ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 6: ΠΡΩΤΟΚΟΛΛΟ ICMP

15 ΝΟΕΜΒΡΙΟΥ, 2022

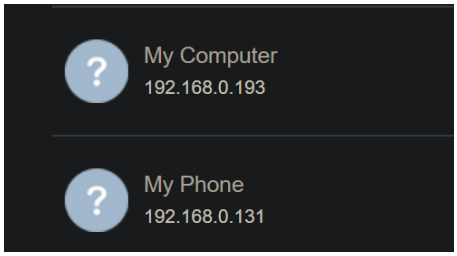
ΘΟΔΩΡΗΣ ΑΡΑΠΗΣ – EL18028

Ονοματεπώνυμο: Θοδωρής Αράπης	**Ομάδα:** 2
Όνομα PC/ΛΣ: DESKTOP-JGHL94V/ WINDOWS 10	**Ημερομηνία:** 15/11/2022
Διεύθυνση IP: 192.168.0.193	**Διεύθυνση MAC:** 70-85-C2-88-FD-B1

Η εργασία ξεκίνησε στο Pclab της σχολής αλλά για συνοχή επιλέχθηκε να γίνει εξολοκλήρου στο σπίτι.

Άσκηση 1: Εντολή ping στο τοπικό υποδίκτυο

Κάνουμε ping προς την διεύθυνση IPv4 (192.168.0.131) του κινητού μας που βρίσκεται στο τοπικό δίκτυο.



1.1

Το φίλτρο σύλληψης είναι το εξής: «ether host 70:85:C2:88:FD:B1»

1.2

Το φίλτρο απεικόνισης είναι το εξής: «arp or icmp»

1.3

Τα πακέτα ARP που καταγράφηκαν, έχουν ως σκοπό να ενημερώσουν το default gateway, σχετικά με τη MAC διεύθυνσή μας, δεδομένης της IPv4 διεύθυνσής μας, καθώς και για την MAC διεύθυνση του κινητού μας, προς το οποίο κάναμε ping, όπως και βλέπουμε παρακάτω

1	0.000000	58:d9:d5:5a:99:50	70:85:c2:88:fd:b1	ARP	60	Who has 192.168.0.193? Tell 192.168.0.1
2	0.000026	70:85:c2:88:fd:b1	58:d9:d5:5a:99:50	ARP	42	192.168.0.193 is at 70:85:c2:88:fd:b1
8	4.564364	70:85:c2:88:fd:b1	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.0.131? Tell 192.168.0.193
9	4.778816	70:5f:a3:b1:cf:56	70:85:c2:88:fd:b1	ARP	60	192.168.0.131 is at 70:5f:a3:b1:cf:56
26	10.021410	70:5f:a3:b1:cf:56	70:85:c2:88:fd:b1	ARP	60	Who has 192.168.0.193? Tell 192.168.0.131
27	10.021438	70:85:c2:88:fd:b1	70:5f:a3:b1:cf:56	ARP	42	192.168.0.193 is at 70:85:c2:88:fd:b1
30	11.009930	58:d9:d5:5a:99:50	70:85:c2:88:fd:b1	ARP	60	Who has 192.168.0.193? Tell 192.168.0.1
31	11.009951	70:85:c2:88:fd:b1	58:d9:d5:5a:99:50	ARP	42	192.168.0.193 is at 70:85:c2:88:fd:b1

1.4

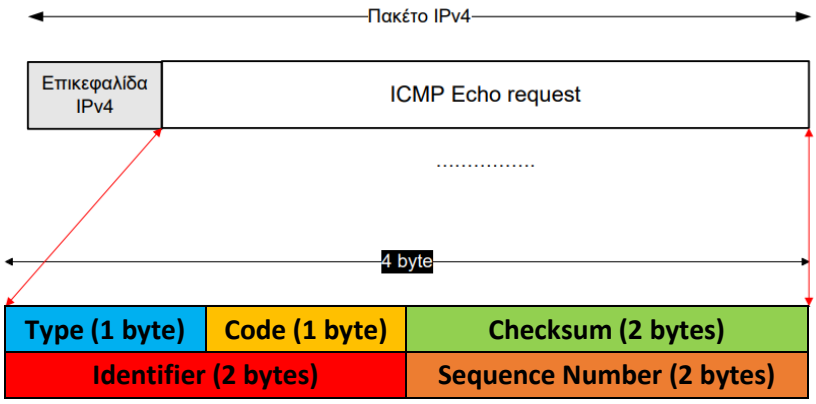
Το όνομα και η τιμή, αντίστοιχα, του πεδίου της επικεφαλίδας IPv4 που προσδιορίζει πως πρόκειται για ICMP μήνυμα, είναι το Protocol με τιμή 0x01.

1.5

Η επικεφαλίδα των ICMP Echo Request μηνυμάτων είναι 8 bytes.

1.6

Μπορούμε να χρησιμοποι



Η θέση τους είναι αυτή που φαίνεται στο σχήμα.

