Further Discussion of Requirements and Objectives on Ethernet Coherent Link Security

Weiqiang Cheng, CMCC

Haojie Wang, CMCC

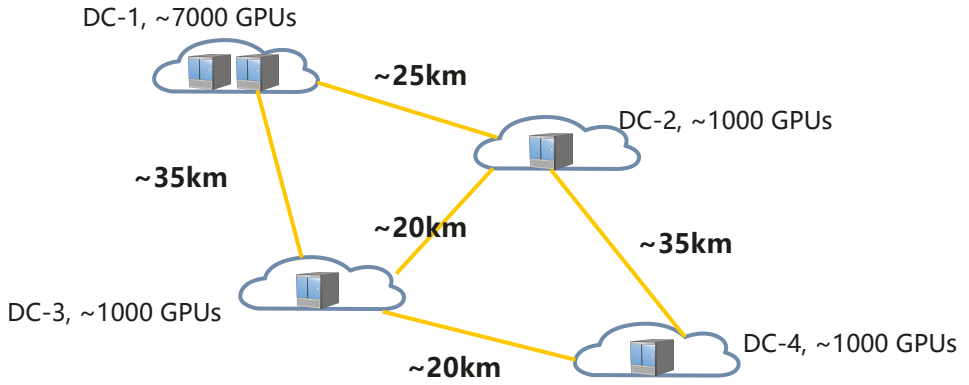
Overview

- The topic of link security underwent multiple discussions within the framework of the AICN item during last year's 802 Nendica sessions.
  - July'24: New requirements and challenges of network link security (**scenarios**, **requirements, gap analysis)**
  - Sept'24: Consideration on a new solution of network link security (**Proposed solution, Technical Characteristics**)
  - Dec'24: Follow-up Discussion of Link Security (**More solution details, Standardization suggestions**)
- **Focus and Objectives of This Contribution**:
  - more focus on security requirements, implementation challenges, and solution feasibility at the Ethernet coherent links at DCI applications.
  - This has heightened attention as its requirements grow increasingly critical, particularly given the rapid advancement of AI/ML applications.
- We hope insights from Nedica's deliberations are anticipated to inform and advance subsequent discussions within the IEEE 802.3 working group.

Application of Distributed Datacenter Interconnection

- Hyperscale Computing Cluster Demands, Single-DC deployments face critical power consumption challenges, with power supply and facility space emerging as primary bottlenecks
- Regionally phased construction of heterogeneous computing pools creates variably sized resource fragments, exacerbating the risk of mismatch between computing supply and application demands

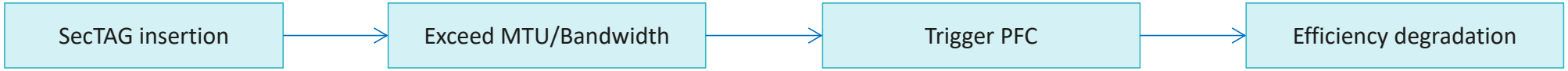
Models	GPT-4	GPT-5	GPT-6
GPU Scaling	~10,000	~100,000	~500,000
Power	~30 MW	~240 MW	~1200 MW



- Distributed Computing Resource Integration via DCI interconnection aggregates computing power across multiple established datacenters, enhancing utilization efficiency while reducing redundant infrastructure investment.
- DCI Links between metropolitan data centers typically span 10km to ~100 km, with bandwidth requirements exceeding 400G and predominantly operating at 800G/1.6T rates.

Requirements and Challenges of DCI Link Security

- DCI Interconnection Security Requirements:
  - The transmission of sensitive data. For example, organizations that handle sensitive or proprietary data, such as health-care records, financial information, or intellectual property.
  - **Physically unmonitored DCI links presents significant risks of link eavesdropping, data leakage, and tampering. This necessitates robust cryptographic assurance of data confidentiality and integrity.**
- Challenges of existing security mechanisms:
  - In DCI egress, output traffic primarily consists of large-sized packets resulting from the aggregation of intra-datacenter data flows.
  - Implementing MACsec encryption requires adding MACsec Security Tag (SecTAG) overhead to these large packets.
  - This may cause packet sizes to exceed MTU or interface bandwidth limitations, thereby triggering Priority Flow Control (PFC) mechanisms and potentially degrading data processing efficiency within the data center.



