

1. Study of networking commands.

1. Hostname

It is a label that is assigned to a device connected to a computer network & is used to identify the device in various forms.

hostname

displays machine host name.

hostname -d

displays domain name the machine belongs to.

hostname -f

displays fully qualified host & domain name.

hostname -i

displays ip address of current machine.

2. Ping

It is a basic internet program that allows a user to verify that a particular ip address exists & can accept requests.

If you do ping www.google.com, it will display its IP address.

Use ctrl + c to stop.

OR ping ip address.

ping google1.com

- will show unknown host.

✓ 3. Netstat

netstat (network statistics) - Most useful & very versatile tool for finding connection to & from the host.

netstat -a (active internet connections)

Display all connections

netstat -t | netstat -t

Display only TCP connection

netstat -u | netstat -u

Display only UDP connection.

netstat -g

Display all multicast n/w subscribed by host.

netstat -l

List only listening ports.

e.g. netstat -a | less

netstat -at | less all tcp ports

netstat -au | less all udp ports

netstat -al | less both tcp & udp

4. Nslookup

Name Server Lookup (nslookup) useful tool for finding info about a named domain.

- It discovers hostname from IP address.
- It discovers IP address from host name.

Reverse domain lookup

nslookup google.com

nslookup ip add

display name & address.

e.g. nslookup 92.129.124.2

✓ 5. Traceroute / Tracert.

Trace the route the packets take b/w your system & the host named.

A hand utility to view no. of hops & response time to get a remote system or website is traceroute. You need an internet connection to make use of this tool.

traceroute machine_name or ip

traceroute google.com

route bet? PC & google

6. ARP (Address Resolution Protocol)

It manipulates or displays the kernel's IPv4 network neighbour cache. It can add entries to the table, delete one or display current content.

arp or arp -e

arp with no mode specifier will print the content of the table. It is possible to limit the no. of entries printed by specifying h/w address type, interface name or host address.

1. arp

2. arp & address
arp -a

arp -a

Displays the entries of address in h/w.

4. Telnet .

The telnet command is used for interac
comm' with another host using Telnet pro
telnet myhost.com

If a connection is established , the host
will prompt for a login name & password

Telnet helps to connect to a remote linux
computer .

eg. telnet localhost

2. Netstat & Route commands.

Using netstat & route commands do the following:-

1. View current routing table.

The routing table is an electronic table that is stored in a router or a networked computer. It stores the routes to particular n/w destinations.

netstat -r

e.g. Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metrix	Ref	Use	If	interface to
n/w or host	gw add							which packet for
	*	if none						-this route will be sent
		set						

default 192.168.0.24 0.0.0.0

genmask 255.255.255.255 for host destination

0.0.0.0 default route

2. Add & Delete routes.

route add -host 8.8.8.8 gw 192.168.0.20

netstat -rn

route del default gw 192.168.0.24

netstat -rn

3. Change default gateway

route del default gw 192.168.216.1

route add default gw 192.168.216.254
netstat -rn

OR

ip r change default via 192.168.216.1
netstat -rn

3. GUI configuration tools

Using GUI configuration tools to add / configure Ethernet card.

giving IP in Linux

1. Terminal method

OR Network - Edit

Nickname - eth0

✓ Active device when computer starts

Statically set IP address

Address 90.0.0.1

Subnetmask 255.0.0.0 Ok

Do you want to continue - yes

Save changes.

Deactivate previous IP

Click on activate for current IP

close

Check PC IP :-

Terminal

ifconfig eth0

2. Appc Places system ↑ Right click

- Add to panel

N/w monitor

+ Add

general - configure

Configure

Statically set IP address

Address 80.0.0.1

Subnet mask 255.0.0.0

yes

ok Deactivate

✓ Activate

close

Terminal

ifconfig eth0

4. Linux Network Configuration

eth 0 First wired interface

eth 1 Second wired interface

eth 0:0 First sub interface to physical interface 0

eth 0:1 Second sub interface to physical interface 0.

1. Determining IP address & MAC address using if-config command.

ifconfig (Interface Configuration)

ifconfig is a system administration utility in Linux like OS for n/w interface configuration.

It displays current n/w configuration inf.

MAC address : First line of o/p, labelled as HWaddr

IP address : inet addr.

(i) ifconfig

Displays all active interface details.

