

Όνοματεπώνυμο: Νίκος Μπέλλος			Ομάδα: 3
Όνομα PC/ΛΣ: BELLOS-DELL-G3 / Windows OS		Ημερομηνία: 28 / 10 / 2021	
Διεύθυνση IP: 192.168 . 1 . 7		Διεύθυνση MAC: 7C - 2A - 31 - 40 - C9 - AF	

## 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 (CLI) `arp -a`.....
- 1.2 (CLI) `arp -d / arp -d *` (Με δικαιώματα admin).....
- 1.3 Default Gateway : 192.168.1.1, DNS Server : 192.168.1.1 (με την εντολή `ipconfig /all`)  
.....  
.....
- 1.4 192.168.1.1 → 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 Ναι υπάρχουν : 192.168.1.1 → 50-78-b3-cd-48-fa  
.....
- 1.6 IPv4 address : 192.168.1.5  
.....
- 1.7 Παρατηρούμε ότι η διεύθυνση που κάναμε ping ξαναεμφανίστηκε στο πίνακα ARP  
192.168.1.1 → 50-78-b3-cd-48-fa  
192.168.1.5 → 38-8b-59-7a-76-80  
.....
- 1.8 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 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.  
.....

#### Άσκηση 2

- 2.1 Καταγράφει τα : Destination, Source, Type και Data (IP, ARP, etc)  
.....  
.....
- 2.2 Όχι, δεν έχει καταγραφεί. Γιατί χρησιμοποιείται μόνο για τον συγχρονισμό και δεν αποτελεί μέρος του πλαισίου Ethernet  
.....
- 2.3 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 Type : 08 00 (HEX)
- 2.5 Τιμή Type : 08 06 (HEX)
- 2.6 Τιμή Type : 86 dd (HEX)
- 2.7 MAC Address (Source) : 7C 2A 31 40 C9 AF
- 2.8 MAC Address (Destination) : 74 9D 79 32 3F 90
- 2.9 Όχι, δεν είναι !
- 2.10 Ανήκει στο Gateway (δρομολογητή), διότι όταν η διεύθυνση ανήκει σε διαφορετικό υποδίκτυο την επίλυση διευθύνσεων MAC αναλαμβάνει ο τοπικός δρομολογητής
- 2.11 Μήκος πλαισίου : 397 Bytes
- 2.12 Προηγούνται : 397 (Συνολικά) - 343 (Payload) = 54 Bytes
- 2.13 MAC Address (Source) : 74 9D 79 32 3F 90
- 2.14 Όχι, δεν είναι και πάλι !
- 2.15 Ανήκει στο Gateway (δρομολογητή)
- 2.16 MAC Address (Destination) : 7C 2A 31 40 C9 AF
- 2.17 Ανήκει στο υπολογιστή μου (είναι η MAC της κάρτας δικτύου μου)
- 2.18 Μήκος πλαισίου : 536 Bytes
- 2.19 Προηγούνται : 536 (συνολικά) - 482 (Payload) = 54 Bytes

### Άσκηση 3

- 3.1 Παγκόσμιες/Μοναδικές (2nd LSB=0)
- 3.2 MAC Address (Destination) : Είναι Ομαδικές (LSB=1) και Τοπικές (2nd LSB=1)
- 3.3 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 of broadcast (Destination) : ff:ff:ff:ff:ff:ff (όλα 1)
- 3.5 Μένουν μόνο τα STP πλαίσια με πρότυπο Ethernet IEEE 802.3
- 3.6 Δηλώνει το μήκος σε bytes των δεδομένων που μένουν εκτός της επικεφαλίδας Ethernet 802.3 και του padding στο τέλος
- 3.7 Το πρότυπο Ethernet II έχει το πεδίο "Type" ενώ το IEEE 802.3 αντικαθιστά αυτό το πεδίο με τα "Length" και "Padding"
- 3.8 Έχει μήκος 3 bytes 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 εξασφαλίζει το ελάχιστο μήκος πλαισίου Ethernet

### Άσκηση 4

- 4.1 Εμφανίζει όλα τα πακέτα όπου η MAC της κάρτας του υπολογιστή μου ταυτίζεται με τη source ή destination των πλαισίων ethernet
- 4.2 Απομονώνει μόνο τα πλαίσια ARP από τα αποτελέσματα του προηγούμενου φίλτρου

- 4.3 Ανταλλάχθηκαν 2 πακέτα (1 request, 1 reply)
- 4.4 Το πεδίο Type (08 06), το οποίο υποδηλώνει το πρωτόκολλο ανώτερου επιπέδου
- 4.5 ..... (χρησιμοποιήσετε το σχήμα στο τέλος)
- 4.6 Έχει τιμή 00 01 (HEX) και είδος κάρτας δικτύου Ethernet (1)
- 4.7 Έχει τιμή 08 00 (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 Υποδηλώνει το μήκος σε bytes της IP διεύθυνσης που πρέπει να "μεταφραστεί" (IPv4), άρα 4 bytes.
- .....
- 4.10 Υποδηλώνει το μήκος σε bytes της MAC διεύθυνσης που ψάχνει να βρει, άρα 6 bytes
- .....
- 4.11 Ανήκει στον υπολογιστή μου (7C:2A:31:40:C9:AF)
- 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 τιμή 00:00:00:00:00:00 (δηλαδή όλα 0)
- 4.20 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 : 00 02 (HEX)
- 4.22 Στο πεδίο "Target IP address" (για αποστολέα ίδιο με το προηγούμενο πλαίσιο)
- 4.23 Στο πεδίο "Target MAC address" (για αποστολέα ίδιο με το προηγούμενο πλαίσιο)
- 4.24 Στο πεδίο "Sender IP address" (για παραλήπτη ίδιο με το προηγούμενο πλαίσιο)
- 4.25 Στο πεδίο "Sender MAC address" (για παραλήπτη ίδιο με το προηγούμενο πλαίσιο)
- 4.26 Μέγεθος πακέτου ARP : 28 bytes, Μέγεθος πλαισίου Ethernet : 60 bytes (42 bytes όταν από WiFi)
- .....
- 4.27 Όχι, το πλαίσιο ethernet στο reply είναι μεγαλύτερο
- 4.28 Προκύπτει λόγω του "Trailer" πεδίου που προστείνεται στο τέλος (ώστε να πληρείται το ελάχιστο των 64 bytes) το οποίο όμως η βιβλιοθήκη pcap δεν καταγράφει για τα ARP request πακέτα
- .....
- 4.29 Το πεδίο "Opcode"
- 4.30 Συνολικά, το πεδίο "Trailer" στο reply, τη τιμή του opcode και τη κενή target MAC address στο request
- 4.31 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.
- .....
- .....

