--------Networking commands --------

While working on the internet , we may come across many problems. To overcome these problems We have some tools or we can say networking commands which can be used to sort out the issue and detect the issue.

Traceroute :-

This command is used to view the route using which you will be transmitted from Your computer to the said website. It is similar to PING except that is identifies the Pathway rather than time.

```
jitendra@PC:~$ traceroute google.com
traceroute to google.com (142.250.183.174), 30 hops max, 60 byte packets
 1  DESKTOP-ACUC1TV.mshome.net (192.168.176.1)  0.421 ms  0.903 ms  0.873 ms
 2  192.168.106.137 (192.168.106.137)  14.338 ms  17.027 ms  15.564 ms
 3  10.8.255.254 (10.8.255.254)  140.743 ms  140.733 ms  140.722 ms
 4  * * *
 5  10.174.171.81 (10.174.171.81)  73.090 ms  73.080 ms  73.070 ms
 6  * * *
 7  192.168.100.25 (192.168.100.25)  49.247 ms  58.473 ms  65.443 ms
 8  * * 192.168.100.66 (192.168.100.66)  84.960 ms
```

▪

--->Some organization set their system to not respond on traceroute command

--->some routers does not respond sometime due to overload

traceroute -I google.com > to use ICMP echo request instead of UDP packets.

traceroute -T google.com > This command will use TCP SYN (synchronize) packets instead

of UDP packets.

traceroute -p 80 google.com > this command will set the destination port number to 80.

traceroute -m 20 google.com > set the maximum number of hops

Nslookup :-

NSLookup (short for "Name Server Lookup") is a command-line tool used to query Domain Name System (DNS) servers to obtain DNS information, such as IP addresses, hostnames, and other DNS records. In general, the NSLookup command is used to troubleshoot DNS-related issues, verify DNS

configurations, and obtain information about DNS servers.

nslookup google.com

```
jitendra@PC:~$ nslookup facebook.com
Server:         192.168.176.1
Address:        192.168.176.1#53

Non-authoritative answer:
Name:   facebook.com
Address: 157.240.16.35
Name:   facebook.com
Address: 2a03:2880:f12f:83:face:b00c:0:25de
```

nslookup 157.240.16.35 > reverse lookup using ip address

```
jitendra@PC:~$ nslookup debug
Server:         192.168.176.1
Address:        192.168.176.1#53

** server can't find debug: NXDOMAIN
```

nslookup debug

Options:

-domain=[domain-name] → allows you to change the default DNS name.
-debug → enables the display of debugging information.
-port=[port-number] → Use the -port option to specify the port number for queries. By default, nslookup uses port 53 for DNS queries
-timeout=[seconds] → you can specify the time allowed for the DNS server to respond. By default, the timeout is set to a few seconds
-type=a → Lookup for a record. We can also view all the available DNS records for a particular record using the -type=a option
-type=any → Lookup for any record. We can also view all the available DNS records using the -type=any option.
-type=hinfo → displays hardware-related information about the host. It provides details about the operating system and hardware platform

-type=mx → Lookup for an mx record. MX (Mail Exchange) maps a domain name to a list of mail exchange servers for that domain. The MX record says that all the mails sent to “google.com” should be routed to the Mail server in that domain.
-type=ns → Lookup for an ns record. NS (Name Server) record maps a domain name to a list of DNS servers authoritative for that domain. It will output the name serves which are associated with the given domain.
-type=ptr → used in reverse DNS lookups. It retrieves the Pointer (PTR) records, which map IP addresses to domain names.
-type=soa → Lookup for a soa record. SOA record (start of authority), provides the authoritative information about the domain, the e-mail address of the domain admin, the domain serial number, etc…

ipconfig :-
This command is used to display detailed information about the network we are connected to. Ipconfig/all will display detailed information. Used in Windows

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

Syntax: ifconfig [options] [interface]

The interface argument specifies the network interface to configure or display. If no interface is specified, ifconfig displays information for all interfaces.

