

**Εργαστηριο δικτυων υπολογιστων**

**Εργαστηριακη ασκηση 12: Υπηρεσιες στο Διαδικτυο**





7 Ioynioy, 2023

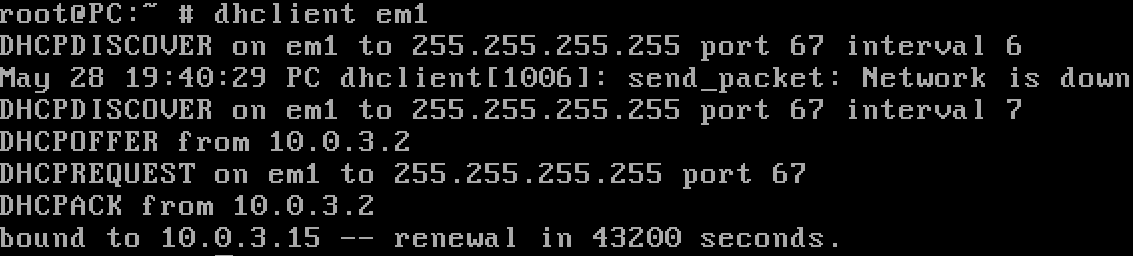
ΘΟΔΩΡΗΣ ΑΡΑΠΗΣ – EL18028

|  |  |
| --- | --- |
| **Ονοματεπώνυμο:** Θοδωρής Αράπης | **Ομάδα:** 3 |
| **Όνομα PC/ΛΣ:** DESKTOP-JGHL94V/ WINDOWS 10 | **Ημερομηνία:** 7/6/2023 |

**Άσκηση 1: Εγκατάσταση DHCP server**

***1***

Το κάνουμε.

***2***

***3***

Μπορούμε να κάνουμε ping.

***4***

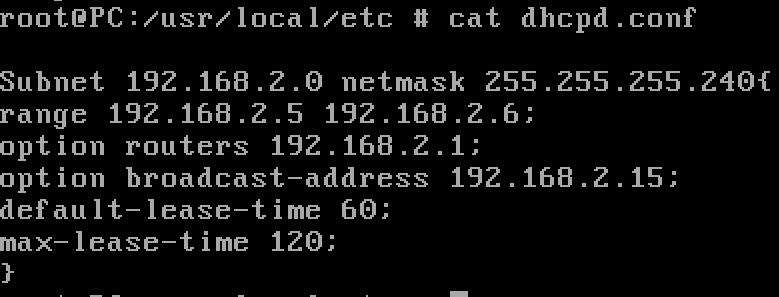
“**pkg update**”.

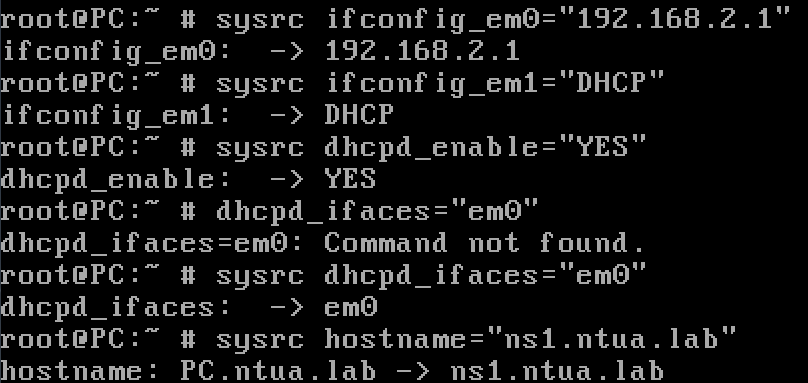
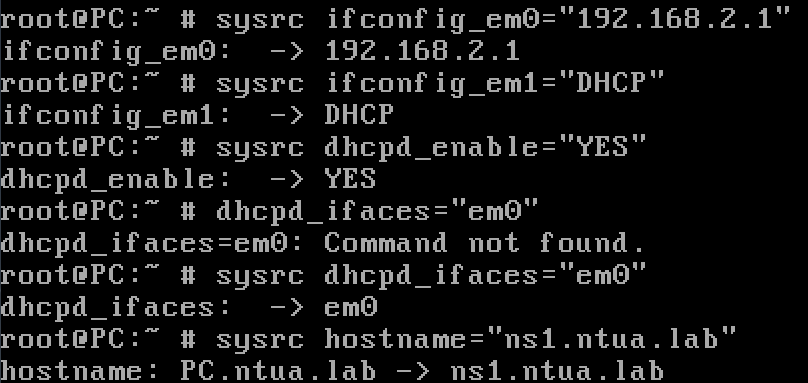
***5***

Κάνουμε export το new.ova.

***1***

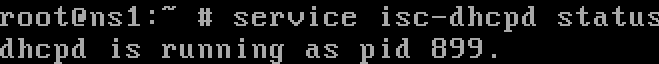
Η εντολή δε λειτουργεί, οπότε εκτελούμε εκ νέου “**dhclient em1**” στο NS1.

***2***

 ***3***

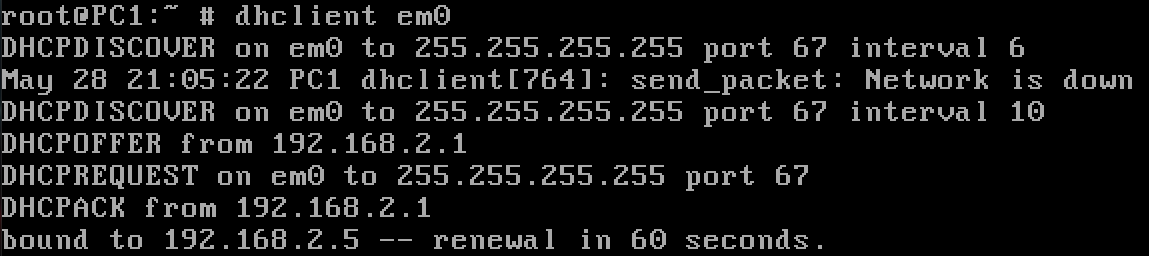
***4***

Εκτελούμε “**reboot**”.

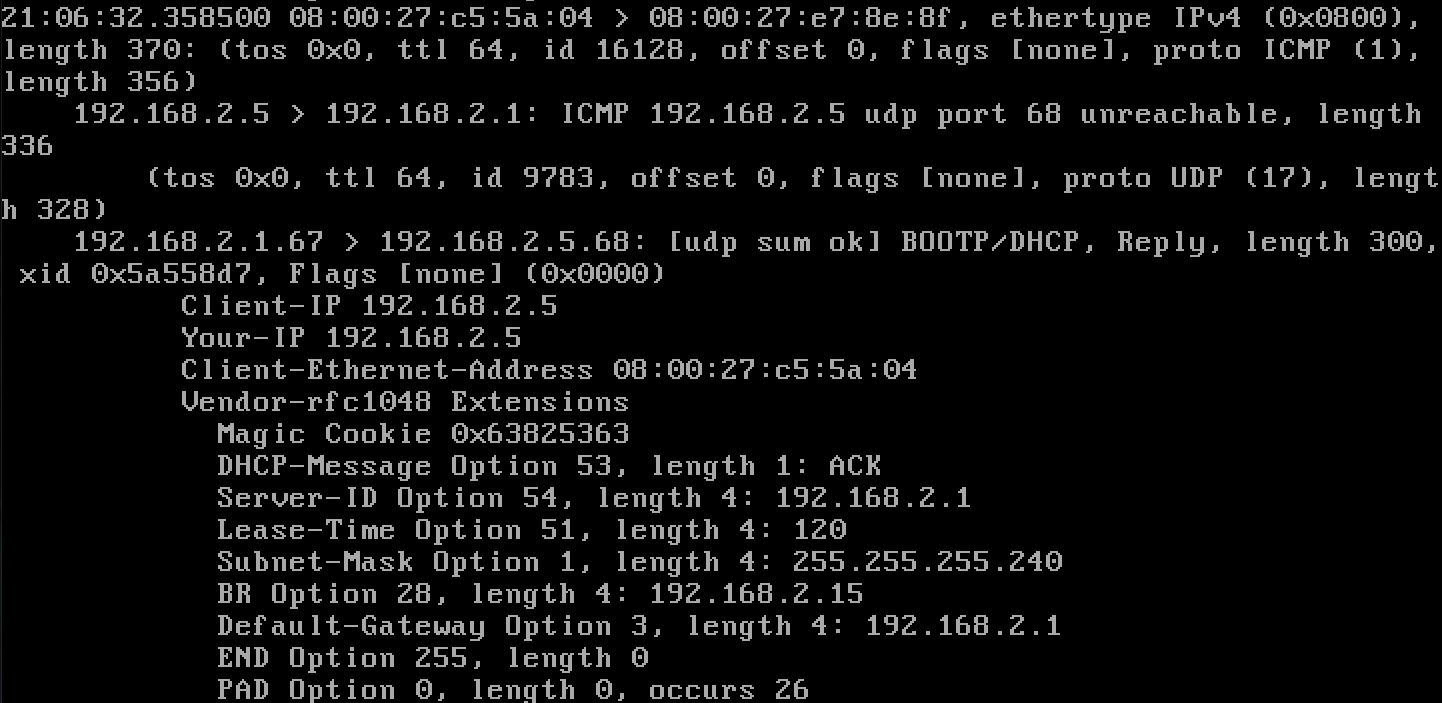
***5***

***1.1***



***1.2***

***1.3***

1. PC1 (0.0.0.0:68) → Broadcast : DHCP Discover
2. NS1 → ff:ff:ff:ff:ff:ff : ARP Request (who has 192.168.2.5)
3. NS1 → PC1 (MAC layer) : DHCP Offer (192.168.2.5)
4. PC1 → Broadcast : DHCP Request (192.168.2.5)
5. NS1 → PC1 : DHCP ACK (192.168.2.5)
6. PC1 → Broadcast : ARP Request (who has 192.168.2.5)
7. NS1 → PC1 : ICMP Echo Request
8. PC1 → Broadcast : ARP Request (who has 192.168.2.1)
9. NS1 → PC1 : ARP Reply
10. PC1 → NS1 : ICMP Echo Reply
11. PC1 → NS1 : DHCP Request
12. NS1 → PC1 : DHCP ACK
13. PC1 → NS1 : ICMP UDP port 68 unreachable + αντίστοιχο ACK με το παραπάνω.

***1.4***

Όπως βλέπουμε από το screenshot στο 1.2, αρχικά το PC1 κάνει broadcast DHCPDISCOVER και λαμβάνει DHCPOFFER από το NS1 (192.168.2.1). Στη συνέχεια το PC1 κάνει Broadcast ένα DHCPREQUEST στο οποίο και αποκρίνεται το NS1 με DHCPACK αποδίδοντάς του την 192.168.2.5.

***1.5***

Του αποδόθηκε η 192.168.2.5, ενώ η διεύθυνση του εξυπηρετητή είναι η 192.168.2.1.

***1.6***

Μετά από 1 λεπτό.

***1.7***

Το UDP.

