Discussion of Ethernet Link Security for Inter-Datacenter Interconnection

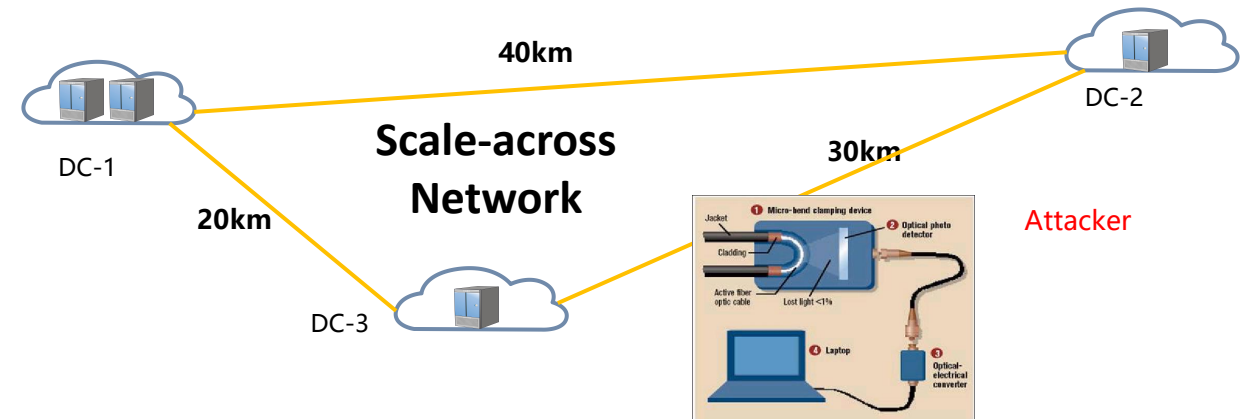Weiqiang Cheng, China Mobile

Haojie Wang, China Mobile

Topics

- Overview
- Requirements
- Gap Analysis
- Proposal

Overview

- This topic has been presented in Nendica to gather more interest and feedback.
  - In 2025, the proposals (802.1-25-0010, 802.1-25-0014) introduces a coherent physical layer security solution for inter-datacenter, which employs the AES-GCM.
- **This topic involve both knowledge of Ethernet physical layer and security**. It has been recommended that the presentation could be delivered within the 802.1 Security TG, with participation from 802.3 experts invited for discussion.
- This contribution intends to:
  - **Discussing the security requirements of inter-datacenter links.**
  - introducing the overall framework of potential physical-layer solution including **Data Plane of Confidentiality, Integrity and Data Origin Authentication, and Control Plane of Authentication, key agreement, port control, and etc**.
  - We aim to explore this topic and its feasibility for standardization within the 802.1 Security TG.

Security Requirements on inter-Datacenter Links

- **Scenario:** With the introduction of the scale-across concept for multi-AI cluster interconnectivity in the second half of 2025 (NVIDIA, Spectrum-XGS Ethernet), inter-datacenter(DC) interconnect based on long-haul coherent Ethernet technologies have garnered widespread attention.

- **Issues:** Massive data of AI/ML application over inter-DC links is valuble and privacy-sensitive[1]. These valuable data become potential eavesdropping targets over inter-DC links. Attackers can intercept optical signals and acquire sensitive data by bending optical fibers, posing a threat to the security and privacy of inter-DC links exposed to the open physical environment[2].

- **Requirement:** Security of inter-DC links should be mandatory.

- **Current Solutions**: The possible methods used to protect data of inter-DC links include MACsec, etc.

40km

DC-2

Scale-across Network

30km

DC-1

20km

Attacker

DC-3

[1]. Security risk assessment within hybrid data centers: A case study of delay sensitive applications
[2]. Eavesdropping G.652 vs. G.657 fibres: a performance comparison

Gap Analysis of Current Solutions

① MACsec will expand the Ethernet frames due to the addition of Security Tag + ICV (32 Bytes).
  - The addition in the frame will expend extra bandwidth. Taking the 64-byte frame as an example, the ratio of bandwidth overhead will exceed 30% (=32/(32+64)).
  - Considering the uncertainty of frame lengths in actual networks, bandwidth resources for security are typically provisioned for the worst-case scenario (64bytes). Thus, over 30% additional bandwidth need be allocated in advance.

