

Ομάδα: netmg034
Μιχάλης Παπαδόπουλος 03114702
Χαράλαμπος Κάρδαρης 03114074

Διαχείριση Δικτύων – Ευφυή Δίκτυα

2η Ομάδα Ασκήσεων

Domain Name System (DNS)

Βοηθήματα για την πραγματοποίηση της άσκησης:

- A. Θα πρέπει να χρησιμοποιήσετε το *unix program 'dig'*. Για το πώς χρησιμοποιείται το συγκεκριμένο πρόγραμμα καθώς και οποιαδήποτε άλλη *unix* εντολή κάνετε *'man <όνομα_εντολής>'* (π.χ. *man dig*) στο *shell* σας.
- B. RFC 1034 "DOMAIN NAMES - CONCEPTS AND FACILITIES"
<http://tools.ietf.org/html/rfc1034>
- C. RFC 1035 "DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION"
<http://tools.ietf.org/html/rfc1035>

1. Κάνετε στον dns-server του Ε.Μ.Π “ulysses.noc.ntua.gr” ένα A-type query για τον node “danaos.cslab.ntua.gr”.
- (α) Σας επέστρεψε μια IP διεύθυνση ή και κάποιες άλλες πληροφορίες για το συγκεκριμένο node ; Εξηγείστε τις συμπληρωματικές πληροφορίες που τυχόν σας επιστρέφει ως απάντηση ο dns-server ulysses.noc.ntua.gr για το συγκεκριμένο node.

```
; <<>> DiG 9.10.3-P4-Debian <<>> @ulysses.noc.ntua.gr danaos.cslab.ntua.gr A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40915
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 6, ADDITIONAL: 8

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;danaos.cslab.ntua.gr.          IN      A

;; ANSWER SECTION:
danaos.cslab.ntua.gr.  86400  IN      CNAME    danaos.cslab.ece.ntua.gr.
danaos.cslab.ece.ntua.gr. 86400  IN      A        147.102.3.1

;; AUTHORITY SECTION:
cslab.ece.ntua.gr.    86400  IN      NS       skiathos.cslab.ece.ntua.gr.
cslab.ece.ntua.gr.    86400  IN      NS       diomedes.noc.ntua.gr.
cslab.ece.ntua.gr.    86400  IN      NS       achilles.noc.ntua.gr.
cslab.ece.ntua.gr.    86400  IN      NS       danaos.cslab.ece.ntua.gr.
cslab.ece.ntua.gr.    86400  IN      NS       scirouter.cslab.ece.ntua.gr.
cslab.ece.ntua.gr.    86400  IN      NS       ulysses.noc.ntua.gr.

;; ADDITIONAL SECTION:
ulysses.noc.ntua.gr.  86400  IN      A        147.102.222.230
achilles.noc.ntua.gr. 86400  IN      A        147.102.222.210
diomedes.noc.ntua.gr. 86400  IN      A        147.102.222.220
skiathos.cslab.ece.ntua.gr. 86400 IN      A        147.102.3.40
scirouter.cslab.ece.ntua.gr. 86400 IN      A        147.102.4.1
ulysses.noc.ntua.gr.  86400  IN      AAAA     2001:648:2000:de::230
achilles.noc.ntua.gr. 86400  IN      AAAA     2001:648:2000:de::210

;; Query time: 0 msec
;; SERVER: 147.102.222.230#53(147.102.222.230)
;; WHEN: Thu Oct 25 12:43:50 EEST 2018
;; MSG SIZE rcvd: 365
```

Ο DNS-Server ulysses.noc.ntua.gr επιστρέφει στο ANSWER SECTION δυο (2) εγγραφές για το node danaos.cslab.ntua.gr.

Αρχικά βλέπουμε ότι το danaos.cslab.ntua.gr αποτελεί ALIAS (CNAME) για το full name danaos.cslab.ece.ntua.gr το οποίο έχει IP: 147.102.3.1

(β) Από τις τυχόν επιπρόσθετες πληροφορίες που σας έχει επιστρέψει μπορείτε να διαπιστώσετε ποιό name-servers είναι υπεύθυνοι (αρμόδιοι) για το domain “cslab.ece.ntua.gr” ;

Στο AUTHORITY SECTION μπορούμε να δούμε τους servers που είναι αρμόδιοι για το συγκεκριμένο domain με IP: 147.102.3.1

- **skiathos.cslab.ece.ntua.gr.**
- **diomedes.noc.ntua.gr.**
- **achilles.noc.ntua.gr.**
- **danaos.cslab.ece.ntua.gr.**
- **scirouter.cslab.ece.ntua.gr.**
- **ulysses.noc.ntua.gr.**

