



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Εργαστήριο Δικτύων Υπολογιστών

Αναφορά 12ης Εργαστηριακής Άσκησης

Ραπτόπουλος Πέτρος (el19145)

Ημερομηνία: 30/5/2023

Άσκηση 1: Εγκατάσταση DHCP server

Προετοιμασία:

```
syslogd_flags="-scc" # to disable compression of repeated messages
root@PC1:~ # sysrc ifconfig_em0="inet 192.168.2.1/28" -f /etc/rc.conf
sysrc: /etc/rc.conf: name contains characters not allowed in shell
root@PC1:~ # sysrc -f /etc/rc.conf ifconfig_em0="inet 192.168.2.1/28"
ifconfig_em0: -> inet 192.168.2.1/28
root@PC1:~ # sysrc -f /etc/rc.conf ifconfig_em1="DHCP"
ifconfig_em1: -> DHCP
root@PC1:~ # sysrc -f /etc/rc.conf dhcpd_enable="YES"
dhcpd_enable: -> YES
root@PC1:~ # sysrc -f /etc/rc.conf hostname="ns1.ntua.lab"
hostname: PC.ntua.lab -> ns1.ntua.lab
root@PC1:~ # sysrc -f /etc/rc.conf dhcpd_ifaces="em0"
dhcpd_ifaces: -> em0
```

```
root@PC1:~ # cat /etc/rc.conf
sshd_enable="YES" # to enable the ssh daemon
hostname="ns1.ntua.lab" # to assign the host name
syslogd_flags="-scc" # to disable compression of repeated messages
ifconfig_em0="inet 192.168.2.1/28"
ifconfig_em1="DHCP"
dhcpd_enable="YES"
dhcpd_ifaces="em0"
```

```
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;
}
```

1.1) Ξεκινήστε μια καταγραφή στο NS1 για το LAN1 με εμφάνιση λεπτομερειών, διευθύνσεων MAC και

απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων. **tcpdump -i em0 -e -nvvv**

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. **dhclient em0**

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

DHCP Request από τον PC1 σε broadcast διεύθυνση

DHCP Reply από τον NS1 στον PC1

DHCP Request από τον PC1 στον NS1

DHCP Reply από τον NS1 στον PC1

ICMP Request από τον NS1 στον PC1

ICMP Reply από τον PC1 στον NS1

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

DHCP Discover από τον πελάτη στον εξυπηρετητή

DHCP Offer από τον εξυπηρετητή στον πελάτη

DHCP Request από τον πελάτη στον εξυπηρετητή

DHCP ACK από τον εξυπηρετητή στον πελάτη

1.5) Ποια διεύθυνση αποδόθηκε στο PC1: **192.168.2.5** και ποια η διεύθυνση IPv4 του εξυπηρετητή: **192.168.2.1**

1.6) Μετά από πόσο χρόνο πρέπει το PC1 να ανανεώσει τη διεύθυνση IPv4 που έλαβε; **Μετά από 60 δευτερόλεπτα**

1.7) Ποιο πρωτόκολλο μεταφοράς βλέπετε ότι χρησιμοποιείται για τα μηνύματα DHCP; **UDP**

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; **Θύρες 67-68**

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.

DHCP Discover, Source: 0.0.0.0, Destination: 255.255.255.255 (broadcast)

DHCP Offer, Source: 192.168.2.1, Destination: 192.168.2.5

DHCP Request, Source: 0.0.0.0, Destination: 255.255.255.255 (broadcast)

DHCP ACK, Source: 192.168.2.1, Destination: 192.168.2.5

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

DHCP Discover, Source: 08:00:27:66:53:11, Destination: ff:ff:ff:ff:ff:ff (broadcast)

DHCP Offer, Source: 08:00:27:38:24:dc, Destination: 08:00:27:66:53:11

DHCP Request, Source: 08:00:27:66:53:11, Destination: ff:ff:ff:ff:ff:ff (broadcast)

