

Όνοματεπώνυμο: Ζευγολατάκος Παναγιώτης		Ομάδα: 3
Όνομα PC/ΛΣ: ranos-PC / Windows 10		Ημερομηνία: 24/10/20
Διεύθυνση IP: 192. 168. 2.2	Διεύθυνση MAC: D0-50-99-75-F8- F8	

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 -4 -n 3

1.2 Το φίλτρο αυτό χρησιμοποιείται έτσι ώστε να μπορέσουμε να δούμε την κίνηση προς και από το μηχάνημα (unicast traffic), απαλείφοντας το θόρυβο στο δίκτυο (multicast και broadcast πακέτα).

1.3 Ποσοστό απώλειας πακέτων: 0%

Μέση καθυστέρηση: 45ms

1.4 Approximate round trip times in milli-seconds:

Minimum = 45ms, Maximum = 45ms, Average = 45ms

1.5 Βρίσκουμε πως τα replies έχουν τις τιμές: 0.045459, 0.045666 και 0.045373 seconds. Παρόλο που έχουν μεγαλύτερη ακρίβεια από τις αντίστοιχες τιμές στο παράθυρο εντολών (δηλαδή οι τελευταίες είναι στρογγυλοποιημένες), συμφωνούν.

1.6 ip

1.7 icmp

1.8 Στάλθηκαν μηνύματα ICMP type 8 (Echo (ping) request).

1.9 Src: 192.168.2.2 (τοπική), Dst: 104.83.115.155

1.10 Ελήφθησαν μηνύματα ICMP type 0 (Echo (ping) reply).

1.11 Src: 104.83.115.155, Dst: 192.168.2.2 (τοπική)

1.12

.....

.....

2

2.1 ping 192.168.2.1 -4 -n 5

ping 192.168.2.2 -4 -n 5

ping 127.0.0.1 -4 -n 5

2.2 Το WireShark έχει καταγράψει 5/15 μηνύματα ICMP Echo request.

2.3 Ο προορισμός τους ήταν η διεύθυνση 192.168.2.1 (διεύθυνση IPv4 της προκαθορισμένης πύλης).

2.4 Όχι, εφόσον ανακατευθύνονται στον υπολογιστή μέσω του loopback interface (έχουν προορισμό την τοπική διεύθυνση IPv4).

2.5 Όχι, εφόσον ανακατευθύνονται στον υπολογιστή μέσω του loopback interface (δρομολογούνται άμεσα).

2.6 Όταν γίνεται ping στη διεύθυνση loopback 127.0.0.1 η εντολή περνάει κατευθείαν στο loopback interface του υπολογιστή, ενώ όταν γίνεται ping στη διεπαφή του υπολογιστή περνάει πρώτα από τον οδηγό Ethernet πριν οδηγηθεί και αυτό στο loopback interface.

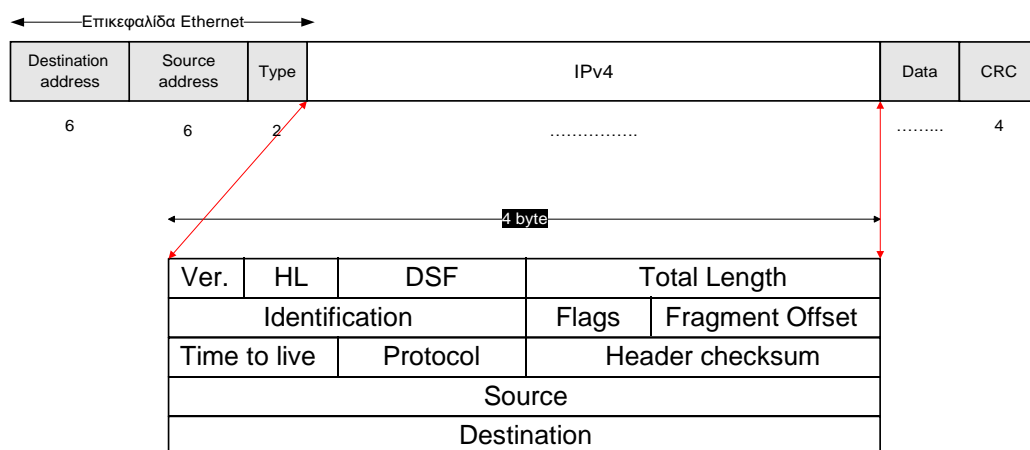
2.7 Παρατηρούμε πως για τα ping request στην ιστοσελίδα της Amazon λαμβάνουμε replies, αλλά για τα ping request στην ιστοσελίδα της Netflix παίρνουμε το μήνυμα “Request timed out.”. Μπορεί στο server της Netflix να υπάρχει κάποιο firewall που να εμποδίζει τα ICMP requests.

