INTERNATIONAL STANDARD

ISO/IEC/IEEE 8802-1AE

First edition
2013-12

AMENDMENT 3
2018-10

Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks —

Part 1AE: Media access control (MAC) security

AMENDMENT 3: Ethernet data encryption devices

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Réseaux locaux et métropolitains —

Partie 1AE: Sécurité du contrôle d'accès aux supports (MAC)

AMENDEMENT 3:

Reference number
ISO/IEC/IEEE 8802-1AE:2013/Amd.3:2018(E)

© IEEE 2017

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

COPYRIGHT PROTECTED DOCUMENT

© IEEE 2017

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO or IEEE at the respective address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Institute of Electrical and Electronics Engineers, Inc
3 Park Avenue, New York
NY 10016-5997, USA

Email: stds.ipr@ieee.org
Website: www.ieee.org

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted (see www.iso.org/directives).

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see http://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

ISO/IEC/IEEE 8802-1AE:2013/FDAmd 3 was prepared by the LAN/MAN of the IEEE Computer Society (as IEEE Std 802.1AEcg-2017) and drafted in accordance with its editorial rules. It was adopted, under the "fast-track procedure" defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

A list of all parts in the ISO/IEC/IEEE 8802 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

IEEE Std 802.1AEcg™-2017
(Amendment to
IEEE Std 802.1AE™-2006
as amended by
IEEE Std 802.1AEbn™-2011
and IEEE Std 802.1AEbw™-2013)

IEEE Standard for
Local and metropolitan area networks—

Media Access Control (MAC) Security

Amendment 3:
Ethernet Data Encryption devices

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 14 February 2017
IEEE-SA Standards Board

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

Abstract: Ethernet Data Encryption devices (EDEs) are specified in this amendment. An EDE is a two-port bridge that uses MACsec to provide secure connectivity for attached customer bridges, or for attached provider bridges. EDEs may allow the customer (or provider) bridges to continue to use a VLAN Identifier (VID) in transmitted frames to select (as already specified in IEEE Std 802.1Q™) between provider network or provider backbone network services.

Keywords: amendment, authorized port, confidentiality, data origin authenticity, EDE, Ethernet Data Encryption device, IEEE 802.1AE, IEEE 802.1AEcg, integrity, LANs, local area networks, MAC Bridges, MAC security, MAC Service, MANs, metropolitan area networks, port-based network access control, secure association, security, transparent bridging

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2017 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 19 May 2017. Printed in the United States of America.

IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-3725-7 STD22415
Print: ISBN 978-1-5044-3726-4 STDPD22415

IEEE prohibits discrimination, harassment, and bullying. For more information, visit http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Copyright © 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association ("IEEE-SA") Standards Board. IEEE ("the Institute") develops its standards through a consensus development process, approved by the American National Standards Institute ("ANSI"), which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Copyright © 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at http://ieeexplore.ieee.org/browse/standards/collection/ieee or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE-SA Website at http://standards.ieee.org.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: http://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at http://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

Participants

At the time this standard was completed, the IEEE 802.1 working group had the following membership:

Glenn Parsons, *Chair*
John Messenger, *Vice Chair*
Mick Seaman, *Security Task Group Chair, Editor*

SeoYoung Baek
Shenghua Bao
Jens Bierschenk
Steinar Bjornstad
Christian Boiger
Paul Bottorff
David Chen
Feng Chen
Weiying Cheng
Rodney Cummings
János Farkas
Norman Finn
Geoffrey Garner
Eric W. Gray
Craig Gunther
Marina Gutierrez
Stephen Haddock
Mark Hantel
Patrick Heffernan
Marc Holness
Lu Huang
Tony Jeffree
Michael Johas Teener
Hal Keen
Stephan Kehrer
Philippe Klein
Jouni Korhonen
Yizhou Li
Christophe Mangin
Tom McBeath
James McIntosh
Tero Mustala
Hiroki Nakano
Bob Noseworthy
Donald R. Pannell
Walter Pienciak
Michael Potts
Karen Randall
Maximilian Riegel
Dan Romascanu
Jessy V. Rouyer
Eero Ryytty
Soheil Samii
Behcet Sarikaya
Frank Schewe
Johannes Specht
Wilfried Steiner
Patricia Thaler
Paul Unbehagen
Hao Wang
Karl Weber
Brian Weis
Jordon Woods
Nader Zein
Helge Zinner
Juan Carlos Zuniga

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Thomas Alexander
Richard Alfvin
Johann Amsenga
Butch Anton
Nancy Bravin
William Byrd
Juan Carreon
Keith Chow
Charles Cook
Rodney Cummings
Janos Farkas
Matthias Fritsche
Yukihiro Fujimoto
Joel Goergen
Randall Groves
Joseph Gwinn
Stephen Haddock
Marco Hernandez
Werner Hoelzl
Noriyuki Ikeuch
Osamu Ishida
Atsushi Ito
Raj Jain
SangKwon Jeong
Piotr Karocki
Jeritt Kent
Stuart Kerry
Yongbum Kim
Hyeong Ho Lee
James Lepp
Jon Lewis
Elvis Maculuba
Michael McInnis
Michael Montemurro
Michael Newman
Satoshi Obara
Bansi Patel
Arumugam Paventhan
Karen Randall
Alon Regev
Maximilian Riegel
Robert Robinson
Jessy Rouyer
Richard Roy
Mick Seaman
Thomas Starai
Walter Struppler
Patricia Thaler
Thomas Tullia
Mark-Rene Uchida
Prabodh Varshney
George Vlantis
Khurram Waheed
Hung-Yu Wei
Andreas Wolf
Chun Yu Charles Wong
Oren Yuen
Zhen Zhou

Copyright © 2017 IEEE. All rights reserved.
© IEEE 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

When the IEEE-SA Standards Board approved this standard on 14 February 2017, it had the following membership:

Jean-Philippe Faure, *Chair*
Vacant Position, *Vice-Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Chuck Adams
Masayuki Ariyoshi
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Gary Hoffman
Michael Janezic
Thomas Koshy
Joseph L. Koepfinger1
Kevin Lu
Daleep Mohla
Damir Novosel
Ronald C. Petersen
Annette D. Reilly
Robby Robson
Dorothy Stanley
Adrian Stephens
Mehmet Ulema
Phil Wennblom
Howard Wolfman
Yu Yuan

*Member Emeritus

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

Introduction

This introduction is not part of IEEE Std 802.1AEcg-2017, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Security—Amendment 3: Ethernet Data Encryption devices.

The first edition of IEEE Std 802.1AE™ was published in 2006. A first amendment, IEEE Std 802.1AEbn™-2011, added the option of using the GCM-AES-256 Cipher Suite. A second, IEEE Std 802.1AEbw™-2013 added the GCM-AES-XPN-128 and GCM-AES-XPN-256 Cipher Suites. These extended packet numbering Cipher Suites allow more than 2^{32} frames to be protected with a single Secure Association Key (SAK) and so ease the timeliness requirements on key agreement protocols for very high speed (100 Gb/s plus) operation. This third amendment, IEEE Std 802.1AEcg™-2017, specifies Ethernet Data Encryption devices (EDEs).

Relationship between IEEE Std 802.1AE and other IEEE Std 802 standards

IEEE Std 802.1X™-2010 specifies Port-based Network Access Control, and provides a means of authenticating and authorizing devices attached to a LAN, and includes the MACsec Key Agreement protocol (MKA) necessary to make use of IEEE 802.1AE.

IEEE Std 802.1AE is not intended for use with IEEE Std 802.11™ Wireless LAN Medium Access Control. An amendment to that standard, IEEE Std 802.11i™-2004, also makes use of IEEE Std 802.1X™, thus facilitating the use of a common authentication and authorization framework for LAN media to which this standard applies and for Wireless LANs.

Copyright © 2017 IEEE. All rights reserved.
© IEEE 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

Contents

1. Overview 15
   1.2 Scope 15
2. Normative references 16
3. Definitions 18
4. Abbreviations and acronyms 20
5. Conformance 21
   5.1 Requirements terminology 21
   5.2 Protocol Implementation Conformance Statement (PICS) 22
   5.3 Required capabilitiesMAC Security Entity requirements 22
   5.4 Optional capabilitiesMAC Security Entity options 23
   5.5 EDE conformance 24
   5.6 EDE-M conformance 24
   5.7 EDE-CS conformance 25
   5.8 EDE-CC conformance 25
   5.9 EDE-SS conformance 25
6. Secure provision of the MAC Service 26
   6.1 MAC Service primitives and parameters 26
   6.2 MAC Service connectivity 26
   6.4 MAC status parameters 27
   6.5 MAC point-to-point parameters 27
   6.10 Quality of service maintenance 27
7. Principles of secure network operation 29
   7.1 Support of the secure MAC Service by an individual LAN 29
   7.3 Use of the secure MAC Service 30
8. MAC Security Protocol (MACsec) 32
   8.3 MACsec operation 32
9. Encoding of MACsec protocol data units 34
   9.9 Secure Channel Identifier (SCI) 34
10. Principles of MAC Security Entity (SecY) operation 35
   10.1 SecY overview 35
   10.2 SecY functions 35
   10.4 SecY architecture 36
   10.5 Secure frame generation 36
   10.6 Secure frame verification 40
   10.7 SecY management 41
11. MAC Security in Systems 52
   11.1 MAC Service interface stacks 52

