

## Εργαστηριακή Άσκηση 5

### Εξερεύνηση του Διαδικτύου

Σε αυτήν την εργαστηριακή άσκηση θα συνεχίσετε την εξέταση των **ιδιοτήτων του πρωτοκόλλου IPv4**. Θα δείτε τον τρόπο χρήσης της επικεφαλίδας TTL του πακέτου IPv4 με σκοπό την εξαγωγή συμπερασμάτων σχετικών με τις διαδρομές εντός του διαδικτύου. Η άσκηση θα σας δώσει μια καλύτερη εικόνα για τη δομή του Internet και ειδικότερα για τη διασύνδεση των κόμβων ή την **τοπολογία**, όπως αλλιώς λέγεται, ενός τοπικού ή ευρύτερου δικτύου. Περισσότερες πληροφορίες για το πρωτόκολλο IPv4 μπορείτε να βρείτε στο [RFC 791](#). Για τη δομή των επικεφαλίδων των πρωτοκόλλων της σουίτας TCP/IP μπορείτε επίσης να συμβουλευθείτε και την **ιστοσελίδα** <http://www.networksorcery.com/enp/default0604.htm> επιλέγοντας το “IP protocol suite” από το αριστερό της μέρος και στη συνέχεια το πρωτόκολλο που σας ενδιαφέρει.

Όπως και στην προηγούμενη εργαστηριακή άσκηση, θα εργαστείτε με το πρόγραμμα Wireshark. Εδώ θα χρησιμοποιήσετε τη λειτουργία *Capture* με φίλτρο, ώστε τα πλαίσια που καταγράφονται να περιέχουν κάποια συγκεκριμένα χαρακτηριστικά. Υπενθυμίζεται ότι το φίλτρο απεικόνισης (*Display*) μπορεί να (απ)ενεργοποιηθεί οποιαδήποτε στιγμή κατά τη διάρκεια της καταγραφής, καθώς επίσης και μετά την ολοκλήρωση αυτής, προκειμένου να αποκρύπτει(αποκαλύπτει) κάποια από τα συλληφθέντα πλαίσια, ενώ το φίλτρο σύλληψης, που επιλέγετε από το μενού *Capture*, ενεργοποιείται πάντοτε **πριν** ξεκινήσει η διαδικασία καταγραφής, με αποτέλεσμα να καταγράφεται μόνο ένα μέρος των διερχόμενων πλαισίων.

Για τις ανάγκες αυτής της άσκησης θα χρειαστεί να συνδεθείτε στο ΕΜΠ χρησιμοποιώντας την υπηρεσία εικονικού ιδιωτικού δικτύου (VPN) του Κέντρου Δικτύων. Επισκεφθείτε την **ιστοσελίδα** <http://www.noc.ntua.gr/help/VPN> και ακολουθήστε τις οδηγίες εκεί για να εγκαταστήσετε το πρόγραμμα OpenVPN στον υπολογιστή σας ανάλογα με το λειτουργικό σύστημα που χρησιμοποιείτε.

**Για τις παρακάτω ασκήσεις απαντήστε στο συνοδευτικό φυλλάδιο, το οποίο θα υποβάλλετε ως αρχείο pdf.**

### 1 Ο χρόνος ζωής των πακέτων IPv4

Στο Internet δεν υπάρχουν συγκεκριμένες οδοί μεταφοράς των πακέτων, καθώς αυτό απαρτίζεται από πολλά επιμέρους δίκτυα (μικρά ή μεγάλα) που συνδέονται μεταξύ τους μέσω πολλαπλών διαφορετικών διαδρομών. Στα δίκτυα αυτά, συνδέονται εξυπηρετητές και απλοί προσωπικοί υπολογιστές μέσω δικτυακών συσκευών, όπως είναι οι μεταγωγείς (switches). Η διαδρομή ενός μηνύματος από την πηγή μέχρι τον προορισμό του καθορίζεται από τους διάφορους δρομολογητές (routers) που μεσολαβούν και η λήψη των αποφάσεων είναι δυναμική, δηλαδή, αλλάζει ανάλογα με τις τρέχουσες συνθήκες.

Η διαδρομή που ακολουθεί ένα πακέτο μπορεί να ανιχνευθεί εμμέσως θέτοντας μεταβαλλόμενες τιμές στο πεδίο Time-To-Live (TTL) της επικεφαλίδας ενός πακέτου IPv4. Κατά το [RFC 791](#) η τιμή του είναι ο μέγιστος χρόνος παραμονής ενός πακέτου εντός του διαδικτύου μετρημένος σε sec. Κάθε δρομολογητής κατά μήκος της διαδρομής προς τον προορισμό οφείλει να το μειώνει τουλάχιστον κατά 1, προτού προωθήσει το πακέτο, ακόμη και εάν η διαδικασία προώθησης διαρκέσει λιγότερο από 1 sec. Όταν το TTL μηδενισθεί ο δρομολογητής οφείλει να στείλει μήνυμα ICMP *Time Exceeded* στην πηγή. Στην πράξη αυτό σημαίνει ότι το TTL μειώνεται κατά ένα σε κάθε βήμα και παρά την ονομασία του μετρά βήματα και όχι χρόνο. Ως αποτέλεσμα αυτής της διαδικασίας, η αποστολή (από τον υπολογιστή σας) ενός πακέτου IPv4 με τιμή TTL ίση με 1 θα προκαλέσει την αποστολή ενός μηνύματος ICMP *Time Exceeded* (προς τον υπολογιστή σας) από τον δρομολογητή που βρίσκεται ένα βήμα πιο πέρα. Η αποστολή ενός πακέτου IPv4 με τιμή TTL ίση με 2 θα προκαλέσει την αποστολή ενός μηνύματος ICMP *Time Exceeded* προς τον υπολογιστή

σας από τον δρομολογητή που βρίσκεται δύο βήματα πιο πέρα, κοκ. Έτσι η επικεφαλίδα TTL, άσχετα με ό,τι υποδηλώνει το όνομα της, δεν έχει πλέον σχέση με χρονική διάρκεια. Εκφράζει απλά το μέγιστο πλήθος κόμβων από τους οποίους μπορεί να περάσει ένα πακέτο IPv4 μέχρι τον προορισμό του.