1.7

Type: 0x08 (Echo (ping) request)

Code: 0x00

1.8

Identifier: 1 (0x0001) σε Big Endian / 256 (0x0100) σε Little Endian

Sequence Number: 16 (0x0010) σε Big Endian / 4096 (0x1000) σε Little Endian

1.9

Το πεδίο δεδομένων των μηνυμάτων ICMP Echo request είναι 32 bytes και αποτελείται από τα εξής δεδομένα:

Data: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69

ASCII representation: a b c d e f g h i j k l m n o p q r s t u v w a b c d e f g h i

1.10

Εξετάζοντας ένα μήνυμα ICMP Echo Reply, βλέπουμε πως και αυτό έχει επικεφαλίδα μήκους 8 bytes και δομή ίδια με των αντίστοιχων request.

1.11

Type: 0x00 (Echo (ping) reply)

Code: 0x00

1.12

Το είδος των μηνυμάτων ICMP καθορίζεται από το πεδίο Type, για το οποίο έχουμε την τιμή 0 εάν πρόκειται για reply και 8 αν πρόκειται για request.

1.13

Identifier: 1 (0x0001) σε Big Endian / 256 (0x0100) σε Little Endian

Sequence Number: 16 (0x0010) σε Big Endian / 4096 (0x1000) σε Little Endian

1.14

Επειδή είχαμε επιλέξει αυθαίρετα το πρώτο ICMP Echo reply, οι τιμές του αντίστοιχου request είναι αυτές που είχαμε βρει νωρίτερα (πρώτο request πακέτο) και ίδιες με αυτές του reply.

1.15

Με βάση την σελίδα που δίνεται βλέπουμε ότι Ο ρόλος των πεδίων Identifier και Sequence Number είναι να βοηθούν στην αντιστοίχιση των echo requests με το αντίστοιχο echo reply.

1.16

Το μήκος του πεδίου δεδομένων των μηνυμάτων ICMP Echo reply, είναι επίσης 32 bytes και έχει ακριβώς τα ίδια δεδομένα με το request, δηλαδή:

Data: 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69

ASCII representation: a b c d e f g h i j k l m n o p q r s t u v w a b c d e f g h i

1.17

Όχι, δεν διαφέρει από το περιεχόμενο του αντίστοιχου request.

1.18

Το Wireshark κατέγραψε 4 μηνύματα echo request και άλλα 4 echo reply. Πράγμα αναμενόμενο καθώς by default η εντολή ping στέλνει 4 πακέτα και περιμένει απάντηση για το καθένα από αυτά.

```
C:\WINDOWS\system32>ping -4 192.168.0.131

Pinging 192.168.0.131 with 32 bytes of data:
Reply from 192.168.0.131: bytes=32 time=222ms TTL=64
Reply from 192.168.0.131: bytes=32 time=121ms TTL=64
Reply from 192.168.0.131: bytes=32 time=34ms TTL=64
Reply from 192.168.0.131: bytes=32 time=49ms TTL=64

Ping statistics for 192.168.0.131:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 34ms, Maximum = 222ms, Average = 106ms
```

Όπως φαίνεται και στην εικόνα, έχουμε 4 replies και από κάτω μας γράφει ότι στάλθηκα 4 πακέτα και ελήφθησαν 4.

1.19

Η σύνταξη της εντολής είναι: «ping -n 2 192.168.0.25»

```
C:\WINDOWS\system32>ping -4 -n 2 192.168.0.25

Pinging 192.168.0.25 with 32 bytes of data:
Reply from 192.168.0.193: Destination host unreachable.
Reply from 192.168.0.193: Destination host unreachable.

Ping statistics for 192.168.0.25:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
```

1.20

Από το Wireshark, βλέπουμε πως στάλθηκαν 6 ARP πακέτα για την ανεύρεση της MAC του υπολογιστή:

2.015135	70:85:c2:88:fd:b1	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.0.25? Tell 192.168.0.193
0.918533	70:85:c2:88:fd:b1	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.0.25? Tell 192.168.0.193
1.000429	70:85:c2:88:fd:b1	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.0.25? Tell 192.168.0.193
0.996090	70:85:c2:88:fd:b1	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.0.25? Tell 192.168.0.193
1.006561	70:85:c2:88:fd:b1	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.0.25? Tell 192.168.0.193
0.997429	70:85:c2:88:fd:b1	ff:ff:ff:ff:ff:ff	ARP	42	Who has 192.168.0.25? Tell 192.168.0.193

1.21

Όπως βλέπουμε από το screenshot παραπάνω, στέλνονται κάθε 1 δευτερόλεπτο περίπου.

1.22

Δε στάλθηκε κανένα ICMP πακέτο.

1.23

Παρατηρούμε ότι η εντολή ping στέλνει τριάδες ARP πακέτων για κάθε πακέτο n, όπου n η τιμή των πακέτων που ορίζουμε να στείλει η εντολή ping στην σύνταξή της (οπότε συνολικά 3·n πακέτα). Εφόσον τα αποτελέσματα του ping ήταν την πρώτη φορά «Destination Host Unreachable» και τα 3 ARP πακέτα δε βρήκαν MAC που να αντιστοιχεί στην αυθαίρετη IP που κάναμε Ping, στάλθηκε και η 2η τριάδα πακέτων, με τα ίδια, ωστόσο, αποτελέσματα. Δηλαδή, τα πακέτα αυτά έγιναν broadcast στο τοπικό μας δίκτυο (με την ερώτηση «Who has 192.168.0.25») χωρίς όμως να λάβουν κάποια απόκριση.

