



Basic Network Information

IP Configuration

`ip addr` Display IP addresses, subnet masks, and interface information.

Example:

```
ip addr show eth0
```

`ifconfig` Display or configure network interface parameters (deprecated, but still used).

Example:

```
ifconfig eth0
```

`hostname` Display the system's hostname.

Example:

```
hostname
```

`hostname -I` Display all IP addresses associated with the hostname.

Example:

```
hostname -I
```

`nmcli` NetworkManager command-line tool for managing network connections.

Example:

```
nmcli device show eth0
```

`ethtool` Display or change Ethernet card settings.

Example:

```
ethtool eth0
```

Routing

`route` Display or manipulate the IP routing table.

Example:

```
route -n
```

`ip route` Show or manipulate routing, devices, policy routing and tunnels.

Example:

```
ip route show
```

`traceroute e` Traces the route packets take to a network host.

Example:

```
traceroute google.com
```

Network Connectivity

Testing Connectivity

`ping` Send ICMP ECHO_REQUEST packets to network hosts.

Example:

```
ping google.com
```

`telnet` Connect to a remote system using the Telnet protocol (unencrypted).

Example:

```
telnet example.com 80
```

`nc (netcat)` Arbitrary TCP and UDP connections and listens. Good for testing network services.

Example:

```
nc -zv example.com 20-30
```

`curl` Transfer data from or to a server.

Example:

```
curl example.com
```

`wget` Retrieve files from the web.

Example:

```
wget https://example.com/file.txt
```

DNS Lookup

`nslookup up` Query Internet name servers interactively.

Example:

```
nslookup example.com
```

`dig` DNS lookup utility. More powerful and flexible than `nslookup`.

Example:

```
dig example.com
```

`host` DNS lookup utility for finding the IP address associated with a hostname or vice versa.

Example:

```
host example.com
```

Network Monitoring

Traffic Monitoring

`tcpdump -i mp` A powerful packet analyzer; it prints a description of the contents of network packets.

Example:

```
tcpdump -i eth0
```

`wireshark -i hark` A network protocol analyzer that lets you capture and interactively browse the traffic running on a computer network. (GUI based).

Example:

Start Wireshark from the GUI or use `tshark` (command-line version).

```
tshark -i eth0
```

`iftop -p` Displays bandwidth usage on an interface by host.

Example:

```
iftop -i eth0
```

`nload -d` Displays network usage in real-time.

Example:

```
nload eth0
```

Connection Monitoring

`netstat -tat` Displays network connections, routing tables, interface statistics, masquerade connections, and multicast memberships.

Example:

```
netstat -an
```

`ss -ss` is used to dump socket statistics. It allows showing information similar to `netstat`.

Example:

```
ss -tulpn
```

`lsof -f` List open files. Can be used to find processes using network connections.

Example:

```
lsof -i :80
```

Firewall Management

iptables

`iptables -L` List current iptables rules.

Example:

```
iptables -L
```

`iptables -A INPUT -p tcp --dport 22 -j ACCEPT` Add a rule to accept SSH traffic.

Example:

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

`iptables -D INPUT -p tcp --dport 22 -j ACCEPT` Delete a rule.

Example:

```
iptables -D INPUT -p tcp --dport 22 -j ACCEPT
```

firewalld

`firewall-cmd --state` Check the status of firewalld.

Example:

```
firewall-cmd --state
```

`firewall-cmd --zone=public -a-add-port=80/tcp --permanent` Open port 80 for HTTP traffic permanently.

Example:

```
firewall-cmd --zone=public --add-port=80/tcp --permanent
```

`firewall-cmd --reload` Reload firewalld to apply changes.

Example:

```
firewall-cmd --reload
```