Exegin Technologies Limited

IEEE 802.15.4 TAP Link Type Specification

Version 1.1

Revision	Description	Author
2019-01-29	Version 1.0 - Initial Release	James Ko
2019-02-21	Fix title. Revised introduction. Fix TLV labels. Removed TI CC24xx FCS Type. Removed pcapng examples.	James Ko
2019-02-22	Added LQI. Clarify length fields.	James Ko
2019-02-27	Added rules for constructing TLVs with bit flags, and padding with zeros.	James Ko
2019-03-13	Version 1.1 Added TLVs for channel center frequency and channel plan	James Ko

March 15, 2019

Contents

1 Introduction

IEEE 802.15.4 is an IEEE standard for Low-Rate Wireless Networks, including Low-Rate Wireless Personal Area Networks (LR-WPANs) and Low-Power Wide Area Networks (LPWAN), defining a number of physical (PHY) layers covering a wide variety of freqency bands and a number of Media Access Control (MAC) sub-layers for managing data and management services including beacon management, channel access, frame delivery and validation, and security mechanisms. Developing, debugging, diagnosing, and maintaining technologies using IEEE 802.15.4 require capturing packets with a sniffer. Sniffers generally output captured packets encapsulated in a pcap or pcapng packet with a specific data link-type (DLT) [1] that is understood by packet analyzers.

Three existing DLTs for IEEE 802.15.4 are defined

- DLT_IEEE802_15_4_WITHFCS (195),
- DLT_IEEE802_15_4_NONASK_PHY (215), and
- DLT_IEEE802_15_4_NOFCS (230).

None of the current DLTs provide a means to include out-of-band meta-data such as received signal strength and channel number which are useful for diagnostics in any wireless transmission system. Also, analyzers supporting DLT_IEEE802_15_4_WITHFCS currently assume a 16-bit FCS following the PHY payload. The IEEE 802.15.4-2015 standard also specifies a 32-bit CRC equivalent to ANSI X3.66-1979 for SUN PHYs or TVWS PHYs.

This document defines a new DLT and format for presenting captured IEEE 802.15.4 packets with meta-data to packet analyzers.

The latest version of this specification is at https://github.com/jkcko/ieee802.15.4-tap.

2 Overview

The IEEE 802.15.4 TAP DLT design is based on an extensible Type-Length-Value (TLV) format. The optional meta-data information in encapsulated in one or more TLVs and included in any packet from a sniffer. Some types may be duplicated by pcapng options but using the TLVs in this DLT enables providing the meta-data information in both pcap and pcapng capture streams. Where types are duplicated by TLVs and pcapng options in the same packet, the DLT TLVs have priority.

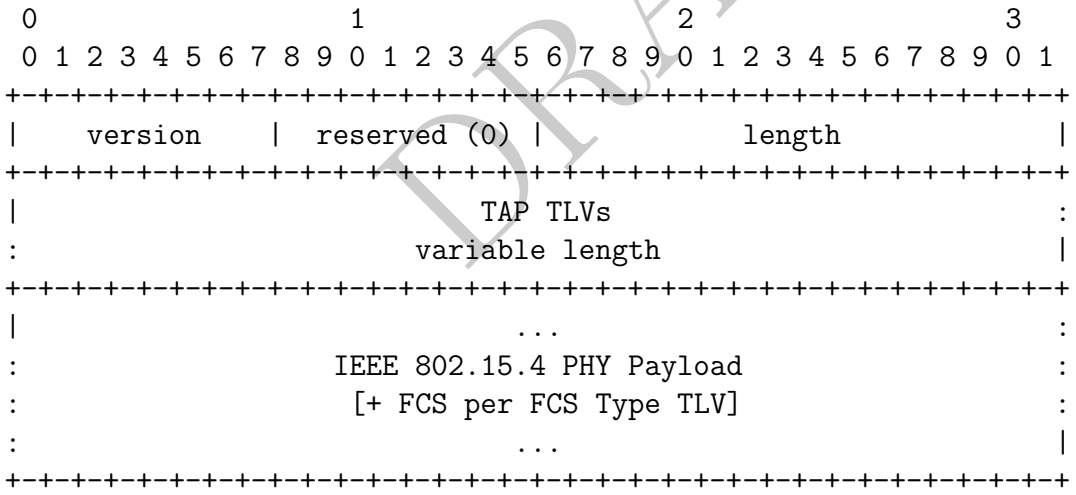
The DLT_IEEE802_15_4_TAP (283) value is specified in the pcap header or pcapng interface description block (IDB) LinkType field before the the first packet.