2. Κάνετε ένα SOA-query στον dns-server “ulysses.noc.ntua.gr” και βρείτε τον name-server που είναι υπεύθυνος για τη ζώνη “netmode.ece.ntua.gr”. Εξηγείστε μας τι άλλες πληροφορίες περιέχονται στο SOA record.

```
$ dig @ulysses.noc.ntua.gr netmode.ece.ntua.gr SOA
```

```
; <<>> DiG 9.10.3-P4-Debian <<>> @ulysses.noc.ntua.gr netmode.ece.ntua.gr SOA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49210
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 6

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;netmode.ece.ntua.gr.      IN      SOA

;; ANSWER SECTION:
netmode.ece.ntua.gr.  86400  IN      SOA      electra.netmode.ece.ntua.gr. admin.netmode.ntua.gr.
2018102501 43200 3600 2592000 86400

;; AUTHORITY SECTION:
netmode.ece.ntua.gr.  86400  IN      NS       electra.netmode.ece.ntua.gr.
netmode.ece.ntua.gr.  86400  IN      NS       achilles.noc.ntua.gr.
netmode.ece.ntua.gr.  86400  IN      NS       ulysses.noc.ntua.gr.

;; ADDITIONAL SECTION:
electra.netmode.ece.ntua.gr. 86400 IN  A       147.102.13.34
ulysses.noc.ntua.gr. 86400 IN  A       147.102.222.230
achilles.noc.ntua.gr. 86400 IN  A       147.102.222.210
ulysses.noc.ntua.gr. 86400 IN  AAAA    2001:648:2000:de::230
achilles.noc.ntua.gr. 86400 IN  AAAA    2001:648:2000:de::210

;; Query time: 0 msec
;; SERVER: 147.102.222.230#53(147.102.222.230)
;; WHEN: Thu Oct 25 16:45:46 EEST 2018
;; MSG SIZE rcvd: 273
```

Στο ANSWER SECTION μπορούμε να δούμε τον main server που είναι αρμόδιος για τη ζώνη του συγκεκριμένου domain:

- **electra.netmode.ece.ntua.gr.**

Στο AUTHORITY SECTION μπορούμε να δούμε τους servers που είναι αρμόδιοι για το συγκεκριμένο domain:

- **electra.netmode.ece.ntua.gr**
- **achilles.noc.ntua.gr.**
- **ulysses.noc.ntua.gr.**

Στο ADDITIONAL SECTION μπορούμε να δούμε τις IPs των name servers που είναι αρμόδιοι για το συγκεκριμένο domain.

3. Κάνετε το απαιτούμενο query στον name-server “electra.netmode.ntua.gr” για να αποκτήσετε το host-name του node 147.102.13.200. Μπορείτε να κάνετε κάποια υπόθεση βασιζόμενη στην απάντηση του DNS server για τον τύπο συσκευής που κατέχει την συγκεκριμένη IP address ?

```
$ dig @electra.netmode.ntua.gr -x 147.102.13.200 PTR
```

```
; <<>> DiG 9.10.3-P4-Debian <<>> @electra.netmode.ntua.gr -x 147.102.13.200
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43699
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1680
;; QUESTION SECTION:
;200.13.102.147.in-addr.arpa. IN PTR

;; ANSWER SECTION:
200.13.102.147.in-addr.arpa. 86400 IN PTR router.netmode.ece.ntua.gr.

;; Query time: 4 msec
;; SERVER: 147.102.13.34#53(147.102.13.34)
;; WHEN: Thu Oct 25 17:22:55 EEST 2018
;; MSG SIZE rcvd: 96
```

Με βάση το host name της συσκευής μπορούμε να υποθέσουμε ότι είναι ένας router.

4. Έστω ότι έχουμε ένα node που έχει πρόσβαση στο Internet και του έχει αποδοθεί Public IP Address από το Διαχειριστή του Domain του. Υπάρχει ενδεχόμενο να μην υφίσταται κανένα Resource Record σχετικά με το συγκεκριμένο node στον name-server του Domain που ανήκει ;

Ναι, υπάρχει το ενδεχόμενο αυτό, δηλαδή να απουσιάζει το Resource Record του node στον αρμόδιο name-server του domain που ανήκει, όταν ο διαχειριστής του δικτύου δεν του έχει αναθέσει κάποιο domain name με βάση τη δενδρική δομή στο αρχείο ζώνης.

Αυτό έχει ως αποτέλεσμα να μην μπορεί να εμφανίσει πληροφορίες σχετικά με το node ο name-server

5. Ποιοί είναι οι mail-servers του domain “ntua.gr”; Παρατηρείτε η απάντηση του name-server να περιλαμβάνει κάποιο επιπρόσθετο πεδίο σε σχέση με απαντήσεις που αφορούν A-records ;

```
; <<>> DiG 9.10.3-P4-Debian <<>> ntua.gr MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56883
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 5, ADDITIONAL: 10
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ntua.gr.                IN      MX
```

```
;; ANSWER SECTION:
ntua.gr.      86394 IN      MX      20 achilles.noc.ntua.gr.
ntua.gr.      86394 IN      MX      20 ulysses.noc.ntua.gr.
ntua.gr.      86394 IN      MX      20 diomedes.noc.ntua.gr.
```

```
;; AUTHORITY SECTION:
ntua.gr.      73611 IN      NS      sns0.grnet.gr.
ntua.gr.      73611 IN      NS      achilles.noc.ntua.gr.
ntua.gr.      73611 IN      NS      ulysses.noc.ntua.gr.
ntua.gr.      73611 IN      NS      sns1.grnet.gr.
ntua.gr.      73611 IN      NS      diomedes.noc.ntua.gr.
```

```
;; ADDITIONAL SECTION:
ulysses.noc.ntua.gr. 10672 IN      A        147.102.222.230
ulysses.noc.ntua.gr. 9625  IN      AAAA     2001:648:2000:de::230
diomedes.noc.ntua.gr. 9625  IN      A        147.102.222.220
achilles.noc.ntua.gr. 11063 IN      A        147.102.222.210
achilles.noc.ntua.gr. 9625  IN      AAAA     2001:648:2000:de::210
sns1.grnet.gr.      1240  IN      A        83.212.5.22
sns1.grnet.gr.      7657  IN      AAAA     2001:648:2ffc:112::2
sns0.grnet.gr.      1240  IN      A        83.212.5.18
sns0.grnet.gr.      7657  IN      AAAA     2001:648:2ffc:111::2
```

```
;; Query time: 0 msec
;; SERVER: 147.102.13.10#53(147.102.13.10)
;; WHEN: Thu Oct 25 12:58:25 EEST 2018
;; MSG SIZE rcvd: 392
```

