INTERNATIONAL STANDARD

ISO/IEC/IEEE 8802-1AE

Second edition
2020-08

Telecommunications and exchange between information technology systems — Requirements for local and metropolitan area networks —

Part 1AE: Media access control (MAC) security

Télécommunications et échange entre systèmes informatiques — Exigences pour les réseaux locaux et métropolitains —

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

Reference number
ISO/IEC/IEEE 8802-1AE:2020(E)

© IEEE 2018

Full document details: ISO/IEC/IEEE 08802-1AE-2020

COPYRIGHT PROTECTED DOCUMENT

© IEEE 2018

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
Email: copyright@iso.org
Website: www.iso.org

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

Published in Switzerland

© IEEE 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

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 was prepared by the LAN/MAN of the IEEE Computer Society (as IEEE Std 802.1AE-2018) 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*.

This second edition cancels and replaces the first edition (ISO/IEC/IEEE 8802-1AE:2013), which has been technically revised. It also incorporates ISO/IEC/IEEE 8802-1AE:2013/Amd 1:2015; ISO/IEC/IEEE 8802-1AE:2013/Amd 2:2015 and ISO/IEC/IEEE 8802-1AE:2013/Amd 3:2018.

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 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO/IEC/IEEE 08802-1AE-2020

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

IEEE Std 802.1AE™-2018
(Revision of IEEE Std 802.1AE-2006)

IEEE Standard for
Local and metropolitan area networks—

Media Access Control (MAC) Security

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 27 September 2018

IEEE-SA Standards Board

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

Abstract: How all or part of a network can be secured transparently to peer protocol entities that use the MAC Service provided by IEEE 802® LANs to communicate is specified in this standard. MAC security (MACsec) provides connectionless user data confidentiality, frame data integrity, and data origin authenticity.

Keywords: authorized port, confidentiality, data origin authenticity, IEEE 802.1AE™, IEEE 802.1AEbn™, IEEE 802.1AEbw™, 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 © 2018 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 26 December 2018. 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 978-1-5044-5215-1 STD23339
Print: ISBN 978-1-5044-5216-8 STDPD23339

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 © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

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 Notices and Disclaimers Concerning IEEE Standards Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

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. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups 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 Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

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.

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.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

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.

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.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

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 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 © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

Participants

At the time this standard was submitted to the IEEE-SA Standards Board for approval, 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
Amelia Andersdotter
Butch Anton
Harry Bims
Demetrio Bucaneg
Stephen Bush
William Byrd
Radhakrishna Canchi
Steven Carlson
Keith Chow
Charles Cook
Richard Doyle
János Farkas
Norman Finn
Michael Fischer
Yukihiro Fujimoto
Randall Groves
Qiang Guo
Stephen Haddock
Marco Hernandez
Werner Hoelzl
Russell Housley
Yasuhiro Hyakutake
Noriyuki Ikeuchi
Atsushi Ito
Raj Jain
Sangkwon Jeong
Piotr Karocki
Stuart Kerry
Yongbum Kim
Hyeong Ho Lee
Suzanne Leicht
Jon Lewis
Elvis Maculuba
Ignacio Marin Garcia
Brett McClellan
Richard Mellitz
John Messenger
Michael Montemurro
Rick Murphy
Nick S. A. Nikjoo
Satoshi Obara
Robert O'hara
Bansi Patel
Clinton Powell
Adee Ran
Karen Randall
R. K. Rannow
Alon Regev
Maximilian Riegel
Robert Robinson
Benjamin Rolfe
Jessy V. Rouyer
Richard Roy
Naotaka Sato
Mick Seaman
Thomas Starai
Walter Struppler
Jasja Tijink
Mark-Rene Uchida
Dmitri Varsanofiev
George Vlantis
Lisa Ward
Stephen Webb
Karl Weber
Chun Yu Charles Wong
Oren Yuen

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

When the IEEE-SA Standards Board approved this standard on 27 September 2018, it had the following membership:

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

Ted Burse
Guido R. Hiertz
Christel Hunter
Joseph L. Koepfinger*
Thomas Koshy
Hung Ling
Dong Liu
Xiaohui Liu
Kevin Lu
Daleep Mohla
Andrew Myles
Paul Nikolich
Ronald C. Petersen
Annette D. Reilly
Robby Robson
Dorothy Stanley
Mehmet Ulema
Phil Wennblom
Philip Winston
Howard Wolfman
Jingyi Zhou

*Member Emeritus

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

Introduction

This introduction is not part of IEEE Std 802.1AE-2018, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Security.

The first edition of IEEE Std 802.1AE was published in 2006. The first amendment, IEEE Std 802.1AEbn™-2011, added the option of using the GCM-AES-256 Cipher Suite. The 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. The third amendment, IEEE Std 802.1AEcg™-2017, specified Ethernet Data Encryption devices (EDEs) that provide transparent secure connectivity while supporting provider network service selection and provider backbone network selection as specified in IEEE Std 802.1Q™.

This revision, IEEE Std 802.1AE-2018, incorporates the text of IEEE Std 802.1AE-2006 and amendments IEEE Std 802.1AEbn-2011, IEEE Std 802.1AEbw-2013, and IEEE Std 802.1AEcg-2017.

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

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

IEEE Std 802.1AE is not intended for use with IEEE Std 802.11™. That standard also uses 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 © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

Contents

1. Overview ... 16

   1.1 Introduction ... 16
   1.2 Scope ... 17

2. Normative references ... 18

3. Definitions ... 19

4. Abbreviations and acronyms ... 23

5. Conformance ... 25

   5.1 Requirements terminology ... 25
   5.2 Protocol Implementation Conformance Statement (PICS) ... 25
   5.3 MAC Security Entity requirements ... 26
   5.4 MAC Security Entity options ... 27
   5.5 EDE conformance ... 27
   5.6 EDE-M conformance ... 28
   5.7 EDE-CS conformance ... 28
   5.8 EDE-CC conformance ... 29
   5.9 EDE-SS conformance ... 29

6. Secure provision of the MAC Service ... 30

   6.1 MAC Service primitives and parameters ... 30
   6.2 MAC Service connectivity ... 32
   6.3 Point-to-multipoint LANs ... 32
   6.4 MAC status parameters ... 33
   6.5 MAC point-to-point parameters ... 33
   6.6 Security threats ... 34
   6.7 MACsec connectivity ... 35
   6.8 MACsec guarantees ... 35
   6.9 Security services ... 36
   6.10 Quality of Service maintenance ... 37

7. Principles of secure network operation ... 39

   7.1 Support of the secure MAC Service by an individual LAN ... 39
   7.2 Multiple instances of the secure MAC Service on a single LAN ... 44
   7.3 Use of the secure MAC Service ... 45

8. MAC Security protocol (MACsec) ... 48

   8.1 Protocol design requirements ... 48
   8.2 Protocol support requirements ... 51
   8.3 MACsec operation ... 53

9. Encoding of MACsec Protocol Data Units ... 55

   9.1 Structure, representation, and encoding ... 55
   9.2 Major components ... 55
   9.3 MAC Security TAG ... 56
   9.4 MACsec EtherType ... 56

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

9.5 TAG Control Information (TCI) ... 57
9.6 Association Number (AN) ... 58
9.7 Short Length (SL) ... 58
9.8 Packet Number (PN) ... 58
9.9 Secure Channel Identifier (SCI) ... 59
9.10 Secure Data ... 59
9.11 Integrity check value (ICV) ... 59
9.12 PDU validation ... 60

10. Principles of MAC Security Entity (SecY) operation ... 61

10.1 SecY overview ... 61
10.2 SecY functions ... 62
10.3 Model of operation ... 63
10.4 SecY architecture ... 63
10.5 Secure frame generation ... 65
10.6 Secure frame verification ... 68
10.7 SecY management ... 72
10.8 Addressing ... 85
10.9 Priority ... 85
10.10 SecY performance requirements ... 86

11. MAC Security in systems ... 87

11.1 MAC Service interface stacks ... 87
11.2 MACsec in end stations ... 88
11.3 MACsec in MAC Bridges ... 89
11.4 MACsec in VLAN-aware Bridges ... 90
11.5 MACsec and Link Aggregation ... 91
11.6 Link Layer Discovery Protocol (LLDP) ... 92
11.7 MACsec in Provider Bridged Networks ... 93
11.8 MACsec and multi-access LANs ... 95

12. MACsec and EPON ... 97

13. MAC Security Entity MIB ... 98

13.1 Introduction ... 98
13.2 The Internet-Standard Management Framework ... 98
13.3 Relationship to other MIBs ... 98
13.4 Security considerations ... 100
13.5 Structure of the MIB module ... 102
13.6 MAC Security Entity (SecY) MIB definitions ... 107

14. Cipher Suites ... 141

14.1 Cipher Suite use ... 141
14.2 Cipher Suite capabilities ... 142
14.3 Cipher Suite specification ... 143
14.4 Cipher Suite conformance ... 143
14.5 Default Cipher Suite (GCM-AES-128) ... 145
14.6 GCM-AES-256 ... 146
14.7 GCM-AES-XPN-128 ... 147
14.8 GCM-AES-XPN-256 ... 148

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

15. Ethernet Data Encryption devices ... 149

15.1 EDE characteristics ... 149
15.2 Securing LANs with EDE-Ms ... 150
15.3 Securing connectivity across PBNs ... 152
15.4 Securing PBN connectivity with an EDE-M ... 153
15.5 Securing PBN connectivity with an EDE-CS ... 154
15.6 Securing PBN connectivity with an EDE-CC ... 156
15.7 Securing PBN connectivity with an EDE-SS ... 158
15.8 EDE Interoperability ... 159
15.9 EDEs, CFM, and UNI Access ... 160

