

Εργαστήριο Δικτύων Υπολογιστών

Εργαστηριακή Άσκηση 12 Υπηρεσίες στο Διαδίκτυο

Όνοματεπώνυμο: Νικόλαος Παγώνας, el18175	Όνομα PC: nick-ubuntu
Ομάδα: 1 (Τρίτη 10:45)	Ημερομηνία Εξέτασης: Τρίτη 31/05/22

Άσκηση 1: Εγκατάσταση DHCP server

Κατασκευάζουμε ένα εικονικό μηχάνημα με βάση ένα νέο FreeBSD 12.3 με 3 κάρτες δικτύου:

1.

Ορίζουμε τη διεπαφή `em1` σε NAT.

2.

Εκτελούμε `dhclient em1`.

3.

Εκτελούμε `ping www.google.com`. Το ping είναι επιτυχές.

4.

Εκτελούμε `pkg update`.

5.

Εκτελούμε `poweroff` και ύστερα από τη διαδρομή `File→Export Appliance...` δημιουργούμε ένα αρχείο `new.ova`.

Στη συνέχεια δημιουργούμε ένα νέο μηχάνημα NS1 βασισμένο στο `new.ova`.

1.

Εκτελούμε `pkg install isc-dhcp44-server`.

2.

Κατασκευάζουμε ένα δικό μας `dhcpd.conf` με περιεχόμενα:

```
default-lease-time 60;           # (e)
max-lease-time 120;              # (f)

subnet 192.168.2.0 netmask 255.255.255.240 {
    range 192.168.2.5 192.168.2.6;  # (b)
    option routers 192.168.2.1;     # (c)
    option broadcast address 192.168.2.15; # (d)
}
```

3.

Εκτελούμε:

```
sysrc ifconfig_em0="192.168.2.1/28" # (a)
sysrc ifconfig_em1="DHCP"           # (b)
sysrc dhcpd_enable="YES"            # (c)
sysrc dhcp_ifaces="em0"             # (d)
sysrc hostname="ns1.ntua.lab"       # (e)
```

4.

Εκτελούμε `reboot`.

5.

Εκτελούμε `service isc-dhcpd status` και επιβεβαιώνουμε ότι η υπηρεσία `dhcpd` τρέχει κανονικά.

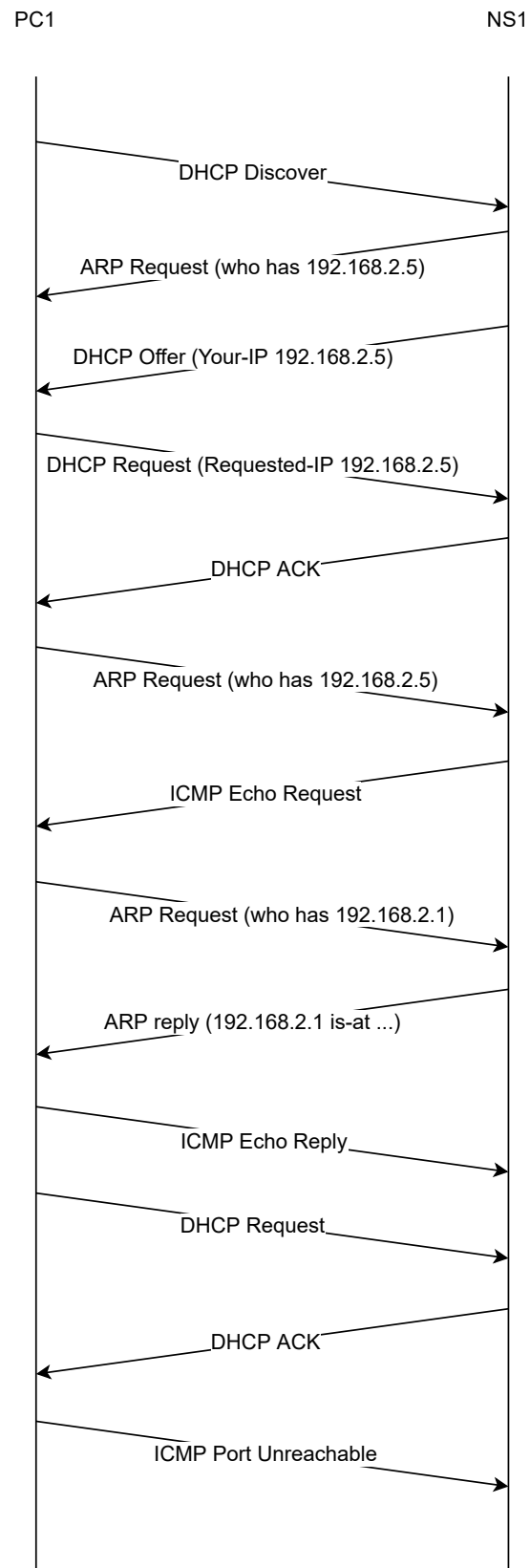
1.1

Στο NS1 εκτελούμε `tcpdump -veni em0`.

1.2

Στο PC1 εκτελούμε `dhclient em0` και περιμένουμε τουλάχιστον δύο λεπτά.

