Όνοματεπώνυμο: Μάρκος Δεληγιάννης		Ομάδα: 3
Όνομα PC/ΛΣ: MarkiniHP / Linux Mint		Ημερομηνία: 19 / 10 / 2022
Διεύθυνση IP: 147 . 102 . 38 . 254	Διεύθυνση MAC:	38 – ea – a7 – d9 – ab – 1a

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

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

Άσκηση 1

1.1 ip -4 neigh

1.2 sudo ip -4 -s neigh flush all

1.3 Default gateway: 147.102.38.200

DNS: 147.102.222.210

Εντολές: ip -4 neigh / ip -4 -r neigh (Για default gateway) & nmcli για DNS

1.4 147.102.38.200 00:00:5e:00:01:25

147.102.38.11 00:0c:29:06:35:c3

147.102.38.5 00:14:38:8d:76:06

.....

1.5 Υπάρχει η διεύθυνση της προκαθορισμένης πύλης (147.102.38.200), αλλά όχι του DNS, όπως είναι λογικό, αφού ο DNS βρίσκεται σε άλλο υποδίκτυο.

1.6 147.102.38.5

1.7 Παρατηρούμε ότι ο πίνακας έχει μόνο entries που αντιστοιχούν στον default gateway και τη διεύθυνση που κάναμε ping.

147.102.38.200 00:00:5e:00:01:25

147.102.38.5 00:14:38:8d:76:06

.....

1.8 Στον πίνακα ARP έχουμε πλέον μόνο τη διεύθυνση του default gateway. Αυτό συμβαίνει διότι κάναμε flush τον πίνακα ARP και ο DNS βρίσκεται σε διαφορετικό υποδίκτυο. Συνεπώς δεν χρειάζεται να γνωρίζουμε την διεύθυνση MAC του, αφού η επικοινωνία γίνεται μέσω του default gateway (του οποίου την MAC χρειαζόμαστε).

1.9 Δεν έχει καταχωρηθεί, διότι ο εξυπηρετητής δεν βρίσκεται στο ίδιο υποδίκτυο με τον υπολογιστή και έτσι δεν χρειαζόμαστε την MAC address του.

Άσκηση 2

2.1 Destination, Source και Type (στο header) και data

.....

.....

2.2 Το προοίμιο δεν έχει καταγραφεί, καθώς δεν αποτελεί μέρος του πακέτου.

.....

2.3 Το CRC επίσης δεν έχει καταγραφεί, καθώς η κάρτα δικτύου (που αναλαμβάνει τον έλεγχο εγκυρότητας) δεν μεταβιβάζει την πληροφορία στο λειτουργικό σύστημα.

.....

2.4 0x0800

2.5 0x0806

2.6 Δεν έχουν καταγραφεί IPv6 πακέτα, είναι γνωστό όμως ότι η τιμή που τους αντιστοιχεί είναι 0x86DD.

2.7 38:ea:a7:d9:ab:1a (Η διεύθυνση MAC της κάρτας δικτύου ethernet του υπολογιστή μας)

2.8 00:00:5e:00:01:25

2.9 Αυτή η διεύθυνση MAC δεν αντιστοιχεί στο edu-dy.cn.ntua.gr.

2.10 Ανήκει στον default gateway, δηλαδή το router του υποδικτύου μας. Αυτό συμβαίνει διότι ο εξυπηρετητής της σελίδας που επισκεφθήκαμε δεν ανήκει στο ίδιο υποδίκτυο με τον υπολογιστή μας και συνεπώς το πλαίσιο προωθείται στον default gateway.

2.11 Το μήκος του πλαισίου σε 465 byte.

2.12 66 bytes

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

2.14 Αυτή η διεύθυνση δεν αντιστοιχεί στο edu-dy.cn.ntua.gr

2.15 Ανήκει στον default gateway του υποδικτύου μας.

2.16 38:ea:a7:d9:ab:1a

2.17 Ανήκει στον υπολογιστή μας.

