Εργαστηριακή Άσκηση 4
Εξερεύνηση του Διαδικτύου

Σκοπός αυτού του εργαστηρίου είναι η εξοικείωση με τις εντολές `ping`, `tracert` και `pathping`, οι οποίες αποτελούν χρήσιμα εργαλεία για τη μέτρηση και τον έλεγχο ενός δικτύου. Η άσκηση αυτή 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. Επίσης θα εξεταστεί η σχέση μεταξύ χρόνου διάδοσης των πακέτων, αριθμού κόμβων και πολυπλοκότητας της δομής των δικτύων. Το εργαστήριο αυτό θα γίνει σε περιβάλλον Microsoft Windows XP, αλλά παρόμοιες εντολές ισχύουν και σε πλατφόρμα Unix. Για περισσότερες πληροφορίες σχετικά με τη σύνταξη των εντολών πηγαίνετε στο Start → Help and Support, μετά στο πεδίο Search πληκτρολογήστε την εντολή που θέλετε ή γράψτε TCP/IP utilities, οπότε εμφανίζονται όλες οι σχετικές εντολές.

Η εντολή `ping` ελέγχει βασικά εάν κάποιος κόμβος (ή ακριβέστερα η διεπαφή (interface) του κόμβου) ενός δικτύου IP είναι ενεργός (*alive* ή *up*). Το `ping` χρησιμοποιεί το πρωτόκολλο ICMP (Internet Control Message Protocol) για να στείλει ένα μήνυμα *Αίτησης Ηχούς* (*Echo Request)*, έτσι ώστε να λάβει μια *Απάντηση Ηχούς* (*Echo Reply)* από τον συγκεκριμένο κόμβο. Για τη μεταφορά του πάνω από το δίκτυο, το μήνυμα ICMP ενθυλακώνεται μέσα στο πακέτο IP. Η συνολική χρονική διάρκεια ταξιδιού RTT (Round-Trip Time) των μηνυμάτων *Echo Request* και *Echo Reply* μέσα στο δίκτυο δίνει μια ένδειξη για τη φόρτιση του δικτύου. Ειδικά στα Windows, το `ping` στέλνει τέσσερα διαδοχικά πακέτα *Αίτησης Ηχούς* (*Echo Request)*, γι' αυτό βλέπετε τέσσερα αποτελέσματα.

Τα αποτελέσματα του ping δεν μπορεί να θεωρηθούν σε καμία περίπτωση πλήρως αξιόπιστα, όσον αφορά τη σωστή επικοινωνία και δρομολόγηση πακέτων. Για παράδειγμα, αν με τη βοήθεια της εντολής αυτής, βρεθεί ένας κόμβος ανενεργός, δεν εξυπακούεται ότι πράγματι είναι. Πιο συγκεκριμένα, αν δε ληφθεί *Echo Reply* από τον κόμβο προορισμού, υπάρχει πιθανότητα ο ίδιος ο κόμβος ή κάποιο τείχος προστασίας (firewall), που παρεμβάλλεται στη διαδρομή, να μπλοκάρει τα μηνύματα του πρωτοκόλλου ICMP και να μας οδηγεί εσφαλμένα στο συμπέρασμα ότι ο κόμβος είναι μη ενεργός (down ή unreachable). Επίσης είναι δυνατό ο κόμβος προορισμού ή κάποια ενδιάμεση συσκευή να μην είναι επαρκώς πληροφορημένη για το δίκτυο του αποστολέα και έτσι να μην είναι δυνατή η σωστή επιστροφή της απάντησης.

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 χρήστες 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 με την εντολή `tracert`. Η `tracert` στέλνει μηνύματα ICMP τύπου *Echo Request* με μεταβαλλόμενες τιμές του πεδίου Time-To-Live (TTL), του πακέτου IP, προς τον προορισμό. Αρχίζει στέλνοντας ένα ή περισσότερα μηνύματα ICMP τύπου *Echo Request* προς τον προορισμό με την τιμή του πεδίου Time-To-Live (TTL) του πακέτου IP ίση με 1. Μετά, στέλνει μια παρόμοια σειρά μηνυμάτων στον ίδιο προορισμό με την τιμή του πεδίου TTL του πακέτου IP ίση με 2. Κατόπιν, επαναλαμβάνει την αποστολή των μηνυμάτων στον προορισμό με την τιμή του πεδίου TTL του πακέτου IP ίση με 3, κοκ. Κάθε δρομολογητής κατά μήκος της διαδρομής προς τον προορισμό μειώνει το TTL κατά 1, προτού προω-