1.3



1.4

Ανταλλάσσονται:

```
DHCPDISCOVER on em0 to 255.255.255.255
DHCPDISCOVER on em0 to 255.255.255.255
DHCPOFFER from 192.168.2.1
DHCPREQUEST on em0 to 255.255.255.255
DHCPACK from 192.168.2.1
```

1.5

Αποδόθηκε η 192.168.2.5, ενώ η IP του εξυπηρετητή είναι 192.168.2.1.

1.6

Μετά από 60 δευτερόλεπτα, όπως φαίνεται στη γραμμή:

```
bound to 192.168.2.5 -- renewal in 60 seconds.
```

1.7

Βλέπουμε ότι χρησιμοποιείται το UDP.

1.8

Οι θύρες πηγής και προορισμού είναι οι 67 (PC1) και 68 (NS1).

1.9

Έχουμε:

Message	Source IP	Destination IP
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

1.10

Έχουμε:

Message	Source MAC	Destination MAC
DHCP DISCOVER	08:00:27:cc:ef:48	ff:ff:ff:ff:ff:ff
DHCP OFFER	08:00:27:64:52:f6	08:00:27:cc:ef:48
DHCP REQUEST	08:00:27:cc:ef:48	ff:ff:ff:ff:ff:ff
DHCP ACK	08:00:27:64:52:f6	08:00:27:cc:ef:48

1.11

Μπορεί να το κάνει χρησιμοποιώντας την διεύθυνση IP 0.0.0.0, τις διευθύνσεις MAC, και την ευρυεκπομπή (όπως φαίνεται στα μηνύματα DHCP DISCOVER/REQUEST).

1.12

Ναι, παρατηρήσαμε πλαίσια ARP από τον NS1, ο οποίος θέλει να εξακριβώσει αν χρησιμοποιεί κάποιος τη διεύθυνση IP που σκοπεύει να προσφέρει.

1.13

Όχι, δεν παρατηρήσαμε.

1.14

Με αυτό το πλαίσιο ARP το PC1 προσπαθεί να επιβεβαιώσει ότι δεν υπάρχει άλλος υπολογιστής με αυτή τη διεύθυνση IP.

1.15

Ναι, παρατηρήσαμε ένα ICMP request από τον NS1, και το αντίστοιχο ICMP reply από το PC1. Αυτή η ανταλλαγή γίνεται προκειμένου να επιβεβαιωθεί ότι η απόδοση διεύθυνσης έγινε χωρίς κάποιο πρόβλημα.

1.16

Διαρκεί 120 δευτερόλεπτα (Lease-Time: 120).

1.17

Περιέχει τα επιπλέον options:

Server-ID Option 54, length 4: 192.168.2.1

Requested_IP Option 50, length 4: 192.168.2.5

1.18

Στο δεύτερο DHCP request:

- Δεν χρησιμοποιείται πλέον η MAC προορισμού ff:ff:ff:ff:ff:ff (broadcast), αλλά η 08:00:27:64:52:f6 (NS1)
- Δεν χρησιμοποιείται η IP πηγής 0.0.0.0, αλλά η 192.168.2.5 (PC1)
- Δεν χρησιμοποιείται η IP προορισμού 255.255.255.255 (broadcast), αλλά η 192.168.2.1 (NS1).
- Εμφανίζεται το επιπλέον option "Client IP: 192.168.2.5"
- Δεν εμφανίζεται το option "Server-ID Option 54, length 4: 192.168.2.1".
- Δεν εμφανίζεται το option "Requested-IP Option 50, length 4: 192.168.2.5".

1.19

Αυτό συμβαίνει διότι ο πελάτης DHCP (PC1) ανανέωσε τη διεύθυνση IPv4 του, οπότε η σύνδεση στη θύρα 68 δεν χρειάζεται πλέον (σε αντίθεση με αυτή του εξυπηρετητή DHCP στη θύρα 67, που πρέπει να παραμένει ανοιχτή για να ακούσει τυχόν αιτήματα από πελάτες).

1.20

Στο αρχείο `/var/db/dhcpd/dhcpd.leases`.

1.21

Γίνονται κάθε ένα λεπτό.

1.22

Περιέχει τις πληροφορίες:

```
starts ...
ends ...
cltt ...
binding state ...
next binding state ...
rewind binding state ...
hardware ethernet ...
uid ...
client-hostname ...
```

1.23

Στο αρχείο `/var/db/dhclient.leases.em0`.

1.24

Περιέχει τις πληροφορίες:

```
interface ...
fixed-address ...
option subnet-mask ...
option routers ...
option broadcast-address ...
option dhcp-lease-time ...
option dhcp-message-type ...
option dhcp-server-identifier ...
renew ...
rebind ...
expire ...
```

1.25

Ο ζητούμενος χρόνος είναι ίσος με `rebind - renew = 45 sec`.

1.26

Ζήτησε 10 παραμέτρους:

Subnet-Mask
BR
Time-Zone
Classless-Static-Route
Default-Gateway
Domain-Name
Domain-Name-Server
Hostname
Option 119 (Domain Search List)
MTU

1.27

Προσδιορίζει τις παραμέτρους Subnet-Mask, BR, και Default-Gateway.

1.28

Στον NS1 εκτελούμε `tcpdump -ni em0`.

1.29

Σε δεύτερη κονσόλα στον NS1 εκτελούμε `service isc-dhcpd stop`.

