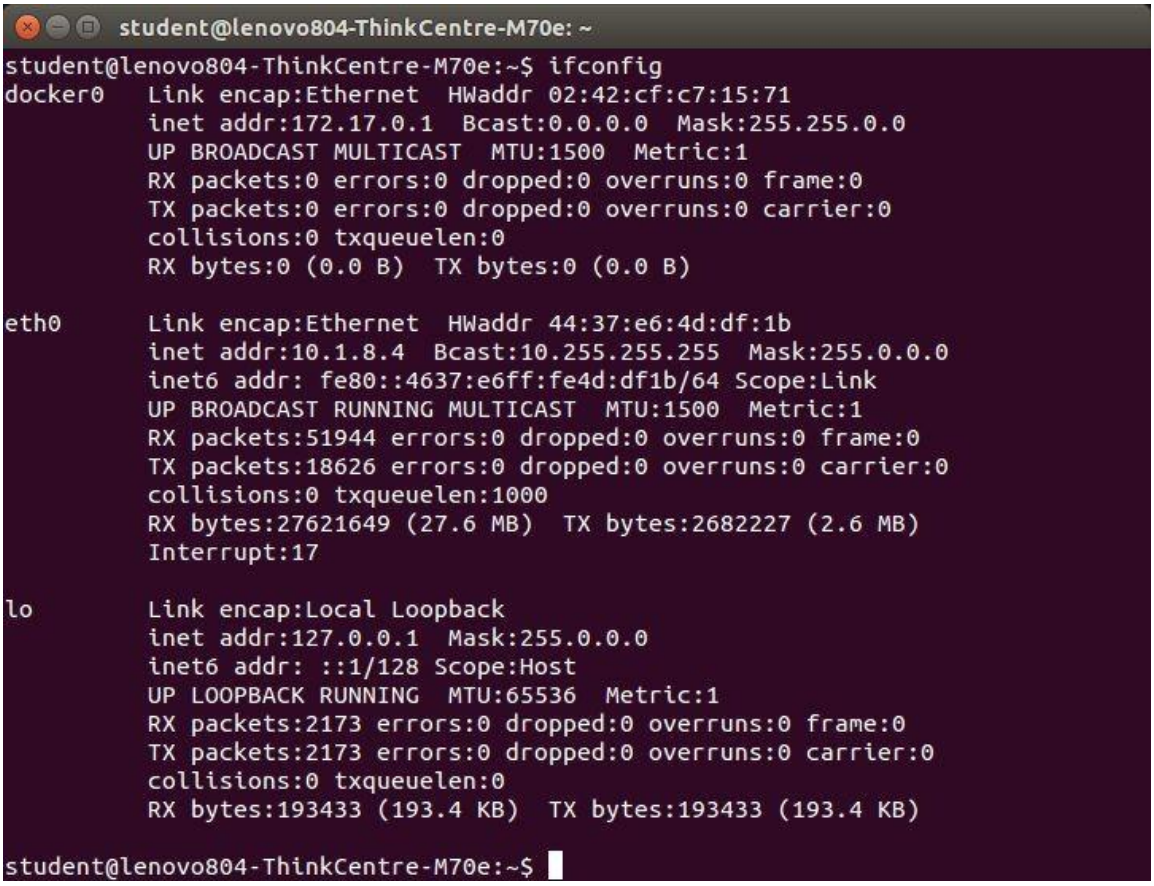
Subject: CSL502 -Computer Networks Lab
Class/Sem: TE(Sem-V) C Scheme
AC YR- 2022-2023

AIM: Use basic networking commands in Linux (ping, tracert, nslookup, netstat, ARP, RARP, ip, ifconfig, dig, route)

THEORY:

1. ifconfig

ifconfig(interface configuration) command is used to configure the kernel-resident network interfaces. It is used at the boot time to set up the interfaces as necessary. After that, it is usually used when needed during debugging or when you need system tuning. Also, this command is used to assign the IP address and netmask to an interface or to enable or disable a given interface.

