ΤΕΙ Ηπείρου
Τμήμα Μηχανικών Πληροφορικής
Διαχείριση Δικτύων

Άσκηση

Εξοικείωση με την εντολή Telnet ως διαγνωστικό εργαλείο

Η βασική λειτουργία της εντολής **telnet** είναι να παρέχει απομακρυσμένη πρόσβαση σε κάποιο υπολογιστή. Η εφαρμογή πελάτη μπορεί να εκτελεστεί από την γραμμή εντολών με την εντολή telnet και το όνομα ή την IP διεύθυνση του υπολογιστή με τον οποίο θέλουμε να συνδεθούμε.

Η εντολή telnet μπορεί να χρησιμοποιηθεί και σαν διαγνωστικό εργαλείο για να ελέγχουμε αν κάποια θύρα (port) σε κάποιον υπολογιστή είναι προσβάσιμη (ανοικτή). Με άλλα λόγια θα μπορούσαμε να την χρησιμοποιήσουμε σαν ένα είδος "ping" για κάποια θύρα.

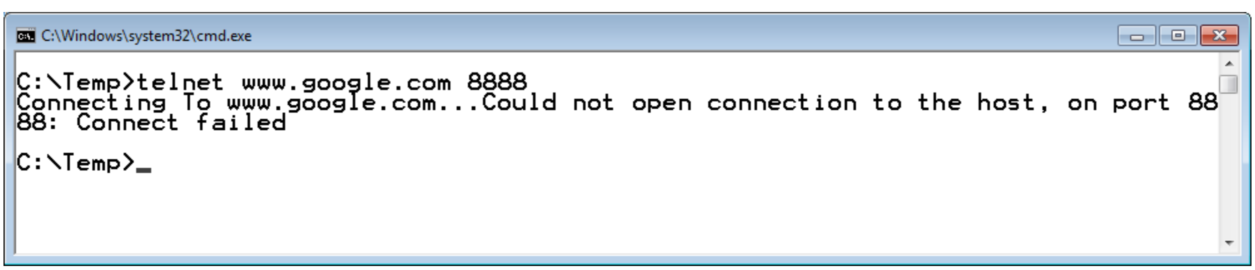
Σημείωση: Στα συστήματα **Windows 7** και **Windows 10** η εφαρμογή telnet (client) δεν είναι ενεργοποιημένη. Μπορείτε να την ενεργοποιήσετε με την γραμμή εντολών. Ξεκινήστε την γραμμή εντολών τρέχοντας στο πρόγραμμα CMD σαν διαχειριστές (Run as Administrator) και στην συνέχεια εκτελέστε την εντολή: `dism /online /Enable-Feature /FeatureName:TelnetClient`

1.

Εκτελέστε την εντολή :

```
telnet www.google.com 8888
```

Παρατηρήστε ότι μετά από κάποιο διάστημα εμφανίζεται κάποιο μήνυμα λάθους της μορφής



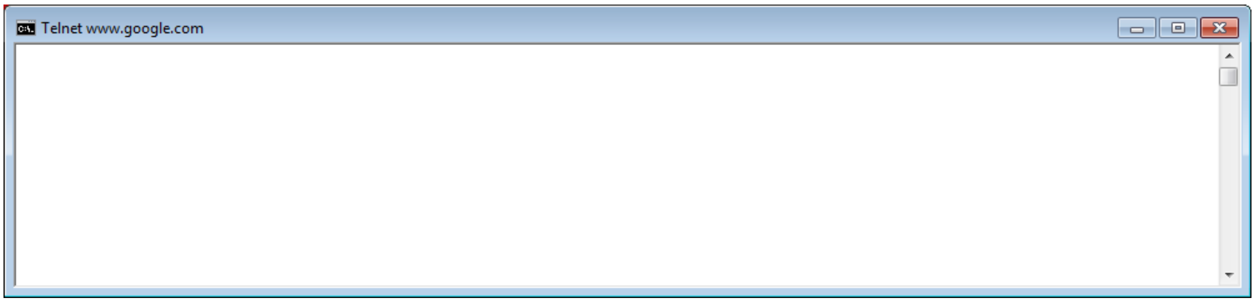
Αυτό σημαίνει ότι η θύρα 8888 δεν είναι προσβάσιμη στον εξυπηρετητή (server) με όνομα www.google.com

2.