***1.8***

PC1: Port 68, NS1: Port: 67

***1.9***

* DHCPDISCOVER: PC1(0.0.0.0) → Broadcast(255.255.255.255)
* DHCPOFFER: NS1(192.168.2.1) → PC1(192.168.2.5)
* DHCPREQUEST: PC1(0.0.0.0) → Broadcast(255.255.255.255)
* DHCPACK: NS1(192.168.2.1) → PC1(192.168.2.5)

***1.10***

* DHCPDISCOVER: 08:00:27:e7:8e:8f → ff:ff:ff:ff:ff:ff
* DHCPOFFER: 08:00:27:c5:5a:04 → ff:ff:ff:ff:ff:ff
* DHCPREQUEST: 08:00:27:e7:8e:8f → ff:ff:ff:ff:ff:ff
* DHCPACK: 08:00:27:c5:5a:04 → 08:00:27:e7:8e:8f

όπου 08:00:27:e7:8e:8f (PC1) και 08:00:27:c5:5a:04 (NS1)

***1.11***

Τα στέλνει μέσω της 0.0.0.0.

***1.12***

Ναι και τα παράγει ο NS1 για να δει εάν έχει κανείς στο τοπικό δίκτυο την IP που πρόκειται να δώσει στο PC1.

***1.13***

Όχι, δε παρατηρήσαμε.

***1.14***

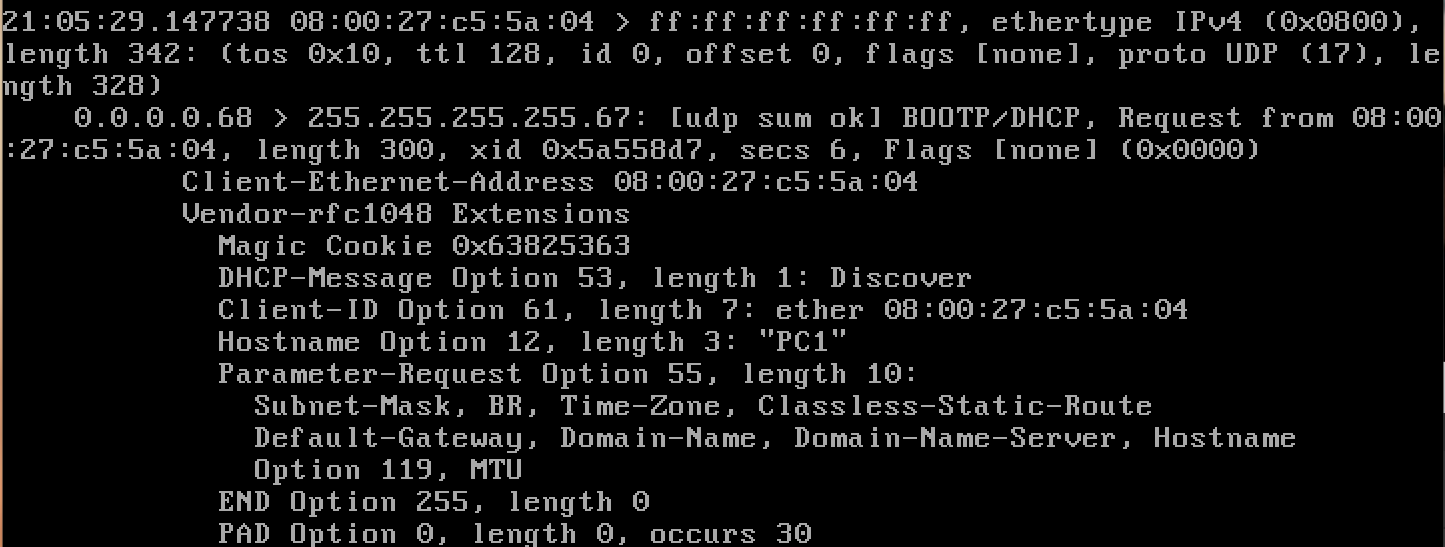
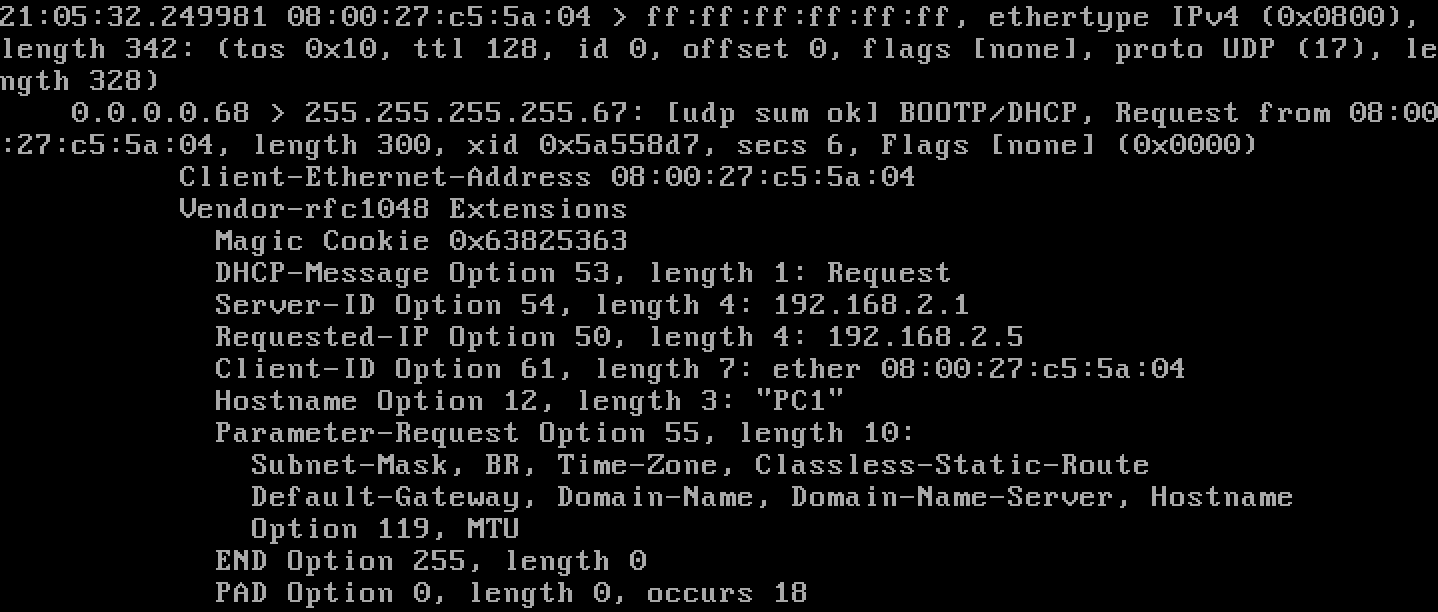
Για να επαληθεύσει πως δεν έχει άλλος την IP του στο ίδιο υποδίκτυο.

***1.15***

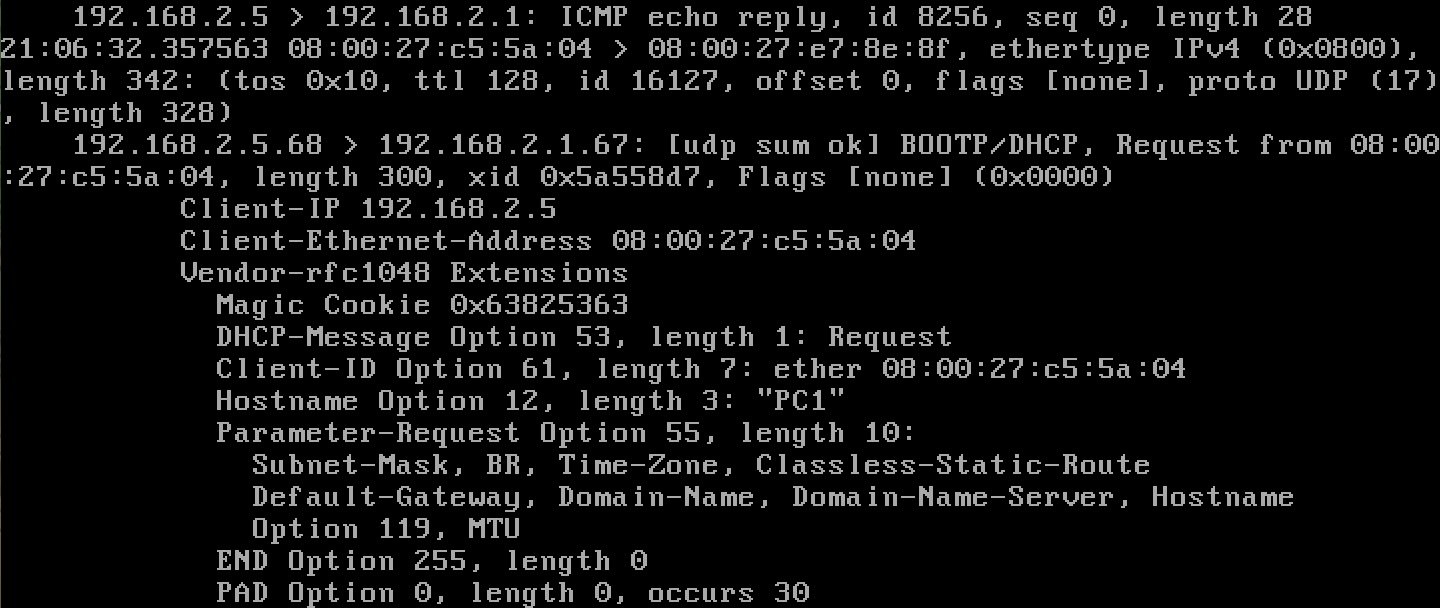
Ναι παρατηρήσαμε πως ο NS1 στέλνει ICMP Echo requests στην IP που μόλις έδωσε στο PC1, πιθανόν για να επαληθεύσει πως η ανάθεση ολοκληρώθηκε επιτυχώς.

***1.16***

Για 2 λεπτά (120 seconds).

***1.17***

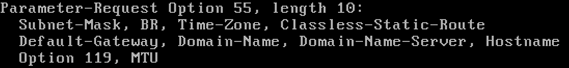
***1.18***

Το δεύτερο μήνυμα έχει επιπλέον το πεδίο “Client-IP: 192.168.2.5” και έχει “Client-ID Option 61, length 7: ether: 08:00:27:c5:5a:04” αντί για την αντίστοιχη γραμμή του Server-ID.

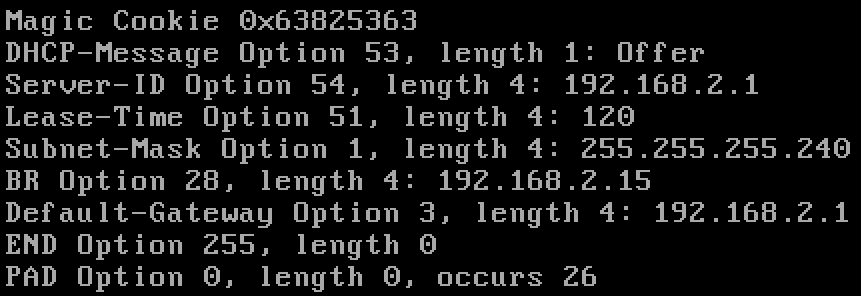
***1.19***

Το χρησιμοποιεί ως επιβεβαίωση στο DHCP ACK.

***1.20***

Ζητήθηκαν 10 παράμετροι.

***1.21***

Ο σέρβερ προσδιορίζει μόνο τα Subnet-Mask, BR (Broadcast), Default Gateway.