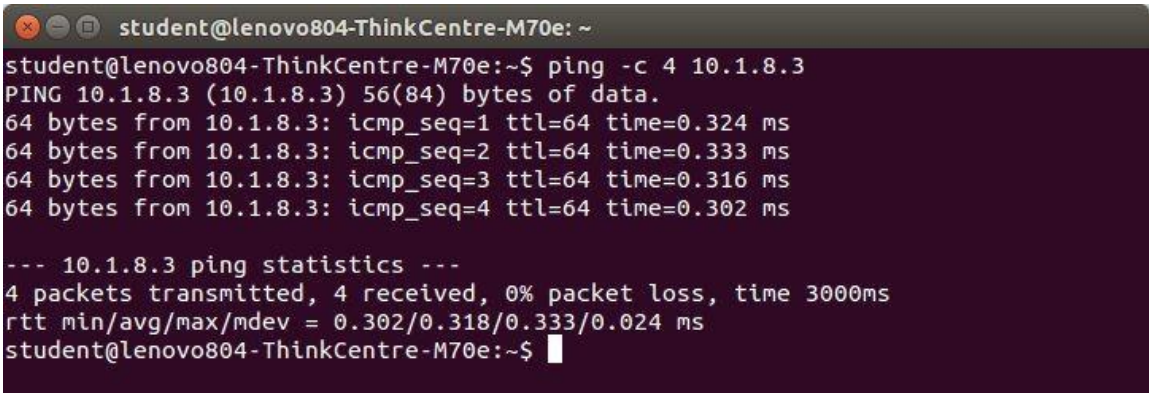


2. NSLOOKUP

Nslookup (stands for "Name Server Lookup") is a useful command for getting information from DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS related problems.

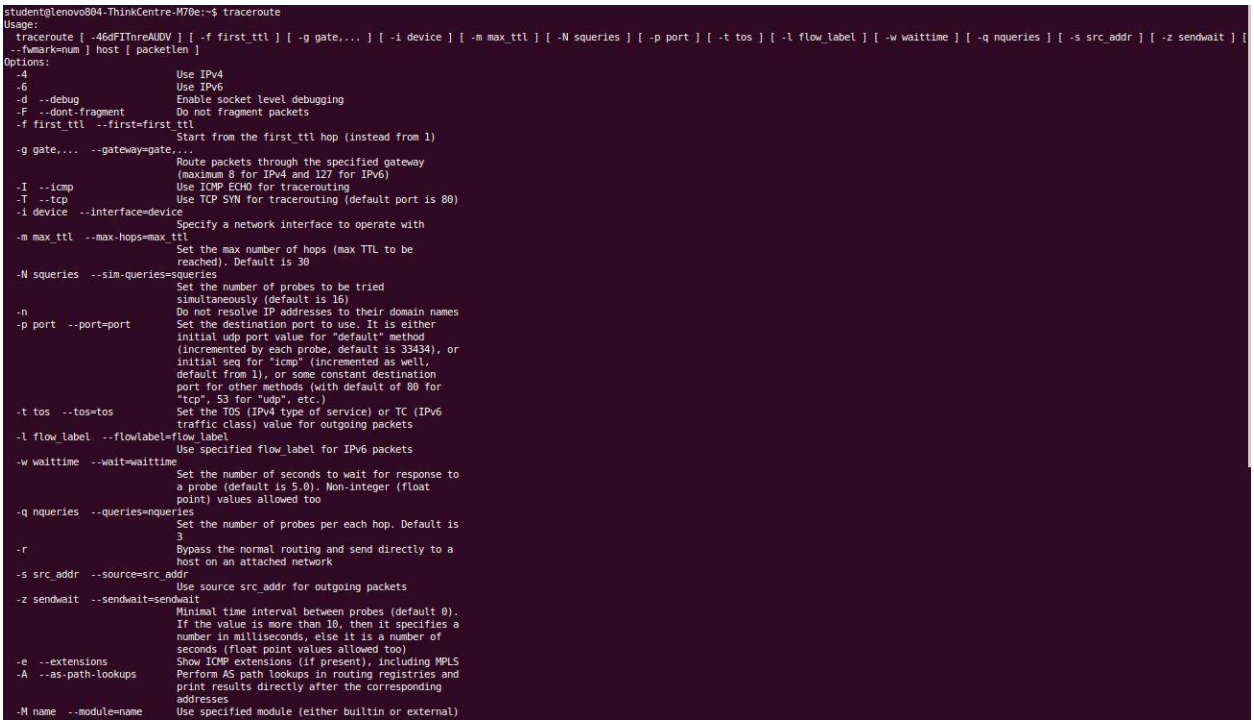
3. Ping

PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and sends a data packet to the specified address with the message "PING" and get a response from the server/host this time is recorded which is called latency. Fast ping low latency means faster connection. Ping uses **ICMP(Internet Control Message Protocol)** to send an **ICMP echo message** to the specified host if that host is available then it sends **ICMP reply message**. Ping is generally measured in millisecond every modern operating system has this ping pre-installed.



