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

The voting results on IEEE Std 802.1AXdz-2025 are in SC6 N18664:
- Support need for ISO standard? Passed 7/0/10
- Support this submission being sent to FDIS ballot? 6/0/11
- 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 802.1AXdz-2025:

IEEE 802.1AXdz normatively references IEEE 802.1Q in clauses 10.2 and 10.7.1, which China has objected to for technical reasons on 802.1Q.

Proposed Change:
China abstains from voting on this amendment until the security issues of the referenced standard are resolved.

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

To clarify, IEEE Std 802.1AXdz-2025, Link Aggregation, Amendment 1: YANG for Link Aggregation, specifies a Unified Modeling Language (UML)-based model and YANG modules for Link Aggregation configuration and status reporting. Comments on ISO/IEC/IEEE 8802-1Q are beyond the scope of IEEE Std 802.1AXdz-2025.

Furthermore, comments submitted on ISO/IEC/IEEE 8802-1Q:2020 were reviewed and responses were liaised in 2020 and 2021; and comments submitted on ISO/IEC/IEEE 8802-1Q:2024 were reviewed and responses were liaised in 2024.

It has been stated in many prior responses to ballot comments from China NB, IEEE Std 802.1Q (ISO/IEC/IEEE 8802-1Q:2020) explains how it can be used in conjunction with IEEE Std 802.1X-2020 (approved as ISO/IEC/IEEE 8802-1X:2021). IEEE Std 802.1Q is not based on nor does it depend on the use of IEEE Std 802.1X-2020. It is offered as an illustrative example to provide additional security through port-based network access control. Specifically, IEEE Std 802.1X may be used to provide a further level of control over the connectivity provided by a Bridge Port to the MAC Relay Entity and the Higher Layer Entities within a Bridge.

IEEE 802 believes that none of the alleged security problems asserted by the China NB have been shown to be valid. Despite numerous communications and requests for further technical information about the vague claims of "security problems" in IEEE 802 security standards since 2013, the China NB has not

---

[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. This Liaison Communication is for information only. Any material excerpted from IEEE copyrighted Works requires permission from IEEE (stds-copyright@ieee.org).

substantiated their assertions. The history of the security technology discussion can be found in documents SC 6N17493 and SC 6N17741.

The invitation for a representative of the China NB (as well as representatives from other interested SC 6 NBs) to attend an IEEE 802 Plenary session remains open.

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.