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

11.3 MACsec in MAC Bridges ... 52
11.4 MACsec in VLAN-aware Bridges ... 53
11.8 MACsec and multi-access LANs ... 53

13. Management protocol MAC Security Entity MIB ... 55

13.1 Introduction ... 55
13.4 Security considerations ... 55
13.5 Structure of the MIB module ... 56
13.6 Definitions for MAC Security Entity (SecY) MIB definitions ... 62

14. Encoding of MACsec protocol data units ... 100

14.5 Default Cipher Suite (GCM–AES–128) ... 100
14.6 GCM-AES-256 ... 100

15. Ethernet Data Encryption devices ... 101

15.1 EDE characteristics ... 101
15.2 Securing LANs with EDE-Ms ... 102
15.3 Securing connectivity across PBNs ... 104
15.4 Securing PBN connectivity with an EDE-M ... 105
15.5 Securing PBN connectivity with an EDE-CS ... 106
15.6 Securing PBN connectivity with an EDE-CC ... 108
15.7 Securing PBN connectivity with an EDE-SS ... 111
15.8 EDE Interoperability ... 111
15.9 EDEs, CFM, and UNI Access ... 113

16. Using MIB modules to manage EDEs ... 114

16.1 Security considerations ... 114
16.2 EDE-M Management ... 114
16.3 EDE-CS Management ... 114
16.4 EDE-CC and EDE-SS Management ... 114

Annex A (normative) PICS Proforma ... 116

A.5 Major capabilities ... 116
A.9 Secure Frame Verification ... 118
A.12 Additional fully conformant Cipher Suite capabilities ... 122
A.13 Additional variant Cipher Suite capabilities ... 123

Annex B (informative) Bibliography ... 125

Annex D (normative) PICS Proforma for an Ethernet Data Encryption device ... 127

D.1 Introduction ... 127
D.2 Abbreviations and special symbols ... 127
D.3 Instructions for completing the PICS proforma ... 128
D.4 PICS proforma for IEEE Std 802.1AE EDE ... 130
D.5 EDE type and common requirements ... 131
D.6 EDE-M Configuration ... 132
D.7 EDE-CS Configuration ... 132
D.8 EDE-CC Configuration ... 133
D.9 EDE-SS Configuration ... 133

Copyright © 2017 IEEE. All rights reserved.
© IEEE 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

Annex E (informative) MKA operation for multiple transmit SCs 134

Annex F (informative) EDE Interoperability and PAE addresses 136

Annex G (informative) Management and MIB revisions..... 139

G.1 Counter changes..... 140
G.2 Available Cipher Suites..... 141

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

Figures

Figure 7-7 Secure Channel and Secure Association Identifiers 30
Figure 10-4 Management controls and counters for secure frame generation 36
Figure 10-5 Management controls and counters for secure frame verification 38
Figure 10-6 SecY managed objects 43
Figure 11-4 MACsec in an IEEE 802.1D VLAN-unaware MAC Bridge 52
Figure 11-5 IEEE 802.1D VLAN-unaware MAC Bridge Port with MACsec 53
Figure 11-6 Addition of MAC Security to a VLAN-aware MAC Bridge 53
Figure 11-15 An example multi-access LAN 54
Figure 13-1 Secy MIB structure 57
Figure 15-1 EDE-Ms connected by a point-to-point LAN 102
Figure 15-2 EDE-Ms securing a point-to-point LAN between Provider Bridges 103
Figure 15-3 MACsec protected frame traversing a PBN 104
Figure 15-4 EDE-Ms securing point-to-point LAN connectivity across a PBN 105
Figure 15-5 EDE-Ms securing multi-point PBN connectivity 106
Figure 15-6 Example of a network with an EDE-CS 107
Figure 15-7 EDE-CS connected to a PBN S-tagged interface 108
Figure 15-8 Using an EDE-CC with a C-tagged provider service interface 109
Figure 15-9 EDE-CC architecture 110

Copyright © 2017 IEEE. All rights reserved.
© IEEE 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

Tables

Table 10-1 Management controls and SecTAG encoding 39
Table 13-1 Controlled Port service management 59
Table 13-2 Transmit and receive SC management 60
Table 13-3 Transmit and receive statistics 61
Table 13-4 Cipher Suite information 62
Table 15-1 PAE Group Addresses 111
Table 15-2 PAE Group Address use 112
Table F-1 Interoperability scenarios and PAE Addresses 138

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

IEEE Standard for
Local and metropolitan area networks—

Media Access Control (MAC) Security

Amendment 3:
Ethernet Data Encryption devices

NOTE—The editing instructions contained in this amendment define how to merge the material contained therein into the existing base standard and its amendments to form the comprehensive standard.

The editing instructions are shown in ***bold italic***. Four editing instructions are used: change, delete, insert, and replace. ***Change*** is used to make corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using ~~strikethrough~~ (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Deletions and insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editing instructions, change markings, and this NOTE will not be carried over into future editions because the changes will be incorporated into the base standard.

Copyright © 2017 IEEE. All rights reserved.
© IEEE 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

1. Overview

1.2 Scope

Change 1.2 as follows:

The scope of this standard is to specify provision of connectionless user data confidentiality, frame data integrity, and data origin authenticity by media access independent protocols and entities that operate transparently to MAC Clients.

NOTE—The MAC Clients are as specified in IEEE Std 802, ~~IEEE Std 802.2™, IEEE Std 802.1D™,~~ IEEE Std 802.1Q™, and IEEE Std 802.1X™.[1]

To this end it

a) Specifies the requirements to be satisfied by equipment claiming conformance to this standard.
b) Specifies the requirements for MAC Security in terms of provision of the MAC Service and the preservation of the semantics and parameters of service requests and indications.
c) Describes the threats, both intentional and accidental, to correct provision of the service.
d) Specifies security services that prevent, or restrict, the effect of attacks that exploit these threats.
e) Examines the potential impact of both the threats and the use of MAC Security on the Quality of Service (QoS), specifying constraints on the design and operation of MAC Security ~~entities and protocols~~.
f) Models support of the secure MAC Service in terms of the operation of media access control method independent MAC Security Entities (SecYs) within the MAC Sublayer.
g) Specifies the format of the MACsec Protocol Data Unit (MPDUs) used to provide secure service.
h) Identifies the functions to be performed by each SecY, and provides an architectural model of its internal operation in terms of Processes and Entities that provide those functions.
i) ~~Specifies the interface/exchanges between a SecY and its associated and collocated MAC Security Key Agreement Entity (KaY, IEEE Std 802.1X) that provides and updates cryptographic keys.~~
i) Specifies each SecY's use of an associated and collocated Port Access Entity (PAE, IEEE Std 802.1X™) to discover and authenticate MACsec protocol peers, and its use of that PAE's Key Agreement Entity (KaY) to agree and update cryptographic keys.
j) Specifies performance requirements and recommends default values and applicable ranges for the operational parameters of a SecY.
k) Specifies how SecYs are incorporated within the ~~architectural structure within~~ architecture of end stations, ~~and~~ bridges, and two-port Ethernet Data Encryption devices (EDEs).
l) Establishes the requirements for management of MAC Security, identifying the managed objects and defining the management operations for SecYs.
m) Specifies the Management Information Base (MIB) module for managing the operation of MAC Security in TCP/IP networks.
n) Specifies requirements, criteria, and choices of Cipher Suites for use with this standard.

~~This standard does not~~

o) ~~Specify how the relationships between MACsec protocol peers are discovered and authenticated, as supported by key management or key distribution protocols, but makes use of IEEE IEEE Std 802.1X™ to achieve these functions.~~

[1]Notes in text, tables, and figures are given for information only, and do not contain requirements needed to implement the standard.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

2. Normative references

Change the Normative references clause as follows:

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

~~Federal Information Processing Standards FIPS 197, Advanced Encryption Standard, 2001, Advanced Encryption Standard Cyclic Block Chaining (AES-CBC).[1]~~

IEEE Std 802®, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture.[2, 3]

~~IEEE Std 802.1D-2003, IEEE Standards for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges.~~

IEEE Std 802.1Q™, IEEE Standards for Local and Metropolitan Area Networks: Bridges and Bridged Networks ~~Virtual Bridged Local Area Networks~~.

IEEE Std 802.1X-2010™, IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control.

IEEE Std 802.1Xbx-2014™, IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control—Amendment 1: MAC Security Key Agreement Protocol (MKA) Extensions.

IEEE Std 802.1AB™~~-2005~~, IEEE Standards for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity and Discovery.

IEEE Std 802.1AC™, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Service Definition.

~~IEEE Std 802.2™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.~~

IEEE Std 802.3™, IEEE Standard for Ethernet~~Information technology—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.~~

~~IEEE Std 802.11™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.~~

~~IEEE Std 802.11i™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11:~~

---

[1] ~~FIPS publications are available from the National Technical Information Service (NTIS), U. S. Dept. of Commerce, 5285 Port Royal Rd., Springfield, VA 22161 (http://www.ntis.org/).~~

[2] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, ~~P.O. Box 1331,~~ Piscataway, NJ 0885~~45-1331~~, USA. IEEE publications can be ordered on-line from the IEEE Standards website: http://www.standards.ieee.org. Through the IEEE Standards Association, industry, and government support, select IEEE standards are available for download at no charge, see http://www.standards.ieee.org/about/get.

[3] The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

~~Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Media Access Control (MAC) Security Enhancements.~~

~~IEEE Std 802.17™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 17: Resilient packet ring (RPR) access method & physical layer specifications.~~

IETF RFC 1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II, K. McCloghrie, M.T. Rose, March 1991.

