Ονοματεπώνυμο: Ανδρέας Στάμος (03120***)	**Ομάδα:** 1
Όνομα PC/ΛΣ: linux / Ubuntu 22.04.2 LTS (με VPN στο δίκτυο του Πολυτεχνείου)	**Ημερομηνία:** 31/10/2023
Διεύθυνση IP: 147.102.131.218	**Διεύθυνση MAC:** DE–3F–DC–B2–E0–D0

Εργαστηριακή Άσκηση 5
Εξερεύνηση του Διαδικτύου

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

Η εργασία υλοποιήθηκε με σύνδεση στο δίκτυο VPN του Πολυτεχνείου.

Άσκηση 1

1.1 147.102.131.218

1.2 255.255.255.0 με μήκος προθέματος 24 bits

1.3 `ping -4 -c 1 -t {TTL} {TARGET IP ADDRESS}`

1.4 3

1.5 147.102.131.202 →
147.102.131.1 →
147.102.224.53 →
176.126.38.1

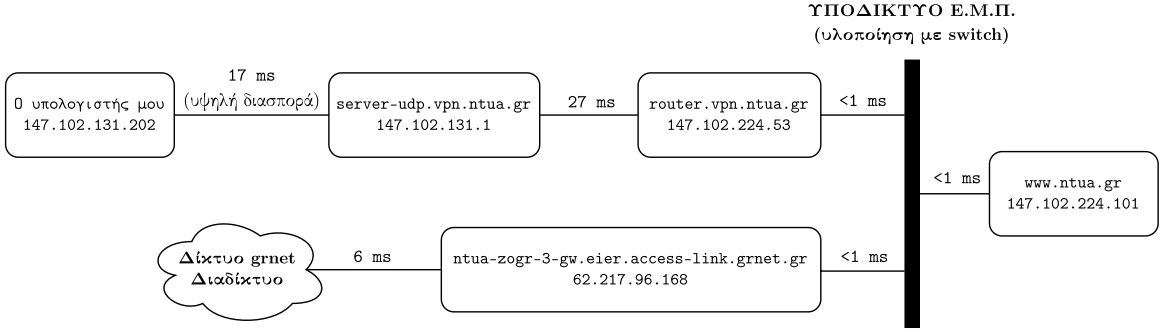
Σημείωση: Ο κάθε ενδιάμεσος δρομολογητής μπορεί να έχει πολλαπλά network interfaces με διαφορετικές IP διευθύνσεις για κάθε network interface, σίγουρα όμως κάθε δρομολογητής σε κάποιο network interface του κατέχει την IP διεύθυνση που αναγράφεται – ενδεχομένως το εν λόγω network interface να είναι διαφορετικό από εκείνα που χρησιμοποιούνται στην δρομόλογηση του πακέτου από τον υπολογιστή μας προς τον προορισμό, καθώς ο ενδιάμεσος δρομολογητής πιθανώς χρησιμοποιεί διαφορετική δρομολόγηση για τα πακέτα από αυτόν προς τα εμάς από ότι εμείς προς τον αρχικό προορισμό. (το ζήτημα σχολιάζεται αναλυτικότερα στο ερώτημα 4.7)

Άσκηση 2

2.1 `traceroute -I -4 www.ntua.gr`

Παρατηρούμε πως η διαδρομή που επιστρέφει το `traceroute` είναι διαφορετική από εκείνη που έχει γραφτεί στην εργασία. Αυτό είναι λογικό αφού βρισκόμαστε σε διαφορετικό τερματικό κόμβο, και συγκεκριμένα στον κόμβο που εξυπηρετείται το VPN, που πιθανώς είναι διαφορετικός από εκεί όπου γράφτηκε η εκφώνηση. Επίσης ενδεχομένως πλέον η ιστοσελίδα `www.ntua.gr` να γίνεται host σε διαφορετικό server από παλαιότερα.

2.2



Εικαζόμενη τοπολογία δικτύου δεδομένων Ε.Μ.Π. (Τα hop times έχουν σημαντική διασπορά)

