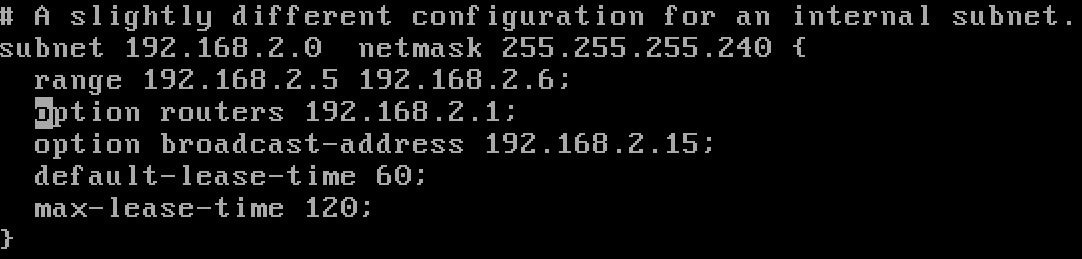
|  |  |  |
| --- | --- | --- |
| **Ονοματεπώνυμο:** | | **Όνομα PC:** |
| **Ομάδα:** | **Ημερομηνία:** | |

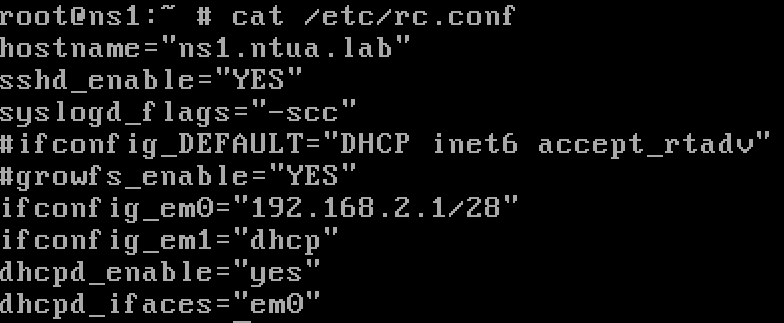
# Εργαστηριακή Άσκηση 12

## Υπηρεσίες στο Διαδίκτυο

#### Απαντήστε στα ερωτήματα στον χώρο που σας δίνεται παρακάτω και στην πίσω σελίδα εάν δεν επαρκεί. Το φυλλάδιο αυτό θα παραδοθεί στον επιβλέποντα.

