

3ο Εργαστήριο Δίκτυα Υπολογιστών
Ονοματεπώνυμο: Βλαχάκης Νικόλαος (el18441) Ομάδα: 4
Όνομα PC/ΛΣ: DESKTOP-91TTTR6, Windows
Ημερομηνία: 27/10/2021
Διεύθυνση IP: 192.168.1.7
Διεύθυνση MAC: 9C-B6-D0-E8-2C-EB

Άσκηση 1)

1.1) arp -a

1.2) arp -d -a

1.3)

Με την εντολή ipconfig/all βρίσκω τόσο την διεύθυνση IPv4 του υπολογιστή μου (192.168.1.7) όσο και τις διευθύνσεις των εξυπηρετητών DNS (192.168.1.1)

1.4)

Internet Address	Physical Address	Type
192.168.1.1	50-78-b3-d0-76-c4	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

1.5) Όπως φαίνεται υπάρχει μόνο διεύθυνση εξυπηρετητή DNS (192.168.1.1)

1.6) 192.168.1.255

1.7)

Internet Address	Physical Address	Type
192.168.1.1	50-78-b3-d0-76-c4	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
239.255.255.250	01-00-5e-7f-ff-fa	static

Παρατηρώ ότι υπάρχει το MAC Address της διεύθυνσης που έκανα κλήση μέσω του command (ping)

1.8) Έχει καταχωρηθεί η 192.168.1.1

1.9) Όχι δεν έχει καταχωρηθεί επειδή βρίσκεται σε διαφορετικό υποδίκτυο.

Άσκηση 2)

2.1) Το Wireshark καταγράφει :

- τα πεδία του Ethernet header , τα οποία περιέχουν destination και source Mac addresses
- το protocol type

2.2) Όχι δεν καταγράφεται το προοίμιο γιατί δεν έχει χρήσιμα data .

2.3) Το CRC δεν υπάρχει στο πλαίσιο Ethernet καθώς δεν το παρέχει by default η βιβλιοθήκη libcap.

2.4) 0x0800

2.5) 0x0806

2.6) 0x86dd

2.7) 9c:b6:d0:e8:2c:eb

2.8) 50:78:b3:d0:76:c4

2.9) Όχι δεν είναι.

2.10)

Η παραπάνω διεύθυνση Mac address ανήκει στους DNS Servers του υπολογιστή μου και πιο συγκεκριμένα στο router του LAN μου . Αυτό γίνεται διότι η διεύθυνση **edu-dy.cn.ntua.gr** βρίσκεται σε διαφορετικό υποδίκτυο οπότε η επικοινωνία γίνεται μέσω του Router.

2.11) 540 Bytes.

2.12) Προηγούνται 54 Bytes.

2.13) 50:78:b3:d0:76:c4

2.14) Όχι δεν είναι.

2.15) Ανήκει στο router του LAN μου .

2.16) 9c:b6:d0:e8:2c:eb

2.17) Η παραπάνω διεύθυνση είναι η MAC adress του υπολογιστή μου.

2.18) 536 Bytes.

2.19) 66 Bytes.

Άσκηση 3)

3.1) Οι διευθύνσεις MAC πηγής των πλαισίων Ethernet είναι ατομικές και μοναδικές .

3.2) Οι διευθύνσεις MAC προορισμού των πλαισίων Ethernet είναι ομαδικές και μοναδικές .

3.3)

θεωρώντας ότι τα bit του πρώτου εκπεμπόμενου Byte της διεύθυνσης MAC είναι αριθμημένα (0 – 7) με 7 το LSB και 0 το MSB, τότε η θέση του πρώτου εκπεμπόμενου bit είναι το 7 και του δεύτερου είναι το 6.

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

3.5) Με το φίλτρο llc παραμένουν μόνο πλαίσια IEEE 802.3

3.6) Το πεδίο μετά τις διευθύνσεις MAC είναι το Length και είναι ένα 7 Bytes πεδίο όπου αποθηκεύει τον αριθμό των Bytes στο πεδίο δεδομένων.

3.7) Τα πλαίσια IEEE 802.3 και Ethernet II ξεχωρίζουν επειδή το Ethernet II έχει πεδίο το Type σε αντίθεση με το IEEE 802.3 που έχει ένα 2-Byte length πεδίο .

