

CS3009D: NETWORKS LABORATORY

ASSIGNMENT 1

Name: **Tom Saju**

Roll Number: **B191290CS**

Batch: **A**

Date: **16th January 2022**

Use the following tools/commands to explore and summarize the network environment available in your system:

1. **ping**
2. **tracert/traceroute**
3. **ip/ifconfig/ipconfig**
4. **dig/nslookup/host**
5. **whois**
6. **route**
7. **tcpdump**
8. **netstat/ss**
9. **dstat**
10. **ifstat**
11. **wget**
12. **tracpath**

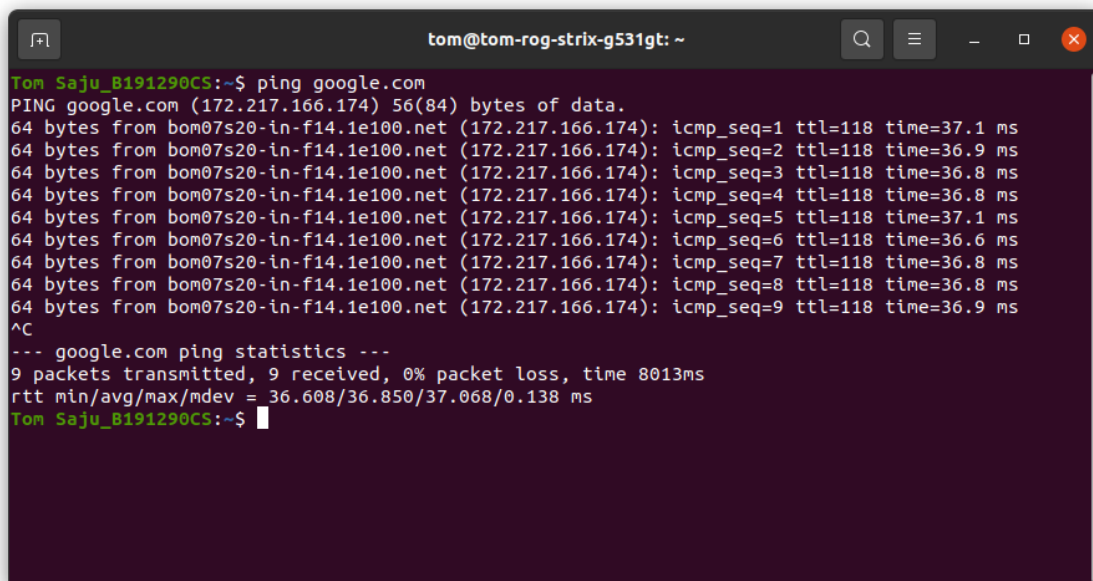
1. ping

Packet Internet Groper (PING) command is used to check the network connectivity between host and server/host. It is used to check whether a network is available and if a host is reachable. With this command, you can check if a server is up and running. When you “ping” a remote host, your machine starts sending Internet Control Message Protocol (ICMP) echo requests and waits for a response. If the connection is established, you’ll receive an echo reply for every request. The output of the ping command contains the amount of time it takes for every packet to reach its destination and return. Also in the terminal, it keeps printing responses until it is stopped.

Example: ping google.com

ping geeksforgeeks.org

ping duckduckgo.com

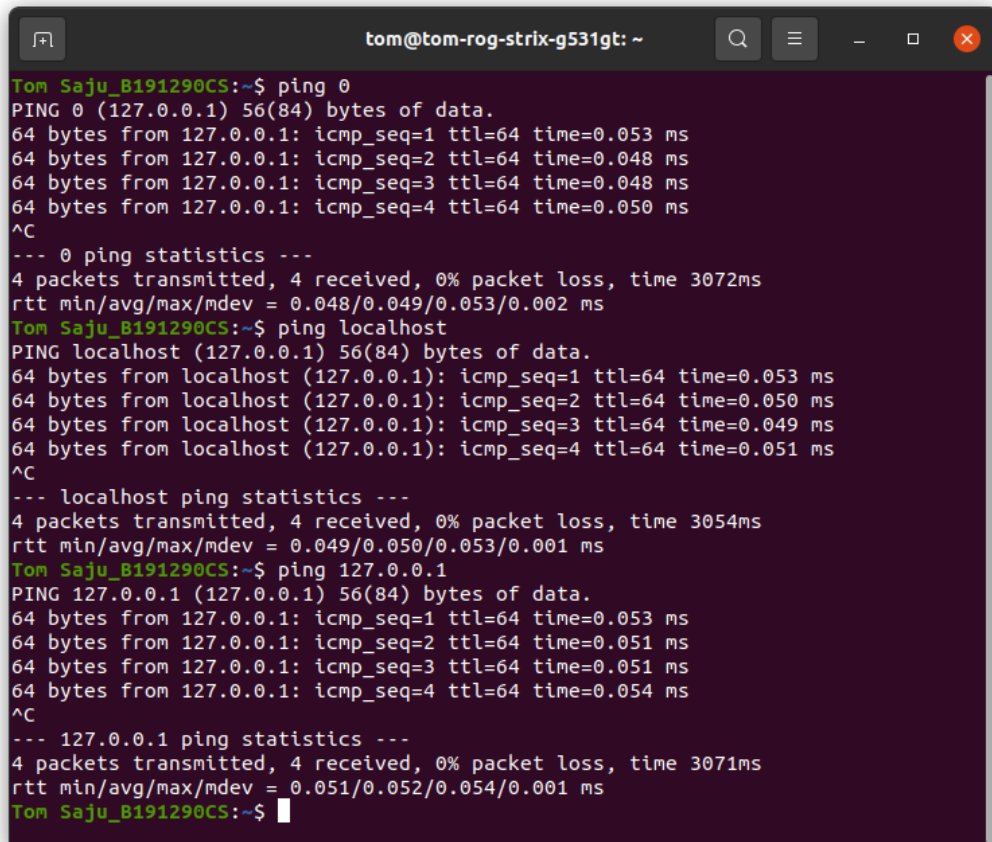


```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ ping google.com  
PING google.com (172.217.166.174) 56(84) bytes of data.  
64 bytes from bom07s20-in-f14.1e100.net (172.217.166.174): icmp_seq=1 ttl=118 time=37.1 ms  
64 bytes from bom07s20-in-f14.1e100.net (172.217.166.174): icmp_seq=2 ttl=118 time=36.9 ms  
64 bytes from bom07s20-in-f14.1e100.net (172.217.166.174): icmp_seq=3 ttl=118 time=36.8 ms  
64 bytes from bom07s20-in-f14.1e100.net (172.217.166.174): icmp_seq=4 ttl=118 time=36.8 ms  
64 bytes from bom07s20-in-f14.1e100.net (172.217.166.174): icmp_seq=5 ttl=118 time=37.1 ms  
64 bytes from bom07s20-in-f14.1e100.net (172.217.166.174): icmp_seq=6 ttl=118 time=36.6 ms  
64 bytes from bom07s20-in-f14.1e100.net (172.217.166.174): icmp_seq=7 ttl=118 time=36.8 ms  
64 bytes from bom07s20-in-f14.1e100.net (172.217.166.174): icmp_seq=8 ttl=118 time=36.8 ms  
64 bytes from bom07s20-in-f14.1e100.net (172.217.166.174): icmp_seq=9 ttl=118 time=36.9 ms  
^C  
--- google.com ping statistics ---  
9 packets transmitted, 9 received, 0% packet loss, time 8013ms  
rtt min/avg/max/mdev = 36.608/36.850/37.068/0.138 ms  
Tom Saju_B191290CS:~$
```

Here,

- from** : The destination and its IP address.
- icmp_seq** : The sequence number of each ICMP packet. Increase by one for every echo request.
- ttl** : TTL (Time to Live) represents the number of network hops a packet can take before a router discards it.
- time** : The time it took for a packet to reach its destination and comes back to the source. Expressed in milliseconds.

