LAB-03 (Ethernet, ARP)

Ex. 1 | ARP table

1.1 | Περιεχόμενα πίνακα ARP
(CLI) `arp -a`

1.2 | Διαγραφή περιεχομένων πίνακα ARP
(CLI) `arp -d` / `arp -d *` (Με δικαιώματα admin)

1.3 | Διευθύνσεις IPv4 default gateway, DNS
Default Gateway : 192.168.1.1, DNS Server : 192.168.1.1 (με την εντολή `ipconfig /all`

1.4 | Περιεχόμενα ARP table
192.168.1.1 → 50-78-b3-cd-48-fa
192.168.1.5 → 38-8b-59-7a-76-80
192.168.1.255 → ff-ff-ff-ff-ff-ff
224.0.0.22 → 01-00-5e-00-00-16
239.255.255.250 → 01-00-5e-7f-ff-fa

1.5 | Επικοινωνία υπολογιστή με gateway
Ναι υπάρχουν : 192.168.1.1 → 50-78-b3-cd-48-fa

1.6 | Άδειασμα ARP table και Ping 192.168.1.5
IPv4 address : 192.168.1.5

1.7 | Καταγραφή ARP table
Παρατηρούμε ότι η διεύθυνση που κάναμε ping ξαναεμφανίστηκε στο πίνακα ARP

1.8 | Ποιές διευθύνσεις IPv4 έχουν καταχωρηθεί
Έχουν καταχωρηθεί : η διεύθυνση που κάναμε ping στο ερώτημα 1.7 (192.168.1.5) διότι ανήκει στο τοπικό υποδίκτυο και στείλαμε πακέτα ping και η διευθύνσεις των DNS server και Default Gateway (192.168.1.1) λόγω της επίσκεψης στη σελίδα του lab3 και της αποστολής πακέτων DNS.

1.9 | Καταχώρηση της IPv4 του ...ntua.gr
Όχι δεν έχει καταχωρηθεί γιατί η IPv4 διεύθυνση ανήκει σε άλλο υποδίκτυο και επομένως στο πίνακα θα καταχωρηθεί η διεύθυνση του gateway (πύλη) η οποία αναλαμβάνει την επικοινωνία μεταξύ των υποδικτύων.

Ex. 2 | Ethernet packet

2.1 | Πεδία πλαισίου Ethernet (Wireshark)
Καταγράφει τα : Destination, Source, Type και Data (IP, ARP, etc)

2.2 | Καταγραφή προοιμίου
Όχι, δέν έχει καταγραφεί. Γιατί χρησιμοποιείται μόνο για τον συγχρονισμό και δεν αποτελεί μέρος του πλαισίου Ethernet

2.3 | Πεδίο CRC (η FCS)
Το λειτουργικό σύστημα δεν αναγνωρίζει το πεδίο CRC/FCS ως μέρος του πλαισίου Ethernet και επομένως η βιβλιοθήκη Npcap δεν μπορεί να το διαβάσει

2.4 | Τιμή πεδίου Type για IPv4
Τιμή Type : 08 00 (HEX)

DIRECTORY

DICTIONARY

ARP (Address Resolution Protocol)
Πρωτόκολλο το οποίο βρίσκει τη MAC address μίας συσκευής στο υποδίκτυο, γνωρίζοντας την IP του.

2.5 | Τιμή πεδίου Type για ARP
Τιμή Type : 08 06 (HEX)

2.6 | Τιμή πεδίου Type για IPv6
Τιμή Type : 86 dd (HEX)

2.7 | MAC of source
MAC Address (Source) : 7C 2A 31 40 C9 AF

2.8 | MAC of destination
MAC Address (Destination) : 74 9D 79 32 3F 90

2.9 | Διεύθυνση ιστοσελίδας
Οχι, δεν είναι !

