$3^ο$ Εργαστήριο στα Δίκτυα Υπολογιστών
Ενθυλάκωση και Επικεφαλίδες

Όνοματεπώνυμο: **Αλέξανδρος Κυριακάκης (03112163)**
Ομάδα: **2**
Όνομα PC/ΛΣ: **MacBook Pro - Alexandros, macOS Catalina**
Ημερομηνία: **19/10/2020**
Διεύθυνση IP: **192.168.1.5**
Διεύθυνση MAC: **a4:83:e7:97:af:31**

1 Ο Πίνακας ARP

1.1 Χρησιμοποίησα την εντολή:

```
$ arp -a
```

1.2 Χρησιμοποίησα την εντολή:

```
$ arp -d -a
```

1.3 Βρήκα την IPv4 του υπολογιστή μου **192.168.1.5** με την εντολή:

```
$ ipconfig getifaddr en0
```

Επίσης βρήκα τους εξυπηρετητές DNS **195.170.0.1, 1.1.1.1** με την εντολή:

```
$ networksetup -getdnsservers Wi-Fi
```

1.4 Το περιεχόμενο του ARP Table είναι:

```
? (192.168.1.1) at 94:a7:b7:47:13:ae on en0 ifscope [ethernet]
? (192.168.1.3) at ae:62:3e:29:77:a0 on en0 ifscope [ethernet]
? (192.168.1.5) at a4:83:e7:97:af:31 on en0 ifscope permanent [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

1.5 Υπάρχει η διεύθυνση της προκαθορισμένης πύλης (**192.168.5**) αλλά όχι του DNS εξυπηρετητή (**195.170.0.1, 1.1.1.1**), όμως γνωρίζουμε ότι τα DNS resolves τα κάνει η default gateway.

1.6 Χρησιμοποίησα τη διεύθυνση **192.168.1.1**.

1.7 Το περιεχόμενο του ARP Table είναι:

```
? (192.168.1.1) at 94:a7:b7:47:13:ae on en0 ifscope [ethernet]
? (192.168.1.5) at a4:83:e7:97:af:31 on en0 ifscope permanent [ethernet]
```

Παρατηρώ ότι έχει ληφθεί το MAC Address της διεύθυνσης που έκανα το call.

1.8 Με την εντολή:

```
dscacheutil -flushcache && sudo killall -HUP mDNSResponder && \
sudo arp -d -a && traceroute edu-dy.cn.ntua.gr && arp -a
```

Έχουν καταχωρηθεί οι εξής διευθύνσεις IPv4:

```
? (192.168.1.1) at 94:a7:b7:47:13:ae on en0 ifscope [ethernet]
? (192.168.1.5) at a4:83:e7:97:af:31 on en0 ifscope permanent [ethernet]
```

Υπάρχουν μόνο η καθορισμένη πύλη για τον υπολογιστή μου και η πύλη που υποδεικνύει ο πίνακας δρομολόγισης για ξένα υποδίκτυα.

1.9 Όχι, διότι βρίσκεται σε διαφορετικό υποδίκτυο.

2 Το πλαίσιο Ethernet

2.1 Η τιμή είναι $0x0800$.

2.2 Είναι $0x0806$.

2.3 Είναι $0x86dd$

2.4 Είναι Source: a4:83:e7:97:af:31

2.5 Είναι Destination: 94:a7:b7:47:13:ae

2.6 Όχι δεν είναι.

2.7 Η MAC διεύθυνση ανήκει στο Router του δικτύου που βρίσκομαι. Αυτό συμβαίνει διότι η διεύθυνση edu-dy.cn.ntua.gr βρίσκεται σε διαφορετικό υποδίκτυο οπότε η επικοινωνία γίνεται μέσω του Router.

2.8 Η δεκαεξαδική τιμή του πεδίου Type είναι $0x0800$ και αυτό σημαίνει ότι είναι IPv4.

2.9 Το μήκος του πλαισίου είναι 429 *Bytes*.

2.10 Προηγούνται 66 *Bytes*.

2.11 Είναι Source: 94:a7:b7:47:13:ae (το Router μου)

2.12 Όχι δεν είναι.

2.13 Στο Router μου.

2.14 Είναι Destination: a4:83:e7:97:af:31

2.15 Στον προσωπικό μου υπολογιστή (αναφερόμενο στην αρχή της άσκησης).

2.16 Είναι $0x0800$.

2.17 Είναι 480 *Bytes*

2.18 Προηγούνται 66 *Bytes*.

2.19 Τα Source MAC Address, Destrination MAC Address και Type.

2.20 Το Wireshark δεν μπορεί να κάνει capture τα πακέτα FCS (CRC) και σε αυτό ευθύνεται το λειτουργικό σύστημά μας μαζί με τις βιβλιοθήκες που χρησιμοποιεί το wireshark οι οποίες χρειάζονται ειδικά modifications για να το πετύχουν.

3 Περισσότερα για τα πακέτα ARP

3.1 Απεικονίζει όλα τα πλαίσια που έχουν ως προορισμό ή πηγή την αναγραφόμενη MAC Address.

3.2 Θα απεικονίζει μόνο τα πλαίσια πρωτοκόλου ARP.

3.3 Ανταλλάχθηκαν 2 πακέτα ARP.

3.4 Θα είχε ως αποτέλεσμα να απεικονίζει όλα πακέτα με Src ή Dst την δοσμένη διευθυνση και όλα τα ARP πακέτα που δεν συμπεριλήφθηκαν στην προηγούμενη συνθήκη.

3.5

- Hardware type: 2 *Bytes*
- Protocol type: 2 *Bytes*
- Hardware size: 1 *Byte*
- Protocol size: 1 *Byte*
- Opcode: 2 *Bytes*
- Sender MAC address: 6 *Bytes*
- Sender IP address: 4 *Bytes*
- Target MAC address: 6 *Bytes*
- Target IP address: 4 *Bytes*
- Padding: $64(Minimum) - 18(Ethernet) - 28(ARP) = 18$ *Bytes*

3.6

- Hardware type: Ethernet
- Protocol type: IPv4

3.7 Διότι ο τύπος της διεύθυνσης του πρωτοκόλλου IPv4 είναι (4 *Bytes*).

3.8 Διότι το μέγεθος της διεύθυνσης υλικού Ethernet είναι 6 *Bytes*

3.9 Η διεύθυνση του αποστολέα ανήκει στον υπολογιστή μου, ενώ του παραλήπτη είναι η διεύθυνση εκπομπής (ff:ff:ff:ff:ff:ff) δηλαδή σε όλες τις συνδεδεμένες συσκευές (multicast/broadcast).

3.10 Είναι $0x0806$ και υποδεικνύει το πρωτόκολλο ARP.

3.11

- Source (a4:83:e7:97:af:31): Είναι ατομική μοναδική διεύθυνση.
- Destination (ff:ff:ff:ff:ff:ff): Είναι ομαδική τοπική διευθυνση.

3.12 Αν θεωρήσουμε ότι τα bit του πρώτου εκπεμπόμενου byte της διευθυνσης MAC είναι αριθμημένα ως εξής $0-7$ με 7 το LSB και 0 το MSB, τότε η θέση του πρώτου εκπεμπόμενου bit είναι το 7 και του δεύτερου το 6.

3.13

- ARP: 28 *Bytes*
- Ethernet: 42 *Bytes*

3.14 Προηγούνται 20 bytes.

3.15 Είναι Opcode: request ($0x0001$)

3.16 Στο Sender MAC address.

3.17 Στο Sender IP address.

3.18 Στο Target IP address.

3.19 Υπάρχει το πεδίο Target MAC address που περιέχει τη διεύθυνση: 00:00:00:00:00:00.

3.20 Η διεύθυνση του αποστολέα ανήκει στο Router και του παραλήπτη στον υπολογιστή μου.

3.21 Η τιμή του είναι $0x0806$ και υποδικνύει το πρωτόκολλο ARP.

3.22 Προηγούνται 20 *Bytes*.

3.23 Είναι Opcode: reply ($0x0002$).

3.24 Στο πεδίο Sender IP address.

3.25 Στο πεδίο Sender MAC address.

3.26 Στο πεδίο Target IP address.

3.27 Στο πεδίο Sender MAC address.

3.28

- ARP: 28 *Bytes*
- Ethernet: 42 *Bytes*

3.29 Ναι είναι ίδια. (Είμαι συνδεδεμένος ασύρματα και δεν παρατηρώ το padding που θα χρειαζόταν εως τα 64 bytes).

3.30 Η διαφορά οφείλεται στο γεγονός ότι το Wireshark θα κάνει capture τα πακέτα πριν φτάσουν στο στρώμα ζεύξης όπου και θα αποκτήσουν το απαραίτητο Padding μέχρι τα 64 byte που είναι το ελάχιστο μέγεθος πλαισίου Ethernet. Αντιθέτως, στην απάντηση όπου το padding έχει γίνει από τον αποστολέα θα είναι εμφανές και στο Wireshark.

3.31 Το πεδίο Type: ARP (0x0806).

3.32 Το πεδίο Opcode: reply ($0x0002$)

3.33 Τότε όλοι οι χρήστες του δικτύου θα έστελναν τα πλαίσια τους σε αυτόν τον κακόβουλο χρήστη ο οποίος θα μπορούσε να τα κάνει resolve, αρα οι χρήστες να τον αποθυκεύσουν στο Arp Table τους, και να κάνει την γνωστή επίθεση Man-In-The-Middle(MITM), με αποτέλεσμα να είναι σε κύνδινο τα δεδομένα των χρηστών.