Note: We can ping to localhost using
ping 0 / ping localhost / ping 127.0.0.1

A terminal window with a dark purple background and white text. The window title is 'tom@tom-roq-strix-g531gt: ~'. The user 'Tom Saju_B191290CS' is at the prompt. They run 'ping 0', which shows four successful pings to 127.0.0.1 with times around 0.05 ms. Then they run 'ping localhost', showing four successful pings to localhost (127.0.0.1) with times around 0.05 ms. Finally, they run 'ping 127.0.0.1', showing four successful pings to 127.0.0.1 with times around 0.05 ms. Each command output includes packet statistics and round-trip time (rtt) details.

```
tom@tom-roq-strix-g531gt: ~  
Tom Saju_B191290CS:~$ ping 0  
PING 0 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.053 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.048 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.048 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.050 ms  
^C  
--- 0 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3072ms  
rtt min/avg/max/mdev = 0.048/0.049/0.053/0.002 ms  
Tom Saju_B191290CS:~$ ping localhost  
PING localhost (127.0.0.1) 56(84) bytes of data.  
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.053 ms  
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.050 ms  
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.049 ms  
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.051 ms  
^C  
--- localhost ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3054ms  
rtt min/avg/max/mdev = 0.049/0.050/0.053/0.001 ms  
Tom Saju_B191290CS:~$ ping 127.0.0.1  
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.053 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.051 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.051 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.054 ms  
^C  
--- 127.0.0.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3071ms  
rtt min/avg/max/mdev = 0.051/0.052/0.054/0.001 ms  
Tom Saju_B191290CS:~$
```

OUTPUTS

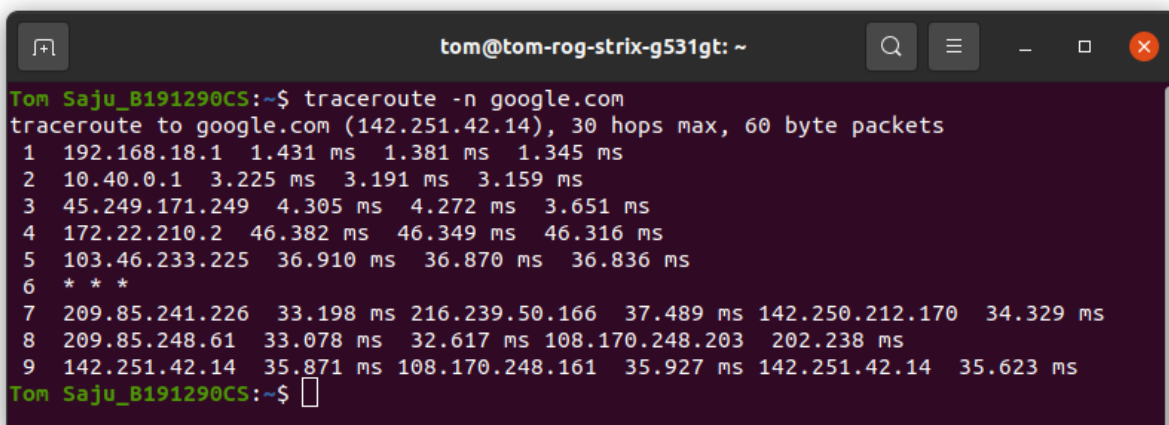
- Case 1:** If we did not get any reply from the destination then it means that there is no network connectivity between host and server/host.
- Case 2:** If the output is “request timed out” then it means the host is down or blocking our ICMP requests.
- Case 3:** If the output is "destination not reachable" then it means that a route to the destination cannot be found.

2. tracer/traceoute

The “traceroute” command in Linux prints the route that the packet takes to reach the host or destination. It displays details about all the hops that the packet visits in between i.e it displays IP addresses and the time it took between each hop. The main use of this tool is to find where the error lies in the network if a data packet is unable to reach the destination.

Example: traceroute facebook.com

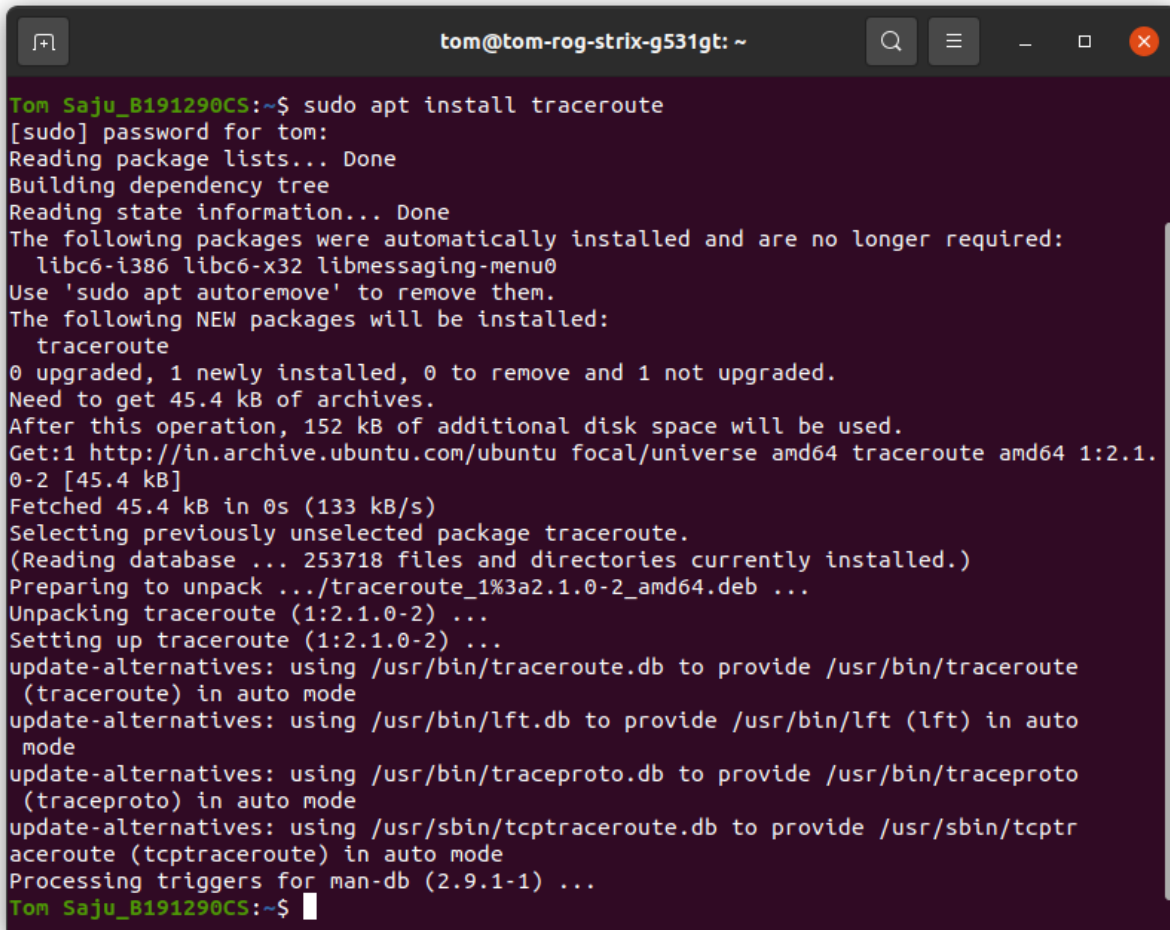
```
traceroute -n google.com
```



```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ traceroute -n google.com  
traceroute to google.com (142.251.42.14), 30 hops max, 60 byte packets  
 1  192.168.18.1  1.431 ms  1.381 ms  1.345 ms  
 2  10.40.0.1  3.225 ms  3.191 ms  3.159 ms  
 3  45.249.171.249  4.305 ms  4.272 ms  3.651 ms  
 4  172.22.210.2  46.382 ms  46.349 ms  46.316 ms  
 5  103.46.233.225  36.910 ms  36.870 ms  36.836 ms  
 6  * * *  
 7  209.85.241.226  33.198 ms  216.239.50.166  37.489 ms  142.250.212.170  34.329 ms  
 8  209.85.248.61  33.078 ms  32.617 ms  108.170.248.203  202.238 ms  
 9  142.251.42.14  35.871 ms  108.170.248.161  35.927 ms  142.251.42.14  35.623 ms  
Tom Saju_B191290CS:~$
```

Note: To install traceroute, use command

“sudo apt install traceroute”

A terminal window with a dark purple background and light green text. The window title is 'tom@tom-rog-strix-g531gt: ~'. The user 'Tom Saju_B191290CS' is at the prompt. They enter 'sudo apt install traceroute'. The terminal shows the password prompt, package list reading, dependency tree building, and state information reading. It lists packages to be removed (libc6-i386, libc6-x32, libmessaging-menu0) and the new package to be installed (traceroute). It shows the disk space requirements and the download of the traceroute package from the Ubuntu archive. The installation process is shown, including unpacking and setting up alternatives for traceroute, lft, traceproto, and tcptraceroute. The terminal ends with the prompt 'Tom Saju_B191290CS:~\$' and a cursor.

