**Commands used**

**DNS**

**Steps to configure Master DNS server:**

1. Update Ubuntu

sudo apt-get update

1. Install BIND9 DNS server

sudo apt-get install bind9

1. Hostname of master DNS server is changed

sudo nano /etc/hostname

primary

1. The host file is edited by using following command

sudo nano /etc/hosts

127.0.0.1 localhost

192.168.40.5 primary.vms.com primary

1. Edit the /etc/network/interfaces file

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet static

address 192.168.40.5

netmask 255.255.255.0

network 192.168.40.0

broadcast 192.168.40.255

gateway 192.168.40.1

dns-nameservers 192.168.40.5

1. The head file is edited by using the following command

sudo nano /etc/resolvconf/resolv.conf.d/head

nameserver 192.168.40.5

nameserver 192.168.40.6

domain vms.com

search vms.com

1. Forwarders are configured by editing this file

sudo nano /etc/bind/named.conf.options

forwarders {

192.168.40.1;

192.168.40.5;

192.168.40.6;

};

1. Forward and Reverse Zones are created by using following commands

sudo nano /etc/bind/named.conf.local

# Forward zone

zone "vms.com" {

type master;

file "/etc/bind/zones/db.vms.com";

allow-transfer {192.168.40.6;};

};

# Reverse IPv4 Zone

zone "40.168.192.in-addr.arpa" {

type master;

file "/etc/bind/zones/db.192";

allow-transfer {192.168.40.6;};

};

1. Make a new directory zones

sudo mkdir /etc/bind/zones

1. Contents of local hostname file are copied to a new file db.vms.com so, that no damage is done to the main file.

sudo cp /etc/bind/db.local /etc/bind/zones/db.vms.com

1. The file db.vms.com is edited to create dns records for forward and reverse zones.

; BIND data file for [vms.com](http://vms.com/)

;

$TTL    604800

@       IN      SOA     [vms.com](http://primary.vms.com/).  [admin.vms.com](http://admin.vms.com/). (

                             2         ; Serial

                        604800      ; Refresh

                         86400          ; Retry

                      2419200          ; Expire

                        604800 )       ; Negative Cache TTL

;

@               IN      NS      [primary.vms.com](http://primary.vms.com/).

@                IN      A       192.168.40.5

primary      IN      A       192.168.40.5

;@ IN A 127.0.0.1

gateway IN A 192.168.40.1

www           IN      CNAME   [anything.vms.com](http://anything.vms.com/).

1. The contents of the local hostname file are copied to db.192 so, that the original file is not damaged.

;

; BIND reverse data file for vms.com

;

$TTL 604800

@ IN SOA primary.vms.com. admin.vms.com. (

1 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTl

;

IN NS primary.

1 IN NS gateway.vms.com.

5 IN PTR primary.vms.com.

**Steps to configure Slave DNS server:**

1. Repeat the first five steps of Master DNS slave.
2. Forward and reverse zones are created.

sudo nano /etc/bind/named.conf.local

* Forward Zone

zone "vms.com" {

type slave;

masters {192.168.40.5;};

file "/etc/bind/zones/db.vms.com";

};

* Reverse Zone

zone "40.168.192.in-addr.arpa" {

type slave;

masters {192.168.40.5;};

file "/etc/bind/zones/db.192";

};

**DHCP:**

DHCP configuration is done by using the following commands:

1. Update Ubuntu

sudo apt-get update

1. DHCP server is installed by using the following command:

sudo apt-get install isc-dhcp-server

1. IP address of the DHCP server is set statically:

sudo nano /etc/network/interfaces

auto lo

iface lo inet loopback

auto eth0

iface eth0 inet static

address 192.168.40.4

netmask 255.255.255.0

gateway 192.168.40.1

network 192.168.40.0

broadcast 192.168.40.255

dns-nameserver 192.168.40.5 192.168.40.6

dns-domain-search vms.com

1. IPV4 forwarding is configured:

sudo nano /etc/sysctl.conf

net.ipv4.conf.default.rp\_filter=1

net.ipv4.ip\_forward=1

1. Eth0 is made as the default interface by using the following command:

sudo nano /etc/default/isc-dhcp-server

INTERFACES="eth0"

