

DNS Server (Debian 4) How To

Ας ξεκινήσουμε με την εγκατάσταση της υπηρεσίας **BIND**.

Σαν **root** δίνουμε την εντολή

```
apt-get install bind9
```

Εφόσον έχουμε εγκαταστήσει την υπηρεσία **BIND** θα απιόξουμε 2 καταλόγους ο ένας θα χρησιμοποιηθεί για τις **πρωτεύοντες ζώνες** (Master Zones) και ο άλλος για τις **δευτερεύοντες ζώνες** (Slave Zones).

Ας μετακινηθώ με στον κατάλογο της υπηρεσίας για να φιλέσουμε τους κατόχους και να
δύσουμε δικά μας

Σαν root:

```
cd /etc/bind/  
mkdir master  
mkdir slave  
chown -R root:bind master/ slave/  
chmod g+w slave
```

Όρανα φτιάχνουμε την πτώτη μας που τένον ζω νη

Σαν root επεξεργασόμαστε το αρχείο `/etc/bind/named.conf` με κάποιο editor π.χ vi και προσθέτουμε στο τέλος του αρχείου κάτι σαν το παρακάτω:

```
zone "mynet.local" {
    type master;
    file      "/etc/bind/master/zone.mynet.local";
};
```

Το παραπάνω είναι μια καταχώρηση ζώης Το **omynet.local** είναι το όνομα της ζώης το **type** ορίζει τον τύπο της ζώης πχ **Master**, **Slave** κ λ π και το **file** ορίζει την διδρομή όπου βρίσκεται το αρχείο της ζώης και όπου θα εγγραφεί τις εγγραφές της ζώης

Τα έγωνα παραδείγματα παραπάνω όπω στο **mynet.local** και το **zone.mynet.local** είναι παραδείγματα εσείς βάλτε στην θέση τους ένα όνομα ζώνης που προτιμάτε πχ. εσείς μπορεί να προτιμάτε αντί να έχετε η ζώνη σας **mynet.local** να έχετε **lab1.local, mynet.gr κ.λπ.**

Κατά το πρώτο φάσμα της κατάρτισης πρέπει να φέρουμε και το αρχείο εγγραφών της ζώνης **zone.mynet.local** που ορίσαμε στο **file** παραπάνω.

Σαν root επεξεργαστούμαστε το αρχείο `/etc/bind/master/zone.mynet.local` που έχουμε δηλώσει στο file παραπάνω και προσθέτουμε ό λατα παρακάτω:

```
$TTL      3600
@         IN      SOA      phoenix.mynet.local. nakalipos.yahoo.gr. (
                        2008050501      ;Serial
                        3600             ;Refresh
                        900              ;Retry
```

		3600000	;Expire
		3600)	;Minimum
	IN	NS	phoenix.mynet.local.
phoenix	IN	A	192.168.0.1
	IN	MX 10	phoenix.mynet.local.
pc-n1	IN	A	192.168.0.2
pc-n2	IN	A	192.168.0.3
pc-n3	IN	A	192.168.0.4
www	IN	CNAME	phoenix.mynet.local.

1. Το \$TTL δηλώνει πόση ώρα σε δευτερόλεπτα θα απαντήσει η απάντηση σε οποιαδήποτε άλλο nameserver τη ζητήσει. Γενικά οι nameservers απαντούν τα αποτελέσματα ανάλυσης προκειμένου να μην χάνουν χρόνο ψάχνοντας ξανά τα ίδια ερωτήματα. Ωστόσο όταν παύσει ο χρόνος που καθορίζεται στο TTL, η απάντηση θα ερωτηθεί πάλι και γίνεται νέαν έρωτηση

2. Το @ καθορίζει ότι υπάρχει κατοχή ονόματος χωρίς τελεία στο τέλος του προθέτει το όνομα της ζώνης: αν δεν βάλουμε στο παραπάνω παράδειγμα το **phoenix.mynet.local.** και βάλουμε μόνο την κατοχή **phoenix** θα έμπαινε μετά από την κατοχή **phoenix** αυτόματα το **.mynet.local.** και θα γινόταν **phoenix.mynet.local.** που είναι πρακτικά το ίδιο στο παραπάνω. Αν όμως προτιμάτε να κάνετε τις κατοχές της ζώνης με το χέρι απλά βάλτε μια τελεία στο τέλος. Προσχή όμως μην κάνετε καμία κατοχή με το πλήρες όνομα και ξαφάστε να βάλτε τελεία στο τέλος γιατί μπορεί να καταλήξει κάτι σαν αυτό **phoenix.mynet.local.mynet.local.** που είναι φασκάλως

3. Το IN καθορίζει ότι η ζώνη περιέχει δεδομένα internet.

4. Το SOA καθορίζει ότι ο συγκεκριμένος server δίνει τελικές (authoritative) απαντήσεις για τα περάσματα της ζώνης

5. Το **phoenix.mynet.local.** είναι το όνομα του server phoenix και το υπόλοιπο **.mynet.local** είναι το όνομα της ζώνης που εξηγήσαμε και παραπάνω.

