**DATA NETWORKING**

**LINUX PROJECT**

Group 4

**1. Rajesh Nadiminti**

**2. Sravani Kishore chepalli**

**3. Mahidhar Kakarla**

**4. Vineela Ganugapenta**

**CONTENTS**

A .Motivation

B. Understanding protocols

C .Required Tools

D. Integration of end systems

E. Testing

1.DNS

2.DHCP

3.Web Server

4.Fire wall

5.Backup

6.NFS

7.VPN

8.FTP

F.Future prospects

G.References

**Motivation**

Not all companieshave the ability to invest the capital to meet the requirements they want .Sometimes they don’t get the right resources or proposed designs .So the main objective for this project is to design a feasible server in terms of resources, interworking and security .The main objective is to simulate DHCP server to lease IP to clients .The client to access the webpage hosted by the web browser by resolving it’s IP from DNS, later the firewall to block the client from insecurity .The client must be able to receive backup files from backup server. This leads to the following tasks

* To build a DNS server with IPV4 and IPV6 records in forward and reverse domains and also implements a master and slave DNS server concept.
* To build DHCP server which can implement IPV4 and IPV6 addresses dynamically using client server protocol with specific lease time and reservation needs in an address protocol .
* To practically implement a web server with proper security implementations.
* To design a robust system which can systematically create a backup of every day work from the current server to different server.

**Understanding protocols**

1. **DNS Server**

The domain name system is a standard technology to maintain websites and other interne domains .It can run special purpose networking such as upgraded software ,featuring a public IP address and also contains a database of network names and internet host addresses .It is a client/server architecture .All the web browsers /DNS clients and issues requests to your internet providers .DNS clients must configure on their network to query the IP addresses of 1 or more DNS servers .On a network ,DNS server addresses can be configured on a router and automatically picked up by client devices or the addresses can be configured on each client individually .Network administrators with the help of internet service provider or third party DNS providers will get their valid addresses .

**Types of DNS Look up’s** :

DNS is most commonly used by web browsers which automatically converts internet domains to IP addresses. It is also used for:

* To deliver internet emails by finding the correct servers.
* Reverse look ups that converts IP addresses to the domain name.

DNS look up requests run over TCP and UDP, Port 53 default.

Ubuntu ships with BIND ,the most common program which maintains a name server on linux. DNS running linux computers are called name servers

**DHCP Server:**

Dynamic host configuration protocol is a client/Server protocol that automatically provides an internet protocol with its IP address and other related configuration such as subnet mask, gateway etc .It is an administrator of networks that manages and automate the assignment of the internet protocol addresses centrally.

Advantages:

* Changes in any IP addresses of the DNS Server can be changed at DHCP location which is more easy to access.
* If any integration of new computers in the network is needed it can contact DHCP for much reduced conflicts

**Web Server**

Web Server process requests of web users via HTTP. It uses client/server mode, and the World Wide Web hypertext transfer protocol. Every website must have a webserver program. Two leading Web servers are Apache, the most widely installed Web server, and Microsoft Internet Information server. Apache is most commonly used Web server.

**Firewall**

It is a security system created to prevent the unauthorized access of any private network. All the request messages and access messages which uses the intranet pass in through the firewall. Firewall examines each message and block certain messages which do not meet the security requirements. Firewall can be hardware or software but the ideal firewall will have the both. The advancement in the firewall has lead us to the remote access to the private networks by secure authentications and certificates.

A software firewall will protect us from outside attempts to control or gain access your computer. Software firewalls are installed on your computer and you can customize them allowing soe control over its function and protection features. Users can configure based on their needs by allowing some access to the network traffic that is preferable by them. This access can be done by closing and opening of the TCP and UDP ports.

**Backup**

**A** backup refers to copying and archiving the data by storing it in the computer.It can be mainly used when there is some loss of th data.In case the data gets corrupted or lost backup is used it is the primary purpose of it.Datalos sis experienced by many users.

Nowadays there is systematical backup of every data in daily basis in any small or large networks.In large scale company backup is must because there are many chances of overloading on the network due to large usage and the chance of the crashing is high .Serves can also be changed when we maintain this backup.

**Tools used**

Ubuntu 12.04 version is used for th implementation of tha above tasks.

