

1. Ifconfig

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ ifconfig
enp4s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.124 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::38e3:2654:2941:1add prefixlen 64 scopeid 0x20<link>
          ether f4:39:09:48:b0:56 txqueuelen 1000 (Ethernet)
            RX packets 378877 bytes 555804472 (555.8 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 152651 bytes 13346498 (13.3 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 464 bytes 44005 (44.0 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 464 bytes 44005 (44.0 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Used to view information about all network interfaces on your Linux system

1. ifconfig -a

To get info about both active and inactive network interfaces, run ifconfig with the -a option

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ ifconfig -a
enp4s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.124 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::38e3:2654:2941:1add prefixlen 64 scopeid 0x20<link>
          ether f4:39:09:48:b0:56 txqueuelen 1000 (Ethernet)
            RX packets 387038 bytes 557076809 (557.0 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 153479 bytes 13412208 (13.4 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 593 bytes 56956 (56.9 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 593 bytes 56956 (56.9 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

1. ifconfig -s

Use the -s flag with ifconfig to display a concise summary of every active interface

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ ifconfig -s
Iface      MTU     RX-OK RX-ERR RX-DRP RX-OVR     TX-OK TX-ERR TX-DRP TX-OVR Flg
enp4s0    1500    387402      0      0 0       153493      0      0 0 BMRU
lo       65536      597      0      0 0           597      0      0 0 LRU
```

1. ifconfig -v

As opposed to the -s flag, the verbose option (-v) prints a more detailed output. Depending on the system, the outcome is either the same as ifconfig without arguments or slightly more in-depth.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ ifconfig -v
enp4s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.124 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::38e3:2654:2941:1add prefixlen 64 scopeid 0x20<link>
          ether f4:39:09:48:b0:56 txqueuelen 1000 (Ethernet)
            RX packets 387582 bytes 557116000 (557.1 MB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 153498 bytes 13413315 (13.4 MB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 597 bytes 57612 (57.6 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 597 bytes 57612 (57.6 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

1. ifconfig | grep inet

The grep command is used to search for patterns in text. When you pipe the output of ifconfig to grep, it will search for all lines that contain the string "inet". This will print all of the IP addresses that are assigned to the system's interfaces.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ ifconfig | grep inet
      inet 192.168.1.124 netmask 255.255.255.0 broadcast 192.168.1.255
      inet6 fe80::38e3:2654:2941:1add prefixlen 64 scopeid 0x20<link>
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
```

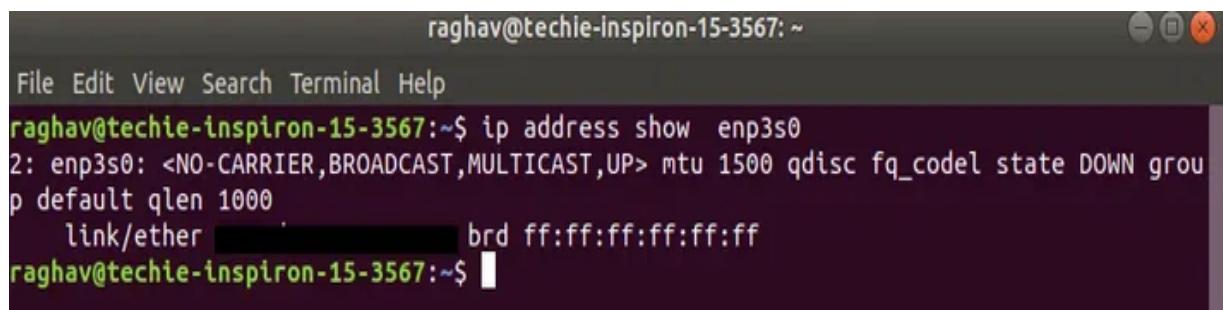
1. ip address

This option is used to show all IP addresses associated with all network devices.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    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: enp4s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether f4:39:09:48:b0:56 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.124/24 brd 192.168.1.255 scope global dynamic noprefixroute enp4s0
        valid_lft 5207sec preferred_lft 5207sec
    inet6 fe80::38e3:2654:2941:1add/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

1. ip addr show enp3s0

Use if we want to view the information of any particular interface



```
raghav@techie-inspiron-15-3567: ~
File Edit View Search Terminal Help
raghav@techie-inspiron-15-3567:~$ ip address show enp3s0
2: enp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether [REDACTED] brd ff:ff:ff:ff:ff:ff
raghav@techie-inspiron-15-3567:~$
```

1. ip link

It is used to display link layer information

```
raghav@techie-inspiron-15-3567: ~
File Edit View Search Terminal Help
raghav@techie-inspiron-15-3567:~$ ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group
  default qlen 1000
    link/loopback brd 00:00:00:00:00:00
2: enp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN mode
  DEFAULT group default qlen 1000
    link/ether [REDACTED] brd ff:ff:ff:ff:ff:ff
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DORMANT g
  roup default qlen 1000
    link/ether [REDACTED] brd ff:ff:ff:ff:ff:ff
raghav@techie-inspiron-15-3567:~$
```

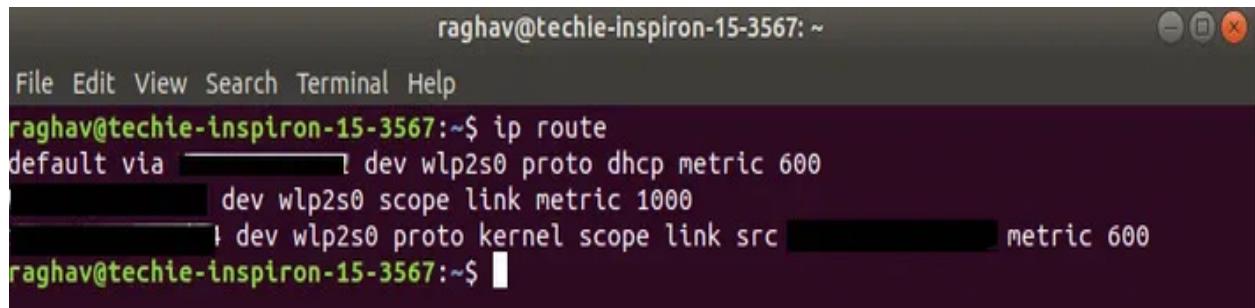
1. ip -s link

link option when used with -s option is used to show the statistics of the various network interfaces.

```
raghav@techie-inspiron-15-3567: ~
File Edit View Search Terminal Help
raghav@techie-inspiron-15-3567:~$ ip -s link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group
  default qlen 1000
    link/loopback brd 00:00:00:00:00:00
      RX: bytes packets errors dropped overrun mcast
        2402011 23218 0 0 0 0
      TX: bytes packets errors dropped carrier collsns
        2402011 23218 0 0 0 0
2: enp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN mode
  DEFAULT group default qlen 1000
    link/ether [REDACTED] brd ff:ff:ff:ff:ff:ff
      RX: bytes packets errors dropped overrun mcast
        0 0 0 0 0 0
      TX: bytes packets errors dropped carrier collsns
        0 0 0 0 0 0
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP mode DORMANT g
  roup default qlen 1000
    link/ether [REDACTED] brd ff:ff:ff:ff:ff:ff
      RX: bytes packets errors dropped overrun mcast
        432091386 361991 0 0 0 0
      TX: bytes packets errors dropped carrier collsns
        32562210 217187 0 0 0 0
raghav@techie-inspiron-15-3567:~$
```

1. ip route

This command helps you to see the route packets your network will take as set in your routing table. The first entry is the default route.



