

Όνοματεπώνυμο : Ιωάννης Μπασδέκης

Ομάδα: 3

Όνομα PC: DESKTOP-0BU537U

Ημερομηνία: 4/6/2023

Μέρος 1ο

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

1.2) dhclient em0

1.3) a) PC1 -> broadcast (DHCP Discover)

b) NS1 -> PC1 (DHCP Offer)

c) PC1 -> broadcast (DHCP Request)

d) NS1 -> PC1 (DHCP ACK)

1.4) DHCPDISCOVER

DHCPOFFER

DHCPREQUEST

DHCPACK

1.5) Αποδόθηκε η 192.168.2.5

Ο εξυπηρετητής έχει την διεύθυνση 192.168.2.1

1.6) 60 sec

1.7) UDP

1.8) 67, 68

1.9) a) 0.0.0.0 -> 255.255.255.255

b) 192.168.2.1 -> 192.168.2.5

c) 0.0.0.0 -> 255.255.255.255

d) 192.168.2.1 -> 192.168.2.5

- 1.10) a) 08:00:27:2b:63:48 -> ff:ff:ff:ff:ff:ff
- b) 08:00:27:70:bb:02 -> 08:00:27:2b:63:48
- c) 08:00:27:2b:63:48 -> ff:ff:ff:ff:ff:ff
- d) 08:00:27:70:bb:02 -> 08:00:27:2b:63:48

1.11) Έχει την διεύθυνση 0.0.0.0 που χρησιμεύει σαν placeholder (μέχρι να πάρει κανονική IPv4

1.12) Ναι, τα παράγει ο NS1 για να μάθει αν υπάρχει στο δίκτυο η διεύθυνση που θέλει να δώσει στον PC1

1.13) Δεν παρατήρησα

1.14) Για να ελέγξει αν η IP που έδωσε, κατά την διάρκεια της απόδοσης, δόθηκε και σε άλλο μηχάνημα

1.15) Ναι, τα παράγει ο NS1 για να ελέγξει αν ισχύει ακόμα η IP

1.16) 120 Sec

1.17) Έχει την IP του server που θα λάβει την διεύθυνση και το πεδίο Requested-IP περιέχει την διεύθυνση που επρόκειτο να πάρει

1.18) Στο πρώτο Request η source IP είναι 0.0.0.0 και η διεύθυνση MAC/IP του παραλήπτη είναι ff:ff:ff:ff:ff:ff / 255.255.255.255 αντίστοιχα ενώ στο δεύτερο οι διευθύνσεις αποστολέα(MAC, IPv4) είναι του PC1 και του παραλήπτη είναι του PC2. Επίσης στο πρώτο request υπάρχουν τα Options Requested-IP και Server-IP ενώ στο 2ο όχι

1.19) Μάλλον για να δείξει ότι χρησιμοποιεί την συγκεκριμένη IP

1.20) 10

1.21) Subnet-Mask
BR
Default-Gateway

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

1.23) 60 Sec

1.24) Την IP που έχει δοθεί

Ημερομηνία και ώρα έναρξης/λήξης (starts/ends)

Την ώρα της τελευταίας συναλλαγής του πελάτη (cltt)

Την κατάσταση του δανείου

Την κατάσταση του δανείου αφού η τωρινή κατάσταση λήξει

Την MAC του πελάτη

Το uid του πελάτη

Το hostname του πελάτη

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

1.26) Διεπαφή

IPv4

subnet-mask

Default router IPv4

broadcast-address

dhcp-lease-time

dhcp-message-type

dhcp Server IPv4

ώρα έναρξης ανανέωσης

ώρα ανανέωσης

ώρα λήξης

1.27) 45 sec

1.28) tcpdump -n -i em0

1.29) service isc-dhcpd stop

1.30) service isc-dhcpd start

1.31) -

1.32) 11 request πριν χάσει την IP που απέχουν περίπου 10 sec

1.33) Όσο έχει IP λαμβάνει ICMP udp port 67 unreachable

1.34) 255.255.255.255 (broadcast)

