Ονοματεπώνυμο: Πυλιώτης Αθανάσιος		**Ομάδα: 3**
Όνομα PC/ΛΣ: DESKTOP-5DLG3IF		**Ημερομηνία: 27/10/2022**
Διεύθυνση IP: 192.168.1.7	**Διεύθυνση MAC:**	**98-54-1B-BD-69-97**

Εργαστηριακή Άσκηση 4
Πρωτόκολλο IPv4 και θρυμματισμός

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 ping www.mit.edu -n 3 -4

1.2 Κάνει capture μόνο unicast και πρακτικά ξεφορτώνεται τον θόρυβο στο δίκτυο. Είναι βολικό αν θες να δεις κίνηση μόνο από και προς τη συσκευή σου.

1.3

```
PS C:\Users\thana> ping www.mit.edu -n 3 -4

Pinging e9566.dscb.akamaiedge.net [92.123.12.49] with 32 bytes of data:
Reply from 92.123.12.49: bytes=32 time=33ms TTL=58
Reply from 92.123.12.49: bytes=32 time=34ms TTL=58
Reply from 92.123.12.49: bytes=32 time=33ms TTL=58

Ping statistics for 92.123.12.49:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 33ms, Maximum = 34ms, Average = 33ms
```

1.4 RTT για πρώτο πακέτο: 33ms

Για δεύτερο πακέτο: 34ms

Για τρίτο πακέτο: 33ms

1.5 RTT για πρώτο πακέτο: 0.033409

Για δεύτερο πακέτο: 0.034540

Για τρίτο πακέτο: 0.033432

Είναι σωστοί χρόνοι κατά προσέγγιση, άρα συμφωνούν.

1.6 ip

1.7 icmp.type == 8 or icmp.type == 0 (8 for request, 0 for reply)

1.8 Requests ICMP. Type: 8

1.9 Destination: 192.168.1.7, Source: 92.123.12.49

1.10 Replies ICMP type 0

1.11 Source: 192.168.1.7, Destination: 92.123.12.49

1.12 Η διεύθυνση του www.mit.edu έχει αλλάξει σε 92.123.12.49 από αυτή που ήταν παλιά. Επίσης, άλλαξε η επίσημη ονομασία πίσω από το δίκτυο e9566.dscb.akamaiedge.net .

2

2.1 ping 192.168.1.1 -n 5 -4 ; ping 192.168.1.7 -n 5 -4 ; ping 127.0.0.1 -n 5 -4

ping <address> -n 5 -4

2.2 5 πακέτα (αυτά που στάλθηκαν στο default gateway)

2.3 192.168.1.1 , άρα το default gateway.

2.4 Όχι δεν παρατήρησα. Τα ICMP περνάνε από τον οδηγό loopback (αφού είναι τοπική διεύθυνση IPv4) και δεν βγαίνουν ποτέ στο τοπικό δίκτυο, άρα δεν ανιχνεύονται από το wireshark.

2.5 Όχι δεν παρατήρησα. Τα ICMP οδηγούνται και αυτά στον οδηγό Loopback, άρα πάλι δεν περνάνε από το τοπικό δίκτυο και δεν περνούν στην ουρά εισόδου IPv4 για να τα καταγράψει το Wireshark.

2.6 Στο δικό μας 192.168.1.7 το πακέτο εισέρχεται στον οδηγό ethernet και μετά αποστέλλεται στον οδηγό Loopback επειδή είναι τοπική διεύθυνση IPv4. Στο 127.0.0.1 πηγαίνει απευθείας στον οδηγό Loopback και στην ουρά εισόδου IPv4

2.7 Όταν κάνω ping www.netflix.com δεν έχω πακέτα replies ενώ στο www.amazon.com έχω. Πιθανότατα το Netflix (ή κάποιος ενδιάμεσος) έχει ενεργοποιήσει firewalls και μπλοκάρουν τα ICMP πακέτα.

3

3.1 host 147.102.40.15

3.2 ip.src == 192.168.1.7

3.3

Internet Protocol Version 4, Src: 192.168.1.7, Dst: 147.102.40.15

Version (4 bits)

Header Length (4 bits)

Differentiated Services Field (1 byte)

Total Length (2 bytes)

Identification (2 bytes)

Flags(1 byte)

Fragment Offset (1 byte)

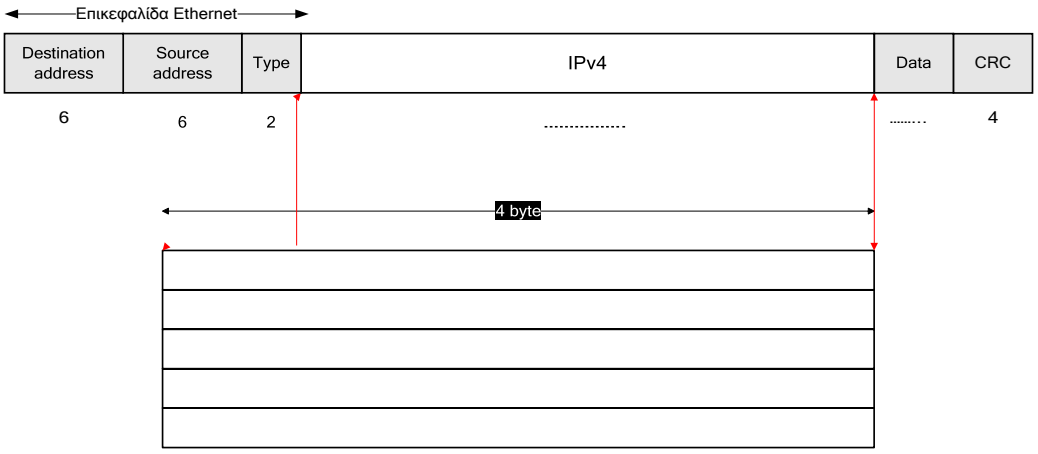
Time to Live (1 byte)

