Εργαστηριακή Άσκηση 12
Υπηρεσίες στο Διαδίκτυο

Σε αυτήν την άσκηση θα εγκαταστήσετε μερικές από τις πιο βασικές υπηρεσίες που απαιτούνται για τη λειτουργία ενός δικτύου, συγκεκριμένα, dhcp, dns, http κλπ. Θα κατασκευάσετε ένα δρομολογητή βασισμένο σε FreeBSD που να παρέχει συνδυασμένα εξυπηρετητή DHCP, εξυπηρετητή DNS και τείχος προστασίας Firewall, όπως συμβαίνει σε έναν οικιακό δρομολογητή, και στη συνέχεια θα προσθέσετε έναν εξυπηρετητή ιστοσελίδων. Θα συνδέσετε το "οικιακό" δίκτυο με ένα δεύτερο δρομολογητή και εξυπηρετητή DNS ως εάν ήταν το δημόσιο δίκτυο Internet. Για τη δρομολόγηση δεν θα χρησιμοποιήσετε το Quagga/FRR, απλώς θα ενεργοποιήσετε την εγγενή δυνατότητα δρομολόγησης που παρέχει το FreeBSD. Σε περιβάλλον FreeBSD για να εγκαταστήσετε μια τέτοια υπηρεσία ακολουθείτε τα επόμενα βήματα:

1. Εγκατάσταση του κατάλληλου πακέτου (package) λογισμικού που υλοποιεί την υπηρεσία.
2. Παραμετροποίηση της υπηρεσίας μέσω των σχετικών με αυτή αρχείων conf.
3. Εγγραφή της κατάλληλης εντολής στο αρχείο /etc/rc.conf ώστε η υπηρεσία να είναι διαθέσιμη μετά την επανεκκίνηση του μηχανήματος.
4. Εισαγωγή των αναγκαίων μεταβλητών στο αρχείο /etc/rc.conf με τη βοήθεια της εντολής *sysrc*.
5. Επιβεβαίωση με την εντολή *service name rcvar*, όπου *name* το όνομα της υπηρεσίας, της ύπαρξης κατάλληλης εγγραφής στο αρχείο /etc/rc.conf, τυπικά της μορφής name_enable="YES".
6. Εκκίνηση, σταμάτημα ή επανεκκίνηση της υπηρεσίας με την εντολή *service name onestart | start | stop | restart*, όπου *name* το όνομα της υπηρεσίας.

Για περισσότερες πληροφορίες σχετικά με τον χειρισμό των υπηρεσιών στο FreeBSD μέσω του /etc/rc.conf δείτε την ιστοσελίδα https://docs.freebsd.org/en/books/handbook/config/#configtuning-rcd καθώς τις σελίδες man των εντολών service και sysrc.

1. Το πρωτόκολλο DHCP

Το Dynamic Host Control Protocol (DHCP) είναι ένα τυποποιημένο πρωτόκολλο βάσει του RFC 2131, που δημιουργήθηκε από την ανάγκη απλοποίησης της διαχείρισης δικτύων βασισμένων στο TCP/IP. Παλαιότερα τα περισσότερα τοπικά δίκτυα είχαν περιορισμένο αριθμό σταθερών υπολογιστών κάτι που επέτρεπε τη στατική ανάθεση IPv4 διευθύνσεων. Αυτό προϋπέθετε τη δια χειρός αλλαγή και ρύθμιση των διευθύνσεων οι οποίες αποθηκεύονταν στο δίσκο του υπολογιστή. Αν χρειαζόταν ποτέ ένας υπολογιστής να αλλάξει διεύθυνση τότε αυτό γίνονταν από την κονσόλα του και συνήθως απαιτούσε επανεκκίνηση. Σχετικά σύντομα, και καθώς άρχισαν να δημιουργούνται όλο και πιο σύνθετα δίκτυα, υπήρξε η ανάγκη για κεντρική διαχείριση των διευθύνσεων IPv4. Το DHCP ορίζει μηχανισμούς δυναμικής εκχώρησης διευθύνσεων IPv4 στους σταθμούς εργασίας ως δάνειο για καθορισμένο χρονικό διάστημα. Έτσι επιτυγχάνεται η επαναχρησιμοποίηση ενός αριθμού διευθύνσεων IPv4 από πολλούς σταθμούς εργασίας. Επιπλέον το DHCP παρέχει τον μηχανισμό με τον οποίο ο σταθμός εργασίας μπορεί μόνος του να ανασύρει τις πληροφορίες που απαιτούνται προκειμένου να λειτουργήσει στο δίκτυο.

Σε συντομία, η λειτουργία του DHCP είναι η ακόλουθη. Μόλις ο υπολογιστής εκκινήσει εκπέμπει ένα μήνυμα αναζήτησης (*DHCP Discover*) εξυπηρετητή DHCP. Οι εξυπηρετητές DHCP που ακούνε αυτό το μήνυμα, απαντούν με μήνυμα προσφοράς (*DHCP Offer*) το οποίο ορίζει διευθύνσεις IPv4. Ο υπολογιστής επιλέγει μία προσφορά και εκπέμπει αίτηση (*DHCP Request*) προς όλους τους εξυπηρετητές δηλώνοντας τη συγκεκριμένη διεύθυνση IPv4 που επέλεξε. Όλοι οι άλλοι

εξυπηρετητές αποχωρούν και ο επιλεχθείς εξυπηρετητής στέλνει επιβεβαίωση (*DHCP ACK*) για την εκχωρούμενη διεύθυνση IPv4. Ο πελάτης επιβεβαιώνει στο τέλος της ανταλλαγής των μηνυμάτων *DHCP Discover/Offer/Request/ACK* ότι η διεύθυνση IPv4 που εκχωρήθηκε δεν χρησιμοποιείται από άλλον. Η διεύθυνση IPv4 παραχωρείται με δάνειο για συγκεκριμένο χρονικό διάστημα (lease time). Προτού λήξει το διάστημα αυτό, ο υπολογιστής πρέπει να ανανεώσει το δάνειο. Όταν ο υπολογιστής τελειώσει, στέλνει μήνυμα απόλυσης (*DHCP Release*) της διεύθυνσης.

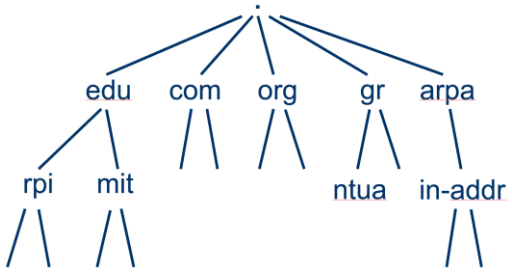
Ουσιαστικά, το DHCP αναλαμβάνει να ορίσει αυτόματα, χωρίς την παρουσία διαχειριστή δικτύου, τις αναγκαίες παραμέτρους λειτουργίας ενός υπολογιστή. Το DHCP υποστηρίζει 3 μηχανισμούς για να αντιστοιχίζει διευθύνσεις:

- Δυναμική αντιστοίχιση (εκχώρηση μιας διεύθυνσης IPv4 για συγκεκριμένο διάστημα)
- Αυτόματη αντιστοίχιση (μόνιμη εκχώρηση μιας διαθέσιμης διεύθυνσης IPv4)
- Χειροκίνητη αντιστοίχιση (εκχώρηση με βάση τη διεύθυνση MAC του αιτούντος)

Τα σχετικά στοιχεία με τα δάνεια εγγράφονται σε αρχεία τόσο στην πλευρά του εξυπηρετητή όσο και του πελάτη. Στην πλευρά του εξυπηρετητή καταγράφεται η ημερομηνία ανάθεσης και η ημερομηνία λήξης του δανείου για κάθε διεύθυνση IPv4 που έχει εκχωρηθεί. Στην πλευρά του πελάτη για το δάνειο που λαμβάνει καταγράφεται η ημερομηνία ανανέωσης (renew), επανασύνδεσης (rebind) και λήξης (expire) του δανείου. Ημερομηνία ανανέωσης είναι η χρονική στιγμή όπου ο πελάτης DHCP πρέπει να ξεκινήσει την προσπάθεια ανανέωσης του δανείου από τον εξυπηρετητή που το έλαβε. Ημερομηνία επανασύνδεσης είναι η χρονική στιγμή όπου ο πελάτης DHCP πρέπει θα ξεκινήσει τη διαδικασία δανεισμού μια νέας διεύθυνσης από οποιονδήποτε άλλο εξυπηρετητή (εάν δεν κατορθώσει την ανανέωση). Ημερομηνία λήξης είναι η χρονική στιγμή όπου ο πελάτης DHCP θα σταματήσει να χρησιμοποιεί τη διεύθυνση IPv4 που έλαβε ως δάνειο εάν δεν έχει κατορθώσει να την ανανεώσει ή να λάβει νέα.

