73

Destination adresinin hex değeri: 00:d0:59:a9:3d:68

17. Open the ethernet-ethereal-trace-1 trace file in . The first and second <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

Arp istekleri broadcast'tir hepsine yollanır ama ARP cevapları direk göndericinin Ethernet adresine gönderilir.