

**δικτυα υπολογιστων**

**Εργαστηριακη ασκηση 5: Εξερευνηση του διαδικτυου**





8 νοεμβριου, 2022

ΘΟΔΩΡΗΣ ΑΡΑΠΗΣ – EL18028

|  |  |  |
| --- | --- | --- |
| **Ονοματεπώνυμο:** Θοδωρής Αράπης | | **Ομάδα:** 2 |
| **Όνομα PC/ΛΣ:** pc-a37/ WINDOWS 95 | | **Ημερομηνία:** 8/11/2022 |
| **Διεύθυνση IP:** 147.102.38.87 | **Διεύθυνση MAC:** 00-11-25-F8-5E-EC | |

**Άσκηση 1: Χρόνος ζωής των πακέτων IPv4**

***1.1***

Η διεύθυνση IPv4 της κάρτας δικτύου του υπολογιστή είναι: 147.102.38.87.

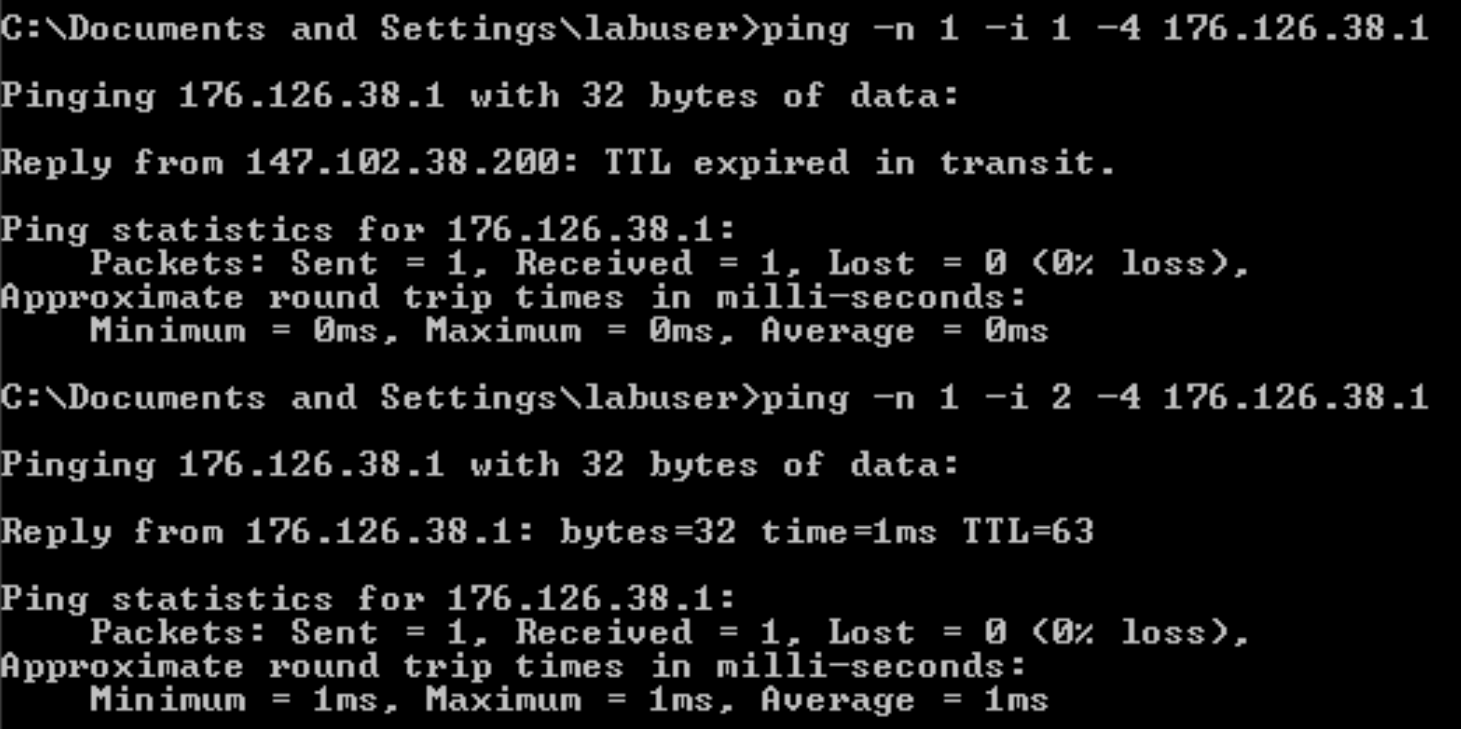
***1.2***

Η μάσκα υποδικτύου είναι η 255.255.255.0, άρα το μήκος του προθέματος δικτύου είναι 24 bits.

***1.3***

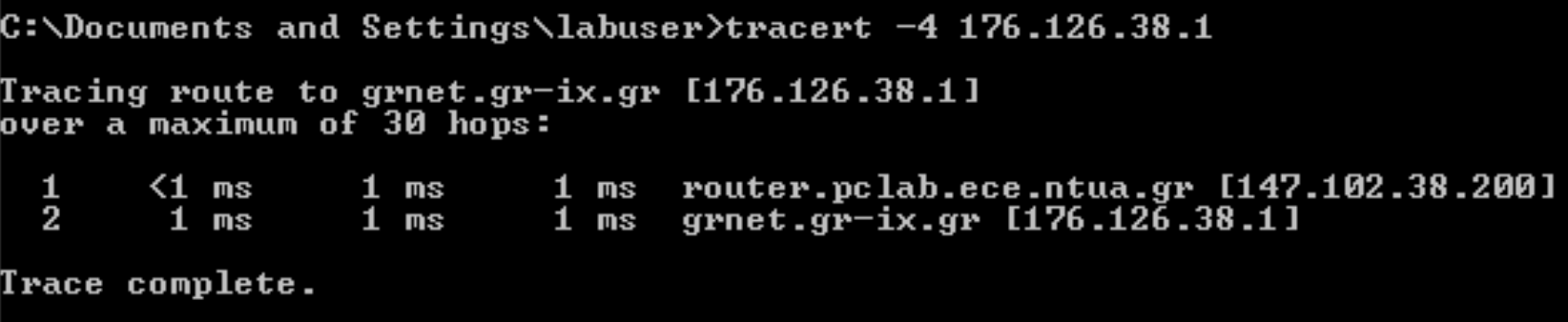
Η σύνταξη της εντολής είναι «ping -n 1 -i TTL -4 IP\_address», όπου TTL η τιμή της επικεφαλίδας TTL και IP\_address η διεύθυνση IPv4 του παραλήπτη.

***1.4***

Εφαρμόζουμε ως φίλτρο σύλληψης το host 147.102.38.87 και ως φίλτρο απεικόνισης το «icmp». Παρατηρούμε πως η ελάχιστη τιμή TTL για να φτάσει το πακέτο στη ζητούμενη διεύθυνση είναι 2.

***1.5***

Μπορούμε να χρησιμοποιήσουμε την εντολή «tracert -4 176.126.38.1» και να δούμε αναλυτικά τους ενδιάμεσους κόμβους που διέσχισε το πακέτο μας.



