| | | | |
|---|---|---|---|
| **Όνοματεπώνυμο:** | **Μάρκος Δεληγιάννης** | **Ομάδα:** | **3** |
| **Όνομα PC/ΛΣ:** | **DESKTOP-SCJFUE1 / W10** | **Ημερομηνία:** | **14 / 12 / 22** |
| **Διεύθυνση IP:** | **147.102.131.23** | **Διεύθυνση MAC:** | **00:FF:EE:DE:8A:A1** |

# 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.**

## *1*

1.1 Οι εξυπηρετητές ανήκουν στο ανώτατο επίπεδο της ιεραρχίας, την **περιοχή κορυφής**.

1.2 Εμφανίστηκαν 13 εξυπηρετητές DNS. Τα στοιχεία ενός από αυτούς είναι τα εξής:
Όνομα: a.root-servers.net
IPv4 address: 198.41.0.4
IPv6 address: 2001:503:ba3e::2:30

1.3 "server a.root-servers.net"

1.4 Ανήκουν στην περιοχή ανωτάτου επιπέδου gr (1 επίπεδο κάτω από τη ρίζα).

1.5 Εμφανίστηκαν 6 εξυπηρετητές DNS. Τα στοιχεία ενός από αυτούς είναι τα εξής:
Όνομα: gr-c.ics.forth.gr
IPv4 address: 194.0.1.25
IPv6 address: 2001:678:4::19

1.6 Τα αποτελέσματα που λαμβάνουμε είναι ακριβώς ίδια με την περίπτωση του "gr.". Συμπεραίνουμε ότι οι εξυπηρετητές κορυφής συμπεριφέρονται στην υποπεριοχή "ntua.gr." (αντίστοιχα για όλες τις υποπεριοχές των περιοχών ανωτάτου επιπέδου) ως μέρος της περιοχής "gr.", χωρίς να γνωρίζουν κάτι περισσότερο για αυτήν.

1.7 "server gr-d.ics.forth.gr"

1.8 Η απάντηση είναι διαφορετική από την περίπτωση του 1.6. Αυτό συμβαίνει διότι οι root servers δεν μπορούν να γνωρίζουν τους εξυπηρετητές DNS σε πολύ πιο χαμηλά επίπεδα, οπότε επιστρέφουν την ίδια απάντηση για όλες τις υποπεριοχές του "gr.". Αντιθέτως οι εξυπηρετητές DNS που αντιστοιχούν στην περιοχή "gr." γνωρίζουν τους κατάλληλους DNS servers χαμηλότερου επιπέδου.

1.9 Εμφανίστηκαν 5 εξυπηρετητές DNS. Τα στοιχεία ενός από αυτούς είναι τα εξής:
Όνομα: ulysses.noc.ntua.gr
IPv4 address: 147.102.222.230

1.10 Οι εξυπηρετητές είναι οι ίδιοι, αλλά εμφανίζεται περισσότερη πληροφορία. Πιο συγκεκριμένα, εμφανίζονται και οι διευθύνσεις IPv6 τριών από τους 5 εξυπηρετητές.

1.11 Εμφανίστηκαν 3 εξυπηρετητές DNS. Ο **psyche.cn.ece.ntua.gr** δεν εμφανίστηκε προηγουμένως.

1.12 Για το domain chemeng.ntua.gr.: achilles.noc.ntua.gr, ulysses.noc.ntua.gr και diomedes.noc.ntua.gr.
Για το domain metal.ntua.gr.: serifos.metal.ntua.gr, ulysses.noc.ntua.gr, achilles.noc.ntua.gr, diomedes.noc.ntua.gr
Παρατηρούμε ότι υπάρχουν γενικοί DNS servers για όλες τις σχολές του πολυτεχνείου, αλλά και ειδικοί σε κάθε τμήμα.

1.13 Κύριος εξυπηρετητής: psyche.cn.ece.ntua.gr
IPv4 διεύθυνση: 147.102.40.1
Serial Number: 2022120501

1.14 Κάθε 8 ώρες (refresh = 28800)

1.15 Για 24 ώρες (TTL = 86400)

1.16 Κύριος εξυπηρετητής DNS: achilles.noc.ntua.gr
IPv4 διεύθυνση: 147.102.222.210
Σειριακός αριθμός: 2022101000
Ένας δευτερεύων εξυπηρετητής αναζητά αλλαγές κάθε 24 ώρες (refresh = 86400)
Οι σχετικές εγγραφές διατηρούνται στην προσωρινή μνήμη μη επίσημων εξυπηρετητών για 24 ώρες (default TTL = 86400).

1.17 Παρατηρούμε ότι ο σειριακός αριθμός περιέχει το έτος (2022), μήνα (10), μέρα (10) και ώρα (00) της τελευταίας αλλαγής.

