10η Εργαστηριακή Άσκηση στα Δίκτυα Υπολογιστών

Ονοματεπώνυμο	Γεώργιος Στεφανάκης
Αρ. Μητρώου	el18436
Ομάδα	4
Λειτουργικό Σύστημα	Manjaro Linux x86_64
Διεύθυνση IP	147.102.131.6
Διεύθυνση MAC	b4:69:21:5e:da:03
Ημερομηνία	2022-12-28

1. Υπηρεσία DNS

1.1. Στην περιοχή ανώτατου επιπέδου.

1.2. Εμφανίστηκαν 13 διαφορετικοί DNS servers.
DNS server: a.rootservers.net
IPv4: 198.41.0.4
IPv6: 2001:503:ba3e::2:30

1.3. server 198.41.0.4

1.4. Βρίσκονται μια στάθμη κάτω από την περιοχή ανωτάτου επιπέδου (κάτω από τη ρίζα).

1.5. Εμφανίστηκαν 6 υπεύθυνοι εξυπηρετητές DNS. Ένας από αυτούς είναι ο gr-c.ics.forth.gr με IPv4 194.0.1.25 και IPv6 2001:678:4::19

1.6. Λαμβάνουμε τα ίδια αποτελέσματα με το 1.4 κάτι που είναι αναμενόμενο γιατί το gr. μας επέστρεψε τους εξυπηρετητές που είναι υπεύθυνοι για το από κάτω επίπεδο που είναι το ntua. Συνεπώς μόλις πληκτρολογήσουμε ntua.gr. για την επίλυση του query θα καταλήξουμε στην στάθμη που είναι το gr.

1.7. server 139.91.1.1

1.8. Η απάντηση δεν είναι ίδια με προηγουμένως γιατί έχουμε μεταφερθεί πλέον μια στάθμη προς τα κάτω και πλέον βλέπουμε τους υπεύθυνους εξυπηρετητές για την από κάτω περιοχή.

1.9. Εμφανίστηκαν 5 εξυπηρετητές και ένας από αυτούς είναι ο achilles.noc.ntua.gr με IPv4 147.102.222.210.

1.10. Ναι, περιέχει ωστόσο περισσότερα στοιχεία για τους DNS servers που αναγράφονται.

1.11. Εμφανίστηκαν 3 εξυπηρετητές DNS και ένας από αυτούς είναι ο psyche.cn.ece.ntua.gr.

1.12. Παρατηρούμε ότι υπάρχουν 3 κοινοί εξυπηρετητές DNS για όλες τις σχολές οι diomedes.noc.ntua.gr, achilles.noc.ntua.gr, ulysses.noc.ntua.gr. Υπάρχουν και μη κοινοί όμως όπως στους τοπογράφους που υπάρχει ο mercator.survey.ntua.gr.

1.13. Ο κύριος εξυπηρετητής είναι ο psyche.cn.ece.ntua.gr με IPv4 147.102.40.1 με σειριακό αριθμό 2022120501.

1.14. Κάθε 28800 / 3600 = 8 ώρες, σύμφωνα με το πεδίο refresh.

1.15. Κάθε 86400 / 3600 = 24 ώρες, σύμφωνα με το πεδίο default TTL.

1.16. Για τους ΗΜΜΥ κύριος εξυπηρετητής DNS είναι ο achilles.noc.ntua.gr με IPv4 147.102.222.210 και serial 2022101000. Το πεδίο refresh έχει τιμή 24 ώρες και το πεδίο TTL έχει τιμή επίσης 24 ώρες.

1.17. Προκύπτουν από την ημερομηνία προσθέτοντας 2 μηδενικά στο τέλος και όποτε γίνεται αλλαγή μέσα σε κάθε μέρα πρέπει να προστεθεί το 01 έτσι ώστε να αλλάξουν τα 2 τελευταία ψηφία (ή μόνο το 1).

