This provides responses to comments on the FDIS ballot on ISO/IEC/IEEE 8802-1AS:2021/FDAmd 2.

The voting results on ballot ISO/IEC/IEEE 8802-1AS:2021/FDAmd 2:

- Do you approve the technical content of the final draft? Passed 12/0/11
- 1 comment with the China NB Abstention vote.

The comments have been processed using the mechanisms defined and agreed in 6N15606. This document provides the responses from IEEE 802[1] to the comments by China NB on this ballot.

China NB comment 1 on ISO/IEC/IEEE 8802-1AS:2021/FDAmd 2:

ISO/IEC/IEEE 8802-1AS:2021/FDAmd 2 is an amendment to IEEE 802.1AS-2020.
China voted against IEEE 802.1AS-2020 FDIS ballot with comments for its reference to IEEE 802.1x and IEEE 802.1AE, which included fundamental technical defects, but the comments was not properly addressed and resolved.
China cannot support the amendment to IEEE 802.1AS to be published as an international standard.

Proposed Change:
The security problems with MACsec must be carefully resolved before using it for security protection in this proposal.

IEEE 802 response to CN.1 on ISO/IEC/IEEE 8802-1AS:2021/FDAmd 2:

To clarify, IEEE Std 802.1ASdn-2024 is an amendment to IEEE Std 802.1AS™-2020, which specifies a YANG data model that allows configuration and state reporting for all managed objects of the base standard. This amendment does not specify, nor does it refer to IEEE Std 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013) or IEEE Std 802.1AE-2018 (ISO/IEC/IEEE 8802-1AE:2020 (Ed2)).

Furthermore, IEEE 802 believes that none of the alleged security problems asserted by the China NB have been shown to be valid. IEEE 802 has supplied a number of communications about the security technology specified in the IEEE 802 security standards: explaining why attacks referenced in China NB contributions are not effective (and will fail); illustrating the use of certificates in IEEE 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013); and describing how the use of the mutual authentication methods specified in IEEE Std 802.1X does not expose the public network or its user to (unspecified) security problems.

The China NB has repeatedly claimed there are “security problems” or “fundamental technical defects”; however, these assertions have not been substantiated, despite requests for further information 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 alleged security defects asserted by the China NB are not valid. Without technical substantiation of any related concerns, IEEE 802 cannot consider modification of the existing IEEE 802 standards.

[1] This document solely represents the views of the IEEE 802 LAN/MAN Standards Committee, and does not necessarily represent a position of IEEE or the IEEE Standards Association. This Liaison Communication is for information only. Any material excerpted from IEEE copyrighted Works requires permission from IEEE (stds-copyright@ieee.org).

Unapproved Draft