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ sudo apt install traceroute  
[sudo] password for tom:  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  libc6-i386 libc6-x32 libmessaging-menu0  
Use 'sudo apt autoremove' to remove them.  
The following NEW packages will be installed:  
  traceroute  
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.  
Need to get 45.4 kB of archives.  
After this operation, 152 kB of additional disk space will be used.  
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 traceroute amd64 1:2.1.0-2 [45.4 kB]  
Fetched 45.4 kB in 0s (133 kB/s)  
Selecting previously unselected package traceroute.  
(Reading database ... 253718 files and directories currently installed.)  
Preparing to unpack .../traceroute_1%3a2.1.0-2_amd64.deb ...  
Unpacking traceroute (1:2.1.0-2) ...  
Setting up traceroute (1:2.1.0-2) ...  
update-alternatives: using /usr/bin/traceroute.db to provide /usr/bin/traceroute (traceroute) in auto mode  
update-alternatives: using /usr/bin/lft.db to provide /usr/bin/lft (lft) in auto mode  
update-alternatives: using /usr/bin/traceproto.db to provide /usr/bin/traceproto (traceproto) in auto mode  
update-alternatives: using /usr/sbin/tcptraceroute.db to provide /usr/sbin/tcptraceroute (tcptraceroute) in auto mode  
Processing triggers for man-db (2.9.1-1) ...  
Tom Saju_B191290CS:~$
```

3. ip/ifconfig/ipconfig

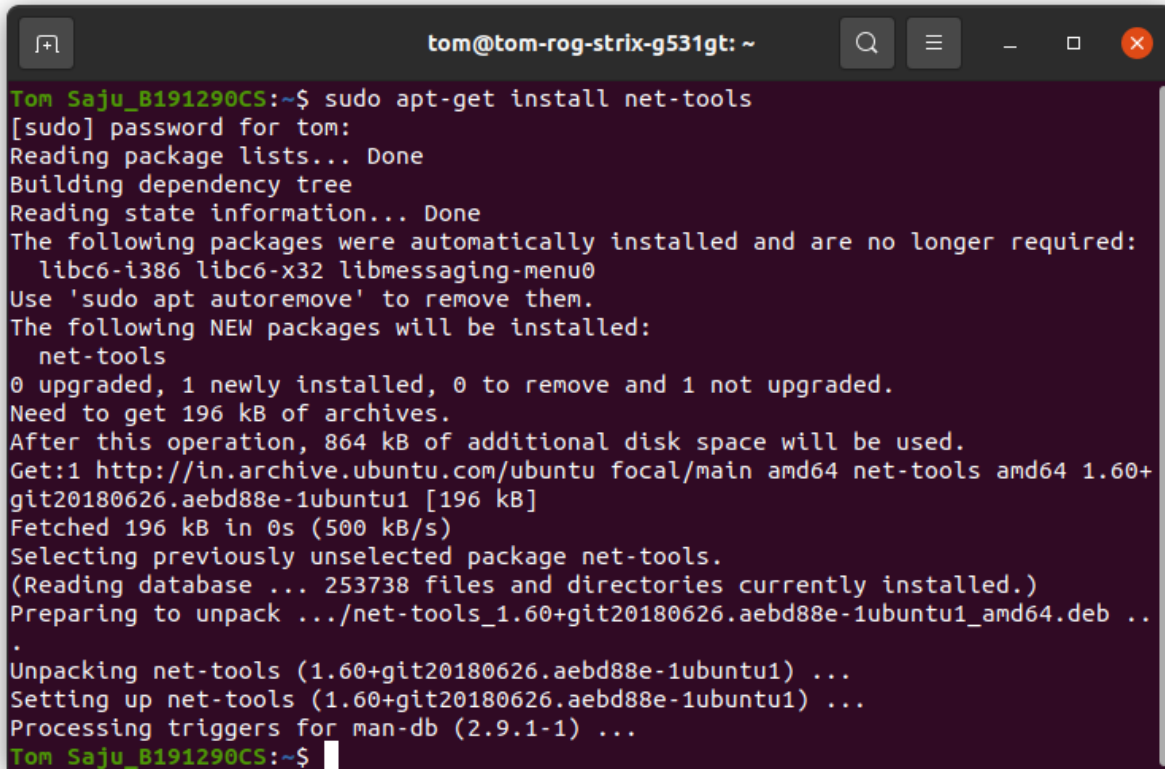
IP: IP (Internet Protocol) Address is an address of your network hardware. It helps in connecting your computer to other devices on your network and all over the world.

ipconfig stands for Internet Protocol Configuration, while ifconfig stands for Interface Configuration. It is often used for troubleshooting network connections. It's generally used to display the TCP/IP address of the system. Ifconfig 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.

Note: In ubuntu install them using the command:

“sudo apt-get install net-tools”

A terminal window with a dark purple background and white text. The window title is 'tom@tom-rog-strix-g531gt: ~'. The user 'Tom Saju_B191290CS' has entered the command 'sudo apt-get install net-tools'. The terminal output shows the process of installing the package, including reading package lists, building a dependency tree, and downloading the package from the Ubuntu archive. The installation is successful, and the prompt returns to the user.

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ sudo apt-get install net-tools  
[sudo] password for tom:  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  libc6-i386 libc6-x32 libmessaging-menu0  
Use 'sudo apt autoremove' to remove them.  
The following NEW packages will be installed:  
  net-tools  
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.  
Need to get 196 kB of archives.  
After this operation, 864 kB of additional disk space will be used.  
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1.60+  
git20180626.aebd88e-1ubuntu1 [196 kB]  
Fetched 196 kB in 0s (500 kB/s)  
Selecting previously unselected package net-tools.  
(Reading database ... 253738 files and directories currently installed.)  
Preparing to unpack .../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb ..  
.  
Unpacking net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...  
Setting up net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...  
Processing triggers for man-db (2.9.1-1) ...  
Tom Saju_B191290CS:~$
```

“ip r”: Find the gateway address in the starting line. 192.168.1.1 is the default gateway in the given image.

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ ip r  
default via 192.168.18.1 dev eno2 proto dhcp metric 100  
169.254.0.0/16 dev eno2 scope link metric 1000  
192.168.18.0/24 dev eno2 proto kernel scope link src 192.168.18.250 metric 100  
Tom Saju_B191290CS:~$
```

“**ifconfig -a**”: Check for IPv4 address beside inet below wlo1, 192.168.1.124 is the IP address in the given image.

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ ifconfig -a  
eno2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.18.250 netmask 255.255.255.0 broadcast 192.168.18.255  
    inet6 fe80::61c9:57c:ab9e:e786 prefixlen 64 scopeid 0x20<link>  
    ether 04:d4:c4:e0:9b:cd txqueuelen 1000 (Ethernet)  
    RX packets 671645 bytes 710350359 (710.3 MB)  
    RX errors 0 dropped 171992 overruns 0 frame 0  
    TX packets 185754 bytes 18296678 (18.2 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 6184 bytes 570088 (570.0 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 6184 bytes 570088 (570.0 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
wlo1: flags=4098<BROADCAST,MULTICAST> mtu 1500  
    ether 40:74:e0:7b:f3:27 txqueuelen 1000 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
Tom Saju_B191290CS:~$
```

4. dig/nslookup/host

nslookup is a command-line administrative tool for testing and troubleshooting DNS servers (Domain Name Server). It is used to query specific DNS resource records (RR) as well.

DNS: The Domain Name System (DNS) is the phone book of the Internet. Humans access information online through domain names, like leetcode.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Example: nslookup google.com

A terminal window with a dark purple background and green text. The window title is 'tom@tom-roq-strix-g531gt: ~'. The user 'Tom Saju_B191290CS' has entered the command 'nslookup google.com'. The output shows the local DNS server (127.0.0.53) and a non-authoritative answer for google.com with IP 142.250.192.142 and its IPv6 address. The prompt returns to the user's shell.

```
tom@tom-roq-strix-g531gt: ~  
Tom Saju_B191290CS:~$ nslookup google.com  
Server:          127.0.0.53  
Address:         127.0.0.53#53  
  
Non-authoritative answer:  
Name:   google.com  
Address: 142.250.192.142  
Name:   google.com  
Address: 2404:6800:4009:82b::200e  
  
Tom Saju_B191290CS:~$
```

Note: To set the servers to mail servers enter interactive mode by giving the command “**nslookup**”

>set type=mx

>google.com


```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ nslookup  
> set type=mx  
> google.com  
Server:          127.0.0.53  
Address:         127.0.0.53#53  
  
Non-authoritative answer:  
google.com       mail exchanger = 10 aspmx.l.google.com.  
google.com       mail exchanger = 50 alt4.aspmx.l.google.com.  
google.com       mail exchanger = 30 alt2.aspmx.l.google.com.  
google.com       mail exchanger = 20 alt1.aspmx.l.google.com.  
google.com       mail exchanger = 40 alt3.aspmx.l.google.com.  
  
Authoritative answers can be found from:  
> exit  
Tom Saju_B191290CS:~$
```