4. TRACEROUTE

traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes. Below image depicts how traceroute command is used to reach the Google(172.217.26.206) host from the local machine and it also prints detail about all the hops that it visits in between.

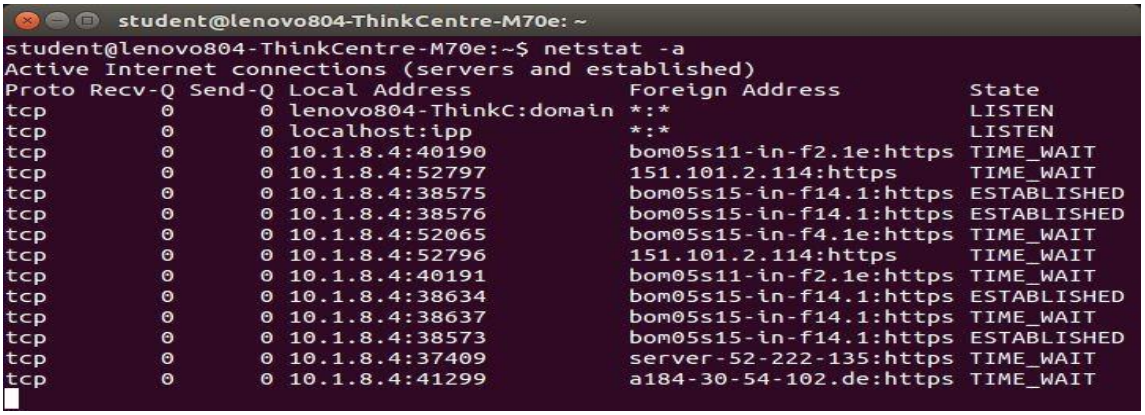


```
student@lenovo804-ThinkCentre-M70e:~$ traceroute
Usage:
  traceroute [ -46dFITnreAUDV ] [ -f first_ttl ] [ -g gate,... ] [ -i device ] [ -m max_ttl ] [ -N squeries ] [ -p port ] [ -t tos ] [ -l flow_label ] [ -w waittime ] [ -q nqueries ] [ -s src_addr ] [ -z sendwait ] [
 --fwmark=num ] host [ packetlen ]
Options:
  -4                        Use IPv4
  -6                        Use IPv6
  -d  --debug               Enable socket level debugging
  -F  --dont-fragment       Do not fragment packets
  -f first_ttl  --first=first_ttl
                            Start from the first_ttl hop (instead from 1)
  -g gate,...  --gateway=gate,...
                            Route packets through the specified gateway
                            (maximum 8 for IPv4 and 127 for IPv6)
  -I  --icmp                Use ICMP ECHO for tracerouting
  -T  --tcp                 Use TCP SYN for tracerouting (default port is 80)
  -i device  --interface=device
                            Specify a network interface to operate with
  -m max_ttl  --max-hops=max_ttl
                            Set the max number of hops (max TTL to be
                            reached). Default is 30
  -N squeries  --sim-queries=squeries
                            Set the number of probes to be tried
                            simultaneously (default is 16)
  -n                        Do not resolve IP addresses to their domain names
  -p port  --port=port      Set the destination port to use. It is either
                            initial udp port value for "default" method
                            (incremented by each probe, default is 33434), or
                            initial seq for "icmp" (incremented as well,
                            default from 1), or some constant destination
                            port for other methods (with default of 80 for
                            "tcp", 53 for "udp", etc.)
  -t tos  --tos=tos         Set the TOS (IPv4 type of service) or TC (IPv6
                            traffic class) value for outgoing packets
  -l flow_label  --flowlabel=flow_label
                            Use specified flow_label for IPv6 packets
  -w waittime  --wait=waittime
                            Set the number of seconds to wait for response to
                            a probe (default is 5.0). Non-integer (float
                            point) values allowed too
  -q nqueries  --queries=nqueries
                            Set the number of probes per each hop. Default is
                            3
  -r                        Bypass the normal routing and send directly to a
                            host on an attached network
  -s src_addr  --source=src_addr
                            Use source src_addr for outgoing packets
  -z sendwait  --sendwait=sendwait
                            Minimal time interval between probes (default 0).
                            If the value is more than 10, then it specifies a
                            number in milliseconds, else it is a number of
                            seconds (float point values allowed too)
  -e  --extensions          Show ICMP extensions (if present), including MPLS
  -A  --as-path-lookups     Perform AS path lookups in routing registries and
                            print results directly after the corresponding
                            addresses
  -M name  --module=name    Use specified module (either builtin or external)
```

