



---

# ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

---

ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 3:ΕΠΙΚΟΙΝΩΝΙΑ ΣΤΟ ΤΟΠΙΚΟ ΔΙΚΤΥΟ

(ΠΛΑΙΣΙΟ ETHERNET ΚΑΙ ΠΡΩΤΟΚΟΛΛΟ ARP)



25 ΟΚΤΩΒΡΙΟΥ, 2022

ΘΟΔΩΡΗΣ ΑΡΑΠΗΣ – EL18028

<b>Όνοματεπώνυμο:</b> Θεodorής Αράπης		<b>Ομάδα:</b> 2
<b>Όνομα PC/ΛΣ:</b> DESKTOP-JGHL94V/ WINDOWS 10		<b>Ημερομηνία:</b> 25/10/2022
<b>Διεύθυνση IP:</b> 192.168.1.5		<b>Διεύθυνση MAC:</b> 70-85-C2-88-FD-B1

## Άσκηση 1: Ο Πίνακας ARP

### 1.1

Οι εντολές «arp -a» και «arp -g» κάνουν ακριβώς την ίδια δουλειά και μας εμφανίζουν τα περιεχόμενα του πίνακα arp.

### 1.2

Με την εντολή «arp -d \*» μπορούμε να διαγράψουμε όλους τους host που είναι αποθηκευμένοι στον πίνακα ARP.

### 1.3

Με την εντολή «ipconfig /all» βρίσκουμε της πληροφορίες που χρειαζόμαστε.

Οι ζητούμενες IP διευθύνσεις είναι οι ακόλουθες:

**Default Gateway:** 192.168.1.1

**DNS Servers:** 192.168.1.1 (Η ίδια συσκευή εκτελεί και τους δύο ρόλους)

### 1.4

Ο πίνακας περιεχομένων ARP είναι ο ακόλουθος.

```
C:\Users\Theodore>arp -a

Interface: 192.168.56.1 --- 0xc
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: 192.168.1.5 --- 0x11
Internet Address      Physical Address      Type
192.168.1.1           3c-98-72-5f-ea-a0    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

Interface: 172.21.80.1 --- 0x2a
Internet Address      Physical Address      Type
172.21.95.255         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
239.255.255.250       01-00-5e-7f-ff-fa    static
255.255.255.255       ff-ff-ff-ff-ff-ff    static
```

### 1.5

Οι διευθύνσεις IP του DNS server με το Default Gateway είναι ίδιες και παρατηρούμε ότι η IP αυτή εμφανίζεται στον πίνακα ARP με τους Host που έχει επικοινωνήσει πρόσφατα ο υπολογιστής μας.

### 1.6

Ανοίγουμε ένα command prompt των windows ως administrators και τρέχουμε την εντολή «arp -d \*».

```
C:\WINDOWS\system32>arp -d *  
C:\WINDOWS\system32>arp -a  
  
Interface: 192.168.56.1 --- 0xc  
Internet Address      Physical Address      Type  
224.0.0.22            01-00-5e-00-00-16    static  
  
Interface: 192.168.1.5 --- 0x11  
Internet Address      Physical Address      Type  
224.0.0.22            01-00-5e-00-00-16    static  
  
Interface: 172.21.80.1 --- 0x2a  
Internet Address      Physical Address      Type  
224.0.0.22            01-00-5e-00-00-16    static  
C:\WINDOWS\system32>
```

Κάνουμε ping προς όλες τις διευθύνσεις αλλά καμία δεν ανταποκρίνεται, καθώς δεν υπάρχει επικοινωνία σε τοπικό δίκτυο. Μόνο η διεύθυνση της συσκευής που εξυπηρετεί ως DNS και default Gateway ανταποκρίνεται.

### 1.7

Παρατηρούμε ότι ο πίνακας arp είναι ίδιος με πριν την διαγραφή των περιεχομένων του.

