# tcpdump Overview - Summary

## What is tcpdump?

tcpdump is a command-line network protocol analyzer (packet sniffer) used to capture and analyze network traffic. Captured data can be saved as packet capture (p-cap) files for later analysis. It is commonly pre-installed on Linux and also compatible with macOS and other Unix-based systems.

## Basic Command Syntax

sudo tcpdump [-i interface] [options] [expressions]  
  
- -i interface: Specify the network interface (e.g., 'any' for all interfaces)  
- sudo: Required for elevated privileges to access packet data

## Common Options

- -w file.pcap: Write captured packets to a p-cap file  
- -r file.pcap: Read and analyze a saved p-cap file  
- -v, -vv, -vvv: Verbosity levels for more detailed output  
- -c N: Capture only N packets  
- -n: Disable name resolution (avoids misleading info and reverse DNS lookups)  
- -nn: Disable resolution of both hostnames and ports

## Filter Expressions

Focus on specific traffic types using filters:  
- Protocols: ip, ip6, tcp, udp  
- Ports: port 80, tcp port 443  
- IPs: host 192.168.1.1  
- Use Boolean logic: and, or, not  
Example:  
sudo tcpdump -r file.pcap -n 'ip and port 80'

## Interpreting Output

Each captured packet line includes:  
- Timestamp  
- Source IP and port  
- Destination IP and port  
- Protocol flags and details (with -v enabled)

## Key Takeaways

tcpdump is essential for network troubleshooting and security incident analysis. Learning how to use interfaces, filters, and verbosity options helps derive valuable insights from raw network traffic.