IEEE 802.1AE (MacSec) & IEEE 802.1Qbb (PFC)

Authors: **Hesham ElBakoury**

Version: 1.0

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

Objectives

- Provides Quick overview of MACSec (IEEE 802.1AE)
- Discuss the impact of IEEE 802.1AE (MacSec) on the operation of IEEE 802.1Qbb (Per-Priprity Flow Control – PFC)

Agenda

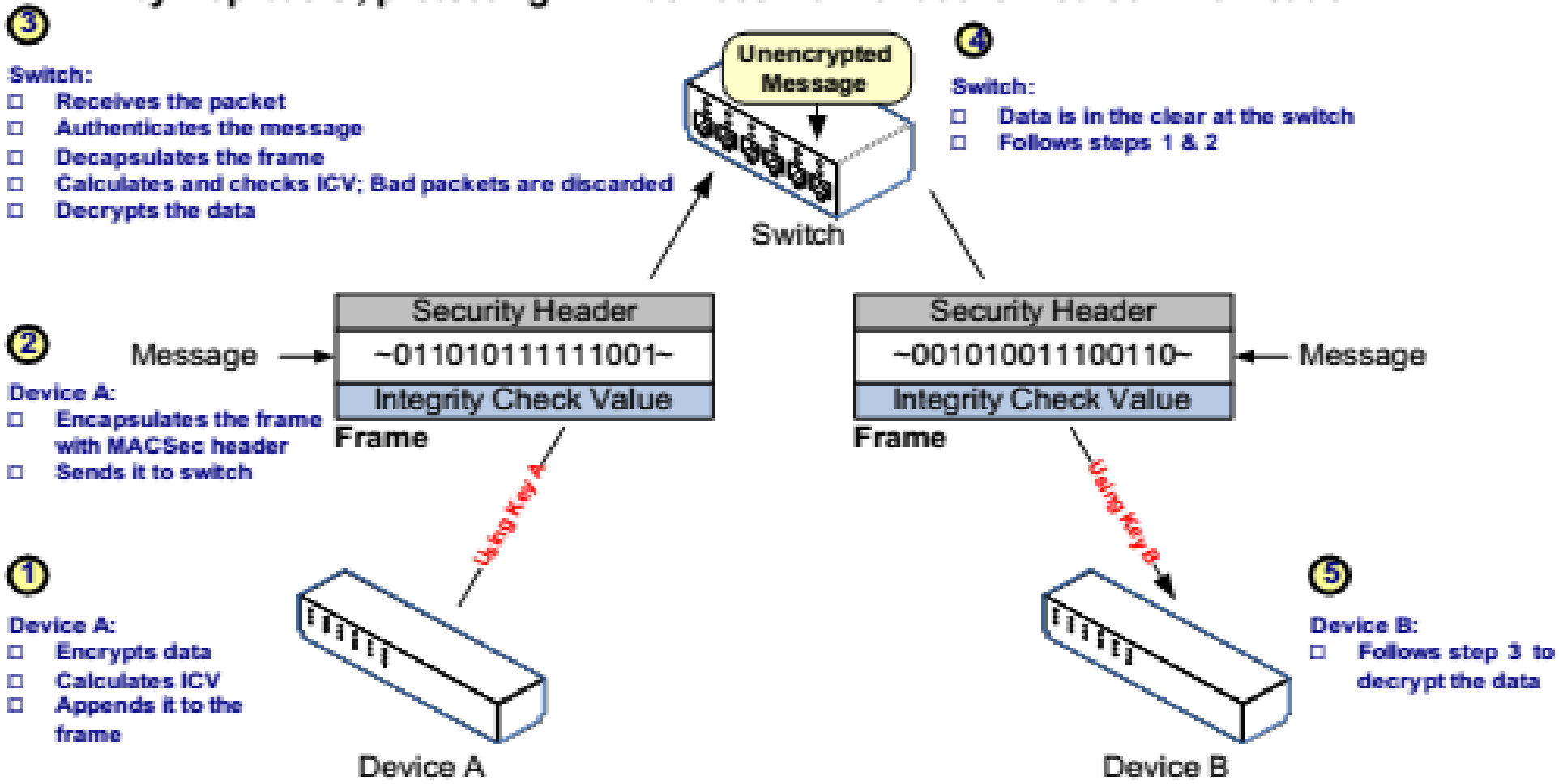
- **What is MACSec ?**
- **How MACSec Works ?**
- **MACSec Frame Format**
- **MACSec & IEEE 802.1Qbb (PFC)**
  - PFC & MACSec Layering Diagram
  - Encryption of PFC MAC Control Frames.
  - PFC Timing Considerations when MACSec is used

What is MACSec – IEEE 802.1AE

- MACSec defines the layer 2 security protocols that provide origin authentication, data integrity checking, and data confidentiality. It defines a frame format that includes data encapsulation, encryption, and authentication.