* DNS Server: bind9.,dnsuils
* DHCP: isc-dhcp-server,radvd
* Web Server: Apache 2
* Firewall: iptables
* Backup: Rsync
* VPN: PPTP
* NFS: Apache2
* SSH: open SSH

**Integration of all devices:**

In this project we have different systems which are assigned with different task. All these systems must be integrated to form a single private network such as DHCP, DNS, and Web Server. Any client which is a part of this network must be assigned an IP address by the DHCP and it should be able to access the permitted Zones and DNS aids for it proper functioning. DNS slave will automatically keep the records on track. A switch is used to connect all the devices using Ethernet cables.

**DNS**

**Description of DNS:**

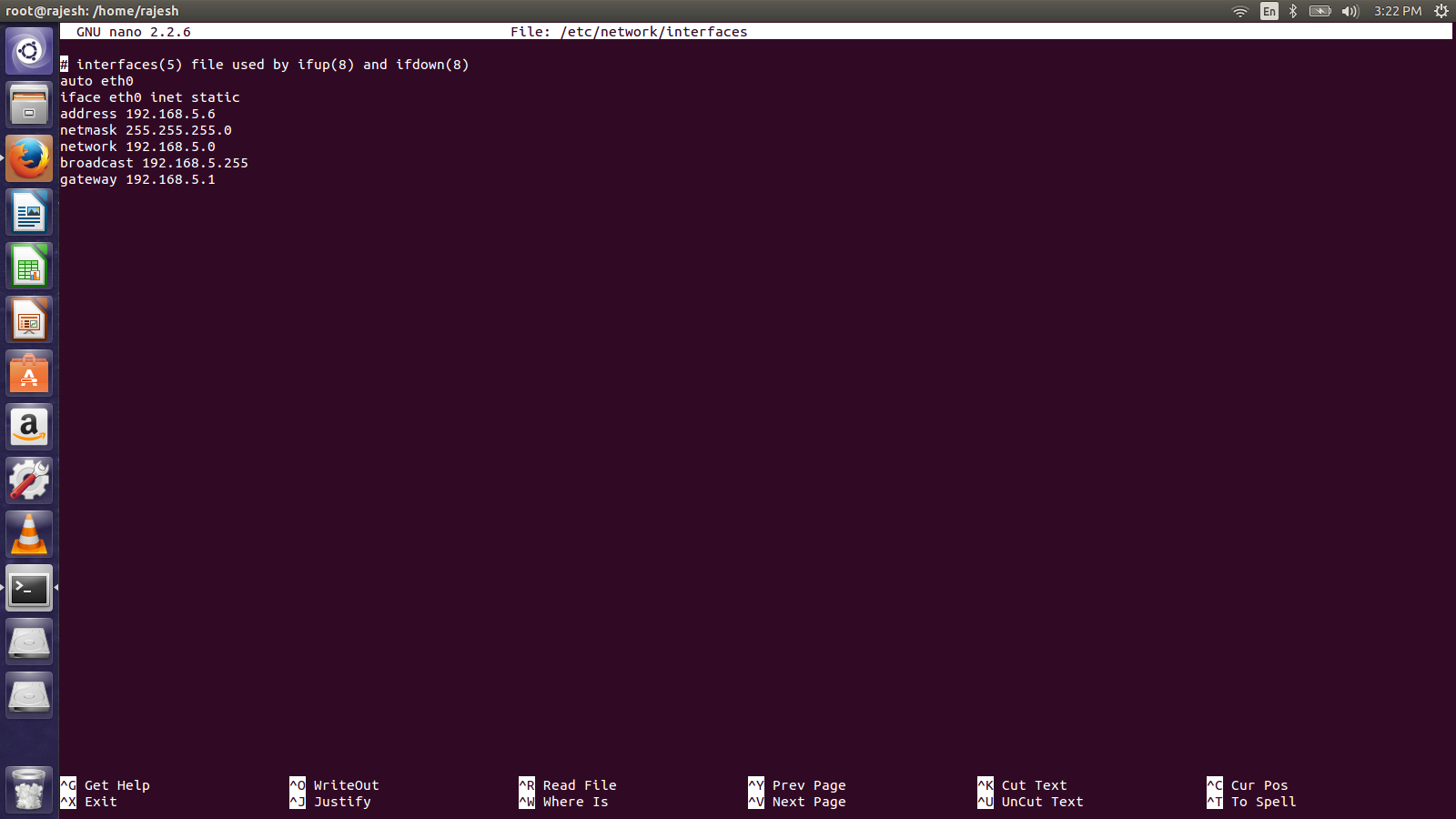
**Steps:**

1. **Configure server with static IP address**

**It is always ideal to configure the server** with static IP address, we know that DHCP assigns IP address dynamically to hosts for a random time and it gets expires after this time over.