A screenshot of a terminal window titled "raghav@techie-inspiron-15-3567: ~". The window has a dark background with light-colored text. At the top, there's a menu bar with "File", "Edit", "View", "Search", "Terminal", and "Help". Below the menu, the command "ip route" is run, showing the system's routing table. The output includes a default route via a wireless interface (wlp2s0) and another route entry. The terminal prompt "raghav@techie-inspiron-15-3567:~\$" is at the bottom.

```
raghav@techie-inspiron-15-3567:~$ ip route
default via [REDACTED] dev wlp2s0 proto dhcp metric 600
[REDACTED] dev wlp2s0 scope link metric 1000
[REDACTED] dev wlp2s0 proto kernel scope link src [REDACTED] metric 600
raghav@techie-inspiron-15-3567:~$
```

1. traceroute 192.168.1.141

tracks the path a packet takes from source to destination on an IP network

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ traceroute 192.168.1.141
traceroute to 192.168.1.141 (192.168.1.141), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

1. traceroute -4 google.com

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ traceroute -4 google.com
traceroute to google.com (142.251.42.46), 30 hops max, 60 byte packets
1 _gateway (192.168.1.1) 0.563 ms 0.526 ms 0.503 ms
2 * * *
3 * * *
4 * * *
5 * * *
6 72.14.242.50 (72.14.242.50) 10.699 ms 4.925 ms 4.730 ms
7 * * *
8 142.250.228.50 (142.250.228.50) 4.548 ms bom12s20-in-f14.1e100.net (142.251.42.46) 3.621 ms 142.250.214.110 (142.250.214.110) 3.561 ms
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$
```

Use ip version 4 i.e. use IPv4

1. traceroute -6 google.com

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ traceroute -6 google.com
traceroute to google.com (2404:6800:4009:81e::200e), 30 hops max, 80 byte packets
connect: Network is unreachable
```

use ip version 6 i.e. use IPv6

1. traceroute -F google.com

Do not fragment packet

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ traceroute -F google.com
traceroute to google.com (142.250.182.206), 30 hops max, 60 byte packets
1 _gateway (192.168.1.1) 0.528 ms 0.496 ms 0.474 ms
2 Archer (192.168.0.1) 2.322 ms 2.292 ms 2.258 ms
3 203.212.25.1 (203.212.25.1) 2.526 ms 2.495 ms 2.465 ms
4 203.212.24.53 (203.212.24.53) 2.433 ms 2.401 ms 2.370 ms
5 175.100.177.53 (175.100.177.53) 3.477 ms 8.962 ms 3.415 ms
6 * * *
7 175.100.188.22 (175.100.188.22) 2.574 ms 2.484 ms 2.438 ms
8 * * *
9 108.170.248.177 (108.170.248.177) 3.961 ms 4.166 ms 142.251.64.12 (142.251
.64.12) 3.899 ms
10 108.170.248.179 (108.170.248.179) 12.455 ms 142.250.214.99 (142.250.214.99)
4.579 ms 4.719 ms
11 bom07s28-in-f14.1e100.net (142.250.182.206) 4.289 ms 108.170.248.193 (108.1
70.248.193) 4.585 ms 2.929 ms
```

1. traceroute -m 5 google.com

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ traceroute -m 5 google.com
traceroute to google.com (142.250.182.206), 5 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  0.489 ms  0.454 ms  0.431 ms
 2  * * *
 3  * * *
 4  * * *
 5  175.100.177.53 (175.100.177.53)  3.575 ms  3.544 ms  3.756 ms
```

Set the max number of hops for the packet to reach the destination. Default value is 30.

(ping reference – www.geeksforgeeks.org)

1. ping www.google.com

To check your internet connection

```
administrator@GFG19566-LAPTOP:~/practice$ ping www.google.com
PING www.google.com (142.250.194.100) 56(84) bytes of data.
64 bytes from del12s04-in-f4.1e100.net (142.250.194.100): icmp_seq=1 ttl=116 time=1.60 ms
64 bytes from del12s04-in-f4.1e100.net (142.250.194.100): icmp_seq=2 ttl=116 time=1.15 ms
64 bytes from del12s04-in-f4.1e100.net (142.250.194.100): icmp_seq=3 ttl=116 time=1.17 ms
64 bytes from del12s04-in-f4.1e100.net (142.250.194.100): icmp_seq=4 ttl=116 time=1.14 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.136/1.264/1.599/0.193 ms
```

1. ping -c 2 www.geeksforgeeks.org

used to define the number of packets to send to the server/host

```
administrator@GFG19566-LAPTOP:~/practice$ ping -c 2 www.geeksforgeeks.org
PING a1991.dscr.akamai.net (23.223.243.58) 56(84) bytes of data.
64 bytes from a23-223-243-58.deploy.static.akamaitechnologies.com (23.223.243.58): icmp_seq=1
  ttl=54 time=4.70 ms
64 bytes from a23-223-243-58.deploy.static.akamaitechnologies.com (23.223.243.58): icmp_seq=2
  ttl=54 time=4.71 ms

--- a1991.dscr.akamai.net ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 4.703/4.704/4.706/0.001 ms
```

1. ping -w 3 www.geeksforgeeks.org

This command instructs the system to stop pinging the specified website after waiting for 3 seconds.

```
File Edit View Search Terminal Help
$ ping -w 3 www.geeksforgeeks.org
PING d13vvqr7dxay1j.cloudfront.net (52.222.128.155) 56(84) bytes of data.
64 bytes from server-52-222-128-155.bom51.r.cloudfront.net (52.222.128.155): icmp_seq=1 ttl=244 time=790 ms
64 bytes from server-52-222-128-155.bom51.r.cloudfront.net (52.222.128.155): icmp_seq=2 ttl=244 time=110 ms
...
--- d13vvqr7dxay1j.cloudfront.net ping statistics ---
3 packets transmitted, 2 received, 33% packet loss, time 2851ms
rtt min/avg/max/mdev = 110.425/450.516/790.607/340.091 ms
$ 
```

1. ping -f www.geeksforgeeks.org

To flood a network with PING packets for testing network performance, use the '-f' option with the PING command.

```
administrator@GFG19566-LAPTOP:~/practice$ sudo ping -f www.geeksforgeeks.org
[sudo] password for administrator:
PING a1991.dscre.akamai.net (104.71.60.41) 56(84) bytes of data.
.
.
.
--- a1991.dscre.akamai.net ping statistics ---
43367 packets transmitted, 43330 received, 0.0853183% packet loss, time 52887ms
rtt min/avg/max/mdev = 0.726/1.122/16.881/0.602 ms, pipe 2, ipg/ewma 1.219/1.095 ms
```

1. ping -s 40 www.geeksforgeeks.org

we can send light and heavy packet to host by using -s option.

```
$ ping -s 40 -c 5 www.geeksforgeeks.org
PING d13vvqr7dxay1j.cloudfront.net (52.222.128.155) 40(68) bytes of data.
48 bytes from server-52-222-128-155.bom51.r.cloudfront.net (52.222.128.155): icmp_seq=1 ttl=244 time=121 ms
48 bytes from server-52-222-128-155.bom51.r.cloudfront.net (52.222.128.155): icmp_seq=2 ttl=244 time=245 ms
.
.
.
--- d13vvqr7dxay1j.cloudfront.net ping statistics ---
5 packets transmitted, 2 received, 60% packet loss, time 4027ms
rtt min/avg/max/mdev = 121.518/183.447/245.376/61.929 ms
$ 
```

1. tracepath

It will print the general syntax of the command along with the various options that can be used with the tracepath command as well as gives a brief description about each option.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ tracepath www.google.com
1?: [LOCALHOST]                                pmtu 1500
1: _gateway                                     0.658ms
1: _gateway                                     0.558ms
2: no reply
3: no reply
4: no reply
5: no reply
6: no reply
7: no reply
8: no reply
^C
```

1. tracepath -n www.google.com

This option prints primarily IP addresses numerically

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ tracepath -n www.google.com
1?: [LOCALHOST]                                pmtu 1500
1: 192.168.1.1                                 0.730ms
1: 192.168.1.1                                 0.699ms
2: no reply
3: no reply
^C
```