An IEEE 802.15.4 TAP packet is encapsulated in the packet data following a pcap record header or in the packet data of a pcapng Enhanced Packet Block (EPB).

2.1 IEEE 802.15.4 TAP Packet

The IEEE 802.15.4 TAP Packet consists of the TAP Header, zero or more TLV fields, the PHY payload (PSDU), and optional FCS bytes. All data fields are encoded in little-endian byte order.

2.1.1 IEEE 802.15.4 TAP Header

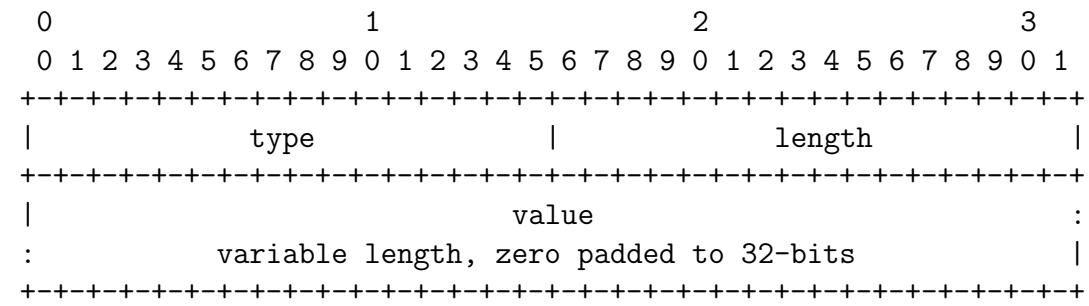


- version - currently only version 0 defined
- reserved - must be set to 0
- length - total length of header and TLVs in octets

Length is a minimum of 4 octets and must be a multiple of 4. Addition of new TLVs does not and must not require incrementing the version number.

2.1.2 IEEE 802.15.4 TAP TLVs

IEEE 802.15.4 TAP TLVs have the following format.



- type - type identifier
- length - number of octets for type in value field (not including padding)
- value - data for type

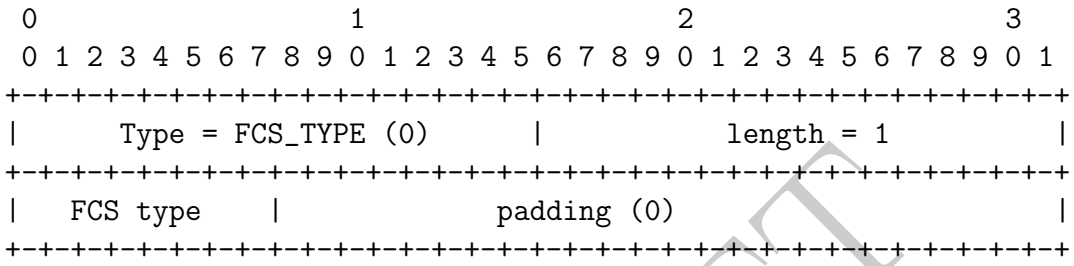
All padding bits must be set to zero. A TLV with zero (0) length is valid with no padding bits. Any TLV which defines a set of flags with as bits must also include a mask of known flags which are being provided by the flag bits. A flags TLV must be defined to have a variable length in multiples of 4-octets where the first half of the octets (i.e. 2 of 4 octets) are the mask and the second half are the flags. Mask and flags must be encoded in little-endian byte order and bit 0 is the least significant bit.

3 IEEE 802.15.4 TAP TLV Types

The following subsections describe the currently defined TLVs. Developers must request a new TLV if the meta-data to include does not match the type of the defined TLVs. Any unknown TLVs will be dissected as a binary blob of the provided length.

3.1 FCS Type

Identifies the FCS type following the PHY Payload. FCS type none (0) is optional if no FCS is present.

