Εργαστηριακή Άσκηση 3 Επικοινωνία στο Τοπικό Δίκτυο

Θοδωρής Φρίξος Παπαρρηγόπουλος
el18040
21/10/2021
Ομάδα 4η.
Ipv6: 2a02:587:4f0e:2b65:34b0:9e4a:d912:2f8a
MAC: 40-1C-83-38-F7-20
Λειτουργικό: Windows
DESKTOP-1403ER3

Άσκηση 1

1.1) > arp -a

1.2) > arp -d * (me administrator rights)

1.3) με > ipconfig /all
IPv4 Address. . . . . : 192.168.1.8
DNS Servers . . . . : fe80::1%2
                                     192.168.1.1
                                     192.168.1.1

1.4)
Interface: 192.168.1.8 --- 0x2

Internet Address	Physical Address	Type
192.168.1.1	38-02-de-f8-09-a0	dynamic
192.168.1.7	d4-1b-81-56-39-61	dynamic
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

1.5) Γνωρίζουμε ότι τα DNS resolves τα κάνει η default gateway συνεπώς δεν βλέπουμε τον DNS εξυπηρετητή παρά την ταύτιση με το default gateway.

1.6)
> ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms

1.7) Υπάρχουν λιγότερες διευθύνσεις

Interface: 192.168.1.8 --- 0x2

Internet Address	Physical Address	Type
192.168.1.1	38-02-de-f8-09-a0	dynamic
224.0.0.22	01-00-5e-00-00-16	static
239.255.255.250	01-00-5e-7f-ff-fa	static

1.8)

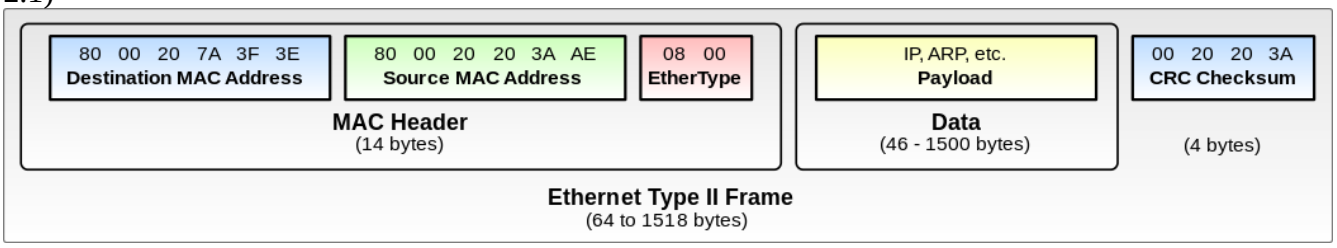
Interface: 192.168.1.8 --- 0x2

Internet Address	Physical Address	Type
192.168.1.1	38-02-de-f8-09-a0	dynamic
224.0.0.22	01-00-5e-00-00-16	static

1.9) Όχι καθώς είναι σε διαφορετικό subnet

Άσκηση 2

2.1)



Μας δείχνει όλο το MAC Header.

2.2)Όχι δεν έχει καταγραφεί καθώς δεν είναι μέρος του πλαισίου Ethernet.
2.3) Το Wireshark δεν μπορεί να κάνει capture τα πακέτα CRC και σε αυτό ευθύνεται το λειτουργικό σύστημά μας μαζί με τις βιβλιοθήκες που χρησιμοποιεί το wireshark οι οποίες χρειάζονται ειδικά modifications για να το πετύχουν.
2.4) 0x0800
2.5) 0x0806
2.6) 0x86dd
2.7) 40:1c:83:38:f7:20
2.8) 38:02:de:f8:09:a0
2.9) Όχι δεν είναι.
2.10) Η MAC διευθυνση ανήκει στο Router του δικτύου που βρίσκομαι. Αυτό συμβαίνει καθώς η διεύθυνση αυτή βρίσκεται σε διαφορετικό υποδίκτυο οπότε η επικοινωνία γίνεται μέσω router.
2.11) 493 bytes
2.12) 493 – 439 = 54 bytes
2.13) 38:02:de:f8:09:a0
2.14) Όχι δεν είναι
2.15) Στο Router
2.16) 40:1c:83:38:f7:20
2.17) Είναι του υπολογιστή μου
2.18) 536 bytes
2.19) 536 – 482 = 54 bytes

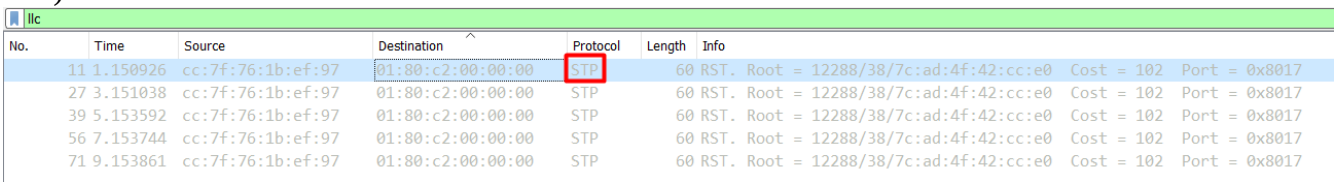
Άσκηση 3

3.1)