② Deploying MACSec on pluggable optical modules poses challenges.
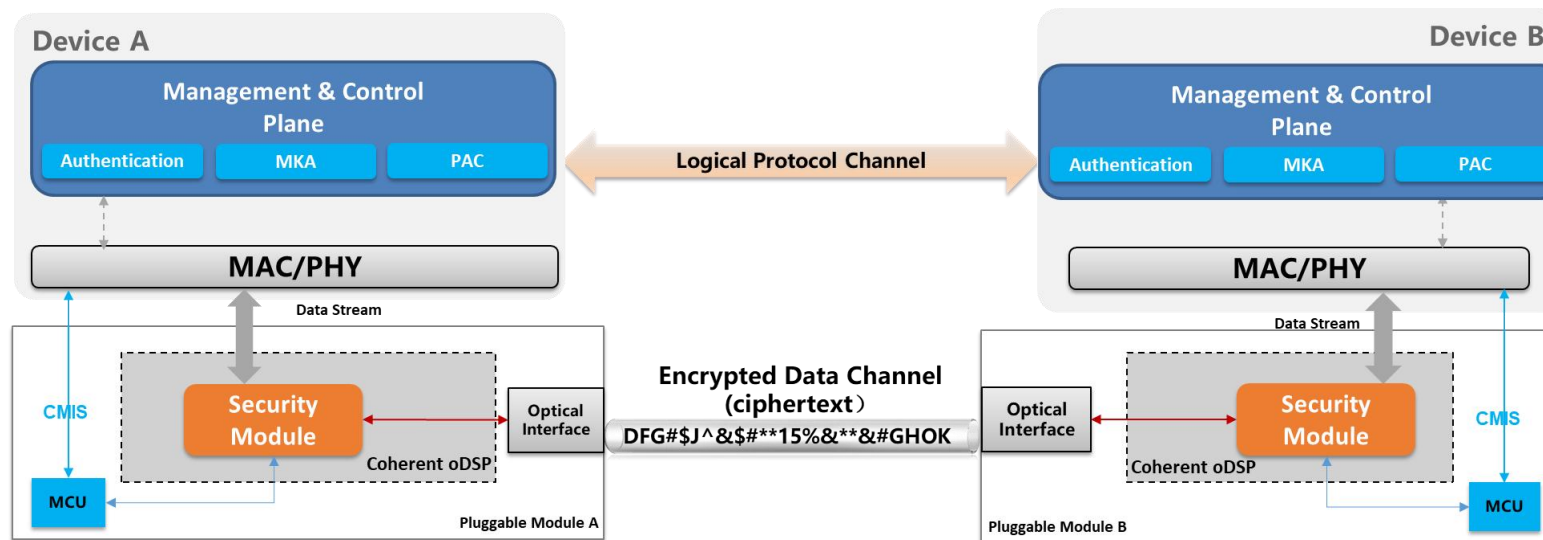 The requirement to implement encryption within pluggable optical modules has emerged with the advantage of easy deployment. This generally requires the implementation of the entire PHY stack back-to-back within oDSP for MACsec.

③ MACSec can not provide a protection of all frames.
  - Unable to provide protection for Ethernet control frames (e.g., PFC, LLDP, BPDU, …) and Ethernet packet characteristics.
  - Pause or Priority Flow Control (PFC) Mechanisms are important for congestion control in AI/ML application, and maybe potentially used to attack data processing. Although 802.1Qdt is formulating protection measures for PFC, the MAC layer will introduce more complex to do this.