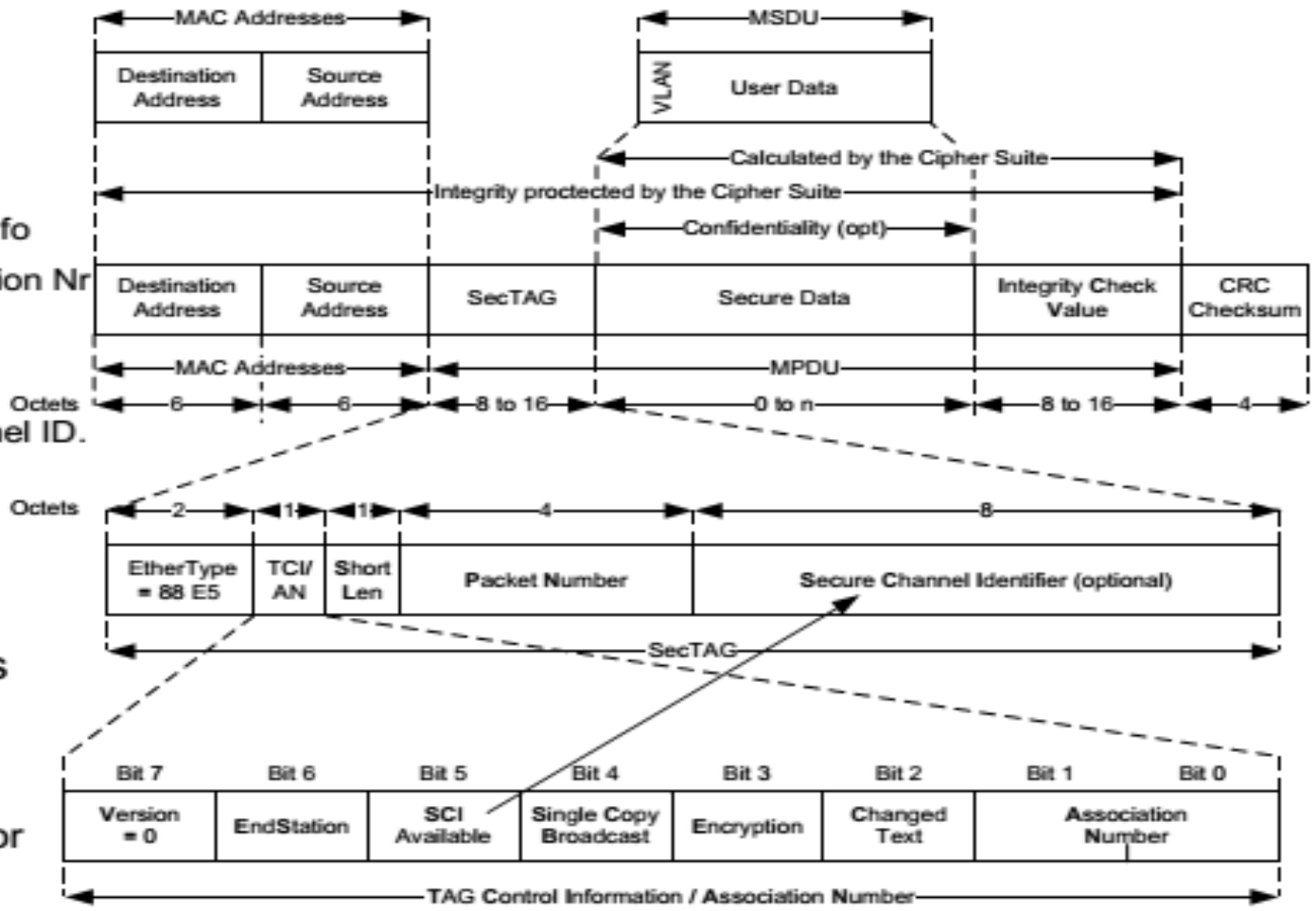
How MACSec Works

802.1AE Media Access Control Security (MACSec) secures traffic on a hop-by-hop basis, protecting LAN devices from unauthorized communication.