1. **Edit the file/ETC/network/interfaces with the below commands**

**Sudo nano /etc/network/interfaces**



**3.Now restart the Networking process as we have made changes to interface files**

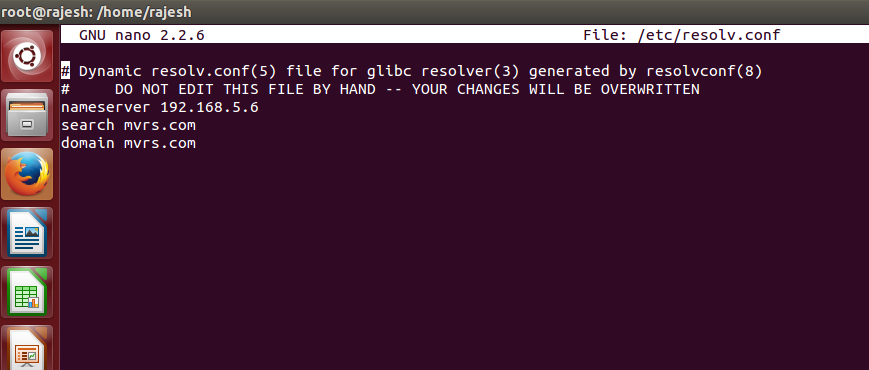
**Sudo /etc/init.d/networking restart**

**4. Install the BIND9 and dnsutils**

apt-get install bind9 bind9utils bind9-doc

sudo apt-get install dnsutils

nano /etc/resolv.conf



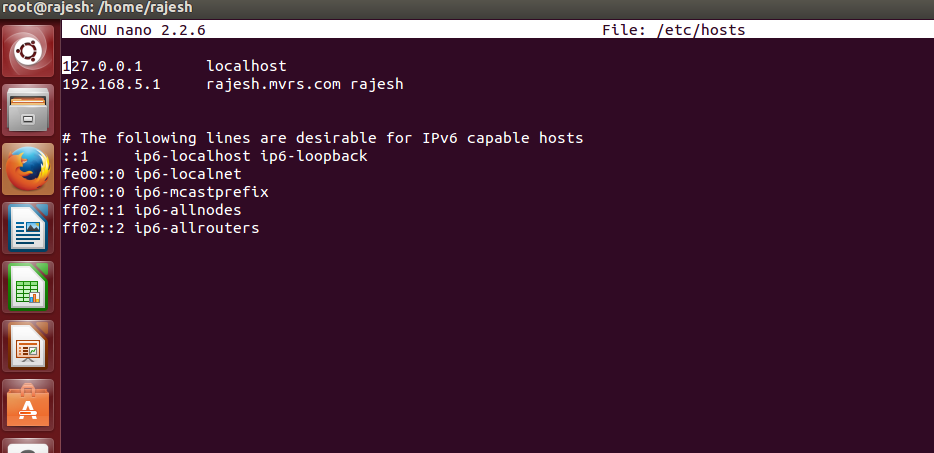
The configuration files re stored in /etc/bind directory.After installation configuration of the following steps need to be done.

