Όνοματεπώνυμο: Ναυσικά Αμπατζή		Ομάδα: 2
Όνομα PC/ΛΣ: Dell XPS 15-7590 Windows		Ημερομηνία: 27 /10 /2020
Διεύθυνση IP: 192.168 .1.4	Διεύθυνση MAC:24-41-8C-65-26-BF	

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 -n 3 -4 www.mit.edu (το -n 3 προδιορίζει τον αριθμό των πακέτων και το -4 το ότι θα είναι IPV4)

1.2 Το φίλτρο not multicast and not broadcast χρησιμοποιείται ώστε να καταγράψουμε μόνο unicast κίνηση και να μην υπάρχει ο θόρυβος του δικτύου. Έτσι θα έχουμε μόνο πακέτα με προορισμό ή αποστολέα τον υπολογιστή μας.

1.3 Ποσοστό απωλειών πακέτων = 0% και μέση καθυστέρηση = 280ms

1.4
```
Reply from 184.51.176.128: bytes=32 time=277ms TTL=53
Reply from 184.51.176.128: bytes=32 time=283ms TTL=53
Reply from 184.51.176.128: bytes=32 time=282ms TTL=53
```

1.5 Σύμφωνα με το wireshark οι RTT είναι : RTT_1 = 0.277406 s =277.406 ms, RTT_2 = 0.283368= 283.368 ms, RTT_3 = 0.282525 s =282.525 ms

Παρατηρώ ότι οι τιμές αυτές διαφέρουν λίγο από αυτές που κατέγραψα από το cmd(max απόκλιση 0.5 ms περίπου)

1.6 Για να παρατηρώ μόνο IPV4 πακέτα θα χρησιμοποιήσω το φίλτρο απεικόνησης : ip

1.7 Για να παρατηρώ μόνο μόνο την κίνηση ICMP που προκάλεσε η εντολή ping : icmp

1.8 Από τον υπολογιστή μου (IPV4 = 192.168.1.4) στάλθηκαν μηνύματα με Type = 8, άρα Echo Requests.

1.9 Διεύθυνση πηγής: 192.168.1.4 και διεύθυνση προορισμού: 184.51.176.128

1.10 Από τον υπολογιστή μου (IPV4 = 192.168.1.4) ελήφθησαν μηνύματα με Type = 0, άρα Echo Replies.

1.11 Διεύθυνση πηγής: 184.51.176.128 και διεύθυνση προορισμού: 192.168.1.4

1.12 Στην τωρινή καταγραφή έχουν σταλεί 3 αντί για 4 πακέτα και γι'αυτό τον λόγο η μέση καθυστέρηση είναι μικρότερη σε σχέση με την καταγραφή του παρελθόντος.

2

2.1 Χρησιμοποίησα τις εξής 3 εντολές : ping -n 5 198.165.1.1, ping -n 5 198.165.1.4, ping -n 5 127.0.0.1

2.2 Έχουν καταγραφεί 5 μηνύματα ICMP Echo request από το Wireshark.

2.3 Ο προορισμός τους ήταν η διεύθυνση της προκαθορισμένης πύλης του υπολογιστή μου(198.164.1.1).

2.4 Όχι δεν παρατήρησα, καθώς η αποστολή γίνεται σε τοπική μου διεύθυνση πριν πάει στον loopback driver οπότε δεν δημιουργούνται πλαίσια ώστε να καταγραφούν από το Wireshark.

2.5 Όχι δεν παρατήρησα, καθώς τα μηνύματα αυτά στέλνονται στον Loopback Driver και όχι στον Ethernet Driver ώστε να δημιουργούνται πλαίσια και να καταγράφονται από το Wireshark.

2.6 Στο Ping στη διεύθυνση loopback τα μηνύματα, όπως φαίνεται και στο σχήμα που δίνεται, στέλνονται στον loopback driver και όχι στον Ethernet σε αντίθεση με αυτά της διεπαφής του υπολογιστή.

2.7 Στο Ping για την ιστοσελίδα του Netflix το αποτέλεσμα είναι Request timed out και για τα 4 πακέτα. Έτσι έχουμε 100% απώλειες. Από την άλλη το ping στην δεύτερη ιστοσελίδα (amazon) είχε 100% επιτυχία, καθώς στάλθηκαν και λήφθηκαν και τα 4 πακέτα. Η διαφορά αυτή οφείλεται στο ότι το ping δημιουργεί ICMP πακέτα, ενώ ο browser δημιουργεί http κίνηση. Έτσι η αποτυχία της μίας προσπάθειας οφείλεται στην ύπαρξη κάποιου firewall που δεν επιτρέπει να επισκεφτούμε την ιστοσελίδα μέσω ping, να στείλουμε δηλαδή ICMP πακέτα.