### 1.8

```
C:\WINDOWS\system32>arp -a  
  
Interface: 192.168.56.1 --- 0xc  
Internet Address      Physical Address      Type  
192.168.56.255        ff-ff-ff-ff-ff-ff    static  
  
Interface: 192.168.1.5 --- 0x11  
Internet Address      Physical Address      Type  
192.168.1.1           3c-98-72-5f-ea-a0    dynamic  
192.168.1.255         ff-ff-ff-ff-ff-ff    static  
  
Interface: 172.21.80.1 --- 0x2a  
Internet Address      Physical Address      Type  
172.21.95.255         ff-ff-ff-ff-ff-ff    static
```

Έχει καταχωρηθεί η διεύθυνση του Default Gateway. Αυτό συμβαίνει διότι ο server της σχολής που είναι υπεύθυνος να μας απαντήσει με τα δεδομένα της σελίδας βρίσκεται

σε διαφορετικό υποδίκτυο από το δικό μας. Συνεπώς, με την σύνδεσή μας στην σελίδα, στέλνουμε μήνυμα πρώτα στον router μας (default gateway) και αυτός με την σειρά του δρομολογεί το αίτημά μας στο υπόλοιπο δίκτυο.

### **1.9**

Όχι, δεν υπάρχει καταχώρηση της διεύθυνσης IPv4 της σελίδας της σχολής, καθώς ο server βρίσκεται σε διαφορετικό υποδίκτυο. Επομένως εμείς απλά επικοινωνούμε με τον router μας (default gateway) όποτε γνωρίζουμε μόνο την δική του IP διεύθυνση.

## **Άσκηση 2: Το πλαίσιο Ethernet**

### **2.1**

Το Wireshark καταγράφει τα πεδία Source MAC address, Destination MAC address και Type του πλαισίου Ethernet.

### **2.2**

Όχι, δεν καταγράφεται το προοίμιο γιατί δεν θεωρείται μέρος του frame.

### **2.3**

Το Wireshark κάνει capture πακέτα που πιάνει η packet capture library του λειτουργικού μας συστήματος, συγκεκριμένα η Npcap για Windows. Η βιβλιοθήκη αυτή καταγράφει πακέτα τα οποία το raw packet capture mechanism του λειτουργικού συστήματος μας επιτρέπει. Συνεπώς, δεν βλέπουμε το πεδίο CRC (Cyclic Redundancy Check), τον αλγόριθμο που παράγεται από το FCS (Frame Check Sequence) αφού πολλά λειτουργικά συστήματα δεν υποστηρίζουν την καταγραφή ενός frame στο Ethernet. Με ειδικά configurations στις βιβλιοθήκες ίσως είναι δυνατή η επίτευξη της καταγραφής αυτής.

### **2.4**

Για πακέτα IPv4 η τιμή του πεδίου Type στην επικεφαλίδα Ethernet είναι: 0x0800

### **2.5**

Για πακέτα IPv4 η τιμή του πεδίου Type στην επικεφαλίδα Ethernet είναι: 0x0806

### **2.6**

Για πακέτα IPv4 η τιμή του πεδίου Type στην επικεφαλίδα Ethernet είναι: 0x86dd

### **2.7**

Η διεύθυνση MAC πηγής του πλαισίου είναι: 70:85:c2:88:fd:b1

## 2.8

Η διεύθυνση MAC προορισμού του πλαισίου είναι: 3c:98:72:5f:ea:a0

## 2.9

Όχι, δεν ανήκει στο edu-dy.cn.ntua.gr.

## 2.10

Ανήκει στην συσκευή που δρα ως Default Gateway, δηλαδή τον router μας, αφού ο υπολογιστής μας χρειάζεται να επικοινωνήσει μόνο με αυτόν και ύστερα αυτός είναι υπεύθυνος να μεταδώσει την πληροφορία στο υπόλοιπο δίκτυο μέχρι τον επιθυμητό προορισμό.

ARP entry:

```
Interface: 192.168.1.5 --- 0x12
Internet Address      Physical Address      Type
192.168.1.1           3c-98-72-5f-ea-a0    dynamic
```

## 2.11

Το πλαίσιο έχει σύνολο 543 bytes.

Frame 171: 543 bytes on wire

## 2.12

Παρατηρούμε ότι προηγούνται 54 byte (η λέξη GET είναι οι δεκαεξαδικοί 47 45 54).

