

|  |                             |
|--|-----------------------------|
| <b>Όνοματεπώνυμο:</b> Ιωάννης Γιαννούκος | <b>Όνομα PC:</b> John John  |
| <b>Ομάδα:</b> 1                          | <b>Ημερομηνία:</b> 7/6/2023 |

## Εργαστηριακή Άσκηση 12

### Υπηρεσίες στο Διαδίκτυο

### Άσκηση 1

#### *Κατασκευή αρχείου new.ona*

- 1) Στις ρυθμίσεις δικτύου του εικ. μηχανήματος ορίζω τη διεπαφή em1 σε NAT.
- 2) `“dhclient em1”`
- 3) Δοκιμάζω εάν μπορώ να κάνω `“ping www.google.com”` και βλέπω ότι μπορώ.
- 4) `“pkg update”`
- 5) `“poweroff”`

#### *Εγκατάσταση DHCP εξυπηρετητή (στο NS1)*

- 1) `“dhclient em1” “pkg install isc-dhcp44-server”`
- 2) Κατασκευάζω ένα δικό μου dhcpd.conf στο /usr/local/etc με `“vi /usr/local/etc/dhcpd.conf”` ώστε να ορίσω 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
  - f. τη μέγιστη διάρκεια δανεισμού ως 120 δευτερόλεπτα

Το τελικό αρχείο περιέχει μόνο τα εξής:

```
subnet 192.168.2.0 netmask 255.255.255.240 {  
    range 192.168.2.5 192.168.2.6;  
    option routers 192.168.2.1;  
    option broadcast-address 192.168.2.15;  
    default-lease-time 60;  
    max-lease-time 120;  
}
```

3) Διορθώνω το αρχείο παραμετροποίησης /etc/rc.conf προσθέτοντας εντολές με τη βοήθεια της εντολής sysrc ώστε:

a. η διεπαφή em0 να έχει τη διεύθυνση IP 192.168.2.1/28:

```
“sysrc -f /etc/rc.conf ifconfig_em0=“inet  
192.168.2.1/28””
```

b. να ξεκινά αυτόματα ο πελάτης DHCP στην κάρτα δικτύου em1:

```
“sysrc -f /etc/rc.conf ifconfig_em1=“DHCP””
```

c. να ενεργοποιείται ο εξυπηρετητής DHCP όταν εκκινεί το μηχάνημα:

```
“sysrc -f /etc/rc.conf dhcpd_enable=“YES””
```

d. η υπηρεσία DHCP να παρέχεται στη διεπαφή em0, και το όνομα του μηχανήματος να οριστεί σε ns1.ntua.lab:

```
“sysrc -f /etc/rc.conf dhcpd_ifaces=“em0”” και  
“sysrc -f /etc/rc.conf hostname=“ns1.ntua.lab””
```

4) Επανεκκινώ το μηχάνημα με “reboot”.

5) Επιβεβαιώνω ότι η υπηρεσία τρέχει με τη βοήθεια της εντολής “service isc-dhcpd status”.

### *Απαντήσεις Ερωτημάτων Άσκησης*

1.1) Ξεκινώ μια καταγραφή στο NS1 για το LAN1 με εμφάνιση λεπτομερειών, διευθύνσεων MAC και απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων εκτελώντας “tcpdump -vvnneni em0”.

1.2) Στο PC1 ξεκινώ τον πελάτη DHCP στη διεπαφή em0 με “dhclient em0” και περιμένω τουλάχιστον δύο λεπτά προτού σταματήσω την

καταγραφή στον εξυπηρετητή ώστε να γίνει και μία προσπάθεια ανανέωσης της διεύθυνσης που θα εκχωρηθεί.

1.3) Παρακάτω φαίνεται ένα σχήμα για την ανταλλαγή των πακέτων, ανεξαρτήτως πρωτοκόλλου, που περιγράφει τη διαδικασία απόδοσης διεύθυνσης IPv4 από τον εξυπηρετητή στον πελάτη.

|                   |                                   |
|-------------------|-----------------------------------|
| PC1 → broadcast : | DHCP Discover                     |
| NS1 → broadcast : | ARP Request (who-has 192.168.2.5) |
| NS1 → PC1 :       | DHCP Offer                        |
| PC1 → broadcast : | DHCP Request                      |
| NS1 → PC1 :       | DHCP Ack                          |
| PC1 → broadcast : | ARP Request (who-has 192.168.2.5) |
| NS1 → PC1 :       | ICMP echo request                 |
| PC1 → broadcast : | ARP request (who-has 192.168.2.1) |
| NS1 → PC1 :       | ARP reply                         |
| PC1 → NS1 :       | ICMP echo reply                   |
| PC1 → NS1 :       | DHCP Request                      |
| NS1 → PC1 :       | DHCP Ack                          |
| PC1 → NS1 :       | ICMP udp port unreachable         |

1.4) Σύμφωνα με την έξοδο της εντολής φλοιού `dhclient`, τα μηνύματα που ανταλλάσσονται με τον εξυπηρετητή είναι τα DHCP {Discover, Offer, Request, Ack}.

```
root@PC:~ # dhclient em0
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 3
Jun  6 09:12:19 PC dhclient[8811]: send_packet: Network is down
DHCPDISCOVER on em0 to 255.255.255.255 port 67 interval 3
DHCPOFFER from 192.168.2.1
DHCPREQUEST on em0 to 255.255.255.255 port 67
DHCPACK from 192.168.2.1
bound to 192.168.2.5 -- renewal in 60 seconds.
root@PC:~ #
```

1.5) Στο PC1 αποδόθηκε η διεύθυνση 192.168.2.5. Η διεύθυνση IPv4 του εξυπηρετητή είναι 192.168.2.1.

1.6) Το PC1 πρέπει να ανανεώσει τη διεύθυνση IPv4 που έλαβε μετά από 60 δευτερόλεπτα.

1.7) Για τα μηνύματα DHCP βλέπω ότι χρησιμοποιείται ως πρωτόκολλο μεταφοράς το UDP.

1.8) Οι θύρες πηγής και προορισμού των μηνυμάτων DHCP μεταξύ του PC1 και του εξυπηρετητή DHCP (NS1) είναι 68 και 67, αντίστοιχα.

