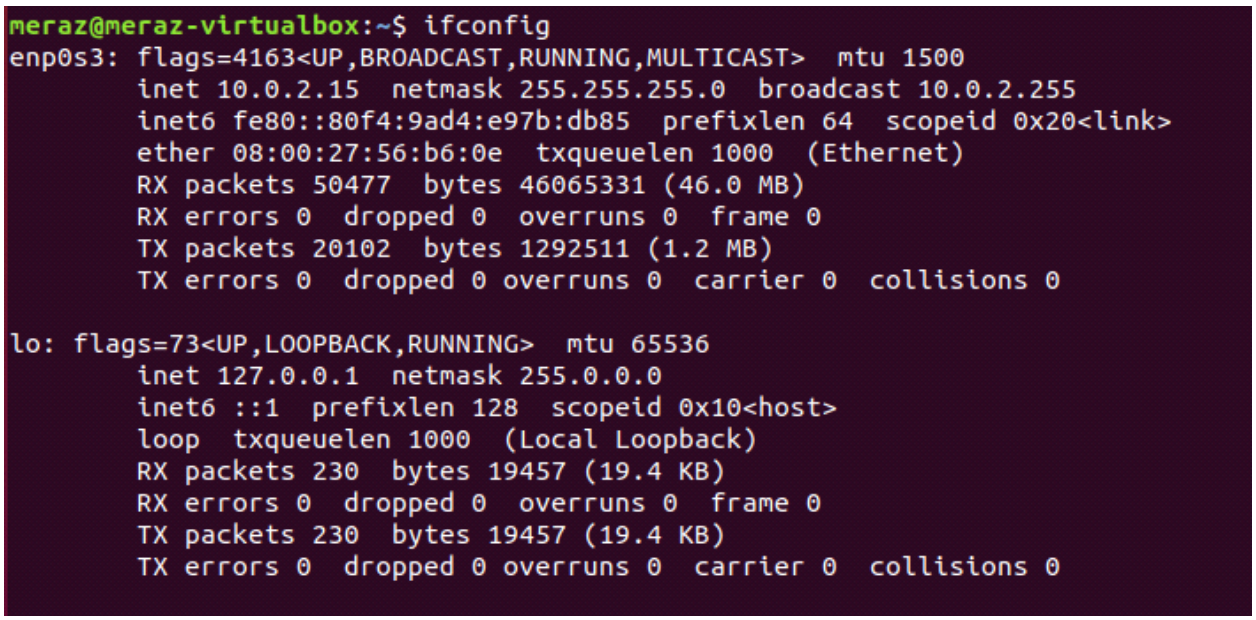
Linux Networking Commands

Ifconfig:



Linux ifconfig stands for interface configurator. It is one of the most basic commands used in network inspection.

ifconfig is used to initialize an interface, configure it with an IP address and enable or disable it. It is also used to display the route and the network interface.

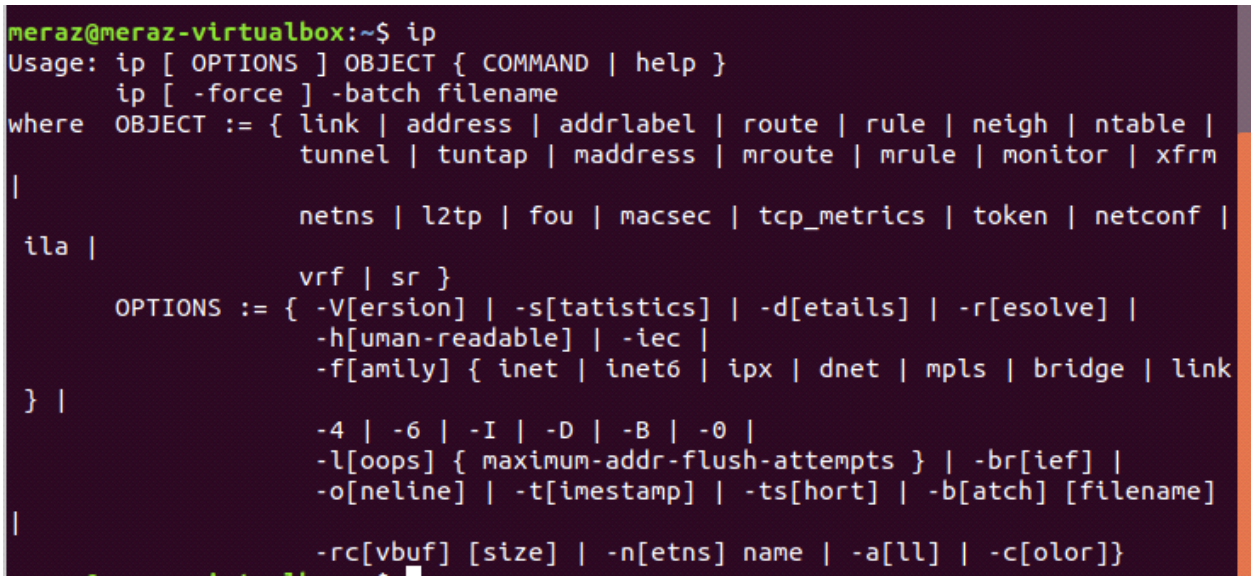
Basic information displayed upon using ifconfig are:

IP address

MAC address

MTU(Maximum Transmission Unit

IP:

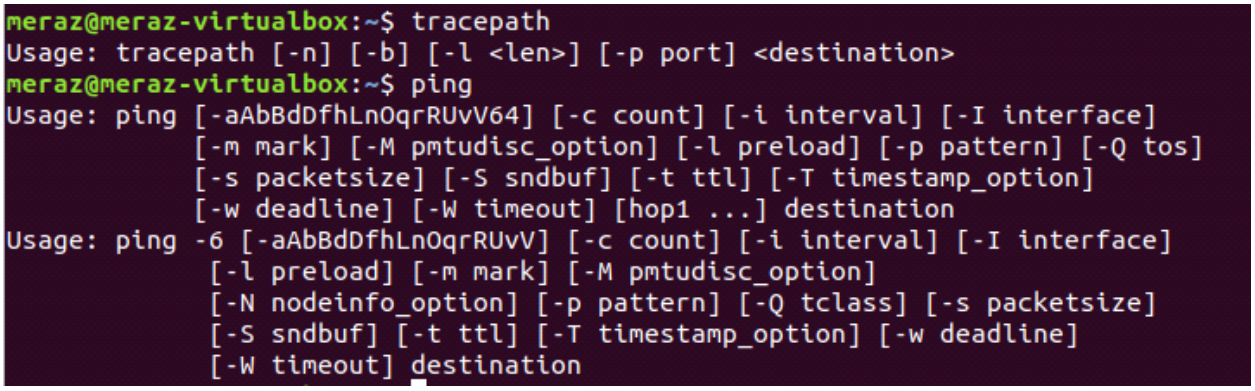


This is the latest and updated version of ifconfig command.

This command gives the details of all networks like ifconfig.

This command can also be used to get the details of a specific interface.

Ping:



Linux ping is one of the most used network troubleshooting commands. It basically checks for the network connectivity between two nodes.

ping stands for Packet INternet Groper.

The ping command sends the ICMP echo request to check the network connectivity.

It keeps executing until it is interrupted.

Netstat:

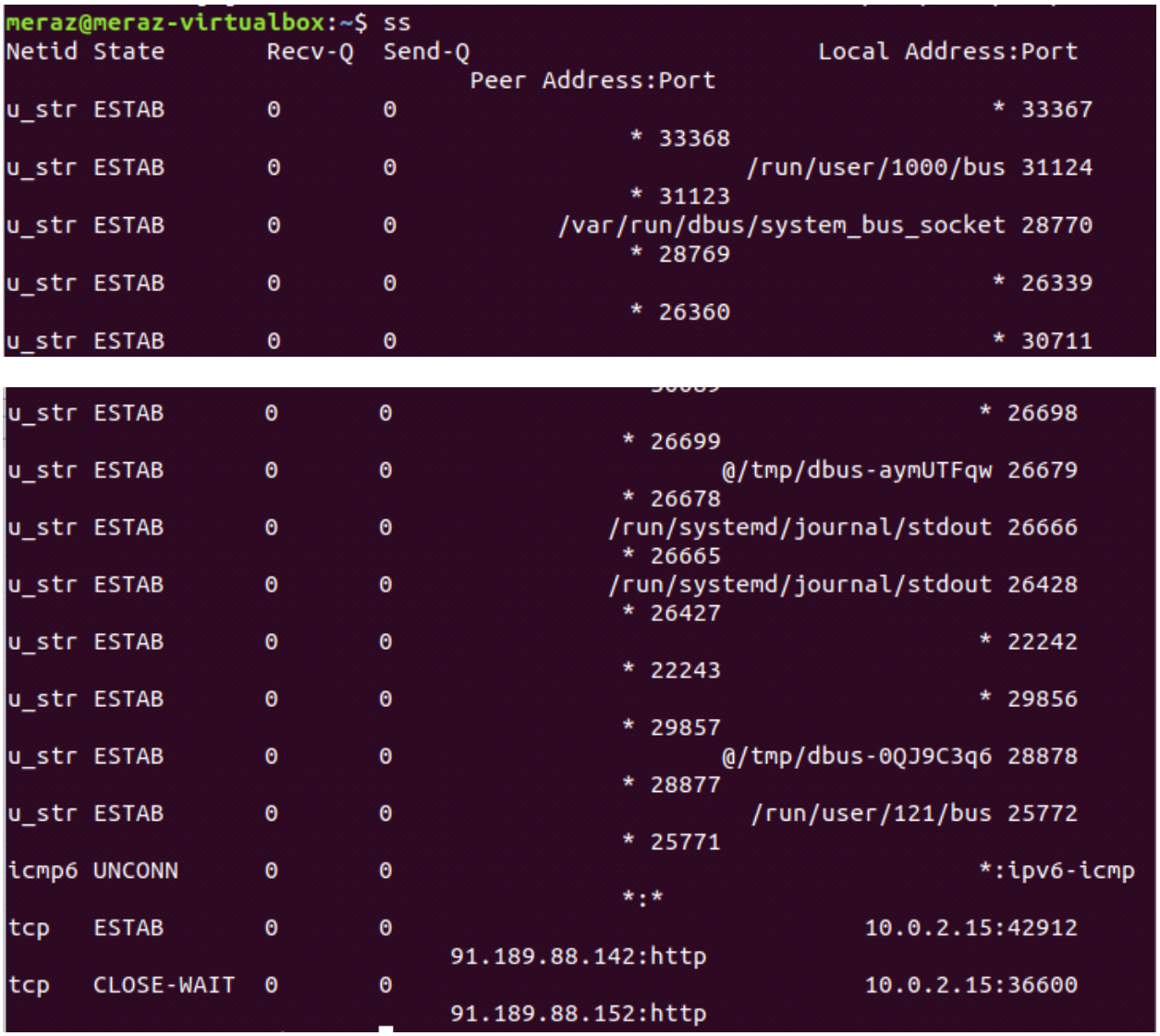
```
meraz@meraz-virtualbox:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 meraz-virtualbox:42912  aerodent.canonical:http ESTABLISHED
tcp        0      0 meraz-virtualbox:36600  actiontoad.canonic:http CLOSE_WAIT
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    27905    /run/user/1000/system
d/notify
unix  2      [ ]         DGRAM                    23974    /run/user/121/systemd
/notify
unix  3      [ ]         DGRAM                    12753    /run/systemd/notify
unix  2      [ ]         DGRAM                    12766    /run/systemd/journal/
syslog
unix  24     [ ]         DGRAM                    12768    /run/systemd/journal/
dev-log
unix  10     [ ]         DGRAM                    12782    /run/systemd/journal/
socket
unix  3      [ ]         STREAM     CONNECTED     33367
unix  3      [ ]         STREAM     CONNECTED     31124    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     28770    /var/run/dbus/system_
bus_socket
```

```
bus_socket
unix  3      [ ]         STREAM     CONNECTED     28856
unix  3      [ ]         STREAM     CONNECTED     31209    @/dbus-vfs-daemon/soc
ket-1LprMZOL
unix  3      [ ]         STREAM     CONNECTED     30090    @/tmp/.X11-unix/X0
unix  3      [ ]         STREAM     CONNECTED     26698
unix  3      [ ]         STREAM     CONNECTED     26679    @/tmp/dbus-aymUTFqw
unix  3      [ ]         STREAM     CONNECTED     26666    /run/systemd/journal/
stdout
unix  3      [ ]         STREAM     CONNECTED     26428    /run/systemd/journal/
stdout
unix  3      [ ]         STREAM     CONNECTED     22242
unix  3      [ ]         STREAM     CONNECTED     29856
unix  3      [ ]         STREAM     CONNECTED     28878    @/tmp/dbus-0QJ9C3q6
unix  3      [ ]         STREAM     CONNECTED     25772    /run/user/121/bus
```

Linux netstat command refers to the network statistics.

It provides statistical figures about different interfaces which includes open sockets, routing tables and connection information.

SS:



Linux ss command is the replacement for netstat command. It is regarded as a much faster and more informative command than netstat.

The faster response of ss is possible as it fetches all the information from within the kernel userspace.

