Τεχνικός Δικτύων & Τηλεπικοινωνιών
Ρίγγας Δημήτρης
Δ.Ι.Ε.Κ. Κέρκυρας, 2014

Πρωτόκολλο ICMP
(Internet Control Message Protocol)

Τι είναι το ICMP

Το πρωτόκολλο Internet Control Message Protocol (ICMP) είναι ένα από τα βασικά πρωτόκολλα του διαδικτύου. Χρησιμοποιείται κυρίως από τα λειτουργικά συστήματα των ηλεκτρονικών υπολογιστών ενός δικτύου για την ανταλλαγή μηνυμάτων λάθους, όπως για παράδειγμα την έλλειψη κάποιας υπηρεσίας από έναν server ή την απουσία ενός υπολογιστή από το δίκτυο.

Το πρωτόκολλο ICMP διαφέρει από τα πρωτόκολλα TCP και UDP διότι συνήθως δεν χρησιμοποιείται από τις εφαρμογές που εκτελούνται σε κάποιον υπολογιστή, αλλά από το λειτουργικό του σύστημα. Το ICMP χρησιμοποιείταια από προγράμματα όπως το ping και το traceroute.

Τα μηνύματα ICMP κατασκευάζονται στο επίπεδο δικτύου και αποτελούν κανονικά πακέτα IP. Όπως και το πρωτόκολλο UDP, το ICMP δεν εγγυάται ότι το πακέτο θα φτάσει αξιόπιστα στον προορισμό του.

Ping

Το εργαλείο ping στέλνει μηνύματα ICMP Echo Request σε κάποιον υπολογιστή του δικτύου για να *διαπιστώσει εάν ο υπολογιστής αυτός υπάρχει ή όχι και επίσης πόσο χρόνο χρειάζεται το μήνυμα να φτάσει σε αυτόν*. Εάν ο υπολογιστής αυτός υπάρχει, θα απαντήσει με μηνύματα Echo Response.

Ο υπολογιστής του αποστολέα δημιουργεί ένα ειδικό πακέτο δεδομένων, το αποστέλλει στην IP διεύθυνση του παραλήπτη και αναμένει ένα συγκεκριμένο χρονικό διάστημα. Στο διάστημα αυτό, το πακέτο θα πρέπει να φτάσει στον παραλήπτη, αυτός να το παραλάβει, να το μαρκάρει ότι το έλαβε και να το ξαναστείλει στον αποστολέα. Το ping χρησιμοποιεί το πρωτόκολλο ICMP για να στείλει ένα πακέτο ECHO_REQUEST ώστε να λάβει ένα πακέτο ECHO_RESPONSE από τον συγκεκριμένο κόμβο. Η συνολική χρονική διάρκεια ταξιδιού *RTT (Round-Trip Time)* των πακέτων ECHO_REQUEST και ECHO_RESPONSE μέσα στο δίκτυο δίνει μια *ένδειξη για τον φόρτο του δικτύου*.

Συνήθως το ping χρησιμοποιείται για να διαπιστώσουμε αν κάποιος υπολογιστής ή άλλη δικτυακή συσκευή είναι εν λειτουργία και συνδεδεμένη με το δίκτυο (alive ή up). Επιπλέον, το ping έχει και κάποιες άλλες πολύ ενδιαφέρουσες ιδιότητες όπως το αναφέρει το χρόνο διάρκειας της διαδρομής των δύο πακέτων (ECHO_REQUEST και ECHO_REPLY (ή RESPONSE)).

Βασική χρήση (από cmd):

```
ping www.google.com
```

Η απάντηση που παίρνουμε είναι:

```
Pinging www.google.gr [74.125.132.94] with 32 bytes of data:
Reply from 74.125.132.94: bytes=32 time=66ms TTL=127
Reply from 74.125.132.94: bytes=32 time=65ms TTL=127
Reply from 74.125.132.94: bytes=32 time=67ms TTL=127
Request timed out.

Ping statistics for 74.125.132.94:
      Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
      Minimum = 65ms, Maximum = 67ms, Average = 66ms
```

Τι έγινε ως εδώ;
Στάλθηκαν πακέτα των **32 bytes** στο www.google.gr δηλ. στην IP **74.125.132.94**. Τα 3 πρώτα πακέτα έφτασαν και επέστρεψαν χωρίς πρόβλημα σε χρόνο **65-67ms**. Ένα πακέτο χάθηκε ή άργησε (**Request timed out.**). Έτσι έχουμε 25% απώλεια και μέσο χρόνο **66ms**.

