

# The DHCP-Dynamic DNS micro-HOWTO

## Purpose

The BIND name server package has had the ability acquire dynamic updates since version 8, and DHCP has had the ability to push updates to BIND starting with version 3. This document outlines a method of creating a functional dynamic DNS server that receives update information from the DHCP server when a lease is handed out to a client. Our example will set up dynamic DNS for the focaf.mhm domain.

## The Platform

BIND and DHCP are included in many modern Linux distributions, however, this micro-HOWTO will focus on the Red Hat and Fedora distributions. It has been successfully tested on Fedora Core 3 and Red Hat Enterprise Linux 4. Other distributions may require adjustments to configuration files and paths, which will not be discussed here.

Hardware requirements are modest, and virtually any PC hardware that is 10 years old or less will run this combination of software. This configuration was tested on a Pentium 3 1400, and a Pentium 4 1.6 GHz. Neither platform showed any noticeable decrease in performance while running the two additional servers.

## Required Software

As mentioned BIND version 8 or higher, and DHCP (not dhclient) version 3 or higher. This platform was tested using BIND 9.1, and DHCP 3.0.1.

## The Steps

If you have not already done so, install the server packages using the manager of your choice.

In Fedora/Red Hat, the BIND named service may be running chrooted. For purposes of this micro-HOWTO, and to avoid problems with the dynamic update, named must be removed from the chroot jail. This is done by editing the file `/etc/sysconfig/named` and commenting out the chroot environment option like so:

```
#ROOTDIR=/var/named/chroot
```

The `/etc/rndc.conf` file should have been created when BIND was installed. If it was not, use the touch command to create the file at `/etc/rndc.conf`, (owner `root:named` – permissions `640`) and then insert the following text:

```
# Start of rndc.conf
key "rndckey" {
    algorithm hmac-md5;
    secret "RJA6mmM1rzEz7WBrImSjeg==";
};

options {
    default-key "rndckey";
    default-server 127.0.0.1;
    default-port 953;
};
# End of rndc.conf
```

Next, create or edit `/etc/named.conf` (owner `root:named` – permissions `640`) with the following information:

```
###
# dynamic DNS control file
###
# Date: February 18, 2006
###

options {
    directory "/var/named";
    forwarders {
        216.171.129.13;//replace with your own upstream DNS
        216.171.129.14;//server info
    };
    forward first;
    listen-on { any; };
    notify no;
};

key "rndckey" {
    algorithm hmac-md5;
    secret "RJA6mmM1rzEz7WBrImSjeg==";
};

controls {
    inet 127.0.0.1 port 953 allow { 127.0.0.1; } keys { rndckey; };
};

zone "." in {
    type hint;
    file "/var/named/root.hint";
};

zone "localhost" in {
    type master;
    file "/var/named/localhost.zone";
};

zone "0.0.127.in-addr.arpa" in {
    type master;
    file "/var/named/127.0.0.zone";
};

zone "focaf.mhm" {
    type master;
    file "/var/named/focaf.mhm.zone";
    allow-update { key "rndckey"; };
};

zone "0.168.192.in-addr.arpa" {
    type master;
    file "/var/named/192.168.0.zone";
    allow-update { key "rndckey"; };
};
```

Notice that this configuration has the key “rndc-key” that contains the same secret string as that in `/etc/rndc.conf`. Also, another zone has been defined in addition to localhost: focaf.mhm. The focaf.mhm zone allows the key “rndckey” to make changes. This is the basic mechanism by which dynamic DNS takes place.

Please note that the file `/etc/rndc.key` should be present. If it isn't, create it (owner `root:named` – permissions `660`) and include the following:

```
key "rndckey" {
    algorithm      hmac-md5;
    secret "RJA6mmM1rzEz7WBrImSjeg==";
};
```

The next several files will be created and/or edited in the `/var/named` directory. All files are owned by `root:named`, and file permissions for `/var/named` and its contents must be `770`.