Capabilities of secure DCI coherent Links

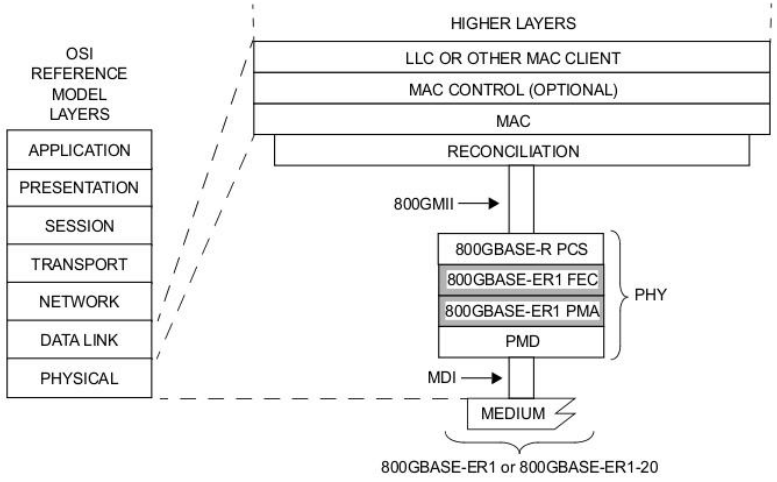
Objective： To deploy low-overhead, and easily deployable security solution on costly DCI links, significantly improving existing bandwidth utilization while ensuring data confidentiality and integrity.

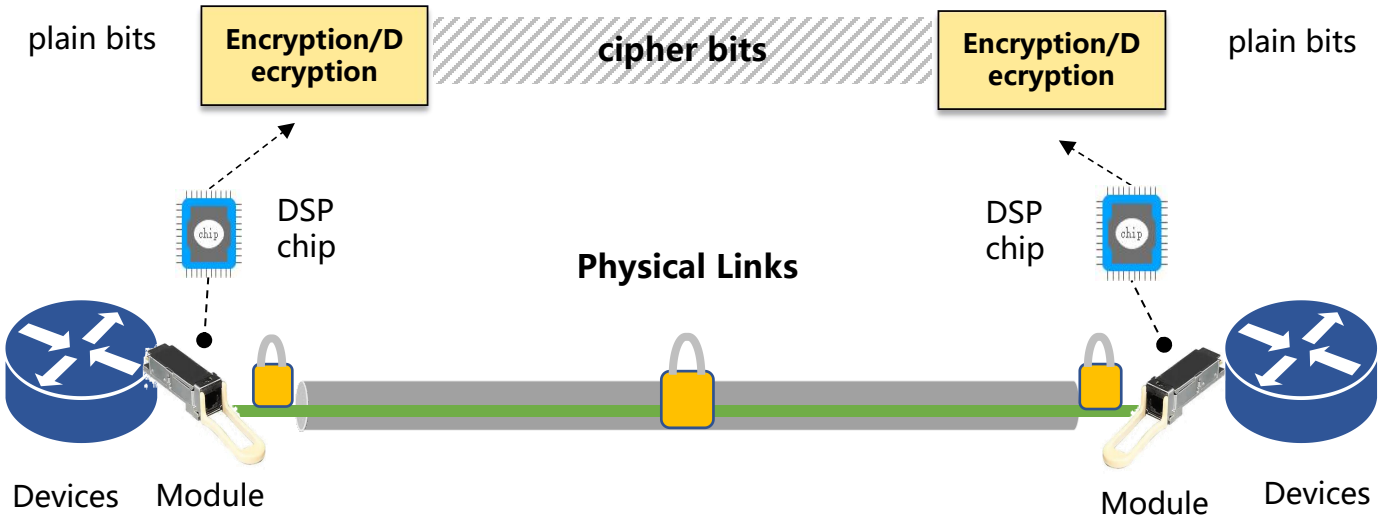
Key Capability Requirements:

- Low Overhead&High Throughput:
  - maximizing data transmission proportion, minimizing SecTag overhead, reducing per-unit effective data transmission costs.
  - Avoid or strictly limit security tags bytes needed by en/decryption to prevent significant payload efficiency loss.
- Simplified Deployment & Compatibility:
  - Compatibility with existing device platforms, avoiding costly core network replacements.
  - Existing key management and authentication systems could be utilized or integrated.

Potential solution: pluggable security in PHY layer

- The IEEE P802.3dj is currently standardizing 800GE ER1-20 and ER1 PMD objectives, targeting DCI interconnections within 40km distances through pluggable optical modules based on coherent optical technologies.
- Coherent optical technologies have been already adopted in ITU-T OTN (G.709.1, FlexOsec), which has incorporated physical-layer cryptographic security capabilities. Similarly, IEEE 802.1 security functions may be implemented equivalently at the Ethernet physical layer.