2. Υπηρεσία DNS

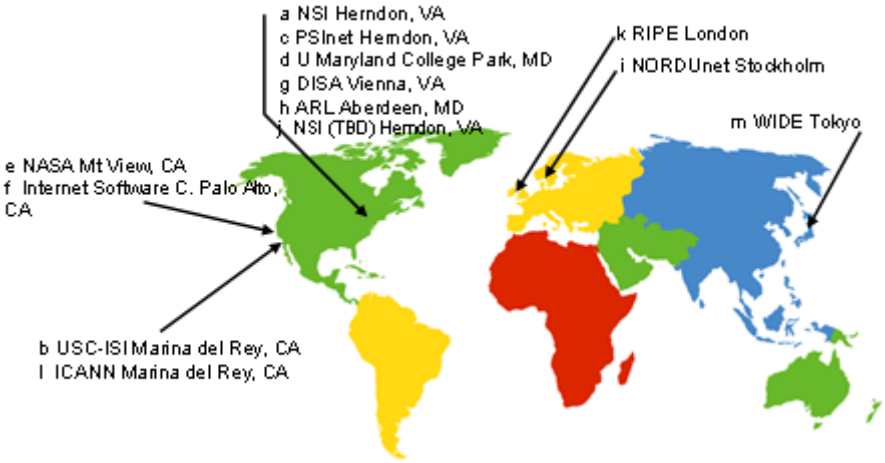
Το DNS είναι απαραίτητο για τη σωστή λειτουργία του παγκοσμίου ιστού (www), για την αποστολή ηλεκτρονικού ταχυδρομείου (e-mail), για τη χρήση περιφερειακών υπηρεσιών όπως FTP, Telnet κλπ. Τα ονόματα στο διαδίκτυο είναι χωρισμένα νοητά σε εκατοντάδες διαφορετικές **περιοχές** (domains) υψηλού επιπέδου, οι οποίες χωρίζονται με τη σειρά τους σε άλλες υποπεριοχές (subdomains) με πολλούς hosts η καθεμία. Η ιεραρχία των περιοχών μπορεί να παρασταθεί με ένα δέντρο όπως στο σχήμα. Το όνομα κάθε host αποτελείται από μια ακολουθία *ετικετών* (labels) που χωρίζονται με τελείες (π.χ. www.mit.edu). Μια περιοχή είναι ένα υποδέντρο του παγκόσμιου δέντρου ονομάτων. Το όνομα περιοχής (domain name) για ένα host είναι η ακολουθία των ετικετών που οδηγούν από το host (φύλλο στο δέντρο ονομάτων) στην κορυφή (ρίζα) του παγκόσμιου δέντρου ονομάτων.



Σχήμα 1: Ιεραρχία DNS

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 {a-m}.root-servers.net. Οι IP διευθύνσεις τους είναι εκ των προτέρων γνωστές (https://www.internic.net/zones/named.root). Ερωτώνται από

τους τοπικούς εξυπηρετητές ονομάτων όταν δεν μπορούν να αναλύσουν κάποιο όνομα. Έτσι 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.



Σχήμα 2: Root name servers

Κάτω από την κορυφή υπάρχουν οι περιοχές ανώτατου επιπέδου (top level domains), η διαχείριση τους (εκτός της .int και .arpa) έχει εκχωρηθεί από την IANA σε άλλους υπεύθυνους οργανισμούς, π.χ. EDUCAUSE για την περιοχή .edu. Η διαχείριση του χώρου ονομάτων κάτω από τις περιοχές ανώτατου επιπέδου έχει εκχωρηθεί σε οργανισμούς, που μπορούν να εκχωρήσουν περαιτέρω τη διαχείριση υπο-περιοχών τους. Η ονομασία περιοχής ανώτατου επιπέδου arpa (ίδιας στάθμης με τις com, edu, gov, int, mil, net, org, ae, …, gr, …, zw) μαζί με τις υπο-περιοχές (που βρίσκονται αμέσως από κάτω της) in-addr και ip6.arpa χρησιμοποιείται από το DNS προκειμένου να απαντηθούν οι ερωτήσεις για το ποιο είναι το όνομα ενός υπολογιστή, δοθείσης της διεύθυνσης IPv4 ή IPv6 αυτού (Reverse Lookup). 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 πρέπει να είναι το πρώτο byte της διεύθυνσης IPv4 (147), η επόμενη στάθμη πρέπει να είναι το δεύτερο byte (102), κοκ. Αυτό σημαίνει ότι το όνομα DNS του υπολογιστή 147.102.222.210 είναι το 210.222.102.147.in-addr.arpa. Αντίστοιχα, η διεύθυνση IPv6 του ίδιου μηχανήματος είναι 2001:648:2000:de::210 και σχετική εγγραφή για αντίστροφη αναζήτηση είναι 0.1.2.0.0.0.0.0.0.0.0.0.0.0.0.0.e.d.0.0.0.0.0.2.8.4.6.0.1.0.0.2.ip6.arpa. Χωρίς αυτόν τον κλάδο του δέντρου DNS θα ήταν πρακτικά αδύνατη η μετάφραση διευθύνσεων σε ονόματα (για να απαντηθεί μια τέτοια ερώτηση θα έπρεπε να ερωτηθούν όλοι οι κόμβοι του δέντρου DNS κάτι που θα έπαιρνε εβδομάδες με το σημερινό μέγεθος του Internet).

Σε κάθε περιοχή στο διαδίκτυο (π.χ. ntua.gr) υπάρχει ένας ή περισσότεροι εξυπηρετητές DNS. Αυτοί περιέχουν μια βάση δεδομένων (ζώνη στην ορολογία του DNS) οι εγγραφές της οποίας αποκαλούνται εγγραφές πόρων (Resource Records – RR). Για πληροφορίες σχετικές με την αντιστοίχιση ονομάτων σε IP διευθύνσεις χρησιμοποιούνται οι εγγραφές τύπου A (address) και/ή AAAA που αντιστοιχίζουν τα ονόματα των κόμβων της συγκεκριμένης περιοχής (π.χ. atlas.central.ntua.gr) σε διευθύνσεις **IPv4** και/ή **IPv6**. Το αντίστροφο γίνεται χρησιμοποιώντας την εγγραφή τύπου PTR (pointer). Επίσης η βάση μπορεί να περιέχει εγγραφές τύπου NS (name servers) με τις διευθύνσεις άλλων εξυπηρετητών DNS «υπεύθυνων» για την περιοχή.

Η πρώτη εγγραφή σε οποιοδήποτε αρχείο περιοχής DNS αποκαλείται Start of Authority (SOA). Η εγγραφή SOA δηλώνει ότι αυτός ο εξυπηρετητής DNS είναι η επίσημη πηγή πληροφόρησης για τα δεδομένα αυτής της περιοχής DNS. Η εγγραφή SOA περιλαμβάνει ένα σειριακό αριθμό, που συνήθως είναι η ημερομηνία της τελευταίας αλλαγής ακολουθούμενη από ένα αύξοντα αριθμό, που

καθιστά την κατανεμημένη βάση δεδομένων συνεπή (consistent). Ο αριθμός αυτός αυξάνει με κάθε αλλαγή και έτσι γίνεται αντιληπτή η αλλαγή των δεδομένων. Εκτός από το όνομα του κύριου εξυπηρετητή DNS της περιοχής, η εγγραφή SOA περιέχει πληροφορίες για το κάθε πότε (refresh time) ένας δευτερεύων εξυπηρετητής DNS ερωτά τον κύριο εξυπηρετητή DNS για αλλαγές. 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.

Ένας υπολογιστής μπορεί να είναι γνωστός στο διαδίκτυο με πολλά ονόματα (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 αυτές τις περιπτώσεις χρησιμοποιούνται εγγραφές τύπου CNAME (canonical name). Για την εύρεση των εξυπηρετητών ηλεκτρονικού ταχυδρομείου μιας περιοχής χρησιμοποιείται η εγγραφή MX (mail exchangers). 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.

Υπάρχουν πολλά είδη εξυπηρετητών ονομάτων ανάλογα με τον ρόλο τους, όπως Επίσημοι (Authoritative), Κύριοι (Primary), Δευτερεύοντες (Secondary), Master και Slave. Για μια περιοχή, ο επίσημος εξυπηρετητής δίνει τις αυθεντικές απαντήσεις, δηλαδή, περιέχει τις αυθεντικές εγγραφές για τους υπολογιστές της περιοχής, σε αντιδιαστολή με πληροφορία που έμαθε ρωτώντας άλλους. Για κάθε ζώνη πρέπει να υπάρχει ένας κύριος εξυπηρετητής και ένας αριθμός από δευτερεύοντες εξυπηρετητές για λόγους αξιοπιστίας. Οι κύριοι εξυπηρετητές DNS συνήθως λειτουργούν ως master και οι δευτερεύοντες συνήθως υλοποιούνται ως slave.

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. Κανένας εξυπηρετητής DNS δεν έχει όλες τις αντιστοιχίες ονομάτων σε διευθύνσεις IP. Για την εξυπηρέτηση μιας αίτησης μπορεί να γίνουν διαδοχικές ερωτήσεις σε άλλους εξυπηρετητές, ακολουθώντας την παγκόσμια ιεραρχία DNS. Το πρωτόκολλο DNS προβλέπει Αναδρομικές (Recursive) ερωτήσεις, όπου ο ερωτώμενος εξυπηρετητής DNS πρέπει να δώσει την απάντηση στην ερώτηση (ή να στείλει μήνυμα λάθους) και Επαναληπτικές (Iterative) ερωτήσεις, όπου ο ερωτώμενος εξυπηρετητής DNS επιστρέφει την καλύτερη δυνατή του απάντηση, ήτοι, την ακριβή απάντηση ή παραπομπή σε άλλο εξυπηρετητή. Ανάλογα με τη λειτουργία τους στη διαδικασία αυτή οι εξυπηρετητές DNS διακρίνονται σε Τοπικούς (Local), Προσωρινής αποθήκευσης (Caching) και Αναδρομής (Recursive), χωρίς να αποκλείεται η μείξη ρόλων και λειτουργιών.

Ένας τοπικός εξυπηρετητής λειτουργεί ως ενδιάμεσος, απαντά για ό,τι ξέρει και προωθεί την ερώτηση εάν απαιτείται. Αν ο τοπικός εξυπηρετητής ονομάτων δεν έχει καταλήξει στο πού θα βρει τη διεύθυνση IP που αντιστοιχεί στο όνομα, ρωτά τους εξυπηρετητές κορυφής. Επί της αρχής, οι επίσημοι εξυπηρετητές αρκούν για τη λειτουργία του διαδικτύου. Όμως μόνο με τους επίσημους εξυπηρετητές απαιτείται αναδρομική λειτουργία στην πλευρά των πελατών. Οι εξυπηρετητές κορυφής απαντούν μόνο σε Επαναληπτικές ερωτήσεις. Οι DNS εξυπηρετητές αναδρομής (recursive DNS servers), απαλλάσσουν τον πελάτη από το φορτίο των διαδοχικών ερωτήσεων μέχρι την εύρεση της ακριβούς απάντησης. Όμως μία συγκεκριμένη ερώτηση μπορεί να επαναληφθεί αρκετές φορές. Η επανάληψη της διαδικασίας επίλυσης εκτός του υπολογιστικού κόστους έχει ως αποτέλεσμα την αυξημένη καθυστέρηση, ειδικά εάν απαιτείται αναδρομή. Για την αποφυγή του παραπάνω οι εξυπηρετητές προσωρινής αποθήκευσης DNS φυλάσσουν για μελλοντική χρήση (μέχρι λήξης της χρονική τους ισχύος) τα αποτελέσματα των ερωτήσεων.

