ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ: ΓΚΟΥΜΕ ΛΑΟΥΡΕΝΤΙΑΝ
ΑΜ: 031 18 014
ΕΞΑΜΗΝΟ: 7^{ο}
ΟΜΑΔΑ: 4
MAC ADDRESS: B4-69-21-1B-6C-FF
IPv4: Άσκ1: 10.3.20.6 καθώς και 10.3.20.29, Άσκ2/Άσκ3: 10.3.20.10, Ασκ4: 10.3.22.1, Άσκ5: 10.3.20.30
ΌΝΟΜΑ ΥΠΟΛΟΓΙΣΤΗ: LAPTOP-B2DVAJKK
ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ: WINDOWS 10

ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

ΕΡΓΑΣΤΗΡΙΑΚΗ ΑΣΚΗΣΗ 6: ΠΡΩΤΟΚΟΛΛΟ ICMP

Άσκηση 1: Εντολή ping στο τοπικό υποδίκτυο

1.1) Το φίλτρο σύλληψης είναι το εξής: **ether host b4:69:21:1b:6c:ff**.

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**, στο οποίο και στείλαμε το ping, **σχετικά με τη MAC διεύθυνσή** μας, δεδομένης της IPv4 διεύθυνσής μας, όπως και βλέπουμε παρακάτω:

```
35 7.280111   Fortinet_da:67… IntelCor_1b:6c… ARP      56 Who has 10.3.20.6? Tell 10.3.20.1
36 7.280162   IntelCor_1b:6c… Fortinet_da:67… ARP      42 10.3.20.6 is at b4:69:21:1b:6c:ff
```

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) Σχετικά με τα πεδία της επικεφαλίδας του μηνύματος ICMP Echo Request, έχουμε:

Πεδίο	**Τιμή**	**Θέση στην επικεφαλίδα (ν-οστο byte)**
Type (1 byte)	8 (0x08) (Echo (ping) request)	1ο
Code (1 byte)	0x00	2ο
Checksum (2 bytes)	0x4cb6	3ο και 4ο
Identifier (2 bytes)	1 (0x0001) (Big Endian) 256 (0x0100) (Little Endian)	5ο και 6ο
Sequence Number (2 bytes)	165 (0x00a5) (Big Endian) 42440 (0xa500) (Little Endian)	7ο και 8ο

Σχηματικά, για το ICMP header έχουμε:

Type (8 bits)	**Code (8 bits)**	**Checksum (16 bits)**
Identifier (16 bits)		**Sequence Number (16 bits)**

1.7) Type: 0x08 (Echo (ping) request) και **Code: 0x00**.

1.8)Identifier: 1 (0x0001) σε Big Endian / 256 (0x0100) σε Little Endian
Sequence Number: 165 (0x00a5) σε Big Endian / 42440 (0xa500) 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

(αντιστοιχεί στους ASCII χαρακτήρες: 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) Μελετώντας ένα μήνυμα ICMP Echo Reply, βλέπουμε πως και αυτό έχει **επικεφαλίδα μήκους 8 bytes και δομή ίδια με των αντίστοιχων request**.

1.11) Type: 0 (0x00) (Echo (ping) reply) και Code: 0 (0x00).

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

1.13) Identifier (BE): 1 (0x0001) / (LE): 256 (0x0100)
Sequence Number (BE): 165 (0x00a5) / (LE): 42440 (0xa500)

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) Ο ρόλος των πεδίων Identifier και Sequence Number είναι **να βοηθούν στην αντιστοίχηση των echo requests με το αντίστοιχο echo reply**, όπως και βλέπουμε στο documentation:

> **Identifier.** 16 bits.
> This field is used to help match echo requests to the associated reply. It may be cleared to zero.
>
> **Sequence number.** 16 bits.
> This field is used to help match echo requests to the associated reply. It may be cleared to zero.

1.16) Το μήκος του πεδίου δεδομένων των μηνυμάτων ICMP Echo reply, είναι επίσης **32 bytes** και έχει ακριβώς τα ίδια data 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

(αντιστοιχεί στους ASCII χαρακτήρες: 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) Όπως είπαμε, **δε διαφέρει το περιεχόμενο αυτό από του αντίστοιχου request**.

