Installing and Configuring A
Forwarding-Caching Domain Name Server (DNS)
for a
Private Local Area Network (LAN)
in Fedora 13

A forwarding-caching nameserver forwards Internet name requests that it cannot resolve from it's own cache to an upstream (ISP) nameserver and adds the result to it's cache.

The following discussions assume that:

- all commands are executed from a **Terminal** window as administrator (*su* or *sudo*), unless otherwise inicated;
- the *local area network* (LAN) consists of several computers;
- the LAN is located behind an Internet router which
  - has an IP address on the LAN of 192.168.0.1;
  - contains an Internet firewall;
  - is the primary gateway (or connection) to the Internet;
  - forwards *domain name server* (DNS) requests to a well-known DNS authority; and
  - is responsible for DHCP management.

Install bind-chroot

1. Install the **bind-chroot** Domain Name Server (DNS):

```
yum install bind-chroot bind-utils
```

2. Modify the following directory/file permissions:

```
chmod 755 /var/named/
chmod 775 /var/named/chroot/
chmod 775 /var/named/chroot/var/
chmod 775 /var/named/chroot/var/named/
chmod 775 /var/named/chroot/var/run/
chmod 777 /var/named/chroot/var/run/named/

cd /var/named/chroot/var/named/
ln -s ../../ chroot
```

3. Modify **/etc/sysconfig/named**:

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

4. Create system startup links:

```
chkconfig --levels 235 named on
```

5. Modify the **/etc/resolv.conf** to include *127.0.0.1* before the gateway address. For example, for this network implementation, the **/etc/resolv.conf** would contain the following records:

```
nameserver 127.0.0.1
nameserver 192.168.0.1
```

This will make the system check the local nameserver first, then the internet gateway DNS. Other computers on the LAN would set the nameserver to the IP address of the nameserver, instead of 127.0.0.1.

Configuring bind-chroot

1. Copy ***non-chroot*** files to the ***chroot*** directory:

```
cp  /etc/named.*  /var/named/chroot/etc
cp  /etc/rndc.*     /var/named/chroot/etc
```

2. Modify the **named.conf** settings:

```
options {
            listen-on port 53 { 127.0.0.1; 192.168.0.0/24; };
            listen-on-v6 port 53 { ::1; };
            directory     "/var/named";
            dump-file     "/var/named/data/cache_dump.db";
            statistics-file "/var/named/data/named_stats.txt";
            memstatistics-file "/var/named/data/named_mem_stats.txt";
            allow-query     { localhost; 192.168.0.0/24; };
            recursion yes;

            forwarders { 8.8.8.8; 8.8.4.4; 192.168.0.1; };
            //forward only;

            dnssec-enable yes;
            dnssec-validation yes;
            dnssec-lookaside auto;

            /* Path to ISC DLV key */
              bindkeys-file "/etc/named.iscdlv.key";
           };

logging {
               channel default_debug {
                  file "data/named.run";
                  severity dynamic;
               };
           };

zone "." IN {
                type hint;
                file "/etc/named.ca";
               };

include "/etc/named.rfc1912.zones";
```

The **`forwarders`** statement tells the nameserver to forward unresolvable queries to the external (ISP) nameservers. The nameservers at 8.8.8.8 and 8.8.8.4 are open nameservers available for anyone to use, provided by Google.com.

The **`forward only`** statement prevents the nameserver from contacting any of the root servers if the ISP nameservers do not resolve the request.

3. Modify the **named.rfc1912.zones** configuration file:

```
zone "localhost.localdomain" IN {
        type master;
        file "/etc/named.localhost";
        allow-update { none; };
};

zone "localhost" IN {
        type master;
        file "/etc/named.localhost";
        allow-update { none; };
};

zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
        type master;
        file "/etc/named.loopback";
        allow-update { none; };
};

zone "1.0.0.127.in-addr.arpa" IN {
        type master;
        file "/etc/named.loopback";
        allow-update { none; };
};

zone "0.in-addr.arpa" IN {
        type master;
        file "/etc/named.empty";
        allow-update { none; };
};

include "/etc/rndc.key";
```

Creating zone files

Instead of creating a user's manual for domain name server (DNS) commands, this section will be a discussion of a fictional home network and examples of configuring a domain name server to provide local computer names consistent with Internet domains.