[Next Sequence Number: 490 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 2802916658  
0101 ... = Header Length: 20 bytes (5)  
> Flags: 0x018 (PSH, ACK)  
Window: 1025  
[Calculated window size: 262400]  
[Window size scaling factor: 256]  
Checksum: 0x8d19 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
> [Timestamps]  
> [SEQ/ACK analysis]  
TCP payload (489 bytes)  
▼ Hypertext Transfer Protocol  
▼ GET /lab3/ HTTP/1.1\r\n  
> [Expert Info (Chat/Sequence): GET /lab3/ HTTP/1.1\r\n  
Request Method: GET

0000 3c 98 72 5f ea a0 70 85 c2 88 fd b1 08 00 45 00  
0010 02 11 4a d2 40 00 40 06 70 f2 c0 a8 01 05 93 66  
0020 28 0f f4 69 00 50 fd 53 03 fa a7 11 1d 32 50 18  
0030 04 01 8d 19 00 00 47 45 54 20 2f 6c 61 62 33 2f  
0040 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a  
0050 20 65 64 75 2d 64 79 2e 63 6e 2e 6e 74 75 61 2e  
0060 67 72 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20  
0070 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72  
0080 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71  
0090 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41  
00a0 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e  
00b0 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30  
00c0 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 20  
00d0 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e  
00e0 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20  
00f0 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 30  
0100 36 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 2f 35  
0110 33 37 3e 33 36 0d 0e 41 63 63 65 70 74 3e 30 74

## 2.13

Η διεύθυνση MAC του αποστολέα είναι: 3c:98:72:5f:ea:a0

### 2.14

Όχι, δεν ανήκει στο edu-dy.cn.ntua.gr.

### 2.15

Η διεύθυνση αυτή, όπως αναφέραμε και σε προηγούμενα ερωτήματα, ανήκει στον router μας.

### 2.16

Η διεύθυνση MAC του παραλήπτη είναι: 70:85:c2:88:fd:b1

### 2.17

Η διεύθυνση αυτή ανήκει στην κάρτα δικτύου του υπολογιστή μας.

### 2.18

Το πλαίσιο έχει μήκος 584 bytes.

Frame 172: 584 bytes on wire

### 2.19

Προηγούνται 67 bytes (Η λέξη OK είναι η οι δεκαεξαδικοί 4f 4b).

> Frame 172: 584 bytes on wire (4672 bits), 584 bytes captured (4672 bits) on interface	0000	70 85 c2 88 fd b1 3c 98	72 5f ea a0 08 00 45 00
> Ethernet II, Src: 3c:98:72:5f:ea:a0, Dst: 70:85:c2:88:fd:b1	0010	02 3a 55 9c 40 00 3a 06	6b ff 93 66 28 0f c0 a8
> Internet Protocol Version 4, Src: 147.102.40.15, Dst: 192.168.1.5	0020	01 05 00 50 f4 69 a7 11	1d 32 fd 53 05 e3 50 18
> Transmission Control Protocol, Src Port: 80, Dst Port: 62569, Seq: 1, Ack: 490, Len	0030	04 06 3c cb 00 00 48 54	54 50 2f 31 2e 31 20 32
▼ Hypertext Transfer Protocol	0040	30 30 20 4f 4b 0d 0a 44	61 74 65 3a 20 54 75 65
▼ HTTP/1.1 200 OK\r\n	0050	2c 20 31 38 20 4f 63 74	20 32 30 32 32 20 31 36
> [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]	0060	3a 34 38 3a 31 38 20 47	4d 54 0d 0a 53 65 72 76
Response Version: HTTP/1.1	0070	65 72 3a 20 41 70 61 63	68 65 2f 32 2e 32 2e 32
Status Code: 200	0080	32 20 28 46 72 65 65 42	53 44 29 20 6d 6f 64 5f
[Status Code Description: OK]	0090	73 73 6c 2f 32 2e 32 2e	32 32 20 4f 70 65 6e 53
Response Phrase: OK	00a0	53 4c 2f 30 2e 39 2e 38	7a 68 2d 66 72 65 65 62

### **Άσκηση 3: Περισσότερα για τα πλαίσια Ethernet**

#### **3.1**

Οι διευθύνσεις MAC πηγής που καταγράφουμε είναι οι ακόλουθες:

- A)** 3c:98:72:5f:ea:a0 (router)
- B)** 70:85:c2:88:fd:b1 (υπολογιστής μας)
- Γ)** 70:5f:a3:b1:cf:56 (κινητή συσκευή)

Εξετάζουμε το byte 0 σε κάθε MAC διεύθυνση. Σε δυαδική μορφή έχουμε για κάθε περίπτωση:

- A)** 00111100
- B)** 01110000
- Γ)** 01110000

Σε όλες τις περιπτώσεις το LSB του byte 0 είναι 0, άρα έχουμε ατομικές διευθύνσεις.

