Εργαστήριο Δικτύων Υπολογιστών
Εργαστηριακή Άσκηση 12

Δημήτριος Κόγιος
03119220

Όνομα PC: lekog-HP-Laptop-15s-fq1xxx

Άσκηση 1:

1.1) tcpdump -i em0 -vv -e -n

1.2) dhclient em0

1.3) PC1 -> NS1 : DHCP Discover
NS1 -> 192.168.2.5 : ARP request (μάλλον έλεγχος)
NS1 -> PC1 : DHCP Offer
PC1 -> NS1 : DHCP Request
NS1 -> PC1 : DHCP ACK
PC1 -> PC1 : ARP request (probe)
NS1 -> PC1 : ICMP echo request
PC1 -> NS1 : ARP request
NS1 -> PC1 : ARP reply
PC1 -> NS1 : ICMP echo reply

1.4) DHCP discover
DHCP offer
DHCP request
DHCP ACK

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

1.6) Renewal in 60 seconds
1.7) Χρησιμοποιούν UDP.

1.8) Θύρα PC1 : 68 , Θύρα NS1 : 67

1.9) 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) PC1 : 08:00:27:c3:5c:c3
NS1 : 08:00:27:8f:54:a8

DHCP discover : PC1 > ff:ff:ff:ff:ff:ff
DHCP offer : NS1 > PC1
DHCP request : PC1 > ff:ff:ff:ff:ff:ff
DHCP ACK : NS1 > PC1

1.11) Λόγω της επικεφαλίδας Ethernet αφού ο DHCP εξυπηρετητής και το PC1 βρίσκονται στο ίδιο LAN.

1.12) Ναι ο NS1 στέλνει ARP για τη διεύθυνση που πρόκειται να αποδόσει στο PC1 ώστε να δει αν αυτή χρησιμοποιείται από κάποιον άλλον.

1.13) Δεν είδα ICMP πριν το DHCP offer αλλά πιο μετά.

1.14) Είναι ARP probe.

1.15) Ναι παρατηρήσαμε ICMP μηνύματα μετά την απόδοση διεύθυνσης τα οποία παράγονται για να επιβεβαίωσουν τη συνδεσιμότητα του dhcp server και client.

1.16) Lease-Time : 120

1.17) Περιέχει Server-ID και Requested-IP.

1.18) Το πρώτο έχει διεύθυνση MAC προορισμού ff:ff:ff:ff:ff:ff ενώ το δεύτερο έχει ως MAC προορισμού τη MAC του NS1. Επίσης, το πρώτο έχει ως IP πηγής 0.0.0.0 και ως IP προορισμού 255.255.255.255 ενώ το δεύτερο έχει ως IP πηγής την 192.168.2.5 και ως IP προορισμού την 192.168.2.1. Το δεύτερο έχει Client-IP 192.168.2.5. Το πρώτο έχει Server-ID και Requested-IP ενώ το δεύτερο όχι.

1.19) Γιατί ανανεώθηκε η IP διεύθυνση και έτσι ο πελάτης κλείνει την port 68 στην οποία ακούει ο DHCP client.

1.20) Ζήτησε 10 παραμέτρους.

```
Subnet-Mask, BR, Time-Zone, Classless-Static-Route
Default-Gateway, Domain-Name, Domain-Name-Server, Hostname
Option 119, MTU
```

1.21) Subnet-Mask , BR , Default-Gateway .

1.22) /var/db/dhcpd/dhcpd.leases

1.23) Κάθε 60 sec.

1.24) IP που αποδόθηκε , ώρα starts , ώρα ends , ώρα cltt , binding state , next binding state , rewind binding state , MAC διεύθυνση του πελάτη , uid , client-hostname .

1.25) /var/db/dhclient.leases.em0

1.26) interface , fixed-address , subnet-mask , routers , broadcast-address , dhcp-lease-time , dhcp-message-type , dhcp-server-identifier , renew , rebind , expire.