1.18) Στο Wireshark καταγράφονται 8 ερωταπαντήσεις request-reply συνολικά, δηλαδή 4 requests και 4 reply. **Αυτό είναι άμεση συνέπεια του ping που κάναμε, καθώς by default στέλνει 4 ICMP πακέτα, και λάβαμε επίσης ως απόκριση 4 reply** (στο terminal).

1.19) Χρησιμοποιήθηκε η εντολή **ping –n 2 10.3.20.20**, η οποία και μας έδωσε τα παρακάτω αποτελέσματα:

```
C:\Users\Αλεξ>ping -n 2 10.3.20.20

Pinging 10.3.20.20 with 32 bytes of data:
Reply from 10.3.20.29: Destination host unreachable.
Reply from 10.3.20.29: Destination host unreachable.

Ping statistics for 10.3.20.20:
    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:

1	0.000000	IntelCor_1b:6c…	Broadcast	ARP	42	Who has 10.3.20.20? Tell 10.3.20.29
2	0.724725	IntelCor_1b:6c…	Broadcast	ARP	42	Who has 10.3.20.20? Tell 10.3.20.29
3	1.725159	IntelCor_1b:6c…	Broadcast	ARP	42	Who has 10.3.20.20? Tell 10.3.20.29
4	2.727459	IntelCor_1b:6c…	Broadcast	ARP	42	Who has 10.3.20.20? Tell 10.3.20.29
8	3.724755	IntelCor_1b:6c…	Broadcast	ARP	42	Who has 10.3.20.20? Tell 10.3.20.29
9	4.725167	IntelCor_1b:6c…	Broadcast	ARP	42	Who has 10.3.20.20? Tell 10.3.20.29

1.21) Με εξαίρεση τα 2 πρώτα που είχαν κενό 0.7 seconds περίπου, τα υπόλοιπα στέλνονται προσεγγιστικά ανά **1 δευτερόλεπτο**:

1	0.000000	IntelCor_1b:6c…	Broadcast	ARP	42	Who has 10.3.20.20? Tell 10.3.20.29
2	0.724725	IntelCor_1b:6c…	Broadcast	ARP	42	Who has 10.3.20.20? Tell 10.3.20.29
3	1.000434	IntelCor_1b:6c…	Broadcast	ARP	42	Who has 10.3.20.20? Tell 10.3.20.29
4	1.002300	IntelCor_1b:6c…	Broadcast	ARP	42	Who has 10.3.20.20? Tell 10.3.20.29
8	0.997296	IntelCor_1b:6c…	Broadcast	ARP	42	Who has 10.3.20.20? Tell 10.3.20.29
9	1.000412	IntelCor_1b:6c…	Broadcast	ARP	42	Who has 10.3.20.20? Tell 10.3.20.29

1.22) Δε στάλθηκε **κανένα** ICMP πακέτο.

1.23) Αν δοκιμάσουμε να στείλουμε 1/2/3/4 πακέτα, καταγράφουμε αντίστοιχα 3/6/9/12 ARP πακέτα, επομένως όπως και τα ICMP πακέτα στέλνονται ανά τριάδες (με tracerout), παρατηρούμε την ίδια συμπεριφορά και με τα ARP 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 $2^{η}$ τριάδα πακέτων, με τα ίδια, ωστόσο, αποτελέσματα. Δηλαδή, τα πακέτα αυτά έγιναν broadcast στο τοπικό μας δίκτυο (με την ερώτηση Who has 10.3.20.20) **χωρίς όμως να λάβουν κάποια απόκριση**.

Άσκηση 2: Εντολή ping σε άλλο υποδίκτυο

Παρατηρούμε αρχικά τον arp πίνακα του υπολογιστή μας με την εντολή **arp -a**.

```
C:\Users\Αλεξ>arp -a

Interface: 10.3.20.10 --- 0x12
  Internet Address      Physical Address      Type
  10.3.20.1             04-d5-90-da-67-b0     dynamic
  10.3.21.255           ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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 --- 0x14
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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
```

2.1) Αφού κάνουμε ping στη διεύθυνση 147.102.1.1 καταγράφονται **ακριβώς οι ίδιες διευθύνσεις με πριν**, τις οποίες και βλέπουμε παρακάτω:

```
C:\Users\Αλεξ>arp -a

Interface: 10.3.20.10 --- 0x12
  Internet Address      Physical Address      Type
  10.3.20.1             04-d5-90-da-67-b0     dynamic
  10.3.21.255           ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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 --- 0x14
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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
```

2.2) Επιλέγουμε το πρώτο κατά σειρά εμφάνισης πακέτο ICMP Echo request και έχουμε: **MAC address Αποστολέα / Παραλήπτη: b4:69:21:1b:6c:ff / 04:d5:90:da:67:b0**.

2.3) IPv4 διεύθυνση Αποστολέα / Παραλήπτη: 10.3.20.10 / 147.102.1.1.
2.4) Οι παραπάνω διευθύνσεις MAC αντιστοιχούν στις IPv4 διευθύνσεις **10.3.20.10 (αποστολέας) και 10.3.20.1 (παραλήπτης, το βλέπουμε στον πίνακα arp)**.

2.5) Ναι, καταγράφηκαν **2 ARP πακέτα**.

2.6) Τα 2 αυτά πακέτα, όπως βλέπουμε και από το περιεχόμενο των ερωταπαντήσεων, έχουν ως σκοπό να ενημερώσουν το default gateway (router) για το **ποια MAC αντιστοιχεί στη διεύθυνσή μας**.

```
 8 0.404837 Fortinet_da:67… IntelCor_1b:6c… ARP      56 Who has 10.3.20.10? Tell 10.3.20.1
 9 0.000041 IntelCor_1b:6c… Fortinet_da:67… ARP      42 10.3.20.10 is at b4:69:21:1b:6c:ff
```

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

2.8) Το TTL που βλέπουμε στις απαντήσεις του παραθύρου εντολών, αλλά και στο Wireshark προφανώς, έχει **τιμή 61**. Γνωρίζουμε ότι σε *nix συστήματα (Unix/Linux) η default τιμή είναι 64, επομένως εύλογα υποθέτουμε πως παρεμβάλλονται 3 κόμβοι από τον host με IP 147.102.1.1. Εάν κάνουμε tracert εκεί, επιβεβαιώνουμε το παραπάνω:

```
C:\Users\Άλεξ>tracert 147.102.1.1

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

  1     3 ms     4 ms     3 ms  10.3.20.1
  2     4 ms     2 ms     3 ms  62.217.77.8
  3     4 ms     3 ms     4 ms  ntua-zogr-3.eier.access-link.grnet.gr [62.217.96.169]
  4     8 ms     5 ms     4 ms  theseas.softlab.ece.ntua.gr [147.102.1.1]
```

Το πακέτο reply, ξεκίνησε από τη διεύθυνση 147.102.1.1 και πέρασε ενδιάμεσα από τους κόμβους με IP 62.217.96.167, 62.217.77.8 και 10.3.20.1, ο καθένας από τους οποίος **μείωσε το TTL κατά 1**.

2.9) Εμφανίζονται μόνο μηνύματα τύπου **ICMP Echo (ping) request**.

icmp

No.	Time	Source	Destination	Protocol	Length	Info
9	0.000000	10.3.20.10	147.102.7.45	ICMP	74	Echo (ping) request id=0x0001, seq=69/17664, ttl=128 (no response found!)
23	4.638987	10.3.20.10	147.102.7.45	ICMP	74	Echo (ping) request id=0x0001, seq=70/17920, ttl=128 (no response found!)
41	4.979928	10.3.20.10	147.102.7.45	ICMP	74	Echo (ping) request id=0x0001, seq=71/18176, ttl=128 (no response found!)
43	5.010995	10.3.20.10	147.102.7.45	ICMP	74	Echo (ping) request id=0x0001, seq=72/18432, ttl=128 (no response found!)

2.10) Προηγουμένως, με το Ping σε ανενεργό υπολογιστή εντός του υποδικτύου μας, λάβαμε απόκριση Destination Host Unreachable, ενώ στον υπολογιστή εκτός του υποδικτύου Request Timed Out. Εάν εστιάσουμε στην κίνηση που καταγράφηκε, θα δούμε πως κάνοντας Ping σε κόμβο εκτός του υποδικτύου μας δε παρατηρούμε 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 IP στην οποία κάναμε Ping. Όταν όμως κάναμε σε κόμβο εκτός του υποδικτύου μας, **η δρομολόγηση έγινε στο Layer 3 (Network)**, το οποίο απαιτεί να γνωρίζει την IP διεύθυνση του κόμβου-στόχου, την οποία και παρείχαμε, οπότε και ο δρομολογητής προώθησε κανονικά το πακέτο εκτός δικτύου. Οπότε στην $2^{η}$ περίπτωση απαιτείται -όσον αφορά φυσικές διευθύνσεις- η MAC διεύθυνση του gateway gaddress, 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 **64 bytes** 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….)** (βλ. 1.9).

3.3) Στους ενδιάμεσους κόμβους παρατηρούμε το μήνυμα **Time-to-live exceeded**.

3.4) Το παραπάνω μήνυμα λάθους έχει ως **Type: 11 (0x0b) (Time-to-live exceeded)** και ως **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** (αντιστοιχεί στο Total Length της IPv4 επικεφαλίδας του ping request που προκάλεσε το συγκεκριμένο ICMP μήνυμα λάθους, το οποίο εδώ χώρεσε ολόκληρο).

3.7) Τα δεδομένα του ICMP μηνύματος λάθους που εξετάσαμε είναι ουσιαστικά το IPv4 πακέτο που προκάλεσε το εν λόγω μήνυμα (Header + τα πρώτα byte του αρχικού μηνύματος, μέχρι το ICMP πακέτο να φτάσει μέγιστο τα 576 bytes).

