Linux 网络工具速查单

smallnest

2024 年 9 月 29 日

目录

1 网络配置与管理工具

1.1 ifconfig

解释：配置和显示网络接口参数（已逐渐被 ip 工具取代）。

语法：

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

常用选项：

- up：激活网络接口
- down：关闭网络接口
- inet：设置 IP 地址
- netmask [mask]：指定网络掩码
- broadcast [address]：设置广播地址

示例：

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

1.2 ip

解释：显示和操作网络接口、路由、策略路由和隧道。

语法：

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

常用选项：

- addr：显示/操作地址
- link：显示/操作设备属性
- route：显示/操作路由表
- neigh：显示/操作邻接信息
- tunnel：显示/操作隧道

示例：

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

1.3 route

解释：显示和操作 IP 路由表（已逐渐被 ip 工具取代）。

语法：

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

常用选项：

- `add`：添加路由
- `del`：删除路由
- `-host`：指定主机路由
- `-net`：指定网络路由
- `gw`：指定网关

示例：

```
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

解释：显示和修改系统的 ARP（地址解析协议）缓存。

语法：

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

常用选项：

- `-a`：显示 ARP 缓存
- `-d`：删除 ARP 条目
- `-s`：设置静态 ARP 条目
- `-i [interface]`：指定接口
- `-n`：不解析主机名

示例：

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

1.5 iptables

解释：配置 Linux 内核防火墙规则和 NAT 功能。

语法：

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

常用选项：

- `-A`：追加规则
- `-D`：删除规则
- `-L`：列出规则
- `-F`：清除规则
- `-P`：设置链默认策略

示例：

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

2 网络连接与传输工具

2.1 netcat

解释：读写网络连接的工具，也被称为”网络瑞士军刀”。

语法：

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

常用选项：

- `-l`：监听模式
- `-v`：详细输出
- `-z`：扫描模式
- `-u`：使用 UDP 协议
- `-n`：不使用 DNS 解析

示例：

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

2.2 telnet

解释：用于通过 Telnet 协议连接远程主机。

语法：

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

常用选项：

- `-l user`：指定登录名
- `-a`：尝试自动登录

示例：

```
telnet google.com 80
```

2.3 ssh/scp

解释：通过安全外壳协议（SSH）进行安全的远程登录和文件传输。

语法：

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

常用选项：

- `-p`：指定端口
- `-i`：指定身份文件
- `-C`：启用压缩
- `-X`：启用 X11 转发
- `-r`：递归复制目录

示例：

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

2.4 whois

解释：查询域名注册信息和 IP 地址所有者信息。

语法：

```
whois [options] query
```

常用选项：

- `-h`：指定 whois 服务器
- `-p`：指定端口

示例：

```
whois google.com
```

3 网络监控与诊断工具

3.1 ping

解释：测试网络连通性，测量往返时间。

语法：

```
ping [options] destination
```

常用选项：

- `-c`：指定发送的请求数目
- `-i`：指定发送请求的间隔时间
- `-s`：指定数据包大小
- `-t`：指定生存时间 TTL

示例：

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

3.2 fping

解释：适用于批量 ping 多个主机，提供更灵活的 ping 功能。

语法：

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

常用选项：

- `-a`：仅显示活动主机
- `-q`：静默模式
- `-t`：发送时间间隔
- `-g`：生成网络范围内的目标

示例：

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

3.3 traceroute

解释：跟踪数据包在网络中的路由路径。

语法：

```
traceroute [options] host
```

常用选项：

- `-m`：设置最大跳数
- `-n`：不解析主机名

- `-p`: 指定使用的端口
- `-I`: 使用 ICMP ECHO 进行探测

示例:

```
traceroute google.com
```

3.4 tcptraceroute

解释: 使用 TCP 数据包跟踪网络路径（适用于防火墙过滤 ICMP 的情况）。
语法:

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

常用选项:

- `-m`: 设置最大跳数
- `-n`: 不解析主机名

示例:

```
tcptraceroute google.com 80
```

3.5 tracepath

解释: 跟踪数据包路径并报告 MTU（最大传输单元）值。
语法:

```
tracepath [options] destination
```

常用选项:

- `-n`: 不解析主机名
- `-b`: 显示路由节点的 AS 号

示例:

```
tracepath google.com
```

3.6 mtr

解释: 集成了 `ping` 和 `traceroute` 功能的网络诊断工具，实时报告网络路径性能。
语法:

```
mtr [options] host
```

常用选项:

- `-r`: 报告模式
- `-c`: 指定测试的次数
- `-t`: 文本输出模式

示例:

```
mtr google.com
```

3.7 iftop

解释：实时显示网络接口的带宽使用情况。

语法：

```
iftop [options]
```

常用选项：

- `-i [interface]`：指定接口
- `-B`：以字节/秒显示速度
- `-n`：不解析地址

示例：

```
iftop -i eth0
```

3.8 tcpdump

解释：捕获和分析网络数据包，用于网络诊断和流量分析。

语法：

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

常用选项：

- `-i`：指定接口
- `-w`：将数据包写入文件
- `-r`：读取数据包文件
- `-n`：不进行 DNS 解析
- `-v`：详细模式

示例：

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

3.9 ss

解释：显示套接字统计信息，替代 `netstat` 工具。

语法：

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

常用选项：

- `-t`：显示 TCP 连接
- `-u`：显示 UDP 连接
- `-a`：显示所有的套接字

- -p: 显示关联的进程

示例:

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

3.10 netstat

解释: 显示网络连接、路由表、接口统计信息等（已逐渐被 ss 工具取代）。
语法:

```
netstat [options]
```

常用选项:

- -a: 显示所有连接和监听端口
- -r: 显示路由表
- -i: 显示接口统计信息
- -s: 显示每个协议的统计数据
- -p: 同时显示进程信息

示例:

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

4 网络性能测试工具

4.1 iperf

解释: 测量网络带宽性能的工具。
语法:

```
iperf [options]
```

常用选项:

- -s: 服务器模式
- -c: 客户端模式
- -u: 使用 UDP 测试
- -t: 测试时长

示例:

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

4.2 iperf3

解释：`iperf` 的改进版本，提供更精确的带宽测量和更多功能。

语法：

```
iperf3 [options]
```

常用选项：

- `-s`：服务器模式
- `-c`：客户端模式
- `-u`：使用 UDP 测试
- `-t`：测试时长
- `-R`：逆向测试，客户端模式下载

示例：

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

5 域名工具

5.1 dig

解释：查询 DNS 记录信息，支持详细的输出格式。

语法：

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

常用选项：

- `+short`：简洁输出
- `+trace`：跟踪域名解析过程
- `@server`：指定 DNS 服务器

示例：

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

5.2 nslookup

解释：查询 DNS 记录信息，使用交互模式。

语法：

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

常用选项：

- `-type=record`：指定查询记录类型（如 A、MX 等）

- `server`：使用指定的 DNS 服务器

示例：

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

5.3 host

解释：查询 DNS 记录信息，简单易用。
语法：

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

常用选项：

- `-t`：指定查询的记录类型
- `-a`：显示查询的所有结果

示例：

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

6 网络扫描与安全工具

6.1 nmap

解释：网络扫描工具，用于发现主机和服务，具有强大的端口扫描功能。
语法：

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

常用选项：

- `-sS`：进行 TCP SYN 扫描
- `-O`：操作系统检测
- `-p`：指定端口扫描范围
- `-A`：启用高级检测
- `-v`：增加详尽输出

示例：

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