2.18 603 bytes

2.19 79 bytes

Άσκηση 3

3.1 Όλες οι διευθύνσεις MAC πηγής είναι ατομικές (LSB=0) και μοναδικές (2ο LSB=0).

.....

3.2 Όλες οι διευθύνσεις MAC προορισμού είναι ομαδικές (LSB=1, όπως είναι αναμενόμενο, αφού φιλτράρουμε multicast διευθύνσεις), αλλά κάποιες από τις διευθύνσεις MAC είναι τοπικές (2ο LSB=1) και κάποιες μοναδικές (2ο LSB=0).

3.3 Το πρώτο και δεύτερο bit της διεύθυνσης MAC είναι το πρώτο και δεύτερο LSB του πρώτου byte αντίστοιχα.

3.4 FF:FF:FF:FF:FF:FF

3.5 Παραμένουν τα πλαίσια με Logical Link Control επικεφαλίδες.

3.6 Το πεδίο αυτό δηλώνει το μήκος των δεδομένων σε byte.

3.7 Το μέγιστο μήκος δεδομένων των πλαισίων IEEE 802.3 είναι 1500 byte και όλα τα πλαίσια Ethernet II έχουν τιμές του πεδίου *Τύπος* μεγαλύτερες από 1536 (0x0600). Συνεπώς με σύγκριση του Type με το 0x0600 ξεχωρίζονται τα δύο είδη πλαισίων.

3.8 Η επικεφαλίδα LLC έχει μέγεθος 3 byte και περιλαμβάνει τα πεδία DSAP, SSAP και Control field.

.....

.....

3.9 Τα πλαίσια αυτά μεταφέρουν δεδομένα του πρωτοκόλλου STP και έχουν μέγεθος 60 byte. Τα δεδομένα του πρωτοκόλλου STP έχουν μέγεθος 36 byte.

3.10 Το παραγέμισα έχει μέγεθος 7 byte και υπάρχει διότι το μέγεθος του πλαισίου Ethernet πρέπει να είναι τουλάχιστον 64 byte (60 χωρίς το CRC που δεν εμφανίζεται στο wireshark). Αφού το μήκος του πακέτου ήταν μικρότερο, προστέθηκε padding στο τέλος ώστε να φτάσει στο επιθυμητό μέγεθος.

Άσκηση 4

4.1 Εμφανίζονται μόνο πλαίσια με πηγή ή προορισμό τον υπολογιστή μας (πιο συγκεκριμένα την κάρτα δικτύου ethernet).

4.2 Εμφανίζονται τα πλαίσια του 4.1 στα οποία ενθυλακώνονται πακέτα ARP.

.....

4.3 Ανταλλάχτηκαν 2 πακέτα, μία ερώτηση και μία απάντηση.

4.4 Τα διαφοροποιεί το πεδίο Type της επικεφαλίδας Ethernet (0x0806 για ARP και 0x0800 για IPv4)

4.5 (βλ. σχήμα στο τέλος)

4.6 Η τιμή είναι 1 (0x0001) και αντιστοιχεί σε κάρτα δικτύου Ethernet.

4.7 Η τιμή είναι 0x0800 και αντιστοιχεί στο πρωτόκολλο IPv4.

4.8 Το Ethertype φέρει την πληροφορία για το πρωτόκολλο που έχει ενθυλακωθεί στο πλαίσιο, ενώ η τιμή του Protocol Type υποδεικνύει το πρωτόκολλο για το οποίο έχει χρησιμοποιηθεί το ARP. Για αυτόν τον λόγο οι δύο τιμές διαφέρουν.

4.9 Το Protocol size έχει τιμή ίση με το μέγεθος (σε byte) της διεύθυνσης του Protocol type. Αφού Protocol type = IPv4 και οι διευθύνσεις IPv4 έχουν μήκος 4 byte η τιμή του Protocol size είναι 4.

4.10 Το πεδίο έχει τιμή ίση με το μέγεθος (σε byte) της διεύθυνσης του Hardware type. Αφού Hardware type = Ethernet και οι Ethernet διευθύνσεις έχουν μήκος 6 byte η τιμή του Hardware size είναι 6.

