ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

MAC = a0:36:bc:a9:7e:58/8c:c8:4b:7c:5d:73

IP = 147.102.203.238/

christos-System-Product-Name/christos-HN-WX9X

LINUX Ubuntu 22.04.3 LTS

<u>3η Εργαστηριακή Αναφορά</u>

Χρήστος Ηλιακόπουλος

ΑΜ: 03120233

ΑΣΚΗΣΗ 1

1.1) arp –n ή ip neigh

1.2) sudo ip -s -s neigh flush all

1.3) η defaul gateway ipv4 διεύθυνση είναι 147.102.200.200 και εμφανίζεται και η διεύθυνση 147.102.203.254 που είναι κάποιας άλλης συσκευλης συνδεδεμένη στο δίκτυο μου

Η διεύθυνση του DNS εξυπηρετητή μου είναι 147.102.224.243

```
christos@christos-HN-WX9X:~$ resolvectl status
Global
       Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
resolv.conf mode: stub

Link 2 (wlp1s0)
    Current Scopes: DNS
         Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
Current DNS Server: 147.102.224.243
       DNS Servers: 147.102.224.243
```

1.4)

```
christos@christos-HN-WX9X:~$ sudo arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
147.102.203.254          ether   00:50:56:b5:aa:aa   C                     wlp1s0
147.102.200.200          ether   08:ec:f5:d0:d9:1d   C                     wlp1s0
christos@christos-HN-WX9X:~$
```

1.5) Υπάρχει της προκαθορισμένης πύλης και άλλη μία διεύθυνση. Όχι δεν εμφανίζεται η διεύθυνση του DNS εξυπηρετητή, καθώς δεν είναι στο ίδιο υποδίκτυο

1.6) 147.102.202.107

```
rtt min/avg/max/mdev = 3.516/6.629/12.295/3.573 ms
christos@christos-HN-WX9X:~$ ping 147.102.202.107
PING 147.102.202.107 (147.102.202.107) 56(84) bytes of data.
64 bytes from 147.102.202.107: icmp_seq=1 ttl=64 time=405 ms
64 bytes from 147.102.202.107: icmp_seq=2 ttl=64 time=240 ms
64 bytes from 147.102.202.107: icmp_seq=3 ttl=64 time=361 ms
^C
--- 147.102.202.107 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 239.753/335.488/405.280/70.021 ms
```

1.7)Παρατηρώ ότι η διεύθυνση που έκανα ping προστέθηκε στον ARK πίνακα

1.8)Έγινε καταχώρηση μόνο της default gateway διεύθυνσης γιατί μόνο αυτή χρειάστηκε

```
christos@christos-HN-WX9X:~$ sudo systemd-resolve --flush-caches
sudo: systemd-resolve: command not found
christos@christos-HN-WX9X:~$ sudo resolvectl flush-caches
christos@christos-HN-WX9X:~$ sudo ip -s -s neigh flush all
147.102.203.254 dev wlp1s0 lladdr 00:50:56:b5:aa:aa used 209/209/188 probes 1 STALE
147.102.202.107 dev wlp1s0 lladdr 80:91:33:dd:11:7f used 433/433/397 probes 4 STALE
147.102.200.200 dev wlp1s0 lladdr 08:ec:f5:d0:d9:1d ref 1 used 430/1/430 probes 4 REACHABLE

*** Round 1, deleting 3 entries ***
*** Flush is complete after 1 round ***
christos@christos-HN-WX9X:~$ sudo arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
147.102.200.200          ether   08:ec:f5:d0:d9:1d   C                     wlp1s0
```

1.9) Όχι, όπως φαίνεται και παραπάνω. Αυτό συνέβη γιατι βρίσκεται σε διαφορετικό υποδίκτυο και επικοινωνία με αυτά επιτυγχάνεται μόνο μέσω του δρομολογητή

