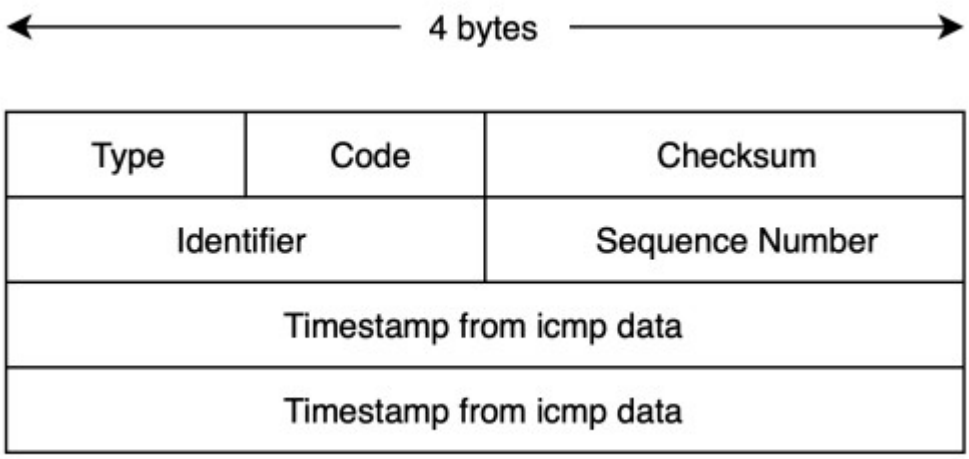
Εργαστηριακή Άσκηση 6 Πρωτόκολλο ICMP

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

Άσκηση 1

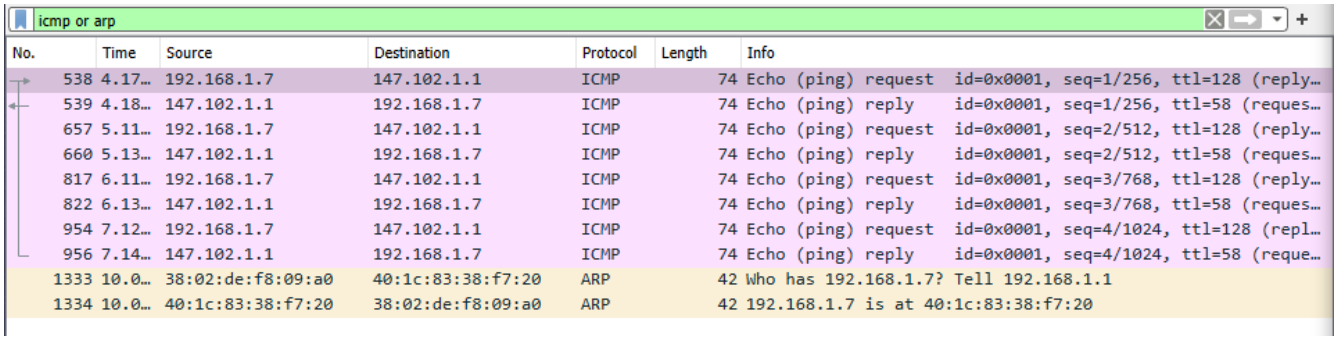
1.1) Το φίλτρο σύλληψης είναι “ether host 40-1C-83-38-F7-20”
1.2) Το φίλτρο απεικόνισης είναι “icmp or arp”
1.3) Καταγράφτηκαν και ο σκοπός τους είναι να γνωστοποιήσουν την MAC address της default gateway (στην οποία έκανα μετάδοση) στον υπολογιστή μου.
1.4) Το όνομα είναι Protocol και η τιμή του είναι ICMP (0x01)
1.5) Είναι 8bytes.
1.6)
Type: 1 byte,
Code: 1 byte,
Checksum: 2 bytes,
Identifier: 2 bytes,
Sequence Number: 2 bytes



