Ονοματεπώνυμο: Μάρκος Δεληγιάννης		Ομάδα: 3
Όνομα PC/ΛΣ: DESKTOP-SCJFUE1 / W10		Ημερομηνία: 9 / 11 / 2022
Διεύθυνση IP: 147.102.131.8	Διεύθυνση MAC: 00-FF-EE-DE-8A-A1	

Εργαστηριακή Άσκηση 6
Πρωτόκολλο ICMP

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 "ether host 00-FF-EE-DE-8A-A1"

1.2 "arp or icmp"

1.3 Τα ARP πακέτα που ανταλλάχτηκαν είχαν ως σκοπό την εύρεση της διεύθυνσης MAC του υπολογιστή στον οποίο κάναμε ping (είναι στο ίδιο υποδίκτυο), ώστε να μπορέσουμε να του στείλουμε πακέτα.

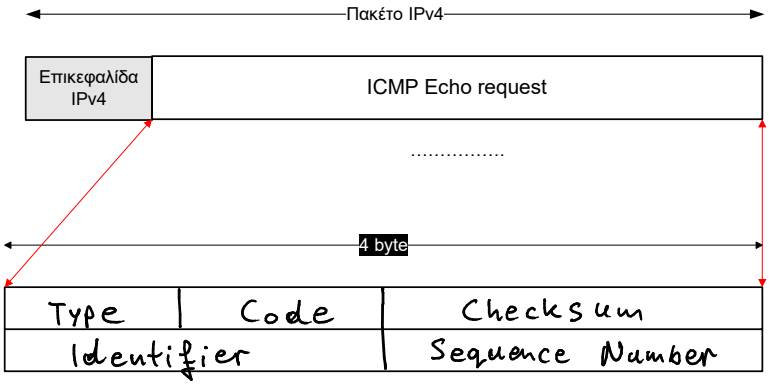
1.4 Το πεδίο Protocol με τιμή 0x01.

1.5 8 bytes

1.6 Type: 1 byte Code: 1 byte Checksum: 2 bytes
Identifier: 2 bytes Sequence Number: 2 bytes

.....

.....



1.7 Type = 0x08

Code = 0x00

1.8 Identifier = 0x0001

Sequence Number = 0x0002

1.9 Το μήκος των δεδομένων είναι 32 bytes. Τα δεδομένα είναι:
abcdefghijklmnopqrstuvwabcdefghi.

1.10 Η επικεφαλίδα έχει ίδιο μήκος (8 bytes) και δομή με την αντίστοιχη του ICMP Echo reply.

1.11 Type = 0x00 και Code = 0x00.

.....

1.12 Το πεδίο Type, το οποίο έχει διαφορετική τιμή στις δύο περιπτώσεις.

1.13 Identifier = 0x0001

Sequence Number = 0x0002

1.14 Identifier = 0x0001

Sequence Number = 0x0002 (ίδιες με το 1.13)

1.15 Το πεδίο ταυτότητας αντιστοιχεί σε μία εντολή ping και το sequence number αντιστοιχεί στον αριθμό σειράς του πακέτου στην ακολουθία. Τα αντίστοιχα πακέτα request και reply έχουν ίδια τιμή identifier και sequence number, οπότε αυτά τα δύο πεδία βοηθούν στην αντιστοίχησή τους.

1.16 Το μήκος των δεδομένων είναι 32 bytes. Τα δεδομένα είναι:
abcdefghijklmnopqrstuvwabcdefghi.

1.17 Τα δεδομένα είναι ακριβώς τα ίδια με την περίπτωση του ICMP Echo request.

1.18 Κάθε ζεύγος αντίστοιχων Echo request / reply αντιστοιχεί σε μία σειρά του ping στο terminal.

.....

1.19 ping -n 2 192.168.1.7 (Η άσκηση έγινε από VPN, εν προκειμένω αναφερόμαστε στο τοπικό μας δίκτυο)

1.20 Στάλθηκαν 3 πακέτα.

1.21 Κάθε περίπου 1 δευτερόλεπτο.

1.22 Δεν στέλνεται κανένα ICMP μήνυμα.