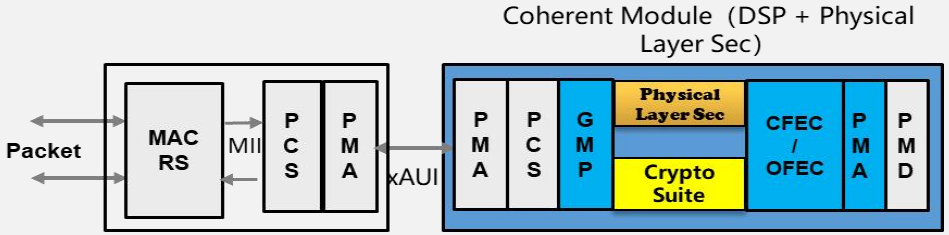




Feasibility Analysis of Confidentiality and Integrity at Coherent Ethernet Physical Layer

Proposed Architecture Design

- Pluggable security in coherent Ethernet physical layer applies the standardized cryptographic suites (e.g., AES-GCM) to encrypt and integrity-protect bitstreams.
- With the inherent FEC capability in the coherent module, integrity verification works with no problem.



- Leveraging the 802.3dj framework, the PAD field within the frame structure may be redefined to carry security encryption parameters (MACSec similar): TCI, AN, PN, SCI, ICV…

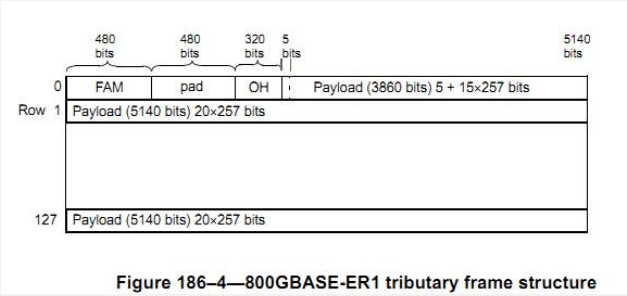
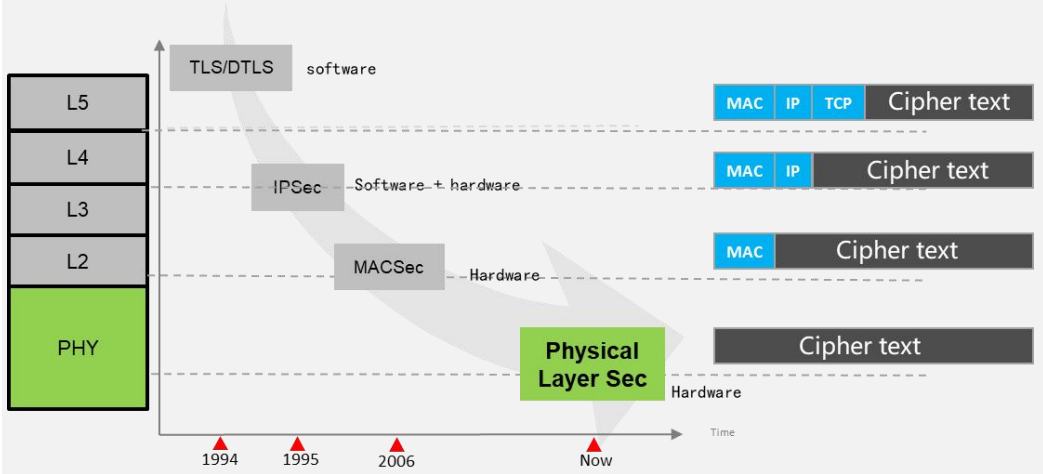


Figure 186–4—800GBASE-ER1 tributary frame structure

Physical Layer Security Advantages



	TLS/DTLS	IPsec	MACsec	Physical Layer Sec
Confidentiality Layer	L4	L3	L2	L1
Overhead	Packet / Frame header consumption			0
Latency	High	High	Medium	Low
Deployment	Device Software / Hardware Update			Optical Module Replacement / Update

Summary

Requirements: The security of DCI links has become increasingly critical, particularly with the emergence of distributed LLM pre-training applications. Consequently, it is necessary to develop a set of security specifications specifically tailored for this scenario.

Objective: Implementing a full-encryption, high-performance, low-overhead, and easily deployable security solution on costly DCI links, significantly improving existing bandwidth utilization while ensuring data confidentiality and integrity.

Methodology: Drawing on the security implementation experience of ITU-T OTN (G.709.1), apply existing cryptography to the coherent Ethernet physical layer, while leveraging the confidentiality, integrity, authentication, and key management standards established in IEEE 802.1AE and IEEE 802.1X for reference.

Q&A!