ΑΣΚΗΣΗ 2

2.1) Destination, Source, Type

ip or ipv6 or arp

No.	Time	Source	Destination	Protocol	Length	Info
240	3.031780822	147.102.201.153	224.0.0.251	MDNS	397	Standard query re
241	3.136243906	147.102.201.162	224.0.0.251	MDNS	374	Standard query re
242	3.136244397	147.102.201.162	224.0.0.251	MDNS	374	Standard query re
243	3.136244537	147.102.237.117	224.0.0.251	MDNS	558	Standard query re
244	3.136244688	147.102.237.117	224.0.0.251	MDNS	558	Standard query re
245	3.136244828	147.102.200.36	224.0.0.251	MDNS	568	Standard query re
246	3.136244968	147.102.200.36	224.0.0.251	MDNS	568	Standard query re
247	3.136245109	147.102.201.42	224.0.0.251	MDNS	124	Standard query 0x
248	3.136245259	147.102.201.42	224.0.0.251	MDNS	124	Standard query 0x
249	3.136340773	147.102.239.81	224.0.0.251	MDNS	193	Standard query 0x
250	3.136340973	147.102.239.81	224.0.0.251	MDNS	193	Standard query 0x
251	3.136341113	147.102.202.77	224.0.0.251	MDNS	273	Standard query 0x
252	3.136341254	147.102.202.77	224.0.0.251	MDNS	273	Standard query 0x
253	3.240951530	147.102.236.186	224.0.0.251	MDNS	489	Standard query re
254	3.240952252	147.102.236.186	224.0.0.251	MDNS	489	Standard query re
255	3.240952392	147.102.202.245	224.0.0.251	MDNS	376	Standard query re
256	3.240952532	147.102.202.245	224.0.0.251	MDNS	376	Standard query re
257	3.240952673	147.102.238.12	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1
258	3.240952823	147.102.238.12	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1
259	3.240952953	147.102.202.172	224.0.0.251	MDNS	308	Standard query 0x
260	3.240953093	147.102.202.172	224.0.0.251	MDNS	308	Standard query 0x
261	3.241038889	147.102.202.76	224.0.0.251	MDNS	750	Standard query 0x
262	3.241039099	147.102.202.76	224.0.0.251	MDNS	750	Standard query 0x
263	3.241039239	147.102.239.176	224.0.0.251	MDNS	217	Standard query 0x

```
▸ Frame 248: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface wlp1s0, id
▾ Ethernet II, Src: ca:b2:7f:70:a0:1c, Dst: 01:00:5e:00:00:fb
  ▸ Destination: 01:00:5e:00:00:fb
  ▸ Source: ca:b2:7f:70:a0:1c
    Type: IPv4 (0x0800)
```

2.2) Δεν υπάρχει κάπου καταγραφή του προοιμίου. Το προοίμιο χρησιμεύει μόνο στο συγχρονισμό

2.3)Δεν γίνεται καταγραφή του CRC, καθώς δεν υποστηρίζεται από το WIRESHARK

2.4)0x0800

2.5) 0x0806

2.6)Δεν καταγράφηκαν, αλλά αν υπήρχε καταγραφή τους θα ήταν 0x86DD

2.7)8c:c8:4b:7c:5d:73

2.8)08:EC:F5:D0:D9:1D

2.9)

```
christos@christos-HN-WX9X:~$ sudo arp -n
[sudo] password for christos:
Address                  HWtype  HWaddress           Flags Mask            Iface
147.102.203.254          ether   00:50:56:b5:aa:aa   C                     wlp1s0
147.102.200.200          ether   08:ec:f5:d0:d9:1d   C                     wlp1s0
```

Όχι, η διεύθυνση αυτή είναι του default gateway. Η διεύθυνση της σελίδας ούτως ή άλλως είδαμε ότι ανήκει σε διαφορετικό υποδίκτυο

2.10) Στον default gateway

2.11)569 bytes

2.12)66 bytes πριν το G

2.13) 08:EC:F5:D0:D9:1D

2.14)Όχι

2.15)Ανήκει στο default gateway

2.16) 8c:c8:4b:7c:5d:73

2.17)Στον δικό μου

2.18) 596 bytes

2.19)79 bytes

ΑΣΚΗΣΗ 3 (Έγινε χρήση του αρχείου που περιέχεται στο σύνδεσμο)

3.1)Ατομικές και μοναδικές (individual και globally unique)

3.2)Τοπικές και ομαδικές (locally administered και group)

3.3)Το πρώτο βρίσκεται στην 7η θέση και το δεύτερο στην 8η θέση

```
▾ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
    .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
▾ Source: IETF-VRRP-VRID_25 (00:00:5e:00:01:25)
    Address: IETF-VRRP-VRID_25 (00:00:5e:00:01:25)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
```

