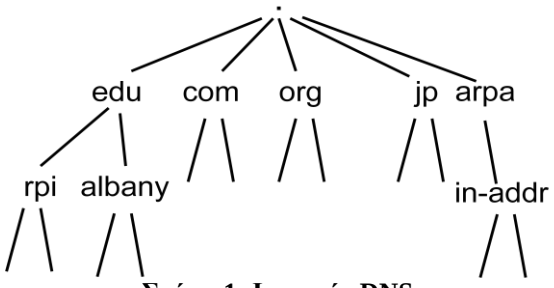
Εργαστηριακή Άσκηση 10
Σύστημα Ονομασίας Περιοχών DNS

Στο διαδίκτυο όνομα είναι μια αλφαριθμητική περιγραφή που απομνημονεύεται εύκολα και χρησιμοποιείται αντί της διεύθυνσης IP. Το όνομα συνίσταται σε μια ακολουθία *ετικετών (labels)* που χωρίζονται με τελείες. Οι ετικέτες αντιστοιχούν σε μια ιεραρχία *περιοχών (domains)* που μπορεί να παρασταθεί με δέντρο. Περιοχή είναι ένα υποδέντρο του δέντρου και *όνομα περιοχής (domain name)* είναι η ακολουθία των ετικετών που οδηγούν στη ρίζα του δέντρου. Σε ένα όνομα, δηλαδή, κάθε ετικέτα από τα αριστερά προς τα δεξιά αντιστοιχεί σε μία *υποπεριοχή (subdomain)* της περιοχής που ορίζει το υπόλοιπο το ονόματος προς τα δεξιά. Για παράδειγμα, το www.ntua.gr είναι ένα όνομα όπου το ntua είναι μια υποπεριοχή του gr και το www μια υποπεριοχή του ntua.gr.

Όπως αναφέρθηκε και στην Εργαστηριακή Άσκηση 2, το διαδίκτυο είναι χωρισμένο νοητά σε εκατοντάδες διαφορετικές *περιοχές ανωτάτου επιπέδου (top level domains)*, όπως com, edu, gov, int, mil, net, org, ae, …, gr, …, zw. Οι περιοχές ανωτάτου επιπέδου βρίσκονται κάτω από την *ρίζα (root)*, που συμβολίζεται με μια τελεία "." στο Σχήμα 1. Οι περιοχές ανωτάτου επιπέδου χωρίζονται με τη σειρά τους σε άλλες υποπεριοχές κοκ και ως φύλλα του δένδρου έχουμε τους hosts που περιλαμβάνει η καθεμία. Με τον τρόπο αυτό σχηματίζεται ο χώρος ονομάτων του παγκόσμιου συστήματος ονομασίας περιοχών DNS (Domain Name System). Πρόκειται για μια κατανεμημένη βάση δεδομένων στο διαδίκτυο που διατηρεί αντιστοιχίες ανάμεσα σε ονόματα και διευθύνσεις IP. Περιλαμβάνει μια ιεραρχία εξυπηρετητών ονομάτων μέσω των οποίων αναλυτές (resolvers) ερωτούν τους εξυπηρετητές περί του χώρου ονομάτων. Τα ονόματα στο DNS έχουν μήκος συνολικά το πολύ 255 byte, η κάθε ετικέτα μπορεί να έχει μέχρι 63 χαρακτήρες LDH (Letters, Digits, Hyphen) και επιτρέπονται το πολύ 127 τέτοιες. Για κάθε περιοχή στο διαδίκτυο (π.χ. ntua.gr) υπάρχει ένας ή περισσότεροι εξυπηρετητές DNS. Το πρωτόκολλο στρώματος εφαρμογών που επιτρέπει σε host, δρομολογητές και εξυπηρετητές να επικοινωνούν με την κατανεμημένη βάση δεδομένων για να μεταφράσουν ονόματα σε διευθύνσεις IP ή το αντίστροφο ονομάζεται και αυτό DNS.



Σχήμα 1: Ιεραρχία DNS

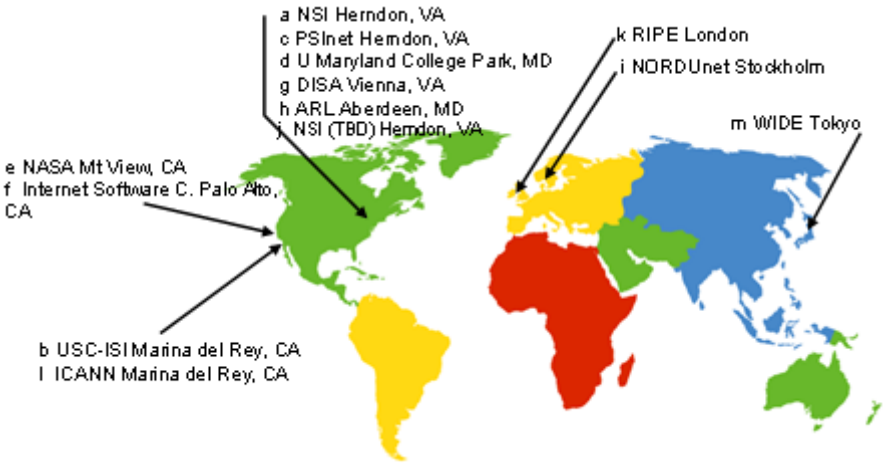
Οι εξυπηρετητές DNS περιέχουν μια βάση δεδομένων με εγγραφές πόρων (Resource Records – RR) διαφόρων τύπων. Οι εγγραφές τύπου A και/ή AAAA, αντιστοιχίζουν τα ονόματα των κόμβων της συγκεκριμένης περιοχής (π.χ. το atlas.central.ntua.gr) σε διευθύνσεις **IPv4** και/ή **IPv6**, αντίστοιχα. Οι εγγραφές τύπου NS (Name Server) δηλώνουν τις διευθύνσεις των «υπεύθυνων» για την περιοχή εξυπηρετητών DNS. Οι εγγραφές τύπου MX (Mail eXchanger) δίνουν τα ονόματα των εξυπηρετητών ηλεκτρονικού ταχυδρομείου για μια περιοχή DNS. Οι εγγραφές τύπου CNAME (Canonical NAME) δηλώνουν το κανονικό όνομα, δοθέντος ενός ψευδωνύμου, ώστε η αναζήτηση DNS να συνεχισθεί με το κανονικό όνομα. Τέλος, οι εγγραφές PTR (PoinTeR) αντιστοιχούν διευθύνσεις IP σε ονόματα, κλπ[1]. Οι εξυπηρετητές DNS απαντούν σε αιτήσεις άλλων εξυπηρετητών DNS καθώς και χρηστών του διαδικτύου για την αντιστοιχία ενός ονόματος σε διεύθυνση IP και το αντίστροφο, ερευνώντας την παγκόσμια ιεραρχία DNS γι' αυτά. Επειδή για

