Ifconfig -> ifconfig (short for **interface configuration**) is a legacy command used in Linux and Unix systems to **view and configure network interfaces**.

ip a -> ip a (short for ip address) is a modern Linux command used to display all network interfaces and their IP address configurations**.**

```
snir1551@snir1551-VirtualBox:~/Desktop$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.127  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 2a00:a041:2d5e:9100:c8b0:9c7b:8206:dca9  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fecf:f4eb  prefixlen 64  scopeid 0x20<link>
        inet6 2a00:a041:2d5e:9100:a00:27ff:fecf:f4eb  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:cf:f4:eb  txqueuelen 1000  (Ethernet)
        RX packets 3442  bytes 2040078 (2.0 MB)
        RX errors 0  dropped 6  overruns 0  frame 0
        TX packets 725  bytes 84983 (84.9 KB)
        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 278  bytes 25273 (25.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 278  bytes 25273 (25.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
snir1551@snir1551-VirtualBox:~/Desktop$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cf:f4:eb brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.127/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
       valid_lft 2279sec preferred_lft 2279sec
    inet6 2a00:a041:2d5e:9100:c8b0:9c7b:8206:dca9/64 scope global temporary dynamic
       valid_lft 86389sec preferred_lft 43189sec
    inet6 2a00:a041:2d5e:9100:a00:27ff:fecf:f4eb/64 scope global dynamic mngtmpaddr
       valid_lft 86389sec preferred_lft 43189sec
    inet6 fe80::a00:27ff:fecf:f4eb/64 scope link
       valid_lft forever preferred_lft forever
```

- Show all network interfaces (including lo, eth0, wlan0, etc.)
- Display assigned IPv4 and IPv6 addresses
- Show interface status (UP/DOWN), MAC address, and other details

netstat -tuln -> used to **list all active listening network ports** on a Linux system **without resolving hostnames or service names**.

ss -tuln -> a **modern, fast, and powerful tool** to display **listening network sockets** on a Linux system

```
snir1551@snir1551-VirtualBox:~/Desktop$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:631                 :::*                    LISTEN
udp        0      0 0.0.0.0:46773           0.0.0.0:*
udp        0      0 127.0.0.54:53           0.0.0.0:*
udp        0      0 127.0.0.53:53           0.0.0.0:*
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp6       0      0 :::5353                 :::*
udp6       0      0 :::56251                :::*
snir1551@snir1551-VirtualBox:~/Desktop$ ss -tuln
Netid      State       Recv-Q      Send-Q           Local Address:Port             Peer Address:Port      Process
udp        UNCONN      0           0                      0.0.0.0:46773                 0.0.0.0:*
udp        UNCONN      0           0                   127.0.0.54:53                    0.0.0.0:*
udp        UNCONN      0           0                127.0.0.53%lo:53                    0.0.0.0:*
udp        UNCONN      0           0                      0.0.0.0:5353                  0.0.0.0:*
udp        UNCONN      0           0                         [::]:5353                     [::]:*
udp        UNCONN      0           0                         [::]:56251                    [::]:*
tcp        LISTEN      0           4096                 127.0.0.1:631                   0.0.0.0:*
tcp        LISTEN      0           4096             127.0.0.53%lo:53                    0.0.0.0:*
tcp        LISTEN      0           4096                127.0.0.54:53                    0.0.0.0:*
tcp        LISTEN      0           4096                        *:22                          *:*
tcp        LISTEN      0           4096                    [::1]:631                     [::]:*
snir1551@snir1551-VirtualBox:~/Desktop$
```

`*:22` → SSH service (open to all IPv4 addresses)

- This means that the SSH service is listening on port 22
- on all available IPv4 network interfaces.
- It is accessible both from the local machine and from remote devices on the network.
- The asterisk `*` means "any IP address" (i.e., 0.0.0.0)

SSH (Secure Shell) is a network protocol that allows secure remote access to another computer over an unsecured network.

