

4^η Εργαστηριακή Άσκηση στα Δίκτυα Υπολογιστών

Όνοματεπώνυμο	Γεώργιος Στεφανάκης
Αρ. Μητρώου	el18436
Ομάδα	4
Λειτουργικό Σύστημα	Manjaro Linux x86_64
Διεύθυνση IP	147.102.238.65
Διεύθυνση MAC	b4:69:21:5e:da:03
Ημερομηνία	2022-10-27

1. Μέτρηση καθυστέρησης

1.1. ping -c 3 -4 www.mit.edu

```
[giorgis@afousis ~]$ ping -c 3 -4 www.mit.edu
PING (104.76.158.49) 56(84) bytes of data:
64 bytes from a104-76-158-49.deploy.static.akamaitechnologies.com (104.76.158.49): icmp_seq=1 ttl=56 time=28.4 ms
64 bytes from a104-76-158-49.deploy.static.akamaitechnologies.com (104.76.158.49): icmp_seq=2 ttl=56 time=28.5 ms
64 bytes from a104-76-158-49.deploy.static.akamaitechnologies.com (104.76.158.49): icmp_seq=3 ttl=56 time=28.4 ms

--- ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 28.413/28.460/28.543/0.058 ms
[giorgis@afousis ~]$
```

1.2. Με το φίλτρο που χρησιμοποιήσαμε αποκλείουμε τα πακέτα που αποτελούν broadcast ή multicast εκπομπές, απαλλασσόμενοι από τον θόρυβο του δικτύου και έτσι βλέπουμε μόνο την κίνηση από και προς τον υπολογιστή μας. Εξαιρούμε έτσι τα πακέτα που εκπέμπονται από έναν σε πολλούς ή από πολλούς σε πολλούς και άρα καταγράφουμε μόνο τα unicast πακέτα.

1.3. Παρατηρούμε από την εκτέλεση της παραπάνω εντολής ότι δεν είχαμε απώλεια πακέτων (0% packet loss), ενώ η μέση καθυστέρηση του RTT είναι ίση με 28.460 ms.

1.4. Οι τιμές των χρόνων που καταγράφηκαν με τη σειρά είναι 28.4, 28.5 και 28.4 ms.

1.5.

ip.addr == 104.76.158.49							
No.	Time	Source	Destination	Protocol	Length	Info	
9	0.000000000	147.102.238.65	104.76.158.49	ICMP	98	Echo (ping) request	id=0x0009, seq=1/256, ttl=64 (reply in 10)
10	0.028361382	104.76.158.49	147.102.238.65	ICMP	98	Echo (ping) reply	id=0x0009, seq=1/256, ttl=56 (request in 9)
13	0.973542875	147.102.238.65	104.76.158.49	ICMP	98	Echo (ping) request	id=0x0009, seq=2/512, ttl=64 (reply in 14)
14	0.028519737	104.76.158.49	147.102.238.65	ICMP	98	Echo (ping) reply	id=0x0009, seq=2/512, ttl=56 (request in 13)
18	0.972803967	147.102.238.65	104.76.158.49	ICMP	98	Echo (ping) request	id=0x0009, seq=3/768, ttl=64 (reply in 19)
19	0.028359370	104.76.158.49	147.102.238.65	ICMP	98	Echo (ping) reply	id=0x0009, seq=3/768, ttl=56 (request in 18)

Βλέπουμε ότι οι χρόνοι για όλα τα reply πακέτα συμφωνούν με τους χρόνους που καταγράφηκαν από την εντολή ping. Οι τιμές που φαίνονται στο Wireshark είναι στρογγυλοποιημένες ως προς το δεύτερο δεκαδικό ψηφίο τους στη γραμμή εντολών.

1.6. Εφαρμόζουμε το φίλτρο "ip".

1.7. ip.addr == 104.76.158.49 and icmp

1.8. Στάλθηκαν μηνύματα τύπου Echo (ping) request.

1.9. Οι διευθύνσεις IPv4 πηγής αυτών των μηνυμάτων είναι 147.102.238.65 (η IP του υπολογιστή μου) και οι διευθύνσεις προορισμού των μηνυμάτων είναι 104.76.158.49 (η IP του www.mit.edu).

1.10. Ελήφθησαν Echo (ping) replies.

1.11. IP πηγής: 104.76.158.49, IP προορισμού: 147.102.238.65.

1.12. Οι αλλαγές που παρατηρούμε είναι οι εξής:

i. Διαφορετική IPv4 του εξυπηρετητή.

- ii. Διαφορετικός χρόνος ζωής πακέτου
- iii. Το γεγονός ότι οι χρόνοι απόκρισης στο παρελθόν είναι σταθεροί παραπέμπει σε ντετερμινιστική διαδικασία ενώ οι σύγχρονοι χρόνοι είναι διαφορετικοί μεταξύ τους και έχουν κάποια τυχαιότητα γεγονός που παραπέμπει σε στοχαστική διαδικασία.

