

LAB-12 (DHCP & DNS)

Όνοματεπώνυμο : Νίκος Μπέλλος (el18183)	Όνομα PC : BELLOS-DELL-G3
Ομάδα : 3	Ημερομηνία : 12/06/2022

Άσκηση 1: Εγκατάσταση DHCP server

1. `tcpdump -i em0 -e -nvvv`
2. `dhclient em0`
3. PC1 : DHCP Request
NS1 : DHCP Reply
PC1 : DHCP Request
NS1 : ICMP Echo Request
NS1 : DHCP Reply
4. DHCP discover
DHCP offer
DHCP request
DHCP ACK
5. Η 192.168.2.5, με διεύθυνση εξυπηρετητή την 192.168.2.1
6. Μετά από 60 sec
7. To UDP
8. Οι 67 και 68
9. DHCP discover : 0.0.0.0 → 255.255.255.255
DHCP offer : 192.168.2.1 → 192.168.2.5
DHCP request : 192.168.2.5 → 192.168.2.1
DHCP ACK : 192.168.2.1 → 192.168.2.5
10. DHCP Request : 08:00:27:73:0C:EE → FF:FF:FF:FF:FF:FF
DHCP Reply : 08:00:27:FD:48:D7 → 08:00:27:73:0C:EE
11. Χρησιμοποιεί τη διεύθυνση 0.0.0.0
12. Ναι παρατηρούμε, γιατί προσπαθεί να εντοπίσει αν η διεύθυνση που πάει να διαθέσει χρησιμοποιείται από κάποιο άλλο μηχάνημα
13. Ναι παρατηρούμε ICMP. Τα παράγει ο NS1 για να ελέγξει αν η εγγραφή ισχύει ακόμα
14. Για να διαπιστώσει αν η ίδια IP έχει δοθεί και σε άλλο μηχάνημα
15. Δεν παράχθηκε ανταλλαγή ICMP
16. Διάρκει 120 sec (χωρίς ανανέωση)
17. Υπάρχει το πεδίο Requested-IP που περιέχει την διεύθυνση IP που επιλέγει το PC1
18. Περιέχει την Client IP address (πριν υπήρχε η Client MAC address)
19. Για ένδειξη κατειλημμένης διεύθυνσης
20. `/var/db/dhcpd/dhcpd.leases`

21. Κάθε 60 sec
22. Ώρα έναρξης
Ώρα λήξης
Κατάσταση
Client
23. /var/db/dhclient.leases.em0
24. Διεπαφή
Δρομολογητής
DHCP server
Static address
Subnet mask
Ώρα έναρξης
Ώρα λήξης
Ώρα ανανέωσης
25. 45 sec
26. 11 παραμέτρους
27. (3 παραμέτρους)
Subnet-mask
BR
Default Gateway
28. `tcpdump -i em0 -e -vvv`
29. `service isc-dhcpd stop`
30. Μετά από 2 λεπτά χάνεται η διεύθυνση
31. Η διεύθυνση του PC1 είναι και πάλι ίδια με πριν
32. Απέχουν 10 δεύτερα περίπου
33. Δεν λαμβάνει απάντηση
34. Στη διεύθυνση broadcast (255.255.255.255)
35. Θεωρεί ότι ο DHCP server έχει αλλάξει και κάνει προσπάθεια για εύρεση νέου (νέας διεύθυνσης δηλαδή)
36. MAC και IPv4 του προηγούμενου DHCP server.
Η διεύθυνση πηγής πλέον γίνεται και πάλι 0.0.0.0
37. Για να διαπιστώσει αν η διεύθυνση αυτή (που υπάρχει στα leases) έχει αποδοθεί κάπου αλλού
38. Διαγράφονται
39. Για να μπορεί να ενημερώσει τόσο ο client το server όσο και το αντίστροφο για τοιχόν αλλαγές

Άσκηση 2: Εγκατάσταση εξυπηρετητή DNS

1. `vi /etc/hosts`
192.168.2.5 PC1 PC1.ntua.lab
192.168.2.6 PC2 PC2.ntua.lab
2. Η χρήση κεφαλαίων δεν επηρεάζει το ping. Επίσης το PC2.ntua.lab δεν απαντάει