1.7)
Type: 8 (0x08)
Code: 0 (0x00)
1.8)
Identification: 0x432d (17197)
Sequence Number: 0x0010 (16)
1.9) Το μήκος είναι 32 bytes και το περιεχόμενο είναι: 61 62 … 77 61 62 63 64 64 .. 69 (Hex)
1.10) Το μήκος επικεφαλίδας ICMP Echo reply είναι 8 bytes και έχει την ίδια δομή με το Echo request
1.11) Type: 0, Code: 0
1.12) Το πεδίο Type
1.13) Identifier: 0x99ec (39404), Sequence Number: 0x0010 (16)
1.14) Identifier: 0x99ec (39404), Sequence Number: 0x0010 (16)
1.15) Βοηθούν στο ταίριασμα των request και replies ενα προς ενα. Όπως βλέπω και στα πακέτα που έστειλα με μία εντολή ping, όλα έχουν το ιδιο Identifier και το Sequence number αυξάνετε όσο

μεταδίδονται νέα. Για να αντιστοιχηθούν ένα προς ένα τα replies σε αυτά που έστειλα, έχουν όλα το ίδιο Identifier με τα Request και τα αντοίστοιχα αύξοντα Sequence Numbers (0,1,2,...).
1.16) Το μήκος είναι 32 bytes
1.17) Οχι δεν διαφέρει
1.18) Είναι άρρηκτα συνδεδεμένα αφού κάθε πληροφορία που τυπώνει η εντολή ping είναι πληροφορία των πακέτων IPv4 που στέλνει, ή παράγωγο αυτής.
1.19) ping <ip> -n 1
1.20) Στάλθηκαν 5 πακέτα ARP μέχρι που η εντολή ping τύπωσε ”Host is down”.
1.21) Κάθε 1 sec.
1.22) Κανένα. (Σε δεύτερη προσπάθεια που έκανα έλαβα ένα Destination Not Reachable)
1.23) Κάθε ένα ICMP πακέτο προκειμένου να φύγει από τον υπολογιστή μου για τον “κενό” προορισμό πρέπει να ξέρει την MAC Address του. Έτσι για τα 5 πρώτα ICMP κάνει αυτόματα 5 broadcast σε όλους τους κόμβους για να μάθει την MAC Address. Αφού δεν λαμβάνει απάντηση υποθέτει ότι ο “Host is down” και παύει να προσπαθεί

Άσκηση 2



No.	Time	Source	Destination	Protocol	Length	Info
538	4.17…	192.168.1.7	147.102.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply…
539	4.18…	147.102.1.1	192.168.1.7	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=58 (reques…
657	5.11…	192.168.1.7	147.102.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply…
660	5.13…	147.102.1.1	192.168.1.7	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=58 (reques…
817	6.11…	192.168.1.7	147.102.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply…
822	6.13…	147.102.1.1	192.168.1.7	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=58 (reques…
954	7.12…	192.168.1.7	147.102.1.1	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (repl…
956	7.14…	147.102.1.1	192.168.1.7	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=58 (reque…
1333	10.0…	38:02:de:f8:09:a0	40:1c:83:38:f7:20	ARP	42	Who has 192.168.1.7? Tell 192.168.1.1
1334	10.0…	40:1c:83:38:f7:20	38:02:de:f8:09:a0	ARP	42	192.168.1.7 is at 40:1c:83:38:f7:20

2.1)