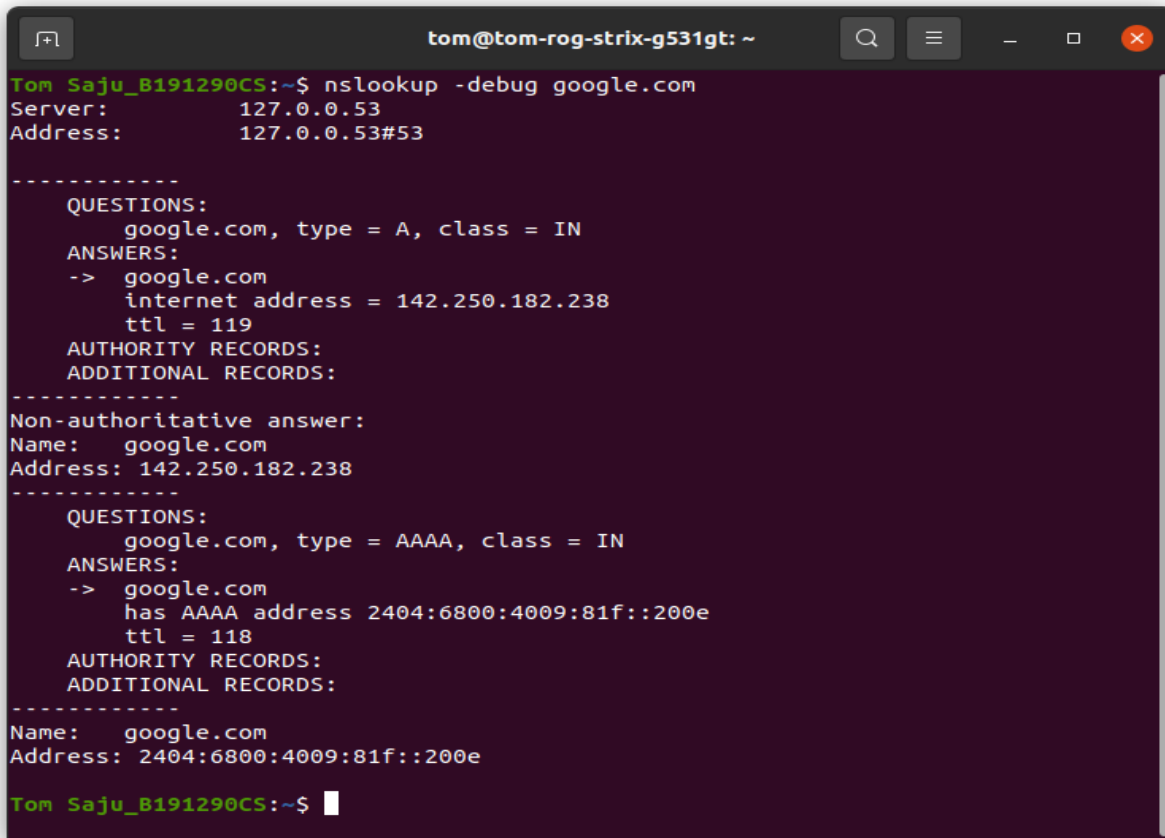
Note: To perform reverse DNS, enter your ip address

Reverse DNS: A reverse DNS lookup or reverse DNS resolution is the querying technique of the Domain Name System to determine the domain name associated with an IP address – the reverse of the usual "forward" DNS lookup of an IP address from a domain name.

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ nslookup  
> 192.168.43.41  
41.43.168.192.in-addr.arpa    name = tom-rog-strix-g531gt.  
41.43.168.192.in-addr.arpa    name = tom-rog-strix-g531gt.local.  
  
Authoritative answers can be found from:  
> exit  
Tom Saju_B191290CS:~$
```

Note: To troubleshoot DNS problem to perform DNS lookup

“nslookup -debug google.com”

A terminal window with a dark purple background and white text. The window title is 'tom@tom-roq-strix-g531gt: ~'. The user 'Tom Saju_B191290CS' has entered the command 'nslookup -debug google.com'. The output shows the server address as 127.0.0.53. It then displays two DNS lookup results for google.com: an A record with IP 142.250.182.238 and a TTL of 119, and an AAAA record with IPv6 address 2404:6800:4009:81f::200e and a TTL of 118. The prompt returns to '~\$' at the end.

```
tom@tom-roq-strix-g531gt: ~  
Tom Saju_B191290CS:~$ nslookup -debug google.com  
Server:          127.0.0.53  
Address:         127.0.0.53#53  
  
-----  
QUESTIONS:  
  google.com, type = A, class = IN  
ANSWERS:  
-> google.com  
   internet address = 142.250.182.238  
   ttl = 119  
AUTHORITY RECORDS:  
ADDITIONAL RECORDS:  
-----  
Non-authoritative answer:  
Name:   google.com  
Address: 142.250.182.238  
-----  
QUESTIONS:  
  google.com, type = AAAA, class = IN  
ANSWERS:  
-> google.com  
   has AAAA address 2404:6800:4009:81f::200e  
   ttl = 118  
AUTHORITY RECORDS:  
ADDITIONAL RECORDS:  
-----  
Name:   google.com  
Address: 2404:6800:4009:81f::200e  
Tom Saju_B191290CS:~$
```

dig google.com

```
tom@tom-roq-strix-g531gt: ~  
Tom Saju_B191290CS:~$ dig google.com  
  
; <<>> DiG 9.16.1-Ubuntu <<>> google.com  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 37688  
;; 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.                52      IN      A      216.58.200.142  
  
;; Query time: 60 msec  
;; SERVER: 127.0.0.53#53(127.0.0.53)  
;; WHEN: Sun Jan 16 20:49:36 IST 2022  
;; MSG SIZE rcvd: 55  
  
Tom Saju_B191290CS:~$
```

5. whois

The whois system is a listing of records that contain details about the ownership of domains and the owners. The Internet corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership, but the list of records is held by many companies, known as registries. Anyone can query the list of records. A whois record contains contact information with the person, company or other entity that registered the DOMAIN name.

Note: Install whois using the command:

“sudo install whois”

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ sudo apt install whois  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  libc6-i386 libc6-x32 libmessaging-menu0  
Use 'sudo apt autoremove' to remove them.  
The following NEW packages will be installed:  
  whois  
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.  
Need to get 44.7 kB of archives.  
After this operation, 279 kB of additional disk space will be used.  
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 whois amd64 5.5.6 [44.7 kB]  
Fetched 44.7 kB in 2s (19.1 kB/s)  
debconf: unable to initialize frontend: Dialog  
debconf: (Dialog frontend requires a screen at least 13 lines tall and 31 columns wide.)  
debconf: falling back to frontend: Readline  
Selecting previously unselected package whois.  
(Reading database ... 253787 files and directories currently installed.)  
Preparing to unpack .../archives/whois_5.5.6_amd64.deb ...  
Unpacking whois (5.5.6) ...  
Setting up whois (5.5.6) ...  
Processing triggers for man-db (2.9.1-1) ...  
Tom Saju_B191290CS:~$
```

Example: whois google.com

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ whois google.com  
Domain Name: GOOGLE.COM  
Registry Domain ID: 2138514_DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.markmonitor.com  
Registrar URL: http://www.markmonitor.com  
Updated Date: 2019-09-09T15:39:04Z  
Creation Date: 1997-09-15T04:00:00Z  
Registry Expiry Date: 2028-09-14T04:00:00Z  
Registrar: MarkMonitor Inc.  
Registrar IANA ID: 292  
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com  
Registrar Abuse Contact Phone: +1.2083895740  
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhi  
bited  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferP  
rohibited  
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhi  
bited  
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhi  
bited  
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferP  
rohibited  
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhi  
bited  
Name Server: NS1.GOOGLE.COM  
Name Server: NS2.GOOGLE.COM  
Name Server: NS3.GOOGLE.COM  
Name Server: NS4.GOOGLE.COM  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of whois database: 2022-01-16T07:59:06Z <<<  
  
For more information on Whois status codes, please visit https://icann.org/epp  
  
NOTICE: The expiration date displayed in this record is the date the  
registrar's sponsorship of the domain name registration in the registry is  
currently set to expire. This date does not necessarily reflect the expiration  
date of the domain name registrant's agreement with the sponsoring  
registrar. Users may consult the sponsoring registrar's Whois database to  
view the registrar's reported date of expiration for this registration.  
  
TERMS OF USE: You are not authorized to access or query our Whois  
database through the use of electronic processes that are high-volume and  
automated except as reasonably necessary to register domain names or  
modify existing registrations; the Data in VeriSign Global Registry  
Services' ("VeriSign") Whois database is provided by VeriSign for  
information purposes only, and to assist persons in obtaining information  
about or related to a domain name registration record. VeriSign does not  
guarantee its accuracy. By submitting a Whois query, you agree to abide
```

```
tom@tom-rog-strix-g531gt: ~  
Name Server: ns2.google.com  
Name Server: ns3.google.com  
DNSSEC: unsigned  
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/  
>>> Last update of WHOIS database: 2022-01-16T08:00:35+0000 <<<  
  
For more information on WHOIS status codes, please visit:  
  https://www.icann.org/resources/pages/epp-status-codes  
  
If you wish to contact this domain's Registrant, Administrative, or Technical  
contact, and such email address is not visible above, you may do so via our web  
form, pursuant to ICANN's Temporary Specification. To verify that you are not a  
robot, please enter your email address to receive a link to a page that  
facilitates email communication with the relevant contact(s).  
  