1. tracepath -b www.makemytrip.com

This option print both of host names and IP addresses

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ tracepath -b www.google.com
1?: [LOCALHOST]                                pmtu 1500
1: _gateway (192.168.1.1)                      0.745ms
1: _gateway (192.168.1.1)                      0.724ms
2: no reply
3: no reply
4: no reply
^C
```

1. tracepath -m 31 www.google.com

This option will set maximum hops (or maximum TTLs) to max_hops instead of 30

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ tracepath -m 31 www.google.com
1?: [LOCALHOST]                                pmtu 1500
1: _gateway                                    0.837ms
1: _gateway                                    0.728ms
2: no reply
3: no reply
4: no reply
5: no reply
6: no reply
7: no reply
8: no reply
9: no reply
10: no reply
^C
```

1. tracepath -p 8080 www.google.com

This option will set the initial destination port to use

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ tracepath -p 8080 www.google.com
1?: [LOCALHOST]                                     pmtu 1500
1: _gateway                                         0.748ms
1: _gateway                                         0.833ms
2: Archer                                           1.490ms
3: Archer                                           1.351ms pmtu 1480
3: 203.212.25.1                                    1.923ms
4: 203.212.24.53                                   2.093ms
5: 175.100.177.53                                  11.035ms
6: 172.16.2.202                                    44.995ms
7: 175.100.188.22                                 3.164ms asymm 11
8: no reply
```

1. netstat

generates displays that show network status and protocol statistics

```
>netstat
ns

      address          Foreign Address      State
.1:49670           LAPTOP-6BJ1JG3N:49671 ESTABLISHED
.1:49671           LAPTOP-6BJ1JG3N:49670 ESTABLISHED
.1:49672           LAPTOP-6BJ1JG3N:49673 ESTABLISHED
.1:49673           LAPTOP-6BJ1JG3N:49672 ESTABLISHED
.29.184:58228     20.198.118.190:https ESTABLISHED
.29.184:58268     20.198.119.84:https ESTABLISHED
.29.184:58975     152.195.38.76:http  LAST_ACK
.29.184:59462     20.212.88.117:https ESTABLISHED
.29.184:59545     1drv:https        ESTABLISHED
.29.184:59547     1drv:https        ESTABLISHED
.29.184:59555     20.189.173.12:https ESTABLISHED
.29.184:59560     51.116.253.168:https TIME_WAIT
.29.184:59566     52.189.124.29:https TIME_WAIT
.29.184:59569     52.189.124.29:https TIME_WAIT
.29.184:59577     52.178.17.234:https ESTABLISHED
.29.184:59579     13.187.4.254:https ESTABLISHED
.29.184:59580     152.195.38.76:http  ESTABLISHED
.29.184:59583     204.79.197.222:https ESTABLISHED
.29.184:59584     51.104.15.253:https ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:58299 sh-in-f188:5228      ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:58349 [2606:4700:8ca3:98df:bdd7:7a:3150:c532]:https CLOSE_WAIT
01:1:6019:d949:70fa:542a:ce47]:58350 bom07s28-in-x03:http  CLOSE_WAIT
01:1:6019:d949:70fa:542a:ce47]:58351 [2606:4700:8d70:bc89:5ed7:b41:3fd7:3718]:https CLOSE_WAIT
01:1:6019:d949:70fa:542a:ce47]:59175 [2603:1063:2202:14::3]:https ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:59298 [2606:4700:8d72:883b:10d7:b41:6810:e095]:https ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:59321 whatsapp-cdn6-shv-01-pnql:https ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:59570 [2405:200:1630:a00::312c:d929]:https ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:59571 [2405:200:1630:a00::312c:d929]:https CLOSE_WAIT
01:1:6019:d949:70fa:542a:ce47]:59574 [2405:200:1630:a00::312c:d91a]:https ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:59575 [2405:200:1630:a00::312c:d91a]:https CLOSE_WAIT
01:1:6019:d949:70fa:542a:ce47]:59576 [2603:1046:c04:c0f::2]:https ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:59581 [2603:1030:13:201::254]:https ESTABLISHED
01:1:6019:d949:70fa:542a:ce47]:59582 [2603:1063:27:2::254]:https ESTABLISHED
```

1. netstat -e

displays Ethernet statistics, including the number of bytes and packets sent and received.

```
k>netstat -e  
stics  
  
Received           Sent  
  
 3515790108      832103148  
 3234354          1569246  
kets             21906          18768  
                0              0  
                0              0  
ls               0              0
```

1. netstat -n

displays network connections and listening ports in numerical format (IP addresses and port numbers) instead of resolving them to hostnames and service names.

```

k>netstat -n
ons

Address      Foreign Address      State
0.1:49670    127.0.0.1:49671    ESTABLISHED
0.1:49671    127.0.0.1:49670    ESTABLISHED
0.1:49672    127.0.0.1:49673    ESTABLISHED
0.1:49673    127.0.0.1:49672    ESTABLISHED
8.29.184:58220 20.198.118.190:443 ESTABLISHED
8.29.184:58260 20.198.119.84:443 ESTABLISHED
8.29.184:59462 20.212.88.117:443 ESTABLISHED
8.29.184:59545 13.107.42.12:443 ESTABLISHED
8.29.184:59547 13.107.42.12:443 ESTABLISHED
8.29.184:59555 20.189.173.12:443 ESTABLISHED
8.29.184:59580 152.195.38.76:80 CLOSE_WAIT
8.29.184:59609 52.109.124.29:443 TIME_WAIT
8.29.184:59613 52.109.56.129:443 TIME_WAIT
8.29.184:59614 157.240.242.61:443 TIME_WAIT
8.29.184:59615 52.109.56.129:443 TIME_WAIT
8.29.184:59618 52.109.56.129:443 TIME_WAIT
8.29.184:59619 52.109.56.129:443 TIME_WAIT
201:1:6019:d949:70fa:542a:ce47]:58299 [2404:6800:4003:c1c::bc]:5228 ESTABLISHED
201:1:6019:d949:70fa:542a:ce47]:58349 [2606:4700:8ca3:98df:bdd7:7a:3150:c532]:443 CLOSE_WAIT
201:1:6019:d949:70fa:542a:ce47]:58350 [2404:6800:4009:81e::2003]:80 CLOSE_WAIT
201:1:6019:d949:70fa:542a:ce47]:58351 [2606:4700:8d70:bc89:5ed7:b41:3fd7:3718]:443 CLOSE_WAIT
201:1:6019:d949:70fa:542a:ce47]:59175 [2603:1063:2202:14::3]:443 ESTABLISHED
201:1:6019:d949:70fa:542a:ce47]:59298 [2606:4700:8d72:883b:10d7:b41:6810:e095]:443 ESTABLISHED
201:1:6019:d949:70fa:542a:ce47]:59321 [2a03:2880:f26e:c2:face:b00c:0:167]:443 ESTABLISHED
201:1:6019:d949:70fa:542a:ce47]:59570 [2405:200:1630:a00::312c:d929]:443 CLOSE_WAIT
201:1:6019:d949:70fa:542a:ce47]:59571 [2405:200:1630:a00::312c:d929]:443 CLOSE_WAIT
201:1:6019:d949:70fa:542a:ce47]:59574 [2405:200:1630:a00::312c:d91a]:443 CLOSE_WAIT
201:1:6019:d949:70fa:542a:ce47]:59575 [2405:200:1630:a00::312c:d91a]:443 CLOSE_WAIT
201:1:6019:d949:70fa:542a:ce47]:59607 [2402:6800:764:a000::8000]:80 TIME_WAIT
201:1:6019:d949:70fa:542a:ce47]:59608 [2a03:2880:f26e:c9:face:b00c:0:7260]:443 TIME_WAIT
201:1:6019:d949:70fa:542a:ce47]:59611 [2a03:2880:f26e:c9:face:b00c:0:7260]:443 TIME_WAIT
201:1:6019:d949:70fa:542a:ce47]:59616 [2a03:2880:f26e:c9:face:b00c:0:7260]:443 TIME_WAIT
201:1:6019:d949:70fa:542a:ce47]:59617 [2a03:2880:f26e:c9:face:b00c:0:7260]:443 ESTABLISHED

```

1. netstat -o

displays active network connections and includes the process ID (PID) associated with each connection.

