This provides responses to comments on the FDIS ballot on ISO/IEC/IEEE 8802-1Q:2024/FDAmd 39 (Ed 3).

The voting results on ballot ISO/IEC/IEEE 8802-1Q:2024/FDAmd 39 (Ed 3):

- Do you approve the technical content of the final draft? Passed 11/0/11
- 1 comment with the China NB Abstention 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 ISO/IEC/IEEE 8802-1Q:2024/FDAmd 39 (Ed 3):

Regarding IEEE 802.1Q™-2022, China NB has already submitted the comments during its 60-day ballot and FDIS ballot to against the reference to IEEE 802.1X, for its security flaws including lack of specifications on pre-established trusted channel which IEEE 802.1X security is relying on, failing to achieve a real mutual authentication between the Supplicant and Authenticator, lack of independent identity for Authenticator resulting in losing the basic credential of identity legitimacy, etc.
However, there are no further steps taken in this new amendment to resolve those comments we submitted. IEEE 802.1X is still the normative reference in IEEE 802.1Q-2022 and IEEE 802.1X is still used in 8.13.9, 10.1, 25.2, 25.6 etc.

Proposed Change:
Delete the references to IEEE 802.1X in IEEE 802.1Q-2022.

IEEE 802 response to CN.1 on ISO/IEC/IEEE 8802-1Q:2024/FDAmd 39 (Ed 3):

To clarify, IEEE Std 802.1Qdx-2024, YANG Data Models for the Credit-Based Shaper, is an amendment to IEEE Std 802.1Q-2022 (ISO/IEC/IEEE 8802-1Q:2024) that specifies a YANG data model that supports configuration and status reporting for credit-based shaper algorithm capabilities in bridges and end stations. This amendment does not specify, nor does it refer to IEEE Std 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013).

Comments on ISO/IEC/IEEE 8802-1Q are beyond the scope of IEEE Std 802.1Qdx-2024. 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 provided 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.

[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).

Unapproved Draft

Furthermore, 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 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.

Unapproved Draft