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

The voting results on IEEE 802.1Xck-2018:

- Support need for ISO standard? Passed 10/0/8
- Support this submission being sent to FDIS? 8/1/9
- 2 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 802.1Xck-2018:

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.

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

Equipment conforming to IEEE 802.1Xck can be used in a variety of environments, each of which has a preferred protocol for network configuration. YANG is a data model for use with a variety of network configuration protocols; one example is NETCONF. IETF RFC 6242 specifies NETCONF over Secure Shell (SSH). Other network configuration protocols specify their own network security. Specifically, see Clause 14.2, Security Considerations, which specifies

> *"The YANG modules defined in Clause 14 are designed to be accessed via the NETCONF protocol (IETF RFC 6241 [B23]). The lowest NETCONF layer is the secure transport layer. It is mandatory to implement secure transport via the NETCONF Protocol over Secure Shell (SSH) (IETF RFC 6242 [B24]). The NETCONF access control model (IETF RFC 6536) provides the means to restrict access for particular NETCONF users to a pre-configured subset of all available NETCONF protocol operations and content."*

The network configuration protocol NETCONF is provided as an example; equipment suppliers must determine what is appropriate for each environment.

China NB comment 2 on IEEE 802.1Xck-2018:

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 response to CN.2 on IEEE 802.1Xck-2018:

The documents referenced in the China NB ballot (6N15556 and 6N15770) are the Summary of Voting on IEEE 802.1AE-2006 (ISO/IEC/IEEE 8802-1AE:2013) documents which date from 2012 and 2013; responses to these comments were submitted from IEEE 802 at that time. The general assertions raised in the China NB's ballots 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 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.

Since that time, however, the China NB has failed to substantiate these assertions, despite numerous requests from IEEE 802. The invitation for a representative of the China NB (as well as representative from other interested SC6 NBs) to attend an IEEE 802 Plenary meeting remains open.

IEEE 802 believes that the security defects asserted by the China NB have all been shown to be not valid and will not make changes to IEEE 802.1Xck-2018 without substantiation of these assertions.