```
k>netstat -o

ons

Address      Foreign Address      State       PID
0.1:49670    LAPTOP-6BJ1JG3N:49671 ESTABLISHED 4892
0.1:49671    LAPTOP-6BJ1JG3N:49670 ESTABLISHED 4892
0.1:49672    LAPTOP-6BJ1JG3N:49673 ESTABLISHED 4892
0.1:49673    LAPTOP-6BJ1JG3N:49672 ESTABLISHED 4892
8.29.184:58220 20.198.118.190:https ESTABLISHED 4636
8.29.184:58260 20.198.119.84:https ESTABLISHED 4032
8.29.184:59462 20.212.88.117:https ESTABLISHED 20408
8.29.184:59545 1drv:https      ESTABLISHED 16660
8.29.184:59547 1drv:https      ESTABLISHED 4032
8.29.184:59555 20.189.173.12:https ESTABLISHED 4032
8.29.184:59580 152.195.38.76:http  CLOSE_WAIT   9648
8.29.184:59615 52.109.56.129:https TIME_WAIT    0
8.29.184:59618 52.109.56.129:https TIME_WAIT    0
8.29.184:59619 52.109.56.129:https TIME_WAIT    0
8.29.184:59620 52.109.124.29:https TIME_WAIT    0
8.29.184:59623 52.109.124.29:https TIME_WAIT    0
201:1:6019:d949:70fa:542a:ce47]:58299 sh-in-f188:5228      ESTABLISHED 11412
201:1:6019:d949:70fa:542a:ce47]:58349 [2606:4700:8ca3:98df:bdd7:7a:3150:c532]:https CLOSE_WAIT   10776
201:1:6019:d949:70fa:542a:ce47]:58350 bom@7s28-in-x03:http  CLOSE_WAIT   10776
201:1:6019:d949:70fa:542a:ce47]:58351 [2606:4700:8d70:bc89:5ed7:b41:3fd7:3718]:https CLOSE_WAIT   10776
201:1:6019:d949:70fa:542a:ce47]:59175 [2603:1063:2202:14::3]:https ESTABLISHED 16660
201:1:6019:d949:70fa:542a:ce47]:59298 [2606:4700:8d72:883b:10d7:b41:6810:e095]:https ESTABLISHED 11412
201:1:6019:d949:70fa:542a:ce47]:59321 whatsapp-cdn6-shv-01-pnql:https ESTABLISHED 11412
201:1:6019:d949:70fa:542a:ce47]:59570 [2405:200:1630:a00::312c:d929]:https CLOSE_WAIT   9648
201:1:6019:d949:70fa:542a:ce47]:59571 [2405:200:1630:a00::312c:d929]:https CLOSE_WAIT   9648
201:1:6019:d949:70fa:542a:ce47]:59574 [2405:200:1630:a00::312c:d91a]:https CLOSE_WAIT   9648
201:1:6019:d949:70fa:542a:ce47]:59575 [2405:200:1630:a00::312c:d91a]:https CLOSE_WAIT   9648
201:1:6019:d949:70fa:542a:ce47]:59617 whatsapp-chatd-edge6-shv-01-pnql:https TIME_WAIT    0
201:1:6019:d949:70fa:542a:ce47]:59621 whatsapp-chatd-edge6-shv-01-pnql:https TIME_WAIT    0
```

1. netstat -r

The -r option of netstat displays the IP routing table. Here is a sample display produced by netstat -r run on machine tenere.

```

ik>netstat -r
=====
a6 5e 99 .....Microsoft Wi-Fi Direct Virtual Adapter
a6 5e 99 .....Microsoft Wi-Fi Direct Virtual Adapter #2
a6 5e 99 .....Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
a6 5e 9a .....Bluetooth Device (Personal Area Network)
ec ac 29 .....Realtek PCIe GbE Family Controller
..... Software Loopback Interface 1
=====

le
=====

      Netmask     Gateway     Interface Metric
0.0       0.0.0.0   192.168.29.1  192.168.29.184 35
0.0       255.0.0.0   On-link      127.0.0.1    331
0.1   255.255.255.255   On-link      127.0.0.1    331
255   255.255.255.255   On-link      127.0.0.1    331
9.0       255.255.255.0   On-link      192.168.29.184 291
184   255.255.255.255   On-link      192.168.29.184 291
255   255.255.255.255   On-link      192.168.29.184 291
0.0       240.0.0.0   On-link      127.0.0.1    331
0.0       240.0.0.0   On-link      192.168.29.184 291
255   255.255.255.255   On-link      127.0.0.1    331
255   255.255.255.255   On-link      192.168.29.184 291
=====

tes:

le
=====

      work Destination     Gateway
0           fe80::1a82:8cff:fee9:7cb9
/128        On-link
5:201:1:6019::/64   On-link
5:201:1:6019:2b57:8769:d6b2:11ef/128
          On-link
=====
```

1. nslookup

used for querying the Domain Name System (DNS) to obtain information about domain names, IP addresses, and related DNS records.

```

tik>nslookup
r: reliance.reliance
5:201:1:6019::c0a8:1d01
```

1. nslookup www.google.com

retrieve and display the IP address associated with the domain name "www.google.com" by querying the DNS.

```
ik>nslookup www.google.com
Ince.reliance
:201:1:6019::c0a8:1d01

Non-existent answer:
www.google.com
94:6800:4009:81f::2004
250.182.228
```

1. nslookup -q=mx www.google.com

Initiates a DNS query specifically for Mail Exchange (MX) records. This will retrieve and display the mail servers responsible for handling email for the specified domain.

```
ik>nslookup -q=mx www.google.com
Ince.reliance
:201:1:6019::c0a8:1d01

Non-existent answer:
Name server = ns1.google.com
Possible mail addr = dns-admin.google.com
TTL = 601989564
TTL = 900 (15 mins)
TTL = 900 (15 mins)
TTL = 1800 (30 mins)
TTL = 60 (1 min)
```

1. nslookup -type=ns wikipedia.org

This command queries the DNS for the authoritative Name Server (NS) records for the domain "example.com."

```
tik>nslookup -type=ns wikipedia.org  
ance.reliance  
5:201:1:6019::c0a8:1d01  
  
tive answer:  
    nameserver = ns1.wikimedia.org  
    nameserver = ns2.wikimedia.org  
    nameserver = ns0.wikimedia.org
```

1. nslookup -type=any google.com

Lookup for any record We can also view all the available DNS records using the -type=any option.

```
tik>nslookup -type=any google.com  
ance.reliance  
5:201:1:6019::c0a8:1d01  
  
tive answer:  
    internet address = 142.250.77.46  
    AAAA IPv6 address = 2404:6800:4009:81c::200e  
  
    try name server = ns1.google.com  
    possible mail addr = dns-admin.google.com  
    = 601989564  
    h = 900 (15 mins)  
    = 900 (15 mins)  
    = 1800 (30 mins)  
    t TTL = 60 (1 min)  
    nameserver = ns4.google.com  
    nameserver = ns2.google.com  
    nameserver = ns3.google.com  
    nameserver = ns1.google.com
```

1. route print

display the current IP routing table.

