tcpdump

Prof. Chien-Chao Tseng

曾 建 超 教授

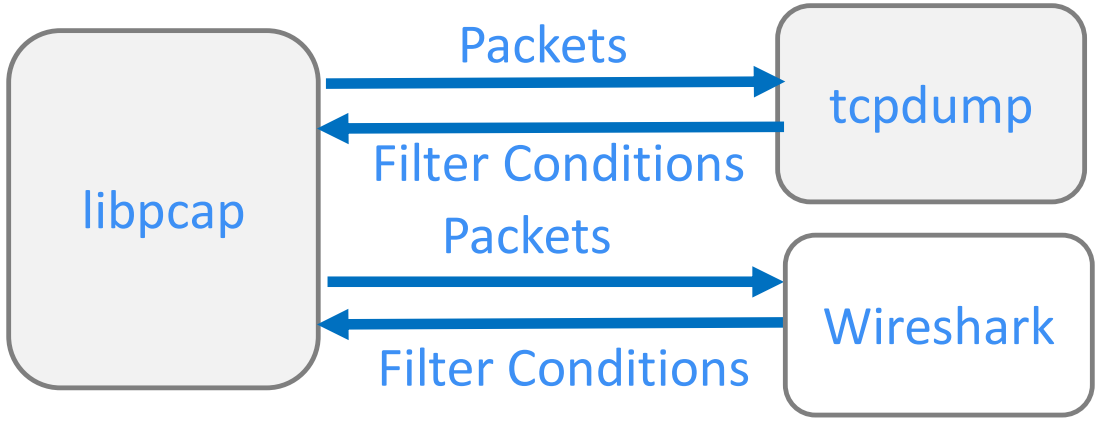
Department of Computer Science
National Yang Ming Chiao Tung University

cctseng@cs.nctu.edu.tw

1. TCPDUMP and Linbpcap
   https://www.tcpdump.org/
2. Man page of TCPDUMP:
   https://www.tcpdump.org/manpages/tcpdump.1.html
3. Man page of PCAP
   https://www.tcpdump.org/manpages/pcap.3pcap.html

tcpdump

- A data-network packet analyzer computer program
- Much like Wireshark
- But runs under a command line interface.
- Can capture and display packets being transmitted or received over a network
- Works on most Unix-like operating systems
  - Uses a packet capture library **libpcap** to capture packets.

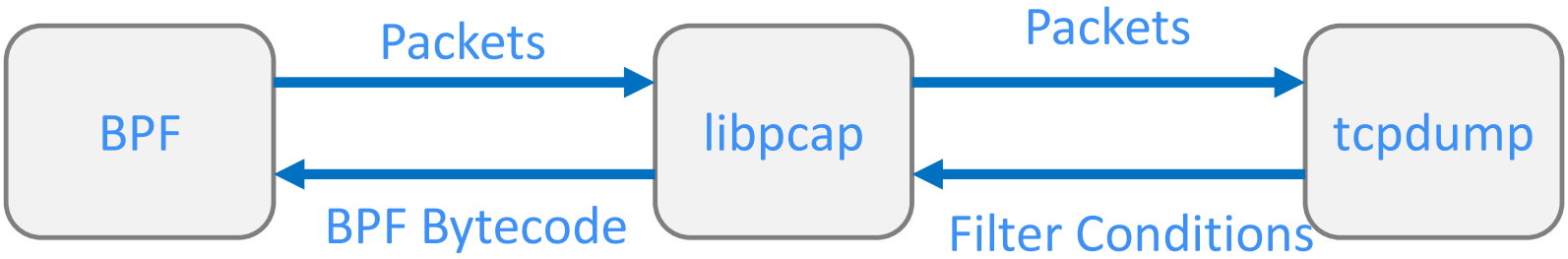


Packet Capture (pcap)

- An application programming interface (API) for capturing network traffic.
- Unix-like systems implement pcap in the *libpcap* library;
  - A port of libpcap named *WinPcap* for Windows, but no longer supported
    - WinDump, Windows version of tcpdump, uses WinPcap.
  - Another port named *Npcap* for Windows 7 and later, still supported.
- Newer versions of pcap can even be used to
  - transmit packets on a network at the link layer, and
  - get a list of network interfaces for possible use with
- pcap API is written in C
  - Java, .NET languages, and scripting languages generally use a wrapper;
  - C++ programs may link directly to the C API or use an object-oriented wrapper.

How tcpdump Works

- Can read packets **from a network interface card** or from **a previously created saved packet file**.
- Can write packets to **standard output** or **a file**.
- Normally need to run tcpdump as a **superuser.**
- Normally apply a BPF-based filter to limit the number of captured packets



- Berkeley Packet Filter (BPF): filter, copy packets
- libpcap: a portable C/C++ library for network packet capture.
  - Translates filter conditions to BPF bytecode
  - Relay captured packets