INTERNATIONAL STANDARD

ISO/ IEC/IEEE 8802-1X

Second edition
2021-12

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

Part 1X: Port-based network access control

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

Partie 1X: Contrôle d'accès au réseau basé sur le port

Reference number
ISO/IEC/IEEE 8802-1X:2021(E)

© IEEE 2020



COPYRIGHT PROTECTED DOCUMENT

© IEEE 2020

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 IEEE at the address below.

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

Email: stds.ipr@ieee.org
Website: www.ieee.org

Published in Switzerland

© IEEE 2020 – All rights reserved

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/IEC documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

ISO/IEC/IEEE 8802-1X was prepared by the LAN/MAN of the IEEE Computer Society (as [IEEE Std 802.1X™-2020) 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*.

A list of all parts in the ISO/IEC/IEEE 8802 series can be found on the ISO and IEC websites.

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 and www.iec.ch/national-committees.

© IEEE 2020 – All rights reserved

IEEE Std 802.1X™-2020
(Revision of IEEE Std 802.1X™-2010
Incorporating IEEE Std 802.1Xbx™-2014
and IEEE Std 802.1Xck™-2018)

IEEE Standard for Local and Metropolitan Area Networks—

Port-Based Network Access Control

Developed by the

**LAN/MAN Standards Committee
of the
IEEE Computer Society**

Approved 30 January 2020

IEEE SA Standards Board

Copyright © 2020 IEEE. All rights reserved.

Abstract: Port-based network access control allows a network administrator to restrict the use of IEEE 802® LAN service access points (ports) to secure communication between authenticated and authorized devices. This standard specifies a common architecture, functional elements, and protocols that support mutual authentication between the clients of ports attached to the same LAN and that secure communication between the ports, including the media access method independent protocols that are used to discover and establish the security associations used by IEEE 802.1AE™ MAC Security.

Keywords: access control, authentication, authorization, controlled port, EAP, EAPOL, IEEE 802.1X, key agreement, LANs, local area networks, MACsec, MACsec Key Agreeement, MAC security, MAC Service, MANs, metropolitan area networks, MKA, port-based network access control, secure association, security, service access point, uncontrolled port

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

Copyright © 2020 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 28 February 2020. 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 978-1-5044-6440-6 STD24052
Print: ISBN 978-1-5044-6441-3 STDPD24052

IEEE prohibits discrimination, harassment, and bullying. For more information, visit
http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Copyright © 2020 IEEE. All rights reserved.

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 the IEEE or viewed at https://standards.ieee.org/ipr/disclaimers.html.

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association ("IEEE SA") Standards Board. IEEE ("the Institute") develops its standards through a consensus development process, approved by the American National Standards Institute ("ANSI"), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Copyright © 2020 IEEE. All rights reserved.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

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

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Copyright © 2020 IEEE. All rights reserved.

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/browse/standards/collection/ieee or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website at http://standards.ieee.org.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website at the following URL: http://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at http://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Copyright © 2020 IEEE. All rights reserved.

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*

Astrit Ademaj
Ralf Assmann
Jens Bierschenk
Christian Boiger
Paul Bottorff
Radhakrishna Canchi
Feng Chen
Weiying Cheng
Paul Congdon
Rodney Cummings
Josef Dorr
Hesham Elbakoury
Thomas Enzinger
János Farkas
Donald Fedyk
Norman Finn
Geoffrey Garner
Craig Gunther
Marina Gutierrez
Stephen Haddock
Mark Hantel
Marc Holness
Satoko Itaya
Yoshihiro Ito
Michael Karl
Stephan Kehrer
Randy Kelsey
Hajime Koto
James Lawlis
Christophe Mangin
Scott Mansfield
Kenichi Maruhashi
David McCall
Larry McMillan
Tero Mustala
Roy Myers
Hiroki Nakano
Bob Noseworthy
Tomoki Ohsawa
Hiroshi Ohue
Donald R. Pannell
Michael Potts
Dieter Proell
Wei Qiu
Karen Randall
Maximilian Riegel
Jessy V. Rouyer
Atsushi Sato
Frank Schewe
Maik Seewald
Johannes Specht
Marius Stanica
Guenter Steindl
Karim Traore
Hao Wang
Xinyuan Wang
Tongtong Wang
Ludwig Winkel
Karl Weber
Brian Weis
Jordon Woods
Nader Zein
Takahiro Yamaura
Helge Zinner
William Zhao
Harald Zweck

Copyright © 2020 IEEE. All rights reserved.