Dig:

```
meraz@meraz-virtualbox:~$ dig

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9408
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       504331  IN      NS      c.root-servers.net.
.                       504331  IN      NS      h.root-servers.net.
.                       504331  IN      NS      k.root-servers.net.
.                       504331  IN      NS      m.root-servers.net.
.                       504331  IN      NS      i.root-servers.net.
.                       504331  IN      NS      e.root-servers.net.
```

```
;; Query time: 48 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Sun Nov 22 10:01:59 +06 2020
;; MSG SIZE  rcvd: 239
```

Linux dig command stands for Domain Information Groper. This command is used in DNS lookup to query DNS name server. It is also used to troubleshoot DNS related issues.

It is mainly used to verify DNS mappings, MX Records, host addresses and all other DNS records for a better understanding of the DNS topography.

This command is an improvised version of nslookup command.

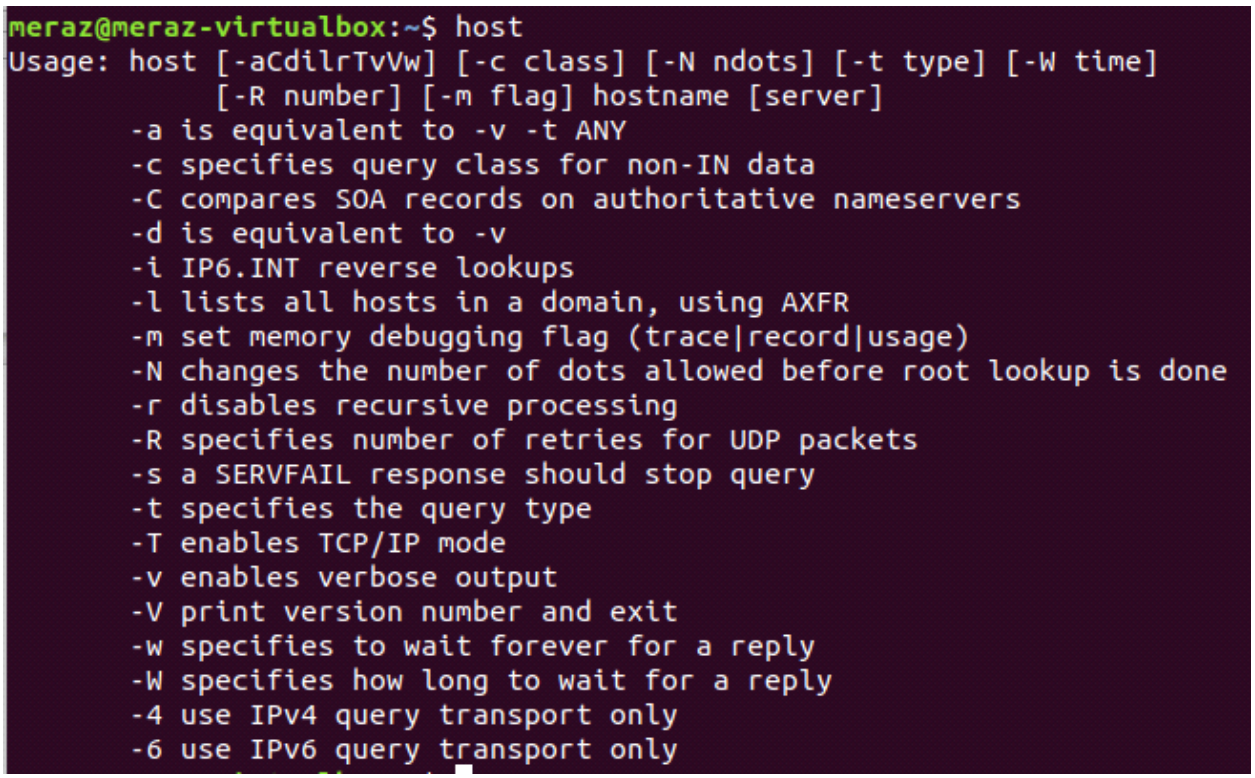
Route:

```
meraz@meraz-virtualbox:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
```

Linux route command displays and manipulates the routing table existing for your system.

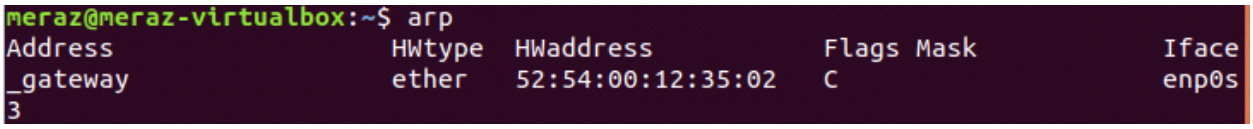
A router is basically used to find the best way to send the packets across to a destination.