Στην πλευρά του πελάτη, ο επιλυτής (resolver) είναι η διεργασία του λειτουργικού συστήματος που χρησιμοποιείται από τα προγράμματα που χρειάζονται να αντιστοιχίσουν ονόματα περιοχών σε διευθύνσεις IP και το αντίστροφο. Στο FreeBSD υπάρχουν τρία αρχεία σχετικά με την παραμετροποίηση του resolver:

/etc/nsswitch.conf: Περιλαμβάνει πληροφορία για τη διαδικασία "name service switch" που ελέγχει τη σειρά με την οποία γίνεται η αναζήτηση μεταξύ των διαφορετικών πηγών πληροφόρησης για υπολογιστές, χρήστες (κωδικούς), ομάδες κλπ. Όσον αφορά την υπηρεσία ονοματοδοσίας, για παράδειγμα, εάν περιέχει τη γραμμή hosts: dns files, τότε για την επίλυση ενός ονόματος θα κληθεί πρώτα το DNS και εάν αυτό αποτύχει θα αναζητηθεί το όνομα στο αρχείο /etc/hosts. Για περισσότερες πληροφορίες δείτε https://www.freebsd.org/cgi/man.cgi?nsswitch.conf.

/etc/resolv.conf: Φυσιολογικά αυτό το αρχείο δεν απαιτείται. Ο επιλυτής θεωρεί ότι στο τοπικό σύστημα τρέχει ένας εξυπηρετητής DNS, το όνομα περιοχής προκύπτει από το όνομα host (ό,τι ακολουθεί την πρώτη τελεία "." στη γραμμή hostname στο /etc/rc.conf) και η διαδρομή αναζήτησης (search) προκύπτει από το όνομα περιοχής. Εάν απαιτείται, η διεύθυνση IP του εξυπηρετητή DNS ορίζεται με τη λέξη nameserver, π.χ. nameserver 192.168.2.1. Μπορούν να ορισθούν μέχρι 3 εξυπηρετητές, μια γραμμή ανά εξυπηρετητή. Το όνομα της τοπικής περιοχής μπορεί να ορισθεί με τη λέξη domain, π.χ. domain ntua.lab. Διαζευκτικά με το domain μπορεί να ορισθεί η διαδρομή αναζήτησης με τη λέξη search, π.χ. search ntua.lab. Ο επιλυτής κατά τη διαδικασία αναζήτησης δοκιμάζει ως επίθεμα διαδοχικά όλες τις λέξεις που ακολουθούν το search μέχρις ότου λάβει απάντηση. Για περισσότερες πληροφορίες δείτε https://www.freebsd.org/cgi/man.cgi?resolv.conf.

/etc/hosts: Περιέχει πληροφορία για γνωστά μηχανήματα εντός του δικτύου και μπορεί να χρησιμοποιηθεί σε συνδυασμό με το DNS. Το αρχείο πρέπει να περιέχει τουλάχιστον μία γραμμή που ορίζει τη διεύθυνση IP του βρόχου επιστροφής. Για κάθε άλλο μηχάνημα πρέπει να υπάρχει σε μια γραμμή η διεύθυνση IP, το επίσημο όνομα του και συνώνυμα χωρισμένα με κενά ή tab.

Άσκηση 1: Εγκατάσταση DHCP server

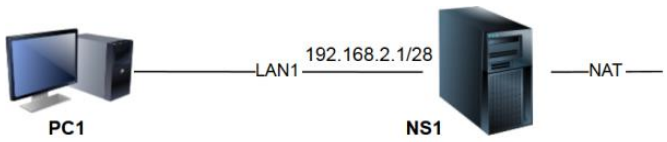
Κατασκευάστε ένα εικονικό μηχάνημα ξεκινώντας από ένα νέο FreeBSD 12.4 με **τρεις** κάρτες δικτύου.

1. Στις ρυθμίσεις δικτύου του εικονικού μηχανήματος ορίστε τη διεπαφή em1 σε NAT.
2. Στη συνέχεια, αφού εκκινήσετε το εικονικό σας μηχάνημα, ως διαχειριστής (root) ενεργοποιήστε τον πελάτη DHCP στην κάρτα δικτύου em1.
3. Δοκιμάστε εάν μπορείτε να κάνετε ping www.google.com. Εάν όχι, ορίστε στο resolv.conf τον κατάλληλο nameserver (για το οικιακό περιβάλλον τη διεύθυνση του δρομολογητή σας, εναλλακτικά, τη διεύθυνση ενός δημόσιου εξυπηρετητή DNS, π.χ. 8.8.8.8 ή 8.8.4.4 για τον εξυπηρετητή DNS της Google).
4. Εκτελέστε την εντολή "pkg update" ώστε να ενημερωθεί το εργαλείο pkg διαχείρισης πακέτων λογισμικού του FreeBSD, απαντώντας θετικά στις ερωτήσεις που θα εμφανισθούν.
5. Κλείστε το εικονικό μηχάνημα με την εντολή poweroff και από τη διαδρομή *File→Export Appliance…* στο VirtualBox δημιουργήστε το αρχείο new.ova.

Στη συνέχεια ξεκινήστε έναν νέο εικονικό μηχάνημα NS1 βασισμένο στο new.ova. Στο NS1 θα εγκαταστήσετε έναν εξυπηρετητή DHCP σύμφωνα με τις παρακάτω οδηγίες. Συμβουλευθείτε την ιστοσελίδα του εγχειριδίου https://docs.freebsd.org/en/books/handbook/network-servers/#network-dhcp προκειμένου να δείτε τη σωστή σύνταξη των εντολών παραμετροποίησης του πελάτη και του εξυπηρετητή DHCP στο FreeBSD καθώς τα αρχεία όπου καταγράφονται τα δάνεια (leases) των διευθύνσεων IP που έχουν αποδοθεί.

1. Εκτελέστε "*pkg install isc-dhcp44-server*" για την από απόσταση εγκατάσταση της έκδοσης 4.4.2 του πακέτου, απαντώντας θετικά στις ερωτήσεις που τυχόν εμφανισθούν.
2. Το αρχείο παραμετροποίησης dhcpd.conf του εξυπηρετητή DHCP βρίσκεται στον φάκελο /usr/local/etc. Αρχικά περιέχει ένα υπόδειγμα παραμετροποίησης, αντίγραφο του οποίου υπάρχει και στο dhcpd.conf.sample. Κατασκευάστε ένα δικό σας dhcpd.conf χρησιμοποιώντας τις κατάλληλες εντολές σύμφωνα με το υπόδειγμα ώστε να ορίσετε μόνο τα ακόλουθα:
   a. εξυπηρετητή DHCP για το υποδίκτυο 192.168.2.0/28,
   b. απόδοση διευθύνσεων από την περιοχή 192.168.2.5 έως 192.168.2.6,
   c. προεπιλεγμένη πύλη τον δρομολογητή 192.168.2.1,
   d. τη σωστή διεύθυνση εκπομπής εντός του ως άνω υποδικτύου,
   e. την προεπιλεγμένη διάρκεια δανεισμού των διευθύνσεων ως 60 δευτερόλεπτα, και
   f. τη μέγιστη διάρκεια δανεισμού ως 120 δευτερόλεπτα.
3. Διορθώστε το αρχείο παραμετροποίησης /etc/rc.conf προσθέτοντας εντολές με τη βοήθεια της εντολής sysrc ώστε:
   a. η διεπαφή em0 να έχει διεύθυνση IP 192.168.2.1/28,
   b. να ξεκινά αυτόματα ο πελάτης DHCP στην κάρτα δικτύου em1,
   c. να ενεργοποιείται ο εξυπηρετητής DHCP όταν εκκινεί το μηχάνημα,
   d. η υπηρεσία DHCP να παρέχεται στη διεπαφή em0, καιτο όνομα του μηχανήματος να οριστεί σε ns1.ntua.lab.
4. Επανεκκινήστε το μηχάνημα.
5. Επιβεβαιώστε ότι η υπηρεσία τρέχει με τη βοήθεια της εντολής "*service isc-dhcpd status*". Εάν όχι, αναζητήστε το λάθος στα μηνύματα που προηγήθηκαν της προτροπής "login:" και διορθώστε το.

Κατασκευάστε το δίκτυο του σχήματος χρησιμοποιώντας το NS1 και προσθέτοντας ως PC1, με μια διεπαφή στο LAN1, ένα νέο εικονικό μηχάνημα FreeBSD 12.4.



Απαντήστε τις παρακάτω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτείται, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε.

1.1. Ξεκινήστε μια καταγραφή στο NS1 για το LAN1 με εμφάνιση λεπτομερειών, διευθύνσεων MAC και απενεργοποιημένη[1] την επίλυση ονομάτων και διευθύνσεων.

1.2. Στο PC1 ξεκινήστε τον πελάτη DHCP στη διεπαφή em0 και περιμένετε τουλάχιστον δύο λεπτά προτού σταματήσετε την καταγραφή στον εξυπηρετητή ώστε να γίνει και μία προσπάθεια ανανέωσης της διεύθυνσης που θα εκχωρηθεί.

1.3. Σχεδιάστε την ανταλλαγή των πακέτων, ανεξαρτήτως πρωτοκόλλου, που περιγράφει τη διαδικασία απόδοσης διεύθυνσης IPv4 από τον εξυπηρετητή στον πελάτη.