Άσκηση 2: Εντολή ping σε άλλο υποδίκτυο

2.1

Ο πίνακας ARP πριν και μετά την καταγραφή είναι:

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.56.1 --- 0xd
  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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.0.193 --- 0x13
  Internet Address      Physical Address      Type
  192.168.0.1           58-d9-d5-5a-99-50     dynamic
  192.168.0.131         70-5f-a3-b1-cf-56     dynamic
  192.168.0.255         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: 172.17.96.1 --- 0x37
  Internet Address      Physical Address      Type
  172.17.111.255        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
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Δεν παρατηρήθηκε καμία αλλαγή μετά την εντολή ping.

2.2

Από την επικεφαλίδα Ethernet βλέπουμε ότι οι διευθύνσεις MAC αποστολέα και παραλήπτη είναι αντίστοιχα:

Source: 70-85-C2-88-FD-B1 (δική μας)

Destination: 58-D9-D5-5A-99-50

2.3

Από την επικεφαλίδα IPv4 βλέπουμε ότι οι διευθύνσεις MAC αποστολέα και παραλήπτη είναι αντίστοιχα:

Source: 192.168.0.193 (δική μας)

Destination: 147.102.1.1

2.4

Κοιτάζοντας τον πίνακα ARP βλέπουμε ότι οι MAC διευθύνσεις αντιστοιχούν:

Source: 70-85-C2-88-FD-B1/ [192.168.0.193] (δική μας)

Destination: 58-D9-D5-5A-99-50 /[192.168.0.1] (default gateway)

2.5

Ναι, καταγράφηκαν 2 πακέτα ARP.

52	3.426148	58:d9:d5:5a:99:50	70:85:c2:88:fd:b1	ARP	60	Who has 192.168.0.193? Tell 192.168.0.1
53	0.000029	70:85:c2:88:fd:b1	58:d9:d5:5a:99:50	ARP	42	192.168.0.193 is at 70:85:c2:88:fd:b1

2.6

Τα πακέτα αυτά (όπως φαίνεται και από την καταγραφή παραπάνω) αποτελούν ένα ζεύγος ερωταπαντήσεων που πραγματοποιεί ο default gateway (ρωτάει κάνοντας broadcast) με την υπολογιστή μας (απαντάει), ώστε να πληροφορηθεί για την διεύθυνση MAC του υπολογιστή μας.

2.7

Εφαρμόζουμε το φίλτρο απεικόνισης «icmp.type==0» (όπου 0 το Type που αντιστοιχεί στα ICMP Echo Reply όπως είδαμε).

icmp.type==0

No.	Time	Source	Destination	Protoc	Lengt	Info
41	23:50:15.193847	147.102.1.1	192.168.0.193	ICMP	74	Echo (ping) reply id=0x0001, seq=24/6144, ttl=56 (request in 40)
43	23:50:16.198622	147.102.1.1	192.168.0.193	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=56 (request in 42)
45	23:50:17.208509	147.102.1.1	192.168.0.193	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=56 (request in 44)
47	23:50:18.213659	147.102.1.1	192.168.0.193	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=56 (request in 46)

2.8

Το TTL που βλέπουμε στις απαντήσεις του παραθύρου εντολών, αλλά και στο Wireshark προφανώς, έχει τιμή 56. Γνωρίζουμε ότι σε *nix συστήματα (Unix/Linux) η default τιμή είναι 64, επομένως εύλογα υποθέτουμε πως παρεμβάλλονται 8 κόμβοι από τον host με IP 147.102.1.1 μέχρι τον υπολογιστή μας (αφού κάθε κόμβος από τον οποίο περνάει το πακέτο μειώνει το TTL του κατά 1). Εάν κάνουμε tracert εκεί, επιβεβαιώνουμε το παραπάνω:

```
C:\WINDOWS\system32>tracert 147.102.1.1

Tracing route to theseas.softlab.ece.ntua.gr [147.102.1.1]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2    <1 ms    <1 ms    <1 ms  speedport.ip [192.168.1.1]
  3     9 ms     8 ms     8 ms  80.106.125.100
  4     9 ms     8 ms     9 ms  79.128.224.21
  5     8 ms     8 ms     8 ms  79.128.250.87
  6     9 ms     9 ms     9 ms  grnet-2.gr-ix.gr [176.126.38.31]
  7    10 ms    10 ms     9 ms  eier-kolettir-AE.backbone.grnet.gr [62.217.100.63]
  8    11 ms    11 ms    11 ms  ntua-zogr-3.eier.access-link.grnet.gr [62.217.96.169]
  9    10 ms    11 ms    10 ms  theseas.softlab.ece.ntua.gr [147.102.1.1]
```

2.9

Εμφανίζονται μόνο μηνύματα τύπου ICMP Echo (ping) request.

1	03:24:25.728139	192.168.0.193	147.102.7.90	ICMP	74	Echo (ping) request id=0x0001, seq=55/14080, ttl=64 (no response found!)
6	03:24:30.313151	192.168.0.193	147.102.7.90	ICMP	74	Echo (ping) request id=0x0001, seq=56/14336, ttl=64 (no response found!)
7	03:24:35.320720	192.168.0.193	147.102.7.90	ICMP	74	Echo (ping) request id=0x0001, seq=57/14592, ttl=64 (no response found!)
13	03:24:40.320584	192.168.0.193	147.102.7.90	ICMP	74	Echo (ping) request id=0x0001, seq=58/14848, ttl=64 (no response found!)

