Ονοματεπώνυμο: Πυλιώτης Αθανάσιος		**Ομάδα:** 3
Όνομα PC/ΛΣ: DESKTOP-5DLG3IF		**Ημερομηνία:** 08/11/2022
Διεύθυνση IP: 147.102.201.104	**Διεύθυνση MAC:**	98-54-1B-BD-69-97

Εργαστηριακή Άσκηση 6
Πρωτόκολλο ICMP

Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δενεπαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

1

1.1 ether host 98:54:1b:bd:69:97

1.2 arp or icmp

1.3 Δεν καταγράφηκαν, άρα έχουμε ήδη επισκεφτεί αυτή τη διεύθυνση και η MAC της θα ήταν αποθηκευμένη στον ARP πίνακα. Έγινε ping στο default gateway, οπότε λογικό να έχει καταγραφεί.

1.4 Protocol: ICMP (1)

1.5 8 bytes, όπως αναμέναμε

1.6 Internet Control Message Protocol

Type: 8 (Echo (ping) request) (1 byte)

Code: 0 (1 byte)

Checksum: 0x4d5a [correct] (2 bytes)

Identifier (BE): 1 (0x0001) (1 byte)

Identifier (LE): 256 (0x0100) (1 byte)

Sequence Number (BE): 1 (0x0001) (1 byte)

Sequence Number (LE): 256 (0x0100) (1 byte)

Πρακτικά identifier και sequence number είναι 2 πεδία όχι 4, απλά το wireshark τα εμφανίζει έτσι.

Τα bold είναι τα πρώτα 4 bytes και τα υπόλοιπα είναι τα δεύτερα 4 bytes (φαίνονται και οι τιμές τους)

(δεν χρησιμοποιήθηκε το σχήμα γιατί δεν μπορούσα να γράψω σε αυτό στο word)

1.7 Type: 8 (echo request) , Code: 0.

1.8 Identifier: 0x00010100 και Sequence Number: 0x00010100

1.9 32 bytes, το περιεχόμενο είναι abcdefghijklmn opqrstuvwabcdefg hi, επειδή δεν μας νοιάζει τι θα στείλουμε, θέλουμε απλά να στείλουμε κάτι κι αυτό είναι το πιο απλό πράγμα που μπορεί να στείλει.

1.10 8 bytes, ναι η δομή είναι ίδια.

1.11 Type: 0 (Echo reply), Code: 0

1.12 το Type, που αλλάζει από 8 σε 0.

1.13 Identifier: 0x00010100 και Sequence Number: 0x00010100

1.14 Identifier: 0x00010100 και Sequence Number: 0x00010100, είναι ίδια.

1.15 “The identifier and sequence number may be used by the echo sender to aid in matching the replies with the echo requests” από τη σελίδα, άρα απλά χρησιμοποιούνται για να ξέρουμε σε ποιο request αντιστοιχεί το reply και αντίστροφα.

1.16 Μήκος 32 bytes, περιεχόμενο abcdefghijklmn opqrstuvwabcdefg hi, ίδιο με του αντίστοιχου request.

1.17 Όχι

1.18 Έχουν το μήκος bytes, 32, που αντιστοιχούν στα data, και γράφει το TTL, το οποίο είναι ίδιο με αυτό που καταγράφει το wireshark.

1.19 ping -n 2 -4 <address> , το -n 2 επιβάλει ανταλλαγή 2 πακέτων.

1.20 Δεν ήρθε κανένα

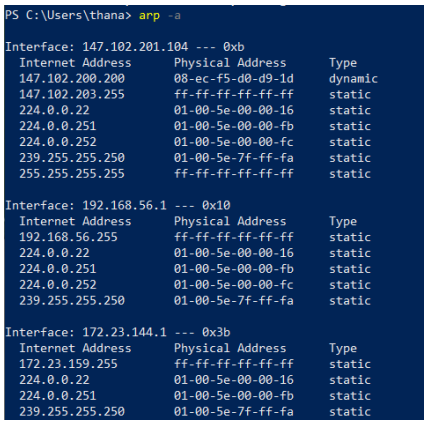
1.21 Δεν είχαμε arp

1.22 2

1.23 2 ICMP request. Πρακτικά έστειλε request και δεν απάντησε οπότε δεν πήρα ποτέ reply.

