

ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

MAC = 8c:c8:4b:7c:5d:73/

IP = 147.102.203.141/147.102.236.193/192.168.1.9

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

LINUX Ubuntu 22.04.3 LTS

### 6η Εργαστηριακή Αναφορά

Χρήστος Ηλιακόπουλος

AM: 03120233

## **ΑΣΚΗΣΗ 1**

1.1) ether host 8c:c8:4b:7c:5d:73

1.2)arp or icmp

1.3)Τα arp πακέτα στάλθηκαν έτσι ώστε να μπορέσει να βρει την φυσική διεύθυνση του υπολογιστή μας (mac address) το gateway, ώστε να μπορέσει να στείλει αρχεία κάνοντας αρχικά χρήση ip address

1.4)Protocol: ICMP(1)

1.5)16 bytes (για λινουξ αφού έχουμε έξτρα το πεδίο timestamp from icmp data)

1.6)

Type : 1 byte

Code: 1 byte

Checksum: 2 bytes

Identifier (BE) και Identifier (LE): συνολικά 2 bytes

Sequence number (BE) και Sequence number (LE): συνολικά 2 bytes

Timestamp from icmp data: 8 bytes

1.7)Type: 8 (Echo (ping) request)

Code: 0

1.8)

Identifier (BE): 17 (0x0011)

Identifier (LE):4352 (0x1100)

Sequence (BE): 1 (0x0001)

Sequence (LE): 256 (0x0100)

1.9) Data:

63e7020000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637

[Length: 48 bytes]

1.10) Ομοίως με πριν είναι πάλι 16 bytes και έχει την ίδια δομή

1.11) Type: 0 (Echo (ping) reply)

Code: 0

1.12) Το πεδίο type

1.13)

Identifier (BE): 17 (0x0011)

Identifier (LE): 4352 (0x1100)

Sequence (BE): 2 (0x0001)

Sequence (LE): 256(0x0100)

1.14) Είναι ίδιες με αυτές της ερώτησης 1.13

1.15) Γίνεται η χρήση τους για την αντιστοίχιση ενός echo request με το παραγόμενο echo reply

1.16)

Data:

4ce5020000000000101112131415161718191a1b1c1d1e1f202122232425262728292a2b2c2d2e2f3031323334353637

Length: 48 bytes

1.17) Όχι, παρατηρούμε ότι είναι ακριβώς το ίδιο

1.18) Στο sequence number (BE) εμφανίεμφανίζεται ο ίδιος αριθμός με αυτόν του τερμιναλ μετά την εκτέλεση της ping, ενώ εμφανίζεται και το response time και στα δυο

```
christos@christos-HN-WX9X:~$ ping 147.102.203.199 -c 2
PING 147.102.203.199 (147.102.203.199) 56(84) bytes of data.
From 147.102.203.141 icmp_seq=1 Destination Host Unreachable
From 147.102.203.141 icmp_seq=2 Destination Host Unreachable

--- 147.102.203.199 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1021ms
pipe 2
```

1.19) ping 147.102.203.199 -c 2

1.20)

No.	Time	Source	Destination	Protocol	Length	Info
12	0.000000000	8c:c8:4b:7c:5d:73	ff:ff:ff:ff:ff:ff	ARP	42	Who has 147.102.203.199? Tell 147.102.203.141
16	1.020078096	8c:c8:4b:7c:5d:73	ff:ff:ff:ff:ff:ff	ARP	42	Who has 147.102.203.199? Tell 147.102.203.141
17	0.360967114	fc:b3:bc:a5:f2:80	8c:c8:4b:7c:5d:73	ARP	60	147.102.236.53 is at fc:b3:bc:a5:f2:80
18	0.0000000391	10:f6:0a:8b:79:73	8c:c8:4b:7c:5d:73	ARP	60	147.102.237.132 is at 10:f6:0a:8b:79:73
21	0.663035558	8c:c8:4b:7c:5d:73	ff:ff:ff:ff:ff:ff	ARP	42	Who has 147.102.203.199? Tell 147.102.203.141
22	0.209645512	fc:b3:bc:a5:f2:80	8c:c8:4b:7c:5d:73	ARP	60	147.102.236.53 is at fc:b3:bc:a5:f2:80
23	0.000000180	10:f6:0a:8b:79:73	8c:c8:4b:7c:5d:73	ARP	60	147.102.237.132 is at 10:f6:0a:8b:79:73
24	0.000000140	70:a8:d3:4b:41:e1	8c:c8:4b:7c:5d:73	ARP	60	147.102.238.138 is at 70:a8:d3:4b:41:e1