Named.conf.options

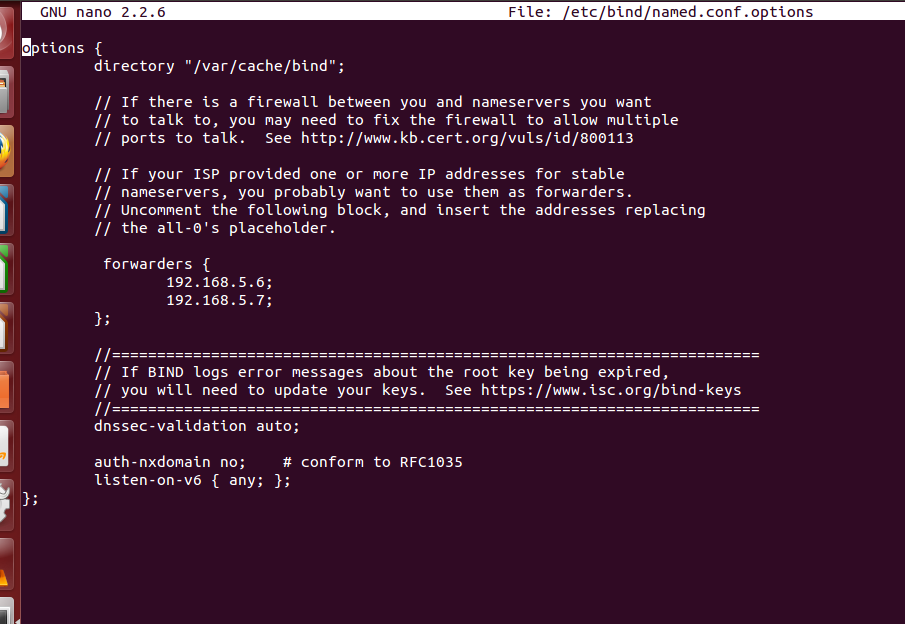
Named.conf.local

**6.Creating domain name for server**

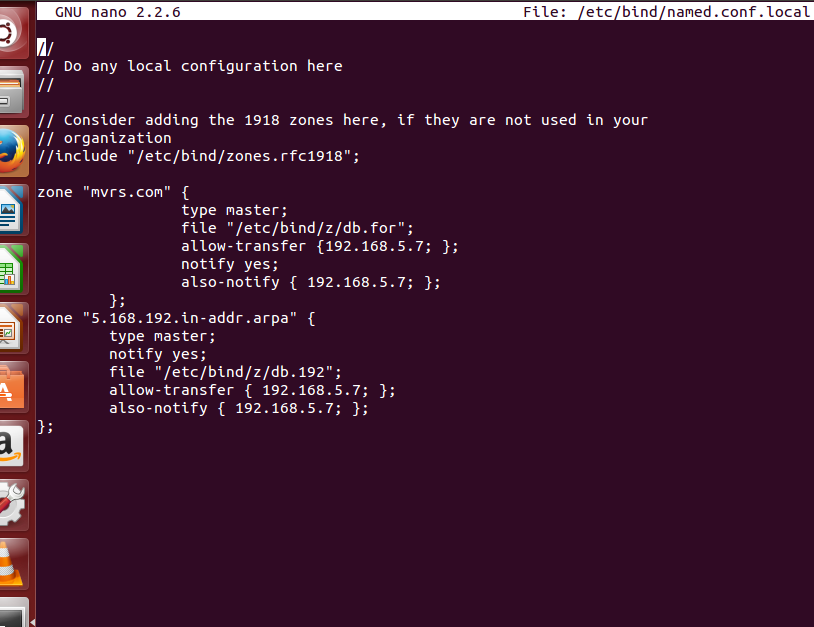
nano /etc/hosts



**7.Named.conf.options**



**8.named.conf.local**



9.**Creating zones directory** (we will create reverse and forward files in this directory)