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

Interface: 192.168.1.7 --- 0x2
  Internet Address      Physical Address      Type
  192.168.1.1           38-02-de-f8-09-a0     dynamic
  192.168.1.255         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
PS C:\Users\papar>
```

2.2) Source: 40:1c:83:38:f7:20, destination: 38:02:de:f8:09:a0
2.3) Αποστολέα: 192.168.1.7, παραλήπτης 147.102.1.1
2.4)
192.168.1.7 → 40:1c:83:38:f7:20
147.102.1.1 → 38:02:de:f8:09:a0
2.5) Ναι.
2.6) Η εντολή ping που έτρέξα έστειλε πακέτα σε εξωτερικό δίκτυο που σημαίνει ότι δρομολογήθηκαν μέσω της default gateway της οποίας έχω ήδη αποθυκευμένη την MAC Address στον ARP πίνακα αυτού υπολογιστή.
2.7) icmp.type == 0
2.8) TTL = 58
2.9) 1 Type: 8 (0x0800) (Echo (ping) Request)
2.10) Θεμελιώδης διαφορά είναι ότι στην περίπτωση του τοπικού μου δικτύου τα πακέτα ICMP δεν έφυγαν ποτέ, αφού δεν είχαν την MAC Address της συσκευής για να συμπληρωθεί η επικεφαλίδα Ethernet. Αντιθέτως δεδομένου ότι τα πακέτα σε εξωτερικά υποδίκτυα δρομολογούνται μέσω της default gateway, έχουμε την MAC Address της, και επίσης αφού δεν μπορούμε να γνωρίζουμε αν οι IPv4 Addresses αντιστοιχούν σε ενεργό κόμβο, τα πακέτα φεύγουν κανονικά. Τέλος δεδομένου ότι διέρχονται από τον DNS μας, στην περίπτωση του εξωτερικού δικτύου, παίρνουμε απάντηση από αυτόν το πακέτο τύπου 3 Destination Unreachable, κάτι που στο τοπικό μας δίκτυο δεν συμβαίνει.

Άσκηση 3

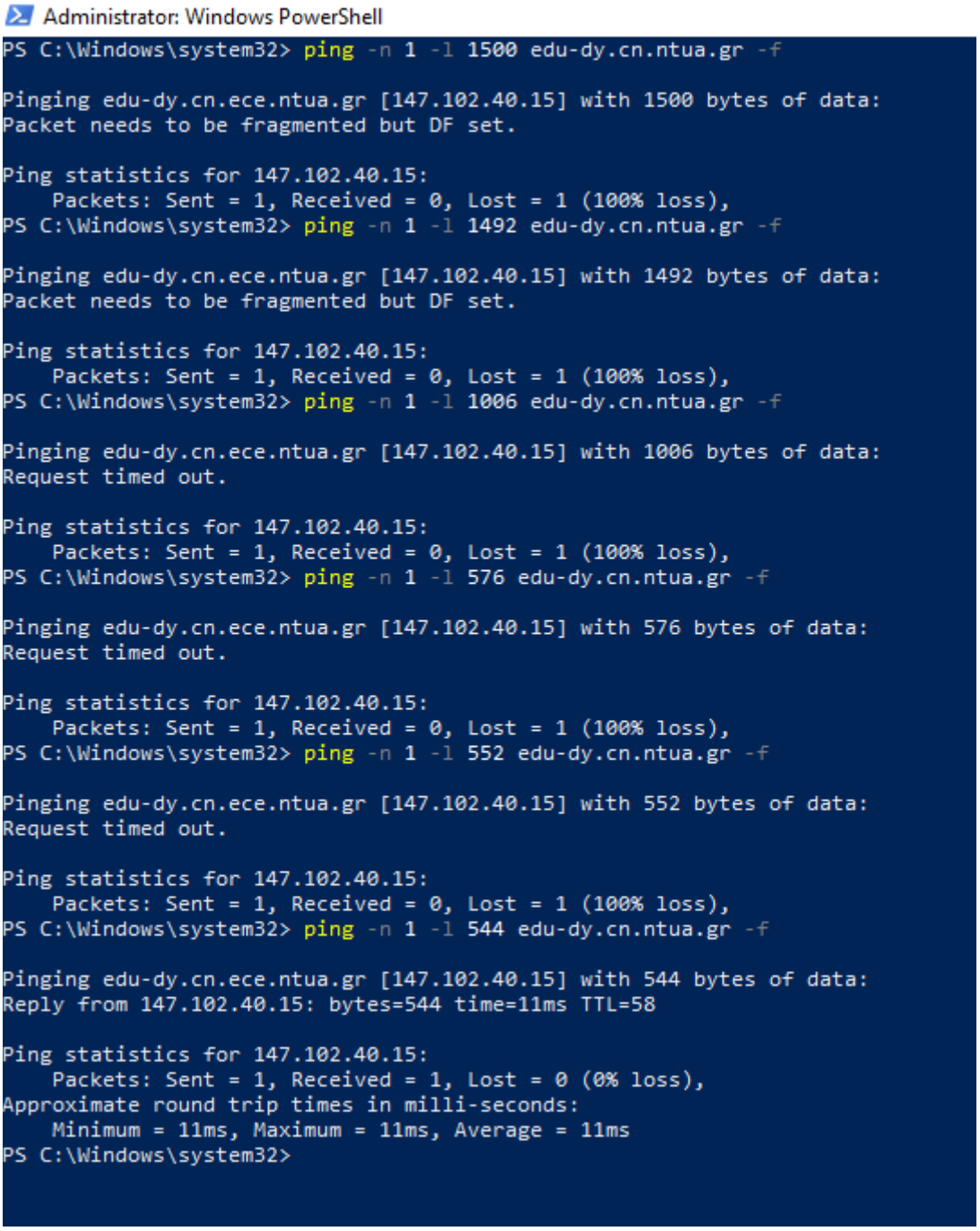
3.1) 64 bytes και μηδενικά
3.2)
Με ping ήταν 32 bytes ενώ τώρα τα διπλάσια
Με ping ήταν οι αύξοντες αριθμοί, ενώ τώρα μηδενικά
3.3) Παρατηρώ το μύνημα “Time-to-live exceeded (Time to live exceeded in transit)”.
3.4)