2

2.1 Έχει τις ίδιες πριν και μετά:



```
PS C:\Users\thana> arp -a

Interface: 147.102.201.104 --- 0xb
  Internet Address      Physical Address      Type
  147.102.200.200       08-ec-f5-d0-d9-1d     dynamic
  147.102.203.255       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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.56.1 --- 0x10
  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: 172.23.144.1 --- 0x3b
  Internet Address      Physical Address      Type
  172.23.159.255        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
```

2.2 Source: 98:54:1b:bd:69:97

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

2.3 Source Address: 147.102.201.104

Destination Address: 147.102.7.1

2.4 98:54:1b:bd:69:97 → 147.102.201.104 , το λάπτοπ μου.

08:ec:f5:d0:d9:1d → 147.102.200.200, default gateway

2.5 όχι

2.6 Δεν υπήρξαν επειδή είχα ήδη την default gateway μου στον πίνακα ARP και ήξερε ποια είναι η MAC της από τη προηγούμενη άσκηση. Για αυτό κι όλας δεν άλλαξε ο πίνακας ARP πριν και μετά την καταγραφή

2.7 icmp.type == 0

2.8 TTL = 63 είναι και στις 2 περιπτώσεις. Προκύπτει επειδή το source περνάει από το default gateway για να έρθει σε εμάς σε αφαιρεί ένα hop, κανονικά θα έστειλε 64 από εκεί που

ξεκίνησε.

2.9 Echo (ping) Request μόνο

2.10 Απλά δεν ήρθε ποτέ απάντηση. Μας έστειλε πως δεν μπορούσε να λάβει απάντηση, επειδή ο υπολογιστής δεν είναι ενεργός.

3

3.1 64 bytes και μόνο μηδενικά, στέλνει ……..

3.2 Καμία σχέση, είναι διπλάσιο από το προηγούμενο σε μήκος, και έχει μηδενικά αντί για ένα τυχαίο μήνυμα.

3.3 Type: 11 (Time-to-live exceeded) και μετά έχει την κεφαλίδα IPv4 του μηνύματος στο οποίο αναφέρεται και τις υπόλοιπες απαντήσεις. Έχει 68 bytes data (χωρίς το header) από IPv4 Header 20 bytes and ICMP Header 8 bytes και 40 bytes data

3.4 Type: 11 (Time-to-live exceeded)

Code: 0 (Time to live exceeded in transit)

3.5 Έχει checksum 2 bytes, unused 1 byte, length 1 byte, unused 2 bytes (6 bytes +2 bytes = 8 bytes)

3.6 8 bytes → header, 68 bytes → data where από IPv4 Header 20 bytes and ICMP Header 8 bytes και 40 bytes data

3.7 IPv4 Header and ICMP Header και data, περιέχει το πακέτο IPv4 μέσα από το header του μέχρι να τελειώσουν τα δεδομένα του ICMP. Οπότε το περιέχει μέσα του.

4

4.1 Ξεκινήσαμε από 1500 και τελικά δούλεψε για 576 bytes MTU (και μικρότερες τιμές).

4.2 Ναι ένα

4.3 79.129.213.16

4.4 Type: 3 (Destination unreachable)

Code: 4 (Fragmentation needed) (Η δικιά μου είχε code: 3 (Port unreachable))

4.5 code προφανώς, αφού ο κώδικας δείχνει πως αυτό είναι το πρόβλημα.

MTU of next hop: 1492 (τιμή των δεδομένων που στάθηκαν)

4.6 Δεν υπάρχει πεδίο δεδομένων σε αυτό το μήνυμα από τη καταγραφή που μας δόθηκε. Τα μόνα δεδομένα είναι το IPv4 πακέτο που προκάλεσε το λάθος και το επιστρέφει, δηλαδή IPv4 header and ICMP header → 20 + 8 = 28 bytes

4.7 1500 bytes

4.8 1492, 1006 bytes MTU (και όσες δοκίμασα παραπάνω με λίγες διαφορές για μέγιστη τιμή 548 bytes data ICMP για να δουλεύει)

4.9 576 bytes MTU

4.10 Ναι είναι της διεπαφής του, αφού το Next-Hop MTU δείχνει το μέγιστο μέγεθος MTU που μπορεί θεωρητικά να σταλεί στα δίκτυα από το router. Της ίδιας της διεπαφής είναι μικρότερο.