1.27) 45 sec.

1.28) tcpdump -i em0 -n

1.29) service isc-dhcpd stop

1.30) Μετά από περίπου δύο λεπτά σβήνεται η διεύθυνση.
service isc-dhcpd start

1.31) Αποδόθηκε.

1.32) Στέλνει Request στα 15 , 15 , 22 , 36 , 16 , 23 , 30 , 47.

1.33) UDP port 67 unreachable δηλαδή ο εξυπηρετητής DHCP δεν ακούει το PC1 αφού όπως είπαμε στο ερώτημα 1.8 , ο εξυπηρετητής ακούει στο port 67.

1.34) Είναι 255.255.255.255 δηλαδή παύει να ρωτάει τον NS1 και ρωτάει όλους τους εξυπηρετητές DHCP στο δίκτυο.

1.35) Από θεωρία :
Ημερομηνία επανασύνδεσης είναι η χρονική στιγμή όπου ο πελάτης DHCP πρέπει θα ξεκινήσει τη διαδικασία δανεισμού μια νέας διεύθυνσης από οποιονδήποτε άλλο εξυπηρετητή (εάν δεν κατορθώσει την ανανέωση).

1.36) Είναι ff:ff:ff:ff:ff:ff και 255.255.255.255 ενώ το πεδίο από το οποίο γίνεται κατανοητό ότι έχει απολεσθεί η διεύθυνση είναι το requested-IP.

1.37) Για να ελεγχθεί ότι η 192.168.2.5 (requested-IP) δεν χρησιμοποιείται από κάποιον άλλον.

1.38) Διαγράφονται και δημιουργούνται καινούργια.

1.39) Γιατί ο server μπορεί να κάνει broadcast το offer και τότε , άμα δεν χρησιμοποιούταν πασίγνωστη θύρα αλλά μια τυχαία πόρτα XXXXX, οι υπόλοιποι hosts του δικτύου που ενδεχομένως να άκουγαν στη δικιά τους XXXXX πόρτα να λάμβαναν αυτό το offer αντί για πακέτα τις δικιάς τους UDP συνδέσεως γεγονός που θα μπορούσε να προκαλέσει πρόβλημα.

https://stackoverflow.com/questions/1790960/why-dhcp-client-listens-on-port-68

Άσκηση 2:

2.1) vi /etc/hosts
Προσθέτουμε :
192.168.2.5 PC1 PC1.ntua.lab
192.168.2.6 PC2 PC2.ntua.lab
και αλλάζουμε τα my.domain σε ntua.lab

2.2) Και στις τρεις περιπτώσεις απαντά το 102.168.2.6 δηλαδή το PC2 ενώ δεν έχει σημασία η χρήση μικρών ή κεφαλαίων γραμμάτων.

2.3) vi /etc/hosts
Προσθέτουμε :
192.168.2.5 PC1 PC1.ntua.lab
192.168.2.6 PC2 PC2.ntua.lab
και αλλάζουμε τα my.domain σε ntua.lab

Απαντάει το PC1 σε ping PC1.

2.4) ping: cannot resolve PC1: Host name lookup failure

2.5) vi /var/tmp/unbound.conf
Προσθέτουμε:
local-data:"PC1.ntua.lab. IN A 192.168.2.5"
local-data:"PC2.ntua.lab. IN A 192.168.2.6"

2.6) Προσθέτουμε:
local-data-ptr:" 192.168.2.5 PC1.ntua.lab."
local-data-ptr:"192.168.2.6 PC2.ntua.lab."

2.7) service unbound restart

2.8) tcpdump -i em0 -v -n

2.9) ifconfig em0 delete
dhclient em0

2.10) Έλαβε την 192.168.2.5.

2.11) Subnet-Mask , BR , Domain-Name , Domain-Name-Server

2.12) Ναι έχει δημιουργηθεί:
search ntua.lab
nameserver 192.168.2.1

2.13) host 192.168.2.5
PC1.ntua.lab

2.14) host NS1
NS1.ntua.lab has address 192.168.2.1

2.15) Ναι μπορούμε.