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

DHCP Discover : 0.0.0.0 → 255.255.255.255

DHCP Offer : 192.168.2.1 → 192.168.2.5

DHCP Request : 0.0.0.0 → 255.255.255.255

DHCP Ack : 192.168.2.1 → 192.168.2.5

DHCP Request : 192.168.2.5 → 192.168.2.1

DHCP Ack : 192.168.2.1 → 192.168.2.5

1.10) Στα ανωτέρω μηνύματα χρησιμοποιήθηκαν οι MAC των PC1 (08:00:27:99:f5:7e) και NS1 (08:00:27:5b:bf:f5), και για τα μηνύματα προς εκπομπή χρησιμοποιήθηκε ως MAC η ff:ff:ff:ff:ff:ff.

1.11) Το PC1 μπορεί να στέλνει και να λαμβάνει μηνύματα DHCP με τη βοήθεια της MAC του και της διεύθυνσεως εκπομπής (broadcast).

1.12) Ναι, παρατηρώ πλαίσια ARP στην καταγραφή πριν την απάντηση DHCP Offer του NS1. Αυτά τα παράγει το NS1, για να επιβεβαιώσει ότι δεν έχει κάποιο άλλο μηχάνημα την διεύθυνση που πρόκειται να δώσει στο PC1.

1.13) Ναι, παρατηρώ μήνυμα ICMP στην καταγραφή πριν την απάντηση DHCP Offer του NS1. Αυτό το παράγει το NS1, για να δει αν η διεύθυνση που έδωσε είναι ακόμα σε ισχύ.

1.14) Το PC1 στέλνει πλαίσιο ARP αναζητώντας την MAC διεύθυνση που αντιστοιχεί στη διεύθυνση IPv4 που μόλις του αποδόθηκε για να επιβεβαιώσει ότι δεν έχει κάποιο άλλο μηχάνημα την διεύθυνση που πρόκειται να χρησιμοποιήσει.

1.15) Ναι, υπήρξε ανταλλαγή μηνυμάτων ICMP στην καταγραφή αμέσως μετά την απόδοση διεύθυνσης στο PC1, για να επιβεβαιώσει το NS1 ότι αποδόθηκε η διεύθυνση στο PC1.

1.16) Η εκχώρηση της διεύθυνσης IPv4 διαρκεί για 120 δευτερόλεπτα.

1.17) Το πρώτο μήνυμα DHCP Request, με το οποίο το PC1 αποδέχεται την προσφερόμενη από τον εξυπηρετητή στο μήνυμα DHCP Offer διεύθυνση IPv4, περιλαμβάνει το πεδίο 'Requested-IP' με το οποίο αιτείται για την διεύθυνση που προσφέρθηκε.

1.18) Το επόμενο μήνυμα DHCP Request, περιέχει το πεδίο Client-IP με τιμή την διεύθυνση IPv4 που του αποδόθηκε, 192.168.2.5.

1.19) Ο πελάτης DHCP παράγει το ICMP μήνυμα udr port unreachable αμέσως μετά την απάντηση DHCP ACK του εξυπηρετητή στο δεύτερο DHCP Request για να υποδείξει στο NS1 ότι η δεν ακούει πλέον στη θύρα 68, καθώς του αποδόθηκε διεύθυνση.

1.20) Ο πελάτης ζήτησε από τον εξυπηρετητή με το μήνυμα DHCP Discover 8 παραμέτρους.

```
Parameter-Request Option 55, length 10:  
  Subnet-Mask, BR, Time-Zone, Classless-Static-Route  
  Default-Gateway, Domain-Name, Domain-Name-Server, Hostname  
Option 119, MTU  
END Option 255, length 0
```

1.21) Από τις παραπάνω ο εξυπηρετητής προσδιόρισε στο μήνυμα DHCP Offer που ακολούθησε 2 από αυτές, που φαίνονται παρακάτω:

```
09:32:17.207877 08:00:27:5b:bf:f5 > 08:00:27:99:f5:7e, ethertype IPv4 (0x0800),  
length 342: (tos 0x10, ttl 128, id 0, offset 0, flags [none], proto UDP (17), le  
ngth 328)  
  192.168.2.1.67 > 192.168.2.5.68: [udp sum ok] BOOTP/DHCP, Reply, length 300,  
xid 0x41c1e3f0, secs 7, Flags [none] (0x0000)  
    Your-IP 192.168.2.5  
    Client-Ethernet-Address 08:00:27:99:f5:7e  
    Vendor-rfc1048 Extensions  
      Magic Cookie 0x63825363  
      DHCP-Message Option 53, length 1: Offer  
      Server-ID Option 54, length 4: 192.168.2.1  
      Lease-Time Option 51, length 4: 120  
      Subnet-Mask Option 1, length 4: 255.255.255.240  
      BR Option 28, length 4: 192.168.2.15  
      Default-Gateway Option 3, length 4: 192.168.2.1  
      END Option 255, length 0  
      PAD Option 0, length 0, occurs 26
```

1.22) Ο εξυπηρετητή καταγράφει τα δάνεια για τις διευθύνσεις που αποδίδει στο αρχείο /var/db/dhcpd/dhcpd.leases.

1.23) Οι εγγραφές για το κάθε δάνειο γίνονται κάθε 60 δευτερόλεπτα.

1.24) Για κάθε δάνειο αποθηκεύονται οι εξής πληροφορίες:

```
lease 192.168.2.5 {  
  starts 2 2023/06/06 10:04:19;  
  ends 2 2023/06/06 10:06:19;  
  cltt 2 2023/06/06 10:04:19;  
  binding state active;  
  next binding state free;  
  rewind binding state free;  
  hardware ethernet 08:00:27:99:f5:7e;  
  uid "\001\010\000'\231\365~";  
  client-hostname "PC";  
}
```

1.25) Ο πελάτης καταγράφει τα δάνεια για τις διευθύνσεις IPv4 που του εκχωρούνται στο αρχείο /var/db/dhclient.leases.em0.

1.26) Για κάθε δάνειο αποθηκεύονται οι εξής πληροφορίες:

```
lease {
  interface "em0";
  fixed-address 192.168.2.5;
  option subnet-mask 255.255.255.240;
  option routers 192.168.2.1;
  option broadcast-address 192.168.2.15;
  option dhcp-lease-time 120;
  option dhcp-message-type 5;
  option dhcp-server-identifier 192.168.2.1;
  renew 2 2023/6/6 10:07:19;
  rebind 2 2023/6/6 10:08:04;
  expire 2 2023/6/6 10:08:19;
}
root@PC:~ #
```

1.27) Μεταξύ μιας αποτυχημένης ανανέωσης (renew) και την αρχή της διαδικασίας επανασύνδεσης (rebind) πρέπει να περάσουν 45 δευτερόλεπτα.