##### 1

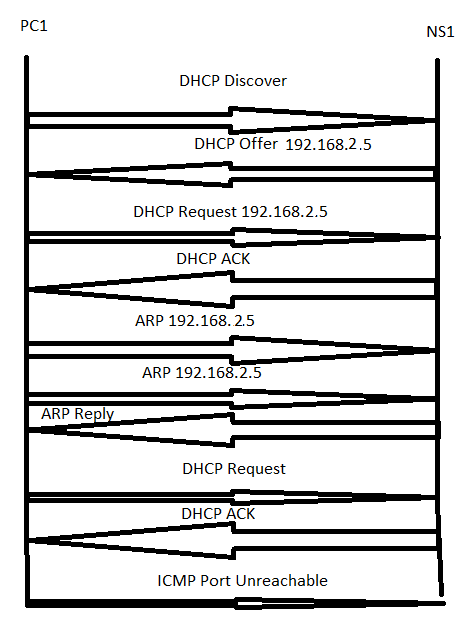




1.1 tcpdump -eevni em0

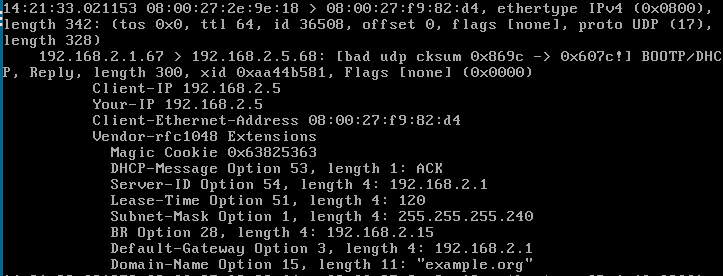
1.2 dhclient em0

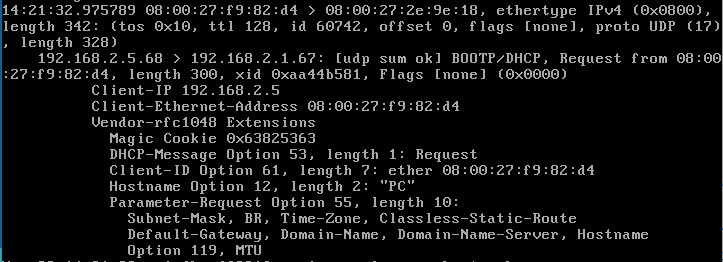
1.3



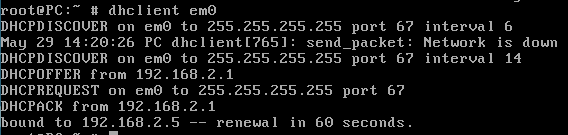
Σε μερικές καταγραφές παρατηρήσαμε και πλαίσια ARP που παράγει ο NS1 για τη διεύθυνση 192.168.2.5 πριν το DHCP Offer για να βεβαιωθεί ότι δε χρησιμοποιείται.

Στο τέλος παρατηρήσαμε και παραγωγή ICMP Echo Request από το NS1 στο PC1 πιθανόν για να βεβαιωθεί ότι αποδόθηκε σωστά η IPv4 διεύθυνση που του ανέθεσε.





1.4 DHCP Discover, DHCP Offer, DHCP Request, DHCP ACK.



1.5 Του αποδόθηκε η 192.168.2.5 και η διεύθυνση του εξυπηρετητή είναι η 192.168.2.1

..........................................................................................................................................................

1.6 60s

1.7 UDP

1.8 Οι θύρες 67(NS1) και 68(PC1).

1.9 Discover 0.0.0.0->255.255.255.255

Offer 192.168.2.1->192.168.2.5

Request 0.0.0.0->255.255.255.255

ACK 192.168.2.1->192.168.2.5

..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

1.10 Discover 08:00:27:f9:82:d4 (MAC PC1)->ff:ff:ff:ff:ff:ff

Offer: 08:00:27:2e:9e:18 (MAC NS1)->08:00:27:f9:82:d4

Request: 08:00:27:f9:82:d4 (MAC PC1)->ff:ff:ff:ff:ff:ff

ACK: 08:00:27:2e:9e:18 (MAC NS1)->08:00:27:f9:82:d4

..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

1.11 Λόγω των MAC addresses. Ο host λαμβάνει πακέτα με τη unicast MAC του την οποία ο DHCP server μαθαίνει από το Discover, ενώ ο server λαμβάνει αρχικά τα broadcast πακέτα και έπειτα τα unicast όταν τον επιλέξει το PC.

..........................................................................................................................................................

1.12 Ναι παρατηρήσαμε και πλαίσια ARP που παράγει ο NS1 για τη διεύθυνση 192.168.2.5 πριν το DHCP Offer για να βεβαιωθεί ότι δε χρησιμοποιείται.

..........................................................................................................................................................

..........................................................................................................................................................

1.13 Όχι δεν παρατηρήσαμε γιατί στάλθηκε ARP και πάντα στέλνεται ένα από τα δύο.

..........................................................................................................................................................

..........................................................................................................................................................

1.14 Για να βεβαιωθεί ότι δεν υπάρχει ήδη άλλος host που τη χρησιμοποιεί δημιουργώντας έτσι conflict.

..........................................................................................................................................................

..........................................................................................................................................................

1.15 Στο τέλος παρατηρήσαμε και παραγωγή ICMP Echo Request από το NS1 στο PC1 πιθανόν για να βεβαιωθεί ότι αποδόθηκε σωστά η IPv4 διεύθυνση που του ανέθεσε.

..........................................................................................................................................................

1.16 Για 2 λεπτά (120 δευτερόλεπτα)

1.17 Το server-id και τη διεύθυνση που του προσφέρθηκε.

