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

The voting results on 802.1AE-2018:

- Support need for ISO standard? Passed 10/0/8
- Support this submission being sent to FDIS? 8/1/9
- 6 comments 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 802.1AE-2018:

The subject of this text is Media Access Control (MAC) Security, the whole subject should be consisting of a multi-angle, multi-structure standard set. The Media Access Control (MAC) Security mechanisms should cover a variety of mechanisms in a variety of network architectures including LAN and WLAN. However, IEEE 802.1AE-2018 is actually just one kind of CSMA/CD LAN Media Access Control (MAC) Security mechanism. It even cannot be used in the WLAN environment. This proposal cannot cover the entire concept of MAC Security, just like the subject of network security technology cannot just have a sensor network security method and one sensor network security method also can not represent all the network security technology methods.

Proposed Change:

NONE

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

The scope of this Standard specifies that it 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 802.1AE-2006 (ISO/IEC/IEEE 8802-1AE:2013).

It is noted that MAC Security as specified in ISO/IEC/IEEE Std 802.1AE (and revised by this standard to include the already approved amendments) can be used with any media access control method that provides the MAC Service specified in ISO/IEC/IEEE 802.1AC. That standard, previously ISO/IEC 15802-1, has defined the MAC Service since its development in the early 1990's and is supported by all IEEE 802 conformant media access control methods. MAC Security as defined in ISO/IEC/IEEE Std 802.1AE is therefore by no means restricted to supporting CSMA/CD (carrier sense multi-access/collision detect), and no such limitation is present in the text.

ISO/IEC/IEEE Std 802.1Q specifically addresses networks that include links supported by provider networks, and 802.1AE-2018 includes the specification developed in IEEE Std 802.1AEcg-2018

specifically supporting the use of MAC Security over WAN links. These WAN links can be supported by any communications technology capable of providing the MAC Service including (but not limited to) a wide variety of technologies (including legacy technologies such as SONET) for which specifications capable of transporting frames as defined by ISO/IEC/IEEE Std 802.3 have been developed. These technologies are not limited to those providing support for CSMA/CD and are not limited to those specified by IEEE Project 802.

ISO/IEC/IEEE Std 802.1AE and its revision IEEE Std 802.1AE-2018 is already part of a multi-angled, multi-structure standard set under the framework provided by ISO/IEC/IEEE Std 802.1X. The security specified by IEEE Std 802.11 (WLAN) also forms part of that set. The structure includes EAP authentication methods specified by the IETF, although ISO/IEC/IEEE Std 802.1X restricts the use of methods to those that provide mutual authentication and are not vulnerable to man-in-the-middle attacks.

China NB comment 2 on IEEE 802.1AE-2018:

IEEE 802.1AE-2018 has referenced IEEE 802.1X in several clauses. However, China NB voted against IEEE 802.1X and submitted quite a lot of technical comments pointing out the security problems of this proposal during the pre-ballot and FDIS ballot in 2013 (as described in 6N15555 and 6N15771, such as "cannot achieve the real mutual authentication between the Supplicant and Authenticator"). Those comments have not been disposed reasonably.

Proposed change: Please delete the references to IEEE 802.1X.

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

The general assertions raised in the China NB's ballot were discussed at length in 2013 at an IEEE 802 meeting in Geneva (with IEEE 802 and Switzerland NB representatives in attendance) and in both 2013 and 2014 at SC6 meetings in Seoul and Ottawa (with IEEE 802, China NB and Switzerland NB representatives in attendance). During those meetings, IEEE 802 fully responded to all of the claims made by both the China NB and Switzerland NB representatives and also provided additional information about the design and specification of IEEE 802 technologies. Specifically,

- In June 2013 in 6N15658 (IEEE 802 Response to 6N15613), IEEE 802 explains why none of the attacks described in 6N15613 (NB' of China's contribution on Effective Attack on IEEE802.1X-the further analysis of 6N15523) are effective and reveals how the attacks described in the China NB contribution 6N15613 will fail.

- In June 2013 in 6N15646 (IEEE 802 Response to 6N15523), IEEE 802 explains why the analysis in 6N15523 (NB of Switzerland's contribution on a comparative analysis of TePAKA4 and IEEE 802.1X Security) is flawed, noting it produces erroneous results based on misunderstandings of technology, invalid assumptions, and analysis using an incorrect model.

