IEEE 802.1 Security
MACsec Privacy YANG Update
Rational for decisions in YANG

Don Fedyk – don.Fedyk@labn.net

Disclaimer

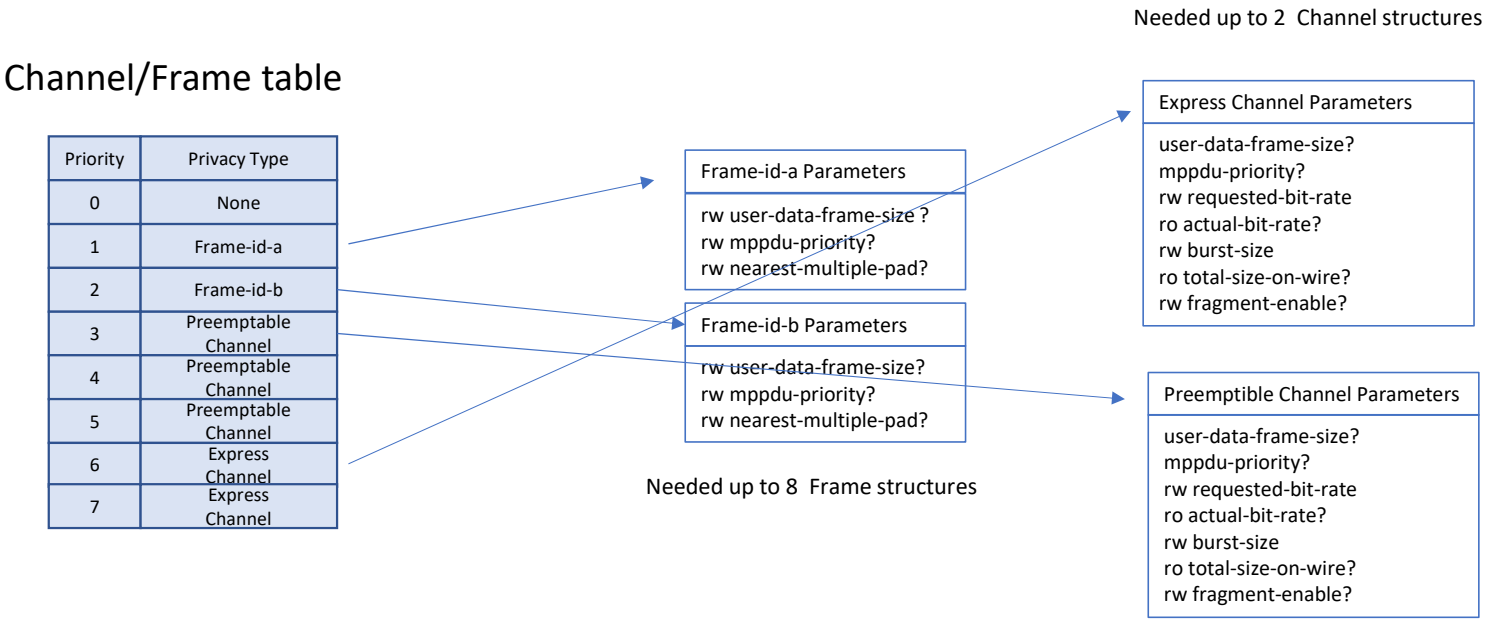
- This is a work in progress. The material here is for discussion purposes and may contain errors.