..........................................................................................................................................................

..........................................................................................................................................................

1.18 Έχει διεύθυνση πηγής την IP που του εκχωρήθηκε νωρίτερα, διεύθυνση προορισμού τη Unicast διεύθυνση του NS1 και MAC προορισμού αυτή του NS1. Δεν έχει το server-id

..........................................................................................................................................................

..........................................................................................................................................................

1.19 Γιατί έχοντας ολοκληρώσει τη διαδικασία απόδοσης διευθύνσεων δεν ακούει πλέον στη θύρα 68 για πακέτα DHCP.

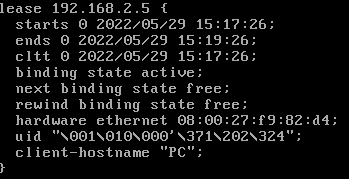
..........................................................................................................................................................

..........................................................................................................................................................

1.20 /var/db/dhcpd/dhcpd.leases

1.21 Κάθε 2 λεπτά.

1.22

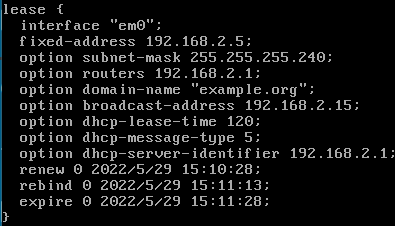


..........................................................................................................................................................

..........................................................................................................................................................

1.23 /var/db/dhclient.leases.em0

1.24

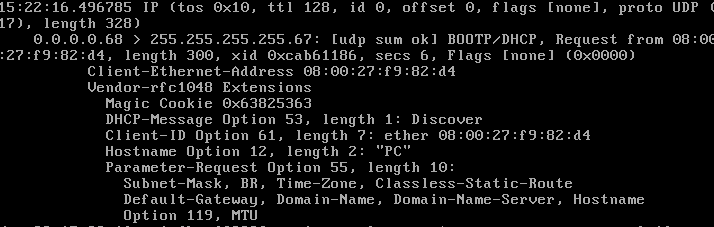


..........................................................................................................................................................

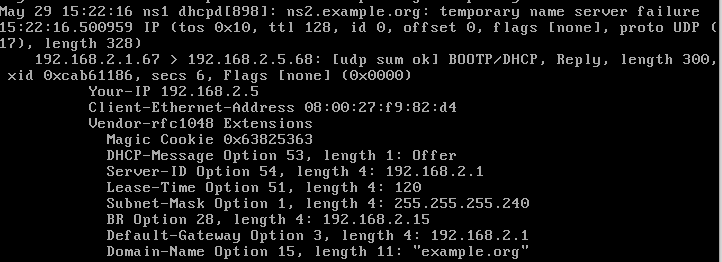
..........................................................................................................................................................

1.25 45s

1.26 7



1.27 Subnet-Mask, BR, Default-Gateway, Domain-Name



..........................................................................................................................................................

..........................................................................................................................................................

1.28 tcpdump -vvni em0

1.29 service isc-dhcpd stop

1.30 service isc-dhcpd start

..........................................................................................................................................................

1.31 Μόλις αποδόθηκε πάλι η 192.168..2.5 σταματήσαμε την καταγραφή.

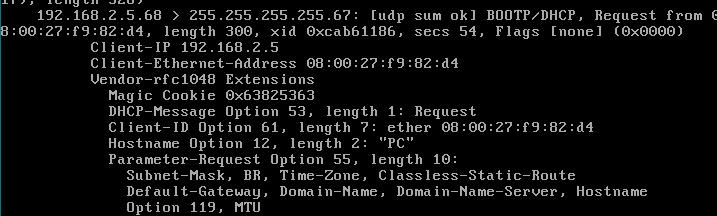
1.32 4 φορές με αποστάσεις 7s, 9s, 11s.

..........................................................................................................................................................

1.33 Λαμβάνει ICMP Port Unreachable για τη θύρα 67 που σημαίνει ότι καμία υπηρεσία του εξυπηρετητή δεν ακούει σε αυτή τη θύρα.