1.30

Στο PC1 εκτελούμε συνεχώς `ifconfig em0` μέχρι η διεπαφή `em0` να μην έχει πλέον διεύθυνση IP. Μόλις συμβεί αυτό, εκτελούμε `service isc-dhcpd start` στον NS1.

1.31

Στο PC1 εκτελούμε συνεχώς `ifconfig em0` μέχρι η διεπαφή `em0` να ξαναποκτήσει διεύθυνση IP. Μόλις συμβεί αυτό, σταματάμε την καταγραφή στον NS1.

1.32

Στάλθηκαν 4 μηνύματα DHCP:

#1 (3 sec) #2 (5 sec) #3 (11 sec) #4 (26 sec) #5

1.33

Λαμβάνει απάντηση "ICMP udp port 67 unreachable", που σημαίνει ότι ο εξυπηρετητής DHCP δεν ακούει στην θύρα 67, το οποίο είναι λογικό, αφού τον απενεργοποιήσαμε, και έτσι δεν προσφέρεται η υπηρεσία DHCP.

1.34

Είναι η διεύθυνση 255.255.255.255 (broadcast).

1.35

Χρησιμοποιείται η 255.255.255.255 ως διεύθυνση προορισμού, επειδή αφού λήξει ο χρόνος επανασύνδεσης (rebind), το PC1 προσπαθεί να δανειστεί μία νέα διεύθυνση από οποιονδήποτε άλλο εξυπηρετητή, όχι υποχρεωτικά από αυτόν που δανείστηκε πριν.

1.36

Είναι:

MAC Destination: ff:ff:ff:ff:ff:ff

IP Destination: 255.255.255.255

Το πεδίο του μηνύματος που δείχνει ότι έχει απολεσθεί η διεύθυνση IP είναι το:

Requested-IP: 192.168.2.5

1.37

Επειδή ο NS1 προσπαθεί να επιβεβαιώσει ότι δεν χρησιμοποιείται από κάποιον άλλον η διεύθυνση που πρόκειται να προσφέρει.

1.38

Στο PC1 εκτελούμε `cat /var/db/dhclient.leases.em0`. Παρατηρούμε ότι με κάθε ανανέωση της IP διεύθυνσης προστίθεται ένα νέο δάνειο στο αρχείο αυτό.

1.39

Αυτό συμβαίνει διότι το DHCP πρέπει να είναι συμβατό με το BOOTP ([RFC 2131](#), "DHCP must provide service to existing BOOTP clients") και ως εκ τούτου, ακολουθούνται αυτά που περιγράφονται στο [RFC 951](#):

We could not simply allow the client to pick a 'random' port number for the UDP source port field; since the server reply may be broadcast, a randomly chosen port number could confuse other hosts that happened to be listening on that port.

Άσκηση 2: Εγκατάσταση εξυπηρετητή DNS

Εγκαθιστούμε έναν εξυπηρετητή DNS στο NS1:

1.

Εκτελούμε `pkg install unbound`.

2.

Εκτελούμε `sysrc unbound_enable="YES"`.

3.

Δημιουργούμε ένα προσωρινό αρχείο `/var/tmp/unbound.conf` με περιεχόμενο:

```
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.
                20200501 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."
forward-zone:
name: "."
forward-addr: 1.1.1.1
forward-addr: 8.8.8.8
forward-addr: 9.9.9.9
```

4.

Εκτελούμε `unbound-checkconf /var/tmp/unbound.conf`. Δεν υπάρχουν λάθη, οπότε εκτελούμε `cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf`.

5.

Εκτελούμε `cat /etc/resolv.conf`. Το αρχείο υπάρχει, οπότε εκτελούμε `rm /etc/resolv.conf`. Δημιουργούμε νέο `/etc/resolv.conf` με περιεχόμενα:

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

6.

Προσθέτουμε στην αρχή του `/usr/local/etc/dhcpd.conf` τις γραμμές:

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

7.

Εκτελούμε `service isc-dhcpd restart`. Δεν υπάρχουν λάθη.

8.

Εκτελούμε `poweroff` και ύστερα δημιουργούμε έναν κλώνο του NS1, τον NS2.

Πριν ξεκινήσουμε την άσκηση, εκτελούμε:

```
### PC1 ###
```

```
ifconfig em0 192.168.2.5/28  
rm /etc/resolv.conf
```

```
### PC2 ###
```

```
ifconfig em0 192.168.2.6/28  
rm /etc/resolv.conf
```

Επίλυση ονομάτων μέσω του αρχείου `/etc/hosts`

2.1

Στο PC1, τροποποιούμε το `/etc/hosts` ως εξής: ("---" σημαίνει διαγραφή γραμμής, ενώ "+++" σημαίνει προσθήκη γραμμής):

```
--- ::1                localhost localhost.my.domain  
+++ ::1                localhost localhost.ntua.lab  
  
--- 127.0.0.1          localhost localhost.my.domain  
+++ 127.0.0.1          localhost localhost.ntua.lab  
  
+++ 192.168.2.5        PC1          PC1.ntua.lab  
+++ 192.168.2.6        PC2          PC2.ntua.lab
```

2.2

Στο PC1 εκτελούμε:

```
ping PC2  
ping pc2  
ping pc2.NTUA.LAB
```

Και στις 3 περιπτώσεις απαντά το PC2, ενώ δεν έχει σημασία η χρήση μικρών ή κεφαλαίων γραμμάτων.