1.35) Θεωρεί ότι χάθηκε ο συγκεκριμένος server οπότε προσπαθεί να βρει νέο server

1.36) Destination MAC = ff:ff:ff:ff:ff:ff

Destination IP = 255.255.255.255

Τα προηγούμενα Request είχαν την διεύθυνση του NS1 όχι broadcast

1.37) Γιατί υπάρχει αυτή η διεύθυνση στα δάνεια του NS1 και θέλει να ελέγξει αν έχει αποδοθεί αλλου στο δίκτυο

1.38) Διαγράφονται

1.39) Από την στιγμή που πρόκειται για απόδοση IP που είναι πολύ βασικό στοιχείο σε ένα δίκτυο πρέπει τόσο ο πελάτης όσο και ο server να ενημερώνονται για αλλαγές άμεσα οπότε πρέπει να ξέρει ο καθένας από που να περιμένει μήνυμα DHCP και χωρίς να χρειάζεται κάποια σύνδεση

Μέρος 2ο

2.1) 192.168.2.5 PC1.ntua.lab PC1
192.168.2.6 PC2.ntua.lab PC2

2.2) Δεν έχει σημασία. Σε όλες τις περιπτώσεις απαντά το PC2

2.3) Ναι απαντά

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

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

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

2.7) cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf
service unbound restart

2.8) tcpdump -e -vvv -i em0

2.9) ifconfig em0 delete
dhclient em0

2.10) 192.168.2.5

2.11) domain-name
domain-name-server

2.12) Ναι
search ntua.lab
nameserver 192.168.2.1

2.13) host 192.168.2.5 -> PC1.ntua.lab

2.14) host NS1 -> 192.168.2.1

2.15) Ναι

2.16) `ifconfig em0 delete`
`dhclient em0`

2.17) 192.168.2.6

2.18) Ναι

2.19) Απο DNS αφού την εγγραφή στο αρχείο `/etc/hosts` την διαγράψαμε σε προηγούμενο ερώτημα

2.20) Όχι το Ping προσπαθεί να στείλει στην 192.168.2.7

2.21) Ο resolver ψάχνει πρώτα στα τοπικά αρχεία και μετά στον DNS

2.22) Στο αρχείο υπάρχει το `hosts: file dns` που συμφωνεί με το παραπάνω συμπέρασμα

2.23) `host PC2 -> 192.168.2.6`

2.24) Η εντολή `host` ρωτάει τον DNS

2.25) `rm -r /etc/resolv.conf`
`resolvconf -u`
Το ίδιο με πριν

2.26) `tcpdump -vvv -e -n -i em0 not port 67 and not port 68`

2.27) `host ntua.lab -> 192.168.2.1`

2.28) Ναι

2.29) `udp`

2.30) 53 και 33760

2.31) 53

2.32) `tcpdump -vvv -e -n -i em0 port 53`

2.33) `host ns1`

2.34) 6

2.35) A, AAAA, MX

Όνομα = `ns1.ntua.lab`

2.36) Σε όλα

2.37) `drill ns1`

`drill ns1.ntua.lab`

2.38) Και για τα δύο ονόματα αλλά απάντηση δόθηκε μόνο για το `ns1.ntua.lab`

2.39) Καθώς στο `resolv.conf` αρχείο υπάρχει το `search ntua.lab` για οτιδήποτε όνομα αναζητήσουμε την `ip` του μπαίνει αυτόματα το `search path` αυτό

2.40) `ping localhost`

`ping pc1`

Δεν υπάρχει κίνηση DNS γιατί το `localhost` καθώς και το `PC1` υπάρχουν στο αρχείο `/etc/hosts`

2.41) `ping ns1`

2.42) 2 μηνύματα DNS τύπου A

2.43) Πάλι 2 μηνύματα

2.44) Συμπεραίνουμε ότι το `PC1` δεν αποθηκεύει κάπου την `ip` του `ns1` οπότε κάθε φορά την ρωτάει

Μέρος 3ο

3.1) hostname = "SRV"
lighttpd_enable="YES"

3.2) mkdir /usr/local/www/data

3.3) vi index.html
"Hello World!"

