Όνοματεπώνυμο: Ζευγολατάκος Παναγιώτης		Ομάδα: 3
Όνομα PC/ΛΣ: panos-PC / Windows 10		Ημερομηνία:19/10/2020
Διεύθυνση IP: 192.168.2.2	Διεύθυνση MAC: D0-50-99-75-F8-F8	

Εργαστηριακή Άσκηση 3
Επικοινωνία στο τοπικό δίκτυο
(πλαίσιο Ethernet και πρωτόκολλο ARP)

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

Άσκηση 1

1.1 arp -a

1.2 arp -d

1.3 ipconfig /all

```
Default Gateway . . . . . . . . . : fe80::1%16
                                    192.168.2.1
DHCP Server . . . . . . . . . . . : 192.168.2.1
DHCPv6 IAID . . . . . . . . . . . : 248533145
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-8A-
DNS Servers . . . . . . . . . . . : fe80::1%16
                                    192.168.2.1
NetBIOS over Tcpip. . . . . . . . : Enabled
```

1.4

```
Interface: 192.168.2.2 --- 0x10
  Internet Address      Physical Address      Type
  192.168.2.1           e0-19-54-25-47-58     dynamic
  192.168.2.255         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
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

1.5 Ναι, υπάρχουν

1.6 Χρήση εντολής arp -d και εντολής ping 192.168.2.3

1.7 Μετά από τη χρήση της εντολής ping 192.168.2.3 παρατηρώ πως έχει προστεθεί στον πίνακα η διεύθυνση 192.168.2.3 που είχε χαθεί από τη χρήση της εντολής arp -d.

1.8 Έχει καταχωρηθεί η διεύθυνση 192.168.2.1, η οποία αντιστοιχεί στον εξυπηρετητή DNS. Αυτό συνέβη, διότι εκείνος βρίσκει ποια IP διεύθυνση αντιστοιχεί στο URL της ιστοσελίδας, επομένως η διεύθυνσή του λαμβάνεται μέσω ARP.

1.9 Όχι, δεν έχει καταχωρηθεί, εφόσον βρίσκεται σε διαφορετικό υποδίκτυο.

Άσκηση 2

2.1 0x0800

2.2 0x0806

2.2 0x86dd

2.4 Source: d0:50:99:75:f8:f8

2.5 Destination: e0:19:54:25:47:58

2.6 Όχι

2.7 Αντιστοιχεί στον δρομολογητή· εφόσον δεν έχουμε απευθείας σύνδεση στο διαδίκτυο, είναι απαραίτητο να χρησιμοποιηθεί ο δρομολογητής.

2.8 Η δεκαεξαδική τιμή του πεδίου είναι 0x0800 και υποδεικνύει πρωτόκολλο IPv4.

2.9 Frame Length: 499 bytes (3992 bits)

2.10 Προηγούνται 54 Bytes.

2.11 Source: e0:19:54:25:47:58

2.12 Όχι

2.13 Στον δρομολογητή.

2.14 Destination: d0:50:99:75:f8:f8

2.15 Στον τοπικό υπολογιστή.

2.16 0x0800

2.17 Frame Length: 468 bytes (3744 bits).

2.18 Προηγούνται 67 Bytes.

2.19 Destination MAC Address, Source MAC Address, Ether Type, Payload.

2.20 Εφόσον η σύλληψή του δεν είναι άμεση, το CRC δεν καταγράφεται από το WireShark. Θα πρέπει το πεδίο FCS να είναι μέρος του πλαισίου.

Άσκηση 3

3.1 Με την εφαρμογή αυτού του φίλτρου παίρνουμε τα πακέτα που έχουν ως Source ή Destination το MAC Address του υπολογιστή.

3.2 Εμφανίζονται μόνο τα πακέτα του προηγουμένου φίλτρου τα οποία έχουν το πρωτόκολλο ARP.

3.3 Ανταλλάχθηκε 1 πακέτο ARP (βλέπουμε το ζευγάρι request-reply στο WireShark).

3.4 Παίρνουμε τα πακέτα που είτε έχουν ως Source ή Destination το MAC Address του υπολογιστή, (λογικό) ή έχουν το πρωτόκολλο ARP.

3.5

3.6 Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)

3.7 Ο τύπος του πρωτοκόλλου είναι IPv4, επομένως το μέγεθος της διεύθυνσης του πρωτοκόλλου είναι 4 Bytes.

3.8 Ο τύπος του πρωτοκόλλου είναι Ethernet, επομένως του μέγεθος της διεύθυνσης του Hardware είναι 6 Bytes (το οποίο είναι MAC Address).

3.9 Η MAC Address του αποστολέα είναι του τοπικού υπολογιστή και η MAC Address του παραλήπτη είναι η ff:ff:ff:ff:ff:ff, επομένως το λαμβάνουν όλοι οι υπολογιστές που είναι συνδεδεμένοι στο τοπικό υποδίκτυο (Broadcast).

3.10 0x0806 και υποδεικνύει πρωτόκολλο ARP.

3.11

