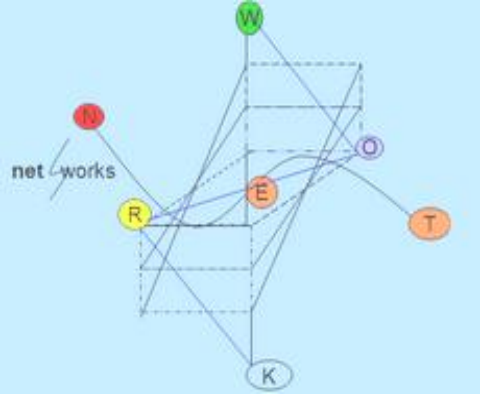


HY335: Δίκτυα Υπολογιστών
Χειμερινό Εξάμηνο 2012-2013
Τμήμα Επιστήμης Υπολογιστών
Πανεπιστήμιο Κρήτης
Διδάσκουσα: Μαρία Παπαδοπούλη

2η σειρά ασκήσεων

Θεωρητικές Ασκήσεις

Απαντήστε σύντομα και περιεκτικά (2-3 προτάσεις) τις παρακάτω θεωρητικές ερωτήσεις.

1. 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  kol1-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.

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

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

4. Το μονοπάτι που μας κάνει report το traceroute είναι το ακριβές μονοπάτι που ακολουθούν όλα τα πακέτα που στέλνει το traceroute. Σωστό, λάθος

δίνοντας ένα σχηματικό παράδειγμα με διάφορους ενδιάμεσους κόμβους και τις τιμές του TTL για κάθε πακέτο.

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

6. Το ping μεταξύ άλλων μας επιστρέφει και το RTT time. Αναφέρετε πιθανούς λόγους που το RTT/2 δεν είναι το one way delay.

7. 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;

8. Έστω ότι το resolv.conf αρχείο σας περιέχει τις εξής εγγραφές

nameserver 9.9.9.9

nameserver 8.8.8.8

nameserver 192.168.1.254

όπου το 192.168.1.254 είναι το gateway σας (το modem/router της ADSL σύνδεσή σας).

Για τις παρακάτω περιπτώσεις απαντήστε ποιος **DNS server** θα χρησιμοποιηθεί.

i. Ο χρήστης επισκέπτεται την ιστοσελίδα http://www.csd.uoc.gr

ii. Ο χρήστης επισκέπτεται την ιστοσελίδα http://www.csd.uoc.gr και ο server 8.8.8.8 είναι down. (μη-προσβάσιμος)

iii. Ο χρήστης επισκέπτεται την ιστοσελίδα http://147.52.78.3 και ο 9.9.9.9 είναι down.

iv. Ο χρήστης επισκέπτεται την ιστοσελίδα http://www.csd.uoc.gr και ο 9.9.9.9 είναι down.

v. Ο χρήστης επισκέπτεται την ιστοσελίδα http://www.csd.uoc.gr και οι 9.9.9.9, 8.8.8.8 είναι down.

9. Πόσες IP διευθύνσεις μπορεί να έχει ένα \16 subnet;

10. Το πανεπιστήμιο Κρήτης έχει ένα \16 subnet. Πόσα \24 subnets μπορεί να έχει το πανεπιστήμιο.

11. Έστω ότι ένα δίκτυο μπορεί να υποστηρίξει το εύρος διευθύνσεων 10.0.0.0-10.255.255.255. Ποιο είναι το network ID και πιό το subnet;

12. Σε ένα υπολογιστή που ανήκει σε κάποιο ιδιωτικό LAN μπορούμε να δώσουμε την IP 147.52.5.5 χωρίς κανένα πρόβλημα. Σωστό, λάθος και γιατί;