2.10

Αριστερά φαίνεται η καταγραφή για το ping σε ανενεργό υπολογιστή εντός του υποδικτύου μας και δεξιά εκτός.

```
C:\WINDOWS\system32>ping -4 -n 2 192.168.0.25

Pinging 192.168.0.25 with 32 bytes of data:
Reply from 192.168.0.193: Destination host unreachable.
Reply from 192.168.0.193: Destination host unreachable.

Ping statistics for 192.168.0.25:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
```

```
C:\WINDOWS\system32>ping 147.102.7.90

Pinging 147.102.7.90 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 147.102.7.90:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Παρατηρούμε ότι στην περίπτωση εντός του υποδικτύου μας λαμβάνουμε απάντηση «Destination host Unreachable», ενώ στην περίπτωση εκτός λαμβάνουμε «Request timed out». Μελετώντας καλύτερα την καταγεγραμμένη κίνηση, βλέπουμε πως κάνοντας ping σε κόμβο εκτός του υποδικτύου μας δε εντοπίζουμε κανένα ARP πακέτο. Ο

λόγος που συμβαίνει αυτό είναι πως στην πρώτη περίπτωση που είμαστε σε κοινό υποδίκτυο, η επικοινωνία γίνεται στο Layer 2 όπου απαιτούνται MAC διευθύνσεις, κάτι που ήταν άγνωστο για την για το μηχάνημα με την IP στην οποία κάναμε ping. Όταν, όμως, κάναμε ping σε κόμβο εκτός του υποδικτύου μας, η δρομολόγηση πραγματοποιήθηκε στο Layer 3 (Network), όπου απαιτείται η γνώση της IP διεύθυνση του κόμβου-στόχου, την οποία και παρείχαμε, επιτρέποντας στον δρομολογητή να προωθήσει κανονικά το πακέτο εκτός του υποδικτύου μας. Επιπλέον, στην περίπτωση αυτή χρειάζεται η MAC διεύθυνση του default gateway, την οποία ο υπολογιστής μας ήξερε ήδη οπότε και δε χρειάστηκαν ARP πακέτα.

Άσκηση 3: Εντολή tracert/traceroute

3.1

Το μήκος του πεδίου δεδομένων των μηνυμάτων ICMP Echo Request είναι 64bytes και αποτελείται από 64 μηδενικά (χαρακτήρας ASCII: '0').

3.2

Παρατηρούμε πως σε σχέση με τα ICMP μηνύματα του ping, διαφέρουν και ως προς το μήκος των δεδομένων (64 αντί 32 bytes) αλλά και ως προς το περιεχόμενο (0000… αντί για abcd….), όπως είδαμε στο ερώτημα 1.9.

3.3

Στους ενδιάμεσους κόμβους παρατηρούμε το μήνυμα «Time-to-live exceeded».

3.4

Το παραπάνω μήνυμα λάθους έχει τις εξής τιμές στα ζητούμενα πεδία:

Type: 11 (0x0b) (Time-to-live exceeded)

Code: 0 (0x00) (Time to live exceeded in transit).

3.5

Πριν τα δεδομένα, η επικεφαλίδα του μηνύματος λάθους έχει επιπλέον τα πεδία Checksum (2 bytes) και Unused (4 bytes).

3.6

Η επικεφαλίδα του ανωτέρω μηνύματος λάθους είναι 8 bytes, ενώ τα δεδομένα 92 bytes.

3.7

Τα δεδομένα του προηγούμενου ICMP μηνύματος λάθους που εξετάσαμε είναι η IPv4 διεύθυνση του πακέτου που προκάλεσε το μήνυμα λάθους, μαζί με όσα περισσότερα δεδομένα χωράνε, ωσότου το πακέτο ICMP φτάσει τα 576 bytes.

Άσκηση 4: Ανακάλυψη MTU διαδρομής (Path MTU Discovery)

4.1

Γνωρίζουμε ότι το MTU προκύπτει ως το άθροισμα των IP header length, ICMP header length και ICMP Payload length, δηλαδή:

$$MTU = IP\ header\ length\ (20\ bytes) + ICMP\ header\ length\ (8\ bytes) + ICMP\ Payload\ Length \Longrightarrow$$

$$ICMP\ Payload\ length\ =\ MTU\ -\ 28bytes$$

Επομένως, οι τιμές μήκους δεδομένων θα προκύψουν από το επιθυμητό MTU size αφαιρώντας 28 bytes για κάθε τιμή. Οπότε έχουμε τις αντιστοιχίσεις:

MTU Size (bytes)	ICMP Payload Size (bytes)
1500	1472
1492	1464
1006	978
576	548
552	524
544	516
512	484
508	480
296	268

Με βάση τις παραπάνω τιμές τρέχουμε την ζητούμενη εντολή ping μέχρι να λάβουμε απάντηση. Τα αποτελέσματα της καταγραφής του Wireshark και της εντολής ping είναι:

1	17:14:17.454402	192.168.0.193	147.102.40.15	ICMP	1506	Echo (ping) request id=0x0001, seq=93/23808, ttl=64 (no response found!)
2	17:14:24.124219	192.168.0.193	147.102.40.15	ICMP	1020	Echo (ping) request id=0x0001, seq=94/24064, ttl=64 (no response found!)
3	17:14:29.207467	192.168.0.193	147.102.40.15	ICMP	590	Echo (ping) request id=0x0001, seq=95/24320, ttl=64 (reply in 4)
4	17:14:29.219645	147.102.40.15	192.168.0.193	ICMP	590	Echo (ping) reply id=0x0001, seq=95/24320, ttl=56 (request in 3)

```
C:\Users\Theodore>ping -n 1 -f -l 1472 edu-dy.cn.ntua.gr

Pinging edu-dy.cn.ece.ntua.gr [147.102.40.15] with 1472 bytes of data:
Packet needs to be fragmented but DF set.