(ii) ifconfig -a

Displays inf. of all active/inactive n/w interfaces on server (eth0, lo, sit0)

(iii) ifconfig eth0

Displays details of specific n/w interface
(only eth0)

(iv) `ifconfig eth0 172.16.25.125`

Assign IP address to n/w interface (ip)

(v) `ifconfig eth0 netmask 255.255.255.224`

Assign netmask to n/w interface. (mask)

(vi) `ifconfig eth0 broadcast 172.16.25.63`

Assign broadcast to n/w interface (Bcast)

(vii) `ifconfig eth0 hw ether AA:BB:CC:DD:EE:FF`

change MAC (Media Access Control) address

of n/w interface (HWaddr)

(viii) `ifconfig eth0 172.16.25.125 netmask 255.255.255.224`

broadcast 172.16.25.63

Assign IP, netmask, broadcast to n/w interface.

(ix) `ifconfig eth0 mtu 1000`

change MTU (Maximum Transfer Unit) for n/w interface. (MTU)

2. Changing IP address using ifconfig.

`ifconfig eth0 172.16.1.100 netmask`

`255.255.0.0 up`

ifconfig eth0 down

- Deactivate eth0

ifconfig eth0 up

- Activate eth0.

3. Static IP address configuration by editing.

cd /etc/sysconfig/network-scripts

vi ifcfg-eth0

OR gedit ifcfg-eth0

DEVICE = eth0

IPADDR = 172.16.1.100

NETMASK = 255.255.0.0

BOOTPROTO = static

ONBOOT = yes

Save - Close

Terminal - ifc service network restart

ifconfig

Check Network.

4 Getting IP address using DHCP

cd /etc/sysconfig/network-scripts

vi ifcfg-eth0

OR gedit ifcfg-eth0

DEVICE = eth0

BOOTPROTO = dhcp

ONBOOT = yes

Save - close

Check Network - dhcp enabled.

Terminal - service network restart.

ifconfig.

5. Configuring /etc/hosts file

gedit /etc/hosts

change/ configure hostname, ip

Save - close

Terminal - ping .

5. Multiple IP addresses on single NIC

You can create the virtual interface by using the ifconfig command.

cd /etc/sysconfig/network-scripts

vi ifcfg-eth0

Save-close

cp ifcfg-eth0 ifcfg-eth0:1

cp ifcfg-eth0 ifcfg-eth0:2

cp ifcfg-eth0 ifcfg-eth0:3

vi ifcfg-eth0

i - Insert

DEVICE = eth0:1

BOOTPROTO = static

IPADDR = 192.168.1.80 (add non-existing IP)

NETMASK = 255.255.255.0

ONBOOT = yes

esc :wq

same for eth0:2 & eth0:3

ifconfig

ifup eth0:1

ifup eth0:2

ifup eth0:3

ifconfig

ifdown eth0:3

ifdown eth0:2

ifdown eth0:1

ifdown

6. Enable IP Forwarding.

Configure Linux as a router by enabling IP forwarding.

Forwarding allows the network packets on one network interface (i.e. eth 0) to be forwarded to another network interface (i.e. eth 1). This allows the Linux computer to connect (through bridge) route network traffic.

IP forwarding can be turned on to allow the computer to act as a gateway or router. In simple words, packet forwarding enables packets to flow through the Linux box from one network to another. The Linux kernel configuration parameter to activate this is named net.ipv4.ip_forward. It can be found in the file /etc/sysctl.conf.

Remove the # from the line related to packet forwarding.

Before:-

```
# Disable packet forwarding  
net.ipv4.ip_forward=0
```

After:-

```
# Enables packet forwarding  
net.ipv4.ip_forward=1
```

The above syntax enables packet forwarding only when you reboot, at which time Linux will create a file in one of the subdirectories of /etc.

RAM memory-based /proc file system. To activate the feature immediately, you have to force Linux to read /etc/sysctl.conf file with the sysctl command using -p switch. The syntax to use sysctl command is as follows:-

sysctl -p

net.ipv4.ip_forward = 1

net.ipv4.conf.default.rp_filter = 1

kernel.sysrq = 0

kernel.core_uses_pid = 1

7. Telnet & SSH

Telnet is a program that allows users to log into server & get a command prompt just as if they are logged into VGA console. A more secure method for remote login would be the' via SSH (Secure Shell), which uses varying degrees of encryption.