Changes to YANG from Comments on 02 Ballot

- Table Restructure
- YANG identities
- Some Xpath checks

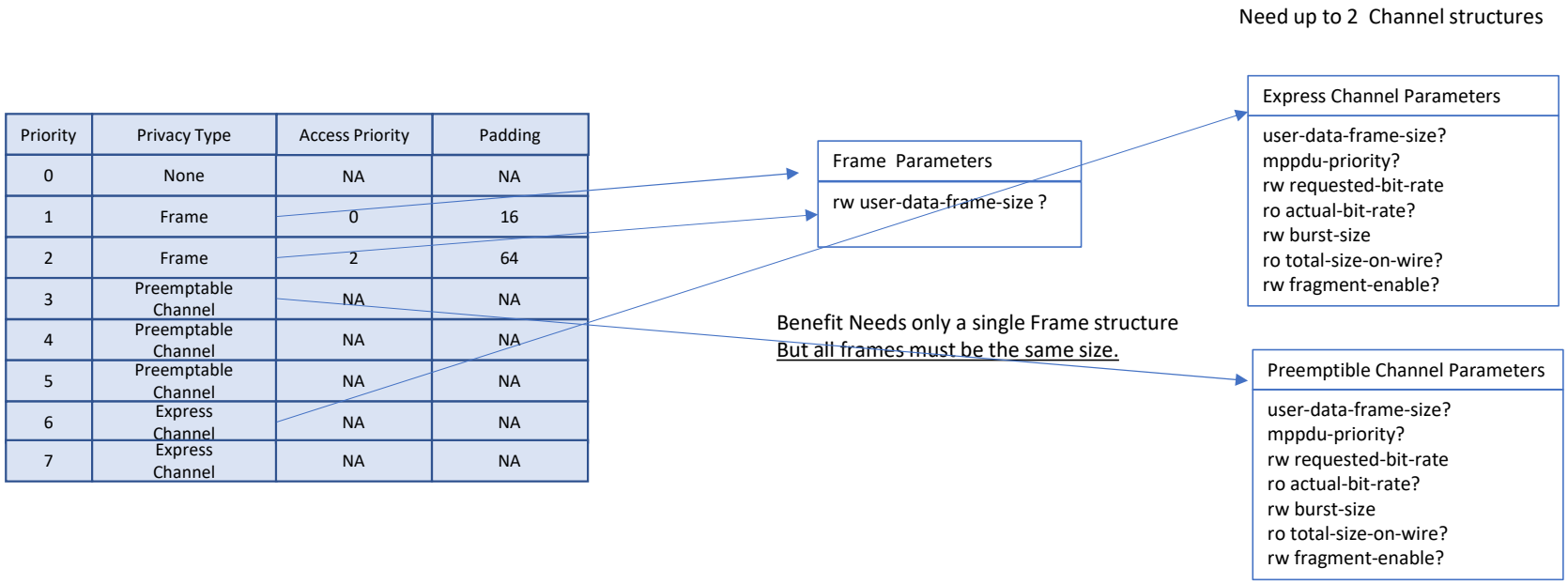
Structure in the 07 Draft

- It was discussed we have coupled the structure of YANG and the table 17-3
- Note text should talk about Table context not YANG structures.



Restructure Change Request by Draft comments

- It was discussed we have coupled the structure of YANG and the table 17-3
- While not independent the aspects of YANG are intertwined in the Table.



Why are the indexed Tables Base on lists?

- YANG uses lists with indexes as a free format table.
- Therefore, for a two-dimensional array with priority as an index uses two leafs (elements)

```
+--rw user-priority-to-pry* [user-priority]
   |  +--rw user-priority          uint8
   |  +--rw privacy-type           identityref
```

- A larger array simply adds leafs to the list. (Note leafs with ? Are optional)

```
+--rw user-priority-to-pry* [user-priority]
   |  +--rw user-priority          uint8
   |  +--rw privacy-type           identityref
   |  +--rw frame-access-priority?   dot1q-types:priority-type
   |  +--rw frame-de-bit-visible?    enumeration
   |  +--rw nearest-multiple-pad?    uint16
```

Why use Identities?

- RFC 7950 “The "identity" statement is used to define a new globally unique, abstract, and untyped identity. The identity's only purpose is to denote its name, semantics, and existence. An identity can be either defined from scratch or derived from one or more base identities.”

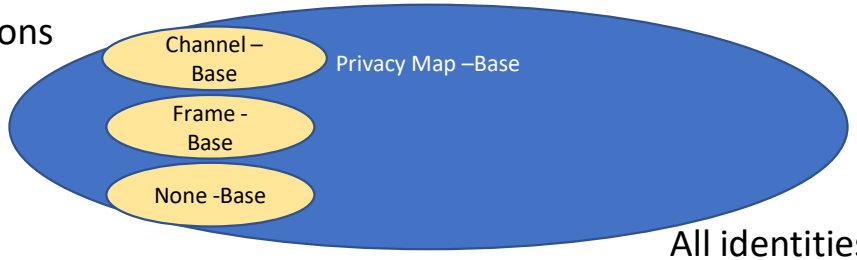
Using Identities we can refer to channel, frame or None or to all by the choice of identity base. (Or a Union) Internally the identity can be represented by 4 values in this case.