[1] Στην ιστοθέση https://en.wikipedia.org/wiki/List_of_DNS_record_types θα βρείτε την πλήρη λίστα με όλους τους τύπους εγγραφών πόρων στα αρχεία ζώνης (zone files) του DNS.

την εξυπηρέτηση μιας αίτησης μπορεί να γίνουν διαδοχικές αιτήσεις σε άλλους εξυπηρετητές, ακολουθώντας την παγκόσμια ιεραρχία DNS, το αποτέλεσμα θα είναι αυξημένη καθυστέρηση. Για την αποφυγή του παραπάνω οι εξυπηρετητές DNS διαθέτουν μια προσωρινή μνήμη (cache) όπου κρατούν τις πιο πρόσφατες αιτήσεις.

Η περιοχή ανωτάτου επιπέδου arpa (ίδιας στάθμης με τις com, edu, gov, int, mil, net, org, ae, …, gr, …, zw) αρχικά είχε διατεθεί στον πρόγονο του σημερινού διαδικτύου, το ARPANET, με την προοπτική να αποσυρθεί μετά την κατάργησή του. Σήμερα όμως χρησιμοποιείται για την απάντηση των αντίστροφων ερωτήσεων (reverse lookups) και περιλαμβάνει τις περιοχές in-addr και ip6. Οι διευθύνσεις IPv4 και IPv6, γραμμένες ως δεκαδικοί ή δεκαξαδικοί χαρακτήρες, σχηματίζουν τις υποπεριοχές. Έτσι τα αιτήματα για το ποιο είναι το όνομα ενός υπολογιστή δοθείσης της διεύθυνσης IP αυτού, ισοδυναμούν με αντιστοιχίες μεταξύ ονομάτων. Για παράδειγμα, στην περίπτωση του ntua.gr, η διεύθυνση υποδικτύου IPv4 είναι η 147.102.0.0/16 (πρώην κατηγορία B – πρόθεμα μήκους 16 bit). Έτσι, η πρώτη στάθμη κάτω από το in-addr.arpa είναι το πρώτο byte της διεύθυνσης IP (147), η επόμενη στάθμη είναι το δεύτερο byte (102), κοκ. Αυτό σημαίνει ότι η διεύθυνση IPv4 147.102.222.210 γράφεται στο DNS ως όνομα 210.222.102.147.in-addr.arpa στον κλάδο in-addr.arpa. Αντίστοιχα, η διεύθυνση IPv6 2001:db8::567:89ab γράφεται στο DNS ως όνομα b.a.9.8.7.6.5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa στον κλάδο ip6.arpa. Χωρίς αυτούς τους κλάδους του δέντρου DNS θα ήταν πρακτικά αδύνατη η μετάφραση διευθύνσεων σε ονόματα. Για να απαντηθεί ένα τέτοιο αίτημα θα έπρεπε να ερωτηθούν όλοι οι κόμβοι του δέντρου DNS κάτι που θα έπαιρνε εβδομάδες με το σημερινό μέγεθος του Internet.

Το ανώτατο επίπεδο στην ιεραρχία του DNS (η ρίζα του δέντρου) ονομάζεται *περιοχή κορυφής* (root zone), ενώ οι αντίστοιχοι *επίσημοι* (*authoritative*) εξυπηρετητές ονομάζονται *εξυπηρετητές κορυφής* (*root name servers*). Υπάρχουν 13 εξυπηρετητές κορυφής με ονόματα {a-m}.root-servers.net όπως στο Σχήμα 2, η φυσική θέση των οποίων είναι κατανεμημένη σε όλη την υφήλιο και η πρόσβαση σε αυτούς γίνεται με anycast. Κάθε αναζήτηση ονόματος DNS ξεκινάει είτε άμεσα από κάποιον εξυπηρετητή κορυφής ή έμμεσα από πληροφορία η οποία έχει ήδη ανακτηθεί από αυτόν και βρίσκεται στη μνήμη προσωρινής αποθήκευσης κάποιου εξυπηρετητή που βρίσκεται χαμηλότερα στην ιεραρχία. Χωρίς τους εξυπηρετητές κορυφής, το διαδίκτυο δεν μπορεί να λειτουργήσει. Αποτελούν κρίσιμη υποδομή, απαραίτητη για τη σωστή λειτουργία του παγκοσμίου ιστού, για την αποστολή ηλεκτρονικού ταχυδρομείου (e-mail), για τη χρήση περιφερειακών υπηρεσιών όπως FTP, Telnet κλπ.