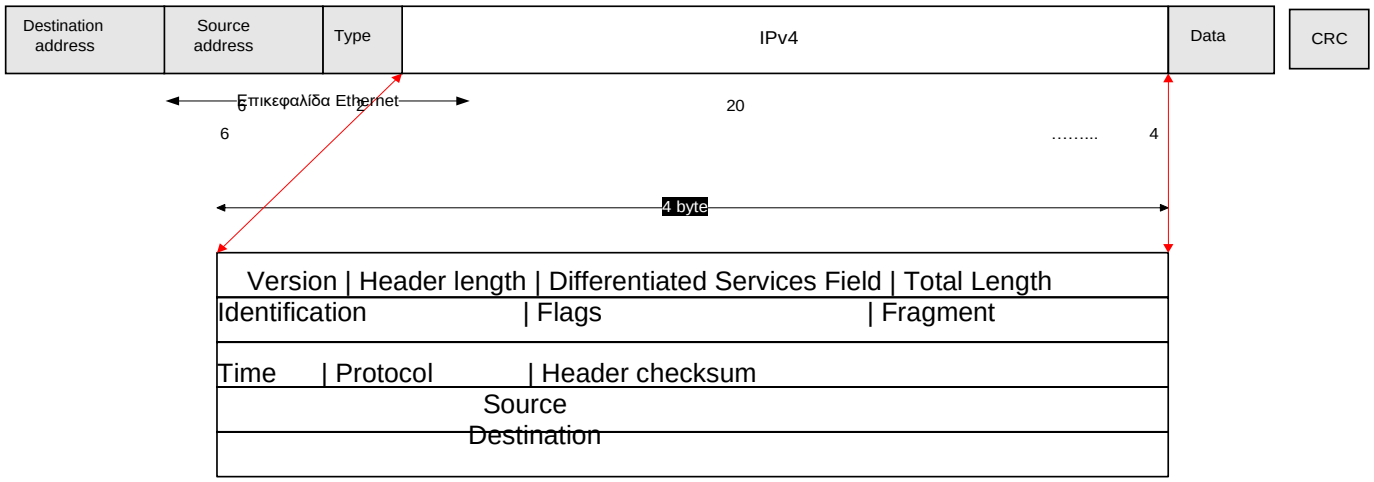
3

3.1 host 192.168.1.4

3.2 ip.src_host == 192.168.1.4

3.3 Version(4 bits) , Header length(4 bits), Differentiated Services Field(8 bits), Total Length(8 bits)

Identification(16 bits), Flags (8 bits), Fragment(8 bits), Time(8 bits), Protocol(8 bits), Header checksum(16 bits), Source(32 bits), Destination(32 bits)



3.4 Αλλάζουν τιμή τα πεδία : Differentiated Services Field, Total Length και Identification

3.5 Το μήκος της επικεφαλίδας IPV4 παραμένει το ίδιο σε όλα τα πακέτα.

3.6 max Total Length = 66 byte και min Total Length = 40 byte

3.7 Στο πεδίο Differentiated Services Field παρατηρούνται οι τιμές : 00(hex) ή 00000000(bin) και

b8(hex) ή 10111000(bin). Η αναμενόμενη τιμή και αυτή που παρατηρείται σχεδόν σε όλα τα Differentiated Services είναι η μηδενική και αντιστοιχεί σε Default Forwarding. Για την τιμή 10111000 υποθέτουμε ότι οφείλεται σε κάποια τριμελή χειραψία αν και δεν ήταν αναμενόμενη. Αντιστοιχεί σύμφωνα με το Wikipedia σε Expedited Forwarding.

3.8 Στο πεδίο Identification οι τιμές ξεκινάνε από 6702(hex) ή 26370 και αυξάνονται με την ίδια σειρά που αυξάνεται και ο αριθμός των πακέτων φτάνοντας μέχρι την τιμή 6732(hex) ή 26418.

3.9 Η σημαία Don’t fragment έχει τιμή 1-Set

3.10 Το πεδίο Fragment Offset έχει τιμή 0

3.11 Το πεδίο Protocol έχει τιμή 6 και ανήκει στο πρωτόλλο TCP.

3.12 Επειδή υπάρχουν πεδία που αλλάζουν κατά τη διέλευση των datagrams από τις διάφορες συσκευές του δικτύου, το header checksum επαναπροσδιορίζεται σε κάθε κόμβο του δικτύου.

4

4.1 ping [IPV4 address] -n 1 -4 -f (Χρησιμοποιώ την 192.168.1.5)

4.2 Η μέγιστη τιμή για την οποία επιτυγχάνει η αποστολή = 1472 byte

4.3 Η μικρότερη τιμή για την οποία απαιτείται θρυμματισμός = 1473 byte

4.4 Φίλτρο Σύλληψης ώστε να έχουμε μόνο unicast : not broadcast and not multicast

4.5 Φίλτρο Απεικόνισης : ip.addr == 192.168.1.5

4.6 Όχι δεν παράγονται πακέτα IPV4 όταν χρησιμοποιώ το μήκος 1473 bytes, καθώς σε αυτή την τιμή απαιτείται θρυμματισμός αφού ξεπερνιέται το μέγιστο επιτρεπτό μήκος πακέτου.