Web-based WHOIS:  
  https://domains.markmonitor.com/whois  
  
If you have a legitimate interest in viewing the non-public WHOIS details, send  
your request and the reasons for your request to whoisrequest@markmonitor.com  
and specify the domain name in the subject line. We will review that request and  
may ask for supporting documentation and explanation.  
  
The data in MarkMonitor's WHOIS database is provided for information purposes,  
and to assist persons in obtaining information about or related to a domain  
name's registration record. While MarkMonitor believes the data to be accurate,  
the data is provided "as is" with no guarantee or warranties regarding its  
accuracy.  
  
By submitting a WHOIS query, you agree that you will use this data only for  
lawful purposes and that, under no circumstances will you use this data to:  
  (1) allow, enable, or otherwise support the transmission by email, telephone,  
  or facsimile of mass, unsolicited, commercial advertising, or spam; or  
  (2) enable high volume, automated, or electronic processes that send queries,  
  data, or email to MarkMonitor (or its systems) or the domain name contacts (or  
  its systems).  
  
MarkMonitor reserves the right to modify these terms at any time.  
  
By submitting this query, you agree to abide by this policy.  
  
MarkMonitor Domain Management(TM)  
Protecting companies and consumers in a digital world.  
  
Visit MarkMonitor at https://www.markmonitor.com  
Contact us at +1.8007459229  
In Europe, at +44.02032062220  
--  
Tom Saju_B191290CS:~$
```

6. route

Routing Table: A routing table is a file containing information on how the information or packets should be transferred: the network path to all nodes or devices within a network. It is a map used by routers and gateways to track paths. The hop-by-hop routing is widely used, the packet contains the routing table to reach the next hop, once reached, it will read the routing table again to reach the next hop.

Using the route command you can communicate with subnets and different networks, you can also block the traffic between networks or devices by modifying the routing table.

Example:

route	To display routing table entries.
route -n	To display routing tables in full numerical entities.
sudo route add default gw 169.154.0.0	To add default gateway.
sudo route add -host 192.168.1.151 reject	To reject a host/network.
route -Cn	To list routing cache information of Device
ip route	To get details of IP routing table
ip route show table local	To get details of local table with destination of localhost.
ip -4/-6 route	To get details of IPv4/IPv6 details.


```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ route  
Kernel IP routing table  
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface  
default          _gateway        0.0.0.0          UG    20600  0      0 wlo1  
link-local       0.0.0.0         255.255.0.0      U     1000   0      0 wlo1  
192.168.1.151    -               255.255.255.255 !H     0     -      0 -  
192.168.43.0     0.0.0.0         255.255.255.0    U     600    0      0 wlo1  
Tom Saju_B191290CS:~$ route -n  
Kernel IP routing table  
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface  
0.0.0.0          192.168.43.1    0.0.0.0          UG     600    0      0 wlo1  
169.254.0.0      0.0.0.0         255.255.0.0      U     1000   0      0 wlo1  
192.168.1.151    -               255.255.255.255 !H     0     -      0 -  
192.168.43.0     0.0.0.0         255.255.255.0    U     600    0      0 wlo1  
Tom Saju_B191290CS:~$ sudo route add default gw 169.154.0.0  
SIOCADDRT: Network is unreachable  
Tom Saju_B191290CS:~$ sudo route add -host 192.168.1.151 reject  
SIOCADDRT: File exists  
Tom Saju_B191290CS:~$ route -Cn  
Kernel IP routing cache  
Source           Destination      Gateway          Flags Metric Ref    Use Iface  
Tom Saju_B191290CS:~$ ip route  
default via 192.168.43.1 dev wlo1 proto dhcp metric 600  
169.254.0.0/16 dev wlo1 scope link metric 1000  
unreachable 192.168.1.151 scope host  
192.168.43.0/24 dev wlo1 proto kernel scope link src 192.168.43.41 metric 600  
Tom Saju_B191290CS:~$ ip route show table local  
broadcast 127.0.0.0 dev lo proto kernel scope link src 127.0.0.1  
local 127.0.0.0/8 dev lo proto kernel scope host src 127.0.0.1  
local 127.0.0.1 dev lo proto kernel scope host src 127.0.0.1  
broadcast 127.255.255.255 dev lo proto kernel scope link src 127.0.0.1  
broadcast 192.168.43.0 dev wlo1 proto kernel scope link src 192.168.43.41  
local 192.168.43.41 dev wlo1 proto kernel scope host src 192.168.43.41  
broadcast 192.168.43.255 dev wlo1 proto kernel scope link src 192.168.43.41  
Tom Saju_B191290CS:~$ ip -4 route  
default via 192.168.43.1 dev wlo1 proto dhcp metric 600  
169.254.0.0/16 dev wlo1 scope link metric 1000  
unreachable 192.168.1.151 scope host  
192.168.43.0/24 dev wlo1 proto kernel scope link src 192.168.43.41 metric 600  
Tom Saju_B191290CS:~$ ip -6 route  
::1 dev lo proto kernel metric 256 pref medium  
2402:3a80:1294:6737::/64 dev wlo1 proto ra metric 600 pref medium  
fe80::/64 dev wlo1 proto kernel metric 600 pref medium  
default via fe80::c30:9dff:fe7b:c904 dev wlo1 proto ra metric 600 pref high  
Tom Saju_B191290CS:~$
```


7. tcpdump

“**tcpdump**” tool allows you to capture and analyze network traffic such as TCP/IP packets going through the system. Normally used to troubleshoot network issues, also used as a security tool.

It scans from all OSI layers (1- 7) and saves the captured information as .pcap file which can be viewed on WIRESHARK or through the command tool itself.

Example:

sudo tcpdump	It will capture packets from the current interface of the network through which the system is connected to the internet.
sudo tcpdump -c 4	It will capture only 4 packets from the interface.
sudo tcpdump -D	It will print all the list of available networks that this tool can capture packets from.
sudo tcpdump -n host 142.250.182.206	To capture packets related to specific host.
sudo tcpdump -n src host 192.168.1.124	packets from source host
sudo tcpdump -n dst port 80	all packets to port 80

```
tom@tom-roq-strix-g531gt: ~  
Tom Saju_B191290CS:~$ sudo tcpdump  
[sudo] password for tom:  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes  
20:41:19.692140 ARP, Request who-has 192.168.1.1 tell 192.168.1.1, length 46  
20:41:19.737413 IP 192.168.1.6.36320 > multiplay.bsnl.in.domain: 10186+ [1au] PTR  
R? 1.1.168.192.in-addr.arpa. (53)  
20:41:19.918281 ARP, Request who-has 192.168.1.1 tell 192.168.1.6, length 28  
20:41:19.924059 ARP, Reply 192.168.1.1 is-at 14:a7:2b:2b:af:48 (oui Unknown), length 28  
20:41:24.738535 IP 192.168.1.6.35164 > multiplay.bsnl.in.domain: 10186+ [1au] PTR  
R? 1.1.168.192.in-addr.arpa. (53)  
20:41:29.744207 IP 192.168.1.6.42045 > multiplay.bsnl.in.domain: 50485+ [1au] PTR  
R? 97.112.248.218.in-addr.arpa. (56)  
20:41:29.744359 IP 192.168.1.6.47494 > multiplay.bsnl.in.domain: 10186+ [1au] PTR  
R? 1.1.168.192.in-addr.arpa. (53)
```

```
tom@tom-roq-strix-g531gt: ~  
Tom Saju_B191290CS:~$ sudo tcpdump -c 4  
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode  
listening on wlo1, link-type EN10MB (Ethernet), capture size 262144 bytes  
20:43:00.301168 IP 192.168.1.1 > all-systems.mcast.net: igmp query v2 [max resp  
time 1]  
20:43:00.302889 IP 192.168.1.6.35164 > multiplay.bsnl.in.domain: 51408+ [1au] PTR  
R? 1.0.0.224.in-addr.arpa. (51)  
20:43:00.309938 IP multiplay.bsnl.in.domain > 192.168.1.6.35164: 51408 1/4/1 PTR  
all-systems.mcast.net. (173)  
20:43:00.314240 IP 192.168.1.6 > 224.0.0.251: igmp v2 report 224.0.0.251  
4 packets captured  
30 packets received by filter  
0 packets dropped by kernel  
Tom Saju_B191290CS:~$
```