1.18 UOA: name: sites2.uoa.gr IPv4 Address: 195.134.71.228
TUC: name: typo3.tuc.gr IPv4 Address: 147.27.15.134
UTH: name: poseidon.uth.grI IPv4 Address: 194.177.200.19

1.19 147.102.40.17 → pegasus.cn.ece.ntua.gr
147.102.40.18 → bbb.cn.ece.ntua.gr

1.20 Όχι, τα bytes είναι σε αντίστροφη σειρά, δηλαδή είναι:
147.102.40.17 → 17.40.102.147.in-addr.arpa

1.21 Κανονικό όνομα: lemmy.metal.ntua.gr
IPv4 διεύθυνση: 147.102.121.10

1.22 Δύο από τους εξυπηρετητές είναι ο achilles.noc.ntua.gr με IPv4 διεύθυνση 147.102.222.210 και ο f0.mail.ntua.gr με IPv4 147.102.222.195.

1.23 Θα προτιμηθεί ο f0.mail.ntua.gr διότι έχει το μικρότερο MX preference (10), δηλαδή τη μεγαλύτερη προτεραιότητα.

1.24 Με αυτήν την εντολή ζητούνται όλες οι εγγραφές RR της περιοχής central.ntua.gr.

1.25 central.ntua.gr. SOA netsrv0.central.ntua.gr dnsmaster.central.ntua.gr (180 21600 1800 604800 900)
central.ntua.gr. TXT "v=spf1 ip4:147.102.222.0/24 ip6:2001:648:2000:de::/64 a -all"
central.ntua.gr. MX 10 ulysses.noc.ntua.gr
central.ntua.gr. NS ulysses.noc.ntua.gr
central.ntua.gr. A 147.102.222.46
acadinfo CNAME beta.central.ntua.gr

## *2*

2.1 "ipconfig /flushdns"

2.2 "host 147.102.131.23"

2.3 Μετά την set domain=. εκτελέσαμε τις εντολές q=ptr, server 147.102.40.1 και 147.102.40.10, για τον πρώτο DNS server, και server 147.102.7.1 και 147.102.40.10 για τον δεύτερο DNS server.

2.4 titan.cn.ece.ntua.gr

2.5 "dns"

2.6 UDP

2.7 Έγιναν 5 αιτήματα.

2.8 Όταν ορίζουμε έναν εξυπηρετητή DNS δίνοντας την IPv4 διεύθυνσή του στέλνεται ένα αίτημα DNS για τον προσδιορισμό του ονόματός του. Ορίσαμε 3 servers, έναν στην αρχή και τους δύο που χρησιμοποιήσαμε. Συνεπώς έγιναν 3 αιτήματα DNS λόγω αυτού, και 2 αιτήματα για την εύρεση του ονόματος που αντιστοιχεί στη δοσμένη IPv4 διεύθυνση.

2.9 Θύρα υπολογιστή μας: 57605 Θύρα εξυπηρετητή: 53

2.10 Η θύρα 53.

2.11 Έχει μήκος 12 bytes.

2.12 Τα δύο IDs είναι ίσα μεταξύ τους (Transaction ID = 0x0003)

2.13 2 bytes.

2.14 Το πρώτο bit (Response).

2.15 Το 6ο bit (Authoritative).

2.16 1 ερώτηση και 0 εγγραφές για όλα τα άλλα (φαίνεται από τα 4 αντίστοιχα πεδία της επικεφαλίδας)

2.17 Ναι

2.18 1 εγγραφή για ερωτήσεις, 1 εγγραφή για απαντήσεις, 3 εγγραφές για επίσημους εξυπηρετητές και 6 επιπρόσθετες εγγραφές.

2.19 Ναι (1 απάντηση, 3 εγγραφές για επίσημους DNS servers και οι διευθύνσεις IPv4 και IPv6 τους).

2.20 Όχι, δεν προέρχεται από τον επίσημο DNS server. Την πληροφορία αυτή φέρει το 6ο bit στις σημαίες (Authoritative), το οποίο είναι 0.

2.21 “dns.flags.response==1”

2.22 16 διευθύνσεις IPv4.

2.23 Μία.

2.24 17 εγγραφές RR δύο ειδών: Μία με type = CNAME και 16 με type = A.

2.25 Οι 16 εγγραφές RR με type = A αντιστοιχούν πλήρως στις διευθύνσεις IPv4 που εμφανίζονται στον φλοιό (τις περιέχουν στο πεδίο Address).

2.26 Η εγγραφή αυτή περιέχει το κανονικό όνομα (canonical name) του www.youtube.com.

2.27 Όταν εκτελούμε την εντολή nslookup εκ νέου παρατηρούμε διαφορετικές IPv4 διευθύνσεις. Συνεπώς το www.youtube.com φιλοξενείται από μία πληθώρα υπολογιστών, όπως είναι και λογικό δεδομένου του πολύ μεγάλου φορτίου που δέχεται ανά πάσα στιγμή.

2.28 Περιλαμβάνει 5 εγγραφές.

2.29 Το επίσημο όνομα είναι “cnn-tls.map.fastly.net” και η IPv6 ενός εκ των εξυπηρετητών είναι 2a04:4e42::773.

