| | |
|---|---|
| **Ονοματεπώνυμο:** Ανδρέας Στάμος (03120***) | **Ομάδα:** 1 |
| **Όνομα PC/ΛΣ:** linux / Ubuntu 22.04.2 LTS (με VPN στο δίκτυο του Πολυτεχνείου) | **Ημερομηνία:** 12/12/2023 |
| **Διεύθυνση IP:** 147.102.131.218 | **Διεύθυνση MAC:** DE–3F–DC–B2–E0–D0 |

# Εργαστηριακή Άσκηση 10
# Σύστημα Ονομασίας Περιοχών DNS

**Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.**

*Η εργασία υλοποιήθηκε με σύνδεση στο δίκτυο VPN του Πολυτεχνείου.*

## 1 Άσκηση 1

**1.1** Στην ρίζα `.`

**1.2** 13 εξυπηρετητές. Οι διευθύνσεις δύο εξυπηρετητών είναι:

m.root-servers.net: 202.12.27.33

a.root-servers.net: 2001:503:ba3e::2:

**1.3** `server a.root-servers.net`

**1.4** Στην περιοχή 1ου επιπέδου `gr.`

**1.5** 6 εξυπηρετητές.

gr-d.ics.forth.gr: 194.0.11.102 και 2001:678:e:102::53

**1.6** Ίδια με του 1.4. Οι εξυπηρετητές DNS κορυφής μας πληροφορούν για τους authoritative εξυπηρετητές του 1ου επιπέδου και μόνο για αυτό.

**1.7** `server 194.0.11.102`

**1.8** Όχι. Ο authoritative εξυπηρετητής της περιοχής `gr.` έχει NS εγγραφή για τους dns εξυπηρετητές του Πολυτεχνείου (οι οποίοι με την σειρά τους μπορούν να απαντήσουν σε ερωτήματα για το ntua.gr)

**1.9** 5 εξυπηρετητές

achilles.noc.ntua.gr: 147.102.222.210

**1.10** Όχι. Στο 1.8 ο εξυπηρετητής μας ενημέρωνε από πού μπορούμε να βρούμε authoritative απαντήσεις χωρίς να δώσει απαντήσεις.

Εδώ μας δίνει απάντηση και επίσης μας πληροφορεί ότι η απάντηση είναι authoritative.

**1.11** 3 εξυπηρετητές

psyche.cn.ece.ntua.gr.: 147.102.40.1

**1.12** Οι εξυπηρετητές ulysses.noc.ntua.gr και achilles.noc.ntua.gr είναι authoritative για όλα τα domains κάτω από το ntua.gr.

**1.13** psyche.cn.ece.ntua.gr.: 147.102.40.1

Serial number: 2023112802

**1.14** 8

**1.15** 7 ημέρες

**1.16** achilles.noc.ntua.gr: 147.102.222.210

serial: 2023090800

Ανανέωση ανά 24 ώρες

Λήξη ανά 24 ώρες

**1.17** Έχει την μορφή YYYYMMDDNN, όπου YYYY το έτος, MM ο μήνας, DD η ημέρα και NN μετρητής για πολλαπλές αλλαγές την ίδια μέρα.

**1.18** Εξυπηρετητής ιστού ≡ Web Server. Άρα μάλλον η ερώτηση αναφέρεται στο όνομα του ιστότοπου.

ΕΚΠΑ: www.uoa.gr, 195.134.71.228, -

ΟΠΑ: wwww.aueb.gr, 195.251.255.156, -

ΑΠΘ: www.auth.gr, 155.207.1.12, 2001:648:2800:1:155:207:1:12

**1.19** 147.102.40.2: soma.cn.ece.ntua.gr

147.102.40.3: gaia.cn.ece.ntua.gr.

**1.20** Η σειρά των bytes είναι ανάποδα από την συνήθη μορφή.

**1.21** CNAME: lemmy.metal.ntua.gr

IPv4: gaia.cn.ece.ntua.gr.

**1.22** f0.mail.ntua.gr: 147.102.222.195

f1.mail.ntua.gr: 147.102.222.196

**1.23** Είτε τον f0.mail.ntua.gr είτε τον f1.mail.ntua.gr καθώς έχουν τον μικρότερο αριθμό προτεραιότητας και άρα την μεγαλύτερη προτεραιότητα.

**1.24** Επιλογή β

Ζητά από τον DNS εξυπηρετητή να του μεταφέρει όλες τις εγγραφές που διαθέτει για ένα domain και όλα τα subdomains αυτού.

