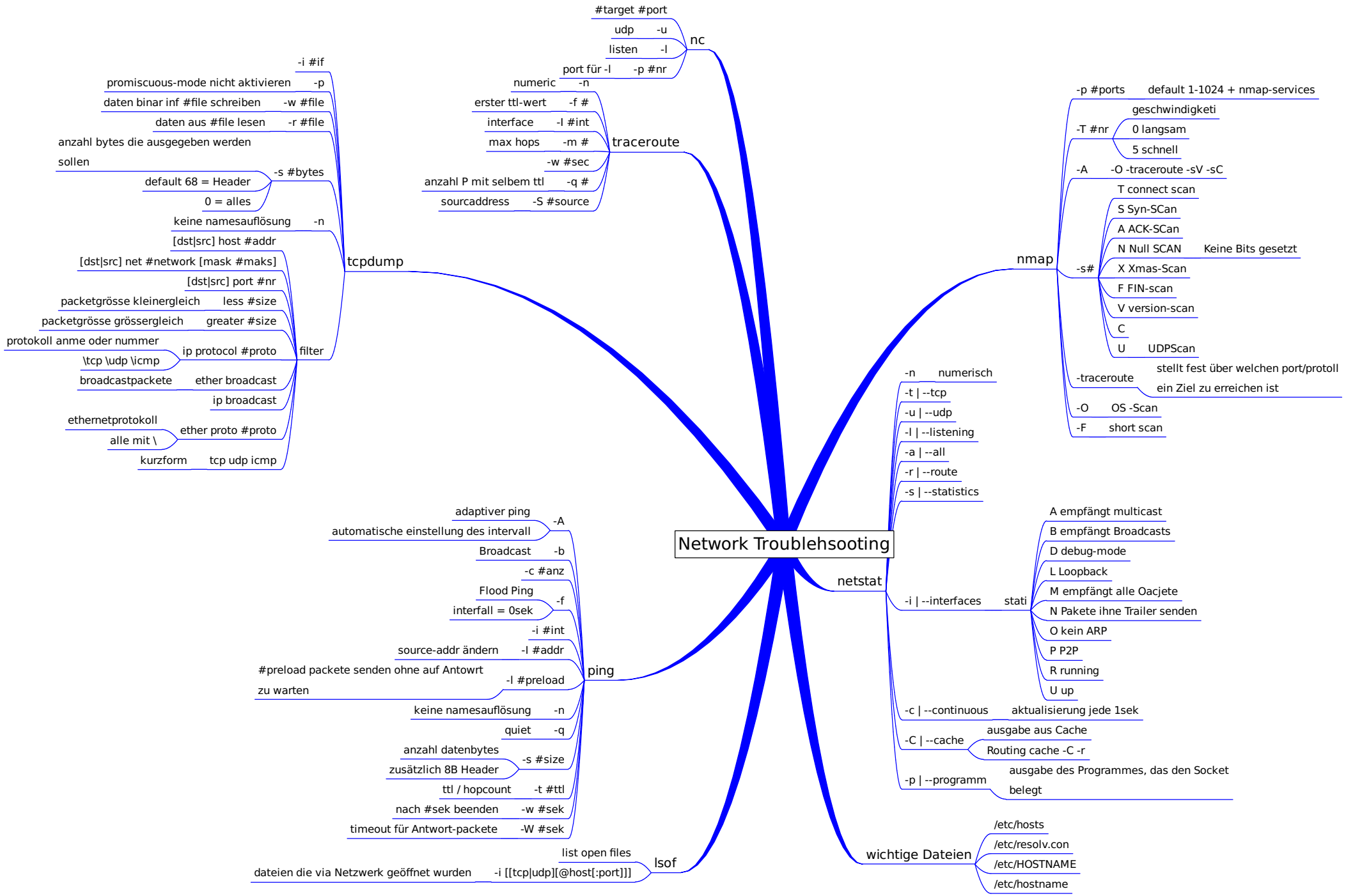
Network Troublehsooting
nc
#target #port
udp -u
listen -l
port für -l -p #nr
traceroute
numeric -n
erster ttl-wert -f #
interface -I #int
max hops -m #
-w #sec
anzahl P mit selbem ttl -q #
sourcaddress -S #source
tcpdump
-i #if
promiscuous-mode nicht aktivieren -p
daten binar inf #file schreiben -w #file
daten aus #file lesen -r #file
-s #bytes
anzahl bytes die ausgegeben werden sollen
default 68 = Header
0 = alles
keine namesauflösung -n
filter
[dst|src] host #addr
[dst|src] net #network [mask #maks]
[dst|src] port #nr
packetgrösse kleinergleich less #size
packetgrösse grössergleich greater #size
ip protocol #proto
protokoll anme oder nummer
\tcp \udp \icmp
ether broadcast
broadcastpackete
ip broadcast
ether proto #proto
ethernetprotokoll
alle mit \
tcp udp icmp
kurzform
ping
-A
adaptiver ping
automatische einstellung des intervall
-b
Broadcast
-c #anz
-f
Flood Ping
interfall = 0sek
-i #int
-I #addr
source-addr ändern
-I #preload
#preload packete senden ohne auf Antowrt zu warten
-n
keine namesauflösung
-q
quiet
-s #size
anzahl datenbytes
zusätzlich 8B Header
-t #ttl
ttl / hopcount
-w #sek
nach #sek beenden
-W #sek
timeout für Antwort-packete
lsof
list open files
-i [[tcp|udp][@host[:port]]]
dateien die via Netzwerk geöffnet wurden
nmap
-p #ports default 1-1024 + nmap-services
-T #nr
geschwindigkeiten
0 langsam
5 schnell
-A -O -traceroute -sV -sC
-s#
T connect scan
S Syn-SCan
A ACK-SCan
N Null SCAN Keine Bits gesetzt
X Xmas-Scan
F FIN-scan
V version-scan
C
U UDPScan
-traceroute
stellt fest über welchen port/protoll ein Ziel zu erreichen ist
-O OS -Scan
-F short scan
netstat
-n numerisch
-t | --tcp
-u | --udp
-l | --listening
-a | --all
-r | --route
-s | --statistics
-i | --interfaces stati
A empfängt multicast
B empfängt Broadcasts
D debug-mode
L Loopback
M empfängt alle Oacjete
N Pakete ihne Trailer senden
O kein ARP
P P2P
R running
U up
-c | --continuous aktualisierung jede 1sek
-C | --cache
ausgabe aus Cache
Routing cache -C -r
-p | --programm
ausgabe des Programmes, das den Socket belegt
wichtige Dateien
/etc/hosts
/etc/resolv.con
/etc/HOSTNAME
/etc/hostname