Άσκηση 4: Ανακάλυψη MTU διαδρομής (Path MTU Discovery)

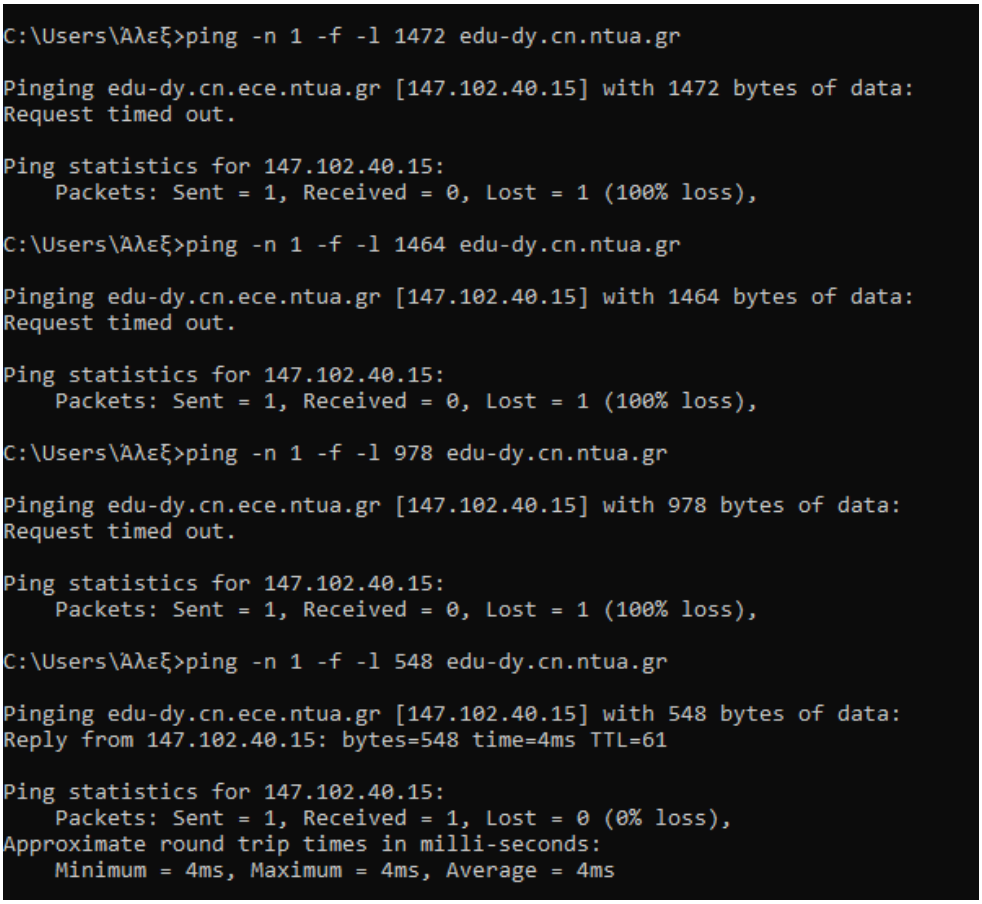
4.1) Σχετικά με τις τιμές payload του ICMP προκειμένου να παραχθούν πακέτα IPv4 με τις επιθυμητές τιμές MTU, μπορούμε να πούμε τα εξής:
Το MTU προκύπτει ως το άθροισμα των IP header length + ICMP header length + ICMP Payload length, δηλαδή

MTU = IP header length (20) + ICMP header length (8) + ICMP Payload Length => ICMP Payload length = MTU – 28bytes

Επομένως, θα προκύψουν από το επιθυμητό **MTU size αφαιρώντας 28 bytes για κάθε τιμή**.

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**

Ενδεικτικά, παρατίθενται σε στιγμιότυπο τα ping με τα εν λόγω μεγέθη, μέχρι που λήφθηκε απόκριση από το 147.102.40.15:



4.2) Όχι, δε παρατηρήθηκε μήνυμα λάθους ICMP Destination Unreachable.

4.3) -

4.4) *Χρησιμοποιούμε την καταγραφή του αρχείου mtu.pcap***.** Βρίσκουμε τις παρακάτω τιμές για τα πεδία **Type: 3 (Destination Unreachable) και Code: 4 (Fragmentation needed)**.

4.5) Το πεδίο, το οποίο υποδεικνύει ότι το λάθος οφείλεται στην απαίτηση μη θρυμματισμού είναι το **Code: 4 (Fragmentation needed)**. 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**.

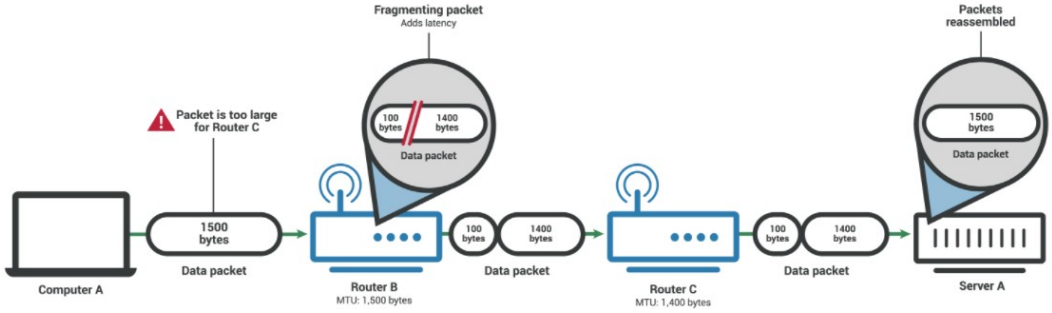
4.7) Για **καμία MTU** δε λάβαμε μήνυμα ICMP Destination Unreachable, επομένως η MTU για την οποία δε λαμβάνουμε μήνυμα ICMP Destination Unreachable για πρώτη φορά είναι **1500 bytes**.

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\Αλεξ>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=5ms TTL=61

Ping statistics for 147.102.40.15:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 5ms, Average = 5ms

C:\Users\Αλεξ>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) Βασιζόμενοι στο documentation βλέπουμε 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 Destinatio 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**. Ενδεικτικά, έχουμε το παρακάτω σχήμα: (*Πηγή: Cloudflare)*



Εδώ, ο Computer A θέλει να στείλει πακέτο 1500 bytes στον Server A από το δίκτυο που μεσολαβούν οι Router B και C. Όλοι εκτός του Router C έχουν MTU 1500 bytes, ενώ εκείνος 1400 bytes. Για αυτό και ο Router B που είναι ο προηγούμενός του κάνει fragmentation προτού το προωθήσει στον C.

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\Αλεξ>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=5ms TTL=61

Ping statistics for 147.102.40.15:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 5ms, Average = 5ms
```

