**Networking tools**

One can use verity of networking to perform task such as obtaining information about other system on your network ,access other system to communicate directly with other users.

Commends:

1. Ping.
2. Finger
3. Host
4. nslookup
5. Trace route
6. netstat

ping:

ping-Packet internet groper

it is used to check connectivity between host and server.

It takes input url or your ip.

A picture containing text, computer, file

Description automatically generated

Syn:

Ping option destination

Ex:

Ping -c 2 [www.youtube.com](http://www.youtube.com)

This commend controls the no of pings

Netset:

It displays various network information such as

* network connectivity
* routing tables
* interface utilities
* masquerad connection
* multicast membership

ex:

netstat

Graphical user interface, text

Description automatically generated

To list sockets:

Netstat -at

To display all tcp ports

Text

Description automatically generated

netstat -au – list all udp

netstat -l – list only listening ports

netstat -lu – list onlylistening udpports

netstat -lt – list only listening tcp ports.

netstat -lx – listening unix ports.

netstat -s ­ -statics for all ports.

Telnet:

* It is a type of protocol enable one computer to connect local computer.
* Used to standard Tcp/ip protocol for virtual mechine.
* Which computer connect which computer accept connection is known as remote computer.
* When connection established between local and remote control during telnet option whatever doing in remote computer it will display in local computer.
* Syntax:

telnet domainname or ip portnumber

tenet installing process:

sudo apt update

sudo apt install telnetd -y

To verify weather installed or not:

systemctl status inetd

Text

Description automatically generated

Text

Description automatically generated

telnet localhost commend:

Text

Description automatically generated

firewalld:

firewalld is an firewall management tool in linux.

firewalld command does

* firewalld uses the command line utility firewall-cmd to **configure and manipulate rules**.
* Before we begin to configure this, we need to make sure that the service is running.
* Using the systemctl command, can enable, disable, start, stop, and restart the firewalld service.

**firewall-cmd --get-zones**



To check firewall active or inactive:

systemctl status firewalld

Text

Description automatically generated

**firewall-cmd –zone=public –list-all** -commend lists the all active services,ports,richrules publiczones

Text

Description automatically generated

**Adding ports in the fire wall:**

**firewall-cmd --permanent --zone=public --add-port=port number**

**ex:**

**Text

Description automatically generated with low confidence**

**Removing ports in the fire wall:**

**firewall-cmd --zone=public --remove-port=port number**

**A screenshot of a computer

Description automatically generated with medium confidence**

**Adding,removing the services:**

****

**Text

Description automatically generated**

**Block incoming and outgoing packets(panic mode)**

**If you want to block any incoming or out going use panic -on commend.**

**Commends**

**sudo firewall-cmd --panic-on**

**sudo firewall-cmd --panic-off**

Text

Description automatically generated