Telnet packages.

zpm - qa telnet

zpm - qa telnet - server

zpm - qa xinetd

xinetd managed service services

/etc/xinetd.d directory is used to manage services, store their configuration files.

Edit following.

/etc/xinetd.d/telnet &
make disable = no

Activate telnet service

service xinetd restart

Test whether Telnet process is running or not using netstat.

netstat -a | grep telnet

Telnet on next reboot.

chkconfig --list | grep telnet

Firewall settings.

Terminal - setup.

Firewall - Enable Disable.

Stopping a Telnet server at boot time.

chkconfig --level 35 telnet off.

Starting a Telnet server at boot time.

chkconfig --level 35 telnet on

Telnet connections.

adduser user

passwd user

New password :-

Retype :-

Login :-

Telnet other pc IP

e.g. telnet 192.168.1.51

Login :- Other PC's login

password.

mkdir Test

cdir Test

Check home.

configuring SSH server

`ps -q a | grep ssh`

or `ps -q a | grep openssh`

start ssh at boot time

`chkconfig --level 35 sshd on`

Start, stop, restart SSH after booting by running
the sshd initialization script.

`service sshd start`

`service sshd stop`

`service sshd restart`

Status of SSH

`pgrep sshd`

`/etc/ssh/sshd_config`

SSH configuration file is stored in above
directory. By default SSH listens on all your NICs
& uses TCP port 22.

Change the TCP port on which SSH listens.

Edit file

Remove # & make port no 435

`service sshd restart`

`netstat -an | grep 435`

Allowing connections .

The open SSH server listens for requests on port 22 & port 6010 for X11 forwarding by default. If custom IPTables rules are being need to block SSH then you need to configure firewall to allow SSH ports.

System → Administration → security level & firewall .

Firewall : Enabled

✓ SSH

Apply
OK .

Edit /etc/hosts .

Open ip netse

Save - Close .

ssh netse

Or ssh ownip

First login: generation of host keys .

ssh otherpc's ip

yes

root's password: redhat .

mkelir Test

amelir Test

copy files.

ls

root - scp file.exe root @ over.ip : /root/

User - scp /home/ other user / file user @ over.ip : /home/

Shutdown

shutdown now

Restart

shutdown -r now

Change password.

useradd

passwd

8. File Transfer Protocol (FTP)

To configure Linux FTP server using FTP (VSFTPD) is very secure.

FTP is an established protocol to copy files betⁿ servers over the Internet.

Port 21 is known as control port.

All commands & responses of FTP server go over the control port.

Port 20 is known as data port that is used for all subsequent data transfers betⁿ client & server.

Starting VSFTPD daemon

service vsftpd

service vsftpd start

status

service vsftpd stop

service vsftpd restart

Testing status of VSFTPD

Always test whether VSFTPD process is running by using command which lists all TCP & UDP ports on which the server is listening for traffic.

netstat -a | grep ftp | grep tcp:21

Change FTP greeting banner.

change default greeting banner in vsftpd.conf file to make it harder for malicious user to determine the type of system you have.

gedit /etc/vsftpd/vsftpd.conf

#Ftp-bANNER = Welcome to RMCE T site.
#Ftp other pc ip.

Using anonymous access.

Anonymous FTP is the selection of websites that need to exchange files with numerous unknown remote users. Users can log in as a user ftp or as a user anonymous to get access to the ftp site.

Steps:-

1. Check for the presence of a test file on FTP client.
ll

2. Connect to network via FTP

ftp <ip
anon

Name :- anonymous

Password :- anonymous

ftp > ha

turn on hash marks as progress
bar while downloading

ftp > bin

binary mode transfer

ftp > get reflpd - *

ftp > quit

221 Goodbye.

Trouble shooting FTP.

1. Initial setup failures could be caused by firewalls along the path bet' client & server blocking some or all types of FTP traffic. To disable default setting of firewall run following command:-

iptables -F

2. There is a possibility that you may not get access to ftp server due to SELinux policy. To disable SELinux ftp policy, run the following command:-

```
setenforce -f /etc/ftp.d.disable-trans
```

Adding FTP user with Read only access to a shared directory.

When anonymous FTP is not desired & ftp access needs to provide to group of trusted user with read-only access to shared directory.