Για τη συνέχεια συνδεθείτε<sup>1</sup> μέσω OpenVPN στο εσωτερικό δίκτυο του ΕΜΠ. Το πρόγραμμα θα δημιουργήσει μια εικονική διεπαφή, που τυπικά έχει την ονομασία TAP ή TUN, με διεύθυνση IPv4 από το χώρο των διευθύνσεων 147.102.0.0/16 του Ιδρύματος. Οι καταγραφές που θα κάνετε στη συνέχεια θα γίνουν στη συγκεκριμένη διεπαφή και όχι σε αυτή της κάρτας δικτύου του υπολογιστή σας.

- 1.1 Ποια είναι η διεύθυνση IPv4 της εικονικής διεπαφής TAP/TUN; Σημειώστε την στο φύλλο απαντήσεων.
- 1.2 Ποια είναι η μάσκα υποδικτύου και ποιο το μήκος προθέματος δικτύου;
- 1.3 Ποια είναι η σύνταξη της εντολής ping ώστε να παράγετε **ένα** μόνο πακέτο **IPv4** με συγκεκριμένη τιμή της επικεφαλίδας TTL;

Ξεκινήστε μια καταγραφή με φίλτρο σύλληψης ώστε να καταγράφονται μόνο τα πλαίσια που περιλαμβάνουν τη διεύθυνση IPv4 της εικονικής διεπαφής TAP/TUN. Χρησιμοποιήστε τη σύνταξη της προηγούμενης ερώτησης για να κάνετε ping στο 176.126.38.1 ξεκινώντας από την τιμή TTL=1 και αυξάνοντάς τη διαδοχικά κατά 1 μέχρι να παύσει να εμφανίζεται το μήνυμα σχετικό με τη λήξη του TTL<sup>2</sup>. Όταν τελειώσει η καταγραφή εφαρμόστε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με το πρωτόκολλο ICMP.

- 1.4 Ποια είναι η ελάχιστη τιμή TTL για να φτάσει το πακέτο στο 176.126.38.1;
- 1.5 Σχεδιάστε ένα απλό διάγραμμα της διαδρομής μέχρι τη διεπαφή με διεύθυνση 176.126.38.1 όπου να εμφανίζονται οι διευθύνσεις IPv4 των ενδιάμεσων διεπαφών. [Υπόδειξη: Απαντήστε με τη βοήθεια του παραθύρου εντολών.]

## 2 Ανακαλύψτε την τοπολογία

Το τέχνασμα της διαδοχικής αύξησης του TTL χρησιμοποιείται από την εντολή tracert (σε μηχανήματα με λειτουργικό σύστημα Windows) ή traceroute (σε μηχανήματα τύπου Unix ή Linux) για να βρεθεί η διαδρομή που ακολουθεί ένα πακέτο. Η tracert στέλνει μηνύματα ICMP Echo Request, όπως κάνατε προηγουμένως, ενώ η traceroute στέλνει δεδομενογράμματα UDP με θύρα προορισμού στην περιοχή από 33434 έως 33534. Τα μηνύματα ICMP Echo Request ή τα δεδομενογράμματα UDP στέλνονται σε τριάδες προς τον προορισμό ενθυλακωμένα σε πακέτα IPv4 με μεταβαλλόμενες τιμές του πεδίου Time-To-Live (TTL). Και στις δύο υλοποιήσεις, η τιμή της παραμέτρου Time-to-live (TTL) κάθε πακέτου IPv4 αρχίζει με την τιμή 1 και αυξάνεται κατά 1 για κάθε διαδοχική αποστολή τριάδων.

Η διαδρομή βρίσκεται εξετάζοντας τα μηνύματα ICMP Time Exceeded, που προκαλούνται από διαδοχικά πακέτα IPv4 με συνεχώς αυξανόμενες τιμές του TTL, και καταγράφοντας την εκάστοτε διεύθυνση IPv4 της πηγής που παράγει το μήνυμα ICMP. Παράλληλα, στην έξοδο εμφανίζονται και οι αντίστοιχες τιμές Round Trip Time (RTT) ανά βήμα. Εάν δεν ληφθεί απάντηση μέσα σε συγκεκριμένο χρονικό διάστημα, 4 sec στα Windows, εμφανίζεται αστεράκι και αποστέλλεται το επόμενο μήνυμα. Εάν δεν ληφθεί καμία απάντηση, εμφανίζονται τρία αστεράκια και η εκτέλεση της εντολής συνεχίζει αυξάνοντας το TTL μέχρις ότου τα πακέτα IPv4 φτάσουν στον προορισμό τους ή μέχρι να εξαντληθεί το μέγιστο επιτρεπτό πλήθος βημάτων, συνήθως 30. Εάν φτάσουν επιτυχώς τα ICMP Echo Request στον προορισμό τους, θα παραχθούν ως απάντηση ICMP Echo Reply. Στην περίπτωση δεδομενογραμμάτων UDP, θα παραχθούν ICMP Destination Unreachable. Εάν παρατηρηθεί μία μόνο εκπνοή χρόνου, το πιθανότερο είναι ότι η διαδρομή (μέχρι το σημείο

<sup>1</sup> Στα μηχανήματα του PC Lab θα κάνετε καταγραφή στην κάρτα δικτύου, γιατί το OpenVPN δεν είναι εγκατεστημένο.