Σχήμα 2: Root name servers

Ο σκοπός αυτής της εργαστηριακής άσκησης είναι η εξέταση του πρωτοκόλλου εφαρμογής DNS με τη βοήθεια της εντολής φλοιού nslookup και του αναλυτή πρωτοκόλλων Wireshark. Η εντολή φλοιού nslookup μπορεί να χρησιμοποιηθεί για τη λήψη πληροφοριών από ένα εξυπηρετητή DNS. Μέσω εντολών φλοιού μπορεί κανείς να ερωτήσει οποιοδήποτε (δημόσιο) εξυπηρετητή DNS για κάποια εγγραφή DNS. Ο ερωτώμενος εξυπηρετητής DNS μπορεί να είναι ένας εξυπηρετητής

κορυφής, ο υπεύθυνος εξυπηρετητής της περιοχής ή οποιοσδήποτε άλλος ενδιάμεσος εξυπηρετητής, τυπικά ο προκαθορισμένος στο εκάστοτε μηχάνημα. Για τον σκοπό αυτό σχηματίζουν αίτημα (query) προς τον προσδιοριζόμενο εξυπηρετητή που περιλαμβάνει ως ερώτηση τον τύπο της ζητούμενης πληροφορίας, λαμβάνουν κάποια απόκριση (response) από τον ερωτούμενο εξυπηρετητή είτε με παραπομπή σε άλλον εξυπηρετητή είτε με τη ζητούμενη, και πιθανώς επιπλέον, πληροφορίες και εμφανίζουν το αποτέλεσμα στην οθόνη. Σε περιβάλλον Windows χρησιμοποιείται η εντολή nslookup, η οποία υπάρχει και σε συστήματα Unix/Linux, αλλά με λιγότερες δυνατότητες. Μπορεί να κληθεί με ή χωρίς παραμέτρους και έχει δύο τρόπους λειτουργίας. Στο μη διαλογικό τρόπο λειτουργίας (non-interactive mode) ζητείται και λαμβάνεται μια συγκεκριμένη πληροφορία, ενώ στη διαλογική χρήση (interactive mode) ανοίγει νέο παράθυρο εντολών από όπου μπορεί να αναζητούνται περισσότερες της μίας πληροφορίες. Σε περιβάλλον Linux/Unix αντίστοιχες εντολές γραμμής είναι οι dig και host, που όμως δεν διαθέτουν διαλογικό τρόπο λειτουργίας.

Ακολουθεί παράδειγμα εκτέλεσης της εντολής nslookup σε μη διαλογικό τρόπο λειτουργίας (non-interactive mode), για την αναζήτηση της διεύθυνσης IP του www.ntua.gr. Το αντίστοιχο αίτημα στην περίπτωση Linux με dig γίνεται με την εντολή dig www.ntua.gr.

```
C:\>nslookup www.ntua.gr
Server:  priamos.telecom.ece.ntua.gr
Address:  147.102.7.1

Non-authoritative answer:
Name:    www.ntua.gr
Addresses:  2001:648:2000:329::101
          147.102.224.101
```

Στην προκειμένη περίπτωση, επειδή στα ορίσματα της εντολής δεν ορίστηκε ο εξυπηρετητής DNS που θα ερωτηθεί, χρησιμοποιείται αυτός που έχει οριστεί τοπικά στο σύστημα. Η έξοδος από την εκτέλεση της εντολής παρέχει δύο πληροφορίες: α) το όνομα (στο παράδειγμα είναι priamos.telecom.ece.ntua.gr) και την IP διεύθυνση, εδώ IPv4 147.102.7.1, του εξυπηρετητή DNS που απάντησε και β) την απόκριση που περιλαμβάνει τη διεύθυνση IPv6 2001:648:2000:329::101 και IPv4 147.102.224.101 του μηχανήματος με όνομα www.ntua.gr.

Στο επόμενο παράδειγμα χρησιμοποιείται η nslookup για την αναζήτηση των ονομάτων των υπεύθυνων εξυπηρετητών DNS της περιοχής et.gr, δηλαδή, η εγγραφή NS. Το αντίστοιχο αίτημα στην περίπτωση Linux με dig γίνεται με την εντολή dig ns et.gr.

```
C:\>nslookup -q=ns et.gr
Server:  priamos.telecom.ece.ntua.gr
Address:  147.102.7.1

Non-authoritative answer:
et.gr   nameserver = ns1.otenet.gr
et.gr   nameserver = ns2.otenet.gr

ns1.otenet.gr   internet address = 195.170.0.2
ns2.otenet.gr   internet address = 195.170.2.1
```

Στην nslookup, ο τύπος αιτήματος προσδιορίζεται από το όρισμα –q, σύντμηση του –querytype, όπου ο τύπος μπορεί να είναι A, AAAA, A+AAAA, ANY, CNAME, MX, NS, PTR, SOA, SRV. Στην περίπτωση της dig αρκεί να δηλωθεί ο ζητούμενος τύπος εγγραφής, πλην της PTR, όπου πρέπει να χρησιμοποιηθεί το όρισμα -x πριν από τη διεύθυνση IP.

Στο τελευταίο παράδειγμα ερωτάται απευθείας ο εξυπηρετητής DNS one.one.one.one, αντί του τοπικού, για τις διευθύνσεις IP του εξυπηρετητή ιστού www.cn.ntua.gr του εργαστηρίου Δικτύων Υπολογιστών. Το αντίστοιχο αίτημα στην περίπτωση Linux με dig γίνεται με την εντολή dig www.cn.ntua.gr @one.one.one.one.

```
C:\>nslookup www.cn.ntua.gr one.one.one.one
Server:  one.one.one.one
Address:  2606:4700:4700::1001

Non-authoritative answer:
Name:    www.cn.ece.ntua.gr
Address:  147.102.40.1
Aliases:  www.cn.ntua.gr
```

Από την απάντηση που επιστρέφεται είναι εμφανές ότι το κανονικό όνομα του εξυπηρετητή ιστού είναι www.cn.ece.ntua.gr και ότι αυτό για το οποίο ερωτήσαμε είναι ψευδώνυμο (alias).

Για τις παρακάτω ασκήσεις απαντήστε στο συνοδευτικό φυλλάδιο, το οποίο θα υποβάλλετε ως αρχείο pdf.

