Ονοματεπώνυμο: Χρήστος Τσούφης		**Ομάδα:** 2
Όνομα PC/ΛΣ: DESKTOP-EUMLCMA/Windows 10		**Ημερομηνία:** 20/10/2020
Διεύθυνση IP: 192.168.1.3	**Διεύθυνση MAC:** 34-F6-4B-07-39-B5	

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

Άσκηση 1

1.1 Παρατήρηση περιεχομένων ARP: `arp -a` ή `arp -g`.

1.2 Διαγραφή περιεχομένων ARP: `arp -d`.

1.3 IPv4 Addresses of Default Gateway: 192.168.1.1 .

IPv4 Addresses of DNS Servers: 192.168.1.1 .

Command: `ipconfig /all`

1.4 Καταγραφή περιεχομένου ARP:

```
Interface: 192.168.56.1 --- 0x5
  Internet Address      Physical Address      Type
  192.168.56.255        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

Interface: 192.168.1.3 --- 0x12
  Internet Address      Physical Address      Type
  192.168.1.1           78-96-82-50-a1-2a     dynamic
  192.168.1.255         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 οι διευθύνσεις.

1.6 Αυτό που εμφανίζεται είναι το εξής:

```
Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

1.7 Τα περιεχόμενα του ARP θα είναι:

```
Interface: 192.168.56.1 --- 0x5
  Internet Address      Physical Address      Type
  192.168.56.255        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

Interface: 192.168.1.3 --- 0x12
  Internet Address      Physical Address      Type
  192.168.1.1           78-96-82-50-a1-2a     dynamic
  192.168.1.2           00-7c-2d-f3-eb-12     dynamic
  192.168.1.255         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
```

Με την χρήση της εντολής, έχει προστεθεί ένα επιπλέον πεδίο, το οποίο είχε χαθεί.

1.8 Η διεύθυνση που καταχωρήθηκε είναι η 192.168.1.1 . Αυτό αιτιολογείται από το γεγονός ότι ο DNS Server, ανακαλύπτει ποια IP address αντιστοιχεί στο URL της ιστοσελίδας.

1.9 Όχι, διότι βρίσκεται σε διαφορετικό υποδίκτυο.

Άσκηση 2

2.1 Η τιμή του πεδίου Type, του Ethernet για IPv4: 0x0800.

2.2 Η τιμή του πεδίου Type, για ARP: 0x0806.

2.3 Η τιμή του πεδίου Type, για IPv6: 0x86dd.

2.4 MAC Address (Source): 34:f6:4b:07:39:b5.

2.5 MAC Address (Destination): e0:19:54:25:47:58.

2.6 Όχι, δεν είναι.

2.7 Ανήκει στον δρομολογητή, αφού δεν υπάρχει απευθείας σύνδεση στο διαδίκτυο.

2.8 Η δεκαεξαδική τιμή του Type: 0x0800 και αφορά το IPv4 Protocol.

2.9 Μήκος Πλαισίων: 499 bytes.

2.10 Προηγούνται του χαρακτήρα ASCII “G”: 54 bytes.

2.11 MAC Address (Source): e0:19:54:25:47:58

2.12 Όχι.

2.13 Αυτή ανήκει στον δρομολογητή.

2.14 MAC Address (Destination): 34:f6:4b:07:39:b5.

2.15 Ανήκει στον τοπικό υπολογιστή.

2.16 Η δεκαεξαδική τιμή του Type: 0x0800.

2.17 Μήκος Πλαισίων: 468 bytes.

2.18 Προηγούνται του χαρακτήρα ASCII “G”: 67 bytes.

2.19 Το Wireshark καταγράφει τα πεδία: MAC Address (Destination), MAC Address (Source), Ether Type, Payload.

2.20 Με το CRC συμβαίνει το εξής: δεν καταγράφεται επειδή η σύλληψή του είναι έμμεση. Για να γίνει καταγραφή, θα πρέπει το πεδίο FCS να αποτελεί μέρος του πλαισίου.

Άσκηση 3

3.1 Η εφαρμογή αυτού του φίλτρου έχει ως αποτέλεσμα τα πακέτα να έχουν ως Source/Destination την MAC Address του υπολογιστή.

3.2 Η 2η εφαρμογή φίλτρου έχει ως αποτέλεσμα να εμφανίζονται μόνο τα πακέτα του προηγούμενου φίλτρου, τα οποία έχουν ARP Protocol.

3.3 Κατά την εκτέλεση της εντολής ping, ανταλλάχθηκε 1 ARP packet, όπως προκύπτει από το ζεύγος request/reply.

3.4 Η χρήση του "or" έχει ως αποτέλεσμα τα packets είτε με Source/Destination MAC Address του υπολογιστή είτε το ARP Protocol.

3.5 Φαίνεται παρακάτω στο σχήμα.

3.6 Hardware Type: Ethernet (1)

Protocol Type: IPv4 (0x0800)

3.7 Αυτό συμβαίνει διότι, ο τύπος του Protocol είναι IPv4, οπότε το μέγεθος της διεύθυνσης του Hardware είναι 4 bytes.

3.8 Αυτό συμβαίνει διότι, ο τύπος του Protocol είναι Ethernet, οπότε το μέγεθος της διεύθυνσης του Hardware είναι 6 bytes.