- In January 2014 in 6N15870 (IEEE 802 response to SC6N15840 – "Intentional Weaknesses in Information Security Standards and Implementations"), IEEE 802 responded to non-specific allegations by the China NB about any security standards developed outside ISO. The China NB suggested that such standards contain intentional weaknesses. IEEE 802 responded that the best way to avoid such issues is to develop standards in an open standards process, such as that provided by IEEE 802.

- In January 2014 in 6N15845 (Explanation of Certificate Use in 802.1X EAP-TLS), IEEE 802 described the use of certificates in IEEE 802.1.

- In July 2015 in 6N16255 (IEEE 802 response to China NB comments on IEEE Std. 802.1Q and 802.1Xbx), IEEE 802 responded to the stated concerns raised on IEEE 802.1Q and IEEE 802.1X. Specifically, it was pointed out that IEEE Std 802.1Q does not depend on the use of IEEE Std 802.1X. In response to the unsubstantiated comment that there are "security problems" in IEEE Std 802.1X, the IEEE response clearly stated that IEEE Std 802.1X does not expose the public network or its user to (unspecified) security problems because it mandates the use of mutual authentication methods, reflecting current needs, best practice, and experience from IEEE 802.1X-2004.

Additionally, at the SC6 meeting in Ottawa in early 2014, the China NB and Switzerland NB representatives committed to providing additional technical details to justify their concerns. No such submissions were made to the SC6 meeting in London later that year, and no technical submissions were received subsequently. Furthermore, there has been no technical discussion since that time.

IEEE 802 is eager to hear and discuss further the details of any new concerns about IEEE 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013) from the China NB. On 21 February 2017, IEEE 802 formally invited a representative of the China NB (as well as representative from other interested SC6 NBs) to attend the IEEE 802 Plenary meeting held in Vancouver, Canada the week starting Monday, 13 March 2017. Unfortunately, our invitation was declined by the China NB. However, the invitation remains open.

IEEE 802 believes that the attacks on IEEE 802.1X-2010 described by the China NB have all been shown to be not valid but continues to invite the China NB to submit any additional technical details for consideration. In the absence of technical substantiation of the claims, IEEE 802 cannot consider modification of the existing IEEE 802 or ISO standards.

China NB comment 3 on IEEE 802.1AE-2018:

Hop-by-Hop Encryption costs high latency, high computing resources and does not support current network coexisting. Network upgrade cost is also very high. The reply in 6N16753 from IEEE 802 did not clarify the problem clear enough. Also in this new version of IEEE 802.1AE, there is no improvement.

Proposed Change:

NONE

IEEE 802 response to CN.3 on IEEE 802.1AE-2018:

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.

This standard does not expose the public network or its user to (unspecified) security problems. Furthermore, the China NB has failed to elaborate on its assertions of security concerns in IEEE 802.1AE-2006 (ISO/IEC/IEEE 8802-1AE:2013), despite numerous requests from IEEE 802 since 2012. IEEE 802 believes that the 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 assertions.

China NB comment 4 on IEEE 802.1AE-2018:

RFC 1213 was updated by RFC 2011, RFC 2012, RFC 2013; in which,
RFC 2011 was Obsoleted by RFC 4293; RFC 2011 was Obsoleted by RFC 4022, RFC 2013 was Obsoleted by RFC 4113.
It is questionable that whether the reference to RFC 1213 is technically advanced.

Proposed Change:

Please check the references.

IEEE 802 response to CN.4 on IEEE 802.1AE-2018:

This standard references IETF RFC 1213 as part of "13.3 Relationships to other MIBs", stating specifically in "13.3.1 System MIB Group" what assumptions are made by this standard concerning the "system" group defined in IETF RFC 3418. The text says:

> "*It is assumed that a system implementing this MIB will also implement the "system" group defined in IETF RFC 3418 (or at least that subset of the system group defined in IETF RFC 1213).*"

This standard does not, therefore, depend on IETF RFC 1213, but does refer to that RFC clarify its assumptions on IETF RFC 3418 implementation. There is no other useful way that would be as informative to the user of the standard as "or at least that subset of the system group defined in IETF RFC 1213". That identified subset is defined (as the text says) in IETF RFC 3418. Differences between IETF RFC 3418 and IETF RFC 1213 are explicitly identified in IETF RFC 3418, so the use of "IETF RFC 1213" as a label for those differences is appropriate. The present standard is not therefore dependent on IETF RFC 1213, however removing the reference from the references list would be editorially problematic, as copy editing would result in restoring the reference.

