This provides responses to comments ISO/IEC JTC1/SC6 ballot of IEEE 802.1AS-2020

The voting results on IEEE 802.1AS-2020 in SC6N17268:

- Support need for ISO standard? Passed 9/0/9
- Support this submission being sent to FDIS? 7/1/10
- 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 802.1AS-2020:

In the referred clause, this proposal uses MACsec, which is defined by IEEE 802.1AE, to provide security protection.

However, the security problems of IEEE 802.1AE have been pointed out by China NB for several times during the past ballots (see 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 IEEE 802.1AE 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 until now, hence the use to MACsec will lead to security risks in implementation.

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

Proposed Change:

Improve the used security mechanisms.

IEEE 802 response to CN.1 on IEEE Std 802.1AS-2020:

IEEE Std 802.1AS-2020 specifies protocols, procedures, and managed objects used to ensure that the synchronization requirements are met for time-sensitive applications, such as audio, video, and time-sensitive control, across networks.

The comment is not applicable to any normative provisions of IEEE Std 802.1AS-2020. Specification of security mechanisms is not part of the scope of this standard. IEEE Std 802.1AS-2020 does not require the use of MACsec [IEEE Std 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE:2020)]. The illustration of the relative placement of MACsec and IEEE Std 802.1AS functionality in Figure 11-3 is purely informative. Additional or alternative security mechanisms, specified outside the scope of IEEE Std 802.1AS, could also be used.

The submitted comments appear to relate more to former claims by the China NB of alleged “security problems” in documents other than the standard that was under ballot. Furthermore, these alleged

"security problems" have yet to be substantiated despite requests made by IEEE 802 in the last several years.

To clarify comments relating to IEEE Std 802.1AE-2006 (ISO/IEC/IEEE 8802-1AE:2013), even though it is not a normative reference in IEEE Std 802.1AS-2020:

- The documents referenced in the China NB ballot comments (i.e., 6N15556 and 6N15770) are the Summary of Voting results on IEEE Std 802.1AE-2006 (ISO/IEC/IEEE 8802-1AE:2013) which date from 2012 and 2013. Responses to these comments were submitted from IEEE 802 to ISO/IEC JTC1/SC6 at that time. IEEE 802 fully responded to all claims made by both the China NB and Switzerland NB representatives and presented additional information about the design and specification of IEEE 802 technologies. Additionally, there have been no submissions providing further technical details to justify concerns from the China NB or Switzerland NB and there has been no detailed technical information or discussion shared since that time.
- Responses to China NB comments on IEEE Std 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE:2020) have been made available in a separate document (6N17266); additionally, 6N17059 was available in October 2019 to provide IEEE 802 responses to similar China NB comments in 6N17080 (results of the 60-day ballot).
- This standard does not expose the public network or its user to (unspecified) security "issues" as stated. Furthermore, the China NB has again failed to elaborate on its assertions of security concerns with IEEE Std 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE:2020), despite numerous requests from IEEE 802 since 2012. IEEE 802 believes that the alleged security defects asserted by the China NB have all been shown to be not valid and cannot consider changes to the existing IEEE 802 or ISO standards without substantiation of these claims:
  - The scope of IEEE Std 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE:2020) is "to specify provision of connectionless user data confidentiality, frame data integrity, and data origin authenticity by media access independent protocols and entities that operate transparently to MAC Clients." It also notes that the MAC Clients are as specified in IEEE Std 802 (ISO/IEC/IEEE 8802-A:2015), IEEE Std 802.1Q (ISO/IEC/IEEE 8802-1Q:2016), and IEEE Std 802.1X (ISO/IEC/IEEE 8802-1X: 2013). It has been confirmed by the IEEE Standards Review Committee and the IEEE Standards Board that IEEE 802.1AE-2018 meets this scope. Additionally, the scope has not been modified since the approval and publication of IEEE Std 802.1AE-2006 (ISO/IEC/IEEE 8802-1AE:2013).
  - As was stated explicitly in 6N16753, the encryption mechanisms used in ISO/IEC/IEEE 802.1AE-2018 (revision to ISO/IEC/IEEE 8802-1AE:2013) are fully capable of being implemented in ISO/IEC/IEEE 8802-3 interface chips (and chips providing a similar transmission capability for other media), and this is in practice how it is done. This requires no additional bandwidth on main system memory and is generally done in a pipelined fashion with a few minimum packet size delays in the pipeline. At the relevant speeds, this is equivalent to a very modest increase in the length of the attached physical medium (wire, fiber or other) and has been available in multiple commercial implementations at full wire speed for over a decade.

- To be clear, IEEE Std 802.1AE (ISO/IEC/IEEE 8802-1AE:2013) already includes Cipher Suite identification and protocol identification mechanisms to facilitate the addition of further standard Cipher Suites (by future amendment of the base standard) or the use of proprietary Cipher Suites (without amending the base standard) should an additional Cipher Suite be required for any reason. Additionally, the mandatory-to-implement Default Cipher Suite GCM-AES-128 was chosen because it is well vetted, internationally designed, and recognized. It is not necessary for the standard to speculate on, or to limit, the reasons why any specific additional Cipher Suite is desired. Technical criteria for additional Cipher Suites are already specified in IEEE Std 802.1AE (ISO/IEC/IEEE 8802-1AE:2013) clause 14.4 (Cipher Suite conformance).

IEEE 802 believes that the security defects asserted by the China NB have all been shown to be not valid and will not make changes without substantiation of these assertions.