* ifconfig (or ip link, ip addr) - for obtaining information about network interfaces
* ping - for validating, if target host is accessible from my machine. ping is also could be used for basic DNS diagnostics - we could ping host by IP-address or by its hostname and then decide if DNS works at all. And then traceroute or tracepath or mtr to look what's going on on the way to there.
* dig - diagnose everything DNS
* dmesg | less or dmesg | tail or dmesg | grep -i error - for understanding what the Linux kernel thinks about some trouble.
* netstat -antp + | grep smth - my most popular usage of netstat command, which shows information about TCP connections. Often I perform some filtering using grep. See also the new ss command (from iproute2 the new *standard* suite of Linux networking tools) and lsof as in lsof -ai tcp -c some-cmd.
* telnet <host> <port> - is very useful for communicating with various TCP-services(e.g. on SMTP, HTTP protocols), also we could check general opportunity to connect to some TCP port.
* iptables-save (on Linux) - to dump the **full** iptables tables
* ethtool - get all the network interface card parameters (status of the link, speed, offload parameters...)
* socat - the swiss army tool to test all network protocols (UDP, multicast, SCTP...). Especially useful (more so than telnet) with a few -d options.
* iperf - to test bandwidth availability
* openssl (s\_client, ocsp, x509...) to debug all SSL/TLS/PKI issues.
* wireshark - the powerful tool for capturing and analyzing network traffic, which allows to analyze and catch many network bugs.
* iftop - show big users on the network/router.
* iptstate (on Linux) - current view of the firewall's connection tracking.
* arp (or the new (Linux) ip neigh) - show the ARP-table status.
* route or the newer (on Linux) ip route - show the routing table status.
* strace (or truss, dtrace or tusc depending on the system) - is useful tool which shows what system calls does the problem process, it also shows error codes(errno) when system calls fails. This information often says enough for understanding the system behavior and solving a problem. Alternatively, using breakpoints on some networking functions in gdb can let you find out when they are made and with which arguments.
* to investigate firewall issues on Linux: iptables -nvL shows how many packets are matched by each rule (iptables -Z to zero the counters). The LOG target inserted in the firewall chains is useful to see which packets reach them and how they have already been transformed when they get there. To get further NFLOG (associated with ulogd) will log the full packet.