Πανεπιστήμιο Ιωαννίνων
Τμήμα Πληροφορικής & Τηλεπικοινωνιών
Διαχείριση Δικτύων

Εξοικείωση με την εντολή netstat

[Η άσκηση βασίζεται στην εκτέλεση της εντολής σε περιβάλλον Windows. Παρόμοια εντολή υπάρχει και στα περιβάλλοντα UNIX/Linux]

Η εντολή **netstat** εμφανίζει πληροφορίες για τις τρέχουσες συνδέσεις TCP/IP και στατιστικά για την δικτυακή κίνηση κάποιου υπολογιστή (host).

Πριν την έναρξη της άσκησης καλό θα ήταν να επισκεφτείτε με το φυλλομετρητή σας ένα δικτυακό portal (πχ. www.yahoo.com) για να δημιουργηθούν αρκετές συνδέσεις. Αυτό μπορείτε να το επαναλάβετε και κατά την διάρκεια της άσκησης όταν χρειαστεί να δημιουργήσετε περισσότερη κίνηση.

1. Εκτελέστε την εντολή: netstat

Εμφανίζονται οι **ενεργές** συνδέσεις που υπάρχουν στον υπολογιστής σας. Παρατηρήστε ότι η πρώτη στήλη εμφανίζει το πρωτόκολλο και ακολουθεί η τοπική IP διεύθυνση και θύρα, το όνομα τομέα του απομακρυσμένου υπολογιστή με το πρωτόκολλο που σχετίζεται με την θύρα και στο τέλος βλέπετε την κατάσταση της σύνδεσης. ESTABLISHED είναι η κανονική κατάσταση μιας σύνδεσης δηλαδή τα δύο άκρα επικοινωνούν κανονικά.

Αν υπάρχουν πολλές συνδέσεις υπάρχει καθυστέρηση για την μετατροπή των απομακρυσμένων διευθύνσεων σε ονόματα τομέα. Για να αποφύγουμε την μετάφραση μπορούμε να χρησιμοποιήσουμε την επιλογή –n

2. Εκτελέστε την εντολή: netstat –n

Παρατηρήστε ότι για τον απομακρυσμένο υπολογιστή βλέπουμε την IP και τον αριθμό θύρας που χρησιμοποιούνται και η εντολή εκτελείτε αρκετά πιο γρήγορα.

3. Εκτελέστε την εντολή: netstat –n –a

Η επιλογή –a εμφανίζει και τις περιπτώσεις όπου ο υπολογιστής μας περιμένει να δεχθεί κάποια σύνδεση [Την επιλογή –n την χρησιμοποιούμε για ταχύτητα]. Έτσι βλέπουμε TCP συνδέσεις σε κατάσταση LISTENING. Επίσης βλέπουμε και τις υποδοχές UDP (IP:Θύρα) στις οποίες μπορούμε να δεχθούμε κάποιο μήνυμα UDP.

Η διεύθυνση 0.0.0.0 σαν τοπική διεύθυνση (Local Address) αντιπροσωπεύει οποιαδήποτε διεύθυνση του υπολογιστή μας. Έχει διαφορετική ερμηνεία εδώ σε σχέση με τον πίνακα δρομολόγησης που εμφανίζεται από την εντολή “route print”

4. Εκτελέστε την εντολή netstat –a –p UDP

Η επιλογή –p όταν ακολουθείται από το όνομα ενός πρωτοκόλλου εμφανίζει πληροφορίες μόνο για το πρωτόκολλο αυτό. Έτσι στην περίπτωση αυτή περιορίζεται το αποτέλεσμα της εντολής σε πληροφορίες μόνο για το πρωτόκολλο UDP.

5. Εκτελέστε την εντολή: netstat –n –o

Παρατηρήστε ότι στο αποτέλεσμα υπάρχει μια επιπλέον στήλη PID (Process Identifier). Αυτός είναι ο αριθμός της διεργασίας που συμμετέχει στην σύνδεση. Μπορείτε να τον χρησιμοποιήσετε για να εντοπίσετε την εφαρμογή πίσω από την διεργασία. Στα Windows με Ctrl-Alt-Del μπορείτε να επιλέξετε τον Διαχειριστή Λειτουργιών (Task Manager). Επιλέξτε την δεύτερη καρτέλα (Processes – Διεργασίες). Στα Windows 10 επιλέξτε τον σύνδεσμο Details Μπορείτε να αναζητήσετε την γραμμή με το PID που σας ενδιαφέρει. Στην αριστερή στήλη Image Name (Όνομα Εικόνας) μπορείτε να δείτε το εκτελέσιμο αρχείο που δημιούργησε την διεργασία. (Σε προηγούμενες εκδόσεις αν δεν εμφανίζεται η στήλη PID επιλέξτε την πηγαίνοντας στο View(Προβολή) -> Column Selection (Επιλογή Στηλών) και επιλέξτε PID)

