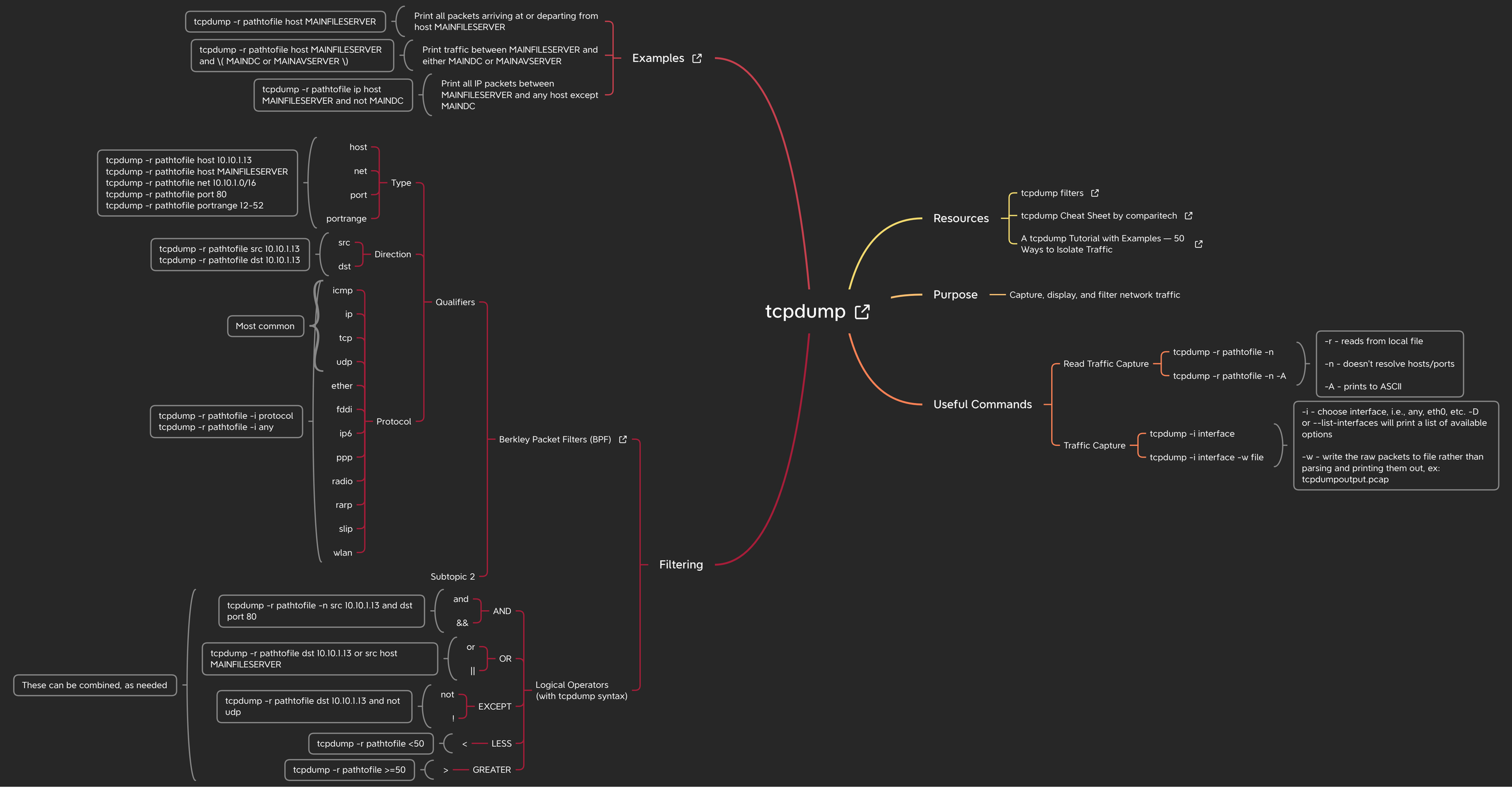
tcpdump
Resources
tcpdump filters
tcpdump Cheat Sheet by comparitech
A tcpdump Tutorial with Examples — 50 Ways to Isolate Traffic
Purpose
Capture, display, and filter network traffic
Useful Commands
Read Traffic Capture
tcpdump -r pathtofile -n
tcpdump -r pathtofile -n -A
-r - reads from local file
-n - doesn't resolve hosts/ports
-A - prints to ASCII
Traffic Capture
tcpdump -i interface
tcpdump -i interface -w file
-i - choose interface, i.e., any, eth0, etc. -D or --list-interfaces will print a list of available options
-w - write the raw packets to file rather than parsing and printing them out, ex: tcpdumpoutput.pcap
Filtering
Examples
tcpdump -r pathtofile host MAINFILESERVER
Print all packets arriving at or departing from host MAINFILESERVER
tcpdump -r pathtofile host MAINFILESERVER and \(MAINDC or MAINAVSERVER \)
Print traffic between MAINFILESERVER and either MAINDC or MAINAVSERVER
tcpdump -r pathtofile ip host MAINFILESERVER and not MAINDC
Print all IP packets between MAINFILESERVER and any host except MAINDC
Berkley Packet Filters (BPF)
Qualifiers
Type
host
net
port
portrange
tcpdump -r pathtofile host 10.10.1.13
tcpdump -r pathtofile host MAINFILESERVER
tcpdump -r pathtofile net 10.10.1.0/16
tcpdump -r pathtofile port 80
tcpdump -r pathtofile portrange 12-52
Direction
src
dst
tcpdump -r pathtofile src 10.10.1.13
tcpdump -r pathtofile dst 10.10.1.13
Protocol
icmp
ip
tcp
udp
ether
fddi
ip6
ppp
radio
rarp
slip
wlan
Most common
tcpdump -r pathtofile -i protocol
tcpdump -r pathtofile -i any
Subtopic 2
Logical Operators (with tcpdump syntax)
AND
and
&&
tcpdump -r pathtofile -n src 10.10.1.13 and dst port 80
OR
or
||
tcpdump -r pathtofile dst 10.10.1.13 or src host MAINFILESERVER
EXCEPT
not
!
tcpdump -r pathtofile dst 10.10.1.13 and not udp
LESS
<
tcpdump -r pathtofile <50
GREATER
>
tcpdump -r pathtofile >=50
These can be combined, as needed