Ethernet Physical Layer Security

- Design concept:
  - ✓ **Data plane:** Using the same methods from FlexOsec in ITU-T G.709.1
  - ✓ **Management and control plane**: Authentication with EAP, MKA, Port Control, etc, referred to 802.1X
- This design bridges the aforementioned gaps by implementing cryptography at the physical layer with full encryption, while leveraging reserved PAD fields to carry the cryptographic parameters without incurring additional bandwidth overhead. Implementing encryption within pluggable optical modules brings the advantage of easy deployment.
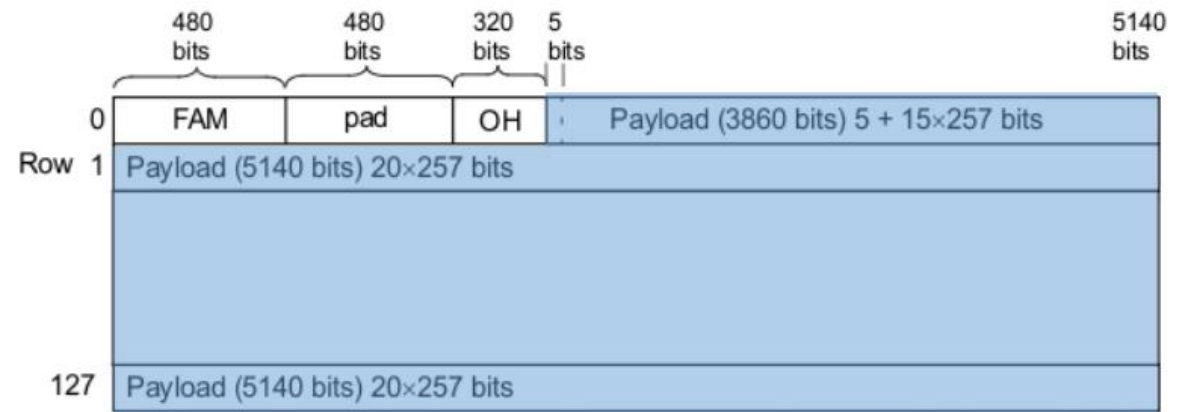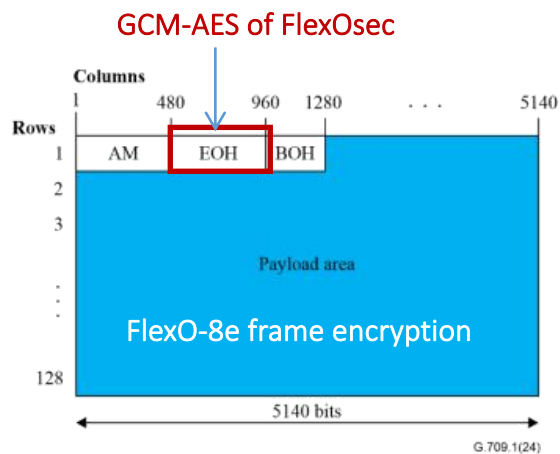
Ethernet Physical Layer Security Supports the Security Objectives of MACsec

Security Objectives	MACsec	Ethernet Physical Layer Security
Data Integrity	GMAC generates authentication tag in **Ethernet frame header** to verify data tampering and identity impersonation	GMAC generates authentication tag in **tributary frame pad** to verify data tampering and identity impersonation
Data Origin Authenticity		
Data Confidentiality	AES-GCM encryption of **Ethernet frame payload**, resistant to brute force attacks	AES-GCM encryption of **tributary frame payload**
Replay Protection	Packet Number in **Ethernet frame header** + Replay Window	Packet Number in **tributary frame pad** + Replay Window
Time Bounding Delivery	Series mechanisms (The MAC Services, Replay Protection, and SecY transmit & receive delay) ensure the **maximum frame lifetime** (2 seconds).	**Maximally inherent from MACsec**

Data Plane: Using the Methods Similar to FlexOsec

- 800GE ER1-20 and ER1 objectives currently standardized by IEEE P802.3dj are just suitable for DCI. Such objectives referred to and reused the physical-layer technologies specified by ITU-T FlexO (G.709.1). Specifically, considering physical layer security (see following figure):
    1. FAM is used for delimiting tributary frames. During the process of physical layer encryption with AES-GCM, FAM+pad are not encrypted;
    2. In the current 802.3 dj (Draft 2.0) specification, the pad field is all zeros, and the receiving side ignores this field. The physical layer security uses part of the pad field to carry cryptographic parameters (e.g., ICV, KI, etc). This mechanism allows for **zero-overhead transmission of security parameters;**
    3. The upper-layer frames & packets (data or protocol) are carried by the payload of the tributary frame, so **all information at the upper layer will be encrypted**, including inter-frame gap, frame headers, and other details.

