

## Experiment 2

### Ping

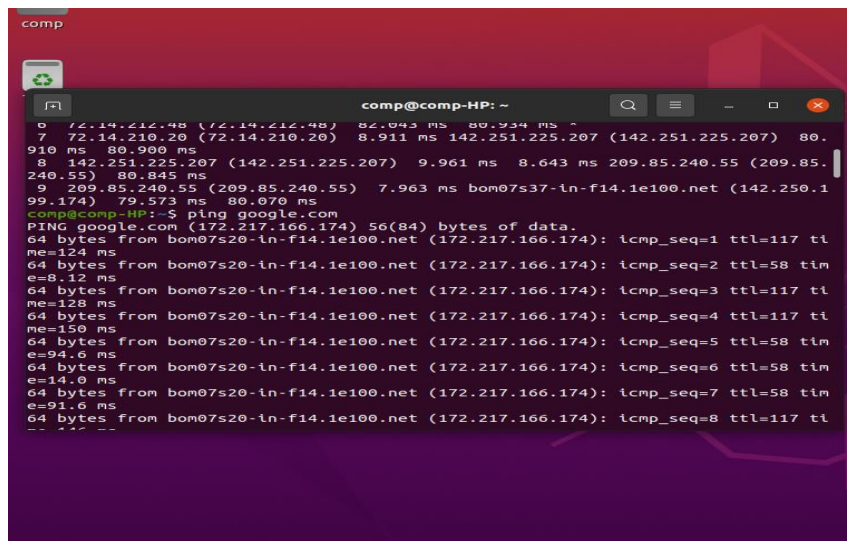
The [ping command](#) is used to ensure that a computer can communicate with a specified device over the network. The ping command sends Internet Control Message Protocol (ICMP) Echo Request messages in the form of packets to the destination computer and waits in order to get the response back. Once the packets are received by the destined computer, it starts sending the packets back. This command keeps executing until it is interrupted.

Ping commands gives details about

- the number of packets transmitted.
- the number of packets received.
- time is taken by the packet to return.

ping command is generally used for the following purposes:

- measuring the time taken by the packets to return to determine the speed of the connection.
- to make sure that the network connection between the host and the destined computer can be established.



```
comp
comp@comp-HP: ~
0 72.14.212.48 (72.14.212.48) 86.043 ms 80.934 ms
7 72.14.210.20 (72.14.210.20) 8.911 ms 142.251.225.207 (142.251.225.207) 80.910 ms 80.900 ms
8 142.251.225.207 (142.251.225.207) 9.961 ms 8.643 ms 209.85.240.55 (209.85.240.55) 80.845 ms
9 209.85.240.55 (209.85.240.55) 7.963 ms bom07s37-ln-f14.1e100.net (142.250.199.174) 79.573 ms 80.070 ms
comp@comp-HP:~$ ping google.com
PING google.com (172.217.166.174) 56(84) bytes of data:
64 bytes from bom07s20-ln-f14.1e100.net (172.217.166.174): icmp_seq=1 ttl=117 time=124 ms
64 bytes from bom07s20-ln-f14.1e100.net (172.217.166.174): icmp_seq=2 ttl=58 time=8.12 ms
64 bytes from bom07s20-ln-f14.1e100.net (172.217.166.174): icmp_seq=3 ttl=117 time=128 ms
64 bytes from bom07s20-ln-f14.1e100.net (172.217.166.174): icmp_seq=4 ttl=117 time=150 ms
64 bytes from bom07s20-ln-f14.1e100.net (172.217.166.174): icmp_seq=5 ttl=58 time=94.6 ms
64 bytes from bom07s20-ln-f14.1e100.net (172.217.166.174): icmp_seq=6 ttl=58 time=14.0 ms
64 bytes from bom07s20-ln-f14.1e100.net (172.217.166.174): icmp_seq=7 ttl=58 time=91.6 ms
64 bytes from bom07s20-ln-f14.1e100.net (172.217.166.174): icmp_seq=8 ttl=117 time=...
```

