MITSUBISHI ELECTRIC
Changes for the Better

802.1CBdb
Generic 2-level stream identification function

IEEE 802.1 Call

29 October, 2018

Contents

- Recall of the proposed generic 2-level stream identification scheme
- Header/payload delineation
- How to deal with encryption

Starting point

GENERIC 2-LEVEL STREAM IDENTIFICATION

MITSUBISHI ELECTRIC
Changes for the Better

The proposal

- Stream identification parameters organized in 2 groups
  - Layer-2 and Upper-Layers
    - Layer-2 group: mandatory
    - Upper-Layers group: optional
  - Minimal mandatory subset in L2 group
    - To be defined
  - Function form:

    $\{N_{L2}; (L2offset1,L2length1); [(L2offset2,L2length2); \ldots; (L2offsetN_{L2},L2lengthN_{L2})]\}$

    +

    $[\{N_{UL}; (ULoffset1,ULlength1); (ULoffset2,ULlength2); \ldots; (ULoffsetN_{UL},ULlengthN_{UL})\}]$

    $N_{L2} > n$ (n=?)

    $N_{UL} \geq 0$, ULoffset1=0

The usual base example

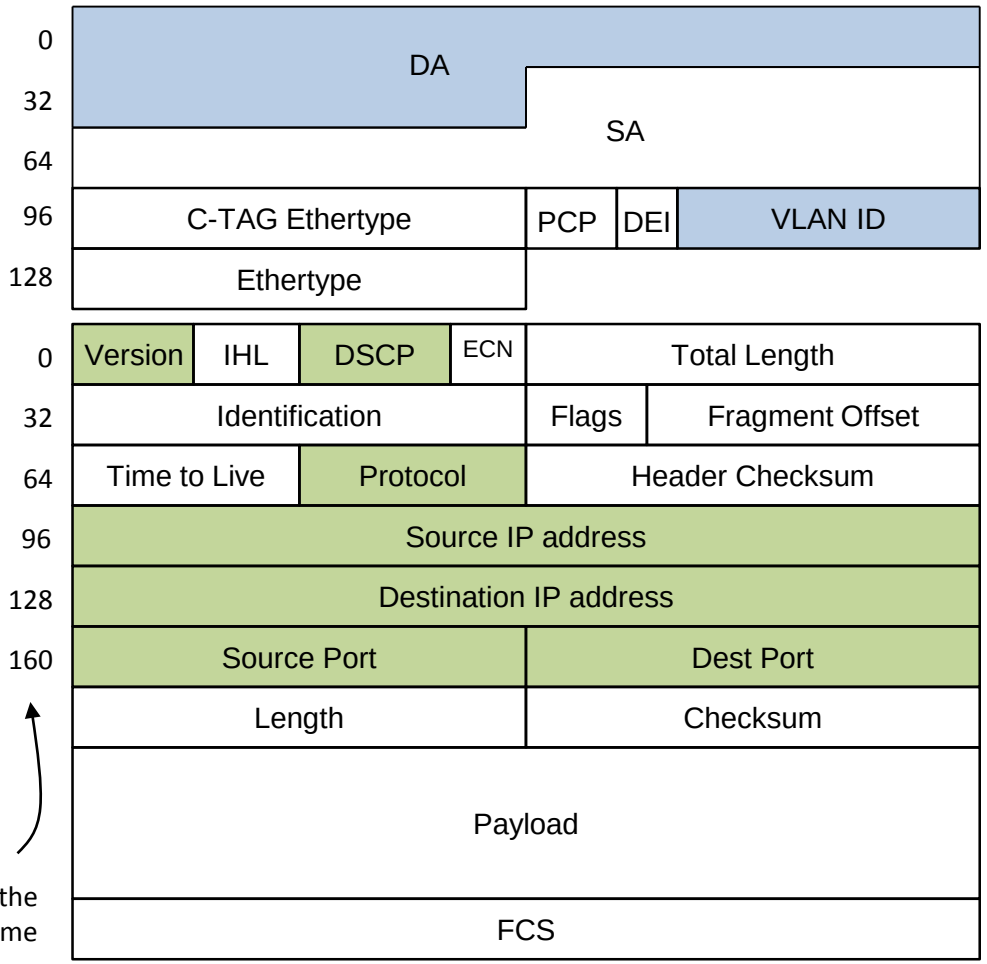
- An example of L2-UL identification:
  - Based on 802.1CB-2017's IPv4 + UDP stream identification