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

Thomas Alexander
Johann Amsenga
Butch Anton
Harry Bims
Kenneth Bow
Rich Boyer
Nancy Bravin
Vern Brethour
Matthew Brown
Demetrio Bucaneg, Jr.
William Byrd
Radhakrishna Canchi
Paul Cardinal
Juan Carreon
Janos Farkas
Avraham Freedman
Devon Gayle
Tim Godfrey
Zhigang Gong
Randall Groves
Marek Hajduczenia
Marco Hernandez
Werner Hoelzl
Yasuhiro Hyakutake
Raj Jain
SangKwon Jeong
Pranav Jha
Lokesh Kabra
Srinivas Kandala
Piotr Karocki
Stuart Kerry
Evgeny Khorov
Yongbum Kim
Hyeong Ho Lee
Suzanne Leicht
James Lepp
Michael Lynch
John Mackay
Jouni Malinen
Roger Marks
Arthur Marris
Stephen McCann
Brett Mcclellan
Richard Mellitz
Michael Montemurro
Nick S.A. Nikjoo
Satoshi Obara
Robert O'Hara
Carlos Pardo
Bansi Patel
Arumugam Paventhan
David Piehler
Walter Pienciak
Clinton Powell
Karen Randall
R. K. Rannow
Maximilian Riegel
Robert Robinson
Jessy Rouyer
John Sargent
Frank Schewe
Michael Seaman
Thomas Starai
Walter Struppler
Michael Thompson
Mark-Rene Uchida
Alexander Umnov
Dmitri Varsanofiev
George Vlantis
Lisa Ward
Stephen Webb
Brian Weis
Scott Willy
Chun Yu Charles Wong
Oren Yuen

When the IEEE SA Standards Board approved this standard on 30 January 2020, it had the following membership:

Gary Hoffman, *Chair*
Vacant, *Vice-Chair*
Jean-Philippe Faure, *Past Chair*
Konstantinos Karachalios, *Secretary*

Ted Burse
Doug Edwards
Travis Griffith
Grace Gu
Guido Hiertz
John Kulick
David J. Law
Joseph L.Koepfinger*
Howard Li
Dong Liu
Kevin Lu
Paul Nikolich
Damir Novosel
Jon Rosdahl
Dorothy Stanley
Mehmet Ulema
Lei Wang
Sha Wei
Philip Winston
Daidi Zhong

*Member Emeritus

Copyright © 2020 IEEE. All rights reserved.

Introduction

This introduction is not part of IEEE Std 802.1X™-2020, IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control.

This edition of IEEE Std 802.1X™ incorporates IEEE Std 802.1X-2010 and its amendments, IEEE Std 802.1Xbx-2014 and IEEE Std 802.1Xck-2018.

The first edition of IEEE Std 802.1X™ was published in 2001. The second edition, IEEE Std 802.1X-2004, clarified mutual authentication and the interface between the IEEE 802.1X state machines and the Extensible Authentication Protocol (EAP) and by IEEE Std 802.11™ in support of IEEE Std 802.1X.

The third edition, IEEE Std 802.1X-2010, added authenticated key agreement in support of IEEE Std 802.1AE™ MAC Security (MACsec) and clarified and generalized the relationship between the common architecture specified for port-based network access control and the functional elements and protocols that support that architecture as specified in IEEE Std 802.1X, other IEEE 802® standards, and IETF RFCs. Further changes updated the standard to reflect best current practice, insisting, for example, on mutual authentication methods and using such methods in examples. A greater emphasis was placed on the security of systems accessing the network, as well as on the security of the network accessed, with a more comprehensive treatment of segregating and limiting connectivity to unauthenticated systems. Applications of port-based network access that use MACsec and/or MACsec Key Agreement protocol (MKA) were described.

IEEE Std 802.1X-2010 included a number of improvements to the specification of the port access control protocol (PACP) state machines and their relationship to EAP methods and state machines. Systems conformant to IEEE Std 802.1X-2020 or IEEE Std 802.1X-2010 should interoperate, without prior configuration, with implementations conforming to IEEE Std 802.1X-2004 and IEEE Std 802.1X-2001. However, it is anticipated that claims of conformance with respect to some existing implementations, not needing to support IEEE Std 802.1AE and already conforming to best current practice as of 2010, will continue to refer to IEEE Std 802.1X-2004.

The first amendment to IEEE Std 802.1X-2010, IEEE Std 802.1Xbx-2014, extended MKA to further support and use the extended packet numbering Cipher Suites specified by the IEEE Std 802.1AEbw™-2013. Secure connectivity association (CA) members can temporarily suspend MKA operation without causing protocol timeouts that would disrupt secure data transfer, thus allowing in-service control plane software upgrades.