IETF RFC 2578, STD 58, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.

IETF RFC 2579, STD 58, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.

IETF RFC 2580, STD 58, Conformance Statements for SMIv2, McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.

IETF RFC 2863, The Interfaces Group MIB using SMIv2, McCloghrie, K. and Kastenholz, F., June 2000.

IETF RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), Preshun, R., ED., December 2002.

~~ISO/IEC 7498-1, Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 1: The Basic Model[4].~~

~~ISO/IEC 7498-2, Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security architecture.~~

ISO/IEC 14882, Information Technology—Programming languages—C++.[4]

~~ISO/IEC 15802-1, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 1: Medium Access Control (MAC) service definition.~~

NIST SP 800-38D, Nov 2007, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.[5]

[4]ISO/IEC publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse (http://www.iso.ch/). ISO/IEC publications are also available in the United States from Global Engineering Documents, 15 Inverness Way East, Englewood, Colorado 80112, USA (http://global.ihs.com/). Electronic copies are available in the United States from the American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (http://www.ansi.org/).

[5]This document is available at http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

3. Definitions

Change the definition of IEEE 802 Local Area Network (LAN) as follows:

3.1 IEEE 802 Local Area Network (LAN): IEEE 802 LANs (also referred to in the text simply as LANs) are LAN technologies that provide a MAC Service equivalent to the MAC Service defined in ~~ISO/IEC 15802-1~~ IEEE Std 802.1AC. IEEE 802 LANs include IEEE Std 802.3 (CSMA/CD), IEEE Std 802.11 (Wireless), IEEE Std 802.17 (Resilient Packet Ring).

Change the definition of Port Identifier as follows:

3.29 Port Identifier: A 16-bit identifier ~~number~~ that ~~is unique within the scope of the address of the port~~ uniquely identifies each of a system's transmit SCs that uses the same MAC address as a component of its SCI.

NOTE—The Port Identifier is not constrained to correspond to any other port number, identifier, or index. There can be more than one SC for a physical port, identifying frames transmitted by separate virtual ports, and more than one SC for a physical or virtual port if that port uses different SCs to transmit frames of different priorities.

Change the definition of Secure Channel Identifier as follows:

3.36 Secure Channel Identifier (SCI): A ~~globally~~ unique identifier for a secure channel, comprises a ~~globally unique~~ MAC Address and a Port Identifier~~, unique within the system allocated that address~~.

NOTE—Key agreement protocols such as MKA (see IEEE Std 802.1X) are responsible for ensuring that each SCI used with a given SAK is unique where a Cipher Suite requires that for nonce construction, as does the Default Cipher Suite (14.5). SCI uniqueness does not rely on MAC Address allocation procedures.

Insert the following definition(s), in the appropriate collating order, renumbering notes as required:

3.41 Ethernet Data Encryption device (EDE): A two-port bridge that transmits and receives frames that are assumed to be unprotected to and from one red-side port, and conditionally relays those frames to and from its other black-side port, protecting and verifying frames transmitted and received on the black-side port using MACsec.

3.42 black-side: Identifies the EDE port that uses MACsec to protect transmitted frames and verify received frames.

3.43 red-side: Identifies the EDE port that does not use MACsec to protect transmitted frames or verify received frames.

3.44 Reserved Address: A group address filtered by a bridge component to restrict the scope of the control protocols using that destination address.

3.45 user priority: In this standard, the priority associated with a transmit request received by a SecY's Controlled Port. The priority associated with a transmit request received by a protocol entity, often a shim, in an interface stack (see IEEE Std 802.1AC).

3.46 access priority: In this standard, the priority associated with a transmit request made by a SecY at its Common Port. The priority associated with a transmit request made by a protocol entity, often a shim, in an interface stack (see IEEE Std 802.1AC).

3.47 edge component: The bridge component in an EDE-CS, EDE-CC, or EDE-SS that is attached to the red-side port.

Copyright © 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

3.48 network component: The bridge component in an EDE-CS, EDE-CC, or EDE-SS that is attached to the black-side port.

3.49 Customer Edge Port: The red-side port of an EDE-CS, EDE-CC, or EDE-SS.

NOTE—The terms *customer* and *provider* applied to the external and internal ports of an EDE-CS are those used by IEEE Std 802.1Q in its description of Provider Edge Bridges and reflect the role of those ports in the layered network architecture. They do not indicate control or ownership of the equipment. In this standard it is convenient to extend the use of those terms to ports that have the same relative relationship to the edge and network components of an EDE-CC or EDE-SS. This is not a suggestion that further variants of PEBs and BEBs be specified, as the existence of additional variants would complicate interoperability, service provision, and the task of this standard.

3.50 Provider Edge Port: A port on the edge component of an EDE-CS, EDE-CC, or EDE-SS that provides internal connectivity to the network component of that EDE.

3.51 Customer Network Port: A port on the network component of an EDE-CS, EDE-CC, or EDE-SS that provides internal connectivity to the edge component of that EDE.

3.52 Provider Network Port: The black-side port of an EDE-CS, EDE-CC, or EDE-SS.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

4. Abbreviations and acronyms

Insert the following abbreviations in the appropriate collating sequence:

EDE	Ethernet Data Encryption device
EDE-CC	Ethernet Data Encryption device with red-side recognition of C-TAGs and black-side addition and removal of C-TAGs
EDE-CS	Ethernet Data Encryption device with red-side recognition of C-TAGs and black-side addition and removal of S-TAGs
EDE-M	VLAN-unaware Ethernet Data Encryption device operating as a Customer Bridge
EDE-SS	Ethernet Data Encryption device with red-side recognition of S-TAGs and black-side addition and removal of S-TAGs
MKA	MACsec Key Agreement protocol (IEEE Std 802.1X)
PCP	Priority Code Point (IEEE Std 802.1Q)
UNI	User Network Interface (IEEE Std 802.1Q)

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

5. Conformance

Change Clause 5 as follows:

A claim of conformance to this standard is a claim that the behavior of an implementation of a MAC Security Entity (SecY) meets the requirements of this standard as they apply to the operation of the MACsec protocol, management of its operation, and provision of service to the protocol clients of the SecY, as revealed through externally observable behavior of the system of which the SecY forms a part.

A claim of conformance may be a claim of full conformance, or a claim of conformance with Cipher Suite variance, as specified in 5.4.

Conformance to this standard does not ensure that the system of which the MAC Security implementation forms a part is secure, or that the operation of other protocols used to support MAC Security, such as key management and network management do not provide a way for an attacker to breach that security.

Conformance to this standard does not require any restriction as to the nature of the system of which a SecY forms part other than as constrained by the SecY's required and optional capabilities (5.3, 5.4). Clause 11 describes the use of SecYs within a number of different types of systems. These include, but are not limited to, systems specified in IEEE Std 802.1Q and those that make use of IEEE Std 802.1X. Successful interoperable use of MACsec in those systems also requires conformance to those standards. In addition Clause 15 of this standard makes use of components specified in IEEE Std 802.1Q to define further systems, Ethernet Data Encryption devices (EDEs), whose purpose is to secure the MAC Service within networks comprising bridging systems specified by IEEE Std 802.1Q in a way that is transparent to the operation of those bridging systems. Additional claims of conformance can be made to this standard in respect of EDEs (5.5–5.7).

5.1 Requirements terminology

For consistency with existing IEEE and IEEE 802.1 standards, requirements placed upon conformant implementations of this standard are expressed using the following terminology:

a) ***shall*** is used for mandatory requirements;

b) ***may*** is used to describe implementation or administrative choices (***may*** means ***is permitted to***, and hence, ***may*** and ***may not*** mean precisely the same thing);

c) ***should*** is used for recommended choices (the behaviors described by ***should*** and ***should not*** are both permissible but not equally desirable choices).

The PICS proforma (see Annex A) reflects the occurrences of the words *shall, may,* and *should* within the standard.

The standard avoids needless repetition and apparent duplication of its formal requirements by using ***is***, ***is not***, ***are***, and ***are not*** for definitions and the logical consequences of conformant behavior. Behavior that is permitted but is neither always required nor directly controlled by an implementor or administrator, or whose conformance requirement is detailed elsewhere, is described by ***can***. Behavior that never occurs in a conformant implementation or system of conformant implementations is described by ***cannot***. ~~The word ***allow*** is used as a replacement for the cliche Support the ability for, and the word ***capability*** means can be configured to.~~

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

5.2 Protocol Implementation Conformance Statement (PICS)

The supplier of a~~n~~ MAC Security Entity (SecY) implementation that is claimed to conform to this standard shall complete a copy of the PICS proforma provided in Annex A (normative) and shall provide the information necessary to identify both the supplier and the implementation.

The supplier of an EDE that is claimed to conform to this standard shall complete a copy of the PICS proforma provided in Annex D (normative) and shall provide the information necessary to identify both the supplier and the implementation. The supplier of an EDE implementation shall also complete or provide copies of the following PICS proforma(s) adhering to any restrictions required by conformance to this standard and marking any exceptions required by conformance to this standard.

a) For all types of EDE, the PICS proforma for each SecY implementation provided in Annex A of this standard.

b) For all types of EDE, the PICS proforma specified by IEEE Std 802.1X.

c) For an EDE-M: the IEEE Std 802.1Q PICS proforma as required for a VLAN-unaware MAC Bridge.

d) For an EDE-CS: the IEEE Std 802.1Q PICS proforma as required for a Provider Edge Bridge.

e) For an EDE-CC: the IEEE Std 802.1Q PICS proforma as required for each of the two C-VLAN components.

f) For an EDE-SS: the IEEE Std 802.1Q PICS proforma as required for each of the two S-VLAN components.