**Σχηματικά**

****

**Σχήμα 1:** *Τa πακέτα μας ξεκινάνε από την διεπαφή pc-a37 [147.102.38.87]. Ύστερα, στον πρώτο κόμβο που συναντάνε στο δίκτυο (διεπαφή 147.102.38.200 του εξυπηρετητή του pclab της σχολής) κατά την διαδρομή τους προς τον προορισμό (176.126.38.1), σταματάνε (TTL = 1) και στέλνονται πίσω στην αφετηρία ενημερώνοντας την διεπαφή μας για της πληροφορίες αυτού του κόμβου. Μετά επαναδρομολογούνται, προσπερνάνε τον προηγούμενο κόμβο (TTL = 2) και φτάνουν στον τελικό προορισμό. Με κίτρινο φαίνονται οι ενδιάμεσοι κόμβοι, ενώ με κόκκινο ο προορισμός και με πράσινο η αφετηρία.*

**Άσκηση 2: Ανακαλύψτε την τοπολογία**

***2.1***

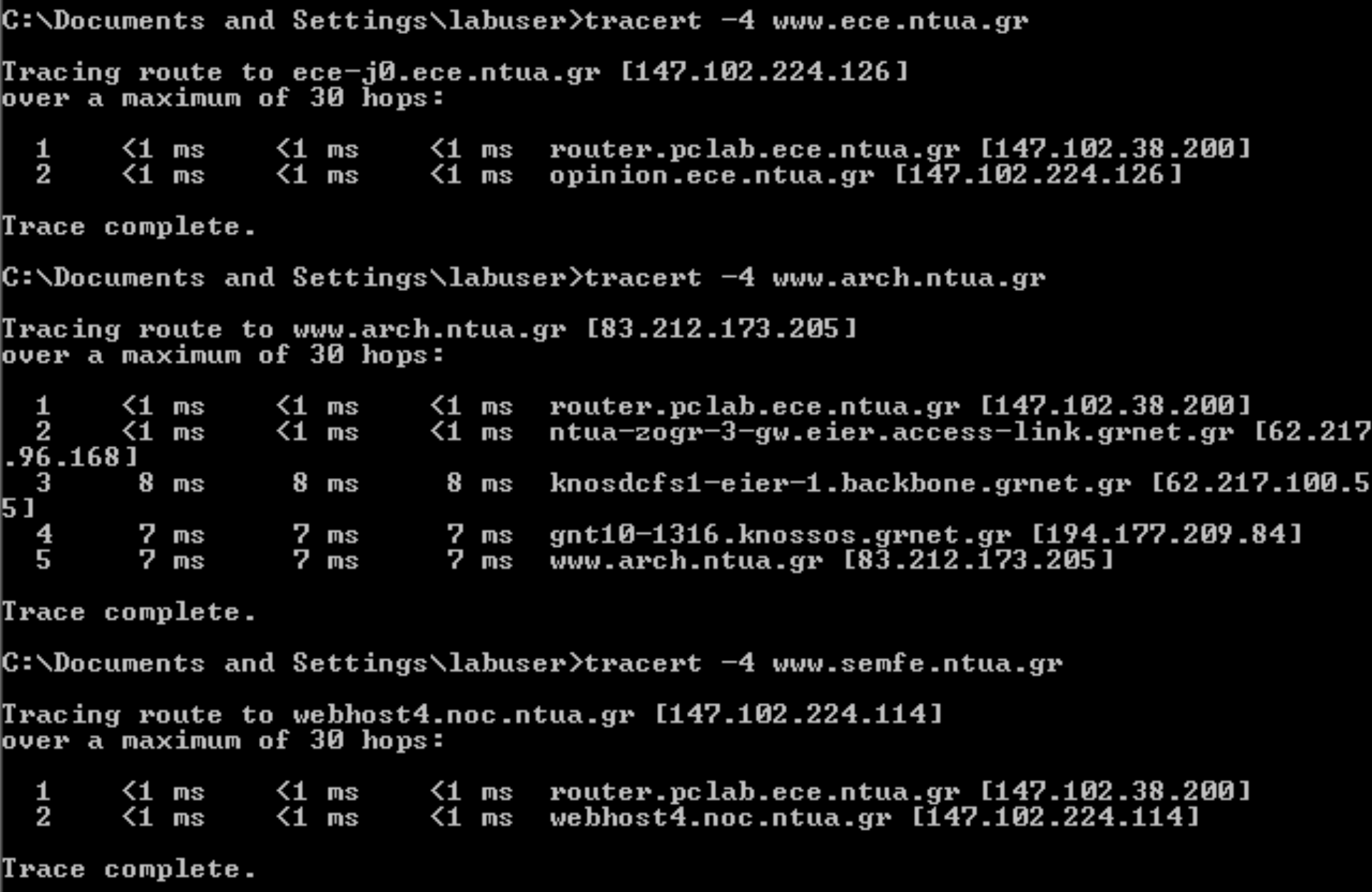
Η σύνταξη της εντολής είναι «tracert -4 www.ntua.gr».

Οι διαφορές που παρατηρούμε συγκριτικά με την παλιά καταγραφή είναι:

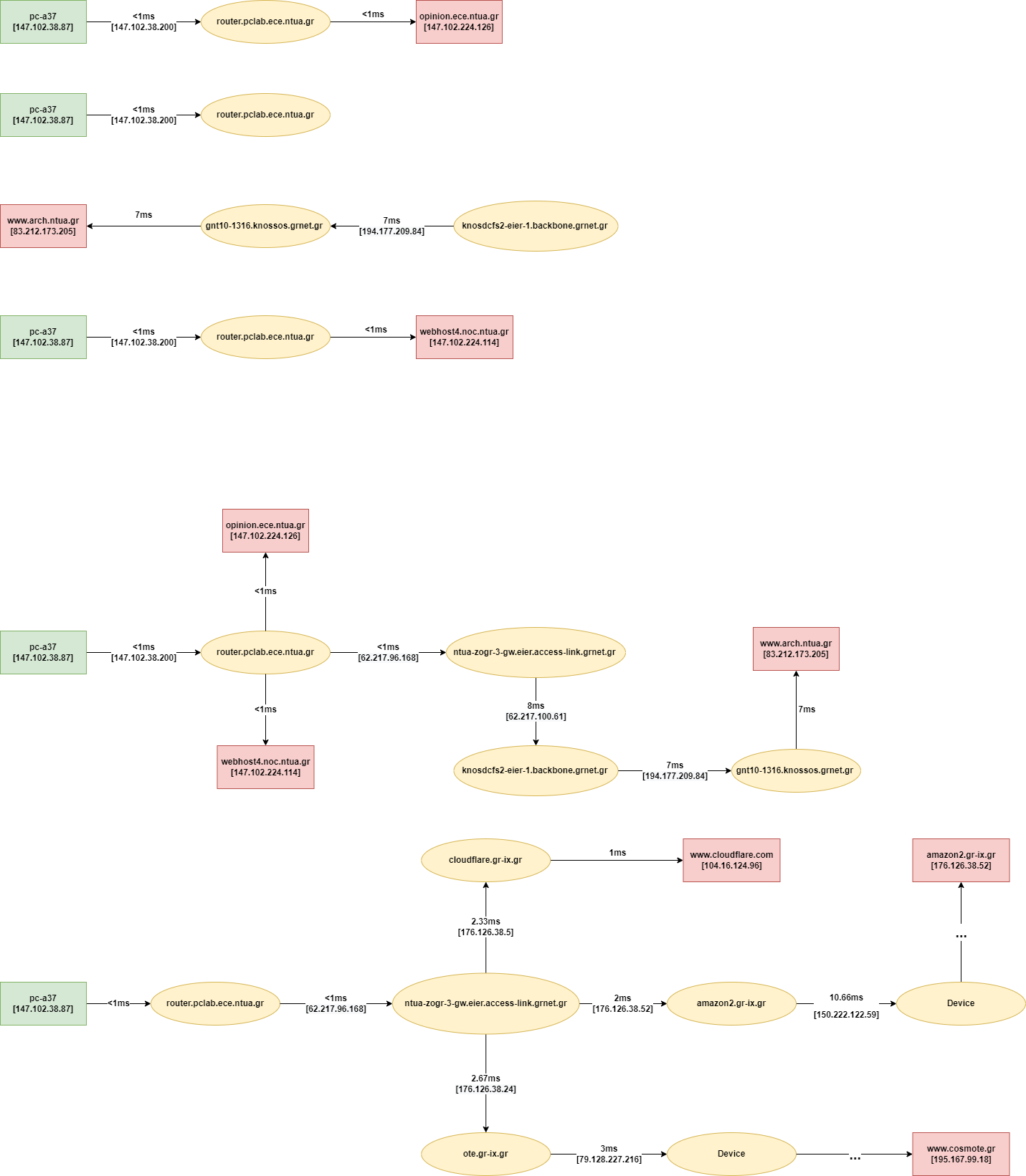
* Η τωρινή ονομασία του server είναι www.ntua.gr, ενώ παλιά ήταν achilles.noc.ntua.gr.
* Η τωρινή ονομασία του router που βρίσκεται ενδιάμεσα της διαδρομής είναι router.pclab.ece.ntua.gr, ενώ παλιά ήταν router-7.telecom.ece.ntua.gr.
* Τόσο ο server όσο και ο ενδιάμεσος κόμβος έχουν διαφορετικές IP διευθύνσεις σε σχέση με παλιά.