Protocol (1 byte)

Header Checksum (2 bytes)

Source Address (4 bytes)

Destination Address (4 bytes)



3.4 Total Length και Identification και header checksum

3.5 Ναι είναι 20 bytes

3.6 Μικρότερο: 40 bytes , Μεγαλύτερο: 66 bytes

3.7 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

00 (HEX) → CS0: Standard service class και b8 (HEX) → EF PHB: Telephony Service Class

3.8 Παρατηρώ πως οι τιμές αλλάζουν κατά 1 HEX κάθε φορά, από το ένα πακέτο IPv4 στο επόμενο, άρα αυξάνονται με μετρητή.

3.9 1

3.10 0

3.11 6 και αντιστοιχεί στο TCP

3.12 Αντιστοιχεί στο άθροισμα των λέξεων που περιέχονται στο IPv4 Header και, αφού αλλάζουν τα περιεχόμενα του Header, αλλάζει και αυτό.

4 → 147.102.38.89 για αυτό (έγινε σε PC της σχολής)

4.1 ping <destination IP> -f -l <Packet Size>

-f → don't fragment , -l → determine packet size

4.2 1472 bytes είναι η μέγιστη τιμή που μπορεί να στείλει unfragmented

4.3 1473 bytes είναι η ελάχιστη τιμή που πρέπει να γίνει fragmented

4.4 not broadcast and not multicast

4.5 ip.addr == 147.102.38.90

4.6 Όχι δεν παράγονται (αναγράφει και στο command πως χάθηκαν τα πακέτα)

4.7 Το μέγεθος MTU IP της διεπαφής μας είναι 1500 bytes. Το βρίσκουμε από το συνολικό μέγεθος data του ICMP μαζί με τα headers, δηλαδή 1472 + 8 + 20 bytes.

4.8 Η μέγιστη τιμή δεδομένων ICMP είναι 65500 bytes γενικά, εκτός του τοπικού δικτύου και αυτή οδηγεί σε μέγιστο πακέτο IPv4.

4.9 Όχι, καθώς στο τοπικό μας δίκτυο η μέγιστη τιμή για την οποία αυτό γίνεται επιτυχές είναι η 1472 bytes, που καταλήγει σε μέγιστο πακέτο IPv4 1500 bytes.

4.10 1500 bytes, όπως αναφέρθηκε και παραπάνω.

4.11 Όχι, έχει μεταφερθεί ως πακέτα μεγέθους 1480 bytes, 4 από αυτά συγκεκριμένα.

4.12 Χρειάστηκαν 4 πακέτα με δεδομένα μεγέθους 1480 bytes, επειδή μερικά από τα bytes δεδομένων που ζητήσαμε πιθανώς μεταφέρθηκαν με το reply στο τέλος (το οποίο στέλνεται ως τελικό πακέτο με όσα περισσεύουν πιθανότατα)

4.13

	Identification	Flags	Fragment offset
1	0x0350	0x01 (more fragments)	0
2	0x0350	0x01 (more fragments)	1480
3	0x0350	0x01 (more fragments)	2960
4	0x0350	0x01 (more fragments)	4440
5	0x0350	0x00 (no more fragments)	5920

Τελευταίο bit των flags: More Fragments. (1 σε όλα εκτός το τελευταίο)

Προτελευταίο bit: Don’t Fragment (πάντα 0)

4.14 Flags ή identification

4.15 Fragment Offset 0 (πρακτικά είναι ακόμα στην αρχή των δεδομένων)

4.16 Συνολικά είναι 1514 bytes, εκ των οποίων 14 είναι ethernet header, 20 IPv4 header και 1480 δεδομένα.

4.17 Fragment Offset 1480 (άρα είναι τα αμέσως επόμενα bytes)

4.18 Ναι

4.19 Από τα flags, γιατί το More Fragments είναι 1 και το flags κομμάτι 0x01 (more flags)

4.20 Fragment Offset και Header Checksum

4.21 Στο προτελευταίο είναι 4440 bytes καθώς έχουν προηγηθεί 3 πακέτα των 1480 bytes και το τελευταίο 5920 bytes καθώς έχουν έρθει τα 4 θραύσματα του πακέτου πρώτα και αυτό είναι το τελευταίο.

4.22 Στα 4 πρώτα μόνο τα Fragment Offset και Header Checksum, στο τελευταίο αλλάζουν αυτά και τα Flags και το total length, καθώς είναι μικρότερο.