
S2E4 - linux cli network tools cheat sheet

Nicholas Morrison nick@nanocat.net



net-tools

- net-tools is an old suite of network-related tools
 - netstat (for looking at open sockets, and the routing table)
 - ifconfig (interface config, for managing wired network interfaces)
 - iwconfig (same but for wireless interfaces)
 - route (for managing the routing table)
 - iptunnel (for creating tunnels)
 - arp (for managing the ARP cache) (Address Resolution Protocol)

iproute2

- iproute2 superceded net-tools, and includes more modern utilities
 - ss (for looking at sockets)
 - ip (for doing almost everything)
 - * ip route (manage routing tables)
 - * ip address (manage ip addresses)
 - * ip neigh (manage ARP cache)
 - * ip tunnel (manage tunnels)
 - iw (managing wireless interfaces)

The ip tool

- ip manages many many aspects of linux networking
- ip route = manage your routing table (try ip -c route)
- ip netns = manage network namespaces (try ip netns exec clab-www-pc1 ip -c route)
- ip address = manage ip addresses (don't forget -c for colour - ip -c address)
- ip neigh = manage ARP cache. (Other hosts in the same layer 2 network are your neighbours.)
- ip -c neigh = with colour!

The ss tool

- ss gives us information about SOCKETS
- a socket is a channel for communicating with a process
- can be network sockets or unix sockets
- (we only care about network sockets right now)
- ss -t -l = listening TCP sockets
- ss -t -a = listening and non-listening TCP sockets
- ss -u -l = listening UDP sockets
- ss -t | grep ssh = show active ssh connections