5.3 ~~Required capabilities~~MAC Security Entity requirements

An implementation of a MAC Security Entity (SecY) for which conformance to this standard is claimed shall

a) Support the Controlled and Uncontrolled Ports, and use a Common Port as specified in Clause 10.

b) Support the MAC status and point-to-point parameters for the Controlled and Uncontrolled Ports as specified in 6.4, 6.5, and 10.7.

c) Process transmit requests from the Controlled Port as required by the specification of Secure Frame Generation (10.5).

d) Process receive indications from the Common Port as required by the specification of Secure Frame Verification (10.6), prior to causing receive indications at the Controlled Port.

e) Encode and decode MACsec PDUs as specified in Clause 9.

f) Use a ~~globally unique~~ 48-bit MAC Address and a 16-bit Port Identifier unique within the scope of that address assignment to identify ~~the~~ each transmit SCI, as specified in 8.2.1.

g) Satisfy the performance requirements specified in Table 10-1 and 8.2.2.

h) Support the Layer Management Interface (LMI) operations required by the Key Agreement Entity as specified in Clause 10.

i) Provide the management functionality specified in 10.7.

j) Protect and validate MACsec PDUs by using Cipher Suites as specified in 14.1.

k) Support Integrity Protection using the Default Cipher Suite specified in Clause 14.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

l) For each Cipher Suite implemented, support a minimum of
   1) One receive SC
   2) Two receive SAKs
   3) One transmit SC
   4) One of the two receive SAKs at a time for transmission, with the ability to change from one to the other within the time specified in Table 10-1

m) Specify the following parameters for each Cipher Suite implemented
   1) The maximum number of receive SCs supported
   2) The maximum number of receive SAKs
   3) The maximum number of transmit SCs supported

An implementation of a ~~MAC Security Entity (~~SecY~~)~~ for which conformance to this standard is claimed shall not

n) Introduce an undetected frame error rate greater than that achievable by preserving the original FCS, as required by 10.4.
o) Implement any Cipher Suite that is additional to those specified in Clause 14 and does not meet all the criteria specified in 14.2, 14.3, and 14.4.1.
p) Support access to MACsec parameters by a management agent using any version of SNMP prior to v3.

An implementation of a ~~MAC Security Entity (~~SecY~~)~~ for which full conformance to this standard is claimed shall not:

q) Implement Cipher Suites other than those specified in Clause 14.

NOTE—Conformance with Cipher Suite variance is allowed, as specified in 5.4 and in 14.4.1.

5.4 ~~Optional capabilities~~MAC Security Entity options

An implementation of a MAC Security Entity (SecY) for which conformance to this standard is claimed may

a) ~~Support network management using the MIB specified in Clause 13.~~
b) ~~Support access to the MIB specified in Clause 13 using SNMP version v3 or higher.~~
a) Support access to MACsec parameters by a management agent using SNMP version v3 and the MIB module specified in Clause 13.
b) Support more than one receive SC.
c) Support more than two receive SAKs.
d) Support more than one transmit SC.
e) Support Confidentiality Protection using the Default Cipher Suite without a confidentiality offset, as specified in Clause 14.
f) Support Confidentiality Protection using the Default Cipher Suite with a confidentiality offset, as specified in Clause 14.
g) Include Cipher Suites that are specified in Clause 14 in addition to the Default Cipher Suite.

An implementation of a SecY that supports more than one transmit SC shall:

h) Support a Traffic Class Table and an Access Priority Table as specified in 10.7.17.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

An implementation of a ~~MAC Security Entity (~~SecY~~)~~ for which conformance with Cipher Suite variance is claimed may:

i) Use Cipher Suites not specified in Clause 14, but meeting the criteria specified in 14.2, 14.3, 14.4.1.

~~NOTE—The term *capability* is used to describe a set of related detailed provisions of this standard. Each capability can comprise both mandatory provisions, required if implementation of the capability is to be claimed, and optional provisions. Each detailed provision is specified in one or more of the other clauses of this standard. The PICS, described in Annex A, provides a useful checklist of these provisions~~

5.5 EDE conformance

Ethernet Data Encryption devices (EDEs) of various types comprise bridging systems and bridge components used as specified in this standard. Clause 15 provides a taxonomy, specification, and a description of the intended use of each type (EDE-M, EDE-CC, EDE-CS, or EDE-SS).

The bridging system and/or bridge components that comprise an implementation of an EDE that is claimed to conform to this standard shall conform to the requirements of (and may use any of the options and recommendations permitted by) IEEE Std 802.1Q, IEEE Std 802.1X, and the provisions of this standard for each MAC Security Entity that is part of the EDE implementation, with the restrictions, additions, exceptions, and clarifications specified in this standard for that type of EDE.

An implementation of any type of EDE that is claimed to conform to this standard shall

a) Have two and only two externally accessible Bridge Ports, a red-side port and a black-side port.

   NOTE—A red-side port can also be referred to as the *customer* or *edge* port and the black-side port as a *provider* or *network* port. The use of either or both of the pair of terms, *customer/provider* and *edge/network* to refer to an EDE-M's ports is consistent with the relative roles played by ports in multicomponent bridges and EDEs.

b) Associate a PAE that includes a KaY capable of operating MKA with each SecY required by this standard for the particular type of EDE (15.2, 15.4, 15.5, 15.6, 15.7).

5.6 EDE-M conformance

An implementation of an EDE-M (15.2, 15.4) that is claimed to conform to this standard shall

a) Comprise a VLAN-unaware MAC Bridge as specified by IEEE Std 802.1Q (IEEE Std 802.1Q-2014 5.14) with the constraints and exceptions specified in this standard.
b) Incorporate a SecY in the black-side port interface stack (15.2, 15.4).
c) Be capable of being configured to secure connectivity within a customer or provider network (as specified in 15.2), using the Nearest non-TPMR group address for group-addressed EAPOL PDUs, and filtering frames whose destination MAC Address is a TPMR component Reserved Address or the Nearest non-TPMR Bridge group address.
d) Be capable of being configured to secure connectivity across a PBN to a peer EDE-M, MACsec-capable Customer Bridge, or an EDE-CS (as specified in 15.4 and 15.5), using the Nearest Customer Bridge group address for group addressed EAPOL PDUs and filtering frames whose destination MAC Address is a C-VLAN component Reserved Address with the exception of the Nearest Customer Bridge group address.

and may

e) Be capable of being configured to secure connectivity across a PBN to a peer EDE-CC (as specified in 15.6), using the EDE-CC PAE group address for group addressed EAPOL PDUs, and filtering

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

frames whose destination MAC Address is a C-VLAN component Reserved Address or the EDE-CC PAE group address.

f) Be capable of being configured to recover signaled priority from a C-VLAN tag and to priority tag (or not) frames transmitted by the black-side port as specified in 15.4.

5.7 EDE-CS conformance

An implementation of an EDE-CS (15.5) that is claimed to conform to this standard shall

a) Comprise a Provider Edge Bridge as specified by IEEE Std 802.1Q (IEEE Std 802.1Q-2014 5.10.2) including one and only one C-VLAN component (identified by this standard as the edge component of the EDE) and an S-VLAN component (the network component of the EDE).
b) Incorporate a SecY in each of the internal Provider Edge Port interface stacks (15.5).
c) Be capable of being configured to use the Nearest Customer Bridge group address for group addressed EAPOL PDUs (15.5).

5.8 EDE-CC conformance

An implementation of an EDE-CC (15.6) that is claimed to conform to this standard shall

a) Comprise two C-VLAN components, each as specified by IEEE Std 802.1Q (IEEE Std 802.1Q-2014 5.5)—an edge component and a network component—internally connected as specified in 15.6.
b) Incorporate a SecY in each of the internal Provider Edge Port interface stacks (15.6).
c) Be capable of being configured to use the EDE-CC PAE group address as the destination MAC address of group addressed EAPOL PDUs for group addressed EAPOL PDUs (as specified in 15.6).
d) Filter and not forward all frames whose destination MAC address is either one of the addresses identified by IEEE Std 802.1Q as a C-VLAN component Reserved Address or the EDE-CC PAE group address.
e) Transmit frames received from the red-side customer port and relayed to the black-side network port untagged if they were received untagged and C-tagged with the same C-VID if they were C-tagged on receipt (15.6).

5.9 EDE-SS conformance

An implementation of an EDE-SS (15.7) that is claimed to conform to this standard shall

a) Comprise two S-VLAN components, each as specified by IEEE Std 802.1Q (IEEE Std 802.1Q-2014 5.6)—an edge component and a network component—internally connected as specified in 15.7.
b) Incorporate a SecY in each of the internal Provider Edge Port interface stacks (15.7).
c) Be capable of being configured to use the EDE-SS PAE group address as the destination MAC address of group addressed EAPOL PDUs for group addressed EAPOL PDUs (as specified in 15.7).
d) Filter and not forward all frames whose destination MAC address is either one of the addresses identified by IEEE Std 802.1Q as an S-VLAN component Reserved Address or the EDE-SS PAE group address.

Transmit frames received from the red-side customer port and relayed to the black-side network port untagged if they were received untagged and S-tagged with the same S-VID if they were S-tagged on receipt (15.7).

