Comments on pre-ballots in ISO/IEC JTC1 SC6:

IEEE 802.1Q-2018

Canada comment

Canada welcomes this update to ISO/IEC/IEEE 8802-1Q:2016

China 1

IEEE 802.1Q-2018 is IEEE 802.1Q-2014 as amended by its 7 amendments and 1 corrigendum.

Regarding IEEE 802.1QTM-2014 project, China NB has already submitted the comments during its 60-day ballot and FDIS ballot against the references to IEEE 802.1X, which has security problems such as "cannot achieve the real mutual authentication between the Supplicant and Authenticator", etc.

However, there is no further steps taken in this new 2018 version to resolve those comments. IEEE 802.1X is still the normative reference in IEEE 802.1Q-2018 and IEEE 802.1X is used in Clause 8.13.9, 10.1, 25.2 etc.

Therefore, China NB cannot support submission of IEEE 802.1Q-2018 for FDIS ballot.

IEEE 802.1Xck-2018

China 1

This proposal does not give a specific scheme to protect network configuration data constructed by YANG Model.

Proposed change: Specify the protection scheme for network configuration data constructed by YANG Model.

In the referred clauses, this amendment specifies using MACSec (defined by IEEE 802.1AE) to protect the security of the network connected to YANG model data. However, China NB has pointed out the security problems of MACSec for several times during the previous ballots, e.g. 6N15556 and 6N15770. Those comments were not disposed reasonably. It is noted that the 2018 version of IEEE 802.1AE is under 60-day ballot. Please refer to the comments for 6N16880.

IEEE 802.1AE-2018

China 1-

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.

China 2

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.

China 3

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.

China 4

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.

China 5

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. Please check the date of referenced IEEE standards.

China 6

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.”