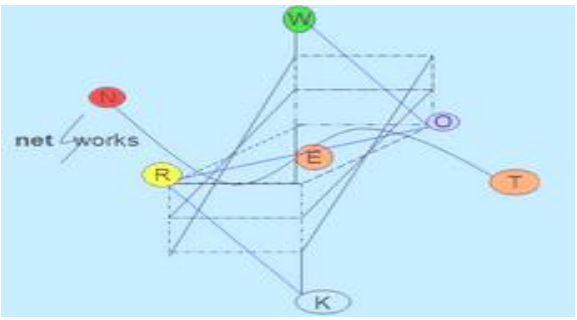

HY335: Δίκτυα Υπολογιστών
Χειμερινό Εξάμηνο 2014-2015
Τμήμα Επιστήμης Υπολογιστών
Πανεπιστήμιο Κρήτης
Διδάσκουσα: Μαρία Παπαδοπούλη

1η σειρά ασκήσεων – Ημερομηνία Παράδοσης 15/11/2014

Σημείωση: Η άσκηση είναι ομαδική, και μπορεί να γίνει από ομάδες 2 ή 3 ατόμων. Δεν θα δοθεί παράταση. Ο βαθμός της άσκησης 4 ή μεγαλύτερος για να περάσει κάποιος το μάθημα.

Απαντήστε σύντομα και περιεκτικά (3-4 προτάσεις) τις παρακάτω ερωτήσεις.

1. Εκτελέστε την εντολή traceroute με destination έναν host της επιλογής σας (π.χ. www.grnet.gr). Source host είναι ο υπολογιστής που τρέχει την εντολή, η οποία να επιστρέφει απαντήσεις(να μην εμπεριέχει "*****" η τελευταία γραμμή της απάντησης).
   - Ποιο είναι ο αριθμός των κόμβων που παρατηρείτε;
   - Πόσα hops γίνονται μέσα στο υποδίκτυο σας; Πως το αναγνωρίσατε;
   - Ποια είναι η συνολική καθυστέρηση ;
2. Όταν εκτελέσουμε την εντολή traceroute, μπορεί ορισμένες φορές να δούμε κάποιους κόμβους που δεν έχουν όνομα και IP αλλά μόνο αστερίσκους. Όπως για παράδειγμα:

```
traceroute to www.grnet.gr (195.251.28.66), 30 hops max, 40 byte packets using UDP
 1  192.168.1.254 (192.168.1.254)  81.041 ms   78.832 ms   77.634 ms
 2  r.edudsl.gr (83.212.27.202)  14.075 ms   14.484 ms   14.852 ms
 3  grnetRouter.edudsl.eie-2.access-link.grnet.gr (194.177.209.193)  13.781 ms   13.723 ms   13.668 ms
 4  koll-to-eie2.backbone.grnet.gr (195.251.27.53)  13.517 ms   13.579 ms   13.701 ms
 5  clientRouter.grnetadm.koletti-1.access-link.grnet.gr (194.177.209.2)  14.872 ms   14.327 ms   40.295 ms
 6  * * *
 7  clientRouter.grnetadm.koletti-1.access-link.grnet.gr (194.177.209.2)(N!)  32.338 ms * *
```

Βρείτε πότε και γιατί γίνεται αυτό, αναφέροντας και τις πηγές σας.

3. Το μονοπάτι που μας δίνει το traceroute είναι πάντα το ίδιο για τον ίδιο προορισμό. Σωστό, λάθος και γιατί;

4. Το μονοπάτι που μας κάνει report το traceroute είναι το μονοπάτι που ακολούθησε το τελευταίο πακέτο που στάλθηκε. Σωστό, λάθος και γιατί;

5. Το μονοπάτι που μας κάνει report το traceroute είναι το ακριβές μονοπάτι που ακολουθούν όλα τα πακέτα που στέλνει το traceroute. Σωστό ή λάθος; Δώστε ένα σχηματικό παράδειγμα με διάφορους ενδιάμεσους κόμβους και τις τιμές του TTL για κάθε πακέτο.

6. Εκτελέστε την εντολή ping με destination έναν host της επιλογής σας (π.χ. www.grnet.gr). Source host είναι ο υπολογιστής που τρέχει την εντολή, η οποία να επιστρέφει απαντήσεις (να μην εμπεριέχει "*****" η τελευταία γραμμή της απάντησης). Χρησιμοποιήστε τα κατάλληλα options ώστε η εντολή να στείλει 100 echo requests.