***2.2***

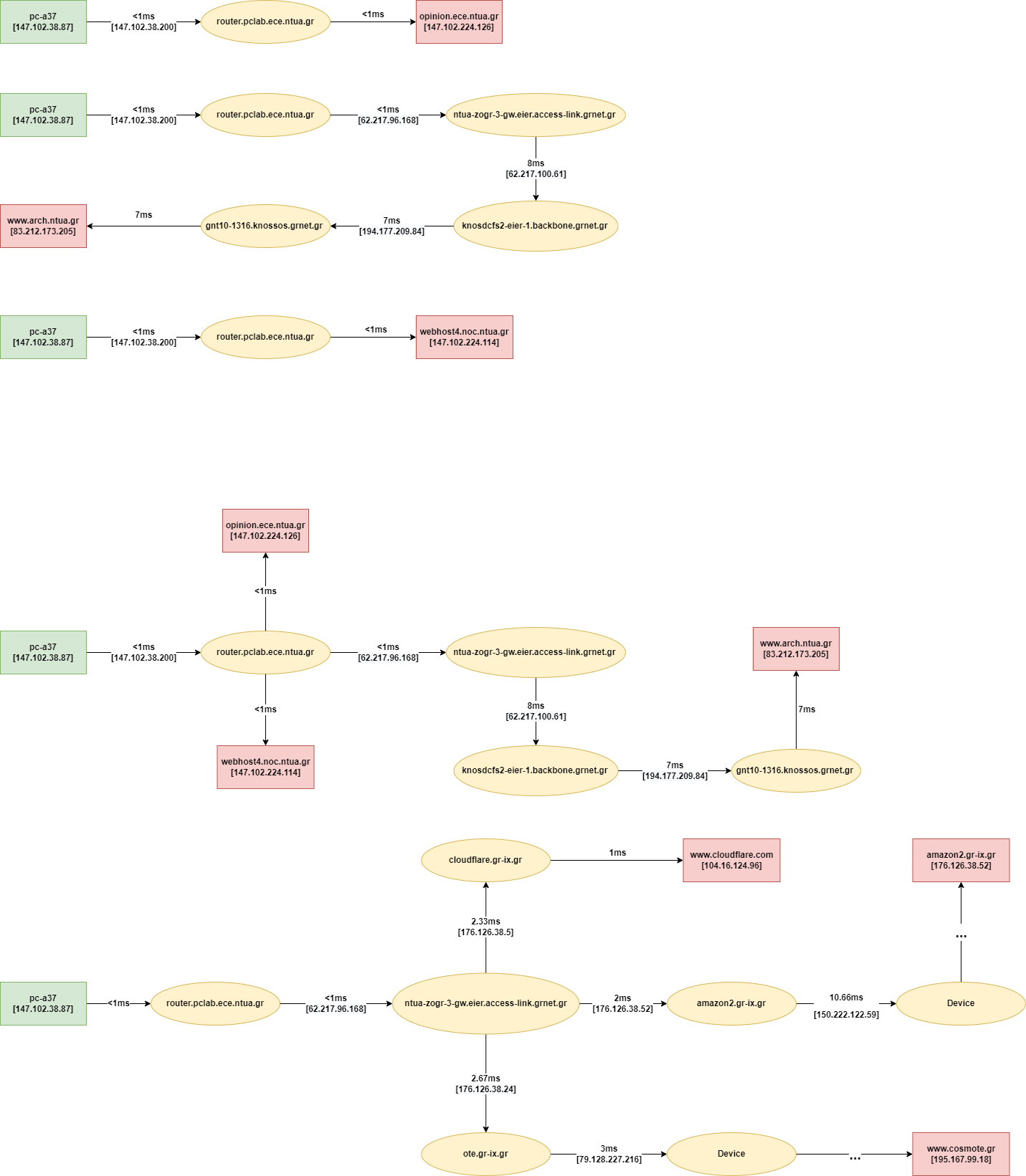
Εκτελούμε την εντολή «tracert» προς τους εξυπηρετητές των σχολών:

* ΗΜΜΥ (www.ece.ntua.gr)
* Αρχιτεκτόνων (www.arch.ntua.gr)
* Σ.Ε.Μ.Φ.Ε. (www.semfe.ntua.gr)