Στην καταγραφή έχουμε τα εξής:

ip.addr==147.102.40.15

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000000	10.3.22.32	147.102.40.15	ICMP	1514	Echo (ping) request id=0x0001, seq=146/37376, ttl=128 (reply in 6)
4	0.004441	147.102.40.15	10.3.22.32	IPv4	586	Fragmented IP protocol (proto=ICMP 1, off=0, ID=6213) [Reassembled in #6]
5	0.000000	147.102.40.15	10.3.22.32	IPv4	586	Fragmented IP protocol (proto=ICMP 1, off=552, ID=6213) [Reassembled in #6]
6	0.000000	147.102.40.15	10.3.22.32	ICMP	410	Echo (ping) reply id=0x0001, seq=146/37376, ttl=61 (request in 3)

Τα 3 τελευταία πακέτα-θραύσματα είναι που λαμβάνει ο υπολογιστής μας. Το πρώτο εξ αυτών έχει μέγεθος **586 bytes**, **διαφορετικό από την MTU που προσδιορίσαμε προηγουμένως** και αυτό, διότι τα πακέτα που μας έρχονται, ενδεχομένως περνάνε 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 ψάχνουμε, ενώ το δεύτερο όρισμα είναι η IP του DNS Server.

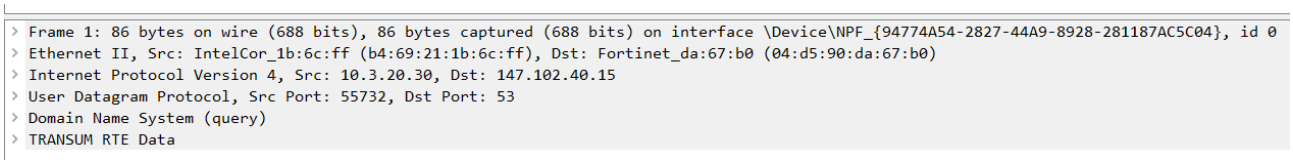
5.3) Στη γραμμή εντολών, λάβαμε μηνύματα **DNS request timed out**, όπως βλέπουμε παρακάτω:

```
C:\Users\Άλεξ>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
```

5.4) Όπως παρατηρούμε, καταγράφηκαν DNS μηνύματα:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.3.20.30	147.102.40.15	DNS	86	Standard query 0x0001 PTR 15.40.102.147.in-addr.arpa
2	0.005006	147.102.40.15	10.3.20.30	ICMP	70	Destination unreachable (Port unreachable)
3	2.018261	10.3.20.30	147.102.40.15	DNS	77	Standard query 0x0002 A edu-dy.cn.ntua.gr
4	0.004587	147.102.40.15	10.3.20.30	ICMP	70	Destination unreachable (Port unreachable)
5	2.002129	10.3.20.30	147.102.40.15	DNS	77	Standard query 0x0003 AAAA edu-dy.cn.ntua.gr
6	0.004901	147.102.40.15	10.3.20.30	ICMP	70	Destination unreachable (Port unreachable)
7	1.998485	10.3.20.30	147.102.40.15	DNS	77	Standard query 0x0004 A edu-dy.cn.ntua.gr
8	0.004333	147.102.40.15	10.3.20.30	ICMP	70	Destination unreachable (Port unreachable)
9	2.002125	10.3.20.30	147.102.40.15	DNS	77	Standard query 0x0005 AAAA edu-dy.cn.ntua.gr
10	0.006172	147.102.40.15	10.3.20.30	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) Όπως είδαμε παραπάνω, **καταγράφηκαν μηνύματα ICMP Destination Unreachable** με προορισμό τη διεύθυνση 147.102.40.15.

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) Δε διαθέτουμε σύστημα Linux/Unix.

Άσκηση 6: IPv6 και ICMPv6

6.1) Ping: **ping 2001:648:2000:329::101**
Tracert: **tracert 2001:648:2000:329::101**

6.2) Φίλτρο σύλληψης **ip6** και φίλτρο απεικόνισης **icmpv6**.

6.3) Type: IPv6 (0x86dd).

6.4) Για ένα τυχαίο πακέτο -και άρα για όλα αφού η επικεφαλίδα κάθε IPv6 πακέτου έχει σταθερό μήκος- έχει μήκος **40 bytes**.

6.5) Για τη δομή της επικεφαλίδας, έχουμε τις παρακάτω γραμμές των 4 bytes (ισοδύναμα 32 bits για να απεικονιστούν ευκολότερα πεδία των 4 bits): *Σημείωση: Οι 2 πρώτες γραμμές αποτελούνται από 1 γραμμή (4 bytes), ενώ οι επόμενες 2 από 4 γραμμές (16 bytes) η κάθε μία*

Version: $0110_2 = 6_{10}$ (4 bits)	**Traffic Class: 0x00 (8 bits)**	**Flow Label: 0x00000 (20 bits)**	
Payload Length: 40_{10} (0x0028) (16 bits)		**Next Header: ICMPv6 (58 = 0x3a) (8 bits)**	**Hop Limit: 128 (0x80) (8 bits)**
Source Address: 2001:648:2d00:1020::1 (128 bits)			
Destination Address: 2001:648:2d00:1020:3d78:71b6:f5c9:1a47 (128 bits)			

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_{10} 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 ομοιότητες σε κάποια πεδία.