DHCP ACK, Source: 08:00:27:38:24:dc, Destination: 08:00:27:66:53:11

- 1.11)** Πώς είναι δυνατόν το PC1 να στέλνει και λαμβάνει μηνύματα DHCP (ενθυλακωμένα σε πακέτα IPv4) παρότι δεν έχει διεύθυνση IPv4; **Χρησιμοποιεί τη διεύθυνση 0.0.0.0**
- 1.12)** Παρατηρήσατε πλαίσια ARP στην καταγραφή πριν την DHCP Offer του NS1; Εάν ναι, ποιος τα παράγει και γιατί; **Παρατηρήσαμε πλαίσια ARP με πηγή τον NS1. Αναζητείται ο κάτοχος της διεύθυνσης 192.168.2.5 ώστε ο DHCP server να είναι σίγουρος ότι η διεύθυνση που πρόκειται να προτείνει δεν χρησιμοποιείται από κάποιον άλλον host.**
- 1.13)** Παρατηρήσατε μήνυμα ICMP στην καταγραφή πριν την απάντηση DHCP Offer του NS1; Όχι
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; **Για να διαπιστώσει αν δόθηκε η ίδια IP σε άλλο μηχάνημα. Κατά αυτόν τον τρόπο ανακοινώνεται επίσης και η νέα αντιστοίχιση IP address-MAC.**
- 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; **Ναι παρατηρήσαμε με πηγή τον NS1. Για να επιβεβαιωθεί ότι έγινε σωστά η ανάθεση της IP διεύθυνσης στον σωστό host.**
- 1.16)** Για πόσο χρόνο διαρκεί η εκχώρηση της διεύθυνσης IPv4; **120 δευτερόλεπτα αν δεν ανανεωθεί**
- 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; **Το πεδίο Requested-IP που περιέχει τη διεύθυνση IP που ζητά ο PC1.**
- 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; **Πλέον δεν υπάρχει το πεδίο Requested-IP αλλά υπάρχει πεδίο Client IP address**
- 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; **Για να ενημερώσει τον host ότι πλέον (μετά την αναγνώριση της ανανέωσης) δεν είναι διαθέσιμος στη συγκεκριμένη θύρα.**
- 1.20)** Πόσες παραμέτρους ζήτησε ο πελάτης από τον εξυπηρετητή με το μήνυμα DHCP Discover; **10**
- 1.21)** Ποιες από αυτές προσδιορίζει τελικά ο εξυπηρετητής DHCP στο μήνυμα DHCP Offer; **4**
- 1.22)** Σε ποιο αρχείο καταγράφει ο εξυπηρετητής τα δάνεια για τις διευθύνσεις που αποδίδει;
/var/db/dhcpd/dhcpd.leases
- 1.23)** Κάθε πότε γίνονται εγγραφές για το κάθε δάνειο; **Κάθε 60 δευτερόλεπτα**
- 1.24)** Ποιες πληροφορίες περιέχει για κάθε δάνειο;
- ```
lease 192.168.2.5 {
 starts 4 2023/06/01 12:42:10;
 ends 4 2023/06/01 12:44:10;
 cltt 4 2023/06/01 12:42:10;
 binding state active;
 next binding state free;
 rewind binding state free;
 hardware ethernet 08:00:27:66:53:11;
 uid "\001\010\000\fs\021";
 client-hostname "PC";
}
```
- 1.25)** Σε ποιο αρχείο καταγράφει ο πελάτης τα δάνεια για τις διευθύνσεις IPv4 που του εκχωρούνται;  
**/var/db/dhclient.leases.emo**
- 1.26)** Ποιες πληροφορίες περιέχει για κάθε δάνειο;
- ```
lease {
  interface "em0";
  fixed-address 192.168.2.5;
  option subnet-mask 255.255.255.240;
  option routers 192.168.2.1;
  option domain-name "example.org";
  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 4 2023/6/1 13:09:14;
  rebind 4 2023/6/1 13:09:59;
  expire 4 2023/6/1 13:10:14;
}
```
- 1.27)** Πόσος χρόνος πρέπει να περάσει μεταξύ μιας αποτυχημένης ανανέωσης και την αρχή της διαδικασίας επανασύνδεσης (rebind); **45 seconds**
- 1.28)** Στον NS1 ξεκινήστε μια νέα καταγραφή στη διεπαφή em0 με απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων και αφήστε την να τρέχει. **tcpdump -i em0 -e -nvvv**

1.29) Σε δεύτερη κονσόλα στον NS1 δώστε εντολή για να σταματήσετε τον εξυπηρετητή DHCP. **service isc-dhcpd stop**

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.

