Δίκτυα υπολογιστών

Εργαστηριακή άσκηση 10 (Σύστημα Ονομασίας Περιοχών DNS)

Τσάκωνας Παναγιώτης (03119610) Ομάδα: 2

Ακαδημαϊκό Έτος: 2022-2023

Άσκηση 1: Υπηρεσία DNS

1.1) Οι εξυπηρετητές DNS που εμφανίζονται ανήκουν στην περιοχή .net .

1.2) Εμφανίζονται 13 DNS servers και η IPv4 διεύθυνση ενός είναι: 198.41.0.4 και η IPv6 διεύθυνση του είναι: 2001:503:ba3e::2:30 .

1.3) Η σύνταξη της εντολής είναι: `server 198.41.0.4` .

1.4) Οι εξυπηρετητές DNS που εμφανίζονται ανήκουν στην περιοχή .gr .

1.5) Εμφανίζονται 6 DNS servers και η IPv4 διεύθυνση ενός είναι: 194.0.1.25 και η IPv6 διεύθυνση του είναι: 2001:678:4::19 .

1.6) Λαμβάνουμε τα ίδια αποτελέσματα με πριν, απ' όπου συμπεραίνουμε ότι οι εξυπηρετητές κορυφής απαντούν με τις διευθύνσεις των DNS servers που βρίσκονται στο πρώτο επίπεδο, δηλαδή .gr στην συγκεκριμένη περίπτωση.

1.7) Η σύνταξη της εντολής είναι: `server 194.0.11.102` .

1.8) Όχι η απάντηση τώρα είναι διαφορετική, διότι ο εξυπηρετητής που ρωτήσαμε τώρα βρίσκεται σε διαφορετικό επίπεδο στην ιεραρχία και επιστρέφει διαφορετικές διευθύνσεις με πριν.

1.9) Εμφανίζονται 3 DNS servers και το όνομα ενός από αυτούς είναι: ulysses.noc.ntua.gr με Pv4 διεύθυνση: 147.102.222.230 .

1.10) Όχι η απάντηση διαφέρει και πάλι.

1.11) Εμφανίζονται 3 εξυπηρετητές και ένας που δεν ταυτίζεται με κάποιον από την ερώτηση 1.9 είναι ο achilles.noc.ntua.gr .

1.12) Για τους αρχιτέκτονες (arch.ntua.gr) παρατηρούμε ότι πέρα από κάποιους κοινούς εξυπηρετητές έχει και έναν επιπλέον, τον diomedes.noc.ntua.gr . Για τους χημικούς (chemeg.ntua.gr) παρατηρούμε ότι έχουν τους ίδιους εξυπηρετητές με τους αρχιτέκτονες και 2 κοινούς με πριν.

1.13) Ο κύριος εξυπηρετητής της διεύθυνσης cn.ntua.gr είναι ο psyche.cn.ece.ntua.gr με διεύθυνση IPv4: 147.102.40.1 και σειριακό αριθμό: 2022120501.

1.14) Κάθε 8 ώρες θα αναζητήσει αλλαγές σχετικά με την περιοχή 'cn.ntua.gr.' ένας δευτερεύων εξυπηρετητής.

1.15) Για 1 ημέρα διατηρούνται οι σχετικές με την περιοχή 'cn.ntua.gr.' εγγραφές στην προσωρινή μνήμη άλλων μη επίσημων εξυπηρετητών.

1.16) Ο κύριος εξυπηρετητής της διεύθυνσης ece.ntua.gr είναι ο achilles.noc.ntua.gr με διεύθυνση IPv4: 1.1.1.1 και σειριακό αριθμό: 2022101000. Κάθε 24 ώρες θα αναζητήσει αλλαγές σχετικά με την περιοχή 'ece.ntua.gr' ένας δευτερεύων εξυπηρετητής. Για 1 ημέρα διατηρούνται οι σχετικές με την περιοχή 'ece.ntua.gr' εγγραφές στην προσωρινή μνήμη άλλων μη επίσημων εξυπηρετητών.