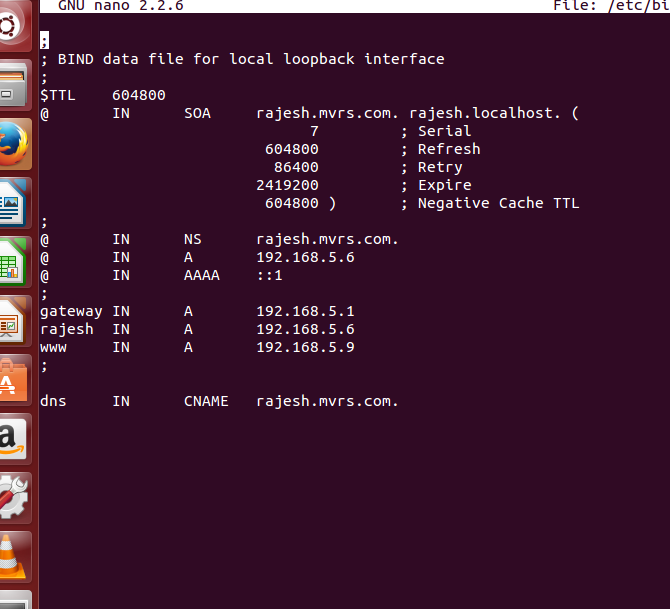
mkdir /etc/bind/z

10. **Copying the contents of default file db.local to db.for**

sudo cp /etc/bind/db.local /etc/bind/z/db.for

11.**Opening the file db.for for editing**

sudo nano /etc/bind/z/db.for

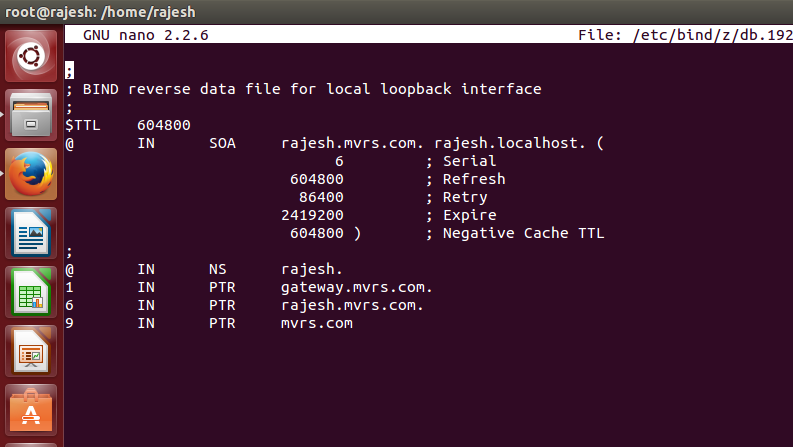


12. **Copying the contents of default file db.127to db.192**

sudo cp /etc/bind/db.127 /etc/bind/z/db.192

13. **Editing the file db.192**

sudo nano /etc/bind/z/db.192



**14. Restarting the bind9 service**

sudo /etc/init.d/bind9 start

**DNS SLAVE CONFIGURATIONS**

**1.Configure a server with static IP address**

**2.Edit the file/etc/network/interfaces with the below commands**

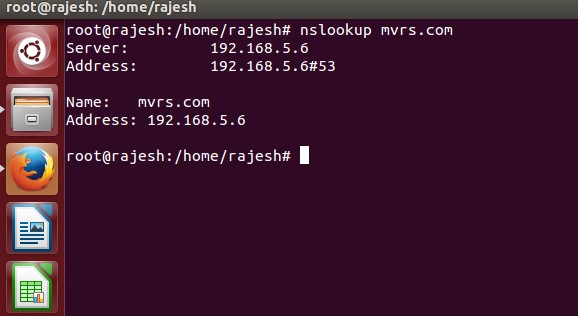
**All the steps from 3 to 7 remain the same**

**8.Named.conf.local**

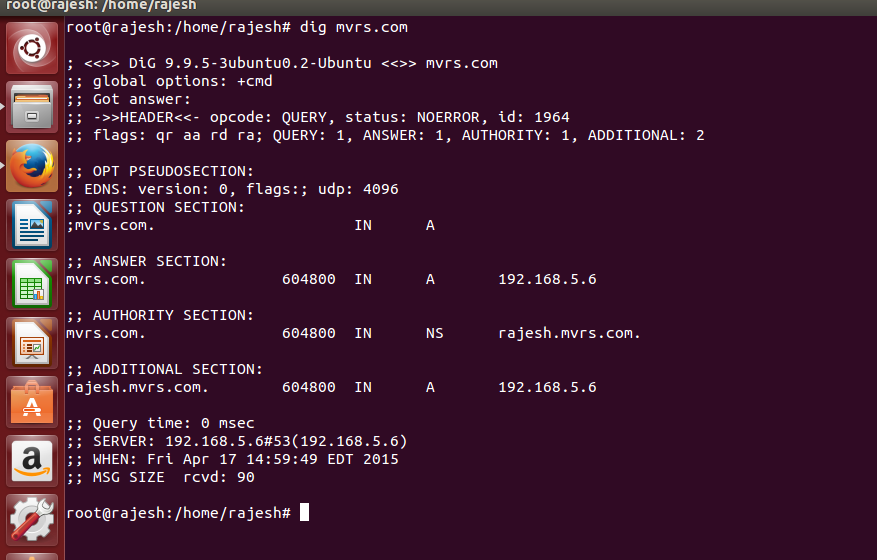
**Test Plans and Results**

The following commands were used for trouble shooting in both Maser and Slave servers

