Δίκτυα Υπολογιστών

Εργαστηριακή Άσκηση 2
Ενθυλάκωση και Επικεφαλίδες

Ονοματεπώνυμο: Νικόλαος Παγώνας, el18175	**Ομάδα:** 4 (Τρίτη εξ' αποστάσεως)
Όνομα PC/ΛΣ: nick-ubuntu/Ubuntu 20.04.3 LTS	**Ημερομηνία:** Τρίτη 19/10/2021
Διεύθυνση IP: `192.168.1.15`	**Διεύθυνση MAC:** `3c:2c:30:e1:1c:55`

1. Στρώμα ζεύξης δεδομένων

1.1

Με το φίλτρο `arp || ip` εμφανίζονται μόνο τα πακέτα που έχουν πρωτόκολλο `ARP` ή `IP`.

1.2

Τα ονόματα των πεδίων της επικεφαλίδας του πλαισίου Ethernet είναι: `Destination, Source, Type`

1.3

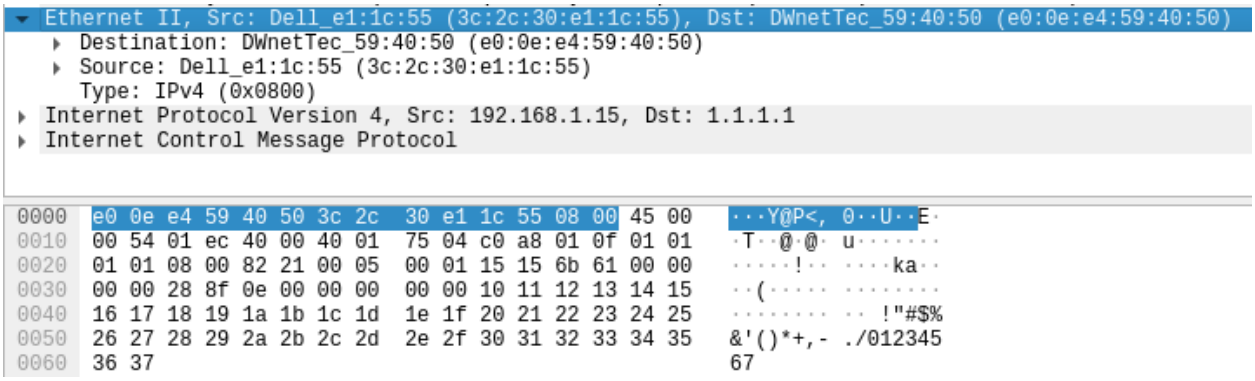
Όχι, δεν υπάρχει τέτοιο πεδίο.

1.4

Οι διευθύνσεις Ethernet έχουν μήκος 6 byte.

1.5

Κάνουμε highlight την επικεφαλίδα Ethernet ώστε να δούμε την αντιστοιχία της σε byte:



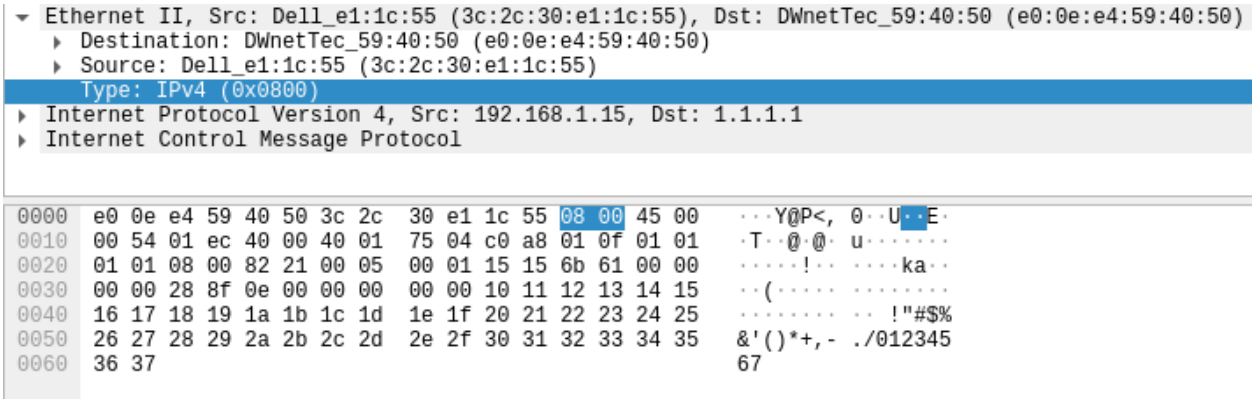
Παρατηρούμε λοιπόν ότι το συνολικό μήκος της επικεφαλίδας Ethernet είναι 14 byte.