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

6. Secure provision of the MAC Service

Change the fourth note as follows:

NOTE 4—The MAC Service and the secure MAC Service are provided at a service access point to a single client. The client is either a logical link control (LLC) Entity or an entity that in turn provides the MAC Service or a MAC Internal Sublayer Service (IEEE Std ~~802.1D~~ 802.1AC, IEEE Std 802.1Q).

6.1 MAC Service primitives and parameters

Change the first paragraph of 6.1 as follows:

The MAC Service (~~ISO/IEC 15802-1~~ IEEE Std 802.1AC) provides unconfirmed connectionless-mode data transfer between source and destination stations. The invocation of a request primitive at a service access point within a source station results, with a high probability, in a corresponding indication primitive at selected service access points in destination stations. A single service request at one service access point results in no more than one service indication at each of the other service access points.

Change the third paragraph of 6.1 and the notes as follows:

The MAC Service can be provided by a single LAN or by a Bridged Local Area Network. The service provided to an LLC Client in an end station is specified in ~~ISO/IEC 15802-1~~ IEEE Std 802.1AC. The service provided by a LAN to a MAC Bridge is the MAC Internal Sublayer Service (ISS), ~~(see IEEE Std 802.1D),~~ an extension of the MAC Service that includes parameters necessary to the bridge relay function including the frame check sequence (FCS). Except as otherwise explicitly noted, the term *MAC Service* as used in the remainder of this clause refers both to the provision of the MAC Service to an LLC client and to provision of the ISS. Multiple instances of the MAC Service can be provided using a single instance of the ISS and supported in VLAN-aware Bridges using the Enhanced Internal Sublayer Service (EISS), (see ~~6.6 of~~ IEEE Std 802.1Q). When a VLAN TAG (IEEE Std 802.1Q) is used to distinguish the service instances supported, the additional parameters of the EISS are all encoded within the ISS MSDU.

NOTE 1—The MAC Service defined in ~~ISO/IEC 15802-1~~ IEEE Std 802.1AC is an abstraction of the features common to a number of specific media access control methods and is a guide to the development of client protocols.

NOTE 2—Some older descriptions of the MAC Service omit the source address parameter. With the addition of this parameter and removal of the frame_type parameter from the ISS (frames other than user_data_frames are always discarded by ISS clients, and thus can be discarded by the media access control method specific functions that provide the ISS), the definitions of the MAC Service and of the Internal Sublayer Service are expected to converge in the future.

NOTE 3—The priority parameter described in this clause is also referred to as the user_priority in some specifications. The functions that support the ISS can calculate an access_priority for use on a LAN in local support of the user_priority. ~~The access_priority parameter can be modified by media access control method specific functions and is not delivered as a MAC Service indication parameter, so is not a concern of this specification.~~

6.2 MAC Service connectivity

Change the third note as follows:

NOTE 3—The original Spanning Tree Protocol (STP) could create loops in the network if symmetric connectivity was not provided. The Rapid Spanning Tree Protocol (RSTP), (see IEEE Std 802.1~~D~~Q), detects non-symmetric connectivity between Bridges, but will deny service until the problem is resolved, and intermittent non-symmetric connectivity can result in data loops. For example, the operation of the OSPF routing protocol on a LAN is inefficient unless all participants can receive frames sent by each other. If a LAN that provides the ISS to attached MAC Bridges merely delivers frames to their intended destination instead of providing full connectivity, learning of source addresses can be inhibited and frames flooded throughout the bridged network for an indefinite period.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

6.4 MAC status parameters

Change the fourth paragraph of 6.4 and the note as follows:

The value of the MAC_Enabled and MAC_Operational parameters are determined by the specific entity providing the MAC Service. ~~IEEE Std 802.1D~~ IEEE Std 802.1AC and IEEE Std 802.1Q specify how that determination is made for provision of the insecure ISS by specific media access control methods, and for provision of the insecure EISS. This standard specifies how these parameters are determined for the secure MAC Service.

NOTE—Correct provision and use of the MAC_Operational parameter is essential for high performance implementation of RSTP (IEEE Std 802.1~~D~~Q), Multiple Spanning Tree Protocol (MSTP, IEEE Std 802.1Q), and Link Aggregation Control Protocol (LACP, IEEE Std ~~802.3~~ 802.1AX). In the absence of this parameter, loss of connectivity is determined by repetitive loss of protocol frames that are normally transmitted at intervals of a few seconds, and it is assumed that frames transmitted immediately after a medium availability transition have a high probability of not being received by protocol peers.

6.5 MAC point-to-point parameters

Change the fourth paragraph of 6.5 and the note as follows:

IEEE Std ~~802.1D~~ 802.1AC and IEEE Std 802.1Q specify how the point-to-point status determination is made for provision of the insecure ISS by specific media access control methods, and for provision of the insecure EISS. This standard specifies how it is determined for the secure MAC Service.

NOTE—RSTP ~~(IEEE Std 802.1D)~~ and MSTP (IEEE Std 802.1Q) require the use of operPointToPointMAC to facilitate rapid reconfiguration in some network failure scenarios. LACP (IEEE Std ~~802.3~~ 802.1AX) does not aggregate links that are not point-to-point and ~~may~~ can use operPointToPointMAC to make this determination.

6.10 Quality of service maintenance

Change the fourth paragraph of 6.10 and split it into two paragraphs as follows:

The operation of MACsec introduces no additional frame loss on individual LAN segments other than that expected for a specific media access control method as a consequence of a small increase in frame size. The operation of MACsec between two customer systems across a provider bridged network can introduce additional frame loss caused by possible frame reordering from expedited forward or link aggregations within the provider bridged network. The reception of misordered frames can cause MACsec implementations to discard additional frames depending upon the configuration of replay protection parameters. MACsec can use separate secure channels to transmit frames with different access priorities and thus reduce or eliminate undesirable frame discard resulting from the mutual reordering of those frames.

Conforming implementations of MACsec are capable of applying a new keying material starting with any frame in a sequence that is received with the minimum intervening spacing specified by the specific media access control method in use. Each frame protected by MACsec remains independent of its predecessors and successors, so loss of a single frame does not imply loss of additional frames.

Change the tenth paragraph of 6.10 as follows:

Use of MACsec on each of a MAC Bridge's Ports will force a change in the data covered by an FCS, even if the frame is being relayed between LANs that use the same media access control method. Application of the techniques described in ~~Annex F of IEEE Std 802.1D~~ Annex O of IEEE Std 802.1Q allow an

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

implementation to achieve an arbitrarily small increase in undetected frame error rate, even in cases where the data that is within the coverage of the FCS is changed.

Change the twelfth paragraph of 6.10 as follows:

Where MACsec is used to support an instance of the ISS that in turn supports the EISS, encoding of the priority parameter of the EISS within the ISS MSDU ensures that priority can be communicated unchanged between service access points that are attached to a single LAN. Since MACsec is terminated ~~on each of the Ports of MAC Bridges attached to such LANs, a Bridge~~ at each of those service access points, a bridge that makes use of that ISS instance to support one of its ports can access or change the priority even if the two instances of MACsec encrypt the MSDU in order to provide confidentiality. An Access Priority Table (10.7.17) can be used to derive the access priority requested from the medium supporting the ISS from the priority requested by the user of the EISS.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

7. Principles of secure network operation

7.1 Support of the secure MAC Service by an individual LAN

Insert the following paragraph after the last paragraph of 7.1:

In the above examples (Figure 7-3, Figure 7-6), each station transmits frames using a single SC. A station can also use multiple transmit SCs, using each transmitted frame's priority to allocate to it one of the SCs. Each of these transmit SCs supports secure transmission for frames of one or more priorities from the transmitting station to all the others in the CA. This use of multiple transmit SCs allows MACsec to enforce in-order delivery (or the use of a smaller replay window than might otherwise be the case) for frames of any given priority.

7.1.2 Secure Channel (SC)

Change 7.1.2 as follows:

Each SecY transmits frames conveying secure MAC Service requests of any given priority on a single SC. Each SC provides unidirectional point-to-multipoint communication, and it can be long lived, persisting through SAK changes. Each SC is identified by a Secure Channel Identifier (SCI) comprising a ~~uniquely allocated~~ 48-bit MAC address concatenated with a 16-bit ~~port number~~ Port Identifier.

NOTE 1—Including the Port Identifier ~~Using an SC identifier that includes a port number~~ component would appear to be unnecessary in the case of a simple system ~~that comprises a single LAN station,~~ with a ~~uniquely allocated 48-bit~~ MAC address~~,~~ and a single SecY for each port. However, some systems require support for more SecYs than they have uniquely allocated addresses, ~~either~~ because they make use of technologies that support virtual MACs, ~~or~~ because their interface stacks include the possibility of including multiple SecYs at different sublayers (as do Provider Bridges [IEEE Std 802.1Q], for example), or because they transmit frames of different priorities using different SCs. ~~Provider bridges (IEEE Std 802.1Q) provide examples of the latter.~~

NOTE 2—An EPON Optical Line Terminator (OLT) can use a distinct SC to support the Single Copy Broadcast (SCB) capability (Clause 12). The formal identifier for this SC comprises a System Identifier for the OLT and a reserved Port ~~Number~~ Identifier. ~~b~~Both can be represented in the secured frame by a single SCB bit (Clause 9).