<sup>2</sup> Εάν αντί μηνύματος λήξης του TTL υπάρξει εκπνοή χρόνου, δοκιμάστε άλλη μία φορά και εάν επιμένει αγνοήστε την και προχωρήστε στο επόμενο βήμα.

αυτό) είναι φορτωμένη. Εάν, ωστόσο, παρατηρηθούν διαδοχικές εκπνοές χρόνου, τότε το πιθανότερο είναι ότι παρεμβάλλεται κάποιο τείχος προστασίας. Σε τέτοια περίπτωση δεν υπάρχει λόγος να περιμένετε την ολοκλήρωση της εντολής, απλά διακόψτε πιέζοντας τον συνδυασμό πλήκτρων <Ctrl>+c. Για μια πιο παραστατική περιγραφή της ανταλλαγής μηνυμάτων στην περίπτωση της εντολής traceroute δείτε το παράδειγμα του διαγράμματος ροής στην ιστοσελίδα <https://www.eventhelix.com/networking/Icmp.pdf>.

Η παροχή τέτοιας λεπτομερούς πληροφόρησης σχετικά με τη διαδρομή των πακέτων ήταν αποδεκτή στις αρχικές ημέρες του διαδικτύου. Αργότερα όμως άρχισε να θεωρείται προβληματική για λόγους ασφαλείας. Η πληροφόρηση που μπορεί να λάβει κανείς μέσω των εντολών ping και traceroute χρησιμοποιήθηκε από ιούς και σκουλήκια για να εντοπίσουν πιθανούς στόχους για την εξάπλωσή τους. Επίσης, οι εντολές χρησιμοποιήθηκαν συχνά από χάκερς για να αποκτήσουν γνώση σε σχέση με την αρχιτεκτονική (εταιρικών) δικτύων και στη συνέχεια να εκμεταλλευθούν πιθανές τρωτότητες κόμβων ή υπολογιστών. Γι' αυτό αρκετά δίκτυα άρχισαν να φιλτράρουν στα όρια τους τα μηνύματα ICMP Echo Request. Έτσι, εν γένει, μπορεί κάποιος να βρει τη διαδρομή μέχρι την άκρη ενός (εταιρικού) δικτύου, αλλά όχι τη διαδρομή στο εσωτερικό του. Παρόλα αυτά αμφότερες οι εντολές είναι χρήσιμα διαγνωστικά εργαλεία και βοηθούν αρκετές φορές στην επίλυση προβλημάτων (δρομολόγησης) ή στην εύρεση των πλησιέστερων κόμβων π.χ. για το κατέβασμα δημοφιλών αρχείων. Να σημειωθεί ότι στο Unix/Linux, η εντολή traceroute μπορεί επίσης να κληθεί με το κατάλληλο τρόπο ώστε να χρησιμοποιήσει πρωτόκολλο ICMP ή το TCP αντί του UDP. Με τη χρήση TCP σε αρκετές περιπτώσεις είναι δυνατό να διαπεραστούν τα τείχη πυρασφάλειας (firewalls) μέσω θυρών π.χ. της 80, που είναι ανοικτές για τους υπολογιστές που βρίσκονται πίσω τους, στέλνοντας τεμάχια TCP SYN, αντί δεδομενογράμματα UDP ή μηνύματα ICMP Echo Request.

Στο παρελθόν εάν από το μηχάνημα Windows με διεύθυνση IP 147.102.7.43 (εντός της Πολυτεχνειούπολης) κάνατε tracert προς τον κεντρικό εξυπηρετητή ιστού του ΕΜΠ [www.ntua.gr](http://www.ntua.gr), θα λαμβάνατε μια απάντηση παρόμοια με την επόμενη:

```
C:\>tracert www.ntua.gr
```

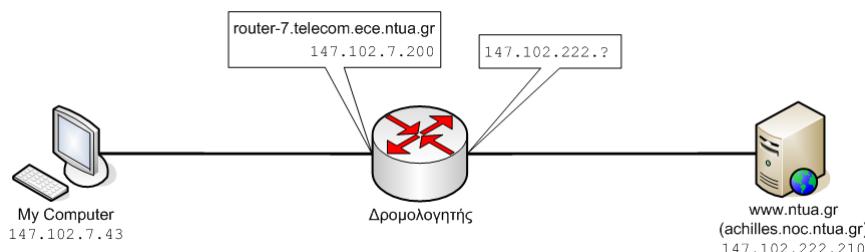
```
Tracing route to achilles.noc.ntua.gr [147.102.222.210]
over a maximum of 30 hops:
```

```
1      2 ms      *      *      router-7.telecom.ece.ntua.gr [147.102.7.200]
2     <1 ms    <1 ms    <1 ms  achilles.noc.ntua.gr [147.102.222.210]
```