1.6

Το πεδίο του πλαισίου Ethernet που καθορίζει το πρωτόκολλο δικτύου είναι το πεδίο Type.

1.7

Η θέση που καταλαμβάνει μέσα στην επικεφαλίδα Ethernet είναι στο τέλος-τέλος (τελευταία δύο bytes), όπως φαίνεται και στην εικόνα:



1.8

Η τιμή του πεδίου αυτού για πακέτα IPv4 είναι 0x0800.

1.9

Για ARP πακέτα, η τιμή του πεδίου είναι 0x0806.

2. Στρώμα Δικτύου

2.1

Το φίλτρο `icmp` εμφανίζει μόνο πακέτα που έχουν πρωτόκολλο ICMP.

2.2

Το μήκος των διευθύνσεων IPv4 είναι 4 bytes.

2.3

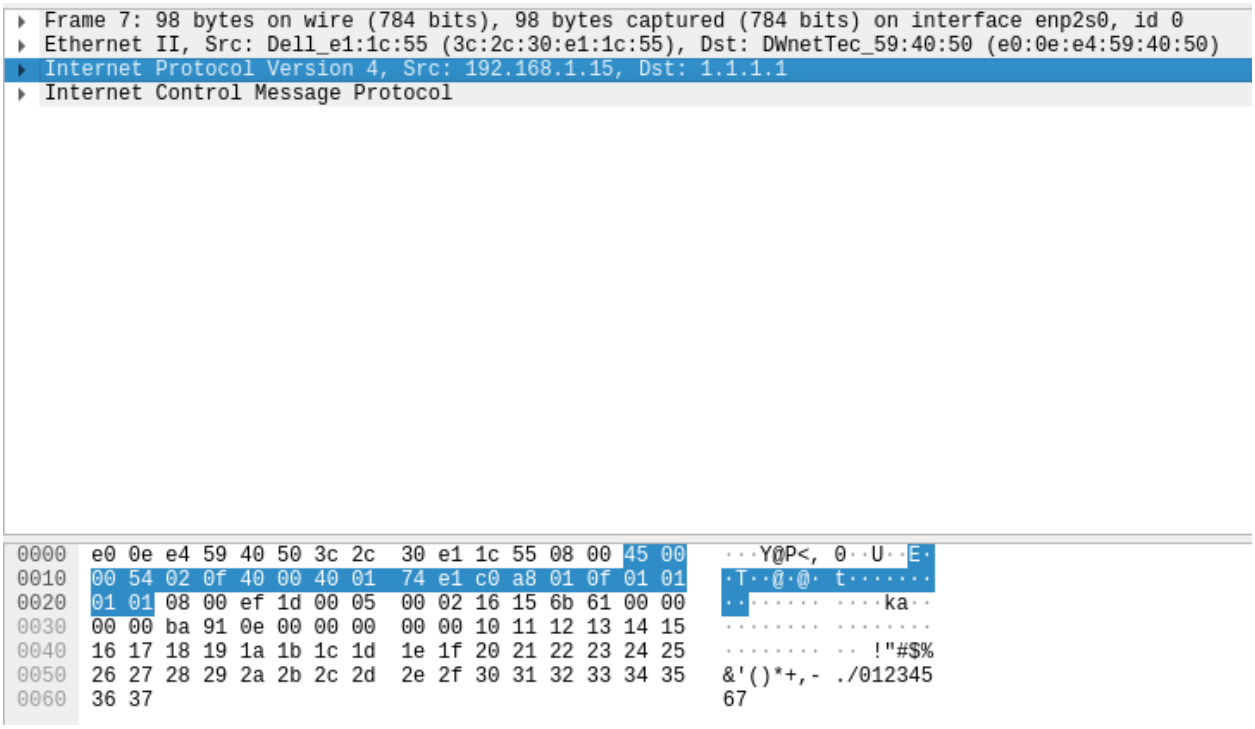
Τα ονόματα των δύο πρώτων πεδίων της επικεφαλίδας IPv4 είναι `Version` και `Header Length`.