3. `vi /etc/hosts`
192.168.2.5 PC1 PC1.ntua.lab
192.168.2.6 PC2 PC2.ntua.lab
Ναι, απαντάει
4. 'Host Name lookup failure'
5. `vi /var/tmp/unbound.conf`
local-data: "PC1.ntua.lab IN A 192.168.2.5"
local-data: "PC2.ntua.lab IN A 192.168.2.6"
6. local-data-ptr: "192.168.2.5 PC1.ntua.lab"
local-data-ptr: "192.168.2.6 PC2.ntua.lab"
7. `cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf`
`service unbound restart`
8. `tcpdump -i em0 -e -vvv`
9. `ifconfig em0 delete`
`dhclient em0`
10. Την 192.168.2.5/28
11. Domain-Name
Domain-Name-Server
12. Ναι έχει δημιουργηθεί αρχείο /etc/resolv.conf στο PC1 (ίδιο με αυτό του DNS server)
Περιεχόμενο :
search ntua.lab
nameserver 192.168.2.1
13. `host 192.168.2.5` → PC1.ntua.lab
14. `host NS1` → 192.168.2.1
15. Ναι
16. `ifconfig em0 delete`
`dhclient em0`
17. 192.168.2.6/28
18. Ναι μπορούμε
19. Από το DNS (η εγγραφή στο /etc/hosts έχει διαγραφεί στο ερώτημα 2.4)
20. Όχι, δεν μπορούμε (γιατί το PC1 στέλνει απάντηση σε λάθος διεύθυνση)
21. Το πρώτο μέρος που ψάχνει ο τοπικός επιλυτής (resolver) είναι οι εγγραφές στο /etc/hosts
22. `cat /etc/nsswitch.conf`
Ναι συμφωνεί (πρώτα ελέγχονται τα files και μετά ο dns)
23. `host PC2` → 192.168.2.6
24. Το host ρωτάει ακευθείαν τον DNS
25. `rm /etc/resolv.conf`
`resolvconf -u`
Είναι το ίδιο

26. `tcpdump -i em0 -e -vvv not port 67`
27. `host ntua.lab` → 192.168.2.1
28. Ναι
29. UDP
30. 53 και 56329
31. Η 53
32. `tcpdump -i em0 -e -vvv port 53`
33. `host ns1`
34. 6 μηνύματα ανταλλάχθηκαν
35. Για το όνομα ns1.ntua.lab
Ερωτήματα τύπου : A, AAAA, MX
36. Και στα 3
37. `drill ns1` , `drill ns1.ntua.lab`
38. Για τα ονόματα ns1, ns1.ntua.lab
Απάντηση υπήρχε για το ns1.ntua.lab
39. Προστίθεται αυτόματα στις εγγραφές (δηλαδή αν γίνει ερώτηση για το PC1 θα ψάξει να βρεί την εγγραφή για το PC1.ntua.lab διότι το search path είναι το ntua.lab (στο /etc/resolv.conf)
40. `ping localhost` , `ping pc1` → Παράγονται μόνο στο localhost γιατί το PC1 περιέχεται στο αρχείο /etc/hosts
41. `ping -c 1 ns1`
42. Παράχθηκαν 2 μηνύματα άνα ping. Ήταν ερωτήματα που αφορούσαν την εγγραφή τύπου A
43. Πλέον παράγεται 1 κάθε φορά
44. Δεν αποθηκεύονται στο PC1 για κάθε ερώτημα που γίνεται προς τον DNS

Άσκηση 3: Εγκατάσταση εξυπηρετητή HTTP

1. `vi /etc/rc.conf`
hostname = "SRV"
lighttpd_enable="YES"
2. `mkdir /usr/local/www/data`
3. `echo "Hello World!" > /usr/local/www/data/index.html`
4. `reboot`
`rm /etc/resolv.conf`
5. `service -e` (βλέπουμε τις ενεργές διαδικασίες)
6. `netstat -a` (είναι ενεργή στη θύρα 80)
7. `ifconfig em0 192.168.2.3/28`
8. NS1
`vi /var/tmp/unbound.conf`

- local-data: "SRV.ntua.lab IN A 192.168.2.3"
- 9. `vi /var/tmp/unbound.conf`
 - local-data-ptr: "192.168.2.3 SRV.ntua.lab"
- 10. `cp /var/tmp/unbound.conf /usr/local/etc/unbound/unbound.conf`
`service unbound restart`
- 11. `tcpdump -i em0 -n -e -vvv`
- 12. PC1
`fetch http://srv.ntua.lab`
- 13. Χρησιμοποιήθηκε το TCP.
Ο εξυπηρετητής ακούει στην πόρτα 80 (default http port)
- 14. Στο αρχείο 'srv.ntua.lab'

Άσκηση 4: Εγκατάσταση ιδιωτικού δρομολογητή και Firewall

1. `sysrc gateway_enable="YES"`
2. `sysrc firewall_enable="YES"`
3. `sysrc firewall_type="open"`
4. `sysrc firewall_nat_enable="YES"`
5. `sysrc ifconfig_em2="192.168.2.17/28"`
6. `cat /etc/rc.conf`
7. `route add default 192.168.2.4`
8. `vi /etc/resolv.conf`
 - search ntua.lab
 - nameserver 192.168.2.1
9. PC1
`vi /etc/rc.conf`
 - ifconfig_em0="DHCP"`service netif restart`
10. PC2
`vi /etc/rc.conf`
 - ifconfig_em0="192.168.2.4/28"
 - defaultrouter="192.168.2.1"
11. `service netif restart`
`service routing restart`
`touch /etc/resolv.conf`
`vi /etc/resolv.conf`
 - search ntua.lab
 - nameserver 192.168.2.1
12. SRV
`vi /etc/rc.conf`
 - ifconfig_em0="192.168.2.18/28"

