



---

# ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

---

## ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 2: ΕΝΘΥΛΑΚΩΣΗ ΚΑΙ ΕΠΙΚΕΦΑΛΙΔΕΣ



18 ΟΚΤΩΒΡΙΟΥ, 2022

ΘΟΔΩΡΗΣ ΑΡΑΠΗΣ – EL18028

Όνοματεπώνυμο: Θοδωρής Αράπης	Ομάδα: 2
Όνομα PC/ΛΣ: DESKTOP-JGHL94V/ WINDOWS 10	Ημερομηνία: 18/10/2022
Διεύθυνση IP: 192.168.1.5	Διεύθυνση MAC: 70-85-C2-88-FD-B1

\*\* Η εργασία ξεκίνησε στο PCLAB της σχολής αλλά λόγω περιορισμού δικαιωμάτων χρήστη στο pc επέλεξα να ξανακάνω από την αρχή την εργασία στον προσωπικό μου υπολογιστή. \*\*

## Άσκηση 1: Στρώμα ζεύξης δεδομένων

### 1.1

Το φίλτρο «arp or ip» μας εμφανίζει τα πλαίσια που διέπονται είτε από το πρωτόκολλο ARP είτε το IPv4.

### 1.2

Οι επικεφαλίδες είναι: Destination, Source και Type.

```

▼ Ethernet II, Src: ASRockIn_88:fd:b1 (70:85:c2:88:fd:b1)
  > Destination: Sercomm_5f:ea:a0 (3c:98:72:5f:ea:a0)
  > Source: ASRockIn_88:fd:b1 (70:85:c2:88:fd:b1)
  Type: IPv4 (0x0800)

```

### 1.3

Όχι, δεν εμφανίζεται κάποιο σχετικό πεδίο.

### 1.4

Το μήκος των διευθύνσεων Ethernet είναι 6 bytes (6 διψήφιοι δεκαεξαδικοί αριθμοί για διεύθυνση MAC).

```

> Frame 31: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{ECE84... 0000 3c 98 72 5f ea a0 70
▼ Ethernet II, Src: ASRockIn_88:fd:b1 (70:85:c2:88:fd:b1), Dst: Sercomm_5f:ea:a0 (3c:98:72:5f:ea:a0) 0010 00 3c dd 5f 00 00 40
  > Destination: Sercomm_5f:ea:a0 (3c:98:72:5f:ea:a0) 0020 01 01 08 00 4d 3d 00

```

### 1.5

Το συνολικό μήκος της επικεφαλίδας Ethernet είναι 14 bytes (6 bytes Destination, 6 bytes Source και 2 Bytes Type).

```

> Frame 31: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{ECE84... 0000 3c 98 72 5f ea a0 70 85 c2 88 fd b1 08 00
▼ Ethernet II, Src: ASRockIn_88:fd:b1 (70:85:c2:88:fd:b1), Dst: Sercomm_5f:ea:a0 (3c:98:72:5f:ea:a0) 0010 00 3c dd 5f 00 00 40 01 d9 b2 c0 a8 01 05

```

## 1.6

Το πεδίο Type καθορίζει το πρωτόκολλο δικτύου (π.χ. 0x0806 για ARP, 0x0800 για IP).

## 1.7

Καταλαμβάνει τα δύο τελευταία byte της επικεφαλίδας Ethernet.

```
> Frame 31: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{ECE84...
Ethernet II, Src: ASRockIn_88:fd:b1 (70:85:c2:88:fd:b1), Dst: Sercomm_5f:ea:a0 (3c:98:72:5f:ea:a0)
  > Destination: Sercomm_5f:ea:a0 (3c:98:72:5f:ea:a0)
  > Source: ASRockIn_88:fd:b1 (70:85:c2:88:fd:b1)
  Type: IPv4 (0x0800)
```

0000	3c 98 72 5f ea a0 70 85 c2 88 fd b1 08 00 4
0010	00 3c dd 5f 00 00 40 01 d9 b2 c0 a8 01 05 0
0020	01 01 08 00 4d 3d 00 01 00 1e 61 62 63 64 6
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 7
0040	77 61 62 63 64 65 66 67 68 69

## 1.8

Το πεδίο αυτό για πακέτα IPv4 έχει τιμή 0x0800.

## 1.9

Δοκιμάζουμε σαν φίλτρο αντί για «arp or ip» σκέτο «arp» και δεν εμφανίζεται καμία καταγραφή. Εκτελώντας άλλες καταγραφές όμως, βρίσκουμε πως η τιμή θα ήταν 0x0806.