```
tom@tom-roq-strix-g531gt: ~  
Tom Saju_B191290CS:~$ sudo tcpdump -D  
1.wlo1 [Up, Running]  
2.lo [Up, Running, Loopback]  
3.any (Pseudo-device that captures on all interfaces) [Up, Running]  
4.eno2 [Up]  
5.bluetooth-monitor (Bluetooth Linux Monitor) [none]  
6.nflog (Linux netfilter log (NFLOG) interface) [none]  
7.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]  
8.bluetooth0 (Bluetooth adapter number 0) [none]  
Tom Saju_B191290CS:~$
```

8. netstat/ss

netstat is a command tool which displays network connections for TCP/UDP and stats for Interfaces, Network protocols, routing tables, etc. ss replaces netstat. ss command tool which dumps socket stats and displays information similarly but it is faster than netstat. With below ss we get detailed Information about how Linux is communicating with other machines, networks, details about network stats, network protocols, linux socket connections. So, using this information, it's easy to troubleshoot network issues.

Example:

ss	Displays all connections.
ss -a	Displays non listening connections.
ss -l	Displays current listening connections.
ss -t	Displays TCP connections.
ss -u	Displays UDP connections.
ss -x	Displays UNIX connections.
ss -s	Displays summary stats.
ss -t -r state established	Displays connections to specific address.
ss -a dst 192.168.1.1	Displays connections to specific address.

A listening connection means the socket is waiting for connection. A non listening socket implies the connection is already made.

ss

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ ss  
Netid State  Recv-Q Send-Q           Local Address:Port  
                Peer Address:Port           Process  
u_str  ESTAB  0      0      * 58377      * 49573  
u_str  ESTAB  0      0      * 61805      /run/user/1000/pulse/native 64549  
u_str  ESTAB  0      0      * 47085      /run/systemd/journal/stdout 45002  
u_str  ESTAB  0      0      * 41530      * 37440  
u_str  ESTAB  0      0      * 36325      /run/dbus/system_bus_socket 31547  
u_str  ESTAB  0      0      * 49085      * 49480  
u_str  ESTAB  0      0      * 49240      /run/systemd/journal/stdout 35785  
u_str  ESTAB  0      0      * 48365      /run/systemd/journal/stdout 47438
```

ss -a

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ ss -a  
Netid      State      Recv-Q      Send-Q      Local Address:  
Port       Peer Address:Port      Process  
nl         UNCONN     0            0            rtnl:  
avahi-daemon/852 *  
nl         UNCONN     0            0            rtnl:  
winbindd/978 *  
nl         UNCONN     0            0            rtnl:  
systemd-resolve/811 *  
nl         UNCONN     0            0            rtnl:  
xdg-desktop-por/3623 *  
nl         UNCONN     0            0            rtnl:  
evolution-sourc/3277 *
```

SS -S

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ ss -s  
Total: 1144  
TCP: 4 (estab 0, closed 1, orphaned 0, timewait 0)  
  
Transport Total IP IPv6  
RAW 1 0 1  
UDP 7 5 2  
TCP 3 2 1  
INET 11 7 4  
FRAG 0 0 0  
  
Tom Saju_B191290CS:~$
```

SS -u

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ ss -u  
Recv-Q Send-Q Local Address:Port Peer Address:Port Process  
0 0 192.168.1.6:wlo1:bootpc 192.168.1.1:bootps  
Tom Saju_B191290CS:~$
```

netstat

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ netstat  
Active Internet connections (w/o servers)  
Proto Recv-Q Send-Q Local Address Foreign Address State  
udp 0 0 192.168.1.6:bootpc 192.168.1.1:bootps ESTABLISHED  
udp 0 0 192.168.1.6:53421 multiplay.bsnl.i:domain ESTABLISHED  
Active UNIX domain sockets (w/o servers)  
Proto RefCnt Flags Type State I-Node Path  
unix 2 [ ] DGRAM 46849 /run/user/1000/systemd/notify  
unix 2 [ ] DGRAM 44190 /run/user/125/systemd/notify  
unix 2 [ ] DGRAM 34640 /var/run/nvidia-xdriver  
er-a2be6ad4 34639 @var/run/nvidia-xdriver  
unix 4 [ ] DGRAM 1664 /run/systemd/notify  
er-a2be6ad4 1678 /run/systemd/journal/  
unix 2 [ ] DGRAM 1688 /run/systemd/journal/  
syslog 1692 /run/systemd/journal/  
unix 22 [ ] DGRAM 1692 /run/systemd/journal/  
dev-log 63975 /run/wpa_supplicant/w  
unix 9 [ ] DGRAM  
socket  
wlo1
```

netstat -at: lists all TCP ports

A terminal window with a dark purple background and light green text. The window title is 'tom@tom-rog-strix-g531gt: ~'. The user 'Tom Saju_B191290CS' has entered the command 'netstat -at'. The output shows active internet connections. The first two lines are headers: 'Proto Recv-Q Send-Q Local Address' and 'Foreign Address'. The following lines show connections for tcp and tcp6 protocols, including listening ports and connections in a TIME_WAIT state.

```
Tom Saju_B191290CS:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 192.168.1.6:52324      maa05s19-in-f10.1:https TIME_WAIT
tcp        0      0 192.168.1.6:48032      maa03s36-in-f10.1:https TIME_WAIT
tcp6       0      0 ip6-localhost:ipp      [::]:*                  LISTEN
Tom Saju_B191290CS:~$
```

9. dstat

dstat is a tool that is used to retrieve information or statistics from components of the system such as network connections, IO devices, or CPU, etc. It is generally used by system administrators to retrieve a handful of information about the above-mentioned components of the system. It itself performs like vmsta, netstat, etc. By using this tool one can even see the throughput for block devices that make up a single file system or storage system.

Note: Install dstat by the command:

“sudo apt install dstat”

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ sudo apt install dstat  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  libc6-i386 libc6-x32 libmessaging-menu0  
Use 'sudo apt autoremove' to remove them.  
The following NEW packages will be installed:  
  dstat  
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.  
Need to get 55.6 kB of archives.  
After this operation, 466 kB of additional disk space will be used.  
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 dstat all 0.7.4-6  
  [55.6 kB]  
Fetched 55.6 kB in 0s (154 kB/s)  
Selecting previously unselected package dstat.  
(Reading database ... 253804 files and directories currently installed.)  
Preparing to unpack .../archives/dstat_0.7.4-6_all.deb ...  
Unpacking dstat (0.7.4-6) ...  
Setting up dstat (0.7.4-6) ...  
/usr/share/dstat/dstat_mysql_keys.py:41: SyntaxWarning: 'str' object is not call  
able; perhaps you missed a comma?  
    if op.debug > 1: print('%s: exception' (self.filename, e))  
/usr/share/dstat/dstat_squid.py:48: SyntaxWarning: 'str' object is not callable;  
perhaps you missed a comma?  
    if op.debug > 1: print('%s: exception' (self.filename, e))  
Processing triggers for man-db (2.9.1-1) ...  
Tom Saju_B191290CS:~$
```

Example:

dstat

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ dstat  
You did not select any stats, using -cdngy by default.  
--total-cpu-usage-- -dsk/total- -net/total- ---paging-- ---system--  
usr sys idl wai stl | read writ | recv send | in out | int csw  
5 1 94 0 0 | 1828k 419k | 0 0 | 0 0 | 1514 4475  
0 0 100 0 0 | 0 0 | 0 0 | 0 0 | 248 689  
2 1 97 0 0 | 0 0 | 0 0 | 0 0 | 902 3541  
0 0 100 0 0 | 0 0 | 0 0 | 0 0 | 213 596  
0 0 100 0 0 | 0 0 | 0 0 | 0 0 | 216 349  
0 0 100 0 0 | 0 0 | 60B 0 | 198 353  
0 0 99 0 0 | 0 88k | 0 0 | 187 361  
0 0 100 0 0 | 0 0 | 0 0 | 162 289  
0 0 100 0 0 | 0 0 | 0 0 | 201 389  
0 0 100 0 0 | 0 0 | 0 0 | 203 381  
0 0 99 0 0 | 0 0 | 0 0 | 190 405  
0 0 100 0 0 | 0 0 | 0 0 | 181 421  
0 1 99 0 0 | 0 0 | 0 0 | 429 2790  
0 0 100 0 0 | 0 0 | 0 0 | 202 357  
0 0 100 0 0 | 0 0 | 0 0 | 164 317  
3 2 95 0 0 | 0 0 | 106B 192B | 1298 4091  
6 1 92 0 0 | 0 0 | 90B 0 | 1506 4878  
5 1 94 0 0 | 0 0 | 0 0 | 1026 3814  
7 1 92 0 0 | 0 0 | 0 0 | 1301 4492  
0 0 100 0 0 | 0 0 | 0 0 | 170 351  
4 1 95 0 0 | 0 232k | 42B 70B | 1197 4279  
6 1 94 0 0 | 0 0 | 0 0 | 1428 5527  
4 1 95 0 0 | 0 0 | 0 0 | 1100 3663 ^C  
Tom Saju_B191290CS:~$
```

dstat –vmstat: To display information displayed by vmstat. It displays process and memory stats.


```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ dstat -vmstat  
Terminal width too small, trimming output.  
---procs--- ---memory-usage----- ---paging-- -dsk/total- ---system-->  
run blk new|_used_ free_ buff_ _cach|_in_ out|_read_ writ_|_int_ _csw_>  
0 0 36|1993M 11.9G 88.1M 1557M| 0 0|1750k 406k|1484 4390>  
0 0 581|1992M 11.9G 88.1M 1557M| 0 0| 0 88k| 891 3010>  
0 0 0|1992M 11.9G 88.1M 1557M| 0 0| 0 0| 170 375>  
0 0 0|1992M 11.9G 88.1M 1557M| 0 0| 0 0| 182 361>  
0 0 0|1992M 11.9G 88.1M 1557M| 0 0| 0 728k| 240 402>  
0 0 0|1992M 11.9G 88.1M 1557M| 0 0| 0 0| 173 359>^C  
Tom Saju_B191290CS:~$
```

The output indicates:

CPU Stats: CPU usage by user, system processes and number of idle processes, and number of waiting processes, hardware and software interrupts.