4.7 Από το ερώτημα 4.2 γνωρίζουμε ότι η μέγιστη τιμή για την οποία επιτυγχάνει η αποστολή είναι τα 1472 byte. Προσθέτοντας σε αυτή την τιμή 20 byte για το IP header και 8 byte για το ICMP Echo Request Header, προκύπτει η MTU τιμή (1500 byte).

4.8 Η τιμή 65.507 bytes. Αυτό προκύπτει καθώς το μέγιστο μέγεθος πακέτου IPV4 είναι 65535 bytes και αφαιρώντας την Ethernet Header, την IPV4 Header και το CRC προκύπτει η παραπάνω τιμή.

4.9 Όχι, το ping δεν επιτυγχάνει. Το μέγιστο επιτρεπτό μέγεθος είναι 65.500 bytes.

4.10 Το μεγαλύτερο πακέτο IPV4 που μπορεί να παραγάγει η εντολή ping στα Windows10 είναι 65.500 byte. Ωστόσο το πραγματικό max ip μέγεθος(τα Linux το επιτρέπουν) είναι 65.535 και αφαιρώντας 20 bytes(ip header) και 8 Bytes(icmp/ping header) προκύπτει 65.507 bytes.

4.11 Όχι δεν έχει μεταφερθεί ως πακέτο IPV4 και αυτό προκύπτει έμμεσα από την κόκκινη επισήμανση στο πεδίο IPV4.

4.12 Χρειάστηκαν 5 πακέτα συνολικά. Αυτό διότι το μέγιστο IPV4 μήκος πακέτου είναι 1500 bytes. Το συνολικό μήκος του μηνύματος είναι 6.108 Bytes και έτσι χρειαζόμαστε 5 πακέτα.

Και 7 στο Ethernet LAN και έτσι θα «σπάσει» σε 6000/1500 = 4 IPV4 πακέτα. Το 5^{ο} πακέτο έχει total length 108 bytes και

4.13

1$_{ο}$ Πακέτο : Identification = 0xcf24(53028) , Don’t Fragment Bit = 0 , More Fragments Bit = 1, Fragment Offset = 0

2$_{ο}$ Πακέτο : Identification = 0xcf24(53028) , Don’t Fragment Bit = 0 , More Fragments Bit = 1, Fragment Offset = 1480

3$_{ο}$ Πακέτο : Identification = 0xcf24(53028) , Don’t Fragment Bit = 0 , More Fragments Bit = 1, Fragment Offset = 2960

4$_{ο}$ Πακέτο : Identification = 0xcf24(53028) , Don’t Fragment Bit = 0 , More Fragments Bit = 1, Fragment Offset = 4440

5$_{ο}$ Πακέτο : Identification = 0xcf24(53028) , Don’t Fragment Bit = 0 , More Fragments Bit = 0, Fragment Offset = 5920

4.14 Το πεδίο της επικεφαλίδας που δείχνει ότι το πακέτο IPV4 έχει θρυμματιστεί είναι το flags, όπου υπάρχει η αναφορά: More Fragments

4.15 Η πληροφορία της επικεφαλίδας IPv4 που δηλώνει ότι αυτό είναι το πρώτο θραύσμα και όχι ένα μεταγενέστερο είναι η τιμή του Fragment Offset, η οποία είναι 0 για το πρώτο θραύσμα.

4.16 Το μήκος του είναι 1472 Byte.

4.17 Εάν κοιτάξουμε το Fragment Offset θα δούμε ότι η τιμή του είναι διάφορη του μηδενός(1480). Έτσι προκύπτει ότι δεν είναι το πρώτο θραύσμα.

4.18 Ναι, ακολουθούν άλλα τρία θραύσματα.

4.19 Το γεγονός ότι μετά το 2ο θραύσμα ακολουθεί κι άλλο φαίνεται στο πεδίο Flags της επικεφαλίδας του, όπου δίπλα από τη τιμή της υπάρχει τη αναφορά : More Fragments

Στο πέμπτο και τελευταίο θραύσμα δεν υπάρχει αυτή η αναφορά.

4.20 Μεταξύ του πρώτου και του δεύτερου θραύσματος αλλάζουν τα πεδία: Flags, Fragment Offset και Header checksum

4.21 Η τιμή του Fragment Offset για το προτελευταίο θραύσμα είναι 4440 και σημαίνει ότι τα δεδομένα που μεταφέρει ξεκινάνε από Byte 4440 στο «αρχικό» IPV4 πακέτο. Ομοίως η τιμή του Fragment Offset για το τελευταίο θραύσμα είναι 5920 και σημαίνει ότι τα δεδομένα που μεταφέρει ξεκινάνε από Byte 5920 στο «αρχικό» IPV4 πακέτο.

4.22 Μεταξύ των θραύσματων αλλάζουν τα πεδία: Flags, Fragment Offset, Total Length και Header checksum