Αντί του domain name μπορούμε να χρησιμοποιήσουμε και μια IP διεύθυνση. Επιπλέον μπορούμε να χρησιμοποιήσουμε διάφορους διακόπτες ώστε να τροποιήσουμε τη λειτουργία του ping.

Αν θέλουμε να εκτελεστούν επαναλαμβανόμενα ping μέχρι να πατήσουμε Ctrl+C, πληκτρολογούμε:

```
ping –t x.x.x.x
```

Για να αλλάξουμε το προεπιλεγμένο μέγεθος των πακέτων από 32 (default τιμή) σε 64 bytes πληκτρολογούμε:

```
ping –l 64 x.x.x.x
```

Για να αλλάξουμε το προεπιλεγμένο πλήθος των πακέτων από 4 σε 10 πληκτρολογούμε:

```
ping –n 10 x.x.x.x
```

Για να αυξήσουμε το χρόνο αναμονής της απάντησης σε 2 sec, πληκτρολογούμε:

```
ping –w 2000 x.x.x.x
```

Μπορούμε, βέβαια, να συνδυάσουμε και πολλές επιλογές σε μία εντολή, π.χ.:

```
ping –n 10 –l 64 x.x.x.x
```

Ειδικές χρήσεις του ping

Κάνοντας *ping στον υπολογιστή μας*, στέλνονται τα πακέτα μέχρι την κάρτα δικτύου και επιστρέφουν. Αν όλα λειτουργούν σωστά και χωρίς προβλήματα, τότε η επιτυχημένη εκτέλεση του ping είναι ένδειξη καλής λειτουργίας της κάρτας δικτύου μας. Αν όχι, κάτι δε λειτουργεί σωστά στο υπολογιστή.

```
ping 127.0.0.1
```

Με την εντολή ping localhost εμφανίζεται το όνομα που έχει δοθεί στο υπολογιστή μας για να τον αναγνωρίζουν οι υπόλοιποι κόμβοι στο δίκτυο.

```
ping localhost
```

Κάνοντας ping <όνομα_υπολογιστή> στα αποτελέσματα φαίνεται η διεύθυνση IP του υπολογιστή που κάνουμε ping.

```
ping <όνομα_υπολογιστή>
```

Σφάλματα ping

Αν με τη βοήθεια του ping, βρεθεί ένας κόμβος ενεργός τότε δεν υπάρχει περίπτωση λάθους. Αν δεν ληφθεί απάντηση (ECHO_REPLY) από τον κόμβο προορισμού, τότε η απάντηση στην ερώτηση «Τι συμβαίνει;» είναι «άγνωστο».

Είναι δυνατόν να υπάρχει κανονική σύνδεση, η οποία μάλιστα να λειτουργεί κιόλας, και παρόλο αυτά να μην λαμβάνουμε απάντηση από τον παραλήπτη, πχ γιατί:

α) μπορεί ο παραλήπτης να βρίσκεται σε μακρινή απόσταση, με αποτέλεσμα να μην επαρκεί ο χρόνος αναμονής (διακόπτης –w), χωρίς, βέβαια, να αποκλείεται το γεγονός της κακής ή και καθόλου σύνδεσης

β) ο παραλήπτης ή κάποιο τείχος προστασίας (firewall), που παρεμβάλλεται στη διαδρομή, μπλοκάρει τα ICMP μηνύματα και έτσι οδηγεί εσφαλμένα στο συμπέρασμα ότι ο κόμβος είναι μη ενεργός (down). Αυτό συνήθως γίνεται ώστε οι κόμβοι να προστατεύονται από κακόβουλες επιθέσεις (κυρίως Denial-Of-Service).[1]