1.28) Στον NS1 ξεκινώ μια νέα καταγραφή στη διεπαφή em0 με απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων εκτελώντας “tcpdump -ni em0”.

1.29) Σε δεύτερη κονσόλα στον NS1 (Alt+F2) δίνω εντολή για να σταματήσω τον εξυπηρετητή DHCP εκτελώντας “service isc-dhcpd stop”.

1.30) Στο PC1 ελέγχω κατά καιρούς το κατά πόσο η διεπαφή em0 διατηρεί τη διεύθυνση που της είχε αποδοθεί εκτελώντας “ifconfig em0 inet”. Από την καταγραφή βλέπω ότι το PC1 στέλνει (αδίκως) μηνύματα DHCP Request για να ανανεώσει την διεύθυνση IPv4 του, και το NS1 απαντά με ICMP udp port 67 unreachable. Μετά από λίγο βλέπω ότι το PC1 δεν έχει πλέον την διεύθυνση IPv4 που του αποδόθηκε. Επανεκκινώ τον εξυπηρετητή DHCP με “service isc-dhcpd restart” (“service isc-dhcpd start”).

1.31) Στο PC1 ελέγχω για το κατά πόσο αποδόθηκε διεύθυνση IPv4 στη διεπαφή em0 εκτελώντας “ifconfig em0 inet”. Επειδή βλέπω ότι η απόδοση διεύθυνσης καθυστερεί, αποσυνδέω και ξανασυνδέω το καλώδιο στη διεπαφή του PC1 στο LAN1. Εκτελώντας “ifconfig em0 inet” βλέπω ότι εν τέλει στο PC1 αποδίδεται η διεύθυνση 192.168.2.5 και πάλι. Σταματώ την καταγραφή στον NS1.

1.32) Το PC1 στέλνει προς τον εξυπηρετητή 12 μηνύματα DHCP Request με χρονική απόσταση μεταξύ τους περίπου 10 δευτερόλεπτα.

1.33) Το PC1 λαμβάνει την απάντηση ICMP 192.168.2.1 udp port 67 unreachable, που σημαίνει ότι η θύρα που προσπαθεί να επικοινωνήσει το PC1 είναι κλειστή και δεν ακούει το NS1.

1.34) Μετά από τις πρώτες ανεπιτυχείς προσπάθειες ανανέωσης, το PC1 στέλνει μηνύματα DHCP Request προς τη διεύθυνση εκπομπής (broadcast).

```
10:12:51.767200 IP 192.168.2.5.68 > 192.168.2.1.67: BOOTP/DHCP, Request from 08:00:27:99:f5:7e, length 300
10:12:51.767201 IP 192.168.2.1 > 192.168.2.5: ICMP 192.168.2.1 udp port 67 unreachable, length 336
10:13:04.806675 IP 192.168.2.5.68 > 192.168.2.1.67: BOOTP/DHCP, Request from 08:00:27:99:f5:7e, length 300
10:13:04.806755 IP 192.168.2.1 > 192.168.2.5: ICMP 192.168.2.1 udp port 67 unreachable, length 336
10:13:20.832646 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 08:00:27:99:f5:7e, length 300
10:13:28.839780 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 08:00:27:99:f5:7e, length 300
10:13:36.846327 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 08:00:27:99:f5:7e, length 300
10:13:53.856329 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 08:00:27:99:f5:7e, length 300
10:14:09.866874 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 08:00:27:99:f5:7e, length 300
10:14:18.877905 IP 0.0.0.0.68 > 255.255.255.255.67: BOOTP/DHCP, Request from 08:00:27:99:f5:7e, length 300
```

1.35) Η διεύθυνση προορισμού των DHCP Request μηνυμάτων άλλαξε, επειδή το PC1, αφού δεν έλαβε καμία απάντηση από την υπηρεσία DHCP του NS1, έκανε προσπάθεια να λάβει διεύθυνση IPv4 από κάποιον άλλον εξυπηρετητή DHCP στο δίκτυο, τουλάχιστον με άλλη διεύθυνση IP.

1.36) Ο προορισμός των μηνυμάτων DHCP Discover που παράγει το PC1 αμέσως μετά την απώλεια διεύθυνσης IPv4 είναι η διεύθυνση εκπομπής 255.255.255.255 (broadcast). Γίνεται κατανοητό ότι έχει απολεσθεί η διεύθυνση IPv4 από το πεδίο Requested-IP του μηνύματος.

1.37) Το NS1 στέλνει μήνυμα ICP echo request προς τη διεύθυνση IPv4 που προσφέρει στο PC1 για να επιβεβαιώσει ότι δεν έχει αποδώσει την διεύθυνση αυτή σε άλλο μηχανήμα.

1.38) Τα δεδομένα του αρχείου με τα δάνεια που κρατά ο πελάτης φαίνεται να έχουν διαγραφεί.

1.39) Στις περισσότερες εφαρμογές πελάτη-εξυπηρετητή, 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. Αυτό, λογικά, συμβαίνει επειδή ο πελάτης σε αυτήν την περίπτωση δεν έχει διεύθυνση IP, επομένως θα πρέπει να δοθεί στον εξυπηρετητή ένας τρόπος επικοινωνίας του με τον πελάτη.

## Άσκηση 2

### *Εγκατάσταση DNS εξυπηρετητή (στον NS1)*

1) “`pkg install unbound`”

2) Διορθώνω το αρχείο παραμετροποίησης `/etc/rc.conf` προσθέτοντας κατάλληλη εντολή ώστε να ενεργοποιείται ο εξυπηρετητής DNS όταν εκκινεί το μηχάνημα με την εντολή “`sysrc -f /etc/rc.conf unbound_enable=“YES”`”.

