LAB ACTIVITY -1

AIM:- To study basic network commands in Linux.

COMMANDS LEARNT:-

ifconfig

ping

tracert/traceroute

nslookup

netstat

ip

arp

rarp

dig

route

ABOUT EACH COMMAND:-

**1.ifconfig**

It is used to configure the kernel-resident network interfaces. It is used at boot time to set up interfaces as necessary. After that, it is usually only needed when debugging or when system tuning is needed.

If no arguments are given, ifconfig displays the status of the currently active interfaces. If a single interface argument is given, it displays the status of the given interface only; if a single -a argument is given, it displays the status of all interfaces, even those that are down. Otherwise, it configures an interface.

Snapshot:

dell@dell-OptiPlex-3050:~$ ifconfig

enp2s0 Link encap:Ethernet HWaddr 50:9a:4c:28:cb:02

inet addr:10.0.1.169 Bcast:10.255.255.255 Mask:255.0.0.0

inet6 addr: fe80::c9be:fa:54eb:5427/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:747779 errors:0 dropped:485 overruns:0 frame:0

TX packets:184618 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:540638497 (540.6 MB) TX bytes:11405194 (11.4 MB)

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:65536 Metric:1

RX packets:3952 errors:0 dropped:0 overruns:0 frame:0

TX packets:3952 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1

RX bytes:536602 (536.6 KB) TX bytes:536602 (536.6 KB)

wlp3s0 Link encap:Ethernet HWaddr bc:a8:a6:6a:0f:fe

inet addr:10.147.40.59 Bcast:10.147.127.255 Mask:255.255.128.0

inet6 addr: fe80::3c70:5302:45cf:2aec/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:420 errors:0 dropped:0 overruns:0 frame:0

TX packets:611 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:62855 (62.8 KB) TX bytes:82348 (82.3 KB)

**2.ping**

PING (Packet INternet Groper) command is the best way to test connectivity between two nodes. Whether it is Local Area Network (LAN) or Wide Area Network (WAN). Ping use ICMP (Internet Control Message Protocol) to communicate to other devices. You can ping host name of ip address using below command.

ping uses the ICMP protocol’s mandatory ECHO\_REQUEST datagram to elicit an ICMP ECHO\_RESPONSE from a host or gateway. ECHO\_REQUEST datagrams (“pings”) have an IP and ICMP header, followed by a struct timeval and then an arbitrary number of “pad” bytes used to fill out the packet.

Snapshot:

ping 10.0.8.106

PING 10.0.8.106 (10.0.8.106) 56(84) bytes of data.

64 bytes from 10.0.8.106: icmp\_seq=1 ttl=64 time=0.457 ms

64 bytes from 10.0.8.106: icmp\_seq=2 ttl=64 time=0.315 ms

64 bytes from 10.0.8.106: icmp\_seq=3 ttl=64 time=0.421 ms

64 bytes from 10.0.8.106: icmp\_seq=4 ttl=64 time=0.336 ms

64 bytes from 10.0.8.106: icmp\_seq=5 ttl=64 time=0.421 ms

64 bytes from 10.0.8.106: icmp\_seq=6 ttl=64 time=0.321 ms

64 bytes from 10.0.8.106: icmp\_seq=7 ttl=64 time=0.257 ms

64 bytes from 10.0.8.106: icmp\_seq=8 ttl=64 time=0.300 ms

^C

--- 10.0.8.106 ping statistics ---

8 packets transmitted, 8 received, 0% packet loss, time 7000ms

rtt min/avg/max/mdev = 0.257/0.353/0.457/0.068 ms

**3.traceroute**

traceroute attempts to trace the route an IP packet would follow to some Internet host by launching probe packets with a small ttl (time to live) then listening for an ICMP "time exceeded" reply from a gateway. It start its probes with a ttl of one and increases this by one until it gets an ICMP "port unreachable" (or [TCP](https://www.computerhope.com/jargon/t/tcpip.htm)reset), which means we got to the "host", or hit a max (which defaults to 30 [hops](https://www.computerhope.com/jargon/h/hops.htm)). Three probes (by default) are sent at each ttl setting and a line is printed showing the ttl, address of the gateway and round trip time of each probe. The address can be followed by additional information when requested. If the probe answers come from different gateways, the address of each responding system will be printed. If there is no response within a 5.0 seconds (default), an "**\***" (asterisk) is printed for that probe.

Snapshot:

traceroute www.9gag.com

traceroute to www.9gag.com (151.101.194.133), 30 hops max, 60 byte packets

1 10.0.0.5 (10.0.0.5) 0.266 ms 0.233 ms 0.210 ms

2 1.6.91.156 (1.6.91.156) 2.856 ms 3.276 ms 3.271 ms

3 \* \* \*

4 \* \* \*

5 \* \* \*

6 \* \* \*

7 \* \* \*

8 \* \* \*

9 \* \* \*

10 \* \* \*

11 \* \* \*

12 \* \* \*

13 \* \* \*

14 \* \* \*

15 \* \* \*

**4.nslookup:**

Nslookup is a program to query Internet domain name servers. Nslookup has two modes: interactive and non-interactive. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain. Non-interactive mode is used to print just the name and requested information for a host or domain.