1. For IPV4 the dhcpd.conf file is edited by using the following commands

sudo nano /etc/dhcp/dhcpd.conf

dhcpd.conf configuration file is created:

subnet 192.168.40.0 netmask 255.255.255.0 {

range 192.168.40.20 192.168.40.40;

option subnet-mask 255.255.255.0;

option broadcast-address 192.168.40.255;

option routers 192.168.40.1;

option domain-name "vms.com";

option domain-name-servers 192.168.40.5;

option domain-name-servers 192.168.40.6;

default-lease-time 600;

max-lease-time 7200; }

1. Resolv.conf file is edited by using the following commands:

sudo nano /etc/resolv.conf

nameserver 192.168.40.5

nameserver 192.168.40.6

1. DHCP server is rebooted

sudo init 6

1. DHCP server is restarted by using the following command:

sudo service isc-dhcp-server restart

**Webserver**

1. Appache2 package is installed

sudo apt-get update

sudo apt-get install apache2

1. Directory is changed to the user defined directory in appache2.conf file

sudo nano /etc/apache2/apache2.conf

<Directory /var/www/web/>

Options Indexes FollowSymLinks

AllowOverride None

Require all granted

</Directory>

1. Changed the document root and replaced it with the path of the folder in which the html file is stored.

sudo nano /etc/apache2/sites-enabled/000-default.conf

DocumentRoot /var/www/web

1. The HTML file is edited
2. IP address is assigned to the webserver from DHCP server.

sudo nano /etc/network/interfaces

auto eth0

allow-hotplug eth0

iface eth0 inet dhcp

1. To listen to HTTP request on IPv4

sudo nano /etc/apache2/ports.conf

NameVirtualhost \*:80

Listen 193.168.40.70:80

1. To restart the server

sudo /etc/init.d/apache2 restart

**Firewall:**

Firewall configuration is done to allow or deny a group of IP’s.

1. Allow the access to the webserver by using the following command

ufw allow from 192.168.40.75 to any

1. Access of webserver to a client is denied

ufw deny from 192.168.40.25 to any port 80

1. The traffic from network 192.168.40.0/24 is allowed on port 80

“sudo ufw allow from 192.168.40.0/24 to any port 80"

1. To check status

ufw status numbered

1. To enable firewall following command is used

ufw status enable

* A particular rule entered can be deleted by using the following command:

ufw delete (rule number)

**Backup**

**Steps to configure Backup server:**

1. Rsync protocol is used here, it provides versality for backing up and storing and synchronizing data. Along with rsync, ssh and sshpass commands are used. The following commands are used to install:

sudo apt-get install rsync

sudo apt-get install ssh

sudo apt-get install sshpass

1. Command used to configure the backup of a file with password protection.

sudo rsync -avz -progress -rsh=”sshpass -p hh ssh -1 newclient” /var/www/web/newclient@192.168.40.25: /home/newclient/backup/

1. Crontab command is used to automatically schedule the backup at any specified time.

sudo crontab -e

00 18 \* \* \* rsync -avz -progress -rsh=”sshpass -p hh ssh -1 newclient” /var/www/web/newclient@192.168.40.25: /home/newclient/backup/

**Steps to configure Backup client:**

1. Repeat the first step of backup server.
2. Make a new directory called as backup inside the home/newclient/

All the backup files will get stored inside this new directory called backup which will be send from webserver.

**Network File System**

**Steps to configure NFS server:**

1. Nfs-kernel-server and rpcbind pakages are installed in the ubuntu machine.

Commands used are:

sudo apt-get update

sudo apt-get install nfs-kernel-server

sudo apt-get install rpcbind

1. Create a directory named DATA1

sudo mkdir DATA1/

1. Provide read, write and execute permissions to this new directory

sudo chmod 777 DATA1/

1. Edit the export file

sudo cd /etc/

sudo nano exports

/home/nfsserver/DATA1 192.168.88.131 /255.255.255.0(rw,sync)

1. The process of giving the access of the NFS server to NFS client is started.

sudo /etc/init.d/nfs-kernel-server start

1. Do sudo showmount -e and check the NFS server and the IP associated.

**Steps to configure NFS client:**

1. Install nfs-common and rpcbind.

sudo apt-get install nfs-common

sudo apt-get install rpcbind

1. Create a new directory in the client so that when the connection between the NFS server and NFS client is done the data from the NFS server can be transferred and stored in this directory.

sudo mkdir NFS

1. Mount the data from the NFS server to the NFS client by providing the data location from the server to the destination path of the client.

Sudo mount 192.168.88.131: /home/nfsserver/DATA1 /home/nfsclient/NFS

**Testing**

DNS

* **nslookup** command is used to query DNS servers.