- defaultrouter="192.168.2.17"

```
service netif restart
```

```
service routing restart
```

13. NS1

```
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 PC2.ntua.lab"

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

```
service unbound restart
```

14. Ναι, μπορούμε.

(Γιατί ο SRV έχει default route και ο NS1 λειτουργεί πλέον και σαν Router)

15. NS1

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

16. Όχι

```
17. ipfw add 1900 allow all from 192.168.2.0/28 to 192.168.2.16/28 in via em0 keep-state
```

18. Ναι μπορούμε

19. Ναι μπορούμε

20. Όχι

```
21. ipfw nat 111 config ip em1 reset
```

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

23. Ναι μπορούμε

```
24. host 147.102.1.1 → theseas.softlab.ece.ntua.gr
```

```
25. tcpdump -i em1 -n -e -vvv
```

```
26. ping -c 2 www.ntua.gr
```

Με την 10.0.3.15

27. Η 147.102.224.101

28. Προς τον NS1

```
29. tcpdump -i em1 -n port 53
```

30. Είναι κάθε φορά διαφορετικός

```
31. tcpdump -i em0 -n port 53
```

32. PC1

```
ping -c 1 courses.cn.ntua.gr
```

CNAME : courses.cn.ece.ntua.gr

33. Έκανε ερώτημα τύπου A

Έλαβε απάντηση τύπου A, CNAME

```
34. tcpdump -i em1 -e -nvvv port 53
```

35. PC1

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

→ 1 ερώτημα DNS. Χρονική διάρκεια ισχύος 20 λεπτά

36. NS1

```
tcpdump -i em0 -e -nvvv port 53
```

PC1

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

Ναι παράγονται. Η χρονική ισχύς μειώνεται συνεχώς και σε κάθε request στέλνεται καινούργιο μήνυμα

37. Ο NS1 αποθηκεύει προσωρινά τις απαντήσεις που λαμβάνει από άλλους εξυπηρετητές DNS λόγω της χρήσης cache που διαθέτει

38. SRV

```
ping -c 1 147.102.224.101
```

Ναι μπορούμε

39. SRV

```
ping ww.ntua.gr
```

Όχι, διότι δεν έχει οριστεί DNS server

40. SRV

```
vi /etc/resolv.conf
```

- nameserver 192.168.2.17

41. Ναι μπορούμε

42. PC1

```
host www.ntua.lab
```

Δεν θα είναι επιτυχημένο το ping γιατί δεν έχει οριστεί πουθενά ως εγγραφή το alias www.ntua.lab

43. NS1

```
vi /var/tmp/unbound.conf
```

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

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

```
service unbound restart
```

44. Απαντάει ο SRV όπως ήταν αναμενόμενο

Άσκηση 5: Εγκατάσταση δημόσιου δρομολογητή και DNS

1.

```
sysrc hostname="ns2.ntua.lab"
```

2.

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



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

3.

```
sysrc ifconfig_em1="DHCP"
```

4.

```
sysrc gateway_enable="YES"
```

5.

```
sysrc firewall_enable="YES"
```

6.

```
sysrc firewall_type="open"
```

7.

```
sysrc firewall_nat_enable="YES"
```

8.

```
vi /etc/rc.conf
```


(remove)

```
dhcpd_enable="YES"
```

(remove) dhcpd_ifaces

9. - dnsd_enable="YES"

10. NS2

```
vi /var/tmp/unbound.conf
```

- access-control 192.0.2.0/24 allow

- local-zone: "ntua.lab" redirect

- local-data: "ntua.lab. IN A 192.0.2.10"

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

```
service unbound restart
```

11. Υπάρχει default διαδρομή προς το 10.0.3.2

12.

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

13.

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

14. PC2

```
vi /etc/rc.conf
```

- ifconfig_em0="192.0.2.2/29"

- defaultrouter="192.0.2.1"

15. PC2

```
service netif restart
```

```
service routing restart
```

```
vi /etc/resolv.conf
```

- search ntua.lab

- nameserver 192.0.2.1

16. Ναι μπορούμε

17. NS1

```
vi /etc/rc.conf
```

- ifconfig_em1="192.0.2.10/29"

- defaultrouter="192.0.2.9"

18.

```
service netif restart
```

```
service routing restart
```

19. Ναι μπορούμε

Λόγω του πίνακα 111 από την άσκηση 4

20. Για το PC1 επιστρέφει την : 192.168.2.18 (SRV)

Για το PC2 επιστρέφει την : 192.0.2.10 (NS1)

21. 'Connection Refused'

22. NS1

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

23. Ναι μπορούμε

24. Απαντάει ο NS1

25. Στο SRV

26. Με το NS1 γιατί δεν υπάρχει αντίστοιχος κανόνας forwarding στο firewall του NS1 για ssh πακέτα

27. NS1

```
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
```

28. Ναι μπορούμε (Μπορούμε να κάνουμε ένα απλό ifconfig και να κοιτάξουμε την ip)