1.17) Καταλαβαίνω ότι πρόκειται για μια ημερομηνία καθώς ξεκινάει από το 2022, δηλαδή το τρέχων έτος.

1.18) di.uoa.gr→195.134.65.123 , cs.unipi.gr→195.251.226.4 , ice.uniwa.gr→195.130.100.83

1.19) 147.102.40.16 → trillium.cn.ece.ntua.gr , 147.102.40.17 → pegasus.cn.ece.ntua.gr .

1.20) Όχι, έχει τη μορφή reverse lookup (π.χ. 16.40.102.147.in-addr.arpa).
1.21) serifos.metal.ntua.gr → 147.102.1.1
1.22) ulysses.noc.ntua.gr → 147.102.222.230 και achilles.noc.ntua.gr → 147.102.222.210
1.23) Θα προτιμηθούν οι f0.mail.ntua.gr και f1.mail.ntua.gr , διότι έχουν μικρότερο αριθμό προτίμησης.
1.24) Το πρωτόκολλο AXFR χρησιμοποιείται για zone transfers, δηλαδή για αντιγραφή δεδομένων DNS μεταξύ εξυπηρετητών.
1.25) Τα πλήρη στοιχεία για κάθε είδος εγγραφής που συνάντησα είναι τα ακόλουθα:

- central.ntua.gr. 86400 IN SOA netsrv0.central.ntua.gr. dnsmaster.central.ntua.gr. 180 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"
- central.ntua.gr. 86400 IN MX 10 achilles.noc.ntua.gr.
- central.ntua.gr. 86400 IN NS netsrv0.central.ntua.gr.
- central.ntua.gr. 86400 IN A 147.102.222.46
- acadinfo.central.ntua.gr. 86400 IN CNAME beta.central.ntua.gr.

Άσκηση 2: Πρωτόκολλο DNS

2.1) Η ακριβής σύνταξη της εντολής που χρησιμοποιήσατε για τον καθαρισμό της προσωρινής μνήμης DNS είναι: `sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder.`
2.2) Η σύνταξη του φίλτρου σύλληψης που χρησιμοποίησα είναι: `host 147.102.236.63.`
2.3) Χρησιμοποίησα την εντολή: `set q=ptr.`
2.4) Το όνομα του 147.102.40.10 είναι: titan.cn.ece.ntua.gr.
2.5) Η σύνταξη του φίλτρου απεικόνισης που χρησιμοποίησα είναι: `dns.`
2.6) Χρησιμοποιήθηκε το πρωτόκολλο μεταφοράς udp από το DNS.
2.7) Έγιναν συνολικά 5 αιτήματα προς εξυπηρετητές DNS από τον υπολογιστή μου.
2.8) Έγιναν περισσότερα από 2, διότι καθάρισα την DNS cache.
2.9) Source Port: 56366 και Destination Port: 53.
2.10) Η θύρα 53 αντιστοιχεί στο πρωτόκολλο εφαρμογής DNS.
2.11) Η επικεφαλίδα DNS έχει μήκος 12 bytes.
2.12) Το Transaction ID του πρώτου αιτήματος για το όνομα του 147.102.40.10 και της αντίστοιχης απόκρισης είναι: 0x942a και παρατηρώ ότι είναι το ίδιο και για το αίτημα και για την απόκριση
2.13) Το πεδίο Flags της επικεφαλίδας DNS έχει μήκος 2 bytes.
2.14) Το πρώτο κατά σειρά bit του πεδίου Flags της επικεφαλίδας DNS δηλώνει αν το συγκεκριμένο μήνυμα είναι αίτημα ή απόκριση.
2.15) Το 6ο κατά σειρά bit του πεδίου Flags δείχνει το κατά πόσο η απόκριση προέρχεται από τον επίσημο εξυπηρετητή DNS.
2.16) Περιέχονται 1 ερώτηση, 0 εγγραφές RR απαντήσεων, 0 εγγραφές RR επίσημων εξυπηρετητών και 0 εγγραφές επιπρόσθετες RR.
2.17) Ναι περιλαμβάνει την ερώτηση για την οποία απαντά.
2.18) Περιλαμβάνει 1 ερώτηση, 1 εγγραφή RR απάντησης, 3 εγγραφές RR επίσημων εξυπηρετητών και 6 εγγραφές επιπρόσθετες RR.