1.4. Σύμφωνα με την έξοδο της εντολής φλοιού dhclient, ποια μηνύματα DHCP ανταλλάσσονται με τον εξυπηρετητή;

1.5. Ποια διεύθυνση αποδόθηκε στο PC1 και ποια η διεύθυνση IPv4 του εξυπηρετητή;

[1] Εάν παραλείψετε την απενεργοποίηση, θα υπάρξει μια αρχική καθυστέρηση, όταν το εικονικό μηχάνημα δεν μπορεί να επικοινωνήσει με τον εξυπηρετητή DNS ή δεν λάβει απάντηση από αυτόν.

1.6. Μετά από πόσο χρόνο πρέπει το PC1 να ανανεώσει τη διεύθυνση IPv4 που έλαβε;

1.7. Ποιο πρωτόκολλο μεταφοράς βλέπετε ότι χρησιμοποιείται για τα μηνύματα DHCP;

1.8. Ποιες είναι οι θύρες πηγής και προορισμού των μηνυμάτων DHCP μεταξύ του PC1 και του εξυπηρετητή DHCP (NS1) όπως προκύπτουν από την καταγραφή;

1.9. Γράψτε τις διευθύνσεις IPv4 αποστολέα και παραλήπτη για καθένα από τα μηνύματα DHCP της καταγραφής που αντιστοιχούν σε αυτά της ερώτησης 1.4.

1.10. Ποιες είναι οι MAC διευθύνσεις πηγής και προορισμού που χρησιμοποιήθηκαν στα ως άνω μηνύματα;

1.11. Πώς είναι δυνατόν το PC1 να στέλνει και λαμβάνει μηνύματα DHCP (ενθυλακωμένα σε πακέτα IPv4) παρότι δεν έχει διεύθυνση IPv4;

1.12. Παρατηρήσατε πλαίσια ARP στην καταγραφή πριν την απάντηση DHCP Offer του NS1; Εάν ναι, ποιος τα παράγει και γιατί;

1.13. Παρατηρήσατε μήνυμα ICMP στην καταγραφή πριν την απάντηση DHCP Offer του NS1; Εάν ναι, ποιος το παράγει και γιατί;

1.14. Ποιος είναι ο λόγος παραγωγής του πλαισίου ARP με το οποίο το PC1 αναζητεί τη MAC διεύθυνση που αντιστοιχεί στη διεύθυνση IPv4 που μόλις του αποδόθηκε;

1.15. Παρατηρήσατε ανταλλαγή μηνυμάτων ICMP στην καταγραφή αμέσως μετά την απόδοση διεύθυνσης στο PC1; Εάν ναι, ποιος νομίζεται ότι είναι λόγος για τον οποίο παράγονται;

1.16. Για πόσο χρόνο διαρκεί η εκχώρηση της διεύθυνσης IPv4; *[Υπόδειξη: Αναζητήστε την τιμή του lease time στο μήνυμα DHCP Offer.]*

1.17. Ποια επιπλέον πληροφορία περιλαμβάνει το πρώτο μήνυμα DHCP Request, με το οποίο το PC1 αποδέχεται την προσφερόμενη από τον εξυπηρετητή στο μήνυμα DHCP Offer διεύθυνση IPv4, σε σχέση με το DHCP Discover όπου το PC1 ζητούσε την απόδοση διεύθυνσης IPv4; *[Υποδ. Δείτε options.]*

1.18. Τι διαφέρει το επόμενο (δεύτερο) μήνυμα DHCP Request, με το οποίο το PC1 ζητά την ανανέωση της διάρκειας εκχώρησης, σε σχέση με το προαναφερθέν DHCP Request, με το οποίο αποδέχεται την προσφορά του εξυπηρετητή; *[Υποδ. Δείτε διευθύνσεις MAC, IP και options.]*

1.19. Για ποιο λόγο νομίζετε ότι ο πελάτης DHCP παράγει το ICMP μήνυμα udp port unreachable αμέσως μετά την απάντηση DHCP ACK του εξυπηρετητή στο δεύτερο DHCP Request;

Εκτός από τη διεύθυνση IPv4, το PC1 ζητά να λάβει από το DHCP και άλλες δικτυακές παραμέτρους αναγκαίες για τη λειτουργία του. Παρατηρώντας τα περιεχόμενα του μηνύματος DHCP Discover, θα βρείτε την επιλογή (option) Parameter Request List που περιλαμβάνει τη λίστα των ζητούμενων δικτυακών παραμέτρων.

1.20. Πόσες παραμέτρους ζήτησε ο πελάτης από τον εξυπηρετητή με το μήνυμα DHCP Discover;

1.21. Ποιες από αυτές προσδιορίζει τελικά ο εξυπηρετητής DHCP στο μήνυμα DHCP Offer;

1.22. Σε ποιο αρχείο καταγράφει ο εξυπηρετητής τα δάνεια για τις διευθύνσεις που αποδίδει;

1.23. Κάθε πότε γίνονται εγγραφές για το κάθε δάνειο;

1.24. Ποιες πληροφορίες περιέχει για κάθε δάνειο; ;

1.25. Σε ποιο αρχείο καταγράφει ο πελάτης τα δάνεια για τις διευθύνσεις IPv4 που του εκχωρούνται;

1.26. Ποιες πληροφορίες περιέχει για κάθε δάνειο;

1.27. Πόσος χρόνος πρέπει να περάσει μεταξύ μιας αποτυχημένης ανανέωσης και την αρχή της διαδικασίας επανασύνδεσης (rebind);

1.28. Στον NS1 ξεκινήστε μια νέα καταγραφή στη διεπαφή em0 με απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων και αφήστε την να τρέχει.

1.29. Σε δεύτερη κονσόλα στον NS1 δώστε εντολή για να σταματήστε τον εξυπηρετητή DHCP.

1.30. Στο PC1 ελέγξτε κατά καιρούς το κατά πόσο η διεπαφή em0 διατηρεί τη διεύθυνση που της είχε αποδοθεί. Όταν διαπιστώσετε ότι διεπαφή em0 δεν έχει πλέον διεύθυνση IPv4, επανεκκινήστε τον εξυπηρετητή DHCP.

1.31. Στο PC1 ελέγξτε για το κατά πόσο αποδόθηκε διεύθυνση IPv4 στη διεπαφή em0. Εάν η απόδοση διεύθυνσης καθυστερεί, αποσυνδέστε και ξανασυνδέστε το καλώδιο στη διεπαφή του PC1 στο LAN1. Μόλις διαπιστώσετε ότι διεπαφή em0 έχει πλέον διεύθυνση IPv4, σταματήστε την καταγραφή στον NS1.

1.32. Όταν σταματήσατε τον εξυπηρετητή DHCP, πόσες φορές στέλνει προς αυτόν μηνύματα DHCP Request το PC1 κα πόσο απέχουν χρονικά μεταξύ τους;

1.33. Ποια είναι η απάντηση που λαμβάνει το PC1 και τι σημαίνει;

1.34. Μετά από τις πρώτες ανεπιτυχείς προσπάθειες ανανέωσης, ποιος είναι ο προορισμός του τελευταίου μηνύματος DHCP Request που στέλνει το PC1;

1.35. Εάν το προηγούμενο μήνυμα παράχθηκε μετά τη λήξη του χρόνου επανασύνδεσης (rebind), αιτιολογήστε τη χρήση της συγκεκριμένης διεύθυνσης προορισμού.

1.36. Ποιος είναι ο προορισμός (διεύθυνση MAC και IPv4) των μηνυμάτων DHCP Discover που παράγει το PC1 αμέσως μετά την απώλεια διεύθυνσης IPv4 και από ποιο πεδίο του μηνύματος γίνεται κατανοητό ότι έχει απολεσθεί η διεύθυνση IPv4;

1.37. Για ποιο λόγο παράγεται ένα ICMP request από τον NS1 προς τη διεύθυνση IPv4 που προσφέρει στο PC1, αμέσως πριν το μήνυμα DHCP Offer;

1.38. Τι συμβαίνει στα δεδομένα του αρχείου με τα δάνεια που κρατά ο πελάτης;

1.39. Στις περισσότερες εφαρμογές πελάτη-εξυπηρετητής, ο εξυπηρετητής έχει μια πασίγνωστη θύρα όπου περιμένει αιτήματα, ενώ ο πελάτης χρησιμοποιεί μια τυχαία (εφήμερη) τιμή για τη θύρα πηγής. Στο DHCP αυτό δεν συμβαίνει. Τόσο ο πελάτης, όσο και ο εξυπηρετητής χρησιμοποιούν πασίγνωστες θύρες. Γιατί νομίζετε ότι συμβαίνει αυτό;

Άσκηση 2: Εγκατάσταση εξυπηρετητή DNS

Στο εικονικό μηχάνημα NS1 θα εγκαταστήσετε έναν εξυπηρετητή DNS, τον Unbound. Ο Unbound είναι ένας υψηλής επίδοσης εξυπηρετητής DNS που αναπτύχθηκε από τα NLnet Labs. Διαθέτει λειτουργίες αναδρομής (recursive), για ότι δεν γνωρίζει ερωτά άλλους μέχρι να βρει την απάντηση, προσωρινής αποθήκευσης (caching), αποθηκεύει αποτελέσματα για κάποιο χρονικό διάστημα ώστε να μην χρειάζεται να ξαναρωτήσει, και επικύρωσης (validating), επιβεβαιώνει όσο είναι δυνατό την ορθότητα της απάντησης. Παρότι διαθέτει ικανότητα λειτουργίας επίσημου εξυπηρετητή (authoritative) δεν είναι κατάλληλος για τέτοια εγκατάσταση σε μεγάλη κλίμακα. Εάν απαιτείται αυτή, υπάρχουν άλλα πλέον κατάλληλα πακέτα λογισμικού, όπως το BIND και το NSD. Ο Unbound μπορεί να χρησιμοποιηθεί σε συνδυασμό με αυτά, απομονώνοντας τους καθαυτού επίσημους εξυπηρετητές από το υπόλοιπο διαδίκτυο. Για μια εισαγωγική περιγραφή των δυνατοτήτων του δείτε https://calomel.org/unbound_dns.html.

1. Εκτελέστε "*pkg install unbound*" για την από απόσταση εγκατάσταση της έκδοσης 1.17.1 του λογισμικού, απαντώντας θετικά στις ερωτήσεις που τυχόν εμφανισθούν.

