

Όνοματεπώνυμο: Ιωάννης Γιαννούκος		Ομάδα: 3
Όνομα PC/ΛΣ: JohnJohn / Windows 11		Ημερομηνία: 19/10/22
Διεύθυνση IP: 147.102.200.73	Διεύθυνση MAC: 3C-6A-A7-9A-B3-CF	

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.

Άσκηση 1

- 1.1) Με το φίλτρο αυτό απομονώνουμε τα πλαίσια τύπου ARP και τα πακέτα ICMP που έχουν ενθυλακωθεί σε επικεφαλίδα τύπου IP.
- 1.2) Destination, Source, Type
- 1.3) Όχι
- 1.4) 6 bytes
- 1.5) 14bytes
- 1.6) Τα 2 τελευταία bytes της επικεφαλίδας του.
- 1.7) Τα bytes 10-11(Hex).
- 1.8) 80 00 (Hex)
- 1.9) 08 06 (Hex)

Άσκηση 2

- 2.1) Απομόνωση των πακέτων στρώματος δικτύου.
- 2.2) 4 bytes
- 2.3) Version, Header Length
- 2.4) Version: 4 bit, τιμή «4»
Header Length: 4 bit, τιμή «5»
- 2.5) 20 bytes, υπογραμμίζονται 20 bytes στο παράθυρο με τα περιεχόμενα.
- 2.6) Το αποτέλεσμα παρέχεται στο πεδίο "Header Length".
- 2.7) 20 bytes (επικεφαλίδα) και 40 bytes (πληροφορία), τα οποία υπογραμμίζονται στο παράθυρο με τα περιεχόμενα. Σύνολο 60 bytes.
- 2.8) Ναι, το πεδίο Total Length. Συμφωνεί.
- 2.9) 32 bytes
- 2.10) Φαίνεται στο πεδίο "Data (32 bytes)".
- 2.11) Το πεδίο Protocol.
- 2.12) Βρίσκεται στο 10^ο byte από την αρχή της επικεφαλίδας.
- 2.13) 01 (Hex)

Άσκηση 3

- 3.1) Απομόνωση πακέτων που έχουν επικεφαλίδα TCP ή UDP, δηλαδή πακέτων στο επίπεδο μεταφοράς.
- 3.2) TCP, TLS, DNS(UDP), HTTP
- 3.3) TCP (IPv4) : Protocol: TCP
UDP (IPv6) : Next Header: UDP
- 3.4) Τα κοινά ονόματα πεδίων των TCP και UDP είναι τα “Source Port”, “Destination Port” και “Checksum”.
- 3.5) 8 bytes
- 3.6) Ναι, το πεδίο Length.
- 3.7) Το πεδίο Header Length, 13^ο byte.
- 3.8) Όχι.
- 3.9) Από τον πίνακα της ιστοσελίδας <http://www.networksorcery.com/enp/default.htm> βλέπουμε ότι με βάση του Destination Port μπορούμε να αποφανθούμε για το αντίστοιχο πρωτόκολλο εφαρμογής.
- 3.10) DNS, HTTP

Άσκηση 4

- 4.1) Το UDP.
- 4.2) Το TCP πρωτόκολλο.
- 4.3) Το bit0 παίρνει τιμή 0 για ερώτηση και 1 για απάντηση.
- 4.4) Destination Port: 53
- 4.5) Source Port: 51486
- 4.6) Source Port: 53
- 4.7) Destination Port: 51486
- 4.8) Είναι κοινές.
- 4.9) DNS Port: 53
- 4.10) Destination Port: 80
- 4.11) Source Port: 55975
- 4.12) Source Port: 80
- 4.13) Destination Port: 55975
- 4.14) HTTP Port (πασίγνωστη): 80
- 4.15) Είναι κοινές.
- 4.16) “GET /lab2/HTTP/1.1
- 4.17) “200 OK”
- 4.18) Διότι χωρίς να την εκτελέσουμε, τα DNS requests θα έπαιρναν απάντηση από την cache του υπολογιστή μας.