1.18.

i. ΑΠΘ: www.auth.gr με Server τον www.cff.auth.gr και IPv4 155.207.1.12 και IPv6 2001:648:2800:1:155:207:1:12.
ii. ΕΚΠΑ: www.uoa.gr με Server τον sites2.uoa.gr και IPv4 195.134.71.228 ενώ δεν διαθέτει IPv6
iii. Πολυτεχνείο Κρήτης: www.tuc.gr με Server τον typo3.tuc.gr και IPv4 147.27.15.134 ενώ δεν διαθέτει IPv6

1.19. Στην IPv4 147.102.40.16 με όνομα trillium.cn.ece.ntua.gr και στην IPv4 147.102.40.17 με όνομα pegasus.cn.ece.ntua.gr

1.20. Στην πρώτη απόκριση έχουμε 16.40.102.147.in-addr.arpa και στην 2η 17.40.102.147.in-addr.arpa δηλαδή παρατηρούμε ότι η IPv4 εμφανίζεται ανεστραμμένη.
1.21. Canonical name: lemmy.metal.ntua.gr
1.22. Δύο ονόματα είναι τα: f0.mail.ntua.gr με IPv4 147.102.222.195 και f1.mail.ntua.gr με IPv4 147.102.222.196.
1.23. Εκείνος με το μικρότερο MX preference, δηλαδή είτε ο f0.mai.ntua.gr, είτε ο f1.mail.ntua.gr.
1.24. Εμφανίζονται όλες οι εγγραφές της περιοχής central.ntua.gr
1.25.
- Για NS: central.ntua.gr. NS netsrv0.central.ntua.gr
- Για SOA: central.ntua.gr. SOA netsrv0.central.ntua.gr dnsmaster.central.ntua.gr. (176 21600 1800 604800 900)
- Για MX: central.ntua.gr. MX 10 ulysses.noc.ntua.gr
- Για A: backend.central.ntua.gr. A 147.102.243.119
- Για CNAME: acadinfo.central.ntua.gr. CNAME beta.central.ntua.gr
- Για TXT: central.ntua.gr. TXT "v=spf1 ip4:147.102.222.0/24 ip6:2001:648:2000:de::/64 a -all"

2. Πρωτόκολλο DNS

2.1. sudo systemd-resolve –flush-caches
2.2. Είναι host 147.102.131.6
2.3.
- server 147.102.1.1
- set domain=.
- 147.102.40.10
- server 147.102.7.1
- 147.102.40.10

2.4. titan.cn.ece.ntua.gr
2.5. dns
2.6. UDP
2.7. Γίνονται 3 αιτήματα, με εξυπηρετητές τους 147.102.1.1, 147.102.40.1 και 147.102.7.1.
2.8. Ο πρώτος από τους προαναφερθέντες εξυπηρετητές DNS είναι ο default, ο 2ος είναι εκείνος που ζητήθηκε να διευθετήσει τη δεδομένη IP την πρώτη φορά και ο 3ος εκείνος που χρησιμοποιήθηκε την τελευταία φορά.
2.9. Έχουμε για ένα αίτημα τα Src Port: 54220 (54220), Dst Port: domain (53) και η αντίστοιχη απόκριση είναι η Src Port: domain (53), Dst Port: 54220 (54220)
2.10. Η θύρα 53
2.11. Έχει μήκος 12 bytes.
2.12. Το Transaction ID είναι κοινό τόσο για το query όσο και για το response και έχει τιμή Transaction ID: 0x0003.
2.13. Έχει μήκος 2 bytes.
2.14. Το πρώτο bit.
2.15. Το έκτο bit.
2.16. Περιέχονται:
- 1 ερώτηση
- 0 εγγραφές RR απαντήσεων
- 0 εγγραφές RR επίσημων εξυπηρετητών
- 0 εγγραφές RR επιπρόσθετες

2.17. Ναι
2.18. Περιλαμβάνει:
- 1 εγγραφή RR απαντήσεων
- 3 εγγραφές RR επίσημων εξυπηρετητών
- 6 εγγραφές RR επιπρόσθετες

2.19. Όχι

2.20. Από το 6ο bit του πεδίου FLAGS, το οποίο είναι 0, καταλαβαίνουμε ότι δεν προέρχεται από εξυπηρετητή DNS.
2.21. Είναι “dns.flags.response == 1”
2.22. Φέρεται να έχει 16 διευθύνσεις.
2.23. Περιλαμβάνει 1 ερώτηση.
2.24. Περιλαμβάνει:
- 17 εγγραφές RR απαντήσεων
- 4 εγγραφές RR επίσημων εξυπηρετητών
- 5 εγγραφές RR επιπρόσθετες

