Ονοματεπώνυμο: Πυλιώτης Αθανάσιος		**Ομάδα: 3**
Όνομα PC/ΛΣ: DESKTOP-5DLG3IF		**Ημερομηνία: 12/10/2022**
Διεύθυνση IP: 192.168.1.3	**Διεύθυνση MAC: 98-54-1b-bd-69-97**	

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 arp → Εμφανίζει τα πακέτα με επικεφαλίδες ARP (Address Resolution Protocol) μόνο. ip → διατηρεί τα πακέτα με επικεφαλίδες IP (Internet Protocol), με το or και τα δύο αυτά

1.2 Οι επικεφαλίδες που έχει είναι: Destination, Source, Type

1.3 Όχι δεν υπάρχει

1.4 Μήκος Διευθύνσεων Ethernet πακέτου σε bytes: 6 (Destination → 6 bytes, Source → 6 bytes)

1.5 Μήκος επικεφαλίδας Ethernet πακέτου σε bytes: 14 (6 + 6 + 2) (Destination → 6 bytes, Source → 6 bytes, Type → 2 bytes)

1.6 Το πρωτόκολλο δικτύου το καθορίζει το πεδίο Type

1.7 Το Type καταλαμβάνει τα τελευταία 2 bytes

1.8 Για πακέτα IPv4 θέλουμε HEX αναπαράσταση ανά byte, άρα: 0x0800

1.9 Για πακέτα IPv4 με πακέτα ARP η τιμή IPv4 είναι: 0x0806

2

2.1 Εμφανίζει όλα τα πακέτα με επικεφαλίδα ICMP (Internet Control Message Protocol)

2.2 Κάθε διεύθυνση IPv4 έχει μήκος 4 bytes

2.3 *Πρώτο πεδίο:* Version, *Δεύτερο πεδίο:* Μήκος Επικεφαλίδας (Header Length)

2.4 *Πρώτο πεδίο:* 4 bits, τιμή 4 (0100) , *Δεύτερο πεδίο:* 4 bits, τιμή 5 (0101)

2.5 Με βάση το παράθυρο περιεχομένων, το συνολικό μήκος τη επικεφαλίδας είναι: 20 bytes

2.6 Προκύπτει από το δεύτερο πεδίο της κεφαλίδας Header Length του IPv4, το οποίο έχει τιμή 5, η οποία αντιστοιχεί σε 20 bytes.

2.7 Με βάση τα δεδομένα καταγραφής, είναι Total Length: 60 bytes

2.8 Το μήκος πακέτου αναγράφεται και στην επικεφαλίδα IPv4 είναι 60 bytes συνολικά, και συμφωνεί με αυτό που βρήκαμε.

2.9 Το μήκος δεδομένων (data) σε bytes είναι ICMP Data + ICMP Header: 32 + 8 = 40 bytes

2.10 Από την επικεφαλίδα Internet Control Message Protocol, βρίσκουμε πως Data (32 bytes) στο πεδίο Data δηλαδή το γράφει δίπλα και προσθέτουμε σε αυτό και το μήκος σε bytes της επικεφαλίδας του ICMP.

2.11 Το πεδίο που λέει Protocol στο IPv4 πλαίσιο.

2.12 Είναι το 10ο bytes από την αρχή της επικεφαλίδας IPv4

2.13 Η τιμή για το πρωτόκολλο ICMP είναι 0x01

3

3.1 tcp → εμφανίζει πακέτα με επικεφαλίδες TCP, udp → εμφανίζει πακέτα με επικεφαλίδες UDP, με το or και τα δύο αυτά.

3.2 Τα πρωτόκολλα στρώματος μεταφοράς που παρατηρούμε είναι: TCP, UDP

3.3 Τιμή Protocol IPv4: TCP: 06 (HEX) , UDP: 11 (HEX)

3.4 Κοινά ονόματα πεδίων σε TCP και UDP: Destination port, Source port, Checksum

3.5 Η επικεφαλίδα του UDP είναι 8 bytes

3.6 Ναι υπάρχει και λέγεται length

3.7 Ναι λέγεται Header Length (20 bytes) στα TCP, είναι μετά το Acknowledgement number και πριν τα flags και το 13^{ο} byte από την αρχή της επικεφαλίδας.

3.8 Όχι δεν υπάρχει. Προκύπτει από το άθροισμα του Header Length και του Payload Length

3.9 Ναι. Είναι πιθανό το Destination Port ή το Source Port να δείχνει τον τύπο πρωτοκόλλου της εφαρμογής. Για παράδειγμα, 434 είναι το Mobile IP agents, 53 είναι DNS, 443 HTTPS

3.10 HTTP (80), DNS (53), HTTPS (443)

4

4.1 Χρησιμοποιεί το πρωτόκολλο μεταφοράς UDP, το οποίο φαίνεται στο Next Header.

4.2 Χρησιμοποιεί το πρωτόκολλο μεταφοράς TCP, το οποίο φαίνεται στο Protocol.

4.3 Το 17^{ο} bit από την αρχή ή το πρώτο bit της σημαίας (QR) το οποίο αν έχει τιμή 0 αντιστοιχεί σε query ενώ αν έχει τιμή 1 αντιστοιχεί σε response.

4.4 Question Destination Port: 53 (για όλες τις ερωτήσεις DNS)

4.5 Question Source Port: **56660**, 51416, 52829, 56382, 57342 (και άλλα πιθανότατα)

4.6 Response Source Port: 53 (για όλες τις απαντήσεις DNS)

4.7 Response Destination Port: **56660**, 51416, 52829, 56382, 57342 (και άλλα πιθανότατα)

4.8 Είναι αντίστοιχες. Κάνουμε στην αρχή μια ερώτηση στη θύρα 53 (DNS), η οποία πηγαίνει σε μία θύρα A να απαντηθεί, και μετά επιστρέφει από την θύρα A στην αρχική μας θύρα 53. Οι θύρες προέλευσης απαντήσεων ταυτίζονται με θύρες προορισμού ερωτήσεων και αντίστροφα.

4.9 Η θύρα αυτή είναι η 53

4.10 HTTP Destination Port: 80 (HTTP)

4.11 HTTP Source Port: 53285

4.12 HTTP Source Port: 80

4.13 HTTP Destination Port: 53285

4.14 Η θύρα αυτή είναι η 80

4.15 Είναι αντίστοιχες. Κάνουμε στην αρχή μια ερώτηση στη θύρα μας 53285, η οποία πηγαίνει στη θύρα 80 (HTTP) να απαντηθεί, και μετά επιστρέφει από την θύρα 80 (HTTP) στην αρχική μας θύρα 53285. Οι θύρες προέλευσης απαντήσεων ταυτίζονται με θύρες προορισμού ερωτήσεων και αντίστροφα.

4.16 Request Method: GET, φαίνεται στην πρώτη σειρά που γράφει GET /lab2/ HTTP/1.1

4.17 HTTP/1.1 200 OK , συνεπώς φόρτωσε κι όλα καλά

4.18 HTTP/1.1 304 Not Modified , άρα χρειάζεται διότι διαφορετικά είναι ήδη φορτωμένη στη

μνήμη και δεν επιτυγχάνεται το request, καθώς έχει ήδη φορτώσει η σελίδα και δεν υπάρχει καμία αλλαγή. Η ipconfic/flushdns χρειάζεται για να καθαρίσει τη DNS cache, καθώς αν την έχουμε επισκεφτεί απαντώνται από την cache και μας επιστρέφει μήνυμα πως δεν έχει αλλάξει κάτι.