16. Using MIB modules to manage EDEs ... 161

16.1 Security considerations ... 161
16.2 EDE-M Management ... 161
16.3 EDE-CS Management ... 161
16.4 EDE-CC and EDE-SS Management ... 161

Annex A (normative) PICS proforma ... 163

A.1 Introduction ... 163
A.2 Abbreviations and special symbols ... 163
A.3 Instructions for completing the PICS proforma ... 164
A.4 PICS proforma for IEEE Std 802.1AE ... 166
A.5 Major capabilities ... 167
A.7 MAC status and point-to-point parameters ... 169
A.6 Support and use of Service Access Points ... 169
A.8 Secure Frame Generation ... 170
A.9 Secure Frame Verification ... 171
A.10 MACsec PDU encoding and decoding ... 172
A.11 Key Agreement Entity LMI ... 172
A.12 Management ... 173
A.13 Additional fully conformant Cipher Suite capabilities ... 177
A.14 Additional variant Cipher Suite capabilities ... 177

Annex B (informative) Bibliography ... 180

Annex C (informative) MACsec test vectors ... 182

C.1 Integrity protection (54-octet frame) ... 183
C.2 Integrity protection (60-octet frame) ... 188
C.3 Integrity protection (65-octet frame) ... 193
C.4 Integrity protection (79-octet frame) ... 198
C.5 Confidentiality protection (54-octet frame) ... 203
C.6 Confidentiality protection (60-octet frame) ... 208
C.7 Confidentiality protection (61-octet frame) ... 213
C.8 Confidentiality protection (75-octet frame) ... 218

Annex D (normative) PICS proforma for an Ethernet Data Encryption device ... 223

D.1 Introduction ... 223
D.2 Abbreviations and special symbols ... 223
D.3 Instructions for completing the PICS proforma ... 224
D.4 PICS proforma for IEEE Std 802.1AE EDE ... 226
D.5 EDE type and common requirements ... 227

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

D.6 EDE-M Configuration 228
D.7 EDE-CS Configuration 229
D.8 EDE-CC Configuration 229
D.9 EDE-SS Configuration 229

Annex E (informative) MKA operation for multiple transmit SCs 230

Annex F (informative) EDE Interoperability and PAE addresses 232

Annex G (informative) Management and MIB revisions 235

G.1 Counter changes 236
G.2 Available Cipher Suites 237

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

Figures

Figure 6-1 MACsec secured LAN with three stations ... 30
Figure 6-2 MACsec Frame, VLAN TAG, and QoS ... 32
Figure 7-1 Two stations connected by a point-to-point LAN ... 40
Figure 7-2 Two stations in a CA created by MACsec Key Agreement ... 40
Figure 7-3 Secure communication between two stations ... 41
Figure 7-4 Four stations attached to a shared media LAN ... 41
Figure 7-5 A CA including ports A, B, and C ... 42
Figure 7-6 Secure communication between three stations ... 42
Figure 7-7 Secure Channel and Secure Association Identifiers ... 44
Figure 8-1 MACsec ... 48
Figure 8-2 MACsec operation ... 54
Figure 9-1 MPDU components ... 56
Figure 9-2 SecTAG format ... 56
Figure 9-3 MACsec EtherType encoding ... 57
Figure 9-4 MACsec TCI and AN Encoding ... 57
Figure 10-1 SecY ... 61
Figure 10-2 SecY architecture and operation ... 64
Figure 10-3 Management controls and counters for secure frame generation ... 66
Figure 10-4 Management controls and counters for secure frame verification ... 69
Figure 10-5 SecY managed objects ... 73
Figure 11-1 Direct support of the MAC Service by a media access method ... 87
Figure 11-2 Provision of MAC Service with media-independent functions ... 88
Figure 11-3 MACsec in an end station ... 88
Figure 11-4 MACsec in a VLAN-unaware MAC Bridge ... 89
Figure 11-5 VLAN-unaware MAC Bridge Port with MACsec ... 89
Figure 11-6 Addition of MAC Security to a VLAN-aware MAC Bridge ... 90
Figure 11-7 IEEE 802.1Q VLAN-aware Bridge Port with MACsec ... 90
Figure 11-8 MACsec and Link Aggregation in an interface stack ... 91
Figure 11-9 IEEE 802.1Q VLAN-aware Bridge Port with MACsec and Link Aggregation ... 92
Figure 11-10 MACsec with LLDP ... 92
Figure 11-11 Internal organization of the MAC sublayer in a Provider Bridged Network ... 93
Figure 11-12 Interface stack for MAC Security to and across provider's network ... 93
Figure 11-13 Provider network with priority selection and aggregation ... 94
Figure 11-14 An example multi-access LAN ... 95
Figure 11-15 Multi-access LAN interface stack ... 96
Figure 12-1 MACsec with EPON, showing SCs and SCB ... 97
Figure 13-1 MACsec Interface Stack ... 98
Figure 13-2 SecY MIB structure ... 103
Figure 14-1 Cipher Suite Protect and Validate operations ... 141
Figure 15-1 EDE-Ms connected by a point-to-point LAN ... 150
Figure 15-2 EDE-Ms securing a point-to-point LAN between Provider Bridges ... 151
Figure 15-3 MACsec protected frame traversing a PBN ... 152
Figure 15-4 EDE-Ms securing point-to-point LAN connectivity across a PBN ... 153
Figure 15-5 EDE-Ms securing multi-point PBN connectivity ... 154
Figure 15-6 Example network with an EDE-CS ... 155
Figure 15-7 EDE-CS connected to a PBN S-tagged interface ... 156
Figure 15-8 Using an EDE-CC with a C-tagged provider service interface ... 157
Figure 15-9 EDE-CC architecture ... 158

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

Tables

Table 9-1 MACsec EtherType allocation ... 56
Table 10-1 Management controls and SecTAG encoding ... 67
Table 10-2 Extended packet number recovery (examples) ... 70
Table 10-3 SecY performance requirements ... 86
Table 13-1 Use of ifGeneralInformationGroup Objects ... 99
Table 13-2 Use of ifCounterDiscontinuityGroup Object ... 100
Table 13-3 Use of ifStackTable ... 100
Table 13-4 Use of ifStackGroup2 Objects ... 100
Table 13-5 Controlled Port service management ... 104
Table 13-6 Transmit and receive SC management ... 105
Table 13-7 Transmit and receive statistics ... 106
Table 13-8 Cipher Suite information ... 107
Table 14-1 MACsec Cipher Suites ... 144
Table 15-1 PAE Group Addresses ... 159
Table 15-2 PAE Group Address use ... 160
Table C-1 Unprotected frame (example) ... 183
Table C-2 Integrity protected frame (example) ... 183
Table C-3 GCM-AES-128 Key and calculated ICV (example) ... 184
Table C-4 GCM-AES-256 Key and calculated ICV (example) ... 185
Table C-5 GCM-AES-XPN-128 Key and calculated ICV (example) ... 186
Table C-6 GCM-AES-XPN-256 Key and calculated ICV (example) ... 187
Table C-7 Unprotected frame (example) ... 188
Table C-8 Integrity protected frame (example) ... 188
Table C-9 GCM-AES-128 Key and calculated ICV (example) ... 189
Table C-10 GCM-AES-256 Key and calculated ICV (example) ... 190
Table C-11 GCM-AES-XPN-128 Key and calculated ICV (example) ... 191
Table C-12 GCM-AES-XPN-256 Key and calculated ICV (example) ... 192
Table C-13 Unprotected frame (example) ... 193
Table C-14 Integrity protected frame (example) ... 193
Table C-15 GCM-AES-128 Key and calculated ICV (example) ... 194
Table C-16 GCM-AES-256 Key and calculated ICV (example) ... 195
Table C-17 GCM-AES-XPN-128 Key and calculated ICV (example) ... 196
Table C-18 GCM-AES-XPN-256 Key and calculated ICV (example) ... 197
Table C-19 Unprotected frame (example) ... 198
Table C-20 Integrity protected frame (example) ... 198
Table C-21 GCM-AES-128 Key and calculated ICV (example) ... 199
Table C-22 GCM-AES-256 Key and calculated ICV (example) ... 200
Table C-23 GCM-AES-XPN-128 Key and calculated ICV (example) ... 201
Table C-24 GCM-AES-XPN-256 Key and calculated ICV (example) ... 202
Table C-25 Unprotected frame (example) ... 203
Table C-26 Confidentiality protected frame (example) ... 203
Table C-27 GCM-AES-128 Key, Secure Data, and ICV (example) ... 204
Table C-28 GCM-AES-256 Key, Secure Data, and ICV (example) ... 205
Table C-29 GCM-AES-XPN-128 Key, Secure Data, and ICV (example) ... 206
Table C-30 GCM-AES-XPN-256 Key, Secure Data, and ICV (example) ... 207
Table C-31 Unprotected frame (example) ... 208
Table C-32 Confidentiality protected frame (example) ... 208
Table C-33 GCM-AES-128 Key, Secure Data, and ICV (example) ... 209
Table C-34 GCM-AES-256 Key, Secure Data, and ICV (example) ... 210
Table C-35 GCM-AES-XPN-128 Key, Secure Data, and ICV (example) ... 211
Table C-36 GCM-AES-XPN-256 Key, Secure Data, and ICV (example) ... 212
Table C-37 Unprotected frame (example) ... 213

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

Table C-38 Confidentiality protected frame (example) 213
Table C-39 GCM-AES-128 Key, Secure Data, and ICV (example) 214
Table C-40 GCM-AES-256 Key, Secure Data, and ICV (example) 215
Table C-41 GCM-AES-XPN-128 Key, Secure Data, and ICV (example) 216
Table C-42 GCM-AES-XPN-256 Key, Secure Data, and ICV (example) 217
Table C-43 Unprotected frame (example) 218
Table C-44 Confidentiality protected frame (example) 218
Table C-45 GCM-AES-128 Key, Secure Data, and ICV (example) 219
Table C-46 GCM-AES-256 Key, Secure Data, and ICV (example) 220
Table C-47 GCM-AES-XPN-128 Key, Secure Data, and ICV (example) 221
Table C-48 GCM-AES-XPN-256 Key, Secure Data, and ICV (example) 222
Table F-1 Interoperability scenarios and PAE Addresses 234

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

IEEE Standard for
Local and metropolitan area networks—
Media Access Control (MAC) Security

1. Overview

1.1 Introduction

IEEE 802® Local Area Networks (LANs) are often deployed in networks that support mission-critical applications. These include corporate networks of considerable extent, and public networks that support many customers with different economic interests. The protocols that configure, manage, and regulate access to these networks typically run over the networks themselves. Preventing disruption and data loss arising from transmission and reception by unauthorized parties is highly desirable, since it is not practical to secure the entire network against physical access by determined attackers.

