



## Δίκτυα υπολογιστών

Εργαστηριακή άσκηση 4 (Πρωτόκολλο IPv4 και θρυμματισμός)

Τσάκωνας Παναγιώτης (03119610)

Ομάδα: 2

Ακαδημαϊκό Έτος: 2022-2023

### Άσκηση 1: Ο Πίνακας ARP

- 1.1) Η ακριβής σύνταξη της εντολής που χρησιμοποίησα είναι η `ping www.mit.edu`.
- 1.2) Η σημασία του φίλτρου σύλληψης που εφαρμόσα είναι ότι καταγράφονται όσα μηνύματα έχουν συγκεκριμένο παραλήπτη και αποστολέα.
- 1.3) Το ποσοστό απωλειών πακέτων είναι μηδενικό και η μέση καθυστέρηση είναι 35.04ms.
- 1.4) Οι τιμές του RTT, όπως εμφανίζονται στο παράθυρο εντολών, είναι: 35.725, 30.511, 34.941, 31.630, 38.009, 38.439.
- 1.5) Οι τιμές του RTT για κάθε ζεύγος Echo Request – Echo Reply, με τη βοήθεια του Wireshark, παρατηρώ ότι είναι οι ίδιες: 35.725, 30.511, 34.941, 31.630, 38.009, 38.439.
- 1.6) Πρέπει να εφαρμόσω το φίλτρο απεικόνισης `ip` προκειμένου να παρατηρώ μόνο πακέτα IPv4.
- 1.7) Το φίλτρο απεικόνισης που πρέπει να εφαρμόσω προκειμένου να παρατηρήσω μόνο την κίνηση ICMP που προκάλεσε η εντολή `ping` είναι το `icmp.type==8 or icmp.type==0`.
- 1.8) Το είδος των μηνυμάτων που στάλθηκε είναι Type:8 (Echo (ping) request).
- 1.9) Οι διευθύνσεις IPv4 πηγής και προορισμού των παραπάνω μηνυμάτων είναι: 147.102.201.66 και 92.123.12.49 αντίστοιχα.
- 1.10) Το είδος των μηνυμάτων που λήφθηκε είναι Type:0 (Echo (ping) reply).
- 1.11) Οι διευθύνσεις IPv4 πηγής και προορισμού των παραπάνω μηνυμάτων είναι: 92.123.12.49 και 147.102.201.66 αντίστοιχα.
- 1.12) Έχει αλλάξει η IP της ιστοσελίδας, οι τιμές του RTT αλλά και τα βήματα.

### Άσκηση 2: Περισσότερα για το Ping

- 2.1) Η ακριβής σύνταξη της εντολής που χρησιμοποίησα είναι `ping <address> -c 5`.
- 2.2) Από τα μηνύματα ICMP Echo request που έχουν αποσταλεί από τον υπολογιστή σας το Wireshark έχει καταγράψει 5.
- 2.3) Ο προορισμός τους ήταν η default gateway 147.102.200.200.
- 2.4) Όχι δεν παρατήρησα πακέτα ICMP Echo request στο δίκτυο με πηγή και προορισμό τη διεύθυνση IPv4 του υπολογιστή σας, διότι μπαίνει κατευθείαν στο loopback driver και έτσι δεν φτάνει ποτέ στην κάρτα δικτύου και έτσι δεν τα εντοπίζει το Wireshark.
- 2.5) Όχι, δεν παρατήρησα αποστολή μηνυμάτων ICMP Echo request προς τη διεύθυνση του βρόχου επιστροφής, διότι αυτό το request μπαίνει στην κάρτα δικτύου και δεν βγαίνει στο τοπικό δίκτυο για να την διαβάσει το Wireshark (εσωτερική κίνηση στο pc μου).
- 2.6) Η διαφορά είναι ότι στο `ping` στη διεπαφή του υπολογιστή το πακέτο εισέρχεται στον οδηγό Ethernet και αυτός το στέλνει στον loopback driver, ενώ όταν κάνουμε `ping` στη διεύθυνση 127.0.0.1, το πακέτο εισέρχεται κατευθείαν στον loopback driver και στέλνεται πίσω στην είσοδο πακέτων IPv4.

- 2.7) Όταν κάνω ping το [www.netflix.com](http://www.netflix.com) δεν υπάρχουν ping replies σε αντίθεση με το [www.amazon.com](http://www.amazon.com) που υπάρχουν. Αυτό συμβαίνει ενδεχομένως επειδή το Netflix έχει ενεργοποιημένο κάποιο firewall που μπλοκάρει τα ICMP πακέτα.

