IEEE 802.3 Ethernet Working Group Draft
Liaison Communication

Source:	IEEE 802.3 Working Group[1]	
To:	Jungyup Oh	ISO/IEC JTC 1/SC 6 Secretariat houman@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
	Jon Lewis	Secretary, IEEE 802.3 Ethernet Working Group jon.lewis@dell.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 IEEE Std 802.3-2018 FDIS ballot	
Approval:	Agreed to at IEEE 802.3 plenary meeting [date]	

Dear ISO/IEC JTC 1 SC 6 Secretariat,

IEEE 802.3 would like to thank China NB for their review and comment on the IEEE Std 802.3-2018 FDIS ballot.

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

Comment CN1:

China has noticed the response in 6N16971. However, the reply did not properly resolve the following technical concerns.

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 for guidance.

[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.

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."

Although some warning hints were given, neither specifying any necessary security mechanisms, nor including/referencing any guidance or specifications for security features, would bring no benefit to avoid the "serious disruption". Furthermore, this sentence shifts security issues to "Agent in the Local System Environment ". The due technology duty was escaped from the description, and there isn't any implementation guarantee can be derived from the proposal.

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 mechanisms for network management. IEEE 802.3 is security agnostic and allows the user to implement any security mechanism that satisfies that user's security requirements for network management.

Comment CN2:

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:

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 this proposal the interpretation of the lack of security mechanism is "Security agnostic".

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