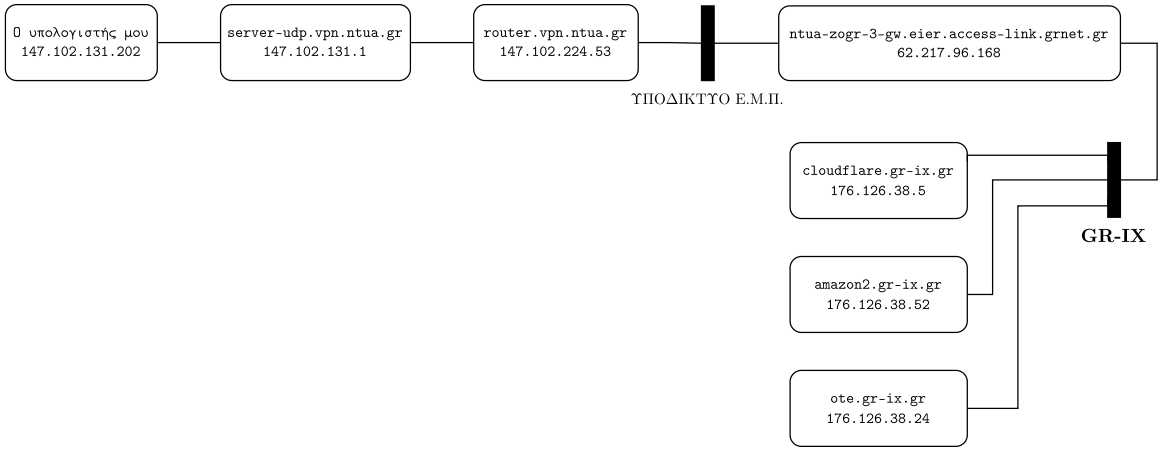
Προσοχή: Προτείνεται η μέλετη της Σημείωσης του ερωτήματος 1.5 και η απάντηση του ερωτήματος 4.7 για την ορθή ερμηνεία του σχήματος.

2.3 Ναι. Στο διάγραμμα του Κέντρου Δικτύων Ε.Μ.Π. παρατηρούμε πως το εσωτερικό δίκτυο του Ε.Μ.Π. αποτελεί ένα ενιαίο υποδίκτυο (που έχει δημιουργηθεί με switches), όπως παρατηρήσαμε και εμείς. Επίσης παρατηρούμε ότι συνδέεται στο διαδίκτυο μέσω του ΕΔΥΤΕ, όπως παρατηρήσαμε και εμείς (κόμβος `ntua-zogr-3-gw.eier.access-link.grnet.gr`).

2.4 `traceroute -I -4 -m 4 {TARGET HOST}`

2.5 `176.126.38.00/24`

2.6



Εικαζόμενη τοπολογία δικτύου δεδομένων Ε.Μ.Π. μέχρι GR-IX

Προσοχή: Η IP διεύθυνση, και κατ' επέκταση το αντίστοιχο domain name, που αναγράφεται σε κάθε ενδιάμεσο κόμβο αντιστοιχεί σε κάποιο από τα πολλά network interface του κόμβου και όχι κατ' ανάγκη σε κάποιο από τα network interfaces που χρησιμοποιούνται στην δρομολόγηση από εμάς προς τον κατά περίπτωση προορισμό (βλ. και Σημείωση ερωτήματος 1.5)

2.7 Ναι.

2.8 `traceroute -I -4 grnet.gr-ix.gr`

2.9 `udp or icmp`

2.10 0x01

2.11 40 bytes

2.12 Αποστέλλονται 6 τριάδες (κάθε τριάδα έχει ίδιο TTL). Εκ πρώτης όψεως, αυτό συμβαίνει επειδή το traceroute έχει default ρύθμιση να στέλνει ταυτόχρονα 16 πακέτα κάθε φορά που στέλνει. Το 18 προφανώς δεν είναι πολλαπλάσιο του 16. Μια εξήγηση που αποστέλλονται 18 πακέτα ήταν αρχικά πως το traceroute αποστέλλει τελικά ακέραιο πλήθος τριάδων με ίδιο TTL. Αυτό όμως τελικά δεν ισχύει, καθώς ακόμα και αν ρυθμίσουμε να αποστέλλεται μόνο ένα πάκετο για κάθε TTL (με `-q 1`), στέλνονται 17 πακέτα συνολικά. Μια νέα εξήγηση που αποστέλλονται παραπάνω από 16 πακέτα είναι πως το traceroute ξεκινά την 2η 16άδα πριν έρθει απάντηση της 1ης 16άδας, οπότε δεν ξέρει ακόμα μέχρι πόσο TTL θα χρειαστεί να φθάσει. Ωστόσο στο Wireshark βλέπουμε ότι απάντηση της 1ης 16άδας έρχεται πριν αποσταλλεί το 17ο πακέτο. Σκεφτήκαμε πως ίσως το Linux αφού λάβει ένα πακέτο αναβάλλει για λίγο την παράδοση του στην αρμόδια διεργασία. Ωστόσο, εκτέλοντας το traceroute με `strace` βλέπουμε πως το Linux παρέδωσε πακέτο απάντησης σε ερώτημα της 1ης 16άδας, προτού το traceroute στείλει 17ο πακέτο. Σκεφτήκαμε κατόπιν να δοκιμάσουμε να βάλουμε χρόνο μεταξύ των probes με το όρισμα `-z {WAIT SECONDS}`. Παρατηρούμε πως η παραπάνω συμπεριφορά δεν συμβαίνει για μεγάλο χρόνο ανάμεσα στα probes, συμβαίνει όμως με μικρό.

