



Lab Exercise 3 – Authoritative DNS Servers

Objectives

Participants should be able to configure primary and secondary name server for a given domain name and do a zone transfer between them. This should include creating, modifying, deleting RRs and incrementing Primary name server serial number. Each participant name servers should be visible from other name servers since we will use the lab root and GTLD server. A custom lab root hint will be used.

*Note: Configure your PC to be the primary (also called master) of your own domain and also a slave for PCs in your right side. PC in your left will act as slave for your own domain. *

Steps:

1. Register your domain name and its name server's FQDN (master & slave) together with their IP addresses to the domain name registry. In our lab you should approach the instructor for registration. Instructor will also act as a GTLD server for this exercise. He will be creating the delegation of .net subdomains to every pc in the lab.
2. Create a new working directory for your master server under `/var/named`

```
mkdir /var/named/master
```

3. Create a zone file for your domain under `/var/named/master` and add necessary resource records like NS record, A record, txt record, MX record that will determine which host is receiving mail for your domain.

For example, if you have `groupXX.net` as your domain, you must create `db.groupXX.net` , with the following base contents (sample configuraiton for server01):

```

$TTL 1d
@ SOA      ns.groupXX.net. email.groupXX.net.  (
        2016010101 ;serial no.
        30m       ;refresh
        15m       ;retry
        1d        ;expire
        30m       ;negative cache ttl
)

        IN NS   ns.groupXX.net.

ns      IN  A    192.168.1XX.1
www     IN  A    192.168.1XX.1

mail01  IN  A    192.168.1XX.200
mail02  IN  A    192.168.1XX.201

groupXX.net.  MX 10   mail01.groupXX.net.
groupXX.net.  MX 20   mail02.groupXX.net.

groupXX.net.  IN  TXT "groupXX Authoritative DNS Server"

```

4. Create the configuration file (`named.conf`). Please note that the primary zone is of "type master" while a secondary zone is of "type slave." Specify your nameserver's working directory.

```

options {
    directory "/var/named/master";
};

zone "groupXX.net" {
    type master;
    file "db.groupXX.net";
};

```

Most authoritative servers are also recursive/caching servers for their own networks. If this is the case, also add the zones defined in the recursive `named.conf` .

```

zone "." {
    type hint;
    file "root.hints";
};

zone "localhost" {
    type master;
    file "db.localhost" ;
};

```

You can copy the `root.hints` & `db.localhost` from previous lab instruction.

5. In `/var/named/master` run `bind` and see if it's running properly. Error messages will give you hints where the error is.

```
named -g -c named.conf
```

6. Once BIND is running, you can do some basic test using DNS tools like `dig`

To test your name server to display the SOA records for your domain.

```
dig @192.168.1XX.1 groupXX.net SOA
```

To test your name server to display NS records

```
dig @192.168.1XX.1 groupXX.net NS
```

To test your name server to display other resource records (A, MX, or TXT). You can also use the `-t` option to set the query type.

```
dig @192.168.1XX.1 ns.groupXX.net A
dig -t MX @192.168.1XX.1 groupXX.net
```

7. Setup your server as the secondary server for your neighbour.
(Optional) Create a folder called `slave`. Your primary server's zonefile will be copied to this folder.

```
mkdir /var/named/slave
```

In your `named.conf`, add the following (`group98.net` is the neighbour zone):

```
zone "groupYY.net" {
    type slave;
    file "/var/named/slave/db.groupYY.net";
    masters { 192.168.1YY.1;
    };
};
```

8. Secure your zones by restricting who can get the zone file.
You can test this by trying zone transfer from another nameserver in the lab.

```
dig @localhost groupYY.net AXFR
```

If successful, you will see all the resource records as an output.

Now, add the following line in your `named.conf` for the zones where you are primary:

```
zone "groupXX.net" {
    type master;
    file "db.groupXX.net";
    allow-transfer { 192.168.1YY.1;
    };
};
```

Execute the same dig command again. If successful, the status in the dig output should say Transfer Failed.

9. You can make `groupYY.net` (the secondary/slave server) as authoritative server. For that add another NS record in the `db.groupXX.net` file:

```
$TTL 1d
@ SOA      ns.groupXX.net. email.groupXX.net.  (
                2016010101 ;serial no.

<config sniff.....>

                IN NS    ns.groupXX.net.
                IN NS    ns.groupYY.net.

<config sniff.....>
```

The complete `named.conf` for an authoritative+recursive server is as follows:

```
// named.conf
// global configuration

options {
    directory "/var/named/master";
};

// root-hints
zone "." {
    type hint;
    file "root.hints";
};

// recursive name server config
zone "localhost" {
    type master;
    file "db.localhost" ;
};

// primary zones
zone "groupXX.net" {
    type master;
    file "db.groupXX.net";
};

// secondary zones
zone "groupYY.net" {
    type slave;
    file "/var/named/slave/db.groupYY.net";
    masters { 192.168.1YY.1;
    };
};
```

Lab Exercise 3 – Authoritative DNS Servers

Created: 12 May 2016

Version 3.1