This provides responses to comments ISO/IEC JTC 1/SC6 ballot of IEEE Std 802.1ASed-2026.

The voting results on IEEE 802.1ASed-2026 are:

- Support need for ISO standard? Passed 6/0/10
- Support this submission being sent to FDIS ballot? 6/0/10
- 1 comment 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 the China NB on this ballot.

China NB comment 1 on IEEE Std 802.1ASed-2026:

IEEE 802.1AS-2025 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. However, these comments submitted by China have not been adequately addressed. So, China abstains on IEEE 802.1AS and it's amendments.

Proposed Change:
Remove the mandatory dependency on MACSec due to its security defects.

IEEE 802 response to CN.1 on IEEE Std 802.1ASed-2026:

To clarify, IEEE Std 802.1ASed-2026 is an amendment to IEEE Std 802.1AS™-2020, which specifies protocols, processes, procedures, functions, mechanisms, and managed objects to enable fault-tolerant timing by increasing the availability of the time and adding time integrity. This is achieved using two or more generalized Precision Time Protocol (gPTP) domains, multiple time distribution paths, the local oscillator clock, and a time selection function with individual processes for times that have interdependencies and times that do not have interdependencies. Specification of security mechanisms is not part of the scope of this standard. Additionally, this amendment does not specify, nor does it refer to IEEE Std 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE:2020 (Ed2)).

The China NB has repeatedly claimed there are “security defects”; however, these assertions have not been substantiated, despite requests for further information from IEEE 802. IEEE 802 believes that none of the alleged security problems asserted by the China NB have been shown to be valid. IEEE 802 has supplied a number of communications about the security technology specified in the IEEE 802 security standards to explain why attacks referenced in China NB contributions are not effective (and will fail).

In summary, the comment is out of scope of this standard and moreover there is no “dependency” on the use of MACsec. Furthermore, 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.

[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.