Disk Stats: Total number of read and write operations on the disk.

Network Stats: Total amount of Bytes received and sent on network interfaces.

Paging Stats: Number of times information is copied into and moved out of memory.

System Stats: Number of interrupts and context switches.

Example:

dstat -c --top-cpu: To display stats of the process which is consuming most of the CPU.

dstat -c --top-mem: To display stats of the process which is consuming most of the memory.

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ dstat -c --top-cpu  
/usr/bin/dstat:2619: DeprecationWarning: the imp module is deprecated in favour  
of importlib; see the module's documentation for alternative uses  
import imp  
--total-cpu-usage-- --most-expensive-  
usr sys idl wai stl|_cpu process_  
5 1 94 0 0|Xorg 0.9  
0 0 100 0 0|gnome-shell 0.2  
0 0 100 0 0|Xorg 0.1  
0 0 99 1 0|gnome-shell 0.1  
1 2 97 0 0|preload 0.9  
0 0 100 0 0|Xorg 0.1  
0 0 100 0 0|Xorg 0.1^C  
Tom Saju_B191290CS:~$ dstat -c --top-mem  
/usr/bin/dstat:2619: DeprecationWarning: the imp module is deprecated in favour  
of importlib; see the module's documentation for alternative uses  
import imp  
--total-cpu-usage-- --most-expensive-  
usr sys idl wai stl|_memory process_  
5 1 94 0 0|gnome-shell 503M  
0 0 100 0 0|gnome-shell 503M  
0 0 100 0 0|gnome-shell 503M  
0 0 100 0 0|gnome-shell 503M  
0 0 100 0 0|gnome-shell 503M  
0 0 100 0 0|gnome-shell 503M  
0 0 100 0 0|gnome-shell 503M^C  
Tom Saju_B191290CS:~$
```

dstat --list: We can display stats of a few plugins. This command will display those plugins.

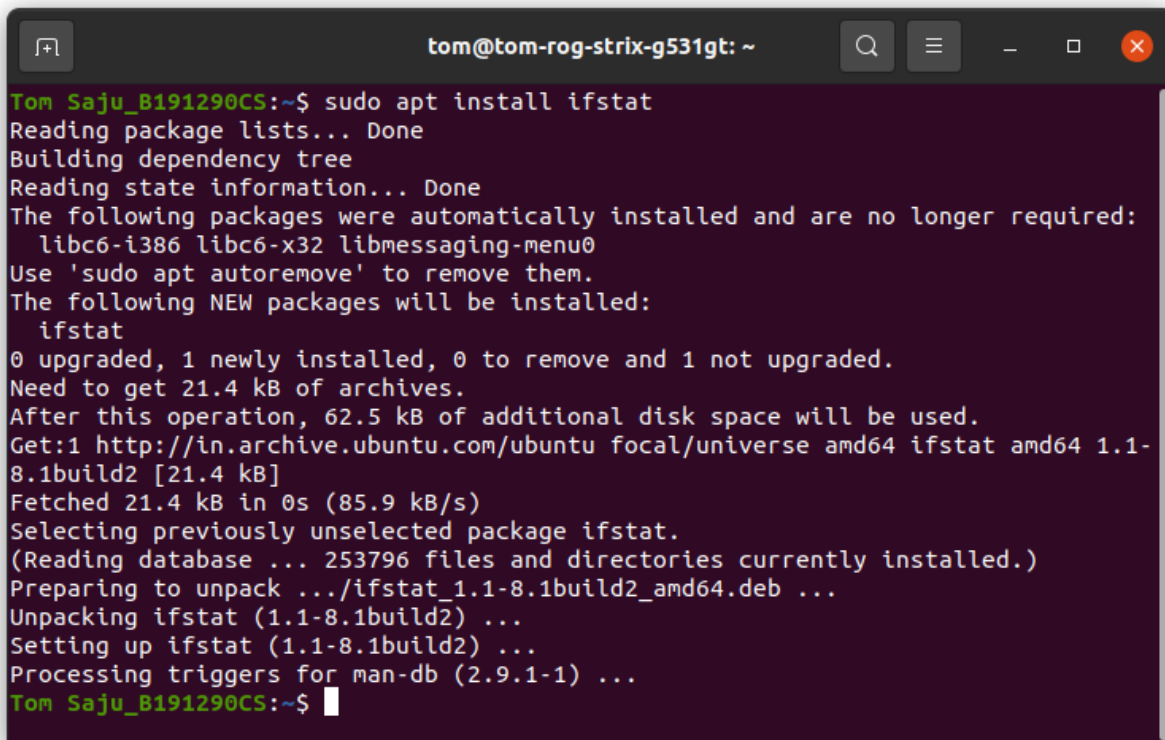
```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ dstat --list  
internal:  
aio,cpu,cpu-adv,cpu-use,cpu24,disk,disk24,disk24-old,epoch,  
fs,int,int24,io,ipc,load,lock,mem,mem-adv,net,page,page24,  
proc,raw,socket,swap,swap-old,sys,tcp,time,udp,unix,vm,  
vm-adv,zones  
/usr/share/dstat:  
battery,battery-remain,condor-queue,cpufreq,dbus,disk-avgqu,  
disk-avgrq,disk-svctm,disk-tps,disk-util,disk-wait,dstat,  
dstat-cpu,dstat-ctxt,dstat-mem,fan,freespace,fuse,gpfs,  
gpfs-ops,helloworld,ib,innodb-buffer,innodb-io,innodb-ops,  
jvm-full,jvm-vm,lustre,md-status,memcache-hits,mongodb-conn,  
mongodb-mem,mongodb-opcount,mongodb-queue,mongodb-stats,mysql-io,  
mysql-keys,mysql5-cmds,mysql5-conn,mysql5-innodb,  
mysql5-innodb-basic,mysql5-innodb-extra,mysql5-io,mysql5-keys,  
net-packets,nfs3,nfs3-ops,nfsd3,nfsd3-ops,nfsd4-ops,nfsstat4,  
ntp,postfix,power,proc-count,qmail,redis,rpc,rpcd,sendmail,  
snmp-cpu,snmp-load,snmp-mem,snmp-net,snmp-net-err,snmp-sys,  
snooze,squid,test,thermal,top-bio,top-bio-adv,top-childwait,  
top-cpu,top-cpu-adv,top-cputime,top-cputime-avg,top-int,top-io,  
top-io-adv,top-latency,top-latency-avg,top-mem,top-oom,utmp,  
vm-cpu,vm-mem,vm-mem-adv,vmk-hba,vmk-int,vmk-nic,vz-cpu,vz-io,  
vz-ubc,wifi,zfs-arc,zfs-l2arc,zfs-zil  
Tom Saju_B191290CS:~$
```

10. ifstat

As dstat, iostat, vmstat displays stats regarding the components of System. ifstat displays network interface statistics. This tool keeps records of the previous data files and displays differences between last and current calls.

Note: Install ifstat by command:

“sudo apt install ifstat”

A terminal window with a dark background and light text. The window title is 'tom@tom-rog-strix-g531gt: ~'. The user 'Tom Saju_B191290CS' is at the prompt. They enter the command 'sudo apt install ifstat'. The terminal shows the standard apt installation process: reading package lists, building a dependency tree, and reading state information. It lists packages that were automatically installed and are no longer required (libc6-i386, libc6-x32, libmessaging-menu0) and suggests using 'sudo apt autoremove' to remove them. It then shows the new packages to be installed: 'ifstat'. It reports that 0 packages are upgraded, 1 is newly installed, 0 are to be removed, and 1 is not upgraded. It shows the disk space requirements: 21.4 kB of archives and 62.5 kB of additional disk space. It then shows the download progress from the Ubuntu archive. Finally, it shows the unpacking and setting up of the ifstat package, and the processing of triggers for man-db. The prompt returns to the user.

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ sudo apt install ifstat  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  libc6-i386 libc6-x32 libmessaging-menu0  
Use 'sudo apt autoremove' to remove them.  
The following NEW packages will be installed:  
  ifstat  
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.  
Need to get 21.4 kB of archives.  
After this operation, 62.5 kB of additional disk space will be used.  
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 ifstat amd64 1.1-  
8.1build2 [21.4 kB]  
Fetched 21.4 kB in 0s (85.9 kB/s)  
Selecting previously unselected package ifstat.  
(Reading database ... 253796 files and directories currently installed.)  
Preparing to unpack .../ifstat_1.1-8.1build2_amd64.deb ...  
Unpacking ifstat (1.1-8.1build2) ...  
Setting up ifstat (1.1-8.1build2) ...  
Processing triggers for man-db (2.9.1-1) ...  
Tom Saju_B191290CS:~$
```