Απο την απάντηση στο QUERY μας (ANSWER SECTION) βλέπουμε τους mail-servers που είναι υπεύθυνοι για το domain ntua.gr.

- diomedes.noc.ntua.gr.
- ulyssees.noc.ntua.gr.
- achilles.noc.ntua.gr.
-

Διπλά στις εγγραφές παρατηρούμε έναν αριθμό (20) που – μια μετρική για το priority των mail-servers, που στη συγκεκριμένη περίπτωση είναι όλοι ισοτιμοί.

Ο αριθμός αυτός δεν παρατηρείται στις απαντήσεις των Α-ερωτήσεων.

6. Κάνετε A-type query για το node “smtp.hol.gr”, το οποίο αποτελεί SMTP-server της HOL. Τι παρατηρείτε; Τι σκοπό εξυπηρετούν οι πολλαπλές εγγραφές ;

```
$ dig smtp.hol.gr A
```

```
; <<>> DiG 9.10.3-P4-Debian <<>> smtp.hol.gr A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50681
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 4

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
smtp.hol.gr.          IN      A

;; ANSWER SECTION:
smtp.hol.gr.          7200    IN      A      194.30.193.54
smtp.hol.gr.          7200    IN      A      194.30.193.52

;; AUTHORITY SECTION:
hol.gr.               7200    IN      NS      ns2.hol.gr.
hol.gr.               7200    IN      NS      ns0.hol.gr.
hol.gr.               7200    IN      NS      ns1.hol.gr.

;; ADDITIONAL SECTION:
ns2.hol.gr.           4105    IN      A      194.30.220.118
ns1.hol.gr.           446     IN      A      194.30.220.119
ns0.hol.gr.           2513    IN      A      194.30.220.110

;; Query time: 6 msec
;; SERVER: 147.102.13.10#53(147.102.13.10)
;; WHEN: Thu Oct 25 17:26:18 EEST 2018
;; MSG SIZE rcvd: 174
```

Παρατηρούμε ότι έχουμε μια διπλή εγγραφή για το συγκεκριμένο domain name. Τέτοιες πολλαπλές εγγραφές υπάρχουν ως μέτρο για την εξασφάλιση της δυνατότητας ενός domain name να απαντάει (σε περίπτωση που μια IP είναι μη διαθέσιμη, γίνονται τα ερωτήματα στην άλλη) καθώς και για διαμοιρασμό του φόρτου ερωτημάτων σε ένα domain name.

7. (α) Βρείτε τους root name-servers της ιεραρχίας του Domain Name System. Ακολουθώντας βρείτε ποιούς name-servers είναι υπεύθυνοι για την ζώνη “gr”, για την ζώνη “ntua.gr” και την ζώνη “netmode.ntua.gr”.

```
$ dig
```

```
; <<>> DiG 9.10.3-P4-Debian <<>>
```

```
;; global options: +cmd
```

```
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37232
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27
```

```
;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags:; udp: 4096
```

```
;; QUESTION SECTION:
```

```
.;                IN      NS
```

```
;; ANSWER SECTION:
```

```
.          328362 IN      NS      k.root-servers.net.
.          328362 IN      NS      e.root-servers.net.
.          328362 IN      NS      d.root-servers.net.
.          328362 IN      NS      b.root-servers.net.
.          328362 IN      NS      m.root-servers.net.
.          328362 IN      NS      l.root-servers.net.
.          328362 IN      NS      i.root-servers.net.
.          328362 IN      NS      c.root-servers.net.
.          328362 IN      NS      h.root-servers.net.
.          328362 IN      NS      g.root-servers.net.
.          328362 IN      NS      a.root-servers.net.
.          328362 IN      NS      j.root-servers.net.
.          328362 IN      NS      f.root-servers.net.
```


