

Όνοματεπώνυμο: Νίκος Μπέλλος		Ομάδα: 3
Όνομα PC/ΛΣ: BELLOS-DELL-G3 / Windows OS		Ημερομηνία: 25 / 10 / 2021
Διεύθυνση IP: 192 . 168 . 1 . 6	Διεύθυνση MAC: 7C - 2A - 31 - 40 - C9 - AF	

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 Εμφανίζονται όλα τα πακέτα που περιέχουν επικεφαλίδες ARP (Address Resolution Protocol) ή IP (Internet Protocol)

1.2 Destination, Source, Type

1.3 Όχι, δεν υπάρχει

1.4 6 bytes

1.5 14 bytes (6 → Destination, 6 → Source, 2 → Type)

1.6 Το πεδίο type του πλαισίου Ethernet

1.7 Καταλαμβάνει τα δύο τελευταία bytes

1.8 HEX τιμή για IPv4 : 08 00

1.9 HEX τιμή για IPv4 (με πακέτα ARP) : 08 06

2

2.1 Εμφανίζονται όλα τα πακέτα με πρωτόκολλο ICMP (Internet Control Message Protocol)

2.2 Μία διεύθυνση IPv4 έχει μήκος 4 bytes

2.3 Πρώτο πεδίο : Version, Δεύτερο πεδίο : Header Length

2.4 Τα πεδία έχουν μήκος 4 bit το καθένα. Το πρώτο έχει τιμή 4 (τύπος πρωτοκόλλου) και το δεύτερο τιμή 5

2.5 Μήκος επικεφαλίδας IPv4 : 20 bytes

2.6 Ταυτίζεται με τη τιμή που αναγράφεται στο πεδίο Header Length της επικεφαλίδας IPv4

2.7 Μήκος πακέτου IPv4 (με βάση τα περιεχόμενα) : 74 bytes

2.8 Το μήκος του πακέτου αναγράφεται και στη λίστα πακέτων και στην επικεφαλίδα Frame και ναι συμφωνεί με αυτό που βρήκαμε παραπάνω

2.9 Μήκος δεδομένων / Data : 32 bytes

2.10 Από την επικεφαλίδα Internet Control Message Protocol κοιτάμε το πεδίο Data στο οποίο αναγράφεται δίπλα το μήκος του

2.11 Το πεδίο που λέγεται 'Protocol'

2.12 Βρίσκεται στο 10 byte από την αρχή της επικεφαλίδας IPv4

2.13 Τιμή Protocol για ICMP : 01 (HEX)

3

- 3.1 Εμφανίζει όλα τα πακέτα που περιέχουν επικεφαλίδες TCP ή UDP
- 3.2 UDP, TCP, QUIC, TLS
- 3.3 Για TCP : 06 (HEX), για UDP : 11 (HEX)
- 3.4 Source Port, Destination Port, Checksum
- 3.5 8 bytes
- 3.6 Υπάρχει το πεδίο Length
- 3.7 Υπάρχει το πεδίο Header Length (1 byte) το οποίο είναι το 13ο byte από την αρχή της επικεφαλίδας
- 3.8 Όχι, δεν υπάρχει. Προκύπτει από το άθροισμα σε bytes του Header Length και του TCP Payload
- 3.9 Το Destination ή το Source Port μπορεί να αποκαλύπτει το τύπο πρωτοκόλλου εφαρμογής (πχ. η πόρτα 443 υποδηλώνει το HTTPS)
- 3.10 DNS, HTTP
- 4.1 Το UDP πρωτόκολλο
- 4.2 Το TCP πρωτόκολλο
- 4.3 Το πρώτο bit. 0 για ερώτηση και 1 για απάντηση
- 4.4 Destination port (DNS query) : 53
- 4.5 Source port (DNS query) : 59374
- 4.6 Source port (DNS response) : 53
- 4.7 Destination port (DNS response) : 59374
- 4.8 Η DNS ερώτηση με την DNS απάντηση "περνάνε" από την ίδια πόρτα
- 4.9 DNS Port : 53
- 4.10 Destination Port : 80
- 4.11 Source Port : 49451
- 4.12 Source Port : 80
- 4.13 Destination Port : 49451
- 4.14 HTTP Port : 80
- 4.15 Οι δύο πόρτες αυτές (source και destination) ταυτίζονται
- 4.16 GET /lab2/ HTTP/1.1
- 4.17 HTTP/1.1 200 OK (ο κωδικός είναι ο 200 ο οποίος συνεπάγεται απάντηση επιτυχής σύνδεσης με το web server)
- 4.18 Η εντολή ipconfig /flushdns χρειάζεται για το καθαρισμό της cache από DNS αρχεία, διότι αν έχουμε επισκευτεί ήδη τη σελίδα τα DNS requests θα απαντηθούν από τη cache και όχι από το DNS server.