2.16) ifconfig em0 delete
dhclient em0

2.17) Έλαβε την 192.168.2.6 .

2.18) Ναι με ping PC1.

2.19) Από τον εξυπηρετητή DNS αφού ούτως ή άλλως είχαμε σβήσει την εγγραφή για το PC1 στο αρχείο /etc/hosts του PC2.

2.20) Όχι -> Host is down

2.21) Συμπεραίνουμε ότι πρώτα ελέγχεται το αρχείο /etc/hosts και αν δεν υπάρχει κάποια εγγραφή συμβουλευόμαστε τον DNS server.

2.22) Ναι -> hosts : files dns

2.23) host PC2
PC2.ntua.lab has address 192.168.2.6

2.24) Γιατί με την εντολή host γίνεται κλήση στον DNS που έχει τη σωστή εγγραφή.

2.25) rm /etc/resolv.conf
resolvconf -u
Τώρα το αρχείο είναι:
search ntua.lab
nameserver 192.168.2.1
Δηλαδή ίδιο με πριν.

2.26) tcpdump -i em0 -n -v '(not port 67 and not port 68)'

2.27) host ntua.lab

2.28) Ναι

2.29) UDP.

2.30) 53 και 43176, 57961, 48355

2.31) Η 53.

2.32) tcpdump -i em0 -n -v port 53

2.33) host NS1

2.34) 6 μηνύματα.

2.35) A? NS1.ntua.lab.
AAAA? NS1.ntua.lab.
MX? NS1.ntua.lab.

2.36) Μόνο στην πρώτη.

2.37) drill ns1
drill ns1.ntua.lab

2.38) Για τα ονόματα ns1. και ns1.ntua.lab.
Για το πρώτο δεν λήφθηκε απάντηση ενώ για το δεύτερο:
ns1.ntua.lab. 3600 IN A 192.168.2.1

2.39) Για την εντολή host μπορούμε να το παραλείψουμε αλλά όχι και για την drill.

2.40) Όχι δεν παράγονται ερωτήσεις για τον DNS αφού localhost είναι εσωτερική διεύθυνση και για το PC1 υπάρχει εγγραφή στο αρχείο /etc/hosts

2.41) ping -c 1 ns1

2.42) Ανταλλάχθηκαν 2 μηνύματα DNS και το ερώτημα ήταν A? ns1.ntua.lab. δηλαδή το PC1 ρώτησε τον DNS εξυπηρετητή αν γνωρίζει την IPv4 διεύθυνση του ns1.ntua.lab.

2.43) Για κάθε ping -c 1 ns1 που κάνουμε παράγεται και ένα νέο ερώτημα προς τον εξυπηρετητή DNS που τον ρωτάει για τη διεύθυνση του ns1.ntua.lab.

2.44) Δεν αποθηκεύονται αφού σε κάθε ping γίνεται ερώτηση. Ωστόσο εάν κάνουμε ping ns1 και το αφήνουμε να τρέξει, δεν ρωτάμε τον DNS για κάθε ICMP echo request που στέλνουμε αλλά μόνο για το πρώτο.

Άσκηση 3:

3.1) sysrc lighttpd_enable="YES"

3.2) mkdir /usr/local/www/data

3.3) touch /usr/local/www/data/index.html
echo "Hello World" > /usr/local/www/data/index.html

3.4) reboot
rm /etc/resolv.conf

3.5) service lighttpd status

3.6) netstat -a | grep http

3.7) ifconfig em0 192.168.2.3/28

3.8) vi /var/tmp/unbound.conf
Προσθέτουμε:
local-data:”SRV.ntua.lab. IN A 192.168.2.3”

3.9) Προσθέτουμε:
local-data-ptr:”192.168.2.3 SRV.ntua.lab.”