2.10 | Που ανήκει η διεύθυνση MAC
Ανήκει στο Gateway (δρομολογητή), διότι όταν η διεύθυνση ανήκει σε διαφορετικό υποδίκτυο την επίλυση διευθύνσεων MAC αναλαμβάνει ο τοπικός δρομολογητής

2.11 | Μήκος πλαισίου
Μήκος πλαισίου : 397 Bytes

2.12 | Bytes πριν το payload (Data)
Προηγούνται : 397 (Συνολικά) - 343 (Payload) = 54 Bytes

2.13 | MAC of source
MAC Address (Source) : 74 9D 79 32 3F 90

2.14 | Είναι η διεύθυνση του edu-dy.cn.ntua.gr ?
Οχι, δεν είναι και πάλι !

2.15 | Σε ποιά διεύθυνση ανήκει ?
Ανήκει στο Gateway (δρομολογητή)

2.16 | MAC of destination
MAC Address (Destination) : 7C 2A 31 40 C9 AF

2.17 | Που ανήκει ?
Ανήκει στο υπολογιστή μου (ειναι η MAC της κάρτας δικτύου μου)

2.18 | Μήκος πλαισίου (HTTP response)
Μήκος πλαισίου : 536 Bytes

2.19 | Bytes πριν το payload (Data)
Προηγούνται : 536 (συνολικά) - 482 (Payload) = 54 Bytes

Ex. 3 | More Ethernet

3.1 |
MAC Address (Source) : Είναι Ατομικές (LSB=0) και Παγκόσμιες/Μοναδικές (2nd LSB=0)

3.2 | Είδος MAC Address (Source)
MAC Address (Destination) : Είναι Ομαδικές (LSB=1) και Τοπικές (2nd LSB=1)

3.3 | Θέση 2 πρώτων bits στη MAC
Μετάδοση ενός Byte (LSB → MSB) : Άρα το πρώτο bit (MSB) θα είναι στη θέση 8 και το επόμενο στη θέση 7.

3.4 | MAC Address για broadcast
MAC Address of broadcast (Destination) : ff:ff:ff:ff:ff:ff (όλα 1)

3.5 | Φίλτρο `llc`
Μένουν μόνο τα STP πλαίσια με πρότυπο Ethernet IEEE 802.3

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

3.7 | IEEE 802.3 vs. Ethernet II
Το πρώτυπο Ethernet II έχει το πεδίο "Type" ενώ το IEEE 802.3 αντικαθιστά αυτό το πεδίο με τα "Length" και "Padding"

3.8 | Logical Link Control (LLC)
Έχει μήκος 3 bytes και περιλαμβάνει τα DSAP, SSAP και Control field

3.9 | Δεδομένα ποιού πρωτοκόλλου ?
Μεταφέρουν δεδομένα του πρωτοκόλλου STP (Spanning Tree Protocol) με μέγεθος 36 Bytes

3.10 | Μέγεθος padding
Έχει μέγεθος 7 bytes και υπάρχει για να εξασφαλίζει το ελάχιστο μήκος πλαισίου Ethernet

Ex. 4 | ARP

4.1 | Φίλτρο `eth.addr == 7C:2A:31:40:C9:AF`
Εμφανίζει όλα τα πακέτα όπου η MAC της κάρτας του υπολογιστή μου ταυτίζεται με τη source ή destination των πλαισίων ethernet

4.2 | Φίλτρο `and arp`
Απομονώνει μόνο τα πλαίσια ARP από τα αποτελέσματα του προηγούμενου φίλτρου

4.3 | Πακέτα για `ping 192.168.1.1`
Ανταλάχτηκαν 2 πακέτα (1 request, 1 reply)

4.4 | Πεδίο διαφοροποίησης από IPv4
Το πεδίο Type (08 06), το οποίο υποδηλώνει το πρωτόκολλο ανώτερου επιπέδου

4.5 | Πακέτο ARP (Address Resolution Protocol)
1. Hardware Type → 2 bytes
2. Protocol Type → 2 bytes
3. Hardware size → 1 byte
4. Protocol size → 1 byte
5. Opcode → 2 bytes
6. Sender MAC Address → 6 bytes
7. Sender IP Address → 4 bytes
8. Targer MAC Address → 6 bytes
9. Target IP Address → 4 bytes

