**Γεννήτριες & Εργαλεία Ανάλυσης Δικτυακής Κίνησης**

**Εισαγωγή**

Σκοπός του εργαστηρίου είναι η εξοικείωση σας με τα εργαλεία που χρησιμοποιούνται για τη δημιουργία και ανάλυση δικτυακής κίνησης. Η κατάλληλη (ναι υπάρχει και ακατάλληλη) χρήση αυτών των εργαλείων μπορεί να σας βοηθήσει στην αξιολόγηση ενός δικτύου, ενός πρωτοκόλλου κ.τ.λ. Υπενθυμίζετε ότι οι βασικοί παράμετροι αξιολόγησης όσο αφορά την απόδοση ενός δικτύου ή ενός πρωτοκόλλου, είναι η ταχύτητα μεταφοράς δεδομένων, η καθυστέρηση (one way delay ή RTT) το jitter και οι απώλειες (άλλοι παράμετροι θα μπορούσαν να είναι η ασφάλεια, η ανεκτικότητα σε σφάλματα κ.α., αλλά δεν θα μας απασχολήσει για ...... σήμερα τουλάχιστον).

Η μεθοδολογία που ακολουθείται εν γένει είναι η εξής:

1. Σχεδιασμός σεναρίων κίνησης παίρνοντας υπόψη δεδομένα που έχουν να κάνουν με τη φύση της αξιολόγησης που επιθυμούμε;
2. Επιλογή των εργαλείων που θα υλοποιήσουν τα σενάρια κίνησης και
3. Επιλογή εργαλείων ανάλυσης της κίνησης.

Εν συνεχεία αφού γίνουν οι προηγούμενες επιλογές προχωράμε στη εκτέλεση του πειράματος. Ανάλογα με τα εργαλεία που έχουν επιλεχθεί η ανάλυση μπορεί να γίνεται σε πραγματικό χρόνο η όχι. Εάν δε γίνεται σε πραγματικό χρόνο είναι προφανές ότι η δημιουργηθείσα κίνηση πρέπει να αποθηκευτεί ώστε να μπορούμε να τη αναλύσουμε αργότερα. Με τη ανάλυση μπορούμε να εντοπίσουμε προβλήματα στη λειτουργία ενός δικτύου η ενός πρωτοκόλλου και να προχωρήσουμε στη διαδικασία επίλυσης τους.

**Γεννήτρια Δικτυακής Κίνησης**

Η γεννήτρια δικτυακής κίνησης που θα χρησιμοποιήσουμε στο σημερινό εργαστήριο είναι το iperf3. Το iperf3 υποστηρίζει τα πρωτόκολλα TCP και UDP και λειτουργεί σε δύο καταστάσεις, αυτή του εξυπηρετητή και αυτή του πελάτη. Όταν θέλουμε να δημιουργήσουμε κίνηση μεταξύ δύο υπολογιστών εκτελούμε το iperf3 σε κατάσταση εξυπηρετητή στον ένα υπολογιστή και σε κατάσταση πελάτη στον άλλο. Έτσι για παράδειγμα εάν θέλουμε στείλουμε κίνηση από τον υπολογιστή Α (IP:193.92.9.4) στον υπολογιστή B (IP:193.92.9.3) τότε εκτελούμε στο Β iperf3 -s (η εντολή αυτή θα πρέπει να τρέξει πρώτη) και στο Α iperf3 -c 193.92.9.3. Οι εντολές αυτές δημιουργούν TCP κίνηση από τον Α στο B διάρκειας 10 δευτερολέπτων.

Για παραπάνω πληροφορίες εκτελέστε iperf3 -h ή man iperf3. Ενδεικτικές επιπλέον επιλογές στο iperf3 είναι:

* -p port\_number: ποίον αριθμό θύρας να χρησιμοποιήσει.
* -u: αποστολή κίνησης udp αντί tcp
* -n #Kb/s: ρυθμός αποστολής κίνησης
* -t #secs: για πόσα δευτερόλεπτα να στέλνει.

**Αποθήκευση Δικτυακής Κίνησης**

Για τη αποθήκευση δικτυακής κίνησης θα χρησιμοποιήσουμε το tcpdump (ναι και το wireshark κάνει αλλά τρώει πιο πολλούς πόρους). Το tcpdump μας δίνει τη δυνατότητα να βλέπουμε/αποθηκεύουμε τη κίνηση διέρχεται από τις κάρτες δικτύου μας. Θα την εκτελείται ως εξής:

* tcpdump -vvv -n -i <interface> <filters> -w <filename>. Για παράδειγμα η εντολή tcpdump -vvv -n -i eth0 icmp -w /home/test/saveit αποθήκευση την icmp κίνηση της κάρτας eth0 στο αρχείο saveit.