### Tracroute:

The [traceroute command](#) is used to get the route of a packet. In other words, the traceroute command is used to determine the path along which a packet travels. It also returns the number of

hops taken by the packet to reach the destination. This command prints to the console a list of hosts through which the packet travels in order to the destination.

```
me=3.25 ms
^C
-- google.com ping statistics --
7 packets transmitted, 7 received, 0% packet loss, time 6010ms
rtt min/avg/max/mdev = 3.246/6.492/8.506/2.077 ms
comp@comp-HP:~$ traceroute www.google.com
traceroute to www.google.com (172.217.160.196), 30 hops max, 60 byte packets
 1  gateway (192.168.3.1) 4.560 ms 4.835 ms 4.826 ms
 2  kjsitfw.somaiya.edu (192.168.3.5) 1.071 ms 1.062 ms 1.054 ms
 3  static-145.46.248.49-tataidc.co.in (49.248.46.145) 1.506 ms nsg-static-161.
246.76.182-airtel.com (182.76.246.161) 1.039 ms 1.030 ms
 4  125.19.216.29 (125.19.216.29) 2.458 ms static-185.174.248.49-tataidc.co.in
(49.248.174.185) 8.438 ms 8.432 ms
 5  10.118.143.1 (10.118.143.1) 9.481 ms 116.119.106.216 (116.119.106.216) 3.1
59 ms 10.118.143.1 (10.118.143.1) 9.454 ms
 6  72.14.212.48 (72.14.212.48) 31.673 ms 4.419 ms 10.118.143.6 (10.118.143.6)
7.988 ms
 7  * * 72.14.210.20 (72.14.210.20) 82.048 ms
 8  * 142.250.235.10 (142.250.235.10) 4.232 ms *
 9  142.250.238.202 (142.250.238.202) 58.180 ms 192.178.110.204 (192.178.110.20
4) 4.806 ms 192.178.110.206 (192.178.110.206) 4.017 ms
10 bom07s16-in-f4.1e100.net (172.217.160.196) 4.009 ms 192.178.110.110 (192.17
8.110.110) 59.030 ms 216.239.47.149 (216.239.47.149) 59.982 ms
comp@comp-HP:~$
```

nslookup :

The nslookup command queries the DNS in order to fetch the IP

address or the domain name from DNS records.

```
Address: 127.0.0.53#53
** server can't find https://www.google.com: No answer received
comp@comp-HP:~$ nslookup google.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: google.com
Address: 142.250.183.206
Name: google.com
Address: 2404:6800:4009:80f::200e

comp@comp-HP:~$ arp
Address HWtype HWaddress
kjsitfw.somaiya.edu ether 00:11:11:11:11:11
_gateway ether 7c:9f:3b:11:11:11
192.168.3.126 ether 6c:5e:00:00:00:00
```

## Netstat:

The [netstat](#) (Network Statistics) is the command that is used to display routing tables, connection information, the status of ports, etc. This command works with Linux Network Subsystem. This command basically displays the content of /proc/net file defined in the Linux file system.

Arp:

The  
ARP  
(Address  
Resolution  
Protocol)

```
comp@comp-HP: ~  
tcp        0      0 comp-HP:59764      ec2-3-233-146-45.:https ESTABLISHED  
tcp        0      0 comp-HP:54104      ec2-108-128-217-2:https ESTABLISHED  
tcp        0      0 comp-HP:56492      server-108-159-61:https TIME_WAIT  
tcp        0      0 comp-HP:46280      server-108-158-46:https ESTABLISHED  
tcp        0      0 comp-HP:35546      server-18-172-78.:https ESTABLISHED  
^C  
comp@comp-HP:~$ netstat  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 comp-HP:41574      ec2-54-72-180-161:https ESTABLISHED  
tcp        0      0 comp-HP:49342      104.26.2.26:https      ESTABLISHED  
tcp        0      0 comp-HP:43648      ip-185-184-8-90.r:https ESTABLISHED  
tcp        0      0 comp-HP:58814      server-18-66-41-1:https ESTABLISHED  
tcp        0      0 comp-HP:40052      server-18-172-78.:https ESTABLISHED  
tcp        0      0 comp-HP:55252      bom12s06-in-f3.1e:https ESTABLISHED  
tcp        0      0 comp-HP:55648      bom12s11-in-f2.1e:https ESTABLISHED  
tcp        0      0 comp-HP:44296      152.199.43.48:https    ESTABLISHED  
tcp        0      0 comp-HP:59764      ec2-3-233-146-45.:https ESTABLISHED  
tcp        0      0 comp-HP:54104      ec2-108-128-217-2:https ESTABLISHED  
tcp        0      0 comp-HP:56492      server-108-159-61:https TIME_WAIT  
tcp        0      0 comp-HP:46280      server-108-158-46:https TIME_WAIT  
tcp        0      0 comp-HP:35546      server-18-172-78.:https ESTABLISHED  
^C  
comp@comp-HP:~$
```

command is used to display and modify ARP cache, which contains the mapping of IP address to MAC address. The system's TCP/IP stack uses ARP in order to determine the MAC address associated with an IP address.

```
comp@comp-HP:~$ arp  
Address HWtype HWaddress Flags Mask Iface  
kjsitfw.somaiya.edu ether 00:1b:17:00:0a:10 C eno1  
_gateway ether 7c:95:f3:80:03:f0 C eno1  
192.168.3.126 ether 6c:3c:8c:40:a2:3f C eno1  
192.168.3.10 ether 00:21:5e:6a:c1:34 C eno1  
avvdc01.svv.local ether 44:a8:42:28:4f:08 C eno1  
comp@comp-HP:~$
```

The ARP (Address Resolution Protocol) contains the mapping of IP address to determine the MAC address.

Ifconfig:

The ifconfig(Interface Configuration) is a utility in an operating system that is used to set or display the IP address and netmask of a network interface. It also provides commands to enable or disable an interface. Many UNIX-like operating systems initialize their network interfaces using ifconfig at boot time.

