MAC Data Security

Approve the formation of the IEEE 802.1 MAC Data Security PAR Study Group with the following scope and duties:

Scope: Investigate reuse and potential extension of the architecture and technology standardized in IEEE Std 802.1 Media Access Control (MAC) Security, a.k.a. "MACsec" to protect data where the underlying transport does not preserve the MAC addresses of the communicating peers, and potential standardization in the form of either an amendment to IEEE Std 802.1AE or a new IEEE 802.1 standard.

Duties: Consider contributions, determine the form of standardization, draft a corresponding Project Authorization Request (PAR) and Criteria for Standards Development (CSD) responses for consideration by the IEEE 802.1 Working Group, and report progress to the Working Group.

For supporting documentation see the following slide(s) and
https://www.ieee802.org/1/files/public/docs2026/new-seaman-mac-data-security-0526- v00.pdf

In the WG, Proposed: Mick Seaman, Second: Karen Randall
— (y/n/a): <y>,<n>,<a>

In the LMSC, mover: Glenn Parsons Second: David Law

MAC Data Security

Scope (brief) of the proposed amendment or new standard:

- Specification of additional Cipher Suites using existing IEEE Std 802.1AE concepts, SecTAG, and Authenticated Encryption with Associated Data (AEAD) cryptography to provide data integrity, optional confidentiality, data origin authenticity, and replay protection without requiring communicating peers to use the same DA & SA MAC addresses.

- Guidance on the use of the Cipher Suites to protect data conveyed by transports that do not preserve original frame DA & SA fields.

MAC Data Security

Need (as currently expressed):

- Extension of the current MACsec performance and protection capabilities to provide end-to-end protection, where those ends typically represent the extent of the responsibility of a single provider organization that can be providing part of the overall application communication path.

  NOTE—Virtual LAN over Cloud scenarios where the entire original frame (DA, SA, and Data) is communicated peer-to-peer are already supported by existing MACsec. However that protection cannot localize faults to specific path segments.

MAC Data Security

Scope constraints

- In: Use of CAK (pairwise symmetric master key, PSK or 802.1X) and existing MKA for SAK distribution and roll-over. Retain means outside the standard for CAK/PSK distribution.
- Out: Specification of new authentication methods for CAK generation or new key agreement (SAK distribution) methods.
- In: Specification or guidance for particular transports and their protocol identification.
- Out: Extension or modification of Cipher Suite to cover transport fields.
- In (must have): MAC Privacy protection

MAC Data Security

Risks: Scale

- Implementation needs rapid (per frame) access to per SA expanded data key (SAK) schedules and data (nextPN etc.) and per SC (secure channel) statistics.
- MACsec very deliberately protected all transmitted traffic through a port using a single SC, with only two SAs concurrent for roll-overs.
- Received traffic uses a single SC per peer, with only two SAKs for all peers (including transmit). Current implementations can support many ports with more (~256+?) SCs.
- Limits may be OK for provider trunk paths and network edges near customers, but well short of per customer protection in the core.