



**IEEE Standard for
Local and metropolitan area networks**

Media Access Control (MAC) Security

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

802.1AETM

IEEE
3 Park Avenue
New York, NY 10016-5997, USA

18 August 2006

IEEE Std 802.1AETM-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 8 June 2006

IEEE-SA Standards Board

Abstract: This standard specifies 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. MAC security (MACsec) provides connectionless user data confidentiality, frame data integrity, and data origin authenticity.

Keywords: authorized port, data origin authenticity, integrity/confidentiality, LANs, local area networks, MAC Bridges, MAC security and tack, MAC Service, MANs, metropolitan area networks, MSAP, port-based network access control, secure association, security, service access point, transparent bridging

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

Copyright © 2006 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 18 August 2006. Printed in the United States of America.

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

Print: ISBN 0-7381-4990-X SH95549
PDF: ISBN 0-7381-4991-8 SS95549

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.

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.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied “**AS IS.**”

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. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, 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 publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received 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 interpretation requests except in those cases where the matter has previously received formal consideration. 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, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

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

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, 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.

Introduction

This introduction is not part of IEEE Std 802.1AE-2006, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security.

This is the first edition of this standard.

Relationship between IEEE Std 802.1AE and other IEEE 802 standards

Another IEEE standard, IEEE Std 802.1X[™]-2004, specifies Port-based Network Access Control, and provides a means of authenticating and authorizing devices attached to a LAN. Use of this standard in conjunction with architecture and protocols of IEEE Std 802.1X-2004 extends the applicability of the latter to publicly accessible LAN/MAN media for which security has not already been defined. A proposed amendment, IEEE P802.1af[™], to IEEE Std 802.1X-2004 is being developed to specify the additional protocols and interfaces necessary.

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

A previous security standard, IEEE Std 802.10[™], IEEE Standard for Interoperable LAN/MAN Security, has been withdrawn.

Notice to users

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/interp/index.html>.

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 with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents or patent applications for which a license may be required to implement an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Participants

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

Tony Jeffree, Chair

Mick Seaman, Interworking and Security Task Group Chair

Allyn Romanow, Editor

Frank Chao, MIB Editor

Brandon Barry	Ken Grewal	Allyn Romanow
Les Bell	Steve Haddock	Dan Romascanu
Mike Borza	Ran Ish-Shalom	Jessy V. Rouyer
Paul Bottorff	Tony Jeffree	Ali Sajassi
Jim Burns	Hal Keen	Dolors Sala
Dirceu Cavendish	Yongbum Kim	Sam Sambasivan
Paul Congdon	Loren Larsen	John Sauer
Sharam Davari	Yannick Le Goff	Mick Seaman
Arjan de Heer	David Melman	Koichiro Seto
Craig Easley	John Messenger	Muneyoshi Suzuki
Anush Elangovan	Dinesh Mohan	Geoff Thompson
Hesham Elbakoury	Bob Moskowitz	John Viega
David Elie-Dit-Cosaque	Don O'Connor	Dennis Volpano
Norm Finn	Glenn Parsons	Karl Weber
David Frattura	Ken Patton	Ludwig Winkel
Anoop Ghanwani	Karen T. Randall	Michael D. Wright

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

Eng Ahmed Abdelhalim	C. G. Guy	Mike Moreton
Butch Anton	Ronald D. Hochnadel	M. Narayanan
Pierrejean Arcos	Andreas J. Holtmann	Michael S. Newman
Chris B. Bagge	Dennis Horwitz	Paul Nikolich
John B. Barnett	Russell D. Housley	Robert O'hara
Mark A. Beadles	David Hunter	Glenn W. Parsons
Michael A. Beck	C. R. Huntley	Vikram Punj
Rahul B. Bhushan	Atsushi Ito	Jose P. Puthenkulam
Gennaro Boggia	Raj Jain	Karen T. Randall
James T. Carlo	David V. James	John J. Roese
Juan C. Carreon	Tony Jeffree	Allyn Romanow
Jon S. Chambers	Peter G. Johansson	Jessy V. Rouyer
Danila Chernetsov	David Johnston	Michael Scholles
Keith Chow	Joe Natharaj Juisai	Stephen C. Schwarm
John L. Cole	Piotr Karocki	Mick Seaman
Paul Congdon	Lior Khermosh	William M. Shvodian
Tommy P. Cooper	Byoung-jo Kim	Thomas M. Siep
Russell S. Dietz	Yongbum Kim	Manikantan Srinivasan
Thomas J. Dineen	Mark J. Knight	Thomas E. Starai
Sean Dougherty	Hermann Koch	Guenter Steindl
Alistair P. Duffly	Thomas M. Kurihara	Michael L. Takefman
Sourav K. Dutta	David J. Law	Joseph J. Tardo
David Elie-Dit-Cosaque	Shawn M. Leard	Michael D. Johas Teener
Michael A. Fischer	Kang Lee	Thomas A. Tullia
Yukihiko Fujimoto	Li Li	Mark-rene Uchida
James P. Gilb	William Lumpkins	Timothy P. Walker
Nikhil Goel	G. L. Luri	Derek T. Woo
Sergiu R. Goma	Jonathon C. Mclendon	Steven A. Wright
Patrick S. Gonia	Francisco J. Melendez	TakahitoYoshizawa
Karanvir Grewal	George J. Miao	Oren Yuen
Randall C. Groves	Gary L. Michel	

