Primary DNS for **PTR** type record **ipv4**

1. A primary DNS server is responsible for reading data related to the domain zone and respond to Ip address of that Fully Qualified Domain Name (FQDN) and vice-versa means take Ip address respond to Fully Qualified Domain Name (FQDN).
2. But here we have used **PTR** record so FQDN to Ip address.
3. Primary DNS is only One But Secondary can be multiple in numbers.
4. The connection between **Client** and **Primary DNS** is through **53/UDP** port.
5. The connection between **Primary DNS** ans **Secondary DNS** is through **53/TCP** port.
6. We can query for ip from primary DNS only means we can't query from secondary DNS
7. The primary server is also responsible for communicating with the secondary server for recovery purpose..
8. 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.
9. 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

- In Image :-

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

};

zone "0.168.192.in-addr.arpa" IN {
                type master;
                file "0.168.192.revdns";
};

zone "10.100.100.in-addr.arpa" IN {
                type master;
                file "10.100.100.revdns";
};
```

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 different Network having different Ip address Pool
"0.168.192.in-addr.arpa" :- Ip address Pool of network "**192.168.0."** means write First 3 Octet of Ip address in reverse order.
master :- is for Primary DNS
0.168.192.revdns :- Zone file Name (name can be any thing but for convenience use name as Network address)

similarly for Network "**100.100.10."**

➔ Now create the zone file (**0.168.192.revdns and 10.100.100.revdns**)

[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 **0.168.192.revdns and 10.100.100.revdns** (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 0.168.192.revdns
[root@piyush named]# cp named.localhost 10.100.100.revdns

➔ Make the owner and group of file to **named**
[root@piyush named]#chown named:named 0.168.192.revdns
[root@piyush named]#chown named:named 10.100.100.revdns

➔ Now editing the files according to the requirement
[root@piyush named]# vim 0.168.192.revdnss

- 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


55 IN PTR  zxc.piyush.com.
100 IN PTR abc.piyush.com.
111 IN PTR xyz.piyush.com.
200 IN PTR rrr.piyush.com.

54 IN  CNAME 55
53 IN  CNAME 55
112 IN  CNAME 111
```

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

Entry Format:- **LastOctetOfIpaddr TTL IN Record_Type FQDN**

55 :- Last Octet of Ip Address
IN **:-** Internet
abc.piyush.com. :- FQDN

RECORD_TYPE

PTR **:-** *For Ip address to FQDN conversion*
CNAME **:-** ***Canonical** name means here **zxc.piyush.com.** Points to same Ip addresses **192.168.0.55** and **192.168.0.54***

➔ *Similarly for Network **100.100.10***
[root@piyush named]# vim 10.100.100.revdnss

- ***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


1 IN PTR  zxc.piyush.io.
22 IN PTR abc.piyush.io.
33 IN PTR xyz.piyush.io.
44 IN PTR rrr.piyush.io.

23 IN CNAME 22
24 IN CNAME 22
45 IN CNAME 44
```

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 or client to check

➔ Firstly adding nameserver as ip of DNS server.

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

```
# Generated by NetworkManager
nameserver 192.168.0.7
~
~
```

Now do query :-

```
[root@piyush ~]# nslookup 100.100.10.1
Server:         192.168.0.7
Address:        192.168.0.7#53

1.10.100.100.in-addr.arpa       name = zxc.piyush.io.
```

```
[root@piyush ~]# nslookup 100.100.10.22
Server:         192.168.0.7
Address:        192.168.0.7#53

22.10.100.100.in-addr.arpa      name = abc.piyush.io.

[root@piyush ~]# nslookup 100.100.10.23
Server:         192.168.0.7
Address:        192.168.0.7#53

23.10.100.100.in-addr.arpa      canonical name = 22.10.100.100.in-addr.arpa.
22.10.100.100.in-addr.arpa      name = abc.piyush.io.

[root@piyush ~]# nslookup 100.100.10.24
Server:         192.168.0.7
Address:        192.168.0.7#53

24.10.100.100.in-addr.arpa      canonical name = 22.10.100.100.in-addr.arpa.
22.10.100.100.in-addr.arpa      name = abc.piyush.io.
```

```
[root@piyush ~]# nslookup 100.100.10.44
Server:         192.168.0.7
Address:        192.168.0.7#53

44.10.100.100.in-addr.arpa      name = rrr.piyush.io.

[root@piyush ~]# nslookup 100.100.10.45
Server:         192.168.0.7
Address:        192.168.0.7#53

45.10.100.100.in-addr.arpa      canonical name = 44.10.100.100.in-addr.arpa.
44.10.100.100.in-addr.arpa      name = rrr.piyush.io.

[root@piyush ~]# nslookup 100.100.10.33
Server:         192.168.0.7
Address:        192.168.0.7#53

33.10.100.100.in-addr.arpa      name = xyz.piyush.io.
```

```
[root@piyush ~]# nslookup 192.168.0.55
Server:         192.168.0.7
Address:        192.168.0.7#53

55.0.168.192.in-addr.arpa       name = zxc.piyush.com.

[root@piyush ~]# nslookup 192.168.0.54
Server:         192.168.0.7
Address:        192.168.0.7#53

54.0.168.192.in-addr.arpa       canonical name = 55.0.168.192.in-addr.arpa.
55.0.168.192.in-addr.arpa       name = zxc.piyush.com.

[root@piyush ~]# nslookup 192.168.0.53
Server:         192.168.0.7
Address:        192.168.0.7#53

53.0.168.192.in-addr.arpa       canonical name = 55.0.168.192.in-addr.arpa.
55.0.168.192.in-addr.arpa       name = zxc.piyush.com.
```

```
[root@piyush ~]# nslookup 192.168.0.100
Server:         192.168.0.7
Address:        192.168.0.7#53

100.0.168.192.in-addr.arpa      name = abc.piyush.com.

[root@piyush ~]# nslookup 192.168.0.111
Server:         192.168.0.7
Address:        192.168.0.7#53

111.0.168.192.in-addr.arpa      name = xyz.piyush.com.

[root@piyush ~]# nslookup 192.168.0.112
Server:         192.168.0.7
Address:        192.168.0.7#53

112.0.168.192.in-addr.arpa      canonical name = 111.0.168.192.in-addr.arpa.
111.0.168.192.in-addr.arpa      name = xyz.piyush.com.

[root@piyush ~]# nslookup 192.168.0.200
Server:         192.168.0.7
Address:        192.168.0.7#53

200.0.168.192.in-addr.arpa      name = rrr.piyush.com.
```

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 on client and DNS server side both.
2. Ip of that hostname may resides in your cache.

Now checking ip of facebook and youtube

```
[root@piyush ~]# nslookup 66.220.144.0
Server:         192.168.0.7
Address:        192.168.0.7#53

** server can't find 0.144.220.66.in-addr.arpa: SERVFAIL

[root@piyush ~]# nslookup 199.223.232.0
Server:         192.168.0.7
Address:        192.168.0.7#53

** server can't find 0.232.223.199.in-addr.arpa: SERVFAIL
```