Ονοματεπώνυμο: Παναγιώτης Σταματόπουλος	**Ομάδα:** 6
Όνομα PC/ΛΣ: TakisAsus/Windows 10	**Ημερομηνία:** 22/10/23
Διεύθυνση IP: 192.168.2.2	**Διεύθυνση Mac:** D4-5D-64-59-27-5F

AM: el20096

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

Άσκηση 1:

*Στον προσωπικό υπολογιστή

1.1: arp -a

1.2: arp -d

1.3: Default Gateway: 192.168.2.1
DNS Server: 192.168.2.1
ipconfig /all

1.4: Το περιεχόμενο του πίνακα ARP:

Ethernet Virtual box:

Ethernet adapter Ethernet:

```
Interface: 192.168.56.1 --- 0x5
  Internet Address      Physical Address      Type
  192.168.56.255        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

Interface: 192.168.2.2 --- 0xe
  Internet Address      Physical Address      Type
  192.168.2.1           8c-dc-02-cf-1f-ac     dynamic
  192.168.2.255         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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

1.5: Ναι, η προκαθορισμένη πύλη συμπίπτει με τον εξυπηρετητή DNS και φαίνεται στον πίνακα

1.6: Μόνο το default gateway 192.168.2.1 φέρνει απάντηση

1.7: Συμπληρώθηκε ξανά η φυσική διεύθυνση στον πίνακα

1.8: Το default gateway 192.168.2.1 καθώς ο εξυπηρετητής της σχολής βρίσκεται σε διαφορετικό υποδίκτυο από τον υπολογιστή μου, επομένως η επικοινωνία γίνεται μέσω της 192.168.2.1

1.9: Όχι, γιατί ο server βρίσκεται σε διαφορετικό υποδίκτυο

Άσκηση 2:

*Στον προσωπικό υπολογιστή

2.1: Destination MAC address, Source MAC address και Ethertype
2.2: Όχι, γιατί δεν είναι μέρος του frame
2.3: Το λειτουργικό σύστημα των Windows δεν υποστηρίζει την καταγραφή FCS ενός frame, επομένως δεν καταγράφεται στο Wireshark πεδίο CRC
2.4: Type: IPv4 (0x0800)
2.5: Type: ARP (0x0806)
2.6: Δεν καταγράφηκαν
2.7: Source MAC Address: D4-5D-64-59-27-5F (Του υπολογιστή μου)
2.8: Destination MAC Address: 8C-DC-02-CF-1F-AC
2.9: Δεν είναι η MAC Address της σελίδας
2.10: Ανήκει στην MAC Address του Default Gateway/ DNS Server (δηλαδή του router μου), γιατί η σελίδα δεν ανήκει στο ίδιο υποδίκτυο με τον υπολογιστή μου
2.11: 493 bytes
2.12: 54 bytes
2.13: Source MAC Address: 8C-DC-02-CF-1F-AC
2.14: Όχι
2.15: Είναι η ίδια με την ερώτηση 2.10, δηλαδή του router μου, καθώς μέσω αυτού επιστρέφεται η απάντηση
2.16: Destination MAC Address: D4-5D-64-59-27-5F
2.17: Στον υπολογιστή μου
2.18: 584 bytes
2.19: 67 bytes

Άσκηση 3:

*Χρησιμοποιώ το αρχείο http://edu-dy.cn.ntua.gr/lab3.pcap

3.1: Είναι όλες ατομικές και παγκοσμίως μοναδικές

3.2: Όλες είναι ομαδικές, αλλά κάποιες είναι τοπικές και άλλες μοναδικές

3.3: Η μετάδοση των byte γίνεται από τα αριστερά προς τα δεξιά και για κάθε byte από το LSB στο MSB, επομένως το πρώτο bit της MAC address θα είναι στη θέση 8 και το δεύτερο στη θέση 7

3.4: FF-FF-FF-FF-FF-FF

3.5: Μένουν μόνο πλαίσια με πρότυπο IEEE 802.3 Ethernet

3.6: Το πεδίο Length δηλώνει το μήκος των δεδομένων

3.7: Στο πρότυπο IEEE 802.3 Ethernet μετά τις MAC addresses υπάρχουν τα πεδία Length και Padding, ενώ στην Ethernet II το πεδίο Type

3.8: 3 bytes, DSAP, SSAP, Control field

3.9: Spanning Tree Protocol, 36 bytes

3.10: 7 bytes, ώστε τα πλαίσια να φτάσουν το ελάχιστο απαραίτητο μήκος

Άσκηση 4:

*Στον προσωπικό υπολογιστή

4.1: Εμφανίζονται μόνο τα πακέτα με destination ή source address τη MAC address του υπολογιστή μου

4.2: Εμφανίζονται μόνο τα πακέτα του ερωτήματος 4.1 που έχουν πρωτόκολλο ARP

4.3: 2 πακέτα, 1 request και 1 reply

4.4: 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

4.6: 0001 (HEX) και υποδεικνύει κάρτα δικτύου Ethernet

4.7: 0800 (HEX) και υποδεικνύει πρωτόκολλο IPv4

4.8: Το Protocol Type αναφέρεται στο πρωτόκολλο του Network Layer, ενώ το Ether Type στο Data Link Layer

4.9: Το Protocol Size δηλώνει το μήκος των διευθύνσεων σε bytes που χρησιμοποιεί το πρωτόκολλο που δηλώνει το Protocol Type, δηλαδή για IPv4 είναι 4

4.10: Το Hardware Size δηλώνει το μήκος των διευθύνσεων σε bytes που χρησιμοποιεί το υλικό της κάρτας δικτύου που δηλώνει το Hardware Type, δηλαδή για Ethernet είναι 6

4.11: Στον υπολογιστή μου

4.12: ff:ff:ff:ff:ff:ff

4.13: 28 bytes ARP request, 42 bytes πλαισίου Ethernet

4.14: 20 bytes

4.15: request 0001 (HEX)

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
4.20: Η διεύθυνση αποστολέα είναι η MAC Address του router μου και παραλήπτη είναι του υπολογιστή μου
4.21: reply 0002 (HEX)
4.22: Sender IP Address
4.23: Sender MAC Address
4.24: Target IP Address
4.25: Sender MAC Address
4.26: 28 bytes ARP reply, 60 bytes πλαισίου Ethernet
4.27: Όχι, το πλαίσιο Ethernet στο reply είναι μεγαλύτερο
4.28: Το πεδίο Opcode (1 request, 2 reply)
4.29: Το Wireshark συλλαμβάνει τα πακέτα που στέλνει ο υπολογιστής πριν τη μετάδοση, πριν δηλαδή προστεθεί το Padding σε αυτά
4.30: Στη συγκεκριμένη περίπτωση παρατηρούμε διαφορά στις MAC διευθύνσεις target και sender, καθώς στο request ψάχνουμε την διεύθυνση, επομένως το πεδίο Target MAC Address παίρνει την τιμή 00:00:00:00:00:00. Επίσης στο πλαίσιο Ethernet του ARP request η destination MAC address παίρνει την τιμή FF:FF:FF:FF:FF:FF γιατί γίνεται broadcast σε όλες τις συσκευές για να απαντήσει εκείνη της οποίας η IP Address ταυτίζεται με το Target IP Address του αιτήματος
4.31: Θα καταγραφόταν η MAC Address του κακόβουλου υπολογιστή σαν Target MAC Address για τη συγκεκριμένη IP Address, με αποτέλεσμα ό,τι πακέτο αποστέλλεται σε αυτήν την IP διεύθυνση να παραλαμβάνεται από τον κακόβουλο υπολογιστή.