-a : This option is used to display all the interfaces available, even if they are down.
-s : To display short list instead of full details

up : This option is used to activate the driver for the given interface.
  Syntax:
ex:- ifconfig interface up

down : This option is used to deactivate the driver for the given interface.
Syntax:
ex:- ifconfig interface down

changing ip/netmask/broadcast address

ifconfig interface addresstype address

netstat :-
Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.
Options:
netstat -a/–all → Show both listening and non-listening sockets. With the –interfaces option, show interfaces that are not up
netstat -at → all tcp connection
netstat -au → all udp connection
netstat -l → all listnening states
netstat -lt → only tcp listening
netstat -s → statstics protocalwise
netstat -st → tcp
netstat -su → for udp
netstat -p → process id process name
netstat -n → numeric port
netstat -c → continuous statistic s
netstat -I → interface/ ifconfig command output
netstat -ie → extended interface
netstat -r → to print routing table
dig
The dig command (Domain Information Groper) is another powerful DNS querying tool that provides detailed information about DNS records and can help diagnose DNS-related issues.
For example:

dig example.com

Ping
Ping is short for Packet Internet Groper. This command is mainly used for checking the network connectivity among host/server and host. The ping command takes the URL or IP address as input and transfers the data packet to a specified address along with a "PING" message. Then, it will get a reply from the host/server. This time is known as "latency".
In Linux, the ping command is a general utility which is used for checking whether any network is present and if a host is attainable. We can test if the server is up and executing using this command. Also, it helps several connectivity issues with troubleshooting.

The ping command permits us to:

Test our Internet connection.
Check if the remote machine is active.
Analyze when there are network problems such as high latency or dropped packages.

Syntax: ping [options] hostname or IP address

For stopping the process, we can use the Ctrl+C keys.
Headers:

From → It tells the target and its IP address.
Important → The IP address might be different for any website depending on our geographical location.
ttl=52 → It tells the value, i.e., Time to Live from 1-255. Also, it indicates network number hops a packet could take before any router removes it.
icmp_seq=1 → It tells the all ICMP packet's sequence number. It increases by a single number for all subsequent echo requests.
time=7.68 ms → It tells the Time that it took any packet for reaching the target and come back to the origin. It expressed in ms (milliseconds).

If we find issues reaching a remote machine or a website, we can ping the localhost to ensure that we have a network connection. We can use anyone of the following ways for checking the interface of the local network:

ping 0: It is one of the quickest option to ping a localhost. The terminal will resolve determine the IP address and gives a response once we enter this command.
ping localhost: We can use the ping localhost name. This name will refer to our system and when we enter this command, we will say "ping this system".
ping 127.0.0.1: A few people prefer entering the IP address to ping the localhost.

Options
ping -4 hostname/IPv4
ping -6 hostname/IPv6
ping -i 0.5 → We use the values which are lower than 1 for decreased the ping time interval.
sudo ping -f hostname-IP → We can apply ping flood for testing the performance of our network under heavy load.
ping -s 1000 google.com → for increasing the size of the packet to 1000 bytes
ping -c 2 google.com → We can use the -c option and a number for automatically making the ping command stop after it transfers a possible number of packets
ping -w 25 google.com → We can include -w and a time interval in seconds to our command for stopping getting a ping result after a particular time. we can type the ping command for stopping printing ping outputs after 25 seconds
ping -c 10 -q youtube.com → The -q switch prints a single line along with the regular ping details and after that gives the statistics in the end. In this command, the "q" letter is short for the "quiet" result.

ping -D youtube.com → Include Timestamp Before Every Line in ping result. If we wish to remember the daytime when we run the ping command, we can add the -D switch

a- It produces a sound if the peer could be reached.

b- It permits ping the IP address of a broadcast.

B- It prevents the ping from changing the probe source address.

c- It limits the number of transferred ping requests.

d- It sets an option, i.e., SO-DEBUG over the used socket.

f- It floods the network by transferring several packets per second.

i- It describes the interval among the successive transmission of the packet. One second is the default value.

I- It sets the IP address of the source to the described IP address of the interface. This option is needed if pinging the lack address of IPv6 link. We can use the name of the device or IP address.

l- It specifies several packets to transfer without delaying a response.

q- It shows IP addresses in the output of the ping instead of hostnames.

T- It fixes the Time To Live.

v- It gives verbose output.

V- It shows the version of the ping and exits to a newer command prompt line.