3.4) ff:ff:ff:ff:ff:ff

3.5)Εμφανίζονται μόνο STP(Spanning tree protocol) πλαισίου IEEE 802.3 ETHERNET

3.6)Το μήκος των δεδομένων (στο πεδίο length φαίνονται πόσα bytes είναι τα δεδομένα μας)

3.7)Στο Ethernet II τα πεδία είναι τα destination, source, type, ενώ στο IEEE 802.3 έχουμε πάλι τα destination και source αλλά τώρα αντί για το type έχουμε το length(μέγεθος δεδομένων) και το padding(προσθήκη μηδενικών για την εξασφάλιση του ελάχιστου μήκους)

3.8)Έχει μέγεθος 3 byte και περιλαμβάνει τα πεδία DSAP, SSAP, Control field

```
▾ Logical-Link Control
  ▸ DSAP: Spanning Tree BPDU (0x42)
  ▸ SSAP: Spanning Tree BPDU (0x42)
  ▸ Control field: U, func=UI (0x03)
```

3.9)Μεταφέρουν δεδομένα του STL πρωτοκόλλου και έχουν μήκος 36 bytes

```
Spanning Tree Protocol
    Protocol Identifier: Spanning Tree Protocol (0x0000)
    Protocol Version Identifier: Rapid Spanning Tree (2)
    BPDU Type: Rapid/Multiple Spanning Tree (0x02)
  ▸ BPDU flags: 0x3c, Forwarding, Learning, Port Role: Designated
  ▸ Root Identifier: 12288 / 38 / 7c:ad:4f:42:cc:e0
    Root Path Cost: 102
  ▸ Bridge Identifier: 32768 / 38 / cc:7f:76:1b:ef:80
    Port identifier: 0x8017
    Message Age: 2
    Max Age: 20
    Hello Time: 2
    Forward Delay: 15
    Version 1 Length: 0

0000  01 80 c2 00 00 00 cc 7f  76 1b ef 97 00 27 42 42   ........ v....'BB
0010  03 00 00 02 02 3c 30 26  7c ad 4f 42 cc e0 00 00   .....<0& |.OB....
0020  00 66 80 26 cc 7f 76 1b  ef 80 80 17 02 00 14 00   .f.&..v. ........
0030  02 00 0f 00 00 00 00 00  00 00 00 00               ........ ....

Spanning Tree Protocol (stp), 36 bytes
```

3.10) Έχει μέγεθος 7 bytes και ο σκοπός του είναι να συμπληρώνει με 0 έως ότου το πλαίσιο έχει το ελάχιστο μέγεθος(64 bytes)

ΑΣΚΗΣΗ 4

4.1) εμφανίζει τα πακέτα που θα έχουν τη συγκεκριμένη mac είτε στο πεδίο source είτε στο destination στο πλαίσιο ethernet

4.2)Θα εμφανίσει τα πακέτα με αυτήν τη mac στο πλαίσιο ethernet και που κάνουν χρήση πρωτοκόλλου ARP

4.3)2 πακέτα

eth.addr == 8c:c8:4b:7c:5d:73 and arp

No.	Time	Source	Destination	Protocol	Length	Info
602	7.941548624	8c:c8:4b:7c:5d:73	ff:ff:ff:ff:ff:ff	ARP	42	Who has 147.102.200.200? Tell 147.102.203.238
604	7.957153531	08:ec:f5:d0:d9:1d	8c:c8:4b:7c:5d:73	ARP	60	147.102.200.200 is at 08:ec:f5:d0:d9:1d

4.4)Στο πεδίο type αντί για τιμή 0x0800 έχει 0x0806

4.5)

- Hardware type: 2 bytes
- Protocol type: 2 bytes
- Hardware size: 1 bytes
- Protocol size: 1 bytes
- Opcode: 2 bytes
- Sender MAC Address: 6 bytes
- Sender IP address: 4 bytes
- Target MAC Address: 6 bytes
- Target IP Address: 6 bytes

```
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 8c:c8:4b:7c:5d:73
    Sender IP address: 147.102.203.238
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 147.102.200.200
```