- L2 parameter list

```
{2;          /* Nb param */
(0,48),      /* DA */
(116,12),    /* VLAN-ID */
```

- UL parameter list

```
{7;          /* Nb param */
(0,4),       /* IP version */
(8,6),       /* DSCP field */
(72,8),      /* Protocol */
(96,32),     /* Source IP */
(128,32),    /*  Dest IP */
(160,16),    /* Source Port */
(176,16)}    /* Dest Port */
```



Last meeting discussion

- Applying mask-and-match to an Ethernet frame requires to be able to determine:
  1. the structure of the frame header
     - Series of header fields
  2. where the frame payload (Upper-layer) starts
     - Which depends on 1.

- How to deal with encryption ?
  - Layer-2 encryption
  - Upper-layer encryption

L2-UL parameters distincion

HEADER/PAYLOAD DELINEATION

MITSUBISHI ELECTRIC
Changes for the Better

Support for evolving Ethernet header

- The 2-level identification requires to be able to delineate the header and the payload of a frame
  - The Ethernet header structure can take various forms
    - Use of the Ethertype as an “escape key” to add fields the base standard Ethernet header
      - The order of the header fields is not standardized
    - Header length is variable
  - Ethertypes codes can be classified in 3 types
    - Frame length indication (Ethernet compatibility)
    - “Payload-type” indication
    - Header field indication (the “escape key”)
  - Ethertype values are independent of this classification
    - Groups of Ethertype values allocated to companies or organisations