4.11 Επειδή, θεωρητικά, θα έπρεπε να μπορεί να σταλεί πακέτο τέτοιου μεγέθους στο δίκτυο. Απλά για τη συγκεκριμένη διεπαφή δεν είναι δυνατό. Ενδέχεται να φταίει και το γεγονός ότι είναι τοπικό δίκτυο.

4.12 Είναι 552 bytes ICMP Data, κατά 4 bytes μεγαλύτερο από αυτό που προσδιόρισα προηγουμένως, ωστόσο δεν υπάρχει επικεφαλίδα ICMP, που μας γλυτώνει 8 bytes, άρα το MTU είναι

572 bytes < 576 bytes. Με βάση τη Wikipedia, το μέγεθος που στέλνεται είναι πολλαπλάσιο του (1464-20)/8 = 180.5 (0, 180.5, 361, 551.5 → 552) και για αυτό το σπάει σε κομμάτια των 552 bytes δεδομένων, εφόσον τα max data είναι παραπάνω κατά 8 πλέον. Είναι λόγω του fragment offset που πρέπει να έχει αυτή τη τιμή και για αυτό δέχεται λίγο μεγαλύτερα πακέτα.

5

5.1 host 147.102.40.15

```
> DNS 147.102.40.15
Server:  [147.102.40.15]
Address:  147.102.40.15

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to 147.102.40.15 timed-out
```

5.2 nslookup και μετά:

> DNS 147.102.40.15

5.3 Request timed out, πρακτικά πως δεν κατάφερε να πάρει απάντηση από το δίκτυο και μπήκε σε timeout για 2 second και ξαναδοκίμασε μετά.

5.4 Ναι, 2

5.5 Destination Port: 53 (User Datagram Protocol header) και το πρωτόκολλο είναι Protocol: UDP (17) (IPv4 Header)

5.6 Ναι

5.7 Type: 3 (Destination unreachable)

Code: 3 (Port unreachable)

5.8 Το πεδίο Code.

5.9 Το Header του UDP Protocol που περιλαμβάνεται στο πακέτο απάντησης με το σφάλμα, που εί αι 53 (και βρίσκουμε πως αυτό σημαίνει DNS).

5.10 Destination unreachable (port unreachable)

6

```
PS C:\Users\thana> ping -6 2001:648:2000:329::101

Pinging 2001:648:2000:329::101 with 32 bytes of data:
Reply from 2001:648:2000:329::101: time<1ms
Reply from 2001:648:2000:329::101: time<1ms
Reply from 2001:648:2000:329::101: time<1ms
Reply from 2001:648:2000:329::101: time<1ms

Ping statistics for 2001:648:2000:329::101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\thana> tracert -6 2001:648:2000:329::101

Tracing route to 2001:648:2000:329::101 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  2001:648:2000:d8:aec:f5ff:fed0:d91d
  2    <1 ms    <1 ms    <1 ms  2001:648:2000:329::101

Trace complete.
```

6.1 ping -6 2001:648:2000:329::101

tracert -6 2001:648:2000:329::101

6.2 Capture: ip6, Display: icmpv6

6.3 Type: IPv6 (0x86dd)

6.4 40 bytes

6.5

Internet Protocol Version 6, Src: fe80::602e:ae6:8803:5878, Dst: ff02::1:ffdc:130c

0110 .... = **Version**: 6 **(0.5 bytes)**

.... 0000 0000 .... = **Traffic Class**: 0x00 (DSCP: CS0, ECN: Not-ECT) **(1 bytes)**