θήσει το πακέτο[1]. Όταν το TTL μηδενισθεί, ο δρομολογητής οφείλει να στείλει μήνυμα ICMP τύπου *Time Exceeded* στην πηγή. Ως αποτέλεσμα αυτής της διαδικασίας, η αποστολή ενός πακέτου IP με τιμή TTL ίση με 1 (από τον υπολογιστή σας) θα προκαλέσει την αποστολή ενός μηνύματος ICMP τύπου *Time Exceeded* προς τον υπολογιστή σας από τον δρομολογητή που βρίσκεται ένα βήμα πιο πέρα. Η αποστολή ενός πακέτου IP με τιμή TTL ίση με 2 θα προκαλέσει την αποστολή ενός μηνύματος ICMP τύπου *Time Exceeded* προς τον υπολογιστή σας από τον δρομολογητή που βρίσκεται δύο βήματα πιο πέρα. Παρόμοια, η αποστολή ενός πακέτου IP με τιμή TTL ίση με 3 θα προκαλέσει την αποστολή ενός μηνύματος ICMP τύπου *Time Exceeded* προς τον υπολογιστή σας από τον δρομολογητή που βρίσκεται τρία βήματα πιο πέρα., κοκ. Ο υπολογιστής σας, εκτελώντας την `tracert`, μπορεί να μάθει τις διευθύνσεις των δρομολογητών μεταξύ αυτού και του εκάστοτε προορισμού. Η διαδρομή βρίσκεται εξετάζοντας τα μηνύματα *Time Exceeded* που προκαλούνται από διαδοχικά μηνύματα ηχούς με συνεχώς αυξανόμενες τιμές του TTL και καταγράφοντας την εκάστοτε διεύθυνση IP της πηγής που παράγει το μήνυμα ICMP τύπου *Time Exceeded.*

Αξίζει να τονιστεί ότι η παράμετρος TTL, άσχετα με ό,τι υποδηλώνει το όνομα της, δεν έχει σχέση με χρονική διάρκεια. Εκφράζει απλά το μέγιστο αριθμό κόμβων από τους οποίους μπορεί να περάσει ένα πακέτο IP μέχρι τον προορισμό του ή τον αριθμό βημάτων (hops) που μπορεί να διανύσει ένα πακέτο IP, άσχετα από τη χρονική διάρκεια του ταξιδιού αυτού. Αντίθετα, η RTT αναφέρεται στο χρόνο. Η `tracert` στέλνει τρία μηνύματα σε κάθε βήμα, γι' αυτό στα δεδομένα κάθε βήματος φαίνονται τρία αποτελέσματα. Επίσης, η `tracert` χρησιμοποιεί το DNS για να αντιστοιχίσει ονόματα στις διευθύνσεις IP των κόμβων της διαδρομής. Η συμπεριφορά αυτή αναιρείται, όταν η εντολή καλείται με την παράμετρο `-d`. Σε περίπτωση που η `tracert` δεν εμφανίζει ονόματα σε ορισμένα ενδιάμεσα βήματα, σημαίνει απλά ότι οι αντίστοιχες διευθύνσεις IP δεν έχουν καταχωρηθεί σε περιοχή του DNS.

Τέλος, η εντολή `pathping` των Windows είναι ένας συνδυασμός των `ping` και `tracert`. Για να χρησιμοποιήσετε τα παραπάνω εργαλεία, ανοίξτε ένα παράθυρο εντολών και πληκτρολογείστε το όνομα της εντολής ακολουθούμενο από τη διεύθυνση ή το όνομα του προορισμού.

ΠΡΟΣΟΧΗ: Οι προηγούμενες εντολές είναι ισχυρά διαγνωστικά εργαλεία που προορίζονται για περιστασιακή χρήση, όταν ανακύπτουν προβλήματα στο δίκτυο. Πρέπει να χρησιμοποιούνται με σύνεση διότι δημιουργούν μεγάλο φορτίο που πιθανώς να εκληφθεί ως επίθεση από τον προορισμό (Denial of Service – DoS attack). **Για τις ανάγκες τις άσκησης να μην χρησιμοποιηθούν πάνω από μία φορά ανά προορισμό εκτός του τοπικού δικτύου!** Μην ξεχνάτε ότι τα αποτελέσματα παραμένουν στην οθόνη εντολών. Μετακινήστε τη δεξιά μπάρα για να δείτε τα μη ορατά μέρη.

