Εθνικό Μετσόβιο Πολυτεχνείο
Δίκτυα Υπολογιστών
Χειμερινό Εξάμηνο 2022-2023
Όνομα:
Ιωάννης Μπασδέκης - 03119198

3η Εργαστηριακή Αναφορά

Μέρος 1ο

1.1) arp -a

1.2) sudo arp -a -d

1.3) Default Gateway: 147.102.200.200 (netstat -nr)
DNS: 147.102.224.243 **(**scutil —dns)

1.4)

```
(base) giannesmpasdekes@MacBook-Air-Giannes ~ % arp -a
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
(base) giannesmpasdekes@MacBook-Air-Giannes ~ % arp -a
? (147.102.200.200) at 8:ec:f5:d0:d9:1d on en0 ifscope [ethernet]
? (147.102.203.255) 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 [ether
(base) giannesmpasdekes@MacBook-Air-Giannes ~ %
```

1.5) Περιέχει του default gateway αλλά όχι του DNS

1.6) 147.102.200.20

1.7) Υπάρχει πλέον η MAC address της IP που κάναμε ping

1.8) Του default gateway

1.9) Όχι γιατί δεν βρίσκεται στο ίδιο υποδίκτυο με τον υπολογιστή μας οπότε απευθυνόμαστε στο default gateway για να μας βρει την MAC address της ιστοσελίδας

Μέρος 2ο

2.1) MAC Destination, MAC Source, Ethertype

2.2) Όχι γιατί πλέον όλα τα ethernet τερματίζουν σε κάποιο είδους switch οπότε ο συγχρονισμός δεν είναι απαραίτητος

2.3) Το libncap (unix), που είναι βιβλιοθήκη του λειτουργικού συστήματος με το οποίο λειτουργεί το wireshark, δεν αναγνωρίζει το CRC

2.4) IPv4: 0x0800

2.5) ARP: 0x0806

2.6) IPv6: 0x86dd

2.7) b0:be:83:20:37:35

2.8) 08:ec:f5:d0:d9:1d

2.9) Όχι

2.10) Είναι του default gateway γιατί εφόσον η διεύθυνση της ιστοσελίδας δεν είναι στο δικό μας υποδίκτυο το MAC address resolve το κανει το default gateway

2.11) 544 bytes

2.12) 66 bytes προηγούνται

2.13) 08:ec:f5:d0:d9:1d

2.14) Όχι

2.15) Default Gateway

2.16) b0:be:83:20:37:35

2.17) Στον δικό μας

2.18) 590 bytes

2.19) 79 προηγούνται

Μέρος 3ο

3.1) Μοναδικές (προηγούμενο bit του LSB= 0), Ατομικές (LSB= 0)

3.2) Ομαδικές (LSB= 1), Μοναδικές (προηγούμενο bit του LSB= 0), Τοπικές (προηγούμενο bit του LSB= 1)

3.3) Πρώτα μεταδίδεται το LSB άρα θα το πρώτο bit (LSB) θα βρίσκεται στην θέση 8 και το αμέσως επόμενο στην θέση 7 (το MSB βρίσκεται στην θέση 1)

3.4) ff:ff:ff:ff:ff:ff

3.5) STP πρωτόκολλα με πρότυπο IEEE 802.3

3.6) Length. Δηλώνει τον αριθμό bytes του πλαισίου χωρις το header και το padding του Ethernet

3.7) Το Ethernet II έχει το πεδίο Type, ενώ το IEEE 802.3 έχει πεδία το length και το padding

3.8) Μέγεθος: 3 bytes Πεδία: DSAP, SSAP, Control Field

3.9) STP πρωτόκολλα με μέγεθος 36 bytes

3.10) Έχει μέγεθος 7 bytes. Υπάρχει γιατί το ελάχιστο μήκος Ethernet πλαισίου σύμφωνα με το IEEE 802.3 πρότυπο είναι 64 bytes οπότε συμπληρώνει τα bytes

Μέρος 4ο

4.1) Εμφανίζει πλαίσια Ethernet που αφορούν την συγκεκριμένη MAC address

4.2) Εμφανίζει μόνο τα ARP πρωτόκολλα

4.3) 2, 1 request + 1 reply

4.4) To Type

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) Τιμή: 0x001, hardware: Ethernet

4.7) Τιμή: 0x0800, IPv4

4.8) Ethertype: ARP, ARP type: IPv4. Το Ethertype μας δηλώνει τι πρωτόκολλο είναι το συγκεκριμένο πλαίσιο και το ARP type μας δηλώνει με τι θέλουμε να βρούμε την MAC address (στην συγκεκριμένη περίπτωση θέλουμε να την βρούμε με IPv4

4.9) Είναι το μήκος της IP που δίνουμε για να βρούμε την MAC address. Στην συγκεκριμένη περίπτωση είναι IPv4 αρα 4 bytes

4.10) Το μήκος της διεύθυνσης που ψάχνουμε. Εδώ είναι MAC address άρα 6 bytes

4.11) Στον υπολογιστή μας

4.12) Το broadcast ff:ff:ff:ff:ff:ff

4.13) ARP request: 28, Ethernet: 42

4.14) 20 bytes

4.15) 0x0001

4.16) Sender MAC address

4.17) Sender IP address

4.18) Target IP address

4.19) Target MAC address

4.20) Αποστολέας: Στην συσκευή που κάναμε ping. Παραλήπτης: η δικιά μας MAC address

4.21) 0x0002

4.22) Sender IP address

4.23) Sender MAC address

4.24) Target IP address

4.25) Target MAC address

4.26) ARP reply: 28, Ethernet: 56

4.27) Όχι

4.28) Το opcode

4.29) Το reply το έπιασε η lipπcap πριν ενθυλακωθεί από την κάρτα δικτύου και δεν έχει το trailer όπως το request που το έπιασε αφού ήρθε στον υπολογιστή μας μέσα απο την κάρτα δικτύου.

4.30) Request:Target MAC address είναι κενό (00:00:00:00:00:00) και επίσης τους διαχωρίζει το opcode

4.31) Θα υπήρχαν 2 reply για κάθε request και στο arp table θα είχαμε 2 MAC address για κάθε IP στο υποδίκτυο, οπότε ό,τι θέλαμε να στείλουμε σε κάποιον (χώρις να είναι στο υποδίκτυο μας αφού έτσι και αλλίως αυτό που θα στείλουμε θα περάσει από το default gateway που είναι στο υποδίκτυό μας) θα το λάμβανε και το κακόβουλος υπολογιστής