3) Δημιουργώ προσωρινό αρχείο `/var/tmp/unbound.conf` με το παρακάτω περιεχόμενο.

```
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) “`unbound-checkconf`” και “`cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf`”

5) “`rm /etc/resolv.conf`” και “`touch /etc/resolv.conf`” και “`vi /etc/resolv.conf`” με τα εξής περιεχόμενα:

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

6) “`vi /usr/local/etc/dhcpd.conf`”, προσθέτω στην αρχή τα ακόλουθα:

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



7) “service isc-dhcpd restart”

8) Κλείνω το εικ. μηχάνημα NS1 και δημιουργώ ένα κλώνο του, το NS2, που θα χρησιμοποιήσω αργότερα (δεν ξεχνώ να επαναρχικοποιήσω τις διευθύνσεις MAC).

### *Επίλυση ονομάτων μέσω του αρχείου /etc/hosts*

Κατασκευάζω το δίκτυο του σχήματος. Επανεκκινώ το PC1 και εάν υπάρχει το αρχείο /etc/resolv.conf, το διαγράφω. Στο PC1 δίνω τη διεύθυνση IP 192.168.2.5/28 στη διεπαφή em0 με “ifconfig em0 inet 192.168.2.5/28”. Στο νέο εικονικό μηχάνημα PC2 βασισμένο στο FreeBSD12.4, δίνω τη διεύθυνση IP 192.168.2.6/28 στη διεπαφή του em0 στο LAN1 με “ifconfig em0 inet 192.168.2.6/28” και εάν υπάρχει το αρχείο /etc/resolv.conf, το διαγράφω.

2.1) Τροποποιώ το αρχείο /etc/hosts στο PC1 ώστε το όνομα της τοπικής περιοχής (my.domain στο αρχείο) να γίνει “ntua.lab” και προσθέτω εγγραφές με τις διευθύνσεις και το ονόματα των PC{1,2} σύμφωνα με το υπόδειγμα που περιέχει το αρχείο. (Παρακάτω εμφανίζω τις γραμμές του αρχείου /etc/hosts που δεν περιέχουν ‘#’, δηλαδή δεν είναι σχόλια)

```
root@PC1:~ # grep -v # /etc/hosts
::1                localhost localhost.ntua.lab
127.0.0.1          localhost localhost.ntua.lab
192.168.2.5        PC1 PC1.ntua.lab
192.168.2.6        PC2 PC2.ntua.lab
root@PC1:~ #
```

2.2) Στο NS1 Εκτελώ διαδοχικά τις εντολές “ping PC2”, “ping pc2”, “ping pc2.NTUA.LAB”. Παρατηρώ ότι όλα τα παραπάνω pings είναι επιτυχημένα. Επομένως, δεν έχει η σημασία η χρήση μικρών ή κεφαλαίων γραμμάτων.

2.3) Επαναλαμβάνω τα προηγούμενα για το PC2 και επιβεβαιώνω ότι στο “ping PC1” απαντά το PC1.

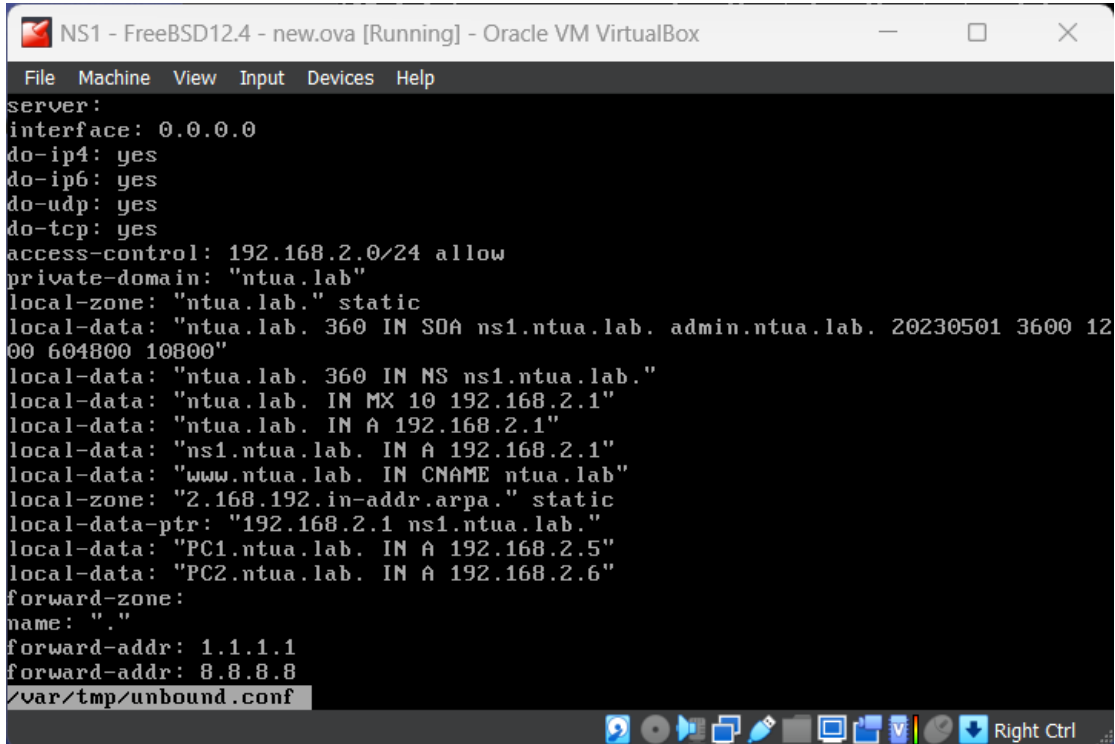
```
root@PC2:~ # grep -v # /etc/hosts
::1                localhost localhost.ntua.lab
127.0.0.1          localhost localhost.ntua.lab
192.168.2.5        PC1 PC1.ntua.lab
192.168.2.6        PC2 PC2.ntua.lab
root@PC2:~ #
```

2.4) Στο PC2 διαγράφω την εγγραφή για το PC1 στο /etc/hosts. Η απάντηση που λαμβάνω εάν κάνω “ping PC1” είναι η εξής:

```
root@PC2:~ # ping PC1
ping: cannot resolve PC1: Host name lookup failure
root@PC2:~ #
```

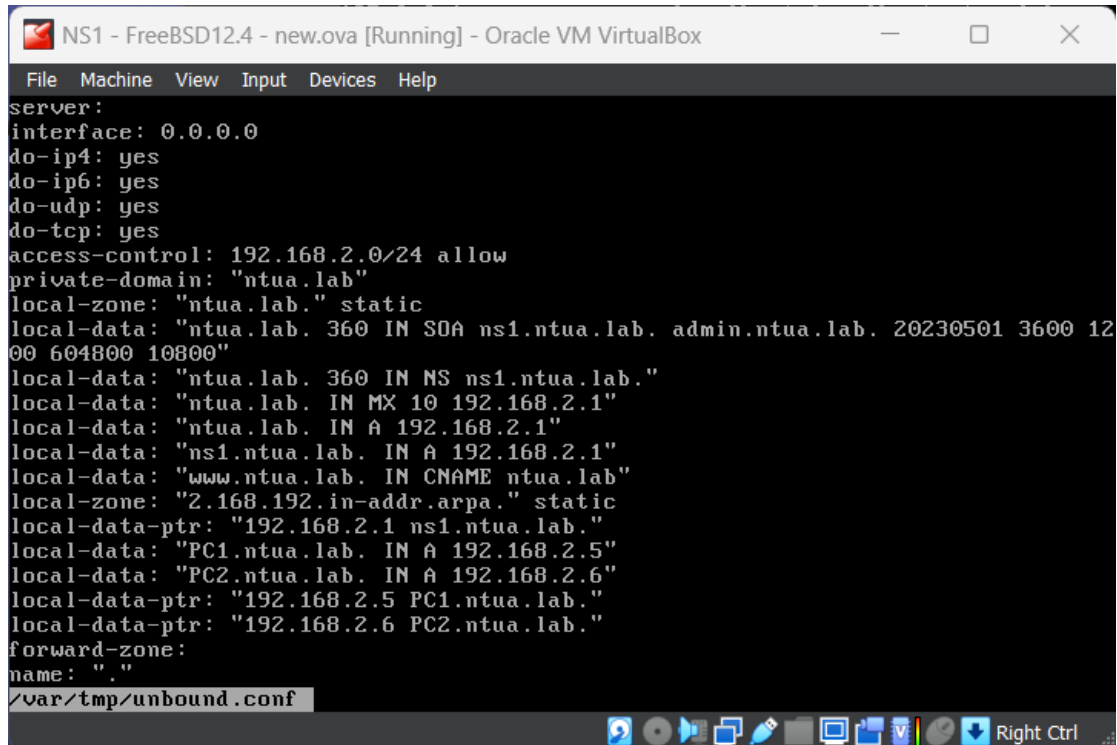
## *Επίλυση ονομάτων μέσω του εξυπηρετητή DNS*

2.5) Ξεκινώ το εικονικό μηχάνημα NS1 και προσθέτω στο αρχείο /var/tmp/unbound.conf εγγραφές τύπου A για τα PC{1,2} με διευθύνσεις IP 192.168.2.5 και 192.168.2.6, αντίστοιχα.



```
server:
interface: 0.0.0.0
do-ip4: yes
do-ip6: yes
do-udp: yes
do-tcp: yes
access-control: 192.168.2.0/24 allow
private-domain: "ntua.lab"
local-zone: "ntua.lab." static
local-data: "ntua.lab. 360 IN SOA ns1.ntua.lab. admin.ntua.lab. 20230501 3600 12
00 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."
local-data: "PC1.ntua.lab. IN A 192.168.2.5"
local-data: "PC2.ntua.lab. IN A 192.168.2.6"
forward-zone:
name: "."
forward-addr: 1.1.1.1
forward-addr: 8.8.8.8
/var/tmp/unbound.conf
```

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



```
server:
interface: 0.0.0.0
do-ip4: yes
do-ip6: yes
do-udp: yes
do-tcp: yes
access-control: 192.168.2.0/24 allow
private-domain: "ntua.lab"
local-zone: "ntua.lab." static
local-data: "ntua.lab. 360 IN SOA ns1.ntua.lab. admin.ntua.lab. 20230501 3600 12
00 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."
local-data: "PC1.ntua.lab. IN A 192.168.2.5"
local-data: "PC2.ntua.lab. IN A 192.168.2.6"
local-data-ptr: "192.168.2.5 PC1.ntua.lab."
local-data-ptr: "192.168.2.6 PC2.ntua.lab."
forward-zone:
name: "."
/var/tmp/unbound.conf
```

2.7) Αφού ελέγξω την ορθότητα του παραπάνω αρχείου με “unbound-checkconf /var/tmp/unbound.conf”, το αντιγράφω στο /usr/local/etc/unbound/unbound.conf με “cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf” και επανεκκινώ τον εξυπηρετητή DNS με “service unbound restart” για να ισχύσουν οι αλλαγές που έκανα.

2.8) Στο NS1 ξεκινώ μια καταγραφή στη διεπαφή em0 με εμφάνιση λεπτομερειών και χωρίς επίλυση ονομάτων εκτελώντας “tcpdump -i em0 -vvvvn”.

2.9) Στο PC1 διαγράφω τη στατική διεύθυνση IP και αποδίδω δυναμικά νέα διεύθυνση IP στη διεπαφή em0 με τις εντολές, αντίστοιχα, “ifconfig em0 delete” και “dhclient em0”.

2.10) Σταματώ την καταγραφή. Ο PC1 έλαβε τη διεύθυνση 192.168.2.5/28 από τον εξυπηρετητή DHCP.

2.11) Ο εξυπηρετητής DHCP απέδωσε επιπλέον, σε σχέση με το 1.21, τις παραμέτρους Domain-Name και Domain-Name-Server.

2.12) Ναι, έχει δημιουργηθεί αρχείο /etc/resolv.conf στο PC1, με το εξής περιεχόμενο:

```
root@PC1:~ # cat /etc/resolv.conf
# Generated by resolvconf
search ntua.lab
nameserver 192.168.2.1
root@PC1:~ #
```

2.13) Εμφανίζω το όνομα που αντιστοιχεί στη διεύθυνση IPv4 που έλαβε το PC1 εκτελώντας “host 192.168.2.5”.

```
root@PC1:~ # host 192.168.2.5
5.2.168.192.in-addr.arpa domain name pointer PC1.ntua.lab.
root@PC1:~ #
```

2.14) Με τη βοήθεια της εντολής host, εμφανίζω τη διεύθυνση του μηχανήματος NS1 εκτελώντας “host NS1”.