1 – Μετρείστε την καθυστέρηση

Εάν κάνετε `ping` στον εξυπηρετητή ιστού του MIT, θα λάβετε μια απάντηση σαν την επόμενη

```
C:\>ping www.mit.edu

Pinging www.mit.edu [18.7.22.83] with 32 bytes of data:

Reply from 18.7.22.83: bytes=32 time=136ms TTL=242
Reply from 18.7.22.83: bytes=32 time=136ms TTL=242
Reply from 18.7.22.83: bytes=32 time=136ms TTL=242
Reply from 18.7.22.83: bytes=32 time=136ms TTL=242

Ping statistics for 18.7.22.83:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 136ms, Maximum = 136ms, Average = 136ms

C:\>
```

[1] Στην πραγματικότητα το σχετικό πρότυπο RFC 791 λέει ότι ο δρομολογητής πρέπει να μειώσει την τιμή του TTL *τουλάχιστον* κατά ένα.

που σημαίνει ότι στάλθηκαν 4 πακέτα μήκους 32 bytes στη διεύθυνση IP 18.7.22.83 του εξυπηρετητή ιστού www.mit.edu, απαντήθηκαν όλα (0% απώλειες) και μετρήθηκε μέση καθυστέρηση 136 ms.

Στη συνέχεια θα καταγραφούν, με τη βοήθεια του Wireshark, τα πακέτα που ανταλλάσσονται όταν εκτελείται η εντολή `ping`. Αφού ξεκινήσετε το Wireshark, προκειμένου να αρχίσει η διαδικασία της καταγραφής, ακολουθήσετε από το μενού επιλογών τη διαδρομή *Capture* → *Options*…. Στο παράθυρο που εμφανίζεται βεβαιωθείτε ότι στο πεδίο *Interface* αναφέρεται το όνομα της κάρτας δικτύου του υπολογιστή σας και ότι καμιά από τις επιλογές της κατηγορίας *Name Resolution* δεν είναι ενεργοποιημένη. Θα χρησιμοποιήσετε φίλτρο σύλληψης προκειμένου να περιορισθεί το πλήθος των πλαισίων που καταγράφονται. Στο σχετικό με το φίλτρο σύλληψης πεδίο γράψτε `not multicast and not broadcast`. Πατώντας το κουμπί *Start* αρχίζει η καταγραφή!

Επαναλάβετε την παραπάνω μέτρηση μέσω της εντολής `ping www.mit.edu` και σταματήστε την καταγραφή μόλις ολοκληρωθεί η εκτέλεση της εντολής πιέζοντας τον συνδυασμό πλήκτρων `<Ctrl>+E`.

1.1 Ποια η σημασία του φίλτρου σύλληψης που εφαρμόσατε; *[Υπόδειξη: Ανατρέξτε στην ιστοσελιδα παραδειγμάτων για φίλτρα σύλληψης http://wiki.wireshark.org/CaptureFilters].*

1.2 Με βάση τα αποτελέσματα από την εκτέλεση της εντολής στο παράθυρο εντολών να καταγράψετε το ποσοστό απωλειών πακέτων, την ελάχιστη, μέση και μέγιστη καθυστέρηση.

1.3 Ποιο φίλτρο απεικόνισης (Display Filter) πρέπει να εφαρμόσετε προκειμένου να παρατηρείτε μόνο την κίνηση ICMP που προκάλεσε η εντολή `ping`; *[Υπόδειξη: Μόλις εφαρμόσετε το ζητούμενο φίλτρο, να καταγραφεί το περιεχόμενο του (πράσινου) πεδίου με την επιγραφή Filter στο κεντρικό παράθυρο του Wireshark.]*

Παρατηρώντας την καταγεγραμμένη κίνηση στο Wireshark να απαντήσετε στα παρακάτω ερωτήματα:

1.4 Να καταγράψετε το πλήθος και το είδος των μηνυμάτων ICMP που στάλθηκαν από τον υπολογιστή σας κατά την εκτέλεση της εντολής `ping`.

1.5 Να καταγράψετε τις διευθύνσεις IP προέλευσης και προορισμού των παραπάνω μηνυμάτων.

1.6 Να καταγράψετε το πλήθος και το είδος των μηνυμάτων ICMP που ελήφθησαν από τον υπολογιστή σας κατά την εκτέλεση της εντολής `ping`.

1.7 Να καταγράψετε τις διευθύνσεις IP προέλευσης και προορισμού των παραπάνω μηνυμάτων.

2 – Αναζητείται το CNN

Ανοίξτε τον πλοηγό ιστού και επισκεφτείτε την κεντρική ιστοσελίδα του CNN (www.cnn.com). Μόλις η σελίδα έχει φορτωθεί πλήρως, χρησιμοποιήστε την εντολή `ping` με προορισμό πάλι τον εξυπηρετητή ιστού του CNN.