Benefit Allows input restrictions without heavy semantics or xpath checks. You cannot configure a Frame identity with channel characteristics, but you can use all three identities in the table lookup by referring to the common base.

Channel only operations

Frame only operations

Non only operations



All identities used for Lookup

Enums Vs Identities

Couldn't you use an Enumeration?

- Yes but Enums have an explicit value that is not required
  - Also, you need additional restrictions if you reuse the Enums – or need to create additional identifiers.

Aren’t Enumerations better mapped to MIBs ?

- Our goal is to utilize YANG and provide MIBs that are compatible but not constrain the YANG by MIB limitations.

Identity Alternative Reference Pointers

- YANG also has Reference to Leafs as a way to link components.
- References require leafs for the detiatnion(they are effectively pointers)
- Due to the nature of channels the fact that we have one or two makes Reference pointers unattractive.
- Reference pointers are ultimatel more bulky than identities.

Input checking

- Input variables can be constrained by YANG or by the Server when processing the YANG (Netconf, Restconf etc).
- Simply constraints are easy and should be encoded in YANG.
- Complex xpath constraints should be used judiciously or not at all.
- Since the table defines optional type channels/frames xpath can key off the defined types. But don’t go overboard.
- Identities can provide input constraint based on the base of the identity. A frame identity cannot be used for channels but both frame and cahnnels can be used when used as lookup identities. This is merely a YANG user input constraint – it has no bearing on the underlying structure.

Xpath Checks that make sense

```
leaf frame-access-priority {
   when "../dot1ae-pry:privacy-type='dot1ae-pry:frame'";
   type dot1q-types:priority-type;
     description
       "Access Priority of the frames that are mapped to
        the Frame table";
     reference
       "20.13.6.2, 20.13.7.2 of IEEE 802.1AEdk";
   }
   leaf frame-de-bit-visible {
     when "../dot1ae-pry:privacy-type='dot1ae-pry:frame'";
     type enumeration {
       enum hidden {
         value 0;
       }
       enum visible {
         value 1;
       }
    }
```

Only allow setting priority and DE bit capability etc. when a Privacy Frame has been configured for this instance – easily handled and prevents errors.

Xpath Checks that make less sense

The attributes for channels are defined in a structure that could also check the existence of the definition of any channel types.

```
choice channels {
   when "../dot1ae-pry:privacy-type='dot1ae-pry:express-channel'" +
     " or "../dot1ae-pry:privacy-type='dot1ae-pry:preeemptable-channel";
```

While this is like the previous case if the channel is removed in the priority lookup table all the associated config must be removed. It might be the case someone wants to test the difference between channels and frames, and this would be annoying to lose all the channel config when the structure is unlinked temporarily.
It is ok to have an unlinked structure.

Other

- Express Privacy Frames and Preemptable Privacy frames typically share a single channel.
- We currently have separate channels for preemptable and express and stipulate if only one is defined, both preemptable and express share the single channel (express or preemptable).
- An explicit choice statement could make this more explicit. The choice would be single combined or separate express and preemptable both must be configured.
- Functionally there would be no difference but the intent in YANG would be clearer.

Proposed Explicit Channel Control

```
choice channels {
  container one-channel {
    description
      "Case for One combined channel";
     uses channel-grouping;
  }
  container two-channels {
    description
      "Case for two channels one for express and one for
       preemptable channel";
    list channel {
     key "channel-id";
     min-elements 2;
     max-elements 2;
      description
        "List of Channels supported with their corresponding
         per channel configuration Note both channles are
         forced to be configured";
      reference
        "20.13.6 of IEEE 802.1AEdk";
      leaf channel-id {
        type identityref {
          base channel-identity;
        }
      }
      uses channel-grouping;
    }
  }
}
```

Up until now we have had a list where 0, 1, 2 entries could be defined.
Here this logic forces the config to one channel (not identified as express or preemptable) or two channels explicitly identified as express or preemptable (reusing the same identity in the priority mapping table but scoped to channels).

