tcpdump Cheat Sheet

tcpdump is a command-line packet analyzer tool used to capture and inspect network traffic. It is commonly used by network administrators and security professionals for troubleshooting, monitoring, and analyzing network packets.

# Basic Syntax

sudo tcpdump [options]

# Common Commands and Examples

* Capture traffic on a specific interface:  
  sudo tcpdump -i eth0
* Capture HTTP traffic (port 80):  
  sudo tcpdump -i eth0 port 80
* Capture packets to/from a specific IP:  
  sudo tcpdump host 192.168.1.100
* Capture traffic from a specific source IP:  
  sudo tcpdump src 192.168.1.100
* Capture traffic to a specific destination IP:  
  sudo tcpdump dst 192.168.1.100
* Save captured packets to a file:  
  sudo tcpdump -i eth0 -w capture.pcap
* Read packets from a saved file:  
  tcpdump -r capture.pcap
* Limit number of packets captured:  
  sudo tcpdump -c 100
* Capture all traffic and display in readable format:  
  sudo tcpdump -A
* Capture only TCP traffic:  
  sudo tcpdump tcp