1. Υπηρεσία DNS

Για τους σκοπούς αυτού του μέρους της άσκησης θα συνδεθείτε με OpenVPN στο εσωτερικό δίκτυο του ΕΜΠ και θα χρησιμοποιήσετε την εντολή nslookup στο διαλογικό τρόπο λειτουργίας (interactive mode). Ανοίξτε ένα παράθυρο εντολών και πληκτρολογήστε nslookup ακολουθούμενο από <Enter>. Στη συνέχεια πληκτρολογήστε server 147.102.222.210 για να επιλέξετε τον εξυπηρετητή DNS που θα απαντά στη συνέχεια. Μέσω της υπο-εντολής set querytype μπορείτε να προσδιορίσετε το είδος πληροφοριών που θα αντλήσετε από τον εξυπηρετητή DNS. Προκειμένου να βρείτε πληροφορίες σχετικές με τους υπεύθυνους εξυπηρετητές μιας περιοχής DNS χρησιμοποιήστε την υπο-εντολή set q=ns.

1.1. Πληκτρολογήστε μια τελεία '.' και μετά <Enter>. Σε ποια περιοχή (στάθμη του Σχήματος 1) ανήκουν οι εξυπηρετητές DNS που εμφανίζονται;
1.2. Καταγράψτε το **πλήθος** των υπεύθυνων εξυπηρετητών DNS που εμφανίστηκαν καθώς και το όνομα και τη διεύθυνση IPv4 και IPv6 **ενός μόνο** από αυτούς.
1.3. Πληκτρολογήστε μια εντολή ώστε να επιλέξετε ως εξυπηρετητή DNS που θα απαντά στα επόμενα τον εξυπερετητή του προηγούμενου ερωτήματος. Ποια είναι η σύνταξη της εντολής;
1.4. Στη συνέχεια, πληκτρολογήστε 'gr.', προσοχή στην τελεία στο τέλος. Σε ποια περιοχή (στάθμη του Σχήματος 1) ανήκουν οι εξυπηρετητές DNS που εμφανίζονται;
1.5. Καταγράψτε το **πλήθος** των υπεύθυνων εξυπηρετητών DNS για την περιοχή 'gr.' καθώς και το όνομα και τη διεύθυνση IPv4 και IPv6 **ενός μόνο** από αυτούς.
1.6. Πληκτρολογήστε τώρα 'ntua.gr.'. Τι αποτελέσματα λαμβάνετε σε σύγκριση με αυτά του ερωτήματος 1.4 και τι συμπεραίνετε για το τι απαντούν οι εξυπηρετητές κορυφής;
1.7. Επιλέξετε ως εξυπηρετητή DNS που θα απαντά στα επόμενα έναν από τους τρεις τελευταίους της απάντησης που λάβατε στο προηγούμενο ερώτημα. Γράψτε τη σύνταξη της εντολής.
1.8. Πληκτρολογήστε τώρα 'ntua.gr.'. Η απάντηση που λαμβάνετε είναι ίδια με αυτήν που είδατε στην ερώτηση 1.6; Εξηγήστε γιατί.
1.9. Καταγράψτε το **πλήθος** των υπεύθυνων εξυπηρετητών DNS για την περιοχή 'ntua.gr.'. καθώς και το όνομα και τη διεύθυνση IPv4 **ενός μόνο** από αυτούς.
1.10. Κατόπιν, επιλέξτε ως εξυπηρετητή DNS αυτόν το όνομα του οποίου καταγράψατε προηγουμένως. Πληκτρολογήστε και πάλι 'ntua.gr.'. Η απάντηση που λαμβάνετε είναι ίδια με αυτήν που είδατε στην ερώτηση 1.8;
1.11. Πληκτρολογήστε το όνομα της περιοχής του Εργαστηρίου Δικτύων Υπολογιστών του Ε.Μ.Π. 'cn.ntua.gr.' και καταγράψτε το πλήθος των υπεύθυνων εξυπηρετητών DNS καθώς και το όνομα ενός από αυτούς που να μην ταυτίζεται με κάποιον από τους εξυπηρετητές της ερώτησης 1.9.
1.12. Βρείτε τα ονόματα των υπεύθυνων εξυπηρετητών DNS για **δύο** περιοχές Σχολών του ΕΜΠ, η μία εκ των οποίων να είναι κάποια εκ των ΑΜ, ΜΜΜ ή ΑΤΜ. Τι παρατηρείτε; *[Υπόδειξη:*

Για να βρείτε το όνομα των περιοχών επισκεφθείτε τη σελίδα https://www.ntua.gr/el/ και στη συνέχεια αφήστε τον δρομέα ακίνητο πάνω από τις εικόνες-ζεύξεις (Σχολές) στο κάτω μέρος της σελίδας. Προσοχή: αφαιρέστε το www. από το όνομα των εξυπηρετητών ιστού των Σχολών για να βρείτε το όνομα της περιοχής.]

Η πρώτη εγγραφή σε οποιοδήποτε αρχείο περιοχής DNS αποκαλείται Start of Authority (SOA). Η εγγραφή SOA δηλώνει ότι ο αυτός ο εξυπηρετητής DNS είναι η επίσημη πηγή πληροφόρησης για τα δεδομένα αυτής της περιοχής DNS. Η εγγραφή SOA περιέχει το όνομα του κύριου εξυπηρετητή DNS της περιοχής, τη διεύθυνση ηλεκτρονικού ταχυδρομείου του διαχειριστή της και ένα σειριακό αριθμό. Επιπλέον περιέχει πληροφορίες για το κάθε πότε (refresh time) ένας δευτερεύων εξυπηρετητής DNS ερωτά τον κύριο εξυπηρετητή DNS για αλλαγές που εντοπίζονται από την αύξηση της τιμής του σειριακού αριθμού. Εάν για κάποιο λόγο η μεταφορά πληροφορίας από τον κύριο εξυπηρετητή αποτύχει, ο δευτερεύων εξυπηρετητής επαναλαμβάνει μετά από λίγο (retry time) μέχρις ότου λήξει ο χρόνος (expire time). Σε αυτήν την περίπτωση, ο δευτερεύων σταματά να απαντά σε ερωτήσεις. Τέλος, με την παράμετρο TTL δηλώνεται ο χρόνος ζωής σε δευτερόλεπτα των δεδομένων στην προσωρινή μνήμη άλλων εξυπηρετητών. Κατά τη διάρκεια αυτή ένας εξυπηρετητής μπορεί να χρησιμοποιήσει τα αποθηκευμένα δεδομένα χωρίς να απευθυνθεί εκ νέου στους επίσημους εξυπηρετητές. Μπορείτε να αντλήσετε εγγραφές RR σχετικές με την αρχή επίσημης πληροφόρησης για μια περιοχή πληκτρολογώντας την υπο-εντολή set q=soa.