Host:



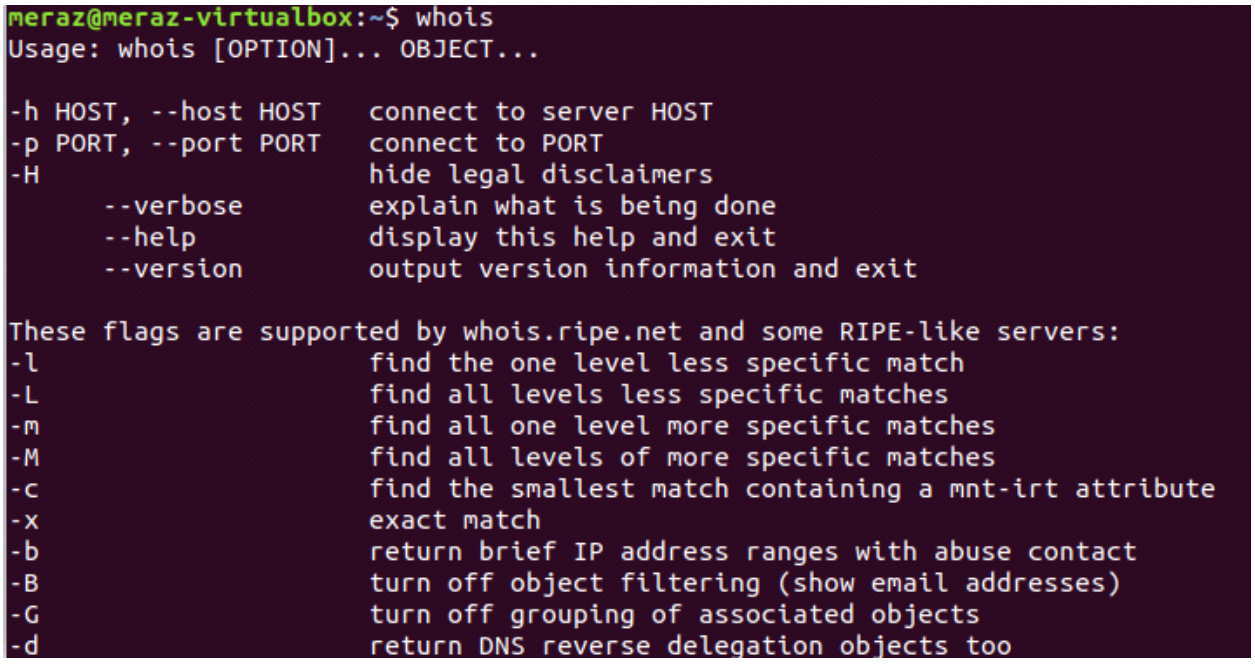
Linux host command displays the domain name for a given IP address and IP address for a given hostname. It is also used to fetch DNS lookup for DNS related query.

ARP:



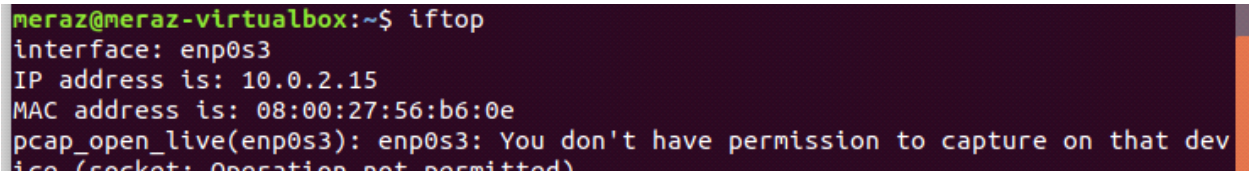
Linux arp command stands for Address Resolution Protocol. It is used to view and add content to kernel's ARP table. All the systems maintain a table of IP addresses and their corresponding MAC addresses. This table is called the ARP Lookup table. When a destination is requested to connect through IP address, your router will check for the MAC address in this table. If it is cached, the table will not be used.

Whois:



Linux whois command is used to fetch all the information related to a website. You can get all the information about a website including the registration and the owner information.

Iftop:



Linux iftop command is used in traffic monitoring.

Use the following command to download iftop on your system.