Σε όλες τις περιπτώσεις το δεύτερο LSB του byte 0 είναι 0, άρα έχουμε παγκόσμιες διευθύνσεις.

#### **3.2**

Οι διευθύνσεις MAC προορισμού που καταγράφουμε είναι οι ακόλουθες:

- A)** 01:80:c2:00:00:00
- B)** 01:00:5e:40:98:8f
- Γ)** 33:33:ef:c0:98:8f
- Δ)** 33:33:00:00:00:01
- Ε)** 01:00:5e:00:00:fb

Εξετάζουμε το byte 0 σε κάθε MAC διεύθυνση. Σε δυαδική μορφή έχουμε για κάθε περίπτωση:

- A)** 00000001
- B)** 00000001
- Γ)** 00110011
- Δ)** 00110011
- Ε)** 00000001

Σε όλες τις περιπτώσεις το LSB του byte 0 είναι 1, άρα έχουμε ομαδικές διευθύνσεις (multicast).

Οι διευθύνσεις A, B, E έχουν στο δεύτερο LSB του byte 0 την τιμή 0, άρα έχουμε παγκόσμιες διευθύνσεις, ενώ οι υπόλοιπες έχουν τιμή 1, άρα τοπικές διευθύνσεις.

### 3.3

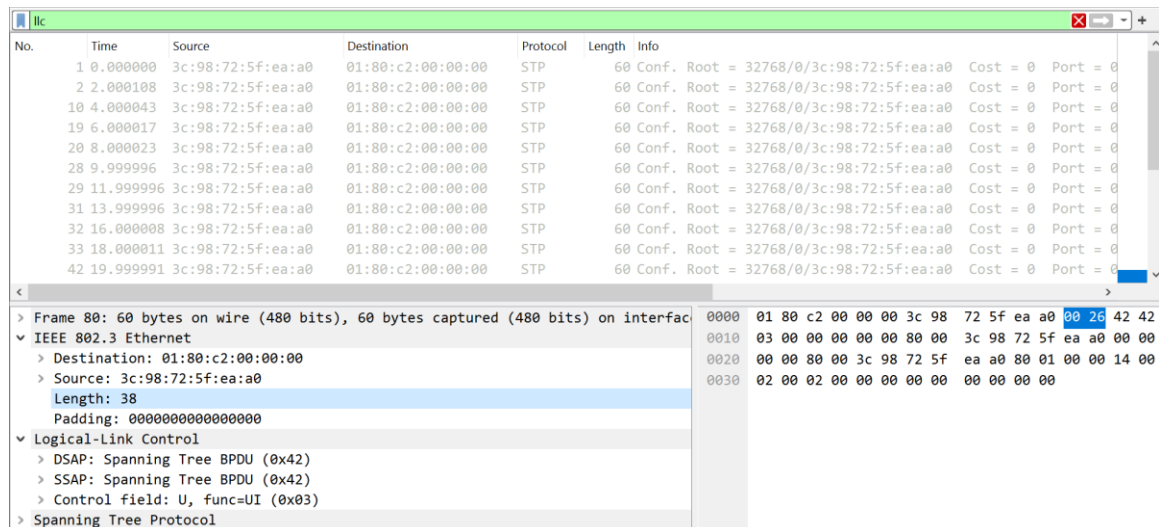
Γνωρίζουμε ότι η διεύθυνση MAC μεταδίδεται κατά byte από αριστερά προς τα δεξιά, ενώ κάθε byte μεταδίδεται από αριστερά προς τα δεξιά. Επομένως πρώτα εμφανίζεται το LSB του πρώτου byte (8ο bit του byte 0) της MAC διεύθυνσης και ύστερα το δεύτερο (7ο bit του byte 0) (δηλαδή τα δύο bytes που εξετάσαμε στα προηγούμενα ερωτήματα.)

