**Birla Institute of Technology &Science, Pilani**

**Computer Networks (CS F 303 / IS F 303)**

**Second Semester 2015-2016**

---

## Lab Session: 5

---

**Aim:** Configuration of DNS Server and its Analysis

**Objective:** To learn about the BIND package, which will be used to create a DNS server and connect different nodes to this host

**Description:** DNS or the Domain Name System is the method that the Internet uses to attach human-usable domain names to the machine-usable IP addresses that are almost never seen by users.Although TCP/IP uses IP addresses to locate and connect to hosts (computers and other TCP/IP network devices), users typically prefer to use friendly names. For example, users prefer the friendly name ***http.abc.rst.xyz***, instead of its IP address, ***#@.*#.&&.@#$**. The Domain Name System (DNS), defined in RFCs 1034 and 1035, is used on the Internet to provide a standard naming convention for locating IP-based computers.

On the Internet, before the implementation of DNS, the use of names to locate resources on TCP/IP networks was supported by a file called Hosts. Network administrators entered names and IP addresses into Hosts, and computers used the file for name resolution.

DNS use a namespace. A namespace is a grouping in which names can be used to symbolically represent another type of information, such as an IP address, and in which specific rules are established that determine how names can be created and used. Some namespaces, such as DNS, are hierarchically structured and provide rules that allow for the namespace to be divided into subsets of names for distributing and delegating parts of the namespace. Other namespaces, such as the Hosts namespace cannot be divided and must be distributed in their entirety. Because of this, using the Hosts file posed a problem for network administrators. As the number of computers and users on the Internet grew, the task of updating and distributing the Hosts file became unmanageable.

DNS replaces the Hosts file with a distributed database that implements a hierarchical naming system. This naming system allows for growth on the Internet and the creation of names that are unique throughout the Internet and private TCP/IP-based intranets.

**DNS using Linux**

Linux uses the 'host' command to perform these attachments, or looksups. To perform a forward lookup, use the syntax: ***$ host www.bits-pilani.ac.in***

The output (when performed within the campus network) that you should see:
*www.bits-pilani.ac.in is an alias for universe.bits-pilani.ac.in.universe.bits-pilani.ac.in* has address 172.22.2.53

To perform a reverse lookup: ***$ host 74.125.236.128***
74.125.236.128 one of the IP address of www.google.com. The output should read as:
*128.236.125.74.in-addr.arpa domain name pointer bom03s02-in-f0.1e100.net.*

BIND is an acronym for the Berkeley Internet Name Domain project, which is a group that maintains the DNS-related software suite that runs under Linux. The most well-known program in BIND is named, the daemon that responds to DNS queries from remote machines.

BIND package gives a machine the ability to be configured as a DNS server, by providing the following 2 files:

1. hosts
2. resolv.conf

A DNS client doesn't store DNS information; it must always refer to a DNS server to get it. The only DNS configuration file for a DNS client is the /etc/resolv.conf file, which defines the IP address of the DNS server it should use.

**Source (for above information) and Resources (for further reading):**

https://www.cs.rutgers.edu/~pxk/417/notes/content/ms_dns.pdf

https://help.ubuntu.com/lts/serverguide/dns.html

http://www.pearsonhighered.com/educator/product/Computer-Networking-A-TopDown-Approach-6E/9780132856201.page

http://www.utc.edu/center-information-security-assurance/pdfs/3.wireshark.dns.pdf

---

## Configuration of DNS Server:

(*Screenshots are provided at the end of the experimentation*)

---

### Step-1

Install the bind9 and dnsutils packages:

**sudo apt-get install bind9**
**sudo apt-get install dnsutils**

### Step-2:

Before you begin the configuration, edit the **/etc/hosts** file and change it to add the domain name as follows:

***127.0.0.1 ubuntu localhost.localdomain localhost***

***x.x.x.x ubuntu.example.com ubuntu***

* x.x.x.x = IP address of the machine, which you want to configure it as a DNS server

### Step-3:

Now, start configuring the DNS server by the editing the files in "**bind**" package.

Edit the file **/etc/bind/named.conf.options** and add the following lines to it at the end.

***forwarders***
***{ x.x.x.x;***
***};***

* x.x.x.x = IP address of the gateway or the DNS IP from ISP

**Restart the bind service: /etc/init.d/bind9 restart**

## Step-4:

**Primary Master:**

Here the bind will be configured as the primary master for the domain **ubuntu.example.com.**

Create the forward zone file by editing the:

**/etc/bind/named.conf.local**

Add the following lines to the file to create zones:

```
zone "example.com" {
type master;
file "/etc/bind/ubuntu.example.com";
};
```

Now use an existing zone file as a template to create the **/etc/bind/ubuntu.example.com** file:

**cp /etc/bind/db.local /etc/bind/*ubuntu*.example.com**

Edit the new zone file **/etc/bind/ubuntu.example.com** and add the following lines to it:

```
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA ubuntu.example.com. root.example.com. (
2 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Negative Cache TTL
;
@           IN    NS       ubuntu.example.com.
@           IN    A        127.0.0.1
@           IN    AAAA      ::1
ubuntu      IN     A       x.x.x.x
```

* x.x.x.x = IP address of the PC where DNS server is being configured

**Restart the bind service: /etc/init.d/bind9 restart**

## Step-5:

**Create the reverse zone file by editing the:**

**etc/bind/named.conf.local** and add the following:

```
zone "x.x.x.in-addr.arpa" {
type master;
notify no;
file "/etc/bind/db.x";
};
```

* x.x.x = The first three octets of DNS server IP address in reverse order

* x = The first octet of the DNS server IP Address

Now create the **/etc/bind/db.x** file:

**cp /etc/bind/db.127 /etc/bind/db.x**

* x = The first octet of the DNS server IP Address

Next edit **/etc/bind/db.x** changing the basically the same options as **/etc/bind/ubuntu.example.com:**

* x = The first octet of the DNS server IP Address

Add the following lines to the above edited file:

```
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@ IN SOA ubuntu.example.com. root.example.com. (
2 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Negative Cache TTL
;
@       IN      NS      ubuntu.
10      IN      PTR     ubuntu.example.com.
```

**Restart the bind service: /etc/init.d/bind9 restart**

## Step-6:

Edit the **/etc/resolv.conf** file and add the following lines:

**nameserver x.x.x.x**
**nameserver y.y.y.y**

* x.x.x.x = IP address of the PC where DNS server is being configured

* y.y.y.y = IP address of any other nameserver in the same LAN (optional)

## Step-7:

**Testing the Configuration:**

Type the following commands on the terminal:

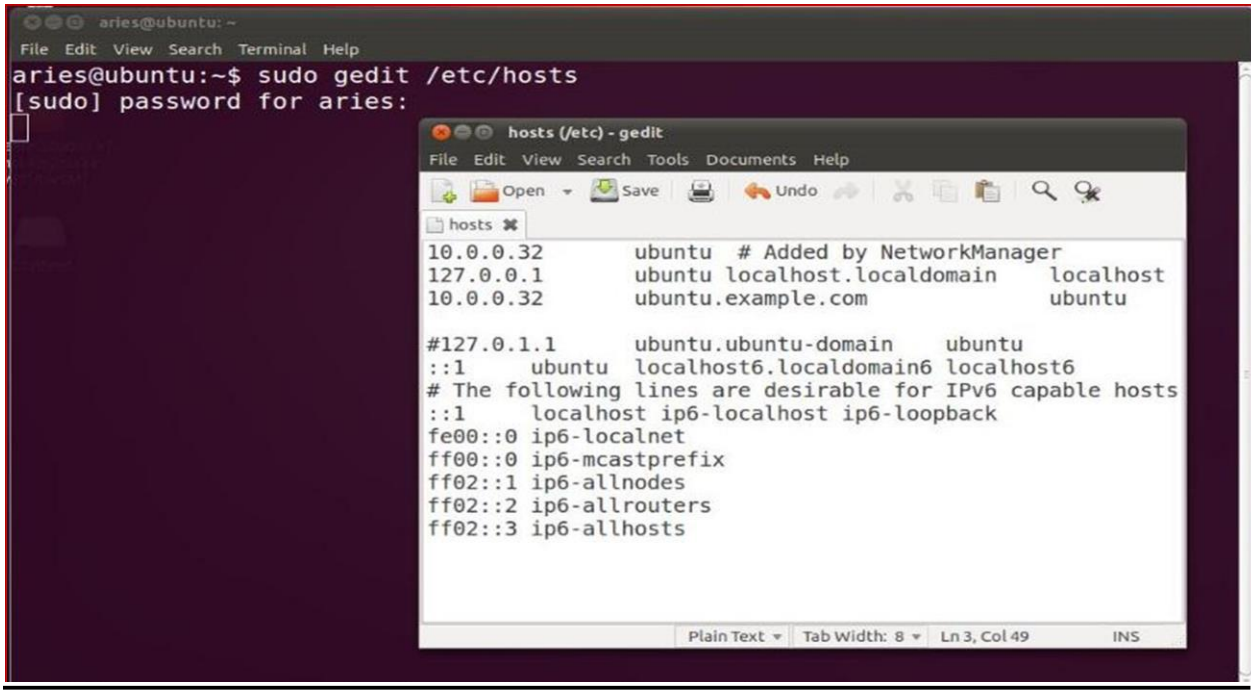
1. **dig -x 127.0.0.1**
2. **ping ubuntu.example.com**
3. **named-checkzone example.com /etc/bind/ubuntu.example.com**

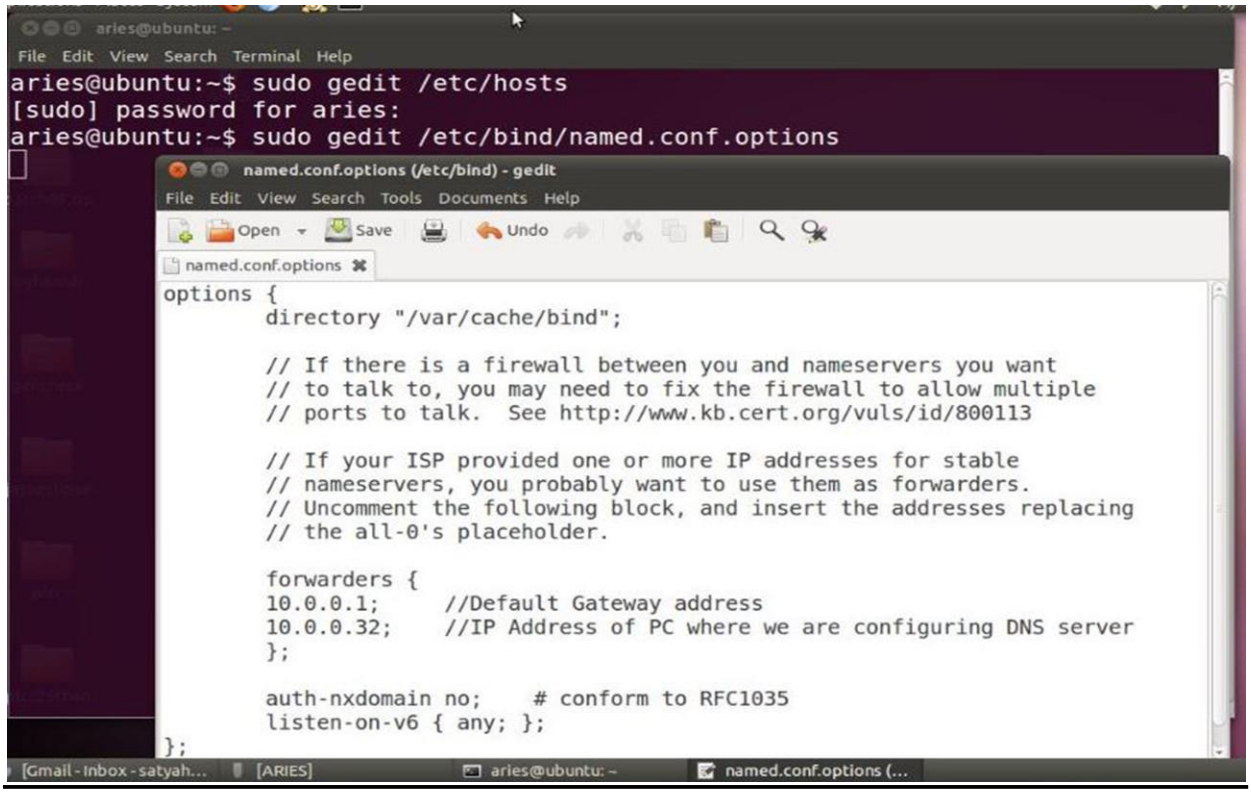
**{returns OK on Successful configuration}**

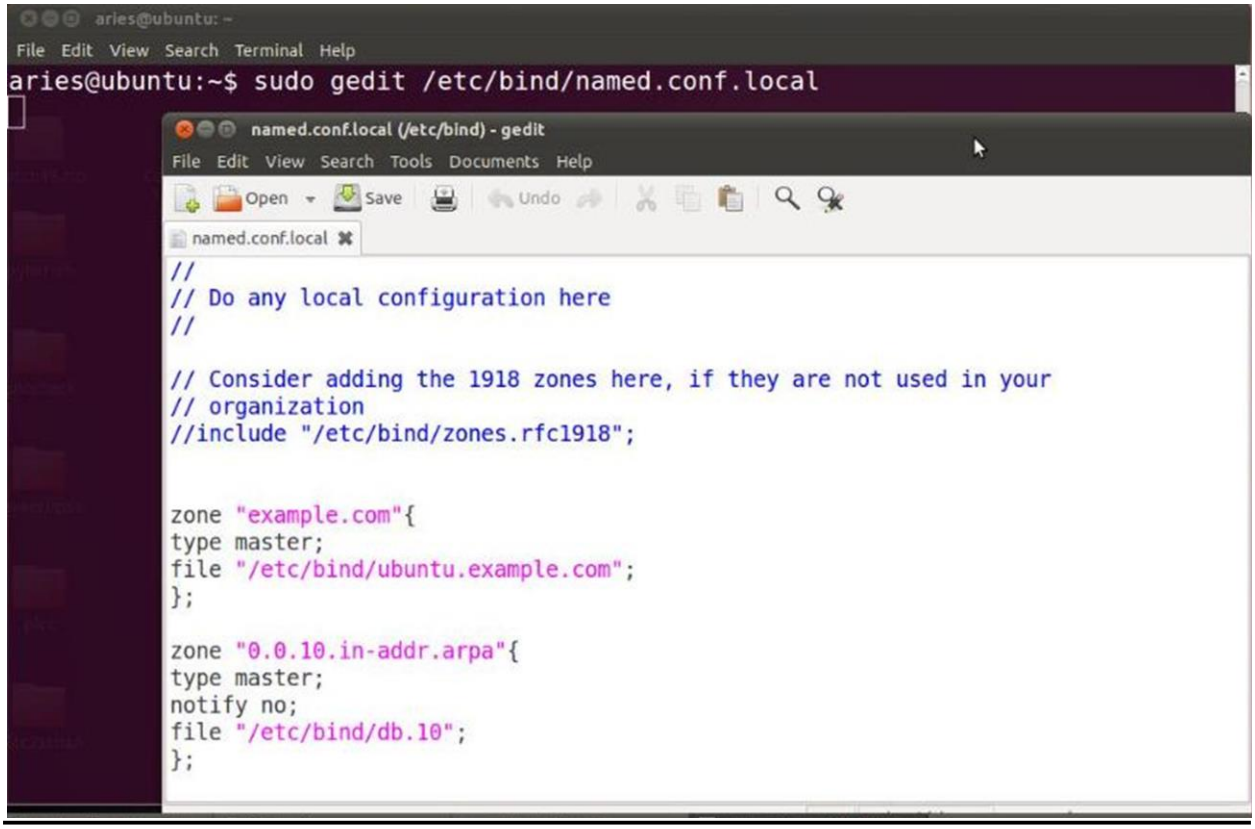
## Note:

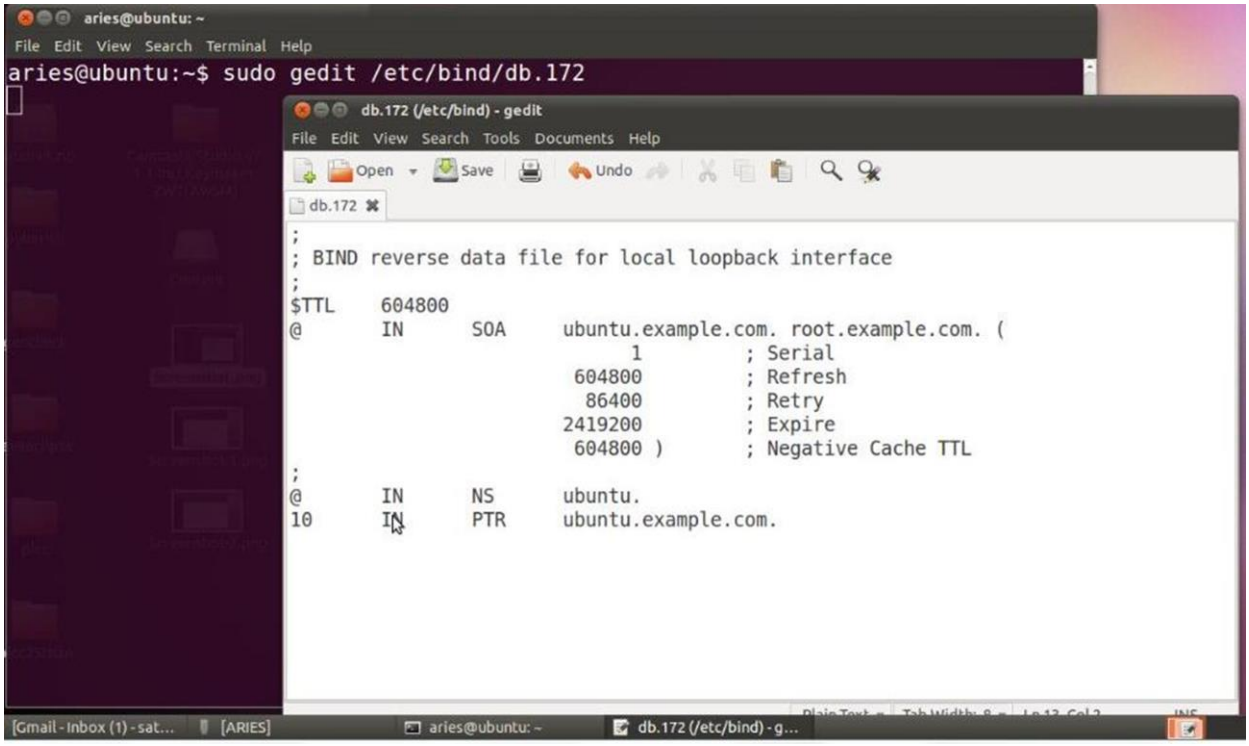
1. *If any issues when executing terminal commands, append "**sudo**" in beginning of each command.*
2. *Entire experiment was tested on Ubuntu 10.10 version by connecting to Default gateway (10.0.0.1) and "10.0.0.32" is IP address of the PC where DNS server is being configured.*
3. *Screenshots of the experimentation are provided hereafter.*
4. *For analysis of DNS using Wirshark follow the supplementary material on DNS provide with the **textbook**. Also available at:*
   http://www.utc.edu/center-information-security-assurance/pdfs/3.wireshark.dns.pdf

## Screenshots




aries@ubuntu: ~
File Edit View Search Terminal Help
aries@ubuntu:~$ sudo gedit /etc/bind/named.conf.local
named.conf.local (/etc/bind) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
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";
zone "example.com"{
type master;
file "/etc/bind/ubuntu.example.com";
};
zone "0.0.10.in-addr.arpa"{
type master;
notify no;
file "/etc/bind/db.10";
};


aries@ubuntu: ~
File Edit View Search Terminal Help
aries@ubuntu:~$ sudo gedit /etc/bind/db.172
db.172 (/etc/bind) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
db.172
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@ IN SOA ubuntu.example.com. root.example.com. (
1 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800 ) ; Negative Cache TTL
;
@ IN NS ubuntu.
10 IN PTR ubuntu.example.com.
[Gmail - Inbox (1) - sat...
[ARIES]
aries@ubuntu: ~
db.172 (/etc/bind) - g...