

# Linux Networking Commands

## Ifconfig:

```
meraz@meraz-virtualbox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::80f4:9ad4:e97b:db85 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:56:b6:0e txqueuelen 1000 (Ethernet)
    RX packets 50477 bytes 46065331 (46.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20102 bytes 1292511 (1.2 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 230 bytes 19457 (19.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 230 bytes 19457 (19.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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:**

```

meraz@meraz-virtualbox:~$ ip
Usage: ip [ OPTIONS ] OBJECT { COMMAND | help }
       ip [ -force ] -batch filename
where  OBJECT := { link | address | addrlabel | route | rule | neigh | ntable |
                  tunnel | tuntap | maddress | mroute | mrule | monitor | xfrm
                  |
                  netns | l2tp | fou | macsec | tcp_metrics | token | netconf |
                  ila |
                  vrf | sr }
       OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] | -r[esolve] |
                   -h[uman-readable] | -iec |
                   -f[amily] { inet | inet6 | ipx | dnet | mpls | bridge | link
                   |
                   -4 | -6 | -I | -D | -B | -O |
                   -l[oops] { maximum-addr-flush-attempts } | -br[ief] |
                   -o[neline] | -t[imestamp] | -ts[hort] | -b[atch] [filename]
                   |
                   -rc[vbuf] [size] | -n[etns] name | -a[ll] | -c[olor]}

```

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:

```

meraz@meraz-virtualbox:~$ tracepath
Usage: tracepath [-n] [-b] [-l <len>] [-p port] <destination>
meraz@meraz-virtualbox:~$ ping
Usage: ping [-aAbBdDfhLnOqrRUvV64] [-c count] [-i interval] [-I interface]
          [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
          [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
          [-w deadline] [-W timeout] [hop1 ...] destination
Usage: ping -6 [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
          [-l preload] [-m mark] [-M pmtudisc_option]
          [-N nodeinfo_option] [-p pattern] [-Q tclass] [-s packetsize]
          [-S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline]
          [-W timeout] destination

```

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/systemd/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

unix    3      [ ]         STREAM        CONNECTED        28856
unix    3      [ ]         STREAM        CONNECTED        31209    @/dbus-vfs-daemon/socket-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:

```

meraz@meraz-virtualbox:~$ ss
Netid State      Recv-Q Send-Q           Peer Address:Port          Local Address:Port
u_str  ESTAB        0      0                * 33367
u_str  ESTAB        0      0                * 33368
u_str  ESTAB        0      0                * 31123
u_str  ESTAB        0      0                * 28769
u_str  ESTAB        0      0                * 26339
u_str  ESTAB        0      0                * 26360
u_str  ESTAB        0      0                * 30711
u_str  ESTAB        0      0                * 26698
u_str  ESTAB        0      0                * 26699
u_str  ESTAB        0      0                * 26678
u_str  ESTAB        0      0                * 26665
u_str  ESTAB        0      0                * 26427
u_str  ESTAB        0      0                * 22242
u_str  ESTAB        0      0                * 22243
u_str  ESTAB        0      0                * 29856
u_str  ESTAB        0      0                * 29857
u_str  ESTAB        0      0                * 28877
u_str  ESTAB        0      0                * 25771
icmp6  UNCONN       0      0                *:*
tcp    ESTAB        0      0                *:*
tcp    CLOSE-WAIT   0      0                *:*

```

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:

```
meraz@meraz-virtualbox:~$ host
Usage: host [-aCdilrTvVw] [-c class] [-N ndots] [-t type] [-W time]
          [-R number] [-m flag] hostname [server]
  -a is equivalent to -v -t ANY
  -c specifies query class for non-IN data
  -C compares SOA records on authoritative nameservers
  -d is equivalent to -v
  -i IP6.INT reverse lookups
  -l lists all hosts in a domain, using AXFR
  -m set memory debugging flag (trace|record|usage)
  -N changes the number of dots allowed before root lookup is done
  -r disables recursive processing
  -R specifies number of retries for UDP packets
  -s a SERVFAIL response should stop query
  -t specifies the query type
  -T enables TCP/IP mode
  -v enables verbose output
  -V print version number and exit
  -w specifies to wait forever for a reply
  -W specifies how long to wait for a reply
  -4 use IPv4 query transport only
  -6 use IPv6 query transport only
```

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:

```
meraz@meraz-virtualbox:~$ arp
Address          HWtype  HWaddress      Flags Mask    Iface
_gateway        ether    52:54:00:12:35:02  C             enp0s3
```

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:

```
meraz@meraz-virtualbox:~$ whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST    connect to server HOST
-p PORT, --port PORT    connect to PORT
-H                      hide legal disclaimers
    --verbose           explain what is being done
    --help              display this help and exit
    --version           output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                      find the one level less specific match
-L                      find all levels less specific matches
-m                      find all one level more specific matches
-M                      find all levels of more specific matches
-c                      find the smallest match containing a mnt-irt attribute
-x                      exact match
-b                      return brief IP address ranges with abuse contact
-B                      turn off object filtering (show email addresses)
-G                      turn off grouping of associated objects
-d                      return DNS reverse delegation objects too
```

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:

```
meraz@meraz-virtualbox:~$ iftop
interface: enp0s3
IP address is: 10.0.2.15
MAC address is: 08:00:27:56:b6:0e
pcap_open_live(enp0s3): enp0s3: You don't have permission to capture on that dev
ice (socket: Operation not permitted)
```

Linux iftop command is used in traffic monitoring.

Use the following command to download iftop on your system.