```
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
```

3.5)
Checksum: 2 bytes
Unused: 1 byte
3.6) 40 bytes
3.7) Το περιεχόμενο του μυνήματος λάθους είναι το IPv4 header του ληφθέντος ICMP request μυνήματος στον κόμβο καθώς και τα πρώτα 64 bit (8 bytes) του ICMP request μυνήματος που έλαβε. (Κάποιοι από τους κόμβους επιστρέφουν και 40 bytes από το περιεχόμενο του ICMP request).

Άσκηση 4

4.1) 1500, 1492, 1006, 576, 552, 544



4.2) Ναι παρατήρησα

4.3) Το παρήγαγε το router μου. Φαίνεται από την source διεύθυνση IPv4, 192.168.1.1.

4.4) Type: 3 (0x03), Code: 4 (0x04)

4.5) Το Code: 4 δηλώνει ότι χρειαζόταν θρυμματισμός, ενώ η τιμή του πεδίου “MTU Next-Hop” είναι 1492.

4.6) Περιέχει την Επικεφαλίδα IPv4 και ICMP καθώς και 520 bytes από το δεδομένα ICMP request

που έλαβε ο κόμβος αυτός.
4.7) 1492 bytes
4.8) Δεν απαντά για τις τιμές: 1500, 1492, 1006, 576, 552.
4.9) Η 544
4.10) Το MTU που εμφανίζεται είναι ενός ενδιάμεσου κόμβου. Με την εντολή tracert -4 147.102.40.15 βρίσκω το μονοπάτι που ακολουθήθηκε, στέλνω Echo Requests σε έναν έναν από τους ενδιάμεσους κόμβους και παρατηρώ ότι πάντα σταματάει η μετάδοση του πακέτου προτού φτάσω στον κόμβο προορισμού και πιο συγκεκριμένα, στον κόμβο grnet-2.gr-ix.gr [176.126.38.31]
4.11) Επειδή ο κόμβος που παρήγαγε το μήνυμα μαλλον έβαλε στα δεδομένα όλη την πληροφορία που έλαβε και έτσι ξεπέρασε το MTU σε κάποιο από τους κόμβους επιστροφής(αφού δεν είναι ααπαραίτητα οι ίδιοι κόμβοι με αυτούς που περνάει όταν πηγαίνει ως εκεί)
4.12) Από την εντολή παράγονται 2 θραύσματα. Το μέγεθος του πακέτου συνολικά είναι 1514 Bytes, τα 14 Bytes είναι του Ethernet II, ενώ τα 20 προέρχονται από την επικεφαλίδα του IPv4 και τα υπόλοιπα 1480 αποτελούν τα δεδομένα. Προφανώς, οι τιμές είναι διάφορες του 1492.

Άσκηση 5

5.1) ip host <ip> (το ip είναι το 147.102.40.15)
5.2) nslookup <ip> edu-dy.cn.ntua.gr (το ip είναι το 147.102.40.15)
5.3) Θέλει να μας δείξει ότι η διεύθυνση του DNS δεν ακούει την συγκεκριμένη θύρα(port)

