Ονοματεπώνυμο: Χαράλαμπος Καμπουγέρης **Ομάδα:** 3, Τετάρτη 10:45-12:30, Αιθ.Α2

Όνομα PC/ΛΣ: CHARALAMPOSs-MacBook-Air/ macOS 14.0 **Ημερομηνία:** 31/10/2023

Διεύθυνση IP: 147.102.238.19(από ΕΜΠ) και 192.168.1.16(από οικιακό δίκτυο) **Διεύθυνση MAC:** 0c:e4:41:e1:6c:74

Εργαστηριακή Άσκηση 4
Πρωτόκολλο IPv4 και θρυμματισμός

Άσκηση 1

1.1 ping -c 3 www.mit.edu

1.2 0% loss, Average delay: 32ms

1.3 round-trip min/avg/max/stddev = 29.350/32.716/37.058/3.222 ms

1.4 Παρατηρούμε ότι έχει αλλάξει το όνομα εξυπηρετητή (e9566.dscb.akamaiedge.net) καθώς και η διεύθυνση ip (104.96.133.24). Επίσης παρατηρούμε διαφορετική τιμή TTL (ttl = 56) καθώς επίσης και γρηγορότερες ταχύτητες(μικρότεροι χρόνοι RRT)

1.5 Με αυτό το φίλτρο δε βλέπουμε κίνηση δικτύου broadcast και multicast, αλλά καταγράφεται μόνο η unicast κίνηση του δικτύου (δηλαδή μόνο μηνύματα από και προς τον υπολογιστή μας)

1.6 Το φίλτρο ip

1.7 Το φίλτρο icmp and ip.addr == 147.102.238.19

1.8 Type: 8 (Echo (ping) request)

1.9 Source Address: 147.102.238.19, Destination Address: 104.96.133.24

1.10 Type: 0 (Echo (ping) reply)

1.11 Source Address: 104.96.133.24, Destination Address: 147.102.238.19

1.12 Echo 1 RTT: [Response time: 31.238 ms]
Echo 2 RTT: [Response time: 38.409 ms]
Echo 3 RTT: [Response time: 29.493 ms]
Ναι συμφωνούν με τις αντίστοιχες στο παράθυρο εντολών.

Άσκηση 2

2.1 ping -c 5 192.168.1.1

2.2 Μόνο 5 μηνύματα έχουν καταγραφεί

2.3 Ο προορισμός τους είναι το default gateway δηλαδή η διεύθυνση 192.168.1.1

2.4 Όχι, δεν παρατήρησα επειδή αυτά τα πακέτα ICMP περνάνε από τον οδηγό loopback και δεν βγαίνουν ποτέ στο τοπικό δίκτυο. Έτσι το Wireshark δεν τα εντοπίζει.

2.5 Όχι, δεν παρατήρησα επειδή και αυτά τα πακέτα ICMP περνάνε από τον οδηγό loopback και δεν βγαίνουν στο τοπικό δίκτυο.

2.6 Η διαφορά είναι ότι όταν στέλνω request στον εαυτό μου, αυτό περνά από τον Ethernet driver όπου και ανακατευθύνεται στον οδηγό loopback. Αντίθετα όταν στέλνω μήνυμα στη διεύθυνση του loopback αυτό πάει κατευθείαν στον οδηγό loopback ο οποίος το στέλνει στην είσοδο πακέτων.

2.7 Όταν κάνω ping το www.netflix.com δεν υπάρχουν ping replies σε αντίθεση με το www.amazon.com και το πιθανότερο είναι ότι το Netflix (ή κάποιος ενδιάμεσος κόμβος) έχει ενεργοποιήσει κάποιο firewall που μπλοκάρει τα ICMP πακέτα.

Άσκηση 3

3.1 host 147.102.40.15

3.2 ip.src == 192.168.1.16

3.3
Version: 1 byte
Header Length: 1 byte
Differentiated Service Field: 1 byte
Total Length: 2 bytes
Identification: 2 bytes
Flags: 1 byte
Fragment Offset: 2 bytes
Time to Live: 1 byte
Protocol: 1 byte
Header Checksum: 2 bytes
Source Address: 4 bytes
Destination Address: 4 bytes

3.4 Αλλάζουν τιμές τα πεδία “Differentiated Service Field”, “Total Length”, “Header Checksum”

3.5 Ναι, είναι 20 bytes

3.6 Το μικρότερο είναι 66 bytes και το μεγαλύτερο είναι 134 bytes.

3.7 Το Differentiated Services Field παίρνει τιμές 0, 8 και 10 (HEX) οι οποίες αντιστοιχούν σε Standard, Low-Priority data και High-throughput data αντίστοιχα, οι οποίες είναι ποιότητες υπηρεσιών.