3.8) Η LLC επικεφαλίδα περιλαμβάνει τα εξής πεδία : DSAP , SSAP , Control field και έχει μέγεθος 3 Bytes.

3.9) Μεταφέρουν δεδομένα του Spanning Tree Protocol και έχουν μέγεθος 60 Bytes .

3.10) Το padding έχει μέγεθος 7 Bytes και υπάρχει με σκοπό να εξασφαλίζει ότι το data length θα πληρεί πάντα το ελάχιστο μήκος των 46 Bytes.

Άσκηση 4)

4.1) Αυτό το φίλτρο απεικονίζει όλα τα πλαίσια που έχουν ως destination ή source την αναγραφόμενη MAC Address

4.2) Απεικονίζει μόνο τα πλαίσια που έχουν ως πρωτόκολλο , το ARP .

4.3) Ανταλλάχτηκαν 2 πακέτα ARP.

4.4) Τα διαφοροποιεί το πεδίο 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
- Padding: $64(\text{Minimum}) - 14(\text{Ethernet}) - 28(\text{ARP}) = 22 \text{ Bytes}$

4.6) Η τιμή είναι 1 και υποδεικνύει Ethernet.

4.7) Η τιμή είναι 0x0800 και υποδεικνύει IPv4.

4.8) το 0x0800 στο Ethertype αντιστοιχεί σε IPv4 .

4.9) Γιατί ο τύπος της διεύθυνσης του πρωτοκόλλου IPv4 είναι (4 Bytes).

4.10) Γιατί το μέγεθος της διεύθυνσης υλικού Ethernet είναι 6 Bytes.

4.11) Η διεύθυνση του αποστολέα ανήκει στον υπολογιστή μου .

4.12) Η διεύθυνση του παραλήπτη είναι η διεύθυνση εκπομπής (ff:ff:ff:ff:ff:ff) δηλαδή είναι όλες οι συνδεδεμένες συσκευές.

4.13) Το συνολικό μέγεθος του πακέτου ARP είναι 28 Bytes και του πλαισίου Ethernet που το μεταφέρει είναι 14 Bytes.

4.14) 20 Bytes.

4.15) Opcode: request (1)

4.16) Sender MAC address

4.17) Sender IP address

4.18) Target IP address

4.19) Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

4.20) Η διεύθυνση MAC του αποστολέα ανήκει στο Router και του παραλήπτη στον υπολογιστή μου.

4.21) Opcode: reply (2)

4.22) Sender IP address

4.23) Sender MAC address

4.24) Target IP address

4.25) Target MAC address

4.26) Το συνολικό μέγεθος σε byte του πακέτου ARP reply είναι 28 Bytes και του πλαισίου Ethernet είναι 14 Bytes.

4.27) Ναι είναι ακριβώς τα ίδια.

4.28) Η διαφορά έγκυται στο ότι το Wireshark θα κάνει capture τα πακέτα πριν φτάσουν στο στρώμα ζεύξης όπου και θα αποκτήσουν το απαραίτητο Padding μέχρι τα 64 Bytes που είναι το ελάχιστο μέγεθος πλαισίου Ethernet ενώ στην απάντηση όπου το padding έχει γίνει από τον αποστολέα θα φαίνεται και στο Wireshark.

4.29) Το πεδίο Opcode υποδικνύει το κατά πόσον πρόκειται για πακέτο ARP request ή ARP reply .
Opcode: reply (2) Opcode: request (1) , δηλαδή το value του εκάστοτε πεδίου όπως φαίνεται αλλάζει ανάλογα αν είναι reply or response .

4.30) Μια προφανής διαφορά είναι ότι στην μία περίπτωση έχω Sender τον υπολογιστή μου και άγνωστο target ενώ στην άλλη έχω Target τον υπολογιστή μου και Sender την απάντηση που ψάχνω .

4.31) Αυτό που θα γινόταν είναι να έστελναν όλοι οι χρήστες του δικτύου τα πλαίσια τους σε αυτόν και έτσι αυτός θα μπορούσε να τα κάνει resolve, οπότε οι χρήστες να τον αποθηκεύσουν στο ARP Table τους , με αποτέλεσμα να είναι σε κίνδυνο τα δεδομένα των χρηστών.