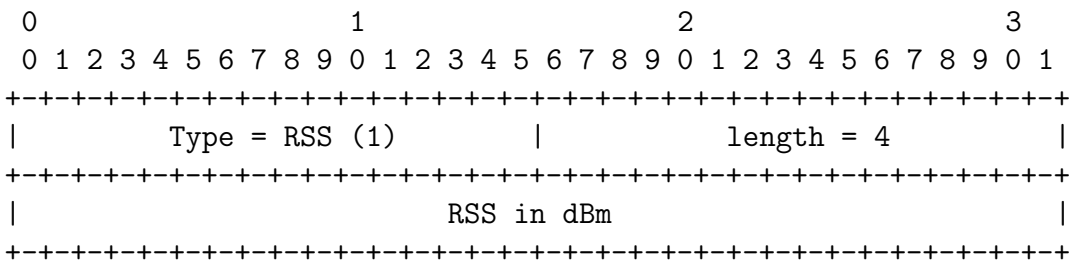


The FCS type is one of

- 0 = None,
- 1 = 16-bit CRC,
- 2 = 32-bit CRC.

3.2 Receive Signal Strength

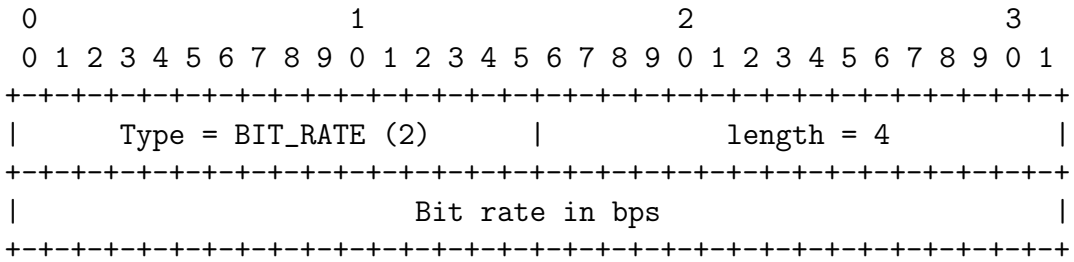
The received signal strength in dBm as a IEEE-754 floating point number.



Note: RSSI in dB must use a different TLV (TBD).

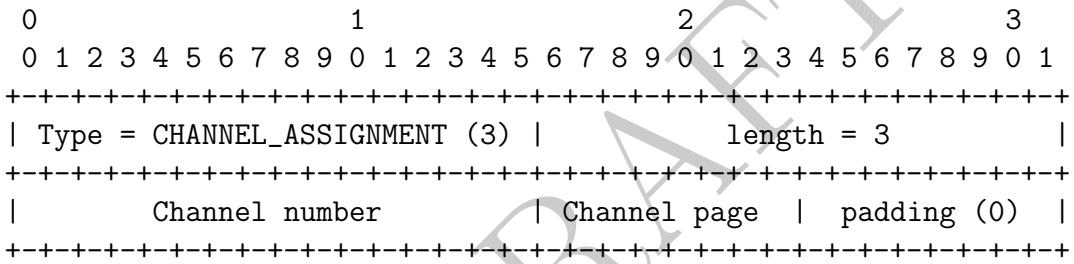
3.3 Bit Rate

The transmission data-rate in bps. The bit-rate may change frame to frame in multi-rate PHY configurations.



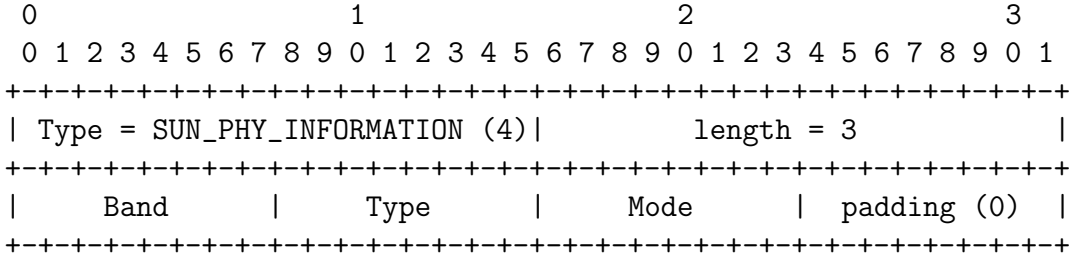
3.4 Channel Assignment

Channel assignments are defined through a combination of channel numbers and channel pages. See IEEE 802.15.4-2015 10.1.2 Channel assignments.



