PCAP and PCAPng
and PCAP Link Types

draft-gharris-opsawg-pcap
draft-tuexen-opsawg-pcap
draft-richardson-opsawg-pcaplinktype

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

github.com/pcapng
www.tcpdump.org
The Story so Far

• After multiple long discussions in 2019 and 2020, WG Adoption call(s) in October 2021.
  - pcap was adopted? pcapng was not?
  - It's really a document set...

• “Consensus” became:
  - remove LINKTYPE registry from pcap document, put it in a new document.
  - New Document is: draft-richardson-opsawg-pcaplinktype-00
3.1. LinkType Registry

IANA is requested to create a new Registry entitled “The PCAP Registry”, and within that Registry to create a table called “PCAP LinkType List.”

The LinkType Registry is a table of 16-bit numbers. The Registry has three sections with different [RFC8126] values:

- values from 0 to 32767 are marked as Specification Required.
- values from 32768 to 65535 are marked as First-Come First-Served.
- values from 65536 to 65539 are marked as Private Use.

The Registry has four columns: the symbolic name (LINKTYPE_xxx), the integer value, a very-short description, and the document/requestor reference.

The Registry shall be populated as follows in the table below. In each case here, the reference should be http://www.tcpdump.org/linktypex.html, which is not repeated.

The initial value of Table is base upon the Link type list maintained by tcpdump and published on the tcpdump.org website at http://www.tcpdump.org/linktypes.html.

There is often an associated DLT value which are often identical in value, but not universally so.

DLT values are associated with specific operating system captures, and are operating system (and thus not subject to standardization).

<table>
<thead>
<tr>
<th>LINKTYPE name</th>
<th>LINKTYPE value</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LINKTYPE_NULL</td>
<td>0</td>
<td>BSD loopback encapsulation</td>
</tr>
<tr>
<td>LINKTYPE_Ethernet</td>
<td>1</td>
<td>IEEE 802.3 Ethernet</td>
</tr>
<tr>
<td>LINKTYPE_EXP_Ethernet</td>
<td>2</td>
<td>Xerox experimental 3Mb Ethernet</td>
</tr>
<tr>
<td>LINKTYPE_AX25</td>
<td>3</td>
<td>AX.25 packet</td>
</tr>
<tr>
<td>LINKTYPE_PRONET</td>
<td>4</td>
<td>Reserved for PRONET</td>
</tr>
<tr>
<td>LINKTYPE_CHAOS</td>
<td>5</td>
<td>Reserved for MIT CHAOSNET</td>
</tr>
<tr>
<td>LINKTYPE_IEEE802_5</td>
<td>6</td>
<td>IEEE 802.5 Token Ring</td>
</tr>
<tr>
<td>LINKTYPE_ARCNET BSD</td>
<td>7</td>
<td>ARCNET Data Packets with BSD encapsulation</td>
</tr>
</tbody>
</table>
PCAP and PCAPng documents

• PCAP document Informational.
  – IETF does not have change control.
  – Recommend be published as Historic

• PCAPng document Informational.
  – new work could amend, etc. under IETF change control

• Both will reference pcap link types for registration
Adoption Call Actions

• Already split out the non-network “systemd” block into
  – draft-richardson-opsawg-pcapng-extras-00
• PCAP / PCAPng can be adopted or go via AD sponsor or via ISE
• PCAP-linktypes needs to be an IETF Action (WG or AD Sponsor) to establish the registry (ISE can not do that)
• Recommend that OPSAWG just adopt and progress.
Discussion