:: ADDITIONAL SECTION:

```
f.root-servers.net. 12220 IN A 192.5.5.241
f.root-servers.net. 12220 IN AAAA 2001:500:2f::f
a.root-servers.net. 501199 IN A 198.41.0.4
a.root-servers.net. 12220 IN AAAA 2001:503:ba3e::2:30
l.root-servers.net. 12220 IN A 199.7.83.42
l.root-servers.net. 12220 IN AAAA 2001:500:9f::42
d.root-servers.net. 12220 IN A 199.7.91.13
d.root-servers.net. 12220 IN AAAA 2001:500:2d::d
c.root-servers.net. 12220 IN A 192.33.4.12
c.root-servers.net. 12220 IN AAAA 2001:500:2::c
g.root-servers.net. 161174 IN A 192.112.36.4
g.root-servers.net. 12220 IN AAAA 2001:500:12::d0d
k.root-servers.net. 588614 IN A 193.0.14.129
k.root-servers.net. 12220 IN AAAA 2001:7fd::1
m.root-servers.net. 12220 IN A 202.12.27.33
m.root-servers.net. 12220 IN AAAA 2001:dc3::35
e.root-servers.net. 12220 IN A 192.203.230.10
e.root-servers.net. 12220 IN AAAA 2001:500:a8::e
i.root-servers.net. 444220 IN A 192.36.148.17
i.root-servers.net. 12220 IN AAAA 2001:7fe::53
b.root-servers.net. 12220 IN A 199.9.14.201
b.root-servers.net. 12220 IN AAAA 2001:500:200::b
h.root-servers.net. 12220 IN A 198.97.190.53
h.root-servers.net. 12220 IN AAAA 2001:500:1::53
j.root-servers.net. 12220 IN A 192.58.128.30
j.root-servers.net. 12220 IN AAAA 2001:503:c27::2:30
```

:: Query time: 0 msec

:: SERVER: 147.102.13.10#53(147.102.13.10)

:: WHEN: Thu Oct 25 17:36:48 EEST 2018

:: MSG SIZE rcvd: 811

Από το ANSWER SECTION βλέπουμε τους root servers:

- **k.root-servers.net.**
- **e.root-servers.net.**
- **d.root-servers.net.**
- **b.root-servers.net.**
- **m.root-servers.net.**
- **l.root-servers.net.**
- **i.root-servers.net.**
- **c.root-servers.net.**
- **h.root-servers.net.**
- **g.root-servers.net.**
- **a.root-servers.net.**
- **j.root-servers.net.**
- **f.root-servers.net.**

\$dig gr NS

```
; <<>> DiG 9.10.3-P4-Debian <<>> gr NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23202
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 11
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;gr.                IN      NS
```

```
;; ANSWER SECTION:
gr.                23163 IN      NS      gr-d.ics.forth.gr.
gr.                23163 IN      NS      gr-c.ics.forth.gr.
gr.                23163 IN      NS      grdns.ics.forth.gr.
gr.                23163 IN      NS      gr-at.ics.forth.gr.
gr.                23163 IN      NS      estia.ics.forth.gr.
gr.                23163 IN      NS      gr-m.ics.forth.gr.
```

```
;; ADDITIONAL SECTION:
gr-c.ics.forth.gr. 38584 IN      A       194.0.1.25
gr-c.ics.forth.gr. 75924 IN      AAAA    2001:678:4::19
grdns.ics.forth.gr. 77401 IN      A       139.91.1.1
gr-d.ics.forth.gr. 57460 IN      A       194.0.11.102
gr-d.ics.forth.gr. 75924 IN      AAAA    2001:678:e:102::53
gr-m.ics.forth.gr. 65362 IN      A       194.0.4.10
gr-m.ics.forth.gr. 75924 IN      AAAA    2001:678:7::4:10
estia.ics.forth.gr. 8840  IN      A       139.91.191.3
estia.ics.forth.gr. 75924 IN      AAAA    2001:648:2c30::191:3
gr-at.ics.forth.gr. 89139 IN      A       78.104.145.227
```

```
;; Query time: 0 msec
;; SERVER: 147.102.13.10#53(147.102.13.10)
;; WHEN: Thu Oct 25 17:40:25 EEST 2018
;; MSG SIZE rcvd: 366
```

\$dig ntua.gr NS

```
; <<>> DiG 9.10.3-P4-Debian <<>> ntua.gr NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30819
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 10
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ntua.gr.                IN      NS
```

```
;; ANSWER SECTION:
ntua.gr.                56577  IN      NS      sns0.grnet.gr.
ntua.gr.                56577  IN      NS      ulysses.noc.ntua.gr.
ntua.gr.                56577  IN      NS      diomedes.noc.ntua.gr.
ntua.gr.                56577  IN      NS      achilles.noc.ntua.gr.
ntua.gr.                56577  IN      NS      sns1.grnet.gr.
```

```
;; ADDITIONAL SECTION:
ulysses.noc.ntua.gr.    80151  IN      A        147.102.222.230
ulysses.noc.ntua.gr.    79129  IN      AAAA     2001:648:2000:de::230
sns1.grnet.gr.          70615  IN      A        83.212.5.22
sns1.grnet.gr.          58583  IN      AAAA     2001:648:2ffc:112::2
sns0.grnet.gr.          70615  IN      A        83.212.5.18
sns0.grnet.gr.          58583  IN      AAAA     2001:648:2ffc:111::2
diomedes.noc.ntua.gr.   79129  IN      A        147.102.222.220
achilles.noc.ntua.gr.   82996  IN      A        147.102.222.210
achilles.noc.ntua.gr.   79129  IN      AAAA     2001:648:2000:de::210
```

```
;; Query time: 0 msec
;; SERVER: 147.102.13.10#53(147.102.13.10)
;; WHEN: Thu Oct 25 17:42:20 EEST 2018
;; MSG SIZE rcvd: 344
```

