

This provides responses to comments on ISO/IEC JTC1/SC6 ballots of IEEE 802.1Qbu-2016 and IEEE 802.1Qbz-2016.

The voting results on IEEE 802.1Qbu-2016 in 6N16541

- Support need for ISO standard? Passed 9/0/11
- Support this submission being sent to FDIS? 7/1/12
- 1 comment was received with the China NB NO vote

The voting results on IEEE 802.1Qbz-2016 in 6N16540

- Support need for ISO standard? Passed 9/0/11
- Support this submission being sent to FDIS? 7/1/12
- 1 comment was received 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 all comments by China NB on both of the ballots.

China NB comment 1 on IEEE 802.1Qbu-2016

IEEE 802.1Qbu-2016 is an amendment to IEEE 802.1Q-2014 that is based on IEEE 802.1x-2010. China has already submitted the comments on IEEE 802.1QTM-2014 during its pre-FDIS ballot and FDIS ballot about the security problems in IEEE 802.1x-2010 that is referenced by IEEE 802.1QTM-2014. Up to now, there is no reasonable and appropriate disposition on Chinese comments. Since IEEE 802.1QbuTM-2016 is based on the standard with technical flaws; therefore, China NB cannot give support on IEEE 802.1Q-2014 and its amendment.

Proposed change: Recommend not referencing the standard with technical flaws or recommend enhancing its security mechanism.

IEEE 802 response to CN.1 on IEEE 802.1Qbu-2016

The China NB's ballot response states it will not approve IEEE 802.1Qbu-2016 because it references IEEE 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013), which the China NB has consistently and repeatedly asserted is defective since at least 2012. However, the China NB has failed to substantiate these assertions, despite numerous requests from IEEE 802. IEEE 802 will not make changes to IEEE 802.1Qbu-2016 without substantiation of these assertions.

Conformance to and use of IEEE 802.1X is not a requirement for conformance to IEEE 802.1Q-2014 in any case.

The general assertions raised in the China NB's ballot 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 of the 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. Specifically,

- In June 2013 in 6N15658 (*IEEE 802 Response to 6N15613*), IEEE 802 explains why none of the attacks described in 6N15613 (*NB' of China's contribution on Effective Attack on IEEE802.1X-the further analysis of 6N15523*) are effective and reveals how the attacks described in the China NB contribution 6N15613 will fail.
- In June 2013 in 6N15646 (*IEEE 802 Response to 6N15523*), IEEE 802 explains why the analysis in 6N15523 (*NB of Switzerland's contribution on a comparative analysis of TePAKA4 and IEEE 802.1X Security*) is flawed, noting it produces erroneous results based on misunderstandings of technology, invalid assumptions, and analysis using an incorrect model.
- In January 2014 in 6N15870 (*IEEE 802 response to SC6N15840 – "Intentional Weaknesses in Information Security Standards and Implementations"*), IEEE 802 responded to non-specific allegations by the China NB about any security standards developed outside ISO. The China NB suggested that such standards contain intentional weaknesses. IEEE 802 responded that the best way to avoid such issues is to develop standards in an open standards process, such as that provided by IEEE 802.

- In January 2014 in 6N15845 (*Explanation of Certificate Use in 802.1X EAP-TLS*), IEEE 802 described the use of certificates in IEEE 802.1.

At the SC6 meeting in Ottawa in early 2014, the China NB and Switzerland NB representatives committed to providing additional technical details to justify their concerns. No such submissions were made to the SC6 meeting in London later that year, and no technical submissions were received subsequently. Furthermore, there has been no technical discussion since that time.

IEEE 802 is eager to hear and discuss further the details of any new concerns about IEEE 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013) from the China NB. On 21 February 2017, IEEE 802 formally invited a representative of the China NB (as well as representative from other interested SC6 NBs) to attend the IEEE 802 Plenary meeting held in Vancouver, Canada the week starting Monday, 13 March 2017. Unfortunately, our invitation was declined by the China NB. However, the invitation remains open. The next suitable venue at which all the IEEE 802 security experts will be in one place is the IEEE 802 plenary meeting in July 2017 in Berlin, Germany.