## localhost.zone

This file should contain the following:

```
$TTL 86400
$ORIGIN localhost.
@      1D      IN      SOA      @ root (
                2006021801
                10800
                3600
                604800
                38400 )

localhost.      IN      NS      redwood
1D IN A 127.0.0.1
localhost.localdomain.      IN A 127.0.0.1
```

The only change you need to make here is to replace the NS pointer with your server's name. In this example, the server is named `redwood.focaf.mhm`, so `redwood` is the localhost NS pointer.

## 127.0.0.zone

This file is the reverse DNS for localhost.zone, and should contain the following:

```
$TTL 3D
@      IN      SOA      redwood.focaf.mhm. root.focaf.mhm. (
                2006021801
                10800
                3600
                604800
                38400 )

0.0.127.in-addr.arpa.      IN      NS      redwood
1                          PTR     localhost.
```

Again, `redwood` is referenced as the NS pointer, and also in the SOA as the primary master server for the domain. Notice the use of a fully qualified domain name in the SOA record. No further changes are required.

## focaf.mhm.zone

Here's where we get into the meat of our dynamic DNS zone:

```
$ORIGIN .
$TTL 38400      ; 10 hours 40 minutes
focaf.mhm      IN      SOA      redwood.focaf.mhm. root.focaf.mhm. (
                2006021829 ; serial
                10800      ; refresh (3 hours)
                3600       ; retry (1 hour)
                604800     ; expire (1 week)
                38400     ; minimum (10 hours 40 minutes)
                )
                NS      redwood.focaf.mhm.
                MX      10      mail.focaf.org.

$ORIGIN focaf.mhm.
$TTL 38400      ; 10 hours 40 minutes
redwood      A      192.168.0.253
ns           CNAME  redwood
```

This is a baseline configuration, and identifies **redwood** as the primary master server for **focaf.mhm** as well as providing a CNAME entry for a common prefix (**ns**). The fixed IP assigned to **redwood** is 192.168.0.253.

*This is the file that will be modified as a result of dynamic DNS, so after some time, new entries will be appended as DHCP hands out leases, but in this example, no new entries have been added as of yet.*

## 192.168.0.zone

```
$ORIGIN .
$TTL 38400      ; 10 hours 40 minutes
0.168.192.in-addr.arpa IN SOA redwood.focaf.mhm. root.focaf.mhm. (
                           2006021826 ; serial
                           10800     ; refresh (3 hours)
                           3600      ; retry (1 hour)
                           604800    ; expire (1 week)
                           38400     ; minimum (10 hours 40 minutes)
                           )
                           NS      redwood.focaf.mhm.
$ORIGIN 0.168.192.in-addr.arpa.
$TTL 38400      ; 10 hours 40 minutes
253             PTR      redwood.focaf.mhm.
```

Here, we see that 253 (192.168.0.253) is statically mapped to **redwood.focaf.mhm**. As leases are handed out, this file too will be updated by the dynamic DNS.

## root.hint

This file is a list of all the root servers in the world. It seldom changes, so once you have it, you probably will not need to update it for a couple of years.

There is a simple way to obtain this file. Run the following command as root from the **/var/named** directory:

```
dig @e.root-servers.net . ns > root.hint
```