MAC Security (MACsec), as defined by this standard, allows authorized systems that attach to and interconnect LANs in a network to maintain confidentiality of transmitted data and to take measures against frames transmitted or modified by unauthorized devices.

MACsec facilitates

a) Maintenance of correct network connectivity and services
b) Isolation of denial of service attacks
c) Localization of any source of network communication to the LAN of origin
d) The construction of public networks, offering service to unrelated or possibly mutually suspicious customers, using shared LAN infrastructures
e) Secure communication between organizations, using a LAN for transmission
f) Incremental and non-disruptive deployment, protecting the most vulnerable network components.

To deliver these benefits, MACsec has to be used in conjunction with appropriate policies for higher-level protocol operation in networked systems, an authentication and authorization framework, and network management. IEEE Std 802.1X™ provides authentication and cryptographic key distribution.[1]

MACsec protects communication between trusted components of the network infrastructure, thus protecting the network operation. MACsec cannot protect against attacks facilitated by the trusted components themselves, and is complementary to, rather than a replacement for, end-to-end application-to-application

[1] Information on other references can be found in Clause 2.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

security protocols. The latter can secure application data independent of network operation, but cannot necessarily defend the operation of network components, or prevent attacks using unauthorized communication from reaching the systems that operate the applications.

1.2 Scope

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 802.1Q™, and IEEE Std 802.1X.[2]

To this end, it

a) Specifies the requirements to be satisfied by equipment claiming conformance to this standard.
b) Specifies the requirements for MACsec 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 MACsec 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 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 architecture of end stations, 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.

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

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used; therefore, 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.

IEEE Std 802®, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.[3,4]

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

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

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

IEEE Std 802.1AB™, IEEE Standard 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 802.3™, IEEE Standard for Ethernet.

IETF RFC 1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II, McCloghrie, K., and Rose, M. T., March 1991.[5]

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., and 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., and Waldbusser, S., April 1999.

IETF RFC 2580, STD 58, Conformance Statements for SMIv2, McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and 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., editor, December 2002.

ISO/IEC 14882, Information Technology—Programming languages—C++.[6]

NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007.[7]

[3] IEEE publications are available from The Institute of Electrical and Electronics Engineers (https://www.standards.ieee.org).
[4] The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.
[5] IETF RFCs are available from the Internet Engineering Task Force (https://www.ietf.org/rfc.html).
[6] ISO/IEC documents are available from the International Organization of Standardization (https://www.iso.org/) and from the International Electrotechnical Commission (http://www.iec.ch). These documents are also available from the American National Standards Institute (https://www.ansi.org/).
[7] NIST Special Publications are available from the National Institute of Standards and Technology (https://csrc.nist.gov/).

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

3. Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.[8]

access priority: The priority associated with a transmit request made by a MAC Security Entity (SecY) at its Common Port.

Association Number (AN): A number that is concatenated with the Secure Channel Identifier (SCI) to identify a Secure Association (SA).

black-side: Identifies the Ethernet Data Encryption device (EDE) port that uses MACsec to protect transmitted frames and verify received frames.

bounded receive delay: A guarantee that a frame will not be delivered after a known bounded time.

NOTE—In the case of the MAC Service, this is typically assumed to be less than two seconds.

Bridged Local Area Network: A concatenation of individual IEEE 802 Local Area Networks (LANs) interconnected by MAC Bridges.

NOTE—Unless explicitly specified the use of the word *network* in this standard refers to a Bridged Local Area Network. The term *Bridged Local Area Network* is not otherwise abbreviated. The term *Local Area Network* and the abbreviation *LAN* are used exclusively to refer to an individual LAN specified by a MAC technology without the inclusion of Bridges. This precise use of terminology within this specification allows a Bridged Local Area Network to be distinguished from an individual LAN that has been bridged to other LANs in the network. In more general usage such precise terminology is not required, as it is an explicit goal of this standard that MAC Security is transparent to the users of the MAC Service.

Cipher Suite: A set of one or more algorithms, designed to provide any number of the following: data confidentiality, data authenticity, data integrity.

Common Port: An instance of the MAC Internal Sublayer Service (ISS) used by the SecY to provide transmission and reception of frames for both the controlled and uncontrolled ports.

Controlled Port: The access point used to provide the secure MAC Service to a client of a MAC Security Entity (SecY).

cryptographic key: A parameter that determines the operation of a cryptographic function such as

a) The transformation from plain text to cipher text and vice versa
b) Synchronized generation of keying material
c) Digital signature computation or validation.[9]

cryptographic mode of operation: An algorithm for the cryptographic transformation of data that features a symmetric key block cipher algorithm. *Syn:* **mode.**[10]

[8] *IEEE Standards Dictionary Online* is available at https://dictionary.ieee.org.

[9] This and some other definitions in this clause have been drawn from ASC TR1/X9, Technical Report for ABA ASC/X9 Standards Definitions, Acronyms, and Symbols, 2002.

[10] This and some other definitions in this clause have been drawn from NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

Customer Edge Port: The red-side port of an Ethernet Data Encryption device (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 (PEBs) 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 Backbone Edge Bridges (BEBs) be specified, as the existence of additional variants would complicate interoperability, service provision, and the task of this standard.

Customer Network Port: A port on the network component of an Ethernet Data Encryption device (EDE-CS, EDE-CC, or EDE-SS) that provides internal connectivity to the edge component of that EDE.

data integrity: A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored.[11]

edge component: The bridge component in an Ethernet Data Encryption device (EDE-CS, EDE-CC, or EDE-SS) that is attached to the red-side port.

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.

IEEE 802 Local Area Network (LAN): LAN technologies that provide a MAC Service equivalent to the MAC Service defined in IEEE Std 802.1AC. IEEE 802 LANs include IEEE Std 802.3 (Ethernet) and IEEE Std 802.11 [B2] (Wireless).

NOTE—IEEE 802 LANs are also referred to in the text of this standard simply as LANs.

initialization vector (IV): A vector used in defining the starting point of an encryption process within a cryptographic algorithm.[12]

integrity: *See:* **data integrity.**

integrity check value (ICV): A value that is derived by performing an algorithmic transformation on the data unit for which data integrity services are provided. The ICV is sent with the protected data unit and is recalculated and compared by the receiver to detect data modification.

key: *See:* **cryptographic key.**

key management: The generation, storage, distribution, deletion, archiving, and application of keys in accordance with a security policy.

Layer Management Interface (LMI): The interface between a protocol entity in a system and the system management, providing for the exchange of parameters with other system entities that are not attached to the service access points used and provided by the protocol entity.

Local Area Network (LAN): *See:* **IEEE 802 Local Area Network (LAN).**

[11] This and some other definitions in this clause have been drawn from NIST Special Publication 800-57, Recommendation for Key Management, 2005.

[12] This and some other definitions in this clause have been drawn from Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, 2001.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

MAC Security Entity (SecY): The entity that operates the MAC Security protocol within a system.

MAC Security TAG (SecTAG): A protocol header, comprising a number of octets and beginning with an EtherType, that is prepended to the service data unit supplied by the client of the protocol and is used to provide security guarantees.

MAC service data unit (MSDU): A sequence of zero or more octets that compose the data to be communicated with a single MAC Service request or indication.

master key: A secret key that is used to derive one or more cryptographic keys that are used directly to protect data transfer.

message authentication: If the message arrives authenticated, the cryptographic guarantee is that the message was not modified in transit and that the message originated from an entity with the proper cryptographic credentials.

mode: *See:* **cryptographic mode of operation.**

multipoint: Involving or potentially involving more than one participant in the role of receiver, or in the role of transmitter, in a single data transfer or set of related data transfers.

network component: The bridge component in an Ethernet Data Encryption device (EDE-CS, EDE-CC, or EDE-SS) that is attached to the black-side port.

nonce: A non-repeating value, such as a counter, used in key management protocols to thwart replay and other types of attack.[13]

Packet Number (PN): A monotonically increasing value that is guaranteed unique for each MACsec frame transmitted using a given Secure Association Key (SAK).

Port Identifier: A 16-bit identifier that uniquely identifies each of a system's transmit Secure Channels (SCs) that uses the same MAC address as a component of its Secure Channel Identifier (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.

Protocol Data Unit (PDU): A unit of data specified in a protocol and consisting of protocol information and, possibly, user data.

Provider Edge Port (PEP): A port on the edge component of an Ethernet Data Encryption device (EDE-CS, EDE-CC, or EDE-SS) that provides internal connectivity to the network component of that EDE.

Provider Network Port: The black-side port of an Ethernet Data Encryption device (EDE-CS, EDE-CC, or EDE-SS).

red-side: Identifies the Ethernet Data Encryption device (EDE) port that does not use MACsec to protect transmitted frames or verify received frames.

Reserved Address: A group address filtered by a bridge component to restrict the scope of the control protocols using that Destination Address (DA).

