Contents

Configuring IPv6 and IPv4, forward and reverse DNS

We can configure IPv4 and IPv6, forward and reverse split DNS with bind so that same server can handle both IPv4 and IPv6 clients and at the same time give different responses based on whether query is coming from intranet IP, localhost or from global Internet, etc.

In our test network we have two networks connected by three machines vm1, vm2 and vm3. vm1 and vm2 are in one network and vm2 and vm3 are in other network so that vm2 can route both IPv4 and IPv6 packets between vm1 and vm3. IP range of network1 is 192.168.201.0/24 and IP range of network2 is 192.168.202.0/24. The whole setup is created on one single base machine using KVM and libvirtd. MAC addresses and IP addresses of vm1, vm2 and vm3 are:

VM	interface	MAC address	IP address(s)
vm1	eth0	00:16:36:00:00:01	192.168.201.244 fd57:1d29:4f94:1:216:36ff:fe00:1/64 fd57:1d29:4f94:a:216:36ff:fe00:1/64
vm2	eth0	00:16:36:00:00:02	192.168.201.4 fd57:1d29:4f94:a:216:36ff:fe00:2/64 fd57:1d29:4f94:1:216:36ff:fe00:2/64
	eth1	00:16:36:00:00:03	192.168.202.17 fd57:1d29:4f94:b:216:36ff:fe00:3/64 fd57:1d29:4f94:2:216:36ff:fe00:3/64
vm3	eth0	00:16:36:00:00:04	192.168.202.30 fd57:1d29:4f94:2:216:36ff:fe00:4/64 fd57:1d29:4f94:b:216:36ff:fe00:4/64

Note that link layer address in range fe80::/10 also get assigned to interfaces for auto-configuration, those addresses are not listed above.

named.conf

First we should configure logging, configure DNS server to listen on all IPv4 and IPv6 interfaces, define forward and reverse zones, etc. using '`named.conf`'. The file should get stored at location '`/var/named/chroot/etc/named.conf`' and symbolic link should get created at '`/etc/named.conf`' which points to original file.

Sample '`named.conf`' would look like

```
options
{
        directory "/var/named"; // the default
        dump-file               "data/cache_dump.db";
        statistics-file         "data/named_stats.txt";
        memstatistics-file      "data/named_mem_stats.txt";
        forwarders  { 192.168.36.222; 192.168.36.204; };
        forward first;
        allow-transfer {localhost; 192.168.0.0/16; };
        recursion yes;
        listen-on { any; };
        listen-on-v6 {  any; };
        max-cache-size 10M;
        files 10000;
        recursive-clients 100;
        tcp-clients 20;
        tcp-listen-queue 5;
        cleaning-interval 60;
        interface-interval 60;
        rrset-order { order cyclic; };
        edns-udp-size 4096;
        version none;
        hostname none;
        server-id none;

};


logging
{
        channel default {
                file "data/default.log" versions 10 size 5M;
                severity dynamic;
                print-category yes;
                print-severity yes;
                print-time yes;
        };
        channel general {
                file "data/general.log" versions 10 size 5M;
                severity dynamic;
                print-category yes;
                print-severity yes;
                print-time yes;
```

```
};
channel security {
        file "data/security.log" versions 10 size 5M;
        severity dynamic;
        print-category yes;
        print-severity yes;
        print-time yes;
};
channel config {
        file "data/config.log" versions 10 size 5M;
        severity dynamic;
        print-category yes;
        print-severity yes;
        print-time yes;
};
channel resolver {
        file "data/resolver.log" versions 10 size 5M;
        severity dynamic;
        print-category yes;
        print-severity yes;
        print-time yes;
};
channel xfer-in {
        file "data/xfer-in.log" versions 10 size 5M;
        severity dynamic;
        print-category yes;
        print-severity yes;
        print-time yes;
};
channel xfer-out {
        file "data/xfer-out.log" versions 10 size 5M;
        severity dynamic;
        print-category yes;
        print-severity yes;
        print-time yes;
};
channel client {
        file "data/client.log" versions 10 size 5M;
        severity dynamic;
        print-category yes;
        print-severity yes;
        print-time yes;
};
channel unmatched {
        file "data/unmatched.log" versions 10 size 5M;
        severity dynamic;
        print-category yes;
        print-severity yes;
        print-time yes;
};
channel network {
        file "data/network.log" versions 10 size 5M;
        severity dynamic;
        print-category yes;
        print-severity yes;
        print-time yes;
};
channel queries {
        file "data/queries.log" versions 10 size 5M;
        severity dynamic;
        print-category yes;
        print-severity yes;
```

```
                print-time yes;
        };
        channel lame-servers {
                file "data/lame-servers.log" versions 10 size 5M;
                severity dynamic;
                print-category yes;
                print-severity yes;
                print-time yes;
        };

        category default {default; };
        category general {general; };
        category security {security; };
        category config {config; };
        category resolver {resolver; };
        category xfer-in {xfer-in; };
        category xfer-out {xfer-out; };
        category client {client; };
        category unmatched {unmatched; };
        category network {network; };
        category queries {queries; };
        category lame-servers {lame-servers; };
};


view "localhost_resolver"
{
        match-clients           { 127.0.0.1; ::1; };
        match-destinations      { 127.0.0.1; ::1; };
        recursion yes;

        zone "168.192.in-addr.arpa." {
                type master;
                file "192.168.reverse.db";
        };
        zone "ipv6test.iiit.ac.in." {
                type master;
                file "ipv6test.iiit.ac.in.zone.db";
        };
        zone "4.9.f.4.9.2.d.1.7.5.d.f.ip6.arpa." {
                type master;
                file "fd57.1d29.4f94.reverse.db";
        };

        include "/etc/named.root.hints";
        include "/etc/named.rfc1912.zones";
};


view "internal"
{
        match-clients           { localnets; 192.168.0.0/16; fd57:1d29:4f94::/48; };
        recursion yes;

        zone "168.192.in-addr.arpa." {
                type master;
                file "192.168.reverse.db";
        };
        zone "ipv6test.iiit.ac.in." {
                type master;
                file "ipv6test.iiit.ac.in.zone.db";
        };
```

```
        zone "4.9.f.4.9.2.d.1.7.5.d.f.ip6.arpa." {
                type master;
                file "fd57.1d29.4f94.reverse.db";
        };
        include "/etc/named.root.hints";
};


key ddns_key
{
        algorithm hmac-md5;
#       secret "use /usr/sbin/dns-keygen to generate TSIG keys";
        secret "MlXuMXqk1WKEzxom7APg6q5MlkfFcZwiYh1BAutyZa7ButPw90fizzS1WPmN";
};


view    "external"
{
        match-clients           { any; };
        match-destinations      { any; };

        recursion no;
        allow-query-cache { none; };

        include "/etc/named.root.hints";
};
```

Note:

- Since we have specified directory as '`directory "/var/named";` ' all the zone files should go in directory '`/var/named/chroot/var/named`' and their symbolic links should be created in '`/var/named`'.
- For root hints file ('`named.root.hints`') and rfc1912 zones file ('`named.rfc1912.zones`') we have specified absolute path. Hence these files should go in '`/var/named/chroot/etc`' and their symbolic links should be created in '`/etc`'.

Default files

Following files that come with bind installation in use should be copied to appropriate locations:

- named.rfc1912.zones
- named.root.hints
- localdomain.zone
- named.broadcast
- named.local
- named.zero
- localhost.zone
- named.ip6.local
- named.root

We can use 'updatedb' and 'locate' combination to find these files. Usually these are already in proper place or located somewhere inside '/usr/share/doc/bind-<ver><tt>' directory.

Forward zone file

We need only one forward zone file for our test domain '<tt>ipv6test.iiit.ac.in'. The file should be stored with name 'ipv6test.iiit.ac.in.zone.db' in '/var/named/chroot/var/named' and symbolic link should be created to '/var/named'. The file should be like

```
$TTL 3600
@ SOA   ns.ipv6test.iiit.ac.in. root.ipv6test.iiit.ac.in. (1 15m 5m 30d 1h)
        NS ns.ipv6test.iiit.ac.in.

localhost       IN      A       127.0.0.1
localhost       IN      AAAA    ::1

vm1             IN      A       192.168.201.244
vm1.ipv4        IN      A       192.168.201.244
vm1             IN      AAAA    fd57:1d29:4f94:1:216:36ff:fe00:1
vm1             IN      AAAA    fd57:1d29:4f94:a:216:36ff:fe00:1
vm1.ipv6        IN      AAAA    fd57:1d29:4f94:1:216:36ff:fe00:1
vm1.ipv6        IN      AAAA    fd57:1d29:4f94:a:216:36ff:fe00:1
ns              IN      CNAME   vm1

vm2             IN      A       192.168.201.4
vm2.ipv4        IN      A       192.168.201.4
vm2             IN      AAAA    fd57:1d29:4f94:1:216:36ff:fe00:2
vm2             IN      AAAA    fd57:1d29:4f94:a:216:36ff:fe00:2
vm2.ipv6        IN      AAAA    fd57:1d29:4f94:1:216:36ff:fe00:2
vm2.ipv6        IN      AAAA    fd57:1d29:4f94:a:216:36ff:fe00:2
vm2             IN      A       192.168.202.17
vm2.ipv4        IN      A       192.168.202.17
vm2             IN      AAAA    fd57:1d29:4f94:2:216:36ff:fe00:3
vm2             IN      AAAA    fd57:1d29:4f94:b:216:36ff:fe00:3
vm2.ipv6        IN      AAAA    fd57:1d29:4f94:2:216:36ff:fe00:3
vm2.ipv6        IN      AAAA    fd57:1d29:4f94:b:216:36ff:fe00:3

vm3             IN      A       192.168.202.30
vm3.ipv4        IN      A       192.168.202.30
vm3             IN      AAAA    fd57:1d29:4f94:2:216:36ff:fe00:4
vm3             IN      AAAA    fd57:1d29:4f94:b:216:36ff:fe00:4
vm3.ipv6        IN      AAAA    fd57:1d29:4f94:2:216:36ff:fe00:4
vm3.ipv6        IN      AAAA    fd57:1d29:4f94:b:216:36ff:fe00:4
```

Here the ?rst line tells that the default time to live (TTL) is 3600 seconds, or one hour. The second line contains the ?rst resource record. The ?@? refers to the zone name, ?example.com.?. The SOA record type, for start of authority, tells a few important things about this zone. The data following consists of the name of the primary name server (dns1), the mail address of the administrator with the ?@? replaced by a dot, and a list of ?ve numeric parameters used by the secondary name servers.

1. The serial number is used by the secondaries to decide if they need to fetch updated zone data from the primary. It must be incremented whenever the zone data on the primary is changed.
2. The refresh and retry values specify the interval at which a secondary name server is supposed to contact the primary to see if the zone has changed and at what interval to retry doing so if the primary server is unreachable. The expire value defines for how long a secondary should continue to retry reaching the

primary until it considers its data entirely outdated and stop serving the zone.
3. The last one is called the minTTL for historical reasons but actually defines how long a cache stores negative results, i.e. the fact that a given name doesn?t have a DNS entry.

Appending an m, h or d to the last four numbers specifies them in minutes, hours or days, respectively.

Reverse zone files

IPv4 reverse zone file

The reverse zone file for '`192.168.0.0/16`' network can contain reverse records for both networks 192.168.201.0/24 and 192.168.202.0/24. Hence we create only one IPv4 reverse zone file with name '`192.168.reverse.db`' in folder '`/var/named/chroot/var/named`' and created symbolic link to '`/var/named`'.

The file should contain information like

```
$TTL 3600
@ SOA   ns.ipv6test.iiit.ac.in. root.ipv6test.iiit.ac.in. (1 15m 5m 30d 1h)
        NS ns.ipv6test.iiit.ac.in.

244.201         PTR     vm1.ipv4.ipv6test.iiit.ac.in.
244.201         PTR     vm1.ipv6test.iiit.ac.in.
4.201           PTR     vm2.ipv4.ipv6test.iiit.ac.in.
4.201           PTR     vm2.ipv6test.iiit.ac.in.
17.202          PTR     vm2.ipv4.ipv6test.iiit.ac.in.
17.202          PTR     vm2.ipv6test.iiit.ac.in.
30.202          PTR     vm3.ipv4.ipv6test.iiit.ac.in.
30.202          PTR     vm3.ipv6test.iiit.ac.in.
```

- Note that names of format vm<n>.ipv4.ipv6test.iiit.ac.in have been intentionally kept before names of format vm<n>.ipv6test.iiit.ac.in.
- We can test reverse lookup using command '`dig @<dns_server> -x <IPv4_address>`'

IPv6 reverse zone file

The reverse zone file for '`4.9.f.4.9.2.d.1.7.5.d.f.ip6.arpa.`' can contain reverse records for all the four ranges (fd57:1d29:4f94:{1,a,2,b}::/64) that we have used in our test network. Hence we need only one IPv6 reverse zone file. The file should be named '`fd57.1d29.4f94.reverse.db`' and stored in '`/var/named/chrooot/var/named`' and symbolic link should be created in folder '`/var/named`'.

The file should contain information like:

```
$TTL 3600
@ SOA   ns.ipv6test.iiit.ac.in. root.ipv6test.iiit.ac.in. (1 15m 5m 30d 1h)
        NS ns.ipv6test.iiit.ac.in.

$ORIGIN 1.0.0.0.4.9.f.4.9.2.d.1.7.5.d.f.ip6.arpa.
;                1 1 1 1 1 1 1
; 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6

1.0.0.0.0.0.e.f.f.f.6.3.6.1.2.0 PTR     vm1.ipv6.ipv6test.iiit.ac.in.
1.0.0.0.0.0.e.f.f.f.6.3.6.1.2.0 PTR     vm1.ipv6test.iiit.ac.in.
2.0.0.0.0.0.e.f.f.f.6.3.6.1.2.0 PTR     vm2.ipv6.ipv6test.iiit.ac.in.
2.0.0.0.0.0.e.f.f.f.6.3.6.1.2.0 PTR     vm2.ipv6test.iiit.ac.in.



$ORIGIN a.0.0.0.4.9.f.4.9.2.d.1.7.5.d.f.ip6.arpa.
;                1 1 1 1 1 1 1
; 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6

1.0.0.0.0.0.e.f.f.f.6.3.6.1.2.0 PTR     vm1.ipv6.ipv6test.iiit.ac.in.
1.0.0.0.0.0.e.f.f.f.6.3.6.1.2.0 PTR     vm1.ipv6test.iiit.ac.in.
2.0.0.0.0.0.e.f.f.f.6.3.6.1.2.0 PTR     vm2.ipv6.ipv6test.iiit.ac.in.
2.0.0.0.0.0.e.f.f.f.6.3.6.1.2.0 PTR     vm2.ipv6test.iiit.ac.in.



$ORIGIN 2.0.0.0.4.9.f.4.9.2.d.1.7.5.d.f.ip6.arpa.
;                1 1 1 1 1 1 1
; 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6


3.0.0.0.0.0.e.f.f.f.6.3.6.1.2.0 PTR     vm2.ipv6.ipv6test.iiit.ac.in.
3.0.0.0.0.0.e.f.f.f.6.3.6.1.2.0 PTR     vm2.ipv6test.iiit.ac.in.
4.0.0.0.0.0.e.f.f.f.6.3.6.1.2.0 PTR     vm3.ipv6.ipv6test.iiit.ac.in.
4.0.0.0.0.0.e.f.f.f.6.3.6.1.2.0 PTR     vm3.ipv6test.iiit.ac.in.
```

Note that:

- We have used '`$ORIGIN 1.0.0.0.4.9.f.4.9.2.d.1.7.5.d.f.ip6.arpa.`' to specify first 16 characters of subnet and specified all reverse PTR records wrt this origin. This way we do not have to type 32 character long IPv6 address for each reverse PTR record.
- We have also specified numbers 2-16 in comments just after origin. These numbers help us in ensuring that we have typed all left-over 16 characters of IPv6 address in PTR record.
- We cannot condense reverse records using techniques like '`::`', hence creating reverse zone file is very lengthy and time-consuming task.
- Here also names of format vm<n>.ipv6.ipv6test.iiit.ac.in have been intentionally kept before names of format vm<n>.ipv6test.iiit.ac.in.
- We can test reverse lookup using command '`dig @<dns_server> -x <IPv6_address>`'

Client configuration

To configure DNS clients we can include following lines in '/etc/sysconfig/network-scripts/ifcfg-eth<n>' file of clients:

```
DNS1=192.168.201.244
SEARCH=ipv6test.iiit.ac.in
```

If we want to use IPv6 address for DNS queries then we can use:

```
DNS1=fd57:1d29:4f94:1:216:36ff:fe00:1
DNS2=fd57:1d29:4f94:a:216:36ff:fe00:1
SEARCH=ipv6test.iiit.ac.in
```

Note:

- In our case DNS was configured on vm1. Hence vm1 IPs are being configured as DNS IPs.
- Client cannot take DNS information from router, it can only take prefix information and configure IPs. Hence we still need DHCPv6 server so that we can distribute DNS information to client from central server.

Firewall considerations

DNS server firewall configuration

On DNS server we need to allow incoming DNS queries on destination port 53. Hence we can use below configuration

```
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
```

```
in both '/etc/sysconfig/iptables' and '/etc/sysconfig/ip6tables' files so that DNS server can receiv
```

DNS client firewall configuration

Note that DNS clients choose random UDP port to send DNS queries to port 53 of DNS server. Then DNS server replies to client on same port from source UDP port 53. Hence in order to allow DNS client to receive DNS replies without them getting filtered by firewall, we can use:

```
-A INPUT -p udp -m udp --sport 53 -j ACCEPT
```

in both '`/etc/sysconfig/iptables`' and '`/etc/sysconfig/ip6tables`' files.

Note:

- The filtering is based on source port and not destination port
- For a process to be able to listen on port 53, super user privileges are required. Hence by ensuring that DNS requests go to port 53 we reduce the possibility of normal user running his/her own DNS server. Also since queries are sent from ports > 1024, a normal user process can query DNS server without any set-uid/set-gid etc. mechanisms.