1.23 Στο παράθυρο εντολών αναφέρεται “Destination Host Unreachable”, το οποίο είναι λογικό, αφού δεν μπορέσαμε να εντοπίσουμε την MAC διεύθυνσή του ώστε να του στείλουμε πακέτα.

2

2.1 147.102.131.1, 224.0.0.22, 239.255.255.250

.....

.....

2.2 MAC αποστολέα: 00:ff:ee:de:8a:a1

MAC παραλήπτη: 00:ff:ef:de:8a:a1

2.3 IPv4 αποστολέα: 147.102.131.8

IPv4 παραλήπτη: 147.102.1.1

2.4 Η MAC αποστολέα φυσικά αντιστοιχεί στην 147.102.131.8, της κάρτας δικτύου του υπολογιστή μας. Η MAC παραλήπτη αντιστοιχεί βάσει του πίνακα ARP αντιστοιχεί στην 147.102.131.1, τον default gateway.

2.5 Δεν παρατηρήσαμε πακέτα ARP.

2.6 Ο λόγος είναι ότι η διεύθυνση που κάναμε ping είναι **εκτός** του τοπικού δικτύου, συνεπώς τα πακέτα δρομολογούνται μέσω του default gateway, του οποίου ήδη γνωρίζαμε την MAC διεύθυνση.

2.7 “icmp.type==0”

2.8 Στο παράθυρο εντολών και στο wireshark έχουμε TTL = 62. Η αποστολή πακέτων με TTL=64 είναι αρκετά συνηθισμένη, το οποίο υποδεικνύει απόσταση 3 από τον κόμβο-προορισμό. Πράγματι, η εκτέλεση tracert επιβεβαιώνει αυτό που παρατηρήσαμε.

2.9 Μόνο ICMP Echo (ping) request.

2.10 Τώρα έχουμε μόνο πακέτα ICMP, χωρίς ARP (ίδιος λόγος με το 2.6), και επιπλέον δεν λαμβάνουμε Echo reply. Αυτό είναι λογικό, διότι τώρα δεν χρειάζεται να ξέρουμε την MAC του προορισμού για να του στείλουμε πακέτα, οπότε αποστέλλονται αιτήματα, αλλά δεν λαμβάνεται απάντηση.

3

3.1 Το μήκος είναι 64 bytes και το περιεχόμενο είναι μόνο μηδενικά.

.....

3.2 Το μήκος είναι διπλάσιο στην περίπτωση της tracert και επιπλέον το περιεχόμενο είναι διαφορετικό.

.....

3.3 Time-to-live exceeded.

3.4 Type = 11 Code = 0

.....

3.5 Το checksum (2 bytes) και το Unused (4 bytes).

.....

.....

3.6 Μέγεθος επικεφαλίδας ICMP = 8 bytes.

Μέγεθος δεδομένων ICMP = 28 bytes.

3.7 Τα δεδομένα του ICMP μηνύματος λάθους είναι οι επικεφαλίδες IPv4 και ICMP του αντίστοιχου πακέτου που εστάλη από εμάς στον 147.102.40.15.

.....

4

4.1 Οι δοσμένες τιμές αντιστοιχούν στο μέγεθος του πακέτου IPv4. Η ping λαμβάνει ως όρισμα το μέγεθος δεδομένων του ICMP πακέτου. Συνεπώς αφαιρώντας 28 (IPv4 και ICMP επικεφαλίδες) έχουμε τιμες 1472, 1464, 978, 548, 524, 516, 484, 480, 268.

4.2 Στην δική μας καταγραφή δεν παρατηρήσαμε μήνυμα λάθους.

4.3 Στην δοσμένη καταγραφή ο κόμβος με IPv4 διεύθυνση 79.129.213.16.

4.4 Type = 3 Code = 4

.....

4.5 Το πεδίο Code, αφού η τιμή 4 σημαίνει ότι χρειάζεται θρυμματισμός.

MTU of next hop = 1492

4.6 Το πεδίο δεδομένων έχει τις επικεφαλίδες IPv4 και ICMP που αντιστοιχούν στο πακέτο που στείλαμε και απορρίφθηκε.

