Δίκτυα Υπολογιστών

Εργαστηριακή Άσκηση 10
Σύστημα Ονομασίας Περιοχών DNS

Ονοματεπώνυμο: Νικόλαος Παγώνας, el18175	**Ομάδα:** 4 (Τρίτη εξ' αποστάσεως)
Όνομα PC/ΛΣ: nick-ubuntu/Ubuntu 20.04.3 LTS	**Ημερομηνία:** Τρίτη 21/11/2021
Διεύθυνση IP: `192.168.1.15`	**Διεύθυνση MAC:** `3c:2c:30:e1:1c:55`

1. Υπηρεσία DNS

1.1

Βρίσκονται στην περιοχή του ανώτατου επιπέδου.

1.2

Εμφανίστηκαν 13 εξυπηρετητές. Ένας από αυτούς είναι ο `a.root-servers.net` με IPv4 διεύθυνση `198.41.0.4` και IPv6 διεύθυνση `2001:503:ba3e::2:30`.

1.3

Η σύνταξη της εντολής είναι `server 198.41.0.4`.

1.4

Βρίσκονται ένα επίπεδο κάτω από την περιοχή ανωτάτου επιπέδου.

1.5

Υπάρχουν 6 εξυπηρετητές DNS για την περιοχή `'gr.'` και ένας από αυτούς είναι ο `gr-c.ics.forth.gr` με IPv4 διεύθυνση `194.0.1.25` και IPv6 διεύθυνση `2001:678:4::19`.

1.6

Τα αποτελέσματα είναι ίδια με του ερωτήματος 1.4.

1.7

Επιλέγουμε τον `gr-c.ics.forth.gr`. Η σύνταξη της εντολής είναι `server 194.0.1.25`.

1.8

Όχι, η απάντηση δεν είναι ίδια με αυτή της ερώτησης 1.6, αφού πλέον βρίσκομαι ένα επίπεδο πιο κοντά στα φύλλα, και άρα βλέπω τους υπεύθυνους servers αυτής της περιοχής.

1.9

Εμφανίστηκαν 5 DNS Servers, ένας από τους οποίους είναι ο `ulysses.noc.ntua.gr` με IPv4 address `147.102.222.230`.

1.10

Ναι, η απάντηση που λαμβάνουμε είναι ίδια.

1.11

Εμφανίστηκαν 3 DNS Servers, ένας από αυτούς είναι ο `psyche.cn.ece.ntua.gr`.

1.12

- Αρχιτέκτονες Μηχανικοί (arch.ntua.gr):
  - diomedes.noc.ntua.gr
  - printsrvx64.arch.ntua.gr
  - feidias.arch.ntua.gr
  - kallikratisv.arch.ntua.gr
  - achilles.noc.ntua.gr
  - ulysses.noc.ntua.gr
- Μηχανικοί Μεταλλείων-Μεταλλουργοί (metal.ntua.gr):
  - ulysses.noc.ntua.gr
  - diomedes.noc.ntua.gr
  - achilles.noc.ntua.gr
  - serifos.metal.ntua.gr

Παρατηρούμε ότι οι εξυπηρετητές `diomedes.noc.ntua.gr, achilles.noc.ntua.gr`, και `ulysses.noc.ntua.gr` είναι κοινοί μεταξύ των δύο σχολών, ενώ υπάρχουν και μη-κοινοί, όπως `feidias.arch.ntua.gr` και `serifos.metal.ntua.gr`.

1.13

Ο κύριος εξυπηρετητής είναι ο `psyche.cn.ece.ntua.gr` με IPv4 διεύθυνση `147.102.40.1`. Ο σειριακός αριθμός είναι 2021111701.

1.14

Την απάντηση μας την δίνει το πεδίο `refresh = 28800 sec`, δηλαδή 8 ώρες.

1.15

Την απάντηση μας την δίνει το πεδίο `minimum = 86400 sec`, δηλαδή 24 ώρες.

1.16

Ο κύριος εξυπηρετητής του ece.ntua.gr είναι ο `achilles.noc.ntua.gr` με IPv4 διεύθυνση `147.102.222.210`, ο σειριακός αριθμός είναι 2021100700, και τα πεδία `refresh` και `minimum` είναι ίσα με 86400 sec, δηλαδή 24 ώρες.

1.17

Τα πρώτα 8 ψηφία θα μπορούσαν να είναι η ημερομηνία (με format YYYYMMDD) και τα 2 τελευταία ψηφία θα μπορούσαν να είναι ένας αριθμός που αυξάνεται κατά 1 κάθε φορά που γίνεται η ενημέρωση των εγγραφών RR.