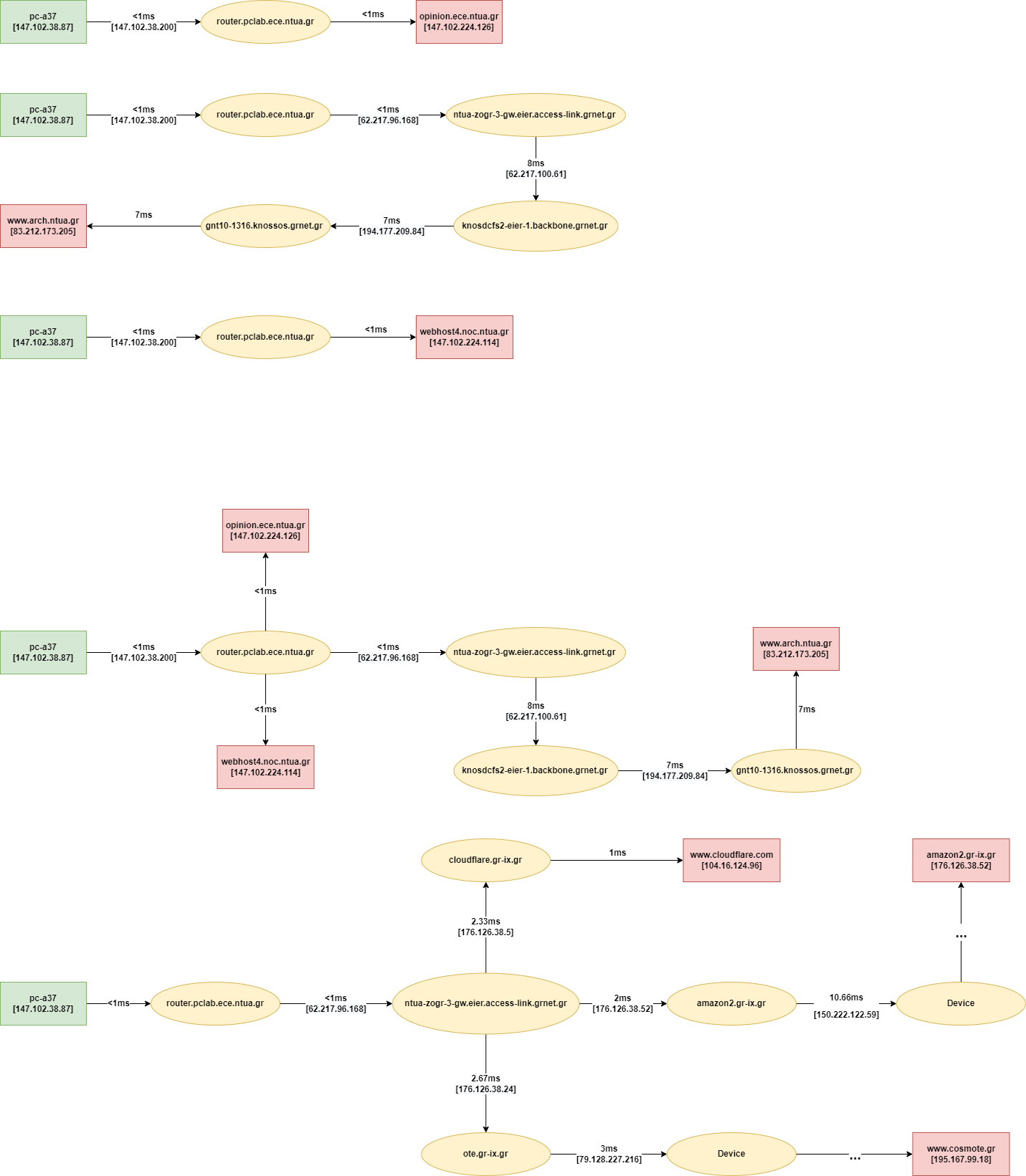
**Σχηματικά**

******

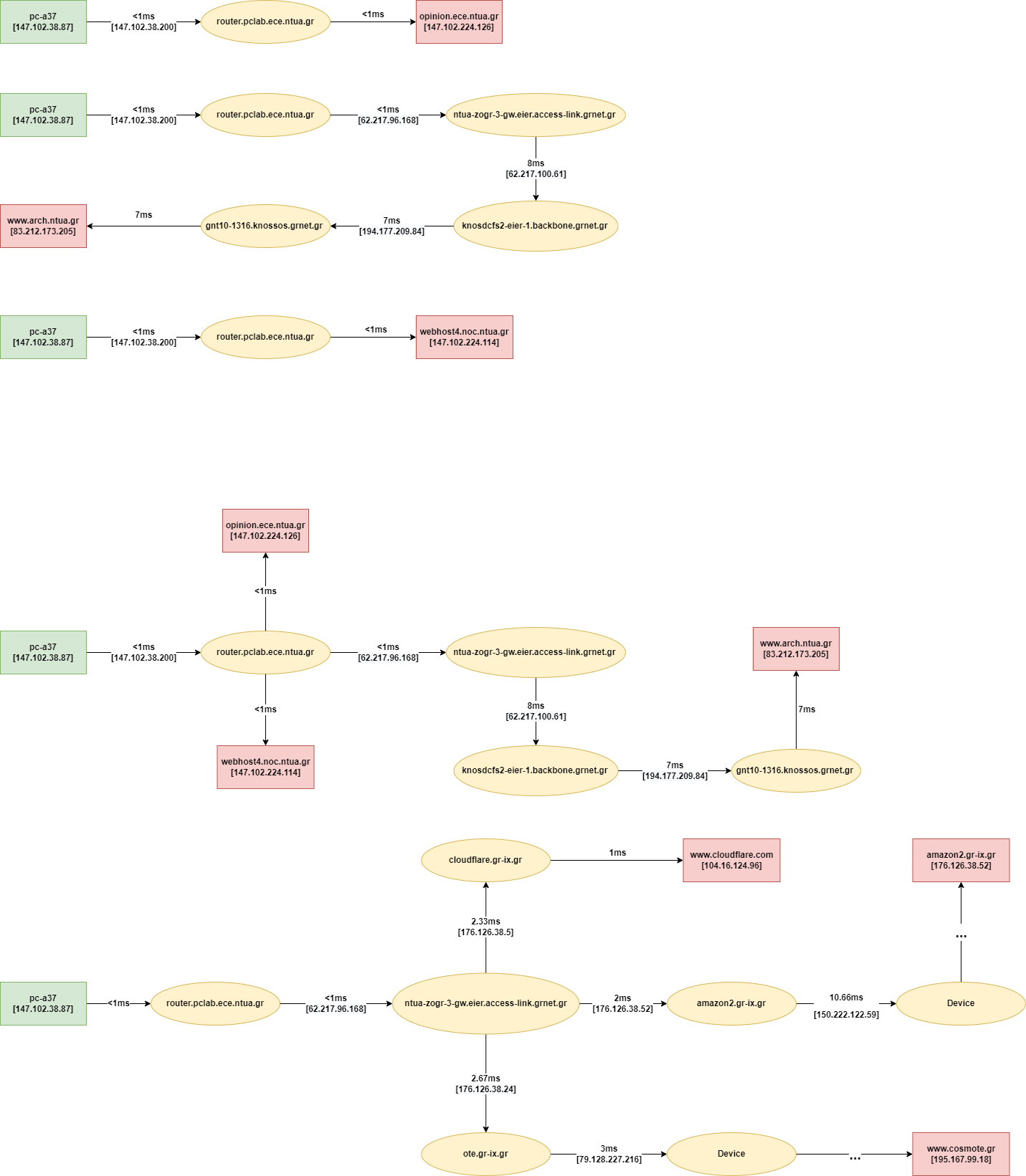
**Σχήμα 2:** *Η τοπολογία του δικτύου που καταλήγει από τον υπολογιστή μας στον εξυπηρετητή της σχολής ΗΜΜΥ και οι μέσοι χρόνοι καθυστέρησης.*

******

**Σχήμα 3:** *Η τοπολογία του δικτύου που καταλήγει από τον υπολογιστή μας στον εξυπηρετητή της σχολής Αρχιτεκτόνων και οι μέσοι χρόνοι καθυστέρησης.*