MITSUBISHI ELECTRIC
Changes for the Better

Support for evolving Ethernet header

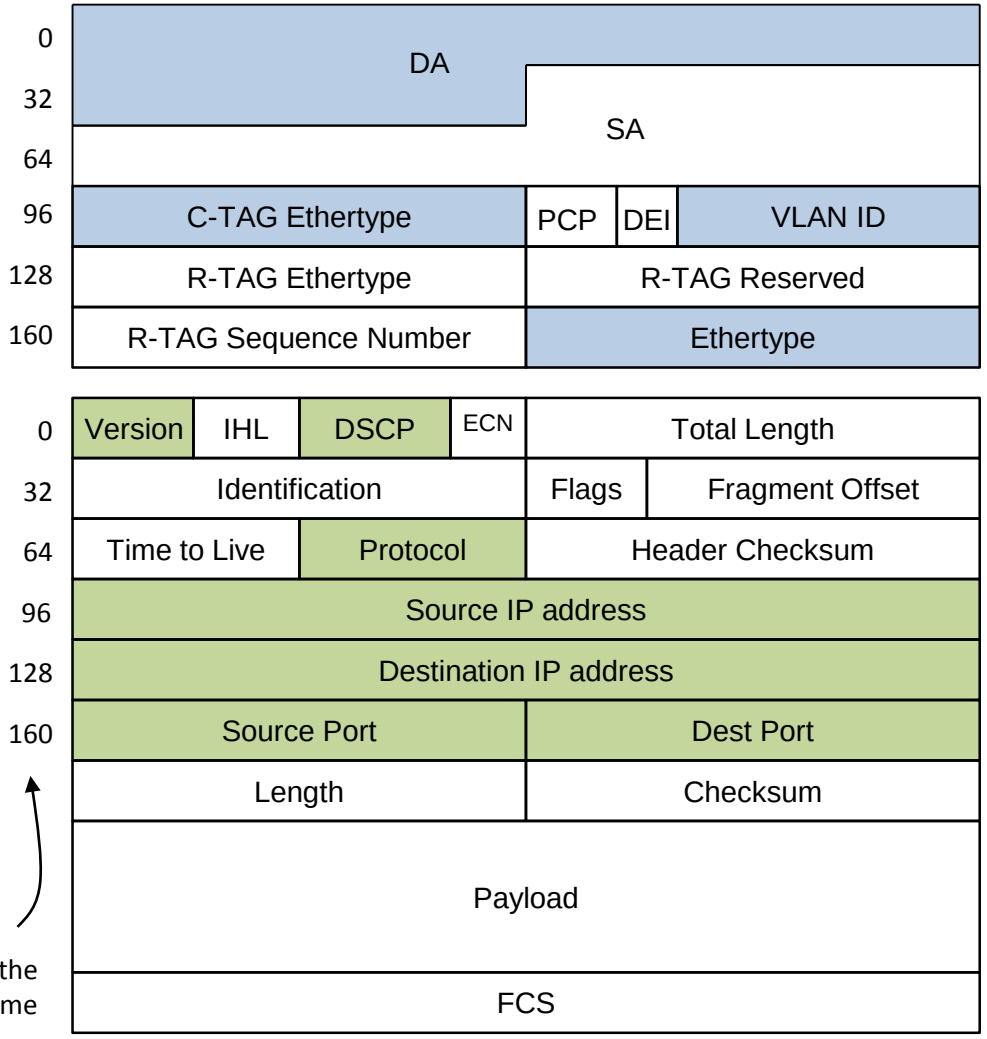
- Mask and match on the frame header
  - Parsing (looking up Ethertypes) to find the fields and hence the frame header structure
    - Limited list of recognized Ethertypes
    - Apply a mask once the header structure is known
    - … not very efficient.
  - Apply arbitrary masks (based on a set of pre-defined expected header formats)
    - Expected match value contains the value of the Ethertype to confirm the field type
    - Requires the definition of the set of pre-defined header formats

Where does the payload start ?

- Once the header format is confirmed:
  - The payload starts after the “Payload-Type” Indication” Ethertype
    - “Payload-type” Ethertype must be part of the L2 identification parameters
    - Upper-layer offset 0

Going further with the base example

- An example of L2-UL identification:
  - Expected header format:
    - VLAN-tagged
    - Redundancy-tagged
  - Expected payload:
    - IP
  - Stream identification type:
    - DA + VLAN + IPv4 + UDP



Going further with the base example

- Corresponding identification parameters:
  - L2 parameter list

```
{4;          /* Nb param */
(0,48),      /* DA */
(96,16),     /* C-TAG Ethertype */
(116,12),    /* VLAN-ID */
(176,16),    /* Ethertype */
```

  - UL parameter list

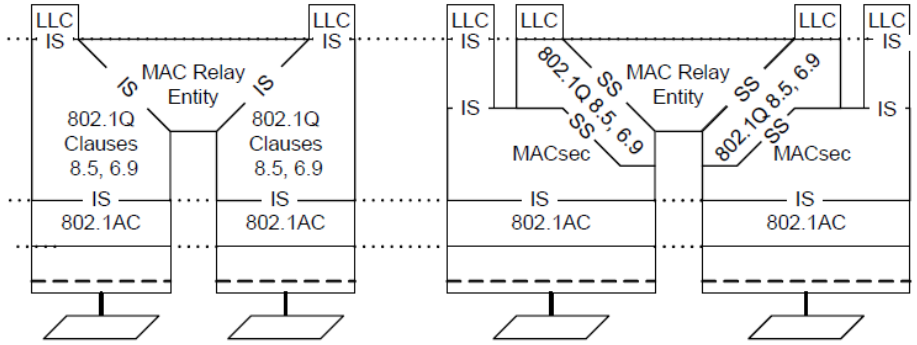
```
{7;          /* Nb param */
(0,4),       /* IP version */
(8,6),       /* DSCP field */
(72,8),      /* Protocol */
(96,32),     /* Source IP */
(128,32),    /*  Dest IP */
(160,16),    /* Source Port */
(176,16)}    /* Dest Port */
```