```
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   Address: Broadcast (ff:ff:ff:ff:ff:ff)
   .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
   .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)

Source: ASRockIn_75:f8:f8 (d0:50:99:75:f8:f8)
   Address: ASRockIn_75:f8:f8 (d0:50:99:75:f8:f8)
   .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
```

Επομένως, το πακέτο στάλθηκε σε ομαδική και τοπική διεύθυνση και στάλθηκε από ατομική και μοναδική διεύθυνση.

3.12 Στο πρώτο και στο δεύτερο LS bit του MS Byte.

3.13 Το ARP έχει μέγεθος 28 Bytes και το πλαίσιο Ethernet που το μεταφέρει έχει μέγεθος 42 Bytes.

3.14 20 Bytes.

3.15 1 (request)

3.16 Sender MAC Address.

3.17 Sender IP Address.

3.18 Targer IP Address.

3.19 Υπάρχει, είναι η Target MAC Address και περιέχει την τιμή 00:00:00:00:00:00.

3.20 Η MAC Address του παραλήπτη είναι η MAC Address του υπολογιστή και η MAC Address του αποστολέα ανήκει στον εξυπηρετητή DNS που έγινε ping.

3.21 0x0806 και υποδεικνύει πρωτόκολλο ARP.

3.22 20 Bytes (το ίδιο με το request).

3.23 2 (reply)

3.24 Sender IP Address.

3.25 Sender MAC Address.

3.26 Target IP Address.

3.27 Sender MAC Address.

3.28 Το ARP έχει μέγεθος 28 Bytes και το πλαίσιο Ethernet που το μεταφέρει έχει μέγεθος 60 Bytes.

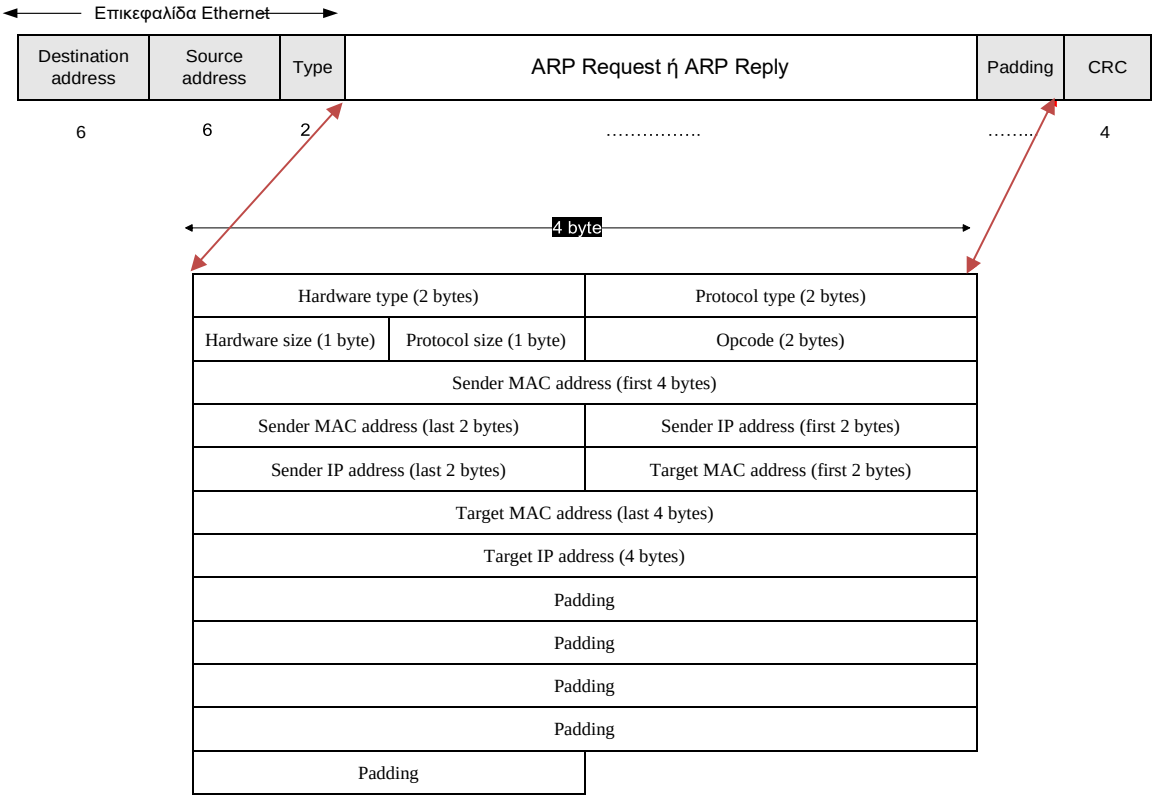