..........................................................................................................................................................

1.34 Η broadcast διεύθυνση.

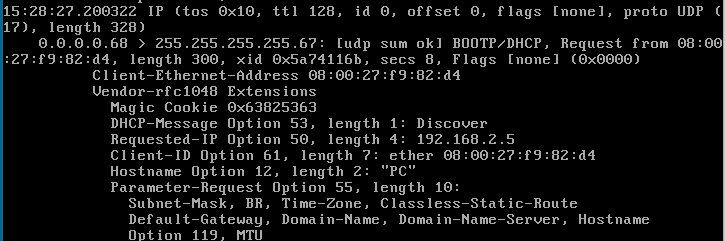


..........................................................................................................................................................

1.35 Έχει λήξει ο χρόνος προσπάθειας επανασύνδεσης στον συγκεκριμένο DHCP Server οπότε γίνεται προσπάθεια σύνδεσης σε άλλον

..........................................................................................................................................................

1.36 Η IP 255.255.255.255 και η MAC ff:ff:ff:ff:ff:ff. Γίνεται κατανοητό από τη διεύθυνση πηγής του μηνύματος.



..........................................................................................................................................................

..........................................................................................................................................................

1.37 Για να ελεγχθεί αν χρησιμοποιείται η προτεινόμενη διεύθυνση που ζητά το PC1 η οποία υπάρχει ήδη στα leases του NS1 ο οποίος ξέρει και τη MAC που της αντιστοιχεί οπότε δεν απαιτείται arp.

..........................................................................................................................................................

1.38 Διαγράφονται.

..........................................................................................................................................................

1.39 Διότι όταν αρχικά ο πελάτης δε θα έχει IPv4 διεύθυνση πρέπει να λάβει κάπως τα μηνύματα του εξυπηρετητή και αν αυτά είναι broadcast και χρησιμοποιούταν μία τυχαία θύρα μπορεί να λαμβάνονταν και από άλλους υπολογιστές και να δημιουργούταν σύγχυση.

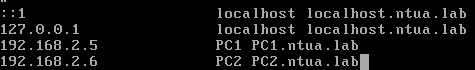
..........................................................................................................................................................

..........................................................................................................................................................

..........................................................................................................................................................

##### 2

2.1



..........................................................................................................................................................

2.2 Απαντά το PC2 σε κάθε περίπτωση. Δεν έχει σημασία η χρήση μικρών ή κεφαλαίων

..........................................................................................................................................................

2.3 Απαντά το PC1.

..........................................................................................................................................................

2.4



2.5



..........................................................................................................................................................

2.6



..........................................................................................................................................................

2.7 service unbound restart

..........................................................................................................................................................

2.8 tcpdump -vvni em0

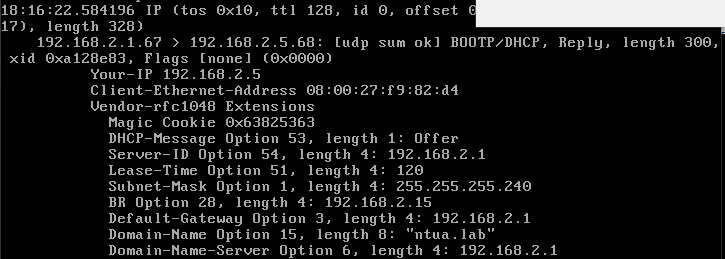
2.9 ifconfig em0 delete

dhclient em0

..........................................................................................................................................................

2.10 Τη διεύθυνση 192.168.2.5

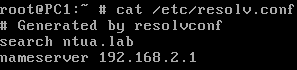
2.11 Τις Domain-Name και Domain-Name-Server.



..........................................................................................................................................................

..........................................................................................................................................................

2.12 Έχει δημιουργηθεί.



..........................................................................................................................................................

2.13 PC1



2.14 192.168.2.1



2.15 Ναι μπορούμε.

2.16 ifconfig em0 delete

dhclient em0

..........................................................................................................................................................