The second amendment to IEEE Std 802.1X-2010, IEEE Std 802.1Xck-2018, specified a YANG data model for configuration and status reporting, using the information model previously specified in this standard.

Copyright © 2020 IEEE. All rights reserved.

Contents

1. Overview ... 16

1.1 Scope ... 16
1.2 Purpose ... 16
1.3 Introduction ... 16
1.4 Provisions of this standard ... 17

2. Normative references ... 19

3. Definitions ... 21

4. Acronyms and abbreviations ... 26

5. Conformance ... 28

5.1 Requirements terminology ... 28
5.2 Protocol Implementation Conformance Statement ... 28
5.3 Conformant systems and system components ... 29
5.4 PAE requirements ... 29
5.5 PAE options ... 30
5.6 Supplicant requirements ... 30
5.7 Supplicant options ... 30
5.8 Authenticator requirements ... 30
5.9 Authenticator options ... 30
5.10 MKA requirements ... 31
5.11 MKA options ... 31
5.12 Virtual port requirements ... 32
5.13 Virtual port options ... 33
5.14 Announcement transmission requirements ... 33
5.15 Announcement transmission options ... 33
5.16 Announcement reception requirements ... 33
5.17 Announcement reception options ... 33
5.18 Requirements for SNMP access to the PAE MIB ... 34
5.19 Options for SNMP access to the PAE MIB ... 34
5.20 PAC requirements ... 34
5.21 System recommendations ... 34
5.22 Prohibitions ... 34
5.23 Requirement for YANG data model of a PAE ... 34
5.24 Options for YANG data model of a PAE ... 34

6. Principles of port-based network access control operation ... 36

6.1 Port-based network access control architecture ... 37
6.2 Key hierarchy ... 38
6.3 Port Access Entity (PAE) ... 43
6.4 Port Access Controller (PAC) ... 46
6.5 Link aggregation ... 48
6.6 Use of this standard by IEEE Std 802.11 ... 49

7. Port-based network access control applications ... 50

7.1 Host access with physically secure LANs ... 50
7.2 Infrastructure support with physically secure LANs ... 53
7.3 Host access with MACsec and point-to-point LANs ... 55

Copyright © 2020 IEEE. All rights reserved.

7.4 Use with MACsec to support infrastructure LANs 56
7.5 Host access with MACsec and a multi-access LAN 58
7.6 Group host access with MACsec 61
7.7 Use with MACsec to support virtual shared media infrastructure LANs 62

8. Authentication using EAP 65

8.1 PACP Overview 66
8.2 Example EAP exchanges 67
8.3 PAE higher layer interface 68
8.4 PAE Client interface 69
8.5 EAPOL transmit and receive 71
8.6 Supplicant and Authenticator PAE timers 71
8.7 Supplicant PACP state machine, variables, and procedures 72
8.8 Supplicant PAE counters 72
8.9 Authenticator PACP state machine, variables, and procedures 73
8.10 Authenticator PAE counters 74
8.11 EAP methods 75

9. MACsec Key Agreement protocol (MKA) 77

9.1 Protocol design requirements 78
9.2 Protocol support requirements 79
9.3 MKA key hierarchy 79
9.4 MKA transport 82
9.5 Key server election 85
9.6 Use of MACsec 86
9.7 Cipher suite selection 87
9.8 SAK generation, distribution, and selection 88
9.9 SA assignment 90
9.10 SAK installation and use 90
9.11 Connectivity change detection 92
9.12 CA formation and group CAK distribution 92
9.13 Secure announcements 93
9.14 MKA participant creation and deletion 93
9.15 MKA participant timer values 94
9.16 MKA management 95
9.17 MKA SAK distribution examples 97
9.18 In-service upgrades 98
9.19 In-service upgrade examples 102

10. Network announcements 105

10.1 Announcement information 105
10.2 Making and requesting announcements 108
10.3 Receiving announcements 110
10.4 Managing announcements 110

11. EAPOL PDUs 112

11.1 EAPOL PDU transmission, addressing, and protocol identification 112
11.2 Representation and encoding of octets 115
11.3 Common EAPOL PDU structure 115
11.4 Validation of received EAPOL PDUs 116
11.5 EAPOL protocol version handling 117
11.6 EAPOL-Start 118

Copyright © 2020 IEEE. All rights reserved.

