Ονοματεπώνυμο: Χαράλαμπος Καμπουγέρης **Ομάδα:** 3, Τετάρτη 10:45-12:30, Αιθ.Α2

Όνομα PC/ΛΣ: CHARALAMPOSs-MacBook-Air/ macOS 14.0 **Ημερομηνία:** 24/10/2023

Διεύθυνση IP: 192.168.1.27 **Διεύθυνση MAC:** 0c:e4:41:e1:6c:74

Εργαστηριακή Άσκηση 3
Επικοινωνία στο τοπικό δίκτυο
(πλαίσιο Ethernet και πρωτόκολλο ARP)

Άσκηση 1

1.1 Περιεχόμενα πίνακα ARP (CLI): arp -a

1.2 Διαγραφή περιεχομένων πίνακα ARP (CLI): sudo arp -d -a

1.3 Default Gateway: 192.168.1.1 (μέσω της εντολής netstat -rn)
DNS Server: 192.168.1.1 (μέσω της εντολής scutil --dns)

1.4 Περιεχόμενα πίνακα ARP:

```
192.168.1.1 –> 50:78:b3:81:2a:66
192.168.1.27 –> c:e4:41:e1:6c:74
224.0.0.251 –> 1:0:5e:0:0:fb
```

1.5 Ναι υπάρχουν (192.168.1.1 –> 50:78:b3:81:2a:66)

1.6 Άδειασμα πίνακα ARP και ping 224.0.0.251
IPv4: 224.0.0.251

1.7 Παρατηρούμε ότι η συγκεκριμένη διεύθυνση έχει προστεθεί ξανά στον πίνακα ARP

1.8 Στον πίνακα ARP έχει προστεθεί μόνο η IPv4 διεύθυνση 192.168.1.1, δηλαδή η διεύθυνση του Default Gateway και του DNS Server, λόγω της επίσκεψης στη σελίδα lab3 και της αποστολής πακέτων DNS.

1.9 Η διεύθυνση IPv4 του site δεν έχει καταχωρηθεί στον πίνακα ARP καθώς ανήκει σε άλλο υποδίκτυο. Επομένως στον πίνακα έχει καταχωρηθεί η διεύθυνση του Default Gataway η οποία αναλαμβάνει την επικοινωνία μεταξύ των υποδικτύων.

Άσκηση 2

2.1 Καταγράφει τα πεδία πλαισίου Destination, Source, Type

2.2 Όχι δεν έχει καταγραφεί, διότι χρησιμοποιείται μόνο για το συγχρονισμό και δεν αποτελεί μέρος του πλαισίου Ethernet.

2.3 Το λειτουργικό σύστημα δεν αναγνωρίζει το πεδίο CRC/FCS ως μέρος του πλαισίου Ethernet, επομένως δεν μπορεί να καταγραφεί.

2.4 Type: IPv4 (0x0800)

2.5 Type: ARP (0x0806)

2.6 Type: IPv6 (0x86dd)

2.7 MAC Address Source: 0c:e4:41:e1:6c:74

2.8 MAC Address Destination: 50:78:b3:81:2a:66

2.9 Όχι δεν είναι, καθώς δεν ανήκει στο ίδιο υποδίκτυο.

2.10 Ανήκει στο Default Gateway, καθώς όταν ανήκει σε άλλο υποδίκτυο αυτό το gateway αναλαμβάνει να επιλύσει τη διεύθυνση MAC του site.

2.11 Μήκος πλαισίου: 426 bytes

2.12 Προηγούνται 66 bytes

2.13 MAC Address Destination: 50:78:b3:81:2a:66

2.14 Όχι δεν είναι. (για τον ίδιο λόγο με ερώτημα 2.10)

2.15 Ανήκει στο Default Gateway

2.16 MAC Address Source: 0c:e4:41:e1:6c:74

2.17 Ανήκει στον υπολογιστή μου

2.18 590 bytes

2.19 77 bytes

Άσκηση 3

3.1 MAC Address (Source): Είναι μοναδικές (2^{nd} LSB = 0) και ατομικές (LSB = 0)

3.2 MAC Address (Destination): Είναι Ομαδικές (LSB = 1) και τοπικές (2^{nd} LSB = 1)

3.3 Μετάδοση ενός Byte (LSB -> MSB): Το πρώτο bit είναι στη θέση 8 και το επόμενο στη θέση 7. (ξεκινώντας την αρίθμηση από τη θέση 1 όπου και βρίσκεται το MSB)