Snapshot:

nslookup www.knowyourmeme.com

Server: 127.0.1.1

Address: 127.0.1.1#53

Non-authoritative answer:

Name: www.knowyourmeme.com

Address: 208.115.103.34

**5.netstat:**

It is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. The type of information printed is controlled by the first argument, as follows:

(none)

By default, netstat displays a list of open sockets. If address families aren’t specified, then the active sockets of all configured address families will be printed.

--route , -r

Display the kernel routing tables. See the description in route(8) for details. netstat -r and route -e produce the same output.

--groups , -g

Display multicast group membership information for IPv4 and IPv6.

--interfaces, -i

Display a table of all network interfaces.

--masquerade , -M

Display a list of masqueraded connections.

--statistics , -s

Display summary statistics for each protocol.

Snapshot:

netstat https://www.reddit.com/r/dankmemes/

Active Internet connections (w/o servers)

Proto Recv-Q Send-Q Local Address Foreign Address State

tcp 1 1 10.0.1.169:39422 segment-119-227.s:https LAST\_ACK

tcp 0 0 10.0.1.169:60752 151.101.153.140:https TIME\_WAIT

tcp 0 0 10.0.1.169:41754 maa03s31-in-f4.1e:https ESTABLISHED

tcp 0 0 10.0.1.169:45724 bom05s10-in-f142.:https ESTABLISHED

tcp 0 0 10.0.1.169:49588 av.siesgst.local:90 ESTABLISHED

tcp 0 0 10.0.1.169:58648 ec2-52-44-97-90.c:https ESTABLISHED

tcp 0 0 10.0.1.169:41750 maa03s31-in-f4.1e:https ESTABLISHED

tcp 0 0 10.0.1.169:56700 bom05s11-in-f14.1:https ESTABLISHED

tcp 0 0 10.0.1.169:52292 bom07s01-in-f130.:https ESTABLISHED

tcp 0 0 10.0.1.169:32788 bom05s10-in-f130.:https ESTABLISHED

tcp 0 0 10.0.1.169:55410 ec2-52-202-9-181.:https ESTABLISHED

tcp 0 0 10.0.1.169:48686 bom07s01-in-f10.1:https ESTABLISHED

tcp 0 0 10.0.1.169:36170 bom07s01-in-f129.:https ESTABLISHED

tcp 0 0 10.0.1.169:45016 sc-in-f188.1e100.n:5228 ESTABLISHED

.

.

.

**5.arp:**

Arp manipulates or displays the kernel's IPv4 network neighbour cache. It can add entries to the table, delete one or display the current content. ARP stands for Address Resolution Protocol, which is used to find the media access control address of a network neighbour for a given IPv4 Address.

arp 10.0.8.106

Address HWtype HWaddress Flags Mask Iface

10.0.8.106 ether 50:9a:4c:28:ca:ed C enp2s0

**5.dig:**

dig (domain information groper) is a flexible tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried. Most DNS administrators use dig to troubleshoot DNS problems because of its flexibility, ease of use and clarity of output. Other lookup tools tend to have less functionality than dig.

dig https://www.reddit.com/r/MemeEconomy/

; <<>> DiG 9.10.3-P4-Ubuntu <<>> https://www.reddit.com/r/MemeEconomy/

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 35516

;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 4000

;; QUESTION SECTION:

;https://www.reddit.com/r/MemeEconomy/. IN A

;; AUTHORITY SECTION:

. 292 IN SOA a.root-servers.net. nstld.verisign-grs.com. 2018081201 1800 900 604800 86400

;; Query time: 1 msec

;; SERVER: 127.0.1.1#53(127.0.1.1)

;; WHEN: Mon Aug 13 10:41:20 IST 2018

;; MSG SIZE rcvd: 141

**5.route:**Route manipulates the kernel's IP routing tables. Its primary use is to set up static routes to specific hosts or networks via an interface after it has been configured with the ifconfig(8) program.

When the add or del options are used, route modifies the routing tables. Without these options, route displays the current contents of the routing tables.

route

Kernel IP routing table

Destination Gateway Genmask Flags Metric Ref Use Iface

default 10.0.0.5 0.0.0.0 UG 100 0 0 enp2s0

default 10.147.0.1 0.0.0.0 UG 600 0 0 wlp3s0

1dot1dot1dot1.c 10.147.0.1 255.255.255.255 UGH 600 0 0 wlp3s0

10.0.0.0 \* 255.0.0.0 U 100 0 0 enp2s0

10.147.0.0 \* 255.255.128.0 U 600 0 0 wlp3s0

link-local \* 255.255.0.0 U 1000 0 0 enp2s0