5. Netstat

Netstat command displays various network related information such as network

connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.,



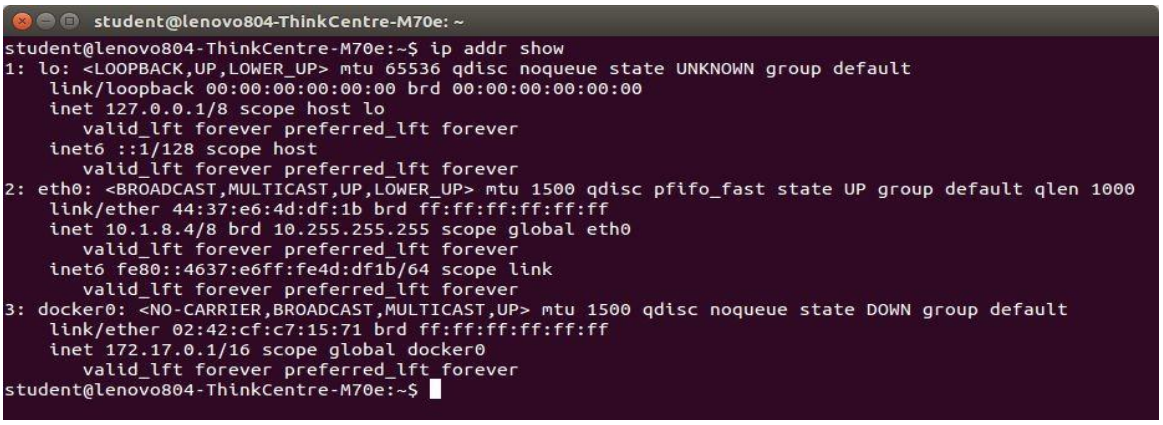
6. ARP

arp command manipulates the System's ARP cache. It also allows a complete dump of the ARP cache. ARP stands for Address Resolution Protocol. The primary function of this protocol is to resolve the IP address of a system to its mac address, and hence it works between level 2(Data link layer) and level 3(Network layer).

7. IP

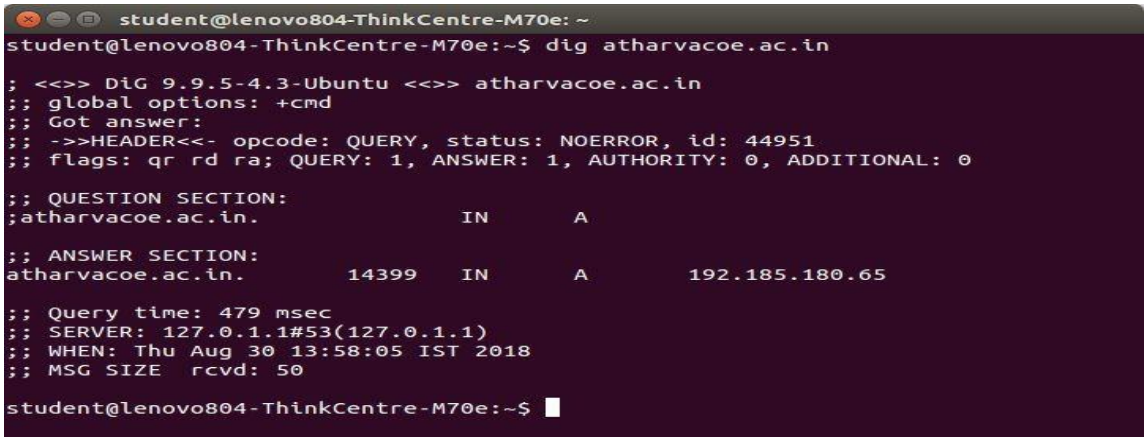
ip command in Linux is present in the net-tools which is used for performing several network administration tasks. IP stands for Internet Protocol. This command is used to show or manipulate routing, devices, and tunnels. It is similar to *ifconfig* command but it is much more powerful with more functions and facilities attached to it. *ifconfig* is one of the deprecated commands in the net-tools of Linux that has not been maintained for many years. ip command is used to perform several tasks like assigning an address to a network interface or configuring network interface parameters.
It can perform several other tasks like configuring and modifying the default and static routing, setting up tunnel over IP, listing IP addresses and property information,

modifying the status of the interface, assigning, deleting and setting up IP addresses and routes.



8. Dig

dig command stands for ***Domain Information Groper***. It is used for retrieving information about DNS name servers. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems and to perform DNS lookups. Dig command replaces older tools such as nslookup and the host.



CONCLUSION: Hence, in this experiment, we have successfully studied some important networking command and also implemented them in Linux