```
root@PC1:~ # host NS1
NS1.ntua.lab has address 192.168.2.1
root@PC1:~ #
```

2.15) Ναι, μπορώ να κάνω ping από το PC1 στο μηχανήμα με όνομα ns1.

2.16) Στο PC2 διαγράφω τη στατική διεύθυνση IPv4 με και αποδίδω δυναμικά νέα διεύθυνση IPv4 στη διεπαφή em0 με τις αντίστοιχες εντολές “ifconfig em0 delete” και “dhclient em0”.

2.17) Το PC2 έλαβε από τον εξυπηρετητή DHCP την διεύθυνση 192.168.2.6/28.

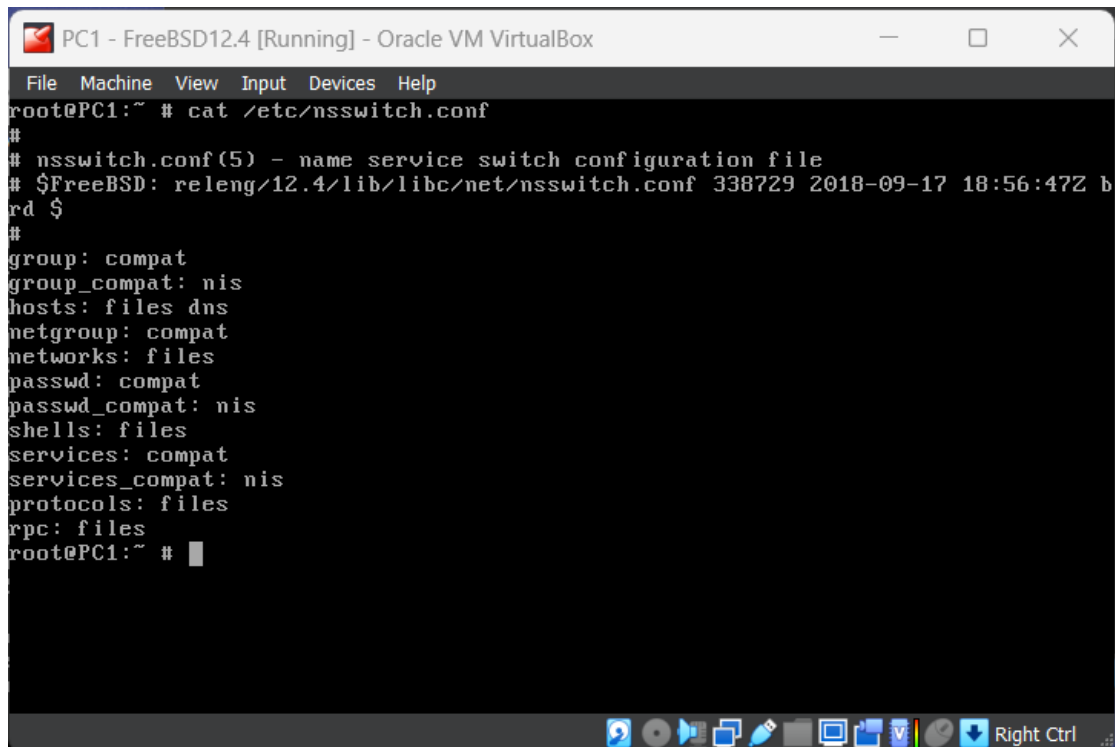
2.18) Ναι, μπορώ από το PC2 να κάνω ping στο PC1 χρησιμοποιώντας το όνομα αυτού.

2.19) Το PC2 έλαβε τη διεύθυνση του PC1 από τον εξυπηρετητή DNS. Κατ’ αρχήν, έχω ήδη σβήσει την εγγραφή στο αρχείο /etc/hosts για το PC1, και, επίσης, με μία καταγραφή tcpdump στο PC2 μπορώ να δω συγκεκριμένα την επικοινωνία του με το NS1.

2.20) Στο αρχείο /etc/hosts του PC1 διορθώνω την εγγραφή για το PC2 αλλάζοντας τη διεύθυνση IP σε 192.168.2.7. Βλέπω ότι πλέον δεν μπορώ να κάνω στο PC1 “ping pc2”.

2.21) Από την παραπάνω διαδικασία συμπεραίνω ότι ένα μηχανήμα, εάν έχει εγγραφή για κάποιον host, τότε δεν επικοινωνεί με τον εξυπηρετητή DNS, ακόμα και στην περίπτωση που η εγγραφή για αυτόν είναι λάθος (πράγμα που δεν μπορεί να καταλάβει το ίδιο το μηχανήμα). Εν τέλει, δεν υφίσταται ποτέ επικοινωνία με τον εξυπηρετητή DNS.

2.22) Παρακάτω φαίνεται το περιεχόμενο του αρχείου /etc/nsswitch.conf στο PC1, όσον αφορά στη σειρά αναζήτησης ονομάτων υπολογιστών (hosts).



```
PC1 - FreeBSD12.4 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@PC1:~ # cat /etc/nsswitch.conf
#
# nsswitch.conf(5) - name service switch configuration file
# $FreeBSD: releng/12.4/lib/libc/net/nsswitch.conf 338729 2018-09-17 18:56:47Z b
rd $
#
group: compat
group_compat: nis
hosts: files dns
netgroup: compat
networks: files
passwd: compat
passwd_compat: nis
shells: files
services: compat
services_compat: nis
protocols: files
rpc: files
root@PC1:~ #
```

Παρατηρώ ότι η σειρά αυτή που αναφέρεται στο αρχείο συμφωνεί με αυτήν που παρατήρησα προηγουμένως.

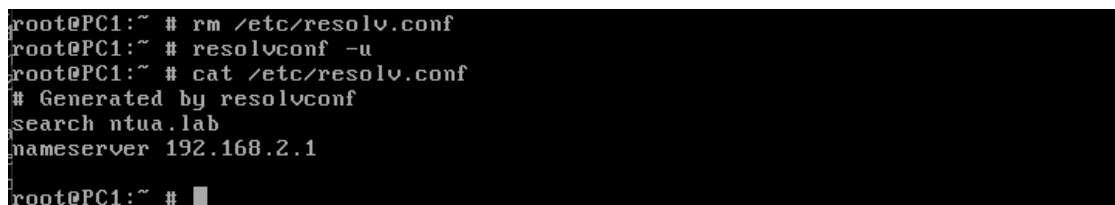
2.23) (PC1) Με τη βοήθεια της εντολής `host` εμφανίζω τη διεύθυνση IP του PC2 εκτελώντας “`host PC2`”.