    - Να υπολογίσετε το bit rate.
    - Να υπολογίσετε το μέσο round trip time (RTT).
    - Να υπολογίσετε την τυπική απόκλιση του round trip time(RTT).
    - Να υπολογίσετε την αθροιστική συνάρτηση πυκνότητας πιθανότητας (cumulative distribution function, CDF) του round trip time(RTT). Μπορείτε να χρησιμοποιήσετε την εντολή cdfplot[1] στο Matlab.

7. Αν το ping δεν μας δώσει κάποια απάντηση, σημαίνει ότι ο προορισμός δεν υπάρχει. Σωστό, λάθος και γιατί;

8. Το ping επιστρέφει και το RTT time. Αναφέρετε πιθανούς λόγους που το RTT/2 δεν είναι το one way delay.

9. Μπαίνοντας σε με ιστοσελίδα χρησιμοποιώντας την IP του web server και όχι το URL (πχ 173.194.35.159), δεν χρησιμοποιείται το DNS πρωτόκολλο. Σωστό λάθος και γιατί;

10. Επηρεάζει ο αριθμός των κόμβων την συνολική καθυστέρηση; Για να απαντήσετε, θα πρέπει να εκτελέσετε την εντολή traceroute σε διαφορετικά destination hosts και να τα συγκρίνετε. Συλλέξετε μετρήσεις και αναλύσετέ τις ώστε να υποστηρίξετε την υπόθεσή σας πειστικά ή δώστε αντιπαραδείγματα για να την αναιρέσετε.

11. Να τρέξετε για μια εβδομάδα, με συστηματικό τρόπο (π.χ. πρωί, μεσημέρι και βραδύ) το traceroute και να βρείτε εάν υπάρχουν trends, πχ. ότι όλες οι

[1] http://www.mathworks.com/help/stats/cdfplot.html

μετρήσεις κατά τη διάρκεια συγκεκριμένης περιόδου (πχ τα πρωινά/καθημερινές) έχουν μεγαλύτερη καθυστέρηση κ.α.

Wireshark/tcpdump

Χρησιμοποιώντας το Wireshark η το tcpdump συλλέξετε τα πακέτα που στέλνονται ή λαμβάνονται από τον υπολογιστή σας για τουλάχιστον μία ώρα. Μετά από αυτό απαντήστε στα παρακάτω ερωτήματα χρησιμοποιώντας το wireshark.

1. Πόσα TCP και πόσα UDP πακέτα στάλθηκαν;
2. Πόσα TCP πακέτα είχαν ως destination port την 80 και πόσα ως source port;
3. Πόσα πακέτα μετέφεραν HTTP δεδομένα; Συγκρίνετε τον αριθμό τους με το ερώτημα b και εξηγήστε τι παρατηρείτε.
4. Υπάρχουν πακέτα που χρησιμοποιούν κάποιο πρωτόκολλο του transport layer εκτός από TCP και UDP; Αναφέρετε ποιο φίλτρο χρησιμοποιήσατε και παραδώστε μαζί με την αναφορά σας και το ask1_d.pcap αρχείο που δείχνει τα αποτελέσματα του φίλτρου.
5. Βρείτε την IP του router σας από τα πακέτα που πιάσατε. Με ποιο φίλτρο την βρήκατε και γιατί; Παραδώστε μαζί με την αναφορά σας και το ask1_e.pcap αρχείο που δείχνει τα αποτελέσματα του φίλτρου.
6. Βρείτε ένα ή περισσότερα arp πακέτα, χωρίς να χρησιμοποιείστε το arp filter του wireshark. Ποιο φίλτρο χρησιμοποιήσατε και γιατί; παραδώστε μαζί με την αναφορά σας και το ask1_f.pcap αρχείο που δείχνει τα αποτελέσματα του φίλτρου. (Σημείωση: Αν δεν υπάρχει κάποιο arp πακέτο σκεφτείτε τρόπους να “αναγκάσετε” την εμφάνισή τους αναφέροντας και τον τρόπο με τον οποίο το επιτύχατε.)
7. Βρείτε όλα τα πακέτα που χρησιμοποιούνται για το DNS εφαρμόζοντας το κατάλληλο φίλτρο. Παραδώστε μαζί με την αναφορά σας και το ask1_g.pcap αρχείο που δείχνει τα αποτελέσματα του φίλτρου.
8. Βρείτε όλα τα πακέτα που χρησιμοποιούνται για το DNS και όλα τα HTTP request πακέτα που φεύγουν από τον υπολογιστή σας. Παρατηρείτε κάποιου είδους συσχέτιση;