This provides responses to comments received on the JTC1 ballot of IEEE Std 802.1CMde-2020 (ISO/IEC/IEEE 8802-1CM:2019/FDAmd 1)

The voting results on IEEE Std 802.1CMde-2020 (ISO/IEC/IEEE 8802-1CM:2019/FDAmd 1) in SC6N17604:

- Support need for ISO standard? Passed 8/1/10
- 2 comments received 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 Std 802.1CMde-2020 (ISO/IEC/IEEE 8802-1CM:2019/FDAmd 1):

IEEE 802.1CMde is an amendment to IEEE 802.1CM- 2018. Claus 1.3 states that it selects features and options that support OSI layers 1 and 2 in bridges and end stations from the following specifications:

— Virtual Local Area Network (VLAN) Bridge specification in IEEE Std 802.1Q

— MAC service specifications in IEEE Std 802.1AC

— MAC/PHY technology specifications in IEEE Std 802.3

— Interspersing express traffic specification in IEEE Std 802.3

— Frame preemption specification in IEEE Std 802.1Q.

China has voted against IEEE 802.1Q-2018 during both 60-day ballot and FDIS ballot to object the references to IEEE 802.1X (see 6N17175). IEEE 802.1X has security problems (see 6N17450) 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.

IEEE Std 802.1AC (see comments in 6N16769) is implemented with IEEE 802.11 architecture and 802.1AE security technology. 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 detailed comments are in 6N17207).

China has also voted against IEEE 802.3 (see 6N17223). IEEE 802 has explicitly stated in comment resolutions of other proposals that a default security mechanism must be specified for reasons such as interoperability, but for IEEE 802.3 the interpretation of the lack of security mechanism is "Security agnostic". For many times, it is strongly suggested that IEEE 802.3 and its amendments specify security mechanisms, or at least specify their references on security mechanism.

Up to now, there is no reasonable and appropriate disposition on the security problems in the referenced standard IEEE 802.1Q, IEEE 802.1AC and IEEE 802.3.

Therefore, China cannot support this amendment to be published as an International Standard.

<u>Proposed Change:</u>

The security defects of the referenced mechanisms and standards must be fixed before publication.pec

IEEE 802 response to CN.1 on IEEE Std 802.1CMde-2020 (ISO/IEC/IEEE 8802-1CM:2019/FDAmd 1):

IEEE Std 802.1CMde-2020 is an amendment to IEEE Std 802.1CM-2018 (ISO/IEC/IEEE 8802-1CM:2019) and specifies profiles that enable the transport of time-sensitive fronthaul streams in Ethernet bridged networks. This amendment does not specify or refer to the use of IEEE Std 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013) or IEEE Std 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE:2020). Additionally, this amendment standard does not refer to IEEE Std 802.1AC-2016 (ISO/IEC/IEEE 8802-1AC:2018) or IEEE Std 802.11 (ISO/IEC/IEEE 8802-11:2018).

The reference to IEEE Std 802.3-2018 is specifically for interspersing express traffic (or frame preemption), which is part of one of the fronthaul profiles but not required by the other standards referenced in this comment. Furthermore, the scope of IEEE Std 802.3 does not include the setting of provisions or any guidance with respect to security mechanisms for network management. IEEE Std 802.3 is security agnostic and allows the user to implement any security mechanism that satisfies that user's security requirements for network management.

Comments on IEEE Std 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013 or IEEE Std 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE:2020) are beyond the scope of IEEE Std 802.1CMde-2020. 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 been unable to substantiate their assertions. 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 Std 802.1CMde-2020 (ISO/IEC/IEEE 8802-1CM:2019/FDAmd 1):

Due to the aforementioned references, IEEE 802.1CM and its amendment must be implemented in combination with the IEEE 802.11 architecture, IEEE 802.3 architecture and some mechanisms with security vulnerabilities.

That means, at the engineering implementation level, IEEE 802.1CM and its amendment will be implemented together with standards with technical defects in security (because the technology involved in the amendment cannot be implemented separately). This objectively strengthens the implementation and promotion of standards with technical defects (based on insecure architecture and mechanisms), and the application and deployment of products conforming to the aforementioned standards will further aggravate the security risks of the network.

Proposed Change:

The security defects of the referenced mechanisms and standards must be fixed before publication to avoid further risks in implementation.

IEEE 802 response to CN.2 on IEEE Std 802.1CMde-2020 (ISO/IEC/IEEE 8802-1CM:2019/FDAmd 1):

The comment on IEEE Std 802.1CMde-2020 is beyond its scope. Neither IEEE Std 802.1CM-2018 nor IEEE Std 802.1CMde-2020 specify or refer to the use of IEEE Std 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013) or IEEE Std 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE:2020). Without technical substantiation of any related concerns, IEEE 802 cannot consider modification of the existing IEEE 802 or ISO standards.