New Proposed YANG

```
module: ieee802-dot1ae-pry
  augment /if:interfaces/if:interface:
    +--rw pry {macsec-priv}?
       +--rw mac-privacy-enabled?          boolean
       +--ro pry-source-address?           ieee:mac-address
       +--rw use-pae-dest-address?         boolean
       +--rw pry-destination-address?      ieee:mac-address
       +--rw user-priority-to-pry* [user-priority]
       |  +--rw user-priority              uint8
       |  +--rw privacy-type               identityref
       |  +--rw frame-access-priority?     dot1q-types:priority-type
       |  +--rw frame-de-bit-visible?      enumeration
       |  +--rw nearest-multiple-pad?      uint16
       +--rw (channels)?
       |  +--:(one-channel)
       |  |  +--rw one-channel!
       |  |     +--rw access-priority?
       |  |     |     dot1q-types:priority-type
       |  |     +--rw user-data-frame-size?   uint16
       |  |     +--rw requested-bit-rate      uint64
       |  |     +--ro actual-bit-rate?        uint64
       |  |     +--rw burst-size              uint32
       |  |     +--ro total-size-on-wire?     uint16
       |  |     +--rw fragment-enable?        boolean
       |  +--:(two-channels)
       |     +--rw two-channels!
       |        +--rw channel* [channel-id]
       |           +--rw channel-id              identityref
       |           +--rw access-priority?
       |           |     dot1q-types:priority-type
       |           +--rw user-data-frame-size?   uint16
       |           +--rw requested-bit-rate      uint64
       |           +--ro actual-bit-rate?        uint64
       |           +--rw burst-size              uint32
       |           +--ro total-size-on-wire?     uint16
       |           +--rw fragment-enable?        boolean
       +--rw privacy-frame!
       |  +--rw user-data-frame-size?   uint16
       +--ro out-mppdus?                       yang:counter64
       +--ro out-user-frames?                  yang:counter64
       +--ro out-user-octets?                  yang:counter64
       +--ro out-pad-octets?                   yang:counter64
       +--ro out-user-fragments?               yang:counter64
       +--ro in-mppdus?                        yang:counter64
       +--ro in-errored-mppdus?                yang:counter64
       +--ro in-user-frames?                   yang:counter64
       +--ro in-errored-user-frames?           yang:counter64
       +--ro in-user-octets?                   yang:counter64
       +--ro in-pad-octets?                    yang:counter64
       +--ro in-user-complete-fragments?       yang:counter64
       +--ro in-user-dropped-fragments?        yang:counter64
       +--ro in-user-errored-fragments?        yang:counter64
```

Either one or two
When two: both channels must be configured and express or preemptable is called out.

Old draft 0.7 Yang.

```
module: ieee802-dot1ae-pry

  augment /if:interfaces/if:interface:
    +--rw pry {macsec-priv}?
       +--rw mac-privacy-enabled?          boolean
       +--ro pry-source-address?           ieee:mac-address
       +--rw use-pae-dest-address?         boolean
       +--rw pry-destination-address?      ieee:mac-address
       +--rw user-priority-to-pry* [user-priority]
       |  +--rw user-priority    uint8
       |  +--rw privacy-type?    union
       +--rw privacy-channel* [channel-id]
       |  +--rw channel-id              identityref
       |  +--rw user-data-frame-size?   uint16
       |  +--rw mppdu-priority?         dot1q-types:priority-type
       |  +--rw requested-bit-rate?     uint64
       |  +--ro actual-bit-rate?        uint64
       |  +--rw burst-size?             uint32
       |  +--ro total-size-on-wire?     uint16
       |  +--rw fragment-enable?        boolean
       +--rw privacy-frame* [frame-id]
       |  +--rw frame-id                identityref
       |  +--rw user-data-frame-size?   uint16
       |  +--rw mppdu-priority?         dot1q-types:priority-type
       |  +--rw nearest-multiple-pad?   uint16
       +--ro out-mppdus?                   yang:counter64
       +--ro out-user-frames?              yang:counter64
       +--ro out-user-octets?              yang:counter64
       +--ro out-pad-octets?               yang:counter64
       +--ro out-user-fragments?           yang:counter64
       +--ro in-mppdus?                    yang:counter64
       +--ro in-errored-mppdus?            yang:counter64
       +--ro in-user-frames?               yang:counter64
       +--ro in-errored-user-frames?       yang:counter64
       +--ro in-user-octets?               yang:counter64
       +--ro in-pad-octets?                yang:counter64
       +--ro in-user-complete-fragments?   yang:counter64
       +--ro in-user-dropped-fragments?    yang:counter64
```

Allowed one or two
When two both channels
Must be configured.