2.25. Οι 16 από αυτές είναι απαντήσεις για τις IPv4 διευθύνσεις του www.youtube.com ενώ η 17η μεταφέρει το canonical name = youtube-ui.l.google.com.
2.26. Η εγγραφή για το CNAME χρειάζεται έτσι ώστε η αναζήτηση DNS να συνεχίσει με το κανονικό όνομα και όχι με το ψευδώνυμο.
2.27. Φαίνεται να φιλοξενείται από πολλούς υπολογιστές αφού η αναζήτηση DNS κατέληξε σε πολλές διαφορετικές IPv4.
2.28. Περιλαμβάνει 5 απαντήσεις RR.
2.29. Ένας από τους εξυπηρετητές είναι ο cnn-tls.map.fastly.net με IPv6 2a04:4e42::773.
2.30. Παρατηρούμε επίσης και άλλο ένα ζεύγος που σχετίζεται με την εύρεση του domain name (PTR records) ώστε να μεταφερθούμε στον πραγματικό εξυπηρετητή.
2.31. Περιλαμβάνει 14 απαντήσεις RR, με τύπους: 1 SOA, 5 NS, 3 MX, 1 A, 1 AAAA, 3 TXT.
2.32. Περιέχει μία απάντηση RR τύπου SOA.
2.33. Primary name server: danaos.cslab.ece.ntua.gr, Responsible authority’s mailbox: root.danaos.cslab.ece.ntua.gr
2.34. Περιλαμβάνει μία RR απάντηση, με canonical name www.cn.ntua.gr και TTL 1200 (20 mins)
2.35. Περιλαμβάνει 3 Answer RRs, 0 Authority RRs και 0 Additional RRs. Οι εξυπηρετητές mail είναι οι diomedes.noc.ntua.gr, achilles.noc.ntua.gr, ulysses.noc.ntua.gr .Το mx preference είναι και των τριών ίσο οπότε είναι και οι τρεις το ίδιο προτιμιτέοι.
2.36. Δύο απαντήσεις RR. Μία από τις εγγραφές TXT έχει μήκος, σε byte, 114, ενώ το μήκος της πληροφορίας είναι 101.
2.37. Answer RRs: 0, Authority RRs: 1, Additional RRs: 0. Απ’ ό,τι φαίνεται η απόκριση παραπέμπει στην αρχή πληροφόρησης για την περιοχή ntua.gr, δηλαδή ο achilles.noc.ntua.gr είναι ο υπεύθυνος εξυπηρετητής και για τα δύο domains.
2.38. Έγιναν 3 αιτήματα DNS και λάβαμε 4 αποκρίσεις.
2.39. Ένα αίτημα έγινε με Source port: 1442, Destination port: 53, και δύο αποκρίσεις που καταγράψαμε είχαν Source port: 52 και Destination port: 1442.
2.40. 39 bytes.
2.41. Το αίτημα είναι τύπου AXFR. Η χρησιμότητά του είναι στην περίπτωση όπου μια δευτερεύουσα βάση (ο πελάτης) ζητάει δεδομένα από μια κύρια βάση (εξυπηρετητής) σε αυτή την επικοινωνία μεταξύ εξυπηρετητών που όμως μοιάζει με επικοινωνία πελάτη εξυπηρετητή.
2.42. Μία απόκριση έχει μήκος 140 bytes και μεταφέρει ένα μήνυμα απάντησης DNS. Μία δεύτερη απόκριση έχει μήκος 529 bytes και μεταφέρει 8 DNS responses.
2.43. Επειδή έχουν το ίδιο Transaction ID.
2.44. 1 question, 1 Answer RR
2.45. Χρησιμοποιείται πρωτόκολλο TCP καθώς είναι πιο αξιόπιστο από το UDP το οποίο έχει μεγαλύτερο ρίσκο απώλειας πακέτων.
2.46. port 53
2.47. 1ο byte: c0 (το όνομα βρίσκεται στο offset 12 του μηνύματος)
11ο byte: 00
4ο από το τέλος byte: 00
Τελευταίο byte: 80
2.48. Υπονοούν ότι το μέρος “ntua.gr” έχει δηλωθεί προηγουμένως στο offset 22 του μηνύματος απόκρισης, αφού το c0 δηλώνει χρήση pointer.