Ping statistics for 147.102.40.15:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

C:\Users\Theodore>ping -n 1 -f -l 1464 edu-dy.cn.ntua.gr

Pinging edu-dy.cn.ece.ntua.gr [147.102.40.15] with 1464 bytes of data:
Request timed out.

Ping statistics for 147.102.40.15:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

C:\Users\Theodore>ping -n 1 -f -l 978 edu-dy.cn.ntua.gr

Pinging edu-dy.cn.ece.ntua.gr [147.102.40.15] with 978 bytes of data:
Request timed out.

Ping statistics for 147.102.40.15:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

C:\Users\Theodore>ping -n 1 -f -l 548 edu-dy.cn.ntua.gr

Pinging edu-dy.cn.ece.ntua.gr [147.102.40.15] with 548 bytes of data:
Reply from 147.102.40.15: bytes=548 time=12ms TTL=56

Ping statistics for 147.102.40.15:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 12ms, Average = 12ms
```

4.2, 4.3

Όχι, δε παρατηρήθηκε μήνυμα λάθους ICMP Destination Unreachable.

4.4

Το μήνυμα λάθους Destination unreachable (από την καταγραφή mtu.pcap) έχει τις εξής τιμές στα ζητούμενα πεδία:

Type: 3 (0x0b) (Destination unreachable)

Code: 4 (0x00) ((Fragmentation needed).

4.5

Το πεδίο, το οποίο υποδεικνύει ότι το λάθος οφείλεται στην απαίτηση μη θρυμματισμού είναι το Code: 4 (Fragmentation needed) της επικεφαλίδας ICMP. Το πεδίο MTU of next hop έχει τιμή 1492

4.6

Το πεδίο δεδομένων του παραπάνω μηνύματος περιλαμβάνει την IP και ICMP επικεφαλίδα του ICMP ping request μηνύματος που το προκάλεσε.

4.7

Για καμία MTU δε λάβαμε μήνυμα ICMP Destination Unreachable, επομένως η MTU για την οποία δε λαμβάνουμε μήνυμα ICMP Destination Unreachable για πρώτη φορά είναι 1500 bytes. Για την δοσμένη καταγραφή mtu.pcap βλέπουμε ότι δεν λαμβάνει μήνυμα ICMP Destination Unreachable για πρώτη φορά στο MTU = 1492.

4.8

Σταματήσαμε την καταγραφή προηγουμένως, όταν το ICMP Payload είχε μήκος 548 bytes - όπου και λάβαμε απάντηση από το 147.102.40.15-, επομένως, δοκιμάζουμε να αυξήσουμε το μέγεθος μέχρι να πάρουμε ως απάντηση το μήνυμα Request Timed out. Το λαμβάνουμε για πρώτη φόρα για ICMP Payload Length = 549 bytes, το οποίο αντιστοιχεί σε MTU (549 + 28) = 577 bytes. Άρα για κάθε MTU ≥ 577 bytes, το 147.102.40.15 δεν απαντά.

```
C:\Users\Theodore>ping -n 1 -f -l 548 edu-dy.cn.ntua.gr

Pinging edu-dy.cn.ece.ntua.gr [147.102.40.15] with 548 bytes of data:
Reply from 147.102.40.15: bytes=548 time=12ms TTL=56

Ping statistics for 147.102.40.15:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 12ms, Average = 12ms

C:\Users\Theodore>ping -n 1 -f -l 549 edu-dy.cn.ntua.gr

Pinging edu-dy.cn.ece.ntua.gr [147.102.40.15] with 549 bytes of data:
Request timed out.

Ping statistics for 147.102.40.15:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
```

4.9

Η μικρότερη από τις παραπάνω MTU για την οποία λαμβάνουμε απάντηση είναι τα 576 bytes.

4.10

Μελετώντας το documentation συμπεραίνουμε πως όταν ένας δρομολογητής αδυνατεί να προωθήσει ένα δεδομενόγραμμα, επειδή έχει μεγαλύτερο MTU από αυτό του επόμενου κόμβου και το bit Don’t Fragment είναι 1, τότε ο δρομολογητής αυτός απαιτείται να επιστρέψει ένα ICMP Destination Unreachable μήνυμα στην πηγή του datagram με το πεδίο Code να έχει τιμή “fragmentation needed and DF set”. (το MTU του next-hop network (επόμενου κόμβου) βρίσκεται στα τελευταία 16 bits του ICMP Header). Εφόσον για MTU 576 bytes δε λαμβάνουμε τέτοιο μήνυμα, σημαίνει πως το MTU αυτό είναι το πολύ ίσο σε σχέση με κάθε MTU στο μονοπάτι ειδάλλως θα απαιτούνταν κάπου fragmentation και θα παίρναμε ICMP Destination Unreachable μήνυμα. Συνεπώς, αφού

για MTU 577 bytes λαμβάνουμε τέτοια μηνύματα λάθους, τα 576 bytes ως MTU είναι πιθανό να αντιστοιχούν είτε στη δικτυακή διεπαφή ενός ενδιάμεσου κόμβου, είτε του 147.102.40.15.

4.11

Όπως είπαμε, το 147.102.40.15 δε προωθεί επιπλέον το πακέτο που λαμβάνει, επομένως και δεν απαντά με ICMP Destination Unreachable όταν λαμβάνει πακέτα IPv4 μεγαλύτερου μεγέθους του MTU της διεπαφής του.

4.12

Κάνουμε Ping χωρίς την απαίτηση μη θρυμματισμού με ICMP Payload 1472 bytes