1.13. Καταγράψτε τον κύριο εξυπηρετητή DNS της περιοχής ‘cn.ntua.gr.’, την IPv4 διεύθυνσή του καθώς και τον σειριακό αριθμό.
1.14. Κάθε πόσες ώρες θα αναζητήσει αλλαγές σχετικά με την περιοχή ‘cn.ntua.gr.’ ένας δευτερεύων εξυπηρετητής;
1.15. Για πόσες ώρες διατηρούνται οι σχετικές με την περιοχή ‘cn.ntua.gr.’ εγγραφές στην προσωρινή μνήμη άλλων μη επίσημων εξυπηρετητών;
1.16. Επαναλάβετε τις ερωτήσεις 1.13 ως 1.15 για την περιοχή ‘ece.ntua.gr.’ της σχολής ΗΜΜΥ του ΕΜΠ.
1.17. Από τις τιμές των σειριακών αριθμών που καταγράψατε, μπορείτε να διακρίνετε κάποιο κανόνα σχετικό με το πώς μπορούν να παραχθούν αυτές, πλην του προφανούς της αύξησης κατά 1 κάθε φορά που γίνεται ενημέρωση των εγγραφών RR;

Για εγγραφές RR σχετικές με την αντιστοίχηση ονομάτων σε IP διευθύνσεις χρησιμοποιείται η υπο-εντολή set q=a για διευθύνσεις IPv4 και υπο-εντολή set q=aaaa για διευθύνσεις IPv6. Το αντίστροφο γίνεται χρησιμοποιώντας την υπο-εντολή set q=ptr.

1.18. Αναζητήστε στο διαδίκτυο και βρείτε τα ονόματα εξυπηρετητών ιστού τριών ελληνικών πανεπιστημίων. Καταγράψτε τα ονόματα και τις διευθύνσεις IPv4 (και IPv6 εάν διαθέτουν) αυτών των εξυπηρετητών ιστού. *[Υπόδειξη: Όταν αναζητούμε πληροφορίες για έναν συγκεκριμένο υπολογιστή, π.χ. έναν εξυπηρετητή ιστού, δεν παραλείπουμε να προσθέσουμε το “www.”, σε αντίθεση με την αναζήτηση πληροφοριών για περιοχές (domains).]*
1.19. Βρείτε και καταγράψτε το όνομα για δύο διευθύνσεις IPv4 (της προτίμησής σας) στο υπο-δίκτυο 147.102.40.16/30.
1.20. Αφού παρατηρήσετε την απόκριση του εξυπηρετητή στο προηγούμενο αίτημα, καταγράψετε τη μορφή αναπαράστασης της διεύθυνσης IPv4, η οποία χρησιμοποιείται από το σύστημα ονοματοδότησης. Έχει τη συνήθη αριθμητική μορφή μιας διεύθυνσης IPv4;

Ένας υπολογιστής μπορεί να είναι γνωστός στο διαδίκτυο με πολλά ονόματα (ψευδώνυμα – aliases). Ένα συνηθισμένο παράδειγμα τέτοιων υπολογιστών είναι αυτοί που φιλοξενούν ιστοσελίδες στο διαδίκτυο, όπου το δευτερεύον όνομά τους είναι το όνομα της ιστοθέσης που φιλοξενούν. Για την εύρεση του κανονικού ονόματος (canonical name) ενός υπολογιστή πληκτρολογήστε την υπο-εντολή set q=cname.

1.21. Καταγράψτε το κανονικό όνομα και τη διεύθυνση IPv4 του υπολογιστή που φιλοξενεί την ιστοθέση της Σχολής ΜΜΜ του Ε.Μ.Π.

Για την εύρεση των εξυπηρετητών ηλεκτρονικού ταχυδρομείου μιας περιοχής χρησιμοποιείται η υπο-εντολή set q=mx. Η σχετική εγγραφή περιλαμβάνει και την προτεραιότητα του εκάστοτε εξυπηρετητή ηλεκτρονικού ταχυδρομείου. Το πρωτόκολλο SMTP προσπαθεί να παραδώσει το ηλεκτρονικό ταχυδρομείο στον εξυπηρετητή με τον μικρότερο αριθμό προτίμησης.

1.22. Καταγράψτε τα ονόματα και τις διευθύνσεις IPv4 δύο εκ των εξυπηρετητών ηλεκτρονικού ταχυδρομείου της περιοχής 'arch.ntua.gr.'.
1.23. Ποιος από τους εξυπηρετητές είναι ο πρώτος που θα προτιμηθεί για την παράδοση ηλεκτρονικού ταχυδρομείου και γιατί;

Ένας εξυπηρετητής DNS μπορεί να πληροφορηθεί σχετικά με τις εγγραφές μιας άλλης περιοχής ζητώντας μια μεταφορά ζώνης (zone transfer). Με την nslookup στα Windows μπορείτε να ζητήσετε τις εγγραφές μιας άλλης περιοχής μέσω της υπο-εντολής ls. Σε Unix/Linux η συγκεκριμένη εντολή δεν είναι υλοποιημένη.