Μετά από 2 λεπτά χάνεται η διεύθυνση, service isc-dhcpd start

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.

Αποδόθηκε διεύθυνση IP και είναι ίδια με προηγούμενως

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

Τα DHCP Request από το PC1 είναι πολλά και απέχουν περίπου 20 δευτερόλεπτα μεταξύ τους.

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

Μερικές φορές δεν λαμβάνει απάντηση ενώ άλλες λαμβάνει udp port 67 unreachable

1.34) Μετά από τις πρώτες ανεπιτυχείς προσπάθειες ανανέωσης, ποιος είναι ο προορισμός του τελευταίου μηνύματος DHCP Request που στέλνει το PC1; **Στη διεύθυνση broadcast**

1.35) Εάν το προηγούμενο μήνυμα παράχθηκε μετά τη λήξη του χρόνου επανασύνδεσης (rebind), αιτιολογήστε τη χρήση της συγκεκριμένης διεύθυνσης προορισμού. **Εγκαταλείπεται η προσπάθεια επανασύνδεσης με τον συγκεκριμένο dhcp server και εκπέμπεται μήνυμα ανακάλυψης νέου.**

1.36) Ποιος είναι ο προορισμός (διεύθυνση MAC και IPv4) των μηνυμάτων DHCP Discover που παράγει το PC1 αμέσως μετά την απώλεια διεύθυνσης IPv4; **Broadcast διευθύνσεις** και από ποιο πεδίο του μηνύματος γίνεται κατανοητό ότι έχει απολεσθεί η διεύθυνση IPv4;; **Για IP διεύθυνση πηγής έχουμε 0.0.0.0 και όχι την προηγούμενη IP**

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; **Για να διαπιστώσει αν η εν λόγω διεύθυνση έχει αποδοθεί σε άλλον host.**

1.38) Τι συμβαίνει στα δεδομένα του αρχείου με τα δάνεια που κρατά ο πελάτης; **Διαγράφονται**

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;

Αυτό είναι απαραίτητο διότι ο πελάτης μπορεί να μην έχει διεύθυνση IP όταν χρησιμοποιεί το πρωτόκολλο DHCP.

Ο server και ο client επικοινωνούν διαμέσου broadcasts και συνεπώς ο εξυπηρετητής εκπέμπει την προτεινόμενη διεύθυνση IP στο UDP στη θύρα 68. Δεν υπάρχει άλλος τρόπος ο εξυπηρετητής να φτάσει τον πελάτη και να του απαντήσει καθώς αυτός δεν έχει διεύθυνση IP.

Άσκηση 2: Εγκατάσταση εξυπηρετητή DNS

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. **vi /etc/hosts**

```
192.168.2.5    PC1.ntua.lab PC1
192.168.2.6    PC2.ntua.lab PC2
```

2.2) Εκτελέστε διαδοχικά τις εντολές "ping PC2", "ping pc2", "ping pc2.NTUA.LAB". Ποιο μηχανήμα απαντά; Έχει σημασία η χρήση μικρών ή κεφαλαίων γραμμάτων; **Το ping ολοκληρώνεται επιτυχώς και στις τρεις περιπτώσεις και απαντάει το PC2. Η χρήση μικρών ή κεφαλαίων γραμμάτων δεν επηρεάζει το ping.**

2.3) Επαναλάβετε τα προηγούμενα για το PC2 και επιβεβαιώστε ότι στο "ping PC1" απαντά το PC1. **vi /etc/hosts**

```
192.168.2.5    PC1.ntua.lab PC1
192.168.2.6    PC2.ntua.lab PC2
```

Ναι απαντάει.