1.18

Πανεπιστήμιο	Όνομα Εξυπηρετητή	IPv4
ΕΚΠΑ	www.uoa.gr	195.134.71.228
ΠΑΠΕΙ	www.unipi.gr	195.251.229.4
ΟΠΑ	www.aueb.gr	195.251.255.156

1.19

- `147.102.40.16` → `trillium.cn.ece.ntua.gr`
- `147.102.40.17` → `pegasus.cn.ece.ntua.gr`

1.20

Όχι, η αναπαράσταση της διεύθυνσης IPv4 είναι όπως περιγράφηκε στην θεωρία της εκφώνησης της άσκησης. Δηλαδή χρησιμοποιείται η περιοχή ανωτάτου επιπέδου arpa και συγκεκριμένα η υποπεριοχή in-addr, και κάθε στάθμη κάτω από το επίπεδο in-addr.arpa αποτελεί και ένα byte της διεύθυνσης IPv4, γι' αυτό και τα byte γράφονται ανάποδα απ' ό,τι συνήθως.

1.21

Το κανονικό όνομα είναι `gyali.metal.ntua.gr` και η διεύθυνση IPv4 είναι `147.102.121.5`.

1.22

- achilles.noc.ntua.gr → 147.102.222.210
- f0.mail.ntua.gr → 147.102.222.195

1.23

Θα προτιμηθεί ένας εκ των `f0.mail.ntua.gr, f1.mail.ntua.gr`, γιατί έχουν μικρότερο αριθμό προτίμησης (και οι δύο έχουν 10 έναντι των υπολοίπων που έχουν 100).

1.24

β)

Σε περιβάλλον Linux, πληκτρολογούμε `dig axfr central.ntua.gr @147.102.222.210`. Το axfr σημαίνει ότι ζητάμε να μεταφερθεί ολόκληρο το αρχείο ζώνης από τον πρωτεύοντα εξυπηρετητή στον δευτερεύοντα.

1.25

- **SOA** → netsrv0.central.ntua.gr. dnsmaster.central.ntua.gr. 176 21600 1800 604800 900
- **TXT** → ”v=spf1 ip4:147.102.222.0/24 ip6:2001:648:2000:de::/64 a -all”
- **MX** → 10 ulysses.noc.ntua.gr.
- **NS** → netsrv0.central.ntua.gr.
- **A** → 147.102.222.46
- **CNAME** → beta.central.ntua.gr.

2. Πρωτόκολλο DNS

2.1

Η σύνταξη της εντολής είναι `sudo systemd-resolve --flush-caches`.

2.2

Η σύνταξη του φίλτρου σύλληψης είναι `host 147.102.131.103`.

2.3

Χρησιμοποίησα τις εντολές:

- `set domain=.`
- `server 147.102.40.1`
- `147.102.40.10`
- `server 147.102.7.1`
- `147.102.40.10`

2.4

Το όνομα του `147.102.40.10` είναι `titan.cn.ece.ntua.gr`.

2.5

Η σύνταξη του φίλτρου απεικόνισης είναι `dns`.

2.6

Το DNS χρησιμοποιεί το UDP.

2.7

Έγιναν 2 αιτήματα.

2.8

N/A

2.9

- Αίτημα:
  - Θύρα προέλευσης: 33696
  - Θύρα προορισμού: 53
- Απόκριση:
  - Θύρα προέλευσης: 53
  - Θύρα προορισμού: 33696

2.10

Η θύρα που αντιστοιχεί στο DNS είναι η 53.

2.11

Η επικεφαλίδα DNS έχει μήκος 12 bytes.

2.12

Το αίτημα και η απόκριση έχουν το ίδιο Transaction ID (`0xa1f4`).

2.13

Το πεδίο Flags έχει μήκος 2 bytes.

2.14

Το πρώτο bit (δηλαδή το MSB).

2.15

Το έκτο bit.

2.16

Στο πρώτο αίτημα περιέχονται:

- 1 ερώτηση
- 0 εγγραφές RR απαντήσεων
- 0 εγγραφές RR επίσημων εξυπηρετητών
- 0 εγγραφές RR επιπρόσθετες

2.17

Ναι, την περιλαμβάνει.

2.18

Περιλαμβάνει:

- 1 εγγραφή RR απαντήσεων
- 3 εγγραφές RR επίσημων εξυπηρετητών
- 6 εγγραφές RR επιπρόσθετες

2.19

Όχι, δεν εμφανίστηκαν.

2.20

Η σύνταξη του νέου φίλτρου απεικόνισης είναι `dns.flags.response == 0`.

2.21

Το `www.youtube.com` φέρεται να έχει 15 διευθύνσεις.