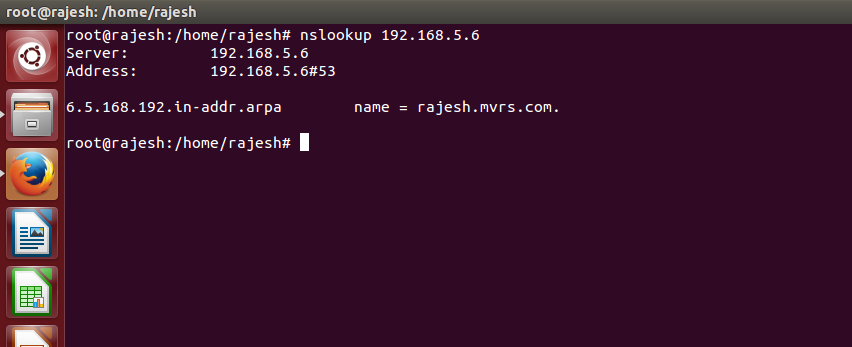
1. Check forward zones



Dig



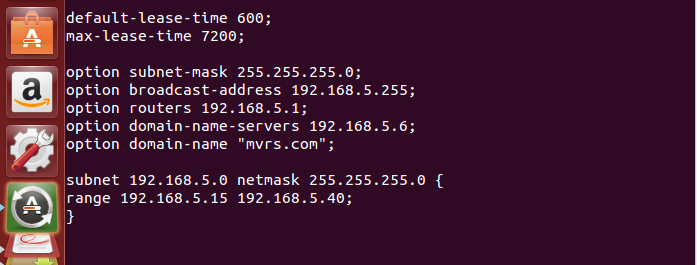
2. Check Reverse zones



**DHCP SERVER CONFIGURATION**

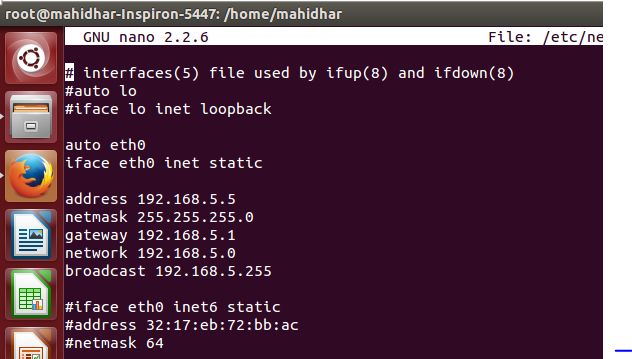
1. Configure the network interface to give a static IP address to the DHCP server

**/etc/network/interfaces**



2) Use the command **sudoapt-get install isc-dhcp-server** in the terminal to install it

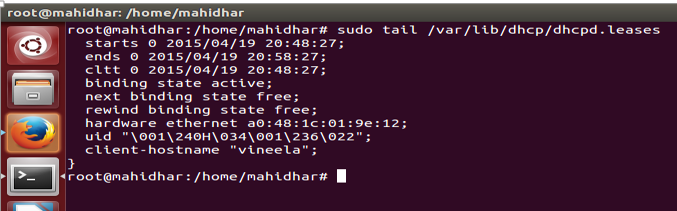
3) For the DHCP to assign Ipv4 addresses edit the file **/etc/dhcp/dhcpd.conf** and provide the range of address you want to the DHCP server to assign.



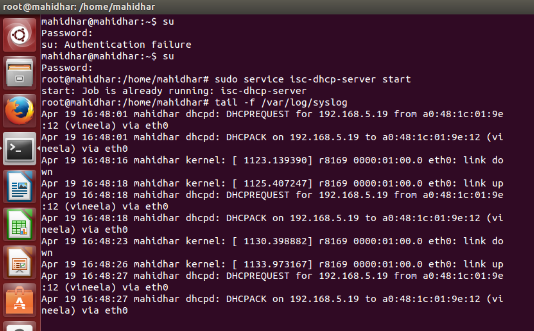
**Testing:**

1) Connect a client in the same network as DHCP server. The server will assign IP address to the client

Use command **sudo tail /var/lib/dhcp/dhcpd.leases** it will show client that is connected.



2. Use command **sudo tail –f /var/log/syslog**



**WEB SERVER**

**WEB SERVER CONFIGURATION:**

**1)**Update the Ubuntu before installing the web server

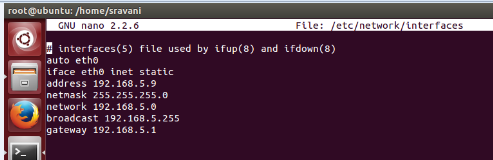
**Sudo apt-get update**

2)Install web server using command line tool in the terminal

**Sudo apt-get install apache2**

3) To assign a static IP address to the webserver

**Sudo nano /etc/network/interfaces**



4)To apply the static IP to we server we need to restart the networking interfaces