.....

4.7 MTU = 1492

4.8 Δεν λαμβάνουμε απάντηση για τιμές MTU = 1492 και 1006

4.9 MTU = 576

4.10 Η MTU αυτή ανήκει στην δικτυακή διεπαφή του 147.102.40.15, διότι για την αμέσως προηγούμενη τιμή που δοκιμάσαμε (1006) δεν λάβαμε πακέτο ICMP Destination unreachable. Οι ενδιάμεσοι κόμβοι όταν λαμβάνουν μηνύματα που δεν μπορούν να προωθήσουν στέλνουν πακέτο ICMP Destination unreachable, συνεπώς συμπεραίνουμε ότι τα πακέτα μας απορρίφθηκαν από τον κόμβο προορισμού, οπότε η MTU ανήκει στην 147.102.40.15.

4.11 Επειδή η διεπαφή αυτή είναι ο προορισμός των πακέτων, οπότε δεν ισχύει ότι ο προορισμός δεν βρέθηκε (Destination unreachable), αλλά ότι ο προορισμός δεν μπόρεσε να αποδεχθεί το πακέτο.

4.12 Το πρώτο θραύσμα που λαμβάνουμε έχει μέγεθος 572. Αυτό δεν είναι η MTU, αλλά η αμέσως μικρότερη τιμή που δίνει μέγεθος IPv4 payload πολλαπλάσιο του 8 (552). Αυτό συμβαίνει διότι το fragment offset μετρά κομμάτια 8 byte, οπότε για τη σωστή επανασυναρμολόγηση του πακέτου πρέπει το payload των θραυσμάτων να έχει μήκος πολλαπλάσιο του 8.

5

5.1 "host 147.102.40.15"

5.2 "nslookup edu-dy.cn.ntua.gr 147.102.40.15"

5.3 Λάβαμε απάντηση "DNS request timed out", το οποίο σημαίνει ότι ο DNS δεν μας απάντησε με την IPv4 διεύθυνση του edu-dy.cn.ntua.gr.

5.4 Ναι, τα μηνύματα που απέστειλε ο υπολογιστής μας.

5.5 Το πρωτόκολλο UDP με θύρα προορισμού 53.

5.6 Ναι

5.7 Type = 3 (Destination unreachable) Code = 3 (Port unreachable)

5.8 Το πεδίο Code.

5.9 Στα δεδομένα ICMP του πακέτου που λαμβάνουμε περιέχονται οι επικεφαλίδες IPv4 και UDP του πακέτου που αντιστοιχεί στο σφάλμα. Στην επικεφαλίδα UDP περιέχεται η πληροφορία για τη θύρα προορισμού (53), η οποία αντιστοιχεί πάντα στα μηνύματα DNS.

5.10 Ο υπολογιστής μας έχει windows.

6

6.1 ping 2001:648:2000:329::101

tracert 2001:648:2000:329::101

6.2 Φίλτρο σύλληψης: "ip6"

Φίλτρο απεικόνισης: "icmpv6"

6.3 Type = 0x86dd (IPv6).

6.4 40 bytes.

6.5 1) Version (4 bits)

2) Traffic Class (8 bits)

3) Flow label (20 bits)

4) Payload length (2 bytes)

5) Next header (1 byte)

6) Hop limit (1 byte)

7) Source address (16 bytes)

8) Destination address (16 bytes) (βλ. σχήμα)

6.6 Το πεδίο Hop limit.