3.9 Η MAC Address του αποστολέα ανήκει στον τοπικό υπολογιστή, ενώ η MAC Address του παραλήπτη είναι η ff:ff:ff:ff:ff:ff, οπότε όλοι οι υπολογιστές που είναι συνδεδεμένοι στο τοπικό δίκτυο, το λαμβάνουν.

3.10 Η δεκαεξαδική τιμή του Type: 0x0806 και αφορά το ARP Protocol.

3.11 Παρακάτω φαίνονται οι διευθύνσεις και το είδος της καθεμίας.

Destination Address	Broadcast (ff:ff:ff:ff:ff:ff)
…. ..1. …. …. …. ….	LG bit: Locally administered address (not factory default)
…. …1 …. …. …. ….	IG bit: Group address (multicast/broadcast)
Source Address	34:f6:4b:07:39:b5
…. ..0. …. …. …. ….	LG bit: Locally administered address (factory default)
…. …0 …. …. …. ….	IG bit: Group address (unicast)

3.12 Εμφανίζονται στο 1ο & 2ο LS bit του MS byte.

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

3.14 Προηγούνται 20 bytes.

3.15 ARP opcode: 1 (request).

3.16 Μεταφέρεται στο MAC Address Sender.

3.17 Μεταφέρεται στο IP Address Sender.

3.18 Περιέχεται στο IP Address Target.

3.19 Υπάρχει και είναι το MAC Address Target 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 DNS Server που έγινε ping.

3.21 Η δεκαεξαδική τιμή του Type: 0x0806 και αφορά το ARP Protocol.

3.22 Προηγούνται 20 bytes.

3.23 ARP opcode: 2 (reply).

3.24 Μεταφέρεται στο IP Address Sender.

3.25 Μεταφέρεται στο MAC Address Sender.

3.26 Μεταφέρεται στο IP Address Target.

3.27 Περιέχεται στο MAC Address Sender.

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

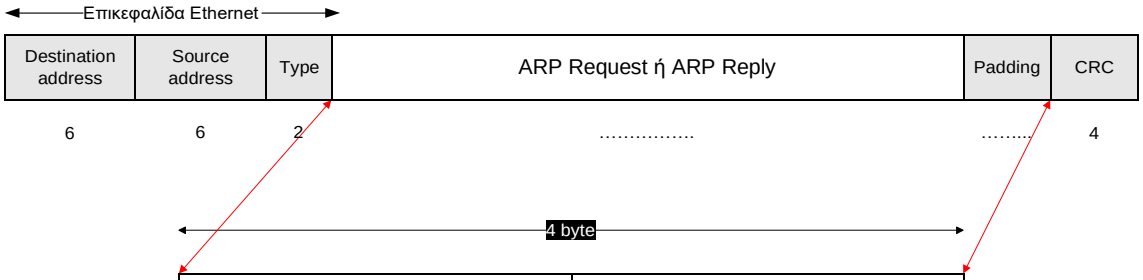
3.29 Όσον αφορά το ARP, είναι το ίδιο με το ερώτημα 3.13. Αντιθέτως, το πλαίσιο Ethernet που το μεταφέρει είναι 18 bytes μεγαλύτερο σε μέγεθος, λόγω του padding.

3.30 Δοθέντος ότι η δομή των πακέτων ARP request/reply είναι η ίδια, το διαφορετικό μήκος πλαισίων Ethernet για ARP (reply/request) packets εξηγείται ως εξής: Η βιβλιοθήκη npcap χρησιμοποιείται για την σύλληψη των απερχόμενων πακέτων πριν μεταδοθούν, οπότε στα ARP requests, δεν έχει προστεθεί ακόμα το padding για να διαμορφωθεί το πλαίσιο Ethernet, ενώ στα ARP replies, έχει προστεθεί, με την προϋπόθεση να έχουν μεταδοθεί.

3.31 Τα διαφοροποιεί το πεδίο Type.

3.32 Το πεδίο Opcode υποδεικνύει κατά πόσο για ARP (reply/request) packet.

3.33 Αυτό που θα συνέβαινε εάν ένας κακόβουλος υπολογιστής στο τοπικό δίκτυο απαντούσε σε όλα τα ARP request, δίνοντας τη δική του διεύθυνση MAC είναι το εξής: Ο υπολογιστής που θα έκανε το request, θα θεωρούσε ότι ο κακόβουλος υπολογιστής είναι ο παραλήπτης και επομένως, θα συνεχιζόταν η επικοινωνία μαζί του, δίνοντας έτσι την δυνατότητα να υποκλέψει μηνύματα (eavesdropping) ή να τα αλλοιώσει (man-in-the-middle attack).



Hardware type: 2 bytes	Protocol type: 2 bytes
Hardware size: 1 byte / Protocol size: 1 byte	Opcode: 2 bytes
MAC Address Sender: first 4 bytes	
MAC Address Sender: last 2 bytes	IP Address Sender: first 2 bytes
IP Address Sender: last 2 bytes	MAC Address Target: first 2 bytes
MAC Address Target: last 4 bytes	
IP Address Target: 4 bytes	
Padding	
Padding	
Padding	
Padding	
Padding	