3.10) unbound-checkconf
cp /var/tmp/unbound.conf
/usr/local/etc/unbound/unbound.conf
service unbound restart

3.11) tcpdump -i em0 -n -v

3.12) fetch http://srv.ntua.lab

3.13) Χρησιμοποιείται TCP και ο εξυπηρετητής http ακούει στη θύρα 80.

3.14) Στο αρχείο /root/srv.ntua.lab

Άσκηση 4:

4.1) sysrc gateway_enable="YES"

4.2) sysrc firewall_enable="YES"

4.3) sysrc firewall_type="open"

4.4) sysrc firewall_nat_enable="YES"

4.5) sysrc ifconfig_em2="192.168.2.17/28"

4.6) cat /etc/rc.conf

4.7) netstat -rn

4.8) Αλλάζουμε τα περιεχόμενα του /etc/resolv.conf σε :

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

4.9) sysrc ifconfig_em0="DHCP"
service netif restart

4.10) sysrc ifconfig_em0="192.168.2.4/28"
sysrc defaultrouter="192.168.2.1"

4.11) service netif restart
service routing restart

Φτιάχνουμε αρχείο /etc/resolv.conf και γράφουμε μέσα:

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

4.12) sysrc ifconfig_em0=”192.168.2.18/28”
sysrc defaultrouter=”192.168.2.17”
service netif restart
service routing restart

4.13) 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 SRV.ntua.lab.”

unbound-checkconf -> no errors
cp /var/tmp/unbound.conf
/usr/local/etc/unbound/unbound.conf
service unbound restart

4.14) Ναι με ping 192.168.2.5 και ping 192.168.2.4 .

4.15) ipfw add 2000 deny all from any to 192.168.2.0/28 recv em2

4.16) Όχι πλέον δεν μπορούμε.

4.17) ipfw add 1900 allow all from 192.168.2.0/28 to
192.168.2.17/28 recv em0 keep-state

4.18) Ναι μέσω ping 192.168.2.18 .

4.19) Ναι μπορούμε.

4.20) Όχι δεν μπορούμε.

4.21) ipfw nat 111 config unreg_only if em1 reset

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

4.23) Ναι πλέον είναι επιτυχές.

4.24) host 147.102.1.1
theseas.softlab.ece.ntua.gr.

4.25) tcpdump -i em1 -n -v

4.26) Με τη διεύθυνση 10.0.3.15

4.27) Είναι 147.102.224.101 .

4.28) Έγινε στον 8.8.8.8.

4.29) tcpdump -i em1 -n -v '(port 53)'

4.30) www.google.com : έγινε ερώτηση στον 8.8.8.8
www.cnn.com : έγινε ερώτηση στον 1.1.1.1
www.yahoo.com : έγινε ερώτηση στον 1.1.1.1
www.mit.edu : έγινε ερώτηση στον 9.9.9.9

4.31) tcpdump -i em0 -n -v '(port 53)'

4.32) CNAME courses.cn.ece.ntua.gr.

4.33) Ο PC1 έκανε ερώτημα A? courses.cn.ntua.gr. και το NS1 του απάντησε με τη διεύθυνση του courses.cn.ntua.gr. (147.102.40.10) και το canonical name.
Το NS1 έκανε δύο ερωτήματα A? courses.cn.ntua.gr. στον DNS

server 9.9.9.9 και για τα δύο έλαβε απάντηση CNAME και A. Μετά ξαναέκανε ερώτηση A? courses.cn.ece.ntua.gr. (δηλαδή χρησιμοποίησε το canonical name) και έλαβε απάντηση A.

4.34) tcpdump -i em1 -n -vvv '(port 53)'

4.35) Παρατηρώ μόνο μία ερώτηση DNS. Η χρονική διάρκεια ισχύος των απαντήσεων DNS είναι 20mins.