Example: ssh username@192.168.1.10

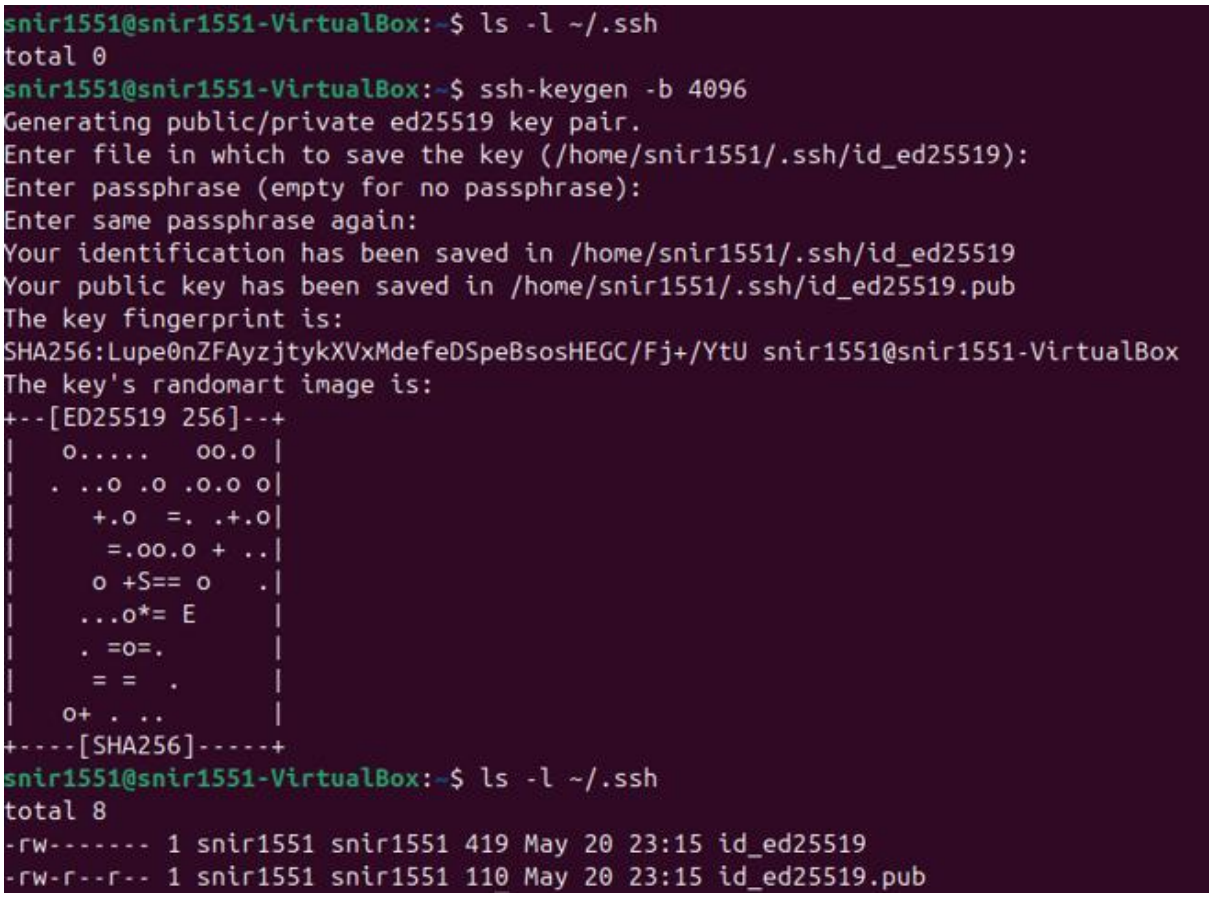
This connects your machine to another device on your network with IP `192.168.1.127` using SSH.

127.0.0.1:22 ->

- This means that the SSH service is listening on port 22
- but only on the local loopback interface (localhost).
- It is accessible only from the same machine and not from remote devices.

Based on the output of `netstat -tuln` and `ss -tuln`, the following ports are open (i.e., in `LISTEN` or `UNCONN` state):

ssh-keygen -b 4096 -> Generate a Secure SSH Key Pair



ssh-keygen -b 4096

- This command generates a new **SSH key pair** (private and public keys) with a **4096-bit key size** for secure authentication with remote servers.
- `ssh-keygen`: The command-line tool used to create, manage, and convert authentication keys for SSH.
- `-b 4096`: Specifies the number of bits in the key. `4096` means a **stronger and more secure key** than the default (which is usually `2048`).