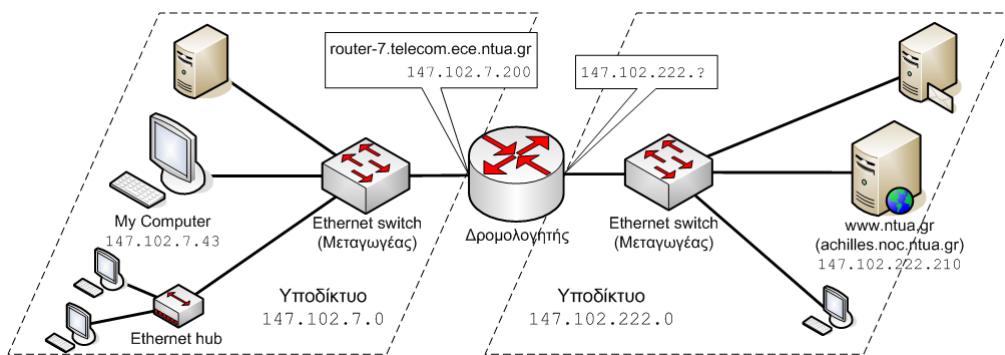
Trace complete.

```
C:\>
```

που σημαίνει ότι το επίσημο όνομα (CNAME) του εξυπηρετητή ιστού είναι [achilles.noc.ntua.gr](http://achilles.noc.ntua.gr), η IPv4 διεύθυνσή του είναι 147.102.222.210 και η διαδρομή μέχρι αυτόν διέρχεται από τον δρομολογητή [router-7.telecom.ece.ntua.gr](http://router-7.telecom.ece.ntua.gr). Οι χρόνοι στην απάντηση αντιστοιχούν στην καθυστέρηση RTT στο συγκεκριμένο βήμα της διαδρομής και όπου εμφανίζεται \* δεν λήφθηκε απάντηση στο Echo Request. Από τα παραπάνω αποτελέσματα μπορείτε να υποθέσετε μια τοπολογία της ακόλουθης μορφής:



Ωστόσο, πιο κοντά στην πραγματική τοπολογία του δικτύου της Πολυτεχνειούπολης είναι το διάγραμμα στο επόμενο σχήμα, όπου φαίνονται, επιπλέον, πιθανοί τρόποι σύνδεσης του σταθμού εργασίας και του εξυπηρετητή ιστού στα επιμέρους τοπικά δίκτυα που ορίζει ο δρομολογητής.



Επαναλάβετε το traceroute ή tracert από τον υπολογιστή σας προς τον κεντρικό εξυπηρετητή ιστού του ΕΜΠ [www.ntua.gr](http://www.ntua.gr), φροντίζοντας να παραχθούν πακέτα IPv4.

- 2.1 Ποια η σύνταξη της εντολής που χρησιμοποιήσατε και ποιες διαφορές παρατηρείτε σε σχέση με το παρελθόν;
- 2.2 Να σχεδιάσετε μια άποψη της τοπολογίας του δικτύου δεδομένων του Πολυτεχνείου όπως φαίνεται από τη σύνδεση που έχετε κάνει με το OpenVPN. Χρησιμοποιήστε διαδοχικά την εντολή traceroute ή tracert όπως πριν με προορισμούς τρεις εξυπηρετητές ιστού των Σχολών του ΕΜΠ ή μία εκ των οποίων να είναι των Αρχιτεκτόνων Μηχανικών. Το σχεδιάγραμμα να περιλαμβάνει τον υπολογιστή σας, τους δρομολογητές και τους εξυπηρετητές ιστού, καταγράφοντας παράλληλα τα ονόματα DNS (αν υπάρχουν), τις IPv4 διευθύνσεις τους, καθώς και τη μέση καθυστέρηση ανά βήμα.

Στη σελίδα <http://www.noc.ntua.gr/el/data-network-infrastructure> το Κέντρο Δικτύων του Ε.Μ.Π. έχει δημοσιεύσει δύο διαγράμματα σχετικά με την τοπολογία του δικτύου δεδομένων του Ε.Μ.Π.

- 2.3 Το σχεδιάγραμμά σας συμφωνεί με το προηγούμενο σχήμα;

Ο κόμβος Greek Internet Exchange (<https://www.gr-ix.gr>) δημιουργήθηκε το 2009 και αποτελεί διάδοχο του AIX (Athens Internet Exchange), το οποίο λειτουργούσε από το 2000. Η διαχείριση και λειτουργία του γίνεται από το τέως Εθνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΔΕΤ Α.Ε.) νυν ΕΔΥΤΕ Α.Ε. Προσφέρει τοπική διασύνδεση (peering) μεταξύ των εμπορικών δικτύων των εταιρειών παροχής υπηρεσιών Internet (ISP) που δραστηριοποιούνται στην ελληνική επικράτεια για την απευθείας ανταλλαγή κίνησης IP μεταξύ τους καθώς και με το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας. Έχει τρία σημεία φυσικής παρουσίας στην Αθήνα, ATH01 – Εθνικό Τιρόμα Ερευνών, ATH02 – Lamda Hellix και ATH03 – Telecom Italia Sparkle Greece και ένα στη Θεσσαλονίκη, THESS01 – Synapsecom Telecoms. Με τη βοήθεια της εντολής traceroute ή tracert, παρατηρήστε τα πρώτα τέσσερα βήματα (διευθύνσεις IPv4) των διαδρομών μέχρι τους εξυπηρετητές ιστού [www.forthnet.gr](http://www.forthnet.gr), [www.vodafone.gr](http://www.vodafone.gr) και [www.cosmote.gr](http://www.cosmote.gr), αντίστοιχα.