Επαναλάβετε την διαδικασία προσπαθώντας να χρησιμοποιήσετε την θύρα 80 που είναι η προεπιλεγμένη θύρα του πρωτοκόλλου HTTP (δηλ. η θύρα που χρησιμοποιούν οι εξυπηρετητές ιστού (web servers))

```
C:\Windows\system32\cmd.exe

C:\Temp> telnet www.google.com 80
```

Αφού πατήσετε enter θα παρατηρήσετε ότι εμφανίζεται μια κενή οθόνη



Αυτό είναι μια ένδειξη ότι η εντολή telnet δημιούργησε μια σύνδεση στην θύρα 80 και μπορούμε να συμπεράνουμε ότι η θύρα αυτή είναι προσβάσιμη στον server www.google.com

Ο λόγος που βλέπουμε μια κενή οθόνη είναι ότι δεν συνδεθήκαμε σε telnet server αλλά σε http server ο οποίος δεν μας έχει στείλει κάποια απόκριση.   Μπορούμε όμως να στείλουμε μια αίτηση HTTP πληκτρολογώντας:

```
GET  /  HTTP/1.1
```

Επειδή δεν φαίνεται τι πληκτρολογείτε πρέπει να είσαστε προσεκτικοί (δεν μπορείτε να διορθώσετε κάτι πατώντας Backspace ή Delete)

Αν πληκτρολογήσατε σωστά την εντολή και **πατήσετε 2 φορές enter** θα εμφανιστεί μια HTTP απόκριση από τον server

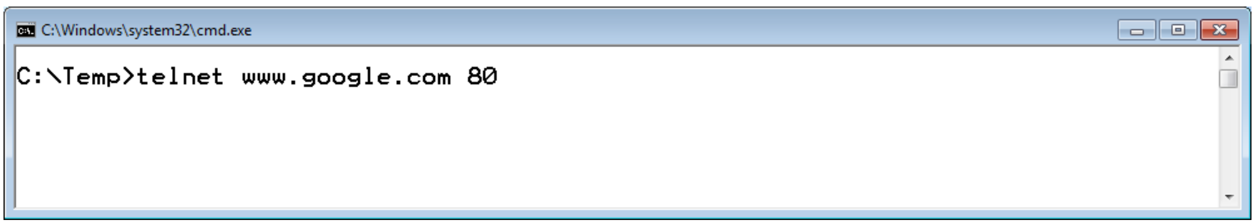
```
Telnet www.google.com

HTTP/1.1 302 Found
Cache-Control: private
Content-Type: text/html; charset=UTF-8
Location: http://www.google.gr/?gfe_rd=cr&ei=F0ijVqKnObPF8AfWk4PADA
Content-Length: 258
Date: Sat, 23 Jan 2016 09:29:59 GMT
Server: GFE/2.0

<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>302 Moved</TITLE></HEAD><BODY>
<H1>302 Moved</H1>
The document has moved
<A HREF="http://www.google.gr/?gfe_rd=cr&amp;ei=F0ijVqKnObPF8AfWk4PADA">here</A>.
</BODY></HTML>
```

Σημείωση: Την διαδικασία που περιγράφεται στο τμήμα αυτό πρέπει να την ακολουθήσετε σχετικά γρήγορα διαφορετικά η σύνδεση θα διακοπεί και θα πρέπει να την επαναλάβετε.

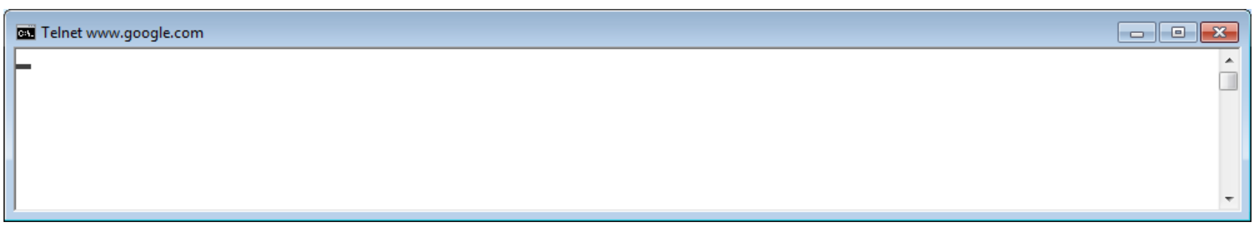
3.

Στην περίπτωση που εξετάσαμε πριν θα μπορούσαμε να ενεργοποιήσουμε και την επιλογή ηχούς (echo) της telnet για να βλέπουμε τι στέλνουμε στον server. Μπορείτε να το πετύχετε με την ακόλουθη διαδικασία.

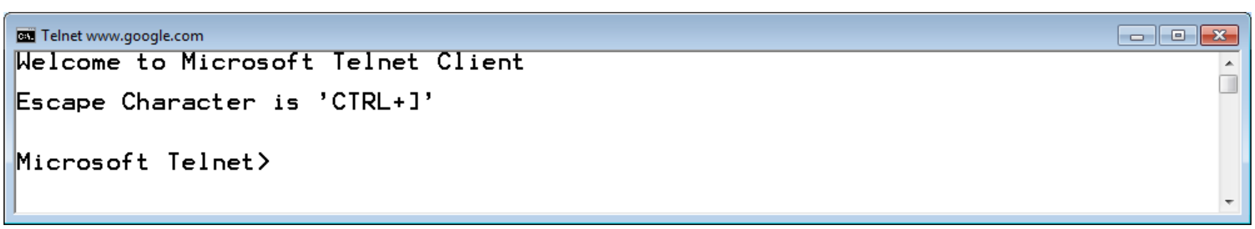
Επαναλάβετε το πρώτο βήμα της προηγούμενης παραγράφου