.... 0000 0000 0000 0000 0000 = **Flow Label**: 0x00000 **(2.5 bytes)**

Payload Length: 32 **(2 bytes)**

Next Header: ICMPv6 (58) (**1 bytes)**

Hop Limit: 255 (**1 bytes)**

Source Address: fe80::602e:ae6:8803:5878 **(16 bytes)**

Destination Address: ff02::1:ffdc:130c **(16 bytes)**

6.6 Hop Limit

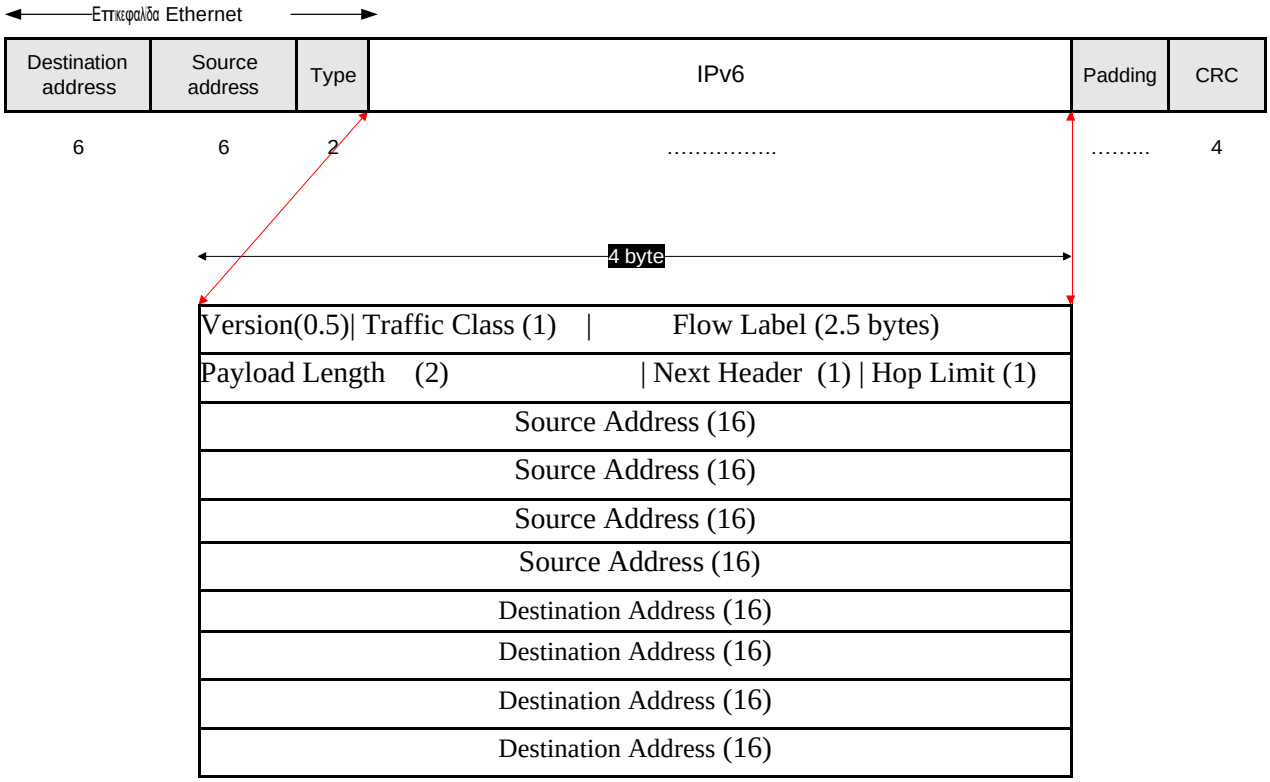
6.7 Next Header: ICMPv6 (58) (0x3a)

6.8 Ναι είναι ίδια.

6.9 Type: Echo (ping) request (128) 0x80 HEX

Το μήκος των δεδομένων είναι 32 bytes: Data (32 bytes)

6.10 Ναι



6.11 Type: Echo (ping) reply (129) 0x81 HEX

Έχει κι αυτό 32 bytes δεδομένων: Data (32 bytes)

6.12 Διαφέρει στο μέγεθος δεδομένων που στέλνει (είναι 64 bytes αντί για 32)

6.13 Ίδια δεν είναι αλλά έχει ίδιες πληροφορίες. Το Type άλλαξε και αντί για 1 bytes unused,

length 1 byte, και 2 bytes unused, έχει 1 byte length of original datagram and 3 bytes reserverd. (και μετά τα headers κανονικά με την ίδια λογική)

6.14 Type: Time Exceeded (3)

ICMPv6 Header + IPv6 Header + ICMPv6 original datagram header + data 64 bytes = 8 bytes + 40 bytes + 8 bytes + 64 bytes = 120 bytes

6.15 μηδενικά τα data, τελείες το περιεχόμενο.

6.16 Ναι, Type: Neighbor Solicitation (135) 0x87 , Type: Neighbor Advertisement (136) 0x88

6.17 Η τιμές του type είναι οι παραπάνω (0x87 and 0x88 HEX) and size 72 bytes = 8 bytes Header + 64 bytes data