This provides responses to comments ISO/IEC JTC1/SC6 ballot of IEEE Std 802.1Qcj-2023.

The voting results on IEEE Std 802.1Qcj-2023 are in SC6 N18215:

- Support need for ISO standard? Passed 9/0/10
- Support this submission being sent to FDIS ballot? 6/0/13
- 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 to the comments by China NB on this ballot.

China NB comment 1 on IEEE Std 802.1Qcj-2023:

Regarding IEEE 802.1Q™-2018, 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 2023 version 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.

IEEE 802 response to CN.1 on IEEE Std 802.1Qcj-2023:

To clarify, IEEE Std 802.1Qcj-2023 is an amendment to IEEE Std 802.1Q-2018 (ISO/IEC/IEEE 8802-1Q:2020) that specifies the protocols, procedures, and management objects for auto-attachment of network devices to Provider Backbone service instances by using Type, Length, Value (TLVs) within the Link Layer Discovery Protocol (LLDP). The amendment simplifies the deployment and administration of PBB networks, e.g., controlled by Shortest Path Bridging (SPB), by allowing for automatic configuration of the virtual LANs and service identifiers, thus allowing access to services of network devices without the need of manual configuration. 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 (Ed 2) are beyond the scope of IEEE Std 802.1Qcj-2023. Furthermore, comments submitted on ISO/IEC/IEEE 8802-1Q (Ed 2) referenced were reviewed and responses were liaised in 2020 and 2021.

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.

Furthermore, IEEE 802 believes that none of the alleged security problems asserted by the China NB have been shown to be valid. In spite of 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 been unable to substantiate their assertions. The history of the security technology discussion can be found in documents SC6N17493 and SC6N17741.

The invitation for a representative of the China NB (as well as representative from other interested SC6 NBs) to attend an IEEE 802 Plenary session remains open.

IEEE 802 believes that the alleged security defects asserted by the China NB have all been shown to be not valid. Without technical substantiation of any related concerns, IEEE 802 cannot consider modification of the existing IEEE 802 or ISO standards.