MACsec Key Agreement is responsible for informing each SecY of the identifier to be used for ~~the~~ each transmitting ~~SecY~~ SC, and of the existence and identifier of each of the SCs for which the SecY is to receive frames. While the structure of the communication facilitated by each SC is point-to-multipoint (which encompasses point-to-point as a special case) the SecY does not have to be aware that its transmissions can reach multiple receivers, that the frames that it receives could be received by other SecYs, or of any relationship or lack of relationship between the inbound SCs (except in determining the value of the operPointToPointMAC status parameter, 6.5, 10.7.4). The operation of the MACsec Key Agreement protocol (MKA, specified in IEEE Std 802.1X) is defined in terms of the behavior of participants, each representing a single KaY and a single transmit SCI. When a SecY uses multiple transmit SCIs, each SCI is represented by a separate participant that sends and receives MKPDUs to and from all the other participants just as if it were representing a separate SecY in the same group CA, see Annex E (informative).

NOTE 3—The point-to-multipoint nature of the SC does have technical consequences, in particular the decision to change from one SA to another is made by the transmitter using the SC, not by one or some number of the receivers.

7.1.3 Secure Association (SA)

Change the first paragraph of 7.1.3 as follows:

Each SC comprises a succession of SAs, each with a different SAK. Each SA is identified by the SC identifier concatenated with a two-bit Association Number (AN, Figure 7-7). The Secure Association

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

Identifier (SAI) thus created allows the receiving SecY to identify the SA and thus the SAK used to decrypt and authenticate the received frame. The ~~AN, and hence the~~ SAI~~,~~ is only unique for the SAs ~~that can be~~ used ~~or recorded~~ by ~~participating~~ SecYs participating in a given CA at any instant.

Change the third and fourth paragraphs of 7.1.3 as follows:

The decision to replace one SA with its successor is made by the SecY that transmits using the SC, after MACsec Key Agreement has informed it that all the other SecYs are prepared to receive using that SA. No notification, other than receipt of a secured frame with a different SAI is sent to the receiver. At any one instant a SecY has to be capable of storing SAKs for two SAs for each inbound SC, and of swapping from one SA to another without notice. Certain LAN technologies can reorder frames of different priority, so reception of frames on a single SC can use interleaved SAs. The time bound within which a receiver can accept interleaved SAs is 0.5 s.

The transmitting SecY does not interleave frames for different SAs on a given SC.

NOTE—When MKA (see IEEE Std 802.1X) is used to distribute the SAKs used by each of the SCs supporting a given CA, the same SAK is used for all SAs with a given AN (at any given time). The transmit SA for each SC is replaced with its successor at approximately the same time so that there is no need for any SecY participating in the CA to support more than two SAKs at a time.

Replace Figure 7-7 with the following:

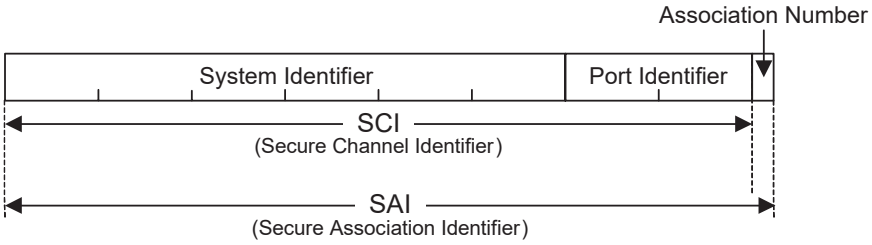


Figure 7-7—Secure Channel and Secure Association Identifiers

7.3 Use of the secure MAC Service

Change the fourth and fifth paragraphs of 7.3 as follows:

The client policies in use at any time should reflect the intersection of the capabilities permitted to the members of the CA. Policies can be

a) Selected by the client on the basis of the level of authorization, as provided by the ~~KaY~~ PAE through a layer management interface (LMI) (see 10.7) or
b) Selected by a central server that forms part of the management framework for the network, and
   1) Securely downloaded or
   2) Communicated to the client using a secure connection

~~MACsec Key Agreement supports mechanisms that securely bind downloads and secure connections to their intended client, thus protecting against a rights amplification attack.~~

7.3.1 Client policies

Delete NOTE 1 as follows, renumbering the subsequent note:

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

~~NOTE 1—To facilitate policy selection by clients of the secure MAC Service, IEEE Std 802.1X specifies authorized permissions, including those required by MAC Bridges (IEEE Std 802.1D) and VLAN aware Bridges (IEEE Std 802.1Q) to support the secure MAC Service in Bridged and Virtually Bridged Local Area Networks.~~

7.3.2 Use of the secure MAC Service by bridges

Change the second paragraph of 7.3.2 and the accompanying note as follows:

~~MACsec Key Agreement can use discovery protocols to identify SecYs that can participate in a CA. These protocols use a Reserved Group MAC Address that is normally filtered by bridges to restrict each instance of the secure MAC Service to an individual LAN.~~

PAEs and KaYs use group addressed frames to identify and communicate with peers whose SecYs are potential participants in the same CA. Frames with the group addresses used for this purpose are filtered by certain bridges and EDEs (Clause 15) to restrict each instance of the secure MAC Service to the appropriate LAN scope. By default PAEs and KaYs for MAC Bridges, VLAN Bridges, Provider Bridges, and Provider Backbone Bridges use the PAE group address specified by IEEE Std 802.1X (also identified as the Nearest Non-TMPR group address by IEEE Std 802.1Q). Use of this address restricts each instance of the secure MAC Service to an individual customer LAN.

~~NOTE 2—Use of this address ensures that the physical topology as perceived by spanning tree protocols aligns with that provided by MAC Security. In Provider Bridged Networks, the Provider Bridge Group Address is used. An exception to the alignment rule occurs with certain types of interface that are supported by Provider Bridge Networks, where a provider operated C-VLAN (see IEEE Std 802.1Q) aware component provides the customer interface.~~

NOTE 2—Use of Reserved Group MAC Addresses helps to ensure that the physical topology as perceived by spanning tree and other configuration protocols aligns with that provided by MAC Security.

Change the third note in 7.3.2 as follows:

NOTE 3—A Bridge Port is one of the bridge's points of attachment to an instance of the MAC Internal Sublayer Service (ISS), and is used by the MAC Relay Entity and associated Higher-Layer Entities as specified in ~~IEEE Std 802.1D and~~ IEEE Std 802.1Q.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

8. MAC Security Protocol (MACsec)

8.1.1 Security requirements

Delete the note in 8.1.1 as follows:

~~NOTE—Key lifetimes are a property of the authentication and authorization provided by key agreement, and can therefore be restricted independently by any system in the CA.~~

8.2.1 SC identification requirements

Change 8.2.1 as follows:

~~The system shall have a globally unique 48-bit MAC Address, the Secure System Address, that can be used to compose the SCI (7.1.2, 9.9), and be capable of allocating a unique 16-bit Port Identifier within the scope of that address.~~

~~NOTE—The Secure System Address can be used for other purposes.~~

Each SecY shall be capable of identifying each of its transmit SCs with an SCI that comprises a unique 48-bit MAC Address and a 16-bit Port Identifier that is unique within the scope of that address (7.1.2, 9.9).

NOTE—MKA (IEEE Std 802.1X) verifies that each participant in any given CA has a unique SCI, as part of satisfying Cipher Suite requirements prior to establishing secure communication.

8.2.5 Authentication requirements

Change 8.2.5 as follows:

The ~~KaY~~ PAE supports mutual authentication of peer stations, and the SecY assumes that such authentication has taken place.

8.2.6 Authorization requirements

Change 8.2.6 as follows:

The ~~KaY~~ PAE provides authorization of services to be delivered to a peer station. ~~The minimum authorization provided should be Host and Infrastructure. Communication of authorization to users of the MAC service occurs via the LMI.~~

~~The KaY provides information to local services to allow cryptographic binding of configuration tunnels (for example, VLAN) to the authenticated connection.~~

The ~~KaY~~ PAE provides information to local services about the currently selected Cipher Suite.

8.3 MACsec operation

Change the fourth paragraph of 8.3 as follows:

On transmission, the frame is first assigned to a transmit SC and to the ~~an~~ SA (7.1.3), identified ~~locally~~ by its Association Number (AN) (see 7.1.3, 9.6), that will be used by that SC to protect the transmitted frame. The AN is used to identify the SAK (7.1.3) and the next PN (3.27, 9.8) for that SA. The AN, the SCI (7.1.2), and the PN are encoded in the SecTAG (the SCI can be omitted for point-to-point CAs if only one transmit SC is

Copyright © 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

in use) along with the MACsec EtherType (9.8) and the number of octets in the frame following the SecTAG (SL, 9.7) if less than 48 (8.1.3).

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

9. Encoding of MACsec protocol data units

9.9 Secure Channel Identifier (SCI)

Change 9.9 as follows:

If the SC bit in the TCI is set, the SCI (7.1.2, 8.2.1) is encoded in octets 9 through 16 of the SecTAG, and facilitates

a) Identification of the SA where the CA comprises three or more ~~peers~~ SCs
b) Network management identification of the SecY that has transmitted the frame

Octets 9 through 14 of the SecTAG encode the System Identifier component of the SCI. This comprises the six octets of a ~~globally unique~~ MAC address ~~uniquely~~ associated with the system that includes the transmitting SecY. The octet values and their sequence conform to the Canonical Format specified by IEEE Std 802.

Octets 15 and 16 of the SecTAG encode the Port Identifier component of the SCI, as an integer.