Example:

ifstat

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ ifstat  
eno2 wlo1  
KB/s in KB/s out KB/s in KB/s out  
0.00 0.00 0.06 0.00  
0.00 0.00 0.00 0.00  
0.00 0.00 0.00 0.00  
0.00 0.00 0.00 0.00  
0.00 0.00 0.00 0.00  
0.00 0.00 0.04 0.07  
0.00 0.00 0.00 0.00  
0.00 0.00 0.00 0.00  
0.00 0.00 0.00 0.00  
0.00 0.00 0.00 0.00  
0.00 0.00 0.06 0.00  
^C  
Tom Saju_B191290CS:~$
```

ifstat -t : To add timestamp to each entry

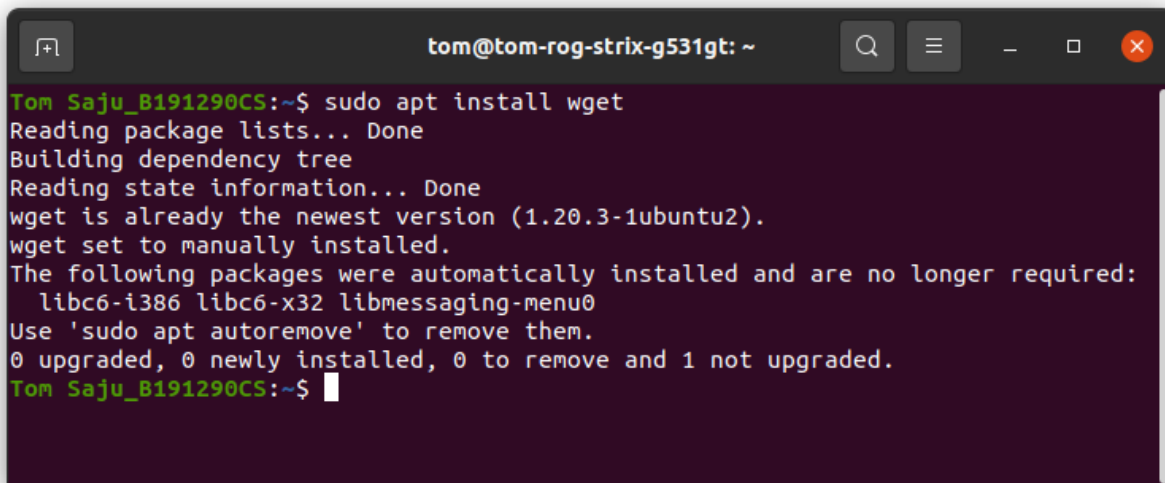
```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ ifstat -t  
Time eno2 wlo1  
HH:MM:SS KB/s in KB/s out KB/s in KB/s out  
20:19:33 0.00 0.00 0.00 0.00  
20:19:34 0.00 0.00 0.00 0.00  
20:19:35 0.00 0.00 0.00 0.00  
20:19:36 0.00 0.00 0.00 0.00  
20:19:37 0.00 0.00 0.00 0.00  
20:19:38 0.00 0.00 0.06 0.00  
20:19:39 0.00 0.00 0.00 0.00  
20:19:40 0.00 0.00 0.00 0.00  
20:19:41 0.00 0.00 0.00 0.00  
^C  
Tom Saju_B191290CS:~$
```

11. wget

wget is the non-interactive network downloader which is used to download files from the server even when the user has not logged on to the system and it can work in the background without hindering the current process. With wget, you can download files using HTTP, HTTPS, and FTP protocols. wget provides a number of options allowing you to download multiple files, resume downloads, limit the bandwidth, recursive downloads, download in the background, mirror a website, and much more.

Note: Install wget by the command:

“sudo apt install wget”

A terminal window with a dark purple background. The title bar shows 'tom@tom-roq-strix-g531gt: ~'. The prompt is 'Tom Saju_B191290CS:~\$'. The command 'sudo apt install wget' has been executed. The output shows that wget is already installed and is the newest version (1.20.3-1ubuntu2). It also lists packages that were automatically installed and are no longer required: libc6-i386, libc6-x32, and libmessaging-menu0. The prompt is now 'Tom Saju_B191290CS:~\$' with a cursor.

```
Tom Saju_B191290CS:~$ sudo apt install wget
Reading package lists... Done
Building dependency tree
Reading state information... Done
wget is already the newest version (1.20.3-1ubuntu2).
wget set to manually installed.
The following packages were automatically installed and are no longer required:
  libc6-i386 libc6-x32 libmessaging-menu0
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
Tom Saju_B191290CS:~$
```

Example:

wget [options] [url]	-
wget google.com	-

wget -b google.com	To download the file in background
wget google.com -o/path/filename.txt	To overwrite the log file of wget command.
wget -c google.com	To resume a partially downloaded file.

```

tom@tom-roq-strix-g531gt: ~
Tom Saju_B191290CS:~$ wget google.com
--2022-01-16 20:10:18-- http://google.com/
Resolving google.com (google.com)... 142.250.67.46, 2404:6800:4007:804::200e
Connecting to google.com (google.com)|142.250.67.46|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.google.com/ [following]
--2022-01-16 20:10:18-- http://www.google.com/
Resolving www.google.com (www.google.com)... 216.58.196.164, 2404:6800:4007:812:
:2004
Connecting to www.google.com (www.google.com)|216.58.196.164|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html          [ <=>          ] 16.06K  --.-KB/s   in 0.02s

2022-01-16 20:10:19 (790 KB/s) - 'index.html' saved [16441]

Tom Saju_B191290CS:~$ 

```

```
tom@tom-roq-strix-g531gt: ~  
Tom Saju_B191290CS:~$ wget google.com $HOME/google.txt  
--2022-01-16 20:13:17-- http://google.com/  
Resolving google.com (google.com)... 216.58.200.142, 2404:6800:4007:804::200e  
Connecting to google.com (google.com)|216.58.200.142|:80... connected.  
HTTP request sent, awaiting response... 301 Moved Permanently  
Location: http://www.google.com/ [following]  
--2022-01-16 20:13:17-- http://www.google.com/  
Resolving www.google.com (www.google.com)... 216.58.196.164, 2404:6800:4007:812:  
:2004  
Connecting to www.google.com (www.google.com)|216.58.196.164|:80... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: unspecified [text/html]  
Saving to: 'index.html'  
  
index.html          [ <=>          ] 16.04K  --.-KB/s    in 0.03s  
2022-01-16 20:13:17 (563 KB/s) - 'index.html' saved [16427]  
  
/home/tom/google.txt: Scheme missing.  
FINISHED --2022-01-16 20:13:17--  
Total wall clock time: 0.2s  
Downloaded: 1 files, 16K in 0.03s (563 KB/s)  
Tom Saju_B191290CS:~$
```

12. tracepath

tracepath command in Linux is used to traces path to destination discovering MTU along this path. It uses UDP port or some random port. It is similar to traceroute, but it does not require superuser privileges and has no fancy options. Tracepath 6 is a good replacement for traceroute 6 and classic example of the application of Linux error queues. The situation with IPv4 is worse because commercial IP routers do not return enough information in ICMP error messages.

Example:

tracepath www.google.com	-
tracepath -n google.com	Prints IP address numerically

tracert -b google.com

Prints both host name ip addresses

```
tom@tom-rog-strix-g531gt: ~  
Tom Saju_B191290CS:~$ tracert google.com  
1?: [LOCALHOST] pmtu 1500  
1: ??? 2.495ms  
1: ??? 111.973ms  
2: ??? 2.342ms pmtu 1452  
2: no reply  
3: no reply  
4: no reply  
5: no reply  
6: no reply  
^C  
Tom Saju_B191290CS:~$ tracert -n google.com  
1?: [LOCALHOST] pmtu 1500  
1: 192.168.1.1 108.667ms  
1: 192.168.1.1 3.639ms  
2: 192.168.1.1 1.745ms pmtu 1452  
2: no reply  
3: no reply  
^C  
Tom Saju_B191290CS:~$ tracert -b www.google.com  
1?: [LOCALHOST] pmtu 1500  
1: ??? (192.168.1.1) 119.284ms  
1: ??? (192.168.1.1) 7.106ms  
2: ??? (192.168.1.1) 4.835ms pmtu 1452  
2: no reply  
^C  
Tom Saju_B191290CS:~$
```

=====