This provides responses to comments received on the ISO/IEC JTC 1/SC 6 ballot of IEEE Std 802.1AS-2025.

The voting results of IEEE Std 802.1AS-2025 are in SC6N18742:

- Support need for ISO standard? Passed 7/0/9
- Support this submission being sent to FDIS ballot? 6/0/10
- 1 comment received with the China NB vote

The comments have been processed in a timely manner using the mechanisms defined and agreed in 6N15606. This document provides the responses from IEEE 802[1] to the comments by China NB on this ballot.

China NB comment 1 on IEEE 802.1AS-2025:

IEEE 802.1AS-2025 is developed based on IEEE 802.1AS-2020 by consolidating three amendments and one corrigendum; however, it relies on the MACSec technology specified in IEEE 802.1AE for its security architecture (see Clause 11.1.4).

In document 6N17207, China explicitly identified significant security defects within IEEE 802.1AE. These concerns primarily include the "mandatory use of AES cryptographic algorithms," "extensive normative references to IEEE 802.1X which contains security flaws (e.g., the inability to achieve true mutual authentication)," and the "excessive computational burden imposed by hop-by-hop encryption." Regrettably, these comments submitted by China have not been adequately addressed.

Consequently, China abstains on this ballot. We reiterate our position that we cannot support the adoption of IEEE 802.1AS-2025 as an International Standard given its dependency on MACSec specified in IEEE 802.1AE, which contains unresolved security defects.

Proposed Change:

Remove the mandatory dependency on MACSec for its security defects.

IEEE 802 response to CN.1 on IEEE 802.1AS-2025:

It is accurate that IEEE Std 802.1AS-2025 is a Maintenance roll-up of IEEE Std 802.1AS™-2020 with the corrigendum IEEE Std 802.1AS-2020/Cor1 and amendments IEEE Std 802.1ASdr, IEEE Std 802.1ASdm, and IEEE Std 802.1ASdn. However, specification of security mechanisms is not part of the scope of this standard. IEEE Std 802.1AS specifies protocols, procedures, and managed objects used to ensure that the synchronization requirements are met for time-sensitive applications, such as audio, video, and time-sensitive control, across networks.

The comment is not applicable to any normative provisions of IEEE Std 802.1AS-2025. IEEE Std 802.1AS-2025 does not require the use of MACsec [IEEE Std 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE:2020)]. The illustration of the relative placement of MACsec and IEEE Std 802.1AS functionality in Figure 11-3 of

[1] This document solely represents the views of the IEEE 802 LAN/MAN Standards Committee, and does not necessarily represent a position of IEEE or the IEEE Standards Association.

Clause 11.1.4 is purely informative. Additional or alternative security mechanisms, specified outside the scope of IEEE Std 802.1AS, may also be used.

To reiterate, the comment is out of scope of this standard and moreover there is no “dependency” on the use of MACsec. The text in the comment from the China NB regarding IEEE Std 802.1AE, AES cryptographic algorithms, and normative references to IEEE 802.1X are inaccurate and incorrect.

IEEE 802 believes that the alleged security defects asserted by the China NB are not valid. Without technical substantiation of any related concerns, IEEE 802 cannot consider modification of the existing IEEE 802 standards.