Essential Linux networking commands

How to find the public and private IP of the current device?

Use `ip addr` to get the private IP, and `curl ifconfig.me` to get the public IP.

How to check open ports in current device?

```
sudo ufw status
```

How to open a port?

```
sudo ufw allow 22

# Remove open port
sudo ufw deny 22

# reload service to take effect
sudo ufw reload
```

How to check if a host is live?

```
ping <domain.com>
```

How to check which ports are currently engaged?

```
netstat -tulpn
```

How to check network bandwidth?

```
sudo iftop
```

How to check network speed?

```
speedtest-cli
```

How to check the open ports of a server?

```
nmap <domain.com>
# or
nmap <ip>
```

How to check which IP tried to establish ssh connection?

```
# complete log
sudo grep "sshd" /var/log/auth.log

# Failed attempts
sudo grep "Failed password" /var/log/auth.log

# Successful attemps
sudo grep "Accepted password" /var/log/auth.log
```

Decide which user can establish a remote ssh connection

```
sudo nano /etc/ssh/sshd_config

# inside the file

# To allow user
AllowUsers user1 user2

# To deny user
DenyUsers root admin
```

How to ban an IP that failed to establish ssh connection?

```
# install fail2ban tool
sudo apt update
sudo apt install fail2ban

# Configure fail2ban
sudo nano /etc/fail2ban/jail.conf

# Unban ip
sudo fail2ban-client set sshd unbanip <ip>

# List banned IP
sudo fail2ban-client status
```

How find details of a domain?

```
whois <IP>
```

How to monitor the network in real time?

```
sudo iftop
```

What is a domain query tool?

A **domain query tool** is a software or command-line utility that allows to query the **Domain Name System (DNS)** to retrieve information about domain names, IP addresses, and other related records. These tools are used to perform DNS lookups and help users and administrators gather details about target domains.

Common tools:

`nslookup`

`dig`

`whois`

What is reverse lookup?

To find the IP associated with a domain name.