```
ik>route print
=====
a6 5e 99 .... Microsoft Wi-Fi Direct Virtual Adapter
a6 5e 99 .... Microsoft Wi-Fi Direct Virtual Adapter #2
a6 5e 99 .... Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
a6 5e 9a .... Bluetooth Device (Personal Area Network)
ec ac 29 .... Realtek PCIe GbE Family Controller
..... Software Loopback Interface 1
=====

Le
=====

  Destination      Netmask        Gateway        Interface Metric
0.0          0.0.0.0      192.168.29.1    192.168.29.184     35
0.0          255.0.0.0           On-link       127.0.0.1      331
0.1  255.255.255.255           On-link       127.0.0.1      331
255  255.255.255.255           On-link       127.0.0.1      331
0.0          255.255.255.0           On-link    192.168.29.184     291
184  255.255.255.255           On-link    192.168.29.184     291
255  255.255.255.255           On-link    192.168.29.184     291
0.0          240.0.0.0           On-link       127.0.0.1      331
0.0          240.0.0.0           On-link    192.168.29.184     291
255  255.255.255.255           On-link       127.0.0.1      331
255  255.255.255.255           On-link    192.168.29.184     291
=====
tes:
```

1. route print -6

displays only the IPv6 routing table. This command provides information about IPv6 routes.

```
tik>route print -6
=====
t
d a6 5e 99 .....Microsoft Wi-Fi Direct Virtual Adapter
d a6 5e 99 .....Microsoft Wi-Fi Direct Virtual Adapter #2
d a6 5e 99 .....Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
d a6 5e 9a .....Bluetooth Device (Personal Area Network)
3 ec ac 29 .....Realtek PCIe GbE Family Controller
.....Software Loopback Interface 1
=====

ble
=====
:
twork Destination      Gateway
/0                      fe80::1a82:8cff:fee9:7cb9
1/128                  On-link
05:201:1:6019::/64     On-link
05:201:1:6019:2b57:8769:d6b2:11ef/128
                         On-link
05:201:1:6019:d949:70fa:542a:ce47/128
                         On-link
80::/64                 On-link
80::7680:a94b:5d3:9a0e/128
                         On-link
00::/8                  On-link
00::/8                  On-link
=====
utes:
```

1. route -F

The ROUTE -F command is used in Windows to flush the IPv4 routing table. It clears all entries from the routing table, effectively removing all configured routes.

```
tik>route -F
operation requires elevation.
```

1. route -p

manipulates network routing tables

```
ik>route -p  
twork routing tables.
```

1. route delete 127.0.01

used to remove a specific route from the routing table.

```
ik>route delete 127.0.01  
operation requires elevation.
```

1. hostname

In Windows, running HOSTNAME in the command prompt will display the current hostname of the computer.

```
utik>hostname  
G3N
```

1. echo %COMPUTERNAME%

displays the name of the computer in uppercase

```
ik>echo %COMPUTERNAME%  
N
```

1. set "_CLUSTER_NETWORK_NAME_=Shrutik_LAPTOP-6BJ1JG3N"

To alter the hostname output

```
tik>set "_CLUSTER_NETWORK_NAME_=Shrutik_LAPTOP-6BJ1JG3N"  
tik>hostname  
-6BJ1JG3N
```

1. curl www.google.com

This command sends a GET request to "https://www.google.com" and displays the response on the terminal.

```
C:\Windows\System32>curl https://www.google.com
<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en-IN"><head><meta content="standard_color_128dp.png" itemprop="image"><title>Google</title><script nonce="i1VgudZ00RejZbLBDGYgNA80,35512,9287,23792,12319,17580,4998,17075,41316,2891,4139,7615,606,58287,5017,13491,230,1014,1,1625,801,10161,23351,22435,9779,12415,30044,3141,17057,33566,10943,28670,3030,15816,1804,7734,6072,116673,43886,3,1603,3,262,3,234,3,2121276,2585,22636438,392913,8163,10336,2709,8027,8639,13021,4427,1359,853,149,2071,3055,2,82,1,6,2815,390,163,1812,2,1769,3334,4,661,3,362,1849,414,2481,673,1448,7,1373,1321,3,1209,548,119,166,1595,132,215,81,4224,111,468,2046,507,550,54,2,4,96,3609,109,841,98,2,287,880,658,606,94,122,740,107,69,742,675,865,14,110,2249,21347689,364337,218,7416,162,908,60',g;).call(this);});})(function(){google.sn='webhp';google.kHL='en-IN';})();(function(){
var h=this||self;function l(){return void 0!==window.google&&void 0!==window.google.kOPI&&0!==window.e("eid"));)a=a.parentNode;return b||m}function q(a){for(var b=null;a&&(!a.getAttribute||!(b=a.getAttribute("src")));)a=a.parentNode;return b||m}function r(a){for(var b=null;a&&(!a.getAttribute||!(b=a.getAttribute("src")));)a=a.parentNode;return b||m}function s(a){for(var b=null;a&&(!a.getAttribute||!(b=a.getAttribute("src")));)a=a.parentNode;return b||m}function t(a,b,c,d,k){var e="";-1==b.search("&ei")&&(e="+p(d),-1==b.search("&lei")&&(d=q(cshid&&f.push(["cshid",h._cshid]));c=c();null!=c&&f.push(["opi",c.toString()]);for(c=0;c<f.length;d));m=google.kEI;google.getEI=p;google.getLEI=q;google.ml=function(){return null};google.log=load=a.onabort=function(){delete n[g]};a.src=c};google.logUrl=function(a,b){b=void 0==b?l:b;return Math.random();while(google.y[c])google.y[c]=[a,b];return!1};google.sx=function(a){google.sy.push([c]{google.lq.push([[a],b,c])});google.loadAll=function(a,b){google.lq.push([a,b])};google.bx=!1;google.erd={jsr:1,bv:1944,de:true};var h=this||self;var k,l=null!=(k=h.mei)?k:1,n,p=null!=(n=h.sdo)?n:!0,q=0,r,t=google.erd,v=t.jsr;gle_+google.aple;if(google.dl)return google.dl(a,e,d),null;b=d;if(0>v){window.console&&console.error=null;q++;d=d||{};b=encodeURIComponent;var c="/gen_204?atyp=i&ei="+b(google.kEI);google.kEXPI&b(t.bv);var f=a.lineNumber;void 0!=f&&(c+="&line="+f);var g=a.fileName;g&&(0<g.indexOf("-extension"),c+="&cad="+b(f.substring(0,300)):"No script found."));google.ple&&1==google.ple&&(e=2);c+="&jsck||"|"N/A");12288<=c.length&&(c=c.substr(0,12288));a=c;m||google.log(0,"",a);return a};window.onerror 0==b||"fileName"in a||(a.fileName=b),google.ml(a,!1,void 0,!1,"SyntaxError"==a.name||"SyntaxError");});});(function(){document.images){new Image().src=src;}}if (!iesg){document.f&&document.f.q.focus();document.gbqf&&document.gbqf.q.focus();}}
```

1. curl -v <https://www.google.com>

used to switch on verbose mode