6. Το **nakalipatos.yahoo.gr.** είναι ένα email (του διαχειριστή της ζώνης) αλλά αντί για **nakalipatos@yahoo.gr.** βάλουμε τελεία ανάμεσα στο **nakalipatos** και στο **yahoo** και στο τέλος γιατί εξηγήσαμε παραπάνω τι σημαίνει το πατάκι.

7. Το Serial είναι μια ακολουθία αριθμών να οποία δηλώνουν το έτος-μήνα-ήμερα-και αριθμό αλλαγών της δεδομένης μέρας του αρχείου για αυτό καθ'εφ'οκείνου θα κάνουμε μια αλλαγή στο αρχείο πρέπει να αλλάξουμε τους αριθμούς αυτών ανάλογα. Για παράδειγμα αν κάνουμε μια αλλαγή μέσα στην ίδια μέρα θα αλλάξουμε απλά στους αριθμούς στο τέλος της ακολουθίας

8. Το Refresh καθορίζει καθ'επ'οχρόνιο σε δευτερόλεπτα θα ελέγξει ο slave server για αλλαγές στην ζώνη του master server.

9. Το Retry καθορίζει καθ'επ'οχρόνιο σε δευτερόλεπτα θα προσπαθεί ο slave nameserver να ξανακάνει Refresh εφόσον δεν μπόρεσε να κάνει στον χρόνο που καθορίζεται από την τιμή του Refresh.

10. Το **Expire** καθορίζει σε πόσες μέρες θα σταματήσει να μας δίνει πληροφορίες ο slave server εφόσον ο πρωτεύων δεν ανταποκρίνεται.

11. Το **Minimum** καθορίζει όποτε έχουμε πάρει μια απάντηση για ένα όνομα που ζητήσαμε που μας λέει ότι δεν υπάρχει, η απάντηση αυτή θεωρείται έγκυρη για το χρονικό αυτό διάστημα (από ημερών στο nameserver που έκανε το ερώτημα). Μετά την παρέλευση αυτού του χρόνου θα γίνει νέο ερώτημα αν ζητηθεί.

12. Το **NS** δηλώνει τον **Name Server (DNS)** της ζώνης

13. Το **MX** δηλώνει τον **Mail Server της ζώνης**. Ακολουθείται από ένα αριθμό (πχ. 10, 20 κλπ) που δείχνει (σε περίπτωση που υπάρχουν περισσότερα από ένα mail servers) ποιός έχει τη μεγαλύτερη προτεραιότητα. Μεγαλύτερη θεωρείται η προτεραιότητα που αντιστοιχεί στο μικρότερο αριθμό.

14. Το **pc-n1** παραπάνω είναι μια καταχώρηση ονόματος μηχανήματος στη ζώνη το **IN** εξηγήσαμε τι είναι, το **A** είναι ο τύπος εγγραφής αληθινού μηχανήματος (**host record**) και το **192.168.0.2** η **IP** του μηχανήματος στην θέση του **pc-n1** **pc-n2** **IP** κ.λ.π βάλτε τις δικές σας τιμές

15. Η καταχώρηση **CNAME** παραπάνω δηλώνει ένα εναλλακτικό όνομα (**alias**) για ένα υπάρχον μηχανήμα για το οποίο υπάρχει εγγραφή τύπου **A**.

Από ημερών ετε αφού κατανοήσετε το αρχείο ρυθμίσεων της ζώνης και κάνετε τις δικές σας καταχωρήσεις.

Προθέστε σαν **root** την καταχώρηση **DNS Server** με κάποιο editor στο αρχείο **/etc/resolv.conf**:

```
domain          mynet.local
nameserver       127.0.0.1
```

Στην θέση του **mynet.local** βάλτε το όνομα της δικής σας ζώνης

Στην καταχώρηση **nameserver** η **IP 127.0.0.1** σημαίνει ότι ο **Name Server (DNS)** τρέχει στην **localhost** ενώ η θέση δηλαδή στο ίδιο το μηχανήμα στα μηχανήματα **Client** όπου πρέπει να βάλετε την διεύθυνση του **Name Server (DNS)** πχ **nameserver 192.168.0.1**.

Σαν **root** επανεκκινήστε την υπηρεσία **BIND**.

```
/etc/init.d/bind restart
```

Θεωρητικά τώρα ο **DNS Server** μας είναι έτοιμος

Μπορείτε να ελέγξετε με την εντολή **nslookup** αν ο **DNS Server** λειτουργεί:

```
nslookup και το όνομα του μηχανήματος
```

Πως Θα Φτιάξετε Ανάποδες Ζώνες Reverse DNS Zones

Οι ανάποδες ζώνες είναι το αντίθετο από της κανονικές ζώνες δηλαδή στις κανονικές ζώνες δίνουμε ένα όνομα μηχάνημα στο nslookup πχ nslookup **phoenix.mynet.local** και παίρνουμε την διεύθυνση IP του μηχανήματος πχ **192.168.0.1**, Στις ανάποδες όμως ζώνες γίνεται ακριβώς το αντίθετο δηλαδή **δίνουμε την διεύθυνση IP του μηχανήματος στο nslookup και παίρνουμε το όνομα του μηχανήματος της συγκεκριμένης διεύθυνσης IP**, για παράδειγμα nslookup **192.168.0.1** και θα πάρουμε ως απάντηση το **phoenix.mynet.local**.