[13] This and some other definitions in this clause have been drawn from ASC TR1/X9, Technical Report for ABA ASC/X9 Standards Definitions, Acronyms, and Symbols, 2002.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

secret key: A cryptographic key used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public.[14]

Secure Association (SA): A security relationship that provides security guarantees for frames transmitted from one member of a Connectivity Association (CA) to the others. Each SA is supported by a single secret key, or a single set of keys where the cryptographic operations used to protect one frame require more than one key.

Secure Association Identifier (SAI): An identifier for an Secure Association (SA), comprising the Secure Channel Identifier (SCI) concatenated with the Association Number (AN).

Secure Association Key (SAK): The secret key used by a Secure Association (SA).

Secure Channel (SC): A security relationship used to provide security guarantees for frames transmitted from one member of a Connectivity Association (CA) to the others. An SC is supported by a sequence of Secure Associations (SAs) thus allowing the periodic use of fresh keys without terminating the relationship.

Secure Channel Identifier (SCI): A unique identifier for a Secure Channel (SC), composed of a MAC Address and a Port Identifier.

NOTE—Key agreement protocols such as the MACsec Key Agreement protocol (MKA) (see IEEE Std 802.1X) are responsible for ensuring that each SCI used with a given Secure Association Key (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.

secure Connectivity Association (CA): A security relationship, established and maintained by key agreement protocols, that comprises a fully connected subset of the service access points in stations attached to a single Local Area Network (LAN) that are to be supported by MACsec.

Short Secure Channel Identifier (SSCI): A 32-bit value, managed by the key agreement protocol, that is unique for each SCI within the context of all MAC Security Entities (SecYs) using a given Secure Association Key (SAK).

spoofing: Claiming a fraudulent identity for purposes of mounting an attack.

Uncontrolled Port: The access point used to provide the insecure MAC Service to a client of a MAC Security Entity (SecY).

user priority: The priority associated with a transmit request received by the Controlled Port of a MAC Security Entity (SecY).

[14] From FIPS 140-2.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

4. Abbreviations and acronyms

The following abbreviations and acronyms are used in this standard.

AES	Advanced Encryption Standard
AN	Association Number
BEB	Backbone Edge Bridge
BPDU	Bridge Protocol Data Unit
CA	secure Connectivity Association
CFM	Connectivity Fault Management
CRC	Cyclic Redundancy Check
DA	Destination Address
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
EISS	Enhanced Internal Sublayer Service
EPON	Ethernet Passive Optical Network
ES	end station
FCS	frame check sequence
GCM	Galois Counter Mode
ICV	integrity check value
ISS	Internal Sublayer Service
IV	initialization vector
KaY	MAC Security Key Agreement Entity
LACP	Link Aggregation Control Protocol
LAN	IEEE 802 Local Area Network
LLC	Logical Link Control (ISO/IEC/IEEE 8802.2™ [B10])
LLDP	Link Layer Discovery Protocol
LMI	Layer Management Interface
MAC	Media Access Control
MACsec	Media Access Control Security
MIB	Management Information Base
MKA	MACsec Key Agreement protocol (IEEE Std 802.1X)

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

MKPDU	MACsec Key Agreement Protocol Data Unit
MPDU	MACsec Protocol Data Unit
MSDU	MAC Service Data Unit
MSTP	Multiple Spanning Tree Protocol
OLT	Optical Line Terminal
ONU	Optical Network Unit
PAE	Port Access Entity
PCP	Priority Code Point (IEEE Std 802.1Q)
PDU	Protocol Data Unit
PEB	Provider Edge Bridge
PEP	Provider Edge Port
PN	Packet Number
QoS	Quality of Service
RSTP	Rapid Spanning Tree Algorithm and Protocol
SA	Secure Association or Source Address, as applicable
SAI	Secure Association Identifier
SAK	Secure Association Key
SC	Secure Channel
SCB	Single Copy Broadcast
SCI	Secure Channel Identifier
SecTAG	MAC Security TAG
SecY	MAC Security Entity
SL	Short Length
SMI	Structure of Management Information
SNMP	Simple Network Management Protocol
SSCI	Short Secure Channel Identifier
STP	Spanning Tree Protocol
UNI	User Network Interface (IEEE Std 802.1Q)

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

5. Conformance

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***.

5.2 Protocol Implementation Conformance Statement (PICS)

The supplier of a 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 and shall provide the information necessary to identify both the supplier and the implementation.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

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 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 802.1Q PICS proforma as required for a VLAN-unaware MAC Bridge.
d) For an EDE-CS: the IEEE 802.1Q PICS proforma as required for a Provider Edge Bridge.
e) For an EDE-CC: the IEEE 802.1Q PICS proforma as required for each of the two C-VLAN components.
f) For an EDE-SS: the IEEE 802.1Q PICS proforma as required for each of the two S-VLAN components.

5.3 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 Protocol Data Units (MPDUs) as specified in Clause 9.
f) Use a 48-bit MAC Address and a 16-bit Port Identifier unique within the scope of that address assignment to identify each transmit SCI, as specified in 8.2.1.
g) Satisfy the performance requirements specified in Table 10-3 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 MPDUs by using Cipher Suites as specified in 14.1.
k) Support Integrity Protection using the Default Cipher Suite specified in Clause 14.
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 10-3.
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.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

An implementation of a 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 frame check sequence (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 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 MAC Security Entity options

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

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.

An implementation of a 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, and 14.4.1.

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 (SecY) that is part of the EDE implementation, with the restrictions, additions, exceptions, and clarifications specified in this standard for that type of EDE.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

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 Port Access Entity (PAE) that includes a MACsec Key Agreement Entity (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 (5.14 of IEEE Std 802.1Q-2018) 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 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 (5.10.2 of IEEE Std 802.1Q-2018) 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).

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

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 (5.5 of IEEE Std 802.1Q-2018)—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 (5.6 of IEEE Std 802.1Q-2018)—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 (Table 8-2 of IEEE Std 802.1Q-2018) or the EDE-SS 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 S-tagged with the same S-VID if they were S-tagged on receipt (15.7).

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

6. Secure provision of the MAC Service

MACsec provides secure communications between stations that are attached to the same LAN. An authenticated and authorized peer MAC Security Entity (SecY) within each station uses the insecure MAC Service provided by the LAN to provide the secure MAC Service to its client (see Figure 6-1). The requirements for MACsec discussed in this clause are informed by the goal of preserving the MAC Service.

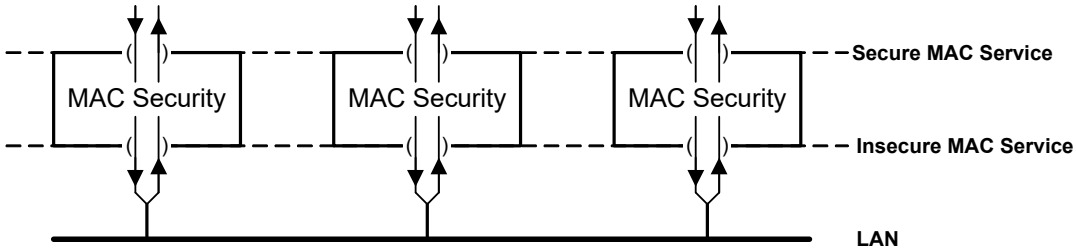

Figure 6-1—MACsec secured LAN with three stations

This clause discusses the

a) Primitives, parameters, connectivity, and status parameters provided by the MAC Service
b) Security threats posed by abuses of the MAC Service
c) Connectivity used and provided by the MACsec protocol
d) Service guarantees provided by MACsec and the security services they support
e) Quality of Service (QoS) issues addressed in the design, implementation, and use of MACsec.

NOTE 1—In order to introduce the concepts used in this standard, this clause can repeat or summarize the specification in other clauses; however, it contains no normative provisions that apply either to the subject matter of those other clauses or to the other standards referenced. For conformance to this standard see Clause 5.

NOTE 2—MACsec does not itself guarantee the security of a Bridged Local Area Network, as that security depends on the security of the individual LANs that comprise the network, on the policies adopted by clients of the secure MAC Service (7.3), and on the security of the MAC Bridges that interconnect those LANs.

NOTE 3—Authentication and authorization are outside the scope of this standard, which ensures secure communication between mutually authenticated and authorized service access points.

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 802.1AC, IEEE Std 802.1Q).

6.1 MAC Service primitives and parameters

The MAC Service (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.

Each request and indication primitive has the following four parameters:

— Destination Address
— Source Address
— Priority
— MAC Service Data Unit (MSDU)

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

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 IEEE Std 802.1AC. The service provided by a LAN to a MAC Bridge is the MAC Internal Sublayer Service (ISS), which 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-2018). 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 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—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 MAC Service provided by a single LAN preserves the relative order of service requests and corresponding service indications with the same requested priority. Each instance of the MAC Service provided using an instance of the EISS preserves the relative order of requests and indications with the same destination address, source address, and priority if the destination address is an individual address, and the relative order of requests and indications with the same destination address and priority if the destination address is a group address.

NOTE 3—A Provider Bridged Network can use the EISS to provide instances of the MAC Service that appear, with the exception of ordering constraints, to be a single LAN and are used as such by MACsec.

The address and MSDU parameters delivered with a service indication have identical values to those supplied with the corresponding service request. The MAC Service does not validate the parameters supplied with the request; for example, it does not provide any assurance that the source address used by an LLC client is the individual address previously allocated to the station.

NOTE 4—For example, in the absence of policies that require authorization to use an address, or check that a MACsec participant does not change its address, the use of MACsec will not protect against ARP spoofing. MACsec can form part of a solution that prevents ARP spoofing provided that suitable client policies are used in conjunction with MACsec, as mentioned in 1.1, in Clause 6, and in Clause 7 (particularly 7.3). In the case of ARP spoofing, appropriate policies include a selection of not accepting frames from an end station with a different source address than that used in the authentication dialogue, not accepting frames from bridges that are not known to obey that rule, requiring use of device identification to ensure use of a legitimate MAC address, and filtering certain higher-layer protocol frames unless received (using MACsec) from a system allowed to send them.

