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 plenary teleconference meeting, 18 November 2021

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 802.3cn-2019, ISO/IEC/IEEE 8802-3:2021/FDAmd 4 (Ed 3)
- IEEE Std 802.3cq-2020, ISO/IEC/IEEE 8802-3:2021/FDAmd 6 (Ed 3)
- IEEE Std 802.3cm-2020, ISO/IEC/IEEE 8802-3:2021/FDAmd 7 (Ed 3)
- IEEE Std 802.3ch-2020, ISO/IEC/IEEE 8802-3:2021/FDAmd 8 (Ed 3)
- IEEE Std 802.3.2-2019, ISO/IEC/IEEE FDIS 8802-3-2
- IEEE Std 802.3cv-2021 60-day ballot
- IEEE Std 802.3cp-2021 60-day ballot
- IEEE Std 802.3ct-2021 60-day ballot

[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.

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

IEEE Std 802.3cn-2019 [ISO/IEC/IEEE 8802-3:2021/FDAmd 4 (Ed 3)]	
Comment CN1	ISO/IEC/IEEE 8802-3:2021/FDAmd 4 is the amendment of IEEE 802.3-2018 as amended by IEEE 802.3cb-2018, 802.3bt-2018 and 802.3cd-2018. Neither IEEE 802.3-2018 nor this amendment specifies 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. 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.

IEEE Std 802.3cq-2020 [ISO/IEC/IEEE 8802-3:2021/FDAmd 6 (Ed 3)]	
Comment CN1	ISO/IEC/IEEE 8802-3:2021/FDAmd 6 is the amendment of IEEE 802.3-2018 as amended by IEEE 802.3cb-2018, 802.3bt-2018, 802.3cd-2018, 802.3cn-2019 and 802.3cg-2019. Neither IEEE 802.3-2018 nor this amendment specifies 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. 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.

IEEE Std 802.3cm-2020 [ISO/IEC/IEEE 8802-3:2021/FDAmd 7 (Ed 3)]	
Comment CN1	ISO/IEC/IEEE 8802-3:2021/FDAmd 7 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 and 802.3cq-2020. Neither IEEE 802.3-2018 nor this amendment specifies 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. 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.

IEEE Std 802.3ch-2020 [ISO/IEC/IEEE 8802-3:2021/FDAmd 8 (Ed 3)]	
Comment CN1	ISO/IEC/IEEE 8802-3:2021/FDAmd 8 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 and 802.3cm-2020. Neither IEEE 802.3-2018 nor this amendment specifies 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. 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.

IEEE Std 802.3.2-2019 [ISO/IEC/IEEE FDIS 8802-3-2]	
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.
Proposed change	Highly recommend to specify security mechanisms or reference security mechanisms for data protection.
Response	The scope of IEEE 802.3.2 does not include the setting of provisions or any guidance with respect to security mechanisms for network management. IEEE 802.3.2 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. China has voted against IEEE 802.3.2-2019 during 60-day ballot and submitted the above technical comments (see 6N17451).The response in 6N17474 from IEEE 802.3 did not accept the recommendations from China and no resolution was given to resolve the security concerns. Therefore, China cannot support the publication of this proposal.
Proposed change	Resolve the technical flaws (security problems) of the referenced standard.
Response	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). It is outside the scope of IEEE 802.3.2 to modify other IEEE 802 or ISO standards.

IEEE Std 802.3cv-2021 60-day ballot	
Comment CN1	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. 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. 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.

IEEE Std 802.3cp-2021 60-day ballot	
Comment CN1	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-2021and 802.3ct-2021. 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. 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.

IEEE Std 802.3ct-2021 60-day ballot	
Comment CN1	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. 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. 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.