3.29 Το ARP έχει ίδιο μέγεθος με το ερώτημα 3.13, αλλά λόγω του padding, το μέγεθος του πλαισίου Ethernet είναι 18 Bytes μεγαλύτερο στο reply.

3.30 Το διαφορετικό μήκος πλαισίων Ethernet για πακέτα ARP reply και ARP request, δοθέντος ότι η δομή των πακέτων ARP request/reply είναι η ίδια, εξηγείται από τη βιβλιοθήκη npcap, η οποία συλλαμβάνει τα απερχόμενα πακέτα προτού μεταδοθούν (και εννοείται τα επερχόμενα πακέτα αφού έχουν μεταδοθεί). Επομένως, στα ARP requests δεν έχει προστεθεί ακόμα το padding για να διαμορφωθεί το πλαίσιο Ethernet, ενώ στα ARP replies έχει προστεθεί (εφόσον έχει μεταδοθεί).

3.31 Το πεδίο Type.

3.32 Το πεδίο Opcode.

3.33 Ο υπολογιστής που θα έκανε το request, θα νόμιζε πως ο κακόβουλος υπολογιστής είναι ο παραλήπτης και έτσι θα συνεχιζόταν η επικοινωνία μαζί του, δίνοντάς του τη δυνατότητα να υποκλέψει μηνύματα (eavesdropping) ή να τα αλλοιώσει κατάλληλα (man-in-the-middle attack).


Επικεφαλίδα Ethernet
Destination address
Source address
Type
ARP Request ή ARP Reply
Padding
CRC
6
6
2
.....
.....
4
4 byte
Hardware type (2 bytes)
Protocol type (2 bytes)
Hardware size (1 byte)
Protocol size (1 byte)
Opcode (2 bytes)
Sender MAC address (first 4 bytes)
Sender MAC address (last 2 bytes)
Sender IP address (first 2 bytes)
Sender IP address (last 2 bytes)
Target MAC address (first 2 bytes)
Target MAC address (last 4 bytes)
Target IP address (4 bytes)
Padding
Padding
Padding
Padding
Padding