4.6) Έχει τιμή ίση με το ένα και υποδεικνύει κάρτα ETHERNET

4.7)Η τιμή του είναι 0x0800 και υποδεικνύει πρωτόκολλο IPv4

4.8)Οι τιμές των πεδίων αντιστοιχούν στα ίδια πρωτόκολλα που χρησιμοποιούνται στο από πάνω layer

4.9)Το protocol size μας δειχνει το μηκος της διευθυνσης του πρωτοκόλλου και στη συγκεκριμένη περίπτωση που έχουμε IPv4 είναι 4 bytes (32 bits)

4.10)Γιατί αναφέρεται στο μέγεθος της φυσικής διεύθυνσης (MAC address) στο δίκτυο, που στην πλειοψηφία οι διευθύνσεις MAC έχουν μέγεθος 48 bits/6bytes

4.11)Στον δικό μου υπολογιστή

4.12)ff:ff:ff:ff:ff:ff

4.13)28 bytes και και 42 bytes

4.14)Συνολικά 20 bytes (14 του Ethernet και 6 από το Hardware type(2), Protocol type(2), Hardware size(1), Protocol size(1))

4.15)Opcode: request (1), άρα 1

4.16)Στο Sender MAC address

4.17)Στο Sender IP address

4.18)Στο Target IP address

4.19)Το Target MAC address και η τιμή της είναι 00:00:00:00:00:00

Για το ARP REPLY πακέτο

```
▾ Ethernet II, Src: 08:ec:f5:d0:d9:1d, Dst: 8c:c8:4b:7c:5d:73
  ▸ Destination: 8c:c8:4b:7c:5d:73
  ▸ Source: 08:ec:f5:d0:d9:1d
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 08:ec:f5:d0:d9:1d
    Sender IP address: 147.102.200.200
    Target MAC address: 8c:c8:4b:7c:5d:73
    Target IP address: 147.102.203.238
```

4.20)Η διεύθυνση MAC του αποστολέα ανήκει στην συσκευή που κάναμε ping, ενώ η MAC του destination είναι ο δικός μας υπολογιστής

4.21)Opcode: reply(2), άρα 2

4.22)Στο Sender IP Address

4.23)Στο Sender MAC Address

4.24)Στο Target IP Adddress

4.25)Στο Target MAC Address

4.26)Το μέγεθος του πακέτου ARP reply είναι 28 bytes και το συνολικό μέγεθος του πλαισίου ethernet που το μεταφέρει είναι 60 bytes (μέγεθος του πλαισίου ethernet II είναι 32 bytes

4.27)Όχι. Το ARP πακέτο είτε είναι reply είτε request είναι το ίδιο. Το συνολικό πλαίσιο ethernet αλλάζει από 42 bytes για το request σε 60 για το reply

4.28)Ο τίτλος του πλαισίου και το πεδίο opcode με την τιμή που περιέχει

```
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 08:ec:f5:d0:d9:1d
    Sender IP address: 147.102.200.200
    Target MAC address: 8c:c8:4b:7c:5d:73
    Target IP address: 147.102.203.238
```

4.29)Στο ότι η βιβλιοθήκη του wireshark κάνει capture τα εξερχόμενα πλαίσια, πρωτού πάνε στην κάρτα δικτύου όπου θα προστεθεί και το padding για να γίνει η μετάδοσή τους

4.30)Το ARP request θα έχει κενή Target MAC Address και στον πεδίο Opcode στο request θα είναι ένα, ενώ στο reply 2. Ακόμη, επειδή το wireshark κάνει capture στα ARK requests πριν πάνε στην κάρτα δικτύου, δεν υπάρχει το πεδίο padding στο πλαίσιο ethernet II

4.31)Θα δημιουργώνταν μία κατάσταση που ονομάζεται arp spoofing (είδος cyber attack). Ουσιαστικά θα έδινε την δική του MAC διεύθυνση στα routing tables και θα λάμβανε πακέτα που δεν προορίζονταν για αυτόν, θα μπορούσε να μεταβάλλει την κίνηση των πακέτων όπως αυτός επιθυμεί με υπερφόρτωση ή και παύση της. Αυτή η συμπεριφορά θα οδηγούσε σε άλλες

καταστάσεις όπως επιθέσεις DoS, man in the middle και γενικότερα σημαντικές επιπτώσεις στην ασφάλεια και την κατάσταση των συνδεδεμένων συστημάτων