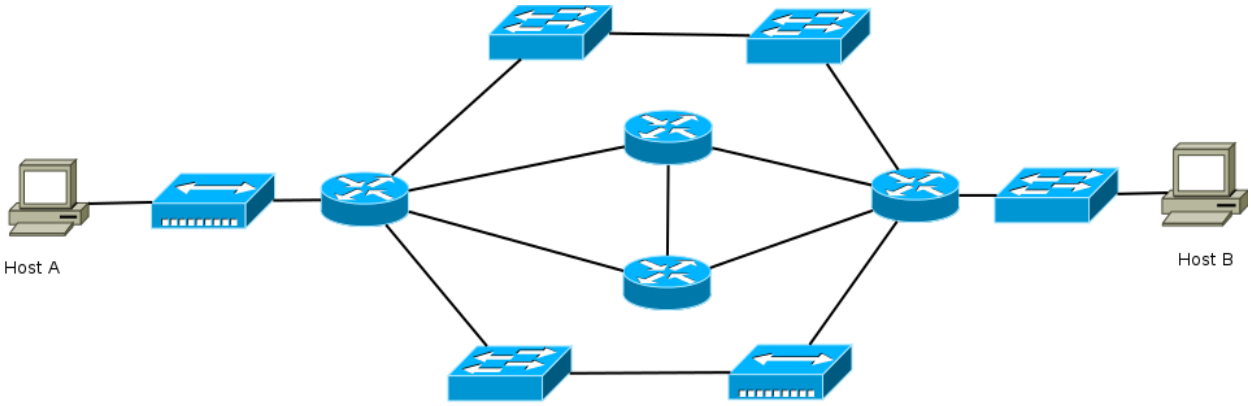
13. Έστω ότι σε ένα home network, ο DHCP είναι ρυθμισμένος να δίνει IPs από την 192.168.1.2 έως την 192.168.1.254 και πως το router σας έχει IP 192.168.1.1. Εσείς για κάποιο λόγο θέλετε να δώσετε μια στατική IP στον σταθερό υπολογιστή σας. Απαντήστε στις παρακάτω ερωτήσεις:

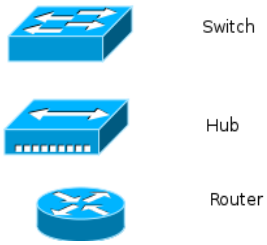
i. Γιατί ο DHCP δεν δίνει την 192.168.1.255 διεύθυνση;

ii. Ποια μπορεί να είναι η στατική IP που θα δώσετε στον υπολογιστή σας;

iii. Δεδομένης της IP που δώσατε τι πρέπει να αλλάξει στον DHCP;

14. Σας δίνετε το παρακάτω δίκτυο, καθώς και τι τύπου είναι ο κάθε ενδιάμεσος κόμβος.





Ονοματίστε τους ενδιάμεσους κόμβους και καταγράψτε όλες τις πιθανές διαδρομές που μπορεί να ακολουθήσει ένα πακέτο από τον host A στον host B, καθώς και τις τιμές TTL του πακέτου σε κάθε κόμβο, θεωρώντας ότι η αρχική του τιμή είναι TTL=30.

Πρακτικές ασκήσεις

Άσκηση 1

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

Πόσα TCP και πόσα UDP πακέτα στάλθηκαν;

Πόσα TCP πακέτα είχαν ως destination port την 80 και πόσα ως source port;

Πόσα πακέτα μετέφεραν HTTP δεδομένα; Συγκρίνετε τον αριθμό τους με το ερώτημα b και εξηγήστε τι παρατηρείτε.

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.

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.

Βρείτε ένα ή περισσότερα arp πακέτα, χωρίς να χρησιμοποιείστε το arp filter του wireshark. Πιο 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.)

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.

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;

Άσκηση 2

Σε κάθε ομάδα θα δοθεί μία λίστα από URLs. Για κάθε ένα από αυτά θα πρέπει να κάνετε τα εξής:

- Να κάνετε ping 30 επαναλήψεων μετρώντας το mean του RTT time.
- Να κάνετε traceroute μετρώντας τον συνολικό αριθμό των hops
- Να κατεβάσετε την σελίδα χρησιμοποιώντας το wget ή οποιοδήποτε αντίστοιχο πρόγραμμα, μετρώντας τον download χρόνο της σελίδας.
- Να μετρήσετε τον χρόνο που χρειάζεται ο DNS σας, να σας επιστρέψει την IP του webserver για το συγκεκριμένο URL.