2.4

Το μήκος σε bit τόσο του πεδίου `Version` όσο και του πεδίου `Header Length` είναι 4 bit (όπως φαίνεται από τον σύνδεσμο που παρατίθεται στην εκφώνηση της αναφοράς, αλλά και από το `Wireshark`). Η τιμή του πεδίου Version είναι **0100** (Version 4), ενώ του πεδίου Header Length είναι **0101**, που αντιστοιχεί σε 20 bytes, όπως αναγράφεται και στο Wireshark.

2.5

Στο Wireshark, κάνουμε highlight την επικεφαλίδα IPv4 και βλέπουμε ότι έχει συνολικό μέγεθος 20 bytes.



2.6

Από το site που παρατέθηκε στην εκφώνηση σχετικά με το πρωτόκολλο IPv4:

IHL, Internet Header Length. 4 bits.
Specifies the length of the IP packet header in 32 bit words. The minimum value for a valid header is 5.

Αυτό σημαίνει ότι αφού το Header Length έχει τιμή 5, τότε η επικεφαλίδα έχει μέγεθος:

$$\frac{5 \cdot 32}{8} = 20 \text{ bytes.}$$

Με αυτόν τον τρόπο λοιπόν προκύπτει και το μέγεθος της επικεφαλίδας, χωρίς να χρειαστούμε τη βοήθεια του παραθύρου περιεχομένων.

2.7

Βλέπουμε από το παράθυρο με τα περιεχόμενα ότι το συνολικό μήκος αυτού του πακέτου είναι 84 bytes.

2.8

Υπάρχει το πεδίο `Total Length` με τιμή 84 bytes, η οποία συμφωνεί με το παραπάνω.

2.9

Το μήκος δεδομένων του πακέτου IPv4 είναι 64 bytes.

2.10

Το μήκος των δεδομένων προκύπτει αν από το `Total Length` αφαιρέσουμε το `Header Length`:

$$(84 - 20 = 64 \text{ bytes})$$

2.11

Το πεδίο που καθορίζει το πρωτόκολλο στρώματος μεταφοράς είναι το `Protocol`.

2.12

Η θέση του σε σχέση με την αρχή της επικεφαλίδας IPv4 είναι στο 10^{o} byte.

2.13

Για το πρωτόκολλο ICMP η τιμή του είναι 01.

3. Στρώμα Μεταφοράς

3.1

Το παραπάνω φίλτρο απεικόνισης εμφανίζει μόνο πακέτα που έχουν πρωτόκολλο `TCP` ή `UDP`.

3.2

Παρατηρούμε τα πρωτόκολλα `TCP` και `UDP`.

3.3

Η τιμή του πεδίου `Protocol` στην επικεφαλίδα IPv4 για το πρωτόκολλο TCP είναι 6, ενώ για το UDP είναι 17 (στο δεκαδικό σύστημα).

3.4

Τα κοινά ονόματα πεδίων μεταξύ των δύο πρωτοκόλλων είναι: `Source Port, Destination Port` και `Checksum`.

3.5

Το μήκος της επικεφαλίδας των δεδομενογραμμάτων UDP είναι 8 bytes.

3.6

Ναι, υπάρχει (το πεδίο `Length`).

3.7

Το πεδίο που καθορίζει το μήκος της επικεφαλίδας του τεμαχίου TCP είναι το `Header Length`, και βρίσκεται στο $13^{ο}$ byte της επικεφαλίδας (συγκεκριμένα στα 4 MSB).

3.8

Δεν υπάρχει πεδίο που να δίνει το συνολικό μήκος ενός τεμαχίου TCP. Το μήκος αυτό προκύπτει ως εξής:

$$\text{Μήκος πλαισίου IP} - (\text{Μήκος επικεφαλίδας IP} + \text{Μήκος επικεφαλίδας TCP})$$

Μπορούμε να βρούμε το μήκος πλαισίου IP από το πεδίο `Total Length` του IP header, το μήκος επικεφαλίδας IP από το πεδίο `Header Length`, και το μήκος επικεφαλίδας TCP από το πεδίο `Header Length` του TCP header.