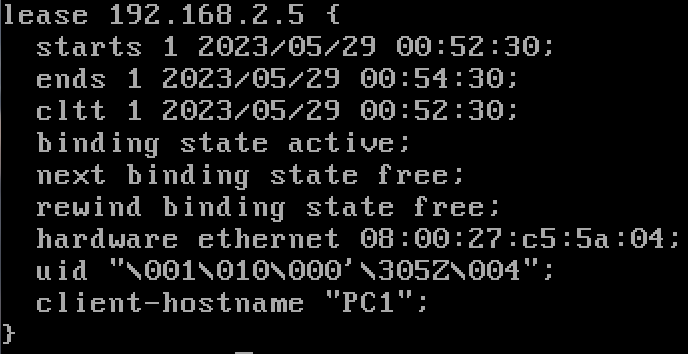
***1.22***

Στο /var/db/dhcpd/dhcpd.leases.

***1.23***

Κάθε λεπτό.

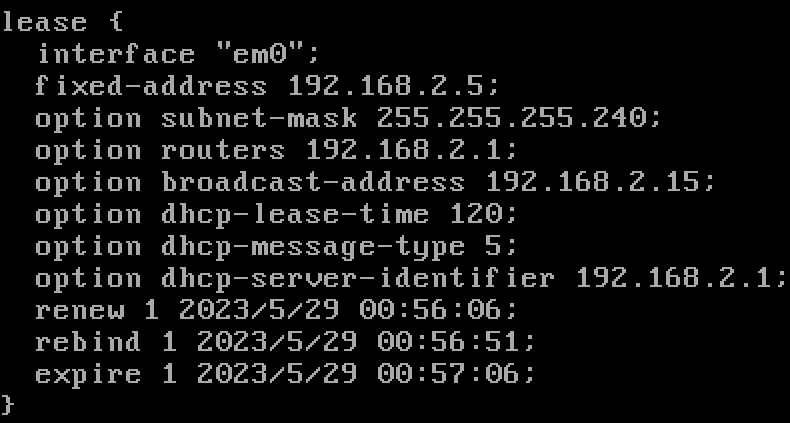
***1.24***

Βλέπουμε τις παρακάτω πληροφορίες:

***1.25***

Στο /var/db/dhclient.leases.em0.

***1.26***

Παρέχονται οι εξής πληροφορίες:

***1.27***

Πρέπει να περάσουν 45 δευτερόλεπτα (rebind – renew).

***1.28***

Εκτελούμε στο NS1 “**tcpdump -ni em0**”.

***1.29***

Εκτελούμε στο NS1 “**service isc-dhcpd stop**”.

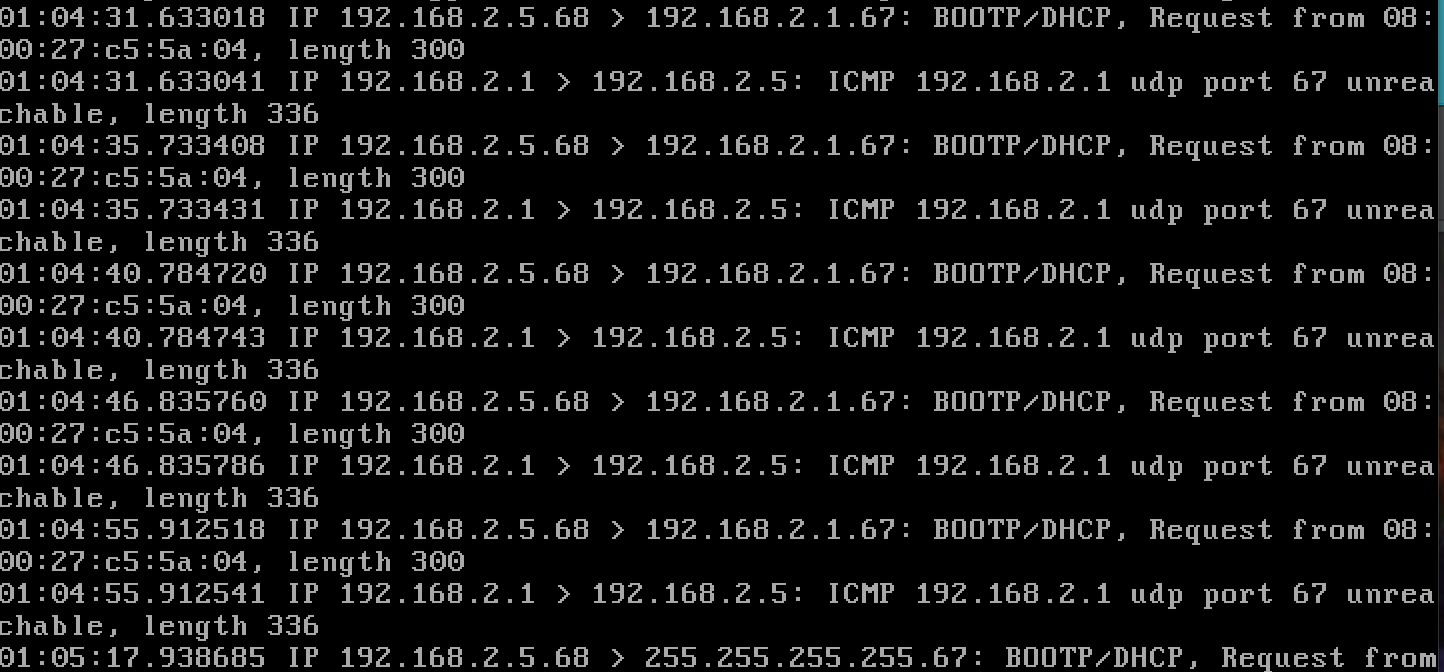
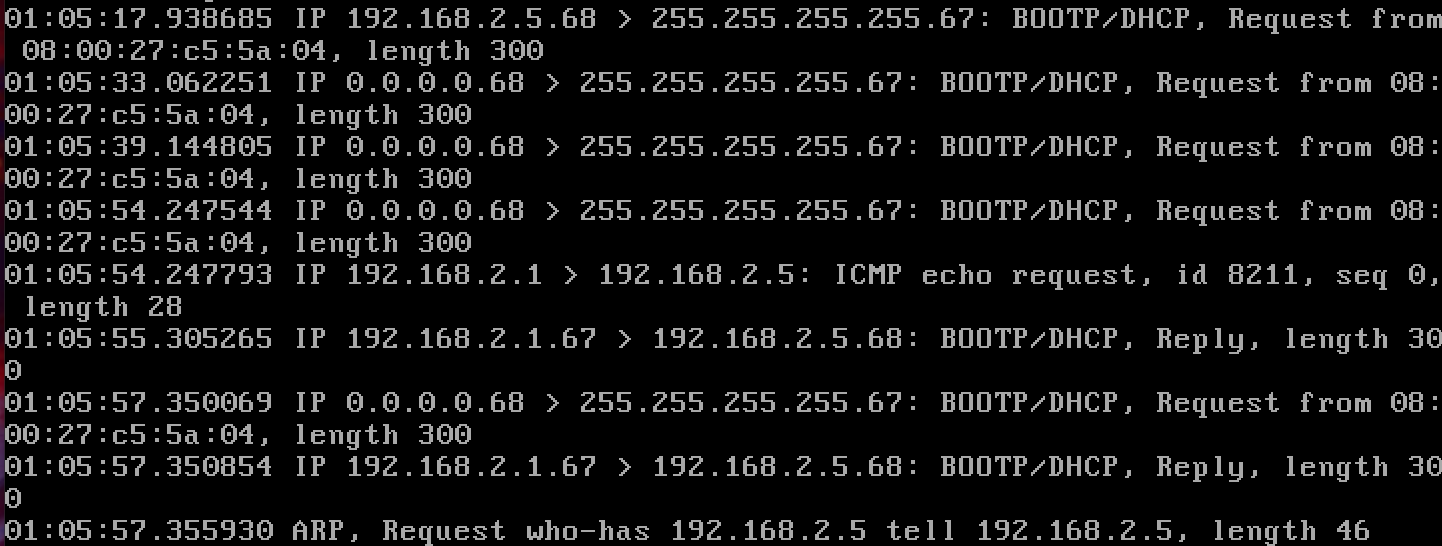
***1.30***

Εκτελούμε στο NS1 “**service isc-dhcpd start**”

***1.31***

Η IPv4 αποδόθηκε μετά από ελάχιστα δευτερόλεπτα.

***1.32***

Για όσο διάστημα το PC1 έχει ακόμα IP διεύθυνση, στέλνει 5 DHCP request προς τον Server, ανά περίπου 5 με 10 δευτερόλεπτα.

***1.33***

Ο σέρβερ απαντάει με “ICMP 192.168.2.1 udp port 67 unreachable”, λέγοντας μας με αυτόν τον τρόπο πως δε λειτουργεί η υπηρεσία dhcp σε αυτόν.

***1.34***

Στέλνει στην 255.255.255.255.

***1.35***

Κάνει Broadcast το προηγούμενο μήνυμα, αφού δε κατάφερε εντός του χρόνου επανασύνδεσης να ανανεώσει την IP του, οπότε και τη ζητάει από οποιονδήποτε άλλον server ακούει.

***1.36***

Από όταν το PC1 έχασε την IP του, στέλνει μηνύματα στην (MAC, IP) = (ff:ff:ff:ff:ff:ff, 255.255.255.255). Από το Source IP address, βλέπουμε πως έχει απολεσθεί η IP του, αφού τα στέλνει από την 0.0.0.0.

***1.37***

Για να επιβεβαιώσει πως δε χρησιμοποιεί κανείς άλλος την IP που πρόκειται να δώσει στο PC1.

***1.38***

Τα δεδομένα που υπήρχαν έχουν γίνει Overwrite από νέα δεδομένα.

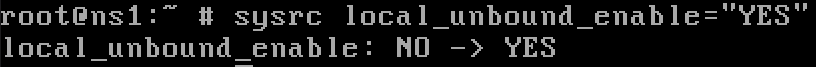
***1.39***

Διότι ο πελάτης στην αρχή, δεδομένου ότι δεν έχει IP, στέλνει το πακέτο από την IP 0.0.0.0 και από τη θύρα 68. Αν χρησιμοποιούσε οποιαδήποτε θύρα, τότε ο στόχος θα ήταν undefined, ενώ με χρήση well-known θύρας ο εξυπηρετητής καταλαβαίνει ποιο μηχάνημα ζητάει IP.

**Άσκηση 2: Εγκατάσταση εξυπηρετητή DNS**

***1***

Εγκαθιστούμε το πακέτο.

***2***

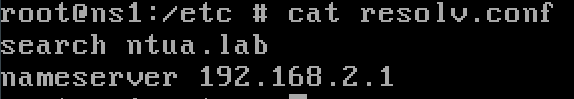
***3***

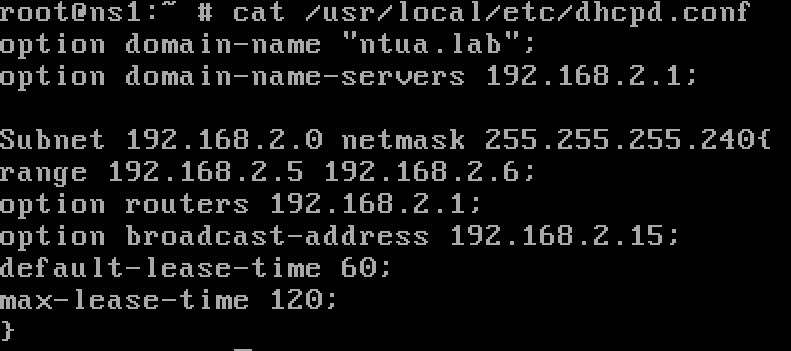
Δημιουργούμε κατάλληλα το αρχείο.