2.4) Στο PC2 διαγράψτε την εγγραφή για το PC1 στο /etc/hosts. Ποια είναι η απάντηση που λαμβάνετε εάν κάνετε "ping PC1"; **ping: cannot resolve PC1: Host name lookup failure**

2.5) Ξεκινήστε το εικονικό μηχανήμα 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.

vi /var/tmp/unbound.conf

local-data: "PC1.ntua.lab IN A 192.168.2.5"

local-data: "PC2.ntua.lab IN A 192.168.2.6"

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

local-data-ptr: "192.168.2.5 PC1.ntua.lab"

local-data-ptr: "192.168.2.6 PC2.ntua.lab"

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. **unbound-checkconf /var/tmp/unbound.conf,**

cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf, service unbound onerestart

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

tcpdump -i em0 -e -nvvv

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

ifconfig em0 delete, dhclient em0

2.10) Σταματήστε την καταγραφή. Ποια διεύθυνση έλαβε το PC1 από τον εξυπηρετητή DHCP; **192.168.2.5**

2.11) Ποιες επιπλέον παραμέτρους έδωσε ο εξυπηρετητής DHCP σε σχέση με αυτές της ερώτησης 1.21. **Domain-Name**

2.12) Έχει δημιουργηθεί αρχείο /etc/resolv.conf στο PC1; **Ναι** Ποιο είναι το περιεχόμενό του; **search ntua.lab**

nameserver 192.168.2.1 (ίδιο με αυτό του DNS server)

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.

host 192.168.2.5 -> PC1.ntua.lab

2.14) Με τη βοήθεια της εντολής host βρείτε τη διεύθυνση του μηχανήματος NS1. **host NS1 -> 192.168.2.1**

2.15) Μπορείτε από το PC1 να κάνετε ping στο μηχανήμα με όνομα ns1; **Ναι**

2.16) Στο PC2 διαγράψτε τη στατική διεύθυνση IPv4 και αποδώστε δυναμικά νέα διεύθυνση IPv4 στη διεπαφή em0.

ifconfig em0 delete, dhclient em0

2.17) Ποια διεύθυνση έλαβε το PC2 από τον εξυπηρετητή DHCP; **192.168.2.6**

2.18) Μπορείτε από το PC2 να κάνετε ping στο PC1 χρησιμοποιώντας το όνομα αυτού; **Ναι μπορούμε**

2.19) Από πού έλαβε το PC2 τη διεύθυνση IP του PC1; Από το αρχείο /etc/hosts ή από τον εξυπηρετητή DNS;

Από τον εξυπηρετητή DNS αφού έχουμε διαγράψει την εγγραφή για το PC1 στο /etc/hosts στο ερώτημα 2.4

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"; **Όχι δεν μπορούμε πλέον**

2.21) Τι συμπεραίνετε για τη σειρά με την οποία γίνεται η αναζήτηση της πληροφορίας από τον τοπικό επιλυτή;

Αν υπάρχει εγγραφή στο /etc/hosts τότε ακολουθείται η πληροφορία αυτή. Έπειτα η πληροφορία που διαφημίζεται από τον εξυπηρετητή DNS

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;

cat /etc/nsswitch.conf, ναι συμφωνεί, πρώτα ελέγχεται το /etc/hosts και έπειτα η πληροφορία από τον dns

2.23) Με τη βοήθεια της εντολής host βρείτε τη διεύθυνση IP του PC2. **host PC2 -> 192.168.2.6**

2.24) Πώς εξηγείται η διαφορετική απάντηση σε σχέση με τη διεύθυνση που λαμβάνει το ping pc2;

To host ρωτάει κατευθείαν τον εξυπηρετητή DNS

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; **rm /etc/resolv.conf, resolvconf -u, είναι το ίδιο**

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. **tcpdump -i em0 -e -nvvv not port 67**

2.27) Με τη βοήθεια της εντολής host στο PC1 βρείτε τη διεύθυνση IP του ntua.lab. **host ntua.lab -> 192.168.2.1**

2.28) Υπάρχει στην καταγραφή κίνηση σχετική με το DNS; **Ναι**

2.29) Ποιο πρωτόκολλο μεταφοράς χρησιμοποιήθηκε από το DNS (TCP ή UDP); **UDP**

2.30) Καταγράψτε τις θύρες (προέλευσης και προορισμού) του πρωτοκόλλου μεταφοράς που χρησιμοποιήθηκαν.

