This provides responses to comments ISO/IEC JTC1/SC6 ballot of IEEE 802.1Qcc-2018

The voting results on IEEE 802.1Qcc-2018 in SC6N17244:

- Support need for ISO standard? Passed 8/0/10
- Support this submission being sent to FDIS? 6/1/11
- 1 comment with the China NB NO 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 802.1Qcc-2018:

IEEE 802.1Qcc is an amendment to IEEE 802.1Q™-2018 (has incorporated IEEE 802.1Q-2014 and its amendments and corrigendum).

China has submitted comments on IEEE 802.1Q-2018 during both 60-day ballot and FDIS ballot to object the references to IEEE 802.1X (The recent comments are included in 6N17175).

IEEE 802.1X has security problems including lack of specifications on pre-established trusted channel which IEEE 802.1X security is relying on, failing to achieve the real mutual authentication between the Supplicant and Authenticator, lack of independent identity for Authenticator resulting in losing the basic credential of identity legitimacy, etc.

Up to now, there is no reasonable and appropriate disposition on the security problems in the base standard IEEE 802.1Q™-2018 and this amendment neither gives solution to the security issues in IEEE 802.1Q™-2018. IEEE 802.1X is still the normative reference in IEEE 802.1Q-2018 and is used in Clause 8.13.9, 10.1, 25.2 etc.

Therefore, China cannot support this amendment to be submitted to the next stage.

Proposed Change:

Improve the referenced security mechanisms.

IEEE 802 response to CN.1 on IEEE 802.1Qcc-2018:

To clarify, IEEE 802.1Qcc-2018 is an amendment to IEEE 802.1Q-2018 (ISO/IEC/IEEE 8802-1Q:2020) that specifies enhancements to protocols, procedures, and managed objects for the configuration of network resources for time-sensitive (i.e., bounded latency) applications. The enhancements address Time-Sensitive Networking (TSN) application requirements beyond audio/video (AV) traffic. This amendment does not specify nor does it refer to IEEE 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013).

Comments on ISO/IEC/IEEE 8802-1Q (Ed 2) are beyond the scope of IEEE 802.1Qcc-2018. Furthermore, comments submitted on ISO/IEC/IEEE 8802-1Q (Ed 2) referenced were already reviewed and responses were liaised on 2 June 2020, with sufficient time for receipt and consideration prior to the close of the ballot on this amendment.

However, to repeat the earlier responses to ballot comments from China NB regarding IEEE Std 802.1Q, IEEE Std 802.1Q explains how it can be used in conjunction with IEEE Std 802.1X (approved as ISO/IEC/IEEE 8802-1X:2013). IEEE Std 802.1Q is not based on nor does it depend on the use of IEEE Std 802.1X-2010. It is provided as an illustrative example to provide additional security through port-based network access control. Specifically, IEEE 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. It is unnecessary to remove the IEEE 802.1X-2010-related descriptions and reference from the text. Furthermore, 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.

To reiterate, the current comment is out of scope of this document and without technical substantiation of any related concerns, IEEE 802 cannot consider modification of the existing IEEE 802 or ISO standards.

China NB comment 2 on IEEE 802.1Qcc-2018:

In the referred clauses, this amendment uses IEEE 802.1AE to provide security protection. However, China NB has pointed out the security problems of IEEE 802.1AE for several times during the past ballots, e.g. 6N15556 and 6N15770.

China also submitted the comments on the new version of IEEE 802.1AE (IEEE 802.1AE-2018). Please refer to the comments in 6N17207. The problems of 1AE include inconsistence between content and title, using high cost Hop-by-Hop Encryption, only permitting to use typical cryptographic algorithms like AES (not including other compliant options that are compliant with ISO/IEC international standards) and so on.

The security issues about IEEE 802.1AE have not been properly resolved, hence the reference to use it will lead to secure risks in implementation.

Proposed Change:

Improve the referenced security mechanisms.

IEEE 802 response to CN.2 on IEEE 802.1Qcc-2018:

To clarify, IEEE 802.1Qcc-2018 does not identify nor require IEEE 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE:2020). There is only a single reference to IEEE 802.1AE, provided as an example of a security tag. There is no dependency in IEEE 802.1Qcc-2018 on IEEE 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE:2020). Comments on IEEE 802. 1AE-2018 (ISO/IEC/IEEE 8802-1AE:2020) are beyond the scope of IEEE 802.1Qcc-2018.

The current comment on IEEE 802.1Qcc-2018 is out of scope of this document and without technical substantiation of any related concerns, IEEE 802 cannot consider modification of the existing IEEE 802 or ISO standards.