3.4) reboot
rm -r /etc/resolv.conf

3.5) service -e

3.6) netstat -a
port 80 active (http port)

3.7) ifconfig em1 192.168.2.3/28

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

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

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

3.11) tcpdump -e -n -vvv -i em1

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

3.13) TCP
Port = 80

3.14) Στο /root/ directory με όνομα srv.ntua.lab

Μέρος 4ο

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) -

4.7) -

4.8) search ntua.lab
nameserver 192.168.2.1

4.9) ifconfig_em0="DHCP"
service netif restart

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

4.11) service netif restart
service routing restart
vi /etc/resolv.conf
search ntua.lab
nameserver 192.168.2.1

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

4.13) local-data: "SRV.ntua.lab IN A 192.168.2.18"

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

local-data-ptr: "192.168.2.18 SRV.ntua.lab"

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

4.14) ΝαΙ

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

4.16) Όχι

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

4.18) ΝαΙ

4.19) ΝαΙ

4.20) Όχι

4.21) ipfw nat 111 config if em1 reset

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

4.23) ΝαΙ

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

4.25) tcpdump -vvv -e -n -i em1

4.26) ping -c 2 www.ntua.gr
10.0.3.15

4.27) 147.102.224.101

4.28) Ο NS1 ρωτάει τον 9.9.9.9

4.29) tcpdump -vvv -e -n -i em1 port 53

4.30) Σε κάποια ο 8.8.8.8 και σε άλλα ο 9.9.9.9

4.31) tcpdump -vvv -e -n -i em0 port 53

4.32) ping -c 1 course.cn.ntua.gr
CNAME = course.cn.ece.ntua.gr

4.33) Και οι δύο έκαναν ερωτήματα A και έλαβαν απάντηση τύπου A και CNAME

4.34) tcpdump -vvv -e -n -i em1 port 53

4.35) drill www.cn.ece.ntua.gr
1 ερώτημα DNS. Διάρκεια 20 minutes

4.36) tcpdump -vvv -e -n -i em0 port 53
Παράγονται σε κάθε drill που κάνουμε και η διάρκεια συνεχώς μειώνεται

4.37) Στον NS1 οι απαντήσεις DNS αποθηκεύονται σε cache και για αυτό παράγεται μόνο μια ερώτηση. Αυτό γίνεται κάθε 20 Minutes

4.38) ping -c 1 147.102.224.101

4.39) ping www.ntua.gr
Όχι καθώς δεν έχουμε ορίσει DNS server

4.40) nameserver 192.168.2.17

4.41) Ναι

4.42) host www.ntua.lab

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

4.44) SRV

Μέρος 5ο

5.1) sysrc hostname="ns2.ntua.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) -

5.9) -

5.10) -

5.11) -

5.12) ipfw nat 222 config ip em1 reset same_ports

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

5.14) ifconfig_em0="192.0.2.2/29"
defaultrouter="192.0.2.1"

5.15) service netif restart, service routing restart
vi /etc/resolv.conf
search ntua.lab
nameserver 192.0.2.1

5.16) Ναι

5.17) vi /etc/rc.conf

ifconfig_em1="192.0.2.10/29"

defaultrouter="192.0.2.9"

5.18) service netif restart, service routing restart

5.19) Ναι μπορούμε αφού παραμένει η λειτουργία του πίνακα 111

5.20) PC1: 192.168.2.18 (SRV)

PC2: 192.0.2.10 (NS1)

5.21) Connection Refused

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

5.23) Ναι

5.24) NS1

5.25) Στον SRV

5.26) Με τον NS1 αφού δεν υπάρχει κανόνας στο firewall του NS1 που να προωθεί πακέτα για ssh σύνδεση

5.27) ipfw nat 111 config ip em1 reset redirect_port tcp 192.168.2.18:80
80 redirect_port tcp 192.168.2.18:22 22

5.28) Ναι

hostname

ifconfig