Primary DNS for **A** type record

1. A primary DNS server is responsible for reading data related to the domain zone.
2. Primary DNS is only One But Secondary can be multiple in numbers.
3. It works on 53/UDP port.
4. We can query for ip from primary DNS only means we can't query from secondary DNS
5. The primary server is also responsible for communicating with the secondary server for recovery purpose..
6. The process of a primary web server communicating with the secondary server is known as a zone transfer, as zone data is being sent from a DNS server to another.
7. Each domain name is assigned to DNS servers for redundancy, and to simplify the process of server administration. If a primary server already contains the zone data for a domain, this data does not need to be replicated because the primary and secondary server continuously share zone data.

➔ Creating Own Primary DNS on Linux using bind pakage For Rhel or CentOs

➔ Installing Software packages bind (it helps us create to primary dns)
[root@piyush Desktop]# yum install bind -y

➔ To see the confriguration file bind
[root@piyush Desktop]# rpm -qc bind
/etc/logrotate.d/named
/etc/named.conf
/etc/named.iscdlv.key
/etc/named.rfc1912.zones

/etc/named.root.key
/etc/rndc.conf
/etc/rndc.key
/etc/sysconfig/named
/var/named/named.ca
/var/named/named.empty
/var/named/named.localhost
/var/named/named.loopback

➔ Now takes backup of **named.conf** file as **named.conf.bak**
➔ **named.conf** looks like this
➔ **[root@piyush etc]# vim named.conf**

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on port 53 { 127.0.0.1; };
        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; };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable re
sion
```

➔ Now empty the content of file.
[root@piyush etc]# echo > named.conf
Now creating the Zone for a particular domain
[root@piyush etc]# vim named.conf

```
        options {
                        directory "/var/named/" ;

};

        zone "piyush.com" IN {
                        type master ;
                        file "mydns" ;
};
```

- In Image :-

  Note:- Ends every line in **named.conf** with ";"

  options :- provides you option where to create zone file and Forwarder DNS
  directory :- where you want to create your Zone File gives the path here

  For every create Zone block
  zone :- for creating zone for domain name
  "piyush.com" :- domain name
  master :- is for Primary DNS
  mydns :- Zone file Name (name can be any thing)

➔ Now create the zone file (**mydns**)
[root@piyush etc]# cd /var/named/
[root@piyush named]# ls
data dynamic named.ca named.empty **named.localhost** named.loopback slaves

➔ Firstly copy the content of **named.localhost** in the file **mydns** (Zone file)
[root@piyush named]# cat named.localhost

```
$TTL 1D
@       IN SOA  @ rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
```

[root@piyush named]# cp named.localhost mydns

➔ Make the owner and group of file to **named**
[root@piyush named]#chown named:named mydns

➔ Now editing the file according to the requirement
[root@piyush named]# vim mydns

- In image :-

```
$TTL 1D
@       IN SOA  @ rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1


zxc.piyush.com. 100       IN A 55.5.5.5
abc.piyush.com. 120       IN A    100.0.0.77
xyz.piyush.com.           IN A    100.100.0.0
rrr.piyush.com.  100      IN AAAA 5555::5555
qwq                       IN AAAA  2004::2000
cba IN  CNAME abc
aaa IN  CNAME abc
fff IN  CNAME rrr
```

FQDN:= Fully Qualified Domain Name hostname.domainname.topleveldomain
hostname.subdomainname.domainname.topleveldomain

Note :-

*If you writing FQDN them put "**.**" **Dot** at end otherwise if you wrinting only hostname no need to put **Dot** at end.*
Not necessary to write TTL

@ NS :- NameServer
piyush.expert.com. :- FQDN of Domain Server

Entry Format:- **FQDM TTL IN Record_Type Ip_address**

abc.piyush.com. :- FQDN

qwq :- *hostname (don't put **Dot** at end Dns Server will automatically append "**piyush.com**" at end)*

RECORD_TYPE

A **:-** *For FQDN to Ip conversion and ipv4*

AAAA :- *For FQDN to Ip conversion and ipv6*

CNAME :- ***Canonical*** *name means here* ***abc.piyush.com.*** *And* ***cba.piyush.com.*** *Points to same ip address* ***100.0.0.10***

Note:-

If firewall is running add dns to firewalld service or flush the firewalld as you wish

➔ Now restart the service if no error in syntax , the service get restart without error

[root@piyush Desktop]# systemctl restart named

[root@piyush Desktop]# systemctl enable --now named

➔ Now move to another pc to check

➔ Firstly adding nameserver as ip of DNS server.

root@piyush Desktop]#vim /etc/resolv.conf

```
# Generated by NetworkManager
nameserver 192.168.0.16
~
```

```
[root@localhost Desktop]# vim /etc/resolv.conf
[root@localhost Desktop]# nslookup zxc.piyush.com
Server:         192.168.0.16
Address:        192.168.0.16#53

Name:   zxc.piyush.com
Address: 55.5.5.5

[root@localhost Desktop]#
```

```
[root@localhost Desktop]# nslookup abc.piyush.com
Server:         192.168.0.16
Address:        192.168.0.16#53

Name:   abc.piyush.com
Address: 100.0.0.77

[root@localhost Desktop]#
```

```
[root@localhost Desktop]# nslookup cba.piyush.com
Server:         192.168.0.16
Address:        192.168.0.16#53

cba.piyush.com  canonical name = abc.piyush.com.
Name:   abc.piyush.com
Address: 100.0.0.77

[root@localhost Desktop]#
```

```
[root@localhost Desktop]# nslookup xyz.piyush.com
Server:         192.168.0.16
Address:        192.168.0.16#53

Name:   xyz.piyush.com
Address: 100.100.0.0

[root@localhost Desktop]#
```

```
[root@localhost Desktop]# host qwq.piyush.com
qwq.piyush.com has IPv6 address 2004::2000
```

But if you use **nslookup** command for ipv6 normally the it will not resolve ip address.

```
[root@piyush ~]# nslookup rrr.piyush.com
Server:         192.168.0.7
Address:        192.168.0.7#53

*** Can't find rrr.piyush.com: No answer
```

You have write like this

```
[root@piyush ~]# nslookup -query=AAAA rrr.piyush.com
Server:         192.168.0.7
Address:        192.168.0.7#53

rrr.piyush.com  has AAAA address 5555::5555
```

```
[root@piyush ~]# nslookup -query=AAAA fff.piyush.com
Server:         192.168.0.7
Address:        192.168.0.7#53

fff.piyush.com  canonical name = rrr.piyush.com.
rrr.piyush.com  has AAAA address 5555::5555
```

As we haven't use **forwarders** in **options** section of **named.conf** file your DNS can't resolve domain name whose entry are not mentioned in **named.conf** file.

Note:- your DNS is resolving the ip of other domainname whose entries are in **named.conf.** There are two reasons for it:-

1. It may goes to router through gateway to search the ip of hostname. You can use " **route del -net 0.0.0.0 gw 192.168.0.1** " to delete gateway.
2. Ip of that hostname may resides in your cache.

```
[root@piyush ~]# nslookup  www.google.com
Server:         192.168.0.7
Address:        192.168.0.7#53

** server can't find www.google.com: SERVFAIL

[root@piyush ~]# nslookup  www.facebook.com
Server:         192.168.0.7
Address:        192.168.0.7#53

** server can't find www.facebook.com: SERVFAIL
```