**1.25**
```
central.ntua.gr. 86400 IN NS achilles.noc.ntua.gr.
central.ntua.gr. 86400 IN MX 10 achilles.noc.ntua.gr.
central.ntua.gr. 86400 IN A 147.102.222.46
pclab.central.ntua.gr. 86400 IN CNAME www4.central.ntua.gr.
central.ntua.gr. 86400 IN SOA netsrv0.central.ntua.gr. dnsmaster.central.ntua.gr. 189
21600 1800 604800 900
central.ntua.gr. 3600 IN TXT "v=spf1 ip4:147.102.222.0/24 ip6:2001:648:2000:de::/64 a
-all"
```

# 2 Άσκηση 2

**2.1** `resolvectl flush-caches`

**2.2** `host 147.102.131.218`

**2.3**
```
server 147.102.40.1
set q=ptr
147.102.40.1
```

**2.4** titan.cn.ece.ntua.gr.

**2.5** `dns`

**2.6** UDP

**2.7** 2

**2.8** Δεν έγιναν, αλλά υποθέτω πως η άσκηση αναφέρεται σε αιτήματα DNS που εκτελούν άλλες διεργασίες που τρέχουν.

**2.9** Το αίτημα έχει θύρα προέλευσης 50166 και θύρα προορισμού 53.

Η απόκριση έχει θύρα προέλευσης 53 και θύρα προορισμού 50166.

**2.10** 53

**2.11** 12 bytes

**2.12** 0x68a5 και είναι ίδιο και στα δύο.

**2.13** 2 bytes

**2.14** 1ο

**2.15** 6ο

**2.16** 1 ερώτηση μόνο και στα δύο.

**2.17** Ναι.

**2.18** Η απόκριση από τον 147.102.40.1 περιέχει μόνο 1 RR για απάντηση.

Η απόκριση από τον 147.102.7.1 περιέχει 1 RR για απάντηση, 3 RRs για επίσημους εξυπηρετητές και 6 επιπρόσθετες RRs.

**2.19** Ναι.

**2.20** Όχι, το AA Flag (Authoritative Answer) έχει τιμή 0.

**2.21** `dns.flags.response == 1`

**2.22** 16

**2.23** 1

**2.24** Περιλαμβάνει 17 RRs για απάντηση μόνο. Πιο συγκεκριμένα στις RRs αυτές είναι 16 RRs τύπου A και 1 RR τύπου CNAME.

**2.25** Το nslookup έδειξε στην οθόνη τις εγγραφές RR τύπου A στις IPv4 διεύθυνσεις που έδειξε.

**2.26** Γενικά για το όνομα www.youtube.com υπάρχει μόνο ένα CNAME προς το όνομα youtube-ui.l.google.com.

Οι εγγραφές τύπου A που επιστρέφονται είναι για αυτό το όνομα, όχι για το www.youtube.com.

**2.27** Οι εγγράφες έχουν γίνει shuffled.

**2.28** Από πολλούς υπολογιστές, προκειμένου να μπορεί να εξυπρετηθεί η τεράστια κίνηση που λαμβάνει.

**2.29** 5

**2.30** Δεν αποστέλλονται πληροφορίες για εξυπηρετητή DNS. Αποστέλλεται εγγραφή τύπου CNAME, και 4 εγγραφές τύπου AAAA, όπως ζήτηθηκε, προς το "κανονικό όνομα" του www.cnn.com

**2.31** Δεν παρατηρήθηκε.

**2.32** 18 και είναι 1 τύπου SOA, 5 τύπου NS, 4 τύπου MX, 1 τύπου A, 1 τύπου AAAA και 6 τύπου TXT.

**2.33** 1

**2.34** mname: danaos.cslab.ece.ntua.gr

rname: root@danaos.cslab.ece.ntua.gr

**2.35** 1 RR για απάντηση

cname: www.cn.ece.ntua.gr.

TTL: 1200 (20 λεπτά)

**2.36** 3 RR για απάντηση. Προτιμητέοι αρμόδιοι εξυπηρετητές ηλεκτρονικού ταχυδρομείου: achilles.noc.ntua.gr, ulysses.noc.ntua.gr, diomedes.noc.ntua.gr (έχουν ίδια προτεραιότητα)

**2.37** 2 RR για απάντηση. Μια από τις απαντήσεις έχει μήκος 114 bytes με το μήκος της πληροφορίας να είναι 101 bytes.

**2.38** Μόνο 1 RR για επίσημο εξυπηρετητή DNS. Παραπέμπει στην αρχή πληροφόρησης διότι δεν διάθετει μια έγκυρη εγγραφή NS για το όνομα www.ntua.gr. Και είναι λογικό να μην διάθετει, διότι τέτοια εγγραφή, ρωτώντας τον επίσημο εξυπηρετητή, βλέπουμε ότι δεν υπάρχει. Εξάλλου εξυπηρετητής DNS για το www.ntua.gr δεν έχει νόημα να υπάρχει, καθώς δεν υπάρχουν ονόματα κάτω από το www.ntua.gr.