4.36) tcpdump -i em0 -n -vvv '(port 53)'
Ναι παράγονται ερωτήματα και για τα δύο drill πράγμα που σημαίνει ότι ο PC1 δεν αποθηκεύει τις απαντήσεις DNS.

4.37) Αποθηκεύονται για 20 mins όπως είπαμε στο 4.35 .

4.38) ping 147.102.224.101
Ναι μπορούμε.

4.39) Όχι δεν μπορούμε γιατί δεν υπάρχει εγγραφή στο αρχείο /etc/hosts για το www.ntua.gr αλλά ούτε και έχουμε ορίσει DNS server αφού δεν υπάρχει αρχείο /etc/resolv.conf .

4.40) vi /etc/resolv.conf
nameserver 192.168.2.17

4.41) Ναι πλέον μπορούμε.

4.42) host www.ntua.lab
www.ntua.lab is an alias for ntua.lab.
host ntua.lab
ntua.lab has address 192.168.2.1
ping www.ntua.lab

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

4.43) vi /var/tmp/unbound.conf
local-data:"www.ntua.lab. IN A 192.168.2.18"
cp /var/tmp/unbound.conf
/usr/local/etv/unbound/unbound.conf
service unbound restart

4.44) Απαντά το 192.168.2.18 δηλαδή το SRV.

Άσκηση 5:

5.1) sysrc hostname="ns2ntua.lab"

5.2) sysrc ifconfig_em0="192.0.2.1/29"
sysrc ifconfig_em2="192.0.2.9/29"

5.3) sysrc ifconfig_em1="DHCP"

5.4) sysrc gateway_enable="YES"

5.5) sysrc firewall_enable="YES"

5.6) sysrc firewall_type="open"

5.7) sysrc firewall_nat_enable="YES"

5.8) sysrc -x dhcpd_enable
sysrc -x dhcp_ifaces

5.9) Μέσω sysrc -a βλέπουμε ότι υπάρχει η γραμμή unbound_enable: YES .

5.10) vi /var/tmp/unbound.conf
Κάνουμε τις απαραίτητες αλλαγές.
unbound-checkconf /var/tmp/unbound.conf
cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf

5.11) reboot
netstat -r

5.12) ifpw nat 222 config if em1 reset same_ports

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

5.14) sysrc ifconfig_em0=”192.0.2.2/29”
sysrc defaultrouter=”192.0.2.1”

5.15) service netif restart
service routing restart
vi /etc/resolv.conf
nameserver 192.0.2.1

5.16) Ναι μπορούμε.

5.17) sysrc ifconfig_em1=”192.0.2.10/29”
sysrc defaultrouter=”192.0.2.9”

5.18) service netif restart
service routing restart

5.19) Ναι και τα δύο ping επιτυγχάνουν συνεπώς παραμένει η λειτουργία του nat 111.

5.20) Στο PC1 : 192.168.2.18
Στο PC2 : 192.0.2.10

5.21) fetch http://www.ntua.lab
fetch: http://www.ntua.lab: Connection refused

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

5.23) Ναι πλέον μπορούμε.

5.24) Απαντά το 192.0.2.10.

5.25) Συνδεόμαστε στο SRV αφού στο PC1 το όνομα www.ntua.lab είναι η διεύθυνση 192.168.2.18 όπως είπαμε στο ερώτημα 5.20 .

5.26) Συνδεόμαστε στο NS1 αφού όπως είπαμε στο 5.20 , στο PC2 το όνομα www.ntua.lab είναι η διεύθυνση 192.0.2.10 και η μετάφραση στον nat 111 είναι για εισερχόμενη κίνηση στην πόρτα 80 ενώ το ssh χρησιμοποιεί την πόρτα 22.

5.27) 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) Πλέον με ssh lab@www.ntua.lab από το PC2 συνδεόμαστε στο SRV , το καταλαβαίνουμε κάνοντας είτε ifconfig ή netstat από το SRV και βλέπουμε την ενεργή σύνδεση στην πόρτα 22 .