Traceroute

Η εντολή αυτή χρησιμοποιείται για την εύρεση *όλων των κόμβων ενός δικτύου από τους οποίους πρέπει να περάσει ένα πακέτο για να φτάσει στον τελικό προορισμό του*. Αυτό που κάνει ουσιαστικά είναι να στέλνει πακέτα UDP με συγκεκριμένο χρόνο ζωής (**TTL - Time To Live**) και να περιμένει πακέτα ICMP που να περιέχουν μήνυμα σφάλματος "ο χρόνος ζωής τελείωσε" (Time To Live exceeded in transit) ή "ο προορισμός δεν βρέθηκε" (Destination unreachable). Στο σημείο αυτό αξίζει να αναφερθεί ότι ο χρόνος ζωής (TTL - Time To Live) ενός πακέτου είναι ο μέγιστος αριθμός των κόμβων του δικτύου από τους οποίους θα πρέπει να περάσει έως ότου φτάσει στον προορισμό του. Εάν ένα πακέτο κατά την πορεία του στο δίκτυο περάσει από περισσότερους κόμβους απ' ότι αναγράφεται στο πεδίο TTL, τότε το πακέτο αυτομάτως απορρίπτεται και ο υπολογιστής ο οποίος διαπίστωσε το σφάλμα στέλνει ένα ICMP μήνυμα σφάλματος στον υπολογιστή που δημιούργησε το πακέτο.

Με την εντολή tracert μπορούμε να *καταγράψουμε την διαδρομή που ακολουθεί ένα πακέτο από τον υπολογιστή μας (αποστολέας) προς έναν υπολογιστή παραλήπτη*. Το tracrt μπορεί να μας πληροφορήσει σχετικά με *την IP διεύθυνση κάθε ενδιάμεσου δρομολογητή*. Επίσης μας παρέχει *χρόνους απόκρισης και το όνομα από κάθε δρομολογητή*. Σε κάποιες περιπτώσεις το tracert δεν

---

[1] Το ping του θανάτου (POD - *Ping Of Death*) είναι ένας τύπος επίθεσης σε έναν ηλεκτρονικό υπολογιστή. Η επίθεση Ping Of Death συντελείται όταν ένας ηλεκτρονικός υπολογιστής στέλνει κακοσχηματισμένα πακέτα ping σε έναν άλλο υπολογιστή με σκοπό να τον θέσει εκτός λειτουργίας.
Η επίθεση *Ping flood* ανήκει στην κατηγορία επιθέσεων άρνησης υπηρεσιών (DOS - Denial of Service) και περιλαμβάνει την συνεχή αποστολή πακέτων ping (ICMP Echo Request) από τον υπολογιστή του επιτιθέμενου προς τον υπολογιστή του αμυνόμενου. Για να επιτύχει αυτή η επίθεση θα πρέπει ο επιτιθέμενος να διαθέτει μεγαλύτερο bandwidth (εύρος ζώνης) από το θύμα.

επιστρέφει πληροφορίες για κάποιους δρομολογητές. Αυτό συμβαίνει διότι είτε περιορίζεται από κάποιο τοίχος προστασίας είτε κάποιος δρομολογητής αντιμετωπίζει σφάλμα υλικού.

Η εντολή στα windows είναι *tracert* και εκτελείται από cmd.

```
tracert google.gr
```

Η απάντηση που παίρνουμε είναι:

```
 Tracing route to google.gr [173.194.70.94]
 over a maximum of 30 hops:
  1    <1 ms    <1 ms    <1 ms  10.0.2.2
  2     1 ms     2 ms     1 ms  192.168.1.1
  3     9 ms     8 ms     9 ms  80.106.108.15
  4    12 ms     8 ms     9 ms  79.128.246.205
  5    16 ms    14 ms    16 ms  thes-crsb-ioan7609a-
1.backbone.otenet.net [79.12 8.228.153]
  6    15 ms    13 ms    12 ms  62.75.8.137
  7    61 ms    58 ms    60 ms  62.75.8.34
  8    67 ms    58 ms    58 ms  74.125.48.24
  9    63 ms    60 ms    60 ms  209.85.252.188
 10    61 ms    61 ms    59 ms  209.85.244.240
 11    60 ms    60 ms    59 ms  209.85.246.152
 12    64 ms    69 ms    60 ms  209.85.240.143
 13    60 ms    59 ms    59 ms  209.85.254.118
 14     *        *        *     Request timed out.
 15    62 ms    63 ms    62 ms  fa-in-f94.1e100.net
[173.194.70.94]  Trace complete.
```

Αν εκτελέσουμε επαναληπτικά την εντολή για τον ίδιο υπολογιστή προορισμού, δεν θα λάβουμε απαραίτητα την ίδια διαδρομή. Δοκιμάστε το.