3 μηνύματα arp από τον υπολογιστή μας που να ρωτάνε για την mac

1.21) Περίπου ανά μισό δευτερόλεπτο

1.22) Κανένα

1.23) Βλέπουμε στο τέρμιναλ το Destination Host Unreachable και αντίστοιχα στο wireshark δεν υπάρχει δεν φαίνεται να στέλνονται icmp γιατί δεν βρέθηκε διεύθυνση για να σταλθούν τα icmp requests

## ΑΣΚΗΣΗ 2

2.1) Περιέχει τον default gateway: 147.102.200.200 με mac: 08:ec:f5:d0:d9:1d και την διεύθυνση 147.102.203.254 με mac: 00:50:56:b5:aa:aa και τα δύο συνδεδεμένα με ethernet

```
christos@christos-HN-WX9X:~$ arp
```

Address	HWtype	HWaddress	Flags	Mask	Iface
147.102.203.254	ether	00:50:56:b5:aa:aa	C		wlp1s
0_gateway	ether	08:ec:f5:d0:d9:1d	C		wlp1s
0					

2.2)

Destination: 08:ec:f5:d0:d9:1d

Source: 8c:c8:4b:7c:5d:73

2.3)

Destination: 147.102.1.1

Source: 147.102.203.141

2.4) Η 147.102.203.141 (δικιά μου) στην 8c:c8:4b:7c:5d:73 και η 147.102.1.1 στην 08:ec:f5:d0:d9:1d

2.5) Όχι, κανένα

2.6) Στέλνουμε ping σε διεύθυνση που δεν ανήκει στο τοπικό μας υποδίκτυο, οπότε υπεύθυνος για την απόστολή των arp είναι κάποιος ενδιάμεσος δρομολογητής

2.7) icmp.type == 0

2.8) Από το πεδίο Time to Live που βρίσκεται στην επικεφαλίδα της IPv4 address

2.9) Μόνο Echo (ping) request

2.10) Είχαμε και τα arp request μηνύματα γιατί ήτανε στο δικό μας υποδίκτυο για να βρούμε τη mac address

### **ΑΣΚΗΣΗ 3**

3.1) 32 bytes

Data: 48494a4b4c4d4e4f505152535455565758595a5b5c5d5e5f6061626364656667

3.2) Σε αυτήν την περίπτωση είναι μικρότερο το μήκος των δεδομένων

3.3) Έχουμε Time to live exceeded

3.4)

Type: 11 (Time-to-live exceeded)

Code: 0 (Time to live exceeded in transit)

3.5)

Checksum: 2 bytes

Unused: 1 byte

Length: 1 byte

Unused: 2 bytes

3.6) 16 bytes ( $76-40-20 = 16$  bytes)

```
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xf4ee [correct]
[Checksum Status: Good]
Unused: 00
Length: 17
[Length of original datagram: 68]
Unused: 0000
Internet Protocol Version 4, Src: 192.168.52.235, Dst: 147.102.40.15
Internet Control Message Protocol
```

3.7) Περιέχεται το ipv4 πακέτο που στάλθηκε στο icmp request

### **ΑΣΚΗΣΗ 4**

4.1) Αφαιρώ τα header length των πακέτων IPv4 και ICMP που είναι συνολικά 28 bytes και ξεκινά από τιμές 1472, 1464, 978, 548 που είναι και η τιμή που για πρώτη φορά θα απαντήσει

```
christos@christos-HN-WX9X:~$ ping -c 1 -M do -s 978 edu-dy.cn.ntua.gr
PING edu-dy.cn.ece.ntua.gr (147.102.40.15) 978(1006) bytes of data.

--- edu-dy.cn.ece.ntua.gr ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

christos@christos-HN-WX9X:~$ ping -c 1 -M do -s 548 edu-dy.cn.ntua.gr
PING edu-dy.cn.ece.ntua.gr (147.102.40.15) 548(576) bytes of data.
556 bytes from edu-dy.cn.ece.ntua.gr (147.102.40.15): icmp_seq=1 ttl=63 time=2
.71 ms

--- edu-dy.cn.ece.ntua.gr ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.714/2.714/2.714/0.000 ms
christos@christos-HN-WX9X:~$
```

