

# 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](https://github.com/pcapng)

[www.tcpdump.org](http://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

# draft-richardson-opsawg-pcaplinktype

- Really boring document, standards track

## 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](#) rules:

- values from 0 to 32767 are marked as Specification Required.
- values from 32768 to 65000 are marked as First-Come First-Served.
- values from 65000 to 65535 are marked as Private Use.

The Registry has four columns: the symbolic name (LINKTYPE\_something), 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/linktypes.html>, which is not repeated.

The initial value of table is base upon the Link type list maintained by libpcap, and published on the tcpdump.org web site as <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 operation system captures, and are operating sys: thus not subject to standardization.

LINKTYPE name	LINKTYPE value	description
LINKTYPE_NULL	0	BSD loopback encapsulat
LINKTYPE_ETHERNET	1	IEEE 802.3 Ethernet
LINKTYPE_EXP_ETHERNET	2	Xerox experimental 3Mb i

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

LINKTYPE name	LINKTYPE value	description
LINKTYPE_NULL	0	BSD loopback encapsulation
LINKTYPE_ETHERNET	1	IEEE 802.3 Ethernet
LINKTYPE_EXP_ETHERNET	2	Xerox experimental 3Mb Ethernet
LINKTYPE_AX25	3	AX.25 packet
LINKTYPE_PRONET	4	Reserved for PRONET
LINKTYPE_CHAOS	5	Reserved for MIT CHAOSNET
LINKTYPE_IEEE802_5	6	IEEE 802.5 Token Ring
LINKTYPE_ARCNET_BSD	7	ARCNET Data Packets with BSD encapsulation

GOES ON LIKE THIS FOR A FEW PAGES

# 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