PCAP and PCAPng

draft-gharris-opsawg-pcap
draft-tuexen-opsawg-pcap

Guy Harris Michael Richardson
Fulvio Risso Michael Tuexen
Jasper Bongertz Gerald Combs

github.com/pcapng
www.tcpdump.org

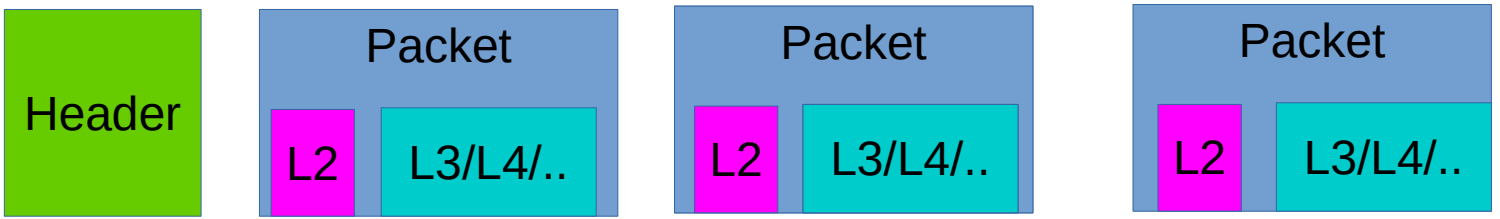
Background

- first IETF connection in IETF90, (Toronto 2014)
- tcpdump/libpcap first created around 1987 by Van Jacobson at LBL.
- TCPDUMP group took over maintenance in ~1998. A bunch of IETFers and others including Bill Fenner, Itojun, ...
- “pcap” format wore out around 2005, but inertia and open source efforts...
- “pcapng” format created around 2009, wireshark reads/writes it, libpcap can read it only at present

PCAP document

- Informational. IETF does not have change control.
  - Could even be published as **Historic**
- PCAP files consist of a header, and then a series of identical link-formats blocks
  - can not “cat” two pcap files together
- LINKTYPE determines format of contents
  - values up to 290 have been allocated
  - see document or http://www.tcpdump.org/linktypes.html

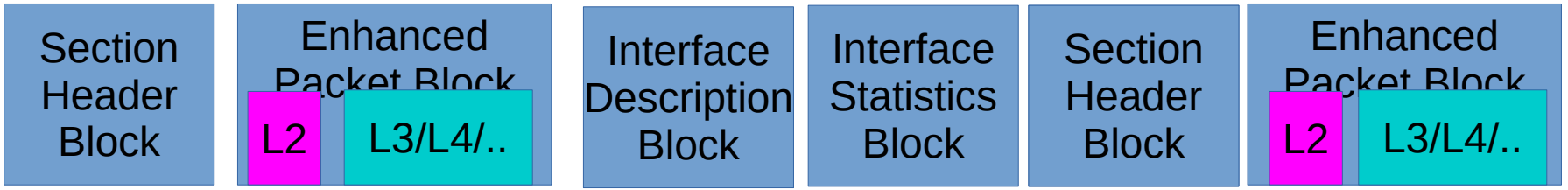
PCAP format



PCAPng document

- Standards Track. IETF does have change control.
  - But, we need to retain compatibility with existing header blocks
  - Could consider Informational, if someone wants to start “pcap3” WG
- PCAPng files consist of a series of blocks, all syntactically identical, which may be in any order
  - can “cat” two PCAPng files together and it makes sense
- LINKTYPE is in common with PCAP
- block type comes in Section Header Block, Interface Description Block, Enhanced Packet Block, Simple Packet Block, Name Resolution Block,Interface Statistics Block
- other types, like “systemd logging” can be moved to another document

PCAPng format



Issues and Next Steps

- adoption
- migration of LINKTYPE to IANA
- the name PCAP”ng”
- establish design team meeting pattern
- get to RFC quickly
- then revise with what might be non-backwards compatible things