4.2) Όχι

4.3)

Type: 3 (Destination unreachable)

Code: 4(Fragmentation needed)

4.4) Το πεδίο code: 4

Next-Hop MTU:1492

4.5)Την επικεφαλίδα IPv4 και το header του ICMP του πακέτου που προκάλεσε το λάθος

4.6)1500 μαζί με τα headers

```
christos@christos-HN-WX9X:~$ ping -c 1 -M do -s 1472 edu-dy.cn.ntua.gr
PING edu-dy.cn.ece.ntua.gr (147.102.40.15) 1472(1500) bytes of data.

--- edu-dy.cn.ece.ntua.gr ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

christos@christos-HN-WX9X:~$ ping -c 1 -M do -s 1473 edu-dy.cn.ntua.gr
PING edu-dy.cn.ece.ntua.gr (147.102.40.15) 1473(1501) bytes of data.
ping: local error: message too long, mtu=1500

--- edu-dy.cn.ece.ntua.gr ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

4.7)Δεν θα λάβουμε απάντηση για τις τιμές 1500, 1492 και 1006

4.8) 576

4.9) Εφόσον μέχρι και 1500 το πακέτο στέλνεται και επειδή δεν λαμβάνουμε απάντηση συμπεραίνουμε ότι είναι τιμή ενδιάμεσου κόμβου

4.10) Παρατηρούμε ότι στις απαντήσεις το πεδίο FLAG το don't fragment έχει την τιμή SET άρα ναι παραμένει

4.11)Γιατί η τελική διεπαφή έχει μεγαλύτερο mtu από τους ενδιάμεσους κόμβους

4.12)586 bytes. Όχι

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	147.102.236.193	147.102.40.15	ICMP	1514	Echo (ping) request id=0x004d, seq=1/256, ttl=64 (reply in 4)
2	0.902737149	147.102.40.15	147.102.236.193	IPv4	586	Fragmented IP protocol (proto=ICMP 1, off=0, ID=d314) [Reassembled in #4]
3	0.000001042	147.102.40.15	147.102.236.193	IPv4	586	Fragmented IP protocol (proto=ICMP 1, off=552, ID=d314) [Reassembled in #4]
4	0.000000080	147.102.40.15	147.102.236.193	ICMP	410	Echo (ping) reply id=0x004d, seq=1/256, ttl=63 (request in 1)

Total Length: 572
Identification: 0xd314 (54036)
Flags: 0x20, More fragments
0... .. = Reserved bit: Not set
.0.. .. = Don't fragment: Not set
..1. .... = More fragments: Set
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 63
Protocol: ICMP (1)
Header Checksum: 0x4b0f (validation disabled)
[Header checksum status: Unverified]
Source Address: 147.102.40.15
Destination Address: 147.102.236.193
[Reassembled IPv4 in frame: 4]
Data (552 bytes)

## ΑΣΚΗΣΗ 5

```
christos@christos-HN-WX9X:~$ dig edu-dy.cn.ntua.gr @147.102.40.15
;; communications error to 147.102.40.15#53: connection refused
;; communications error to 147.102.40.15#53: connection refused
;; communications error to 147.102.40.15#53: connection refused

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> edu-dy.cn.ntua.gr @147.102.40.15
;; global options: +cmd
;; no servers could be reached
```

Και

```
christos@christos-HN-WX9X:~$ dig @147.102.40.15 edu-dy.cn.ntua.gr
;; communications error to 147.102.40.15#53: connection refused
;; communications error to 147.102.40.15#53: connection refused
;; communications error to 147.102.40.15#53: connection refused

; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> @147.102.40.15 edu-dy.cn.ntua.gr
; (1 server found)
;; global options: +cmd
;; no servers could be reached
```

Αλλάζει το αποτέλεσμα αν διαφοροποιήσουμε τη σειρά στην εντολή

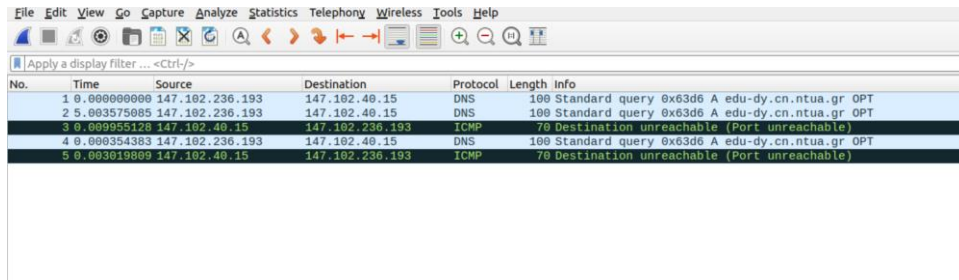
5.1) ip and host 147.102.40.15

5.2) dig @147.102.40.15 edu-dy.cn.ntua.gr και dig edu-dy.cn.ntua.gr @147.102.40.15

5.3) κρατάω την περίπτωση dig @147.102.40.15 edu-dy.cn.ntua.gr

```
; <<>> DiG 9.18.18-0ubuntu0.22.04.1-Ubuntu <<>> @147.102.40.15 edu-dy.cn.ntua.gr
; (1 server found)
;; global options: +cmd
;; no servers could be reached
```

5.4) Ναι



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	147.102.236.193	147.102.40.15	DNS	100	Standard query 0x63d6 A edu-dy.cn.ntua.gr OPT
2	5.003575089	147.102.236.193	147.102.40.15	DNS	100	Standard query 0x63d6 A edu-dy.cn.ntua.gr OPT
3	0.009955128	147.102.40.15	147.102.236.193	ICMP	70	Destination unreachable (Port unreachable)
4	0.009354383	147.102.236.193	147.102.40.15	DNS	100	Standard query 0x63d6 A edu-dy.cn.ntua.gr OPT
5	0.003019809	147.102.40.15	147.102.236.193	ICMP	70	Destination unreachable (Port unreachable)

5.5) Το UDP και το destination port είναι το 53

5.6) Ναι

5.7)

Type: 3 (Destination unreachable)

Code: 3(Port unreachable)

5.8) Το πεδίο Code

5.9) Επειδή τα μηνύματα DNS είναι γνωστό ότι έχουν ως θύρα προορισμού την 53

5.10) Υπό κανονικές συνθήκες θα γινόταν Echo (ping) reply, εδώ όμως έχουμε destination unreachable

## **ΑΣΚΗΣΗ 6**

6.1) ping -6 -c 4 2001:648:2000:329::101/ traceroute -6 -l 2001:648:2000:329::101

6.2) Φίλτρο σύλληψης: ip6 / Φίλτρο απεικόνισης: icmpv6

6.3) Type: IPv6 (0x86dd)

6.4) 40 bytes

6.5)

Version: 1 byte

Traffic Class: 4 bytes

Flow label: 3 bytes

Payload Length: 2 bytes

Next Header: 1 byte

Hop Limit: 1 byte

Source IPv6 Address: 16 bytes

Destination IPv6 Address: 16 bytes

6.6) To Hop Limit

6.7) Next Header: ICMPV6 (58) η τιμή είναι 58

6.8) Ναι

6.9) Type: Echo (ping) request (128) και το μήκος των δεδομένων είναι 32 bytes

6.10) Ναι

6.11) Type: Echo (ping) reply (129) και το μήκος των δεδομένων είναι 32 bytes

6.12) Τα data είναι 64 bytes αντί για 32 bytes

6.13) Όχι, υπάρχει και το πεδίο reserved

6.14)

Type: Time Exceeded (3)

Και τα δεδομένα είναι 72 byte από το icmpv6 request αλλά και 40 bytes από το header του ipv6, άρα 112 bytes

6.15) Το icmpv6 αρχείο request και το header ipv6 του

6.16) Neighbor Advertisement, Neighbor Solicitation

6.17)

Type: Neighbor Advertisement (136)

Type: Neighbor Solicitation (135)

και τα δύο με μήκος frame 86 bytes