Πως θα φτιάξετε τώρα ανάποδες ζώνες

Σαν root ετεξεργασείτε με κάποιο editor το **/etc/bind/named.conf** και προσθέστε τα παρακάτω:

```
zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/master/0.168.192.in-addr-arpa";
};
```

Το **0.168.192.-in-addr.arpa** είναι το όνομα της ανάποδης ζώνης με την ανάποδη διεύθυνση της διεύθυνσης IP και το **.in-addr.arpa** είναι απαραίτητο να μπει στο τέλος για να δηλώσει ότι είναι ανάποδη ζώνη

Θα δημιουργήσουμε και θα ετεξεργαστούμε σαν root τώρα με κάποιο editor το αρχείο ανάποδης ζώνης **/etc/bind/master/0.168.192.in-addr-arpa** που ορίσαμε στο αρχείο **/etc/bind/named.conf**:

```
vi /etc/bind/master/0.168.192.in-addr-arpa
```

Κα να προσθέσουμε τα παρακάτω:

```
$TTL      3600
@         IN      SOA      phoenix.mynet.local. nakaliptos.yahoo.gr. (
                                2008050501      ; Serial
                                3600              ; Refresh
                                900               ; Retry
                                3600000          ; Expire
                                3600 )           ; Minimum
1         IN      NS       phoenix.mynet.local
1         IN      A        phoenix.mynet.local
1         IN      MX       phoenix.mynet.local
2         IN      A        pc-n1
3         IN      A        pc-n2
4         IN      A        pc-n3
```

Εδώ το @ έχει τον ρόλο που εξηγήσαμε παραπάνω μόνο που αντί να συμπληρώνει το όνομα της ζώνης συμπληρώνει στο τέλος τον αριθμό του **0.168.192.in-addr-arpa**, για παράδειγμα στην κατωίτηση παραπάνω **1 IN A phoenix.mynet.local** δίνει από το 1 θα μπει και το 192.168.0. και θα γίνει **192.168.0.1**

Αποθηκεύστε αφού κατανοήσετε το αρχείο ρυθμίσεων της ζώνης και κάνετε τις δικές σας καταχωρήσεις.

Κα σαν root επανεκκινήστε την υπηρεσία BIND.

```
/etc/init.d/bind restart
```

Μπορείτε να ελέγξετε τώρα με την εντολή `nslookup` αν η ανάποδη ζώνη λειτουργεί:

```
nslookup και την διεύθυνση IP του μηχανήματος
```

Πως να κάνετε μεταφορές ζωνών (Zone Transfers) από πρωτεύοντες Name Servers (DNS)

Σαν `root` στο μηχάνημα που θέλετε να κάνετε την μεταφορά ζώνης από τον **πρωτεύον** Name Server επεξεργαστείτε με κάποιο `editor` το αρχείο `/etc/bind/named.conf` και προσθέστε τα παρακάτω:

```
zone "mynet.local" {
    type slave;
    file "/etc/bind/slave/zone.mynet.local";
    masters {
        192.168.0.1;
    };
};
```

Το `mynet.local` είναι το όνομα της ζώνης του πρωτεύοντος το οποίο θέλετε να κάνετε μεταφορά στον δευτερεύον Name Server.

Εδώ θα πρέπει να παρατηρήσετε ότι ο τύπος ζώνης είναι `Slave` και το `masters` όπου δηλώνουμε την διεύθυνση IP του πρωτεύοντος nameserver.

Καθώς ήταν για την ασφαλεία του πρωτεύοντος nameserver να περιορίσετε παλαιές **διευθύνσεις IP δευτερεύον nameserver** θα επιτρέπονται να κάνουν μεταφορά ζώνης **ναλλιώς οποιοσδήποτε nameserver θα μπορεί να κάνει μεταφορά!**

Αν θέλετε να κάνετε την παραπάνω ρύθμιση επεξεργαστείτε σαν `root` στον **πρωτεύον** nameserver το αρχείο `/etc/bind/named.conf.options` και προσθέστε στα `options` το παρακάτω:

```
allow-transfer {
    127.0.0.1; και την διεύθυνση IP του δευτερεύον Name server με ;
};
```

Έτσι τα σαν `root` κάντε επανεκκίνηση την υπηρεσία **BIND** στο **πρωτεύον** Name Server:

```
/etc/init.d/bind restart
```

Το ίδιο και στον **δευτερεύον** Name Server:

```
/etc/init.d/bind restart
```

Εφόσον όλα πάνε καλά πρέπει το αρχείο `/etc/bind/slave/zone.mynet.local` που δημιουργήσαμε να περιέχει τις καταχωρήσεις από την ζώνη του πρωτεύοντος.