Όνοματεπώνυμο: Μάρκος Δεληγιάννης		Ομάδα: 3
Όνομα PC/ΛΣ: MarkiniHP / Linux Mint		Ημερομηνία: 12 / 10 / 2022
Διεύθυνση IP: 192 . 168 . 1 . 12	Διεύθυνση MAC: 38 – EA – A7 – D9 – AB – 1A	

Εργαστηριακή Άσκηση 2
Ενθυλάκωση και Επικεφαλίδες

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 Με αυτό το φίλτρο απεικόνισης εμφανίζονται μόνο τα πλαίσια με επικεφαλίδες ARP ή IP.
1.2 Τα ονόματα των πεδίων είναι: Destination (Προορισμός), Source (Πηγή) και Type (Τύπος).
1.3 Δεν υπάρχει τέτοιο πεδίο στην επικεφαλίδα Ethernet.
1.4 Οι διευθύνσεις Ethernet είναι της μορφής xx:xx:xx:xx:xx:xx, με x δεκαεξαδικό ψηφίο, οπότε το μήκος είναι 6 byte.
1.5 Μήκος επικεφαλίδας = Μήκ. Dest. + Μήκ. Src + Μήκ. Type = 6 + 6 + 2 = 14 byte
1.6 Το πεδίο Type, με τιμή IPv4.
1.7 Επιλέγοντας το πεδίο Type υπογραμμίζεται το 13ο και 14ο byte της επικεφαλίδας.
1.8 Για πακέτα IPv4 η τιμή του πεδίου Type είναι 0x0800.
1.9 Για πακέτα ARP έχουμε την τιμή 0x0806.

2

2.1 Με αυτό το φίλτρο απεικόνισης εμφανίζονται μόνο τα πλαίσια με επικεφαλίδες ICMP.
2.2 Οι διευθύνσεις IPv4 είναι της μορφής x.x.x.x, με x από 0 μέχρι 255, οπότε έχουν μέγεθος 4 byte.
2.3 Πρώτο πεδίο: έκδοση του πρωτοκόλλου (version) Δεύτερο Πεδίο: μέγεθος της επικεφαλίδας (IHL).
2.4 Και τα δύο έχουν μήκος 4 bit (το καθένα). Η τιμή του version είναι 0b0100=4 και του IHL 0b0101=5.
2.5 Επιλέγοντας την επικεφαλίδα IPv4 στο κάτω μέρος της οθόνης εμφανίζεται το μήκος του header (20 byte).
2.6 Η τιμή του πεδίου IHL είναι 0b0101=5. Σύμφωνα με το πρωτόκολλο αυτές είναι οι 32 bit λέξεις (4 byte) που αποτελούν το header. Συνεπώς το μήκος της επικεφαλίδας είναι 5*4=20 byte, όπως αναμέναμε.
2.7 Μήκ. πακέτου IPv4 = Συνολ. Μήκ. Πλαισίου – Μήκ. Επικεφ. Ethernet = 98 byte – 14 byte = 84 byte.
2.8 Το 5ο πεδίο της επικεφαλίδας (Total length) επιτελεί αυτόν το σκοπό και έχει τιμή 84, το οποίο βρίσκεται σε συμφωνία με το 2.7.
2.9 Μήκ. Δεδομένων = Συνολ. Μήκ. - Μήκ. Επικεφ. = 84 byte – 20 byte = 64 byte.
2.10 Προκύπτει με την αφαίρεση: Total length (του IPv4 πακέτου) - IHL

.....

2.11 Το πεδίο protocol.
2.12 Το πεδίο protocol είναι το 10ο byte της επικεφαλίδας IPv4.
2.13 Για το ICMP η τιμή του είναι 0x01.

3

3.1 Το φίλτρο αυτό απομονώνει τα πλαίσια με επικεφαλίδες tcp και udp.

3.2 TCP και UDP.

3.3 TCP: 6 UDP: 17

3.4 Τα κοινά πεδία είναι το source port, destination port και το checksum.

.....

3.5 8 byte.

3.6 Το πεδίο Length έχει τη ζητούμενη πληροφορία.

3.7 Το πεδίο Data offset, το οποίο είναι το 13ο byte της επικεφαλίδας TCP.

3.8 Δεν υπάρχει τέτοιο πεδίο. Για την εύρεση της ζητούμενης πληροφορίας αφαιρούμε από το Total Length (της IPv4 επικεφαλίδας) το IHL.

3.9 Δεν υπάρχει τέτοιο πεδίο, καθώς το πρωτόκολλο εφαρμογής εξαρτάται από τη θύρα που χρησιμοποιείται.

3.10 TLSv1.2*, DNS, HTTP. *Δεν είναι ακριβώς, δεν κατατάσσεται εύκολα σε OSI

4.1 UDP

4.2 TCP

4.3 Το bit QR. Παίρνει την τιμή 0 για ερώτηση και 1 για απάντηση.

4.4 Στη θύρα 53.

4.5 Θύρα 36336.

4.6 Θύρα 53.

4.7 Θύρα 36336.

4.8 Είναι ίδιες, όπως είναι αναμενόμενο.

.....

4.9 Η θύρα 53.

4.10 Η θύρα 80.

4.11 Η θύρα 44920.

4.12 Η θύρα 80.

4.13 Η θύρα 44920.

4.14 Η θύρα 80.

4.15 Είναι ίδιες, όπως είναι αναμενόμενο.

.....

4.16 Get request.

4.17 Κωδικός κατάστασης: 200 (OK).

4.18 Η εντολή χρειαζόταν ώστε να μην υπάρχει τοπικά αρχείο αντιστοίχισης ονομάτων με διευθύνσεις ip και ο υπολογιστής να αναγκαστεί να κάνει DNS request. Στην περίπτωσή μας βέβαια, παρόλο που δεν κάνουμε flush την cache το αίτημα έγινε ξανά. Αυτό οφείλεται στο ότι το ΛΣ (Linux) δεν κρατάει σχολαστικά cache για τα αιτήματα DNS.