\$dig netmode.ntua.gr NS

; <<>> DiG 9.10.3-P4-Debian <<>> netmode.ntua.gr NS

:: global options: +cmd

:: Got answer:

:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34643

:: flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 6

:: OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4096

:: QUESTION SECTION:

;netmode.ntua.gr. IN NS

:: ANSWER SECTION:

netmode.ntua.gr. 2831 IN NS **achilles.noc.ntua.gr.**

netmode.ntua.gr. 2831 IN NS **ulysses.noc.ntua.gr.**

netmode.ntua.gr. 2831 IN NS **electra.netmode.ece.ntua.gr.**

:: ADDITIONAL SECTION:

ulysses.noc.ntua.gr. 79995 IN A 147.102.222.230

ulysses.noc.ntua.gr. 78973 IN AAAA 2001:648:2000:de::230

electra.netmode.ece.ntua.gr. 8382 IN A 147.102.13.34

achilles.noc.ntua.gr. 82840 IN A 147.102.222.210

achilles.noc.ntua.gr. 78973 IN AAAA 2001:648:2000:de::210

:: Query time: 0 msec

:: SERVER: 147.102.13.10#53(147.102.13.10)

:: WHEN: Thu Oct 25 17:44:56 EEST 2018

:: MSG SIZE rcvd: 231

(β) Δοκιμάστε να τρέξετε την εντολή ‘dig +trace netmode.ntua.gr’. Από ποιο name-server πήρατε την κάθε απάντηση ;

```
; <<>> DiG 9.10.3-P4-Debian <<>> +trace netmode.ntua.gr
;; global options: +cmd
.          327828 IN      NS      g.root-servers.net.
.          327828 IN      NS      l.root-servers.net.
.          327828 IN      NS      m.root-servers.net.
.          327828 IN      NS      e.root-servers.net.
.          327828 IN      NS      f.root-servers.net.
.          327828 IN      NS      b.root-servers.net.
.          327828 IN      NS      k.root-servers.net.
.          327828 IN      NS      j.root-servers.net.
.          327828 IN      NS      a.root-servers.net.
.          327828 IN      NS      i.root-servers.net.
.          327828 IN      NS      c.root-servers.net.
.          327828 IN      NS      h.root-servers.net.
.          327828 IN      NS      d.root-servers.net.
.          414265 IN      RRSIG   NS 8 0 518400 20181106050000 20181024040000 2134 .
U+MGSYDgKo+5jyYLe+S79ElGmlL47I9evDL4rBfqHQMFTnj5ygh9xzK+
6IQMTIppGB5oB7w7LAQ2bpu5Fzkc23jXh8icWyFDFJv4UjEFlOMUVYmU
Xe8xBpHhZl1mFShXoNDnOWOtLgEjDDjzBNqnGDKbRpjD+oesysqP28S
tipkyErUvzWEOqXtmsfR46j/ihaSX8D49CKJ76fEndQzfTAVForOrcgW
yYxUZhboSetZKTESpamdqsOGMREN7XEB1n3VXblzs0H9aC/L/VburAzU
vGk8/RWLZZwm/hQMjbsLlu3JzPBtjZyz2fNEJMyEChsnjmFafGAjj4cc gMQj/Q==
;; Received 1097 bytes from 147.102.13.10#53(147.102.13.10) in 0 ms

gr.         172800 IN      NS      gr-c.ics.forth.gr.
gr.         172800 IN      NS      gr-d.ics.forth.gr.
gr.         172800 IN      NS      gr-m.ics.forth.gr.
gr.         172800 IN      NS      estia.ics.forth.gr.
gr.         172800 IN      NS      gr-at.ics.forth.gr.
gr.         172800 IN      NS      grdns.ics.forth.gr.
gr.         86400 IN      DS      35136 7 2
F7BF4C362B838C2069C9083FD38846BBB5D79EDBDE298F9268997307 EA7DD5C3
gr.         86400 IN      RRSIG   DS 8 1 86400 20181107050000 20181025040000 2134 .
krYtnAqebBce4APqLBYsH3WnTWZjv5/bGM9Y1dmewskjnHKkmvS2yl/K
9lWJ+NfzrsGxhp/3l7rbWv7G/fvWG3TPLLJ0zr5nnL4MMxgoZFU7lsr7
tx/p8fLws/zsV/OXXV1/LVlrsJunVpn05k72VUCYl4FZWvy9Td1yeD3S
JBgLiBNLHsy6c+xT68M5bFi3rHQbAAfs9xQjTiLQH6DQYAkUGd/Y12
sV9NF8WavRbjlBEHgOshCBBxBc9SIW3v43/ekJx0eJTspAUffgsQ05br
Thzh9jcs6EN8qMYfutrChGkVd7Fr14YqrvMU5D/DmwwBiRZ5Wun/m0dn lAHrUQ==
;; Received 714 bytes from 192.5.5.241#53(f.root-servers.net) in 2 ms

ntua.gr.    10800 IN      NS      sns0.grnet.gr.
ntua.gr.    10800 IN      NS      sns1.grnet.gr.
ntua.gr.    10800 IN      NS      ulysses.noc.ntua.gr.
ntua.gr.    10800 IN      NS      achilles.noc.ntua.gr.
ntua.gr.    10800 IN      NS      diomedes.noc.ntua.gr.
e5housd976jc4sbdh69jcejib7h0fh77.gr. 1800 IN NSEC3 1 1 10 BEEF
E5SU995F3VVTU91L67CESCJ4BHMU48C6 NS SOA RRSIG DNSKEY NSEC3PARAM
e5housd976jc4sbdh69jcejib7h0fh77.gr. 1800 IN RRSIG NSEC3 7 2 1800 20181124120143
20181025120143 7835 gr.
YnHiRGsxV5p6eM1NsEl2mc2anHEzAhOKXyigZ/tcXFyFVyeW7rtasJXU
HMRjyAdVvtG5s4dVMQVKECwZduP48sVz9ab2vRbdD6VAHqdBpKZD7pY4
sUzfY84ekY02+IyPNL3gUij67v9zK3/TwEN1uTV1jUE6vzfYdxACPcN5 14c=
n8ev6fgrf9b1ot00nrehrm8kmv5rleng.gr. 1800 IN NSEC3 1 1 10 BEEF
N92S6CUR4GAJRHMI8OSKSRNEFKHI7O0K DNAME RRSIG
```