53 και μία δυναμική θύρα για τον host (68354)

2.31) Ποια από τις παραπάνω θύρες αντιστοιχεί στο πρωτόκολλο εφαρμογής DNS; **53**

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. **tcpdump -i em0 -nvvv port 53**

2.33) Στο PC1 αναζητήστε τη διεύθυνση IP του NS1 με την εντολή host. **host ns1**

2.34) Πόσα μηνύματα DNS ανταλλάχθηκαν; **6**

2.35) Σε τι είδους ερωτήματα προς τον εξυπηρετητή DNS αντιστοιχούσαν και για ποιο όνομα έγιναν αυτές;

Για το όνομα ns1.ntua.lab και για εγγραφές τύπου A, AAAA, MX

2.36) Σε ποιες εξ αυτών δόθηκε απάντηση; **Και στις 3**

2.37) Αναζητήστε τη διεύθυνση IP του ns1 και του ns1.ntua.lab με την εντολή drill. **drill ns1, drill ns1.ntua.lab**

2.38) Για ποιο όνομα έγιναν ερωτήσεις και ποια απάντηση λήφθηκε;

ns1, ns1.ntua.lab, απάντηση πήραμε για το ns1.ntua.lab

2.39) Τι συμπεραίνεται σχετικά με τη χρήση του επιθέματος ntua.lab (search path) από τις δύο εντολές;

Προστίθεται αυτόματα στις εγγραφές, δηλαδή αν γίνει ερώτηση για το PC1 θα αναζητηθεί εγγραφή για το PC1.ntua.lab διότι το search path που έχουμε ορίσει στο αρχείο /etc/resolv.conf είναι το ntua.lab

2.40) Στο PC1 κάντε “ping localhost” και μετά “ping pc1”. Παράγονται ερωτήσεις προς τον εξυπηρετητή DNS και σε ποια περίπτωση; **ping localhost, ping pc1, παράγονται ερωτήσεις μόνο στη περίπτωση του localhost γιατί η πληροφορία για το PC1 περιέχεται στο αρχείο /etc/hosts.**

2.41) Στο PC1 κάντε “ping ns1” και σταματήστε το. **ping ns1**

2.42) Πόσα μηνύματα DNS ανταλλάχθηκαν και σε τι είδους ερωτήματα προς τον εξυπηρετητή DNS αφορούσαν; **2 μηνύματα και αφορούσαν εγγραφές τύπου A**

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;

Παράγεται 1 μήνυμα για κάθε ping

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

Άσκηση 3: Εγκατάσταση εξυπηρετητή HTTP

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.

vi /etc/rc.conf, hostname = “SRV”, lighttpd_enable = “YES”

3.2) Δημιουργήστε τον φάκελο /usr/local/www/data. **mkdir /usr/local/www/data**

3.3) Εντός του προηγούμενου φακέλου δημιουργήστε ένα αρχείο με όνομα index.html και περιεχόμενο την πρόταση “Hello World!” **echo “Hello World!” > /usr/local/www/data/index.html**

3.4) Επανεκκινήστε το εικονικό μηχανήμα SRV και, εάν υπάρχει, διαγράψτε το αρχείο /etc/resolv.conf. **reboot, rm /etc/resolv.conf**

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

3.6) Πώς θα μπορούσατε να δείτε το ίδιο με την εντολή netstat; **netstat -a**

3.7) Τοποθετήστε τη διεπαφή του SRV στο LAN1 και ορίστε σε αυτήν την IPv4 διεύθυνση 192.168.2.3/28. **ifconfig em1 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. **vi /var/tmp/unbound.conf, local-data: “SRV.ntua.lab IN A 192.168.2.3”**

3.9) Προσθέστε στο αρχείο την αντίστροφη εγγραφή PTR για τη διεύθυνση 192.168.2.3. **vi /var/tmp/unbound.conf, local-data-ptr: “192.168.2.3 SRV.ntua.lab”**