2.3

Στο PC2, τροποποιούμε το `/etc/hosts` ως εξής:

```
--- ::1                localhost localhost.my.domain
+++ ::1                localhost localhost.ntua.lab

--- 127.0.0.1          localhost localhost.my.domain
+++ 127.0.0.1          localhost localhost.ntua.lab

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

Ύστερα εκτελούμε `ping PC1` και επιβεβαιώνουμε ότι όντως απαντά το PC1.

2.4

Στο PC2 διαγράφουμε την εγγραφή του `/etc/hosts`:

```
192.168.2.5          PC1          PC1.ntua.lab
```

Ύστερα εκτελούμε `ping PC1`. Αυτή τη φορά λαμβάνουμε μήνυμα λάθους:

```
ping: cannot resolve PC1: Host name lookup failure
```

Επίλυση ονομάτων μέσω του εξυπηρετητή DNS

2.5

Ξεκινάμε τον NS1 και προσθέτουμε στο `/var/tmp/unbound.conf` τις γραμμές:

```
local-data: "PC1.ntua.lab. IN A 192.168.2.5"
local-data: "PC2.ntua.lab. IN A 192.168.2.6"
```

2.6

Στο NS1, στο `/var/tmp/unbound.conf`, προσθέτουμε τις γραμμές:

```
local-data-ptr: "192.168.2.5 PC1.ntua.lab."
local-data-ptr: "192.168.2.6 PC2.ntua.lab."
```

2.7

Στον NS1 εκτελούμε:

```
unbound-checkconf /var/tmp/unbound.conf      # No errors found.
cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf
service unbound restart
```

2.8

Στον NS1 εκτελούμε `tcpdump -vni em0`.

2.9

Στο PC1 εκτελούμε:

```
ifconfig em0 delete
dhclient em0
```

2.10

Σταματάμε την καταγραφή. Το PC1 έλαβε την 192.168.2.5.

2.11

Απέδωσε επιπλέον τις παραμέτρους "Domain-Name" και "Domain-Name-Server".

2.12

Στο PC1 εκτελούμε `cat /etc/resolv.conf`. Το αρχείο έχει δημιουργηθεί και έχει περιεχόμενο:

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

2.13

Στο PC1 εκτελούμε:

```
host 192.168.2.5
```

OR

```
drill -x 192.168.2.5
```

Στην 192.168.2.5 αντιστοιχεί το όνομα PC1.ntua.lab.

2.14

Στο PC1 εκτελούμε `host NS1` και έχουμε:

```
NS1.ntua.lab has address 192.168.2.1
```

2.15

Στο PC1 εκτελούμε `ping ns1`. Το ping είναι επιτυχές.

2.16

Στο PC2 εκτελούμε:

```
ifconfig em0 delete  
dhclient em0
```

2.17

Έλαβε τη διεύθυνση 192.168.2.6.

2.18

Στο PC2 εκτελούμε `ping PC1`. Το `ping` είναι επιτυχές.

2.19

Την έλαβε από τον εξυπηρετητή DNS, αφού προηγουμένως είχαμε διαγράψει την σχετική εγγραφή του `/etc/hosts` που αφορά το PC1 (ερώτημα 2.4). Μπορούμε να το επιβεβαιώσουμε και στην πράξη, κάνοντας καταγραφή στον NS1 στη διεπαφή `em0` πριν εκτελέσουμε το `ping`.

2.20

Στον PC1, αλλάζουμε τη διεύθυνση IP σε 192.168.2.7 στο αρχείο `/etc/hosts` και ύστερα εκτελούμε `ping PC2`. Το `ping` αποτυγχάνει με μήνυμα λάθους "Host is down".

2.21

Συμπεραίνουμε ότι πρώτα ελέγχεται το αρχείο `/etc/hosts`, και αν δεν υπάρχει σχετική εγγραφή καλείται ο εξυπηρετητής DNS.

2.22

Στο PC1 εκτελούμε `cat /etc/nsswitch.conf`. Είναι:

```
hosts: files dns
```

Δηλαδή πρώτα ελέγχεται το αρχείο `/etc/hosts` και ύστερα καλούνται οι εξυπηρετητές DNS. Η σειρά αυτή συμφωνεί με αυτή που είδαμε προηγουμένως.

2.23

Στο PC1 εκτελούμε `host PC2`. Η έξοδος της εντολής είναι:

```
PC2.ntua.lab has address 192.168.2.6
```

2.24

Σύμφωνα με την εντολή `man host`, το `host` είναι εργαλείο που εκτελεί DNS lookups, οπότε δεν ασχολείται καθόλου με το περιεχόμενο του αρχείου `/etc/hosts`.

2.25

Στο PC1 εκτελούμε:

```
rm /etc/resolv.conf  
resolvconf -u  
cat /etc/resolv.conf
```

Τώρα το περιεχόμενο του /etc/resolv.conf είναι:

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

Πρωτόκολλο DNS

2.26

Στο NS1 εκτελούμε `tcpdump -vni em0 "not port 67 and not port 68"`.

2.27

Στο PC1 εκτελούμε `host ntua.lab`.

2.28

Ναι, υπάρχει.

2.29

Χρησιμοποιήθηκε το UDP.

2.30

Οι θύρες προέλευσης και προορισμού είναι οι 53, 16104, 21507 και 45142.

2.31

Η θύρα 53.

2.32

Στο NS1 εκτελούμε `tcpdump -vni em0 "udp port 53"`.

2.33

Στο PC1 εκτελούμε `host NS1`.

2.34

Ανταλλάχθηκαν 6 μηνύματα.

2.35

Αντιστοιχούσαν σε ερωτήματα είδους A, AAAA και MX για το όνομα NS1.ntua.lab.

2.36

Δόθηκε απάντηση μόνο στο ερώτημα είδους A (δηλαδή για την διεύθυνση IPv4).

2.37

Στο PC1 εκτελούμε:

```
drill ns1  
drill ns1.ntua.lab
```

2.38

Έγιναν οι ερωτήσεις για τα ονόματα:

```
### drill ns1 ###  
---> name: ns1  
  
### drill ns1.ntua.lab ###  
---> name: ns1.ntua.lab
```

και λήφθηκαν οι απαντήσεις:

```
### drill ns1 ###  
---> <no answer>  
  
### drill ns1.ntua.lab ###  
---> ns1.ntua.lab. 3600 IN A 192.168.2.1
```

2.39

Συμπεραίνουμε ότι στην εντολή host δεν απαιτείται η χρήση του επιθέματος ntua.lab, ενώ στην εντολή drill χρειάζεται.

2.40

Στο PC1 εκτελούμε:

```
ping localhost  
ping pc1
```

Δεν παράγονται ερωτήσεις προς τον εξυπηρετητή DNS σε καμία περίπτωση.

2.41

Στο PC1 εκτελούμε `ping -c 1 ns1`.

2.42

Ανταλλάχθηκαν 2 μηνύματα DNS, που αφορούσαν το ερώτημα A? ns1.ntua.lab, δηλαδή είδους A (IPv4 διεύθυνση) για το όνομα ns1.ntua.lab.

2.43

Στο PC1 εκτελούμε:

```
ping -c 1 ns1  
ping -c 1 ns1  
ping -c 1 ns1
```

Παρατηρούμε να παράγονται 3 επιπλέον ερωτήματα προς τον εξυπηρετητή DNS, όσα και τα ping που εκτελέσαμε.

2.44

Συμπεραίνουμε ότι οι απαντήσεις του εξυπηρετητή DNS δεν αποθηκεύονται προσωρινά στο PC1.

Άσκηση 3: Εγκατάσταση εξυπηρετητή HTTP

Για την εγκατάσταση του εξυπηρετητή HTTP στον SRV κάνουμε τα εξής:

1.

Επιβεβαιώνουμε ότι η διεπαφή em1 είναι σε NAT.

2.

Εκτελούμε `dhclient em1`.

3.

Εκτελούμε `ping www.google.com`. Το ping είναι επιτυχές.

4.

Εκτελούμε `pkg install lighttpd`.

5.

Απενεργοποιούμε τις διεπαφές πλην της em0 και εκτελούμε `rm /etc/resolv.conf`.

3.1

Στον SRV εκτελούμε:

```
sysrc hostname="SRV"  
sysrc lighttpd_enable="YES"
```


3.2

Στον SRV εκτελούμε:

```
mkdir /usr/local/www/data
```

3.3

Στον SRV εκτελούμε:

```
echo "Hello World!" > /usr/local/www/data/index.html
```

3.4

Στον SRV εκτελούμε:

```
reboot  
rm /etc/resolv.conf
```

3.5

Μπορούμε να εκτελέσουμε `service lighttpd status`.

3.6

Μπορούμε να εκτελέσουμε την εντολή `netstat -an | grep 80` ή την `netstat -a | grep http`.
Αν υπάρχει εξυπηρετητής http θα εμφανιστεί έξοδος της μορφής:

tcp6	0	0	*.http	*.*	LISTEN
tcp4	0	0	*.http	*.*	LISTEN

3.7

Τοποθετούμε τη διεπαφή `em0` του SRV στο LAN1 και ύστερα εκτελούμε:

```
ifconfig em0 192.168.2.3/28
```

3.8

Στο `/var/tmp/unbound.conf` του NS1 προσθέτουμε τη γραμμή:

```
local-data: "SRV.ntua.lab. IN A 192.168.2.3"
```

3.9

Στο `/var/tmp/unbound.conf` του NS1 προσθέτουμε τη γραμμή:

```
local-data-ptr: "192.168.2.3 SRV.ntua.lab."
```

3.10

Στον NS1 εκτελούμε:

```
unbound-checkconf /var/tmp/unbound.conf # No errors found.  
cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf  
service unbound restart
```

3.11

Στον SRV εκτελούμε `tcpdump -ni em0`.

3.12

Στο PC1 εκτελούμε `fetch http://srv.ntua.lab`.

3.13

Χρησιμοποιήθηκε το TCP, ενώ ο εξυπηρετητής http ακούει στη θύρα 80.

3.14

Αποθηκεύτηκε στο `srv.ntua.lab`.

Άσκηση 4: Εγκατάσταση ιδιωτικού δρομολογητή και Firewall

4.1

Στον NS1 εκτελούμε `sysrc gateway_enable="YES"`.

4.2

Στον NS1 εκτελούμε `sysrc firewall_enable="YES"`.

4.3

Στον NS1 εκτελούμε `sysrc firewall_type="open"`.

4.4

Στον NS1 εκτελούμε `sysrc firewall_nat_enable="YES"`.

4.5

Στον NS1 εκτελούμε `sysrc ifconfig_em2="192.168.2.17/28"`.

4.6

Στον NS1 εκτελούμε:

```
cat /etc/rc.conf          # Everything OK.
```

4.7

Στο NS1 εκτελούμε `poweroff`, τοποθετούμε τη διεπαφή `em2` του NS1 στο DMZ και το επανεκκινούμε. Ύστερα εκτελούμε `netstat -rn` και βλέπουμε ότι η προκαθορισμένη πύλη είναι σωστά ρυθμισμένη.

4.8

Στο NS1 εκτελούμε `vi /etc/resolv.conf` και αλλάζουμε τα περιεχόμενα του αρχείου σε:

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

Επιβεβαιώνουμε ότι η επίλυση ονομάτων λειτουργεί.

4.9

Στο PC1 εκτελούμε:

```
sysrc ifconfig_em0="DHCP"
service netif restart
```

4.10

Στο PC2 εκτελούμε:

```
sysrc ifconfig_em0="192.168.2.4/28"
sysrc defaultrouter="192.168.2.1"
```

4.11

Στο PC2 εκτελούμε:

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

Αλλάζουμε το περιεχόμενο του `/etc/resolv.conf` σε:

```
nameserver 192.168.2.1
```

Τέλος επιβεβαιώνουμε ότι η επίλυση ονομάτων λειτουργεί με οποιαδήποτε από τις παρακάτω εντολές:

```
ping PC1
---> Successful

host PC1.ntua.lab
---> PC1.ntua.lab has address 192.168.2.5

host 192.168.2.5
---> 5.2.168.192.in-addr.arpa domain name pointer PC1.ntua.lab
```

4.12

Τοποθετούμε την διεπαφή em0 του SRV στο τοπικό δίκτυο DMZ και ύστερα στον SRV εκτελούμε:

```
sysrc ifconfig_em0="192.168.2.18/28"
sysrc defaultrouter="192.168.2.17"
service netif restart
service routing restart
```

4.13

Στον NS1 εκτελούμε `vi /var/tmp/unbound.conf` και διορθώνουμε τις γραμμές ("---" → παλιά γραμμή, "+++" → καινούργια γραμμή):

```
--- local-data: "PC2.ntua.lab. IN A 192.168.2.6"
+++ local-data: "PC2.ntua.lab. IN A 192.168.2.4"

--- local-data: "SRV.ntua.lab. IN A 192.168.2.3"
+++ local-data: "SRV.ntua.lab. IN A 192.168.2.18"

--- local-data-ptr: "192.168.2.6 PC2.ntua.lab."
+++ local-data-ptr: "192.168.2.4 PC2.ntua.lab."

--- local-data-ptr: "192.168.2.3 SRV.ntua.lab."
+++ local-data-ptr: "192.168.2.18 SRV.ntua.lab."
```

Ύστερα εκτελούμε:

```
unbound-checkconf /var/tmp/unbound.conf      # No errors found.
cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf
service unbound restart
```

4.14

Στον SRV εκτελούμε:

```
ping 192.168.2.5    # PC1
ping 192.168.2.4    # PC2
ping 192.168.2.1    # NS1
```

Ναι, μπορούμε να κάνουμε ping στα μηχανήματα του LAN1 χρησιμοποιώντας την IP διεύθυνσή τους.

4.15

Στο NS1 εκτελούμε:

```
ipfw add 2000 deny all from any to 192.168.2.0/28 in via em2
```

4.16

Στον SRV εκτελούμε `ping 192.168.2.5`. Δεν λαμβάνουμε απάντηση.

4.17

Στον NS1 εκτελούμε (όλο μαζί μία εντολή):

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

4.18

Στο PC1 εκτελούμε `ping SRV`. Το ping είναι επιτυχές.

4.19

Στο NS1 εκτελούμε `ping 147.102.1.1`. Το ping είναι επιτυχές.

4.20

Στο PC1 εκτελούμε `ping 147.102.1.1`. Δεν λαμβάνουμε απάντηση.

4.21

Στον NS1 εκτελούμε:

```
ipfw nat 111 config unreg_only if em1 reset
```

4.22

Στον NS1 εκτελούμε:

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

4.23

Στο PC1 εκτελούμε `ping 147.102.1.1`. Το ping είναι επιτυχές.

4.24

Στο PC1 εκτελούμε `host 147.102.1.1`. Το όνομα του μηχανήματος με αυτή τη διεύθυνση IP είναι `theseas.softlab.ece.ntua.gr`.

4.25

Στον NS1 εκτελούμε `tcpdump -ni em1`.

4.26

Στο PC1 εκτελούμε `ping -c 2 www.ntua.gr`. Τα πακέτα που παράγει το PC1 εμφανίζονται με διεύθυνση πηγής 10.0.3.15.

4.27

Είναι η 147.102.224.101.

4.28

Έγινε προς τον 9.9.9.9 (dns9.quad9.net).

4.29

Στον NS1 εκτελούμε `tcpdump -ni em1 "udp port 53"`.

4.30

Στο PC2 εκτελούμε:

```
#1: ping -c 1 www.google.com
#2: ping -c 1 www.cnn.com
#3: ping -c 1 www.yahoo.com
#4: ping -c 1 www.mit.edu
```

Κάθε φορά καλείται ένας εξυπηρετητής από αυτούς που έχουμε ορίσει, δηλαδή 1.1.1.1, 8.8.8.8 και 9.9.9.9.

4.31

Σε νέο παράθυρο στον NS1 εκτελούμε `tcpdump -ni em0 "udp port 53"`.

4.32

Στο PC1 εκτελούμε `ping -c 1 courses.cn.ntua.gr`. Το canonical name του `courses.cn.ntua.gr` είναι `courses.cn.ece.ntua.gr`.

4.33

Το PC1 έκανε ερώτημα "A":

A? `courses.cn.ntua.gr`.

και έλαβε απάντηση "CNAME", "A" από τον NS1:

```
CNAME courses.cn.ece.ntua.gr, A 147.102.40.10
```

Επίσης, ο NS1 έκανε ερωτήματα είδους "A" στους εξωτερικούς εξυπηρετητές DNS:

```
#1 A? courses.cn.ntua.gr.  
#2 A? courses.cn.ece.ntua.gr
```

και έλαβε απαντήσεις είδους "CNAME", "A" και "A" αντίστοιχα:

```
#1 CNAME courses.cn.ece.ntua.gr, A 147.102.40.10  
#2 A 147.102.40.10
```

4.34

Στον NS1 εκτελούμε `tcpdump -vvvni em1 "udp port 53"`.

4.35

Στο PC1 εκτελούμε:

```
drill www.cn.ece.ntua.gr  
drill www.cn.ece.ntua.gr
```

Παρατηρήσαμε μόνο ένα ερώτημα DNS:

```
A? www.cn.ece.ntua.gr
```

Οι απαντήσεις DNS ισχύουν για 20 λεπτά.

4.36

Στον NS1 εκτελούμε `tcpdump -vvvni em0 "udp port 53"`. Ύστερα στο PC1 εκτελούμε:

```
drill www.cn.ece.ntua.gr  
drill www.cn.ece.ntua.gr
```

Παράγονται μηνύματα DNS κάθε φορά που εκτελούμε την εντολή `drill`. Παρατηρούμε ότι η χρονική διάρκεια ισχύος των απαντήσεων DNS μειώνεται συνεχώς.

4.37

Συμπεραίνουμε ότι οι απαντήσεις που λαμβάνει ο τοπικός εξυπηρετητής DNS στο NS1 αποθηκεύονται προσωρινά.

4.38

Στον SRV εκτελούμε `ping 147.102.224.101`. Το `ping` είναι επιτυχές.

4.39

Στον SRV εκτελούμε `ping www.ntua.gr`. Το ping αποτυγχάνει με μήνυμα λάθους:

```
ping: cannot resolve www.ntua.gr: Host name lookup failure
```

Αυτό συμβαίνει διότι:

- Δεν υπάρχει εγγραφή σχετική με τον `www.ntua.gr` στο αρχείο `/etc/hosts`.
- Δεν έχει οριστεί εξυπηρετητής DNS, αφού δεν υπάρχει το αρχείο `/etc/resolv.conf`.

4.40

Στον SRV εκτελούμε:

```
echo "nameserver 192.168.2.17" > /etc/resolv.conf
```

4.41

Στον SRV εκτελούμε `ping www.ntua.gr`. Το ping είναι επιτυχές.

4.42

Στο PC1 εκτελούμε `host www.ntua.lab` και παίρνουμε την απάντηση:

```
www.ntua.lab is an alias for ntua.lab
```

Για να πάρουμε τη διεύθυνση IP πρέπει να ξαναεκτελέσουμε την `host`, αλλά αυτή τη φορά να βάλουμε σαν όρισμα την έξοδο του προηγούμενου `host`, δηλαδή:

```
host $(cat ntua.lab)
```

Οπότε παίρνουμε ως απάντηση τη διεύθυνση `192.168.2.1`.

Στο PC1 εκτελούμε `ping www.ntua.lab`. Το ping αποτυγχάνει με μήνυμα λάθους:

```
ping: cannot resolve www.ntua.lab: Unknown server error
```

4.43

Στον NS1 εκτελούμε `vi /usr/local/etc/unbound/unbound.conf` και προσθέτουμε πριν από την εγγραφή `CNAME` τη γραμμή:

```
local-data: "www.ntua.lab. IN A 192.168.2.18"
```

Ύστερα εκτελούμε `service unbound restart`.

4.44

Στο PC1 εκτελούμε `ping www.ntua.lab`. Απαντά το SRV (192.168.2.18).

Άσκηση 5: Εγκατάσταση δημόσιου δρομολογητή και DNS

Πριν ξεκινήσουμε, τοποθετούμε τις διεπαφές του NS2 ως εξής:

```
em0: LAN2  
em1: NAT  
em2: WAN
```

5.1

Στον NS2 εκτελούμε `sysrc hostname="ns2.ntua.lab"`.

5.2

Στον NS2 εκτελούμε:

```
sysrc ifconfig_em0="192.0.2.1/29"  
sysrc ifconfig_em2="192.0.2.9/29"
```

5.3

Στον NS2 εκτελούμε `sysrc ifconfig_em1="DHCP"`.

5.4

Στον NS2 εκτελούμε `sysrc gateway_enable="YES"`.

5.5

Στον NS2 εκτελούμε `sysrc firewall_enable="YES"`.

5.6

Στον NS2 εκτελούμε `sysrc firewall_type="open"`.

5.7

Στον NS2 εκτελούμε `sysrc firewall_nat_enable="YES"`.

5.8

Στον NS2 εκτελούμε:

```
sysrc -a      # To see DHCP server related settings  
  
# DHCP server related:  
# dhcp_ifaces  
# dhcpd_enable  
  
sysrc -x dhcp_ifaces  
sysrc -x dhcpd_enable
```

5.9

Στον NS2 εκτελούμε `sysrc -a`. Επιβεβαιώνουμε ότι υπάρχει (`unbound_enable: YES`).

5.10

Στον NS2 εκτελούμε `vi /var/tmp/unbound.conf` και αλλάζουμε τις γραμμές ("`---`" → γραμμή που διαγράφηκε, "`+++`" → γραμμή που προστέθηκε):

```
### NTUA.LAB RELATED LINES ###

--- private-domain: "ntua.lab"
--- local-zone: "ntua.lab." static
--- local-data: "ntua.lab. 360 IN SOA ns1.ntua.lab. admin.ntua.lab.
                20200501 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-data-ptr: "192.168.2.1 ns1.ntua.lab."

### ACCESS-CONTROL ###

--- access-control: 192.168.2.0/24 allow

### NEW LINES ###

+++ access-control: 192.0.2.0/24 allow
+++ local-zone: "ntua.lab." redirect
+++ local-data: "ntua.lab. IN A 192.0.2.10"
```

Ύστερα εκτελούμε:

```
unbound-checkconf /var/tmp/unbound.conf    # No errors found.
cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf
```

5.11

Στον NS2 εκτελούμε:

```
reboot
netstat -rn    # default gateway exists, OK.
```

5.12

Στον NS2 εκτελούμε:

```
ipfw nat 222 config if em1 reset same_ports
```

5.13

Στον NS2 εκτελούμε:

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

5.14

Στο PC2 εκτελούμε:

```
sysrc ifconfig_em0="192.0.2.2/29"  
sysrc defaultrouter="192.0.2.1"
```

5.15

Συνδέουμε το PC2 στο LAN2 και εκτελούμε:

```
service netif restart  
service routing restart  
echo "nameserver 192.0.2.1" > /etc/resolv.conf  
host google.com           # Name resolution OK.
```

5.16

Στο PC2 εκτελούμε `www.ntua.gr`. Το ping είναι επιτυχές.

5.17

Στον NS1 εκτελούμε:

```
sysrc ifconfig_em1="192.0.2.10/29"  
sysrc defaultrouter="192.0.2.9"
```

5.18

Μετακινούμε την em1 του NS1 στο WAN και ύστερα εκτελούμε:

```
service netif restart  
service routing restart
```

5.19

Εκτελούμε:

```
### NS1 ###  
ipfw zero
```

```
### PC1 ###  
ping www.ntua.gr
```

```
### NS1 ###
ipfw show          # NAT 111 rule used
ipfw zero
```

```
### SRV ###
ping www.ntua.gr
```

```
### NS1 ###
ipfw show          # NAT 111 rule used
```

Και τα δύο ping είναι επιτυχή, ενώ παραμένει η λειτουργία του πίνακα nat 111.

5.20

Εκτελούμε:

```
### PC1 ###
host www.ntua.lab
```

```
### PC2 ###
host www.ntua.lab
```

Στο PC1 δίνει διεύθυνση 192.168.2.18, ενώ στο PC2 192.0.2.10.

5.21

Στο PC2 εκτελούμε `fetch http://www.ntua.lab`. Η εντολή αποτυγχάνει με μήνυμα λάθους "Connection refused".

5.22

Στον NS1 εκτελούμε:

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

5.23

Στο PC2 εκτελούμε `fetch http://www.ntua.lab`. Πλέον μπορούμε να κατεβάσουμε κανονικά την ιστοσελίδα.

5.24

Στο PC2 εκτελούμε `ping www.ntua.lab`. Απαντά το NS1 (192.0.2.10).

5.25

Στο PC1 εκτελούμε `ssh lab@www.ntua.lab`. Συνδεόμαστε στο SRV, όπως φαίνεται και από το prompt.

5.26

Στο PC2 εκτελούμε `ssh lab@www.ntua.lab`. Συνδεόμαστε στο μηχάνημα NS1 (όπως φαίνεται από το prompt), αφού στο PC2 το όνομα `www.ntua.lab` αντιστοιχεί στη διεύθυνση `192.0.2.10`, όπως μπορούμε να επιβεβαιώσουμε και με την εντολή `host www.ntua.lab`.

5.27

Στο NS1 εκτελούμε (όλο μαζί μία εντολή):

```
ipfw nat 111 config unreg_only if em1 reset \  
redirect_port tcp 192.168.2.18:80 80          \  
redirect_port tcp 192.168.2.18:22 22
```

5.28

Στο PC2 εκτελούμε `ssh lab@www.ntua.lab`. Συνδεόμαστε στον SRV, όπως μπορούμε να επιβεβαιώσουμε από το prompt, την εντολή `hostname`, ή -αν θέλουμε να είμαστε απολύτως σίγουροι- διασταυρώνοντας τις διευθύνσεις MAC στην έξοδο της `ifconfig`.