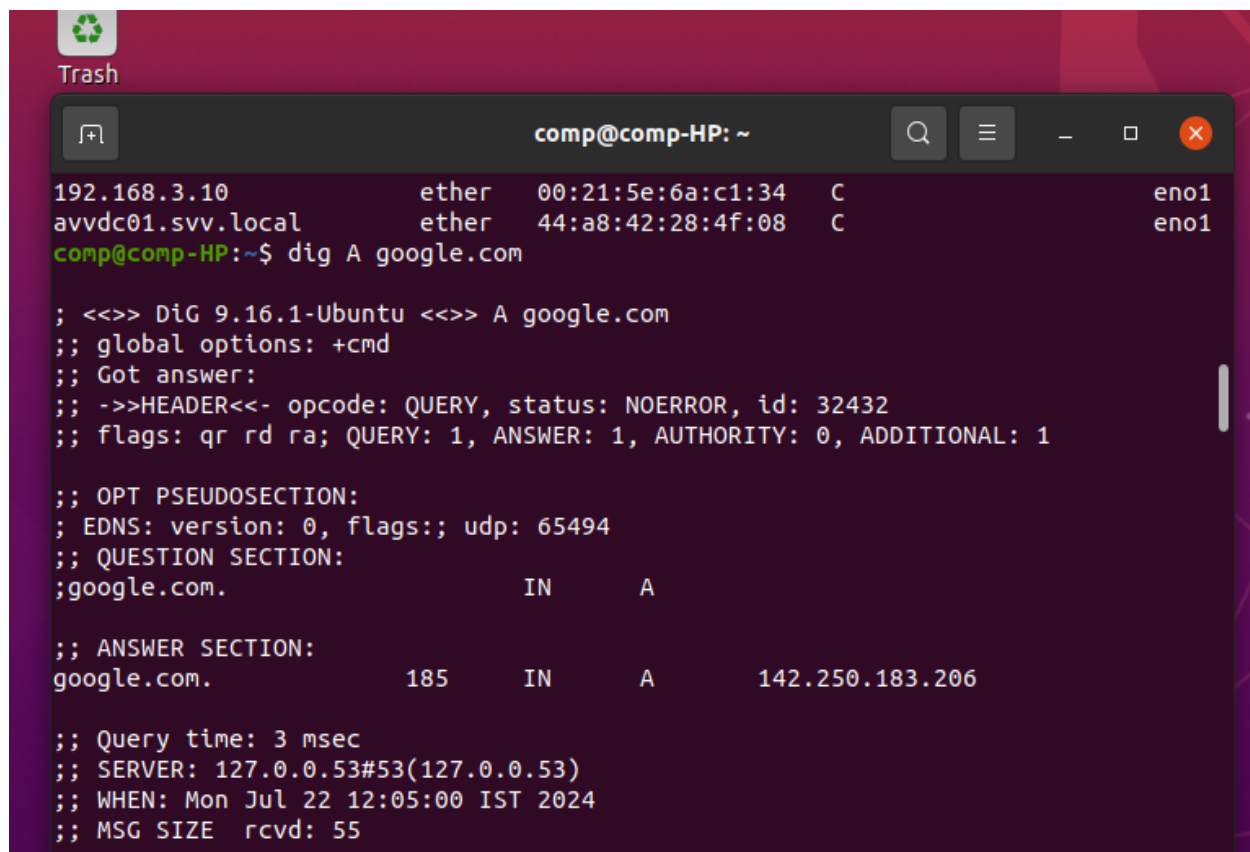
ifconfig is also used to view the MTU(Maximum transmission unit).

```
comp@comp-HP: ~  
192.168.3.126 ether 6c:3c:8c:40:a2:3f C eno1  
192.168.3.10 ether 00:21:5e:6a:c1:34 C eno1  
avvdc01.svv.local ether 44:a8:42:28:4f:08 C eno1  
comp@comp-HP:~$ ifconfig  
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet 192.168.3.45 netmask 255.255.255.0 broadcast 192.168.3.255  
inet6 fe80::35:9949:b50a:c078 prefixlen 64 scopeid 0x20<link>  
ether c0:18:03:c1:b3:ec txqueuelen 1000 (Ethernet)  
RX packets 663420 bytes 417976091 (417.9 MB)  
RX errors 18 dropped 0 overruns 0 frame 10  
TX packets 205124 bytes 46200965 (46.2 MB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
device interrupt 19 memory 0x80900000-80920000  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
inet 127.0.0.1 netmask 255.0.0.0  
inet6 ::1 prefixlen 128 scopeid 0x10<host>  
loop txqueuelen 1000 (Local Loopback)  
RX packets 25947 bytes 2649668 (2.6 MB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 25947 bytes 2649668 (2.6 MB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
comp@comp-HP:~$
```

Protocol) command is used to determine the MAC address associated with an IP address.

Dig:

The [Dig Command](#) is called domain information groper; it is a tool used to find query information related to domain name and troubleshoot DNS issue in Linux. This tool can provide various types of DNS records, such as CNAME, MX records and records etc.



```
192.168.3.10      ether  00:21:5e:6a:c1:34  C      eno1
avvdc01.svv.local ether  44:a8:42:28:4f:08  C      eno1
comp@comp-HP:~$ dig A google.com

; <<>> DiG 9.16.1-Ubuntu <<>> A google.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 32432
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                 185     IN      A      142.250.183.206

;; Query time: 3 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Jul 22 12:05:00 IST 2024
;; MSG SIZE  rcvd: 55
```