6.9) Αναφερόμενοι στο πεδίο **Type** του ICMPv6 Echo ping request, έχει τιμή **128_{10} (0x80)**, ενώ μεταφέρει **32 bytes δεδομένων**.

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

6.11) Type: Echo ping reply (129_{10} = 0x81) και μεταφέρει δεδομένα επίσης **32 bytes**.

6.12) Το παραγόμενο από tracert ICMPv6 Echo Request έχει τιμή στο πεδίο **Type: Neighbor Solicitation (135)**. Επιπλέον, **διαφέρουν** και κάποια πεδία της επικεφαλίδας τους όπως φαίνεται παρακάτω ($1^η$ εικόνα ICMPv6 από tracert, ενώ $2^η$ εικόνα ICMPv6 από ping):

```
Type: Neighbor Solicitation (135)
Code: 0
Checksum: 0x3811 [correct]
[Checksum Status: Good]
Reserved: 00000000
Target Address: 2001:648:2d00:1020:3d78:71b6:f5c9:1a47
ICMPv6 Option (Source link-layer address : 04:d5:90:da:67:b0)
  Type: Source link-layer address (1)
  Length: 1 (8 bytes)
  Link-layer address: Fortinet_da:67:b0 (04:d5:90:da:67:b0)
```

```
Internet Control Message Protocol v6
  Type: Echo (ping) reply (129)
  Code: 0
  Checksum: 0x113b [correct]
  [Checksum Status: Good]
  Identifier: 0x0001
  Sequence: 37
  [Response To: 60]
  [Response Time: 6,556 ms]
  Data (64 bytes)
```

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.

```
27 0.001861 2001:648:2d00:… 2001:648:2d00:… ICMP… 174 Time Exceeded (hop limit exceeded in transit)
28 0.000954 2001:648:2d00:… 2001:648:2000:… ICMP… 126 Echo (ping) request id=0x0001, seq=24, hop limit=1 (no response found!)
```

```
Source Address: 2001:648:2d00:1020::1
Destination Address: 2001:648:2d00:1020:3d78:71b6:f5c9:1a47
Internet Control Message Protocol v6
  Type: Time Exceeded (3)
  Code: 0 (hop limit exceeded in transit)
  Checksum: 0xdc72 [correct]
  [Checksum Status: Good]
  Reserved: 00000000
  Internet Protocol Version 6, Src: 2001:648:2d00:1020:3d78:71b6:f5c9:1a47, Dst: 2001:648:2000:329::101
  Internet Control Message Protocol v6
```

6.14) Όπως είδαμε, το Type έχει τιμή **Type: Time Exceeded (3)** και το μήκος δεδομένων του είναι **120 – (1 + 1 + 2 + 4) = 112 bytes**. (τα byte στην παρένθεση είναι μήκη πεδίων της επικεφαλίδας).

6.15) Αντίστοιχα με το ICMP περιέχει το IPv6 πακέτο που το προκάλεσε ως δεδομένα, δηλαδή τα ICMPv6 δεδομένα του πακέτου 27 παρακάτω, είναι το πακέτο IPv6:

```
26 3.044481 2001:648:2d00:… 2001:648:2000:… ICMP… 126 Echo (ping) request id=0x0001, seq=23, hop limit=1 (no response found!)
27 0.001861 2001:648:2d00:… 2001:648:2d00:… ICMP… 174 Time Exceeded (hop limit exceeded in transit)
```

6.16) Πέρα από τα **ping request/reply**, τα **Time Exceeded** και το **Neighbor Solicitation** παρατηρήθηκαν και ICMPv6 μηνύματα τύπου **Neighbor Advertisement**.

6.17) Τα ICMPv6 μηνύματα τύπου Neighbor Solicitation / Neigbor Advertisement έχουν **συνολικό μήκος 86 bytes (86 – 14 = 72 bytes αναφερόμενοι μόνο στο IPv6 πακέτο)**.