The network will be a simple, single IP Class-C local area network not directly visible to the Internet. There will be no need for sub-nets (single IP Class-C) or slave domain name servers. Also, there will be no need for a mail server as no mail handler will be provided for the LAN. All requests that cannot be handled directly by the domain name server will be forwarded to the internet gateway for routing to an external DNS.

In the following example, the network will have 4 computers (desktop/laptop), 2 servers and 1 printer. The 2 servers (Fedora13Server and FreeBSD8Server) each have 2 high-speed Ethernet network adapters. The printer and each of the desktop/laptop computers have 1 Ethernet (Gb) and 1 WiFi Wireless Adapter, with fixed addresses, as follows:

192.168.0.1	**Gateway**	**; Internet gateway/router/firewall/dhcp**
192.168.0.100	**Fedora13Server**	**; Gnome-based Fedora 13 Server Ethernet 1**
192.168.0.101	**Fedora13Server2**	**; Gnome-based Fedora 13 Server Ethernet 2**
192.168.0.102	**FreeBSD8Server**	**; FreeBSD8 Server Ethernet 1**
192.168.0.103	**FreeBSD8Server2**	**; FreeBSD8 Server Ethernet 2**
192.168.0.110	**Michael**	**; Michael's XPHome Ethernet**
192.168.0.111	**MichaelW**	**; Michael's XPHome Wireless**
192.168.0.115	**FranXPHome**	**; Fran's Dell 1150 Ethernet**
192.168.0.116	**FranXPHomeW**	**; Fran's Dell 1150 Wireless**
192.168.0.120	**XPProHome**	**; My XPProHome Development Ethernet**
192.168.0.121	**XPProHomeW**	**; My XPProHome Development Wireless**
192.168.0.130	**Fedora13Dev**	**; My Fedora 13 Development Ethernet**
192.168.0.131	**Fedora13DevW**	**; My Fedora 13 Development Wireless**
192.168.0.190	**Printer1**	**; Printer 1 Ethernet**
192.168.0.191	**Printer1W**	**; Printer 1 Wireless**

The following names are aliases for **Fedora13Server**:

ns1	; primary nameserver

The following names are aliases for **FreeBSD8Server**:

ns2	; backup nameserver
FreeBSD	; generic reference
www	; http server
talk	; IM server
ftp	; FTP server

and a variable number of portable ethernet and WiFi-based devices, such as cell phones, cameras, printers, iPods and game cubes.

The local area network name is **home**, and the top-level domain (e.g. - .com, .edu, .gov, .org) is **.lan**, providing a domain name of **home.lan** for devices connected to the LAN.

As indicated above, the primary nameserver (**ns1**) will be on **Fedora13Server** at IP address **192.168.0.100**.

DNS Zone Naming

The name of a DNS zone must follow accepted naming standards. For ***each*** domain you create, you need to consider two zones:

- **Forward referencing zones**. Forward zones are used to define domain-name based computer names (for example, www.home.lan and fedora13Dev.home.lan). The name of the zone is the name of the domain. For this network, the zone name is "**home.lan**".

- **Reverse referencing zones**. Reverse zones are used to lookup the forward name based on the IP address. It is used by secure connections to insure that the IP address returned by a forward name lookup actually belongs to the name that was looked up. The reverse zone name is constructed by reversing the first 3 octets of the IP address and appending the special domain name ***in-addr.arpa***. For this network, the zone name is “**0.168.192.in-addr.arpa**”.

Creating zone name entries

Add the following to the end of the **named.rfc1912.zones** file:

```
zone "0.168.192.in-addr.arpa" IN
{
        type master;
        file "/etc/home.lan-reverse.db";
        allow-update { key "rndckey"; };
        notify yes;
};
zone "home.lan" IN
{
        type master;
        file "/etc/home.lan-forward.db";
        allow-update { key "rndckey"; };
        notify yes;
};
```

Creating zone resource records

The first entry in the zone file is the zone's time to live (TTL) value. The purpose of a TTL is to reduce the number of DNS queries the authoritative DNS server has to answer. We'll set the TTL to 7 days (604800 seconds).

The next (optional) entry can be an ORIGIN record. The purpose of the ORIGIN record is to set the default domain for the remainder of the file (or until the next ORIGIN record). It is usually used if the zone file has a non-standard name, or if multiple types of records are mixed within the same file.

The remainder of the records in the zone file are resource records, which define the rest of the information in the zone file. The types of records used are:

- **SOA – Start of Authority**
  Contains general administrative and control information about the domain, most of which applies to *slave* servers, and not to *master* servers.

- **NS – nameserver definition**
  Specifies the IP address, Name (A), or CNAME of the name server for this domain

- **MX – mail exchange server record**
  Mail server DNS name. As no mail server is defined for this network, we will not be defining a MX record.

- **A – Forward address record**
  Associates the name of a host in the domain with it's IP address

- **PTR – Reverse address record**
  Associates the IP address of a host with it's name

- **CNAME – alias record**
  Specifies an alternate name for a host.

In each of the records, names can be fully qualified host names, or they can be relative host names.

- **Fully Qualified Name**
  Any name ending in a **period** (**.**) is considered to be fully qualified, and will be used exactly as provided by the DNS server.

- **Relative Name**
  Any name ***NOT*** ending in a **period** (**.**) is considered a relative name. The DNS server will automatically append the zone name to the end of a relative host name to make it a fully qualified host name.

- **Use of the @ character**
  The **@** character is a short-cut for the current **ORIGIN** name. If an **ORIGIN** record is not provided, it defaults to the current zone name in ***named.conf***.

A note about creating a reverse host name.

Reverse host names are constructed by reversing the order of the host's IP address and appending the special reverse DNS domain, ***in-addr.arpa***. Remember to put a period at the end of the in-addr.arpa domain, or the DNS server will append the current ORIGIN (or zone) name.

We will use the fully qualified name in the reverse domain zone file to avoid (human) confusion. The relative host IP address can be specified by simply using the last number in the 4 octet IP address without using a terminating period character (the DNS server will automatically append the proper domain).

For example, instead of putting 1.0.168.192.in-addr.arpa., we could simply put 1 (without a terminating period character).

The SOA *serial number* field usage

Contains a serial number for the current configuration. We will use the defacto standard for a SOA record - the 8 digit date (format YYYYMMDD) with an incrementing single digit number appended to the end. This number should be changed each time a change is made to the zone file (this is more important in master/slave DNS relationships, but it is wise to follow the rule).

Simply incrementing the final digit (mod 10) of the serial number for additional changes on the same day, will produce a unique enough serial number.

Creating the required zone files

1. Create a reverse domain lookup file, **home.lan-reverse.db**:

```
$TTL 604800
$ORIGIN 0.168.192.in-addr.arpa.

@       IN      SOA     @       root.home.lan. (
                                        201007130       ; serial
                                        604800          ; refresh
                                        86400           ; retry
                                        2419200         ; expire
                                        604800)         ; ttl
```

```
                IN      A       192.168.0.100

                IN      NS      Fedora13Server.home.lan.
                IN      NS      Fedora13ServerW.home.lan.

1.0.168.192.in-addr.arpa.       IN      PTR     Gateway.home.lan.

100.0.168.192.in-addr.arpa.     IN      PTR     Fedora13Server.home.lan.
101.0.168.192.in-addr.arpa.     IN      PTR     Fedora13Server2.home.lan.

102.0.168.192.in-addr.arpa.     IN      PTR     FreeBSD8Server.home.lan.
103.0.168.192.in-addr.arpa.     IN      PTR     FreeBSD8Server2.home.lan.

110.0.168.192.in-addr.arpa.     IN      PTR     Michael.home.lan.
111.0.168.192.in-addr.arpa.     IN      PTR     MichaelW.home.lan.

115.0.168.192.in-addr.arpa.     IN      PTR     FranXPHome.home.lan.
116.0.168.192.in-addr.arpa.     IN      PTR     FranXPHome.home.lan.

120.0.168.192.in-addr.arpa.     IN      PTR     XPPro.home.lan.
121.0.168.192.in-addr.arpa.     IN      PTR     XPProW.home.lan.

130.0.168.192.in-addr.arpa.     IN      PTR     Fedora13Dev.home.lan.
131.0.168.192.in-addr.arpa.     IN      PTR     Fedora13DevW.home.lan.

190.0.168.192.in-addr.arpa.     IN      PTR     Printer1.home.lan.
191.0.168.192.in-addr.arpa.     IN      PTR     Printer1w.home.lan.
```

2. Create a forward domain lookup file, **home.lan-forward.db**:

```
$TTL 604800
$ORIGIN ewdesigns.lan.

@       IN      SOA     @       root.ewdesigns.lan. (
                                        201007130       ; serial
                                        604800          ; refresh
                                        86400           ; retry
                                        2419200         ; expire
                                        604800)         ; ttl

                        IN      NS      Fedora13        ; nameserver

Gateway                 IN      A       192.168.0.1     ; LAN gateway

Fedora13Server          IN      A       192.168.0.100   ; Fedora 13 Ethernet 1
Fedora13Server2         IN      A       192.168.0.101   ; Fedora 13 Ethernet 2

FreeBSD8Server          IN      A       192.168.0.102   ; FreeBSD8 Ethernet 1
FreeBSD8Server2         IN      A       192.168.0.103   ; FreeBSD8 Ethernet 2

Michael                 IN      A       192.168.0.110   ; XPHome Ethernet
MichaelW                IN      A       192.168.0.111   ; XPHome Wireless

FranXPHome              IN      A       192.168.0.115   ; Fran's Dell 1150 Ethernet
FranXPHomeW             IN      A       192.168.0.116   ; Fran's Dell 1150 Wireless

XPProHome               IN      A       192.168.0.120   ; XPProHome Ethernet
XPProHomeW              IN      A       192.168.0.121   ; XPProHome Wireless

Fedora13Dev             IN      A       192.168.0.130   ; Fedora 13 Development Ethernet
Fedora13DevW            IN      A       192.168.0.131   ; Fedora 13 Development Wireless
```

```
Printer1            IN     A      192.168.0.190  ; Printer 1 Ethernet
Printer1W           IN     A      192.168.0.191  ; Printer 1 Wireless
```

3. Add aliases to the forward domain lookup file (home.lan-forward.db):

```
ns1         IN     CNAME        Fedora13            ; primary nameserver

ns2         IN     CNAME        FreeBSD8            ; backup nameserver
FreeBSD     IN     CNAME        FreeBSD8            ; generic reference
www         IN     CNAME        FreeBSD8            ; http server
talk        IN     CNAME        FreeBSD8            ; IM server
```

4. Copy the zone files (e.g. - ***home.lan-forward.db***, ***home.lan-reverse.db***) to the ***chroot*** zone directory and set the proper owner and permissions:

```
/var/named/chroot/etc
chown root:named /var/named/chroot/etc/home*.db
chmod 644 /var/named/chroot/etc/home*.db
```

5. If the domain name server (named) is not running (ps ax **|** grep named), start the DNS server:

```
/etc/init.d/named start
```

If the domain name server is already running, restart the DNS server:

```
/etc/init.d/named restart
```

Additonal references

1. **How to setup a home DNS server**
   http://www.redhat.com/magazine/025nov06/features/dns/

2. **Quick HOWTO : Ch18 Configuring DNS**
   http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch18_:_Configuring_DNS#Redhat_.2F_Fedora

3. **Bind 9 Administratrator Reference manual**
   http://www.bind9.net/arm97.pdf

4. **Bind 9 home page**
   http://www.bind9.net/