2.1 Τι παράδοξο παρατηρείτε και τι μπορείτε να υποθέσετε για να το εξηγήσετε;

3 – Ανακαλύψτε την τοπολογία

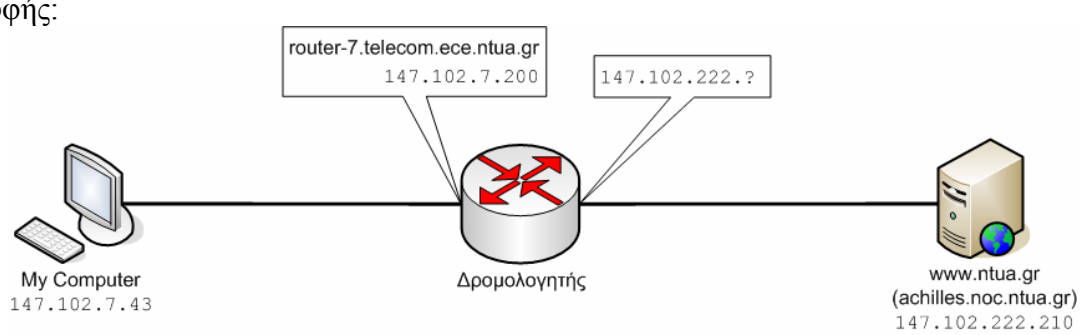
Εάν κάνετε `tracert` στον εξυπηρετητή ιστού του ΕΜΠ, θα λάβετε μια απάντηση σαν την επόμενη

```
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    <1 ms    <1 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]
```

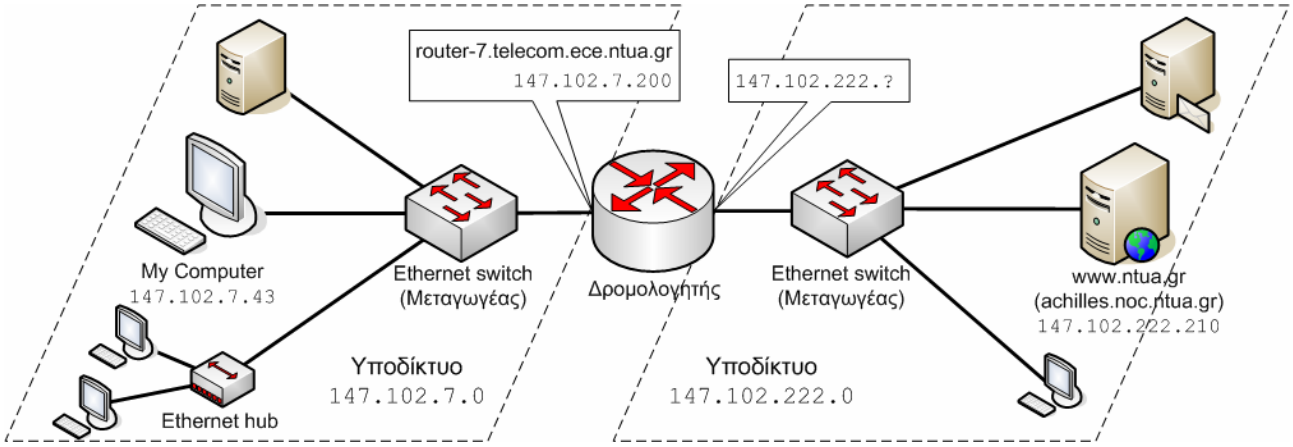
```
Trace complete.

C:\>
```

που σημαίνει ότι το επίσημο όνομα (CNAME) του εξυπηρετητή ιστού είναι achilles.noc.ntua.gr, η IP διεύθυνσή του 147.102.222.210 και η διαδρομή μέχρι αυτόν διέρχεται από ένα δρομολογητή. Η `tracert` στέλνει τρία *Echo Request* σε κάθε βήμα προς τον προορισμό και εμφανίζει τις αντίστοιχες τιμές RTT ανά βήμα. Εάν για κάποιο *Echo Request* δεν ληφθεί απάντηση μέσα σε συγκεκριμένο χρονικό διάστημα, συνήθως 4 s, αποστέλλεται το επόμενο *Echo Request*. Εάν δεν ληφθεί καμία απάντηση, εμφανίζεται μήνυμα εκπνοής χρόνου και η `tracert` συνεχίζει, αυξάνοντας το TTL μέχρι να φθάσει το μέγιστο επιτρεπτό πλήθος βημάτων, συνήθως 30. Εάν παρατηρηθεί μία μόνο εκπνοή χρόνου, το πιθανότερο είναι ότι η διαδρομή (μέχρι το σημείο 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 `tracert`, απλά διακόψτε πιέζοντας τον συνδυασμό πλήκτρων `<Ctrl>+c`.