How to deal with encrypted frames

LAYER 2 AND UPPER LAYER ENCRYPTION

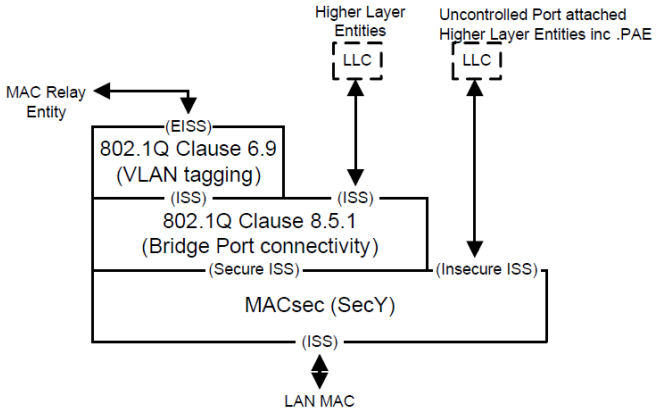
Layer-2 encryption

- MACsec in the protocol stack
  - Example: MACsec in VLAN-aware networks
    - MACsec integration in Ethernet protocol stack



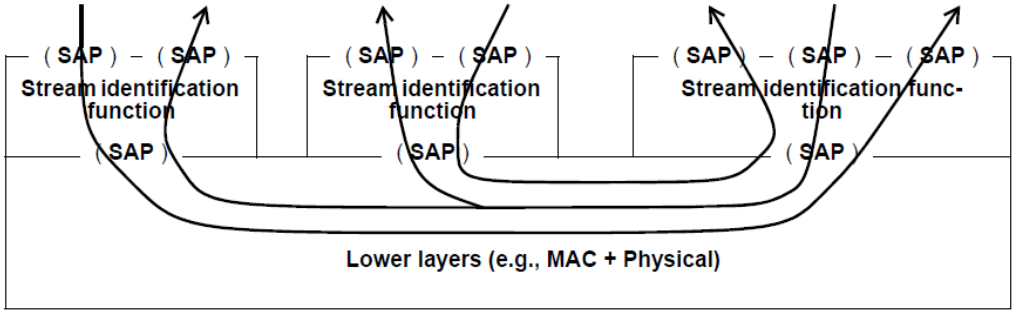
Numeric references in this figure are to 8.5 and 6.9 of IEEE Std 802.1Q-2018.

- MACsec is an “intermediate” layer above the MAC layer that offers a similar service as the MAC layer to the upper layers through a secure (protected) and an insecure (transparent) access point provided by a MACsec entity (SecY).
  - In particular, VLANs are located “on top” of MACsec

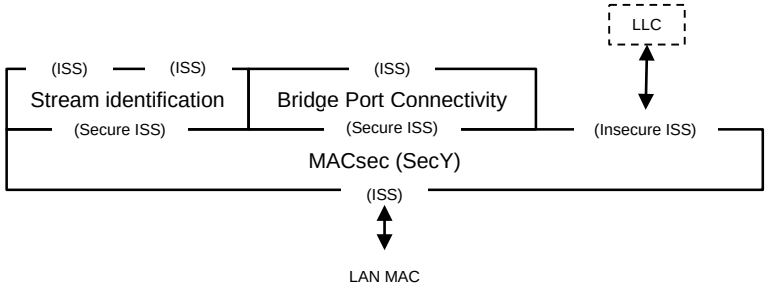


Layer-2 encryption

- Stream identification and MACsec
  - Stream identification layering follows 802.1AC:
    - “Stream identification utilizes a single Service Access Point (SAP) to a connectionless packet service offered by the layer below it [e.g., the Intermediate Sublayer Service (ISS) in 802.1AC], and offers an array of SAPs to the layers above it, corresponding to different Streams“.