China NB comment 5 on IEEE 802.1AE-2018:

It is noted that there are lots of references to other projects, for one instance, IEEE 802.1Q. Most of the references are pointing specific technical parts. However, there is no specific date of the referenced document. This does not conform to "For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies."

The same issue also applies for other referenced IEEE standards.

Proposed Change:

Please check the date of referenced IEEE standards.

IEEE 802 response to CN.5 on IEEE 802.1AE-2018:

When there is no date (publication year) for the referenced standard, the most recent publication is the reference. When referring to a specific clause of a referenced standard in the text, IEEE 802.1AE-2018 does include the publication year of that referenced standard in the reference pointer. In this way, IEEE 802.1AE-2018 (revision to ISO/IEC/IEEE 8802-1AE:2013) conforms to the IEEE Standards Association Standards Style Manual, which states:

> *"Dated and/or undated references are allowed in standards. Using undated references helps eliminate the burden of continuous updates to align standards as they are revised, while ensuring that the most up-to-date information on technologies and statutes is referenced (when appropriate). Dated references can be used in certain circumstances, such as when a high degree of specificity is needed. Note that in-text reference to a specific clause, subclause, table, or figure of another document shall be dated even if the undated version of the document is listed in the normative references. "*

IEEE 802.1 Working Group could not find document references in the text that were non-conformant to this provision in the IEEE SA Standards Style Manual. The China NB is welcome to provide a specific citation(s) for any references that they would like to point out.

China NB comment 6 on IEEE 802.1AE-2018:

14.5 Default Cipher Suite (GCM-AES-128) and 14.6 GCM-AES-256 further specify that the mandatory cryptographic algorithm in implementation of the standard is AES. However, policy and regulation limitations on application of cryptographic algorithm differ from countries and regions. In addition, there are many other international algorithms for choice. Therefore, it is unreasonable to specify cryptographic algorithms as mandatory implementation in this standard.

The reply in 6N16753 said that "It was not within the scope of the 802.1AEcg project to change the Cipher Suites, and no such changes were made". In this new version of IEEE 802.1AE, this should be considered carefully.

Proposed change:

Noting that in TMB Resolution 70/2018 (72nd meeting of the Technical Management Board) regarding Legal statements in ISO deliverables,

• text relating to compliance with contractual obligations, legal requirements and government regulations exists in many ISO standards; and

• ISO deliverables can be used to complement such requirements and serve as useful tools for all related stakeholders (which can include government authorities and industry players);

ISO clarifies that, for all ISO deliverables:

a) Statements that include an explicit requirement or recommendation to comply with any specific law, regulation or contract (such as a normative reference to such requirements), or portion thereof, are not permitted;

b) Statements related to legal and regulatory requirements that do not violate point a) are permitted;

It is then suggested that the text shall make it clear that "Cryptographic algorithms to be applied to information security mechanism may be subject to national and regional regulations. In this International Standard, cryptographic algorithms are instantiated, and may be chosen according to specific requirements in different countries and regions."

IEEE 802 response to CN.6 on IEEE 802.1AE-2018:

ISO/IEC/IEEE 8802-1AE:2013 and the proposed revision in IEEE 802.1AE-2018 do not contain any statements that violate TMB Resolution 70/2018 (per point a above). There is no reference to any specific law, regulation or contract in this standard. Furthermore, all standards need to have mandatory-to-implement options to ensure interoperability, which is a primary purpose of international standardization.

The mandatory-to-implement Default Cipher Suite, GCM-AES-128, specified in ISO/IEC/IEEE 802.1AE-2018 (revision to ISO/IEC/IEEE 8802-1AE:2013) was chosen because it is well vetted, internationally designed, and recognized. 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. 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).