

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

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

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.

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.

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.

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.

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	Marc Holness	Karen Randall
Shenghua Bao	Lu Huang	Maximilian Riegel
Jens Bierschenk	Tony Jeffree	Dan Romascanu
Steinar Bjornstad	Michael Johas Teener	Jessy V. Rouyer
Christian Boiger	Hal Keen	Eero Ryytty
Paul Bottorff	Stephan Kehrer	Soheil Samii
David Chen	Philippe Klein	Behcet Sarikaya
Feng Chen	Jouni Korhonen	Frank Schewe
Weiyang Cheng	Yizhou Li	Johannes Specht
Rodney Cummings	Christophe Mangin	Wilfried Steiner
János Farkas	Tom McBeath	Patricia Thaler
Norman Finn	James McIntosh	Paul Unbehagen
Geoffrey Garner	Tero Mustala	Hao Wang
Eric W. Gray	Hiroki Nakano	Karl Weber
Craig Gunther	Bob Noseworthy	Brian Weis
Marina Gutierrez	Donald R. Pannell	Jordon Woods
Stephen Haddock	Walter Pieniac	Nader Zein
Mark Hantel	Michael Potts	Helge Zinner
Patrick Heffernan		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	Yasuhiro Hyakutake	Clinton Powell
Richard Alfvén	Noriyuki Ikeuchi	Adee Ran
Amelia Andersdotter	Atsushi Ito	Karen Randall
Butch Anton	Raj Jain	R. K. Rannow
Harry Bims	Sangkwon Jeong	Alon Regev
Demetrio Bucaneg	Piotr Karocki	Maximilian Riegel
Stephen Bush	Stuart Kerry	Robert Robinson
William Byrd	Yongbum Kim	Benjamin Rolfe
Radhakrishna Canchi	Hyeong Ho Lee	Jessy V. Rouyer
Steven Carlson	Suzanne Leicht	Richard Roy
Keith Chow	Jon Lewis	Naotaka Sato
Charles Cook	Elvis Maculuba	Mick Seaman
Richard Doyle	Ignacio Marin Garcia	Thomas Starai
János Farkas	Brett McClellan	Walter Struppler
Norman Finn	Richard Mellitz	Jasja Tjink
Michael Fischer	John Messenger	Mark-Rene Uchida
Yukihiro Fujimoto	Michael Montemurro	Dmitri Varsanofiev
Randall Groves	Rick Murphy	George Vlantis
Qiang Guo	Nick S. A. Nikjoo	Lisa Ward
Stephen Haddock	Satoshi Obara	Stephen Webb
Marco Hernandez	Robert O'hara	Karl Weber
Werner Hoelzl	Bansi Patel	Chun Yu Charles Wong
Russell Housley		Oren Yuen

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

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.

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

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

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

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

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

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

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-XPB-128 Key, Secure Data, and ICV (example).....	216
Table C-42	GCM-AES-XPB-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-XPB-128 Key, Secure Data, and ICV (example).....	221
Table C-48	GCM-AES-XPB-256 Key, Secure Data, and ICV (example).....	222
Table F-1	Interoperability scenarios and PAE Addresses	234

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.

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.