Server side :-

```
mkdir /home/remote
```

R W E
7 = 1 1 1 binary

```
ls /home/
```

5 = 1 0 1

```
chmod 750 /home/remote
```

0 = 0 0 0

```
chmod -R 750 /home/remote
```

```
groupadd tecmp
```

```
chown root:tecmp /home/remote
```

```
useradd -g tecmp -d /home/remote user1
```

user2

user3

```
passwd user1
```

user2

user3

```
ls
```

```
ls /home/remote/
```

```
cp a.out /home/remote  
ls /home/remote/  
chmod -R 750 /home/remote/  
cd /home/remote/
```

ls

create file touch abc.txt
gedit abc.txt
service vsftpd restart
gedit /etc/vsftpd/vsftpd.conf
restart
grep decomp /etc/group

Make it in executable
chmod 777 abc.txt

Transfer files.

ftp other pc's ip
Name user:
password user:
get abc.txt

ftp > dir
check access
file

Check directory remote.
File received - abc.txt
edit abc.txt
make send file
put abc.txt
File transferred.

Multiple files

get *.txt
put *.txt

9. Configure Web Server.

Configure Apache (httpd) server.

A web server provides the ability to host websites or take advantage of web based app's.

In the simplest terms it is a place where a website that can be viewed in the Internet browser resides.

The Apache server is a powerful, efficient & extensible Web server. It uses httpd daemon, which is Apache Hyper Text Transfer Protocol (HTTP) server program. It is designed to be run as a standalone daemon process. Apache Web server supports virtual hosting on which you can host multiple website on single Apache server.

Apache start at boot.

chkconfig --level 345 httpd on

service httpd start

service httpd stop

service httpd restart

service httpd status

Test Apache process

psgrep httpd

Edit /etc/httpd/conf/httpd.conf

<Virtual Host * >

Default directives

</Virtual Host>

Use following commands to keep web pages of different websites into the directories.

<Virtual Host 192.168.1.160 : 80>

Document Root "/var/www/html/sites1"

Server Name www.abc.com

</Virtual Host>

<Virtual Host 192.168.1.161 : 80>

Document Root "/var/www/html/sites2"

Server Name www.bcd.com

</Virtual Host>

<Virtual Host 192.168.1.162 : 80>

Document Root "/var/www/html/sites3"

Server Name www.abc.com

</Virtual Host>

Set multiple IPs.

ifconfig eth0:1 192.168.1.161 netmask 255.255.255.0

ifconfig eth0:2 192.168.1.162 netmask 255.255.255.0

service network restart

ifconfig

Edit /etc/hosts.

192.168.1.160 www.abc.com

192.168.1.161 www.pqr.com

192.168.1.162 www.xyz.com

Use following commands to create document
directories to host multiple websites on a single
Apache.

cd /var/www/html

mkdir site1

mkdir site2

mkdir site3

(cd /var/www/html/site1)

// edit site2, site3

gedit site1

<html>

<head>

<title>

NPL

</title>

</head>

<body>

<h1>

Welcome to RMCE T..!!

</h1>

</body>

</html>

Save as index.html

service httpd restart

service named restart

Open browser

http://192.168.1.160

http://192.168.1.161

http://192.168.1.162

or

http://www.abc.com

http://www.pqr.com

http://www.xyz.com

1. Aim :- To study history & architecture of Unix / Linux O.S.

Lab objective :- To introduce basic Unix general purpose commands.

Theory - include architecture also.

Conclusion :- Unix has a deep history which helps to understand its effective functionality & architecture.

2. Aim :- To study & implement Unix general purpose utility commands.

Lab objective :- as above.

Theory :-

(1) cal

you can invoke 'cal' command to see the calendar of any specific month or a complete yr.

\$ cal cal of current month.

\$ cal 03 2018 cal of Month of March.

(2) date

It shows date & time to nearest second.
current

\$ date

(3) echo

It prints the given string.

Syntax :- \$ echo "String"

e.g. \$ echo "FAMT"

Syntax :- \$ echo -n "String"

(Don't print a new line)

e.g. \$ echo -n "FAMT"

(4) bc : The calculator

\$ bc

12+5

\$ bc 12 + 12 ; 2^2

o/p. 14 4

4

(5) passwd : Changing your password.

\$ passwd

passwd:

Enter your login password:

New password:

Re-enter new password:

(6) who

Displays the users who logged in to the system.

\$ who

(7) who am i

Displays the name of current user of this system.