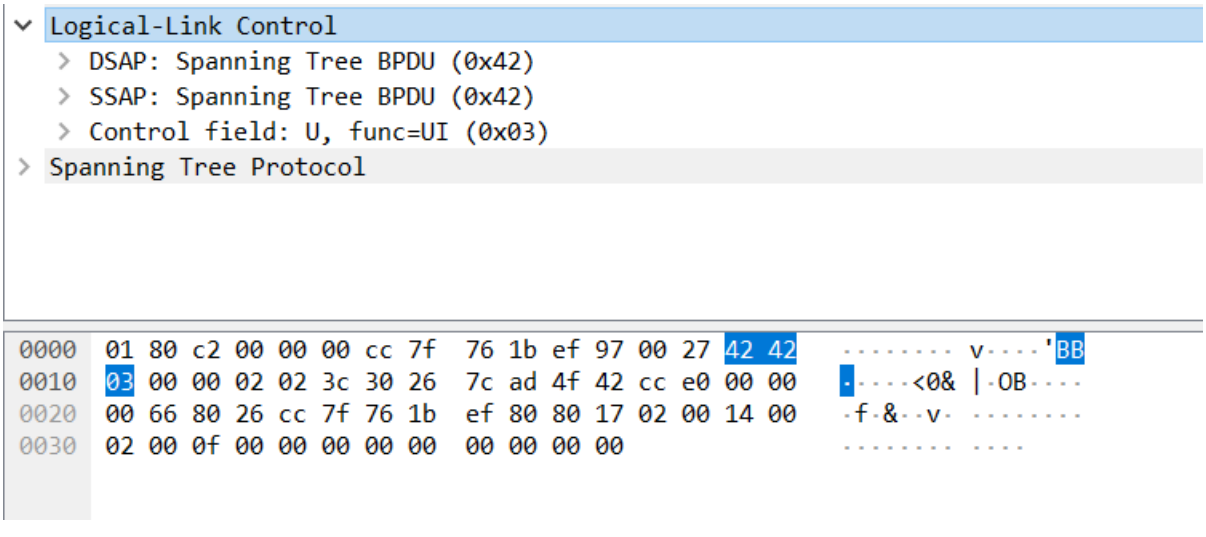
```
Source: 78:45:c4:25:f6:8a
   Address: 78:45:c4:25:f6:8a
   .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
   .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
```

Παρατηρώ πως στο 2ο byte και τα 2 LSB είναι 0, δηλώνουνε δηλαδή μοναδική και ατομική MAC address

3.2) Παρατηρώ πως στο 2ο byte και τα 2 LSB είναι 1, και δηλώνουνε τοπική και ομαδική MAC address. Συγκεκριμένα, παρατηρούμε ότι αποτελείται αποκλειστικά από άσσους και άρα αναφέρεται σε broadcast
3.3) Εμφανίζεται στο LSB του πρώτου byte αριστερά.
3.4) ff:ff:ff:ff:ff
3.5) STP πλαίσια



3.6) Είναι το πεδίο length για το μήκος των δεδομένων
3.7) Για Ethernet II το πεδίο type έχει τιμή πάνω από 1536, ενώ <= 1500 για Ethernet IEEE 802.3
3.8)



Είναι μέγεθος 3 byte και περιέχει τα πεδία DSAP, SSAP, Control Field
3.9) Τα πλαίσια IEEE 802.3 μεταφέρουν πλάισια του STP και έχουν μέγεθος 60 bytes
3.10) Το padding έχει μέγεθος 7 bytes και υπάρχει καθώς το πακέτο που ενθυλακώνονται έχουν μέγεθος 39 bytew ενώ το ελάχιστο είναι 46 και για το λόγο αυτό κάνει pad με 7 bytes (39 + 7 = 46)

Άσκηση 4

4.1) Απεικονίζει όλα τα πλαίσια που έχουν ως προορισμό ή πηγή την αναγραφόμενη MAC Address.
4.2) Θα απεικονίζει μόνο τα πλαίσια πρωτοκόλου ARP που έχουν προορισμό ή πηγή τον υπολογιστή μου.
4.3) 6 πακέτα ARP

eth.addr == 40:1c:83:38:f7:20 and arp

No.	Time	Source	Destination	Protocol	Length	Info
118	1.37…	38:02:de:f8:09:a0	40:1c:83:38:f7:20	ARP	42	Who has 192.168.1.8? Tell 192.168.1.1
119	1.37…	40:1c:83:38:f7:20	38:02:de:f8:09:a0	ARP	42	192.168.1.8 is at 40:1c:83:38:f7:20
980	10.5…	40:1c:83:38:f7:20	38:02:de:f8:09:a0	ARP	42	Who has 192.168.1.1? Tell 192.168.1.8
981	10.5…	38:02:de:f8:09:a0	40:1c:83:38:f7:20	ARP	42	192.168.1.1 is at 38:02:de:f8:09:a0
1369	14.0…	38:02:de:f8:09:a0	40:1c:83:38:f7:20	ARP	42	Who has 192.168.1.8? Tell 192.168.1.1
1370	14.0…	40:1c:83:38:f7:20	38:02:de:f8:09:a0	ARP	42	192.168.1.8 is at 40:1c:83:38:f7:20