3.4 MAC Address: Broadcast (ff:ff:ff:ff:ff:ff)

3.5 Παραμένουν τα πλαίσια με πρωτόκολλο STP και πρότυπο Ethernet IEEE 802.3

3.6 Πεδίο Length: Δηλώνει το μήκος σε bytes των δεδομένων που απομένουν εκτός της επικεφαλίδας Ethernet 802.3 και του padding στο τέλος

3.7 Το πρότυπο Ethernet II έχει πεδίο “Type” ενώ το IEEE 802.3 αντικαθιστά αυτό το πεδίο με τα πεδία “Length” και “Padding”

3.8 Έχει μέγεθος 3bytes και περιλαμβάνει τα DSAP, SSAP και Control field

3.9 Μεταφέρουν δεδομένα του πρωτοκόλλου STP (Spanning Tree Protocol) με μέγεθος 36 Bytes

3.10 Έχει μέγεθος 7 bytes και υπάρχει για να εξασφαλίζεται το ελάχιστο μήκος πλαισίου Ethernet.

Άσκηση 4

4.1 eth.addr == 0c:e4:41:e1:6c:74: Μας εμφανίζει μόνο τα πακέτα ethernet που στέλνει ή δέχεται ο υπολογιστής μου

4.2 Απομονώνει μόνο τα πλαίσια ARP από τα αποτελέσματα που έχουν εμφανιστεί λόγω του προηγούμενου φίλτρου

4.3 Ανταλλάχθηκαν 2 πακέτα, ένα request και ένα reply

4.4 Το πεδίο Type (0806)

4.5
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

4.6 Έχει τιμή 0011 (HEX) και είδος κάρτας δικτύου Ethernet (1)

4.7 Έχει τιμή 0800 (HEX) και υποδεικνύει το πρωτόκολλο IPv4

4.8 Το Protocol Type έχει τιμή IPv4 (08 00), ενώ το Ethertype του Ethernet II τιμή ARP (08 06)

4.9 Το Protocol size μας δίνει το μήκος διεύθυνσης IPv4 και για αυτό το λόγο η τιμή του είναι 4 bytes

4.10 Το Hardware size δίνει το μήκος της διεύθυνσης MAC του υπολογιστή που ψάχνει να βρει και για αυτό είναι 6 bytes.

4.11 Ανήκει στον υπολογιστή μου (MAC: 0c:e4:41:e1:6c:74)

4.12 MAC Address: ff:ff:ff:ff:ff:ff (δηλαδή broadcast προς όλες τις κάρτες του τοπικού υποδικτύου)

4.13 Μέγεθος πακέτου ARP: 28 bytes, Μέγεθος πλαισίου Ethernet: 42 bytes

4.14 Προηγούνται 20 bytes

4.15 Τιμή opcode: 00 01 (HEX)

4.16 Στο πεδίο Sender MAC address

4.17 Στο πεδίο Sender IP address

4.18 Στο πεδίο Target IP address

4.19 Ναι υπάρχει η Target MAC address και έχει την τιμή 00:00:00:00:00:00

4.20 Η διεύθυνση MAC του αποστολέα ανήκει στον υπολογιστή προς τον οποίο έγινε το ping ενώ η MAC του παραλήπτη ανήκει στον δικό μου υπολογιστή

4.21 Τιμή opcode: 00 02 (HEX)

4.22 Στο πεδίο Sender IP address

4.23 Στο πεδίο Sender MAC address

4.24 Στο πεδίο Target IP address

4.25 Στο πεδίο Target MAC address

4.26 Το πλαίσιο ethernet έχει μέγεθος 60 bytes, ενώ το ARP reply 28 bytes

4.27 Όχι το πλαίσιο ethernet που μεταφέρει το ARP reply έχει μεγαλύτερο μήκος

4.28 Το πεδίο Opcode που αν είναι 1 είναι request και αν είναι 2 είναι reply

4.29 Η βιβλιοθήκη libpcap έπιασε το ARP reply πριν ενθυλακωθεί μέσα από τη κάρτα δικτύου οπότε δεν έχει trailer, ενώ το request το έπιασε μέσα απο τη καρτα δικτύου και άρα έχει trailer.

4.30 Διαφέρουν στο ότι ένα ARP request πρέπει να έχει την target MAC

address μηδενική καθώς δεν μπορεί να τη ξέρει, ενώ κατά την επιστροφή (reply) αυτή η διεύθυνση έχει προσδιοριστεί στο πεδίο Sender MAC address. Επίσης, διαφέρει το opcode.

4.31 Θα υπήρχαν δύο ARP replies για κάθε request και στο ARP table θα είχαμε δύο MAC διευθύνσεις για κάθε IP στο υποδίκτυο. Οπότε, ό,τι στέλναμε θα το λάμβανε και ο κακόβουλος υπολογιστής