2.17 Την 192.168.2.6

2.18 Ναι μπορούμε.

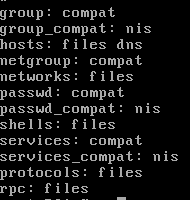
2.19 Από το /etc/hosts

2.20 Όχι δε μπορούμε.

2.21 Ότι πρώτα κοιτά το /etc/hosts και αν εκεί δε βρει αντιστοίχηση ρωτά τον nameserver.

..........................................................................................................................................................

2.22 files dns. Ναι συμφωνεί η σειρά αναζήτησης με αυτή που παρατηρήσαμε προηγουμένως.



..........................................................................................................................................................

2.23 192.168.2.6



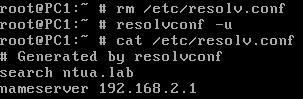
2.24 Η host ρωτά κατευθείαν τον dns server χωρίς να εξετάσει τα τοπικά αρχεία.

..........................................................................................................................................................

2.25 rm /etc/resolv.conf

cat /etc/resolv.conf

Είναι το ίδιο με το αρχικό.



..........................................................................................................................................................

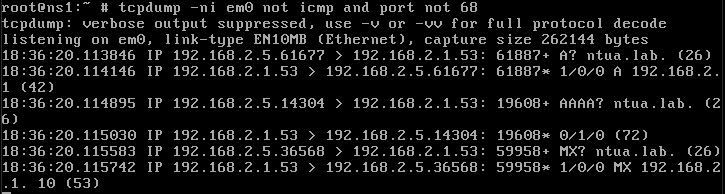
..........................................................................................................................................................

2.26 tcpdump -vvni em0 not icmp and port not 68

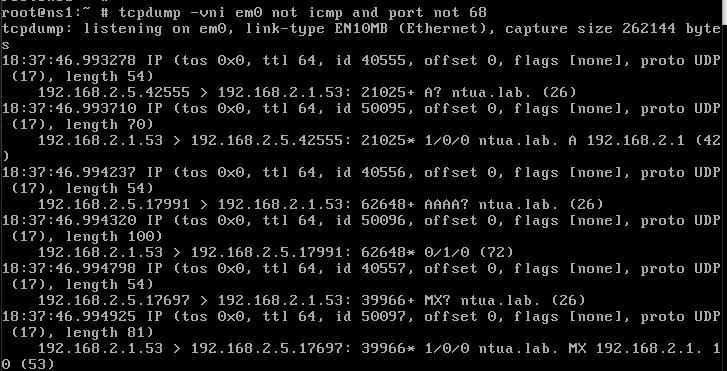
2.27 192.168.2.1



2.28 Ναι υπάρχει.



Και αναλυτικά:



2.29 UDP

2.30 PC1: 42555, 17991, 17696

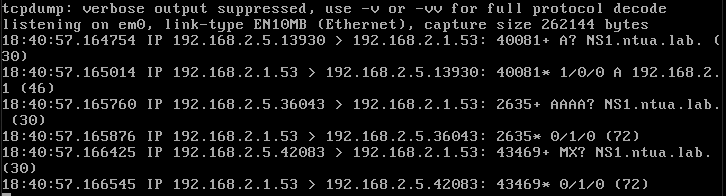
NS1: 53

2.31 Η 53.

2.32 tcpdump -ni em0 port 53

2.33 host NS1

2.34 Ανταλλάχθηκαν 6 μηνύματα.



2.35 Σε ερωτήματα αντιστοίχισης ονόματος σε IPv4 και IPv6 (A/AAAA) διεύθυνση και σε αναζήτηση εξυπηρετητών ηλεκτρονικού ταχυδρομείου (MX)

..........................................................................................................................................................

..........................................................................................................................................................

2.36 Σε όλες στάλθηκε μήνυμα απάντηση αλλά ουσιαστική απάντηση δόθηκε μόνο στην ερώτηση για την IPv4 διεύθυνση.