```
C:\Windows\System32>curl -v https://www.google.com
*   Trying [2404:6800:4009:81f::2004]:443...
* Connected to www.google.com (2404:6800:4009:81f::2004) port 443
* schannel: disabled automatic use of client certificate
* ALPN: curl offers http/1.1
* ALPN: server accepted http/1.1
* using HTTP/1.1
> GET / HTTP/1.1
> Host: www.google.com
> User-Agent: curl/8.4.0
> Accept: */*
>
* schannel: remote party requests renegotiation
* schannel: renegotiating SSL/TLS connection
* schannel: SSL/TLS connection renegotiated
< HTTP/1.1 200 OK
< Date: Sun, 28 Jan 2024 16:09:54 GMT
< Expires: -1
< Cache-Control: private, max-age=0
< Content-Type: text/html; charset=ISO-8859-1
< Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-qd
sp.withgoogle.com/csp/gws/other-hp
< P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
< Server: gws
< X-XSS-Protection: 0
< X-Frame-Options: SAMEORIGIN
< Set-Cookie: 1P_JAR=2024-01-28-16; expires=Tuesday, 27-Feb-2024 16:09:54 GMT; path=/; domain=.go
< Set-Cookie: AEC=Ae3NU904KB3H34tbJeU8qGpj-p1D9DXccZjuCDQLCQ9U2dHT1UBTdiyWbk; expires=Friday, 2
< Set-Cookie: NID=511=qADbFWv4JmQpWcbMy8pBm5PVsW9U_b0ItCpKdOoPKYWe1DyUZrnzeiiNl027lbHyC-6N936
Jul-2024 16:09:54 GMT; path=/; domain=.google.com; HttpOnly
< Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
< Accept-Ranges: none
< Vary: Accept-Encoding
< Transfer-Encoding: chunked
```

1. curl -vL <https://www.google.com>

used to ask for both verbose mode and that curl follows HTTP redirects

```
C:\Windows\System32>curl -vL https://www.google.com
*   Trying [2404:6800:4009:81f::2004]:443...
* Connected to www.google.com (2404:6800:4009:81f::2004) port 443
* schannel: disabled automatic use of client certificate
* ALPN: curl offers http/1.1
* ALPN: server accepted http/1.1
* using HTTP/1.1
> GET / HTTP/1.1
> Host: www.google.com
> User-Agent: curl/8.4.0
> Accept: */*
>
* schannel: remote party requests renegotiation
* schannel: renegotiating SSL/TLS connection
* schannel: SSL/TLS connection renegotiated
* schannel: failed to decrypt data, need more data
< HTTP/1.1 200 OK
< Date: Sun, 28 Jan 2024 16:16:37 GMT
< Expires: -1
< Cache-Control: private, max-age=0
< Content-Type: text/html; charset=ISO-8859-1
< Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-kl8biC7kX8MqlIGu0llHsp.withgoogle.com/csp/gws/other-hp
< P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
< Server: gws
< X-XSS-Protection: 0
< X-Frame-Options: SAMEORIGIN
< Set-Cookie: 1P_JAR=2024-01-28-16; expires=Tue, 27-Feb-2024 16:16:37 GMT; path=/; domain=.google.com; Secure
< Set-Cookie: AEC=Ae3NU9Nh8aKtbSUhRJEPEY96u4V4-pIihhtB42Tpiq5X-EiRoU7Wfs-2nyQ; expires=Fri, 26-Jul-2024 16:16:37
< Set-Cookie: NID=511=re-1bYoFJsCRzRl6bbN9sBeaVz6qM]mUPZxqVL_ETHbz_Uf6biVAEh-D_igU3SIHZI6flobAYlEYDmxNbSZNhDh0
Jul-2024 16:16:37 GMT; path=/; domain=.google.com; HttpOnly
< Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
< Accept-Ranges: none
< Vary: Accept-Encoding
< Transfer-Encoding: chunked
```

1. curl -A "shrutik gupta" <https://www.google.com>

used to pass on an argument to an option

```
C:\Windows\System32>curl -A "shrutik gupta" https://www.google.com
<!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en-IN"><head>
  <img alt="Standard_color_128dp.png" itemprop="image"><title>Google</title><script nonce="sf-vSNdTuv_Q5t
  0705,44798,23792,12311,17588,4998,17075,38444,2872,2891,4140,4208,3406,606,60690,2614,1372
  ,2006,8155,23351,22435,9779,38678,3781,20198,33565,34492,5122,3030,15816,1804,7734,6072,72
  86,3,1603,3,262,3,234,3,2121276,2585,22636438,397039,1298,2526,1,212,10336,2709,6577,1450,
  5120,3336,50,1043,39,1541,42,5057,435,1894,2901,2212,149,2071,1603,4,1532,1,6,2815,1350,27
  64,585,4,168,2,521,661,64,133,100,1222,1213,548,119,43,1,122,1406,189,132,25,190,82,2489,1
  343,2609,108,268,179,171,6,363,4,406,155,2,144,1049,35,488,12,2,550,202,184,57,19,542,7,79
  ;(function(){var a;(null==(a=window.google)?0:a.stvsc)?google.kEI=_g.kEI:window.google=_g;
  var h=this||self;function l(){return void 0!==window.google&&void 0!==window.google.kOPI&&
  e("eid"));)a=a.parentNode;return b||m}function q(a){for(var b=null;a&&(!a.getAttribute()|
  |&&(google.ml&&google.ml(Error("a"),!1,{src:a,glmm:1}),a="");return a}
  function t(a,b,c,d,k){var e="";-1===-b.search("&ei")&&(e="&ei="+p(d),-1===-b.search("&lei="cshid&&g&&f.push(["cshid",h._cshid]);c=c();null!=c&&f.push(["opi",c.toString()]);for(c=0;c
  d});m=google.kEI;google.getEI=p;google.getLEI=q;google.ml=function(){return null};google.l
  load=a.onabort=function(){delete n[g]};a.src=c});google.logUrl=function(a,b){b=void 0==b?
  =Math.random();while(google.y[c])google.y[c]=[a,b];return!1};google.sx=function(a){google
  ,c}{google.lq.push([[a],b,c])};google.loadAll=function(a,b){google.lq.push([a,b])};google.
  ={};(function(){
  document.documentElement.addEventListener("submit",function(b){var a;if(a=b.target){var c=
  propagation()),!0);document.documentElement.addEventListener("click",function(b){var a;a:{}
  ;break a}a!=1}a&&b.preventDefault(),!0);).call(this);</script><style>#gbar,#guser{font-
  order-top:1px solid #c9d7f1;font-size:1px}.gbh{height:0;position:absolute;top:24px;width:1
  in !important}a.gb1,a.gb4{color:#00c !important}.gb1 .gb4{color:#dd8e27 !important}.gbf .
  {padding:3px 8px 0}td{line-height:.8em}.gac_m td{line-height:17px}form{margin-bottom:20px}
  }.gsfs{font:17px arial,sans-serif}.ds{display:inline-box;display:inline-block;margin:3px 0
  er,a:active{text-decoration:underline}.fl a{color:#1967d2}a:visited{color:#681da8}.sblc{pa
  x;border-color:#dadce0 #70757a #dadce0;height:30px}.lsbb{display:block}#WqQANb a{d
  ursor:pointer;height:30px;margin:0;outline:0;font:15px arial,sans-serif;vertical-align:top
  .google.erd={jsr:1,bv:1944,de:true};
  var h=this||self;var k,l=null!=(k=h.mei)?k:1,n,p=null!=(n=h.sdo)?n:!0,q=0,r,t=google.erd,v
  le_+google.aple;if(google.dl) return google.dl(a,e,d),null;b=d;if(0>v){window.console&&con
  turn null;q++&d=d||{};b=encodeURIComponent;var c="/gen_204?atyp=i&ei="+b(google.kEI);googl
  b(t.bv);var f=a.lineNumber;void 0==f&&(c+="&line="+f);var g=a.fileName;g&&(0<g.indexOf("-"
  ,c+="&cad="+b(f?f.substring(0,300):"No script found."));google.ple&&1==google.ple&&(e=2)
  ck||"N/A");12288<=c.length&&(c=c.substr(0,12288));a=c;m||google.log(0,"",a);return a};wind
  d 0==b||"fileName"in a||(a.fileName=b),google.ml(a,!1,void 0,!1,"SyntaxError"==a.name||"
  11});});});</script></head><body bgcolor="#fff"><script nonce="sf-vSNdTuv_Q5twNbfIGsg">(fun
  ument.images){new Image().src=src;};
  if (!iesg){document.f&&document.f.q.focus();document.gbqf&&document.gbqf.q.focus();}
```

1. arp /a

used to display the arp cache tables for all interfaces, type