Εάν δε βάλετε το όρισμα εγγραφής σε αρχείο η κίνηση εμφανίζεται στην οθόνη σας. Επίσης εάν θέλετε να διαβάσετε το αρχείο αργότερα η εντολή είναι

* tcpdump -vvv -n -r <filters> <filename> Τα αρχεία που θα σώζεται με το tcpdump είναι αυτά τα οποία θα αναλύσουμε αργότερα.

**Ανάλυση Δικτυακής Κίνησης**

Για τη ανάλυση της δικτυακής κίνησης θα χρησιμοποιήσουμε το tcptrace. Το tcptrace είναι εξαιρετικό για τη ανάλυση TCP κίνησης (ναι, δεν είναι τόσο εξαιρετικό για UDP). Στη πιο απλή περίπτωση το τρέχετε ως εξής: tcptrace <όνομα αρχείου που αποθηκεύσατε με το tcpdump>.

Για πιο πολλές λεπτομέρειες εκτελέστε, tcptrace -lWr <όνομα αρχείου που αποθηκεύσατε με το tcpdump>.

Για να δημιουργήσετε γραφική για το throughput εκτελέστε, tcptrace -zxy -xtraffic'-B -i1' <όνομα αρχείου που αποθηκεύσατε με το tcpdump>.

Για να δημιουργήσετε γραφική για το RTT εκτελέστε, tcptrace -zxy -xtraffic'-R -i1' <όνομα αρχείου που αποθηκεύσατε με το tcpdump>.

Για να δημιουργήσετε γραφική για τα Losses εκτελέστε, tcptrace -zxy -xtraffic'-L -i1' <όνομα αρχείου που αποθηκεύσατε με το tcpdump>.

Τα αρχεία των γραφικών τελειώνουν σε .xpl. Για να τα δείτε εκτελέστε, xpl2gpl <xpl αρχείο> και gnuplot <gpl αρχείο>.

Για παραπάνω πληροφορίες εκτελέστε man tcptrace ή διαβάστε το εγχειρίδιο στο http://www.tcptrace.org/manual/index.html.

**Εργασίες**

1.Αποστείλετε TCP κίνηση διάρκειας 1 λεπτού στο server στη θύρα 5007.

1.Αναλύστε λεπτομερώς τη κίνηση με το όρισμα -lWr.

2.Εμφανίστε τις γραφικές για throughput, RTT και losses.

3.Πόσο είναι το μέσο RTT;

4.Πόσο είναι το μέσο throughput;

5.Είχατε απώλειες και πόσες;

2.Αποστείλετε UDP κίνηση 3Mbps και διάρκειας 1 λεπτού στο server στη θύρα 5008.

1.Πόσο είναι το jitter και πόσα τα losses (βρείτε το από το iperf);

2.Το tcptrace τι πληροφορίες μπορεί να μας δώσει για τη UDP κίνηση; Παραθέστε τις.

**Υποσημείωση**

1. Πριν τα πειράματα, εκτελέστε σε κάθε εικονικό μηχάνημα την εντολή iptables –F
2. Για να δείτε τα γραφήματα, πρέπει πρώτα να εκτελώντας τις εντολές
	1. sudo apt -get install gawk
	2. sudo apt-get install gnuplot-x11

Στην αναφορά σας περιμένω να δω στην “εισαγωγή” λίγο θεωρία σχετικά με TCP/UDP συνδέσεις. Στο τμήμα “μέθοδοι” να φαίνονται οι εργασίες που έχετε να κάνετε και ο εξοπλισμός που χρησιμοποιήσατε. Επίσης να δίνεται την μεθοδολογία που χρησιμοποιήσατε. Στα αποτελέσματα να φαίνονται οι εντολές και οι έξοδοι τους (εάν θέλετε χρησιμοποιήστε screenshots). Στα συμπεράσματα να σχολιάσετε εν συντομία τα αποτελέσματα της εργαστηριακής άσκησης κάνοντας αναφορά στο τι αποκομίσατε σαν γνώση και εάν τα αποτελέσματα είναι ίδια με αυτά που περιμένατε. Στις αναφορές παραθέσετε τις όποιες εξωτερικές πηγές χρησιμοποιήσατε.

Χρησιμοποιήστε το template που βρίσκεται στο e-class για την αναφορά σας. Δείτε και το παράδειγμα αναφοράς που έχω για να πάρετε μια ιδέα.