2.37 drill ns1

drill ns1.ntua.lab

2.38 Για το όνομα ns1. και ns1.ntua.lab. Λήφθηκε απάντηση για το ns1.ntua.lab.

..........................................................................................................................................................

2.39 Ότι η drill δεν το χρησιμοποιεί.

2.40 Σε καμία από τις δύο περιπτώσεις αφού χρησιμοποιούνται οι Local αντιστοιχίσεις.

2.41 ping ns1

2.42 Ανταλλάχθηκαν 2 μηνύματα DNS και αφορούσαν στην εύυρεση της IPv4 διεύθυνσης του υπολογιστή ns1.ntua.lab.

2.43 Παράγονται ερωτήματα προς τον εξυπηρετητή DNS. Παράγεται ένα για κάθε ping που ξεκινάμε.

..........................................................................................................................................................

2.44 Ότι έχουν πολύ μικρή διάρκεια ζωής εκτός εάν χρησιμοποιούνται.

..........................................................................................................................................................

##### 3

3.1 sysrc lighttpd\_enable=yes

3.2 mkdir -p /usr/local/www/data

3.3 touch /usr/local/www/data/index.html

vi /usr/local/www/data/index.html

..........................................................................................................................................................

3.4 reboot

rm /etc/resolv.conf

3.5 service lighttpd status

3.6 netstat -an | grep 80 για να δούμε αν υπάρχει εφαρμογή που ακούει στη θύρα http 80.

3.7 ifconfig em0 192.168.2.3/28

3.8 local-data: “SRV.ntua.lab A 192.168.2.3”

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

3.10 unbound-checkconf

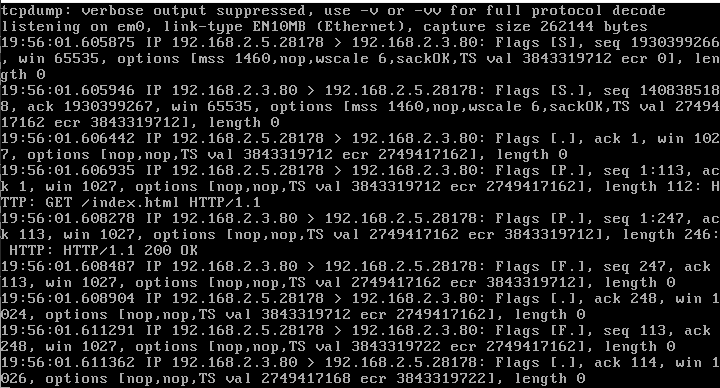
cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf

service unbound restart

3.11 tcpdump -ni em0

3.12 fetch http://srv.ntua.lab/index.html

3.13 Το πρωτόκολλο TCP. Ο εξυπηρετητής HTTP ακούει στη θύρα 80.



3.14 Στο τρέχον directory στο αρχείο index.html.

##### 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 sysrc -a

4.7 Υπάρχει ήδη προεπιλεγμένη πύλη στη διεύθυνση 10.0.3.2

..........................................................................................................................................................

..........................................................................................................................................................

4.8



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



..........................................................................................................................................................

..........................................................................................................................................................

4.12 sysrc ifconfig\_em0=”192.168.2.18/28”

sysrc defaultrouter=”192.168.2.17”

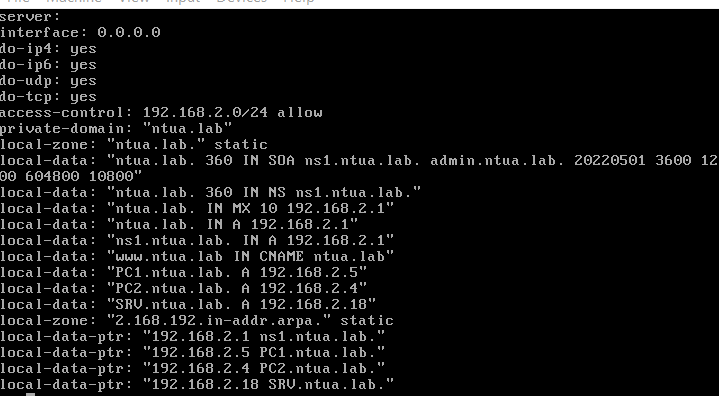
service netif restart

service routing restart

..........................................................................................................................................................