3

3.1 host 192.168.2.2

3.2 ip.src_host == 192.168.2.2 and (telnet or ftp)

3.3 Version (4 bits), Header Length (4 bits), Differentiated Services Field (8 bits), Total Length (16 bits), Identification (16 bits), Flags (3 bits), Fragment offset (εδώ 0 / 13 bits), Time to live (8 bits), Protocol (8 bits), Header checksum (16 bits), Source (32 bits), Destination (32 bits).



3.4 Total Length, Identification, Header Checksum.

3.5 Ναι.

3.6 Min: 40 byte, Max: 224 byte.

3.7 Το πεδίο Differentiated Services Field έχει την τιμή 0x00, που αντιστοιχεί στο όνομα DF (CS0), άρα αντιστοιχεί σε best-effort traffic.

3.8 Είναι διαφορετικές, αλλά οι τιμές είναι αυξανόμενες κατά ένα ή παραπάνω.

3.9 0x4000

3.10 Έχει την τιμή 1.

3.11 Έχει την τιμή 6 και αντιστοιχεί στο πρωτόκολλο TCP.

3.12 Το πεδίο Header Checksum χρησιμοποιείται για error checking. Ο τρόπος με τον οποίο δουλεύει είναι με άθροισμα των ψηφίων ανά 16 bit και 1's complement για κάθε 16 bit λέξεις στην επικεφαλίδα. Εφόσον υπολογίζεται από τα περιεχόμενα της επικεφαλίδας, είναι λογικό να έχει διαφορετικές τιμές για κάθε επικεφαλίδα (αφού καθεμία είναι διαφορετική).

4

4.1 ping 192.168.2.1 -f -4 -n 1 -l 1480 (όπου 1480 το μέγεθος του πακέτου σε bytes).

4.2 1472 bytes.

4.3 1473 bytes.

4.4 not multicast and not broadcast

4.5 ip.addr == 192.168.2.1

4.6 Όχι, δεν παράγονται πακέτα IPv4 με αυτήν την τιμή, επειδή δεν μπορούν να μεταδοθούν χωρίς να γίνει fragmentation (και δεν το επιτρέπουμε με τη χρήση του flag -f).

4.7 Η MTU της διεπαφής του υπολογιστή μου είναι 1500 bytes, εφόσον το μέγιστο μέγεθος που επιτρέπεται να μεταδοθεί χωρίς fragmentation είναι 1472 bytes + 20 bytes για το IP Header + 8 bytes για το ICMP Header.

4.8 65507 bytes.

4.9 Αποτυγχάνει (τα Windows επιτρέπουν μέχρι τα 65500 bytes).

4.10 65528 bytes (έναντι των $2^{16}-1=65535$ bytes / λόγω του ping of death)

4.11 Όχι.

4.12 Χρειάστηκαν 5 πακέτα IPv4, γιατί η MTU έχει όριο 1500 bytes για IPv4 πακέτα και άρα πρέπει να γίνει fragmentation.

4.13 Identification: 0xe60b

Don't Fragment Bit: 0

More Fragments: 1

Fragment Offset: 0 / 1480 / 2960 / 4440

4.14 Το bit "More Fragments". Αν έχει την τιμή 1, σημαίνει πως είναι fragment και ακολουθούν κι άλλα.

4.15 Το Fragment Offset (έχει την τιμή 0).

4.16 1480 bytes.

4.17 Η τιμή του Fragment Offset δεν είναι 0.

4.18 Ναι.

4.19 Το bit "More Fragments" έχει την τιμή 1.

4.20 Fragment Offset, Header Checksum.

4.21 Κάθε πεδίο Fragment Offset ενός θραύσματος είναι 1480 bytes παραπάνω από το προηγούμενό του. Επομένως, για το προτελευταίο και το τελευταίο θραύσμα θα είναι $4440 [= 3 \cdot 1480]$ και $5920 [= 4 \cdot 1480]$ αντίστοιχα.

4.22 More Fragments bit (στο τέλος), Fragment Offset, Header Checksum, Total Length (στο τέλος).