```
tik>arp /a

2.168.29.184 --- 0x8
  Address      Physical Address      Type
 1           18-82-8c-e9-7c-b9      dynamic
255          ff-ff-ff-ff-ff-ff      static
              01-00-5e-00-00-16      static
              01-00-5e-00-00-fb      static
              01-00-5e-00-00-fc      static
.250         01-00-5e-7f-ff-fa      static
.255         ff-ff-ff-ff-ff-ff      static
```

1. arp -s 192.168.1.2 ab:cd:ef:gh:ij:kl

used to add a new entry to the ARP cache

```
ARP entry added for 192.168.1.2
```

1. arp -d 192.168.1.2

used to remove an entry from the ARP cache

```
ARP entry removed for 192.168.1.2
```

1. arp -v

This option shows the verbose information.

```
root@kali:~# arp -v
Address          ] on eth0  HWtype  HWaddress      Flags Mask       Iface
machine1        ether    08:00:27:ad:87:b3  C          eth0
machine2        ether    08:00:27:27:d6:c7  C          eth0
10.0.2.3        ether    08:00:27:e5:fd:ed  C          eth0
_gateway        ether    52:54:00:12:35:00  C          eth0
Entries: 4      Skipped: 0      Found: 4
```

1. arp -H ether

This tells arp which class of entries it should check for.

Address	HWtype	HWaddress	Flags	Mask	Iface
machine1	ether	08:00:27:ad:87:b3	C		eth0
machine2	ether	08:00:27:27:d6:c7	C		eth0
10.0.2.3	ether	08:00:27:e5:fd:ed	C		eth0
_gateway	ether	52:54:00:12:35:00	C		eth0

1. whois tsec.edu

WHOIS is used to query a database and retrieve information about the registration details of domain names, including ownership, registration and expiration dates, name servers, and contact information.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ whois tsec.edu
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.
```

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: <http://whois.educause.edu>

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail. The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

Domain Name: TSEC.EDU

Registrant:

Thadomal Shahani Engineering College
P.G Kher Marg, Bandra(W)
Mumbai, Maharashtra 400 050
India

Administrative Contact:

Dr. Gopakumaran Thampi
Thadomal Shahani Engineering College
Nari Gurshahani Marg, Bandra(W)
Mumbai, 400050
India

1. whois -H tsec.edu

When you use the ‘whois’ command, the output often includes legal disclaimers.
If you want to hide these disclaimers, you can use the -H flag.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ whois tsec.edu
This Registry database contains ONLY .EDU domains.
The data in the EDUCAUSE Whois database is provided
by EDUCAUSE for information purposes in order to
assist in the process of obtaining information about
or related to .edu domain registration records.
```

The EDUCAUSE Whois database is authoritative for the
.EDU domain.

A Web interface for the .EDU EDUCAUSE Whois Server is
available at: <http://whois.educause.edu>

By submitting a Whois query, you agree that this information
will not be used to allow, enable, or otherwise support
the transmission of unsolicited commercial advertising or
solicitations via e-mail. The use of electronic processes to
harvest information from this server is generally prohibited
except as reasonably necessary to register or modify .edu
domain names.

Domain Name: TSEC.EDU

Registrant:

Thadomal Shahani Engineering College
P.G Kher Marg, Bandra(W)
Mumbai, Maharashtra 400 050
India

Administrative Contact:

Dr. Gopakumaran Thampi
Thadomal Shahani Engineering College
Nari Gurshahani Marg, Bandra(W)
Mumbai, 400050
India

1. whois -i tsec.edu

By default, the ‘whois’ command is case-sensitive. However, you can make it case-insensitive by using the -i flag.

```
-----  
Domain Name: TSEC.EDU
```

Registrant:

Thadomal Sahani Engineering College
P.G Kher Marg, Bandra(W)
Mumbai, Maharashtra 400 050
India

Administrative Contact:

Dr. Gopakumaran Thampi
Thadomal Shahani Engineering College
Nari Gurshahani Marg, Bandra(W)
Mumbai, 400050
India

1. whois -l tsec.edu

If you're writing a script and need the output of the 'whois' command to be on one line, you can use the -l flag.

```
lab1003@lab1003-HP-280-G4-MT-Business-PC:~$ whois tsec.edu  
This Registry database contains ONLY .EDU domains.  
The data in the EDUCAUSE Whois database is provided  
by EDUCAUSE for information purposes in order to  
assist in the process of obtaining information about  
or related to .edu domain registration records.  
  
The EDUCAUSE Whois database is authoritative for the  
.EDU domain.  
  
A Web interface for the .EDU EDUCAUSE Whois Server is  
available at: http://whois.educause.edu  
  
By submitting a Whois query, you agree that this information  
will not be used to allow, enable, or otherwise support  
the transmission of unsolicited commercial advertising or  
solicitations via e-mail. The use of electronic processes to  
harvest information from this server is generally prohibited  
except as reasonably necessary to register or modify .edu  
domain names.
```

1. ss

The output returns a list of open non-listening sockets with established connections.

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
u_seq	ESTAB	0	0	@0002b 40545	* 40546
u_seq	ESTAB	0	0	@0002a 40543	* 40544
u_str	ESTAB	0	0	* 47336	* 47335
u_str	ESTAB	0	0	* 37615	* 37616
u_str	ESTAB	0	0	* 37263	* 36819
u_str	ESTAB	0	0	* 37816	* 37817
u_str	ESTAB	0	0	* 40173	* 40174
u_str	ESTAB	0	0	* 38066	* 39294

1. ss --all

List all listening and non-listening connections with

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
nl	UNCONN	0	0	rtnl:avahi-daemon/911	*
nl	UNCONN	0	0	rtnl:1828717503	*
nl	UNCONN	0	0	rtnl:chrome/4111	*
nl	UNCONN	0	0	rtnl:vmnet-natd/1562	*
nl	UNCONN	0	0	rtnl:kernel	*
nl	UNCONN	0	0	rtnl:vmnet-bridge/1495	*
nl	UNCONN	0	0	rtnl:chrome/4058	*
nl	UNCONN	0	0	rtnl:dnsmasq/1170	*

1. ss --listen

used to display only listening sockets, which are omitted by default

Netid	State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
nl	UNCONN	0	0	rtnl:avahi-daemon/911	*
nl	UNCONN	0	0	rtnl:1828717503	*
nl	UNCONN	0	0	rtnl:chrome/4111	*
nl	UNCONN	0	0	rtnl:vmnet-natd/1562	*
nl	UNCONN	0	0	rtnl:kernel	*
nl	UNCONN	0	0	rtnl:vmnet-bridge/1495	*
nl	UNCONN	0	0	rtnl:chrome/4058	*
nl	UNCONN	0	0	rtnl:dnsmasq/1170	*

1. ss --tcp

used to list TCP connections

State	Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
ESTAB	0	0	192.168.100.2:34494	108.177.126.188:5228
ESTAB	0	0	192.168.100.2:45618	142.250.184.150:https
ESTAB	0	0	192.168.100.2:39146	52.85.7.80:https

1. ss -udp

used to show a list of UDP connections

Recv-Q	Send-Q	Local Address:Port	Peer Address:Port
0	0	192.168.100.2:36036	216.58.206.206:https

(reference – www.thegeekstuff.com)

1. dig redhat.com

When you pass a domain name to the dig command, by default it displays the A record

```
$ dig redhat.com

; <>> DiG 9.7.3-RedHat-9.7.3-2.el6 <>> redhat.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62863
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 3

;; QUESTION SECTION:
;redhat.com.           IN      A

;; ANSWER SECTION:
redhat.com.        37      IN      A      209.132.183.81

;; AUTHORITY SECTION:
redhat.com.        73      IN      NS     ns4.redhat.com.
redhat.com.        73      IN      NS     ns3.redhat.com.
redhat.com.        73      IN      NS     ns2.redhat.com.
redhat.com.        73      IN      NS     ns1.redhat.com.

