INDIAN INSTITUTE OF INFORMATION TECHNOLOGY KALYANI
Autonomous institution under MHRD, Govt. Of India
&
Department of Information Technology & Electronics, Govt. of West Bengal
WEBEL IT Park Campus (Near Buddha Park), Kalyani -741235, West Bengal
Tel : 033 2582 2240, website : www.iiitkalyani.ac.in

Lab Assignment #06

Submit on or before 19/02/18

Weekly contact : **0 – 0 – 3 (L – T – P)**
Course No. : **CS 612**
Course Title : **Computer Networks**
Instructor-In-Charge : **Dr. SK Hafizul Islam (hafi786@gmail.com)**

Aim

- DNS server configuration and analysis of traffic using Wireshark.

Objective

- We will learn how to install and configure DNS in Ubuntu system.

DNS

DNS is used to resolve hostnames into IP addresses and vice versa. A computer that runs DNS is called nameserver (NS). The Ubuntu OS ships with BIND9 (Berkley Internet Naming Daemon), the most common program used for maintaining a nameserver on Linux. We will configure one system for Primary DNS nameserver, another system for secondary DNS nameserver, and the third system one for DNS client. All systems are running with Ubuntu OS. The most common configurations for BIND9 are a caching nameserver (NS), primary, and as a secondary. When configured as a caching nameserver, the BIND9 will find the answer to name queries and remember the answer when the domain is queried again. As a primary nameserver, the BIND9 reads the data for a zone from a zone file on its host and is authoritative for that zone. In a secondary nameserver configuration, the BIND9 gets the zone data from another nameserver authoritative for the zone.

We will use three systems, one for Primary DNS nameserver, other for secondary DNS nameserver, and the third one for DNS client. All systems are running with Ubuntu OS.

Primary DNS server

OS: Ubuntu
Hostname: pri.iiitkalyani
IP address: **172.16.4.3**
(to change the host name --- *hostname pri.iiitkalyani*. To change the name permanently, run command to edit the host files: sudo gedit /etc/hostname /etc/hosts)

Secondary DNS server

OS: Ubuntu
Hostname: sec.iiitkalyani
IP address: **172.16.4.4**

DNS Client

OS: Ubuntu
Hostname : client.iiitkalyani
IP address: **172.16.4.5**

DNS Server (BIND9) Installation Guide

PART 1: Install and configure Caching nameserver

PART 2: Install and configure Primary DNS nameserver (PC1) or Master DNS nameserver

PART 3: Install and configure Secondary DNS nameserver (PC2) or Slave DNS nameserver

PART 4: Configuring DNS Client (PC3)

PART 1: Install (in PC1 & PC3) and configure Caching nameserver

Caching nameserver saves the DNS query results locally for a particular period of time. It reduces the DNS server's traffic by saving the queries locally; therefore it improves the performance and efficiency of the DNS server.

Step 1: At a terminal prompt, enter the following command to update ubuntu

- *sudo –i*
- *sudo apt-get update*
- *sudo apt-get upgrade*
- *sudo apt-get dist-upgrade*

Step 2: Install BIND9 packages which are used to setup DNS server.

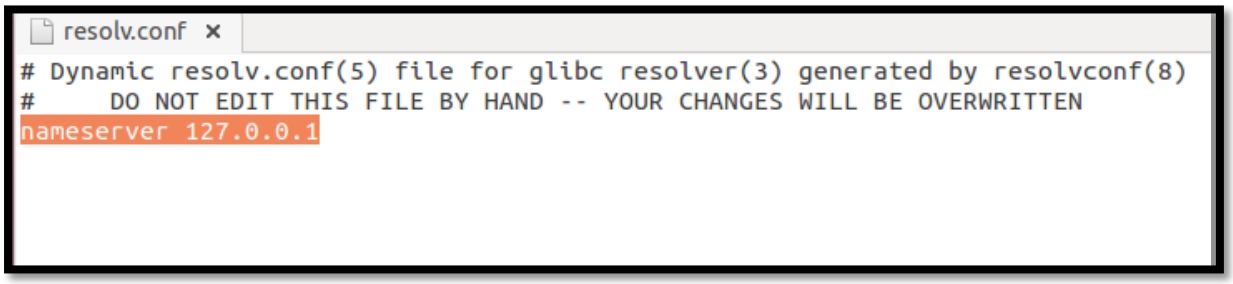
- *sudo apt-get install bind9 bind9utils bind9-doc*