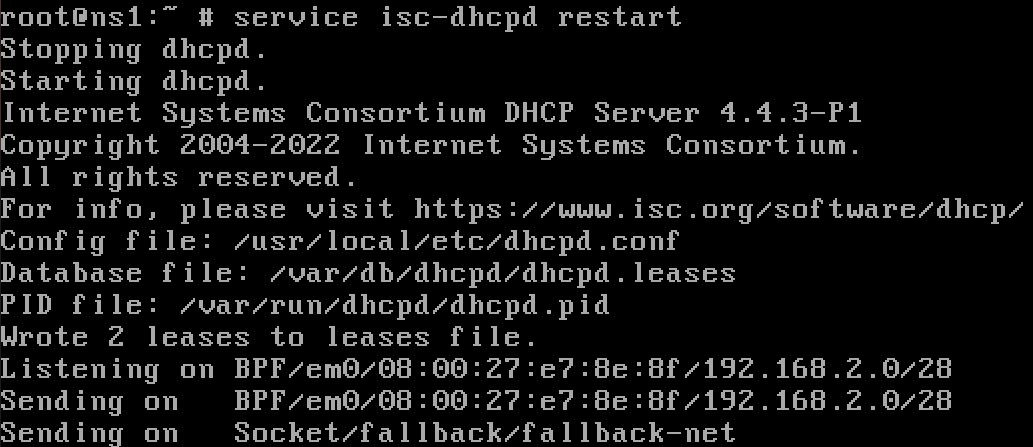
***4***

Δεν υπάρχουν λάθη, οπότε το αντιγράφουμε στο κατάλληλο destination

***5***

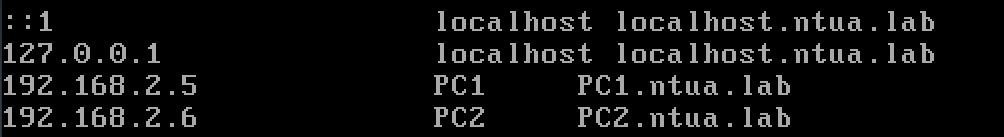
Δημιουργούμε το αρχείο:

***6***

***7***

***8***

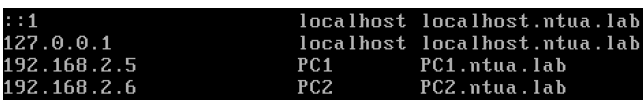
Δημιουργούμε τον κλώνο.

***2.1***

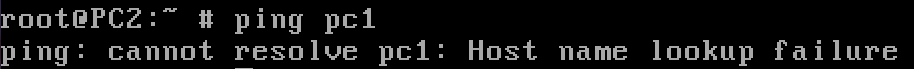
***2.2***

Σε όλα τα ping απαντάει το PC2, επομένως το αν έχουμε μικρά/κεφαλαία είναι αδιάφορο.

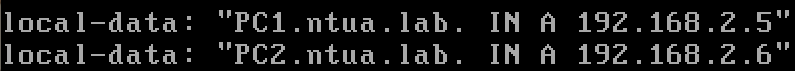
***2.3***

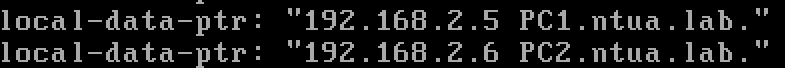
Αντίστοιχα τροποποιούμε κατάλληλα το αρχείο του PC2 και κάνουμε ping.

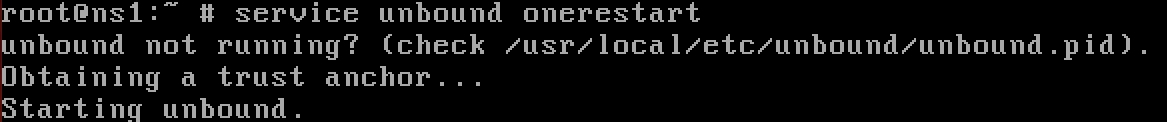
***2.4***

Αφού διαγράψουμε την εγγραφή για το PC1 λαμβάνουμε την παρακάτω απάντηση:

***2.5***

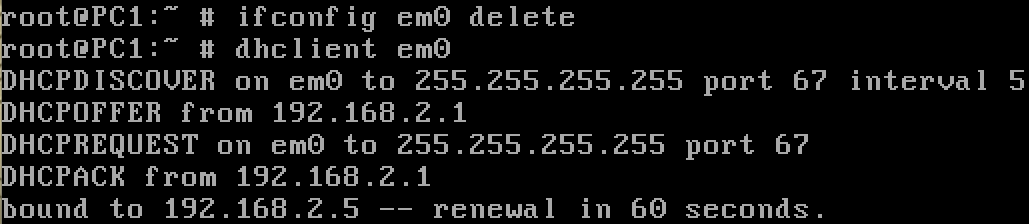
Προσθέτουμε τις παρακάτω εγγραφές:

***2.6***

***2.7***

***2.8***

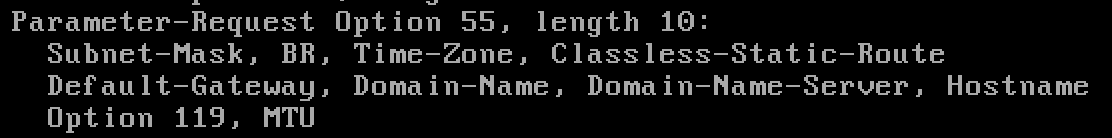
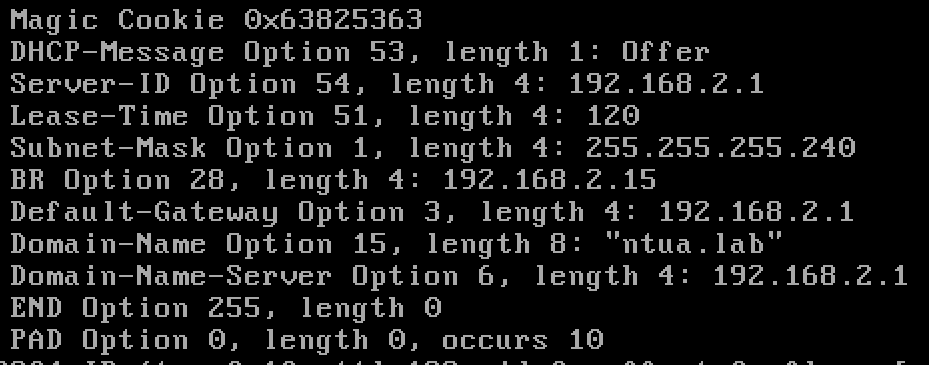
Εκτελούμε “**tcpdump -vvvni em0**”.

***2.9***

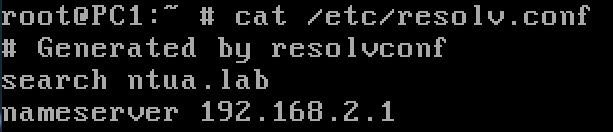
***2.10***

Έλαβε την 192.168.2.5.

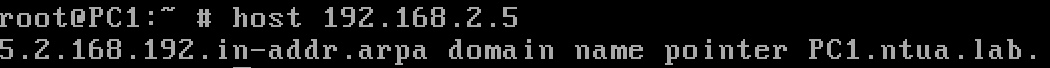
***2.11***

Από τις ζητούμενες από το PC1 παραμέτρους, βλέπουμε πως ο NS1 αποδίδει επιπλέον αυτή τη φορά τις “Domain-Name” και “Domain-Name-Server” με τιμές “ntua.lab” και “192.168.2.1” αντίστοιχα.

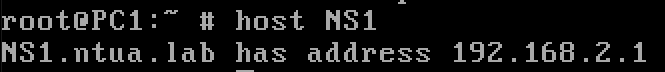
***2.12***

Ναι έχει δημιουργηθεί:

***2.13***

Είναι PC1.ntua.lab, όπως βλέπουμε παρακάτω.

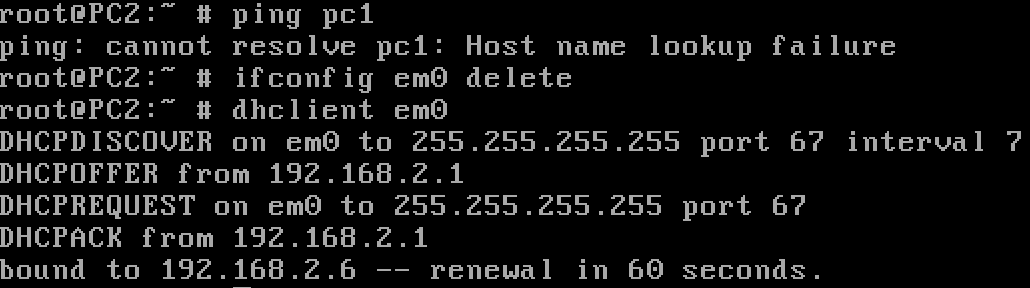
***2.14***

Βλέπουμε στο PC1 πως αντιστοιχεί στην 192.168.2.1.

***2.15***

Ναι.

***2.16***



***2.17***

Έλαβε την 192.168.2.6.

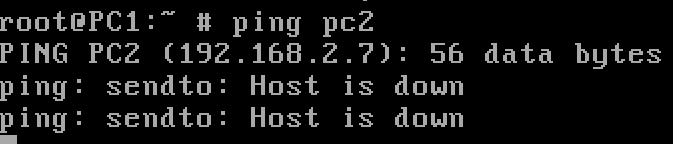
***2.18***

Ναι μπορούμε να κάνουμε “**ping PC1**”.

***2.19***

Το έλαβε από το DNS, καθώς από το /etc/hosts έχουμε διαγράψει τη σχετική εγγραφή.

***2.20***

Αφού τροποποιήσουμε κατάλληλα την εγγραφή για το PC2, μπορούμε να κάνουμε μεν “**ping pc2**”, αλλά δεδομένου ότι στέλνεται στην 192.168.2.7, λαμβάνουμε το εξής μήνυμα σφάλματος:

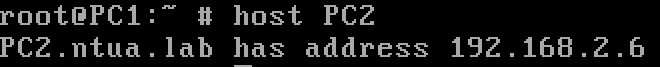
***2.21***

Δεδομένου ότι το παραπάνω ping απέτυχε, πρέπει να έγινε πρώτα αναζήτηση στο /etc/hosts και στη συνέχεια στο DNS, καθώς διαφορετικά θα πετύχαινε το παραπάνω ping.

***2.22***

Εκτελούμε στο PC1 “**cat /etc/nsswitch.conf**”, οπότε και βλέπουμε την παρακάτω γραμμή, η οποία δηλώνει πως πρώτα γίνεται αναζήτηση στο /etc/hosts και μετά στον DNS server, επιβεβαιώνοντας το παραπάνω.