### Άσκηση 3: Επικεφαλίδες IPv4

- 3.1) Η σύνταξη του φίλτρου σύλληψης που χρησιμοποίησα είναι: Capture filter : host 147.102.40.15.  
3.2) Η σύνταξη του φίλτρου απεικόνισης ώστε να παραμείνουν μόνο τα πακέτα IPv4 που έστειλε ο υπολογιστής σας είναι: Display filter: ip.src == 147.102.201.66.  
3.3) Τα ονόματα και το μήκος σε bit των πεδίων της επικεφαλίδας του πακέτου IPv4 είναι τα ακόλουθα:

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) Αλλάζουν τα πεδία Total Length και Identification.  
3.5) Το μήκος της επικεφαλίδας IPv4 παραμένει το ίδιο σε όλα τα πακέτα (20 bytes).  
3.6) Το μικρότερο πακέτο IPv4 που παρατήρησα είναι 40 bytes και το μεγαλύτερο 66 bytes.  
3.7) Παίρνει τις τιμές 0x00 → CS0: Standard Service class και 0xb8 → EF PHB: Telephony Service class.  
3.8) Οι τιμές του πεδίου Identification αυξάνονται με τη χρήση ενός μετρητή.  
3.9) Η σημαία Don't Fragment έχει τιμή 1.  
3.10) Το πεδίο Fragment Offset έχει τιμή 0.  
3.11) Το πεδίο Protocol έχει τιμή 0x06 και αντιστοιχεί στο πρωτόκολλο TCP.  
3.12) Η τιμή του πεδίου Header Checksum αλλάζει σε κάθε πακέτο IPv4, διότι αναπαριστά το άθροισμα των λέξεων που περιέχονται στο IPv4 header και από τη στιγμή που υπάρχουν πεδία που αλλάζουν, τότε αλλάζει και αυτό.

## Άσκηση 4: Θρυμματισμός (Fragmentation) στο IPv4

- 4.1) Η ακριβής σύνταξη της εντολής ping που πρέπει να χρησιμοποιήσω είναι: `ping -n 1 -4 -f -l`.
- 4.2) Η μέγιστη τιμή για την οποία επιτυγχάνει η αποστολή είναι 1472 bytes.
- 4.3) Η μικρότερη τιμή για την οποία απαιτείται θρυμματισμός είναι 1473 bytes.
- 4.4) Η σύνταξη του φίλτρου σύλληψης που χρησιμοποίησα είναι: Capture filter: not multicast and not broadcast.
- 4.5) Η σύνταξη του φίλτρου απεικόνισης που εφάρμοσα είναι: Display filter: `ip.addr == 147.102.38.68`.
- 4.6) Όχι, δεν παράγονται πακέτα IPv4, διότι η τιμή της MTU είναι μεγάλη και δεν μπορεί να μεταδοθεί.
- 4.7) Το μέγεθος της MTU της διεπαφής του υπολογιστή μου είναι 1514 bytes, όπως το κατέγραψε το Wireshark.
- 4.8) Η τιμή 1472 bytes οδηγεί σε πακέτο IPv4 μέγιστου μήκους.
- 4.9) Για μήκος δεδομένων 1472 bytes και χωρίς τη παράμετρο -f στην εντολή επιτυγχάνεται το ping.
- 4.10) Το μεγαλύτερο πακέτο IPv4 έχει μήκος 1514 bytes.
- 4.11) Όχι, έχει μεταφερθεί ως πολλά.
- 4.12) Χρειάστηκαν 5 πακέτα, διότι το κάθε ένα από αυτά έχει μέγιστο μήκος ICMP 1480 bytes και επειδή  $6000/1480 = 5$ , δημιουργούνται 5 πακέτα.
- 4.13) (0x3622, 0, 1, 0), (0x3622, 0, 1, 1480), (0x3622, 0, 1, 2960), (0x3622, 0, 1, 4440), (0x3622, 0, 1, 5920).
- 4.14) Το flag More Fragments Bit της επικεφαλίδας IPv4 δηλώνει ότι το πακέτο έχει θρυμματιστεί.
- 4.15) Το πεδίο Fragment Offset το οποίο έχει τιμή 0, και δηλώνει ότι αυτό το πακέτο είναι το πρώτο που φθάνει.
- 4.16) Το μήκος του πρώτου θραύσματος είναι 1480 bytes σε δεδομένα και το μήκος πακέτου είναι 1514 bytes.
- 4.17) Το πεδίο Fragment Offset δηλώνει ότι δεν είναι το πρώτο θραύσμα, διότι η τιμή του δεν είναι 0.
- 4.18) Ναι, ακολουθούν και άλλα θραύσματα.
- 4.19) Είναι ενεργοποιημένο το flag More fragments.
- 4.20) Μεταξύ του πρώτου και του δεύτερου θραύσματος αλλάζει μόνο το πεδίο Fragment Offset.
- 4.21) Για το προτελευταίο η τιμή είναι 4440 bytes, δηλαδή  $3 * 1480$  bytes (δηλαδή δηλώνει ότι έχουν προηγηθεί 3 θραύσματα με μήκος δεδομένων 1480 bytes). Για το τελευταίο η τιμή είναι 5920 bytes, δηλαδή  $4 * 1480$  bytes και προκύπτει αντίστοιχα.
- 4.22) Τα πεδία της επικεφαλίδας IPv4 που αλλάζουν μεταξύ των θραυσμάτων είναι τα: Fragment Offset, More fragments και Total Length.