IEEE 802.3 Ethernet Working Group
DRAFT Liaison Communication

Source:	IEEE 802.3 Working Group[1]	
To:	KwanHoo Shin	ISO/IEC JTC 1/SC 6 Secretariat kyleshin7@tta.or.kr
CC:	Konstantinos Karachalios	Secretary, IEEE-SA Standards Board Secretary, IEEE-SA Board of Governors sasecretary@ieee.org
	Paul Nikolich	Chair, IEEE 802 LMSC p.nikolich@ieee.org
	Adam Healey	Vice-chair, IEEE 802.3 Ethernet Working Group adam.healey@broadcom.com
	Pete Anslow	Secretary, IEEE 802.3 Ethernet Working Group panslow@ciena.com
	Andrew Myles	Chair, IEEE 802 JTC1 Standing Committee amyles@cisco.com
	Jodi Haasz	Manager, Operational Program Management, IEEE-SA j.haasz@ieee.org
From:	David Law	Chair, IEEE 802.3 Ethernet Working Group dlaw@hpe.com
Subject:	Liaison reply to China NB comments on the IEEE Std 802.3cb-2018 and IEEE Std 802.3-2018 60-day ballots	
Approval:	Agreed to at IEEE 802.3 interim meeting, Salt Lake City, UT, USA, 23rd May 2019	

Dear ISO/IEC JTC 1 SC 6 Secretariat,

IEEE 802.3 would like to thank China NB for their review and comment on the following ballots.

- IEEE Std 802.3cb-2018 60-day ballot (comments provided in document 6N16889)
- IEEE Std 802.3-2018 60-day ballot (comments provided in document 6N16892)

Please find below the comment and proposed changes as received followed by the response of the IEEE 802.3 Ethernet Working Group.

[1] This document solely represents the views of the IEEE 802.3 Working Group, and does not necessarily represent a position of the IEEE, the IEEE Standards Association, or IEEE 802.

6N16889, CN-1 (IEEE Std 802.3cb-2018):

Comment:

IEEE 802.3cb is the amendment of IEEE 802.3-2018. We've noticed that IEEE 802.3-2018 is also under 60-day ballot in SC 6 (and later than this proposal), i.e. IEEE 802.3-2018 is not approved. However, the amendment of IEEE 802.3-2018 has been submitted for approval. This do not comply with the procedure of developing international standards. Besides, an amendment based on a standard that has not been published will lack the necessary and stable reference and support in terms of technical aspects. China NB can not support the project submit to FDIS ballot at this stage.

Proposed change:

[None]

Response from the IEEE 802.3 Ethernet Working Group:

The FDIS ballot for IEEE Std 802.3cb-2018 has been requested to be held until the completion of the FDIS ballot on IEEE Std 802.3-2018.

6N16889, CN-2 (IEEE Std 802.3cb-2018):

Comment:

China NB has submitted comments on IEEE 802.3 project for several times in the past. It is a pity that IEEE 802.3-2018 (a collection of IEEE 802.3-2015 and all its amendments) and this amendment did not make effort on specifying security mechanism or technical features of security, and the proposal did not include or reference any security mechanisms.

Regarding this comment, IEEE 802.3 WG has been alleging that IEEE 802.3 is security agnostic and people can use any security mechanism. In fact, network standards rely severely on security mechanisms. The security of Ethernet is an important part of cyber space security. The lack of security mechanisms will introduce various security threats to Ethernet, such as forgery devices, communications from eavesdropping and tampering. In addition, due to the lack of necessary guidance, the implementer selecting any security mechanism brings risks like potential compatibility problems. Apart from this, the selected security mechanisms themselves may also have problems, which lead to security risks in systems that complying with the proposal. Therefore, it is disastrous to apply any security mechanism to the Ethernet for this approach might weaken Ethernet security and endanger other networks.

Proposed change:

It is strongly suggested that IEEE 802.3 and its amendments specify security mechanisms, or at least specify their references on security mechanism.

Response from the IEEE 802.3 Ethernet Working Group:

Potential compatibility problems and potential issues with chosen security mechanisms are among the reasons that IEEE 802.3 remains security agnostic. This approach enables the users of Ethernet networks to select the correct security mechanism, from those available at the time, and at the correct level (e.g., link, application) to satisfy the user's security requirements.

6N16892, CN1 (IEEE Std 802.3-2018):

Comment:

Standard for Ethernet is quite huge (over 5000 pages). The current edition is a collection of IEEE 802.3 -2015 and its amendments. From the form of text, each section is separate and contains its own overview, annexes and page numbers, which cause confusion when referencing.

Proposed change:

Maybe the text can be re-organized into several parts, taking ISO standard system as an instance (Part 1, Part 2,…), to facilitate reading and referencing.

Response from the IEEE 802.3 Ethernet Working Group:

The IEEE 802.3 Ethernet Working Group has considered a number of approaches to organizing the IEEE 802.3 Standard for Ethernet and considers publication of the standard as eight separate sections to be the best approach. Clause and annex numbering is continuous across sections hence any portion of the standard is unambiguously referenced by its subclause or annex number.

6N16892, CN2 (IEEE Std 802.3-2018):

Comment:

Clauses like 5.2.1 and 30.1 refer that "The improper use of some of the facilities described in this subclause may cause serious disruption of the network. In accordance with ISO management architecture, any necessary security provisions should be provided by the Agent in the Local System Environment. This can be in the form of specific security features or in the form of security features provided by the peer communication facilities."

The problem is that the text does not provide specific provisions or any guidance about security features that should be met, and necessary security techniques are not given.

Proposed change:

Related references or indexes could be introduced in general for guidance.

Response from the IEEE 802.3 Ethernet Working Group:

The scope of IEEE 802.3 does not include the setting of provisions or any guidance with respect to security. IEEE 802.3 is security agnostic and allows the user to run any security protocol over an Ethernet network that satisfies that user's security requirements.

6N16892, CN3 (IEEE Std 802.3-2018):

Comment:

China NB has submitted comments on IEEE 802.3 project for several times in the past. It is a pity that IEEE 802.3-2018 did not make effort on specifying security mechanism or technical features of security, and the proposal did not include or reference any security mechanisms.

Regarding this comment, IEEE 802.3 WG has been alleging that IEEE 802.3 is security agnostic and people can use any security mechanism. In fact, network standards rely severely on security mechanisms. The security of Ethernet is an important part of cyber space security. The lack of security mechanisms will introduce various security threats to Ethernet, such as

forgery devices, communications from eavesdropping and tampering. In addition, due to the lack of necessary guidance, the implementer selecting any security mechanism brings risks like potential compatibility problems. Apart from this, the selected security mechanisms themselves may also have problems, which lead to security risks in systems that complying with the proposal. Therefore, it is disastrous to apply any security mechanism to the Ethernet for this approach might weaken Ethernet security and endanger other networks.

Proposed change:

It is strongly suggested that IEEE 802.3 and its amendments specify security mechanisms, or at least specify their references on security mechanism.

Response from the IEEE 802.3 Ethernet Working Group:

Potential compatibility problems and potential issues with chosen security mechanisms are among the reasons that IEEE 802.3 remains security agnostic. This approach enables the users of Ethernet networks to select the correct security mechanism, from those available at the time, and at the correct level (e.g., link, application) to satisfy the user's security requirements.

Sincerely,
David Law
Chair, IEEE 802.3 Ethernet Working Group