Από τα παραπάνω αποτελέσματα της `tracert` μπορείτε να υποθέσετε μια τοπολογία της ακόλουθης μορφής:



Ωστόσο, πιο κοντά στην πραγματική τοπολογία του δικτύου είναι το παρακάτω διάγραμμα, όπου φαίνονται, επιπλέον, πιθανοί τρόποι σύνδεσης του σταθμού εργασίας και του εξυπηρετητή ιστού στα επιμέρους τοπικά δίκτυα που ορίζει ο δρομολογητής:



Χρησιμοποιώντας διαδοχικά την εντολή `tracert` προς διαφορετικούς προορισμούς μπορείτε να συμπεράνετε την πιθανή τοπολογία ενός δικτύου. Αρκεί να καταγράψετε σε μορφή σχεδιαγράμματος τη διαδοχή των διεπαφών όπως εμφανίζονται από την εκτέλεση της εντολής `tracert`.

3.1 Να σχεδιάσετε μια άποψη της τοπολογίας του δικτύου δεδομένων του Πολυτεχνείου όπως φαίνεται από το εργαστήριο προσωπικών υπολογιστών. Χρησιμοποιείστε διαδοχικά την εντολή `tracert`[2] με προορισμούς τους εξυπηρετητές ιστού των Σχολών Ηλεκτρολόγων, Αρχιτεκτόνων και Μηχανολόγων Μηχανικών (www.ece.ntua.gr, www.arch.ntua.gr και

[2] Υπενθυμίζουμε ότι εάν παρατηρηθούν διαδοχικές εκπνοές χρόνου, τότε το πιθανότερο είναι ότι παρεμβάλλεται κάποιο τείχος προστασίας, οπότε διακόψτε την εντολή `tracert` πιέζοντας τον συνδυασμό πλήκτρων `<Ctrl>+c`.

www.mech.ntua.gr, αντίστοιχα). Το σχεδιάγραμμα να περιλαμβάνει το σταθμό εργασίας σας, τους δρομολογητές και τους εξυπηρετητές ιστού, καταγράφοντας παράλληλα τα ονόματα DNS (αν υπάρχουν), τις διευθύνσεις IP τους, καθώς και την καθυστέρηση.

Στη σελίδα http://www.noc.ntua.gr/modules/ContentExpress/img_repository/topology_zografou.jpg το Κέντρο Δικτύων του Ε.Μ.Π. έχει δημοσιεύσει την τοπολογία του δικτύου δεδομένων του Ε.Μ.Π.

3.2 Το σχεδιάγραμμά σας συμφωνεί με το προηγούμενο σχήμα;

Ο κόμβος Athens Internet Exchange (http://www.aix.gr/) προσφέρει τοπική διασύνδεση (peering) μεταξύ των εμπορικών δικτύων των εταιρειών παροχής υπηρεσιών Internet (ISP) στη χώρα μας μέσω ενός μεταγωγέα (switch) Ethernet που στεγάζεται σε χώρο του κτιρίου ΟΤΕ στην οδό Κωλέττη. Με τη βοήθεια της εντολής `tracert` στη γραμμή εντολών, παρατηρήστε τις διαδρομές μέχρι τους εξυπηρετητές ιστού των γνωστών ISPs: OTEnet, FORTHnet και Vivodi (www.otenet.gr, www.forthnet.gr και www.vivodi.gr αντίστοιχα). Σε περίπτωση εκπνοής χρόνου μπορείτε να διακόψετε την εκτέλεση και να προχωρήσετε στον επόμενο ISP.

3.3 Βάσει των αποτελεσμάτων της εντολής tracert για τους παραπάνω προορισμούς, σχεδιάστε την τοπολογία του δικτύου από τον υπολογιστή σας μέχρι την κεντρική διεπαφή (interface) που είναι κοινή και στις τρεις διαδρομές.