..........................................................................................................................................................

4.13



service unbound restart

..........................................................................................................................................................

4.14 Ναι μπορούμε.

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

4.16 Όχι δεν μπορούμε.

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 μπορούμε.

4.19 Ναι μπορούμε.

4.20 Όχι δεν μπορούμε.

4.21 ipfw nat 111 config if em1 unreg\_only reset

4.22 ipfw add 3000 nat 111 ip from any to any via em1

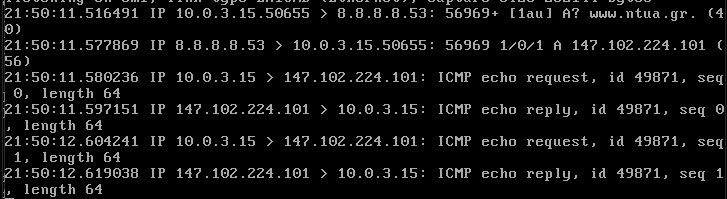
4.23 Ναι μπορούμε.

4.24 theseas.softlab.ece.ntua.gr



4.25 tcpdump -ni em1

4.26 Με τη διεύθυνση 10.0.3.15

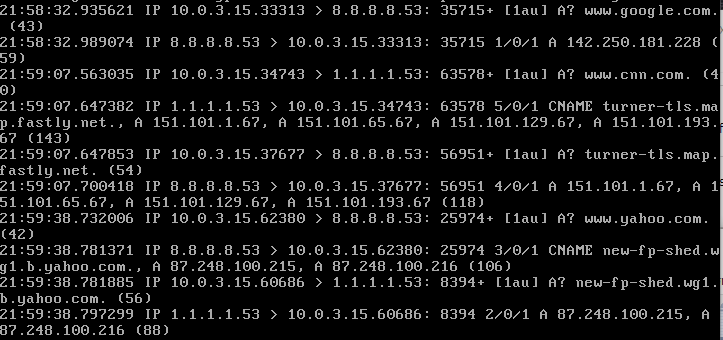


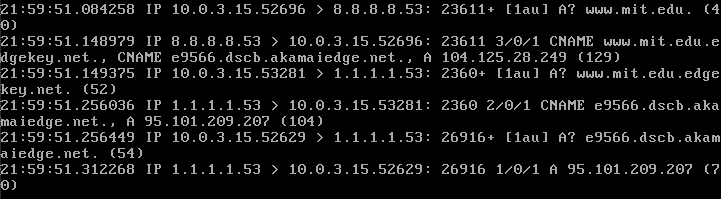
4.27 Η 147.102.224.101

4.28 Προς τον 8.8.8.8

4.29 tcpdump -ni em1 port 53

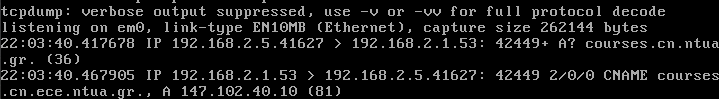
4.30 Ότι διαφέρει.





4.31 tcpdump -ni em0 port 53

4.32 courses.cn.ece.ntua.gr



4.33 Το PC1 έκανε ερώτημα A και έλαβε απάντηση CNAME και A. Ο NS1 έκανε και αυτός ερώτημα A και έλαβε απάντηση CNAME και επιπλέον έκανε ερώτημα A για το πραγματικό όνομα του υπολογιστή και έλαβε απάντηση Α.

..........................................................................................................................................................

..........................................................................................................................................................

4.34 tcpdump -vvvni em1 port53

4.35 Παρατηρήσαμε ένα ερώτημα DNS. Η χρονική διάρκεια των απαντήσεων DNS είναι 20 λεπτά.

..........................................................................................................................................................