\$ who am i

(8.) wc

It counts no. of characters, bytes, lines, chars in longest line.

\$ wc - m college.txt

\$ wc - c college.txt

\$ wc - l college.txt

\$ wc - L college.txt

(9.) tail

Prints required no. of lines in file counting from end of file.

Syntax :- tail - n filename

n: No. of lines to be displayed.

\$ tail - 2 one.txt

(10.) head

Prints required no. of lines in file counting from beginning of file.

Syntax :- head - n filename

n: No. of lines to be displayed.

head - 2 one.txt

For head

\$ cat one.txt

Welcome to FAMT

Ratnagiri

IT dept.

Unix lab

For tail

\$ cat one.txt

Welcome to FA

Ratnagiri

-1-

-1-

o/p :- Welcome to FAMT

Ratnagiri

o/p :- IT dept

Unix lab

(11) cat

a) Create a new file

Syntax :- cat > filename

\$ cat > one.txt

hi

Welcome to Unix lab

FAMT

Ratnagiri

Press ctrl + z to save

[z]+ stopped cat > one.txt

b) Display contents of file

Syntax : cat * filename

\$ cat one.txt

(12) mkdir

Make directories

Syntax :- mkdir filename

\$ mkdir programme

\$ ls

(13) cd

Change directory.

Syntax :- cd directory name

\$ cd programme

\$ cd ..

\$ cd programme

\$ mkdir shell program

\$ cd shell programs

\$ cd

(14) pwd

Print working directory

\$ pwd

\$ cd

\$ pwd

(15) ls

List files & directories

\$ ls

ls -l : lists files & directories in long listing mode

\$ ls -l

\$ ls -a

\$ ls -z

(16) `mv`

a) Move a file to directory

Syntax :- `mv source file destination directory`
\$ `mv coll.txt programme`
\$ `cd programme`
\$ `ls`

a) Move contents of one file to another .

Syntax :- `mv source file destination file`.
\$ `cat one.txt`

hi, welcome to Unix lab
FAMT

\$ `mv one.txt new.txt`.

\$ `cat new.txt`

hi, Welcome to IT lab

FAMT

(17) `rm` : Remove a file

Syntax : `rm filename`

\$ `ls`

\$ `rm new.txt`

\$ `ls`

(18) `rmdir`

Remove a directory

Syntax :- `rmdir Directory name`

\$ `ls`

\$ `rmdir`

(19) rm -rf (remove a directory which is not empty)

Syntax : rm -rf directory name

\$ ls

rm -rf program

\$ ls

(20) man

\$ man

Display user manual.

(21) finger

Used to look up user on a remote m/c.

\$ finger

(22) clear

Clear the terminal screen.

\$ clear.

(23) more

lets you to view text files or other type in scrollable manner.

\$ more.

(24) logout

(25) Shutdown

\$ shutdown now

3. Aim:- To study Unix networking & file system commands.

Lab objective:- To learn n/w unix commands

Theory:-

1. Netstat

2. Ping

3. Hostname

4. Traceroute

5. Tracepath

It performs a very similar f? to traceroute
The main difference is that tracepath doesn't take complicated options.

tracepath machine-name or ip

6. FindSmb

It is used to list inf? about machines that respond to SMB name queries.

e.g. windows based machines sharing their hard disks.

Syntax:- findsmb

? nmap.

It is network exploration tool & security scanner. It is very advanced n/w tool used to query machine as to whether they are up, by what ports are open on those machines.

nmap machine_name

8. Network configuration :

a) ifconfig

b) ifup

use ifup device name to bring an interface up by following a script (which will contain your default n/w settings.)

ifup eth0

will bring eth0 up if it is currently down

c) ifdown

ifdown eth0

d) ifcfg

use ifcfg to configure a particular interface.

e.g. change eth0 from 192.168.0.1 to 192.168.0.2

ifcfg eth0 del 192.168.0.1

ifcfg eth0 add 192.168.0.2

The first command takes eth0 down & removes that stored IP address & second one brings it back up with new address.

e) route:-

The route command is used to display
modify the routing table. To add a gateway as
the default -

route add default gw some-computer

Conclusion :-

This experiment explains various tools
which can be useful when n/w with other comp
both within n/w & across the internet, obtain
more infⁿ about other computers. This exp also
include infⁿ on tools for n/w configuration,
file transfer & working with remote m/c.