Τις παραπάνω μετρήσεις θα τις επαναλάβετε για 3 ημέρες. Κάθε μέρα θα πρέπει να κάνετε τουλάχιστον 10 μετρήσεις σε τυχαίες χρονικές στιγμές.

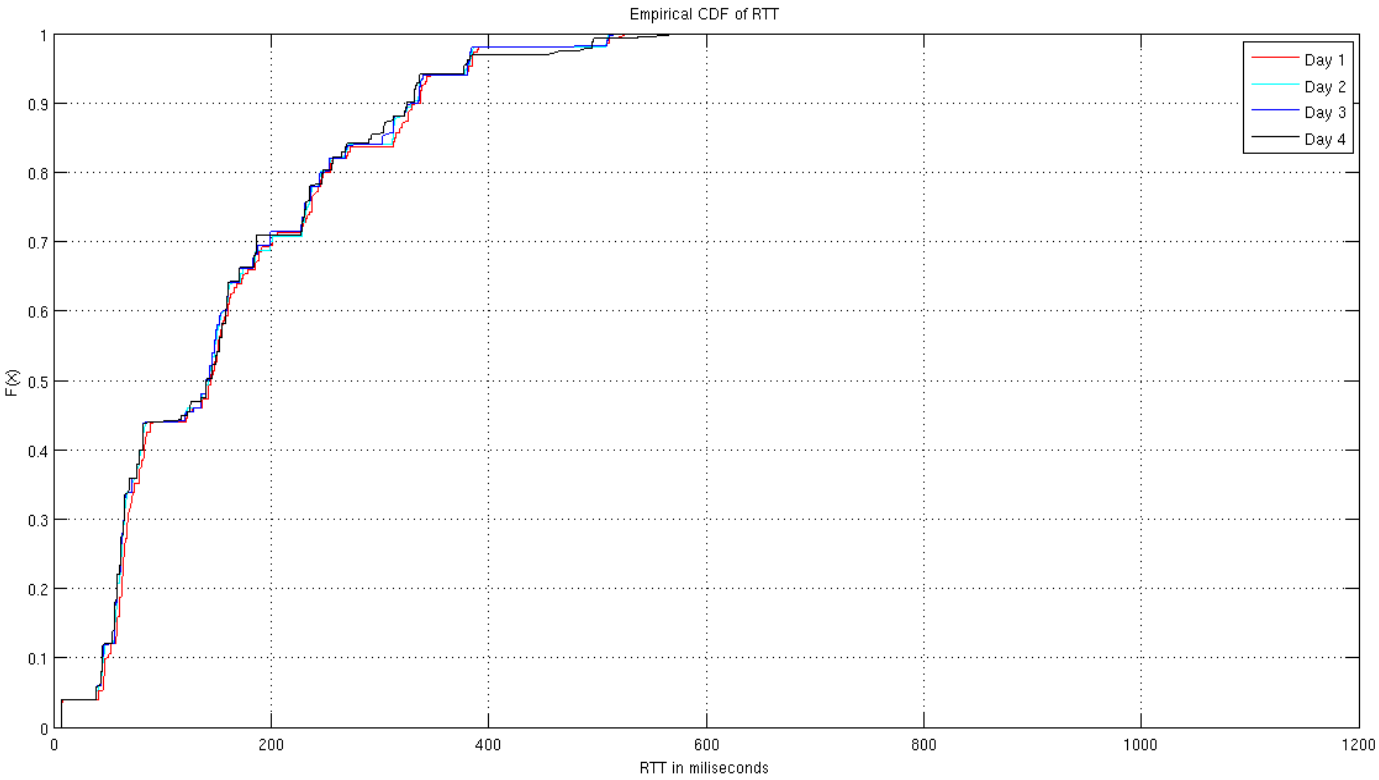
Μόλις τελειώσετε με τις μετρήσεις θα πρέπει να κάνετε τα εξής:

Δημιουργείστε έναν πίνακα που για κάθε URL θα έχει το mean RTT time ανάλογα με την ημέρα. Για παράδειγμα:

URL	Day 0	Day 1	Day 2
www.grnet.gr	2 ms	2.01 ms	1.987 ms
www.uoc.gr	1.25 ms	1.222 ms	0.98 ms

Κάντε το ίδιο για το mean hops count, download time και DNS query time. Δηλαδή στο τέλος θα πρέπει να έχετε τέσσερις πίνακες.

Έχοντας κάνει τους πίνακες υπολογίστε τα τέσσερα αντίστοιχα CDF plots εξηγώντας για κάθε plot, τι παρατηρείτε. Για παράδειγμα το CDF plot για το mean RTT time θα πρέπει να έχει 3 διαφορετικές γραμμές, μία για κάθε μέρα, με ξεχωριστό χρώμα, όπως η παρακάτω εικόνα:



Κάντε plot την συσχέτιση που έχουν τα εξής ζεύγη για κάθε μία από τις τρεις ημέρες, σχολιάζοντας τα αποτελέσματα του κάθε plot.

i. RTT time-download time

ii. RTT time-hops count

iii. RTT time-DNS query time

Διαλέξτε τέσσερα URLs και αφού βρείτε σε πια χώρα βρίσκεται ο webserver τους, σχολιάστε αν υπάρχει συσχέτιση μεταξύ RTT time και του αριθμού των hops με την γεωγραφική απόσταση.

Άσκηση 3

Σας δίνεται το αρχείο "Syslog.txt" το οποίο περιέχει δεδομένα που έχει συγκεντρώσει κάποιος διαχειριστής δικτύου. Κάθε γραμμή του αρχείου αυτού αντιστοιχεί σε ένα γεγονός που προκαλείται από κάποιο πελάτη 802.11 (WiFi) και έχει τις εξής στήλες:

1. Χρόνος στον οποίο συμβαίνει το γεγονός (σε δευτερόλεπτα από το 1-1-1970).
2. ID του Access point στο οποίο συμβαίνει το γεγονός (κάθε Access point αντιστοιχεί σε ένα μοναδικό αριθμό).
3. ID του πελάτη 802.11 που προκαλεί το γεγονός (κάθε διαφορετική MAC διεύθυνση αντιστοιχεί σε ένα μοναδικό ID πελάτη).
4. Τύπος μηνύματος syslog (μπορεί να πάρει τις τιμές VxW and IOS).
5. Τύπος γεγονότος (μπορεί να πάρει τις τιμές Authenticated, Associated, Reassociated, Roamed, Deauthenticated, Disassociated, Rebooted).
6. Λόγος για τον οποίο συμβαίνει το γεγονός.

Ερωτήματα:
a) Κάντε parsing του αρχείου "Syslog.txt". **Υπόδειξη**: για το σκοπό αυτό μπορείτε να χρησιμοποιήσετε τις παρακάτω εντολές matlab:

```
fid = fopen('Syslog_data.txt');
C = textscan(fid, '%d %d %d %s %s %s %s %s %s %s %s %s %s %s %s %s');
fclose(fid);
```

Η εντολή textscan παράγει ως έξοδο μία δομή που στο matlab ονομάζεται cell array. Για να προσπελάσετε την πρώτη στήλη του αρχείου "Syslog_data.txt" μπορείτε να εκτελέσετε την εντολή C{1}; , για τη δεύτερη στήλη την εντολή C{2}; και ούτω καθεξής.

b) Επιλέξτε τη στήλη που περιέχει τα IDs των Access points και βρείτε όλα τα διαφορετικά IDs που εμφανίζονται σε αυτή τη στήλη. **Υπόδειξη**: μπορείτε να χρησιμοποιήσετε την εντολή unique του matlab.

c) Επιλέξτε τις γραμμές του αρχείου που αντιστοιχούν στον τύπο γεγονότος "Associated".