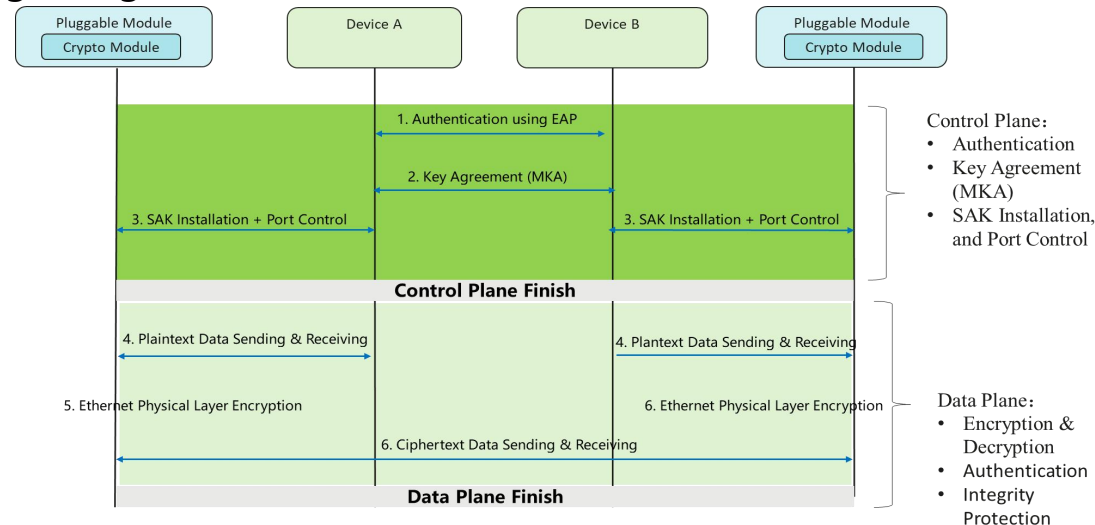# Management and Control Plane: Directly Inherits from 802.1X-2020

- **The complete operational process:**   .

  The device uses EAP to complete identity authentication -> The device uses the MKA protocol to complete key agreement -> SA & SAK installation into optical module -> opening of the MACSec controlled port, enable physical security in optical module -> Data transmission with physical security.

- **Specifically, regarding the controlled and uncontrolled ports:**
  1. During session setup, control protocols authenticate via the uncontrolled port. If successful, keys are delivered to the optical module and the controlled port opens. If it fails, the port stays closed and the module's security is disabled.
  2. After initial setup, re-authentication messages pass through the optical module's security layer, which already has synchronized keys for encryption. MAC layer protocols proceed unaware of this physical layer processing.
  3. If encryption/decryption keys become misaligned, continuous CRC errors occur due to broken mapping of plaintext message content and its CRC. This triggers a link failure, which forces both sides to restart the secure session establishment from the beginning.

Reusing MACSec's proven key management mechanism avoids reinventing the wheel for physical layer security.

The CMIS interface mechanism between the device and the optical module is out of scope.

Summary of Progress on Pending Issues

	Comments or Questions	Quick Answer
Cryptography Related	How control & management plane run and the relation with data plane	Directly Inherent 802.1X-2020
	The relationship and mutual influence between FEC and encryption engines	The coherent optical module first performs FEC and then executes cryptographic processing
	Attack model must be considered comprehensively in Ethernet physical layer	See page 7
	How to Adapt the MACSec Port Control Mechanism, and the influence to YANG model	See page 9
Performance Related	The latency introduced by integrity checks at PHY-layer	for coherent PHY, the transmission delay over the fiber link alone exceeds 100μs. The delay required for ICV operations is negligible
	Visualization of Security Association Parameters for the 802.3 Physical Layer	See page 8
	Message header overhead benefits, and comparison with overhead introduced by 802.1AEdk	See page 5 and 8

Proposal

- Hope to build consensus on the aforementioned security requirements and the physical-layer security solution.
- Seek to promote the initiation of standardization efforts within the 802.1 Security Task Group.

Q&A!