### 3.4

Η διεύθυνση MAC για τα broadcast πλαίσια περιέχει μόνο άσσους (δηλαδή «ff:ff:ff:ff:ff:ff»).

### 3.5

Εμφανίζει μόνο τα πακέτα που διέπονται από το πρωτόκολλο IEEE 802.3 Ethernet.



The image shows a Wireshark packet capture window. The top pane displays a list of captured packets, all of which are STP (Spanning Tree Protocol) frames. The bottom pane shows a detailed view of the selected packet (No. 42), which is an IEEE 802.3 Ethernet frame. The frame details are as follows:

- Frame 80: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
- IEEE 802.3 Ethernet
  - Destination: 01:80:c2:00:00:00
  - Source: 3c:98:72:5f:ea:a0
  - Length: 38
  - Padding: 0000000000000000
- Logical-Link Control
  - DSAP: Spanning Tree BPDU (0x42)
  - SSAP: Spanning Tree BPDU (0x42)
  - Control field: U, func=UI (0x03)
- Spanning Tree Protocol

The packet bytes pane shows the raw data of the frame, with the first few bytes highlighted in blue: 0000 01 80 c2 00 00 00 3c 98 72 5f ea a0 00 26 42 42.

### 3.6

Στα πλαίσια IEEE 802.3, μετά τις διευθύνσεις MAC υπάρχει το πεδίο length που δηλώνει το μήκος σε byte των δεδομένων που περιέχονται στο πεδίο δεδομένων.

### 3.7

Αρχικά, τα πλαίσια IEEE 802.3 περιέχουν το πεδίο Length αντί για το type που περιέχουν τα πλαίσια Ethernet II. Ακόμη, τα πλαίσια IEEE 802.3 περιέχουν τη επικεφαλίδα Logical



Link Control (LLC) η οποία προσδιορίζει το πρωτόκολλο ανωτέρου στρώματος, ενώ τα πλαίσια Ethernet II όχι.

### **3.8**

Η επικεφαλίδα Logical Link Control (LLC) έχει μέγεθος 3 byte και περιλαμβάνει τα πεδία:

**DSAP:** Destination Service Access Point, δρα ως δείκτης σε ένα memory buffer στον αποδέκτη και λέει στον NIC του δέκτη σε ποιο buffer να αποθηκεύσει την πληροφορία που δέχεται

**SSAP:** Source Service Access Point, παρόμοια λειτουργία με το DSAP αλλά για τον αποστολέα

### **Control field**

### **3.9**

Μεταφέρουν δεδομένα του πρωτοκόλλου STP (Spanning Tree Protocol) και έχουν μέγεθος 38 bytes.

### **3.10**

Το padding έχει μέγεθος 8 byte στην περίπτωση μας και χρησιμεύει ώστε τα πλαίσια να φτάσουν το ελάχιστον μήκος που απαιτείται να έχουν (64 bytes). Οπότε έχουμε αναλυτικά:

6 bytes διεύθυνση προορισμού, 6 bytes διεύθυνση πηγής, 2 bytes Length, 38 bytes payload (ελάχιστο απαιτούμενο 46 οπότε γι' αυτό έχουμε padding 8 bytes), padding 8 bytes και 4 bytes FCS, τα οποία δεν εμφανίζονται, άρα συνολικά 64 bytes.

## Άσκηση 4: Περισσότερα για πακέτα ARP

### 4.1

Το φίλτρο αυτό μας εμφανίζει όλα τα πλαίσια που στέλνονται ή λαμβάνονται από την διεύθυνση MAC που συμπληρώσαμε (συγκεκριμένα του υπολογιστή μας).

### 4.2

Το φίλτρο κάνει ότι και πριν απλά σαν επιπλέον περιορισμό στα πλαίσια που εμφανίζει έχουμε τώρα ότι αυτά πρέπει να ενθυλακώνουν ΚΑΙ το ARP πρωτόκολλο.

