

EXPERIMENT NO.2

AIM: Use basic networking commands in Linux (ping, tracer, 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.

```
student@lenovo804-ThinkCentre-M70e: ~  
student@lenovo804-ThinkCentre-M70e:~$ ifconfig  
docker0    Link encap:Ethernet  HWaddr 02:42:cf:c7:15:71  
            inet addr:172.17.0.1  Bcast:0.0.0.0  Mask:255.255.0.0  
            UP BROADCAST MULTICAST  MTU:1500  Metric:1  
            RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:0  
            RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)  
  
eth0       Link encap:Ethernet  HWaddr 44:37:e6:4d:df:1b  
            inet addr:10.1.8.4  Bcast:10.255.255.255  Mask:255.0.0.0  
            inet6 addr: fe80::4637:e6ff:fe4d:df1b/64 Scope:Link  
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
            RX packets:51944 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:18626 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:1000  
            RX bytes:27621649 (27.6 MB)  TX bytes:2682227 (2.6 MB)  
            Interrupt:17  
  
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:2173 errors:0 dropped:0 overruns:0 frame:0  
            TX packets:2173 errors:0 dropped:0 overruns:0 carrier:0  
            collisions:0 txqueuelen:0  
            RX bytes:193433 (193.4 KB)  TX bytes:193433 (193.4 KB)  
  
student@lenovo804-ThinkCentre-M70e:~$
```

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.

```
student@lenovo804-ThinkCentre-M70e: ~
student@lenovo804-ThinkCentre-M70e:~$ nslookup www.atharvacoe.ac.in
Server:          127.0.1.1
Address:         127.0.1.1#53

Non-authoritative answer:
www.atharvacoe.ac.in canonical name = atharvacoe.ac.in.
Name:   atharvacoe.ac.in
Address: 192.185.180.65

student@lenovo804-ThinkCentre-M70e:~$
```

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.

```
student@lenovo804-ThinkCentre-M70e: ~
student@lenovo804-ThinkCentre-M70e:~$ ping -c 4 10.1.8.3
PING 10.1.8.3 (10.1.8.3) 56(84) bytes of data.
64 bytes from 10.1.8.3: icmp_seq=1 ttl=64 time=0.324 ms
64 bytes from 10.1.8.3: icmp_seq=2 ttl=64 time=0.333 ms
64 bytes from 10.1.8.3: icmp_seq=3 ttl=64 time=0.316 ms
64 bytes from 10.1.8.3: icmp_seq=4 ttl=64 time=0.302 ms

--- 10.1.8.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.302/0.318/0.333/0.024 ms
student@lenovo804-ThinkCentre-M70e:~$
```

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 [-46dFIrtroAUW] [-f first_ttl] [-g gate,...] [-i device] [-m max_ttl] [-N nqueries] [-p port] [-t tos] [-l flow_label] [-w waittime] [-q nqueries] [-s src_addr] [-z sendwait] [-]
  --mark=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 nqueries --sin-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.,

```
student@lenovo804-ThinkCentre-M70e:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 lenovo804-ThinkC:domain *:.*                     LISTEN
tcp        0      0 localhost:ipp           *.*                      LISTEN
tcp        0      0 10.1.8.4:40190          bom05s11-in-f2.1e:https TIME_WAIT
tcp        0      0 10.1.8.4:52797          151.101.2.114:https     TIME_WAIT
tcp        0      0 10.1.8.4:38575          bom05s15-in-f14.1:https ESTABLISHED
tcp        0      0 10.1.8.4:38576          bom05s15-in-f14.1:https ESTABLISHED
tcp        0      0 10.1.8.4:52065          bom05s15-in-f4.1e:https TIME_WAIT
tcp        0      0 10.1.8.4:52796          151.101.2.114:https     TIME_WAIT
```


6. ARP

```
student@lenovo804-ThinkCentre-M70e: ~
student@lenovo804-ThinkCentre-M70e:~$ arp -v
Address                HWtype  HWaddress          Flags Mask          Iface
10.8.1.3                (incomplete)
10.0.0.3                ether    08:35:71:f0:35:c0   C                  eth0
10.1.8.3                ether    44:37:e6:4d:e0:f7   C                  eth0
Entries: 3      Skipped: 0      Found: 3
student@lenovo804-ThinkCentre-M70e:~$
```

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.

```
student@lenovo804-ThinkCentre-M70e: ~
student@lenovo804-ThinkCentre-M70e:~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 44:37:e6:4d:df:1b brd ff:ff:ff:ff:ff:ff
    inet 10.1.8.4/8 brd 10.255.255.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::4637:e6ff:fe4d:df1b/64 scope link
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:cf:c7:15:71 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 scope global docker0
        valid_lft forever preferred_lft forever
student@lenovo804-ThinkCentre-M70e:~$
```

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](#).

```
student@lenovo804-ThinkCentre-M70e: ~
student@lenovo804-ThinkCentre-M70e:~$ dig atharvacoe.ac.in

; <<>> DiG 9.9.5-4.3-Ubuntu <<>> atharvacoe.ac.in
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 44951
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;atharvacoe.ac.in.                IN      A

;; ANSWER SECTION:
atharvacoe.ac.in.                14399   IN      A      192.185.180.65

;; Query time: 479 msec
;; SERVER: 127.0.1.1#53(127.0.1.1)
;; WHEN: Thu Aug 30 13:58:05 IST 2018
;; MSG SIZE rcvd: 50

student@lenovo804-ThinkCentre-M70e:~$
```

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

Questions:

1. What are different networking commands in Linux? Explain the purpose of each command.
2. Which command is used to check the connectivity between two hosts?