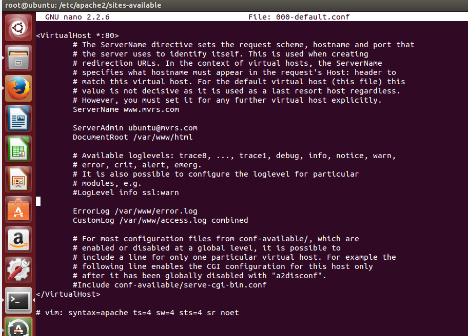
**sudo /etc/init.d/networking restart**

5)To check the applied changes regarding IP address

**ifconfig**

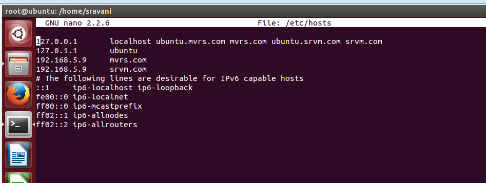
6)The sample web page location is at

**sudo nano /etc/apache2/sites-available/000-default.conf**

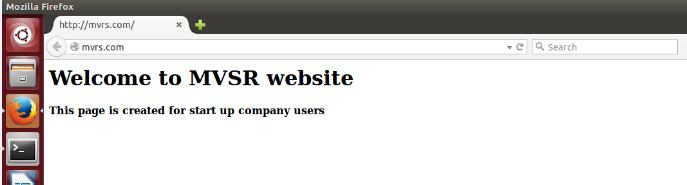


7) Now we can assign domain name to the webpage

**Sudo nano /etc/hosts**



8) To check the edited web page, go to any browser and type local host



**FIRE WALL**

**Step 1:-**

Install IP tables by giving command **sudo apt-get install ip tables**

**Step 2:-**

To block ICMP request on webserver use command as below:

**Sudo iptables –A INPUT –p icmp –j REJECT**

-A is to reject ICMP packets in to server (Input Chain)

**Step 3:-**

To reject telnet request at port 23 use following command

**Sudo iptables –A INPUT –p tcp –d port 23 –j REJECT**

**Step 4:-**

To allow access to particular IP’s

**Sudo ufw allow from (IP)**

**BACKUP**

**CONFIGURATION OF BACKUP FOR WEBSERVER**

Backup of system can be done in two ways in UBUNTU

1. Using GUI
2. Using command line tools

Some of the utilities available for the backup in Ubuntu server are tar,rsync,dump,duplicity,backup,and backup-manager

Here we have used rsync command line tool which effectively copy files from local hostusing ssh.local transmission of files is also easy using this.

**INSTALLATION OF RSYNC:**

**Command:sudo apt-get installrsync**

* **A backup server** mjst be created before configuring he rsync tool so that whenever here is a problem in the server he backup can be used.
* **The server IP address should be made static s that it can be in the same neywork of the main web server.**
* **By the help of allowing ssh on both side of the server the main server can be made availabl to the back up server.**
* **Rsync can be configured in such a way that the file containing the webpage of main web server is copied to the backup server.**

**CONFIGURATION OF RSYNS:**

**The** rsync can be configured using a command line in the terminal of backup server

**W**e mus see the backup server must be in a root mode before the execution

Sudo bash is used to enter into the rootmode.

After entering into the root mode the format of the command line to be executed at the backup server is

Sudorsync—dry-run—delete-azvv-e sshhostname@IP address of main web server:/Directory of Web page of main web server/ / directory of webpage of backup server/

Dry-run is included for the test basis initially for the start up.

Command:

**Sudorsync-delete-azvv-e**

**ssh 192.168.5.6:/VAR/www/index.html/home/rajesh/backup**

**VPN CONFIGURATION**

**CONFIGURATIONS AT THE VPN SERVER.**

**1.**Install pptpd and ufw

**sudo apt-get install pptpdufw**

2.open the ports needed. The guide suggest 22 ssh and 1723 for pptpvpn

**Sudo ufw allow 22**

**Sudo ufw allow 1723**

**Sudo ufw enable**

3.**Edit /etc/ppp/pptpd.conf** to add local vpn for IP’s of system

Local IP 192.168.5.6

Remote IP 192.168.5.15-70

If your system is VPS use public IP for local IP. If it is not and under local network use computer network IP.

We can even use ranges if the IP exists under your subnetwork

6.**edit/etc/ppp/chap-secrets** to add the authentication data

The format for **edit/etc/ppp/chap-secret** is

**[username] [service] [password] [Allowed IP Address]**

7.Restart pptpd, To run this command in terminal we use **sudo /etc/init.d/pptpd restart**