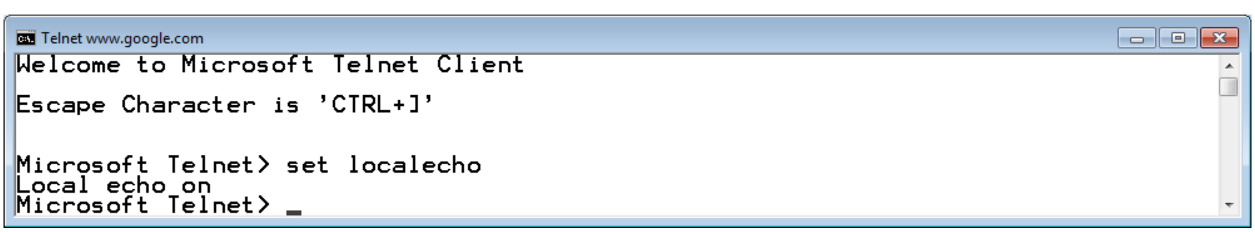
Όταν εμφανιστεί η κενή οθόνη



Πατήστε τον χαρακτήρα διαφυγής Ctrl-] . Θα μεταφερθείτε στην κατάσταση ελέγχου

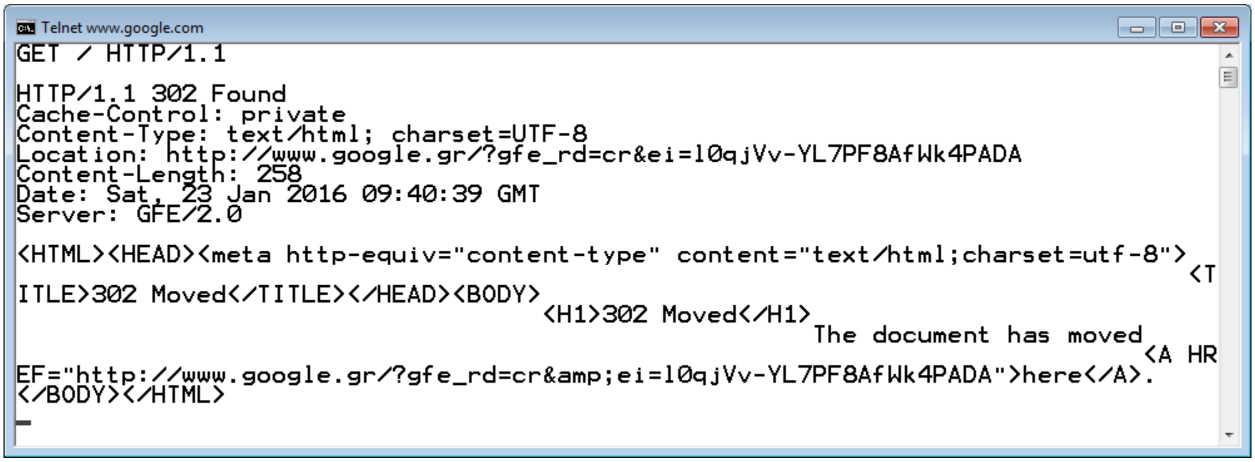


Εισάγετε την εντολή set localecho



Πατήστε enter για να μεταφερθείτε στην κατάσταση σύνδεσης

Μπορείτε τώρα να πληκτρολογήσετε την εντολή GET / HTTP/1.1 ακολουθούμενη από δύο enter και θα λάβετε την προηγούμενη απάντηση. Αυτή την φορά θα εμφανίζονται οι χαρακτήρες που στέλνετε.



Κάτι επιπλέον που μαθαίνουμε από την συγκεκριμένη HTTP απόκριση είναι μια εφαρμογή της ανακατεύθυνσης σε νέα σελίδα (URL).

Γενικά μπορείτε να παρατηρήσετε ότι αν και στον φυλλομετρητή σας εισάγετε την διεύθυνση www.google.com στην συνέχεια ο φυλλομετρητή σας εμφανίζει μια διεύθυνση της μορφής: https://www.google.gr/?gfe_rd=cr&dcr=0&ei=vCc5Wp7oPOjw8AfM-Y7oCA δηλαδή ανακατευθύνεστε σε άλλη σελίδα.

Αυτό επιτυγχάνετε γιατί η πρώτη απόκριση από την διεύθυνση www.google.com είναι ένα μήνυμα σαν αυτό που εμφανίζεται στο παράδειγμα telnet. Η πρώτη γραμμή στην απόκριση (κατάσταση απόκρισης) HTTP/1.1 302 Found ενημερώνει τον browser ότι πρέπει να φορτώσει κάποιο άλλο έγγραφο. Η διεύθυνση του νέου εγγράφου αναφέρετε στην επικεφαλίδα *Location:* λίγο πιο κάτω. Με τον τρόπο αυτό ο φυλλομετρητής κάνει μια νέα κλίση στο νέο URL.