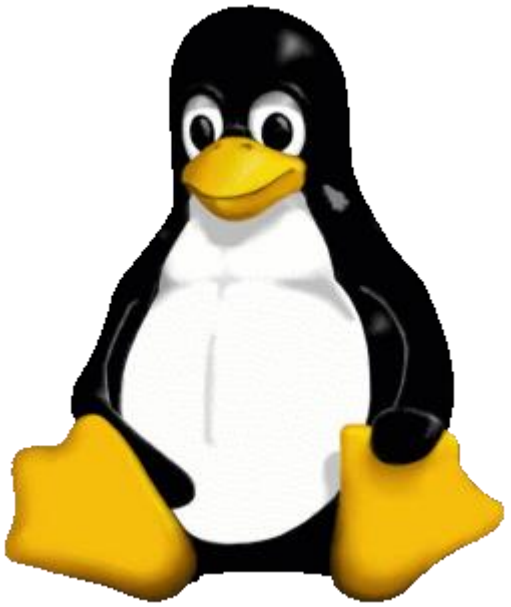
GNU/Linux

By Dr. Amir



IP

To quickly identify all available Ethernet interfaces, you can use the *ip* command as shown below.

```
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 6
    link/loopback 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_
    inet6 ::1/128 scope host
       valid_lft forever preferred_
2: enp0s25: <BROADCAST,MULTICAST,UP
    link/ether 00:16:3e:e2:52:42 br
    inet 10.102.66.200/24 brd 10.10
       valid_lft 3257sec preferred_
    inet6 fe80::216:3eff:fee2:5242/
       valid_lft forever preferred_
```

Assigning static ip with ip command

```
/sbin/ip link   # show list of network interfaces
/sbin/ip addr add 192.168.10.12/255.255.255.0 broadcast 192.168.10.255 dev eth0
/sbin/ip addr show
```

Ip route

Use the IP route to print or display the routing table. The following command displays the contents of the routing table:

```
$ ip route show
default via 10.0.2.2 dev enp0s3
10.0.0.0/24 dev enp0s8  proto kernel  scope link  src 10.0.0.51
10.0.2.0/24 dev enp0s3  proto kernel  scope link  src 10.0.2.15
```

nmap

Nmap (“Network Mapper”) is a powerful utility used for network discovery, security auditing, and administration.

Many system admins use it to determine which of their systems are online, and also for OS detection and service detection.

```
$ nmap 10.0.0.50

Starting Nmap 7.01 ( https://nmap.org ) at 2020-09-07 10:32 UTC
Nmap scan report for 10.0.0.50
Host is up (0.00077s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
3306/tcp closed mysql
```

Nmap … -O

Use -O flag to identify which operating system a host is running.

```
$ sudo  nmap 10.0.0.50 -O
Starting Nmap 7.01 ( https://nmap.org ) at 2020-09-07 13:44 UTC
Nmap scan report for 10.0.0.50
Host is up (0.00053s latency).
...
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.10 - 3.19
Network Distance: 1 hop
OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.95 seconds
```

ping

Use ping to see if a host is alive. This super simple command helps you check the status of a host or a network segment. Ping command sends an ICMP ECHO_REQUEST packet to the target host and waits to see if it replies.

```
$ ping -c 3 google.com
PING google.com (172.217.167.238): 56 data bytes
64 bytes from 172.217.167.238: icmp_seq=0 ttl=118 time=7.898 ms
64 bytes from 172.217.167.238: icmp_seq=1 ttl=118 time=7.960 ms
64 bytes from 172.217.167.238: icmp_seq=2 ttl=118 time=6.247 ms

--- google.com ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 6.247/7.368/7.960/0.793 ms
```

SS

use ss command with -t and -a flags to list all TCP sockets. This displays both listening and non-listening sockets.

```
$ ss -t -a
State      Recv-Q Send-Q        Local Address:Port          Peer Address:Port
LISTEN     0      128               *:sunrpc                   *:*
LISTEN     0      128               *:http                     *:*
LISTEN     0      128               *:ssh                      *:*
LISTEN     0      128               *:60031                    *:*
ESTAB      0      0          10.0.2.15:ssh              10.0.2.2:51699
ESTAB      0      0          10.0.2.15:ssh              10.0.2.2:51049
LISTEN     0      128            :::sunrpc                  :::*
LISTEN     0      128            :::http                    :::*
LISTEN     0      128            :::ssh                     :::*
LISTEN     0      128            :::54715                   :::*
```

Assigning static ip with ifconfig command

```
/sbin/ifconfig -a   # show list of network interfaces even if down
/sbin/ifconfig eth0 192.168.10.12 netmask 255.255.255.0 broadcast 192.168.10.255
/sbin/ifconfig      # no arguments defaults to showing the current IP configuration
```

lshw

This command provides greater details around the hardware capabilities of specific adapters.

```
[sudo] password for amir:
  *-network
       description: Wireless interface
       product: Wireless 8265 / 8275
       vendor: Intel Corporation
       physical id: 0
       bus info: pci@0000:02:00.0
       logical name: wlp2s0
       version: 78
       serial: 7c:11:cb:49:8f:4d
       width: 64 bits
       clock: 33MHz
       capabilities: pm msi pciexpress
eless
       configuration: broadcast=yes dri
ic firmware=34.0.1 ip=192.168.43.187 la
EEE 802.11
       resources: irq:131 memory:a10000
amir@huawei-matebook-x:~$
```