11.7 EAPOL-Logoff ... 119
11.8 EAPOL-EAP ... 119
11.9 EAPOL-Key ... 119
11.10 EAPOL-Encapsulated-ASF-Alert ... 120
11.11 EAPOL-MKA ... 120
11.12 EAPOL-Announcement ... 130
11.13 EAPOL-Announcement-Req ... 136

12. PAE operation ... 137

12.1 Model of operation ... 137
12.2 KaY interfaces ... 139
12.3 CP state machine interfaces ... 141
12.4 CP state machine ... 142
12.5 Logon Process ... 142
12.6 CAK cache ... 146
12.7 Virtual port creation and deletion ... 147
12.8 EAPOL Transmit and Receive Process ... 148
12.9 PAE management ... 150

13. PAE MIB ... 153

13.1 The Internet Standard Management Framework ... 153
13.2 Structure of the MIB ... 153
13.3 Relationship to other MIBs ... 153
13.4 Security considerations ... 162
13.5 Definitions for PAE MIB ... 162

14. YANG Data Model ... 212

14.1 PAE management using YANG ... 212
14.2 Security considerations ... 213
14.3 802.1X YANG model structure ... 214
14.4 Relationship to other YANG data models ... 215
14.5 Definition of the IEEE 802.1X YANG data model ... 229
14.6 YANG data model use in network access control applications ... 261

Annex A (normative) PICS proforma ... 266

A.1 Introduction ... 266
A.2 Abbreviations and special symbols ... 266
A.3 Instructions for completing the PICS proforma ... 267
A.4 PICS proforma for IEEE 802.1X ... 269
A.5 Major capabilities and options ... 270
A.6 PAE requirements and options ... 270
A.7 Supplicant requirements and options ... 271
A.8 Authenticator requirements and options ... 271
A.9 MKA requirements and options ... 271
A.12 Management and remote management ... 273
A.13 Virtual ports ... 273
A.10 Announcement transmission requirements ... 273
A.11 Announcement reception requirements ... 273
A.14 PAC ... 274
A.15 YANG requirements and options ... 274

Copyright © 2020 IEEE. All rights reserved.

Annex B (informative) Bibliography 275

Annex C (normative) State diagram notation 278

Annex D (informative) IEEE 802.1X EAP and RADIUS usage guidelines 280

D.1 EAP Session-Id 280
D.2 RADIUS Attributes for IEEE 802 Networks 280

Annex E (informative) Support for ‘Wake-on-LAN’ protocols 281

Annex F (informative) Unsecured multi-access LANs 282

Annex G (informative) Test vectors 284

G.1 KDF 284
G.2 CAK Key Derivation 285
G.3 CKN Derivation 285
G.4 KEK Derivation 286
G.5 ICK Derivation 286
G.6 SAK Derivation 287

Copyright © 2020 IEEE. All rights reserved.

Figures

Figure 6-1 Port-based network access control processes ... 37
Figure 6-2 Port-based network access control with MACsec ... 38
Figure 6-3 MKA key hierarchy ... 39
Figure 6-4 Use of pairwise CAKs to distribute group SAKs ... 39
Figure 6-5 Network access control with MACsec and a multi-access LAN ... 46
Figure 6-6 -Port Access Controller ... 47
Figure 6-7 -PACs and Link Aggregation in an interface stack ... 49
Figure 6-8 SecYs and Link Aggregation in an interface stack ... 49
Figure 7-1 Network access control with a physically secure point-to-point LAN ... 50
Figure 7-2 Network access control with a physically secure point-to-point LAN ... 51
Figure 7-3 Network access controlled VLAN-aware Bridge Port with PAC ... 52
Figure 7-4 Selective relay to a physically secured unauthenticated port ... 53
Figure 7-5 Network infrastructure with a physically secure point-to-point LAN ... 54
Figure 7-6 Network access control with MACsec and a point-to-point LAN ... 55
Figure 7-7 Network access control with MACsec and a point-to-point LAN ... 56
Figure 7-8 Point-to-point LAN within a secured network ... 56
Figure 7-9 Shared media LAN within a secured network ... 57
Figure 7-10 Network access control within the network infrastructure ... 57
Figure 7-11 Network access control with MACsec and a multi-access LAN ... 58
Figure 7-12 Network access control with MACsec and a multi-access LAN ... 59
Figure 7-13 Secure and unsecured connectivity on a multi-access LAN ... 60
Figure 7-14 Group host access ... 61
Figure 7-15 Multipoint connectivity across a Provider Bridged Network ... 62
Figure 7-16 Internal organization of the MAC sublayer in a Provider Bridged Network ... 63
Figure 7-17 Secure PBN transit and access with priority selection ... 64
Figure 7-18 Secure PBN transit and with priority selection ... 64
Figure 8-1 PAEs, PACP, EAP Messages, and EAPOL PDUs ... 66
Figure 8-2 Authenticator-initiated EAP-TLS (success) ... 68
Figure 8-3 Supplicant-initiated EAP exchange ... 68
Figure 8-4 PAE state machines and interfaces ... 70
Figure 8-5 PAE Timer state machines ... 72
Figure 8-6 Supplicant PACP state machine ... 73
Figure 8-7 Authenticator PACP state machine ... 74
Figure 11-1 Common EAPOL PDU structure ... 115
Figure 11-2 EAPOL Start-PDU (Protocol Version ≤ 2) ... 118
Figure 11-3 EAPOL Start-PDU (Protocol Version ≥ 3) ... 118
Figure 11-4 EAPOL-EAP Packet Body with EAP packet format ... 119
Figure 11-5 EAPOL-Key Packet Body with Key Descriptor format ... 119
Figure 11-7 MKPDU—Parameter set encoding ... 121
Figure 11-6 EAPOL-MKA Packet Body with MKPDU format ... 121
Figure 11-8 Basic Parameter Set ... 125
Figure 11-9 Live Peer List and Potential Peer List parameter sets ... 125
Figure 11-11 Distributed SAK parameter set (GCM-AES-128) ... 126
Figure 11-10 MACsec SAK Use parameter set ... 126
Figure 11-12 Distributed SAK parameter set (other MACsec Cipher Suites) ... 127
Figure 11-13 Distributed CAK parameter set ... 127
Figure 11-14 KMD parameter set ... 127
Figure 11-15 Announcement parameter set ... 128
Figure 11-16 XPN parameter set ... 128
Figure 11-17 ICV Indicator ... 128
Figure 11-18 EAPOL-Announcement ... 130
Figure 11-19 EAPOL-Announcement TLV format ... 130

