

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:  
**iTeh STANDARD PREVIEW**

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

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

<https://standards.iteh.ai/catalog/standards/sist/0075012e-4e41-493e-be9a-60845cad8e13/iso-iec-ieee-8802-1ae-2020>



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



© IEEE 2018

## **iTeh STANDARD PREVIEW (standards.iteh.ai)**

[ISO/IEC/IEEE 8802-1AE:2020](#)

<https://standards.iteh.ai/catalog/standards/sist/0075012e-4e41-493e-bc9a-60845cad8e13/iso-iec-ieee-8802-1ae-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](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)  
Published in Switzerland

Institute of Electrical and Electronics Engineers, Inc  
3 Park Avenue, New York  
NY 10016-5997, USA  
  
Email: [stds.ipr@ieee.org](mailto:stds.ipr@ieee.org)  
Website: [www.ieee.org](http://www.ieee.org)

## 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](http://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.

### iTeh STANDARD PREVIEW

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](http://www.iso.org/patents)) or the IEC list of patent declarations received (<http://patents.iec.ch>).41-493e-be9a-  
<https://standards.itehpreview.org/iso-iec-ieee-8802-1ae-2020>

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](http://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](http://www.iso.org/members.html).

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC/IEEE 8802-1AE:2020](#)

<https://standards.iteh.ai/catalog/standards/sist/0075012e-4e41-493e-bc9a-60845cad8e13/iso-iec-ieee-8802-1ae-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**

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

Sponsor

**LAN/MAN Standards Committee**

of the

**IEEE Computer Society**

[ISO/IEC/IEEE 8802-1AE:2020](#)

<https://standards.iteh.ai/catalog/standards/sist/0075012e-4e41-493e-bc9a-60845cad8e13/iso-iec-ieee-8802-1ae-2020>

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<sup>®</sup> 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<sup>™</sup>, IEEE 802.1AEbn<sup>™</sup>, IEEE 802.1AEbw<sup>™</sup>, IEEE 802.1AEcg<sup>™</sup>, 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

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC/IEEE 8802-1AE:2020](#)

<https://standards.iteh.ai/catalog/standards/sist/0075012e-4e41-493e-bc9a-60845cad8e13/iso-iec-ieee-8802-1ae-2020>

---

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.

**iTeh STANDARD PREVIEW**  
 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.”  
<https://standards.iteh.ai/catalog/standards/sist/0075012e-4e41-493e-be9a-60845cad8e13/iso-iec-ieee-8802-1ae-2020>

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

## **iTEH STANDARD PREVIEW (standards.iteh.ai)**

### **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

### iTeh STANDARD PREVIEW

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**

Seo Young Back	Marc Holness	Karen Randall
Shenghua Bao	Lu Huang	Maximilian Riegel
Jens Bierschenk	Tony Jeffree	Dan Romascanu
Steinar Bjornstad	Michael Jonas 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 Piencikak	Nader Zein
Mark Hantel	Michael Potts	Helge Zinner
Patrick Heffernan		Juan Carlos Zuniga

## iTeh STANDARD PREVIEW (standards.iteh.ai)

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

[ISO/IEC/IEEE 8802-1AE:2020](#)

Thomas Alexander	Yasuhiro Hyakutake	Clinton Powell
Richard Alfvín	60845cad8e802-1ae-2020	Adee Ran
Amelia Andersdotter	Noriyuki Ikeuchi	Karen Randall
Butch Anton	Atsushi Ito	R. K. Rannow
Harry Bims	Raj Jain	Alon Regev
Demetrio Bucaneg	Sangkwon Jeong	Maximilian Riegel
Stephen Bush	Piotr Karocki	Robert Robinson
William Byrd	Stuart Kerr	Benjamin Rolfe
Radhakrishna Canchi	Yongbum Kim	Jessy V. Rouyer
Steven Carlson	Hyeong Ho Lee	Richard Roy
Keith Chow	Suzanne Leicht	Naotaka Sato
Charles Cook	Jon Lewis	Mick Seaman
Richard Doyle	Elvis Maculuba	Thomas Starai
János Farkas	Ignacio Marin Garcia	Walter Struppler
Norman Finn	Brett McClellan	Jasja Tijink
Michael Fischer	Richard Mellitz	Mark-Rene Uchida
Yukihiro Fujimoto	John Messenger	Dmitri Varsanofiev
Randall Groves	Michael Montemurro	George Vlantis
Qiang Guo	Rick Murphy	Lisa Ward
Stephen Haddock	Nick S. A. Nikjoo	Stephen Webb
Marco Hernandez	Satoshi Obara	Karl Weber
Werner Hoelzl	Robert O'hara	Chun Yu Charles Wong
Russell Housley	Bansi Patel	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

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC/IEEE 8802-1AE:2020](#)

<https://standards.iteh.ai/catalog/standards/sist/0075012e-4e41-493e-bc9a-60845cad8e13/iso-iec-ieee-8802-1ae-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.

## 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