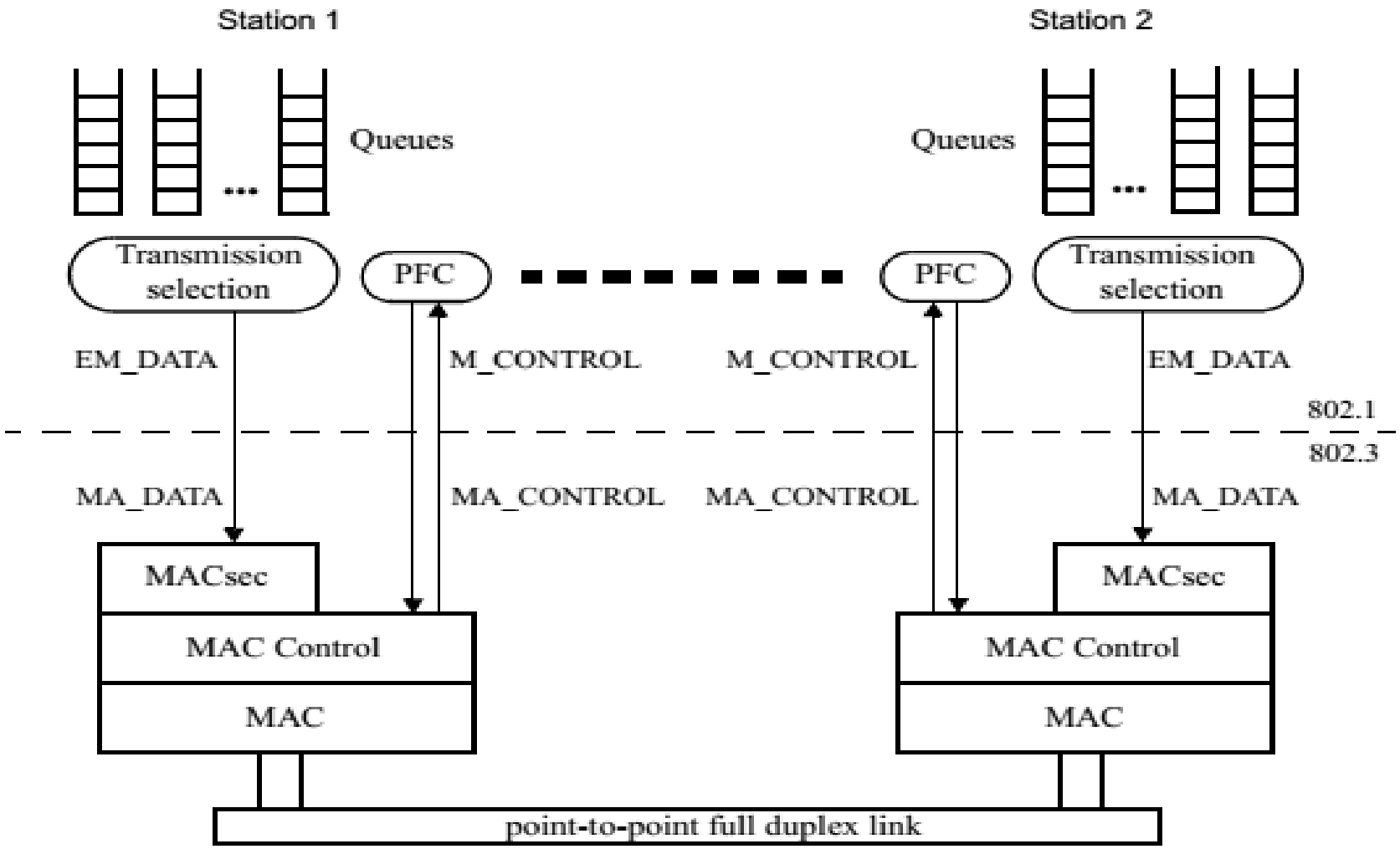


MACSec Frame Format

- Integrity protects
  - Destination address
  - Source Address
  - Security tag
    - Ethertype 0x88E5
    - TCI: Tag Control Info
    - AN: Chan.Association Nr
    - SL: Short Length
    - PN: Packet Nr
    - SCI: Secure Channel ID.
  - Secure data
    - Encrypted payload
  - Adds an ICV
- Confidentiality protects
  - User data
    - Encrypted payload
  - including VLAN tag for 802.1Q



