

IEEE 802.3 Ethernet Working Group
Draft Liaison Communication

Source: IEEE 802.3 Working Group¹

To: Jungyup Oh ISO/IEC JTC 1/SC 6 Secretariat
[REDACTED]

CC: Konstantinos Karachalios Secretary, IEEE-SA Standards Board
Secretary, IEEE-SA Board of Governors
[REDACTED]

Paul Nikolich Chair, IEEE 802 LMSC
[REDACTED]

Adam Healey Vice-chair, IEEE 802.3 Ethernet Working Group
[REDACTED]

Jon Lewis Secretary, IEEE 802.3 Ethernet Working Group
[REDACTED]

Andrew Myles Chair, IEEE 802 JTC1 Standing Committee
[REDACTED]

Jodi Haasz Senior Manager, Operational Program Management,
IEEE-SA
[REDACTED]

From: David Law Chair, IEEE 802.3 Ethernet Working Group
[REDACTED]

Subject: Liaison reply to China NB comments on ballots

Approval: Agreed to at IEEE 802.3 interim teleconference meeting, 15 September 2022

Dear ISO/IEC JTC 1 SC 6 Secretariat,

The IEEE 802.3 Ethernet Working Group thanks China NB for their review and comment on the following ballots.

- IEEE Std 802.3cv-2021, ISO/IEC/IEEE 8802-3:2021/FDAmD 12 (Ed 3)
- IEEE Std 802.3cp-2021, ISO/IEC/IEEE 8802-3:2021/FDAmD 13 (Ed 3)
- IEEE Std 802.3ct-2021, ISO/IEC/IEEE 8802-3:2021/FDAmD 14 (Ed 3)

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

Sincerely,
David Law
Chair, 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.

| IEEE Std 802.3cv-2021, ISO/IEC/IEEE 8802-3:2021/FDAmD 12 (Ed 3) | |
|---|---|
| Comment CN1 | <p>IEEE 802.3cv-2021 is the amendment of IEEE 802.3-2018 as amended by IEEE 802.3cb-2018, 802.3bt-2018, 802.3cd-2018, 802.3cn-2019, 802.3cg-2019, 802.3cq-2020, 802.3cm-2020, 802.3ch-2020, 802.3ca-2020, 802.3cr-2021 and 802.3cu -2021.</p> <p>Neither IEEE 802.3-2018 nor its amendments specify security mechanism of Ethernet, and also the proposal does not reference any security mechanisms. China has submitted this comment for many times during development of IEEE 802.3.</p> <p>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 standard. Therefore, it is disastrous to apply any security mechanism to the Ethernet for this approach might weaken Ethernet security and endanger other networks.</p> <p>At the engineering implementation level, amendments of IEEE 802.3 must be implemented at the basis of IEEE 802.3 architecture (because the technology involved in the amendment cannot be implemented separately). This objectively strengthens the implementation and promotion of standards with technical defects (no security mechanism defined resulting in huge security risks). Furthermore, the application and deployment of products conforming to the base standards will further aggravate the security risks of the network.</p> <p>China has submitted the same comments with 60-day ballot, but the comments were not properly addressed.</p> |
| Proposed change | It is strongly suggested that IEEE 802.3 and its amendments specifying security mechanisms. |
| Response | 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. 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. |

| IEEE Std 802.3cp-2021, ISO/IEC/IEEE 8802-3:2021/FDAmD 13 (Ed 3) | |
|---|--|
| <p>Comment CN1</p> | <p>IEEE 802.3cp-2021 is the amendment of IEEE 802.3-2018 as amended by IEEE 802.3cb-2018, 802.3bt-2018, 802.3cd-2018, 802.3cn-2019, 802.3cg-2019, 802.3cq-2020, 802.3cm-2020, 802.3ch-2020, 802.3ca-2020, 802.3cr-2021, 802.3cu-2021 and 802.3cv-2021.</p> <p>Neither IEEE 802.3-2018 nor its amendments specify security mechanism of Ethernet, and also the proposal does not reference any security mechanisms. China has submitted this comment for many times during development of IEEE 802.3.</p> <p>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 standard. Therefore, it is disastrous to apply any security mechanism to the Ethernet for this approach might weaken Ethernet security and endanger other networks.</p> <p>At the engineering implementation level, amendments of IEEE 802.3 must be implemented at the basis of IEEE 802.3 architecture (because the technology involved in the amendment cannot be implemented separately). This objectively strengthens the implementation and promotion of standards with technical defects (no security mechanism defined resulting in huge security risks). Furthermore, the application and deployment of products conforming to the base standards will further aggravate the security risks of the network.</p> <p>China has submitted the same comments with 60-day ballot, but the comments were not properly addressed.</p> |
| <p>Proposed change</p> | <p>It is strongly suggested that IEEE 802.3 and its amendments specifying security mechanisms.</p> |
| <p>Response</p> | <p>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. 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.</p> |

| IEEE Std 802.3ct-2021, ISO/IEC/IEEE 8802-3:2021/FDAmD 14 (Ed 3) | |
|---|--|
| Comment CN1 | <p>IEEE 802.3cp-2021 is the amendment of IEEE 802.3-2018 as amended by IEEE 802.3cb-2018, 802.3bt-2018, 802.3cd-2018, 802.3cn-2019, 802.3cg-2019, 802.3cq-2020, 802.3cm-2020, 802.3ch-2020, 802.3ca-2020, 802.3cr-2021, 802.3cu-2021, 802.3cv-2021 and 802.3ct-2021.</p> <p>Neither IEEE 802.3-2018 nor its amendments specify security mechanism of Ethernet, and also the proposal does not reference any security mechanisms. China has submitted this comment for many times during development of IEEE 802.3.</p> <p>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 standard. Therefore, it is disastrous to apply any security mechanism to the Ethernet for this approach might weaken Ethernet security and endanger other networks.</p> <p>At the engineering implementation level, amendments of IEEE 802.3 must be implemented at the basis of IEEE 802.3 architecture (because the technology involved in the amendment cannot be implemented separately). This objectively strengthens the implementation and promotion of standards with technical defects (no security mechanism defined resulting in huge security risks). Furthermore, the application and deployment of products conforming to the base standards will further aggravate the security risks of the network.</p> <p>China has submitted the same comments with 60-day ballot, but the comments were not properly addressed.</p> |
| Proposed change | It is strongly suggested that IEEE 802.3 and its amendments specifying security mechanisms. |
| Response | 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. 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. |