Τελικά, η πιο λογική εξήγηση είναι πως το traceroute αποστέλλει πακέτα με αυξανόμενο TTL (ή όσο εμείς ρυθμίσουμε το πλήθος ταυτόχρονων αποστολών πακέτων) μέχρι να λάβει Reply από τον target host (όχι από ενδιάμεσους κόμβους), χωρίς να περιμένει απάντηση από ενδιάμεσους κόμβους. Αυτή είναι λογική συμπεριφορά, καθώς ενδιάμεσοι κόμβοι μπορεί να κάνουν drop το πακέτο, χωρίς όμως να στέλνουν ICMP TTL exceeded.

2.13 Παραλήπτης είναι σε όλα το 176.126.38.1 (grnet.gr-ix.gr).

Για την 1η τριάδα requests λαβάμε απαντήσεις από το 147.102.131.1 (server-udp.vpn.ntua.gr).

Για την 2η τριάδα requests λαβάμε απαντήσεις από το 147.102.131.202 (router.vpn.ntua.gr).

Για την 3η τριάδα requests και για τις επόμενες λαβάμε απαντήσεις από το 176.126.38.1 (grnet.gr-ix.gr).

2.14 Ναι.

2.15 1η τριάδα: TTL=1
2η τριάδα: TTL=2
3η τριάδα: TTL=3
4η τριάδα: TTL=4
5η τριάδα: TTL=5
6η τριάδα: TTL=7

2.16 1η τριάδα: TTL=64
2η τριάδα: TTL=254
3η τριάδα: TTL=62
4η τριάδα: TTL=62
5η τριάδα: TTL=62
6η τριάδα: TTL=62

2.17 Κάθε δρομολογητής προτού προωθήσει ένα πακέτο μειώνει κατά ένα το TTL του. Αν το TTL μηδενιστεί, δεν προωθεί το πακέτο και στέλνει στον αποστολέα ένα ICMP TTL exceeded.
Η 1η τριάδα είχε TTL=1, οπότε στον 1ο δρομολογητή μηδενίστηκε και άρα ο 1ος δρομολογητής δεν προώθησε το πακέτο και έστειλε στον αποστολέα ICMP TTL exceeded.
Η 2η τριάδα είχε TTL=2, οπότε στον 2ο δρομολογητή μηδενίστηκε και άρα 2 1ος δρομολογητής δεν προώθησε το πακέτο και έστειλε στον αποστολέα ICMP TTL exceeded.

2.18 Όταν είναι ενδιάμεσος κόμβος που έγινε TTL=0 απαντά με type 0x11 (TTL exceeded).
Όταν είναι ο τελικός κόμβος απαντά με type 0x00 (Echo reply).

Άσκηση 3

3.1 `traceroute -I -4 nic.gr-ix.gr`

3.2 `icmp`

3.3 Ο υπολογιστής μου (147.102.131.218) →
server-udp.vpn.ntua.gr (147.102.131.1) →
router.vpn.ntua.gr (147.102.224.53) →
ntua-zogr-3-gw.eier.access-link.grnet.gr (62.217.96.168) →
* * * →
nic2.gr-ix.gr (195.130.66.4)

Προτείνεται η μέλετη της Σημείωσης του ερωτήματος 1.5 και η απάντηση του ερωτήματος 4.7 για την ορθή ερμηνεία.

3.4 Time To Live, Identification και Header Checksum

3.5 Version, Header Length, DSF, Total Length, Flags, Fragment Offset, Protocol, Source Address, Destination Address

3.6 Source Address και Destination Address ώστε το Echo Request να δρομολογηθεί προς τον στον σωστό παραλήπτη και επίσης το αντίστοιχο Echo Reply να δρομολογηθεί προς τα εμάς καθώς και Protocol καθώς στέλνονται πακέτα τύπου ICMP

3.7 Το TTL προκειμένουν να μηδενιστεί σε ενδιάμεσους δρομολογήτες, οι οποίο αφού μηδενίσουν το TTL θα μας στείλουν ICMP TTL Exceeded, οπότε έτσι θα μπορέσουμε να ανακαλύψουμε την διαδρομή που ακολουθεί ένα πακέτο. Αφού αλλάζει το TTL, θα πρέπει να αλλάζει και το Header Checksum.

3.8 64

3.9 Ναι. Ο δρομολογητής αυτός είναι ακριβώς γειτονικός μας, δηλαδή στο υποδίκτυο μας. Αφού δεν παρεμβάλλονται δρομολογήτες, το TTL παραμένει σταθερά στην αρχική τιμή του.