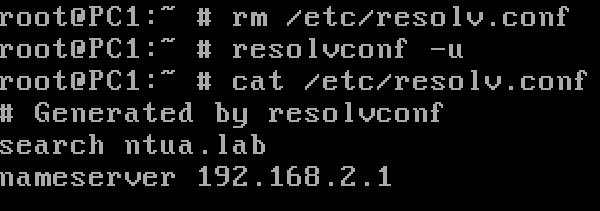
***2.23***

Έχει την 192.168.2.6.

***2.24***

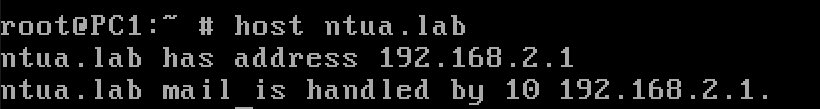
Η εντολή “**host PC2**” κάνει DNS query στον DNS server που έχουμε ορίσει, ενώ το Ping αντλεί τα δεδομένα από το /etc/hosts.

***2.25***

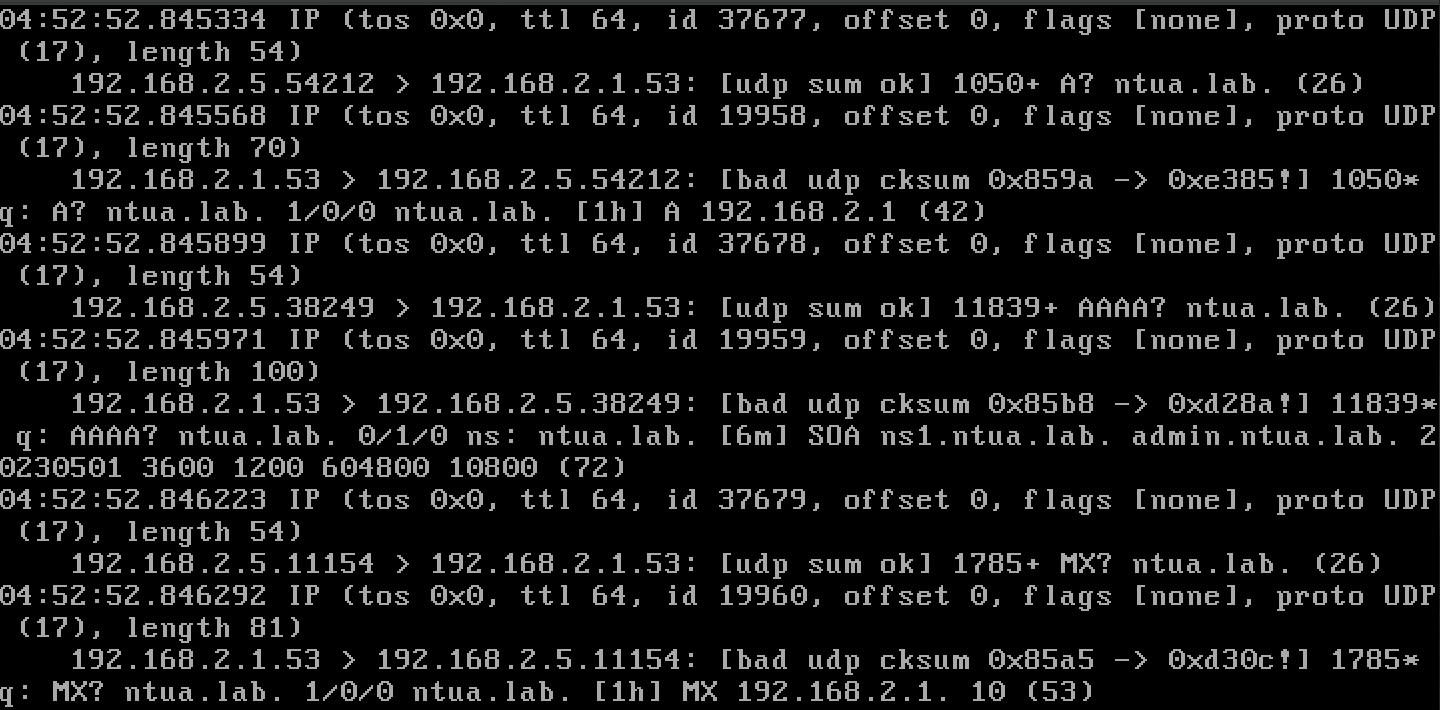
Το ίδιο περιεχόμενο που είχε πριν διαγραφεί.

***2.26***

***2.27***

Βλέπουμε πως έχει την 192.168.2.1.

***2.28***

Ναι, μέρος της οποίας φαίνεται παρακάτω:

***2.29***

To UDP.

***2.30***

Χρησιμοποιήθηκε η θύρα 53 από τον DNS server και μία δυναμική κάθε φορά από τον πελάτη.

***2.31***

Η θύρα 53.

***2.32***

***2.33***

Εκτελούμε στο PC1 “**host ns1**” και παίρνουμε ως απάντηση το 192.168.2.1.

***2.34***

6 μηνύματα.

***2.35***

Το πρώτο αίτημα είναι Α? για το “ns1.ntua.lab.”, ενώ το 2ο και 3ο αντίστοιχα είναι ΑΑΑΑ? και MX? αντίστοιχα για το ίδιο όνομα.

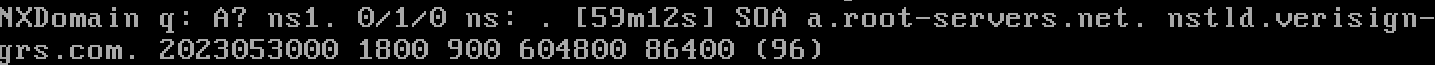
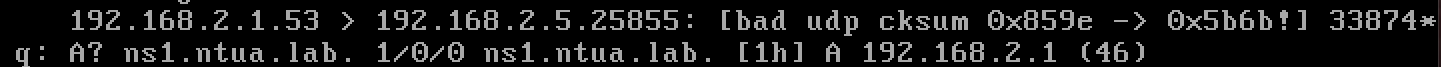
***2.36***

Σε όλες λήφθηκαν απαντήσεις. Ωστόσο, μόνο στο Α? έχουμε ως απάντηση αυτό που όντως ψάχναμε (screenshot 1), ενώ τα επόμενα 2 ερωτήματα λαμβάνουν αυτό που βλέπουμε στα screenshot 2 και 3 ως απάντηση.

***2.37***

Εκτελούμε στο PC1 “**drill ns1**” και “**drill ns1.ntua.lab**”.

***2.38***

Με την πρώτη εντολή έγινε ερώτηση για το “ns1.”, ενώ με τη δεύτερη για το “ns1.ntua.lab.”. Οι ερωτήσεις ήταν αμφότερες τύπου Α?, ενώ οι αντίστοιχες απαντήσεις φαίνονται παρακάτω:

***2.39***

Η χρήση του επιθέματος είναι απαραίτητη αν θέλουμε να κάνουμε το σωστό query.

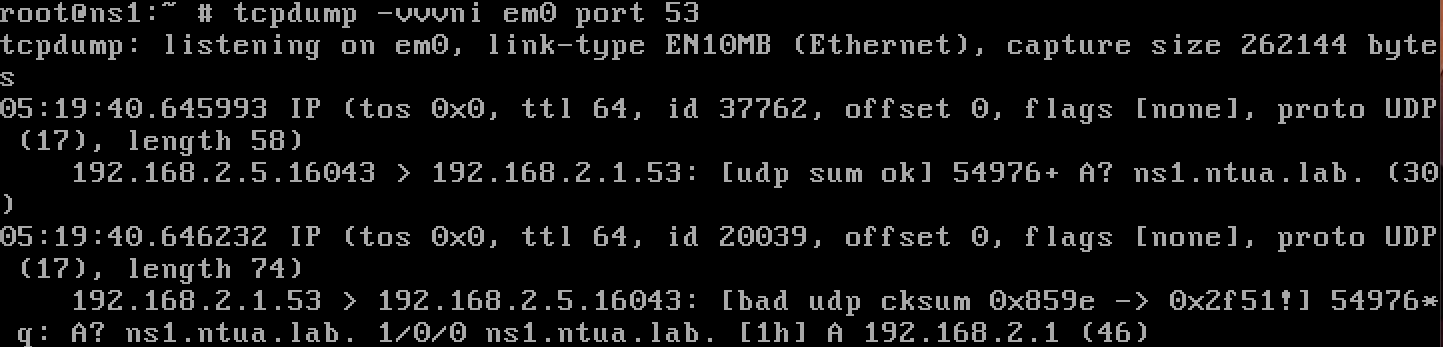
***2.40***

Δε φαίνεται να παράγονται DNS queries.

***2.41***

Εκτελούμε το ping.

***2.42***

Ανταλλάχθηκαν συνολικά 2 μηνύματα, ένα query και ένα response, τα οποία αφορούσαν A? ερωτήματα προς τον DNS server για το “ns1.ntua.lab.”.

***2.43***

Εκτελούμε στο PC1 “**ping -c 1 ns1**” 3 φορές. Παράχθηκαν 3 A? ερωτήματα για το “ns1.ntua.lab.” και οι αντίστοιχες απαντήσεις.

***2.44***

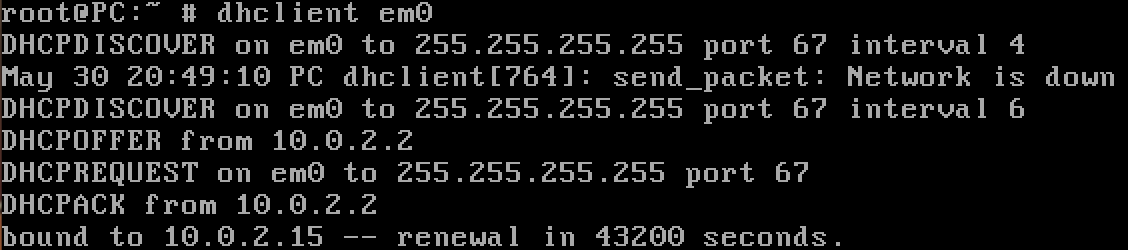
Δεν αποθηκεύονται οι απαντήσεις του DNS server στο PC1.

**Άσκηση 3: Εγκατάσταση εξυπηρετητή HTTP**

***1***

Η em0 είναι σε NAT.

***2***

“**dhclient em0**”.

***3***

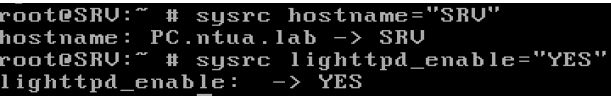
Μπορούμε να κάνουμε ping κατευθείαν.

***4***

Εγκαθιστούμε το πακέτο.

***5***

Εισάγουμε το SRV1 και εκτελούμε “**ifconfig em0 192.168.2.3/28**”.

***3.1***

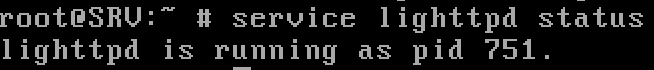
***3.2***

Εκτελούμε “**mkdir /usr/local/www/data**”.