MACSec & PFC


Station 1
Station 2
Queues
Queues
Transmission selection
PFC
PFC
Transmission selection
EM_DATA
M_CONTROL
M_CONTROL
EM_DATA
802.1
802.3
MA_DATA
MA_CONTROL
MA_CONTROL
MA_DATA
MACsec
MAC Control
MAC
MACsec
MAC Control
MAC
point-to-point full duplex link

IEEE 802.1AE Clause 6.10

- MACsec does not provide guarantees for frames, known as MAC control frames, that are internal to the operation of a particular media access method and cannot defend against abuses that use or affect such frames. MAC control frames are not forwarded by MAC Bridges, so attacks that exploit them can be localized to particular LANs.
- NOTE—Where, within the operation of a particular media access control method, it is possible to establish secure Connectivity Associations (CAs) prior to performing certain control functions, those functions should be supported by frames transmitted using an instance of the ISS. The parameters of those frames can then be protected by MACsec, and the scope for abuse restricted. It is nota requirement of the Open Systems Interconnection (OSI) layer model (ISO 7498) that management and control of a particular layer be carried out purely within that layer by protocols whose identifiers and formats are specific to that layer. For example SNMP can be used to manage MAC Bridges.

PFC Request Processing

- Upon receipt of a PFC M_CONTROL.indication, the PFC Receiver programs up to eight separate timers, each associated with a different priority, depending on the priority_enable_vector.
- For each bit in the priority_enable_vector that is set to one, the corresponding timer value is set to the corresponding time value in the time_vector parameter.
- Priority_Paused[n] is set to TRUE when the corresponding timer value (i.e., priority_timer[n]) is nonzero.
- Priority_Paused[n] is set to FALSE when the corresponding timer value (i.e., priority_timer[n]) counts down to zero.
- A time value of zero in the time_vector parameter has the same effect as the timer having counted down to zero.
- If PFC is not enabled for priority n then a request with timer value other than zero should not be generated and if such request is received then the time parameter is ignored.

Timing Considerations (1) – IEEE 802.1Q 36.1.3.3

- For effective flow control on a point-to-point full duplex link, it is necessary to place an upper bound on the length of time that a device can transmit data frames after receiving a PFC M_CONTROL.indication with e[n] set to one in priority_enable_vector and a nonzero time[n] in the time_vector operands.
- If MACsec is not supported, a queue shall go into paused state in no more than 614.4 ns since the reception of a PFC M_CONTROL.indication that paused that priority. This delay is equivalent to 12 pause quanta (i.e., 6144 bit times) at the speed of 10 Gb/s, 48 pause quanta (i.e., 24576 bit times) at the speed of 40 Gb/s, and 120 pause quanta (i.e., 61440 bit times) at the speed of 100 Gb/s.

Timing Considerations (2) – IEEE 802.1Q 36.1.3.3

- If MACsec is used, a queue shall go into paused state in no more than 614.4 ns + 'SecYtransmit delay' (see Table 10-1 of IEEE Std 802.1AE) since the reception of a PFC M_CONTROL.indication that paused that priority. The 'SecY transmit delay' is defined as the wire transmit time for a maximum sized MPDU + 4 times the wire transmit time for 64 octet MPDUs. For a 2 000 bytes frame the 'SecY transmit delay' is 8*(2 000+20) + 8*4*(64+12+4+20) = 19 360 bit times.
- NOTE—19 360 bit times is an appropriate value for 'SecY transmitdelay' for speeds up to 10 Gb/s. Support for the speeds of 40 Gb/s and 100 Gb/s can require a higher value

THANK YOU

IEEE 802.1Qbb Worst Case Delay Scenario