2.19) Όχι δεν εμφανίσθηκαν όλες οι προηγούμενες πληροφορίες για εγγραφές RR στο παράθυρο της γραμμής εντολών.

2.20) Όχι δεν προέρχεται από τον επίσημο εξυπηρετητή DNS, αλλά βρήκα την σχετική πληροφορία στα DNS Flags.

2.21) Η σύνταξη του νέου φίλτρου απεικόνισης είναι: `dns.flags.response == 1.`

2.22) Το www.youtube.com σύμφωνα με το αποτέλεσμα της εντολής `nslookup` φέρεται να έχει 16 διευθύνσεις IPv4.

2.23) Περιλαμβάνει 1 ερώτηση.

2.24) Το τμήμα της απάντησης στην παραπάνω απόκριση περιλαμβάνει 16 A και 1 CNAME εγγραφές.

2.25) Οι εγγραφές είναι αυτές που εμφανίστηκαν σαν αποτέλεσμα της εντολής.

2.26) Υπάρχει και μια εγγραφή RR τύπου CNAME, διότι το www.youtube.com είναι alias για άλλο domain.

2.27) Η ιστοθέση www.youtube.com φιλοξενείται από πολλαπλούς εξυπηρετητές.

2.28) Το τμήμα της απάντησης για διευθύνσεις IPv6 του www.cnn.com περιλαμβάνει 5 εγγραφές RR απαντήσεων.

2.29) Το επίσημο όνομα και τη διεύθυνση IPv6 ενός εκ των εξυπηρετητών που περιλαμβάνει η απόκριση για το www.cnn.com είναι τα ακόλουθα: cnn-tls.map.fastly.net και 2a04:4e42:600::773 αντίστοιχα.

2.30) …..

2.31) Περιέχονται 14 συνολικά εγγραφές RR, οι οποίες είναι: SOA, NS, A, AAAA, MX, TXT.

2.32) Το πλήθος των RR απαντήσεων στην απόκριση σχετικά με την αρχή πληροφόρησης για την περιοχή cslab.ntua.gr είναι 1.

2.33) Το όνομα (mname – master name) του κύριου εξυπηρετητή DNS της περιοχής cslab.ntua.gr είναι: danaos.cslab.ece.ntua.gr και η διεύθυνση ηλεκτρονικού ταχυδρομείου είναι: root@danaos.cslab.ece.ntua.gr .

2.34) Το κανονικό όνομα του www.cn.ntua.gr είναι: www.cn.ece.ntua.gr και η διάρκεια ζωής της εγγραφής είναι 20 λεπτά.

2.35) Το πλήθος των RR απαντήσεων στην απόκριση σχετικά με τους αρμόδιους εξυπηρετητές ηλεκτρονικού ταχυδρομείου της περιοχής elab.ntua.gr είναι 3. Οι εξυπηρετητές έχουν και οι 3 ίδιο συντελεστή προτίμησης (20), επομένως αφήνεται στο πρόγραμμα-πελάτη να επιλέξει ποιον θα χρησιμοποιήσει.

2.36) Το πλήθος των RR απαντήσεων στην απόκριση για την περιοχή telecom.ntua.gr είναι 2, η μία έχει μήκος 81 bytes και μεταφέρει πληροφορία 68 bytes.