Type: ARP (0x0806)

## Άσκηση 2: Στρώμα ζεύξης δεδομένων

### 2.1

Το φίλτρο «icmp» εμφανίζει τα πακέτα του Στρώματος δικτύου που διέπονται από το πρωτόκολλο ICMP.

### 2.2

Οι διευθύνσεις στο πρωτόκολλο IPv4 έχουν μήκος 4 bytes (0.0.0.0 έως 255.255.255.255)

### 2.3

Το πρώτο πεδίο είναι το version και το δεύτερο είναι το Header Length.

```
▼ Internet Protocol Version 4, Src: 192.168.1.5, Dst: 1.1.1.1
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
```

### 2.4

Το κάθε πεδίο έχει μήκος 4 bit και έχουν τιμές Version = 0100 =  $4_{10}$  και Header Length = 0101 =  $5_{10}$ .

### 2.5

Επιλέγουμε ένα τυχαίο πακέτο και κάνουμε κλικ στην επικεφαλίδα του IPv4. Στα περιεχόμενα βλέπουμε ότι υπογραμμίζονται 20 διψήφιοι δεκαεξαδικοί αριθμοί. Άρα, η επικεφαλίδα IPv4 έχει μήκος 20 bytes.

```
> Frame 31: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{ECE84...}
> Ethernet II, Src: ASRockIn_88:fd:b1 (70:85:c2:88:fd:b1), Dst: Sercomm_5f:ea:a0 (3c:98:72:5f:ea:a0)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 1.1.1.1
> Internet Control Message Protocol
```

0000	3c 98 72 5f ea a0 70 85 c2 88 fd b1 08 00 45 00
0010	00 3c dd 5f 00 00 40 01 d9 b2 c0 a8 01 05 01 01
0020	01 01 08 00 4d 3d 00 01 00 1e 61 62 63 64 65 66
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0040	77 61 62 63 64 65 66 67 68 69

### 2.6

Έχουμε από πριν ότι Header Length = 0101 =  $5_{10}$ . Σύμφωνα με το Documentation, το Header Length: “Specifies the length of the IP packet header in 32 bit words”. Συνεπώς θα ισχύει ότι (32 bits = 4 bytes)  $5 \cdot 4 = 20$  bytes.

### 2.7

Πατώντας την επικεφαλίδα του Ethernet Layer, βρίσκουμε ότι καταλαμβάνει 14 bytes από τα συνολικά 74 bytes (on wire) του πλαισίου. Άρα, 60 bytes αντιστοιχούν στο πακέτο IPv4, θεωρώντας ότι το ICMP πρωτόκολλο είναι μέρος του IP Layer.

## 2.8

Ναι, υπάρχει το πεδίο total length που περιέχει την τιμή του συνολικού μήκους του data-gram.

## 2.9

Το payload του πακέτου έχει μήκος 40 bytes.

## 2.10

Το payload του πακέτου IPv4 προκύπτει αν από το Total Length του πακέτου (60 bytes) αφαιρέσουμε το Header Length (20 bytes).

## 2.11

Το πεδίο Protocol της επικεφαλίδας IPv4 καθορίζει το πρωτόκολλο ανωτέρου στρώματος.

## 2.12

Το πεδίο αυτό βρίσκεται στο 10ο byte της επικεφαλίδας IPv4.

Total Length: 60	0000	3c 98 72 5f ea a0 70 85 c2 88 fd b1 08 00 45 00
Identification: 0xdd5f (56671)	0010	00 3c dd 5f 00 00 40 01 d9 b2 c0 a8 01 05 01 01
> 000. .... = Flags: 0x0	0020	01 01 08 00 4d 3d 00 01 00 1e 61 62 63 64 65 66
...0 0000 0000 0000 = Fragment Offset: 0	0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
Time to Live: 64	0040	77 61 62 63 64 65 66 67 68 69
Protocol: ICMP (1)		

## 2.13

Για το πρωτόκολλο ICMP η τιμή του είναι 1.

## Άσκηση 3: Στρώμα Μεταφοράς

### 3.1

Το φίλτρο «tcp or udp» εμφανίζει τα πακέτα τα οποία ενθυλακώνουν είτε το πρωτόκολλο TCP είτε το UDP στο στρώμα μεταφοράς τους.

### 3.2

Παρατηρούμε τα πρωτόκολλα TCP Και UDP του στρώματος μεταφοράς.