```
C:\Users\Theodore>ping -n 1 -l 1472 edu-dy.cn.ntua.gr

Pinging edu-dy.cn.ece.ntua.gr [147.102.40.15] with 1472 bytes of data:
Reply from 147.102.40.15: bytes=1472 time=13ms TTL=56

Ping statistics for 147.102.40.15:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 13ms, Average = 13ms
```

Και στην καταγραφή λαμβάνουμε:

ip.addr==147.102.40.15

No.	Time	Source	Destination	Protoc	Length	Info
19	19:04:09.592618	192.168.0.193	147.102.40.15	IPv4	1506	Fragmented IP protocol (proto=ICMP 1, off=0, ID=eab0) [Reassembled in #20]
20	19:04:09.592618	192.168.0.193	147.102.40.15	ICMP	42	Echo (ping) request id=0x0001, seq=157/40192, ttl=64 (reply in 21)
21	19:04:09.605782	147.102.40.15	192.168.0.193	ICMP	1514	Echo (ping) reply id=0x0001, seq=157/40192, ttl=56 (request in 20)

Βλέπουμε ότι το πακέτο σπάει σε fragments κατά την διαδρομή του από εμάς προς τον host edu-dy.cn.ntua.gr. Το πακέτο απάντησης έρχεται ολόκληρο σε εμάς (1500 bytes), που σημαίνει πως λογικά πέρασε από διαφορετικούς ενδιάμεσους κόμβους.

Άσκηση 5: Απρόσιτη θύρα (Port Unreachable)

5.1

Χρησιμοποιήθηκε το φίλτρο σύλληψης «host 147.102.40.15 and ip»

5.2

Για την εντολή nslookup η σύνταξη που χρησιμοποιήθηκε είναι η «nslookup edu-dy.cn.ntua.gr 147.102.40.15», όπου το πρώτο όρισμα είναι το name της διεύθυνσης IP που ψάχνουμε, ενώ το δεύτερο όρισμα είναι η IP του DNS Server.

5.3

Στο παράθυρο εντολών λάβαμε την απάντηση «DNS request timed out».

```
C:\WINDOWS\system32>nslookup edu-dy.cn.ntua.gr 147.102.40.15
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  147.102.40.15

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

Μας ενημερώνει ότι μάλλον δεν ακούει κανένας εξυπηρετητής στην θύρα αυτή.

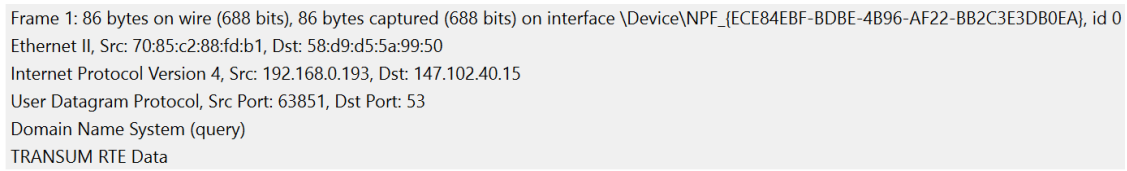
5.4

Ναι παρατηρούμε μηνύματα DNS στην καταγραφή.

1	0.000000	192.168.0.193	147.102.40.15	DNS	86	Standard query 0x0001 PTR 15.40.102.147.in-addr.arpa
2	0.010971	147.102.40.15	192.168.0.193	ICMP	70	Destination unreachable (Port unreachable)
3	2.001187	192.168.0.193	147.102.40.15	DNS	77	Standard query 0x0002 A edu-dy.cn.ntua.gr
4	0.010822	147.102.40.15	192.168.0.193	ICMP	70	Destination unreachable (Port unreachable)
5	2.000952	192.168.0.193	147.102.40.15	DNS	77	Standard query 0x0003 AAAA edu-dy.cn.ntua.gr
6	0.011616	147.102.40.15	192.168.0.193	ICMP	70	Destination unreachable (Port unreachable)
7	2.001455	192.168.0.193	147.102.40.15	DNS	77	Standard query 0x0004 A edu-dy.cn.ntua.gr
8	0.011249	147.102.40.15	192.168.0.193	ICMP	70	Destination unreachable (Port unreachable)
9	2.000477	192.168.0.193	147.102.40.15	DNS	77	Standard query 0x0005 AAAA edu-dy.cn.ntua.gr
10	0.011354	147.102.40.15	192.168.0.193	ICMP	70	Destination unreachable (Port unreachable)

5.5

Το πρωτόκολλο μεταφοράς των ανωτέρω DNS μηνυμάτων είναι το UDP με θύρα προορισμού την 53, όπως παρατηρούμε:



5.6

Ναι παρατηρήσαμε μηνύματα λάθους ICMP Destination Unreachable, όπως φαίνεται και στην καταγραφή παραπάνω.