- 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. **`unbound-checkconf /var/tmp/unbound.conf`**
`cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf`, `service unbound restart`
- 3.11)** Στο SRV ξεκινήστε μια καταγραφή για την κίνηση στο LAN1 με απενεργοποιημένη την επίλυση ονομάτων και διευθύνσεων. **`tcpdump -i em1 -nnvv`**
- 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. **`fetch http://srv.ntua.lab`**
- 3.13)** Ποιο πρωτόκολλο μεταφοράς χρησιμοποιήθηκε: **TCP** και σε ποια θύρα ακούει ο εξυπηρετητής `http:: 80`
- 3.14)** Σε ποιο αρχείο αποθηκεύτηκε το περιεχόμενο της ιστοσελίδας που κατεβάσατε; **Στο αρχείο 'srv.ntua.lab'**

Άσκηση 4: Εγκατάσταση ιδιωτικού δρομολογητή και Firewall

- 4.1)** Ενεργοποιήστε τη λειτουργία δρομολόγησης (προώθηση πακέτων) **`sysrc -f /etc/rc.conf gateway_enable="YES"`**
- 4.2)** Να ενεργοποιήσετε το τείχος προστασίας `ipfw`. **`sysrc -f /etc/rc.conf firewall_enable="YES"`**
- 4.3)** Να καθορίσετε ανοικτή λειτουργία για το τείχος προστασίας. **`sysrc -f /etc/rc.conf firewall_type="open"`**
- 4.4)** Επιτρέψτε τη λειτουργία NAT για το τείχος προστασίας `ipfw`. **`sysrc -f /etc/rc.conf firewall_nat_enable="YES"`**
- 4.5)** Να ορίσετε 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)** Να επιβεβαιώσετε ότι οι τιμές των μεταβλητών στο `/etc/rc.conf` είναι σωστές. **`cat /etc/rc.conf`**
- 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.
`route add default 10.0.2.2`
- 4.8)** Διορθώστε το αρχείο `/etc/resolv.conf` όπως ορίσθηκε προηγουμένως στο βήμα 5 της άσκησης 2 και επιβεβαιώστε ότι η επίλυση ονομάτων λειτουργεί. **`vi /etc/resolv.conf`, `search ntua.lab`, `nameserver 192.168.2.1`, `host ns1`**
- 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`. **`vi /etc/rc.conf`, `ifconfig_emo="DHCP"`, `service netif restart`**
- 4.10)** Στο `PC2` προσθέστε τις κατάλληλες εντολές στο `/etc/rc.conf` ώστε, όταν εκκινεί, η διεπαφή `emo` να λαμβάνει τη διεύθυνση `192.168.2.4/28` και ο προεπιλεγμένος δρομολογητής να είναι η διεπαφή του `NS1` στο `LAN1`.
`vi /etc/rc.conf`, `ifconfig_emo="192.168.2.4/28"`, `defaultrouter="192.168.2.1"`
- 4.11)** Επανεκκινήστε τις υπηρεσίες `netif` και `routing` του `PC2`. **`service netif restart`, `service routing restart`**
Εάν δεν υπάρχει, δημιουργήστε αρχείο `/etc/resolv.conf`, όπως κάνατε προηγουμένως για το `PC1` και επιβεβαιώστε ότι η επίλυση ονομάτων λειτουργεί. **`vi /etc/resolv.conf`, `search ntua.lab`, `nameserver 192.168.2.1`, `host ns1`**
- 4.12)** Τοποθετήστε τη διεπαφή `emo` 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`.
**`vi /etc/rc.conf`, `ifconfig_emo="192.168.2.18/28"`, `defaultrouter="192.168.2.17"`,
`service netif restart`, `service routing restart`**
- 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.
`vi /var/tmp/unbound.conf`
`local-data: "SRV.ntua.lab IN A 192.168.2.18"`
`local-data-ptr: "192.168.2.18 SRV.ntua.lab"`
`local-data: "PC2.ntua.lab IN A 192.168.2.4"`
`local-data-ptr: "192.168.2.4 PC2.ntua.lab"`
`unbound-checkconf /var/tmp/unbound.conf`, `cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf`
`service unbound restart`

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

Ναι μπορούμε καθώς έχουμε ορίσει προεπιλεγμένη πύλη για το SRV και ο NS1 λειτουργεί ως δρομολογητής.