IEEE 802 believes that the attacks on IEEE 802.1X-2010 described by the China NB have all been shown to be not valid but continues to invite the China NB to submit any additional new technical details for consideration. In the absence of technical substantiation of the claims, IEEE 802 cannot consider modification of the existing IEEE 802 or ISO standards.

China NB comment 1 on IEEE 802.1Qbz-2016

IEEE 802.1Qbz-2016 is an amendment to IEEE 802.1Q-2014 that is based on IEEE 802.1X-2010. China has already submitted the comments on IEEE 802.1Q-2014 during its pre-FDIS ballot and FDIS ballot about the security problems in IEEE 802.1x-2010 that is referenced by IEEE 802.1Q-2014. Up to now, there is no reasonable and appropriate disposition on Chinese comments. Since IEEE 802.1Qbz-2016 is based on the standard with technical flaws; therefore, China NB cannot give support on IEEE 802.1Q-2014 and its amendment.

Proposed change: Recommend not referencing the standard with technical flaws or recommend enhancing its security mechanism.

IEEE 802 response to CN.1 on IEEE 802.1Qbz-2016

The China NB's ballot response states it will not approve IEEE 802.1Qbz-2016 because it references IEEE 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013), which the China NB has consistently and repeatedly asserted is defective since at least 2012. However, the China NB has failed to substantiate these assertions, despite numerous requests from IEEE 802. IEEE 802 will not make changes to IEEE 802.1Qbz-2016 without substantiation of these assertions.

Conformance to and use of IEEE 802.1X is not a requirement for conformance to IEEE 802.1Q-2014 in any case.

The general assertions raised in the China NB's ballot 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 of the 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. Specifically,

- In June 2013 in 6N15658 (*IEEE 802 Response to 6N15613*), IEEE 802 explains why none of the attacks described in 6N15613 (*NB' of China's contribution on Effective Attack on IEEE802.1X-the further analysis of 6N15523*) are effective and reveals how the attacks described in the China NB contribution 6N15613 will fail.
- In June 2013 in 6N15646 (*IEEE 802 Response to 6N15523*), IEEE 802 explains why the analysis in 6N15523 (*NB of Switzerland's contribution on a comparative analysis of TePAKA4 and IEEE 802.1X Security*) is flawed, noting it produces erroneous results based on misunderstandings of technology, invalid assumptions, and analysis using an incorrect model.

- In January 2014 in 6N15870 (*IEEE 802 response to SC6N15840 – “Intentional Weaknesses in Information Security Standards and Implementations”*), IEEE 802 responded to non-specific allegations by the China NB about any security standards developed outside ISO. The China NB suggested that such standards contain intentional weaknesses. IEEE 802 responded that the best way to avoid such issues is to develop standards in an open standards process, such as that provided by IEEE 802.
- In January 2014 in 6N15845 (*Explanation of Certificate Use in 802.1X EAP-TLS*), IEEE 802 described the use of certificates in IEEE 802.1.

At the SC6 meeting in Ottawa in early 2014, the China NB and Switzerland NB representatives committed to providing additional technical details to justify their concerns. No such submissions were made to the SC6 meeting in London later that year, and no technical submissions were received subsequently. Furthermore, there has been no technical discussion since that time.

IEEE 802 is eager to hear and discuss further the details of any new concerns about IEEE 802.1X-2010 (ISO/IEC/IEEE 8802-1X:2013) from the China NB. On 21 February 2017, IEEE 802 formally invited a representative of the China NB (as well as representative from other interested SC6 NBs) to attend the IEEE 802 Plenary meeting held in Vancouver, Canada the week starting Monday, 13 March 2017. Unfortunately, our invitation was declined by the China NB. However, the invitation remains open. The next suitable venue at which all the IEEE 802 security experts will be in one place is the IEEE 802 plenary meeting in July 2017 in Berlin, Germany.

IEEE 802 believes that the attacks on IEEE 802.1X-2010 described by the China NB have all been shown to be not valid but continues to invite the China NB to submit any additional new technical details for consideration. In the absence of technical substantiation of the claims, IEEE 802 cannot consider modification of the existing IEEE 802 or ISO standards.