The priority parameter delivered with a service indication has an identical value to that supplied with the corresponding service request, where the media access control method used supports communication of priority. The access to the LAN granted by the media access control method can take the requested priority value into account, but can also be based on other factors. The IEEE 802.3™ media access control method does not convey priority, and the priority value delivered with the service indication is determined by management of the receiving station. However, where the EISS is used to support an instance of the MAC Service, the priority parameter of the EISS is encoded within a VLAN TAG (IEEE Std 802.1Q) that forms the initial octets of the MSDU accompanying a service request to the instance of the ISS used to support the EISS. Figure 6-2 shows the priority field encapsulated in the VLAN TAG within the Secure Data portion of the MACsec frame. In this case, the value of the priority parameter delivered with the service indication will be identical to that provided with the corresponding request.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

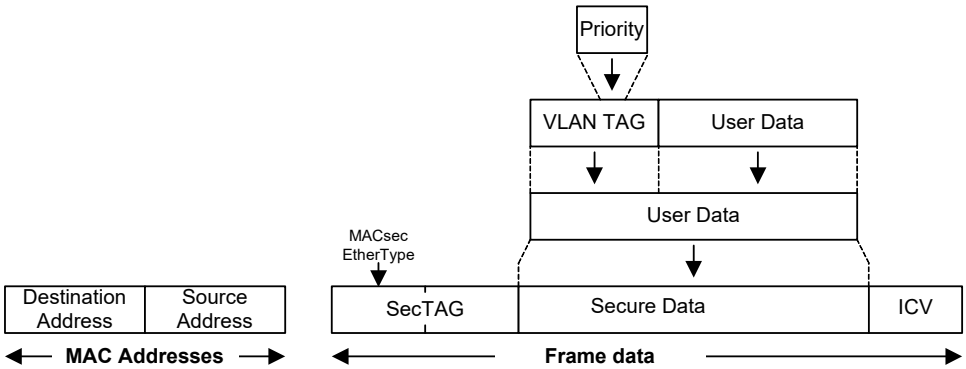

Figure 6-2—MACsec Frame, VLAN TAG, and QoS

6.2 MAC Service connectivity

The MAC Service provided by a single point-to-point or shared media LAN provides symmetric and transitive connectivity between all the stations connected to that LAN. Following a service request at one service access point, a corresponding service indication occurs, with high probability, at all the MAC ISS access points in other stations attached to the same LAN. Service indications at service access points that provide the MAC Service to an LLC Entity are filtered by media access functions, generally within each receiving station, to exclude frames that are not destined to an individual or group address used by the client.

NOTE 1—Symmetric connectivity means that if station A can communicate with station B, then B can also communicate with A. Transitive connectivity means that if station A can communicate with B, and B with C, then A can also communicate with C.

NOTE 2—Some media access control devices or methods are capable of not delivering some or all frames with unwanted destination addresses to some or all stations.

MAC Service clients and client protocols can operate incorrectly if the connectivity provided is not as expected. While some protocols can detect the lack of symmetric connectivity, they can simply deny service as a result. Protocols can operate inefficiently if transitive connectivity is not provided. While MAC Bridges can filter frames to restrict provision of service, the use of Virtual LANs (VLANs), with each VLAN providing full connectivity, is preferred to lessen the administrative burden of ensuring correct connectivity.

NOTE 3—The original Spanning Tree Protocol (STP) could create loops in the network if symmetric connectivity was not provided. The Rapid Spanning Tree Algorithm and Protocol (RSTP), (see IEEE Std 802.1Q), 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.

6.3 Point-to-multipoint LANs

A point-to-multipoint LAN provides connectivity from a single distinguished station to one or more other stations, i.e., from one point to multiple other points, and from each of the other stations to the distinguished station. The point-to-multipoint LAN does not provide direct connectivity between pairs of stations unless the distinguished station is one of the pair. Efficient multicast and broadcast from the distinguished station to all the others is provided: a single service request with a given destination address can result in service indications at each multipoint station wishing to receive frames with that destination address. Communication between the other stations occurs via the distinguished station, as specified by the relevant standard for the particular technology.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

NOTE—Examples of point-to-multipoint LANs include IEEE 802.3 Ethernet Passive Optical Network (EPON) (see Clause 12), IEEE Std 802.11™ [B2], and certain provider network VLAN configurations. Depending on the particular LAN or network technology the distinguished stations are variously referred to as optical line terminals (OLTs), wireless access points (WAPs), head-ends, concentrators, star concentrators, or root nodes, and the other stations as optical network units (ONUs), stations, modems, or leaf nodes.

6.4 MAC status parameters

Each service access point can make available status parameters that reflect the operational state and administrative controls for the service instance provided at that access point.

The **MAC_Enabled** parameter is TRUE if use of the service is permitted and is otherwise FALSE. The value of this parameter is determined by administrative controls specific to the entity providing the service.

The **MAC_Operational** parameter is TRUE if, and only if, service requests can be made and service indications can occur.

The value of the MAC_Enabled and MAC_Operational parameters are determined by the specific entity providing the MAC Service. 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 802.1Q), Multiple Spanning Tree Protocol (MSTP, IEEE Std 802.1Q), and Link Aggregation Control Protocol (LACP, IEEE Std 802.1AX™ [B4]). 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

Each service access point can make available status parameters that reflect the point-to-point status for the service instance provided, and that allow administrative control over the use of that information.

If the **operPointToPointMAC** parameter is TRUE, the service is used as if it provides connectivity to at most one other system; if FALSE, the service is used as if it can provide connectivity to a number of systems.

The **adminPointToPointMAC** parameter can take one of three values. If it is

a) **ForceTrue**, operPointToPointMAC shall be TRUE, regardless of any indications to the contrary generated by the service providing entity.
b) **ForceFalse**, operPointToPointMAC shall be FALSE.
c) **Auto**, operPointToPointMAC is as currently determined by the service providing entity.

IEEE Std 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 and MSTP (IEEE Std 802.1Q) require the use of operPointToPointMAC to facilitate rapid reconfiguration in some network failure scenarios. LACP (IEEE Std 802.1AX [B4]) does not aggregate links that are not point-to-point and can use operPointToPointMAC to make this determination.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

6.6 Security threats

The expected features of the MAC Service described in 6.1 through 6.5—the relationships between service requests and indications, preservation of the parameters of these primitives, the connectivity provided, and the relationship of the MAC status parameters to the connectivity—can be accidentally and unintentionally distorted through misconfiguration or deliberately abused. Misconfiguration or abuse can result in

a) Inability to issue service requests
b) Indiscriminate loss of service indications
c) Specifically targeted loss of service indications
d) Repeated service indications at the intended destinations
e) Service indications with modified address or data parameters
f) Additional service indications with unmodified or selectively modified parameters
g) Service indications at unintended recipients
h) Delayed service indications that can disrupt network operation
i) Disclosure of the MSDU to unauthorized parties.

Deliberate abuse can serve as a basis for an attack upon the resources accessible from a LAN through attacks on the protocols that use the service and provide access to or control over those resources. The effort required by an attacker to abuse the service in any particular way depends in general on the media access control method used by the LAN, and the particular devices and components that support it.

The MAC Service does not guarantee the origin or authenticity of service requests and the accompanying parameters. Since a station's sole use of its source address and the restriction of service indications to intended recipients can depend on cooperative behavior from other stations, it is usually easy for an attacker that can attach a station to a LAN to receive any service indication and to issue additional service requests with parameters based on those indications. Other service abuses can require physical access to inconveniently located components.

It is beyond the scope of this standard to enumerate all the ways in which abuses of the service can be exploited. They include techniques commonly referred to as passive wiretapping, masquerading, and man-in-the-middle attacks. The latter is facilitated by source address spoofing, usually after another station with that source address has been observed to have been granted access to some resource. Attacks can include

j) Denial of service, to all or to selected stations
k) Theft of service
l) Access to confidential information
m) Modification of confidential information
n) Access to or control over restricted resources.

MACsec does not protect against brute force denial of service attacks that can be mounted by abusing the operation of particular media access control methods through degrading the communication channel or transmitting erroneous media access method specific control frames.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

6.7 MACsec connectivity

The connectivity provided (6.2) between the MAC Internal Sublayer Service (ISS) access points of stations connected to a single LAN composes an insecure association between communicating stations. Key agreement protocols as defined in IEEE Std 802.1X establish and maintain a secure Connectivity Association (CA), which is a fully (i.e., symmetric and transitive) connected subset of the ISS service access points. Each instance of MACsec operates within a single CA.

NOTE 1—ISO/IEC 15802, the MAC Service definition, introduces the term *Connectivity Association* to discuss the relationship between service access points without referring to the details of particular media access control methods or to terms such as *physical connection* or *logical connection* that have other associated attributes and meanings.

MACsec itself does not provide comprehensive monitoring of the connectivity provided by a CA, although it can detect and will signal certain failures to the local MAC Security Key Agreement Entity (KaY). Together, operation of key agreement protocols and MACsec ensures that the status parameters provided by an instance of the secure MAC Service correctly reflect both the current connectivity and changes in the connectivity of the CA. Specifically

a) MAC_Operational is only True if the CA is complete (i.e., is symmetric and transitive), and the local MACsec Entity (SecY) can both receive and transmit.

   NOTE 2—EPON is discussed in Clause 12.

b) If MAC_Operational is True in stations wanting to join a new CA and in stations already in the target CA, and if stations are added to the CA, MAC_Operational transitions to False in either all the stations originally participating in the CA or in all those added, for sufficient duration such that clients of the service are aware of the transition.