3.5 SUN PHY Information

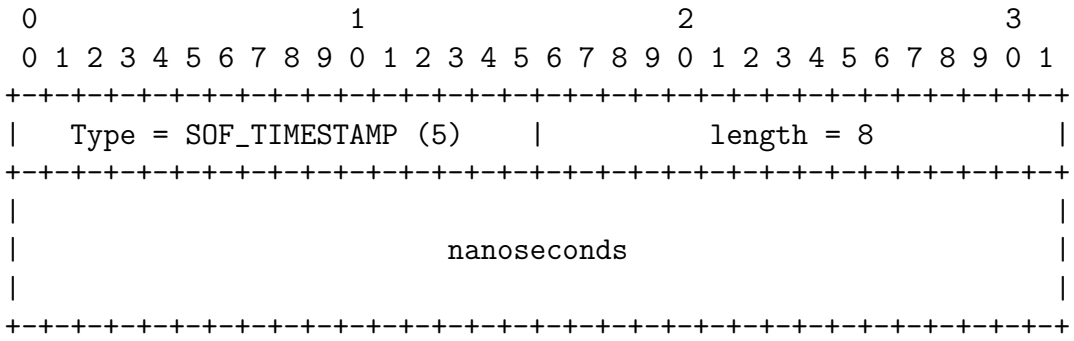
An IEEE 802.15.4 SUN PHY is configured to operate in a specified frequency band, encoding type, and rate mode.



- Band - IEEE 802.15.4 Table 7-19 Frequency band identifer values.
- Type - IEEE 802.15.4 Table 7-20 Modulation scheme encoding values.
- Mode - IEEE 802.15.4 Rate mode depends on the Band and Type.

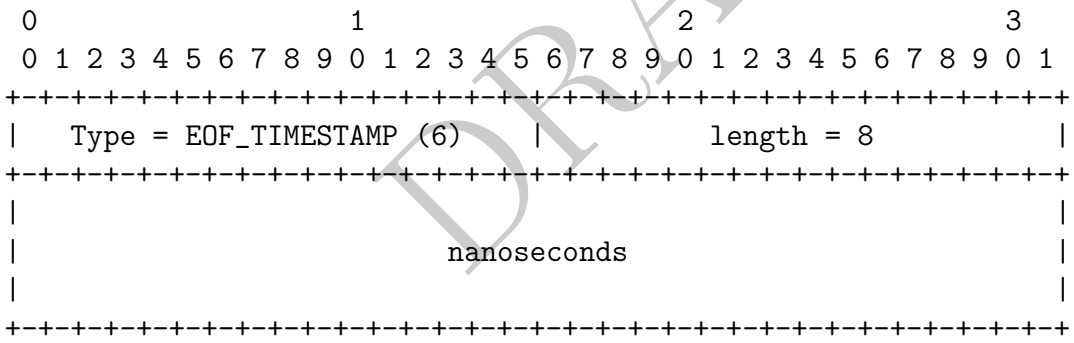
3.6 Start of Frame Timestamp

The start of frame timestamp is a monotonically increasing time in nanoseconds since power on of the receiving device. This value differs from the timestamp in the pcap or pcapng header which is based on the clock time reported by the sniffer.



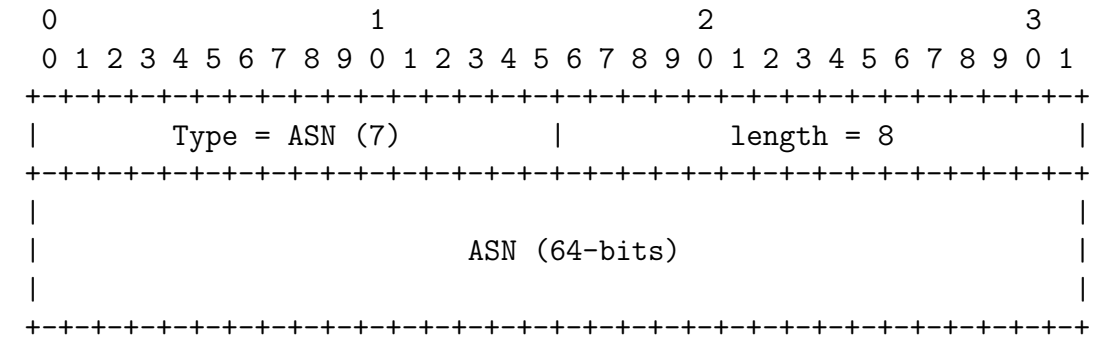
3.7 End of Frame Timestamp

The end of frame timestamp is a monotonically increasing time in nanoseconds since power on of the receiving device. This value is important to time-slotted MACs where a packet may overflow a time slot, or where there are timing constraints on the ack sent in response to a data frame.



