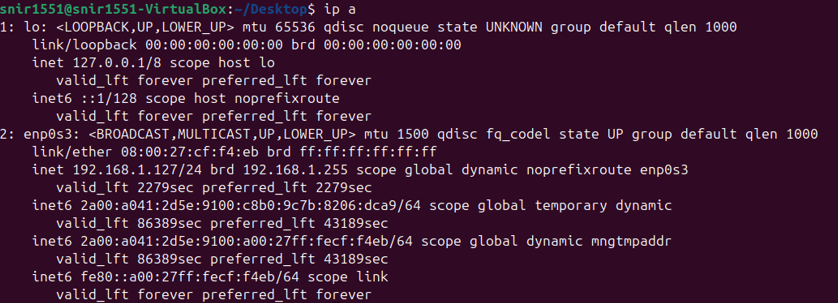


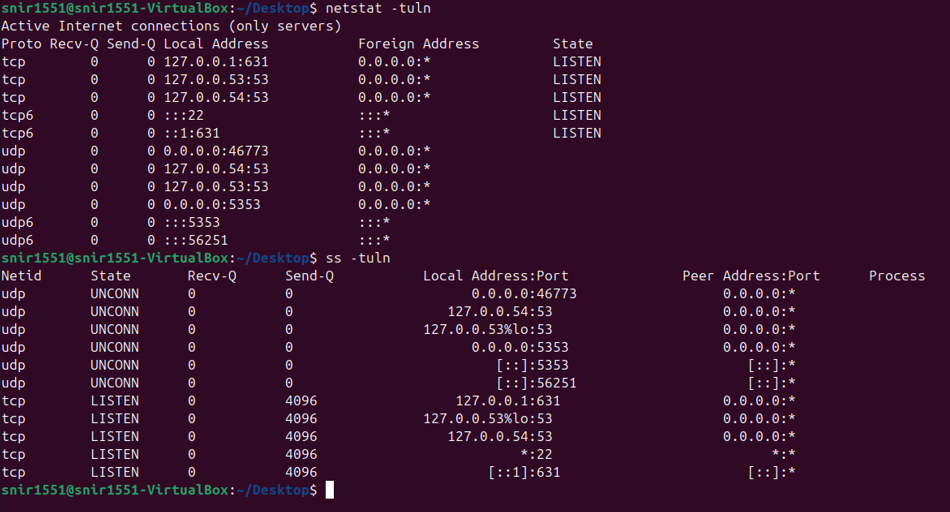
Ifconfig -> ifconfig (short for **interface configuration**) is a legacy command used in Linux and Unix systems to **view and configure network interfaces**.

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

It’s part of the iproute2 suite and replaces the older ifconfig command.



* 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 — similar to netstat -tuln, but more efficient.

\*: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.

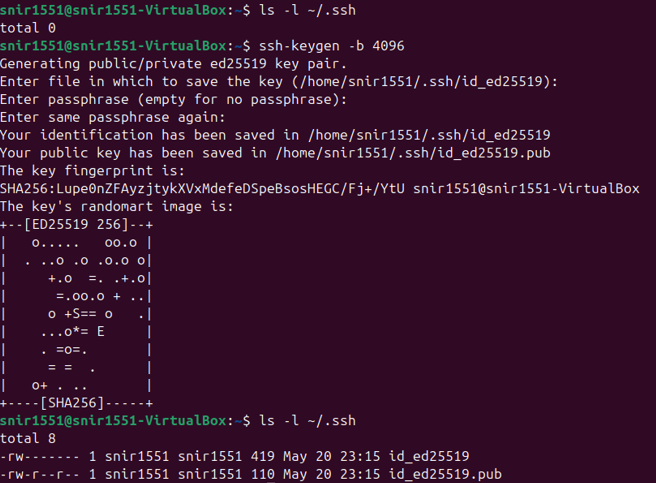
Example: ssh username@192.168.1.10

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):



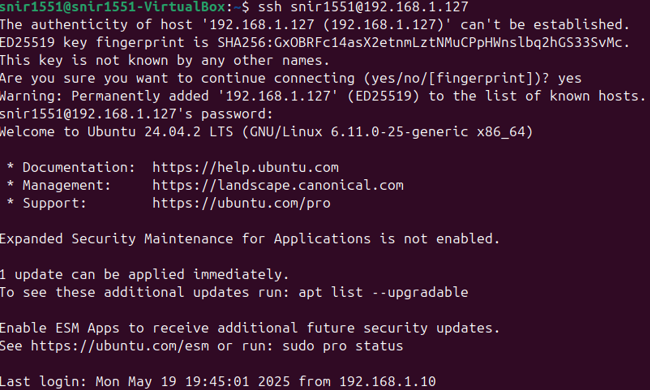
ssh-keygen -b 4096 -> Generate a Secure SSH Key Pair

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)

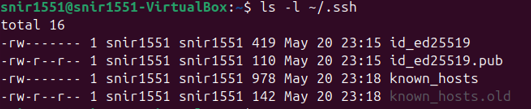


1. If SSH is not installed (rare, but possible), install it with: sudo apt install openssh-server
2. Start the SSH service on your VM: sudo systemctl start ssh
3. sudo systemctl status ssh

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**.

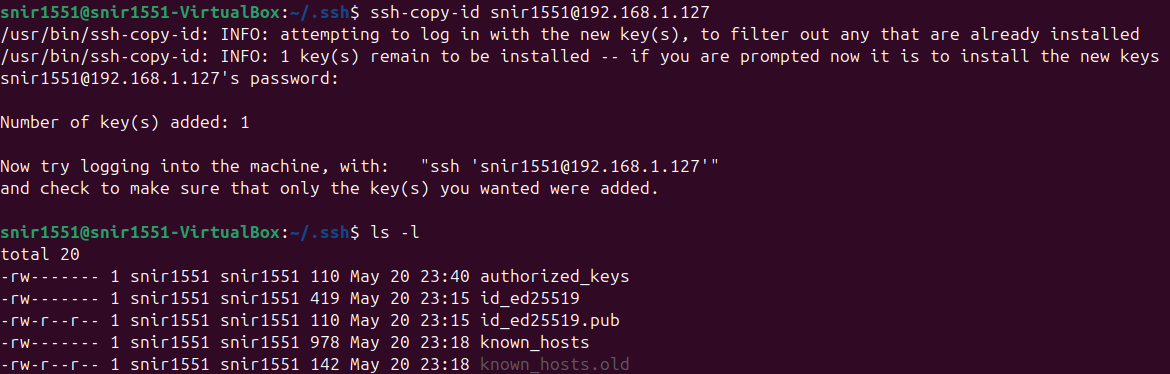


known\_hosts file:

* 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.



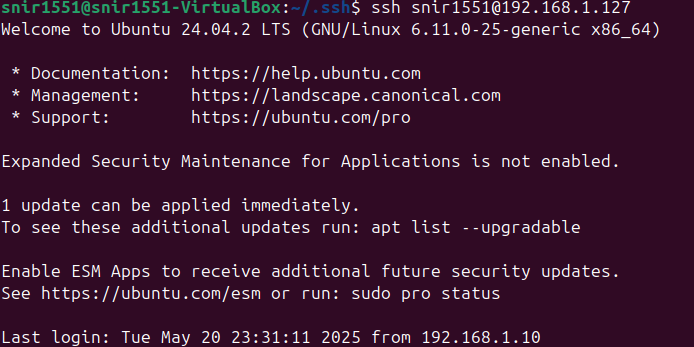
ssh-copy-id user@remote\_host

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.



without needing to enter a password.