3.4 Ποια είναι η διεύθυνση IP της κοινής διεπεφής που προσδιορίσατε στο ερώτημα 3.3 και ποια είναι η διεύθυνση του υποδικτύου IP του AIX;

4 – Μετρείστε τις απώλειες

Η `pathping` μετρά καθυστερήσεις και απώλειες με μεγαλύτερη ακρίβεια από ότι η `ping`. Το ακόλουθο παράδειγμα είναι από το Help and Support των Windows XP.

```
D:\>pathping -n corp1

Tracing route to corp1 [10.54.1.196]
over a maximum of 30 hops:
  0  172.16.87.35
  1  172.16.87.218
  2  192.168.52.1
  3  192.168.80.1
  4  10.54.247.14
  5  10.54.1.196

Computing statistics for 125 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           172.16.87.35
                                 0/ 100 =  0%   |
  1   41ms     0/ 100 =  0%     0/ 100 =  0%  172.16.87.218
                               13/ 100 = 13%   |
  2   22ms    16/ 100 = 16%     3/ 100 =  3%  192.168.52.1
                                 0/ 100 =  0%   |
  3   24ms    13/ 100 = 13%     0/ 100 =  0%  192.168.80.1
                                 0/ 100 =  0%   |
  4   21ms    14/ 100 = 14%     1/ 100 =  1%  10.54.247.14
                                 0/ 100 =  0%   |
  5   24ms    13/ 100 = 13%     0/ 100 =  0%  10.54.1.196

Trace complete.
D:\>
```

Πρώτα εμφανίζεται η διαδρομή όπως και στην εντολή `tracert`. Μετά εμφανίζεται ένα μήνυμα για προσεγγιστικό χρόνο αναμονής (125 s στο παράδειγμα) που εξαρτάται από το πλήθος βημάτων μέχρι τον προορισμό. Σ' αυτό το διάστημα συγκεντρώνονται στατιστικά στοιχεία από όλους τους δρομολογητές και τις μεταξύ τους ζεύξεις. Στο τέλος της περιόδου αναμονής, εμφανίζονται τα αποτελέσματα. Στο παράδειγμα, η ζεύξη μεταξύ 172.16.87.218 και 192.168.52.1 παρουσιάζει απώλειες

13% (το σύμβολο | δίπλα στο ποσοστό απωλειών υποδεικνύει τη ζεύξη). Οι δρομολογητές στα βήματα 2 και 4 (προσδιορίζονται από τη διεύθυνση IP τους) επίσης χάνουν πακέτα (3% και 1%, αντίστοιχα), αλλά αυτό δεν επηρεάζει την ικανότητά τους να προωθούν κίνηση που δεν προορίζεται για αυτούς.

Στη συνέχεια θα ελέγξετε τυχόν απώλειες κατά μήκος της διαδρομής (Αθήνα, Λάρισα, Θεσσαλονίκη, Ξάνθη) προς τον εξυπηρετητή ιστού του Δημοκριτείου Πανεπιστημίου Θράκης. Για το σκοπό αυτό θα εκτελέσετε **μία μόνο** φορά την εντολή `pathping -4 –q 30 www.duth.gr` **(προσοχή: η μέτρηση με pathping απαιτεί συνήθως αρκετά δευτερόλεπτα)**.

4.1 Ποια είναι η σημασία των παραμέτρων `-4` και `-q` που χρησιμοποιήσατε κατά την κλήση της `pathping`; *[Υπόδειξη: `pathping /?`]*
4.2 Με βάση τα αποτελέσματα της `pathping`, να καταγράψετε τις καθυστερήσεις στις ζεύξεις με την ακόλουθη μορφή: <αριθμός βήματος> <καθυστέρηση>.
4.3 Δώστε μια εξήγηση για τις τιμές που καταγράψατε με βάση το φορτίο και τη χωρητικότητα των γραμμών και των δρομολογητών όπως εμφανίζεται στα στατιστικά κίνησης του δικτύου ΕΔΕΤ στη διεύθυνση http://netmon.grnet.gr/map.shtml. *[Υπόδειξη: Τοποθετήστε τον δρομέα σε κατάλληλα σημεία του χάρτη για να δείτε τις σχετικές πληροφορίες.]*

5 – Περισσότερα για το Ping

Σε αυτή την άσκηση θα καταγραφούν, με τη βοήθεια του Wireshark, τα πακέτα που ανταλλάσσονται όταν εκτελείται η εντολή `ping`. Ξεκινήσετε μια καταγραφή με το Wireshark χρησιμοποιώντας το φίλτρο σύλληψης και το φίλτρο απεικόνισης της ερώτησης 1. Στη συνέχεια, από τη γραμμή εντολών, εκτελέστε διαδοχικά την εντολή `ping` ως εξής:

i. `ping <IP>`, όπου `<IP>` η διεύθυνση ενός γειτονικού υπολογιστή σας
ii. `ping <My IP>`, όπου `<My IP>` η διεύθυνση IP του υπολογιστή σας
iii. `ping 127.0.0.1`