```
PS C:\Windows\system32> nslookup 147.102.40.15 edu-dy.cn.ntua.gr
Server:  UnKnown
Address:  147.102.40.15

*** UnKnown can't find 147.102.40.15: No response from server
PS C:\Windows\system32>
```

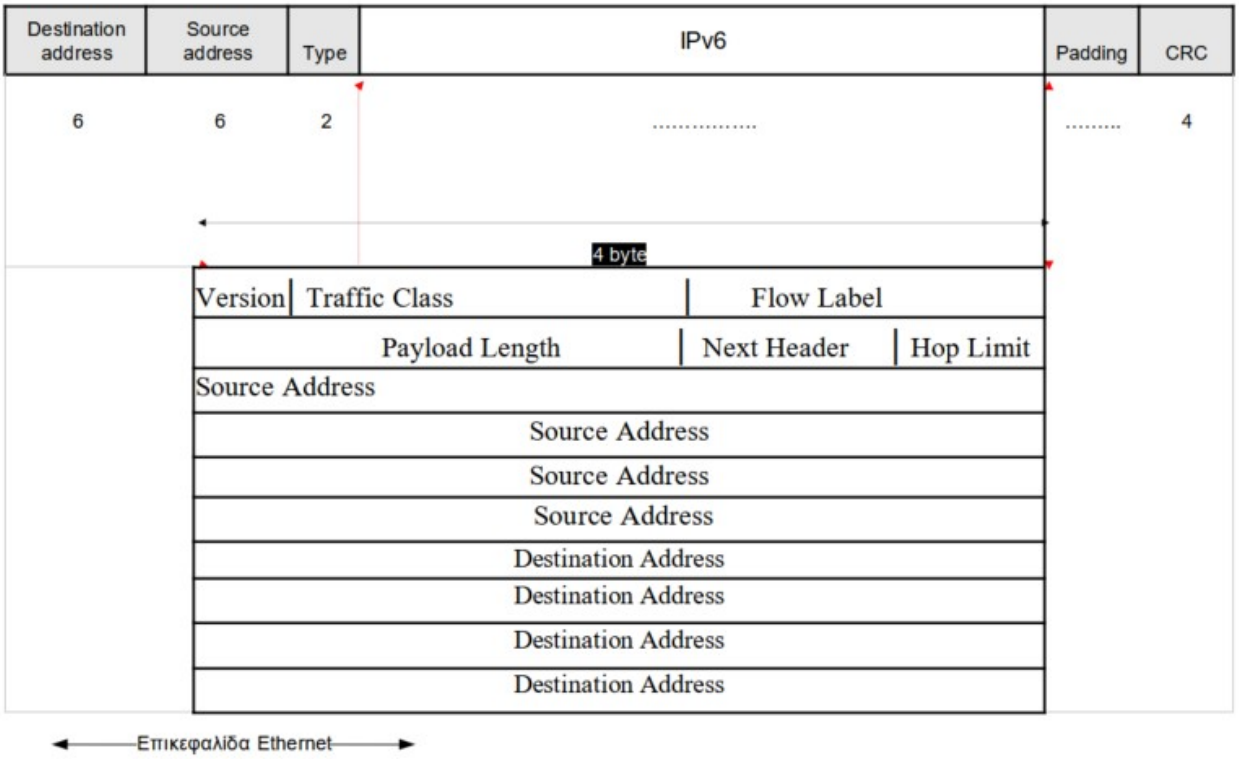
5.4) Ναι, παρατήρησα
5.5) Το πρωτόκολλο μεταφοράς είναι το UDP και η θύρα προορισμού η 53
5.6) Ναι παρατήρησα
5.7) Type: 3 (0x03) Code: 3(0x03)
5.8) Το πεδίο Code
5.9) Η θύρα 53 είναι προκαθορισμένη για χρήση DNS Queries
5.10) Με tracert και ίδιο φίλτρο σύληψης παρατήρησα ότι απαντά με το ίδιο ακριβώς μήνυμα, Destination Unreachable (Port Unreachable)

Άσκηση 6

6.1)