By default, this creates two files:

- `~/.ssh/id_rsa` – the **private key** (keep it secret!)
- `~/.ssh/id_rsa.pub` – the **public key** (can be shared with servers)

```
snir1551@snir1551-VirtualBox:~$ ssh snir1551@192.168.1.127
The authenticity of host '192.168.1.127 (192.168.1.127)' can't be established.
ED25519 key fingerprint is SHA256:GxOBRFc14asX2etnmLztNMuCPpHWnslbq2hGS33SvMc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.127' (ED25519) to the list of known hosts.
snir1551@192.168.1.127's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Mon May 19 19:45:01 2025 from 192.168.1.10
```

1. If SSH is not installed (rare, but possible), install it with: sudo apt install openssh-server
2. Start the SSH service on your VM: sudo systemctl start ssh
3. sudo systemctl status ssh

ssh snir1551@192.168.1.127: This command initiates a **secure SSH connection** to a remote machine with the IP address `192.168.1.127`,
using the **username** `snir1551`.

- ssh – The command to start an SSH (Secure Shell) connection.
- snir1551 – The username on the remote machine.
- 192.168.1.127 – The IP address of the remote machine.

After you enter the password and connect to the machine,
to exit from it, press **Ctrl + D**.

```
snir1551@snir1551-VirtualBox:~$ ls -l ~/.ssh
total 16
-rw------- 1 snir1551 snir1551 419 May 20 23:15 id_ed25519
-rw-r--r-- 1 snir1551 snir1551 110 May 20 23:15 id_ed25519.pub
-rw------- 1 snir1551 snir1551 978 May 20 23:18 known_hosts
-rw-r--r-- 1 snir1551 snir1551 142 May 20 23:18 known_hosts.old
```

`known_hosts` file:

- The `~/.ssh/known_hosts` file stores the public fingerprints (host keys) of remote servers you have connected to via SSH.

Purpose of this file:

- It helps verify the identity of a server during SSH connection.
  When you connect to a server for the first time, its key is added to this file.
  On future connections, SSH checks if the server's key matches the one stored — ensuring you're talking to the same server.

ssh-copy-id user@remote_host

```
snir1551@snir1551-VirtualBox:~/.ssh$ ssh-copy-id snir1551@192.168.1.127
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
snir1551@192.168.1.127's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'snir1551@192.168.1.127'"
and check to make sure that only the key(s) you wanted were added.

snir1551@snir1551-VirtualBox:~/.ssh$ ls -l
total 20
-rw------- 1 snir1551 snir1551 110 May 20 23:40 authorized_keys
-rw------- 1 snir1551 snir1551 419 May 20 23:15 id_ed25519
-rw-r--r-- 1 snir1551 snir1551 110 May 20 23:15 id_ed25519.pub
-rw------- 1 snir1551 snir1551 978 May 20 23:18 known_hosts
-rw-r--r-- 1 snir1551 snir1551 142 May 20 23:18 known_hosts.old
```

ssh-copy-id

- ssh-copy-id copies your public SSH key to the remote server's authorized_keys file, so that you can log in without a password in the future (using SSH key authentication).
- `user` – The username on the remote machine.
- `remote_host` – The IP address or hostname of the remote machine.

```
snir1551@snir1551-VirtualBox:~/.ssh$ ssh snir1551@192.168.1.127
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Tue May 20 23:31:11 2025 from 192.168.1.10
```

without needing to enter a password.

```
snir [ ~ ]$ echo "Hello from my computer! $(whoami)" > myfile.txt
snir [ ~ ]$ ls
clouddrive  Linux-VM01_key.pem  myfile.txt
snir [ ~ ]$ cat myfile.txt
Hello from my computer! snir
snir [ ~ ]$ scp -i Linux-VM01_key.pem myfile.txt snir1551@20.217.201.167:/home/snir1551/
myfile.txt
snir [ ~ ]$
```

```
snir1551@Linux-VM01:~$ ls -l
total 4
-rw-r--r-- 1 snir1551 snir1551 29 May 21 08:03 myfile.txt
snir1551@Linux-VM01:~$ cat myfile.txt
Hello from my computer! snir
snir1551@Linux-VM01:~$
logout
Connection to 20.217.201.167 closed.
```

```
snir [ ~ ]$ mkdir newFolder
snir [ ~ ]$ scp -i Linux-VM01_key.pem snir1551@20.217.201.167:/home/snir1551/myfile.txt ~/newFolder/myfile_copy.txt
myfile.txt
snir [ ~ ]$ ls -l ~/newFolder
total 4
-rw-r--r-- 1 snir snir 29 May 21 08:13 myfile_copy.txt
snir [ ~ ]$ cat ~/newFolder/myfile_copy.txt
Hello from my computer! snir
snir [ ~ ]$
```