***3.3***

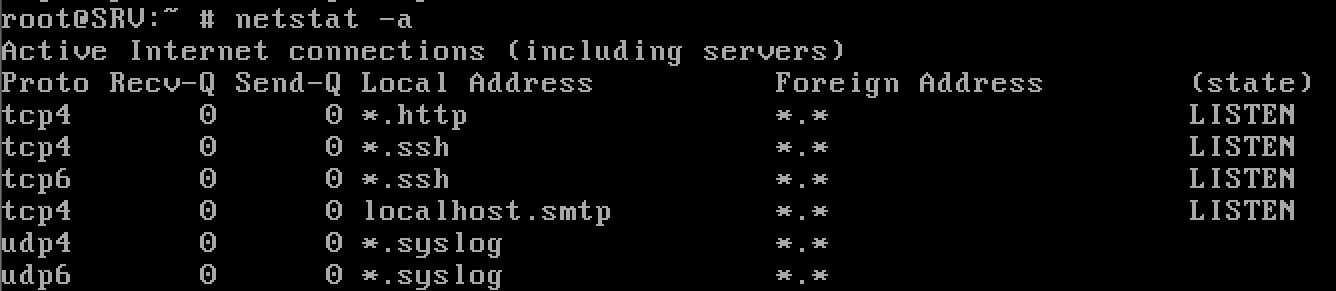
***3.4***

Κάνουμε επανεκκίνηση.

***3.5***

***3.6***

Με “**netstat -a**” βλέπουμε πως τρέχουν 2 υπηρεσίες http, μία για tcp4 και μία για tcp6.

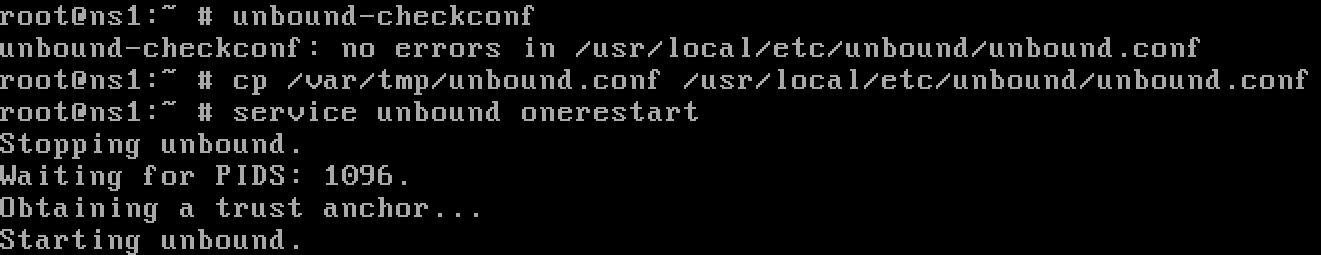


***3.7***

“**ifconfig em0 192.168.2.3/28**”.

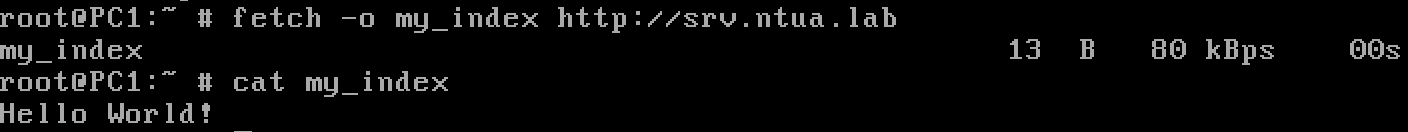
***3.8***

***3.9***

***3.10***

***3.11***

Εκτελούμε στο SRV “**tcpdump -vvvni em0**”.

***3.12***

***3.13***

Χρησιμοποιήθηκε το πρωτόκολλο μεταφοράς TCP, και ο http server ακούει στη θύρα 80.

***3.14***

Στο /root/my\_index.

**Άσκηση 4: Εγκατάσταση ιδιωτικού δρομολογητή και Firewall**

***4.1***

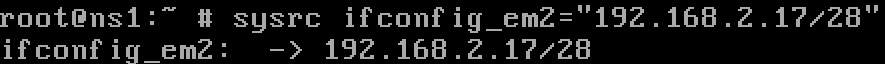
Εκτελούμε “**sysrc gateway\_enable=”YES”** ”

***4.2***

Ενεργοποιούμε το firewall, ωστόσο δεν έχουμε φορτώσει το ipfw module.

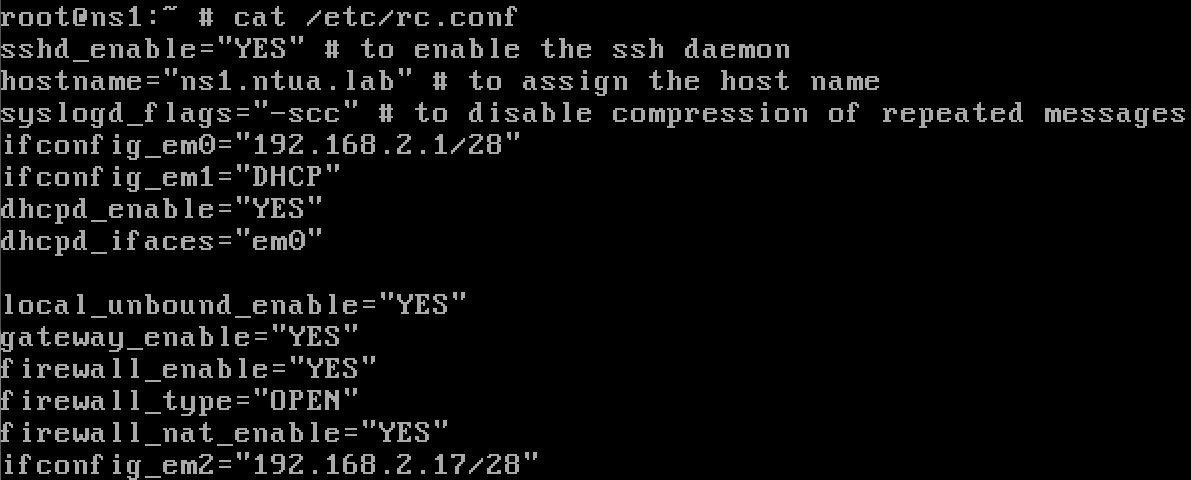
***4.3***

***4.4***

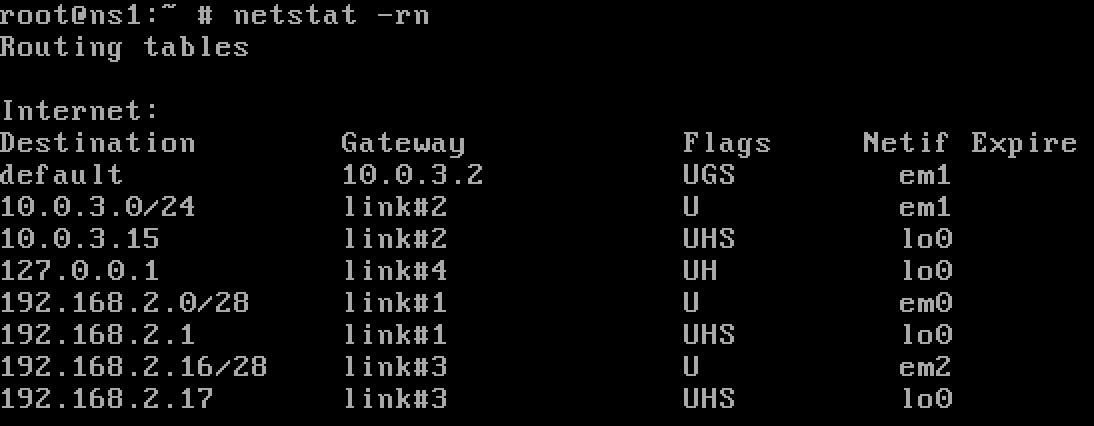
***4.5***

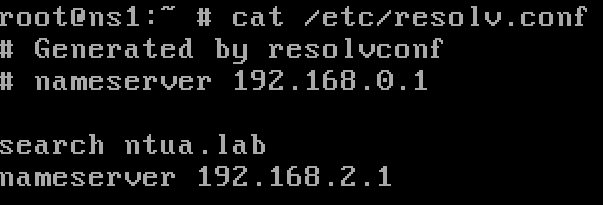
***4.6***

Επιβεβαιώνουμε τις τιμές.



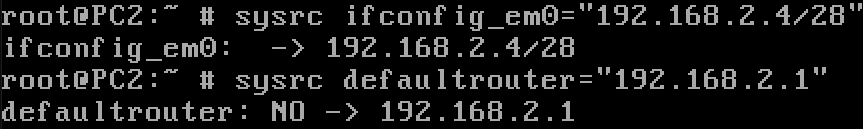
***4.7***

Κάνουμε reboot το NS1 και βλέπουμε πως υπάρχει κανονικά η προκαθορισμένη πύλη:

***4.8***

***4.9***

Εκτελούμε στο PC1 “**sysrc ifconfig\_em0=”DHCP”** ” και “**service netif restart**”.

***4.10***

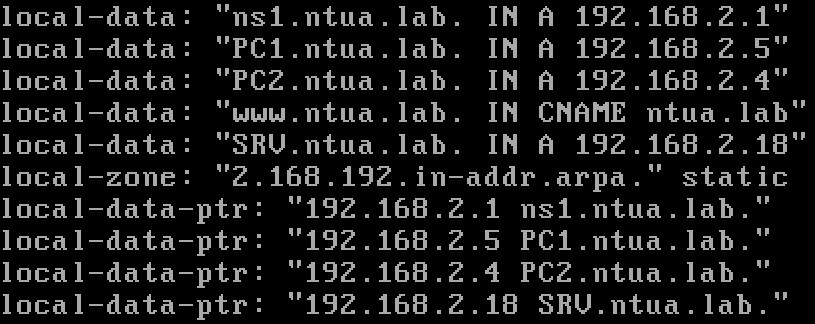
***4.11***

Εκτελούμε στο PC2 “**service netif restart**” και “**service routing restart**”.

***4.12***

Εκτελούμε στο SRV “**sysrc ifconfig\_em0=“192.168.2.18/28**”, “**sysrc defaultrouter=”192.168.2.17**”, “**service netif restart**” και “**service routing restart**”.

***4.13***

Τροποποιούμε κατάλληλα το αρχείο.

***4.14***

Ναι.

***4.15***

***4.16***

Όχι.