n8ev6fgrf9b1ot00nrehrm8kmv5rleng.gr. 1800 IN RRSIG NSEC3 7 2 1800 20181124120143 20181025120143 7835 gr. KMjRSdgIcfYbc8y04bx4Mayg+5sxxgKsjjE6UeHPQVE+L3dnskN8YUP/IL5uE+cdCJy5+zqSgM/t64Welu0csttAX+1tDQXe8COkrocngF7KsbUf XHtJkNuYmIwxVB4P0YM1VNaLQ8VDxNKxqJ6AGGNriC3eHwYvbzOSlavJ UKk= ;; Received 695 bytes from 78.104.145.227#53(**gr-at.ics.forth.gr**) in 28 ms

netmode.ntua.gr. 86400 IN A 147.102.222.196
netmode.ntua.gr. 86400 IN A 147.102.222.195
netmode.ntua.gr. 86400 IN NS achilles.noc.ntua.gr.
netmode.ntua.gr. 86400 IN NS ulysses.noc.ntua.gr.
netmode.ntua.gr. 86400 IN NS electra.netmode.ece.ntua.gr.
;; Received 263 bytes from 147.102.222.230#53(**ulysses.noc.ntua.gr**) in 0 ms

Το option +trace εμφανίζει στο τερματικό όλες τις ερωτήσεις που κάνει η dig σε διαφορετικούς name servers για να πάρει απάντηση. Την τελική απάντηση στην περίπτωση μας την παίρνει από τον name server του ntua **ulysses.noc.ntua.gr**.

Τα προηγούμενα βήματα είναι να πάρει από τον αντίστοιχο name server μια απάντηση ως πριν το ποια ομάδα servers να ρωτήσει στο επόμενο βήμα.

Οι name servers που δίνουν απάντηση είναι με τη σειρά

147.102.13.10 → f.root-servers.net → gr-at.ics.forth.gr → ulysses.noc.ntua.gr

8. Κάνετε δύο διαδοχικά A-type query με ενδιάμεση παύση μερικών δευτερολέπτων στον name-server “electra.netmode.ntua.gr” για τον node “space.netmode.ece.ntua.gr”. Κάνετε την ίδια διαδικασία για τον node “achilles.noc.ntua.gr”. Τι διαφορές παρατηρείτε όσον αφορά τα A-type Resource Records στις δυο περιπτώσεις, όσον αφορά το TTL; Εξηγήστε.

```
netmg034@maria:~/lab2$ dig @electra.netmode.ntua.gr space.netmode.ece.ntua.gr >
                                                    2.8.1.1
netmg034@maria:~/lab2$ dig @electra.netmode.ntua.gr space.netmode.ece.ntua.gr A >
                                                    2.8.1.2
netmg034@maria:~/lab2$ dig @electra.netmode.ntua.gr achilles.noc.ntua.gr A > 2.8.2.1
netmg034@maria:~/lab2$ dig @electra.netmode.ntua.gr achilles.noc.ntua.gr A > 2.8.2.2

netmg034@maria:~/lab2$ diff 2.8.1.*
6c6
< ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38004
---
> ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32400
19c19
< ;; WHEN: Thu Oct 25 13:10:57 EEST 2018
---
> ;; WHEN: Thu Oct 25 13:12:22 EEST 2018
```