- 2.4 Ποια σύνταξη της εντολής traceroute ή tracert χρησιμοποιήσατε ώστε να παράγετε πακέτα IPv4 και να περιορίσετε το μέγιστο πλήθος βημάτων σε τέσσερα;
- 2.5 Βάσει των αποτελεσμάτων για τους παραπάνω προορισμούς, σχεδιάστε την τοπολογία του δικτύου από τον υπολογιστή σας μέχρι τον κόμβο GR-IX όπως φαίνεται από τη σύνδεση που έχετε κάνει με το OpenVPN.
- 2.6 Το σχεδιάγραμμά σας συμφωνεί με την πλήρη τοπολογία που θα βρείτε στην ιστοσελίδα<sup>3</sup> <https://grnet.gr/infrastructure/network-and-topology/>;
- 2.7 Ποια είναι η διεύθυνση του υποδικτύου IPv4 του GR-IX;

Χρησιμοποιώντας φίλτρο σύλληψης όπως πριν, καταγράψτε τη δικτυακή κίνηση όταν εκτελείτε την εντολή traceroute ή tracert με προορισμό το [grnet.gr-ix.gr](https://grnet.gr-ix.gr) παράγοντας πακέτα IPv4 (όχι IPv6) και φροντίζοντας να μην γίνεται επίλυση των διευθύνσεων IPv4 σε ονόματα. Όταν τελειώσει η

<sup>3</sup> Στο σχήμα ο δρομολογητής του ΕΜΠ αναφέρεται ως NTUASW στον κόμβο EIE.

καταγραφή εφαρμόστε ένα φίλτρο απεικόνισης, ώστε να παραμείνουν μόνο πλαίσια σχετιζόμενα με τα πρωτόκολλα UDP ή ICMP.

- 2.8 Ποια σύνταξη της εντολής traceroute ή tracert χρησιμοποιήσατε;
- 2.9 Γράψτε τη σύνταξη του φίλτρου απεικόνισης που χρησιμοποιήσατε.
- 2.10 Καταγράψτε την τιμή του πεδίου Protocol της επικεφαλίδας IPv4 ενός μηνύματος που στάλθηκε κατά την εκτέλεση της εντολής.
- 2.11 Πόσα byte μεταφέρει το προηγούμενο πακέτο IPv4 στο πεδίο δεδομένων;
- 2.12 Πόσες τριάδες μηνυμάτων αποστέλλονται και πόσες λαμβάνονται;
- 2.13 Καταγράψτε για κάθε τριάδα μηνυμάτων που στείλατε τη διεύθυνση IPv4 του παραλήπτη του μηνύματος και για κάθε τριάδα που προκλήθηκε ως απάντηση τη διεύθυνση IPv4 από όπου έρχεται η απάντηση.
- 2.14 Είναι οι διευθύνσεις από όπου λάβατε απαντήσεις ίδιες με αυτές που σημειώσατε προηγουμένως στο ερώτημα 1.5;
- 2.15 Καταγράψτε τις τιμές του πεδίου TTL του πακέτου IPv4 για κάθε τριάδα μηνυμάτων που στείλατε.
- 2.16 Καταγράψτε τις αντίστοιχες τιμές του πεδίου TTL για κάθε τριάδα απαντήσεων που λάβατε.
- 2.17 Γιατί οι πρώτοι κόμβοι της διαδρομής απαντούν με μήνυμα ICMP *Time-to-live exceeded*;
- 2.18 Με ποιο τύπο μηνύματος ICMP απαντά ο προορισμός;

### **3 Περισσότερα για τις επικεφαλίδες πακέτων IP**

Ακολούθως ξεκινήστε μια νέα καταγραφή με φίλτρο σύλληψης ώστε να παρατηρείτε μόνο μηνύματα ICMP. Αναζητήστε με tracert ή traceroute τη διαδρομή μέχρι το μηχάνημα [nic.gr-ix.gr](http://nic.gr-ix.gr). Στην περίπτωση της traceroute χρησιμοποιήστε στην κατάλληλη σύνταξη ώστε να παραχθούν μηνύματα ICMP *Echo Request*.

- 3.1 Ποια σύνταξη της εντολής χρησιμοποιήσατε;
- 3.2 Ποιο φίλτρο σύλληψης χρησιμοποιήσατε;
- 3.3 Σχεδιάστε ένα απλό διάγραμμα της διαδρομής.

Επιλέξτε ένα μήνυμα ICMP *Echo Request* και στο παράθυρο με τις λεπτομέρειες αναπτύξτε τις επικεφαλίδες του πρωτοκόλλου IPv4. Στη συνέχεια ταξινομήστε κατά αύξουσα σειρά τα πακέτα IPv4 σύμφωνα με τη διεύθυνση IPv4 της πηγής τους (Source) κάνοντας κλικ στην αντίστοιχη επικεφαλίδα του παράθυρου με τη λίστα καταγεγραμμένων πακέτων. Εάν το βέλος δείχνει προς τα κάτω (φθίνουσα σειρά), κάντε πάλι κλικ στην επικεφαλίδα ώστε να δείχνει προς τα άνω (αύξουσα σειρά). Στη λίστα θα πρέπει να εμφανίζονται τώρα με τη σειρά όλα τα πακέτα IPv4 που έστειλε ο υπολογιστής σας. Επιλέξτε το πρώτο πακέτο IPv4 που έστειλε ο υπολογιστής σας και αναπτύξτε τα περιεχόμενά της επικεφαλίδας Internet Protocol Version 4. Χρησιμοποιώντας το πλήκτρο ↓ (κάτω βέλος) μετακινηθείτε από το πρώτο στο τελευταίο πακέτο IPv4 της σειράς που έστειλε ο υπολογιστής σας.