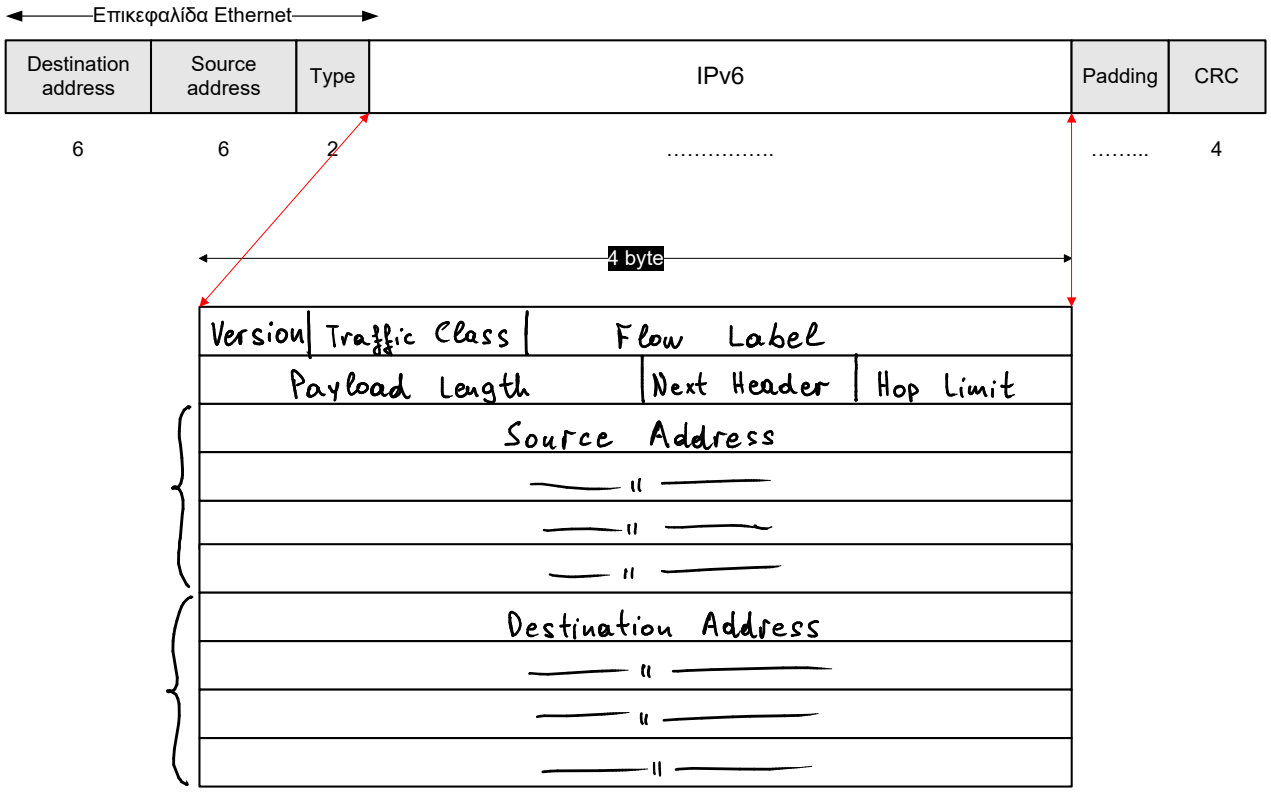
6.7 Το πεδίο Next Header με τιμή 58 (ICMPv6).

6.8 Η δομή της επικεφαλίδας είναι ίδια με αυτή του ICMPv4.

6.9 Type = 128 (Echo (ping) request)

Μήκος δεδομένων = 32 bytes.

6.10 Η δομή της επικεφαλίδας είναι πράγματι ίδια.



6.11 Type = 129 και μήκος δεδομένων = 64 bytes.

.....

6.12 Το hop limit έχει μικρή τιμή (π.χ. 1 ή 2 αντί για 128), ώστε να ελεγχθεί η εγγύτητα του προορισμού.

6.13 Η μόνη διαφορά είναι ότι το ICMPv6 έχει ένα επιπλέον πεδίο “Length of original datagram” (1 byte).

6.14 Type = 3 και μήκος δεδομένων = 112 bytes.

.....

6.15 Το πεδίο δεδομένων του περιέχει ολόκληρο το πακέτο IPv6 που προκάλεσε το error (112 bytes).

6.16 Ναι, παρατηρούνται και ICMPv6 μηνύματα Neighbor Soliciation και Neighbor Advertisement.

.....

6.17 Neighbor Soliciation: Type = 135 Μήκος μηνυμάτων = 32 bytes.
Neighbor Advertisment: Type = 136 Μήκος μηνυμάτων = 32 bytes.