   Determining which group transitions MAC_Operational to False is outside the scope of this specification and is determined by the KaY and signaled through the LMI.

c) If MAC_Operational is False in stations wanting to join a CA, and if these stations are added to a CA, there is no change in the MAC_Operational status of the stations already in the target CA, and MAC_Operational will transition to True in the joining stations after some period of time. This is the typical case for a single station joining a CA, in which its MAC_Operational is False until the join is accomplished when its state transitions to MAC_Operational True.

d) If adminPointToPointMAC is set to Auto and MAC_Operational is True, then operPointToPointMAC is True only if at most one other station is participating in the CA. If adminPointToPointMAC is set to forceFalse, then operPointToPointMAC must be False, regardless of the number of stations in the CA.

NOTE 3—Communication between KaYs in stations that compose a CA does not depend on the operation of MACsec.

6.8 MACsec guarantees

At each service access point that is a member of a CA, MACsec ensures that any service indication

a) Is the result of a service request at a service access point that is also a member of the same CA
b) Has the parameter values that are identical to those supplied with the service request

and can also ensure that

c) No more than one indication results from one service request
d) A service indication does not occur after a known bounded time has elapsed since the service request was made
e) The values of the octets that comprise the MAC Service Data Unit (MSDU) parameter cannot be ascertained except by members of the CA.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

MACsec does not

f) Conceal the following from stations that are not members of the CA:
   1) Service requests
   2) Values of service request address parameters
   3) The number of octets that comprises the MSDU
g) Validate the parameters provided with a service request.

MACsec provides guarantees to within known bounds that are derived from the cryptographic methods and other mechanisms used.

The known bounded time in item d) is typically longer than required to enforce the maximum transit delay requirements of the MAC Service.

NOTE—The addition of explicit time indications to the MAC Security TAG (SecTAG) to provide tight bounds for transit delay was considered in the development of this standard, but the value delivered is small for the added complexity and the burden imposed on key agreement protocols. Higher-layer protocols that have tight timing requirements typically add their own timing markers. As these markers are carried within the MSDU, their integrity is protected by MACsec.

6.9 Security services

The guarantees provided by MACsec support the following security services for stations participating in MACsec:

a) Connectionless data integrity [6.8a), 6.8b)]
b) Data origin authenticity [6.8a)]. If the connectivity model is point-to-point, the originator is authenticated, but if the connectivity model is multipoint, then the authenticated originator is any member of the CA, rather than a particular individual station.
c) Confidentiality [6.8d)]
d) Replay protection [6.8c), 6.8d)]
e) Bounded receive delay

and can be used to limit the nature and extent of

f) Denial of service attacks.

MACsec does not support

g) Non-repudiation (ISO/IEC 7498-2)

or protect against

h) Traffic analysis (ISO/IEC 7498-2).

A MAC Bridge that forwards a frame with an erroneous source MAC address can unintentionally facilitate a denial of service or other attack on other LANs within a Bridged Local Area Network. The MAC Bridge should use MACsec in conjunction with an appropriate policy to verify the binding of the source MAC address to access to resources.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

6.10 Quality of Service maintenance

The quality of the MAC Service can be lowered by direct attacks on the operation of particular media access control methods and indirect attacks on their resource allocation procedures facilitated by masquerading and unauthorized data modification. MACsec does not provide guarantees for frames, known as MAC control frames, that are internal to the operation of a particular media access method and cannot defend against abuses that use or affect such frames. MAC control frames are not forwarded by MAC Bridges, so attacks that exploit them can be localized to particular LANs.

NOTE—Where, within the operation of a particular media access control method, it is possible to establish secure Connectivity Associations (CAs) prior to performing certain control functions, those functions should be supported by frames transmitted using an instance of the ISS. The parameters of those frames can then be protected by MACsec, and the scope for abuse restricted. It is not a requirement of the Open Systems Interconnection (OSI) layer model (ISO 7498) that management and control of a particular layer be carried out purely within that layer by protocols whose identifiers and formats are specific to that layer. For example, SNMP can be used to manage MAC Bridges.

Operation of a security protocol has the potential to lower some aspects of QoS. The operation and design of MACsec is discussed below as it relates to

a) Service availability
b) Frame loss
c) Frame misordering
d) Frame duplication
e) Frame transit delay
f) Frame lifetime
g) Undetected frame error rate
h) Maximum service data unit size supported
i) Frame priority
j) Throughput.

Use of MACsec can lower service availability if delays occur in the creation of Connectivity Associations or in the distribution and maintenance of cryptographic keying material. Failures or attacks upon the system that supports authentication and authorization can result in denial of service.

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 transit 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.

MACsec does not introduce any additional potential for duplicating or misordering frames. No retransmission mechanisms are added to relax requirements for distribution and use of MACsec related information. MACsec implementations are required to preserve the sequence of requests and indications between the secure service access point supported and the insecure service access point used.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

Since the MAC Service is provided at an abstract interface within an end station, it is not possible to specify the total frame transit delay precisely. It is, however, possible to measure the additional transit delay introduced by an additional component or intermediate system.

The minimum additional transit delay introduced by MACsec is due to the increase in the MSDU size required to convey security information and essential buffering requirements required to meet the processing requirements of particular Cipher Suites. Specific limits are placed on the additional delays allowed to MACsec implementations (Table 10-3). The permitted delay is short compared with the upper bound mandated by the MAC Service, so it does not threaten the correct operation of higher-layer protocols.

Frame lifetime can be increased by MACsec if additional delay is introduced by providing security. The typical bound on frame lifetime is approximately two seconds.

MACsec does not increase the undetected frame error rate for frames received and transmitted on a single LAN. The frame check sequence (FCS) method used by each specific media access control method protects the entire frame including information added by MACsec. The integrity check added by MACsec can increase the probability of detecting unintentional frame modifications, particularly where those do not correspond to the expected noise characteristics for which the FCS was originally designed, but equally is not a substitute for the FCS since it is designed to ensure that an attacker has an exceedingly low chance of predicting how to make an undetected modification to the frame's parameters rather than to efficiently detect burst noise characteristics.

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 O of IEEE Std 802.1Q-2018 allow an 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.

The MSDU size that can be supported by an IEEE 802 LAN varies with the media access control method and its associated parameters (speed, electrical characteristics, etc.), and can be constrained by the owner of the LAN. MACsec adds security information to a transmitted MSDU, and thus the secure MAC service offers a smaller MSDU size than the insecure MAC service that it employs.

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 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.

Cryptography can be computationally intensive, and the operation of MACsec has the potential to lower throughput. The Cipher Suite(s) mandated and recommended by this standard have been chosen, in part, for their ability to support economic implementation across the range of LAN MAC data rates.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

7. Principles of secure network operation

This clause establishes the principles and a model of secure network operation. It describes the security relationships used to support the secure MAC Service (Clause 6), and how that service is used to provide overall network security. It provides the context necessary to understand the operation of the MAC Security protocol (MACsec) (see Clause 8) and individual MAC Security Entities (SecYs) (see Clause 10).

Secure network operation comprises use of the secure MAC Service on each of the individual LANs that compose the network together with the application of appropriate security policies by the MAC Service clients in end stations and in intermediate systems that forward frames. This clause defines

a) The security relationships that support secure MAC Service

and describes how the secure MAC Service is

b) Supported on each of the individual LANs that compose the network (7.1)
c) Used by the protocol entities that are its Clients (7.3)

and delineates the responsibilities of the

d) Key Agreement Entities (KaYs, IEEE Std 802.1X)
e) MAC Security Entities
f) Clients of the secure MAC Service.

Security relationships and the terms that identify them have been defined, in various ways, by a number of publicly available documents. This standard has deliberately chosen new terms to minimize confusion whenever differences could exist between previously used terms and the requirements. For example, the attributes associated with an Secure Association Identifier (SAI) (see Figure 7-7) are similar to but not exactly the same as those associated with the Security Parameter Index (SPI) defined by IPsec (IETF RFC 4303 [B8]). The normative properties of all terms used in this standard are as defined by this standard.

NOTE 1—The use of the term *secure network* in this clause refers to a network of end stations, LANs, bridges, routers and similar systems, and the servers and services that support these. The description and specification in this clause are limited to use of the secure MAC Service to contribute to overall system security (see Clause 1).

NOTE 2—In order to introduce the concepts used in this standard, this clause can repeat or summarize the specification in other clauses; however, it contains no normative provisions that apply either to the subject matter of those other clauses or to the other standards referenced. For conformance to this standard (see Clause 5).

NOTE 3—The term *individual LAN* is used in this standard to refer explicitly to an instance of media access method-specific technologies providing the MAC Service directly. The term excludes larger networks or subsets of a network that are created by aggregation or concatenation of individual LANs by Link Aggregation or bridges.

NOTE 4—The examples presented in this clause are intended to serve as a guide to best practice; however, the use of MAC Security is not limited to the examples given. Limits to the use of MAC Security that are required for the successful operation of network configuration and other protocols are made explicit.

7.1 Support of the secure MAC Service by an individual LAN

Each port that is capable of participating in an instance of the secure MAC Service comprises both a KaY and a SecY. Each KaY discovers or is made aware of the KaYs present in other stations attached to the same LAN, ensures that those stations are mutually authenticated and authorized, and creates and maintains the secure relationships between the stations that are used by the SecYs to transmit and receive frames. Specifically

a) A secure Connectivity Association (CA) is created to meet the requirements of the MAC Service (6.2) and MACsec (6.7) for connectivity between the stations attached to an individual LAN.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

b) Each CA is supported by unidirectional Secure Channels (SCs), each SC supporting secure transmission of frames through the use of symmetric key cryptography, from one of the systems to all the others in the CA.

c) Each SC is supported by an overlapped sequence of Security Associations (SAs).

d) Each SA uses a fresh Secure Association Key (SAK) to provide the MACsec service guarantees (6.8) and security services (6.9) for a sequence of transmitted frames.