3.9

Με βάση το `Destination Port` του TCP header μπορούμε να βρούμε τον τύπο του πρωτοκόλλου εφαρμογής, αντιστοιχώντας το εκάστοτε port, με τη βοήθεια του πίνακα που βρίσκεται στο link της εκφώνησης.

3.10

Άλλα πρωτόκολλα εφαρμογής που παρατηρήθηκαν στον πίνακα είναι:

- RWP, Remote Write Protocol
- FTP, File Transfer Protocol
- SMTP, Simple Mail Transfer Protocol

- RAP, Internet Route Access Protocol
- Internet Message Protocol
- MTP, Mail Transfer Protocol

4. Στρώμα Εφαρμογής

4.1

Το `DNS` χρησιμοποιεί το πρωτόκολλο `UDP`.

4.2

Το `HTTP` χρησιμοποιεί το πρωτόκολλο `TCP`.

4.3

Όπως βλέπουμε στο λινκ που παρατέθηκε στην εκφώνηση (αλλά και στο Wireshark), το πρώτο bit της σημαίας μας δείχνει αν πρόκειται για ερώτηση (οπότε θα είναι 0) ή για απάντηση (οπότε θα είναι 1).

4.4

Η θύρα προορισμού των ερωτήσεων DNS είναι η 53.

4.5

Αντίστοιχα, οι θύρες προέλευσης των ερωτήσεων DNS είναι οι 34512, 33415, 35278, 41535, 34401, 48900, 45347, 57290, 56403, 58318.

4.6

Η θύρα προέλευσης των απαντήσεων DNS είναι πάλι η 53.

4.7

Οι θύρες προορισμού των απαντήσεων DNS είναι οι 34512, 33415, 35278, 41535, 34401, 48900, 45347, 57290, 56403, 58318.

4.8

Οι θύρες προορισμού των απαντήσεων είναι ίδιες με τις θύρες προέλευσης των ερωτήσεων DNS που βρήκαμε πριν, και με ίδια σειρά. Αυτό είναι λογικό, αφού η θύρα στην οποία γίνεται μία ερώτηση θα πρέπει να είναι και η θύρα στην οποία θα δοθεί η απάντηση.

4.9

Η well-known θύρα όπου ακούει ο εξυπηρετητής DNS είναι η 53.

4.10

Η θύρα προορισμού των μηνυμάτων HTTP που παράγει ο υπολογιστής μας είναι η θύρα 80.

4.11

Η θύρα προέλευσης των μηνυμάτων HTTP που έστειλε ο υπολογιστής μας είναι η 42994.

4.12

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

4.13

Η θύρα προορισμού των απαντήσεων είναι η 42994.

4.14

Η well-known θύρα όπου ακούει ο εξυπηρετητής HTTP είναι η 80.

4.15

Παρατηρούμε ότι οι θύρες προέλευσης των μηνυμάτων HTTP είναι ίδιες με τις θύρες προορισμού των αντίστοιχων απαντήσεων του εξυπηρετητή. Αυτό είναι λογικό, αφού η θύρα στην οποία γίνεται μία ερώτηση θα πρέπει να είναι και η θύρα στην οποία θα δοθεί η απάντηση.

4.16

Η ονομασία του πρώτου μηνύματος HTTP από τον υπολογιστή μας προς τον server είναι:
`GET /lab2/ HTTP/1.1 .`

4.17

Η απάντηση είναι: `HTTP/1.1 200 OK` άρα ο κωδικός είναι 200 OK.

4.18

Βλέπουμε ότι αν ξαναεπισκεφτούμε την ιστοσελίδα, δεν καταγράφεται κίνηση πακέτων με πρωτόκολλο DNS, αφού οι αντιστοιχίσεις υπάρχουν αποθηκευμένες από πριν και άρα δεν χρειάζεται να ξαναγίνει η αντιστοίχιση. Εκτελώντας την εντολή `sudo systemd-resolve --flush-caches`, σιγουρεύουμε ότι θα σταλούν και αυτά τα πακέτα.