2. Διορθώστε το αρχείο παραμετροποίησης /etc/rc.conf προσθέτοντας την κατάλληλη εντολή ώστε να ενεργοποιείται ο εξυπηρετητής DNS όταν εκκινεί το μηχάνημα.
3. Δημιουργήστε ένα προσωρινό αρχείο /var/tmp/unbound.conf με το παρακάτω περιεχόμενο (χωρίς τα σχόλια). Για τις διαθέσιμες παραμέτρους διάρθρωσης του unbound και περισσότερες εξηγήσεις δείτε https://www.freebsd.org/cgi/man.cgi?unbound.conf καθώς και το αρχείο /usr/local/etc/unbound/unbound.conf.sample.

```
server:
interface: 0.0.0.0                    # to listen for queries to all available interfaces.
do-ip4: yes                            # to answer or issue IPv4 queries.
do-ip6: yes                            # to answer or issue IPv6 queries.
do-udp: yes                            # Enable UDP.
do-tcp: yes                            # Enable TCP.
access-control: 192.168.2.0/24 allow   # to control which clients are allowed to make (recursive) queries.
private-domain: "ntua.lab"             # Allow the domain (and its subdomains) to contain private addresses.
local-zone: "ntua.lab." static         # to answer queries for this domain
local-data: "ntua.lab. 360 IN SOA ns1.ntua.lab. admin.ntua.lab. 20230501 3600 1200 604800 10800"
local-data: "ntua.lab. 360 IN NS ns1.ntua.lab."
local-data: "ntua.lab. IN MX 10 192.168.2.1"
local-data: "ntua.lab. IN A 192.168.2.1"
local-data: "ns1.ntua.lab. IN A 192.168.2.1"
local-data: "www.ntua.lab. IN CNAME ntua.lab"
local-zone: "2.168.192.in-addr.arpa." static
local-data-ptr: "192.168.2.1 ns1.ntua.lab."    # instead of PTR records.
forward-zone:
name: "."                              # queries not answered locally are forwarded to the following servers
forward-addr: 1.1.1.1
forward-addr: 8.8.8.8
forward-addr: 9.9.9.9
```

4. Ελέγξτε την ορθότητα του αρχείου παραμετροποίησης /var/tmp/unbound.conf εκτελώντας την εντολή unbound-checkconf. Εάν υπάρχουν λάθη, διορθώστε. Εάν όχι, αντιγράψτε το στο /usr/local/etc/unbound/unbound.conf.
5. Εάν υπάρχει αρχείο /etc/resolv.conf, διαγράψτε το. Δημιουργήστε νέο αρχείο /etc/resolv.conf, εισάγετε τα ακόλουθα και αποθηκεύστε το:

```
search ntua.lab
nameserver 192.168.2.1
```

6. Στο αρχείο /usr/local/etc/dhcpd.conf προσθέστε στην αρχή τα ακόλουθα και αποθηκεύστε το:

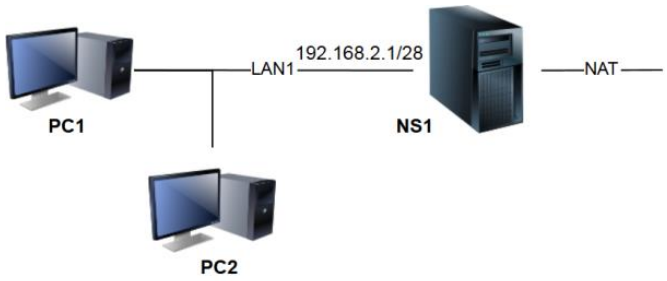
```
option domain-name "ntua.lab";
option domain-name-servers 192.168.2.1;
```

7. Επανεκκινήστε την υπηρεσία DHCP και ελέγξτε για τυχόντα λάθη. Εάν υπάρχουν διορθώστε το αρχείο παραμετροποίησης.
8. Κλείστε το εικονικό μηχάνημα NS1 και στη συνέχεια δημιουργήστε ένα κλώνο του, το NS2, που θα χρησιμοποιήσετε αργότερα. Μην παραλείψετε να επαναρχικοποιήσετε τις διευθύνσεις MAC.

Επίλυση ονομάτων μέσω του αρχείου /etc/hosts

Μια απλή μέθοδος για να αντιστοιχηθούν ονόματα με διευθύνσεις IP είναι η χρήση του αρχείου /etc/hosts. Με κάθε εγγραφή στο αρχείο έχετε μια στατική αντιστοίχιση ονομάτων και διευθύνσεων IP. Όταν σε μια εντολή δικτύου, όπως το ping, χρησιμοποιείτε το όνομα του host, θα γίνει αναζήτηση στο τοπικό αρχείο /etc/hosts για να μεταφραστεί το όνομα host σε διεύθυνση IP.

Κατασκευάστε το δίκτυο του σχήματος. Επανεκκινήστε το PC1 και εάν υπάρχει το αρχείο /etc/resolv.conf διαγράψτε το. Στο PC1, δώστε τη διεύθυνση IP 192.168.2.5/28 στη διεπαφή em0. Στο νέο εικονικό μηχάνημα PC2 βασισμένο στο FreeBSD 12.4, δώστε τη διεύθυνση IP 192.168.2.6/28 στη διεπαφή του em0 στο LAN1 και εάν υπάρχει το αρχείο /etc/resolv.conf διαγράψτε το.



Απαντήστε τις παρακάτω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτείται, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε.

2.1 Τροποποιήστε το αρχείο /etc/hosts στο PC1 ώστε το όνομα της τοπικής περιοχής (my.domain στο αρχείο) να γίνει “ntua.lab” και προσθέστε εγγραφές με τις διευθύνσεις και τα ονόματα των PC1 και PC2 σύμφωνα με το υπόδειγμα που περιέχει το αρχείο.

2.2 Εκτελέστε διαδοχικά τις εντολές “ping PC2”, “ping pc2”, “ping pc2.NTUA.LAB”. Ποιο μηχάνημα απαντά; Έχει σημασία η χρήση μικρών ή κεφαλαίων γραμμάτων;

2.3 Επαναλάβετε τα προηγούμενα για το PC2 και επιβεβαιώστε ότι στο “ping PC1” απαντά το PC1.

2.4 Στο PC2 διαγράψτε την εγγραφή για το PC1 στο /etc/hosts. Ποια είναι η απάντηση που λαμβάνετε εάν κάνετε “ping PC1”;

Επίλυση ονομάτων μέσω του εξυπηρετητή DNS

2.5 Ξεκινήστε το εικονικό μηχάνημα NS1 και προσθέστε στο αρχείο /var/tmp/unbound.conf εγγραφές τύπου A για τα PC1, PC2 με διευθύνσεις IP 192.168.2.5 και 192.168.2.6, αντίστοιχα.

2.6 Προσθέστε στο αρχείο τις αντίστροφες PTR εγγραφές για τις διευθύνσεις IP 192.168.2.5 και 192.168.2.6.

2.7 Αφού ελέγξετε την ορθότητά του, αντιγράψτε το στο /usr/local/etc/unbound/unbound.conf και επανεκκινήστε τον εξυπηρετητή DNS για να ισχύσουν οι αλλαγές που κάνατε.

2.8 Στο NS1 ξεκινήστε μια καταγραφή στη διεπαφή em0 με εμφάνιση λεπτομερειών και χωρίς επίλυση ονομάτων.

2.9 Στο PC1 διαγράψτε τη στατική διεύθυνση IP και αποδώστε δυναμικά νέα διεύθυνση IP στη διεπαφή em0.

2.10 Σταματήστε την καταγραφή. Ποια διεύθυνση έλαβε το PC1 από τον εξυπηρετητή DHCP;

2.11 Ποιες επιπλέον παραμέτρους απέδωσε ο εξυπηρετητής DHCP σε σχέση με αυτές της ερώτησης 1.21.

2.12 Έχει δημιουργηθεί αρχείο /etc/resolv.conf στο PC1; Ποιο είναι το περιεχόμενό του;

2.13 Με τη βοήθεια της εντολής host (το αντίστοιχο στο FreeBSD της nslookup των Windows) ή της drill (το αντίστοιχο της dig σε συστήματα Linux) βρείτε το όνομα που αντιστοιχεί στη διεύθυνση IPv4 που έλαβε το PC1.

2.14 Με τη βοήθεια της εντολής host βρείτε τη διεύθυνση του μηχανήματος NS1.

2.15 Μπορείτε από το PC1 να κάνετε ping στο μηχάνημα με όνομα ns1;

2.16 Στο PC2 διαγράψτε τη στατική διεύθυνση IPv4 και αποδώστε δυναμικά νέα διεύθυνση IPv4 στη διεπαφή em0.
2.17 Ποια διεύθυνση έλαβε το PC2 από τον εξυπηρετητή DHCP;
2.18 Μπορείτε από το PC2 να κάνετε ping στο PC1 χρησιμοποιώντας το όνομα αυτού;
2.19 Από πού έλαβε το PC2 τη διεύθυνση IP του PC1; Από το αρχείο /etc/hosts ή από τον εξυπηρετητή DNS;
2.20 Στο αρχείο /etc/hosts του PC1 διορθώστε την εγγραφή για το PC2 αλλάζοντας τη διεύθυνση IP σε 192.168.2.7. Μπορείτε τώρα στο PC1 να κάνετε "ping pc2";
2.21 Τι συμπεραίνετε για τη σειρά με την οποία γίνεται η αναζήτηση της πληροφορίας από τον τοπικό επιλυτή (resolver);
2.22 Ποιο είναι το περιεχόμενο του αρχείου /etc/nsswitch.conf στο PC1 όσον αφορά στη σειρά αναζήτησης ονομάτων υπολογιστών (hosts); Συμφωνεί η σειρά αναζήτησης με αυτή που παρατηρήσατε στις προηγούμενες δοκιμές ping;
2.23 Με τη βοήθεια της εντολής host βρείτε τη διεύθυνση IP του PC2.
2.24 Πώς εξηγείται η διαφορετική απάντηση σε σχέση με τη διεύθυνση που λαμβάνει το ping pc2; *[Υποδ. Δείτε σελίδα man για το host]*.
2.25 Στο PC1 διαγράψτε το αρχείο /etc/resolv.conf και στη συνέχεια εκτελέστε την εντολή resolvconf –u. Ποιο είναι το περιεχόμενο του αρχείου /etc/resolv.conf τώρα;