2.37) Παρατηρώ ότι έγινε 1 ερώτηση, 0 εγγραφές RR απαντήσεων, 1 εγγραφή RR επίσημων εξυπηρετητών και 0 εγγραφές επιπρόσθετες RR. η απόκριση παραπέμπει την αρχή πληροφόρησης για την περιοχή ntua.gr, επειδή δεν υπάρχουν εγγραφές του τύπου που ζητήθηκε για το συγκεκριμένο όνομα.

2.38) Έγινε 1 αίτημα DNS και λήφθηκαν 2 αποκρίσεις. Το πρωτοκολλο μεταφοράς που χρησιμοποιήθηκε είναι το TCP.

2.39) Για το αίτημα: Source Port: 55635 → Destination Port: 53.
Για την απόκριση: Source Port: 53 → Destination Port: 55635.

2.40) Το μήκος του αιτήματος προς τον εξυπηρετητή 147.102.222.210 είναι 48 bytes.

2.41) Ο τύπος του αιτήματος είναι: AXFR και χρησιμοποιείται για την αντιγραφή όλων των εγγραφών περιοχής μεταξύ εξυπηρετητών DNS.

2.42) Μεταφέρονται 9 μηνύματα με αυτές τις αποκρίσεις. Τα 2 πακέτα IPv4 που τα μεταφέρουν είναι συνολικού μήκους 149 και 615 bytes αντίστοιχα.

2.43) Αυτό γίνεται κατανοητό από το γεγονός ότι τόσο το αίτημα όσο και οι αποκρίσεις έχουν το ίδιο Transaction ID.

2.44) Παρακάτω ακολουθεί σχετικός πίνακας με τις αποκρίσεις του εξυπηρετητή 147.102.222.210:

DNS Response #	Question	Answer RRs	Authority RRs	Additional RRs
1 (AXRP)	1	1	0	1
2 (SOA)	0	1	0	1
3 (SOA)	0	1	0	1
4 (SOA)	0	1	0	1
5 (SOA)	0	1	0	1
6 (SOA)	0	1	0	1
7 (SOA)	0	1	0	1
8 (SOA)	0	1	0	1
9 (SOA)	0	1	0	1

2.45) Έγινε αλλαγή πρωτοκόλλου στρώματος μεταφοράς όπως εντοπίστηκε στην ερώτηση 2.38, διότι ο μηχανισμός AXFT προορίζεται για μεταφορά μεγάλου όγκου δεδομένων, τα οποία μάλιστα είναι σημαντικά, επομένως πρέπει να εξασφαλιστεί αξιοπιστία μεταφοράς.

2.46) Το φίλτρο σύλληψης που πρέπει να χρησιμοποιήσω στο Wireshark για να καταγραφούν μόνο μηνύματα DNS είναι: `udp.port == 53` .

2.47) Το 1ο byte έχει τιμή: 1100 0000 και υποδεικνύει ότι πρέπει να είναι pointer, το 11ο byte έχει τιμή: 0000 0000 και αποτελεί το 1ο από τα 2 bytes από το πεδίο Data Length, το 4ο πριν το τέλος byte έχει τιμή: 0000 0000 και αποτελεί το 1ο byte από το minimum TTL πεδίο και το τελευταίο byte έχει τιμή: 1000 0000 και αποτελεί το τελευταίο byte από το minimum TTL πεδίο.

2.48) Τα 2 τελευταία byte στο παράθυρο με περιεχόμενα είναι pointer με offset 10110 = 22. Βάσει όμως το RFC 1035 το πραγματικό offset είναι +2 άρα 24. Η ετικέτα .ntua.gr επαναχρησιμοποιείται.

2.49) Επιλέγοντας τη διεύθυνση ηλεκτρονικού ταχυδρομείου του διαχειριστή παρατηρώ ότι και πάλι πρόκειται για κάποιο pointer, λογικά για το noc.ntua.gr, (από κάποιο primary name Server).