NOTE—An SC can be required to last for many years without interruption, since interrupting the MAC Service can cause client protocols to re-initialize and recalculate aggregations, spanning trees, and routes (for example). An SC lasts through a succession of SAs, each using a new SAK, to defend against a successful attack on a key while it is still in use. In contrast it is desirable to use a new SAK at periodic intervals to defend against a successful attack on a key while it is still in use. In addition, the MACsec protocol (Clause 8 and Clause 9) only allows 2^{32}–1 frames to be protected with a single key unless a Cipher Suite that supports extended packet numbering is used. Since 2^{32} minimum-sized IEEE 802.3 frames can be sent in approximately 5 min at 10 Gb/s, this can force the use of a new SA.

These security relationships (CAs, SCs, and SAs) and the information associated with each of them are further discussed in 7.1.1, 7.1.2, and 7.1.3. Their mutual relationship, and the insecure connectivity provided by the LAN that supports them, are illustrated in Figure 7-1 through Figure 7-3 for a point-to-point LAN and in Figure 7-4 through Figure 7-6 for stations attached to a shared media LAN.

Figure 7-1 shows two stations, A and B, connected to a point-to-point LAN that provides insecure bi-directional connectivity.

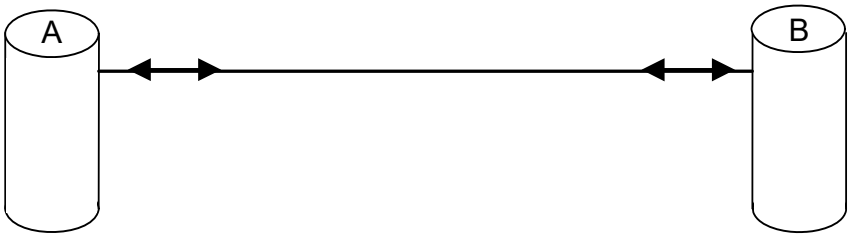

Figure 7-1—Two stations connected by a point-to-point LAN

Figure 7-2 depicts the CA created by MACsec Key Agreement following mutual authentication and authorization of A and B.

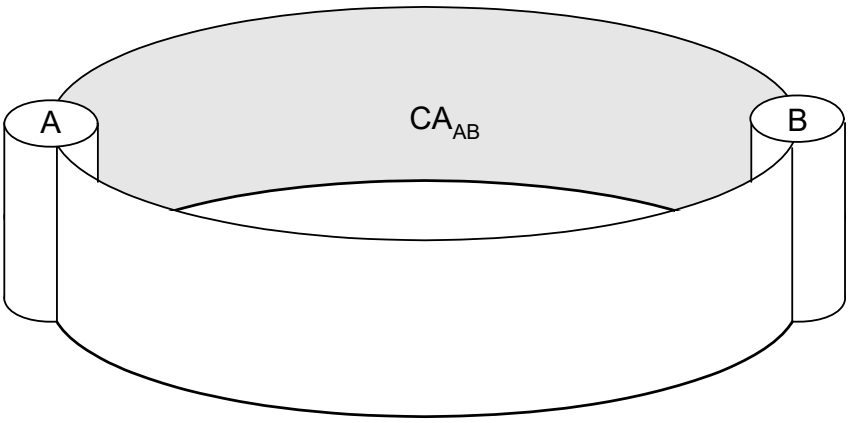

Figure 7-2—Two stations in a CA created by MACsec Key Agreement

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

Figure 7-3 shows the two SCs that support the CA.

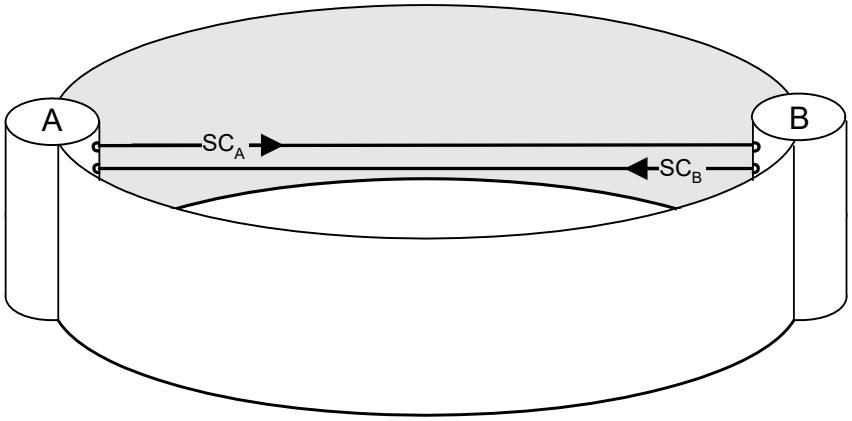

Figure 7-3—Secure communication between two stations

Figure 7-4 shows four stations, A, B, C, and D, attached to a shared media LAN that provides full but insecure connectivity between the stations.

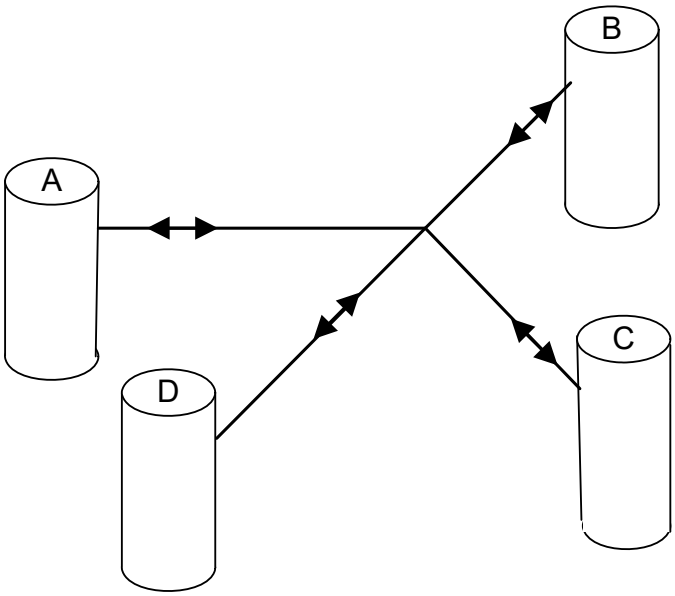

Figure 7-4—Four stations attached to a shared media LAN

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

Figure 7-5 depicts a CA created by MACsec Key Agreement following mutual authentication and authorization of A, B, and C. The CA excludes D.

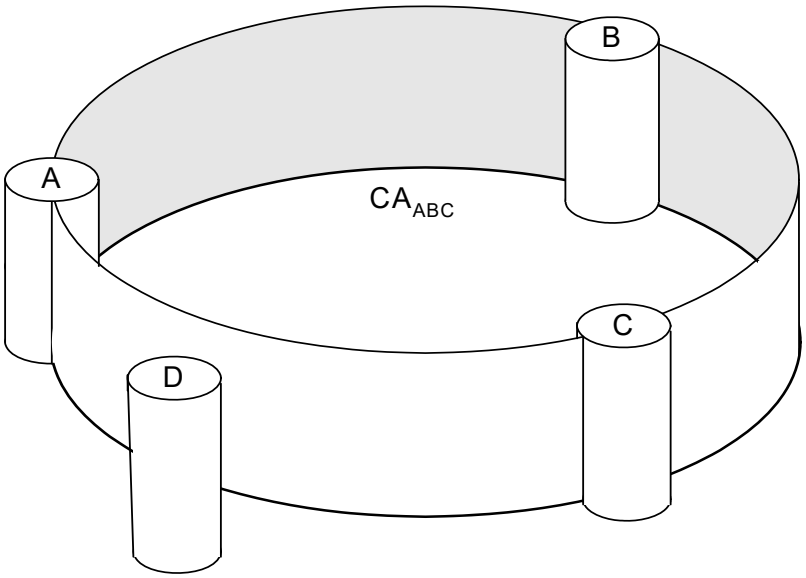

Figure 7-5—A CA including ports A, B, and C

Figure 7-6 shows the three SCs that support the CA, one for transmission by each of A, B, and C.

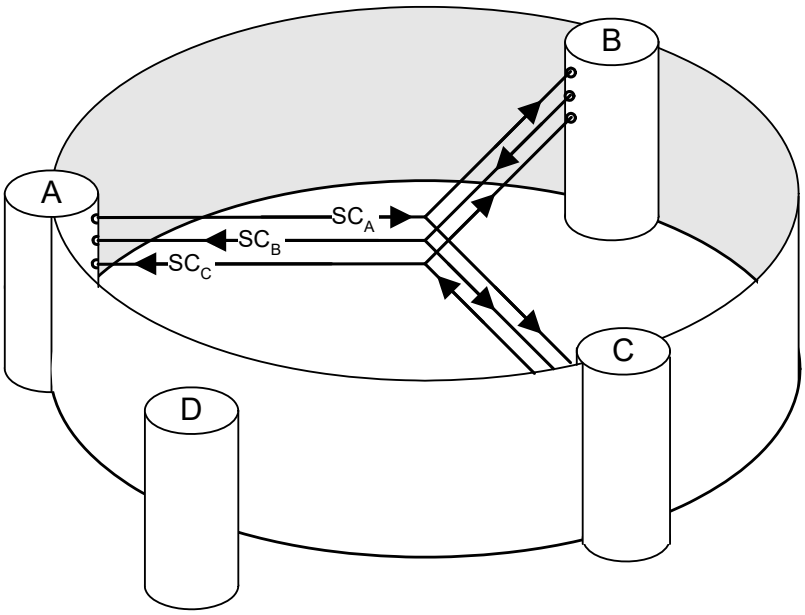

Figure 7-6—Secure communication between three stations

While D can send and receive frames using the insecure connectivity provided by the shared LAN, it does not have SAKs that would allow it to participate in any of the SAs that currently support SC_A, SC_B, or SC_C; therefore, D cannot compromise the integrity, confidentiality, or origin of any of the frames being exchanged by A, B, and C.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

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.