4.11 Η διεύθυνση αυτή (38:ea:a7:d9:ab:1a) αντιστοιχεί στον υπολογιστή μας, ο οποίος κάνει το ARP request.

4.12 Η διεύθυνση παραλήπτη είναι ff:ff:ff:ff:ff:ff, αφού κάνουμε broadcast σε όλες τις συσκευές του υποδικτύου μας.

4.13 Το μέγεθος του πακέτου ARP request είναι 28 byte και το μέγεθος του πλαισίου Ethernet που το μεταφέρει είναι 42 byte (το padding το προσθέτει η κάρτα δικτύου και δεν φαίνεται στο wireshark).

4.14 20 byte

4.15 0x0001 (1)

4.16 Στο πεδίο Sender MAC address.

4.17 Στο πεδίο Sender IP address.

4.18 Στο πεδίο Target IP address.

4.19 Υπάρχει και περιέχει την τιμή 00:00:00:00:00:00

4.20 Η διεύθυνση MAC του αποστολέα (00:00:5e:00:01:25) ανήκει στον υπολογιστή του οποίου την MAC αναζητούσαμε (εν προκειμένω στον default gateway). Η διεύθυνση MAC του παραλήπτη (38:ea:a7:d9:ab:1a) αντιστοιχεί στον υπολογιστή μας.

4.21 0x0002 (2)

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 Sender MAC address.

4.26 Το μέγεθος του πακέτου ARP reply είναι 28 byte και το μέγεθος του πλαισίου Ethernet που το μεταφέρει είναι 60 byte.

.....

4.27 Το μέγεθος του πακέτου ARP είναι το ίδιο και στις δύο περιπτώσεις. Φαινομενικά τα μεγέθη των πλαισίων Ethernet διαφέρουν (48 και 60 bytes) όμως αυτό δεν ισχύει στην πραγματικότητα (αναλυτικότερα στο 4.29).

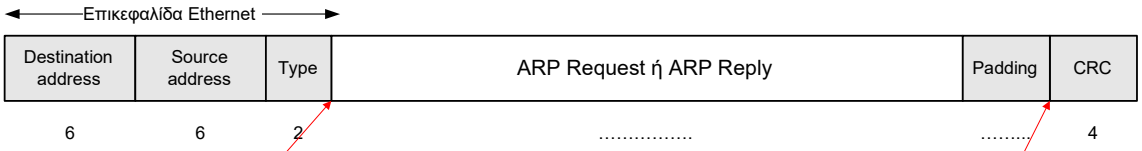
4.28 Το πεδίο opcode, με τιμή 1 για request και 2 για reply.

.....

4.29 Το zero padding για να φτάσει το πλαίσιο ethernet το επιθυμητό μήκος των 64 byte (με το CRC) γίνεται από την κάρτα δικτύου και συνεπώς δεν ανιχνεύεται από το wireshark.

4.30 Η τιμή του opcode είναι διαφορετική, και στο ARP request η διεύθυνση MAC που ζητείται είναι κενή.

4.31 Οι υπολογιστές του δικτύου αρχικά δεν θα μπορούσαν να καταλάβουν ότι ο υπολογιστής είναι κακόβουλος, με αποτέλεσμα πακέτα που δεν αφορούν τον υπολογιστή να αποστέλλονται σε αυτόν. Όταν όμως κάποιος υπολογιστής κάνει αίτημα ARP για δύο διαφορετικές IP διευθύνσεις και λάβει την ίδια MAC διεύθυνση τότε ανιχνεύει τον κακόβουλο υπολογιστή και αυτή η MAC διεύθυνση μαρκάρεται ως αναξιόπιστη.



4 byte

Hardware type:	2 byte
Protocol type:	2 byte
Hardware size:	1 byte
Protocol size:	1 byte
Opcode:	2 byte
Sender MAC address:	6 byte
Sender IP address:	4 byte
Target MAC address:	6 byte
Target IP address:	4 byte