LAB-10 (DNS)

Ex. 1 | Υπηρεσία DNS

1. Στη περιοχή .net
2. Εμφανίστηκαν 13 διαφορετικοί DNS servers. DNS server: a.root-servers.net, IPv4: 198.41.0.4, IPv6: 2001:503:ba3e::2:30
3. server 198.41.0.4
4. Ανήκουν στη περιοχή .gr
5. Εμφανίζονται 6 διαφορετικού DNS servers. DNS server: gr-d.ics.forth.gr, IPv4: 194.0.11.102, IPv6: 2001:678:e:102::53
6. Λαμβάνουμε τα ίδια αποτελέσματα με πριν. Συμπεραίνουμε ότι οι εξυπηρετητές κορυφής απαντούν με τις διευθύνσεις των DNS servers που βρίσκονται στο πρώτο επίπεδο (δηλαδή το gr σε αυτή τη περίπτωση)
7. server 139.91.191.3
8. Όχι, η απάντηση τώρα είναι διαφορετική γιατί ο εξυπηρετητής που ρωτήσαμε βρίσκεται σε διαφορετικό επίπεδο στην ιεραρχία και επιστρέφει διαφορετικές διευθύνσεις
9. Εμφανίζονται 3 εξυπηρετητές. DNS server: achilles.noc.ntua.gr, IPv4: 147.102.222.210
10. Όχι, η απάντηση διαφέρει
11. Εμφανίζονται 3 εξυπηρετητές. Ένας που δεν ταυτίζεζαι με κάποιον από την 1.9 είναι ο psyche.cn.ece.ntua.gr
12. Για τους αρχιτέκτονες (arch.ntua.gr) παρατηρούμε ότι πέρα από κάποιους κοινούς εξυπηρετητές έχει κάποιους επιπλέον όπως ο kallikratisv.arch.ntua.gr
13. SOA: psyche.cn.ece.ntua.gr, IPv4: 147.102.40.1, SN: 2021122301
14. Κάθε 8 ώρες
15. Για 1 ημέρα
16. SOA: psyche.cn.ece.ntua.gr, IPv4: 147.102.222.210, SN: 2021100700, TTL: 1 ημέρα
17. Πρόκειται για μία ημερομηνία (επειδή ξεκινάνε με το 2021)
18. www.ntua.gr → 147.102.224.101, www.uoa.gr → 195.134.71.228, www.aueb.gr → 195.251.255.156
19. trillium.cn.ece.ntua.gr, ulysses.noc.ntua.gr
20. Όχι, έχει τη μορφή reverse lookup (ex. 40.102.147.in-addr.arpa)
21. gyali.metal.ntua.gr → 147.102.121.5
22. f0.mail.ntua.gr → 147.102.222.195, f1.mail.ntua.gr → 147.102.222.196
23. Θα είναι ο f1.mail.ntua.gr γιατί έχει τη μικρότερη τιμή MX preference

DIRECTORY

NOTES

📝 **Για να βρείς την IP μίας διεύθυνσης**

`nslookup <dns name>`

24. Εμφανίζει μία λίστα με όλες τις εγγραφές της περιοχής central.ntua.gr
25. MX → 10 ulysses.noc.ntua.gr, NS → netsrv0.central.ntua.gr, A → 147.102.222.46, CNAME → beta.central.ntua.gr, SOA → netsrv0.central.ntua.gr dnsmaster.central.ntua.gr. (176 21600 1800 604800 900)

Ex. 2 | Πρωτόκολλο DNS

1. ipconfig /flushdns
2. Capture filter: host 147.102.136.49
3. Στη κονσόλα του nslookup, την εντολή ‘set q=ptr’
4. titan.cn.ece.ntua.gr
5. Display filter: dns
6. Το UDP
7. Έγιναν συνολικά 10 αιτήματα
8. Λόγω της εκκαθάρισης της DNS cache
9. Source Port: 60818, Destination Port: 53
10. Η 53
11. DNS Header Length: 12 bytes
12. Transaction ID: 0x0003, Ταυτίζονται
13. 2 bytes
14. Το πρώτο bit δηλώνει request / reply
15. Το εκτρο bit δηλώνει αν το reply προέρχεται από τον SOA
16. Questions: 1, Answer RRs: 0, Authority RRs: 0, Additional RRs: 0
17. Ναι, την περιλαμβάνει
18. Answer RRs: 1, Authority RRs: 3, Additional RRs: 6
19. Ναι, εμφανίστηκαν όλες
20. Display filter: dns.flags.response==1
21. Φαίνεται να έχει 14 διευθύσεις IPv4
22. 1 ερώτηση
23. 15 απαντήσεις RR, 4 επίσημων εξυπηρετητών, 7 επιπρόσθετες
24. Προκύπτει από τις 14 διευθύσεις του 2.21 και ακόμα μία για το cname του www.YouTube.com
25. Γιατί το www.youtube.com είναι ψευδόνυμο (alias)
26. Το www.youtube.com βρίσκεται σε πολλούς servers για αυτό και υπάρχουν περισσότερες από 1 διευθύσεις IP
27. Περιλαμβάνει 10 εγγραφές RR
28. 4 εγγραφές. Είναι υπεύθυνοι για την περιοχή fastly.net
29. 4 εγγραφές τύπου A. Μεταφέρουν την IPv4 των επίσημων εξυπηρετητών.
30. ns1.fastly.net : 23.235.32.32

31. Περιέχονται 17 εγγραφές RR. 2 answer RR, 5 authority RR, 7 additional RR
32. Περιέχονται 12 εγγραφές (1 answer, 4 authority, 7 additional)
33. danaos.cslab.ece.ntua.gr. Email διαχειριστή: root.danaos.cslab.ece.ntua.gr
34. ulysses.noc.ntua.gr, diomedes.noc.ntua.gr, achilles.noc.ntua.gr
35. Εμφανίζονται 11 εγγραφές. Το cname του www.cn.ntua.gr είναι το www.cn.ece.ntua.gr
36. Εμφανίζονται 12 εγγραφές. Το όνομα του προτιμότερου από αυτούς είναι ο ulysses.noc.ntua.gr
37. Έγιναν 2 αιτήματα, λήφθηκαν 3 αποκρίσεις DNS και το πρωτόκολλο μεταφοράς είναι το TCP και το UDP για το πρώτο ζευγάρι qrery, response
38. Source Port: 62715, Destination Port: 53
39. 39 bytes
40. Ο τύπος αιτήματος είναι AXFR και είναι για μεταφορά DNS ζώνης
41. Έχουν μήκη 84 και 55 bytes και μεταφέρουν συνολικά 9 μηνύματα DNS (1+8)
42. Έχουν την ίδια τιμή στο πεδίο Transaction ID
43. Απόκριση 1 - Questions: 1, Answer RRs: 1, Authority RRs: 0, Additional RRs: 0,
    Απόκριση 2 - Questions: 0, Answer RRs: 1, Authority RRs: 0, Additional RRs: 0
44. Ώστε κατά τη μεταφορά ζώνης DNS να υπάρχει πιο αξιόπιστη και ασφαλής επικοινωνία
45. Capture filter: udp.port == 53