7.1.1 Connectivity Association (CA)

MACsec Key Agreement is responsible for discovering, authenticating, and authorizing the potential participants in a CA. A SecY, as specified in this standard, does not need to be aware of the CA, except as a list of SCs in which it needs to participate. Since all the SCs in a CA use the same Cipher Suite at any one time, the Cipher Suite can be considered a property of the CA. A change in the Cipher Suite necessitates an interruption to the service provided by the CA.

Each SecY participates in only a single CA at any one time. There is a limit, readable by management and by the KaY, on the number of peer SecYs that can participate in a CA (10.7.7, 13.5).

NOTE—If this specification had allowed different SCs to use different Cipher Suites, a SecY implementing more than one Cipher Suite would have to be capable of simultaneous transmitting using one Cipher Suite and receiving using one or more other Cipher Suites.

7.1.2 Secure Channel (SC)

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 48-bit MAC address concatenated with a 16-bit Port Identifier.

NOTE 1—Including the Port Identifier component would appear to be unnecessary in the case of a simple system with a MAC address and a single SecY for each port. However, some systems require support for more SecYs than they have uniquely allocated addresses 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.

NOTE 2—An EPON Optical Line Terminal (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 Identifier. 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 each transmitting 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 MACsec Key Agreement PDUs (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.

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.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

7.1.3 Secure Association (SA)

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 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 SAI is only unique for the SAs used by SecYs participating in a given CA at any instant.

MACsec Key Agreement is responsible for creating and distributing SAKs to each of the SecYs in a CA. This key creation and distribution is independent of the cryptographic operation of each of the SecYs. The same SAK can be used for SAs that compose different SCs, provided that every initialization vector (IV) used with the SAK is unique. When the Default Cipher Suite (14.5) is used, the SCI is included in the IV to ensure uniqueness across SCs.

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.

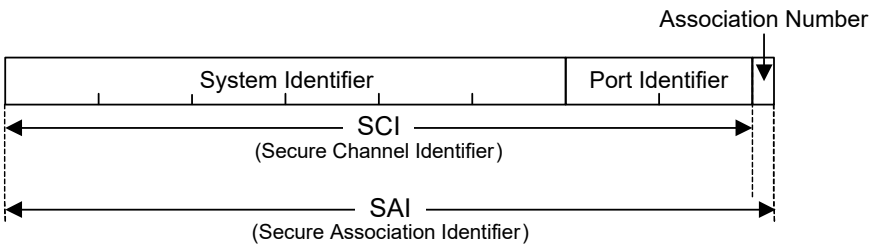

Figure 7-7—Secure Channel and Secure Association Identifiers

If a SecY does not have a usable SA for its outbound SC, i.e., an SA that can be used at no notice for frame transmission with a PN value that is not exhausted, or any of the current SAs for inbound SCs are not usable, then the MAC_Operational status parameter (6.4) will transition to FALSE.

7.2 Multiple instances of the secure MAC Service on a single LAN

Each service access point for an instance of the secure MAC Service is supported by a service access point for an instance of an insecure MAC Internal Sublayer Service (ISS). Multiple instances of the secure MAC Service can be provided by a single LAN, provided that each instance is uniquely identified by unencrypted fields contained in each received frame. These fields identify separate instances of the insecure MAC ISS, each capable of supporting a distinct service access point for MACsec.

Identification of each insecure service instance, and multiplexing and demultiplexing to and from the transmission capabilities provided by the LAN, can be performed wholly below the ISS by a media-specific or media-dependent function. Some media are defined to support such a multiplexing function, e.g., the

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

LLID used by IEEE 802.3 EPON (see Clause 12). Where such media-specific multiplexing functions are not available, the source address or SCI may be used (11.8). Provider Bridges are also capable of supporting multiple instances of the ISS over a network of individual LANs (see 11.6).

MACsec should not be used to support multiple instances of the secure MAC Service on a single physical LAN without the use of unencrypted frame fields to identify separate instances of insecure service, each supporting a single instance of secure service. While the use of security to provide multiplexing is impossible to prevent (since different cryptographic keys can be used to separate connectivity), relying solely on security to define the connectivity makes deployment and fault management difficult—the topology of an entire network could change as security was enabled or disabled on a single LAN. Key agreement protocols that use the insecure MAC service can require a matching instance of that service for each secure service instance.

NOTE 1—The service access point for the secure MAC Service is referred to as Controlled Port of the SecY (Clause 10) and the service access point for the insecure MAC Service as the SecY's Common Port. Access to the insecure service for protocol entities above MAC Security is provided at the Uncontrolled Port.

NOTE 2—Although the field or fields used to provide service instance multiplexing are not parameters of the ISS, and thus are not protected, the integrity of the secure MAC Service is not compromised. If the unprotected fields are modified, the frame can be delivered to the wrong SecY, but will subsequently fail integrity checks. Different SecYs use different security associations, keys, and cryptographic nonces. Additional management parameters are (cryptographically) bound to individual SecYs, not to the values of frame fields.

The secure MAC Service requirements for symmetric and transitive connectivity ensure that two or more service instances on the same LAN will appear as separate LANs to the clients of the SecYs. There is therefore no conflict between the use of bridges and the provision of multiple secure service instances.

When clients that are connected to a first service instance change and connect to a second service instance, the secure connectivity alters. MAC_Operational temporarily transitions to False for a minimum amount of time to allow the CA to re-establish its membership (as determined by the KaY). In particular, each time membership of a CA changes, MAC_Operational transitions False for at least one of each pair of SecYs whose connectivity has changed. For example, if members of CA_x leave CA_x and join CA_y and if CA_y has MAC_Operational True, then MAC_Operational transitions to False for either the members of CA_x who are joining CA_y or for the original members of CA_y. MAC_Operational transitions to True once all the new members have joined CA_y.

NOTE 3—Two SecYs that connect to the same LAN and participate in the same CA appear connected to the same LAN (as one would expect) and appear connected to different LANs as they participate in distinct CAs. The effect is similar to partitioning a LAN by switching a repeater on or off.

Distinct instances of the secure point-to-point MAC Service can be provided by a bridge to different end stations connected to the same shared media by using the source address of the frames transmitted by each end station to identify one of a number of SecYs in the receiving bridge (11.8). Where the source address is not sufficient to select the receiving SecY, the SCI can be used to provide service instance multiplexing for both secured and unsecured frames (11.8, 9.5, 10.6).

NOTE 4—IEEE Std 802.11 [B2] specifies its own mechanisms for identifying separate secure associations.

7.3 Use of the secure MAC Service

The secure MAC Service guarantees (6.8) the integrity of the parameters of each service indication, and that each indication is a result of a request made by a SecY that is a member of the same CA as the receiver, though not by any particular member. Management controls associated with each KaY can require certain authentication and key management methods to ensure these guarantees. However, the degree of trust placed in the security of the communication does not imply the degree of trust associated with the communicating peers. Accordingly, the MACsec Key Agreement framework facilitates authorization of each potential member and allows management of the acceptable authorization for inclusion in the CA.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020

The secure MAC service does not itself provide any means to label or distinguish different levels of authorization, and does not associate different levels of authorization with individual invocations of the service. A station either participates in a service instance or it does not.

To ensure correct operation of client protocols, secure service indications are not filtered or modified by a SecY except as specified in Clause 8 and Clause 9. Each protocol entity that is a client of the secure MAC Service should implement suitable policies (7.3.1) to support overall network security.

NOTE 1—For example, correct operation of Spanning Tree Protocol depends on the delivery of BPDUs to the Spanning Tree Protocol Entity of a given bridge from all the other bridges attached to the LAN that transmit frames that can be relayed by the given bridge. If a SecY were to require a higher level of authorization to pass received BPDUs through the Controlled Port, data loops in the network could result. However, the STP Entity can adopt a policy of discarding frames rather than permit another system that is not authorized as a bridge to be the Designated Bridge for the CA.

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 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

NOTE 2—If one of the members of the CA is a bridge (strictly speaking the Bridge Port is the CA member), the other members should adopt policies that reflect their confidence in the policies applied by the bridge to forward frames. In this case the trust is partly transitive—the question to be answered by each member of the CA is the degree of trust to place in the bridge's trust of systems that originate frames that the bridge will forward.

7.3.1 Client policies

Client policies, which are not specified in this standard, can include but are not limited to

a) Limiting the set of protocol procedures that can be invoked by the peer
b) Segregating communications between different sets of peer users of the MAC Service
c) Filtering, i.e., discarding, received frames

Clients of the secure MAC Service can also record any exceptional policy actions taken, so as to initiate further administrative action, outside the scope of this standard, with the entities responsible for the operation of the authenticated peer systems.

NOTE—A VLAN-aware Bridge that assigns frames that have been received from a specific Bridge Port (the bridge's point of attachment to a service instance) to a VLAN on the basis of the authorization associated with the Port provides an example of policy of segregating communications, as described in item b) above.

7.3.2 Use of the secure MAC Service by bridges

Each Bridge Port uses the service provided by an individual LAN (see Clause 11), which is not dependent for its connectivity on the operation of other bridges. This ensures that the configuration protocols used by bridges, including the spanning tree protocol, operate over a physical topology (comprising a bipartite graph of bridges and individual LANs connected by Bridge Ports) that is not itself dependent on the active topology, or subsets of the active topology, calculated by those same configuration protocols.

NOTE 1—The apparent exception to this configuration restriction, which does not permit the creation of security associations to create "secure tunnels" through selected bridges in a Bridged Local Area Network, is the use of a Provider Bridged Network as specified in IEEE Std 802.1Q. However, a Provider Bridged Network appears to Customer Bridges as a single LAN providing full connectivity independent of the operation of Customer Bridge protocols.

Copyright © 2018 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 08802-1AE-2020