Δίκτυα Υπολογιστών

Εργαστηριακή Άσκηση 4
Πρωτόκολλο IPv4 και θρυμματισμός

Ονοματεπώνυμο: Νικόλαος Παγώνας, el18175	**Ομάδα:** 4 (Τρίτη εξ' αποστάσεως)
Όνομα PC/ΛΣ: nick-ubuntu/Ubuntu 20.04.3 LTS	**Ημερομηνία:** Τρίτη 02/11/2021
Διεύθυνση IP: `192.168.1.15`	**Διεύθυνση MAC:** `3c:2c:30:e1:1c:55`

1 - Μετρήστε την καθυστέρηση

1.1

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

1.2

Με το φίλτρο `not multicast and not broadcast` ουσιαστικά καταγράφουμε μόνο τα unicast πακέτα, ώστε να αφαιρέσουμε τον "θόρυβο" που εισάγουν οι broadcast και multicast εκπομπές, αφού μας ενδιαφέρει μόνο η κίνηση από και προς το μηχάνημά μας.

1.3

Έχουμε: 0% packet loss, μέση καθυστέρηση 41.458 ms

1.4

- 64 bytes from 23.79.130.108: icmp_seq=1 ttl=58 time=41.2 ms
- 64 bytes from 23.79.130.108: icmp_seq=2 ttl=58 time=42.2 ms
- 64 bytes from 23.79.130.108: icmp_seq=3 ttl=58 time=41.0 ms

1.5

Με το Wireshark έχουμε αντίστοιχα:

- time = 0.0412
- time = 0.0421
- time = 0.0409

Οι τιμές είναι πρακτικά οι ίδιες.

1.6

Για να βλέπουμε μόνο πακέτα IPv4, μπορούμε να εφαρμόσουμε το φίλτρο απεικόνισης `ip.version == 4`

1.7

Πρέπει να εφαρμόσουμε το φίλτρο:
`icmp && (ip.src == 23.79.130.108 || ip.dest == 23.79.130.108)`
ώστε να βλέπουμε μόνο ICMP πακέτα, και είτε η πηγή είτε ο προορισμός να αφορούν την IPv4 διεύθυνση του www.mit.edu.

1.8

Στάλθηκαν μηνύματα ICMP Echo Request.

1.9

Διεύθυνση πηγής είναι η 192.168.1.15, ενώ διεύθυνση προορισμού είναι η 23.79.130.108.

1.10

Στάλθηκαν μηνύματα ICMP Echo Reply.

1.11

Διεύθυνση πηγής είναι η 23.79.130.108, ενώ διεύθυνση προορισμού είναι η 192.168.1.15.

1.12

Παρατηρούμε ότι έχει αλλάξει η διεύθυνση IPv4 του www.mit.edu από 18.7.22.83 σε 23.79.130.108.

2 - Περισσότερα για το ping

2.1

Η ακριβής σύνταξη της εντολής που χρησιμοποιήσαμε είναι:

```
ping -4 -c 5 192.168.1.7 && ping -4 -c 5 192.168.1.15 && ping -4 -c 5 127.0.0.1
```

όπου 192.168.1.7 μία συσκευή στο τοπικό μας δίκτυο, 192.168.1.15 η κάρτα δικτύου του υπολογιστή μας και 127.0.0.1 ο βρόχος επιστροφής.

2.2

Έχουν καταγραφεί 5 ICMP Request.

2.3

Ο προορισμός ήταν 192.168.1.7 (η συσκευή του τοπικού μας δικτύου).

2.4

Δεν παρατηρήσαμε αποστολή μηνυμάτων ICMP Echo Request που έχουν πηγή και προορισμό την διεύθυνση IPv4 του υπολογιστή μας, γιατί όπως βλέπουμε και στο σχήμα, τα πακέτα προωθούνται στον οδηγό loopback, οπότε δεν καταγράφονται από το Wireshark.

2.5

Για τον ίδιο λόγο, δεν παρατηρούμε αποστολή μηνυμάτων ICMP Echo Request ούτε σε αυτήν την περίπτωση.

2.6

Η διαφορά είναι πως όταν κάνουμε ping στην διεύθυνση loopback, τα πακέτα δεν φεύγουν ποτέ από τον υπολογιστή μας, ενώ όταν κάνουμε ping την 192.168.1.15, το πακέτο περνάει από τον οδηγό Ethernet (παρόλο που στην συνέχεια θα προωθηθεί και πάλι στον οδηγό loopback).

2.7

Παρατηρούμε ότι ενώ η σελίδα www.netflix.com φορτώνει κανονικά στον browser, όταν πάμε να κάνουμε ping request δεν λαμβάνουμε απάντηση. Αντίθετα, η σελίδα www.amazon.com φορτώνει στον browser και απαντάει σε ping requests.

Μία υπόθεση είναι ότι το δίκτυο του netflix (ή κάποιο ενδιάμεσο firewall) μπλοκάρει τα ping requests για λόγους ασφαλείας/προστασίας του δικτύου.