- 3.4 Ποια πεδία της επικεφαλίδας IPv4 αλλάζουν;
- 3.5 Ποια πεδία της επικεφαλίδας IPv4 παραμένουν αμετάβλητα σε όλη τη σειρά;
- 3.6 Ποια πεδία της επικεφαλίδας IPv4 πρέπει να παραμείνουν αμετάβλητα και γιατί;
- 3.7 Ποια πεδία της επικεφαλίδας IPv4 **πρέπει** να αλλάξουν και γιατί;

Στη συνέχεια με τα πακέτα IPv4 ταξινομημένα όπως πριν, βρείτε την πρώτη σειρά μηνυμάτων ICMP *Time Exceeded* που στέλνονται από τον κοντινότερο προς τον υπολογιστή σας δρομολογητή.

- 3.8 Ποια είναι η τιμή του πεδίου TTL της επικεφαλίδας IPv4 του πρώτου πακέτου της σειράς ICMP *Time Exceeded*;
- 3.9 Παραμένουν οι τιμές του πεδίου αυτού σταθερές για όλα τα πακέτα της πρώτης σειράς ICMP *Time Exceeded*; Γιατί;
- 3.10 Καταγράψτε τις τιμές του πεδίου TTL της επικεφαλίδας IPv4 των πακέτων των επόμενων ICMP *Time Exceeded*. Τι παρατηρείτε;

Εντοπίστε την τελευταία σειρά μηνυμάτων ICMP *Echo Reply* που στέλνονται από τον προορισμό [nic.gr-ix.gr](#) προς τον υπολογιστή σας.

- 3.11 Ποια είναι η τιμή του πεδίου TTL της επικεφαλίδας των αντίστοιχων πακέτων IPv4.
- 3.12 Ποια ήταν η τιμή του πεδίου TTL στη διεπαφή του [nic.gr-ix.gr](#) όπου παράχθηκαν;

## 4 IPv4 options

Πληροφορίες για τη διαδρομή στο δίκτυο μπορεί να λάβει κανείς χρησιμοποιώντας προαιρετικές επιλογές (options) των επικεφαλίδων IPv4. Η πλειονότητα των πακέτων IPv4 περιλαμβάνουν τη συνήθη επικεφαλίδα των 20 byte με τα πεδία που είδατε σε αυτήν και τις προηγούμενες ασκήσεις. Οι δημιουργοί του IPv4 προέβλεψαν τη δυνατότητα μετά το σταθερό μέρος (20 byte) της επικεφαλίδας να ακολουθούν προαιρετικές επιλογές (options). Όλοι οι δρομολογητές απαιτείται να τις διαβάζουν και να ενεργούν κατάλληλα. Όμως, το μέγιστο μήκος επικεφαλίδας IPv4 είναι 60 byte, οπότε μόνο 40 byte είναι διαθέσιμα για προαιρετικές επιλογές. Οι πιο συνήθεις εξ αυτών σχετίζονται με τη δρομολόγηση πηγής (Source Routing), την καταγραφή διαδρομών (Record Route) και την καταγραφή χρόνων (Time stamp). Στην περίπτωση της καταγραφής διαδρομών, όταν ο δρομολογητής λάβει ένα πακέτο με την προαιρετική επιλογή της καταγραφής διαδρομής ενεργοποιημένη, εισάγει την IPv4 διεύθυνση της διεπαφής μέσω της οποίας θα το προωθήσει στη θέση της επικεφαλίδας που ορίζει ο σχετικός δείκτης, αυξάνει τον δείκτη κατά 4 και προωθεί το πακέτο. Εάν η επικεφαλίδα γεμίσει, το πακέτο προωθείται χωρίς την καταγραφή νέας διεύθυνσης IPv4.

Ξεκινήστε μια νέα καταγραφή με φίλτρο σύλληψης όπως πριν και χρησιμοποιήστε την εντολή `ping` για να καταγράψετε τη διαδρομή από τον προσωπικό σας υπολογιστή μέχρι τον κεντρικό εξυπηρετητή ιστού του ΕΜΠ [www.ntua.gr](http://www.ntua.gr). Ανατρέξτε στη σχετική με την εντολή `ping` τεκμηρίωση του λειτουργικού σας συστήματος για να βρείτε τον σωστό τρόπο κλήσης για την καταγραφή διαδρομών.

- 4.1 Ποια είναι η ακριβής σύνταξη της εντολής `ping` ώστε να στείλετε ένα μόνο πακέτο IPv4 με ενεργοποιημένη την επιλογή της καταγραφής διαδρομής για το μέγιστο δυνατό πλήθος διευθύνσεων;
- 4.2 Τι μέγεθος έχει η επικεφαλίδα του πακέτου IPv4 που έστειλε ο υπολογιστής σας;
- 4.3 Τι μέγεθος έχει η επικεφαλίδα του πακέτου IPv4 που έλαβε ο υπολογιστής σας;
- 4.4 Εξηγήστε πώς προσδιορίζεται το παραπάνω μήκος από τα στοιχεία που περιέχει η επικεφαλίδα.
- 4.5 Με βάση την παραπάνω καταγραφή σχεδιάστε τη διαδρομή από τον υπολογιστή σας μέχρι τον εξυπηρετητή ιστού [www.ntua.gr](http://www.ntua.gr) σημειώνοντας τις διευθύνσεις IPv4 **όλων** των διεπαφών από όπου πέρασε το μήνυμα ICMP. *Σημείωση:* Οι διευθύνσεις IPv4 αντιστοιχούν στις απερχόμενες διεπαφές των κόμβων κατά μήκος της διαδρομής.