1.24. α) Σε περιβάλλον Windows πληκτρολογήστε την υπο-εντολή ls –d central.ntua.gr. Ποια είναι η σημασία της παραπάνω σύνταξης της υπο-εντολής ls;
β) Σε περιβάλλον Linux, αφού εξέλθετε της nslookup με exit, πληκτρολογήστε dig axfr central.ntua.gr @147.102.222.210. Τι σημαίνει το afxr; *[Υπόδειξη: Συμβουλευτείτε προαναφερθείσα ιστοσελίδα https://en.wikipedia.org/wiki/List_of_DNS_record_types.]*
1.25. Για κάθε είδος εγγραφής (π.χ. NS, MX, A, AAAA, CNAME, HINFO, TXT, SOA, κλπ.) που θα συναντήσετε στην απάντηση της προηγούμενης ερώτησης καταγράψτε τα πλήρη στοιχεία **μίας** περίπτωσης.

2 – Πρωτόκολλο DNS

Σε αυτό το μέρος της άσκησης θα δείτε τη δομή των μηνυμάτων που χρησιμοποιεί το πρωτόκολλο DNS με τη βοήθεια του Wireshark. Περισσότερες πληροφορίες για τα μηνύματα του DNS μπορείτε να βρείτε στην ιστοσελίδα: http://www.networksorcery.com/enp/protocol/dns.htm. Θα χρησιμοποιήσετε τη λειτουργία *Capture* με φίλτρο, ώστε τα πλαίσια που καταγράφονται να περιέχουν κάποια συγκεκριμένα χαρακτηριστικά. Υπενθυμίζεται ότι το φίλτρο απεικόνισης *(Display)*, που επιλέγετε από το μενού *Analyze*, μπορεί να (απ)ενεργοποιηθεί οποιαδήποτε στιγμή κατά τη διάρκεια της καταγραφής, καθώς επίσης και μετά την ολοκλήρωση αυτής, προκειμένου να αποκρύπτει (αποκαλύπτει) κάποια από τα συλληφθέντα πλαίσια, ενώ το φίλτρο σύλληψης, που επιλέγετε από το μενού *Capture*, ενεργοποιείται πάντοτε **πριν** ξεκινήσει η διαδικασία καταγραφής, με αποτέλεσμα να καταγράφεται μόνο ένα μέρος των διερχόμενων πλαισίων. Προσοχή: η απενεργοποίηση του φίλτρου απεικόνισης γίνεται πιέζοντας το κουμπί Clear (η διαγραφή του φίλτρου στο πεδίο εισαγωγής δεν το ακυρώνει!).

Και για αυτό το μέρος της άσκησης θα συνεχίσετε συνδεδεμένοι με OpenVPN στο εσωτερικό δίκτυο του ΕΜΠ. Με τη βοήθεια του Wireshark να καταγράψετε την κίνηση ενώ κάνετε χρήση της υπηρεσίας DNS. Εφαρμόστε φίλτρο σύλληψης για να παρατηρείτε μόνο την κίνηση που σχετίζεται με τη διεύθυνση IP του υπολογιστή σας και ξεκινήστε την καταγραφή. Καθαρίστε την προσωρινή μνήμη DNS (DNS cache) που διατηρεί ο υπολογιστής χρησιμοποιώντας την κατάλληλη εντολή φλοιού ανάλογα με το λειτουργικό σύστημα που χρησιμοποιείτε. Στη συνέχεια εκτελέστε την εντολή φλοιού nslookup – 147.102.1.1 ακολουθούμενη από <Enter> ώστε να εισέλθετε στο διαλογικό τρόπο λειτουργίας με αρχικό εξυπηρετητή DNS τον 147.102.1.1. Δώστε αρχικά την εντολή set domain=. ώστε να μην δημιουργεί το nslookup περιττά αιτήματα επισυνάπτοντας το όνομα της τοπικής περιοχής στο όνομα που δίνετε. Μετά βρείτε το όνομα του υπολογιστή 147.102.40.10 έχοντας ως εξυπηρετητή DNS τον υπολογιστή 147.102.40.1. Επαναλάβετε το αίτημα με εξυπηρετητή τον 147.102.7.1 και τερματίστε την καταγραφή. Εφαρμόστε κατάλληλο φίλτρο απεικόνισης ώστε να παραμείνουν μόνο μηνύματα του πρωτοκόλλου DNS.

2.1 Ποια είναι η ακριβής σύνταξη της εντολής που χρησιμοποιήσατε για τον καθαρισμό της προσωρινής μνήμης DNS; *[Υπόδειξη: Δείτε σχετικές οδηγίες στην Εργαστηριακή Άσκηση 7, μέρος 4. Μετάδοση δεδομένων με UDP.]*
2.2 Ποια είναι η σύνταξη του φίλτρου σύλληψης που χρησιμοποιήσατε;
2.3 Ποιες υπο-εντολές της nslookup χρησιμοποιήσατε για να βρείτε το ζητούμενο όνομα υπολογιστή;
2.4 Ποιο είναι το όνομα του 147.102.40.10;
2.5 Ποια είναι η σύνταξη του φίλτρου απεικόνισης που χρησιμοποιήσατε;
2.6 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιήθηκε από το DNS (TCP ή UDP);
2.7 Πόσα αιτήματα προς εξυπηρετητές DNS έγιναν από τον υπολογιστή σας;
2.8 Εάν έγιναν περισσότερα των δύο, ποιος ήταν ο λόγος;
2.9 Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιήθηκαν σε ένα αίτημα και την αντίστοιχη απόκριση.
2.10 Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής DNS;

Τα μηνύματα DNS έχουν την ίδια μορφή τόσο για τα αιτήματα (queries) όσο και για τις αποκρίσεις (responses). Διαθέτουν μια επικεφαλίδα σταθερού μήκους ακολουθούμενη από δεδομένα μεταβλητού μήκους που χωρίζονται σε τέσσερα τμήματα: τις ερωτήσεις, τις εγγραφές RR (Resource Records) για τις απαντήσεις, τις εγγραφές RR για τους επίσημους (authoritative) εξυπηρετητές και επιπρόσθετες (additional) εγγραφές RR. Δείτε λεπτομέρειες http://www.networksorcery.com/enp/default.htm. Τα πεδία της επικεφαλίδας ορίζουν το περιεχόμενο των τεσσάρων τμημάτων, το πλήθος των ερωτήσεων και το πλήθος των εγγραφών RR κάθε κατηγορίας. Παρατηρώντας το περιεχόμενο των πεδίων της επικεφαλίδας των μηνυμάτων DNS, απαντήστε τις επόμενες ερωτήσεις.