The output file will look very much like the one below.

```
;      This file holds the information on root name servers needed to
;      initialize cache of Internet domain name servers
;      (e.g. reference this file in the "cache . <file>"
;      configuration file of BIND domain name servers).
;
;      This file is made available by InterNIC
;      under anonymous FTP as
;      file      /domain/named.root
;      on server  FTP.INTERNIC.NET
;      -OR-      RS.INTERNIC.NET
;
;      last update:   Jan 29, 2004
;      related version of root zone:  2004012900
;
;
;      formerly NS.INTERNIC.NET
;
.      3600000      IN      NS      A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000      A      198.41.0.4
;
;      formerly NS1.ISI.EDU
;
.      3600000      NS      B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000      A      192.228.79.201
;
;      formerly C.PSI.NET
;
.      3600000      NS      C.ROOT-SERVERS.NET.
```

```

C.ROOT-SERVERS.NET.      3600000      A      192.33.4.12
;
; formerly TERP.UMD.EDU
;
.                          3600000      NS
D.ROOT-SERVERS.NET.      3600000      A      D.ROOT-SERVERS.NET.
;                          128.8.10.90
; formerly NS.NASA.GOV
;
.                          3600000      NS
E.ROOT-SERVERS.NET.      3600000      A      E.ROOT-SERVERS.NET.
;                          192.203.230.10
; formerly NS.ISC.ORG
;
.                          3600000      NS
F.ROOT-SERVERS.NET.      3600000      A      F.ROOT-SERVERS.NET.
;                          192.5.5.241
; formerly NS.NIC.DDN.MIL
;
.                          3600000      NS
G.ROOT-SERVERS.NET.      3600000      A      G.ROOT-SERVERS.NET.
;                          192.112.36.4
; formerly AOS.ARL.ARMY.MIL
;
.                          3600000      NS
H.ROOT-SERVERS.NET.      3600000      A      H.ROOT-SERVERS.NET.
;                          128.63.2.53
; formerly NIC.NORDU.NET
;
.                          3600000      NS
I.ROOT-SERVERS.NET.      3600000      A      I.ROOT-SERVERS.NET.
;                          192.36.148.17
; operated by VeriSign, Inc.
;
.                          3600000      NS
J.ROOT-SERVERS.NET.      3600000      A      J.ROOT-SERVERS.NET.
;                          192.58.128.30
; operated by RIPE NCC
;
.                          3600000      NS
K.ROOT-SERVERS.NET.      3600000      A      K.ROOT-SERVERS.NET.
;                          193.0.14.129
; operated by ICANN
;
.                          3600000      NS
L.ROOT-SERVERS.NET.      3600000      A      L.ROOT-SERVERS.NET.
;                          198.32.64.12
; operated by WIDE
;
.                          3600000      NS
M.ROOT-SERVERS.NET.      3600000      A      M.ROOT-SERVERS.NET.
;                          202.12.27.33
; End of File

```

## Now For Some DHCP

The `/etc/dhcpd.conf` file is not created when `dhcpd` is installed. As root, create it now:

```
touch /etc/dhcpd.conf
```

Next, use your favorite text editor to copy the following into the newly created `/etc/dhcpd.conf`:

```
ddns-domainname "focaf.mhm";
ddns-update-style interim;
option routers 192.168.0.1;
option domain-name-servers 192.168.0.253;
option netbios-name-servers 192.168.0.253;
option netbios-node-type 8;

key "rndckey" {
    algorithm hmac-md5;
    secret "RJA6mmM1rzEz7WBrImSjeg==";
};

# focaf.mhm site
subnet 192.168.0.0 netmask 255.255.255.0 {
    allow client-updates;
    ddns-updates on;
    authoritative;
    range 192.168.0.200 192.168.0.249;
    option subnet-mask 255.255.255.0;
    allow unknown-clients;
}

# focaf.mhm zone
zone focaf.mhm. {
    primary 192.168.0.253;
    key "rndckey";
}

# reverse DNS for focaf.mhm zone
zone 0.168.192.in-addr.arpa {
    primary 192.168.0.253;
    key "rndckey";
}
```

## Finally

It's time to see if it works! From a console (as root), run:

```
tail -f /var/log/messages
```

From a second console, as root, start (or restart) services:

```
/sbin/service dhcpd restart
/sbin/service named restart
```

Check for error messages in the first console. If none appear, you did it! If errors are present, the first thing to check is syntax of the configuration files, which are common problems and sometimes hard to detect.