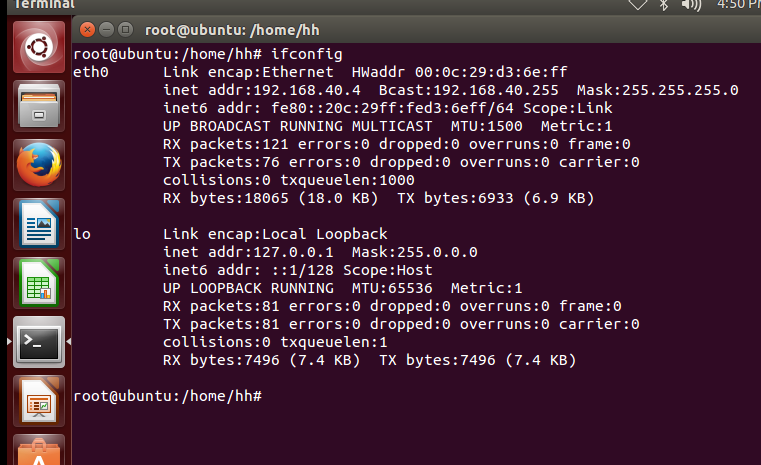
For example: nslookup vms.com

* **dig** command is used perform nslookups, the response is returned from the name servers.

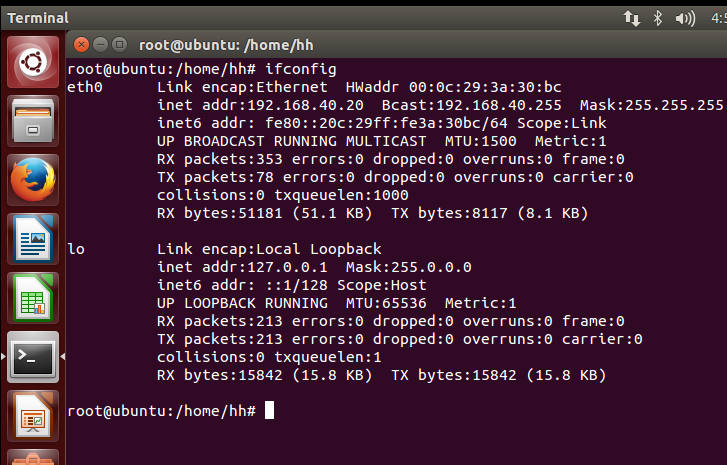
DHCP

* use the **ifconfig** command at client and check whether it has been assigned a IP address from the defined pool of IP addresses.
* On the client for the DHCP message the logs can be checked by using the **grep -i dhcp /var/log/syslog** command.

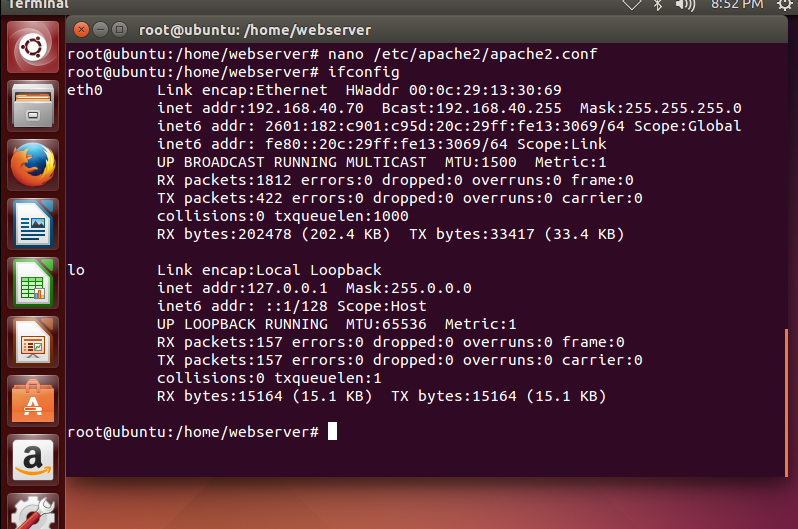
IP assigned to DHCP by DHCP server:



IP assigned to client by DHCP server:

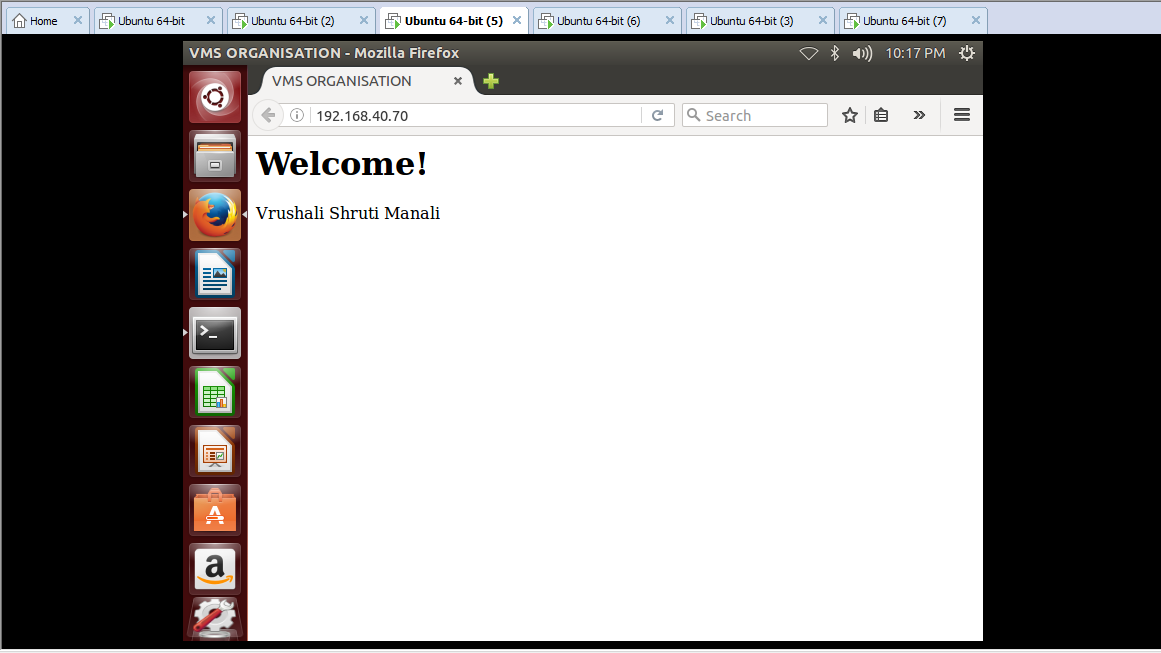


IP assigned to webserver by DHCP server:



Webserver

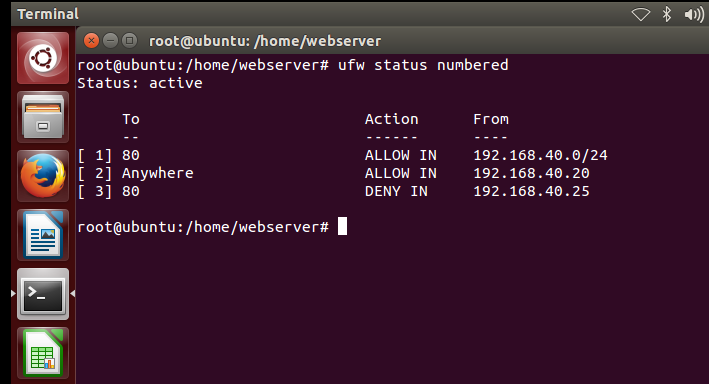
* The webserver can be tested by entering the URL of the website vms.com in the client machine. The webpage opens successfully indicating that the webserver and client are working as desired.

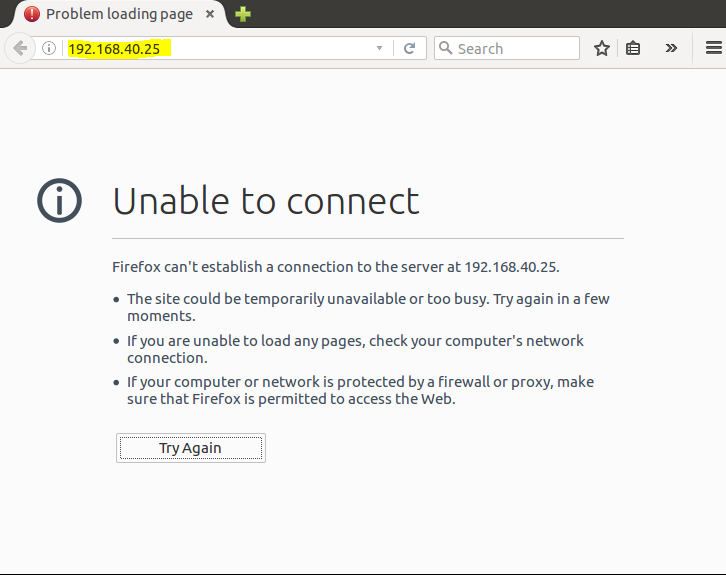


Firewall

* Firewall is build at the webserver blocking and allowing the desired IP’s. So, when the HTTP request is send from any client which is blocked to the webserver, the packet is blocked by the firewall and the access to the webpage is denied to that client thus protecting our system.

For example: HTTP request from the client with IP address 192.168.40.25 is blocked and hence the access to the webpage is denied.





Backup

* The testing of the backup can be done by checking the backup server after the scheduled time, and if the data from the web server is backed up on the back up server then it indicates that the functioning of the backup is successful.

NFS

* NFS can be tested by checking if the changes made in the nfsserver is reflected in the nfsclient machine after a connection is setup between the two machines.

