Ονοματεπώνυμο: Χρήστος Τσούφης			**Ομάδα:** 2
Όνομα PC/ΛΣ: DESKTOP-EUMLCMA/Windows 10		**Ημερομηνία:**	13/10/2020
Διεύθυνση IP: 192.168.1.3	**Διεύθυνση MAC:**	34-F6-4B-07-39-B5	

Εργαστηριακή Άσκηση 2
Ενθυλάκωση και Επικεφαλίδες

1

1.1 Το φίλτρο απεικόνισης αποσκοπεί στην διατήρηση των πλαισίων τόσο του επιπέδου ζεύξης όσο και των υπολοίπων επιπέδων που ενθυλακώνονται σε αυτό το επίπεδο. Γνωρίζει δηλαδή, μόνο τα πλαίσια που μεταδίδονται με το πρωτόκολλο ARP ή IP.

1.2 Τα ονόματα των πεδίων της επικεφαλίδας του πλαισίου Ethernet είναι: Destination (6 bytes), Source (6 bytes), Type (2 bytes).

1.3 Δεν εντοπίζεται τέτοιο πεδίο.

1.4 Το μήκος των διευθύνσεων Ethernet είναι 6 bytes.

1.5 Το συνολικό μήκος της επικεφαλίδας Ethernet είναι 14 bytes.

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

1.7 Η θέση που καταλαμβάνει μέσα στην επικεφαλίδα Ethernet είναι τα bytes 12-13.

1.8 Για πακέτα IPv4: 0x0800

1.9 Για πακέτα ARP:0x0806

2

2.1 Το φίλτρο απεικόνισης αποσκοπεί στην απεικόνιση του πρωτοκόλλου ICMP καθώς, όπως είναι φανερό από το σχήμα αντιστοίχισης βασικών πρωτοκόλλων, δεν χρησιμοποιείται από τα πρωτόκολλα TCP, UDP, DNS, HTTP.

2.2 Το μήκος των διευθύνσεων IPv4 είναι 4 bytes

2.3 Τα ονόματα των πρώτων δύο πεδίων της επικεφαλίδας IPv4 είναι Version & Header Length.

2.4 Τα παραπάνω πεδία έχουν μήκος 4 bits το καθένα και μοιράζονται 1 byte (Header Length: 20, Version: 4).

2.5 Το συνολικό μήκος σε byte της επικεφαλίδας IPv4 είναι 20 bytes.

2.6 Το μήκος αυτό προκύπτει ως εξής: 5*32 bits = 160 bits = 20 bytes.

2.7 Το συνολικό μήκος είναι 60 bytes.

2.8 Το σχετικό πεδίο βρίσκεται στα 16-17 bytes γιατί περιέχουν πληροφορία για το μήκος του πακέτου και είναι 0x3c οπότε 60 bytes, όπως και στο ερωτ. 2.7 .

2.9 Το μήκος δεδομένων του πακέτου IPv4 είναι 40 bytes.

2.10 Το μήκος δεδομένων προκύπτει μέσω του τύπου: Μήκος δεδομένων = Συνολικό Μήκος – Μήκος Επικεφαλίδας.

2.11 Το πεδίο της επικεφαλίδας που καθορίζει το πρωτόκολλο στρώματος μεταφοράς της σουίτας TCP/IP είναι το ICMP (1).

2.12 Η θέση του είναι στο 9^{ο} byte της επικεφαλίδας IPv4.

2.13 Η τιμή είναι 01.

3

3.1 Το φίλτρο απεικόνισης αποσκοπεί στην διατήρηση τόσο των δεδομενογραμμάτων UDP και των τεμαχίων TCP του επιπέδου μεταφοράς, όσο και όλων των επιπέδων που ενθυλακώνουν αυτό το επίπεδο.

3.2 Τα πρωτόκολλα στρώματος μεταφοράς είναι: TCP & UDP.

3.3 Η τιμή του πεδίου Protocol στην IPv4 για το TCP είναι: TCP (6).

Η τιμή του πεδίου Protocol στην IPv4 για το UDP είναι: UDP (17).

3.4 Τα ονόματα είναι: Source Port, Destination Port, Checksum.

3.5 Το μήκος είναι 8 bytes.

3.6 Το πεδίο είναι το Length.

3.7 Το πεδίο είναι το Header Length και η θέση του είναι στο 12^{ο} byte της επικεφαλίδας.

3.8 Δεν υπάρχει πεδίο στην επικεφαλίδα για το συνολικό μήκος τεμαχίων TCP αλλά μπορεί να προκύψει από την πράξη: IP Total Length – IP Header Length.

3.9 Δεν υπάρχει πεδίο που να προσδιορίζει τον τύπο του πρωτοκόλλου εφαρμογής αλλά μπορεί να προκύψει από το port.

3.10 Τα πρωτόκολλα στρώματος εφαρμογής που παρατηρήθηκαν είναι: TLSv1.3, TLSv1.2, QUIC, NBNS, DNS, LLMNR.

4

4.1 Το DNS χρησιμοποιεί το πρωτόκολλο μεταφοράς UDP.

4.2 Το HTTP χρησιμοποιεί το πρωτόκολλο μεταφοράς TCP.

4.3 Το MSB bit του flag στην επικεφαλίδα DNS καθορίζει το κατά πόσον πρόκειται για ερώτηση (τιμή 0) ή απάντηση (τιμή 1).

4.4 Η θύρα προορισμού των ερωτήσεων DNS: Port 53.

4.5 Οι θύρες πηγής των ερωτήσεων DNS: Ports 52035, 56568, 58770, 60480, 61648.

4.6 Η θύρα πηγής των απαντήσεων DNS: Port 53.

4.7 Οι θύρες προορισμού των απαντήσεων του DNS: Ports 52035, 56568, 58770, 60480, 61648.

4.8 Οι θύρες προέλευσης των ερωτήσεων με τις θύρες προορισμού των απαντήσεων είναι ίδιες.

4.9 Η θύρα που ακούει ο εξυπηρετητής DNS: Port 53.

4.10 Η θύρα προορισμού των μηνυμάτων HTTP: Port 80.

4.11 Η θύρα πηγής των απαντήσεων HTTP του υπολογιστή: Ports 55552.

4.12 Η θύρα πηγής των αντίστοιχων απαντήσεων HTTP του εξυπηρετητή είναι: Port 80.

4.13 Η θύρα προορισμού των απαντήσεων HTTP: Port 55552.

4.14 Η θύρα που ακούει ο εξυπηρετητής HTTP είναι: Port 80.

4.15 Η θύρα πηγής των μηνυμάτων HTTP είναι ίδια με την θύρα προορισμού των αντίστοιχων απαντήσεων του εξυπηρετητή.

4.16 Η ονομασία του 1^{ου} μηνύματος είναι: GET /lab2/HTTP/1.1

4.17 Ο κωδικός απάντησης είναι 200 OK.

4.18 Χρειαζόταν η εκτέλεση αυτής της εντολής διότι αυτή διαγράφει την αντιστοίχιση ονόματος-DNS και χωρίς αυτήν δεν εμφανίζονται DNS μηνύματα αν έγινε επίσκεψη ξανά στην ιστοσελίδα.