3.10 Τα TTL διαφέρουν, αφενός καθώς από πιο "μακρινούς" δρομολογητές το πακέτο ICMP TTL Exceeded θα πρέπει να περάσει από περισσότερους κόμβους για να φτάσει σε εμάς, οπότε θα έχει μειωθεί περισσότερο το TTL και αφετέρου καθώς διαφορετικοί δρομολογητές πιθανώς αρχικοποιούν το TTL σε διαφορετική τιμή. Αν γνωρίζουμε σε ποια τιμή ο δρομολογητής αρχικοποίησε το TTL, αφαιρώντας από αυτήν το TTL που λάβαμε, μπορούμε να βρούμε πόσους κόμβους μακριά μας είναι ο δρομολογητής που απέστειλε το ICMP TTL Exceeded.

3.10 Τα TTL μειώνονται κατά 1. Αυτό είναι λογικό αφού εμείς είχαμε αποστείλει IP πακέτα με TTL που αύξανανε κατά 1. Πάραυτα, δεν είναι αναγκαστικό να συμβεί, αφενός καθώς το πακέτο ICMP TTL Exceeded μπορεί να ακολουθήσει άλλη διάδρομη από του πακέτου Echo Request και αφετέρου καθώς ενδιάμεσοι δρομολογητές μπορεί να αρχικοποιούν το TTL σε διαφορετικές, αυθαίρετες τιμές.

3.11 60

3.12 Το πακέτο πέρασε από 4 δρομολογητές και έφτασε εμάς. Αρά όταν παράχθηκε είχε αρχική τιμή $60 + 4 = 64$.

Άσκηση 4

4.1 `ping -R -4 -c 1 www.ntua.gr`

4.2 60

4.3 60

4.4 20 bytes τα συνήθη πεδία της IPv4 επικεφαλίδας + 40 bytes τα Options

4.5 Ο υπολογιστής μου (147.102.131.218) →
vpn2.noc.ntua.gr (147.102.224.52) →
router.web.noc.ntua.gr (147.102.224.97) →
www.ntua.gr (147.102.224.101)

4.6 194.177.210.210, 5 hops μακριά

4.7 Αν το ελάχιστου κόστους μονοπάτι (έστω p) από τον Α προς τον Β περνάει από τον κόμβο Γ, τότε το τμήμα του p ως τον Γ είναι το ελαχίστου κόστους μονοπάτι από τον Α ως τον Γ. Υποθέτοντας ότι ο γράφος είναι μη κατευθυνόμενος (έχει το ίδιο βάρος σε μία ακμή και προς τις δύο κατευθύνσεις) μπορούμε να συμπεράνουμε ότι το μονοπάτι ελάχιστου κόστους από τον Γ προς τον Α είναι το αντεστράμμενο του ελάχιστου από τον Α ως τον Γ, δηλαδή το αντεστραμμένο του τμήματος του p ως Γ.

Με βάση αυτή την ιδιότητα, θεωρητικά, το ICMP TTL Exceeded θα αποστάλει από την ίδια διεπαφή με εκείνη που έφτασε το πάκετο που απέκτησε μηδενικό TTL. Συνεπώς, θεωρητικά, το `traceroute` μας επιστρέφει τις IP διευθύνσεις των **εισερχόμενων** διεπάφων των ενδιάμεσων κόμβους.

Δυστυχώς, όμως, η δρομολόγηση στο δίκτυο είναι μόνο κατά προσέγγιση ελάχιστου κόστους. Επίσης, μπορεί κάποιες συνδέσεις να είναι ασύμμετρες (δηλαδή διαφορετικού κόστους προς τις δύο κατευθύνσεις), οπότε το μονοπάτι ελαχίστου κόστους από τον Α προς τον Γ να είναι διαφορετικό από το μονοπάτι ελαχίστου κόστους από τον Γ προς τον Α. Αυτά μπορεί να οδηγήσουν τον ενδιάμεσο δρομολογητή Γ να στείλει το ICMP TTL Exceeded, στο οποίο στηρίζεται το `traceroute`, σε διαφορετικό network interface από εκείνο όπου προήλθε το πακέτο που έγινε drop. Αν συμβεί αυτό, η μόνη διαφορά θα είναι ότι στο ICMP TTL Exceeded δεν θα βλέπουμε την IP διεύθυνση της εισερχόμενης διεπαφής του ενδιάμεσου δρομολογητή, αλλά κάποιας αλλής διεπαφής του ίδιου δρομολογητή.

Ευελεπιστώντας ότι τα παραπάνω δεν θα συμβούν, θεωρούμε ότι το `traceroute` πράγματι επιστρέφει τις IP διευθύνσεις των εισερχόμενων διεπαφών των ενδιάμεσων κόμβων.

Από traceroute:

server-udp.vpn.ntua.gr (147.102.131.1) →
router.vpn.ntua.gr (147.102.224.53) →
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 vpn-131-202.vpn.ntua.gr (147.102.131.218) →
vpn2.noc.ntua.gr (147.102.224.52) →
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