3.8 Το identification έχει παντού τιμή 0

3.9 Παντού τιμή 1

3.10 Παντού τιμή 0

3.11 Έχει τιμή 6 και αντιστοιχεί στο πρωτόκολλο TCP

3.12 Το Header Checksum προκύπτει από τα bytes του κάθε πακέτου IPv4. Δεδομένου ότι σε κάθε πακέτο αλλάζουν κάποια bytes, είναι λογικό να αλλάζει και η τιμή του Header Checksum.

Άσκηση 4

4.1 ping -o -D -s <packet size> <destination address>
(Σε windows: ping -n 1 -f -l <size> <destination address>)

4.2 Με δοκιμές βρίσκω ότι η μέγιστη τιμή είναι 1472 bytes

4.3 Η ελάχιστη τιμή για την οποία απαιτείται θρυμματισμός είναι τα 1473 bytes

4.4 Capture filter: not broadcast not unicast

4.5 Display filter: ip.addr == 147.102.224.52

4.6 Όχι, δεν παράγονται, διότι το πακέτο που πάει να μεταδοθεί ξεπερνάει το μήκος της MTU και δε μεταδίδεται.

4.7 Το Wireshark κατέγραψε ότι το μέγεθος του Ethernet frame που στάλθηκε όταν κάναμε το echo request ήταν 1514 bytes. Από αυτά, τα 14 bytes αποτελούν το Ethernet Header, οπότε το MTU έχει μέγεθος 1500 bytes (Το FCS δεν καταγράφεται από το Wireshark).

4.8 Από την επικεφαλίδα ICMP και πεδίο Data προκύπτει ότι το maximum Length είναι 1472 bytes

4.9 Ναι για μήκος πακέτου 1472 και χωρίς την παράμετρο -D επιτυχγάνεται το ping

4.10 Το μεγαλύτερο πακέτο IPv4 (επικεφαλίδες Ethernet II, IPv4, ICMP) έχει μήκος 1514 bytes

4.11 Όχι, έχει σπάσει πολλά μικρότερα πακέτα

4.12 Χρειάστηκαν 5 πακέτα. Το μέγιστο πακέτο που στέλνεται χωρίς θρυμματισμό είναι

1472 bytes. Κάθε πλαίσιο από τα πρώτα 4 έχει συνολικό μέγεθος 1514 bytes, όπου 14 bytes είναι το Ethernet header, 20 bytes είναι το IP header και 1480 είναι το ICMP πακέτο. Το τελευταίο πλαίσιο έχει μέγεθος 122 bytes, από τα οποία πάλι 14 αντιστοιχούν στο Ethernet header και 20 στο IP header. Επιπλέον, 8 bytes αντιστοιχούν στο ICMP header, άρα μένουν 80 bytes. Συνεπώς, 4 · 1480 + 80 = 6000 bytes.

4.13

Θραύσματα	Identification	Don't Fragment Bit	More Fragments Bit	Fragment Offset
1ο	0x2826	0	1	0
2ο	0x2826	0	1	1480
3ο	0x2826	0	1	2960
4ο	0x2826	0	1	4440
5ο	0x2826	0	0	5920

4.14 Το πεδίο More Fragments Bit που έχει τιμή 1

4.15 Το Fragment Offset που έχει τιμή 0

4.16 Το συνολικό μήκος του θραύσματος είναι 1514 bytes.

4.17 Το Fragment Offset είναι μη μηδενικό (1480)

4.18 Ναι ακολουθούν και άλλα θραύσματα και το καταλαβαίνουμε από το πεδίο More Fragments Bit που έχει τιμή 1

4.19 Αλλάζουν τα πεδία Fragment Offset και More Fragments Bit και το Total Length. Το πεδίο More Fragments Bit διαφέρει μόνο όταν το ένα θραύσμα είναι το τελευταίο, όπου και θα έχει τιμή 0

4.20 Τα πεδία που δεν αλλάζουν είναι το Identification και Don't Fragment Bit

4.21 Το μήκος των θραυσμάτων (ICMP πακέτο) εκτός του τελευταίου είναι 1480 bytes. Παρατηρούμε ότι η τιμή του πεδίου Fragment Offset ισούται με την αντίστοιχη τιμή του προηγούμενου πακέτου προσθέτοντας 1480 και ξεκινώντας από το πρώτο που έχει τιμή 0.

4.22 Το τελευταίο πακέτο έχει μήκος 122bytes. Αυτό προκύπτει καθώς στείλαμε πακέτο 6000 bytes το οποίο θρυμματίστηκε σε 4 πακέτα συνολικού μήκους 1514 bytes, εκ των οποίων τα 1480 είναι το ICMP πακέτο. Οπότε για το τελευταίο πακέτο ισχύει 6000 - 4*1480 = 80 bytes ICMP πακέτο. Προσθέτοντας Ethernet header 14 bytes, IP header 20 bytes και ICMP header 8 bytes προκύπτει μήκος 122 bytes.