Copyright © 2020 IEEE. All rights reserved.

Figure 11-20 NID Set TLV format 132
Figure 11-21 Access Information TLV format 132
Figure 11-22 Access Information TLV format 133
Figure 11-23 Key Management Domain TLV format 134
Figure 11-24 Organizationally Specific TLV format 134
Figure 11-25 Organizationally Specific Set TLV format 134
Figure 11-26 EAPOL-Announcement-Req (Protocol Version = 3) 136
Figure 12-1 PAE state machines—overview and interfaces 138
Figure 12-2 CP state machine 143
Figure 12-3 PAE management information 152
Figure 13-1 Use of the ifStackTable 154
Figure 14-1 YANG model structure 214
Figure 14-2 YANG object hierarchy with IEEE Std 802.1X 214
Figure 14-3 IETF System Management YANG data model 216
Figure 14-4 IETF Interface Management YANG data model 218
Figure 14-5 Explicit Interface Model of Bridge Port 224
Figure 14-6 Augmented Interface Mode of Bridge Port 225
Figure 14-7 Bridge Port with LAG Interface stack model 225
Figure 14-8 Bridge Port YANG Interface stack model with MACsec 226
Figure 14-9 Augmented Interface Model of Bridge Port with MACsec 226
Figure 14-10 YANG Interface Model with MACsec and virtual ports 227
Figure 14-11 Explicit Interface Model of Bridge Port LAG with MACsec on members 227
Figure 14-12 Augmented Interface Model of Bridge Port LAG with MACsec on members 228
Figure 14-13 IEEE 802.1X YANG model for host (7.1) 261
Figure 14-14 IEEE 802.1X YANG model for network access point (7.1) 262
Figure 14-15 IEEE 802.1X YANG model for network access point (7.3) 263

Copyright © 2020 IEEE. All rights reserved.

Tables

Table 5-1 System recommendations 35
Table 9-1 MKA Algorithm Agility parameter values 81
Table 9-2 Key Server Priority values 85
Table 9-3 MKA Participant timer values 94
Table 10-1 Announcement performance parameters 109
Table 11-1 EAPOL group address assignments 113
Table 11-2 EAPOL Ethernet Type assignment 114
Table 11-3 EAPOL Packet Types 116
Table 11-4 EAPOL Packet Type Destination Addressing 117
Table 11-5 Descriptor Type value assignments 120
Table 11-6 MKA parameters—fixed width encoding 122
Table 11-7 MKPDU parameter sets 123
Table 11-8 EAPOL-Announcement TLVs 131
Table 11-9 Access Information 133
Table 13-1 Use of ifGeneralInformationGroup objects 154
Table 13-4 PAE managed object cross-reference table 155
Table 13-2 Use of ifCounterDiscontinuityGroup Object 155
Table 13-3 Use of ifStackGroup2 Objects 155
Table 13-5 PAC managed object cross-reference table 161
Table 14-1 PAE System cross-reference table 217
Table 14-2 PAE cross-reference table 219
Table C-1 State machine symbols 279

Copyright © 2020 IEEE. All rights reserved.