### 3.3

Για πακέτα που μεταφέρονται με πρωτόκολλο TCP, στο πεδίο protocol έχουν τιμή 6, ενώ αυτά που μεταφέροντα με UDP (IPv6 protocol) έχουν τιμή 17.

Protocol: TCP (6)

Next Header: UDP (17)

### 3.4

Κοινά είναι τα πεδία: Source Port, Destination Port, Checksum

▼ User Datagram Protocol, Src Port: 62328, Dst Port: 443

Source Port: 62328

Destination Port: 443

Length: 1234

Checksum: 0xecb7 [unverified]

[Checksum Status: Unverified]

[Stream index: 8]

> [Timestamps]

UDP payload (1226 bytes)

▼ Transmission Control Protocol, Src Port: 443, Dst Port: 53339, Seq: 1, Ack: 1, Len: 0

Source Port: 443

Destination Port: 53339

[Stream index: 0]

[Conversation completeness: Incomplete (12)]

[TCP Segment Len: 0]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 3347957630

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 1221356802

0101 .... = Header Length: 20 bytes (5)

> Flags: 0x010 (ACK)

Window: 8

[Calculated window size: 8]

[Window size scaling factor: -1 (unknown)]

Checksum: 0xfabd [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

> [Timestamps]

### 3.5

Το μήκος της επικεφαλίδας UDP είναι 8 bytes.

> Frame 216: 1288 bytes on wire (10304 bits), 1288 bytes captured (10304 bits) on interface \Device\N	0030	00 00 00 00 20 04	f3 78	01 bb 04 d2 ec b7	5d d9
> Ethernet II, Src: ASRockIn_88:fd:b1 (70:85:c2:88:fd:b1), Dst: Sercomm_5f:ea:a0 (3c:98:72:5f:ea:a0)	0040	4d 07 18 33 ab 26	9a b5	4d f6 93 4a 6e 29	87 9e
> Internet Protocol Version 6, Src: 2a02:587:e81a:ebdc:dd5:6a3f:8ad5:d7a, Dst: 2a00:1450:4001:801::20	0050	e7 21 c8 62 c0 bb fe 1c	37 5d 64 dd 34 62 48	c4	
▼ User Datagram Protocol, Src Port: 62328, Dst Port: 443	0060	8b 02 31 a1 e8 43 f4 f1	0b 79 57 ae fb 46 2d	7b	

### 3.6

Ναι, υπάρχει το πεδίο Length που μας δίνει το συνολικό μήκος των UDP datagrams.

### 3.7

Το πεδίο Header Length στην επικεφαλίδα IPv4 μας πληροφορεί για το μήκος της επικεφαλίδας και βρίσκεται στα πρώτα 4 bits του 13ου byte της επικεφαλίδας TCP.

### 3.8

Όχι δεν υπάρχει πεδίο που να μας πληροφορεί για το συνολικό μήκος των τεμαχίων TCP. Αυτό μπορεί να προκύψει αφαιρώντας την τιμή του πεδίου Header Length από την τιμή του πεδίου Total Length της επικεφαλίδας IPv4.

### 3.9

Στην επικεφαλίδα TCP υπάρχει η θύρα 443 (HTTPS, HTTP over SSL/TLS) είτε ως Source είτε ως Destination. Όμοια και στην επικεφαλίδα UDP υπάρχει η θύρα 443 πάλι είτε ως Source είτε ως Destination.

### 3.10

Παρατηρήσαμε επίσης (με την ίδια διαδικασία με το προηγούμενο ερώτημα) ορισμένες επικεφαλίδες TCP με την θύρα 80 (HTTP). Ακόμη παρατηρήσαμε πακέτα που ενθυλακώνουν το πρωτόκολλο στρώματος εφαρμογής DNS.

## **Άσκηση 4: Στρώμα Εφαρμογής**

### **4.1**

Παρατηρούμε ότι το DNS χρησιμοποιεί το πρωτόκολλο του στρώματος μεταφοράς UDP.

### **4.2**

Παρατηρούμε ότι το HTTP χρησιμοποιεί το πρωτόκολλο του στρώματος μεταφοράς TCP.

### **4.3**

Το 17ο bit (πεδίο QR) καθορίζει αν είναι Query (τιμή 0) ή Response (τιμή 1).

### **4.4**

Η θύρα προορισμού των DNS ερωτήσεων είναι η 53 (DNS, Domain Name System).

