Linux Network Tools Cheatsheet v1.0

smallnest

October 1, 2024

1 Network Configuration and Management Tools

1.1 ifconfig

Description: Configure and display network interface parameters (gradually being replaced by the `ip` tool).
Syntax:

```
ifconfig [interface] [options]
```

Common options:

- `up`: Activate network interface
- `down`: Deactivate network interface
- `inet`: Set IP address
- `netmask [mask]`: Specify network mask
- `broadcast [address]`: Set broadcast address

Examples:

```
ifconfig eth0 up
ifconfig eth0 192.168.1.100
```

1.2 ip

Description: Display and manipulate network interfaces, routing, policy routing, and tunnels.
Syntax:

```
ip [OPTIONS] OBJECT { COMMAND | help }
```

Common options:

- `addr`: Display/manipulate addresses
- `link`: Display/manipulate device properties
- `route`: Display/manipulate routing table
- `neigh`: Display/manipulate neighbor information
- `tunnel`: Display/manipulate tunnels

Examples:

```
ip addr show
ip link set eth0 up
ip route add default via 192.168.1.1
```

1.3 route

Description: Display and manipulate IP routing table (gradually being replaced by the `ip` tool).
Syntax:

```
route [add|del] [-net|-host] target [netmask Nm] [gw Gw]
```

Common options:

- `add`: Add route
- `del`: Delete route
- `-host`: Specify host route
- `-net`: Specify network route
- `gw`: Specify gateway

Examples:

```
route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.1.1
route del -net 192.168.1.0 netmask 255.255.255.0
```

1.4 arp

Description: Display and modify the system's ARP (Address Resolution Protocol) cache.
Syntax:

```
arp [-v] [-i if] [-H type] [-A family] [-d hostname] [hostname]
```

Common options:

- `-a`: Display ARP cache
- `-d`: Delete ARP entry
- `-s`: Set static ARP entry
- `-i [interface]`: Specify interface
- `-n`: Don't resolve hostnames

Examples:

```
arp -a
arp -d 192.168.1.1
arp -s 192.168.1.1 00:11:22:33:44:55
```

1.5 iptables

Description: Configure Linux kernel firewall rules and NAT functionality.
Syntax:

```
iptables [-t table] -[AD] chain rule-specification [options]
```

Common options:

- `-A`: Append rule
- `-D`: Delete rule
- `-L`: List rules
- `-F`: Flush rules
- `-P`: Set chain default policy

Examples:

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

2 Network Connection and Transfer Tools

2.1 netcat

Description: A utility for reading from and writing to network connections, also known as the "Swiss Army knife" of networking.
Syntax:

```
nc [options] hostname port
```

Common options:

- `-l`: Listen mode
- `-v`: Verbose output
- `-z`: Scan mode
- `-u`: Use UDP protocol
- `-n`: Don't use DNS resolution

Examples:

```
nc -l -p 12345
nc -v google.com 80
```

2.2 telnet

Description: Used to connect to remote hosts using the Telnet protocol.
Syntax:

```
telnet [hostname [port]]
```

Common options:

- `-l user`: Specify login name
- `-a`: Attempt automatic login

Examples:

```
telnet google.com 80
```

2.3 ssh/scp

Description: Secure remote login and file transfer using the Secure Shell (SSH) protocol.
Syntax:

```
ssh [user@]hostname [command]
scp [options] [user@]hostname:source target
```

Common options:

- `-p`: Specify port
- `-i`: Specify identity file
- `-C`: Enable compression
- `-X`: Enable X11 forwarding
- `-r`: Recursively copy directories

Examples:

```
ssh user@remotehost
scp file.txt user@remotehost:/path/to/destination
```

2.4 whois

Description: Query domain registration information and IP address ownership information.
Syntax:

```
whois [options] query
```

Common options:

- `-h`: Specify whois server
- `-p`: Specify port

Examples:

```
whois google.com
```

3 Network Monitoring and Diagnostic Tools

3.1 ping

Description: Test network connectivity and measure round-trip time.
Syntax:

```
ping [options] destination
```

Common options:

- `-c`: Specify the number of requests to send
- `-i`: Specify the interval between sending requests
- `-s`: Specify the packet size
- `-t`: Specify the Time To Live (TTL)

Examples:

```
ping -c 4 google.com
```

3.2 fping

Description: Suitable for pinging multiple hosts in batch, providing more flexible ping functionality.
Syntax:

```
fping [options] [targets...]
```

Common options:

- `-a`: Show only active hosts
- `-q`: Quiet mode
- `-t`: Time interval between pings
- `-g`: Generate targets within a specified range

Examples:

```
fping -a google.com yahoo.com
```

3.3 traceroute

Description: Trace the route packets take in the network.
Syntax:

```
traceroute [options] host
```

Common options:

- `-m`: Set maximum hop count
- `-n`: Do not resolve hostnames
- `-p`: Specify the port to use
- `-I`: Use ICMP ECHO for probing

Examples:

```
traceroute google.com
```

3.4 tcptraceroute

Description: Trace network path using TCP packets (useful when firewalls filter ICMP).
Syntax:

```
tcptraceroute [options] host [port]
```

Common options:

- `-m`: Set maximum hop count
- `-n`: Do not resolve hostnames

Examples:

```
tcptraceroute google.com 80
```

3.5 tracepath

Description: Trace packet path and report MTU (Maximum Transmission Unit) values.
Syntax:

```
tracepath [options] destination
```

Common options:

- `-n`: Do not resolve hostnames
- `-b`: Show AS numbers of routers

Examples:

```
tracepath google.com
```

3.6 mtr

Description: Network diagnostic tool combining functionality of `ping` and `traceroute`, reporting real-time network path performance.
Syntax:

```
mtr [options] host
```

Common options:

- `-r`: Report mode
- `-c`: Specify the number of pings
- `-t`: Force text output mode

Examples:

```
mtr google.com
```

3.7 iftop

Description: Display real-time bandwidth usage on network interfaces.
Syntax:

```
iftop [options]
```

Common options:

- `-i [interface]`: Specify interface
- `-B`: Display bandwidth in bytes/sec
- `-n`: Do not resolve addresses

Examples:

```
iftop -i eth0
```

3.8 tcpdump

Description: Capture and analyze network packets, used for network diagnostics and traffic analysis.
Syntax:

```
tcpdump [options] [expression]
```

Common options:

- `-i`: Specify interface
- `-w`: Write packets to file
- `-r`: Read packets from file
- `-n`: Do not resolve DNS
- `-v`: Verbose mode

Examples:

```
tcpdump -i eth0
tcpdump -w capture.pcap
```

3.9 ss

Description: Display socket statistics, replacing the `netstat` tool.
Syntax:

```
ss [options] [filter]
```

Common options:

- `-t`: Show TCP connections
- `-u`: Show UDP connections
- `-a`: Show all sockets
- `-p`: Show processes using sockets
- `-s`: Show summary statistics

Examples:

```
ss -t
ss -u
ss -s
```

3.10 netstat

Description: Display network connections, routing tables, interface statistics, etc. (gradually being replaced by the `ss` tool).
Syntax:

```
netstat [options]
```

Common options:

- `-a`: Show all connections and listening ports
- `-r`: Show routing table
- `-i`: Show interface statistics
- `-s`: Show statistics for each protocol
- `-p`: Show process information

Examples:

```
netstat -a
netstat -r
```

4 Network Performance Testing Tools

4.1 iperf

Description: Tool for measuring network bandwidth performance.
Syntax:

```
iperf [options]
```

Common options:

- `-s`: Server mode
- `-c`: Client mode
- `-u`: Use UDP for testing
- `-t`: Test duration

Examples:

```
iperf -s
iperf -c server_ip
```

4.2 iperf3

Description: Improved version of `iperf`, providing more accurate bandwidth measurement and additional features.
Syntax:

```
iperf3 [options]
```

Common options:

- `-s`: Server mode
- `-c`: Client mode
- `-u`: Use UDP for testing
- `-t`: Test duration
- `-R`: Reverse test, client downloads in client mode

Examples:

```
iperf3 -s
iperf3 -c server_ip
```

5 Domain Name Tools

5.1 dig

Description: Query DNS record information, supporting detailed output format.
Syntax:

```
dig [options] [name] [type]
```

Common options:

- `+short`: Concise output
- `+trace`: Trace the domain name resolution process
- `@server`: Specify DNS server

Examples:

```
dig google.com
dig +trace google.com
```

5.2 nslookup

Description: Query DNS record information, using interactive mode.
Syntax:

```
nslookup [options] [name | - [server]]
```

Common options:

- `-type=record`: Specify query record type (such as A, MX, etc.)
- `server`: Use specified DNS server

Examples:

```
nslookup google.com
nslookup -type=MX google.com
```

5.3 host

Description: Query DNS record information, simple and easy to use.
Syntax:

```
host [options] [name] [server]
```

Common options:

- `-t`: Specify the type of record to query
- `-a`: Display all query results

Examples:

```
host google.com
host -t MX google.com
```

6 Network Scanning and Security Tools

6.1 nmap

Description: Network scanning tool used for discovering hosts and services, with powerful port scanning capabilities.
Syntax:

```
nmap [options] [targets]
```

Common options:

- `-sS`: Perform TCP SYN scan
- `-O`: Operating system detection
- `-p`: Specify port scan range
- `-A`: Enable advanced detection
- `-v`: Increase verbosity

Examples:

```
nmap -sS 192.168.1.0/24
nmap -O 192.168.1.1
```