4.36 Παράγονται ερωτήματα DNS από το PC1 και απαντήσεις από τον NS1. Για τη χρονική διάρκεια ισχύος των απαντήσεων DNS παρατηρούμε ότι συνεχώς μειώνεται.

..........................................................................................................................................................

..........................................................................................................................................................

4.37 Ότι αποθηκεύονται για συγκεκριμένο χρόνο και όσο ισχύουν δεν ξαναρωτά τους εξωτερικούς εξυπηρετητές DNS για κάτι που έχει ήδη εγγραφή.

4.38 Ναι μπορούμε.

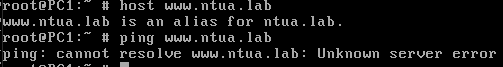
4.39 Όχι διότι δεν έχει οριστεί εξυπηρετητής DNS σε αυτό το μηχάνημα για να μεταφραστεί το όνομα.

4.40



4.41 Ναι μπορούμε.

4.42 Όχι μας απαντά απλώς ότι είναι ψευδώνυμο για το όνομα ntua.lab. Αν κάνουμε ping στο www.ntua.lab λαμβάνουμε σφάλμα ότι δεν μπορεί να επιλυθεί το όνομα.



..........................................................................................................................................................

4.43



service unbound restart

..........................................................................................................................................................

4.44 Απαντά ο SRV.

***5***

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”

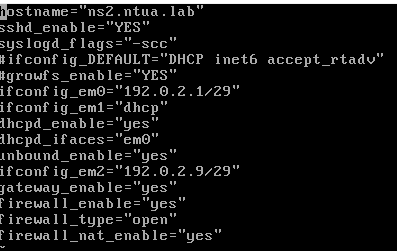
5.4 sysrc gateway\_enable=”yes”

5.5 sysrc firewall\_enable=”yes”

5.6 sysrc firewall\_type=”open”

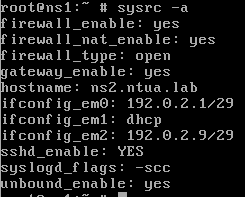
5.7 sysrc firewall\_nat\_enable=”yes”

5.8 vi /etc/rc.conf



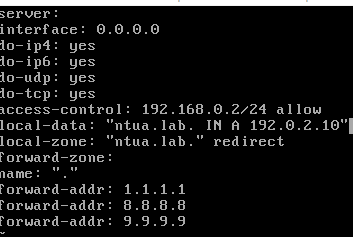
..........................................................................................................................................................

5.9 sysrc -a



Υπάρχει η εντολή για ενεργοποίηση της υπηρεσίας DNS (unbound\_enable).

5.10



..........................................................................................................................................................

5.11 netstat -rn. Υπάρχει προκαθορισμένη διαδρομή.

5.12 ipfw nat 222 config if em1 reset same\_ports

5.13 ipfw add 1100 nat 222 all 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



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 μπορούμε. Η λειτουργία του πίνακα NAT παραμένει.

5.20 PC1: 192.168.2.18

PC2: 192.0.2.10

5.21 Όχι. Εμφανίζεται το λάθος connection refused.



..........................................................................................................................................................

5.22 ipfw nat 111 config if em1 unreg\_only reset redirect\_port tcp 192.168.2.18:80 80

5.23 Ναι τώρα μπορούμε.

5.24 Ναι μπορούμε. Απαντά ο NS1

5.25 Στον SRV.

5.26 Με τον NS1 διότι η διεύθυνση www.ntua.lab μεταφράζεται στην IP της διεπαφής του NS1 στο WAN λόγω της παραμετροποίησης του Unbound στον NS2 καθώς το ssh δε χρησιμοποιεί τη θύρα 80 ώστε να ανακατευθυνθεί η κίνηση tcp που δημιουργεί.

5.27 ipfw nat 111 config if em1 unreg\_only reset redirect\_port tcp 192.168.2.18:80 80 redirect\_port tcp 192.168.2.18:22 22

5.28 Ναι τώρα μπορούμε. Από το prompt ή εκτελώντας την εντολή who βλέπουμε τον εαυτό μας στα συνδεδεμένα μηχανήματα.