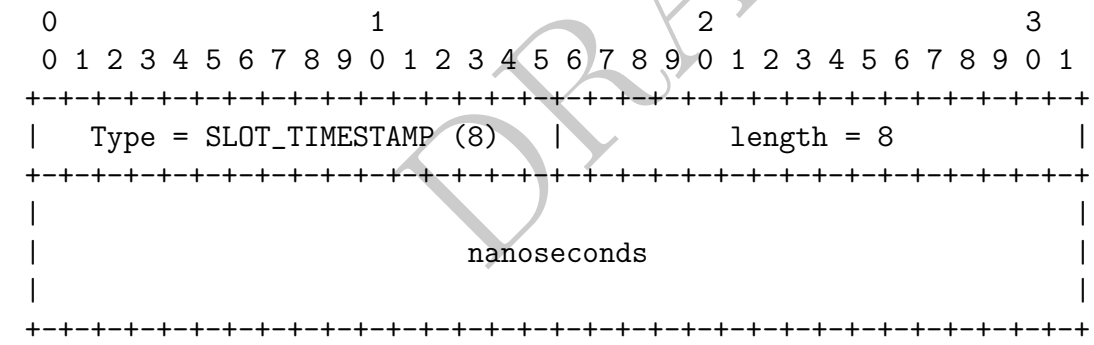
3.8 Absolute Slot Number (ASN)

For a Time-Slotted Channel Hopping MAC, the Absolute Slot Number (ASN) is a monotonically increasing number which is synchronized across all nodes on the network and forms part of the nonce for decryption.



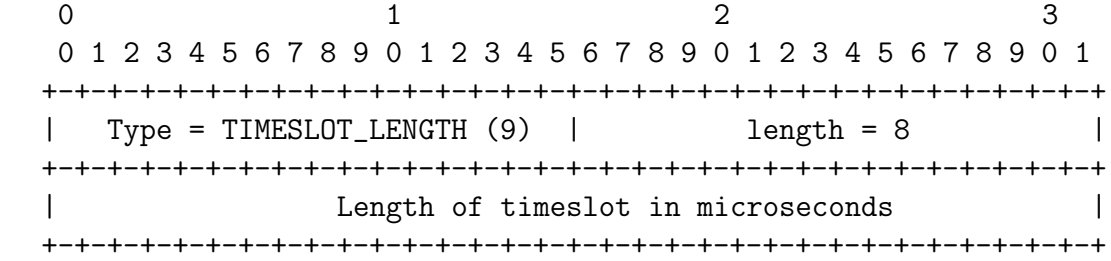
3.9 Start of Slot Timestamp

The start of slot timestamp is a monotonically increasing time in nanoseconds since power on of the receiving device. For a Time-Slotted Channel Hopping MAC, the start of slot timestamp, which preceeds the start of frame timestamp, is essential for debugging and optimizing TSCH configurations.



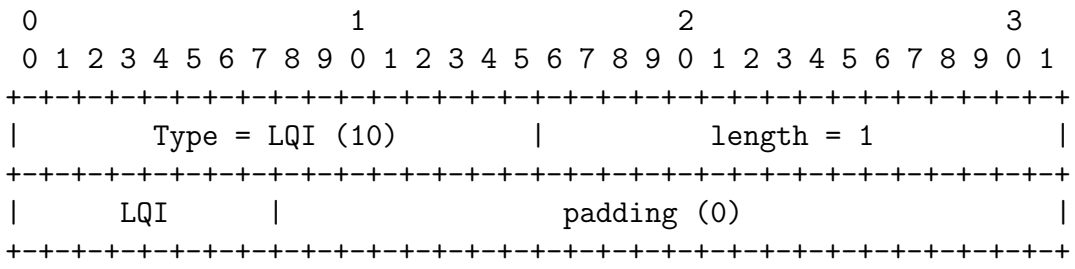
3.10 Timeslot Length

The timeslot length in a Time-Slotted Channel Hopping MAC is used for calculating the delta between end of frame and end of slot.