Μόλις ολοκληρωθεί η εκτέλεση της εντολής σταματήστε την καταγραφή. **Προσοχή: Συνεννοηθείτε με τους διπλανούς σας ώστε να μην κάνετε ταυτόχρονα ping ο ένας στον άλλον κατά τη διάρκεια της καταγραφής!** Με βάση τα αποτελέσματα στο παράθυρο της γραμμής εντολών:

5.1. Να καταγραφεί το πλήθος των πακέτων που στάλθηκαν στον γειτονικό σας υπολογιστή.
5.2. Να καταγραφεί το πλήθος των πακέτων που στάλθηκαν στη διεύθυνση IP του υπολογιστή σας (δηλαδή, στον οδηγό της κάρτας δικτύου του υπολογιστή σας).
5.3. Να καταγραφεί το πλήθος των πακέτων που στάλθηκαν στη διεύθυνση του βρόχου επιστροφής (loopback) `127.0.0.1`.

Παρατηρώντας την καταγεγραμμένη κίνηση στο Wireshark να απαντήσετε στα παρακάτω ερωτήματα:

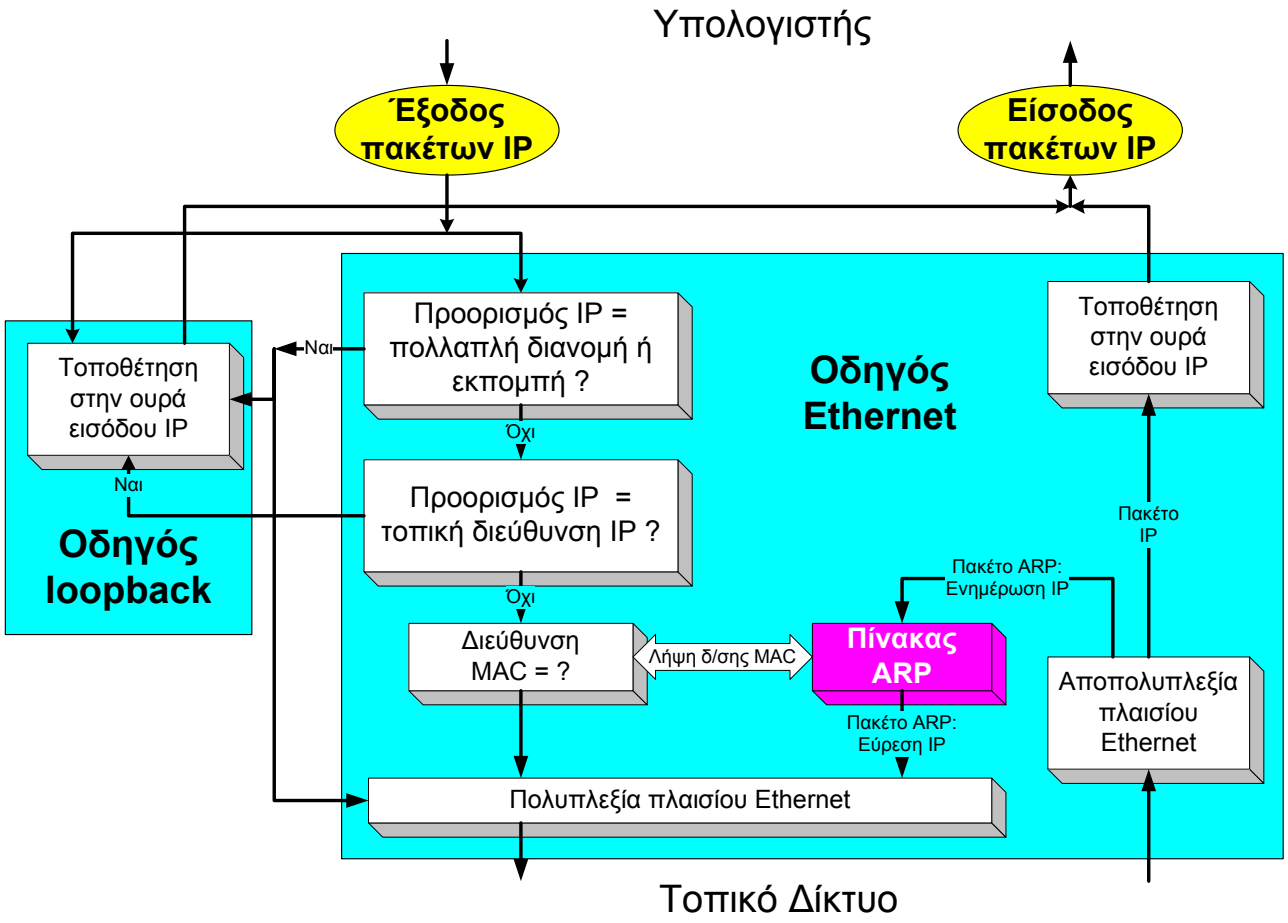
5.4. Πόσα μηνύματα *Echo request* που έχουν αποσταλεί από τον υπολογιστή σας έχει καταγράψει το Wireshark;
5.5. Ποιος είναι ο προορισμός τους;
5.6. Παρατηρήσατε αποστολή μηνυμάτων *Echo request* στο δίκτυο με πηγή και προορισμό την διεύθυνση IP του υπολογιστή σας;
5.7. Παρατηρήσατε αποστολή μηνυμάτων *Echo request* στο δίκτυο που να φέρουν τη διεύθυνση του βρόχου επιστροφής;
5.8. Ποια η διαφορά όταν κάνετε `ping` στη διεπαφή του υπολογιστή (δηλαδή, στην τοπική διεύθυνση IP) σε σχέση με `ping` στη διεύθυνση loopback αυτού (`127.0.0.l`); *[Υπόδειξη: Η απάντηση σχετίζεται με το ρόλο του βρόχου επιστροφής σε ένα δικτυωμένο σταθμό εργασίας. Συμβουλευθείτε το επόμενο σχήμα.]*