2.30 Στην ερώτηση που ζητά το όνομα του εξυπηρετητή με IPv4 διεύθυνση 1.1.1.1 (ο DNS server που ορίσαμε αρχικά).

2.31 Παρατηρούμε 14 εγγραφές RR για απαντήσεις. 3 είναι τύπου κειμένου (type TXT), 1 είναι για διευθύνσεις IPv6 (type AAAA), 1 είναι για διευθύνσεις IPv4 (type A), 3 είναι για ηλεκτρονικό ταχυδρομείο (type MX), 5 είναι για υπεύθυνους εξυπηρετητές (type NS) και μία είναι για την αρχή πληροφόρησης (type SOA).

2.32 Παρατηρούμε μόνο 1 εγγραφή RR.

2.33 mname: danaos.cslab.ece.ntua.gr
rname: root.danaos.cslab.ece.ntua.gr

2.34 Παρατηρούμε 1 εγγραφή RR. Το κανονικό όνομα (CNAME) είναι www.cn.ece.ntua.gr και η διάρκεια ζωής της εγγραφής είναι 20 λεπτά (TTL = 1200).

2.35 Παρατηρούμε 3 εγγραφές RR. Οι εξυπηρετητές είναι ισοδύναμοι μεταξύ τους, δεδομένου ότι έχουν την ίδια προτεραιότητα (preference = 20). Αναφέρουμε το όνομα ενός από αυτούς: diomedes.noc.ntua.gr

2.36 Παρατηρούμε 2 εγγραφές RR. Το μήκος της πρώτης είναι 114 bytes. Το μήκος της πληροφορίας είναι 102 bytes.

2.37 Παρατηρούμε 1 εγγραφή RR, η οποία είναι για επίσημους εξυπηρετητές. Η απόκριση αυτή είναι type SOA, οπότε παραπέμπει στην αρχή πληροφόρησης για την περιοχή ntua.gr.

2.38 Έγιναν 2 αιτήματα DNS, ένα για την εύρεση του ονόματος του DNS server 147.102.222.210 και ένα για την εντολή ls -d planetlab.ntua.gr. Λήφθηκαν 3 αποκρίσεις DNS, μία για το όνομα του DNS server και 2 για την εντολή ls -d planetlab.ntua.gr. Για την εντολή server 147.102.222.210 τα μηνύματα DNS που λήφθηκαν χρησιμοποιούν UDP, ενώ τα 3 μηνύματα που αντιστοιχούν στην εντολή ls -d planetlab.ntua.gr χρησιμοποιούν TCP.

2.39 Θύρα client: 55587 Θύρα server: 53

2.40 39 bytes.

2.41 Type = AXFR. Αντιστοιχεί στη μεταφορά ζώνης, κατά την οποία ένας εξυπηρετητής DNS λαμβάνει πληροφορίες για τις εγγραφές μίας άλλης περιοχής.

2.42 Οι αποκρίσεις του εξυπηρετητή έχουν μήκος 86 bytes και 475 bytes. Η πρώτη μεταφέρει ένα μήνυμα DNS response ενώ η δεύτερη μεταφέρει 8 μηνύματα.

2.43 Όλες οι απαντήσεις έχουν το ίδιο Transaction ID με το αίτημα που έγινε (0x000a).

2.44 1ο μήνυμα: Μόνο 1 εγγραφή για ερωτήσεις και 1 εγγραφή για απαντήσεις.
Υπόλοιπα: Μόνο 1 εγγραφή για απαντήσεις.

2.45 Επειδή στέλνονται πολλά RR και πρέπει να διασφαλιστεί η ακεραιότητα της πληροφορίας είναι προτιμότερο να χρησιμοποιηθεί TCP, το οποίο είναι πιο αξιόπιστο από το UDP.

2.46 “port 53” (αφού δεν υπάρχει φίλτρο σύλληψης dns)

2.47 1ο: 0x09 (μήκος της ετικέτας planetlab)
11ο: 0x04 (μήκος της ετικέτας ntua)
4ο πριν το τέλος: 0x02 (μήκος της ετικέτας gr)
Τελευταίο: 0x00 (σηματοδοτεί το τέλος του ονόματος)

2.48 Τα δύο bytes είναι 0xc016. Τα δύο πρώτα bits είναι 1, το οποίο σημαίνει ότι πρόκειται για pointer και τα υπόλοιπα bits αντιστοιχούν στο offset, μετρώντας από το ID. Το offset είναι 0x16=22, οπότε αντιστοιχεί στο “ntua.gr”.

2.49 Παρατηρούμε ότι αποτελείται μόνο από 2 bytes, τα 2 MSB των οποίων είναι 1, οπότε το όνομα έχει συμπιεστεί σε έναν απλό δείκτη. Το offset είναι 0x38, οπότε με υπολογισμούς προκύπτει ότι το όνομα στο οποίο δείχνει ο δείκτης είναι το noc.ntua.gr