**2.39** Έγινε 1 αίτημα και λήφθηκαν 9 αποκρίσεις.

**2.40** TCP. Θύρα εξυπηρετητή: 53. Θύρα πελάτη: 39289

**2.41** `port 53`

**2.42** Το AXFR χρησιμοποιείται για την μετάδοση μιας ολόκληρης βάσης ονομάτων. Ο λόγος που γίνεται η μετάδοση είναι για να στηθεί ένας δευτερεύων εξυπηρετητής DNS, ο οποίος θέλει να είναι σίγουρος ότι έλαβε από τον επίσημο εξυπηρετητή όλη την βάση, ώστε να μπορεί να εξυπηρετεί σωστά τους πελάτες. Το TCP προσφέρει την αξιοπιστία αυτή, ενώ το UDP όχι. Επίσης το μέγεθος των δεδομένων που πρόκειται να μεταδοθεί είναι, δυνητικά, μεγάλο, οπότε ο έλεγχος ροής για την προστασία του παραλήπτη αλλά και ο έλεγχος συμφόρησης για την προστασία κρίνονται σημαντικοί, υπηρεσία που επίσης προσφέρει το TCP και όχι το UDP.

**2.43** 60 bytes

**2.44** Σκοπός είναι να δημιουργηθεί ένα αντίγραφο της βάσης ενός DNS εξυπηρετητή, συνήθως με σκοπό να στηθεί ένας δευτερεύων εξυπηρετητής DNS.

**2.45** 9

**2.46** Έχουν ίδιο Transcation ID με το αίτεξυπηρετητή, συνήθως με σκοπό να στηθεί ένας δευτερεύων εξυπηρετητής DNS.

**2.47** Όλες περιλαμβάνουν 1 RR για απάντηση και 1 RR για επιπρόσθετες πληροφορίες.

**2.48** Το TCP δεν προσφέρει υπηρεσία διαχωρισμού μηνυμάτων μεταξύ τους. Ως υπηρεσία προσφέρει στο ανώτερο στρώμα ένα αξιόπιστο byte stream. Αν ανώτερα στρώματα επιθυμούν να διαχωρίσουν μηνύματα, πρέπει να το υλοποιήσουν μόνα τους αυτό. Τον σκοπό αυτό εξυπηρετεί το πεδίο που δηλώνει το πεδίο Length, μεγέθους 2 bytes. Κάθε μήνυμα τελειώνει μετά από bytes πλήθους Length, οπότε ξεκινά νέο μήνυμα.

**2.49** Για να εμφανισθεί το ζητούμενο, επιλέγουμε στην απόκριση για την εγγραφή τύπου SOA, στο πέδιο της ερώτησης.

Τότε παρατηρούμε ότι το 1ο byte έχει τιμή 0x09. Τα MSB 2 bits είναι 00, διότι πρόκειται για label και όχι για δείκτη σε label. τα υπόλοιπα LSB 6 bits είναι 0χ09 & 0x3f = 0x09 = 9, καθώς η συμβολοσειρά `planetlab` που είναι το 1ο label, έχει μήκος 9 χαρακτήρες (και άρα 9 bytes).

Το 11ο byte όμοια έχει τα 2 MSB bits 00 για τον ίδιο λόγο και τα 6 LSB bits 0x04 & 0x3f = 0x04 = 4, καθώς η συμβολοσειρά `ntua` έχει μήκος 4.

Το 4ο byte από το τέλος όμοια έχει τα 2 MSB bits 00 για τον ίδιο λόγο και τα 6 LSB bits 0x02 & 0x3f = 0x02 = 2, καθώς η συμβολοσειρά `gr` έχει μήκος 4.

Το τελευταίο byte έχει όμοια τα 2 MSB bits 00 για τον ίδιο λόγο και τα 6 LSB bits 0x00 καθώς με το 0x00 συμβολίζεται το label της ρίζας.

**2.50** Τα δύο τελευταία bytes είναι 0xc016. Τα 2 MSB bits είναι 11, που σημαίνει πως πρόκειται για δείκτη. Τα 14 LSB bits είναι 0xc016 & 0x3fff = 0x0016 = 22, που σημαίνει πως στο 22ο byte (zero-indexed) από την αρχή του μηνύματος DNS, θα βρούμε τα υπόλοιπα labels μετά από αυτά που έχουν δοθεί. Πράγματι, στο 22ο byte ξεκινά το label του ntua.gr. (το 22ο byte είναι το 0x04 που σχολιάστηκε στο ερώτημα 2.49)

**2.51** Δείχνει στο τμήμα του κύριου εξυπηρετητή ονομάτων που ξεκινά στο noc, δηλαδή μπορούν να υπάρχουν αλυσίδες από δείκτες για να βρεθεί η τιμή ενός label.