Πρωτόκολλο DNS

2.26 Ξεκινήστε μια καταγραφή στο NS1 με απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων στη διεπαφή em0 φροντίζοντας να μην καταγράφονται τα σχετικά με το DHCP μηνύματα.
2.27 Με τη βοήθεια της εντολής host στο PC1 βρείτε τη διεύθυνση IP του ntua.lab.
2.28 Υπάρχει στην καταγραφή κίνηση σχετική με το DNS;
2.29 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιήθηκε από το DNS (TCP ή UDP);
2.30 Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιήθηκαν.
2.31 Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής DNS;
2.32 Στο NS1 ξεκινήστε στη διεπαφή em0 μια νέα καταγραφή με απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων συλλαμβάνοντας μόνο μηνύματα DNS και αφήστε την να τρέχει.
2.33 Στο PC1 αναζητήστε τη διεύθυνση IP του NS1 με την εντολή host.
2.34 Πόσα μηνύματα DNS ανταλλάχθηκαν;
2.35 Σε τι είδους ερωτήματα προς τον εξυπηρετητή DNS αντιστοιχούσαν και για ποιο όνομα έγιναν αυτές;
2.36 Σε ποιες εξ αυτών δόθηκε απάντηση;
2.37 Αναζητήστε τη διεύθυνση IP του ns1 και του ns1.ntua.lab με την εντολή drill.
2.38 Για ποιο όνομα έγιναν ερωτήσεις και ποια απάντηση λήφθηκε;
2.39 Τι συμπεραίνεται σχετικά με τη χρήση του επιθέματος ntua.lab (search path) από τις δύο εντολές;
2.40 Στο PC1 κάντε "ping localhost" και μετά "ping pc1". Παράγονται ερωτήσεις προς τον εξυπηρετητή DNS και σε ποια περίπτωση;
2.41 Στο PC1 κάντε "ping ns1" και σταματήστε το.

2.42 Πόσα μηνύματα DNS ανταλλάχθηκαν και σε τι είδους ερωτήματα προς τον εξυπηρετητή DNS αφορούσαν;

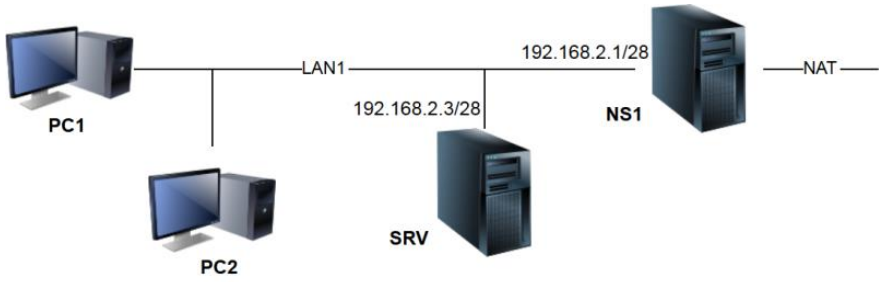
2.43 Στο PC1 ξανακάντε “ping ns1” και σταματήστε το. Επαναλάβετε τουλάχιστον δύο φορές. Παρατηρείτε να παράγονται ερωτήματα προς τον εξυπηρετητή DNS; Εάν ναι, πόσα έγιναν;

2.44 Τι συμπεραίνετε σχετικά με το κατά πόσο οι απαντήσεις του εξυπηρετητή DNS αποθηκεύονται προσωρινά στο PC1;

Άσκηση 3: Εγκατάσταση εξυπηρετητή HTTP

Ετοιμάστε ένα νέο FreeBSD 12.4 εικονικό μηχάνημα για το SRV. Για την εγκατάσταση του εξυπηρετητή HTTP ακολουθήστε τις παρακάτω οδηγίες.

1. Επιβεβαιώστε ότι η διεπαφή em0 είναι σε NAT.
2. Στη συνέχεια, αφού εκκινήσετε το εικονικό σας μηχάνημα, ως διαχειριστής (root) ενεργοποιήστε τον πελάτη DHCP στην κάρτα δικτύου.
3. Δοκιμάστε εάν μπορείτε να κάνετε ping www.google.com. Εάν όχι, ορίστε στο resolv.conf τον κατάλληλο εξυπηρετητή DNS.
4. Εκτελέστε “*pkg install lighttpd*” για την από απόσταση εγκατάσταση της έκδοσης 1.4.69 του πακέτου, απαντώντας θετικά στις ερωτήσεις που τυχόν εμφανισθούν.
5. Διαγράψτε το αρχείο /etc/resolv.conf και προσθέστε το SRV στο δίκτυο LAN1 όπως στο παρακάτω σχήμα.



Απαντήστε τις παρακάτω ερωτήσεις καταγράφοντας παράλληλα, όπου απαιτείται, την ακριβή σύνταξη των εντολών που χρησιμοποιήσατε.

3.1 Στο αρχείο /etc/rc.conf ορίστε το όνομα του μηχανήματος σε SRV και προσθέστε την εντολή lighttpd_enable = “YES” ώστε να ξεκινά η υπηρεσία http όταν επανεκκινεί.

3.2 Δημιουργήστε τον φάκελο /usr/local/www/data.

3.3 Εντός του προηγούμενου φακέλου δημιουργήστε ένα αρχείο με όνομα index.html και περιεχόμενο την πρόταση “Hello World!”

3.4 Επανεκκινήστε το εικονικό μηχάνημα SRV και, εάν υπάρχει, διαγράψτε το αρχείο /etc/resolv.conf.

3.5 Πώς μπορείτε να βεβαιωθείτε ότι η υπηρεσία HTTP έχει ενεργοποιηθεί στο SRV με τη βοήθεια της εντολής service;

3.6 Πώς θα μπορούσατε να δείτε το ίδιο με την εντολή netstat;

3.7 Τοποθετήστε τη διεπαφή του SRV στο LAN1 και ορίστε σε αυτήν την IPv4 διεύθυνση 192.168.2.3/28.

3.8 Προσθέστε εγγραφή A για το SRV με διεύθυνση IPv4 192.168.2.3 στο αρχείο /var/tmp/unbound.conf του NS1.

3.9 Προσθέστε στο αρχείο την αντίστροφη εγγραφή PTR για τη διεύθυνση 192.168.2.3.

3.10 Αφού ελέγξετε την ορθότητά του, αντιγράψτε το στο /usr/local/etc/unbound/unbound.conf και επανεκκινήστε τον εξυπηρετητή DNS για να ισχύσουν οι αλλαγές που κάνατε.

3.11 Στο SRV ξεκινήστε μια καταγραφή για την κίνηση στο LAN1 με απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων.

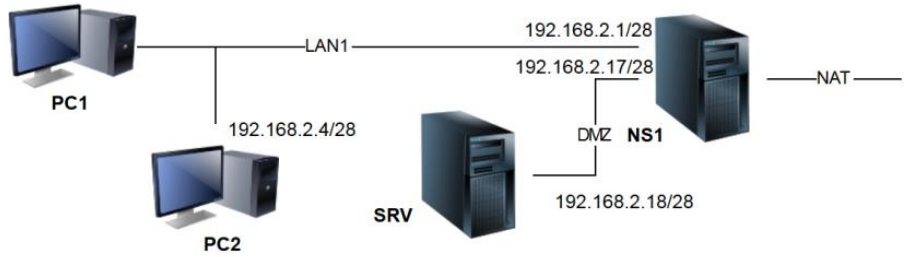
3.12 Στο PC1 χρησιμοποιήστε την εντολή fetch για να κατεβάσετε με μη διαδραστικό τρόπο από το url http://srv.ntua.lab την ιστοσελίδα που κατασκευάσατε πριν και να την αποθηκεύσετε. *[Υποδ. Δείτε σελίδα man για τη σύνταξη της fetch.]*

3.13 Ποιο πρωτόκολλο μεταφοράς χρησιμοποιήθηκε και σε ποια θύρα ακούει ο εξυπηρετητής http;

3.14 Σε ποιο αρχείο αποθηκεύτηκε το περιεχόμενο της ιστοσελίδας που κατεβάσατε;

Άσκηση 4: Εγκατάσταση ιδιωτικού δρομολογητή και Firewall

Κατασκευάστε το δίκτυο του επόμενου σχήματος σύμφωνα με τις οδηγίες που ακολουθούν. Πρώτα θα μετατρέψετε το εικονικό μηχάνημα NS1 σε δρομολογητή και θα ενεργοποιήσετε σε αυτό το τείχος προστασίας. Για τη σύνταξη των σχετικών με το τείχος προστασίας ipfw εντολών δείτε Εργαστηριακή Άσκηση 10 και https://docs.freebsd.org/en/books/handbook/firewalls/#firewalls-ipfw.



Με τη βοήθεια της εντολής sysrc προσθέστε την κατάλληλη εντολή στο αρχείο /etc/rc.conf του NS1 ώστε:

4.1 Να ενεργοποιήστε τη λειτουργία δρομολόγησης (προώθηση πακέτων).

4.2 Να ενεργοποιήσετε το τείχος προστασίας ipfw.

4.3 Να καθορίσετε ανοικτή λειτουργία για το τείχος προστασίας.

4.4 Να επιτρέψετε τη λειτουργία NAT για το τείχος προστασίας ipfw.

4.5 Να ορίσετε στη διεπαφή em2 του NS1 την IP διεύθυνση 192.168.2.17/28.

4.6 Να επιβεβαιώσετε ότι οι τιμές των μεταβλητών στο /etc/rc.conf είναι σωστές.

