IEEE 802.3 Ethernet Working Group
Liaison Communication

Source: IEEE 802.3 Working Group[1]

To:	Jungyup Oh	ISO/IEC JTC 1/SC 6 Secretariat
CC:	Konstantinos Karachalios	Secretary, IEEE-SA Standards Board Secretary, IEEE-SA Board of Governors
	Paul Nikolich	Chair, IEEE 802 LMSC
	Adam Healey	Vice-chair, IEEE 802.3 Ethernet Working Group
	Jon Lewis	Secretary, IEEE 802.3 Ethernet Working Group
	Andrew Myles	Chair, IEEE 802 JTC1 Standing Committee
	Jodi Haasz	Senior Manager, Operational Program Management, IEEE-SA
From:	David Law	Chair, IEEE 802.3 Ethernet Working Group

Subject: Liaison reply to China NB comments on ballots

Approval: Agreed to at IEEE 802.3 interim teleconference meeting, 20 January 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 802.3cb-2018, ISO/IEC/IEEE 8802-3:2021/FDAmd 1 (Ed 3)
- IEEE Std 802.3bt-2018, ISO/IEC/IEEE 8802-3:2021/FDAmd 2 (Ed 3)
- IEEE Std 802.3cd-2018, ISO/IEC/IEEE 8802-3:2021/FDAmd 3 (Ed 3)
- IEEE Std 802.3cg-2019, ISO/IEC/IEEE 8802-3:2021/FDAmd 5 (Ed 3)
- IEEE Std 802.3ca-2020, ISO/IEC/IEEE 8802-3:2021/FDAmd 9 (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 802.3cb-2018, ISO/IEC/IEEE 8802-3:2021/FDAmd 1 (Ed 3)	
Comment CN1	IEEE 802.3cb-2018 is the amendment 1 of IEEE 802.3-2018. 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 the 60-day ballots and FDIS ballots on IEEE 802.3 proposals. 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. 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.
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.
Comment CN2	ISO/IEC/IEEE 8802-3:2021/FDAmd 1 (Ed 3) is the first amendment of ISO/IEC/IEEE 8802-3:2021. As indicated on the cover pages of the other IEEE 802.3 amendments, the subsequent amendments are based on IEEE 802.3-2018 as amended by the previous amendments. From the procedure aspect, it is very confused that amendment 4,6,7,8 of IEEE 802.3-2018 have already finished FDAmd ballots before this amendment.
Proposed change	The approval process of amendments should follow the logic order.
Response	The amendments were intended to be balloted in the correct order. Moving forward, IEEE will inform ISO of the ordering of amendments.

IEEE Std 802.3bt-2018, ISO/IEC/IEEE 8802-3:2021/FDAmd 2 (Ed 3)	
Comment CN1	IEEE 802.3bt-2018 is an amendment of IEEE 802.3-2018 as amended by IEEE 802.3cb-2018. 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 the 60-day ballots and FDIS ballots on IEEE 802.3 proposals. 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. 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.
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.
Comment CN2	ISO/IEC/IEEE 8802-3:2021/FDAmd 2 is the Amendment 2 of ISO/IEC/IEEE 8802-3:2021. As indicated on the cover pages of the other IEEE 802.3 amendments, the subsequent amendments are based on IEEE 802.3-2018 as amended by the previous amendments. From the procedure aspect, it is very confused that amendment 4,6,7,8 of IEEE 802.3-2018 have already finished FDAmd ballots before this amendment.
Proposed change	The approval process of amendments should follow the logic order.
Response	The amendments were intended to be balloted in the correct order. Moving forward, IEEE will inform ISO of the ordering of amendments.

IEEE Std 802.3cd-2018, ISO/IEC/IEEE 8802-3:2021/FDAmd 3 (Ed 3)	
Comment CN1	IEEE 802.3cd-2018 is an amendment of IEEE 802.3-2018 as amended by IEEE 802.3cb-2018 and IEEE 802.3bt-2018. 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 the 60-day ballots and FDIS ballots on IEEE 802.3 proposals. 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. 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.
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.
Comment CN2	ISO/IEC/IEEE 8802-3:2021/FDAmd 3 is the Amendment 3 of I ISO/IEC/IEEE 8802-3:2021. As indicated on the cover pages of the other IEEE 802.3 amendments, the subsequent amendments are based on IEEE 802.3-2018 as amended by the previous amendments. From the procedure aspect, it is very confused that amendment 4,6,7,8 of IEEE 802.3-2018 have already finished FDAmd ballots before this amendment.
Proposed change	The approval process of amendments should follow the logic order.
Response	The amendments were intended to be balloted in the correct order. Moving forward, IEEE will inform ISO of the ordering of amendments.

IEEE Std 802.3cg-2019, ISO/IEC/IEEE 8802-3:2021/FDAmd 5 (Ed 3)	
Comment CN1	IEEE 802.3cg-2019 is an amendment to IEEE 802.3-2018 as amended by IEEE Std 802.3cb™-2018, IEEE Std 802.3bt™-2018, IEEE Std 802.3cd™-2018 and IEEE Std 802.3cn™-2019. 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 the 60-day ballots and FDIS ballots on IEEE 802.3 proposals. 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. 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.
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.
Comment CN2	As indicated on the cover pages of the other IEEE 802.3 amendments, the subsequent amendments are based on IEEE 802.3-2018 as amended by the previous amendments. From the procedure aspect, it is very confused that amendment 6,7,8 of IEEE 802.3-2018 have already finished FDAmd ballots before this amendment 5.
Proposed change	The approval process of amendments should follow the logic order.
Response	The amendments were intended to be balloted in the correct order. Moving forward, IEEE will inform ISO of the ordering of amendments.

IEEE Std 802.3ca-2020, ISO/IEC/IEEE 8802-3:2021/FDAmd 9 (Ed 3)	
Comment CN1	IEEE Std 802.3ca™-2020 is an amendment to IEEE Std 802.3™-2018 as amended by IEEE Std 802.3cb™-2018, IEEE Std 802.3bt™-2018, IEEE Std 802.3cd™-2018, IEEE Std 802.3cn™-2019, IEEE Std 802.3cg™-2019, IEEE Std 802.3cq™-2020, IEEE Std 802.3cm™-2020 and IEEE Std 802.3ch™-2020. 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 the 60-day ballots and FDIS ballots on IEEE 802.3 proposals. 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. 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.
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.