4.6 | Πεδίο Hardware Type
Έχει τιμή 00 01 (HEX) και είδος κάρτας δικτύου Ethernet (1)

4.7 | Πεδίο Protocol Type
Έχει τιμή 08 00 (HEX) και υποδεικνύει το πρωτόκολλο IPv4

4.8 | Protocol Type & Ethertypes
Το Protocol Type εχει τιμή IPv4 (08 00), ενώ το Ethertype του Ethernet II τιμή ARP (08 06)

4.9 | Protocol size
Υποδηλώνει το μήκος σε bytes της IP διεύθυνσης που πρέπει να "μεταφραστεί" (IPv4), άρα 4 bytes.

4.10 | Hardware size
Υποδηλώνει το μήκος σε bytes της MAC διεύθυνσης που ψάχνει να βρει, άρα 6 bytes

4.11 | Διεύθυνση MAC αποστολέα
Ανήκει στον υπολογιστή μου (`7C:2A:31:40:C9:AF`)

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

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

4.14 | Bytes πριν το opcode
Προηγούνται 20 bytes

4.15 | Τιμή opcode
Τιμή opcode : 00 01 (HEX)

4.16 | Πεδίο sender MAC
Στο πεδίο "Sender MAC address"

4.17 | Πεδίο sender IPv4
Στο πεδίο "Sender IP address"

4.18 | Πεδίο target IPv4
Στο πεδίο "Target IP address"

4.19 | Πεδίο target MAC
Ναι υπάρχει η "Target MAC address" και έχει τιμή `00:00:00:00:00:00` (δηλαδή όλα 0)

4.20 | MAC of receiver, sender
Η MAC αποστολέα ανήκει στη συσκευή που κάναμε ping (`74:9d:79:32:3f:90`) και του παραλήπτη στη κάρτα δικτύου του υπολογιστή μου (`7C:2A:31:40:C9:AF`)

4.21 | Τιμή opcode
Τιμή opcode : 00 02 (HEX)

4.22 | Πεδίο sender IPv4
Στο πεδίο "Target IP address" (για αποστολέα ίδιο με το προηγούμενο πλαίσιο)

4.23 | Πεδίο sender MAC
Στο πεδίο "Target MAC address" (για αποστολέα ίδιο με το προηγούμενο πλαίσιο)

4.24 | Πεδίο target IPv4
Στο πεδίο "Sender IP address" (για παραλήπτη ίδιο με το προηγούμενο πλαίσιο)

4.25 | Πεδίο target MAC
Στο πεδίο "Sender MAC address" (για παραλήπτη ίδιο με το προηγούμενο πλαίσιο)

4.26 | Μέγεθος πακέτου ARP
Μέγεθος πακέτου ARP : 28 bytes, Μέγεθος πλαισίου Ethernet : 60 bytes (42 bytes όταν από WiFi)

4.27 | vs. 4.13
Όχι, το πλαίσιο ethernet στο reply είναι μεγαλύτερο

4.28 | Διαφορετικό μήκος πλαισίου
Προκύπτει λόγω του "Trailer" πεδίου που προστείθεται στο τέλος (ώστε να

πληρείται το ελάχιστο των 64 bytes) το οποίο όμως η βιβλιοθήκη npcap δεν καταγράφει για τα ARP request πακέτα

4.29 | Πεδιο request / reply
Το πεδίο "Opcode"

4.30 | Άλλες διαφορές
Συνολικά, το πεδίο "Trailer" στο reply, τη τιμή του opcode και τη κενή target MAC address στο request

4.31 | Κακόβουλος υπολογιστής
Θα υπήρχαν για κάθε ARP request δύο ARP responses και σε πολλές περιπτώσεις/θέσεις στο ARP table θα ήταν αποθηκευμένος ο κακόβουλος υπολογιστής και τα μηνύματα θα στέλνονταν σε αυτόν.