### 4.3

Ανταλλάχθηκαν 8 πακέτα ARP.

eth.addr == 70:85:C2:88:FD:B1 and arp						
No.	Time	Source	Destination	Protocol	Length	Info
42	9.029996	70:85:c2:88:fd:b1	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.1.1? Tell 192.168.1.5
43	9.030322	3c:98:72:5f:ea:a0	70:85:c2:88:fd:b1	ARP	60	192.168.1.1 is at 3c:98:72:5f:ea:a0
51	11.990341	3c:98:72:5f:ea:a0	70:85:c2:88:fd:b1	ARP	60	Who has 192.168.1.5? Tell 192.168.1.1
52	11.990372	70:85:c2:88:fd:b1	3c:98:72:5f:ea:a0	ARP	42	192.168.1.5 is at 70:85:c2:88:fd:b1
118	26.349968	3c:98:72:5f:ea:a0	70:85:c2:88:fd:b1	ARP	60	Who has 192.168.1.5? Tell 192.168.1.1
119	26.349996	70:85:c2:88:fd:b1	3c:98:72:5f:ea:a0	ARP	42	192.168.1.5 is at 70:85:c2:88:fd:b1
169	40.710229	3c:98:72:5f:ea:a0	70:85:c2:88:fd:b1	ARP	60	Who has 192.168.1.5? Tell 192.168.1.1
170	40.710256	70:85:c2:88:fd:b1	3c:98:72:5f:ea:a0	ARP	42	192.168.1.5 is at 70:85:c2:88:fd:b1

```
C:\WINDOWS\system32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

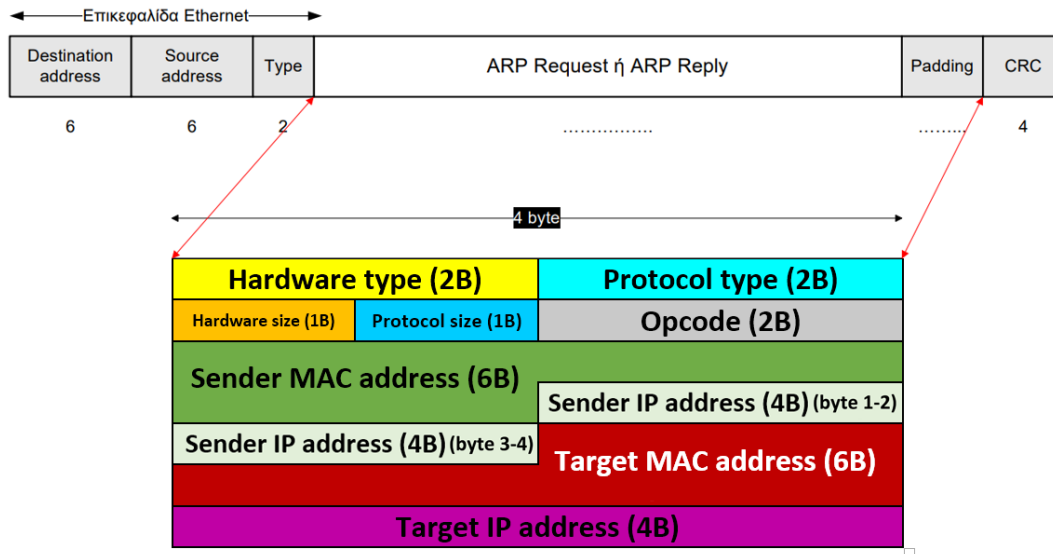
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Παρατηρήσαμε ότι χρειάστηκε να περιμένουμε λίγα δευτερόλεπτα αφότου τελείωσε η εκτέλεση της εντολής «ping ...» προκειμένου να καταγράψει όλα τα πακέτα το Wireshark.

### 4.4

Η διαφοροποίηση βρίσκεται στο πεδίο Type του πλαισίου Ethernet, όπου τα πακέτα ARP έχουν τιμή 0x0806, ενώ τα πακέτα IPv4 έχουν τιμή 0x0800.

#### 4.5



#### 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 υποδεικνύει το 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

Το πεδίο Protocol size έχει τιμή 4 γιατί συμβολίζει το μήκος της διεύθυνσης πρωτοκόλλου, η οποία στην περίπτωση μας είναι IPv4 άρα αναπαρίσταται με 4 bytes.

#### 4.10

Όσον αφορά το Hardware Size, διαβάζουμε ότι πρόκειται για το μήκος των διευθύνσεων Hardware σε bytes. Επομένως, αναφέρεται σε διευθύνσεις MAC, οι οποίες 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