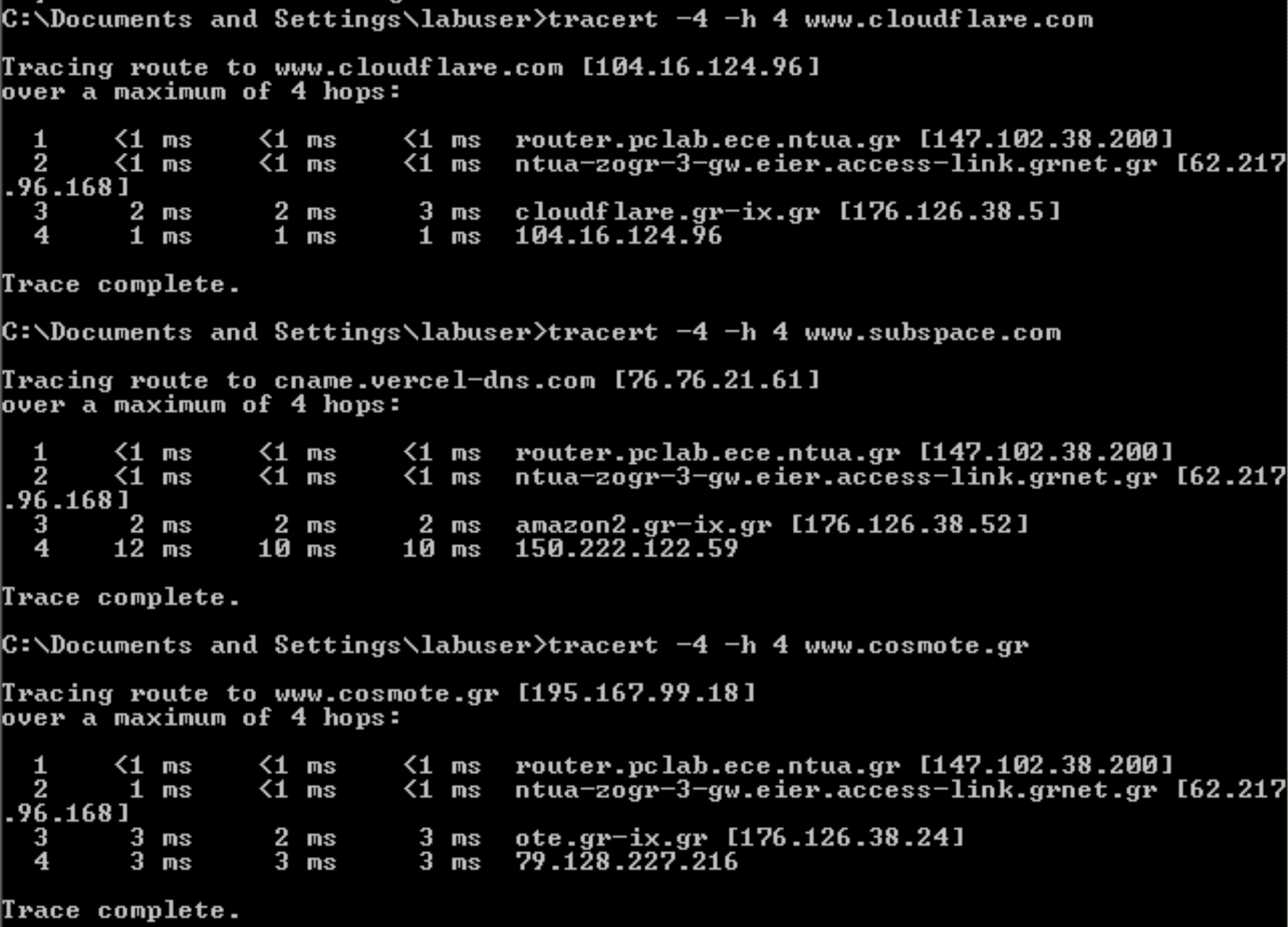
**

**Σχήμα 4:** *Η τοπολογία του δικτύου που καταλήγει από τον υπολογιστή μας στον εξυπηρετητή της σχολής Σ.Ε.Μ.Φ.Ε. και οι μέσοι χρόνοι καθυστέρησης.*

******

**Σχήμα 5:** *Η τοπολογία του δικτύου δεδομένων του πολυτεχνείου όπως φαίνεται από τον υπολογιστή μας και οι μέσοι χρόνοι καθυστέρησης.*

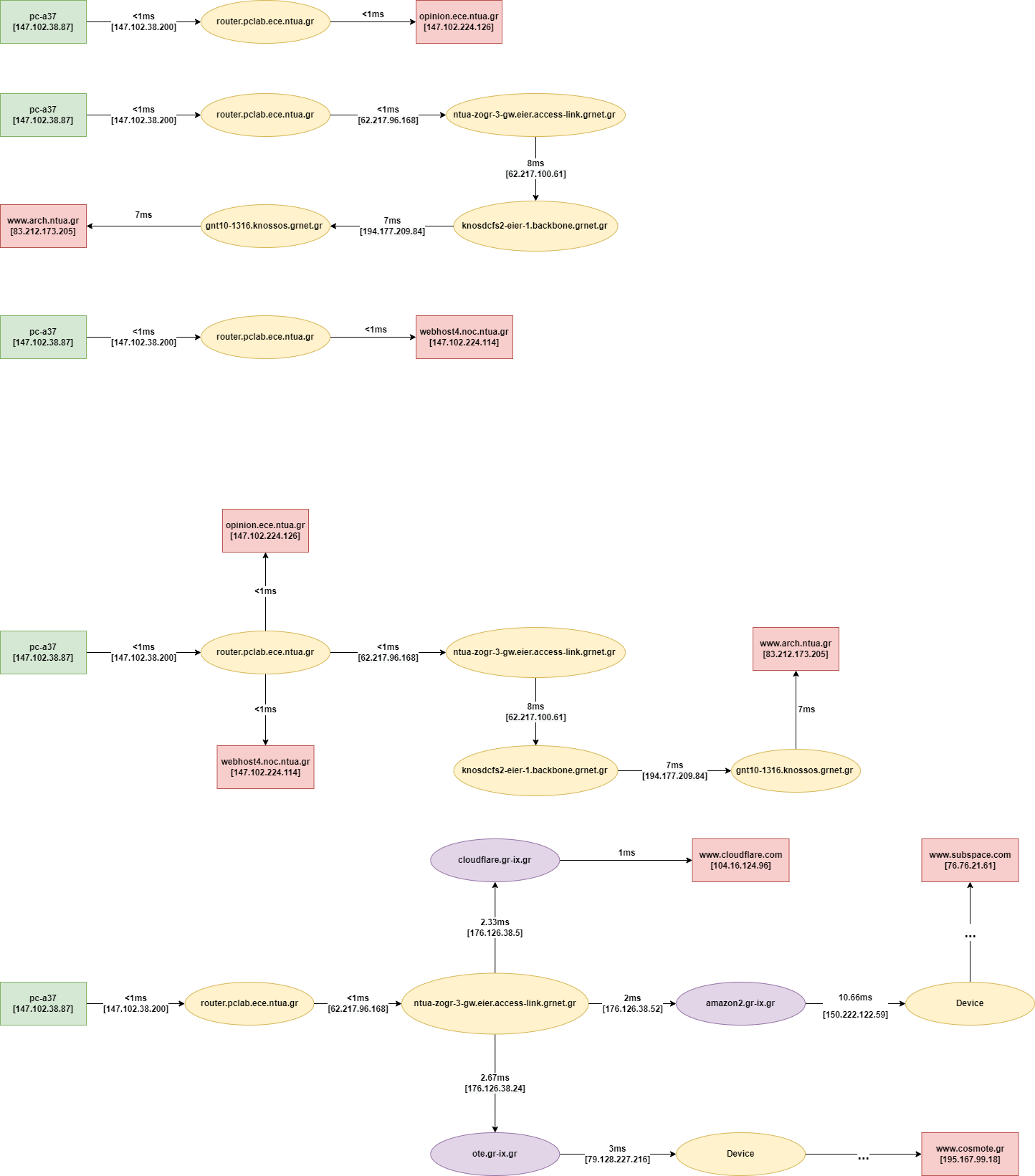
***2.3***

Ενώ παρουσιάζονται κάποιες ομοιότητες, όπως το ότι η σχολή Αρχιτεκτόνων ανήκει σε διαφορετικό υποδίκτυο από τις υπόλοιπες, κατά τα άλλα διαφέρουν αρκετά, πράγμα που οφείλεται στην παλαιότητα του διαγράμματος του Κέντρου Δικτύων.***2.4***

Η σύνταξη της εντολής που χρησιμοποιήσαμε είναι «tracert -4 -h 4 target\_name», όπου το «-4» επιβάλλει IPv4 διευθύνσεις και το «-h 4» δηλώνει το μέγιστο πλήθος βημάτων (hops).

***2.5***

Η διεύθυνση υποδικτύου IPv4 του GR\_IX είναι 176.126.38.0.

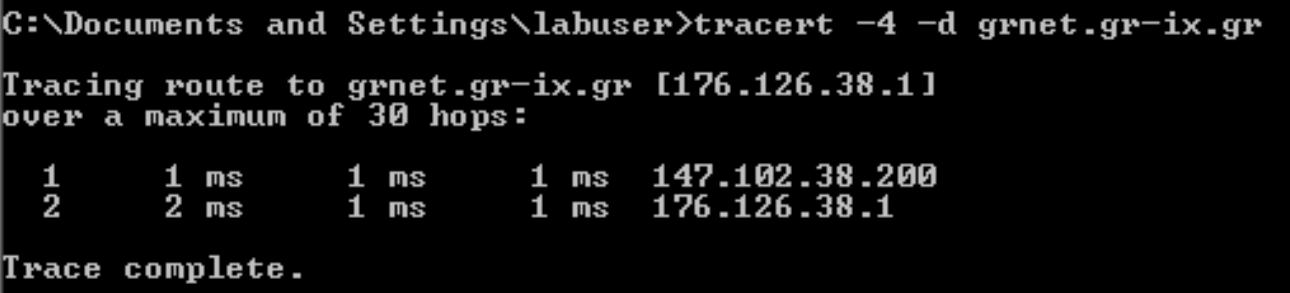
***2.6***

**Σχήμα 6:** *Η τοπολογία του δικτύου από τον υπολογιστή μας μέχρι τον κόμβο GR-IX (μωβ χρώμα) και ύστερα μέχρι τους εξυπηρετητές των ιστοσελίδων που δίνει η εκφώνηση.*

***2.7***

Ναι, συμφωνεί αρκετά.

***2.8***

Χρησιμοποιήθηκε η εντολή «tracert -4 -d grnet.gr-ix.gr».

***2.9***

Χρησιμοποιήθηκε το φίλτρο απεικόνισης «udp or icmp».

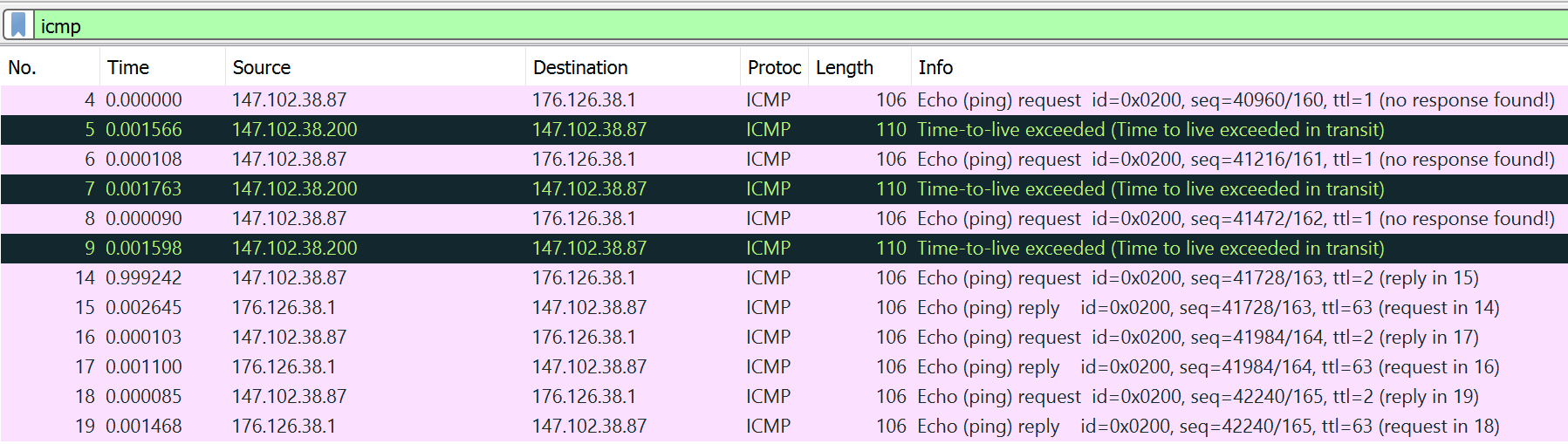
***2.10***

Το πεδίο Protocol της επικεφαλίδας IPv4 ενός μηνύματος (όπως και των υπολοίπων) που στείλαμε έχει τιμή 0x01, δηλαδή πρωτόκολλο ICMP.

***2.11***

Το προηγούμενο μήνυμα έχει Payload Length (μήκος πεδίου δεδομένων) 72 bytes (Total Length (92) – Header Length (20) = Payload Length (72)).

***2.12***

Αποστέλλεται αρχικά μία τριάδα μηνυμάτων με τιμή TTL ίση με 1. Δεν φτάνουν στον προορισμό και λαμβάνουμε απάντηση TTL exceeded. Επομένως, ξαναστέλνονται 3 μηνύματα με τιμή TTL 2 και αυτή την φορά φτάνουν στο προορισμό και λαμβάνουμε απάντηση από τον server στόχο μας. Οπότε συνολικά στάλθηκα 2 τριάδες μηνυμάτων και ελήφθησαν 2.

***2.13***

Έχουμε τις εξής τριάδες μηνυμάτων:

* ***TTL = 1:*** (Request) Destination IPv4 = 176.126.38.1 (x3)

(Reply) Source IPv4 = 147.102.38.200 (x3)

* ***TTL = 2:*** (Request) Destination IPv4 = 176.126.38.1 (x3)

(Reply) Source IPv4 = 176.126.38.1 (x3)

***2.14***

Ναι, οι παραπάνω IPv4 addresses των πηγών των απαντήσεων είναι ίδιες με αυτές που βρήκαμε στο 1.5 ερώτημα.

***2.15***

Στην πρώτη τριάδα μηνυμάτων που στείλαμε αντιστοιχεί TTL = 1 και στην δεύτερη TTL = 2.

***2.16***

Στην πρώτη τριάδα μηνυμάτων που λάβαμε αντιστοιχεί TTL = 255 και στην δεύτερη TTL = 63.

***2.17***

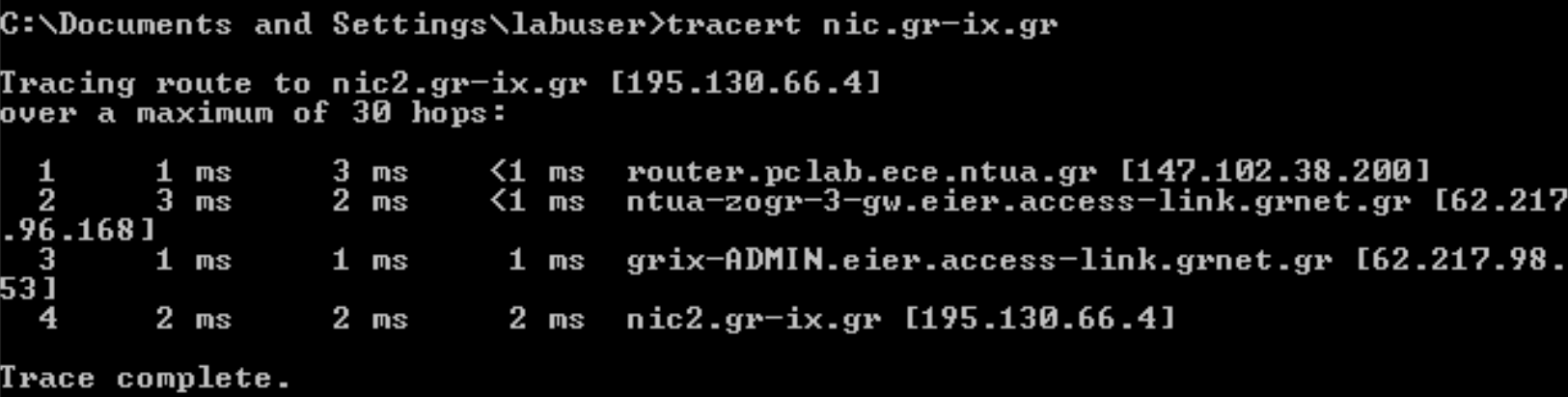
Οι πρώτοι κόμβοι απαντούν με μήνυμα ICMP Time-to-live exceeded, διότι σε εκείνους μηδενίστηκε το TTL χωρίς να αποτελούν τον τελικό προορισμό (μηδενίζεται κατά 1 σε κάθε κόμβο, επομένως στην πρώτη τριάδα μας απάντησε έτσι ο πρώτος κόμβος, ενώ η δεύτερη τριάδα έφτασε στον τελικό προορισμό).

***2.18***

Ο προορισμός απαντά με Echo (ping) reply.

**Άσκηση 3: Περισσότερα για τις επικεφαλίδες πακέτων IP**

***3.1***

Χρησιμοποιήθηκε η εντολή «tracert nic.gr-ix.gr».

***3.2***

Χρησιμοποιήθηκε το φίλτρο σύλληψης «icmp».

***3.3***

**Σχήμα 7:** *Η που καταγράφει η εντολή tracert από τον υπολογιστή μας μέχρι το μηχάνημα nic.gr-ix.gr.*

Οι IPv4 των διεπαφών που απαντούν φαίνονται πάνω στα βέλη, τα οποία δείχνουν προς τις συσκευές που υλοποιούν τις διεπαφές.

***3.4***

Αλλάζουν τα πεδία Identification, Header Checksum και time to live.

***3.5***

Παραμένουν αμετάβλητα όλα τα υπόλοιπα πεδία.

***3.6***

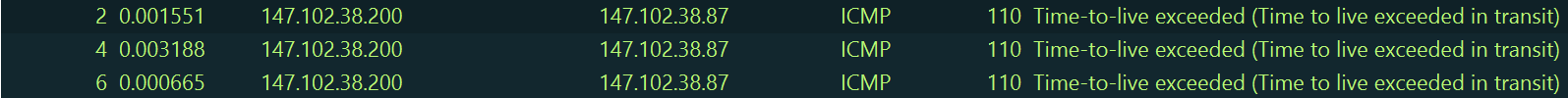
Πρέπει να παραμείνουν αμετάβλητα τα εξής πεδία:

* **Version**, για να καθορίσει ότι πρόκειται για IPv4 πακέτα
* **Total Length**, καθώς το default ICMP payload είναι 56 bytes, επομένως εάν προσθέσουμε το ICMP header (8), το IPv4 header (20) και το Ethernet Header (8) φτάνουμε τα 92 bytes
* **Protocol**, καθώς πρέπει να έχει τιμή ICMP για την καταγραφή που κάναμε
* **Source address**, αφού μελετάμε πακέτα που έστειλε ο υπολογιστής μας
* **Destination address**, διότι με το συγκεκριμένο tracert έχουμε δεδομένο τελικό στόχο κατά το capturing

***3.7***

Πρέπει να αλλάξουν τα εξής πεδία:

* **Identification**, καθώς σε μια αμφίδρομη επικοινωνία καθορίζεται μοναδικά το κάθε πακέτο
* **Time to Live**, προκειμένου να φτάσει τον τελικό επιθυμητό στόχο (όχι πάντα απαραίτητο, μπορεί να φτάναμε στο στόχο με TTL = 1)
* **Header Checksum**, εφόσον προκύπτει με βάση όλα τα υπόλοιπα πεδία και είδαμε πως το Identification αλλάζει, άρα και αυτό

***3.8***

Η τιμή του ζητούμενου πεδίου είναι TTL = 255.

***3.9***

Τα πακέτα αυτά προκύπτουν ως απάντηση στην τριάδα μηνυμάτων που στείλαμε με TTL = 1, εφόσον προέρχονται από τον κοντινότερο σε εμάς δρομολογητή. Επομένως, αφού στείλαμε τριάδα, λάβαμε επίσης τριάδα, η οποία προφανώς έχει ίδιο TTL.

***3.10***

Κατά σειρά, τα επόμενα ICMP Time Exceeded πακέτα προέρχονται από τις παρακάτω διευθύνσεις με τα αντίστοιχα TTL:

• ntua-zogr-3-gw.eier.access-link.grnet.gr (62.217.96.168) → TTL = 254

• grix-ADMIN.eier.access-link.grnet.gr (62.217.98.53) → TTL = 253

Παρατηρούμε πως καθώς κατευθυνόμαστε σε αύξουσα σειρά source πακέτων το TTL μειώνεται. Αυτό είναι αναμενόμενο, καθώς ο κάθε επόμενος (με κατεύθυνση από εμάς προς τον τελικό προορισμό) δρομολογητής έχει μπροστά του έναν παραπάνω κόμβο (σε σχέση με τον προηγούμενο), οπότε και όταν φτάνει σε εμάς το πακέτο, το TLL του έχει μειωθεί ανάλογα με το πόσους δρομολογητές πέρασε.

***3.11***

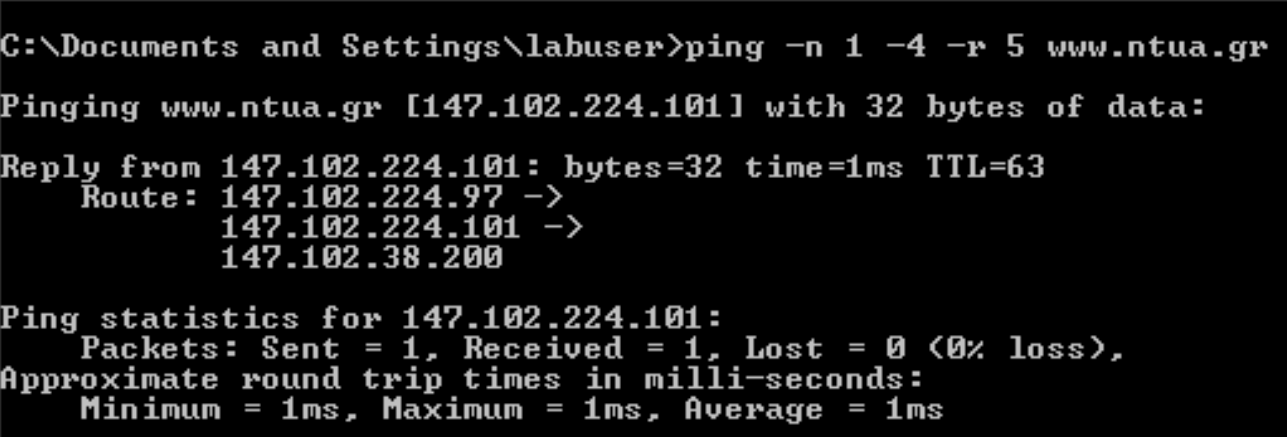
Η τιμή του πεδίου TTL της επικεφαλίδας των αντίστοιχων πακέτων IPv4 είναι TTL = 61.

***3.12***

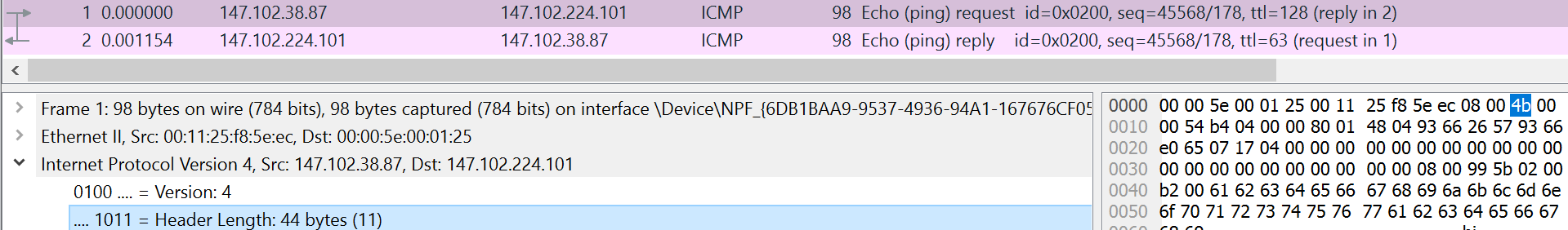
Στη διεπαφή του nic.gr-ix.gr η τιμή του πεδίου TTL ήταν 64. Αυτό ισχύει διότι το wireshark κάνει capture τα πακέτα στον υπολογιστή μας, επομένως για να έφτασε σε εμάς με TTL = 61, πέρασε από τους 3 (όπως είδαμε εκτελώντας την εντολή tracert) ενδιάμεσους κόμβους μειώνοντας κάθε φορά κατά 1 το TTL.

**Άσκηση 4: IPv4 options**

***4.1***

Η ακριβής σύνταξη της εντολής ping, ώστε να στείλουμε ένα μόνο πακέτο IPv4 με ενεργοποιημένη την επιλογή της καταγραφής διαδρομής για το μέγιστο δυνατό πλήθος διευθύνσεων είναι «ping -n 1 -4 -r 5 www.ntua.gr»

***4.2***

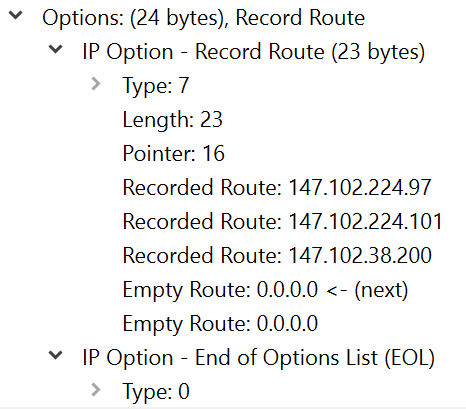
Η επικεφαλίδα IPv4 του πακέτου που έστειλε ο υπολογιστής μας έχει μέγεθος 44 bytes.

***4.3***

Αντίστοιχα, η επικεφαλίδα IPv4 του πακέτου που έλαβε ο υπολογιστής μας έχει μέγεθος 44 bytes.

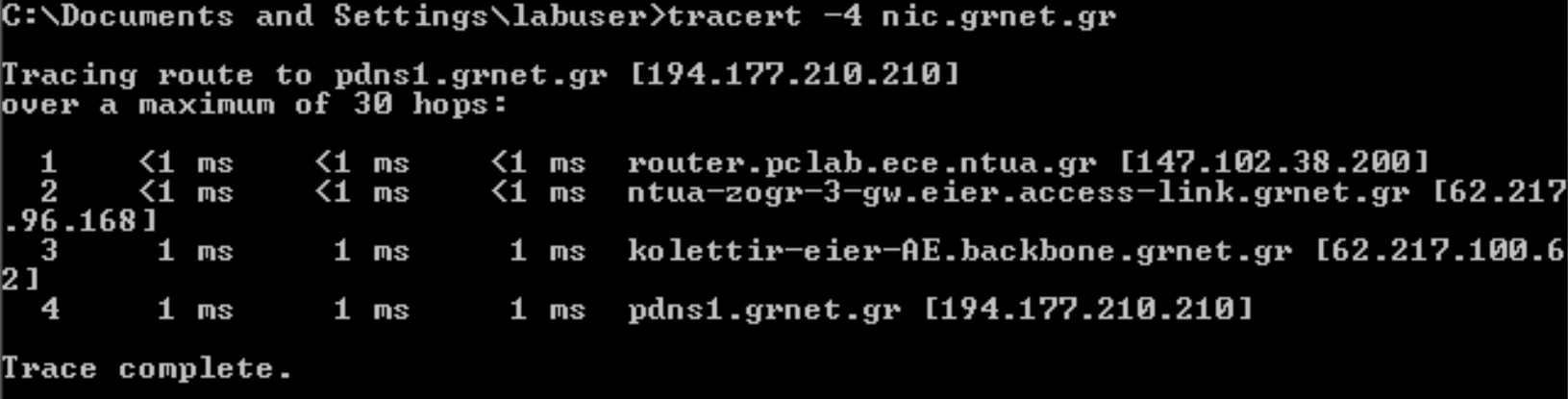
***4.4***

Τα πρώτα 20 bytes είναι τα γνωστά, όπως τα έχουμε αναλύσει στις προηγούμενες εργαστηριακές ασκήσεις. Τα υπόλοιπα 24 bytes που ακολουθούν, συγκροτούν ένα πεδίο που λέγεται Options. Το πεδίο αυτό έχει αυτό το μήκος καθώς περιέχει 4 bytes για τα υποπεδία του Type, Length, Pointer και EOL Type (ένα byte για κάθε πεδίο), και τα υπόλοιπα bytes αντιστοιχίζονται σε IPv4 διευθύνσεις των διεπαφών της οποίες συναντάει το πακέτο Echo (ping) reply κατά την διαδρομή του από την αφετηρία στον προορισμό. Συγκεκριμένα συνάντησε 3 διεπαφές (συν άλλες δύο μηδενικές (empty) IPv4), άρα σύνολο 24 bytes.



***4.5***

**Σχήμα 8:** *Η τοπολογία του δικτύου από τον υπολογιστή μας μέχρι την ιστοσελίδα www.ntua.gr, καταγράφοντας τις διεπαφές που προωθούν τα μηνύματα (απερχόμενες διεπαφές).*

***4.6***

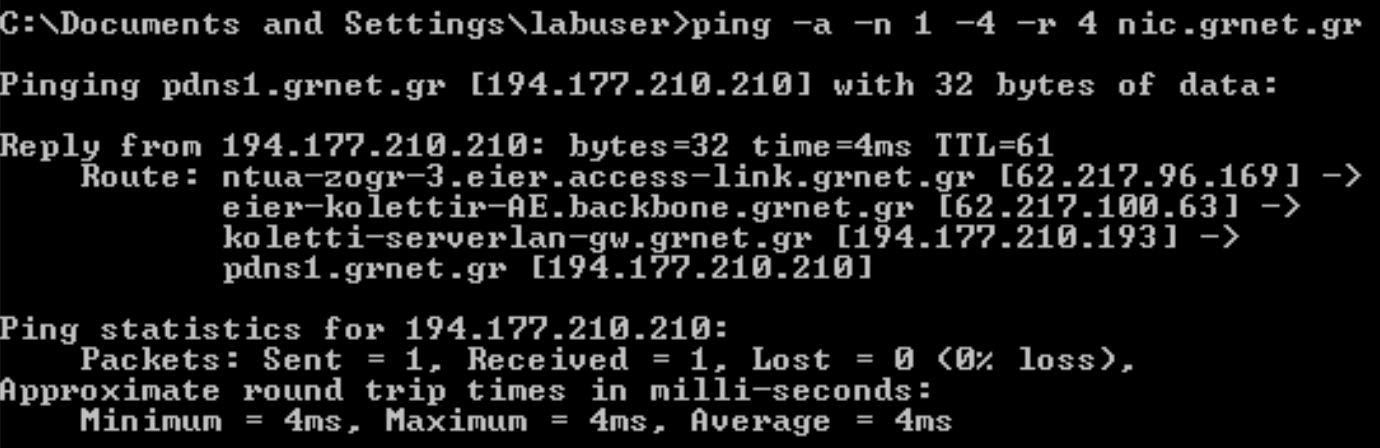
Βλέπουμε πως η IPv4 διεύθυνση του nic.grnet.gr είναι 194.177.210.210 και πως απέχει 4 βήματα από τον υπολογιστή μας.

***4.7***

Καταγράφουμε τις εξής IPv4 διευθύνσεις μέχρι τον nic.grnet.gr (Αναφέρονται σε διευθύνσεις, οι οποίες μας απαντάνε):

* router.pclab.ece.ntua.gr (147.102.38.200)
* ntua-zogr-3-gw.eier.access-link.grnet.gr (62.217.96.168)
* kolettir-eier-AE.backbone.grnet.gr (62.217.100.62)
* pdns1.grnet.gr (194.177.210.210)

***4.8***



Καταγράφουμε τις εξής IPv4 addresses (Αναφέρονται σε διευθύνσεις απερχόμενων διεπαφών)

* ntua-zogr-3.eier.access-link.grnet.gr (62.217.96.169)
* eier-kolettir-AE.backbone.grnet.gr (62.217.100.63)
* koletti-serverlan-gw.grnet.gr (194.177.210.193)
* pdns1.grnet.gr (194.177.210.210)

***4.9***

**Σχήμα 9:** *Η τοπολογία του δικτύου από τον υπολογιστή μας μέχρι τον nic.grnet.gr. Με κόκκινο φαίνονται οι διεπαφές που απαντάνε πίσω (tracert), ενώ με μαύρο αυτές που προωθούν τα μηνύματα (ping).*