Pathping

Το εργαλείο PathPing είναι ένα εργαλείο εντοπισμού διαδρομής που συνδυάζει τα χαρακτηριστικά του Ping και Tracert με πρόσθετες πληροφορίες. Το PathPing στέλνει για ορισμένο χρόνο πακέτα σε κάθε δρομολογητή στο δρόμο για έναν τελικό προορισμό, και στη συνέχεια υπολογίζει τα αποτελέσματα με βάση τα πακέτα που επιστρέφονται από κάθε hop. Το PathPing δείχνει το βαθμό της απώλειας πακέτων σε κάθε δεδομένο δρομολογητή ή σύνδεσμο, έτσι μπορείτε να εντοπίσετε ποιοι δρομολογητές ή συνδέσεις μπορεί να προκαλέσουν προβλήματα στο δίκτυο.

Εκτέλεση από cmd:

```
pathping google.gr
```

Το αποτέλεσμα που παίρνουμε είναι:

```
Tracing route to google.gr [173.194.70.94]
over a maximum of 30 hops:
 0  winxp-on-mac [10.0.2.15]
 1  10.0.2.2
 2  192.168.1.1
 3  80.106.108.15
 4  79.128.246.205
 5  thes-crsb-ioan7609a-1.backbone.otenet.net [79.128.228.153]
 6  62.75.8.137
 7  62.75.8.34
 8  74.125.48.24
 9  209.85.252.188
10  209.85.244.240
11  209.85.246.152
12  209.85.240.143
13  209.85.254.118
14     *        *        *
Computing statistics for 350 seconds...
           Source to Here   This Node/Link Hop  RTT    Lost/Sent = Pct
Lost/Sent = Pct  Address
  0                                           winxp-on-mac [10.0.2.15]
                                 0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  10.0.2.2
                                 0/ 100 =  0%   |
  2    3ms     5/ 100 =  5%     5/ 100 =  5%  192.168.1.1
                                 0/ 100 =  0%   |
  3   11ms     1/ 100 =  1%     1/ 100 =  1%  80.106.108.15
```

```
                                  0/ 100 =  0%   |
  4   10ms     0/ 100 =  0%     0/ 100 =  0%  79.128.246.205
                                  0/ 100 =  0%   |
  5   22ms     1/ 100 =  1%     1/ 100 =  1%  thes-crsb-ioan7609a-
1.backbone.ote net.net [79.128.228.153]
                                  0/ 100 =  0%   |
  6  ---     100/ 100 =100%   100/ 100 =100%  62.75.8.137
                                  0/ 100 =  0%   |
  7  ---     100/ 100 =100%   100/ 100 =100%  62.75.8.34
                                  0/ 100 =  0%   |
  8   61ms     2/ 100 =  2%     2/ 100 =  2%  74.125.48.24
                                  0/ 100 =  0%   |
  9   65ms     0/ 100 =  0%     0/ 100 =  0%  209.85.252.188
                                100/ 100 =100%   |
 10  ---     100/ 100 =100%     0/ 100 =  0%  209.85.244.240
                                  0/ 100 =  0%   |
 11  ---     100/ 100 =100%     0/ 100 =  0%  209.85.246.152
                                  0/ 100 =  0%   |
 12  ---     100/ 100 =100%     0/ 100 =  0%  209.85.240.143
                                  0/ 100 =  0%   |
 13  ---     100/ 100 =100%     0/ 100 =  0%  209.85.254.118
                                  0/ 100 =  0%   |
 14  ---     100/ 100 =100%     0/ 100 =  0%  winxp-on-mac [0.0.0.0]
Trace complete.
```