NOTE—The 64-bit value FF-FF-FF-FF-FF-FF-FF-FF is never used as an SCI and is reserved for use by implementations to indicate the absence of an SC or an SCI in contexts where an SC can be present.

An explicitly encoded SCI field in the SecTAG is not required on point-to-point links, which are identified by the operPointToPointMAC status parameter of the service provider, if the transmitting SecY uses only one transmit SC. In ~~the point-to-point~~ that case, the secure association created by the SecY for the peer SecYs, together with the direction of transmission of the secured MPDU, can be used to identify the transmitting SecY. ~~and t~~Therefore, an explicitly encoded SCI is unnecessary. Although the SCI does not have to be repeated in each frame when only two SecYs participate in a CA (see Clause 8, Clause 9, and Clause 10), the SCI (for Cipher Suites using a 32-bit PN) or the SSCI (for Cipher Suites using a 64-bit PN) still forms part of the cryptographic computation.

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

10. Principles of MAC Security Entity (SecY) operation

Change the note following the initial paragraph of Clause 10 as follows:

NOTE—Clause 6 defines the properties of the secure MAC Service, Clause 7 describes the security relationships used to support the service and how the service is used, providing the context within which each SecY operates, Clause 8 sets out requirements for the MACsec protocol and introduces the operation of the protocol, and Clause 9 specifies the encoding of parameters in MPDUs. This clause does not repeat all the information provided in those prior clauses, but includes sufficient reference to facilitate an understanding of SecY operation. IEEE Std 802.1AC-2012 Clause 7 and IEEE Std 802.1X-2010 Annex D describe the basic architectural concepts and terms used in this clause, including service, service access point, service primitive, and ports.

10.1 SecY overview

Change the sixth and following paragraphs and notes of 10.1 as follows:

The KaY is part of the Port Access Entity (IEEE Std 802.1X) associated with the SecY and uses the service provided by the Uncontrolled Port to transmit and receive frames that support key agreement protocols. These frames are distinguished by EtherType, so other selected protocol entities can also communicate using insecure frames by making use of ~~an~~ the Uncontrolled Port ~~provided by the KaY as illustrated in Figure 10-2~~.

~~The KaY also uses the Controlled Port provided by the SecY, providing its own Controlled Port for use by other protocols. This allows the KaY to provide MAC status parameters (6.4) that correctly reflect the secure connectivity to those users. The KaY does not modify frames that pass between its Controlled Port and the SecY's Controlled Port. However the KaY can use the secure service provided by the SecY to complete authentication, authorization, or the acquisition of client policies, prior to enabling transmission and reception through its Controlled Port.~~

The KaY determines the value of the MAC_Operational parameter (IEEE Std 802.1AC) associated with Controlled Port (10.7.4, 10.7.5) consistent with the provisions of this standard (6.4, 6.5, 6.7, 7.1.3, 7.2, 10.5.1, 10.5.2, 10.7.14, 10.7.2, 10.7.25).

~~NOTE 2—Operation of the SecY without protection or validation allows the same interfaces and relationships to be maintained between entities within a system when SecY functionality is not required. This provides a useful migration path for networks comprising systems that will incorporate SecY functionality at different times.~~

The KaY communicates transmit and receive keys and other information (10.2) to the SecY through its Layer Management Interface (LMI) ~~as illustrated in Figure 10-2~~. The LMI is also used to exchange information with local protocol entities responsible for network management, such as an SNMP Agent.

NOTE ~~2~~3— The term *local* refers to any other entity residing within the same system. Information exchange with a local entity can be modelled as occurring through its LMI (10.1, 10.3, 10.4, Figure 10-1~~, Figure 10-2~~), thus facilitating information exchange between entities not necessarily adjacent in a protocol layer reference model. No constraints are placed on the information exchanged, but there is no synchronization with any particular invocation of service at a service access point, so LMI exchanges do not effectively add to the parameters of a service such as the MAC service.

Delete Figure 10-2, renumbering subsequent figures as required.

10.2 SecY functions

Change bullet h) of 10.2 as follows:

h) ~~A replay window to support use of MACsec over provider networks that misorder frames with different transmission priority and or addresses. Frames within the window can be received out of~~

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

~~order, but are not replay protected. The window size can be set to zero to enforce strict reception ordering and replay protection.~~

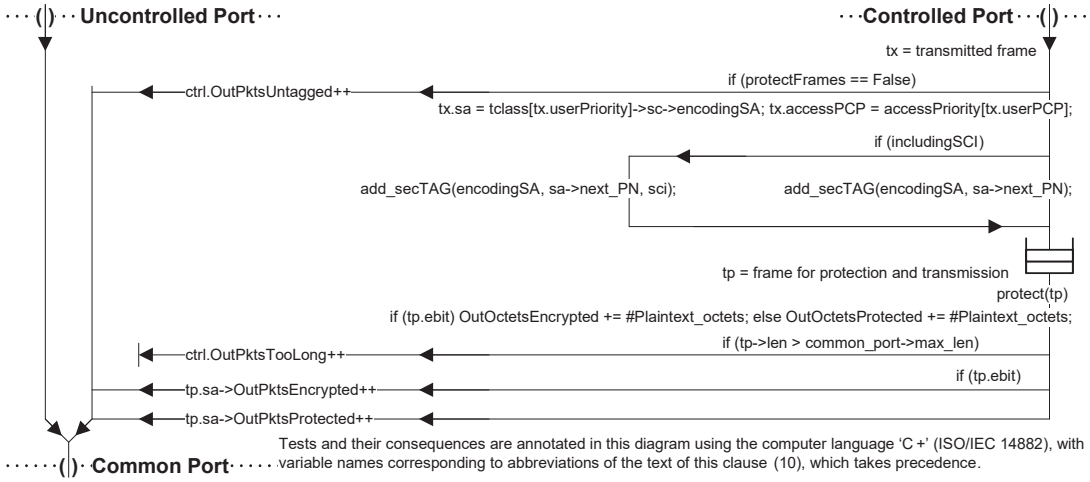
h) Use of multiple transmit SCs and a configurable replayWindow to support media access control methods and provider networks that can misorder frames with different priorities and/or addresses.

10.4 SecY architecture

Change the fifth paragraph of 10.4 as follows:

Management controls are provided to allow a SecY to be incorporated in a network system before MACsec is deployed, and to facilitate staged deployment. If protectFrames is not set, frames submitted to the Controlled Port are transmitted without modification. The validateFrames control allows untagged frames to be received, and Cipher Suite validation of tagged frames to be disabled or its result simply counted without frame discard. The protectFrames and validateFrames controls can also be set to allow the SecY to function completely transparently. The replayProtect and replayWindow controls allows replay protection to be disabled, to operate on a packet number window, or to enforce strict frame order. If replayProtect is set but the replayWindow is not zero, frames within the window can be received out of order, however they are not replay protected. Management counters allow configuration and operational errors to be identified and rectified before enabling secure operation. The effect of the controls, and the counters maintained, are summarized in Figure 10-4 and Figure 10-5.

Replace Figure 10-4 with the following figure:



NOTE 1—Secure generation frame counters are identified as reported by management. Confidentiality or integrity only protection is selected for an SA when it is created, so either but not both of the OutOctetsEncrypted or OutOctetsProtected counts and either OutPktsEncrypted or the OutPktsProtected will be incremented while that SA is in use, and the current value of the packet counter can be derived from nextPN for the SA less any change in the value of OutPktsTooLong since that SA has been used for protection, allowing an implementation to optimize counter resources.

Figure 10-4—Management controls and counters for secure frame generation

10.5 Secure frame generation

Change bullet f) of 10.5 as follows:

f) Issues a request to the Transmit Multiplexer with the destination and source MAC addresses~~, and priority of the frame as received from the Controlled Port,~~ and an MPDU comprising the octets of the SecTAG, Secure Data, and the ICV concatenated in that order (10.5.5). If the SecY does not

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

implement an Access Priority Table (10.7.17) the priority of the request is the same as that received from the Controlled Port, otherwise it is the access priority given by the table for the received priority.

10.5.1 Transmit SA assignment

Change 10.5.1 as follows:

~~Each SA is identified by its Association Number (AN).~~ Each frame is assigned to the SA identified by the current value of the encodingSA variable for the selected transmit SC. If the SecY does not implement a Traffic Class Table it uses a single transmit SC. If implemented, the Traffic Class Table specifies the value of the most significant four bits of the SCI's Port Identifier component for each possible transmit request user priority, allowing selection of one of up to eight distinct SCs (see 10.7.17).

The encodingSA ~~This~~ is updated following an LMI request from the KaY to start transmitting using the SA and can be read but not written by network management. Frames will be protected using the encodingSA immediately after the last frame assigned to the previous SA has been protected. If the SA ~~identified by the encodingSA~~ is not available for use, and the management control protectFrames is set, MAC_Operational transitions to False for the Controlled Port, and frames are neither accepted or delivered using the port.