Υπόδειξη: μπορείτε να αντιστοιχήσετε τους τύπους των γεγονότων σε διαφορετικά IDs. Για παράδειγμα τα γεγονότα "Associated" μπορείτε να τα αντικαταστήσετε με το ID 1, τα γεγονότα "Authenticated" με το ID 2 και ούτω καθεξής. Για να κάνετε κάτι τέτοιο μπορεί και πάλι να σας βοηθήσει η εντολή unique και συγκεκριμένα το τρίτο όρισμα εξόδου. Αφού αντιστοιχήσετε τους τύπους των γεγονότων σε ids θα έχετε ένα διάνυσμα που θα περιέχει σε κάθε γραμμή το id του γεγονότος που συμβαίνει σε αυτή τη γραμμή. Αμέσως μετά επιλέξτε από αυτό το διάνυσμα τις γραμμές που έχουν το id του γεγονότος "Associated". Αυτό μπορείτε να το κάνετε με δύο τρόπους:

Έστω ότι έχετε ένα διάνυσμα στήλη a και θέλετε να επιλέξετε τις γραμμές στις οποίες το διάνυσμα a παίρνει την τιμή 100, τότε εκτελείτε τις παρακάτω εντολές:

```
% Ορίζεται ένα Boolean vector που παίρνει την τιμή 1 στις γραμμές που
```

```
% ικανοποιείται η συνθήκη a == 100 και 0 στις υπόλοιπες γραμμές.
boolean_vec = a == 100;

% Έχοντας τώρα ορίσει το διάνυσμα boolean_vec μπορείτε να το
% χρησιμοποιήσετε για να επιλέξετε από ένα διάνυσμα b (που έχει το ίδιο
% μέγεθος με το διάνυσμα a) τις γραμμές εκείνες στις οποίες το a παίρνει την
% τιμή 100.
b1 = b(boolean_vec);
```

Εναλλακτικά μπορείτε να εκτελέσετε τις παρακάτω εντολές:

```
% Βρίσκετε τους δείκτες των γραμμών του διανύσματος a για τους οποίους το a
% παίρνει  την τιμή 100.
indices = find(a == 100);

% Έχοντας τώρα ορίσει το διάνυσμα με τους δείκτες indices μπορείτε να το
% χρησιμοποιήσετε για να επιλέξετε από ένα διάνυσμα b (που έχει το ίδιο
% μέγεθος με το διάνυσμα a) τις γραμμές εκείνες στις οποίες το a παίρνει την
% τιμή 100.
b1 = b(indices);
```

Οι γραμμές που επιλέξατε με την παραπάνω διαδικασία αντιστοιχούν στις αφίξεις χρηστών που πραγματοποιούνται σε όλα τα Access points του δικτύου. Θεωρήστε ότι οι αφίξεις αυτές περιγράφονται από μία στοχαστική διαδικασία Poisson. Εκτιμήστε την παράμετρο αυτής της στοχαστικής διαδικασίας που ταιριάζει καλύτερα στα δεδομένα.

d) Πάρτε 10000 τυχαία δείγματα από τη στοχαστική διαδικασία Poisson που εκτιμήσατε στο προηγούμενο ερώτημα. **Υπόδειξη**: μπορείτε να χρησιμοποιήσετε τη συνάρτηση του matlab exprnd. Κατασκευάστε ένα ιστόγραμμα καθώς και τα διαγράμματα cdf και ccdf που αντιστοιχούν στους χρόνους μεταξύ διαδοχικών γεγονότων.

Παραδώστε τον κώδικα Matlab καθώς και τις παρατηρήσεις σας, για κάθε ερώτημα. Για την άσκηση αυτή μπορούν να σας βοηθήσουν τα slides του 4ου φροντιστηρίου.