IEEE Standard for Local and Metropolitan Area Networks—

Port-Based Network Access Control

1. Overview

1.1 Scope

For the purpose of providing compatible authentication, authorization, and cryptographic key agreement mechanisms to support secure communication between devices connected by **IEEE 802**® Local Area Networks (LANs), this standard

a) Specifies a general method for provision of port-based network access control.

b) Specifies protocols that establish secure associations for IEEE Std 802.1AE™ MAC Security.

c) Facilitates the use of industry standard authentication and authorization protocols.

1.2 Purpose

IEEE 802 LANs are deployed in networks that convey or provide access to critical data, that support mission critical applications, or that charge for service. Protocols that configure, manage, and regulate access to these networks and network-based services and applications typically run over the networks themselves. Port-based network access control regulates access to the network, guarding against transmission and reception by unidentified or unauthorized parties, and consequent network disruption, theft of service, or data loss.

1.3 Introduction

The stations attached to an IEEE 802 LAN transmit and receive data frames using the service provided by the IEEE 802 LAN MAC at a service access point, often referred to as a port, within each end station or bridge. Port-based network access control specifies a common architecture comprising cooperative functional elements and protocols that

a) Use the service provided by the LAN MAC, at a common service access point, to support a Controlled Port that provides secure access-controlled communication and an Uncontrolled Port that supports protocols that initiate the secure communication or do not require protection.

b) Support mutual authentication between a Port Access Entity (PAE) associated with a Controlled Port, and a peer PAE associated with a peer port in a LAN attached station that desires to communicate through the Controlled Port.

c) Secure the communication between the Controlled Port and the authenticated peer port, excluding other devices attached to or eavesdropping on the LAN.

d) Provide the Controlled Port with attributes that specify access controls appropriate to the authorization accorded to the peer station or its user.

Copyright © 2020 IEEE. All rights reserved.

This standard specifies the use of EAP, the Extensible Authentication Protocol (IETF RFC 3748 [B14][1]), to support authentication using a centrally administered Authentication Server and defines EAP encapsulation over LANs (EAPOL, Clause 11) to convey the necessary exchanges between peer PAEs attached to a LAN.

Where communication over the LAN connecting a Controlled Port to its peer(s) is physically secure, no additional protocol is required to protect their communication. This mode of operation is supported by this standard. More commonly intrusion into the LAN communication is a principal security threat, and the result of mutual authentication is not simply Controlled Port authorization to transmit and receive data, but secure distribution of master keys and associated data to the communicating peers. Proof of possession of master keys subsequently serves as proof of mutual authentication in key agreement protocols. These protocols generate keys that are used to cryptographically protect data frames transmitted and received by the Controlled Port. IEEE Std 802.11™ Wireless LANs specifies protocols that associate wireless stations with access points and initiate mutual authentication using the procedures specified in this standard, the subsequent generation of keys to protect data transfer, and the cryptographic methods that protect data frames using those keys. IEEE Std 802.1AE MAC Security (MACsec) specifies cryptographic support of the Controlled Port for other media access methods. Authenticated key agreement for MAC Security, as specified in this standard, specifies the generation of the Secure Association Keys (SAKs) used by MACsec.

Use of the Controlled Port can be restricted by access controls bound to the results of authentication and distributed via AAA protocols such as Diameter (IETF RFC 6733 [B25]) or RADIUS (IETF RFC 2865 [B6]). Attributes supporting certain port-based network access control scenarios are described in IETF RFC 3580 [B13], IETF RFC 4675 [B17], IETF RFC 4849 [B18], IETF RFC 7268 [B28], and IETF RFC 8044 [B29].

Clause 7 illustrates use of the above components and protocols in typical network access control scenarios.

1.4 Provisions of this standard

The scope (1.1) of this standard is addressed by detailed specification of the following:

a) The principles of port-based network access control operation, identifying the protocol components that compose a port-based network access control implementation (Clause 6).

b) A PAE component, that supports authentication, authorization, and the key agreement functionality required by IEEE Std 802.1AE to allow a MAC Security Entity (SecY) to protect communication through a port (6.3, Clause 12).

c) A Port Access Controller (PAC) component, that controls communication where the attached LAN is deemed to be physically secure and provides point-to-point connectivity (6.4).

d) The key hierarchy used by the PAE and SecY (6.2).

e) The use of EAP by PAEs to support authentication and authorization using a centrally administered Authentication or AAA Server (Clause 8).

f) An encapsulation format, EAPOL, that allows EAP Messages and other protocol exchanges to support authentication and key agreement to be carried directly by a LAN MAC service (Clause 11).

g) A MAC Security Key Agreement protocol (MKA) that the PAE uses to discover associations and agree the keys used by a SecY (Clause 9).

h) An EAPOL Announcement protocol that allows a PAE to indicate the availability of network services, helping other PAEs to choose appropriate credentials and parameters for authentication and network access (Clause 10).

i) Requirements for management of port-based access control, identifying the managed objects and defining the management operations for PAEs (12.9).