Step 3: A very useful package for testing and troubleshooting DNS issues is the *dnsutils* package. To install *dnsutils* enter the following:

- *sudo apt-get install dnsutils*

Step 4: Edit the resolve.conf file. Change nameserver IP address to 127.00..1 or your primary server IP address (172.16.4.3).

- *sudo –i*
- *gedit /etc/resolv.conf*



Step 5: Configure the "caching nameserver".

Caching nameserver will remember all the DNS queries made and serve locally when the domain is queried second time. The default configuration is setup to act as a caching nameserver. Uncomment and edit the following in /etc/bind/named.conf.options. And then, add your ISP's DNS or Google public DNS server IP addresses (8.8.8.8 and 8.8.4.4).

- *sudo –i*
- *gedit /etc/bind/named.conf.options*

```
        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
                8.8.8.8;
                8.8.4.4;
        };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;
```

Step 5: Restart bind9 service to take effect the changes.

- *sudo systemctl restart bind9*

Step 6: Check if the caching nameserver it is working or not using command:

- *dig -x 127.0.0.1*

If the caching nameserver is successfully installed in your machine, then you will get the following message

```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> -x 127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22769
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;1.0.0.127.in-addr.arpa. IN PTR

;; ANSWER SECTION:
1.0.0.127.in-addr.arpa. 604800 IN PTR localhost.

;; AUTHORITY SECTION:
127.in-addr.arpa. 604800 IN NS localhost.

;; ADDITIONAL SECTION:
localhost. 604800 IN A 127.0.0.1
localhost. 604800 IN AAAA ::1

;; Query time: 0 msec
;; SERVER: 192.168.1.200#53(192.168.1.200)
;; WHEN: Tue Aug 23 15:53:59 IST 2016
;; MSG SIZE rcvd: 132
```

PART 2: Install (in PC1) and configure Primary DNS nameserver

Step 1: At a terminal prompt, enter the following command to install DNS nameserver

- *sudo –i*
- *sudo apt-get update*
- *sudo apt-get upgrade*
- *sudo apt-get dist-upgrade*
- *sudo apt-get install bind9 bind9utils bind9-doc*

Step 2: All configuration file be will be available under */etc/bind/* directory. Edit bind9 configuration file, called *named.conf*

- *sudo –i*
- *gedit /etc/bind/named.conf*

"named.conf" file should have the following lines in it. If the lines are not there, just add them.

- *include "/etc/bind/named.conf.options";*
- *include "/etc/bind/named.conf.local";*

- *include "/etc/bind/named.conf.default-zones";*

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

Step 3: We need to define the forward and reverse zone files.
Create a forward zone *fz.iiitkalyani* by copying *db.local* configuration file.

- *sudo mkdir /etc/bind/fz.iiitkalyani*
- *sudo cp /etc/bind/db.local /etc/bind/fz.iiitkalyani*

Step 4: Test with dig command

- *dig fz.iiitkalyani*

```
root@user-Precision-Tower-3420:~# dig fz.iiitkalyani

; <<>> DiG 9.10.3-P4-Ubuntu <<>> fz.iiitkalyani
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 4781
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;fz.iiitkalyani.        IN    A

;; AUTHORITY SECTION:
.          10753    IN    SOA    a.root-servers.net. nstld.verisign-grs.com. 2018012500 1800 900 604800 86400

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Jan 25 14:31:40 IST 2018
;; MSG SIZE  rcvd: 118

root@user-Precision-Tower-3420:~#
```

Step 5: Edit /etc/bind/fz.iiitkalyani as follows.

- *sudo -i*
- *gedit /etc/bind/fz.iiitkalyani*

```
$TTL 86400
@   IN  SOA    pri.iiitkalyani. root.iiitkalyani.
(
      2011071001  ;Serial
      3600        ;Refresh
      1800        ;Retry
      604800      ;Expire
      86400       ;Minimum TTL
)
@       IN  NS      ns.
@       IN  NS      pri.iiitkalyani.
@       IN  NS      sec.iiitkalyani.
@       IN  A       172.16.4.3
@       IN  A       172.16.4.4
@       IN  A       172.16.4.5
pri     IN  A       172.16.4.3
sec     IN  A       172.16.4.4
client  IN  A       172.16.4.5
```

Step 6: Test with dig command as

- *dig fz.iiitkalyani*

Step 7: Create reverse zone file *rz.iiitkalyani* by copying *db.127* configuration file.

- *sudo mkdir /etc/bind/rz.iiitkalyani*
- *sudo cp /etc/bind/db.127 /etc/bind/rz.iiitkalyani*

Step 8: Open */etc/bind/rz.iiitkalyani* file and edit like below.

- *sudo -i*
- *gedit /etc/bind/rz.iiitkalyani*

```
$TTL 86400
@   IN  SOA    pri.iiitkalyani.  root.Iiitkalyani.
(
2011071002  ;Serial
3600        ;Refresh
1800        ;Retry
604800      ;Expire
86400       ;Minimum TTL
)
@       IN  NS      pri.iiitkalyani.
@       IN  NS      sec.iiitkalyani.
@       IN  PTR     iiitkalyani.
pri     IN  A       172.16.4.3
sec     IN  A       172.16.4.4
client  IN  A       172.16.4.5
3       IN  PTR     pri.iiitkalyani.
4       IN  PTR     sec.iiitkalyani.
5       IN  PTR     client.iiitkalyani.
```

Step 9: On the Primary nameserver, the zone transfer needs to be allowed. Add the allow-transfer option to the example forward and reverse zone definitions in /etc/bind/named.conf.local. Open */etc/bind/named.conf.local* configuration file and add the below lines to include forward and reverse zone files

- *sudo -i*
- *gedit /etc/bind/named.conf.local*

```
// Do any local configuration here
// Consider adding the 1918 zones here, if they are not used in your organization
//include "/etc/bind/zones.rfc1918";
//forward zone file
zone "iiitkalyani.ac.in"
{
type master;
file "/etc/bind/fz.iiitkalyani";
allow-transfer {172.16.4.4;};
also-notify {172.16.4.4;};
};
//reverse zone
zone "4.16.172.in-addr.arpa"
{
type master;
file "/etc/bind/rz.iiitkalyani";
allow-transfer {172.16.4.4;};
also-notify {172.16.4.4;};
};
```

Here, “fz.iiitkalyani” is the forward zone file. “rz.iiitkalyani” is the reverse zone files. And **172.16.4.4** is the IP address of secondary DNS server. We do this because; the secondary DNS will start to fetch the queries if primary server is down. (**also-notify {172.16.4.4;}; -- Primary DNS notifying secondary DNS of zone changes.**

Step 10: Set the proper permissions and ownership to the bind9 directory.

- *sudo chmod -R 755 /etc/bind*
- *sudo chown -R bind:bind /etc/bind*

Step 11: Check the DNS configuration files with commands:

- *sudo named-checkconf /etc/bind/named.conf*
- *sudo named-checkconf /etc/bind/named.conf.local*

If the above commands return nothing, it means DNS configuration is valid.

Step 12: Check the zone files using commands:

- *sudo named-checkzone iitkalyani /etc/bind/fz.iitkalyani*

Step 13: Check the reverse zone file:

- *sudo named-checkzone iitkalyani /etc/bind/rz.iitkalyani*

Step 14: Add the DNS server IP address. In our case, the DNS server IP is the same IP address of this machine itself.

- *sudo –i*
- *gedit /etc/network/interfaces*
- *dns-nameservers <IP Address>*

Step 15: Now restart the service.

- *sudo service bind9 restart*

Step 16: Testing primary DNS server. Verify DNS server using dig or nslookup commands.

- *dig google.com or nslookup iiitkalyani.ac.in*

Part 3: Install (in PC2) and configure Secondary DNS nameserver

You need a separate system to setup this server. We need secondary DNS server, because in case of any problem with Primary DNS, then secondary dns server will still resolve quires.

Step 1: Install BIND9

- *sudo –i*
- *sudo apt-get update*
- *sudo apt-get upgrade*
- *sudo apt-get dist-upgrade*
- *sudo apt-get install bind9 bind9utils bind9-doc*

Step 2: Configure secondary DNS server. Edit bind9 configuration file.

- *sudo –i*
- *gedit /etc/bind/named.conf*

Add the following lines if they are not there.

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

Step 3: Define zone files. To do so, edit *named.conf.local* file.

- *sudo –i*
- *gedit /etc/bind/named.conf.local*

Add or modify the following lines. Replace IP address and zone files with your own values.

```
zone "iiitkalyani.ac.in" {
type slave;
file "/var/cache/bind/fz.iiitkalyani";
masters { 172.16.4.3; };
};
zone "4.16.172.in-addr.arpa" {
type slave;
file "/var/cache/bind/rz.iiitkalyani ";
masters { 172.16.4.3; };
};
```

Here, 172.16.4.3 is the IP address of the primary DNS server. Please note that the path of zone files must be /var/cache/bind/ directory.

Step 4: Set the proper permission and ownership to the bind directory.

- *sudo chmod -R 755 /etc/bind*
- *sudo chown -R bind:bind /etc/bind*

Step 5: Edit network configuration file and add the primary and secondary DNS server's IP address.

- *sudo gedit /etc/network/interfaces*
- *dns-nameservers 172.16.4.3 (Primary server IP)*
- *dns-nameservers 172.16.4.4 (Secondary server IP)*

Step 6: Restart bind9 service to take effect the changes.

- *sudo systemctl restart bind9*

Step 7: Reboot your system

Step 8: Test DNS server.

- *dig rz.iiitkalyani*

PART 4: Configuring DNS client (in PC3)

You need a separate system to configure DNS client.

Step 1: Edit network configuration file in the client system:

- *sudo –i*
- *gedit /etc/network/interfaces*

Step 2: Add the nameserver IP addresses.

- *nameserver 172.16.4.3 (Name of the primary nameserver)*
- *nameserver 172.16.4.4 (Name of the secondary nameserver)*

Save and close the file.

Step 4: Reboot your system

Step 5: Test the DNS servers using any one of the following commands:

- *dig pri.iiitkalyani*
- *dig sec.iiitkalyani*
- *dig client.iiitkalyani*

Step 6: Solve the DSN Query

- *nslookup iiitkalyani.ac.in*

Assignment 1

- **Close all the browsers**
- **Open the Wireshark in client and Primary DNS server machine.**
- **Execute a DNS Query on the client machine**
- **Capture some packets on Client and DNS server**
- **Analyze the packets**

Assignment 2

- **Close all the browsers**
- **Open the Wireshark in client and Primary DNS server machine.**
- **Execute a reverse DNS Query on the client machine**
- **Capture some packets on Client and DNS server**
- **Analyze the packets**

Reference

1) https://help.ubuntu.com/lts/serverguide/dns-configuration.html
2) https://www.ostechnix.com/install-and-configure-dns-server-ubuntu-16-04-lts/