Στη συνέχεια θα σχεδιάστε τη διαδρομή προς τον κόμβο [nic.grnet.gr](#). Η επειδή όπως είδατε το μέγιστο πλήθος διευθύνσεων που μπορούν να καταγραφούν είναι περιορισμένο θα βρείτε τα στοιχεία σε δύο φάσεις. Πρώτα θα κάνετε traceroute ή tracert προς τον προορισμό και θα εντοπίσετε τις διευθύνσεις IPv4 των διεπαφών των κόμβων που απαντούν στα ληγμένα TTL, δηλαδή, αυτών προς την πλευρά του υπολογιστή σας.

- 4.6 Ποια είναι η διεύθυνση IPv4 του [nic.grnet.gr](#); Πόσα βήματα μακριά από τον προσωπικό σας υπολογιστή βρίσκεται;
- 4.7 Καταγράψτε τις διευθύνσεις IPv4 των διεπαφών μέχρι τον [nic.grnet.gr](#).

Στη συνέχεια θα χρησιμοποιήσετε την επιλογή καταγραφής διαδρομής στο `ping` προς τον [nic.grnet.gr](#) για τόσα βήματα όσα βρήκατε προηγουμένως στην ερώτηση 4.6.

- 4.8 Καταγράψτε τις διευθύνσεις IPv4 των απερχόμενων διεπαφών μέχρι τον προορισμό.
- 4.9 Σχεδιάστε τη διαδρομή από τον υπολογιστή σας μέχρι τον [nic.grnet.gr](#) σημειώνοντας τις διευθύνσεις IPv4 **όλων** των διεπαφών από όπου πέρασε το μήνυμα ICMP.

Όνοματεπώνυμο: Νικόλας Μπέλλος (ει18183)	Ομάδα: 3
Όνομα PC/ΛΣ: BELLOS-DELL-G3 / Windows OS	Ημερομηνία: 15 / 11 / 2021
Διεύθυνση IP: 147 . 102 . 131 . 125	Διεύθυνση MAC: 7C - 2A - 31 - 40 - C9 - AF

## 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.

**1**

- 1.1 147.102.131.125  
 1.2 Subnet mask : 255.255.0.0, Prefix Length : 16  
 1.3 ping <address> -n 1 -4 -i 1  
 1.4 Path From : 147.102.131.125 To : 176.102.131.125

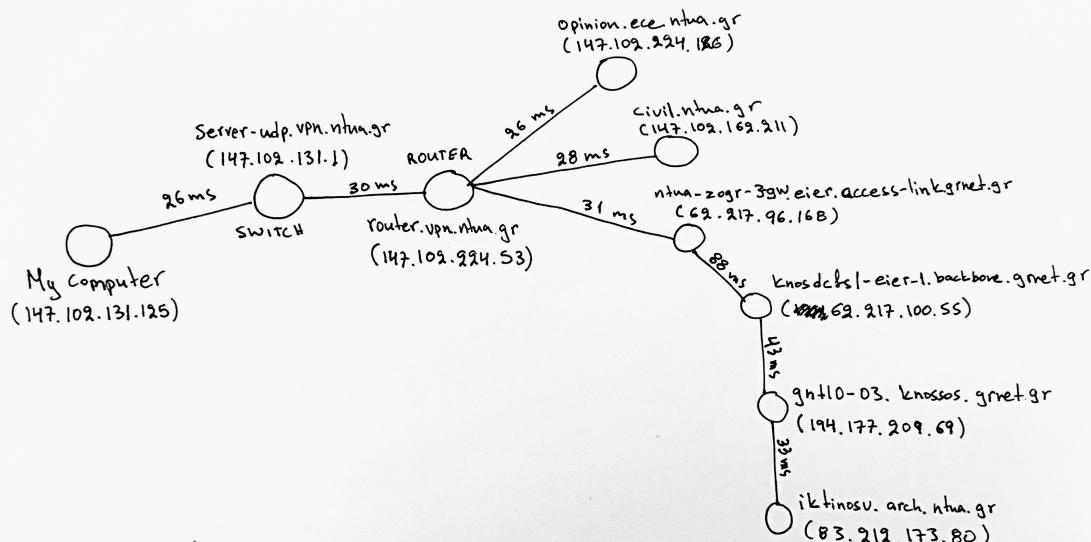
1.5



**2**

- 2.1 tracert -4 www.ntua.gr . Οι διαφορές είναι ,πέρα από το όνομα www.ntua.gr του εξυπηρετητή που δεν είναι πλέον achilles... και άρα δεν φαίνεται η δομή του υποδικτύου, ότι υπάρχει πέραν από το router και ένας κόμβος που δρά σαν switch (server-udp.vpn.ntua.gr).

2.2



2.3 Ναι, συμφωνεί

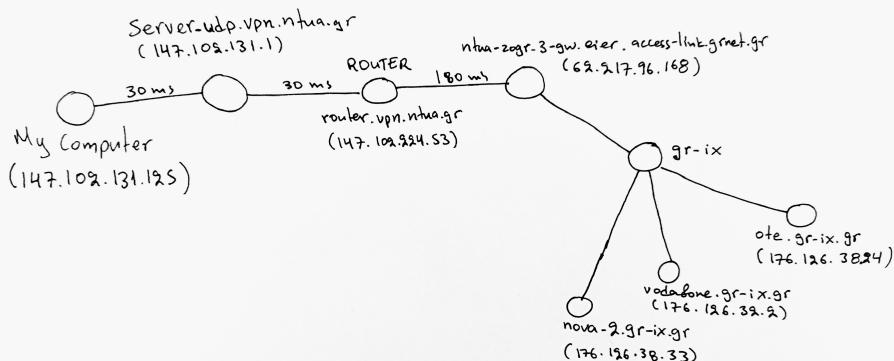
---



---

2.4 tracert -4 -h 4 <address>

2.5



2.6 Ναι, συμφωνεί

---



---

2.7 Subnet IPv4 Address : 176.126.38.0/24

2.8 tracert -4 -d grnet.gr-ix.gr

2.9 Display filter : udp or icmp

2.10 Protocol : 01 (HEX) → ICMP

2.11 Μεταφέρει 64 bytes

2.12 Αποστέλνονται 3 τριαδες και λαμβάνονται επίσης 3

2.13 1. Request Destination IPv4 address : 176.126.38.1, Reply Source IPv4 address : 147.102.131.1