Τι συνέβη;
Όταν εκτελείται το PathPing, τα πρώτα αποτελέσματα που βλέπετε στη λίστα είναι η διαδρομή καθώς ελέγχεται για προβλήματα. Αυτό είναι το ίδιο μονοπάτι που εμφανίζεται μέσω Tracert. Το PathPing στη συνέχεια εμφανίζει ένα μήνυμα κατειλημμένης για τα επόμενα XX δευτερόλεπτα (απαιτεί 25 δευτερόλεπτα ανά hop). Κατά τη διάρκεια αυτής της περιόδου PathPing συγκεντρώνει πληροφορίες από όλους τους δρομολογητές που αναφέρθηκαν προηγουμένως και από τις συνδέσεις μεταξύ τους. Στο τέλος της περιόδου αυτής, εμφανίζει τα αποτελέσματα των δοκιμών.
Τα ποσοστά απωλειών που εμφανίζονται για τις συνδέσεις (που σημειώνονται ως "|" στη δεξιά στήλη) υποδεικνύουν απώλειες των πακέτων που προωθούνται κατά μήκος της διαδρομής. Η απώλεια αυτή υποδηλώνει σύνδεσμο υπό συμφόρηση.
Τα ποσοστά απώλειας που εμφανίζονται για δρομολογητές (που υποδεικνύεται από τις διευθύνσεις IP τους στη δεξιά στήλη) δείχνουν ότι οι εν λόγω δρομολογητές ενδέχεται να είναι υπερφορτωμένοι.

Εντολή netstat

Το netstat είναι ένα εργαλείο γραμμής εντολών που εμφανίζει τις συνδέσεις δικτύου (εισερχόμενες και εξερχόμενες), πίνακες δρομολόγησης, και άλλα στατιστικά ενός πρωτόκολλου δικτύου.

Βασική χρήση από cmd:
`netstat`
Δείχνει τις ενεργές TCP συνδέσεις.

Μερικοί χρήσιμοι διακόπτες:

`netstat -a`
Εμφανίσει ολες τις ενεργές TCP συνδέσεις και όλα τα TCP και UDP ports στα οποία *ακούει* ο υπολογιστής.

`netstat -an`
Εμφανίσει ό,τι και η εντολή `netstat -a`, αλλά οι διευθύνσεις και οι θύρες εμφανίζονται αριθμητικά όχι ονομαστικά.

`netstat -ao`
Εμφανίσει ό,τι και η εντολή `netstat -a`, και επιπλέον το process ID (PID) για κάθε σύνδεση.

`netstat -ap udp`
Εμφανίσει ό,τι και η εντολή `netstat -a`, αλλά μόνο για το πρωτόκολλο udp.

`netstat -ρ`
Εμφανίζει τα network interfaces του υπολογιστή και τους πίνακες δρομολόγησης.

`netstat -e`

Εμφανίζει τα στατιστικά χρήσης του Ethernet, όπως το πλήθος πακέτων και bytes που έχουν σταλεί ή ληφθεί.

`netstat -s`
Εμφανίζει στατιστικά ανά πρωτόκολλο (TCP, UDP, ICMP και IP).

`netstat –sp icmp`
Εμφανίζει στατιστικά μόνο για το πρωτόκολλο ICMP.

`netstat -b`
Δείχνει τις ενεργές TCP συνδέσεις και το όνομα τουυ προγράμματος που τις χειρίζεται.

`netstat 5`
Δείχνει τις ενεργές TCP συνδέσεις ανά 5 δευτερόλεπτα, μέχρι να πατήσουμε Ctrl+C.

Οι διακόπτες του netstat μπορούν να συνδυαστούν μεταξύ τους.

Αν θέλουμε να αποθηκεύσουμε σε ένα αρχείο τα προγράμματα που δημιουργούν connections στον υπολογιστή μας για να τα ελέγξουμε δίνουμε την εντολή:
`netstat -ba >> conns.txt`

Πηγές:
1. http://el.wikipedia.org/wiki/ICMP
2. http://www.teicm.gr/icd/staff/chilas/files/Lab_DI/11_Εντολές%20ελέγχου.pdf
3. http://aetos.it.teithe.gr/~dchaidar/arxeia/diktua/Lab8_commands1.pdf
4. http://el.wikipedia.org/wiki/Ping_Of_Death
5. http://support.microsoft.com/kb/314067/el
6. http://technet.microsoft.com/en-us/library/bb490947.aspx
7. http://en.wikipedia.org/wiki/Netstat
8.