5.7

Όλα τα ICMP μηνύματα αυτά έχουν:

Type: 3 (Destination Unreachable) και

Code : 3 (Port Unreachable)

5.8

Το πεδίο Code δηλώνει πως ο λόγος αποτυχίας είναι κάποια απρόσιτη θύρα.

5.9

Ενώ γνωρίζουμε πως η θύρα 53 αναφέρεται στο DNS, μπορούμε να το συμπεράνουμε από το Wireshark καθώς τα DNS queries γίνονται στη θύρα αυτή.

5.10

Δεν διαθέτουμε σύστημα Linux/Unix.

Άσκηση 6: IPv6 and ICMPv6

6.1

ping: «ping 2001:648:2000:329::101»

tracert: «tracert 2001:648:2000:329::101»

6.2

Το φίλτρο σύλληψης που χρησιμοποιήσαμε είναι το «ip6» και το φίλτρο απεικόνισης είναι το «icmpv6».

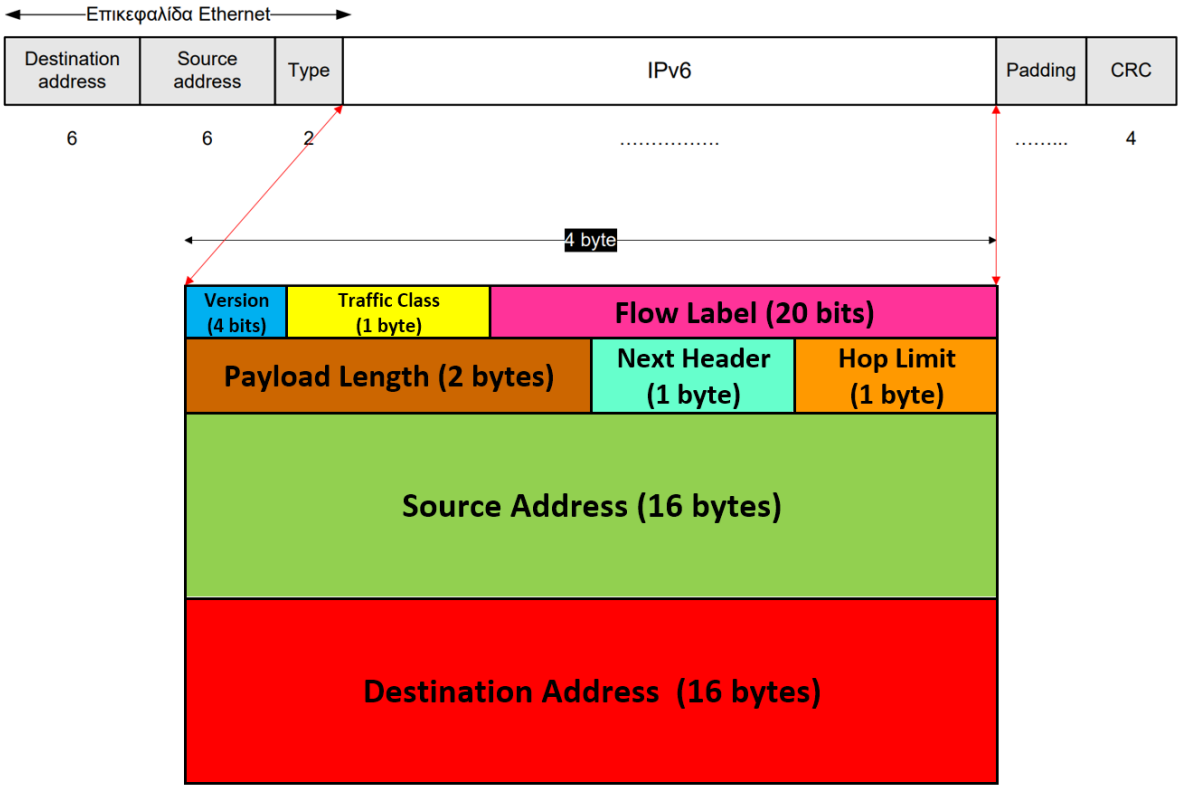
6.3

Το πεδίο Type έχει την τιμή: IPv6 (0x86dd).

6.4

Το μήκος επικεφαλίδας των πακέτων IPv6 είναι σταθερό σε όλα τα πακέτα και ίσο με 40bytes.

6.5



6.6

Η επικεφαλίδα Hop Limit είναι η αντίστοιχη της επικεφαλίδας TTL.

6.7

Η επικεφαλίδα Next Header δείχνει το πρωτόκολλο τα δεδομένα του οποίου μεταφέρει το πακέτο IPv6 με τιμή 58 για το ICMPv6 πρωτόκολλο.

6.8

Στην ερώτηση 1.6 είχαμε επικεφαλίδα πακέτου ICMP, επομένως η τρέχουσα επικεφαλίδα διαφέρει σε σχέση με αυτήν παρά το γεγονός πως παρουσιάζονται έντονες ομοιότητες σε κάποια πεδία.