```
root@PC1:~ # host PC2
PC2.ntua.lab has address 192.168.2.6
root@PC1:~ #
```

2.24) Η διαφορετική απάντηση σε σχέση με τη διεύθυνση που λαμβάνει το `ping pc2` εξηγείται από το γεγονός ότι η εντολή `host` ρωτά κατευθείαν τον εξυπηρετητή DNS, και δεν χρησιμοποιεί το αρχείο `/etc/hosts`.

2.25) Στο PC1 διαγράψω το αρχείο `/etc/resolv.conf` με “`rm /etc/resolv.conf`” και στη συνέχεια εκτελώ την εντολή “`resolvconf -u`”. Το περιεχόμενο, πλέον, του αρχείου `/etc/resolv.conf` φαίνεται παρακάτω:



```
root@PC1:~ # rm /etc/resolv.conf
root@PC1:~ # resolvconf -u
root@PC1:~ # cat /etc/resolv.conf
# Generated by resolvconf
search ntua.lab
nameserver 192.168.2.1
root@PC1:~ #
```

## *Πρωτόκολλο DNS*

2.26) Ξεκινώ μια καταγραφή στο NS1 με απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων στη διεπαφή em0 φροντίζοντας να μην καταγράφονται τα σχετικά με το DHCP μηνύματα εκτελώντας `tcpdump -vnnvni em0 not port 67`.

2.27) Με τη βοήθεια της εντολής host στο PC1 εμφανίζω τη διεύθυνση IP του ntua.lab εκτελώντας `host ntua.lab`.

2.28) Ναι, υπήρξε στην καταγραφή κίνηση σχετική με το DNS.

2.29) Από το DNS ως πρωτόκολλο μεταφοράς χρησιμοποιήθηκε το UDP.

2.30) Χρησιμοποιήθηκαν ως θύρες προέλευσης και προορισμού οι 53 και 50724, αντίστοιχα.

2.31) Στο πρωτόκολλο εφαρμογής DNS αντιστοιχεί η θύρα 53.

2.32) Στο NS1 ξεκινώ στη διεπαφή em0 μια νέα καταγραφή με απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων συλλαμβάνοντας μόνο μηνύματα DNS `tcpdump -vnnvni em0 port 53` και την αφήνω να τρέχει.

2.33) Χρησιμοποιώντας την εντολή host στο PC1 εμφανίζω τη διεύθυνση IP του NS1 εκτελώντας `host NS1`.

2.34) Ανταλλάχθηκαν 6 μηνύματα DNS.

2.35) Τα μηνύματα αυτά αντιστοιχούσαν σε ερωτήματα προς τον εξυπηρετητή τύπου A?, AAAA? και MX?, και αυτά έγιναν για το όνομα NS1.ntua.lab.

2.36) Παρόλο που ο εξυπηρετητής DNS απάντησε και στα 3 δεδομενογράμματα UDP, δόθηκε απάντηση μόνο στο πρώτο από αυτά, δηλαδή στο A?.

2.37) Με την εντολή drill εμφανίζω τη διεύθυνση IP του ns1 και του ns1.ntua.lab εκτελώντας, αντίστοιχα, `drill ns1` και `drill ns1.ntua.lab`.

```
PC1 - FreeBSD12.4 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@PC1:~ # drill ns1
;; ->>HEADER<<- opcode: QUERY, rcode: NXDOMAIN, id: 51892
;; flags: qr rd ra ; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;; ns1. IN      A

;; ANSWER SECTION:

;; AUTHORITY SECTION:
.          3360    IN      SOA      a.root-servers.net. nstld.verisign-grs.com. 2023
060700 1800 900 604800 86400

;; ADDITIONAL SECTION:

;; Query time: 0 msec
;; SERVER: 192.168.2.1
;; WHEN: Wed Jun 7 18:03:56 2023
;; MSG SIZE rcvd: 96
root@PC1:~ #
```

```
PC1 - FreeBSD12.4 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@PC1:~ # drill ns1.ntua.lab
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 55798
;; flags: qr aa rd ra ; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;; ns1.ntua.lab. IN      A

;; ANSWER SECTION:
ns1.ntua.lab. 3600    IN      A          192.168.2.1

;; AUTHORITY SECTION:

;; ADDITIONAL SECTION:

;; Query time: 0 msec
;; SERVER: 192.168.2.1
;; WHEN: Wed Jun 7 18:04:06 2023
;; MSG SIZE rcvd: 46
root@PC1:~ #
```

2.38) Οι ερωτήσεις έγιναν για τα ονόματα ns1 και ns1.ntua.lab και λήφθηκε απάντηση μόνο για το ns1.ntua.lab, όπως φαίνεται και παραπάνω (*ANSWER SECTION*).

2.39) Από την παραπάνω διαδικασία συμπεραίνω ότι η χρήση του επιθέματος ntua.lab είναι υποχρεωτική για να ληφθεί απάντηση, δηλαδή πρέπει να συμπεριλαμβάνω το search path στα ερωτήματα DNS που κάνω.

2.40) Στο PC1 κάνω “`ping localhost`” και μετά “`ping pc1`”. Δεν παράγονται ερωτήσεις προς τον εξυπηρετητή DNS, καθώς τα ονόματα `localhost` και `PC1` περιέχονται στο αρχείο `/etc/hosts`. (βλ. εικόνα ερωτήματος 2.1)

2.41) Στο PC1 κάνω “`ping ns1`” και το σταματώ (ή “`ping -c 2 ns1`”).

2.42) Ανταλλάχθηκαν 2 μηνύματα DNS (μία ερωταπάντηση) και αφορούσαν ερώτημα προς τον εξυπηρετητή DNS τύπου A? για το `ns1.ntua.lab`. Δόθηκε κανονικά απάντηση η διεύθυνση `192.168.2.1`.

2.43) Στο PC1 ξανακάνω “`ping ns1`” και το σταματώ (ή “`ping -c 2 ns1`”). Επαναλαμβάνω ακόμα δύο φορές. Παρατηρώ ότι δεν παράγονται συνέχεια ερωτήματα προς τον εξυπηρετητή DNS. Συγκεκριμένα, έγιναν 3 ερωτήματα (εκτέλεσα συνολικά 3 φορές “`ping -c 2 ns1`”).

2.44) Από τα παραπάνω συμπεραίνω ότι οι απαντήσεις του εξυπηρετητή DNS αποθηκεύονται προσωρινά στο PC1, τουλάχιστον για κάθε διεργασία ξεχωριστά. Για παράδειγμα, για κάθε ένα `ping` ξεχωριστά από τα παραπάνω αποστάλθηκε ένα ερώτημα, όσα πακέτα ICMP echo request και αν στάλθηκαν στο καθένα.

### **Άσκηση 3**

#### ***Εγκατάσταση εξυπηρετητή HTTP (στο SRV)***

- 1) Επιβεβαιώνω ότι η διεπαφή `em0` είναι σε NAT.
- 2) Στη συνέχεια, αφού εκκινήσω το εικονικό μου μηχάνημα, ως διαχειριστής (`root`) ενεργοποιώ τον πελάτη DHCP στην κάρτα δικτύου με “`dhclient em0`”.
- 3) Μπορώ να κάνω `ping` στο [www.google.com](http://www.google.com).
- 4) Εκτελώ “`pkg install lighttpd`” για την από απόσταση εγκατάσταση της έκδοσης 1.4.69 του πακέτου, απαντώντας θετικά στις ερωτήσεις που εμφανίζονται.
- 5) Διαγράφω το αρχείο `/etc/resolv.conf` με “`rm /etc/resolv.conf`” και προσθέτω το SRV στο δίκτυο LAN1.



### *Απαντήσεις Ερωτημάτων Άσκησης*

(Παρόλο που δεν αναφέρεται στην εκφώνηση, αργότερα θα χρειαστεί να έχω εγκατεστημένο το πακέτο unbound, κυρίως για να μπορέσω να εκτελέσω την εντολή “unbound-checkconf *cfgfile*”. Επομένως, εκτελώ “pkg install unbound”).

3.1) Στο αρχείο /etc/rc.conf ορίζω το όνομα του μηχανήματος σε SRV και προσθέτω την εντολή lighttpd\_enable=“YES” ώστε να ξεκινά η υπηρεσία http όταν κάνει επανεκκίνηση. Τα παραπάνω κάνω με τις αντίστοιχες εντολές “sysrc -f /etc/rc.conf hostname=“SRV”” και “sysrc -f /etc/rc.conf lighttpd\_enable=“YES””.

3.2) Δημιουργώ τον φάκελο /usr/local/www/data με την εντολή “mkdir /usr/local/www/data”.

3.3) Εντός του προηγούμενου φακέλου δημιουργώ ένα αρχείο με όνομα index.html και περιεχόμενο την πρόταση ‘Hello World!’ με τις αντίστοιχες εντολές “touch /usr/local/www/data/index.html” και “echo “Hello World!” > /usr/local/www/data/index.html”.

3.4) Επανεκκινώ το εικονικό μηχανήμα SRV και, διαγράφω το αρχείο /etc/resolv.conf με τις αντίστοιχες εντολές “reboot” και “rm /etc/resolv.conf”.

3.5) Εκτελώντας “service lighttpd status” βεβαιώνομαι ότι η υπηρεσία HTTP έχει ενεργοποιηθεί στο SRV.

3.6) Μπορώ να βεβαιωθώ για το παραπάνω επίσης με την εντολή “netstat -a | grep http”.

3.7) Τοποθετώ τη διεπαφή του SRV στο LAN1 και ορίζω σε αυτήν την IPv4 διεύθυνση 192.168.2.3/28 εκτελώντας “ifconfig em0 inet 192.168.2.3/28”.

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

```
(“echo ‘server:’ >> /var/tmp/unbound.conf”),  
(“echo ‘interface: 0.0.0.0’ >> /var/tmp/unbound.conf”),  
“echo ‘local-data: “SRV.ntua.lab. IN A 192.168.2.3”’ >>  
/var/tmp/unbound.conf”
```

(Οι δύο πρώτες εντολές είναι απαραίτητες για να λειτουργήσει σωστά το αρχείο.)

3.9) Προσθέτω στο αρχείο την αντίστροφη εγγραφή PTR για τη διεύθυνση 192.168.2.3 εκτελώντας “echo ‘local-data-ptr: “192.168.2.3 SRV.ntua.lab”’ >> /var/tmp/unbound.conf”.

3.10) Στη συνέχεια, αφού ελέγξω για την ορθότητά του με “unbound-checkconf /var/tmp/unbound.conf”, το αντιγράφω στο /usr/local/etc/unbound/unbound.conf με “cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf” και επανεκκινώ τον εξυπηρετητή DNS με “service unbound restart” για να ισχύσουν οι αλλαγές που έκανα.

3.11) Στο SRV ξεκινώ μια καταγραφή για την κίνηση στο LAN1 με απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων με “tcpdump -vni em0”.

3.12) Στο PC1, χρησιμοποιώντας την εντολή fetch, κατεβάζω-αποθηκεύω με μη διαδραστικό τρόπο από το url <http://srv.ntua.lab> την ιστοσελίδα που κατασκεύασα πριν, εκτελώντας “fetch <http://srv.ntua.lab>”.

3.13) Το πρωτόκολλο μεταφοράς που χρησιμοποιήθηκε για το παραπάνω είναι το TCP στην θύρα 80.

3.14) Το περιεχόμενο της ιστοσελίδας που κατέβασα στο 3.12 αποθηκεύτηκε στο αρχείο srv.ntua.lab.

## Άσκηση 4

Με τη βοήθεια της εντολής sysrc στο αρχείο /etc/rc.conf του NS1:

4.1) ...ενεργοποιώ τη λειτουργία δρομολόγησης:

“sysrc -f /etc/rc.conf gateway\_enable=“YES””

4.2) ...ενεργοποιώ το τείχος προστασίας ipfw:

“sysrc -f /etc/rc.conf firewall\_enable=“YES””

4.3) ...καθορίζω ανοικτή λειτουργία για το τείχος προστασίας:

“sysrc -f /etc/rc.conf firewall\_type=“open””

4.4) ...επιτρέπω τη λειτουργία NAT για το τείχος προστασίας ipfw:

“sysrc -f /etc/rc.conf firewall\_nat\_enable=“YES””

4.5) ...ορίζω στη διεπαφή em2 του NS1 την IP διεύθυνση 192.168.2.17/28:

“sysrc -f /etc/rc.conf ifconfig\_em2=“192.168.2.17/28””

4.6) Επιβεβαιώνω ότι οι τιμές των μεταβλητών στο `/etc/rc.conf` είναι σωστές με `cat /etc/rc.conf`.

4.7) Στη συνέχεια κλείνω το εικονικό μηχάνημα NS1, τοποθετώ τη διεπαφή του em2 στο τοπικό δίκτυο DMZ και το επανεκκινώ. Ορίζω προκαθορισμένη πύλη τη διεύθυνση IPv4 του NAT στο host μηχάνημα με `route add default ...`.