When the IEEE-SA Standards Board approved this standard on 8 June 2006, it had the following membership:

Steve M. Mills, *Chair*
Richard H. Hulett, *Vice Chair*
Don Wright, *Past Chair*
Judith Gorman, *Secretary*

Mark D. Bowman
Dennis B. Brophy
William R. Goldbach
Arnold M. Greenspan
Robert M. Grow
Joanna N. Guenin
Julian Forster*
Mark S. Halpin
Kenneth S. Hanus

William B. Hopf
Joseph L. Koepfinger*
David J. Law
Daleep C. Mohla
T. W. Olsen
Glenn Parsons
Ronald C. Petersen
Tom A. Prevost

Greg Ratta
Robby Robson
Anne-Marie Sahazizian
Virginia C. Sulzberger
Malcolm V. Thaden
Richard L. Townsend
Walter Weigel
Howard L. Wolfman

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*
Richard DeBlasio, *DOE Representative*
Alan H. Cookson, *NIST Representative*

Don Messina
IEEE Standards Program Manager, Document Development

Michael Kipness
IEEE Standards Program Manager, Technical Program Development

Contents

1. Overview	1
1.1 Introduction	1
1.2 Scope	2
2. Normative references	3
3. Definitions	5
4. Abbreviations and acronyms	8
5. Conformance	10
5.1 Requirements terminology	10
5.2 Protocol Implementation Conformance Statement (PICS)	10
5.3 Required capabilities	10
5.4 Optional capabilities	11
6. Secure provision of the MAC Service	13
6.1 MAC Service primitives and parameters	13
6.2 MAC Service connectivity	15
6.3 Point-to-multipoint LANs	16
6.4 MAC status parameters	16
6.5 MAC point-to-point parameters	16
6.6 Security threats	17
6.7 MACsec connectivity	18
6.8 MACsec guarantees	19
6.9 Security services	19
6.10 Quality of service maintenance	20
7. Principles of secure network operation	22
7.1 Support of the secure MAC Service by an individual LAN	22
7.2 Multiple instances of the secure MAC Service on a single LAN	27
7.3 Use of the secure MAC Service	28
8. MAC Security Protocol (MACsec)	31
8.1 Protocol design requirements	32
8.2 Protocol support requirements	34
8.3 MACsec operation	36
9. Encoding of MACsec protocol data units	38
9.1 Structure, representation, and encoding	38
9.2 Major components	38
9.3 Security TAG	39
9.4 MACsec EtherType	39
9.5 TAG Control Information (TCI)	40
9.6 Association Number (AN)	41
9.7 Short Length (SL)	41
9.8 Packet Number (PN)	41
9.9 Secure Channel Identifier (SCI)	41
9.10 Secure Data	42

9.11	Integrity Check Value (ICV)	42
9.12	PDU validation	43
10.	Principles of MAC Security Entity (SecY) operation	44
10.1	SecY overview	44
10.2	SecY functions	46
10.3	Model of operation	47
10.4	SecY architecture	47
10.5	Secure frame generation	50
10.6	Secure frame verification	51
10.7	SecY management	53
10.8	Addressing	63
10.9	Priority	63
10.10	SecY performance requirements	63
11.	MAC Security in Systems	65
11.1	MAC Service interface stacks	65
11.2	MACsec in end stations	66
11.3	MACsec in MAC Bridges	66
11.4	MACsec in VLAN-aware Bridges	67
11.5	MACsec and Link Aggregation	68
11.6	Link Layer Discovery Protocol (LLDP)	69
11.7	MACsec in Provider Bridged Networks	70
11.8	MACsec and multi-access LANs	72
12.	MACsec and EPON	74
13.	Management protocol	76
13.1	Introduction	76
13.2	The Internet-Standard Management Framework	76
13.3	Relationship to other MIBs	76
13.4	Security considerations	78
13.5	Structure of the MIB	80
13.6	Definitions for MAC Security MIB	84
14.	Cipher Suites	121
14.1	Cipher Suite use	121
14.2	Cipher Suite capabilities	122
14.3	Cipher Suite specification	123
14.4	Cipher Suite conformance	123
14.5	Default Cipher Suite (GCM–AES–128)	124
Annex A	(normative) PICS Proforma	126
A.1	Introduction	126
A.2	Abbreviations and special symbols	126
A.3	Instructions for completing the PICS proforma	127
A.4	PICS proforma for IEEE Std 802.1AE	129
A.5	Major capabilities	130
A.6	Support and use of Service Access Points	131
A.7	MAC status and point-to-point parameters	132
A.8	Secure Frame Generation	133

A.9	Secure Frame Verification	134
A.10	MACsec PDU encoding and decoding	135
A.11	Key Agreement Entity LMI	135
A.12	Additional fully conformant Cipher Suite capabilities	139
A.13	Additional variant Cipher Suite capabilities	140
Annex B (informative) Bibliography		142

**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 P802.1af[™] [B2]¹ provides authentication and cryptographic key distribution.

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

¹The numbers in brackets correspond to those of the bibliography in Annex B.