4.4)

```
Frame Number: 980
Frame Length: 42 bytes (336 bits)
Capture Length: 42 bytes (336 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]
Ethernet II, Src: 40:1c:83:38:f7:20, Dst: 38:02:de:f8:09:a0
  Destination: 38:02:de:f8:09:a0
  Source: 40:1c:83:38:f7:20
  Type: ARP (0x0806)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: 40:1c:83:38:f7:20
```

```
0000  38 02 de f8 09 a0 40 1c  83 38 f7 20 08 06 00 01   8·····@· ·8· ····
0010  08 00 06 04 00 01 40 1c  83 38 f7 20 c0 a8 01 08   ·····@· ·8· ····
0020  38 02 de f8 09 a0 c0 a8  01 01                     8····· ··
```

4.5)

```
Frame 118: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{065E544F-FE2E-44B1-A3C5-53895F3E5671}, id 0
Ethernet II, Src: 38:02:de:f8:09:a0, Dst: 40:1c:83:38:f7:20
  Destination: 40:1c:83:38:f7:20
  Source: 38:02:de:f8:09:a0
  Type: ARP (0x0806)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: 38:02:de:f8:09:a0
  Sender IP address: 192.168.1.1
  Target MAC address: 00:00:00:00:00:00
  Target IP address: 192.168.1.8
```

```
0000  40 1c 83 38 f7 20 38 02  de f8 09 a0 08 06 00 01   @··8· 8· ········
0010  08 00 06 04 00 01 38 02  de f8 09 a0 c0 a8 01 01   ·····8· ········
0020  00 00 00 00 00 00 c0 a8  01 08                     ····· ··
```

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

4.6) Hardware type: Ethernet – κάρτα δικτύου
4.7) Protocol type: IPv4
4.8) Για ίδια παίρνουν ίδια τιμή
4.9) Καθώς ο τύπος της διεύθυνσης του πρωτοκόλλου IPv4 είναι (4 Bytes)
4.10) Καθώς το μέγεθος της διεύθυνσης υλικού Ethernet είναι 6 Bytes
4.11) Η διεύθυνση του αποστολέα ανήκει στο Router
4.12) 38:02:de:f8:09:a0
4.13)
ARP: 28 Bytes
Ethernet: 42 Bytes
4.15) 20 bytes προηγούνται του opcode
4.16) Στο Sender MAC address
4.17) Στο Sender IP address
4.18) Στο Target IP address
4.19) Υπάρχει το πεδίο Target MAC address που περιέχει τη διεύθυνση: 00:00:00:00:00:00.
4.20) Η διεύθυνση του αποστολέα ανήκει στο Router και του παραλήπτη στον υπολογιστή μου
4.21) Η τιμή του είναι 0x0002
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)
ARP: 28 Bytes
Ethernet: 42 Bytes
4.27) Ναι είναι ίδια. (Είμαι συνδεδεμένος ασύρματα και δεν παρατηρώ το padding που θα χρειαζόταν εως τα 64 bytes)
4.28) Η διαφορά οφείλεται στο γεγονός ότι το Wireshark θα κάνει capture τα πακέτα πριν φτάσουν στο στρώμα ζεύξης όπου και θα αποκτήσουν το απαραίτητο Padding μέχρι τα 64 byte που είναι το ελάχιστο μέγεθος πλαισίου Ethernet. Αντιθέτως, στην απάντηση όπου το padding έχει γίνει από τον αποστολέα θα είναι εμφανές και στο Wireshark.
4.29) Το opcode
4.30) Οι διαφορές που παρατηρούμε είναι ότι στο request έχουμε Target MAC addr να είναι 00:00:00:00:00:00 καθώς δεν την γνωρίζουμε ακόμα ενώ στο response λαμβάνουμε πίσω την MAC address της συσκευής
4.31) Τότε όλοι οι χρήστες του δικτύου θα έστελναν τα πλαίσια τους σε αυτόν τον κακόβουλο χρήστη ο οποίος θα μπορούσε να τα κάνει resolve, αρα οι χρήστες να τον αποθυκεύσουν στο Arp Table τους, και να κάνει την γνωστή επίθεση Man-In-The-Middle(MITM), με αποτέλεσμα να είναι σε κύνδινο τα δεδομένα των χρηστών.