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 == 192.168.1.15 && ip.version == 4`

3.3

- Version: 4 bit
- Header Length: 4 bit
- Differentiated Services Field: 1 byte (DSCP 6 bit, ECN 2 bit)
- Total Length: 2 byte
- Identification: 2 byte
- Flags: 3 bit
- Fragment Offset: 13 bit
- Time to Live: 1 byte
- Protocol: 1 byte
- Header Checksum: 2 byte
- Source (IP) Address: 4 byte
- Destination (IP) Address: 4 byte

3.4

Αλλάζουν τα:

- Differentiated Services Field
- Total Length
- Identification
- Time to Live
- Header Checksum
- Source Address (εναλλάσσεται μεταξύ των δύο εμπλεκόμενων διευθύνσεων)
- Destination Address (εναλλάσσεται μεταξύ των δύο εμπλεκόμενων διευθύνσεων)

3.5

Ναι, είναι το ίδιο.

3.6

Το μικρότερο μήκος πακέτου είναι 40 bytes και το μεγαλύτερο 146 bytes.

3.7

Το πεδίο Differentiated Services Field έχει τιμή 0x00 (Standard) ή 0x10 (CS2)

3.8

Είναι διαφορετικό για κάθε πακέτο.

3.9

Η τιμή της σημαίας Don't Fragment είναι 1.

3.10

Το πεδίο Fragment offset έχει τιμή 0.

3.11

Το πεδίο Protocol έχει τιμή 6 και αντιστοιχεί στο πρωτόκολλο TCP.

3.12

Το Header Checksum εξαρτάται από τις τιμές των πεδίων της επικεφαλίδας, και εφόσον αυτές είναι διαφορετικές από πακέτο σε πακέτο (για παράδειγμα το Identification είναι διαφορετικό για κάθε πακέτο), τότε είναι λογικό να αλλάζει και η τιμή του Header Checksum.

4 - Θρυμματισμός (Fragmentation) στο IPv4

4.1

```
ping -M do -4 -c 1 -s <desirable size> aaaa.bbbb.cccc.dddd
```

4.2

Η μέγιστη τιμή για την οποία επιτυγχάνει η αποστολή είναι 1472.

4.3

Η μικρότερη τιμή για την οποία απαιτείται θρυμματισμός είναι 1473.

4.4

```
not broadcast and not multicast
```

4.5

```
(ip.src == 192.168.1.7 || ip.dst == 192.168.1.7) && ip.version == 4
```

4.6

Δεν παράγονται πακέτα IPv4 διότι ο έλεγχος για υπέρβαση του MTU γίνεται προτού το πακέτο σταλεί στο τοπικό δίκτυο.

4.7

Παρατηρούμε ότι όταν δίνουμε την τιμή 1472 στο ping, το Wireshark καταγράφει μέγεθος δεδομένων 1500 bytes, άρα MTU = 1500 bytes.

4.8

Το μέγιστο μέγεθος IPv4 πακέτου είναι 65.535 bytes. Αν αφαιρέσουμε τις επικεφαλίδες IPv4 και ICMP μας μένουν 65.535 - 20 - 8 = 65.507 bytes. Επομένως η τιμή 65.507 οδηγεί σε πακέτο μέγιστου μήκους.

4.9

Το ping στην διεύθυνση του υπολογιστή μας επιτυγχάνει.

4.10

Το μέγιστο μέγεθος πακέτου που μπορεί να παράγει η εντολή ping είναι 65.535 bytes.

4.11

Όχι, δεν έχει μεταφερθεί ως ένα πακέτο IPv4.

4.12

Εδώ απαιτείται fragmentation (κάτι που αυτή τη φορά επιτρέπεται). Έχουμε $\left\lceil \frac{6000}{1472} \right\rceil = 5$ πακέτα.

4.13

Identification	Don't fragment Bit	More fragments Bit	Fragment Offset
0x870b	0	1	0
0x870b	0	1	1480
0x870b	0	1	2960
0x870b	0	1	4440
0x870b	0	0	5920

4.14

Βλέπουμε ότι το πακέτο έχει θρυμματιστεί από το More Fragments Bit = 1 ή το Don't fragment = 0.

4.15

Μπορούμε να καταλάβουμε ότι πρόκειται για το πρώτο θραύσμα από το Fragment Offset = 0.

4.16

Το μήκος του πρώτου θραύσματος είναι 1514 bytes.

4.17

Βλέπουμε ότι δεν πρόκειται για το πρώτο θραύσμα από το Fragment Offset = 1480 (δηλαδή $\neq 0$).

4.18

Ναι, ακολουθούν κι άλλα θραύσματα.

4.19

Φαίνεται ότι ακολουθούν κι άλλα θραύσματα από το More Fragments bit = 1.

4.20

Fragment Offset και Header Checksum

4.21

Κάθε πακέτο εισάγει στο offset: μήκος δεδομένων 1472 bytes και μήκος επικεφαλίδας ICMP 8 bytes, άρα

- Προτελευταίο (4ο πακέτο, έχουν προηγηθεί 3 πακέτα): $3 \times (1472 + 8) = 4440$ bytes
- Τελευταίο (5ο πακέτο, έχουν προηγηθεί 4 πακέτα): $4 \times (1472 + 8) = 5920$ bytes

4.22

Τα πεδία που αλλάζουν μεταξύ των θραυσμάτων είναι: Total Length, Flags, Fragment Offset, Header Checksum.