Sample Yanglint Validation One Channel

```
"ieee802-dot1ae-pry:pry": {
        "mac-privacy-enabled": true,
        "use-pae-dest-address": false,
        "pry-source-address": "11-22-33-44-55-66",
        "pry-destination-address": "11-22-33-44-55-66",
        "user-priority-to-pry": [
          {
            "user-priority": 0,
            "privacy-type": "none"
          },
          {
            "user-priority": 1,
            "privacy-type": "frame",
            "frame-access-priority": 1,
            "frame-de-bit-visible": "visible",
            "nearest-multiple-pad": 16
          },
          {
            "user-priority": 2,
            "privacy-type": "frame",
            "frame-access-priority": 1,
            "frame-de-bit-visible": "hidden",
            "nearest-multiple-pad": 64
          },
          {
            "user-priority": 3,
            "privacy-type": "express-channel"
          },
          {
            "user-priority": 4,
            "privacy-type": "express-channel"
          },
          {
            "user-priority": 5,
            "privacy-type": "preemptable-channel"
          },
          {
            "user-priority": 6,
            "privacy-type": "preemptable-channel"
          },
          {
            "user-priority": 7,
            "privacy-type": "preemptable-channel"
          }
        ],
        "one-channel": {
          "access-priority": 3,
          "user-data-frame-size": 1518,
          "requested-bit-rate": "10000000000",
          "actual-bit-rate": "9705882352",
          "total-size-on-wire": 1520,
          "burst-size": 10000,
          "fragment-enable": true
        },
        "privacy-frame": {
          "user-data-frame-size": 1518
        }
      },
```

Sample Yanglint Validation Two Channel


```
"ieee802-dot1ae-pry:pry": {
      "mac-privacy-enabled": true,
      "use-pae-dest-address": false,
      "pry-source-address": "11-22-33-44-55-66",
      "pry-destination-address": "11-22-33-44-55-66",
      "user-priority-to-pry": [
        {
          "user-priority": 0,
          "privacy-type": "none"
        },
        {
          "user-priority": 1,
          "privacy-type": "frame",
          "frame-access-priority": 1,
          "frame-de-bit-visible": "visible",
          "nearest-multiple-pad": 16
        },
        {
          "user-priority": 2,
          "privacy-type": "frame",
          "frame-access-priority": 1,
          "frame-de-bit-visible": "hidden",
          "nearest-multiple-pad": 64
        },
        {
          "user-priority": 3,
          "privacy-type": "express-channel"
        },
        {
          "user-priority": 4,
          "privacy-type": "express-channel"
        },
        {
          "user-priority": 5,
          "privacy-type": "preemptable-channel"
        },
        {
          "user-priority": 6,
          "privacy-type": "preemptable-channel"
        },
        {
          "user-priority": 7,
          "privacy-type": "preemptable-channel"
        }
      ],
      "two-channels": {
        "channel": [
          {
            "channel-id": "express-channel",
            "access-priority": 3,
            "user-data-frame-size": 1518,
            "requested-bit-rate": "10000000000",
            "actual-bit-rate": "9705882352",
            "total-size-on-wire": 1520,
            "burst-size": 10000,
            "fragment-enable": true
          },
          {
            "channel-id": "preemptable-channel",
            "access-priority": 4,
            "user-data-frame-size": 1518,
            "requested-bit-rate": "10000000000",
            "actual-bit-rate": "9705882352",
            "total-size-on-wire": 1520,
            "burst-size": 10000,
            "fragment-enable": true
          }
        ]
      },
      "privacy-frame": {
        "user-data-frame-size": 1518
      }
```

Comments?
Thank You