;; ADDITIONAL SECTION:
ns1.redhat.com.    73      IN      A      209.132.186.218
ns2.redhat.com.    73      IN      A      209.132.183.2
ns3.redhat.com.    73      IN      A      209.132.176.100
```

1. dig redhat.com +noall +answer

+noanswer – Turn off the answer section

```
$ dig redhat.com +noall +answer

; <>> DiG 9.7.3-RedHat-9.7.3-2.el6 <>> redhat.com +noall +answer
;; global options: +cmd

redhat.com.          60      IN      A      209.132.183.81
```

1. dig redhat.com MX +noall +answer

To query MX records, pass MX as an argument to the dig command

```
$ dig redhat.com MX +noall +answer

; <>> DiG 9.7.3-RedHat-9.7.3-2.el6 <>> redhat.com MX +noall +answer
;; global options: +cmd

redhat.com.          513      IN      MX      5 mx1.redhat.com.
redhat.com.          513      IN      MX      10 mx2.redhat.com.
```

1. dig redhat.com NS +noall +answer

To query the NS record use the type NS

```
$ dig redhat.com NS +noall +answer

; <>> DiG 9.7.3-RedHat-9.7.3-2.el6 <>> redhat.com NS +noall +answer
;; global options: +cmd

redhat.com.      558    IN    NS    ns2.redhat.com.
redhat.com.      558    IN    NS    ns1.redhat.com.
redhat.com.      558    IN    NS    ns3.redhat.com.
redhat.com.      558    IN    NS    ns4.redhat.com.
```

1. dig @ns1.redhat.com redhat.com

By default dig uses the DNS servers defined in your /etc/resolv.conf file. If you like to use a different DNS server to perform the query, specify it in the command line as @dnsserver.

```
$ dig @ns1.redhat.com redhat.com

; <>> DiG 9.7.3-RedHat-9.7.3-2.el6 <>> @ns1.redhat.com redhat.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20963
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
redhat.com.           IN      A

;; ANSWER SECTION:
redhat.com.          60      IN      A      209.132.183.81

;; AUTHORITY SECTION:
redhat.com.          600     IN      NS     ns1.redhat.com.
redhat.com.          600     IN      NS     ns4.redhat.com.
redhat.com.          600     IN      NS     ns3.redhat.com.
redhat.com.          600     IN      NS     ns2.redhat.com.
```

1. mtr -t baeldung.com

The `-t` option indicates we want to see the output in the curses-based terminal

```
$ mtr -t baeldung.com
      My traceroute [v0.94]
myhome (192.168.0.7)                                2022-06-08T01:41:48+0700
Keys: Help   Display mode   Restart statistics   Order of fields   quit
                                         Packets          Pings
Host
1. _gateway                               Loss% Snt Last Avg Best Wrst StDev
2. 11.68.93.1                             0.0% 21 4.8 4.7 3.3 12.0 1.9
3. bex-0005-pele.fast.net.id             0.0% 21 12.9 14.5 11.9 22.2 2.7
4. bex-0005-pele.fast.net.id             0.0% 21 19.4 17.6 14.3 27.3 3.5
5. fm-dyn-www-73-22-333.fast.net.id    0.0% 21 21.9 18.2 13.6 33.7 5.0
6. fm-dyn-www-136-22-333.fast.net.id   0.0% 20 16.9 19.1 15.6 35.4 4.9
7. 172.66.40.248                         0.0% 20 24.1 20.5 16.0 41.9 5.8
```

1. mtr -o 'SA' -t baeldung.com

Suppose we are only interested in the Snt and Avg columns. We could launch mtr with the -o option.

```
$ mtr -o 'SA' -t baeldung.com
      My traceroute [v0.94]
myhome (192.168.0.7)                                2022-06-10T02:41:12+0700
Keys: Help   Display mode   Restart statistics   Order of fields   quit
                                         Packets
                                         Pings          Snt   Avg
1. _gateway                                         8   3.9
2. 11.68.93.1                                       8   14.9
3. bel-cgom-pend.fast.net.id                      8   15.9
4. bel-cgom-pend.fast.net.id                      8   16.6
5. lynx-static-333-56-777-888.lynx.net.id        7   29.4
6. lynx-static-333-56-777-888.lynx.net.id        7   30.9
7. 13335.sgw.equinix.com                          7   31.8
8. 162.158.160.15                                 7   32.2
9. 172.66.43.8                                    7   29.7
```

1. mtr -m 3 -t baeldung.com

we can use the -m option to limit the nodes that we want to investigate.

```
$ mtr -m 3 -t baeldung.com
      My traceroute [v0.94]
myhome (192.168.0.7)                                2022-06-16T01:07:58+0700
Keys: Help   Display mode   Restart statistics   Order of fields   quit
                                         Packets          Pings
Host           Loss%    Snt    Last     Avg   Best  Wrst StDev
1. _gateway        0.0%    4     6.7    5.0   4.3   6.7   1.2
2. 11.68.93.1       0.0%    4    13.2   14.1  13.2  15.3   0.9
3. bel-cgom-pend.fast.net.id  0.0%    4    17.9   17.2  15.1  19.1   1.7
```

1. mtr -f 3 -t baeldung.com

We can filter out the first two hops using the -f option.

```
$ mtr -f 3 -t baeldung.com
      My traceroute [v0.94]
myhome (192.168.0.7)                                2022-06-16T01:33:03+0700
Keys: Help   Display mode   Restart statistics   Order of fields   quit
                                         Packets          Pings
Host           Loss%    Snt    Last     Avg   Best  Wrst StDev
3. bel-cgom-pend.fast.net.id  0.0%   13    82.7   31.4  14.3  90.4  26.5
4. bel-cgom-pend.fast.net.id  0.0%   13    98.0   29.8  14.4  98.0  25.9
5. fm-dyn-333-22-92-876.fast. 0.0%   13    49.4   39.1  15.1  205.3 51.6
6. fm-dyn-333-456-62-876.fast 0.0%   12    94.6   29.1  14.7  94.6  24.4
7. 172.66.40.248            0.0%   12    25.3   32.4  15.1  97.7  27.9
```

1. mtr -r baeldung.com

we can let mtr do the job for a while and read the result later with the -r option.

Start: 2022-06-16T03:04:54+0700

HOST: myhome	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. -- _gateway	0.0%	10	5.6	5.1	3.5	9.6	1.8
2. -- 11.68.93.1	0.0%	10	13.8	13.6	11.3	14.8	1.1
3. -- bel-cgom-pend.fast.net.id	0.0%	10	16.6	18.1	14.9	32.6	5.2
4. -- bel-cgom-pend.fast.net.id	0.0%	10	15.5	17.2	14.7	23.8	2.8
5. -- fm-dyn-222-11-92-133.fast	0.0%	10	15.6	17.2	15.1	23.1	2.6
6. -- fm-dyn-122-122-62-133.fas	0.0%	10	18.6	18.9	15.7	27.7	3.5
7. -- 172.66.40.248	0.0%	10	16.5	16.8	14.3	25.0	3.1

Conclusion: LO1 Achieved.