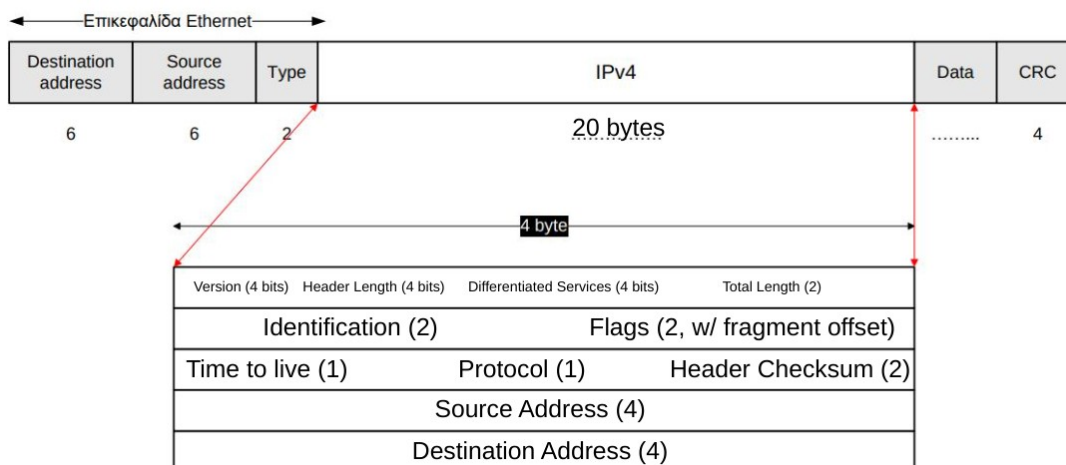
2. Περισσότερα για το Ping

Η άσκηση αυτή εκτελέστηκε σε υπολογιστή συνδεδεμένο ασύρματα σε τοπικό δίκτυο, με IPv4 192.168.1.16.

- 2.1.
 - i. Default gateway: ping -c 5 -4 192.168.1.1
 - ii. Local IPv4: ping -c 5 -4 192.168.1.16
 - iii. Loopback: ping -c 5 -4 127.0.0.1
- 2.2. Το Wireshark κατέγραψε μόνο 5 μηνύματα Echo (ping) request.
- 2.3. Ο προορισμός τους ήταν η διεύθυνση προκαθορισμένης πύλης 192.168.1.1.
- 2.4. Όχι δεν παρατηρήσαμε κάτι τέτοιο. Αυτό οφείλεται όπως βλέπουμε και στο σχήμα στο ότι όταν η διεύθυνση προορισμού IPv4 είναι η ίδια με την τοπική διεύθυνση, το μήνυμα προωθείται στο loopback και από εκεί επιστρέφει στην είσοδο του υπολογιστή μας. Άρα το μήνυμα δεν μπήκε ποτέ στο τοπικό δίκτυο για αυτό δεν καταγράφηκε από το Wireshark.
- 2.5. Όπως και στο προηγούμενο ερώτημα δεν παρατηρούμε κάτι διότι από την έξοδο πακέτων IPv4 του υπολογιστή μας θα πάει στον Οδηγό loopback και πίσω στην είσοδο του υπολογιστή μας και άρα δε θα καταγραφεί από το Wireshark.
- 2.6. Η κύρια διαφορά είναι ότι όταν κάνουμε ping στη διεύθυνση loopback το πακέτο δε θα φύγει ποτέ από τον υπολογιστή μας. Αντίθετα όταν κάνουμε ping στην ip μας το πακέτο θα περάσει πρώτα από τον Οδηγό ethernet και από εκεί θα προωθηθεί πίσω στον Οδηγό loopback.
- 2.7. Το παράδοξο έγκειται στο ότι ενώ και το www.netflix.com και το www.amazon.com ανοίγουν κανονικά στον browser, εντούτοις το www.netflix.com δεν απαντάει στα ping requests ενώ το www.amazon.com απαντάει. Μια υπόθεση που μπορούμε να κάνουμε είναι ότι το Netflix χρησιμοποιεί κάποιο τείχος προστασίας firewall ενώ το Amazon όχι.

3. Επικεφαλίδες IPv4

- 3.1. Η σύνταξη του φίλτρου σύλληψης είναι host 147.102.40.15.
- 3.2. Η σύνταξη του φίλτρου απεικόνισης είναι ip.src == 147.102.238.65.
- 3.3. Με συνολικό header length 20 byte βλέπουμε παρακάτω στο σχήμα τα ονόματα και το μέγεθος των πεδίων της επικεφαλίδας IPv4.