### **4.5**

Οι θύρες πηγής των DNS ερωτήσεων είναι: 51970, 58062, 62516, 64865, 63536, 57521, 54333, 59083, 64759, 61710, 60674, 62357, 56309

### **4.6**

Η θύρα πηγής των DNS απαντήσεων είναι η 53.

### **4.7**

Οι θύρες προορισμού των DNS απαντήσεων είναι: 51970, 58062, 62516, 64865, 63536, 57521, 54333, 59083, 64759, 61710, 60674, 62357, 56309 (προφανώς οι ίδιες με τις θύρες πηγής των DNS ερωτήσεων)

### **4.8**

Παρατηρούμε ότι οι θύρες προέλευσης των DNS ερωτήσεων είναι οι θύρες των DNS απαντήσεων και αντιστρόφως, η θύρα προορισμού των DNS ερωτήσεων είναι η θύρα προέλευσης των DNS απαντήσεων.

### **4.9**

Εύκολα συμπεραίνουμε από τις παραπάνω παρατηρήσεις (και με βάση το documentation TCP/UDP ports) ότι η πασίγνωστη θύρα που ακούει ο DNS Server είναι η 53.

### **4.10**

Τα HTTP μηνύματα που παράγει ο υπολογιστής μας (source IP είναι η IP του υπολογιστή μας) έχουν ως Destination Port την θύρα 80 (HTTP, HyperText Transfer Protocol).



#### 4.11

Οι θύρες πηγής των HTTP μηνυμάτων που έστειλε ο υπολογιστής μας είναι οι 53461 και 50858.

#### 4.12

Η θύρα πηγής των αντίστοιχων απαντήσεων HTTP του εξυπηρετητή ιστού είναι η 80.

#### 4.13

Οι θύρες προορισμού των αντίστοιχων απαντήσεων HTTP του εξυπηρετητή ιστού είναι οι 53461 και 50858.

#### 4.14

Εύκολα συμπεραίνουμε από τις παραπάνω παρατηρήσεις (και με βάση το documentation TCP/UDP ports) ότι η πασίγνωστη θύρα που ακούει ο HTTP Server είναι η 80.

#### 4.15

Όπως περιμέναμε, οι θύρες πηγής των ερωτήσεων HTTP ταυτίζονται με τις θύρες προορισμού των απαντήσεων HTTP και αντίστροφα.

#### 4.16

```
GET /lab2/ HTTP/1.1
Host: edu-dy.cn.ntua.gr
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: _ga=GA1.2.250670653.1654437880

HTTP/1.1 200 OK
Date: Sat, 15 Oct 2022 22:44:53 GMT
Server: Apache/2.2.22 (FreeBSD) mod_ssl/2.2.22 OpenSSL/0.9.8zh-freebsd DAV/2
Last-Modified: Sat, 08 Oct 2022 21:43:41 GMT
ETag: "18afa1-a3-5ea8cd1e01d40"
Accept-Ranges: bytes
Content-Length: 163
Cache-Control: max-age=84600, public
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

<HTML>
  <HEAD>
    <TITLE>CN Lab2</TITLE>
  </HEAD>
  <body>
    <h1>Hello labuser!</h1>
    <h2>Computer Networks 2022-23</h2>
    <h3>Lab 2</h3>
  </body>
</HTML>
```

Το πρώτο μήνυμα HTTP έχει ονομασία GET /lab2/ HTTP/1.1.

#### **4.17**

Ο κωδικός απάντησης που μας επιστρέφει ο εξυπηρετητής ιστού είναι «HTTP/1.1 200 OK».

#### **4.18**

Παρατηρούμε ότι δεν εμφανίζεται καμία καταγραφή πρωτοκόλλων DNS. Αυτό συμβαίνει διότι όταν επισκεπτόμαστε μία σελίδα, αποθηκεύεται προσωρινά το DNS της σε ένα τοπικό buffer, με σκοπό την ταχύτερη φόρτωση της σελίδας κατά την επόμενη σύνδεσή μας εκεί. Ως εκ τούτου, αποφεύγεται η μετάφραση από DNS σε IP στο Ίντερνετ και γίνεται τοπικά. Η εντολή «flushdns» καθαρίζει αυτήν την μνήμη και έτσι επαναλαμβάνεται η διαδικασία μετάφρασης του ονόματος της σελίδας σε IP μέσω Ίντερνετ την επόμενη φορά που θα επιχειρήσουμε να συνδεθούμε στην σελίδα.