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

Copyright © 2020 IEEE. All rights reserved.

j) SMIv2 MIB objects that can be used with SNMPv3 to manage PAEs (Clause 13).
k) YANG configuration and operational state models for PAE and PAE System components (Clause 14).

The use of port-based network access control in a number of applications is described (Clause 7) to illustrate the use of these components and the requirements taken into account in their specification. To facilitate migration to this standard, Annex F (informative) uses the same concepts to describe the architectural modeling of unsecured multi-access LANs, a widely deployed form of authenticated port-based network access control that does not meet the security requirements of this standard. Administrative connectivity to unauthenticated devices, as required for use of industry standard 'Wake-on-LAN' (WoL) protocols, is described for the scenarios of Clause 7; Annex E (informative) provides background information on WoL.

This standard defines conformance requirements (Clause 5) for the implementation of the following:

l) Port Access Entities (PAEs)
m) Port Access Controllers (PACs)

Annex A provides PICS (Protocol Implementation Conformance Statement) Proformas for completion by suppliers of implementations that are claimed to conform to this standard.

The basic architectural concepts, such as 'port', on which this standard relies are reviewed in IEEE Std 802.1AC.

This standard uses and selects options provided by EAP and AAA protocol specifications, but does not modify those specifications (see Clause 2 for references). Annex D (informative) provides EAP and RADIUS usage guidelines.

The specification and conformance requirements for association discovery and key agreement for IEEE 802.11 Wireless LANs are outside the scope of this standard (see IEEE Std 802.11). That standard makes use of the PAE specified by this standard.

Copyright © 2020 IEEE. All rights reserved.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

DMTF, Alert Standard Format (ASF) Specification, Version 2.0, 23 April 2003.[2]

iana-if-type YANG Module, Internet Assigned Numbers Authority.[3]

IEEE Std 802®, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.[4, 5]

IEEE Std 802d™, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture Amendment 1: Allocation of Uniform Resource Name (URN) Values in IEEE 802 Standards.

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

IEEE Std 802.1AB™, IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity and Discovery.

IEEE Std 802.1AC™, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Service Definition.

IEEE Std 802.1AE™, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security.

IEEE Std 802.1AX™, IEEE Standard for Local and Metropolitan Area Networks: Link Aggregation.

IEEE Std 802.2™, 1998 Edition [ISO/IEC 8802-2: 1998], Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.[6]

IEEE Std 802.3™, IEEE Standard for Ethernet.

IEEE Std 802.11™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

IEEE Std 802.1AR™, IEEE Standard for Local and Metropolitan Area Networks: Secure Device Identifier.

IETF RFC 2578, STD 58, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and Waldbusser, S., April 1999.[7]

IETF RFC 2579, STD 58, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and Waldbusser, S., April 1999.

[2]DMTF publications are available from the DMTF at https://www.dmtf.org.

[3] Available at https://www.iana.org/assignments/iana-if-type/iana-if-type.xhtml.

[4] IEEE publications are available from The Institute of Electrical and Electronics Engineers https://standards.ieee.org.

[5] The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

[6] ISO and ISO/IEC documents are available from the International Organization of Standardization (http://www.iso.org) and from the International Electrotechnical Commission (http://www.iec.ch). These documents are also available from the American National Standards Institute (http://ansi.org).

[7]IETF RFCs are available from the Internet Engineering Task Force website at https://www.ietf.org.

Copyright © 2020 IEEE. All rights reserved.

IETF RFC 2580, STD 58, Conformance Statements for SMIv2, McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and Waldbusser, S., April 1999.

IETF RFC 2863, The Interfaces Group MIB using SMIv2, McCloghrie, K., and Kastenholz, F., June 2000.

IETF RFC 3394, Advanced Encryption Standard (AES) Key Wrap Algorithm, J. Schaad, and Housley R., September 2002.

IETF RFC 3418, STD 62, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), Preshun, R., Case, J., McCloghrie, K., Rose, M., Waldbusser, S., December 2002.

IETF RFC 3629, STD 63, UTF-8, a transformation format of ISO 10646, Yergeau, F., November 2003.

IETF RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.3, Diercks, T., Rescorla, E., April 2006.

IETF RFC 4493, The AES-CMAC Algorithm, Song, J.H., Lee, J., and Iwata, T., June 2006.