2. Request Destination IPv4 address : 176.126.38.1, Reply Source IPv4 address : 147.102.224.53

3. Request Destination IPv4 address : 176.126.38.1, Reply Source IPv4 address : 147.102.131.1

---



---

2.14 Ναι, όλες ταυτίζονται

2.15 1. TTL = 64

2. TTL = 254

3. TTL = 62

2.16 1. TTL = 64

2. TTL = 254

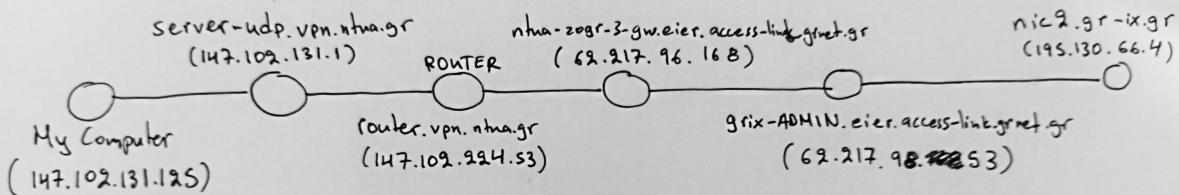
3. TTL = 62

- 2.17 Γιατί το πεδίο TTL έχει μικρότερη τιμή από αυτή που απαιτείται για να φτάσει το αντίστοιχο μήνυμα από τη πηγή στο προορισμό και στον αντίστοιχο κόμβο μηδενίζεται η τιμή του.
- 2.18 ICMP Type : 0 (Echo ping reply).

### 3

- 3.1 tracert nic.gr-ix.gr
- 3.2 Capture filter : icmp

3.3



3.4 Πεδία που αλλάζουν : 'Identification', 'Time to Live', 'Header Checksum'

3.5 Αμετάβλημα πεδία : 'Version', 'Header Length', 'Differentiated Services', 'Total Length', 'Flags', 'Protocol', 'Source Address', 'Destination Address'

3.6 Τα πεδία 'Version', 'Header Length', 'Differentiated Services', 'Total Length', 'Flags', 'Protocol' γιατί πρόκειται για τον ίδιο ακριβώς τυπο μηνύματος. Ακόμα, τα πεδία 'Source Address', 'Destination Address' γιατί σε όλα τα πακέτα ο υπολογιστής μας προσπαθεί να φτάσει τον ίδιο παραλήπτη.

3.7 Τα πεδία 'Time to Live', 'Header Checksum' αλλάζουν γιατί το tracert αυξανει σταδιακά το TTL των πακέτων καθώς και το 'Identification' γιατί κάθε πακέτο είναι αυτοτελές και διαφορετικό από τα υπόλοιπα.

3.8 TTL : 64

3.9 Ναι, παραμένουν για όλα τα πακέτα, γιατί πρόκειται για την ίδια τριάδα πακέτων τα οποία στέλνονται από τον ίδιο διαμεσολαβητή στο δίκτυο.

3.10 2η σειρά → TTL : 254, 3η σειρά → TTL : 253, 4η σειρά → TTL : 252. Παρατηρούμε ότι η τιμές αυτές είναι μεγαλύτερες από αυτή της 1ης σειράς.

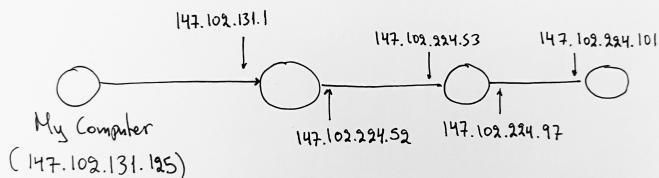
3.11 TTL : 60

3.12 Ο υπολογιστής μας από τη διεπαφή του nic.gr-ix.gr απέχει 5 κόμβους (δηλαδή υπάρχουν 4 ενδοιάμεσοι). Οπότε αν σε κάθε κόμβο η τιμή του TTL μειώνεται κάτα 1 τότε η αρχική του τιμή ήταν TTL = 64

**4**

- 4.1 ping -n 1 -4 -r 9 www.ntua.gr.....
- 4.2 Header Length : 60 bytes.....
- 4.3 Header Length : 60 bytes.....
- 4.4 Πρώτα 20 bytes → τα κύρια πεδία του IPv4. Τα υπόλοιπα 40 bytes → τα options (πχ. διαδρομή)

4.5



- 4.6 IPv4 Address : 194.177.210.210. Βρίσκεται 5 βήματα μακριά από τον υπολογιστή μου.
- 4.7 147.102.131.125 → 147.102.131.1 → 147.102.224.53 → 62.217.96.168 → 62.217.100.62  
→ 194.177.210.210
- 4.8 Απέρχομενες επαφές (IPv4) : 147.102.224.52, 62.217.96.169, 62.217.100.63, 194.177.210.193,  
194.177.210.210

4.9