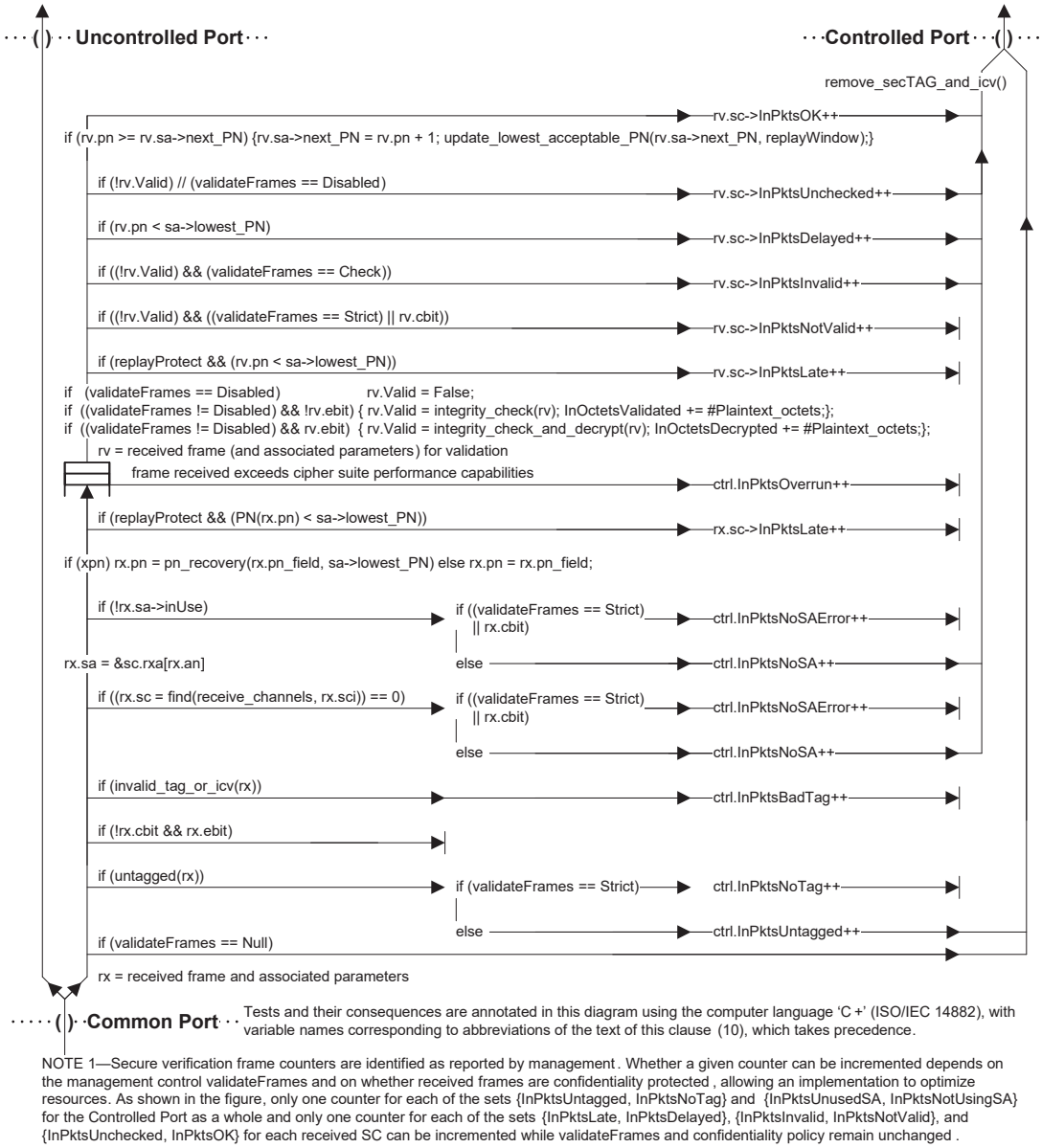
Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

Replace Figure 10-5 with the following figure:



NOTE 1—Secure verification frame counters are identified as reported by management. Whether a given counter can be incremented depends on the management control validateFrames and on whether received frames are confidentiality protected, allowing an implementation to optimize resources. As shown in the figure, only one counter for each of the sets {InPktsUntagged, InPktsNoTag} and {InPktsUnusedSA, InPktsNotUsingSA} for the Controlled Port as a whole and only one counter for each of the sets {InPktsLate, InPktsDelayed}, {InPktsInvalid, InPktsNotValid}, and {InPktsUnchecked, InPktsOK} for each received SC can be incremented while validateFrames and confidentiality policy remain unchanged.

Figure 10-5—Management controls and counters for secure frame verification

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

10.5.3 SecTAG encoding

Change 10.5.3 as follows:

The SecTAG is encoded as specified in Clause 9.

The SC bit in the SecTAG shall be set and the SCI explicitly encoded in the SecTAG, and the management status parameter includingSCI set to True, if and only if

a) The management control alwaysIncludeSCI is True,
   or
b) The number of transmit SCs is greater than one,
   or
c) The number of receive SCs enabled for reception is greater than one, and
   1) The management control useES is False,
      and
   2) The management control useSCB is False.

If the management control useES is True and ~~alwaysIncludeSCI~~ includingSCI is False, the ES bit in the SecTAG shall be set. Otherwise, if useES is False or alwaysIncludeSCI is True, the ES bit shall be clear.

If the management control useSCB is True and ~~alwaysIncludeSCI~~ includingSCI is False, the SCB bit in the SecTAG shall be set. Otherwise, if useSCB is False or ~~alwaysIncludeSCI~~ includeSCI is True, the SCB bit shall be clear.

NOTE—These rules cover the case where useSCB is True and the number of active receive channels is greater than one. However SCB bit use is currently restricted to supporting a transmit only EPON interface (see Clause 12).

Table 10-1 summarizes the rules [a) through c) above], with each of the columns to the right representing a valid combination of controls, number of SCs, and SecTAG encoding.

Insert a new Table 10-1 as follows, renumbering subsequent tables as required:

Table 10-1—Management controls and SecTAG encoding

Mgmt controls	alwaysIncludeSCI	T[a]	F	F	F	F	F
	useES	—	—	F	T	T	F
	useSCB	—	—	F	T	F	T
#SCs	#transmitSCs > 1	—	T	—	F	F	F
	#receiveSCs enabled for reception > 1	—	—	T	—	—	—
Mgmt status	includingSCI	T	T	T	F	F	F
SecTAG encoding	SC bit set? (SCI explicitly encoded)	Y	Y	Y	N	N	N
	ES bit set?	N	N	N	Y	Y	N
	SCB bit set?	N	N	N	Y	N	Y

[a]T = True, F = False, — = don't care, Y= Yes, N = No

Copyright © 2017 IEEE. All rights reserved.

© IEEE 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018

~~If the management control alwaysIncludeSCI is set, or the number of receive SCs with SAs enabled for reception is greater than one and both useES and useSCB are False, the SC bit in the SecTAG shall be set and the SCI explicitly encoded in the SecTAG; otherwise, the SC bit shall be clear and the SCI not explicitly encoded.~~

The values of useES, useSCB, and alwaysIncludeSCI can be written and read by management. The read-only management status parameter includeSCI is True if an SCI is explicitly encoded in each SecTAG, and False otherwise. The number of active receive SCs is controlled by the KaY but can be read by management.

If a frame is to be integrity protected, but not encrypted, with the number and value of the octets of the Secure Data exactly the same as those of the User Data and an ICV of 16 octets, then the E bit shall be clear and the C bit clear. The E bit shall be clear and the C bit set if the frame is not encrypted but the octets of the Secure Data differ from those of the User Data or the ICV is not 16 octets.

If both confidentiality (through encryption) and integrity protection are applied to a frame, then both the E bit and the C bit shall be set. The SecY shall not encode a SecTAG that has both the E bit set and the C bit clear for any frame received from the Controlled Port for transmission.

~~If the alwaysIncludeSCI control is set or the number of receive SCs with SAs enabled for reception is greater than 1, the SCI is included in the SecTAG; otherwise, it is omitted. The value of alwaysIncludeSCI can be written and read by management. The number of active receive SCs is controlled by the KaY, but can be read by management.~~

10.6 Secure frame verification

Change the second paragraph of 10.6 as follows:

If the management control validateFrames is not Strict, frames without a SecTAG are received, counted, and delivered to the Controlled Port; otherwise, they are counted and discarded. If validateFrames is Disabled, cryptographic validation is not applied to tagged frames, but frames whose original service user data can be recovered are delivered. Frames with a SecTAG that has the TCI E bit set but the C bit clear are discarded, as this reserved encoding is used to identify frames with a SecTAG that are not to be delivered to the Controlled Port. If validateFrames is Null, all received frames are delivered to the Controlled Port without modification, irrespective of the absence, presence, or validity of a SecTAG, and the processing described in a) through j) above and in 10.6.1 through 10.6.5 is not performed. Figure 10-5 summarizes the operation of secure frame verification management controls and counters.

Setting validateFrames to Null shall also cause the secure frame generation control protectFrames (10.5) to become False, thus allowing a port that includes a SecY to behave as if the SecY were not present. In particular, it allows a MACsec-capable bridge or EDE to forward frames that have a SecTAG but no other outer tag (such as a VLAN tag).

10.6.1 Receive SA assignment

Change the first and second paragraphs of 10.6.1 as follows:

An SCI is associated with the received frame and used to locate the receive SC. If an SCI is not explicitly encoded in the SecTAG, the ~~default~~ value established by the KaY for a single peer is used.

If the SC is not found, ~~it~~ the received SCI may be recorded to assist network management resolution of the problem, and:

a) If validateFrames is Strict or the C bit in the SecTAG is set, the ~~InPktsNoSCI~~ InPktsNoSAError counter is incremented and the frame is discarded; otherwise

Copyright © 2017 IEEE. All rights reserved.

Documents
Document Sharing Hub
© IEEE 2017 – All rights reserved

Full document details: ISO_IEC_IEEE 8802-1AE_2013_Amd 3_2018