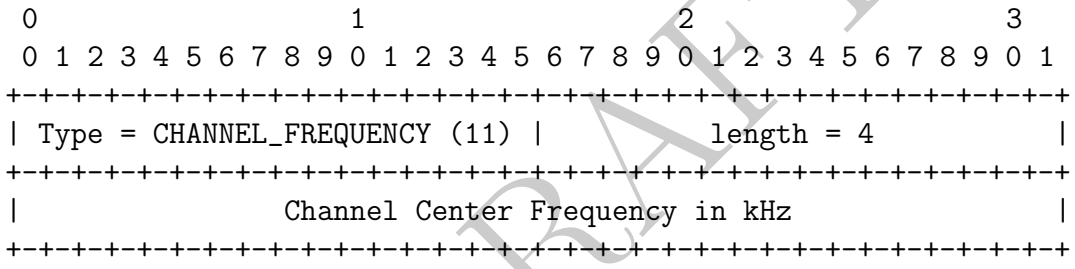
3.11 Link Quality Indicator

The Link Quality Indicator (LQI) measurement is a characterization of the strength and/or quality of the received packet. See IEEE 802.15.4-2015 10.2.6 Link quality indicator.



3.12 Channel Center Frequency

A sniffer may provide the channel center frequency of the receiver as an IEEE-754 floating point number in kHz.

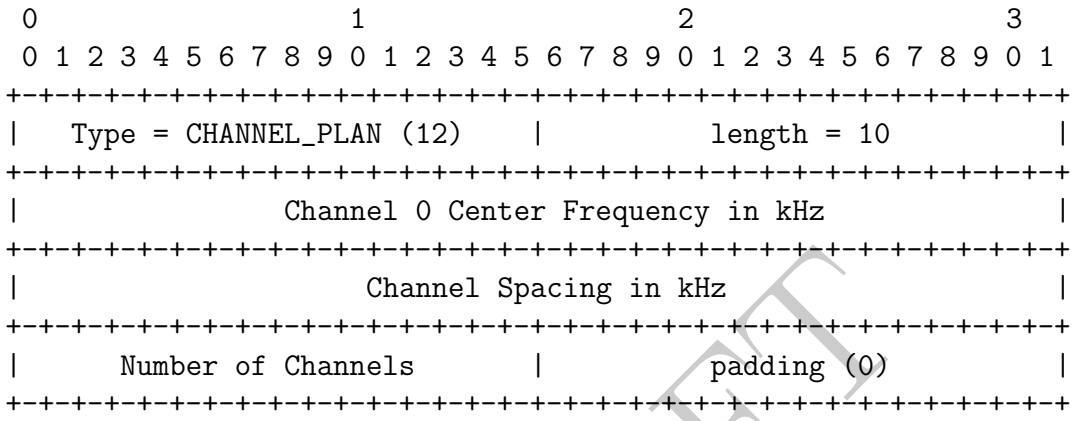


3.13 Channel Plan

A channel plan defines the channel 0 center frequency, channel spacing and number of channels. The center frequency of channel N in the channel plan is given by the following formula.

$$ChanCenterFreqN = ChanCenterFreq0 + (N \times ChanSpacing)$$

Frequency values are in kHz and encoded as an IEEE-754 floating point number.



4 Glossary

Notation	Description
CRC	Cyclic Redundancy Check
DLT	Data-Link Type
EPB	Enhance Packet Block (pcapng)
FCS	Frame Check Sequence
IDB	Interface Description Block (pcapng)
IEEE	Institute of Electrical and Electronics Engineers
LR-WPAN	Low-Rate Wireless Personal Area Network
LPWAN	Low-Power Wide Area Network
LQI	Link Quality Indicator
MAC	Medium Access Control
pcap	Packet Capture File Format [2]
pcapng	PCAP Next Generation Capture File Format [3]
PDU	Protocol Data Unit
PHY	Physical Layer
SUN	Smart Utility Network
TLV	Type-Length-Value
TSCH	Time-Slotted Channel Hopping
TVWS	Television White Space

5 References

1. Data-Link Types - https://www.tcpdump.org/linktypes.html
2. Packet Capture File Format - https://www.tcpdump.org/manpages/pcap-savefile.5.html
3. PCAP Next Generation Capture File Format - https://github.com/pcapng/pcapng

6 Contributers

The following have contributed to this spec as authors or reviewers.

Dario Tedeschi <dat[at]exegin.com>
Guy Harris <guy[at]alum.mit.edu>
James Ko <jck[at]exegin.com>
Jeremie Faucher-Goulet <Jeremie.Faucher-Goulet[at]trilliant.com>
Sandra Jessen <sdj[at]exegin.com>