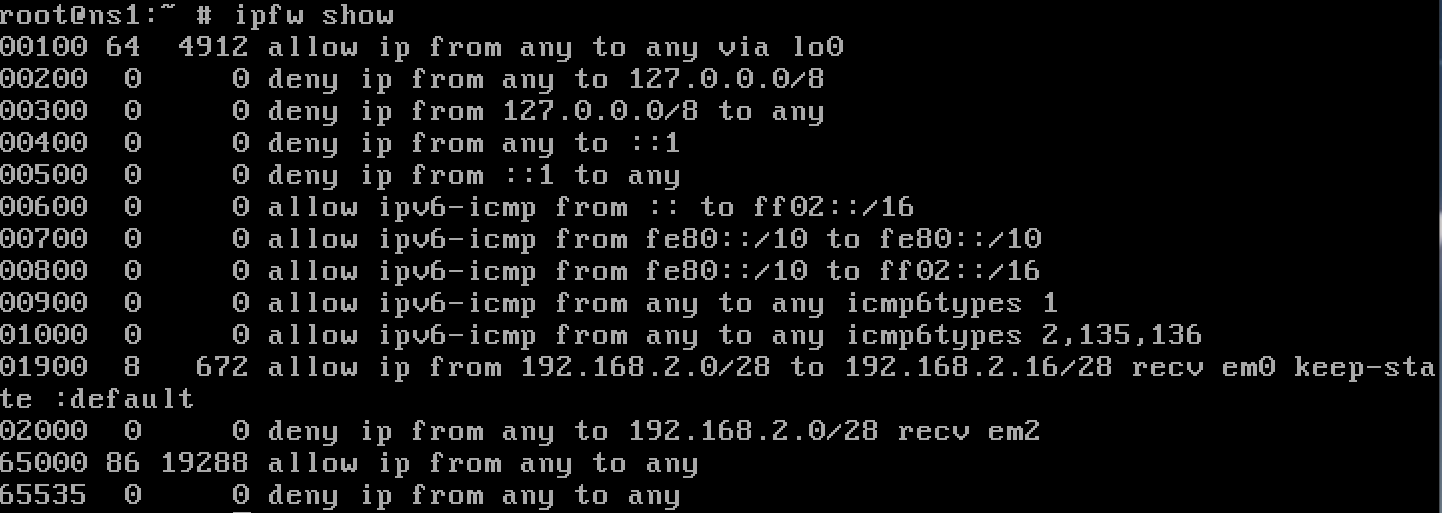
***4.17***

Εκτελούμε “**ipfw add 1900 allow all from 192.168.2.0/28 to 192.168.2.16/28 recv em0 keep-state**”.

***4.18***

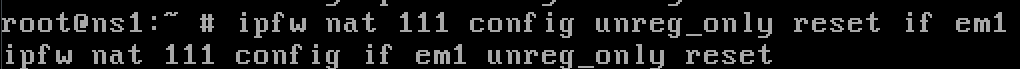
Ναι, τώρα μπορούμε ενώ πριν τον κανόνα όχι.

***4.19***

Ναι, καθώς πιάνεται από τον 1ο κανόνα που επιτρέπει οποιαδήποτε κίνηση από την loopback.

***4.20***

Όχι.

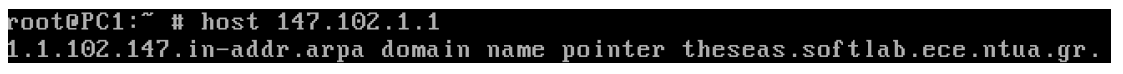
***4.21***

***4.22***

***4.23***

Ναι.

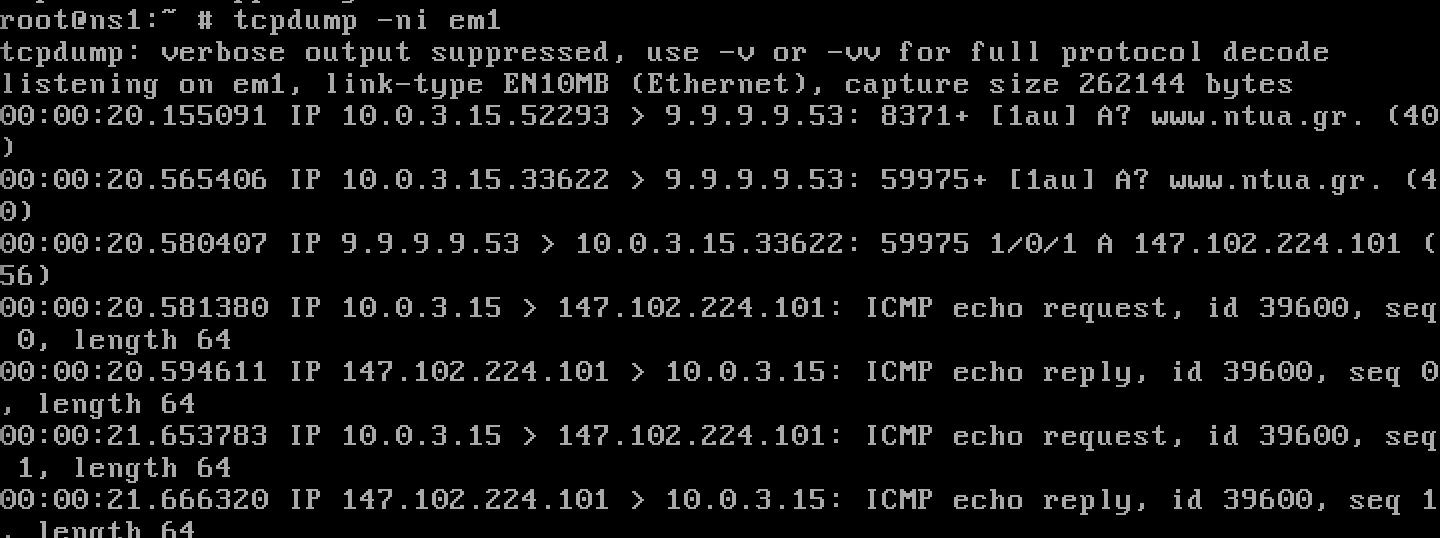
***4.24***

Η 147.102.1.1 αντιστοιχεί στην theseas.softlab.ece.ntua.gr

***4.25***

“**tcpdump -ni em1**”.

***4.26***

Με την “10.0.3.15”.

***4.27***

Η “147.102.224.101”.

***4.28***

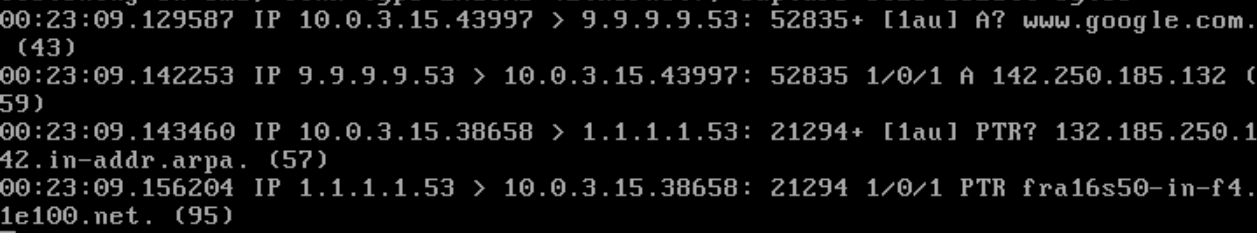
Προς τον “9.9.9.9”.

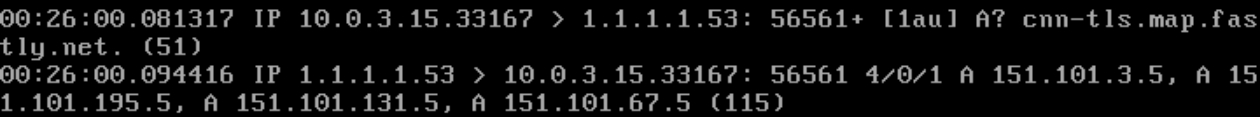
***4.29***

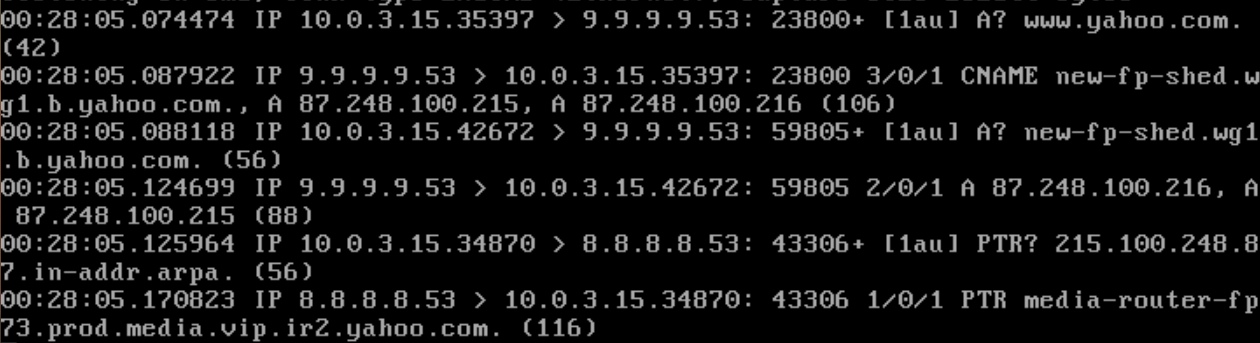
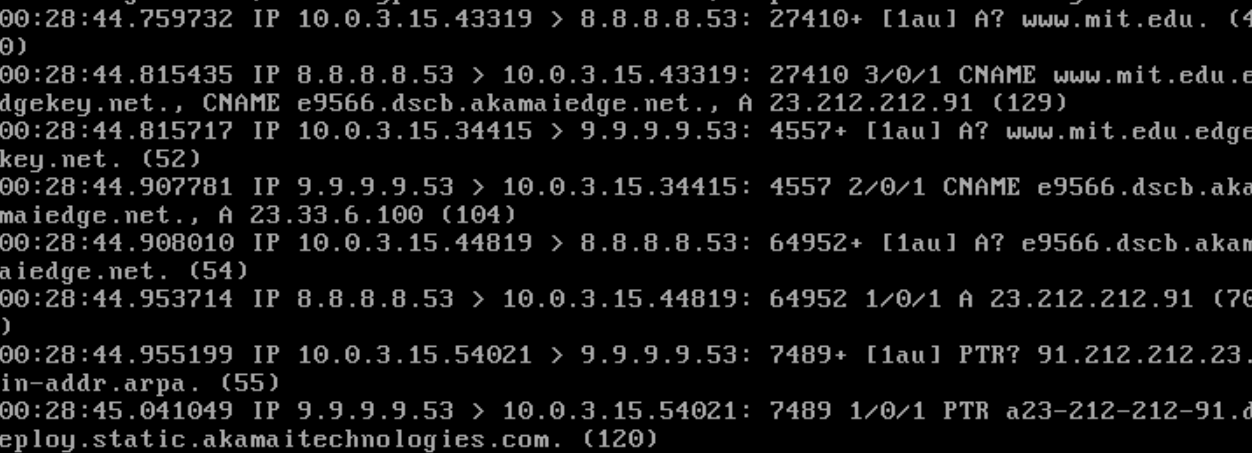
Εκτελούμε “**tcpdump -ni em1 port 53**”.

***4.30***

Παρατηρούμε τα εξής:

* www.google.com → 9.9.9.9
* www.cnn.com → 1.1.1.1, αλλά κάνει και στο 8.8.8.8



* www.yahoo.com → 9.9.9.9, αλλά κάνει και στο 8.8.8.8
* www.mit.edu → 8.8.8.8, αλλά στη συνέχεια και στο 9.9.9.9

Παρατηρούμε ότι αρχικά γίνονται DNS queries στο 8.8.8.8, ο οποίος και απαντάει στο NS1 με το Canonical Name, για το οποίο στη συνέχεια ρωτάμε τον 1.1.1.1, δίνοντας αυτή την απάντηση στο PC1. Χρησιμοποιούνται επομένως, οι DNS servers που ορίσαμε στην αρχή στο αρχείο unbound.conf, χωρίς κάποια σειρά.

