



## ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

### ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

**ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΓΚΟΥΜΕ ΛΑΟΥΡΕΝΤΙΑΝ**

**ΑΜ: 031 18 014**

**ΕΞΑΜΗΝΟ: 7<sup>ο</sup>**

**ΟΜΑΔΑ: 4**

**MAC ADDRESS: B4-69-21-1B-6C-FF**

**IPv4: Άσκ.1 και Άσκ.4 : 10.3.20.12, Άσκ2 και Άσκ3 : 10.3.20.36**

**ΌΝΟΜΑ ΥΠΟΛΟΓΙΣΤΗ: LAPTOP-B2DVAJKK**

**ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ: WINDOWS 10**

### ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ



## ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 3: ΕΠΙΚΟΙΝΩΝΙΑ ΣΤΟ ΤΟΠΙΚΟ ΔΙΚΤΥΟ (ΠΛΑΙΣΙΟ ETHERNET ΚΑΙ ΠΡΩΤΟΚΟΛΛΟ ARP)

### Άσκηση 1: Ο πίνακας ARP

1.1) Πληκτρολογώντας “arp/?” στο terminal, βλέπουμε πως η εντολή για να δούμε τα περιεχόμενα του πίνακα ARP είναι η “arp -a”.

1.2) Με την εντολή “arp -d \*” καθαρίζουμε την ARP cache κάθε host του υπολογιστή μας.

1.3) Με την εντολή “ipconfig/all” βρίσκουμε “Default Gateway: 10.3.20.1” και για τους εξυπηρετητές DNS: “DNS Servers: 62.217.126.164 / 194.177.210.210 (primary και secondary)”.

1.4) Το περιεχόμενο του πίνακα ARP φαίνεται παρακάτω:

```
C:\WINDOWS\system32>arp -a

Interface: 10.3.20.12 --- 0x12
    Internet Address      Physical Address        Type
    10.3.20.1             04-d5-90-da-67-b0      dynamic
    10.3.21.255           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

Interface: 192.168.56.1 --- 0x14
    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
```

1.5) Παρατηρούμε πως εμφανίζεται η διεύθυνση της προκαθορισμένης πύλης (10.3.20.1) αλλά όχι των εξυπηρετητών DNS. Ωστόσο, παρατηρούμε τη διεύθυνση 192.168.56.1 η οποία είναι η IPv4 διεύθυνση του Ethernet adapter VirtualBox Host-Only Network.

1.6) Προκειμένου να διαγράψουμε την ARP cache απαιτούνται δικαιώματα διαχειριστή. Αφού τα αποκτήσουμε, εκτελούμε την εντολή διαγραφής “arp -d \*” και τα περιεχόμενα του πίνακα μετά από αυτήν είναι:

```
C:\WINDOWS\system32>arp -a

Interface: 10.3.20.12 --- 0x12
    Internet Address      Physical Address        Type
    10.3.20.1             04-d5-90-da-67-b0      dynamic
    224.0.0.22            01-00-5e-00-00-16      static

Interface: 192.168.56.1 --- 0x14
    Internet Address      Physical Address        Type
    224.0.0.22            01-00-5e-00-00-16      static
```

Δοκιμάζοντας όλες τις διευθύνσεις του πίνακα ARP (εκτός της προκαθορισμένης πύλης), **δε λαμβάνουμε απάντηση από πουθενά** (και αυτό διότι δεν υπάρχει επικοινωνία σε τοπικό δίκτυο), καθώς όλα τα αιτήματα κάνουν time out. Κατόπιν υποδείξεως του υπεύθυνου του εργαστηρίου, κάνουμε ping στη διεύθυνση του **default gateway**, όπου και παίρνουμε απάντηση.

**1.7)** Παρατηρούμε πως ο **πίνακας ARP έγινε ίδιος όπως πριν τη διαγραφή**.

**1.8)** Έχει καταχωρηθεί η διεύθυνση της **προκαθορισμένης πύλης** και αυτό, διότι ο σέρβερ της σελίδας του εργαστηρίου ανήκει σε διαφορετικό υποδίκτυο από το δικό μας, επομένως όταν συνδεόμαστε στη σελίδα του εργαστηρίου, στέλνουμε το μήνυμα πρώτα στον router μας (ο οποίος λειτουργεί ως default gateway), ο οποίος και αναλαμβάνει να κάνει τη δρομολόγηση στο υπόλοιπο δίκτυο.

**1.9)** **Όχι** δεν έχει καταχωρηθεί, καθώς επικοινωνούμε με τον δρομολογητή μας, αφού η σελίδα του εργαστηρίου είναι σε σέρβερ διαφορετικό του υποδικτύου μας.

## **Άσκηση 2: Το πλαίσιο Ethernet**

**2.1)** Το Wireshark καταγράφει τα πεδία **Destination MAC address, Source MAC address** και **Type**.

**2.2)** Το προοίμιο **δεν έχει καταγραφεί**, και αυτό διότι δε θεωρείται μέρος του frame.

**2.3)** Το CRC (Cyclic Redundancy Check) είναι ο αλγόριθμος που παράγει το FCS (Frame Check Sequence). Το Wireshark καταγράφει πακέτα τα οποία κάνει capture η packet capture library του λειτουργικού συστήματός μας (Npcap για τα Windows). Η βιβλιοθήκη αυτή καταγράφει πακέτα, τα οποία το raw packet capture mechanism του ΛΣ μας επιτρέπει. Δεδομένου ότι τα περισσότερα ΛΣ **δεν υποστηρίζουν καταγραφή του FCS ενός frame στο Ethernet**, δε βλέπουμε το πεδίο FCS. Η δυνατότητα αυτή μπορεί ενδεχομένως να επιτευχθεί κάνοντας ειδικά configurations στις βιβλιοθήκες.

**2.4)** Για πακέτα **IPv4**, το πεδίο **Type** έχει τιμή **0x0800**.

**2.5)** Για πακέτα **ARP**, το πεδίο **Type** έχει τιμή **0x0806**.

**2.6)** Για πακέτα **IPv6**, το πεδίο **Type** έχει τιμή **0x86dd**.

**2.7)** Η διεύθυνση MAC **πηγής** του πλαισίου είναι **b4:69:21:1b:6c:ff**.

**2.8)** Η διεύθυνση MAC **προορισμού** του πλαισίου είναι **04:d5:90:da:67:b0**.

**2.9)** Η διεύθυνση αυτή **δεν ανήκει** στο **edu-dy.cn.ntua.gr**.

2.10) Η διεύθυνση αυτή ανήκει στον **router** μας, ο οποίος λειτουργεί ως gateway και προωθεί το πλαίσιο σε επόμενα routers μέχρι να φτάσει στον τελικό του προορισμό.

2.11) Το πλαίσιο είναι συνολικά **503 bytes**.

2.12) Προηγούνται **54 bytes** (όσα είναι μπροστά από τα μπλε bytes στην παρακάτω εικόνα).

704	46.597...	10.3.20.36	147.102.40.15	HTTP	503 GET /lab3/ HTTP/1.1
705	46.608...	147.102.40.15	10.3.20.36	HTTP	537 HTTP/1.1 200 OK (text/html)
706	46.621...	2001:648:2d00:...	2001:648:2ffc:...	DNS	111 Standard query 0xff56 A webadvisorc.rest.gti.mca
707	46.621...	2001:648:2d00:...	2001:648:2ffc:...	DNS	111 Standard query 0x4a04 AAAA webadvisorc.rest.gti.
708	46.627...	2001:648:2ffc:...	2001:648:2d00:...	DNS	214 Standard query response 0x4a04 AAAA webadvisorc.
> Frame 704: 503 bytes on wire (4024 bits), 503 bytes captured (4024 bits) on interface \Device\NPF_{94774A...}					
> Ethernet II, Src: b4:69:21:1b:6c:ff, Dst: 04:d5:90:da:67:b0					
> Internet Protocol Version 4, Src: 10.3.20.36, Dst: 147.102.40.15					
> Transmission Control Protocol, Src Port: 59823, Dst Port: 80, Seq: 1, Ack: 1, Len: 449					
> Hypertext Transfer Protocol					
> TRANSMISSION RTE Data					
0000	04 d5 90 da 67 b0 b4 69	21 1b 6c ff 08 00 45 00	....g..i!.l...E.		
0010	01 e9 41 b0 40 00 80 06	dd c2 0a 03 14 24 93 66	..A.@... ..\$.f		
0020	28 0f e9 af 00 50 a8 24	8d ef c3 69 17 39 50 18	(....P.\$ ...i.9P.		
0030	02 00 75 82 00 00 47 45	54 20 2f 6c 61 62 33 2f	..u...GE T /lab3/		
0040	20 48 54 54 50 2f 31 2e	31 0d 0a 48 6f 73 74 3a	HTTP/1.1..Host:		
0050	20 65 64 75 2d 64 79 2e	63 6e 2e 6e 74 75 61 2e	edu-dy. cn.ntua.		
0060	67 72 0d 0a 43 6f 6e 6e	65 63 74 69 6f 6e 3a 20	gr..Conn ection:		
0070	6b 65 65 70 2d 61 6c 69	76 65 0d 0a 55 70 67 72	keep-ali ve..Upgr		
0080	61 64 65 2d 49 6e 73 65	63 75 72 65 2d 52 65 71	ade-Inse cure-Req		

2.13) Η διεύθυνση MAC του αποστολέα είναι **04:d5:90:da:67:b0**.

2.14) Η διεύθυνση αυτή **δεν ανήκει** στον ιστότοπο του εργαστηρίου.

2.15) Ανήκει στον **δρομολογητή** μας.

2.16) Η διεύθυνση MAC του παραλήπτη είναι **b4:69:21:1b:6c:ff**.

2.17) Αυτή, ανήκει στην **κάρτα δικτύου Wi-Fi του υπολογιστή** μας.

2.18) Το μήκος του πλαισίου είναι **537 bytes**.

2.19) Αντίστοιχα με το ερώτημα 2.12, βρίσκουμε, μετρώντας τα bytes πριν από το κόκκινο κουτάκι (χαρακτήρας 'O') **67 bytes**.

704	46.597...	10.3.20.36	147.102.40.15	HTTP	503 GET /lab3/ HTTP/1.1
705	46.608...	147.102.40.15	10.3.20.36	HTTP	537 HTTP/1.1 200 OK (text/html)
706	46.621...	2001:648:2d00::...	2001:648:2ffc::...	DNS	111 Standard query 0xff56 A webadvisorc.
707	46.621...	2001:648:2d00::...	2001:648:2ffc::...	DNS	111 Standard query 0x4a04 AAAA webadviso
708	46.627...	2001:648:2ffc::...	2001:648:2d00::...	DNS	214 Standard query response 0x4a04 AAAA
709	46.627...	2001:648:2ffc::...	2001:648:2d00::...	DNS	215 Standard query response 0xff56 A web.

  

> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]	
Response Version:	HTTP/1.1
Status Code:	200
[Status Code Description: OK]	
Response Phrase:	OK
Date:	Fri, 22 Oct 2021 19:10:29 GMT\r\n

  

0000	b4 69 21 1b 6c ff 04 d5	90 da 67 b0 08 00 45 00	il·1... ·g...E·
0010	02 0b 0e fb 40 00 3d 06	53 56 93 66 28 0f 0a 03	...@...= SV·f(...
0020	14 24 00 50 e9 af c3 69	17 39 a8 24 8f b0 50 18	·\$·P...i ·9·\$·P·
0030	04 06 f9 4e 00 00 48 54	54 50 2f 31 2e 31 20 32	...N·HT TP/1.1 2
0040	30 30 20 4f 4b 0d 0a 44	61 74 65 3a 20 46 72 69	00 OK·D ate: Fri
0050	2c 20 32 32 20 4f 63 74	20 32 30 32 31 20 31 39	, 22 Oct 2021 19
0060	3a 31 30 3a 32 39 20 47	4d 54 0d 0a 53 65 72 76	:10:29 G MT·Serv
0070	65 72 3a 20 41 70 61 63	68 65 2f 32 2e 32 2e 32	er: Apac he/2.2.2
0080	32 20 28 46 72 65 65 42	53 44 29 20 6d 6f 64 5f	2 (FreeB SD) mod_
0090	73 73 6c 2f 32 2e 32 2e	32 32 20 4f 70 65 6e 53	ssl/2.2. 22 OpenS

### Άσκηση 3: Περισσότερα για τα πλαίσια Ethernet

**3.1)** Η μόνη διεύθυνση MAC πηγής πλαισίων είναι η δική μας (b4:69:21:1b:6c:ff), επομένως, αρκεί να εξετάσουμε το byte 0, το οποίο σε δυαδική μορφή είναι:  $b4_{16} = 1011\ 0100_2$ . Εφόσον το **LSB** του byte 0 είναι 0, πρόκειται για **ατομική διεύθυνση**, ενώ το **δεύτερο LSB** είναι επίσης 0, που σημαίνει πως έχουμε **παγκόσμια διεύθυνση**.

**3.2)** Ως MAC διευθύνσεις προορισμού, καταγράφονται οι εξής:

- 01:00:5e:7f:ff:fa → Εξετάζουμε τα 2 bits μικρότερης αξίας του πρώτου byte ( $01_{16} = 0000\ 0001_2$ ), επομένως πρόκειται για **ομαδική, παγκόσμια διεύθυνση**.
- 01:00:5e:00:00:fb → **Ομαδική, παγκόσμια διεύθυνση**.
- 33:33:00:00:00:fb →  $0011\ 0011$  → **Ομαδική, τοπική διεύθυνση**.

**3.3)** Γνωρίζουμε ότι η μετάδοση των byte, για όλα τα πεδία ενός πλαισίου, γίνεται από αριστερά προς τα δεξιά και για κάθε byte πρώτα μεταδίδεται το λιγότερο σημαντικό bit (LSB) και τελευταίο το MSB. Επομένως, στο πρώτο byte μιας διεύθυνσης MAC, το πρώτο bit εμφανίζεται **τέρμα δεξιά, ενώ το επόμενο αμέσως αριστερά του**. Αν για παράδειγμα πρώτο byte →  $35_{16} = 0011\ 0101_2$ , τότε πρώτο bit το 1 και δεύτερο το 0 από τα υπογραμμισμένα.

**3.4)** Η διεύθυνση MAC για τα πλαίσια εκπομπής (**broadcast**) είναι **ff:ff:ff:ff:ff:ff**.

**3.5) Κανένα πλαίσιο.** (Παρατήρηση, για να δούμε τι κάνει, δοκιμάζουμε να το εφαρμόσουμε στο αρχείο καταγραφής που κατεβάσαμε. Εκεί παρατηρούμε πως εμφανίζει πακέτα πρωτοκόλλου **IEEE 802.3 Ethernet** αντί για **Ethernet II**).

**3.6)** Χρησιμοποιώντας το αρχείο που κατεβάσαμε, καθώς στη δική μας καταγραφή δεν εμφανίζονται πακέτα με το φίλτρο IIc, παρατηρούμε πως το πεδίο μετά τις MAC

διευθύνσεις είναι το **Length**, το οποίο και δηλώνει το **πλήθος των δεδομένων του πλαισίου** σε bytes.

**3.7)** Μια διαφορά των πλαισίων IEEE 802.3 σε σχέση με αυτά του Ethernet II, είναι πως **αντί για το πεδίο Type υπάρχει το πεδίο Length**. Μια επιπρόσθετη διαφορά, είναι πως τα πλαίσια IEEE 802.3 περιέχουν μια **επικεφαλίδα Logical Link Control (LLC)**, καθοριζόμενη από το πρότυπο IEEE 802.3, η οποία και προσδιορίζει το πρωτόκολλο ανωτέρου στρώματος που ενθυλακώνεται.

**3.8)** Η επικεφαλίδα LLC, **μήκους 3 bytes**, περιλαμβάνει τα πεδία **DSAP** (Destination Service Access Point, ένα πεδίο 1 byte, το οποίο δρα ως δείκτης σε ένα memory buffer στον αποδέκτη και λέει στο NIC του δέκτη σε ποιον buffer να βάλει την πληροφορία που δέχεται), **SSAP** (Source Service Access Point, αντίστοιχο με DSAP για τον αποστολέα) και **Control Field**.

**3.9)** Τα πλαίσια IEEE 802.3 μεταφέρουν δεδομένα του πρωτοκόλλου **Spanning Tree Protocol**, μεγέθους (Length) **39 bytes**.

**3.10)** Το παραγέμισμα (padding) προστίθεται προκειμένου τα πλαίσια να φτάσουν το ελάχιστο μήκος που πρέπει να έχουν (64 bytes). Στη συγκεκριμένη περίπτωση, το padding ανέρχεται σε **7 bytes**, αναμενόμενο, καθώς όπως είδαμε έχουμε 39 bytes δεδομένων, ενώ το ελάχιστο μήκος δεδομένων είναι 46 bytes. (Συνολικά: (6+6) bytes για MAC addresses, 2bytes για το Length, 39 bytes payload, 7 bytes padding = 60bytes, και προσθέτοντας τα 4 bytes FCS, τα οποία δεν εμφανίζονται, έχουμε αθροιστικά 64 bytes).

## **Άσκηση 4: Περισσότερα για τα πακέτα ARP**

**4.1)** Εμφανίζει όλα τα πακέτα εκείνα, **στα οποία εμπλέκεται η MAC διεύθυνση της κάρτας δικτύου του υπολογιστή μας**, επομένως πρακτικά είναι σα να μην υπάρχει το φίλτρο. Ενδεικτικά, αν βάλουμε το φίλτρο αυτό με ένα not από μπροστά, ο πίνακας είναι άδειος.

**4.2)** Εμφανίζονται πλέον όσα πακέτα από τη συνολική κίνηση, **ενθυλακώνουν το πρωτόκολλο ARP**.

**4.3)** Καταγράφηκε ανταλλαγή **6 πακέτων**.

**4.4)** Τα πακέτα ARP διαφέρουν από τα IPv4 στο πεδίο **Type** του πλαισίου Ethernet (0x0806 για ARP, ενώ 0x0800 για IPv4).

**4.5)** Έχουμε τα παρακάτω πεδία:



- **Destination (MAC Address): 6 bytes**
- **Source (MAC Address): 6 bytes**
- **Type: 4 bytes**
- **Trailer (Padding): 14 bytes**
- **Hardware Type: 1 bytes**
- **Protocol Type: 1 bytes**
- **Hardware Size: 1 byte**
- **Protocol Size : 1 byte**
- **Opcode: 2 byte**
- **Sender MAC Address: 6 bytes**
- **Sender IP Address: 4 bytes**
- **Target MAC Address: 6 bytes**
- **Target IP Address: 4 bytes**

**4.6)** Η τιμή του πεδίου **Hardware Type** είναι **0x0001** και υποδεικνύει κάρτα δικτύου τύπου **Ethernet**.

**4.7)** Η τιμή του πεδίου **Protocol Type** είναι **0x0800** και αναφέρεται στο πρωτόκολλο **IPv4**.

**4.8)** Το πεδίο **Protocol Type** αναφέρεται στο πρωτόκολλο του **Network Layer** (π.χ. **IPv4**), ενώ το **EtherType** αναφέρεται στο πρωτόκολλο που είναι ενθυλακωμένο στο **payload** του πλαισίου και χρησιμοποιείται στο άκρο λήψης από το **Data Link Layer** για να προσδιορίσει τον τρόπο επεξεργασίας του **payload** αυτού (π.χ. **ARP**).

**4.9)** Διαβάζουμε, στο σχετικό site το εξής:

**Protocol address length. 8 bits.**  
Length of the protocol address in bytes.

Επομένως, εφόσον έχουμε **IPv4** πρωτόκολλο και οι διευθύνσεις του πρωτοκόλλου αυτού αποτελούνται από **4 bytes** προκύπτει το **4**.

**4.10)** Αντίστοιχα για το **Hardware Size** διαβάζουμε πως πρόκειται για το μήκος των διευθύνσεων **Hardware** σε bytes. Επομένως, πρόκειται για **διευθύνσεις MAC**, οι οποίες όπως γνωρίζουμε αποτελούνται από **6 bytes**.

**4.11)** Η διεύθυνση **MAC** αποστολέα του πλαισίου **Ethernet** που μεταφέρει το εν λόγω **ARP Request** ανήκει στον υπολογιστή μας.

**4.12)** Η διεύθυνση MAC του παραλήπτη του πλαισίου αυτού είναι: **ff:ff:ff:ff:ff:ff**. (broadcast). Την τιμή αυτή διαβάζουμε στο Ethernet Header, ενώ από τα πεδία του ARP βλέπουμε ως Target MAC address το 00:00:00:00:00:00, το οποίο υποδηλώνει πως δε γνωρίζουμε τη MAC του παραλήπτη, του οποίου ωστόσο γνωρίζουμε την IP. Επομένως, ο υπολογιστής μας κάνει broadcast το request προκειμένου να λάβει ως απάντηση τη MAC διεύθυνση του Gateway gate (router).

**4.13)** Το **πλαίσιο Ethernet** (συνολικό μήκος) είναι **42 bytes**, ενώ το πακέτο **ARP** είναι τα **28** εξ αυτών.

**4.14)** Του πεδίου Opcode **προηγούνται 20 bytes**.

**4.15)** Το Opcode έχει τιμή: **request (1 → 0x0001)**.

**4.16)** Η διεύθυνση MAC του αποστολέα είναι στο πεδίο **Sender MAC address** εντός του πακέτου ARP request.

**4.17)** Αντίστοιχα, η διεύθυνση IP του αποστολέα, είναι στο **Sender IP address**.

**4.18)** Η διεύθυνση IPv4 του υπολογιστή, του οποίου αναζητείται η MAC είναι στο πεδίο **Target IP address**.

**4.19)** Το πεδίο **Target MAC address** αναφέρεται στη ζητούμενη διεύθυνση MAC, αλλά στο προκειμένω πακέτο έχει τιμή 00:00:00:00:00:00. Η διεύθυνση αυτή υποδηλώνει άγνωστη διεύθυνση, πράγμα αναμενόμενο, καθώς το ARP request στέλνεται προκειμένου να ληφθεί ως απάντηση η MAC της συσκευής της οποία γνωρίζουμε την IP.

**4.20)** Η διεύθυνση MAC του **αποστολέα** ανήκει στο **router** μας, ενώ του **παραλήπτη** στον υπολογιστή μας.

**4.21)** Opcode: **reply (2) → 0x0002**.

**4.22)** Η διεύθυνση IPv4 του αποστολέα είναι στο πεδίο **Sender IP address** του πακέτου ARP reply.

**4.23)** Αντίστοιχα, η διεύθυνση MAC του αποστολέα στο πεδίο **Sender MAC address**.

**4.24)** Ενώ η διεύθυνση IPv4 του παραλήπτη στο πεδίο **Target IP address**.

**4.25)** Ξανά, η διεύθυνση MAC του υπολογιστή που έχει τη διεύθυνση IPv4 για την οποία έγινε η ερώτηση βρίσκεται στο πεδίο **Sender MAC address**, αφού ο αρχικά ερωτηθείς είναι πλέον αποστολέας του ARP reply.



**4.26)** Το πακέτο **ARP reply** είναι **28 bytes**, ενώ το πλαίσιο **Ethernet 56 bytes**. (Σημείωση: Μας εμφανίζονται 14 bytes padding, επομένως, αθροιστικά, έχουμε:  $(6+6)$ bytes για τις MAC διευθύνσεις, 2byte για το Type, 28bytes για το ARP πακέτο και 14 bytes Padding, το οποίο μας δίνει αθροιστικά 56bytes. Θέλουμε, ωστόσο 60 bytes, ώστε μαζί με το crc να φτάσουμε το ελάχιστο μέγεθος των 56, άρα θα έπρεπε το Padding να είναι 18 bytes. Σύμφωνα με τον υπεύθυνο του εργαστηρίου, πιθανόν είναι σφάλμα του δρομολογητή).

**4.27)** Τα συνολικά μεγέθη αιτήματος-απάντησης **διαφέρουν**, ενώ το μέγεθος του πακέτου ARP είναι ίδιο.

**4.28)** Η διαφορά αυτή έγκειται στο γεγονός ότι τα προς αποστολή πλαίσια συλλαμβάνονται προτού μεταδοθούν, επομένως **δεν έχει προστεθεί το Padding σε αυτά**, σε αντίθεση με τα πακέτα που λαμβάνουμε.

**4.29)** Το πεδίο **Opcode** προσδιορίζει εάν πρόκειται για request( $1_{10}$ ) ή reply( $2_{10}$ )

**4.30)** Πέραν της διαφοράς με το Padding, η άλλη διαφορά μεταξύ αιτήματος και απάντησης ARP είναι πως **η ερώτηση γίνεται προκειμένου να μάθουμε τη MAC address μιας γνωστής IP**, επομένως το **Target MAC address είναι το 00:00:00:00:00:00 (άγνωστο)**, ενώ στην απάντηση, είναι πλέον γνωστή η **διεύθυνση αυτή και έχει τον ρόλο του Sender MAC address**. Επιπλέον, επειδή ακριβώς δε γνωρίζουμε ποια συσκευή έχει τη δεδομένη IP, το request γίνεται broadcast (ff:ff:ff:ff:ff:ff) προκειμένου να το λάβουν όλες οι συσκευές και να απαντήσει εκείνη της οποίας το IP address ταυτίζεται με το **Sender IP address** του αιτήματος. Αντιθέτως, στην **απάντηση είναι γνωστές οι διευθύνσεις MAC αποστολέα και παραλήπτη**, επομένως έχουμε unicast μεταξύ αυτών.

**4.31)** Εφόσον ο κακόβουλος χρήστης απαντούσε τα αιτήματα ARP με τη δική του MAC, τότε όλοι οι **Hosts του τοπικού δικτύου θα ανακατεύθυναν τα πακέτα τους προς αυτόν**, με αποτέλεσμα να αποκτήσει πρόσβαση σε όσα δεδομένα εκείνοι στέλνουν.