4.15) Στο NS1 προσθέστε κανόνα με αριθμό 2000 ώστε να απαγορεύεται οποιαδήποτε εισερχόμενη κίνηση μέσω της διεπαφής στο DMZ προς το LAN1. **ipfw add 2000 deny all from any to 192.168.2.0/28 in via em2**

4.16) Μπορείτε από το SRV να κάνετε ping στο PC1; **Όχι**

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.

ipfw add 1900 allow all from 192.168.2.0/28 to 192.168.2.16/28 in via em0 keep-state

4.18) Μπορείτε από το PC1 να κάνετε ping στο SRV; **Ναι**

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

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

4.21) Δημιουργήστε στο τείχος προστασίας του NS1 πίνακα in-kernel nat με αριθμό παρουσίας 111 ώστε τα πακέτα με ιδιωτικές 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. **ipfw nat 111 config if em1 reset**

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).

ipfw add 3000 nat 111 ip4 from any to any via em1

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

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

host 147.102.1.1 -> theseas.softlab.ece.ntua.gr

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

tcpdump -i em1 -nvvv

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; **ping -c 2 www.ntua.gr, 10.0.3.15**

4.27) Ποια είναι η διεύθυνση προορισμού των ICMP echo request; **147.102.224.101**

4.28) Προς ποιον εξυπηρετητή DNS έγινε η ερώτηση για την επίλυση του ονόματος www.ntua.gr; **NS1**

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. **tcpdump -i em1 -n port 53**

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; **Είναι διαφορετικός για κάθε ping**

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. **tcpdump -i em0 -n port 53**

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; **courses.cn.ece.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;

Έκανε ερώτημα τύπου A και έλαβε απάντηση τύπου A, CNAME

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.

tcpdump -i em1 -nvvv port 53

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 διάρκεια ισχύος των απαντήσεων DNS;

drill www.cn.ece.ntua.gr -> 1 ερώτημα DNS, χρονική διάρκεια ισχύος 20 λεπτά

- 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; **(NS1) tcpdump -i em0 -nnvv port 53 (PC1) drill www.cn.ece.ntua.gr, ναι παράγονται, η χρονική ισχύς μειώνεται για κάθε μήνυμα DNS**
- 4.37) Τι συμπεραίνετε σχετικά με το κατά πόσο αποθηκεύονται προσωρινά οι απαντήσεις που λαμβάνει ο τοπικός εξυπηρετητής DNS στο NS1;
- Ο NS1 αποθηκεύει προσωρινά τις απαντήσεις που λαμβάνει από άλλους εξυπηρετητές DNS λόγω της cache**
- 4.38) Μπορείτε από το SRV να κάνετε ping στον εξυπηρετητή http του ΕΜΠ με διεύθυνση IPv4 147.102.224.101; **Ναι**
- 4.39) Μπορείτε από το SRV να κάνετε ping στον εξυπηρετητή www.ntua.gr; Γιατί; **Όχι δεν έχει οριστεί DNS server**
- 4.40) Στο /etc/resolv.conf του SRV ορίστε ως εξυπηρετητή DNS τη διεπαφή του NS1 στο DMZ.
- vi /etc/resolv.conf, nameserver 192.168.2.17**
- 4.41) Μπορείτε τώρα από το SRV να κάνετε ping στο www.ntua.gr; **Ναι**
- 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; host www.ntua.lab, το ping δεν είναι επιτυχημένο διότι δεν έχουμε ορίσει εγγραφή για το alias www.ntua.lab
- 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.
- vi /var/tmp/unbound.conf**
- local-data: "www.ntua.lab IN A 192.168.2.18"**
- unbound-checkconf /var/tmp/unbound.conf, cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf**
- service unbound restart**
- 4.44) Από το PC1 κάντε ping στο www.ntua.lab. Ποιο μηχανήμα απαντά; **SRV**