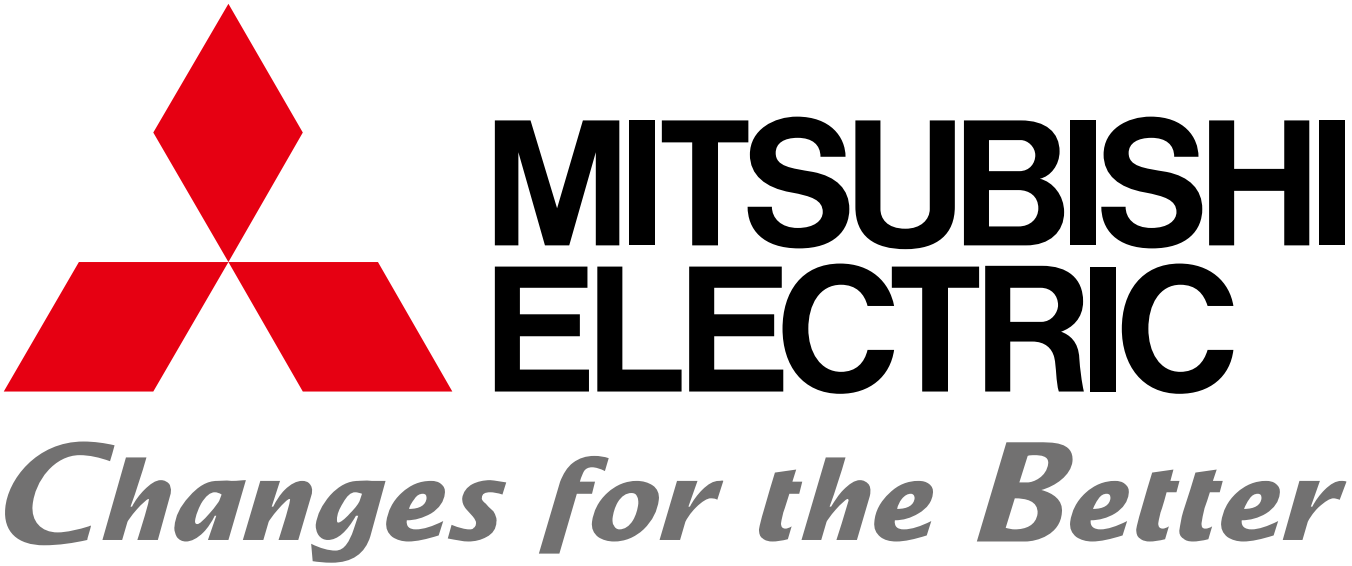
  - As a consequence, stream identification functions can be “users” of the transparent service provided by a MACsec SecY’s.



Upper-Layer encryption

- If Upper-Layer parameters are used for stream identification
- Frame payloads may be encrypted; 2 examples:
  - IPsec: Encapsulating Security Payload in Transport Mode:
    - End-to-end encryption
    - The stream correspondence has to be established prior to the payload encryption
      - Requires a mapping between the Upper-Layer-based identification and a “pure” Layer-2 stream (using L2 parameters only)
        - » Use of active stream identification to encapsulate the original stream into a L2-identified stream (i.e. with MAC addresses + VLAN-ID)
  - OPC UA: PubSub over TSN
    - L2 and OPC UA addressing/communication identification are tightly intricated
      - no real problem: stream identification is embedded in OPC UA PubSub over TSN
        - » Unique StreamId for a Publisher WriterGroup Subscriber DataSetReader NetworkMessages exchange.
    - Stream identification based on DestMAC + VLAN-ID

Thank you for your attention


MITSUBISHI
ELECTRIC
Changes for the Better