4.7 Στη συνέχεια κλείστε το εικονικό μηχάνημα NS1, τοποθετήστε τη διεπαφή του em2 στο τοπικό δίκτυο DMZ και επανεκκινήστε το. Εάν δεν υπάρχει, ορίστε ως προκαθορισμένη πύλη τη διεύθυνση IPv4 του NAT στο host μηχάνημα.

4.8 Διορθώστε το αρχείο /etc/resolv.conf όπως ορίσθηκε προηγουμένως στο βήμα 5 της άσκησης 2 και επιβεβαιώστε ότι η επίλυση ονομάτων λειτουργεί.

4.9 Στο PC1 προσθέστε την κατάλληλη εντολή στο /etc/rc.conf ώστε όταν εκκινεί να λαμβάνει διεύθυνση IP μέσω DHCP και επανεκκινήστε την υπηρεσία netif.

4.10 Στο PC2 προσθέστε τις κατάλληλες εντολές στο /etc/rc.conf ώστε, όταν εκκινεί, η διεπαφή em0 να λαμβάνει τη διεύθυνση 192.168.2.4/28 και ο προεπιλεγμένος δρομολογητής να είναι η διεπαφή του NS1 στο LAN1.

4.11 Επανεκκινήστε τις υπηρεσίες netif και routing του PC2. Εάν δεν υπάρχει, δημιουργήστε αρχείο /etc/resolv.conf, όπως κάνατε προηγουμένως για το PC1 και επιβεβαιώστε ότι η επίλυση ονομάτων λειτουργεί.

4.12 Τοποθετήστε τη διεπαφή em0 του SRV στο τοπικό δίκτυο DMZ, προσθέστε τις κατάλληλες εντολές στο /etc/rc.conf ώστε όταν εκκινεί να λαμβάνει την IPv4 διεύθυνση 192.168.2.18/28, ο προεπιλεγμένος δρομολογητής να είναι η διεπαφή του NS1 στο DMZ και επανεκκινήστε τις υπηρεσίες netif και routing.

4.13 Διορθώστε στο αρχείο /var/tmp/unbound.conf τις εγγραφές για τα PC2 και SRV, ελέγξτε την ορθότητά του, αντιγράψτε το στο αρχείο /usr/local/etc/unbound/unbound.conf του NS1 και επανεκκινήστε τον εξυπηρετητή DNS.

4.14 Από το SRV μπορείτε να κάνετε ping σε μηχανήματα του LAN1 χρησιμοποιώντας την IPv4 διεύθυνσή τους;

Το SRV βρίσκεται στην DMZ, ήτοι πρέπει να είναι προσβάσιμο από όλους, αλλά να μην έχει το ίδιο πρόσβαση στο εσωτερικό δίκτυο LAN1. Προς τούτο θα πρέπει να ορίσετε τους κατάλληλους κανόνες τείχους προστασίας με το ipfw.

4.15 Στο NS1 προσθέστε κανόνα με αριθμό 2000 ώστε να απαγορεύεται οποιαδήποτε εισερχόμενη κίνηση μέσω της διεπαφής στο DMZ προς το LAN1.

4.16 Μπορείτε από το SRV να κάνετε ping στο PC1;

4.17 Προσθέστε (stateful) κανόνα με αριθμό 1900 που να επιτρέπει εισερχόμενη κίνηση στη διεπαφή em0 από το LAN1 προς στο DMZ και το αντίστροφο για κίνηση που γεννιέται ως απάντηση.

4.18 Μπορείτε από το PC1 να κάνετε ping στο SRV;

4.19 Μπορείτε από το NS1 να κάνετε ping στη διεύθυνση IP 147.102.1.1;

4.20 Μπορείτε από το PC1 να κάνετε ping στη διεύθυνση IP 147.102.1.1;

Ο λόγος που δεν δουλεύει το δεύτερο ping, όπως μπορείτε εύκολα να διαπιστώσετε κάνοντας μια καταγραφή στη διεπαφή em1 του NS1, οφείλεται στο γεγονός ότι το host μηχάνημα αναζητεί την πηγή της κίνησης στο υποδίκτυο του NAT. Για αυτό τα πλαίσια ARP request που παράγει δεν παίρνουν απάντηση. Ένας τρόπος για να ξεπεράσετε το προηγούμενο πρόβλημα συνίσταται στο να "μασκαρευτεί" η κίνηση που διαβιβάζεται από τη διεπαφή em1 ως κίνηση που παράγει η ίδια η em1. Προς τούτο πρέπει α) να δημιουργηθεί στο τείχος προστασίας πίνακας NAT με την εντολή "ipfw nat *nat_number* config *nat-configuration*", ώστε η κίνηση που ωθείται στο NAT με αριθμό *nat_number* να υφίσταται τη μετάφραση διευθύνσεων που θα ορίσετε στο *nat-configuration*, και β) να εγγραφεί στο τείχος προστασίας κανόνας (rule) ώστε η κίνηση που ταιριάζει σε αυτόν να ωθείται στο NAT με αριθμό *nat_number* ώστε να υφίσταται την οριζόμενη σε αυτό μετάφραση διευθύνσεων IP (και θυρών).

4.21 Δημιουργήστε στο τείχος προστασίας του NS1 πίνακα in-kernel nat με αριθμό παρουσίας 111 ώστε τα πακέτα με <u>ιδιωτικές</u> διευθύνσεις που ωθούνται σε αυτόν να υφίστανται μετάφραση στη διεύθυνση της διεπαφής em1 και επιπλέον να αρχικοποιείται (reset) σε περίπτωση αλλαγής της διεύθυνσης IP της διεπαφής.

4.22 Προσθέστε κανόνα με αύξοντα αριθμό 3000, ώστε όλη η κίνηση IPv4 *δια μέσου* της διεπαφής em1 να ωθείται στον πίνακα NAT με αριθμό παρουσίας 111 για να υφίσταται την οριζόμενη σε αυτό μετάφραση διευθύνσεων IP (και θυρών).

4.23 Μπορείτε τώρα από το PC1 να κάνετε ping στη διεύθυνση IPv4 147.102.1.1;

4.24 Με τη βοήθεια της εντολής host ή drill βρείτε το όνομα του μηχανήματος με την παραπάνω διεύθυνση IP.

4.25 Ξεκινήστε μια καταγραφή με απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων στη διεπαφή em1 του NS1.

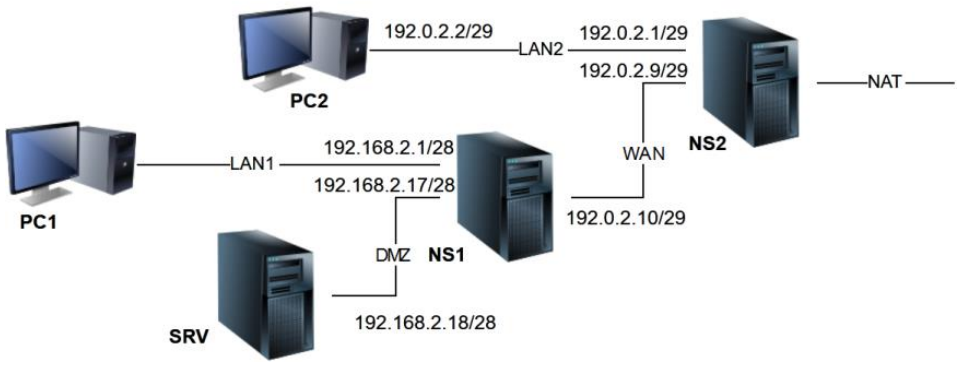
4.26 Στο PC1 κάντε ping –c 2 www.ntua.gr και σταματήστε την καταγραφή. Με ποια διεύθυνση πηγής εμφανίζονται τα πακέτα IPv4 που παράγει το PC1;
4.27 Ποια είναι η διεύθυνση προορισμού των ICMP echo request;
4.28 Προς ποιον εξυπηρετητή DNS έγινε η ερώτηση για την επίλυση του ονόματος www.ntua.gr;
4.29 Ξεκινήστε νέα καταγραφή στη διεπαφή em1 του NS1 συλλαμβάνοντας μόνο μηνύματα DNS και με απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων ώστε να παρατηρείτε τα ερωτήματα που κάνει ο NS1 προς εξωτερικούς εξυπηρετητές DNS.
4.30 Στο PC2 κάντε ping –c 1 κατά σειρά στα www.google.com, www.cnn.com, www.yahoo.com, www.mit.edu. Τι παρατηρείτε όσον αφορά τον εξωτερικό εξυπηρετητή DNS προς τον οποίο απευθύνονται τα εκάστοτε ερωτήματα για την επίλυση ονομάτων;
4.31 Σε νέο παράθυρο στο NS1 ξεκινήστε αντίστοιχη της προηγούμενης καταγραφή στη διεπαφή em0 αυτή τη φορά, ώστε να παρατηρείτε και τα ερωτήματα προς τον NS1.
4.32 Στο PC1 εκτελέστε την εντολή ping –c 1 courses.cn.ntua.gr και σταματήστε τις καταγραφές. Ποιο είναι το επίσημο όνομα (canonical name) του υπολογιστή courses.cn.ntua.gr;
4.33 Τι είδους ερώτημα έκανε το PC1 και τι είδους απάντηση έλαβε από τον NS1; Αντίστοιχα, τι είδους ερωτήματα έκανε ο NS1 προς τους εξωτερικούς εξυπηρετητές DNS και τι είδους απαντήσεις έλαβε;
4.34 Ξεκινήστε νέα καταγραφή στη διεπαφή em1 του NS1 συλλαμβάνοντας μόνο μηνύματα DNS με εμφάνιση όσο το δυνατόν περισσότερων λεπτομερειών και απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων.
4.35 Στο PC1 εκτελέστε διαδοχικά δύο φορές την εντολή drill για να βρείτε τη διεύθυνση IPv4 του www.cn.ece.ntua.gr. Πόσα ερωτήματα DNS παρατηρήσατε; Ποια είναι η χρονική διάρκεια ισχύος των απαντήσεων DNS;
4.36 Στον NS1 ξεκινήστε αντίστοιχη της ερώτησης 4.34 καταγραφή στη διεπαφή em0 αυτή τη φορά και επαναλάβετε δύο φορές την εντολή drill της προηγούμενης ερώτησης.Παράγονται μηνύματα DNS από το PC1; Εάν ναι, τι παρατηρείτε για τη χρονική διάρκεια ισχύος των απαντήσεων DNS;
4.37 Τι συμπεραίνετε σχετικά με το κατά πόσο αποθηκεύονται προσωρινά οι απαντήσεις που λαμβάνει ο τοπικός εξυπηρετητής DNS στο NS1;
4.38 Μπορείτε από το SRV να κάνετε ping στον εξυπηρετητή http του ΕΜΠ με διεύθυνση IPv4 την 147.102.224.101;
4.39 Μπορείτε από το SRV να κάνετε ping στον εξυπηρετητή στο www.ntua.gr; Γιατί;
4.40 Στο /etc/resolv.conf του SRV ορίστε ως εξυπηρετητή DNS τη διεπαφή του NS1 στο DMZ.
4.41 Μπορείτε τώρα από το SRV να κάνετε ping στο www.ntua.gr;
4.42 Στο PC1 μπορείτε με τη βοήθεια της εντολής host να βρείτε τη διεύθυνση IPv4 για το www.ntua.lab;Τι θα συμβεί εάν κάνετε ping στο www.ntua.lab;