Δεν παρατηρείται κάποια αλλαγή στο TTL για τις απαντήσεις του domain space.netmode.ece.ntua.gr και μάλλον ο name-server electra.netmode.ntua.gr είναι αρμόδιος εξυπηρέτησης για το node space.netmode.ece.ntua.gr .

```
netmg034@maria:~/lab2$ diff 2.8.2.*
6c6
< ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36661
---
> ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39055
15c15
< achilles.noc.ntua.gr. 44525 IN A 147.102.222.210
---
> achilles.noc.ntua.gr. 44512 IN A 147.102.222.210
18,20c18,20
< noc.ntua.gr. 44525 IN NS ulysses.noc.ntua.gr.
< noc.ntua.gr. 44525 IN NS achilles.noc.ntua.gr.
< noc.ntua.gr. 44525 IN NS diomedes.noc.ntua.gr.
---
> noc.ntua.gr. 44512 IN NS ulysses.noc.ntua.gr.
> noc.ntua.gr. 44512 IN NS achilles.noc.ntua.gr.
> noc.ntua.gr. 44512 IN NS diomedes.noc.ntua.gr.
23,26c23,26
< ulysses.noc.ntua.gr. 46310 IN A 147.102.222.230
< diomedes.noc.ntua.gr. 45666 IN A 147.102.222.220
< ulysses.noc.ntua.gr. 46310 IN AAAA 2001:648:2000:de::230
< achilles.noc.ntua.gr. 44525 IN AAAA 2001:648:2000:de::210
---
> ulysses.noc.ntua.gr. 46297 IN A 147.102.222.230
> diomedes.noc.ntua.gr. 45653 IN A 147.102.222.220
> ulysses.noc.ntua.gr. 46297 IN AAAA 2001:648:2000:de::230
> achilles.noc.ntua.gr. 44512 IN AAAA 2001:648:2000:de::210
28c28
< ;; Query time: 7 msec
---
> ;; Query time: 1 msec
30c30
```

< ;; WHEN: Thu Oct 25 13:11:33 EEST 2018

> ;; WHEN: Thu Oct 25 13:11:46 EEST 2018

Αντίθετα, στην περίπτωση του node `achilles.noc.ntua.gr` το TTL των εγγραφών μειώνεται από 44525 σε 44512 με αποτέλεσμα να καταλαβαίνουμε ότι ο server `achilles.noc.ntua.gr` δεν είναι authoritative server για το συγκεκριμένο node.

9. Θεωρείστε ότι είστε διαχειριστής του web-site “www.example.com” και θέλετε να το μετακινήσετε σε ένα web-server με διαφορετική IP address από τον αρχικό web-server.
- (α) Τι αλλαγές θα κάνατε πριν την μεταφορά του web-site στο A-type Resource Record του “www.example.com”;
- (β) Μετά την ολοκλήρωση της μεταφοράς του web-site στο νέο web-server πως θα διαμορφωθεί το νέο A-type record;
- (Θεωρείστε ότι το αρχικό Resource Record είναι της μορφής “www.example.com. 172800 IN A 150.123.43.15”)

(a) Πριν αλλάξουμε την IP address στο zone file του server, είναι καλή πρακτική να μειώσουμε αρχικά το TTL σε μια πολύ μικρή τιμή για μια πιο smooth ανανέωση των εγγραφών στους υπόλοιπους εξυπηρετητές. Στη συνέχεια αλλάζουμε την διεύθυνση IP και επαναφέρουμε την αρχική τιμή TTL στον authoritative server.

(b)	www.example.com.	172800	IN	A	150.123.43.15	– BEFORE
	www.example.com.	172800	IN	A	<NEW IP ADDRESS>	– AFTER

10. Γράψτε ένα script (sh/bash, csh, tcsh, perl,...) το οποίο να δίνει την αντιστοιχία όλων των IP διευθύνσεων του υποδικτύου 147.102.13.0/24 με το hostname τους, κάνοντας χρήση PTR type queries (χρησιμοποιείστε το πρόγραμμα *host* αντί για το *dig*). Πως θα μπορούσαμε να παίρναμε το ίδιο αποτέλεσμα με την χρήση μόνο μίας εντολής; (*Hint: AXFR type*)

```
#!/bin/bash
```

```
for i in {0..254}  
do  
    name=$(host 147.102.13.$i | awk '{print $5}')  
    echo 147.102.13.$i $name >> hostnames.txt  
done
```

Η διεύθυνση 147.102.13.255 είναι η διεύθυνση για broadcast του υποδικτύου 147.102.13.0/24

Η εντολή `$ dig @electra.netmode.ece.ntua.gr netmode.ece.ntua.gr axfr` επιστρέφει τα ζητούμενα hostnames σε αντιστοιχία με τα IPs τους.

11. Στο αρχείο /home/netmg/cache.txt δίνεται ένα στιγμιότυπο της DNS cache για τον κόμβο dolly.netmode.ece.ntua.gr. Εξηγήστε τις πληροφορίες που περιέχει η cache για καθένα από τους παρακάτω κόμβους:

(α) hermes.cti.gr
; additional
hermes.cti.gr. 1092 \-AAAA ;-\$NXRRSET

RR Set that should exist does not

*<https://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml>

(β) 157.111.242.109.in-addr.arpa.
; answer
157.111.242.109.in-addr.arpa. 69536 PTR adsl-157.109.242.111.tellas.gr.