2.22

Το μήνυμα αυτό περιλαμβάνει 1 ερώτηση.

2.23

Η απόκριση περιλαμβάνει:

- 16 εγγραφές RR απάντησης
- 4 εγγραφές RR επίσημων εξυπηρετητών
- 6 εγγραφές RR επιπρόσθετες

Συνολικά λοιπόν περιλαμβάνει 26 εγγραφές.

2.24

15 από τις 16 εγγραφές απαντήσεων είναι απαντήσεις για την IPv4 διεύθυνση του www.youtube.com, ενώ η 1 από αυτές περιεχει το CNAME (canonical name) youtube-ui.l.google.com.

2.25

Υπάρχει και μία εγγραφή τύπου CNAME επειδή το www.youtube.com δεν αντιστοιχεί στο canonical name.

2.26

Η ιστοθέση www.youtube.com λογικά φιλοξενείται από πολλούς υπολογιστές, αφού οι αναζητήσεις οδηγούν σε πολλές διαφορετικές IPv4 διευθύνσεις.

2.27

Περιλαμβάνει 2 εγγραφές απάντησης, μία για τη διεύθυνση IPv6 και μία για το CNAME.

2.28

Περιλαμβάνει 4 εγγραφές επίσημων εξυπηρετητών. Οι επίσημοι εξυπηρετητές αυτοί είναι υπεύθυνοι για την περιοχή fastly.net

2.29

Επιστρέφονται 4 επιπρόσθετες εγγραφές, οι οποίες είναι τύπου A και μεταφέρουν τις διευθύνσεις IPv4 των επίσημων εξυπηρετητών DNS.

2.30

Ένας εκ των επίσημων εξυπηρετητών είναι ο `ns1.fastly.net` με διεύθυνση IPv4 `23.235.32.32`.

2.31

Υπάρχουν 2 εγγραφές απαντήσεων, η μία περιέχει την IPv4 διεύθυνση (147.102.224.101) και η άλλη την IPv6 (2001:648:2000:329::101) διεύθυνση του www.ntua.gr.

2.32

Η απόκριση περιέχει 4 εγγραφές αρχής πληροφόρησης.

2.33

Το mname του κύριου εξυπηρετητή DNS της περιοχής cslab.ntua.gr είναι danaos.cslab.ece.ntua.gr και το rname είναι root.danaos.cslab.ece.ntua.gr.

2.34

Άλλοι επίσημοι εξυπηρετητές είναι οι ulysses.noc.ntua.gr, diomedes.noc.ntua.gr και achilles.noc.ntua.gr.

2.35

Η απόκριση σχετικά με το κανονικό όνομα του www.cn.ntua.gr περιέχει συνολικά 10 εγγραφές. Το κανονικό όνομα του www.cn.ntua.gr είναι www.cn.ece.ntua.gr.

2.36

Η απόκριση σχετικά με τους αρμόδιους εξυπηρετητές ηλεκτρονικού ταχυδρομείου της περιοχής elab.ntua.gr περιέχει συνολικά 12 εγγραφές. Οι τρεις εξυπηρετητές είναι ισοδύναμοι, καθώς και οι τρεις έχουν preference 20.

2.37

Έγινε 1 αίτημα και λήφθηκαν 2 αποκρίσεις, ενώ χρησιμοποιήθηκε TCP αυτή τη φορά.

2.38

Για το αίτημα:

- Θύρα προέλευσης: 38105
- Θύρα προορισμού: 53

Για τις αποκρίσεις:

- Θύρα προέλευσης: 53
- Θύρα προορισμού: 38105

2.39

Το μήκος του αιτήματος είναι 60 bytes.

2.40

Ο τύπος του αιτήματος είναι AXFR (Zone Transfer), και με αυτόν τον τρόπο αιτούμαστε την μεταφορά του αρχείου περιοχής από τον πρωτεύοντα εξυπηρετητή στον δευτερεύοντα.

2.41

Η μία απόκριση έχει μήκος 125 bytes (1 μήνυμα DNS) και η άλλη 787 bytes (8 μηνύματα DNS).

2.42

Το καταλαβαίνουμε γιατί οι αποκρίσεις έχουν ίδιο Transaction ID με το αίτημα.

2.43

Όλα τα μηνύματα DNS (response) περιέχουν μία εγγραφή RR απάντησης και μία εγγραφή RR επιπρόσθετη.

2.44

Επειδή το TCP είναι πιο αξιόπιστο, ειδικά όταν μεταφέρουμε μεγάλα πακέτα όπως αυτά που συμμετέχουν σε ένα zone transfer.

2.45

Το φίλτρο σύλληψης είναι `port 53`.