```
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: 70:85:c2:88:fd:b1
  Sender IP address: 192.168.1.5
  Target MAC address: 00:00:00:00:00:00
  Target IP address: 192.168.1.1
```

No.	Time	Source	Destination	Protocol	Length	Info
42	9.029996	70:85:c2:88:fd:b1	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.1.1? Tell 192.168.1.5

Η διεύθυνση MAC του παραλήπτη του πλαισίου αυτού είναι: ff:ff:ff:ff:ff:ff. (broadcast). 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 έχει συνολικό μήκος 42 bytes, ενώ το πακέτο ARP αποτελεί τα 28 εξ αυτών.

#### 4.14

Του πεδίου Opcode προηγούνται 20 bytes.

#### 4.15

Η τιμή του πεδίου Opcode είναι 0x0001 (request).

#### 4.16

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

#### **4.17**

Αντίστοιχα, η διεύθυνση IP του αποστολέα, είναι στο πεδίο 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. Στην δική μας περίπτωση, 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 οποίας γνωρίζουμε την IP.

#### **4.20**

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

#### **4.21**

Η τιμή του πεδίου Opcode στο ARP reply έχει τιμή 0x0002.

#### **4.22**

Η διεύθυνση IPv4 του αποστολέα βρίσκεται στο πεδίο Sender IP address του πακέτου ARP reply.

#### **4.23**

Η διεύθυνση MAC του αποστολέα βρίσκεται στο πεδίο Sender MAC address.

#### **4.24**

Η διεύθυνση IPv4 του παραλήπτη βρίσκεται στο πεδίο Target IP address.

#### **4.25**

Η διεύθυνση MAC του υπολογιστή που έχει τη διεύθυνση IPv4 για την οποία έγινε η ερώτηση βρίσκεται στο πεδίο Sender MAC address, αφού δίνει την απάντηση στην ερώτηση που κάναμε broadcast προηγουμένως, οπότε τώρα είναι ο αποστολέας του ARP reply.

#### **4.26**

Το πλαίσιο Ethernet έχει συνολικό μήκος 60 bytes, ενώ το πακέτο ARP αποτελεί τα 28 εξ αυτών. Εμφανίζονται επιπλέον 18 byte trailer (padding και CRC).

#### **4.27**

Το μέγεθος του ARP είναι ακριβώς το ίδιο και στις δύο περιπτώσεις, διαφέρει όμως το συνολικό μήκος του frame, με το reply να είναι μεγαλύτερο κατά 18 bytes.

#### **4.28**

Το πεδίο Opcode προσδιορίζει εάν πρόκειται για request(0x0001) ή reply(0x0002).

#### **4.29**

Η διαφορά αυτή οφείλεται 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.

#### **4.30**

Μία διαφορά μεταξύ αιτήματος και απάντησης ARP είναι πως η ερώτηση γίνεται με σκοπό να γίνει γνωστή η MAC address μιας εκ των προτέρων γνωστής IP. Έτσι, το Target MAC address είναι το 00:00:00:00:00:00, δηλαδή άγνωστο, ενώ στην απάντηση, είναι πλέον γνωστή η διεύθυνση αυτή και έχει τον ρόλο του Sender MAC address. Επιπρόσθετα, 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. Αντίθετα, στην απάντηση είναι γνωστές οι διευθύνσεις MAC αποστολέα και παραλήπτη και συνεπώς έχουμε unicast μεταξύ αυτών.

#### **4.31**

Εάν ένας κακόβουλος χρήστης απαντούσε σε όλα τα αιτήματα ARP παραχωρώντας την δική του MAC, τότε ότι πακέτα έστελναν οι χρήστες στο τοπικό δίκτυο προς τις διευθύνσεις IP με τις οποίες έκαναν τα request προηγουμένως θα στέλνονταν προς τον κακόβουλο χρήστη. Συνεπώς, θα αποκτούσε πρόσβαση στα δεδομένα αυτά.