Πληροφορία για το host name της διεύθυνσης 109.242.111.157

(γ) blue.snd.edu.gr
; authauthority
42.212.83.in-addr.arpa. 23645 NS nic.grnet.gr.
23645 NS red1.snd.edu.gr.
23645 NS foo.grnet.gr.
23645 NS blue.snd.edu.gr.

Πληροφορία για τους authoritative name servers της διεύθυνσης 83.12.212.42

(δ) bender.papagou.gr
; additional
bender.papagou.gr. 1524 \-ANY ;-\$NXDOMAIN

Non-Existent Domain

(ε) inria.fr
; answer
inria.fr. 14846 MX 10 mail1-smtp-roc.national.inria.fr.
14846 MX 10 mail2-smtp-roc.national.inria.fr.
14846 MX 10 mail3-smtp-sop.national.inria.fr.
14846 MX 10 mail4-smtp-sop.national.inria.fr.

Πληροφορία για τους mail servers

(στ) www.ert.gr
; answer
www.ert.gr. 18889 CNAME www.ertonline.gr.

Πληροφορία για το canonical name

12. Πραγματοποιήστε ερωτήματα τύπου “A”, “NS” για το RR: “harvard.edu” και “www.harvard.edu”. Τι παρατηρείτε; Προσπαθήστε να αιτιολογήσετε τι συμβαίνει; (hint: www.cloudflare.com)

```
netmg034@maria:~/lab2$ dig harvard.edu A
; <<>> DiG 9.10.3-P4-Debian <<>> harvard.edu A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2994
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;harvard.edu.                IN      A
```

```
;; ANSWER SECTION:
harvard.edu.                300     IN      A      23.22.75.102
```

```
;; AUTHORITY SECTION:
harvard.edu.                146540 IN      NS      ext-dns-2.harvard.edu.
harvard.edu.                146540 IN      NS      ext-dns-1.harvard.edu.
```

```
;; ADDITIONAL SECTION:
ext-dns-1.harvard.edu.     146540 IN      A      128.103.200.35
ext-dns-2.harvard.edu.     146540 IN      A      128.103.200.162
```

```
;; Query time: 128 msec
;; SERVER: 147.102.13.10#53(147.102.13.10)
;; WHEN: Thu Oct 25 13:40:36 EEST 2018
;; MSG SIZE rcvd: 136
```

```
netmg034@maria:~/lab2$ dig www.harvard.edu A
; <<>> DiG 9.10.3-P4-Debian <<>> www.harvard.edu A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24732
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 5, ADDITIONAL: 11
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.harvard.edu.           IN      A
```

```
;; ANSWER SECTION:
www.harvard.edu.           1910    IN      CNAME    www.harvard.edu.cdn.cloudflare.net.
www.harvard.edu.cdn.cloudflare.net. 300     IN      A      104.16.151.6
www.harvard.edu.cdn.cloudflare.net. 300     IN      A      104.16.152.6
www.harvard.edu.cdn.cloudflare.net. 300     IN      A      104.16.153.6
www.harvard.edu.cdn.cloudflare.net. 300     IN      A      104.16.155.6
www.harvard.edu.cdn.cloudflare.net. 300     IN      A      104.16.154.6
```

```
;; AUTHORITY SECTION:
cloudflare.net.            91504   IN      NS      ns3.cloudflare.net.
cloudflare.net.            91504   IN      NS      ns2.cloudflare.net.
cloudflare.net.            91504   IN      NS      ns4.cloudflare.net.
cloudflare.net.            91504   IN      NS      ns5.cloudflare.net.
cloudflare.net.            91504   IN      NS      ns1.cloudflare.net.
```

:: ADDITIONAL SECTION:

ns3.cloudflare.net.	224	IN	A	198.41.222.31
ns3.cloudflare.net.	20	IN	AAAA	2400:cb00:2049:1::c629:de1f
ns5.cloudflare.net.	224	IN	A	198.41.223.31
ns5.cloudflare.net.	20	IN	AAAA	2400:cb00:2049:1::c629:df1f
ns2.cloudflare.net.	224	IN	A	198.41.222.131
ns2.cloudflare.net.	20	IN	AAAA	2400:cb00:2049:1::c629:de83
ns4.cloudflare.net.	224	IN	A	198.41.223.131
ns4.cloudflare.net.	20	IN	AAAA	2400:cb00:2049:1::c629:df83
ns1.cloudflare.net.	224	IN	A	173.245.59.31
ns1.cloudflare.net.	20	IN	AAAA	2400:cb00:2049:1::adf5:3b1f

:: Query time: 48 msec

:: SERVER: 147.102.13.10#53(147.102.13.10)

:: WHEN: Thu Oct 25 13:40:45 EEST 2018

:: MSG SIZE rcvd: 482

Παρατηρούμε ότι, στην περίπτωση του harvard.edu (χωρίς το www.) ο authoritative server είναι ο ext-dns-2.harvard.edu.

Στη δεύτερη περίπτωση (www.harvard.edu) υπεύθυνοι name-server είναι οι ns[1..5].cloudflare.net.

Καταλαβαίνουμε ότι το Harvard επέλεξε να χρησιμοποιεί υπηρεσία CDN από την εταιρεία CloudFlare για αύξηση του availability και του responsiveness.

(Έτσι προστατεύει την σελίδα και από επιθέσεις DDoS)