***4.31***

Εκτελούμε στο NS1 “**tcpdump -ni em0 port 53**”.

***4.32***

Είναι “courses.cn.ece.ntua.gr”.

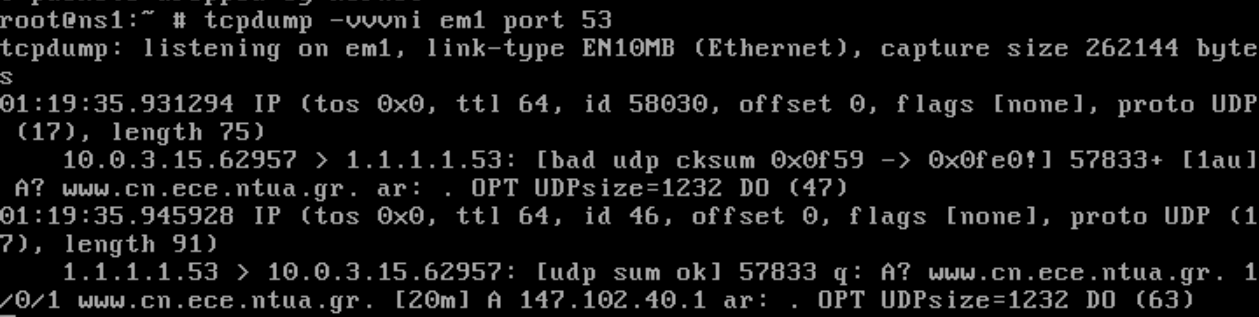
***4.33***

Το PC1 έκανε A? Query, δηλαδή ζήτησε την IP για το courses.cn.ntua.gr, ενώ ο NS1 του απάντησε πέραν της ζητούμενης IP με το canonical name του courses.cn.ntua.gr. Ο NS1 από την άλλη, έκανε A? Query στον DNS server, από όπου και έλαβε το CNAME του courses.cn.ntua.gr, οπότε και στη συνέχεια έκανε 2ο A? Query σε άλλον DNS server

***4.34***

Εκτελούμε “**tcpdump -vvvni em1 port 53**”.

***4.35***

Παρατηρούμε 2 ερωτήματα DNS, ενώ η χρονική διάρκεια ισχύος είναι 1200 sec, το οποίο φαίνεται από την εντολή “**drill www.cn.ece.ntua.gr**”, καθώς την πρώτη φορά η τιμή ήταν 1200, ενώ λίγα δευτερόλεπτα μετά 1181.

***4.36***

Παράγονται DNS A? Queries από τον PC1 στο NS1. Όσον αφορά τη χρονική διάρκεια των απαντήσεων βλέπουμε πως βαίνει μειούμενη.

***4.37***

Συμπεραίνουμε πως αποθηκεύονται στον NS1 για 20 λεπτά.

***4.38***

Ναι μπορούμε.

***4.39***

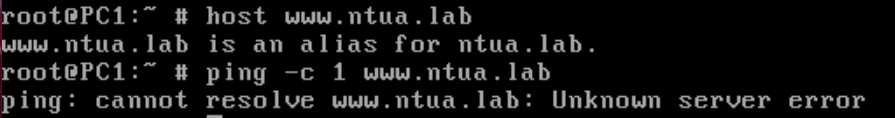
Όχι, καθώς αποτυγχάνει η dns αναζήτηση για το όνομα www.ntua.gr.

***4.40***

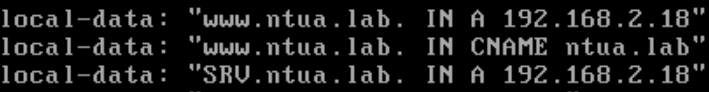
***4.41***

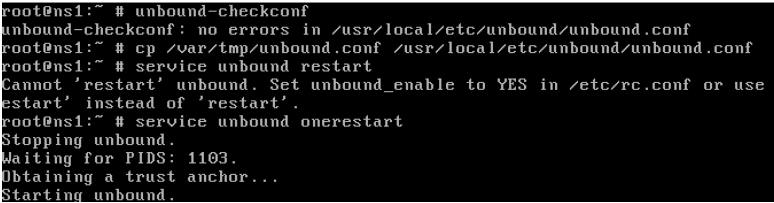
Ναι.

***4.42***

Με την εντολή host βλέπουμε μόνο το alias, ενώ και το Ping αποτυγχάνει.

***4.43***

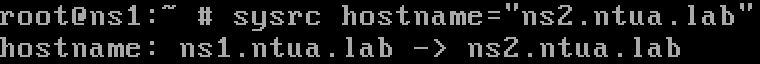
Πραγματοποιούμε την αλλαγή:

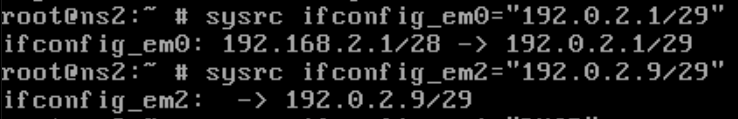


***4.44***

Απαντάει ο SRV.

**Άσκηση 5: Εγκατάσταση δημόσιου δρομολογητή και DNS**

***5.1***

***5.2***

***5.3***

***5.4***

***5.5***

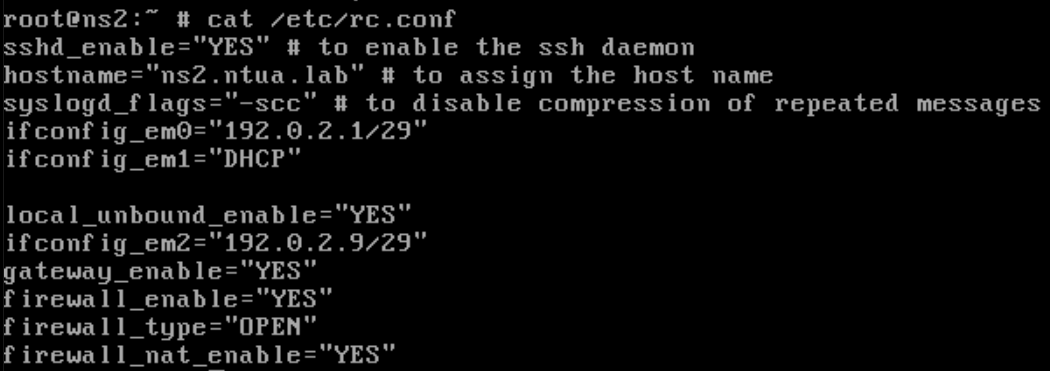
***5.6***

***5.7***

***5.8***

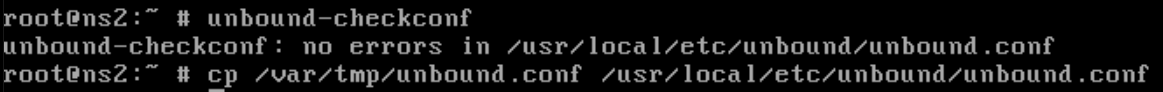
Διαγράφουμε τα παρακάτω:

***5.9***

Βλέπουμε παρακάτω την εντολή “**local\_unbound\_enable=“YES”** ”.

***5.10***

Κάνουμε τις αλλαγές και το αντιγράφουμε.

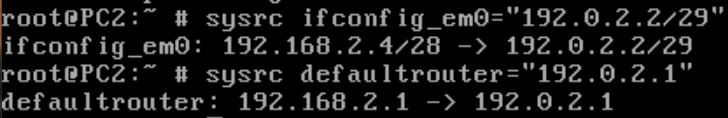


***5.11***

Υπάρχει ως προκαθορισμένη διαδρομή η 10.0.3.2.

***5.12***

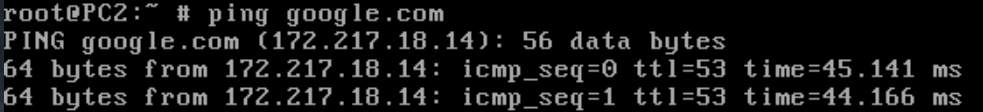
***5.13***

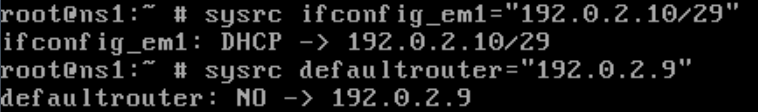
***5.14***

***5.15***

Εκτελούμε τις οδηγίες.

***5.16***

Ναι.

***5.17***

***5.18***

Κάνουμε τα ζητούμενα.

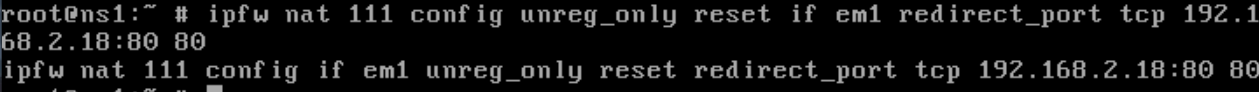
***5.19***

Μπορούμε από αμφότερα, και βλέπουμε να αυξάνεται ο μετρητής του κανόνα που αφορά τον πίνακα 111, άρα παραμένει σε λειτουργία όταν χρησιμοποιούμε και τα 2 pings.

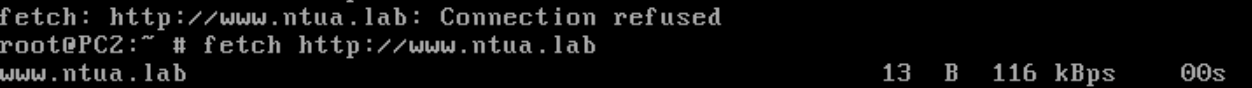
***5.20***

Στο PC1 επιστρέφεται η 192.168.2.18, ενώ στο PC2 η 192.0.2.10.

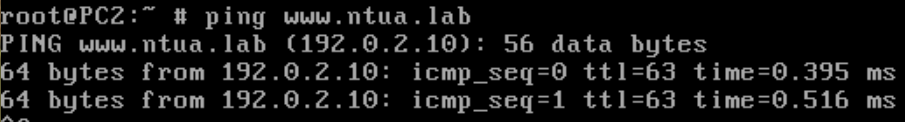
***5.21***

***5.22***

***5.23***

Ναι, πλέον μπορούμε.

***5.24***

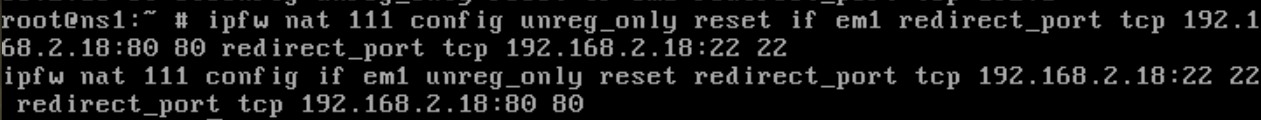
Ναι μπορούμε και απαντάει το 192.0.2.10, δηλαδή το NS1.

***5.25***

Απαντά το SRV.

***5.26***

Στο NS1, αφού είδαμε πως για τον PC2 το www.ntua.lab είναι στην 192.0.2.10, δηλαδή στο NS1.

***5.27***

***5.28***

Μπορούμε και το επιβεβαιώνουμε από το prompt: