IEEE 802.3 Ethernet Working Group <mark>Draft</mark>
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 802.3.2-2019 60-day pre-ballot

Approval: Agreed to at IEEE 802.3 interim meeting <mark>[date]</mark>

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 802.3.2-2019 60-day pre-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:

This proposal defines YANG modules for various Ethernet devices specified in IEEE Std 802.3. China NB has submitted comments on IEEE 802.3 project for several times in the past for its not specifying security mechanism or technical features of security, nor referencing any security mechanisms.

Also for this proposal, there is no specific protection scheme for network configuration data constructed by YANG model, hence will lead to potential security risks.

---

[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.

Proposed change:

Highly recommend to specify security mechanisms or reference security mechanisms for data protection.

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:

IEEE 802.1Q (which references IEEE 802.1X technology) is the normative reference of this proposal. Figure 7-5 also use IEEE 802.1Q bridge. China NB has voted against IEEE 802.1Q for several times and the comments about IEEE 802.1Q can be found in 6N17175.

Proposed change:

Resolve the technical flaws (security problems) of the referenced standard.

Response from the IEEE 802.3 Ethernet Working Group:

As was noted in the response to 6N17175, IEEE Std 802.1Q explains how it can be used in conjunction with IEEE Std 802.1X (approved as ISO/IEC/IEEE 8802-1X:2013). IEEE Std 802.1Q is not based on nor does it depend on the use of IEEE Std 802.1X-2010. Instead, it is provided as an illustrative example to provide additional security through port-based network access control. We also refer the China NB to previous rebuttals of similar claims of defects in IEEE Std 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013).

Sincerely,
David Law
Chair, IEEE 802.3 Ethernet Working Group