2.11 Τι μήκος έχει η επικεφαλίδα DNS;
2.12 Καταγράψτε το Transaction ID του πρώτου αιτήματος για το όνομα του 147.102.40.10 και της αντίστοιχης απόκρισης. Ποια είναι η σχέση μεταξύ τους;
2.13 Τι μήκος έχει το πεδίο Flags της επικεφαλίδας DNS;
2.14 Ποιο κατά σειρά bit του πεδίου Flags της επικεφαλίδας DNS δηλώνει αν το συγκεκριμένο μήνυμα είναι αίτημα ή απόκριση;
2.15 Ποιο κατά σειρά bit του πεδίου Flags δείχνει το κατά πόσο η απόκριση προέρχεται από τον επίσημο εξυπηρετητή DNS;
2.16 Στο πρώτο αίτημα για την εύρεση του ονόματος του 147.102.40.10, πόσες ερωτήσεις περιέχονται, πόσες εγγραφές RR απαντήσεων, πόσες επίσημων εξυπηρετητών και πόσες επιπρόσθετες;
2.17 Παρατηρήστε την απόκριση στο προηγούμενο αίτημα. Περιλαμβάνει την ερώτηση για την οποία απαντά;
2.18 Πόσες εγγραφές RR απαντήσεων, πόσες επίσημων εξυπηρετητών και πόσες επιπρόσθετες περιλαμβάνει;
2.19 Εμφανίσθηκαν όλες οι προηγούμενες πληροφορίες για εγγραφές RR στο παράθυρο της γραμμής εντολών;

Ξεκινήστε μια νέα καταγραφή με το προηγούμενο φίλτρο σύλληψης. Εκτελέστε την υπο-εντολή `set q=a` της nslookup για να βρείτε τη διεύθυνση IPv4 του www.youtube.com και κατόπιν την υπο-εντολή `set q=aaaa` για να βρείτε τη διεύθυνση IPv6 του www.cnn.com. Στη συνέχεια σταματήστε την καταγραφή και εφαρμόστε κατάλληλο φίλτρο ώστε να παραμείνουν μόνο μηνύματα DNS, αποκρίσεις, από τον εξυπηρετητή DNS.

2.20 Ποια είναι η σύνταξη του νέου φίλτρου απεικόνισης; *[Υπόδειξη: Επιλέξτε το bit της επικεφαλίδας που δηλώνει ότι πρόκειται για απόκριση και μετά δεξί κλικ, Apply as filter → Selected.]*
2.21 Πόσες διευθύνσεις IPv4 φέρεται να έχει το www.youtube.com σύμφωνα με το αποτέλεσμα της εντολής nslookup;

2.22 Εντοπίστε το μήνυμα που μεταφέρει την απόκριση του εξυπηρετητή DNS στο αίτημα για να βρεθεί η διεύθυνση IPv4 του ονόματος www.youtube.com. Πόσες ερωτήσεις περιλαμβάνει;
2.23 Πόσες και ποιου είδους εγγραφές RR περιλαμβάνει το τμήμα της απάντησης στην παραπάνω απόκριση;
2.24 Πώς σχετίζονται οι εγγραφές αυτές με τις διευθύνσεις IPv4 που προσδιορίσατε στην ερώτηση 2.21;
2.25 Για ποιο λόγο στο τμήμα της απάντησης στην παραπάνω απόκριση υπάρχει και μια εγγραφή RR τύπου CNAME;
2.26 Κατά τη γνώμη σας, η ιστοθέση www.youtube.com φιλοξενείται από έναν υπολογιστή ή περισσότερους; Αιτιολογήστε. *[Υπόδειξη: Μέσω της nslookup ξαναβρείτε τη διεύθυνση IPv4 του www.youtube.com και παρατηρήστε τις διαφορές με την προηγούμενη απόκριση του εξυπηρετητή DNS.]*
2.27 Εντοπίστε το μήνυμα που μεταφέρει την απόκριση του εξυπηρετητή DNS στο αίτημα για να βρεθεί η διεύθυνση IPv6 του ονόματος www.cnn.com. Πόσες εγγραφές RR περιλαμβάνει το τμήμα της απάντησης για διευθύνσεις IPv6 του www.cnn.com;
2.28 Πόσες εγγραφές RR περιλαμβάνει το τμήμα της απάντησης για τους επίσημους εξυπηρετητές DNS; Για ποια περιοχή DNS είναι αυτοί υπεύθυνοι και γιατί;
2.29 Πόσες επιπρόσθετες εγγραφές RR επιστρέφονται στην απόκριση για το www.cnn.com; Τι τύπου είναι αυτές και ποια πληροφορία μεταφέρουν;
2.30 Καταγράψτε το όνομα και τη διεύθυνση IPv4 ενός εκ των επίσημων εξυπηρετητών DNS που περιλαμβάνει η απόκριση για το www.cnn.com;

Ξεκινήστε μια νέα καταγραφή με το προηγούμενο φίλτρο σύλληψης. Εκτελέστε τις επόμενες υποεντολές της nslookup:

- set q=any και βρείτε όλες τις εγγραφές για τον εξυπηρετητή ιστού www.ntua.gr
- set q=soa και βρείτε την αρχή πληροφόρησης για την περιοχή cslab.ntua.gr
- set q=cname και βρείτε το επίσημο όνομα του www.cn.ntua.gr
- set q=mx και βρείτε τους εξυπηρετητές ηλεκτρονικού ταχυδρομείου της περιοχής elab.ntua.gr

σταματήστε την καταγραφή και εφαρμόστε φίλτρο απεικόνισης ώστε να παραμείνουν μόνο μηνύματα σχετικά με το πρωτόκολλο DNS. Με βάση τα αποτελέσματα της καταγραφής απαντήστε στις ακόλουθες ερωτήσεις:

2.31 Καταγράψτε το πλήθος των εγγραφών RR που περιέχει το τμήμα της απάντησης στην απόκριση για τον www.ntua.gr καθώς και τις πληροφορίες που αυτά περιέχουν.
2.32 Καταγράψτε το πλήθος των εγγραφών RR που περιέχει η απόκριση σχετικά με την αρχή πληροφόρησης για την περιοχή cslab.ntua.gr.
2.33 Ποιο είναι το όνομα (mname – master name) του κύριου εξυπηρετητή DNS της περιοχής cslab.ntua.gr και ποια η διεύθυνση ηλεκτρονικού ταχυδρομείου (rname – responsible's name) του διαχειριστή αυτής; *[Υποδ. Δείτε https://en.wikipedia.org/wiki/SOA_record σχετικά με τα πεδία mname και rname.]*
2.34 Πλην του κύριου εξυπηρετητή, ποιοι είναι οι άλλοι επίσημοι εξυπηρετητές για την περιοχή cslab.ntua.gr;
2.35 Καταγράψτε το πλήθος των εγγραφών που περιέχει η απόκριση σχετικά με το κανονικό όνομα του www.cn.ntua.gr καθώς και το κανονικό όνομα αυτού.
2.36 Καταγράψτε το πλήθος των εγγραφών που περιέχει η απόκριση σχετικά με τους αρμόδιους εξυπηρετητές ηλεκτρονικού ταχυδρομείου της περιοχής elab.ntua.gr καθώς και το όνομα του πλέον προτιμότερου εξ αυτών.

Στη συνέχεια ξεκινήστε νέα καταγραφή με το Wireshark με φίλτρα καταγραφής και απεικόνισης όπως πριν. Σε περιβάλλον Windows στο παράθυρο εντολών της nslookup επιλέξτε ως εξυπηρετητή τον 147.102.222.210 και δώστε την εντολή ls –d planetlab.ntua.gr, πληκτρολογήστε exit για έξοδο

και σταματήστε την καταγραφή. Σε περιβάλλον Linux, αφού εξέλθετε της nslookup με exit, πληκτρολογήστε dig axfr planetlab.ntua.gr @147.102.222.210.

2.37 Πόσα αιτήματα DNS έγιναν, πόσες αποκρίσεις DNS λήφθηκαν και ποιο πρωτόκολλο μεταφοράς χρησιμοποιήθηκε;

2.38 Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιήθηκε για το αίτημα προς τον εξυπηρετητή 147.102.222.210 και τις αποκρίσεις που ελήφθησαν.

2.39 Ποιο είναι το μήκος του αιτήματος προς τον εξυπηρετητή 147.102.222.210; *[Υπόδειξη: Επιλέξτε τη γραμμή που αντιστοιχεί στο πρωτόκολλο DNS στο παράθυρο με τις λεπτομέρειες επικεφαλίδας του Wireshark, οπότε στο κατώτατο μέρος της οθόνης θα εμφανισθεί το πλήθος των byte που το συνθέτουν.]*

2.40 Ποιος είναι ο τύπος του αιτήματος και ποιο το νόημά του; *[Υπόδειξη: Δείτε ιστοσελίδα https://en.wikipedia.org/wiki/DNS_zone_transfer.]*

2.41 Εντοπίστε τις αποκρίσεις του εξυπηρετητή 147.102.222.210. Τι μήκος έχουν και πόσα μηνύματα DNS (response) μεταφέρονται με αυτές; *[Υπόδειξη: Σε κάθε μήνυμα DNS αντιστοιχεί μία επικεφαλίδα πρωτοκόλλου DNS στο παράθυρο με τις λεπτομέρειες επικεφαλίδων.]*

2.42 Πώς γίνεται κατανοητό ότι τα προηγούμενα μηνύματα DNS αποτελούν την απάντηση στο αίτημα που έγινε; *[Υπόδειξη: Δείτε τιμές πεδίου Transaction ID.]*

2.43 Πόσες εγγραφές RR για ερωτήσεις, απαντήσεις, επίσημους εξυπηρετητές και επιπρόσθετες πληροφορίες περιλαμβάνει το κάθε μήνυμα DNS (response) που περιέχεται στις αποκρίσεις του εξυπηρετητή 147.102.222.210;

2.44 Γιατί νομίζετε ότι έγινε η αλλαγή πρωτοκόλλου στρώματος μεταφοράς που εντοπίσατε στην ερώτηση 2.37;

2.45 Ποιο φίλτρο σύλληψης πρέπει να χρησιμοποιήσετε στο Wireshark για να καταγράφετε μόνο μηνύματα DNS;

Όνοματεπώνυμο:	**Ομάδα:**
Όνομα PC/ΛΣ:	**Ημερομηνία: / /**
Διεύθυνση IP: . . .	**Διεύθυνση MAC: - - - - -**

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 .....

1.2 .....

.....

.....

1.3 .....

1.4 .....

.....

1.5 .....

.....

.....

1.6 .....

.....

1.7 .....

1.8 .....

.....

1.9 .....

.....

1.10 .....

.....

1.11 .....

.....

1.12 .....

.....

.....

1.13 .....

.....

.....

1.14 .....

2