6.9

Το ζητούμενο πεδίο έχει τιμή:

Type: 128 (0x80),

Ενώ το μήκος των δεδομένων που μεταφέρει είναι 32 bytes.

6.10

Ναι, το ICMPv6 Echo reply έχει ίδια δομή με το ICMPv6 Echo request.

6.11

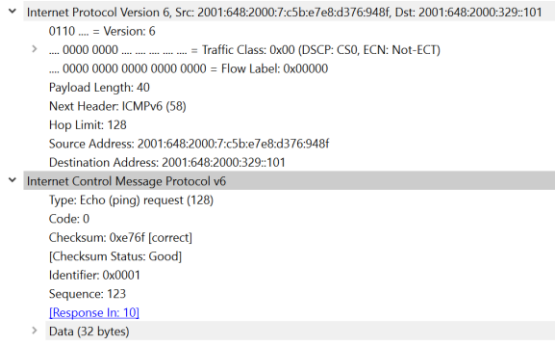
Το ζητούμενο πεδίο έχει τιμή:

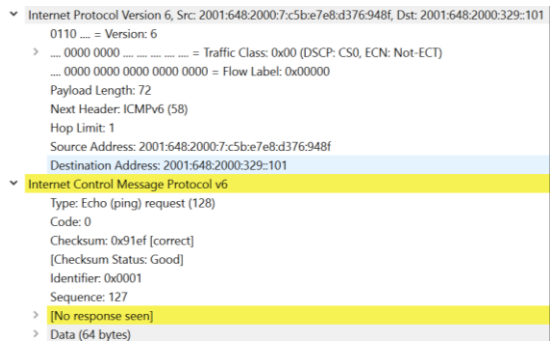
Type: 129 (0x81),

Ενώ το μήκος των δεδομένων που μεταφέρει είναι 32 bytes.

6.12

Αριστερά φαίνονται τα IPv6 και ICMPv6 headers του μηνύματος echo Request που παράγεται από την εντολή ping και αριστερά από την tracert.

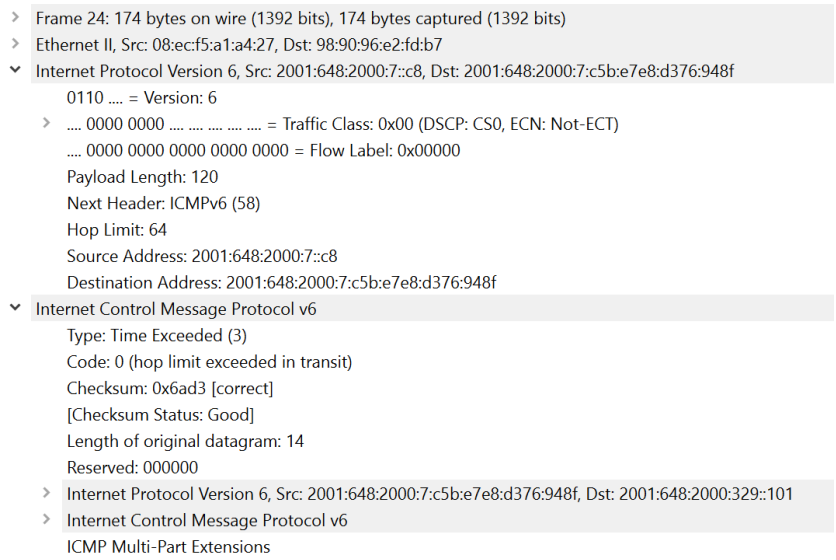




Βλέπουμε ότι έχουν διαφορετική τιμή Payload length (40 και 72 bytes αντίστοιχα, χωρίς την επικεφαλίδα ICMPv6 είναι 32 και 64 bytes), διαφορετική τιμή Hop Limit προφανώς (ping 128 και tracert 1) και τέλος έχουν άλλες τιμές στα πεδία Checksum και Sequence.

6.13

Η επικεφαλίδα ενός ICMPv6 Time Exceeded μηνύματος παρουσιάζει την παρακάτω δομή, η οποία δε διαφέρει από το αντίστοιχο ICMP Time Exceeded με εξαίρεση το πεδίο Reserved όπου προηγουμένως ήταν Unused.



6.14

Το ζητούμενο πεδίο έχει τιμή:

Type: Time Exceeded (3),

Ενώ το μήκος των δεδομένων που μεταφέρει είναι:

Data = Payload Lengrh - ICMPv6 Header = 120 – 8 = 112 bytes.

6.15

Αντίστοιχα με το ICMP, το πεδίο των δεδομένων περιέχει τους IPv6 και ICMPv6 headers του πακέτου που προκάλεσε το αυτό μήνυμα λάθους.

6.16

Πέρα από τα ping και tracert request/reply και το μήνυμα λάθους Time Exceeded, παρατηρήθηκαν τα ICMPv6 μηνύματα τύπου Neighbor Advertisement και Neighbor Solicitation.

6.17

Τα ICMPv6 μηνύματα τύπου Neighbor Solicitation / Neigbor Advertisement έχουν συνολικό μήκος 86 bytes (86 – 14 = 72 bytes αναφερόμενοι μόνο στο IPv6 πακέτο), ενώ το πεδίο Type έχει τιμές Neighbor Solicitation (135) και Neigbor Advertisement (136) αντίσοτιχα.