Στη συνέχεια, με τη βοήθεια του Wireshark και τα ίδια φίλτρα σύλληψης και απεικόνισης, να καταγραφεί η κίνηση κατά την εκτέλεση τις εντολής `ping -n 3 www.uoi.gr`

5.9. Ποια η διαφορά στον τρόπο κλήσης του `ping` στην παραπάνω περίπτωση; *[Υπόδειξη: `ping /?`]*

5.10. Να καταγραφούν οι τιμές του RTT, όπως εμφανίζονται στη γραμμή εντολών.

5.11. Να καταγραφούν οι τιμές του RTT για κάθε ζεύγος *Echo Request – Reply*, με τη βοήθεια του Wireshark. *[Υπόδειξη: Στο παράθυρο παρατήρησης των πακέτων στο Wireshark υπάρχει η δυνατότητα να τεθεί ένα πακέτο ως σημείο χρονικής αναφοράς για αυτά που έπονται κάνοντας δεξί κλικ στο συγκεκριμένο πακέτο και επιλέγοντας Set Time Reference (toggle).]*



6 – Dr. Ping

Είναι η πρώτη σας μέρα στην καινούργια σας δουλειά και διαπιστώνετε ότι ο σταθμός εργασίας που σας αναθέτουν έχει πρόβλημα με τη διασύνδεση του στο Internet, καθώς δε μπορείτε να επισκεφτείτε καμία ιστοσελίδα. Το εικονίδιο δείχνει ότι η κάρτα δικτύωσης είναι συνδεδεμένη στο Τοπικό Δίκτυο και επομένως αποκλείεται να υπάρχει πρόβλημα καλωδίωσης.

6.1 Με ποιους προορισμούς θα μπορούσατε να χρησιμοποιήσετε διαδοχικά το `ping` για να διαπιστώσετε την αιτία του προβλήματος; Να αναφέρετε τρεις έως πέντε προορισμούς που θα δοκιμάζατε αιτιολογώντας κάθε επιλογή σας. *[Υπόδειξη: Συμβουλευτείτε τα θέματα του Help and Support των Windows που εμφανίζονται γράφοντας `ping test tcp/ip configuration` στο πεδίο Search.]*

Όνοματεπώνυμο:	**Αρ. PC:**
Ομάδα:	**Ημερομηνία:**
Διεύθυνση IP: . . .	**Διεύθυνση MAC: - - - - -**

Εργαστηριακή Άσκηση 4
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 .....

.....

1.2 .....

.....

1.3 .....

.....

1.4 .....

1.5 .....

1.6 .....

1.7 .....

2

2.1 .....

.....

3

3.1 (Σχεδιάστε το σχήμα στο διαθέσιμο χώρο της επόμενης σελίδας).....

3.2 .....

3.3 (Σχεδιάστε το σχήμα στο διαθέσιμο χώρο της τελευταίας σελίδας).....

3.4 .....

4

4.1 .....

.....

4.2 .....

.....

4.3 .....

.....

.....

5

5.1 .....
5.2 .....
5.3 .....
5.4 .....
5.5 .....
5.6 .....
5.7 .....
5.8 .....
5.9 .....
5.10 .....
5.11 .....
.....

Σχήμα ερώτησης 3.1

6

6.1 .....

.....

.....

.....

.....

Σχήμα ερώτησης 3.3