Όπως μόλις είδατε για τοπικές εγγραφές τύπου CNAME το unbound δεν απαντά δίνοντας και τη διεύθυνση IPv4, όπως έγινε προηγουμένως στην ερώτηση 4.33. Για να επικοινωνήσετε με τον www.ntua.lab πρέπει να ορίσετε ρητά τη διεύθυνση IPv4 αυτού.

4.43 Στον NS1 προσθέστε πριν την εγγραφή τύπου CNAME εγγραφή τύπου A με την οποία να αποδίδεται διεύθυνση IP στο www.ntua.lab ίδια με αυτή του SRV. Επανεκκινήστε τον εξυπηρετητή DNS ώστε να ισχύσουν οι αλλαγές.
4.44 Από το PC1 κάντε ping στο www.ntua.lab. Ποιο μηχάνημα απαντά;

Άσκηση 5: Εγκατάσταση δημόσιου δρομολογητή και DNS

Το "οικιακό" δίκτυο της προηγούμενης άσκησης θα συνδεθεί στο "δημόσιο". Προς τούτο το εικονικό μηχάνημα NS2, που κατασκευάσατε στην άσκηση 2, μιμείται το "δημόσιο" δρομολογητή. Θα ξεκινήσετε τροποποιώντας τα αρχεία παραμετροποίησης του NS2 ώστε να λειτουργεί ως δρομολογητής με ενσωματωμένο εξυπηρετητή DNS. Στη συνέχεια θα μεταφέρετε τον NS1 στο WAN. Μέχρι εκείνο το σημείο θα διατηρήσετε το NS1 συνδεδεμένο στο NAT.



Προτού εκκινήσετε το NS2, τοποθετήστε τις διεπαφές του στα σωστά δίκτυα όπως στο σχήμα. Στη συνέχεια με τη βοήθεια της sysrc προσθέστε κατάλληλες εντολές στο αρχείο /etc/rc.conf ώστε:

5.1 Να ορίσετε το όνομα του μηχανήματος ως ns2.ntua.lab.

5.2 Να ορίσετε ως διευθύνσεις των διεπαφών em0 και em2 του NS2 τις 192.0.2.1/29 και 192.0.2.9/29, αντίστοιχα.

5.3 Να ορίσετε ότι η διεπαφή em1 θα λάβει δυναμικά διεύθυνση μέσω DHCP.

5.4 Να ενεργοποιηθεί η λειτουργία δρομολόγησης.

5.5 Να ενεργοποιηθεί το τείχος προστασίας ipfw.

5.6 Να ορισθεί ανοικτή λειτουργία για το τείχος προστασίας. .

5.7 Να ενεργοποιηθεί η λειτουργία NAT του τείχους προστασίας. .

5.8 Να διαγράψετε από το αρχείο /etc/rc.conf τις σχετικές με τον εξυπηρετητή DHCP γραμμές.

5.9 Να δείτε όλες τις μεταβλητές του αρχείου /etc/rc.conf και επιβεβαιώσετε ότι υπάρχει η εντολή για ενεργοποίηση της υπηρεσίας DNS.

5.10 Τροποποιήστε το αρχείο /var/tmp/unbound.conf επιτρέποντας πρόσβαση από το υποδίκτυο 192.0.2.0/24 και εκτρέποντας τις ερωτήσεις για την περιοχή ntua.gr στον ίδιο, αντικαθιστώντας τις εγγραφές από την access-control μέχρι και πριν την forward-zone ως εξής:

```
access-control: 192.0.2.0/24 allow
local-zone: "ntua.lab." redirect          # to block any query for this domain
local-data: "ntua.lab. IN A 192.0.2.10"   # and answer with NS1 public address
```

Αφού ελέγξετε την ορθότητά του, αντιγράψτε το στο /usr/local/etc/unbound/unbound.conf.

5.11 Επανεκκινήστε το NS2 και εάν δεν υπάρχει προκαθορισμένη διαδρομή, ορίστε ως προκαθορισμένη πύλη τη διεύθυνση IPv4 του NAT στο host μηχάνημα.

5.12 Δημιουργήστε στο τείχος προστασίας του NS2 πίνακα in-kernel NAT με αριθμό παρουσίας 222 ώστε τα πακέτα που ωθούνται σε αυτόν να υφίστανται μετάφραση στη διεύθυνση της διεπαφής em1, να αρχικοποιείται (reset) σε περίπτωση αλλαγής της διεύθυνσης IP και επιπλέον να μη γίνονται κατά το δυνατό αλλαγές στις θύρες.

5.13 Προσθέστε κανόνα με αύξοντα αριθμό 1100 ώστε όλη η κίνηση IPv4 δια μέσου της διεπαφής em1 να ωθείται στον πίνακα NAT με αριθμό παρουσίας 222 για να υφίσταται την οριζόμενη σε αυτό μετάφραση διευθύνσεων (και θυρών).

5.14 Στο PC2 τροποποιήστε το αρχείο /etc/rc.conf ώστε, όταν εκκινεί, η διεπαφή em0 να λαμβάνει τη διεύθυνση 192.0.2.2/29 και ο προεπιλεγμένος δρομολογητής να είναι η διεπαφή του NS2 στο LAN2.

5.15 Συνδέστε το PC2 στο LAN2 και επανεκκινήστε τις υπηρεσίες netif και routing. Εάν δεν υπάρχει, δημιουργήστε αρχείο /etc/resolv.conf ορίζοντας τον NS2 ως εξυπηρετητή DNS και επιβεβαιώστε ότι η επίλυση ονομάτων λειτουργεί.

5.16 Μπορείτε από το PC2 να κάνετε ping στο www.ntua.gr;

5.17 Στο NS1 τροποποιήστε το αρχείο /etc/rc.conf ώστε, όταν εκκινεί, η διεπαφή em1 να λαμβάνει τη διεύθυνση 192.0.2.10/29 και ο προεπιλεγμένος δρομολογητής να είναι η διεπαφή του NS2 στο WAN.

5.18 Μετακινήστε τη διεπαφή em1 του NS1 στο δίκτυο WAN και επανεκκινήστε τις υπηρεσίες netif και routing.

5.19 Μπορείτε από το PC1 και το SRV να κάνετε ping στο www.ntua.gr; Παραμένει η λειτουργία του πίνακα nat 111;

5.20 Ποια διεύθυνση IPv4 επιστρέφει το DNS για το www.ntua.lab στο PC1 και ποια στο PC2;

5.21 Χρησιμοποιώντας την εντολή fetch μπορείτε από το PC2 να κατεβάσετε την ιστοσελίδα http://www.ntua.lab; Ποιο λάθος εμφανίζεται;

Για να είναι εφικτή η πρόσβαση στην ιστοσελίδα από το δημόσιο δίκτυο, θα πρέπει τα τεμάχια TCP που καταφτάνουν στη δημόσια διεύθυνση του NS1 με θύρα προορισμού 80 να ανακατευθυνθούν (redirect) στην ιδιωτική διεύθυνση του εξυπηρετητή HTTP. Όπως πριν, πρέπει να εγκατασταθεί στο τείχος προστασίας κανόνας που να ωθεί την εισερχόμενη κίνηση στη λειτουργία NAT και να δημιουργηθεί πίνακας NAT που να ορίζει την επεξεργασία που αυτή θα υφίσταται.

5.22 Δημιουργήστε στο τείχος προστασίας του NS1 πίνακα in-kernel NAT με αριθμό παρουσίας 111 (θα αντικαταστήσει τον υπάρχοντα) επαναλαμβάνοντας τις εντολές της ερώτησης 4.21 και προσθέτοντας εντολή που να ανακατευθύνει την εισερχόμενη κίνηση tcp με προορισμό τη θύρα 80 στην ιδιωτική διεύθυνση 192.168.2.18 του SRV.

5.23 Μπορείτε τώρα στο PC2 να κατεβάσετε την ιστοσελίδα http://www.ntua.lab;

5.24 Μπορείτε από το PC2 να κάνετε ping το www.ntua.lab; Ποιο μηχάνημα απαντά;

5.25 Σε ποιο μηχάνημα συνδέστε με ssh lab@www.ntua.lab από το PC1;

5.26 Εάν προσπαθήσετε το προηγούμενο από το PC2, με ποιο μηχάνημα θα συνδεθείτε; Γιατί;

5.27 Στο NS1 τροποποιήστε όπως πριν τον πίνακα NAT με αριθμό 111 προσθέτοντας εντολή ώστε να προωθείται στο SRV και η εισερχόμενη κίνηση προς την πόρτα 22.

5.28 Μπορείτε τώρα να συνδεθείτε με ssh από το PC2 στο SRV; Πώς επιβεβαιώνετε ότι πράγματι συνδεθήκατε στο SRV και όχι στο NS1;