Άσκηση 5: Εγκατάσταση δημόσιου δρομολογητή και DNS

- 5.1) Να ορίσετε το όνομα του μηχανήματος ως ns2.ntua.lab. **sysrc hostname="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. **sysrc ifconfig_em0="192.0.2.1/29", sysrc ifconfig_em2="192.0.2.9/29"**
- 5.3) Να ορίσετε ότι η διεπαφή em1 θα λάβει δυναμικά διεύθυνση μέσω DHCP. **sysrc ifconfig_em1="DHCP"**
- 5.4) Να ενεργοποιηθεί η λειτουργία δρομολόγησης. **sysrc gateway_enable="YES"**
- 5.5) Να ενεργοποιηθεί το τείχος προστασίας ipfw. **sysrc firewall_enable="YES"**
- 5.6) Να ορισθεί ανοικτή λειτουργία για το τείχος προστασίας. **sysrc firewall_type="open"**
- 5.7) Να ενεργοποιηθεί η λειτουργία NAT του τείχους προστασίας. **sysrc firewall_nat_enable="YES"**
- 5.8) Να διαγράψετε από το αρχείο /etc/rc.conf τις σχετικές με τον εξυπηρετητή DHCP γραμμές.
- vi /etc/rc.conf, (remove) dhcpd_enable="YES", (remove) dhcp_ifaces**
- 5.9) Να δείτε όλες τις μεταβλητές του αρχείου /etc/rc.conf και επιβεβαιώσετε ότι υπάρχει η εντολή για ενεργοποίηση της υπηρεσίας DNS. **unbound_enable="YES"**
- 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. **vi /var/tmp/unbound.conf**
- access-control: 192.0.2.0/24 allow**
- local-zone: "ntua.lab." redirect**
- local-data: "ntua.lab. IN A 192.0.2.10"**
- unbound-checkconf /var/tmp/unbound.conf, cp /var/tmp/unbound.conf /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 μηχανήμα. **reboot, υπάρχει ορισμένη προκαθορισμένη πύλη**

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.

ipfw nat 222 config if em1 same_ports reset

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).

ipfw add 1100 nat 222 ip4 from any to any via em1

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.

vi /etc/rc.conf

ifconfig_em0="192.0.2.2/29"

defaultrouter="192.0.2.1"

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.

service netif restart, service routing restart, vi /etc/resolv.conf

search ntua.lab, nameserver 192.0.2.1

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

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.

vi /etc/rc.conf

ifconfig_em1="192.0.2.10/29"

defaultrouter="192.0.2.9"

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

service netif restart, service routing restart

5.19) Μπορείτε από το PC1 και το SRV να κάνετε ping στο www.ntua.gr; **Ναι**

Παραμένει η λειτουργία του πίνακα nat 111; **Ναι**

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

Για το PC1 επιστρέφεται 192.168.2.18 (SRV). Για το PC2 επιστρέφεται 192.0.2.10 (NS1).

5.21) Χρησιμοποιώντας την εντολή fetch μπορείτε από το PC2 να κατεβάσετε την ιστοσελίδα <http://www.ntua.lab>;

Όχι δεν μπορούμε Ποιο λάθος εμφανίζεται; **connection refused**

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.

ipfw nat 111 config if em1 reset redirect_port tcp 192.168.2.18:80 80

5.23) Μπορείτε τώρα στο PC2 να κατεβάσετε την ιστοσελίδα <http://www.ntua.lab>; **Ναι**

5.24) Μπορείτε από το PC2 να κάνετε ping to www.ntua.lab; **Ναι** Ποιο μηχανήμα απαντά; **NS1**

5.25) Σε ποιο μηχανήμα συνδέστε με ssh lab@www.ntua.lab από το PC1; **SRV**

5.26) Εάν προσπαθήσετε το προηγούμενο από το PC2, με ποιο μηχανήμα θα συνδεθείτε; **NS1** Γιατί; **Η διεύθυνση IP που έχει δοθεί στην εγγραφή για το www.ntua.lab είναι αυτή του NS1. Επίσης δεν υπάρχει κανόνας στο firewall προώθησης των πακέτων προς το SRV**

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.

ipfw nat 111 config if em1 reset redirect_port tcp 192.168.2.18:80 80 redirect_port tcp 192.168.2.18:22 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; **Ναι μπορούμε, φαίνεται από το hostname**