**8.Edit /etc/sysctl.conf**

Uncomment this for enable IP forwarding

**/etc/sysctl.conf:net.ipv4.ip\_forward=1**

To reload configuration: sudosysctl-p

**CONFIGURATIONS AT VPN CLIENT**

1. Install PPTP in client machine

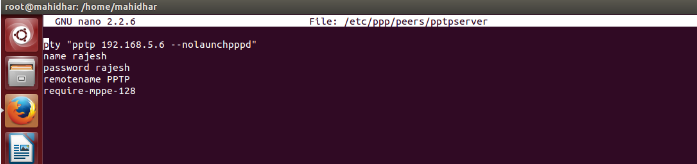
**sudo apt-get install pptp**

1. Add required Kernel module

**modprobe ppp\_mppe**

1. Now open the peers file and add the following lines using this commands

**sudo nano /etc/ppp/peers/pptpserver**

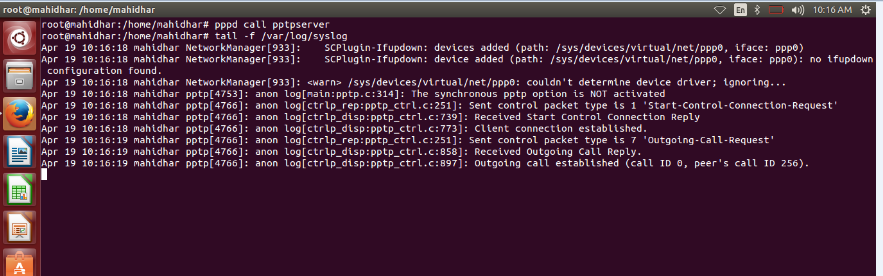


4. Now call the pptpd server using the command bellow. This will establish connection between pptpd server and client.

**Pppd call pptpserver**

5. Now open the syslog file in which we can see successful connection from PPTP server.

**Tail -f /var/log/syslog**



**Virtual hosting**

Virtual server hosting has features of shared as well as dedicated hosting. It is one among numerous types of web hosting accounts that you can select to host your website online. If you need to manage and setup a webpage on a server it is not only expensive but hard also. Through virtual hosting u can host many domain names on one server, it can also make server to distribute resources without having all services to utilize a single host name.

**1)** The process of creating virtual hosting is similar to webserver.

2) create new file in sites-available folder that will be used by the server to access the new site.

**Sudo nano /etc/apache2/sites-available/site2.conf**

3) Now change the directory to sites-available using the below command.

**Cd /etc/apache2/sited-available**

4) now open the new site2.conf file and modify the directory path and server name using below command

**sudo nano /site2.conf**

5) Now save the file and restart the apache server.

**Sudo /etc/init.d/apache2 restart**

**NFS**

1. Install the NFS server by using below command:

**Sudo apt-get install nfs-kernel-server**

**2.**Create a directory that can be shared.Provide the permissions

Sudo mkdir /home/sravani/dn

3.Create some files in the shared directory and create the user and group

Sudo chown sravani:mvrs /home/sravani/dn

4.Edit the **/etc/exports** file and enter the details of the directory which should be shared and provide permissions accordingly modify as shown below

/home/sravani/dn client-ip (rw,sync,no\_root\_bquash,no\_subtree\_check)

5. Restart the server by using the following command

**Sudo /etc/init.d/nfs-kernel-server restart**

**6.** **sudo show mount –e** can be used to see the directory or files

7. on the client side nfs –common by using command

**Sudo apt-get install nfs-common**

8. Now create a directory

Sudo mkdir –p /home/rajesh/NFS

9) Now connect both client and server and mount the files

Sudo mount 192.168.5.9:/home/sravani/dn /home/rajesh/NFS

10) To check the mounted files

mount –t NFS

To test NFS:

In Client:

1) to see the mounted file:

Sudo touch /home/rajesh/NFS/test.txt

FTP:

1) install vsftpd

Sudo apt-get install vsftpd

2) modify the permissions to the files using the vsftp.conf

Sudo nano /etc/vsftpd.conf

* Enable anonymous
* Enable local
* Enable write
* Uncomment ASCII upload
* Uncomment ASCII download
* Uncomment and modify ftpd\_banner
* Modify pam to ftp

3) add a group to share files

Groupadd mvrs

4) add user to access the group

Useradd –g mvrs –d /home/mahidhar/mvrs ftp

5) create password to the user ftp

Passwd ftp

Create new password: \*\*\*\*\*\*

Confirm new password: \*\*\*\*\*\*

6) to change the permissions to the user add the below line

Chmod 775 /home/mahidhar/FTP-shared

7) to add users to the group

Chwon root:mvrs /home/mahidhar/FTP-shared

8) start the ftp service

Sudo service vsftpd restart

To test FTP :

* ftp localhost
* enter username
* enter password
* now change the local directory “lcd /home/mahidhar/FTP-shared”
* to download file “get download “filename” ”
* to upload file “sent upload “filename” ”.