```
PS C:\Windows\system32> ping -6 2001:648:2000:329::101

Pinging 2001:648:2000:329::101 with 32 bytes of data:
Request timed out.
Reply from 2001:648:2000:329::101: time=8ms
Reply from 2001:648:2000:329::101: time=8ms
Reply from 2001:648:2000:329::101: time=8ms

Ping statistics for 2001:648:2000:329::101:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 8ms, Average = 8ms
PS C:\Windows\system32> 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  2a02:587:4f0f:632e:3a02:deff:fef8:9a0
  2     *        *        *     Request timed out.
  3     *        6 ms     *     2a02:580:50da:4a4::
  4     *        *        *     Request timed out.
  5     7 ms     7 ms     8 ms  grnet.gr-ix.gr [2001:7f8:6e::1]
  6     7 ms     7 ms     7 ms  kolettir-eier-AE.backbone.grnet.gr [2001:648:2ff2:101::1]
  7    10 ms    18 ms    10 ms  ntua-zogr-2.kolettir.access-link.grnet.gr [2001:648:2ffd:3323:2::2]
  8     8 ms    12 ms     8 ms  2001:648:2000:329::101

Trace complete.
PS C:\Windows\system32>
```

6.2) ip6, icmpv6
6.3) Type: IPv6 (0x86dd)
6.4) 40 bytes
6.5) Version: 4 bits, Traffic Class: 8 bits, Flow Label: 4 bits + 2 bytes, Payload Length: 2 bytes, Next Header: 1 byte, Hop Limit: 1 byte, Source Address: 16 bytes, Destination Address: 16 bytes



6.6) Είναι το Hop Limit
6.7) Είναι το Next Header και η τιμή της για ICMPv6 είναι 58 (0x3a)
6.8) Ναι είναι ίδια
6.9) Η τιμή του πεδίου Type είναι 128 (0x80) και το μήκος των δεδομένων του είναι 8 bytes.
6.10) Ναι είναι ίδια.
6.11) Η τιμή του πεδίου Type είναι 129 (0x81) και το μήκος των δεδομένων του είναι 8 bytes.
6.12) Διαφέρουν σε όλα τα πεδία εκτός από το Type και το Code.
6.13) Δεν είναι ίδια, διαφέρει μόνο στο ότι τώρα έχει το πεδίο Reversed εκεί που πρίν είχε το πεδίο Unused
6.14) Η τιμή του πεδίου Type είναι 3 (0x03) και το μήκος των δεδομένων του είναι 56 bytes.
6.15) Τις επικεφαλίδες των IPv6 και ICMPv6 του μηνύματος που έλαβα μαζί με τα δεδομένα αυτού του μηνύματος.
6.16) Ναι, παρατήρησα μηνύματα ICMPv6 Neighbor Solicitation
6.17) Type: Neighbor Solicitation (135)(0x87) με μήκος δεδομένων 32 bytes
Και Type: Neighbor Advertisement (136) (0x88) με μήκος δεδομένων 32 bytes