- 3.4. Διαφορετικές τιμές παρουσιάζουν τα πεδία Total length, Header checksum, Identification.
- 3.5. Το μήκος της επικεφαλίδας IPv4 είναι πάντα ίδιο και ίσο με 20 bytes.
- 3.6. Το μικρότερο που παρατηρώ είναι 54 bytes και το μεγαλύτερο 80 bytes.

- 3.7. Η τιμή του Differentiated Services Field είναι 0x00 και αντιστοιχεί στην default ποιότητα υπηρεσίας (Standard) αφού στην προκείμενη άσκηση δεν υπάρχουν ιδιαίτερες απαιτήσεις για την κατηγοριοποίηση του είδους της κίνησης στο δίκτυο.
- 3.8. Οι τιμές του πεδίου Identification διαφοροποιούνται από πακέτο σε πακέτο και είναι ο αύξοντας αριθμός που ανατίθεται σε κάθε πακέτο για την αναγνώριση της σειράς με την οποία στάλθηκε.
- 3.9. Σε όλα τα πακέτα παρατηρούμε ότι η τιμή του Don't Fragment είναι ίση με 1.
- 3.10. Το Fragment Offset έχει τιμή 0.
- 3.11. Η τιμή που έχει το πεδίο Protocol είναι 0x06 και αντιστοιχεί στο TCP.
- 3.12. Η τιμή του Header Checksum αλλάζει από πακέτο σε πακέτο διότι υπολογίζεται κάθε φορά με βάση τα περιεχόμενα του κάθε πακέτου έτσι ώστε όταν φτάσει στον παραλήπτη να μπορεί αυτός να ελέγξει αν οι πληροφορίες που έλαβε περιέχουν λάθη ή όχι. Αφού εξαρτάται λοιπόν από τα περιεχόμενα του κάθε πακέτου είναι αναμενόμενο η τιμή του header checksum να διαφέρει από πακέτο σε πακέτο.

4. Θρυμματισμός (Fragmentation) στο IPv4

- 4.1. Η εντολή έχει τη μορφή "ping -D -s <PACKET_SIZE> -c 1 <IPv4_ADDRESS>".
- 4.2. Είναι 1472 bytes.
- 4.3. Είναι 1473 bytes.
- 4.4. Το φίλτρο σύλληψης που χρησιμοποιήσαμε είναι "not broadcast and not multicast".
- 4.5. Το φίλτρο απεικόνισης είναι "ip.src == 192.168.1.1 or ip.dst == 192.168.1.1".
- 4.6. Όχι δεν παράγονται πακέτα σε αυτή τη περίπτωση αφού το πακέτο είναι μεγαλύτερο του MTU και δεν μπορεί να διαδοθεί και συνεπώς δε θα μπει στον οδηγό Ethernet άρα ούτε στο τοπικό δίκτυο για να μπορέσει να το καταγράψει το Wireshark.
- 4.7. Όχι δεν παράγονται, διότι το πακέτο είναι μεγαλύτερο του MTU και δεν μπορεί να ταξιδέψει. Συνεπώς δεν θα μπει στον οδηγό Ethernet και αρα στο τοπικό δίκτυο και έτσι δεν θα το καταγράψει το Wireshark.
- 4.8. Από την επικεφαλίδα ICMP και πεδίο Data προκύπτει ότι Maximum Length = 1472 bytes.
- 4.9. Για μήκος δεδομένων 1472 και χωρίς τη παράμετρο -f 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 γιατί το κάθε ένα έχει μέγιστο μήκος ICMP 1480 bytes.
- 4.13.

Identification	Don't Fragment Bit	More Fragments Bit	Fragment Offset
0x1ce1	0	1	1
0x1ce1	0	1	1480
0x1ce1	0	1	2960
0x1ce1	0	1	5550
0x1ce1	0	0	5920

- 4.14. Το πεδίο "More Fragments Bit".
- 4.15. Το πεδίο 'Fragment Offset', το οποίο είναι 0.
- 4.16. Το μήκος πακέτου είναι 1514 bytes, 1480 εκ των οποίων είναι δεδομένα.
- 4.17. Το πεδίο "Fragment Offset" μ το οποίο δεν είναι 0.
- 4.18. Ναι.
- 4.19. Είναι ενεργοποιημένο το flag "More fragments".
- 4.20. Μόνο το πεδίο "Fragment Offset".
- 4.21. Για το πρωτελευταίο η τιμή είναι $4440 = 3 \times 1480$, δηλαδή έχουν προηγηθεί 3 θραύσματα με μήκος δεδομένων 1480. Για το τελευταίο η τιμή είναι $5920 = 4 \times 1480$ και προκύπτει αντίστοιχα, δηλαδή 4 θραύσματα.
- 4.22. Διαφορετικά είναι τα πεδία Fragment Offset, More Fragments, και Total Length.