802.1AE™

IEEE Standard for Local and metropolitan area networks

Media Access Control (MAC) Security

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

18 August 2006

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 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

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

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

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
Les Bell
Mike Borza
Paul Bottorff
Jim Burns
Dirceu Cavendish
Paul Congdon
Sharam Davari
Arjan de Heer
Craig Easley
Anush Elangovan
Hesham Elbakoury
David Elie-Dit-Cosaque
Norm Finn
David Frattura
Anoop Ghanwani
Ken Grewal
Steve Haddock
Ran Ish-Shalom
Tony Jeffree
Hal Keen
Yongbum Kim
Loren Larsen
Yannick Le Goff
David Melman
John Messenger
Dinesh Mohan
Bob Moskowitz
Don O'Connor
Glenn Parsons
Ken Patton
Karen T. Randall
Allyn Romanow
Dan Romascanu
Jessy V. Rouyer
Ali Sajassi
Dolors Sala
Sam Sambasivan
John Sauer
Mick Seaman
Koichiro Seto
Muneyoshi Suzuki
Geoff Thompson
John Viega
Dennis Volpano
Karl Weber
Ludwig Winkel
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
Butch Anton
Pierrejean Arcos
Chris B. Bagge
John B. Barnett
Mark A. Beadles
Michael A. Beck
Rahul B. Bhushan
Gennaro Boggia
James T. Carlo
Juan C. Carreon
Jon S. Chambers
Danila Chernetsov
Keith Chow
John L. Cole
Paul Congdon
Tommy P. Cooper
Russell S. Dietz
Thomas J. Dineen
Sean Dougherty
Alistair P. Duffy
Sourav K. Dutta
David Elie-Dit-Cosaque
Michael A. Fischer
Yukihiro Fujimoto
James P. Gilb
Nikhil Goel
Sergiu R. Goma
Patrick S. Gonia
Karanvir Grewal
Randall C. Groves
C. G. Guy
Ronald D. Hochnadel
Andreas J. Holtmann
Dennis Horwitz
Russell D. Housley
David Hunter
C. R. Huntley
Atsushi Ito
Raj Jain
David V. James
Tony Jeffree
Peter G. Johansson
David Johnston
Joe Natharoj Juisai
Piotr Karocki
Lior Khermosh
Byoung-jo Kim
Yongbum Kim
Mark J. Knight
Hermann Koch
Thomas M. Kurihara
David J. Law
Shawn M. Leard
Kang Lee
Li Li
William Lumpkins
G. L. Luri
Jonathon C. Mclendon
Francisco J. Melendez
George J. Miao
Gary L. Michel
Mike Moreton
M. Narayanan
Michael S. Newman
Paul Nikolich
Robert O'hara
Glenn W. Parsons
Vikram Punj
Jose P. Puthenkulam
Karen T. Randall
John J. Roese
Allyn Romanow
Jessy V. Rouyer
Michael Scholles
Stephen C. Schwarm
Mick Seaman
William M. Shvodian
Thomas M. Siep
Manikantan Srinivasan
Thomas E. Starai
Guenter Steindl
Michael L. Takefman
Joseph J. Tardo
Michael D. Johas Teener
Thomas A. Tullia
Mark-rene Uchida
Timothy P. Walker
Derek T. Woo
Steven A. Wright
TakahitoYoshizawa
Oren Yuen

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

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

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