SWITCH

The Swiss Education & Research Network

Packet Capture and Analysis

Simon Leinen <simon@switch.ch>

Basic Packet Capturing Tools

SWITCH
The Swiss Education & Research Network

tcpdump

- Captures and summarizes packets
- Can read/write from/to files in “libpcap” format

Ethereal

- Subsumes tcpdump's functionality
- Graphical (Ethereal) and traditional (tethereal) user interfaces
- Extensible design
  - Abundance of protocol “dissectors” even for new/exotic protocols
- Includes many useful analysis tools
- Works under Windows (requires WinPcap)

These tools can be combined

- Use tcpdump (possibly remotely) to capture packets to .pcap file
- Analyze later using Ethereal
- Ethereal understands many other trace file formats (Solaris `snoop` etc.)

Packet Tracing Caveats

SWITCH
The Swiss Education & Research Network

- Capture enough (you can always filter later)
  - tcpdump's default capture length is small (96 bytes)
    - use something like `-s 1540` if you are interested in payloads
  - Seemingly unrelated traffic can impact performance
    - E.g. Web pages from foo.example.com may load slowly because of the images from advertisements.example.net
    - But may have to filter aggressively when there is a lot of background traffic
- Collecting on several points can be very useful
  - On the endpoints of the communication
  - Near “suspicious” intermediate points (firewall)
  - Synchronized clocks (e.g. by NTP) are very useful for matching traces
- Address-to-name resolution can slow display and causes traffic
  - With tcpdump, consider using `-n` or tracing to file (`-w file`)

Exercises

SWITCH
The Swiss Education & Research Network

http://192.168.1.70/gn2/

...or in the tech-ws/capture/examples directory on the memory stick

broken-site-1.pcap – failed connection to HTTP server

broken-site-2.pcap – successful transfer from same HTTP server

broken-site-3.pcap – transfer that breaks in the middle

iperf-upstream.pcap – iperf server->client, seen at server

iperf-downstream.pcap – iperf server->client, seen at client

The Swiss Education & Research Network