Από την έκδοση Windows 7 υπάρχει και η επιλογή –b που μπορεί να εμφανίσει το εκτελέσιμο αρχείο κάτω από κάθε γραμμή σύνδεσης. Για να δουλέψει η επιλογή αυτή θα πρέπει να ξεκινήσετε την γραμμή εντολών σαν διαχειριστής (Run as administrator)

6. Εκτελέστε την εντολή: netstat –n 1

Παρατηρήστε ότι η εντολή εκτελείται κάθε ένα δευτερόλεπτο. Τον χρόνο της επανάληψης μπορείτε να το καθορίσετε από τον αριθμό της τελευταίας παραμέτρου. Με το τρόπο αυτό μπορείτε να παρακολουθήσετε τις συνδέσεις στον υπολογιστή σας για κάποιο μεγάλο διάστημα. Για να τερματίσετε την εντολή θα πρέπει να δώσετε τους χαρακτήρες Ctrl-C.

Μπορείτε επίσης να αποθηκεύσετε το αποτέλεσμα της εντολής σε κάποιο αρχείο χρησιμοποιώντας ανακατεύθυνση εξόδου δίνοντας για παράδειγμα την εντολή: netstat –n 1 > \temp\ns.txt

Μετά από κάποιο διάστημα μπορείτε να τερματίσετε την εντολή (Ctrl-C) και να δείτε τα περιεχόμενα του αρχείου \temp\ns.txt που δημιούργησε. Θα μπορούσατε να χρησιμοποιήσετε έναν επεξεργαστή κειμένου αλλά για γρήγορη επισκόπηση μπορείτε να χρησιμοποιήσετε την εντολή more \temp\ns.txt που εμφανίζει το αρχείο σελίδα-σελίδα. Πατάτε SPACE για την επόμενη σελίδα.

7. Εκτελέστε την εντολή: netstat –f

Παρατηρήστε ότι στην θέση της απομακρυσμένης διεύθυνσης εμφανίζεται το πλήρες όνομα τομέα του απομακρυσμένου υπολογιστή (fully qualified name).

8. Εκτελέστε την εντολή: netstat –s

Παρατηρήστε ότι εμφανίζονται στατιστικές πληροφορίες για την κίνηση του TCP/IP οργανωμένη σε περιοχές για τα πρωτόκολλα IP, ICMP, TCP & UDP.

9. Εκτελέστε την εντολή: netstat –s –a –p TCP

Παρατηρήστε ότι εμφανίζονται οι στατιστικές πληροφορίες του πρωτοκόλλου TCP και όλες οι συνδέσεις του. Γενικά μπορούμε να συνδυάσουμε την επιλογή –s με την επιλογή –p και να εμφανίσουμε στατιστικές πληροφορίες για συγκεκριμένο πρωτόκολλο.

10. Εκτελέστε την εντολή: netstat –e

Εμφανίζονται στατιστικές πληροφορίες για όλη την δικτυακή κίνηση των επαφών του υπολογιστή μας όπως συνολικός αριθμός byte ή πακέτων που έχουν αποσταλεί η παραληφθεί από την στιγμή εκκίνησης του υπολογιστή μας. Μεγάλος αριθμός λαθών μπορεί να σηματοδοτεί κάποια συμφόρηση ή κάποιο πρόβλημα με την κάρτα δικτύου μας.

Ερωτήσεις

- Ποια επιλογή εκτέλεσης της netstat θα χρησιμοποιήσουμε για να εμφανίσουμε το μέγεθος όλων των μηνυμάτων που έχουν σταλεί ή παραληφθεί από την επαφή ethernet του υπολογιστή μας.
- Ποια επιλογή εκτέλεσης της netstat θα μας βοηθήσει να εντοπίσουμε την εφαρμογή που δημιούργησε κάποια ενεργή σύνδεση TCP.
- Ποια(ες) επιλογή(ες) εκτέλεσης της netstat θα μας βοηθήσει να εμφανίσουμε όλες τις δυνατές πληροφορίες (στατιστικά, και θύρες αναμονής πακέτων) για το πρωτόκολλο UDP.
- Ποια είναι η χρησιμότητα της επιλογής –n στην εντολή netstat
- Πως μπορούμε να εκτελούμε την netstat συνέχεια κάθε 5 δευτερόλεπτα.