IETF RFC 5216, The EAP-TLS Authentication Protocol, Simon, D., Aboba, B., and Hurst, R., March 2008.

IETF RFC 5247, Extensible Authentication Protocol (EAP) Key Management Framework, Aboba, B., Simon, D., and Eronen, P., October 2007.

IETF RFC 7170, Tunnel Extensible Authentication Protocol (TEAP) Version 1, Zhou, H., Cam-Winget, N., Salowey, J., and Hanna, S., May 2014.

IETF RFC 7317, A YANG Data Model for System Management, Bierman A., and Bjorklund M., August 2014.

IETF RFC 7950, The YANG 1.1 Data Modeling Language, Bjorklund, M., editor., August 2016.

IETF RFC 8343, A YANG Data Model for Interface Management, Bjorklund, M., March 2018.

IETF RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3, Rescorla, E., August 2018.

ISO/IEC 18033-3: 2010, Information technology—Security techniques—Encryption algorithms—Part 3:Block ciphers.

NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions, Lily Chen, October 2009.[8]

[8] NIST Special Publication FIPS 800-108 is available at https://csrc.nist.gov/publications/detail/sp/800-108/final.

Copyright © 2020 IEEE. All rights reserved.

3. Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.[9,10]

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

authentication exchange: A mechanism to verify the identity of an entity by means of information exchange.

NOTE—For example, Extensible Authentication Protocol (EAP) and Simple Authentication and Security Layer (SASL).[11]

authentication process: The cryptographic operations and supporting data frames that perform the actual authentication.

Authentication Server: An entity that provides an authentication service to an Authenticator. This service determines, from the credentials provided by the Supplicant, whether the Supplicant is authorized to access the services provided by the system in which the Authenticator resides.

NOTE—The Authentication Server function can be co-located with an Authenticator, or it can be accessed remotely via a network to which the Authenticator has access.

Authenticator: An entity that facilitates authentication of other entities attached to the same LAN.

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

NOTE—In the case of protocols designed to use the MAC Service the receive delay is typically assumed to be less than two seconds.

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

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

Bridge Port: A Port of an IEEE 802.1Q Bridge.

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

clear: When applied to a Boolean variable, **clear** means to make the value of the variable false. *See also:* **set**.

client: The protocol entity that makes use of a service.

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

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

[9] *IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

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

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

Copyright © 2020 IEEE. All rights reserved.

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

a) The transformation from plain text to cipher text and vice versa
b) Synchronized generation of keying material
c) Digital signature computation or validation[12]

cryptographic mode of operation: Also referred to as mode. An algorithm for the cryptographic transformation of data that features a symmetric key block cipher algorithm.[13]

data integrity: A property whereby data has not been altered in an unauthorized manner since it was created, transmitted, or stored.[14]

extended packet number (XPN): A 64-bit packet number (PN) specified in IEEE Std 802.1AE.

frame: MAC protocol data unit (MPDU).

IEEE 802 Local Area Network (LAN): An instance of a LAN technology that provides a MAC Service equivalent to that defined in IEEE Std 802.1AC. IEEE 802 LANs include IEEE Std 802.3 (CSMA/CD) and IEEE Std 802.11 (Wireless).

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

ifIndex: A unique identifying number associated with a logical or physical interface. The term ifIndex is defined and used by SNMP standards.

initialization vector (IV): A vector used in defining the starting point of an encryption process within a cryptographic algorithm.[15]

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

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

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

Key Agreement Entity (KaY): A PAE entity responsible for MKA.

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

Key Management Domain (KMD): A string that identifies systems that share cached CAKs.

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

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

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

[13]This and other definitions in this clause have been drawn from Federal Information Processing Standard (FIPS) 300-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001.

[14]This and other definitions in this clause have been drawn from Federal Information Processing Standard (FIPS) 800-57, Recommendation for Key Management, 2005.

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

Copyright © 2020 IEEE. All rights reserved.

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

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

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

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

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

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

network access point: A system, typically incorporating bridging or routing functionality, that comprises one or more network access ports that provides controlled access to a network for one or more systems, usually hosts.

network access port: A point of attachment of a system to a LAN. It can be a physical port, for example, a single LAN MAC attached to a physical LAN segment, or a logical port, for example, an IEEE 802.11 association between a station and an access point.

Network Identity (NID): A UTF-8 (IETF RFC 3629) string identifying an network or network service.

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

packet number (PN): A monotonically increasing value that is guaranteed unique for each MACsec frame transmitted using a given SA.

Port: A service access point for the MAC Service or MAC Internal Sublayer Service.

port access entity (PAE): The protocol entity associated with a Port. It can support the protocol functionality associated with the Authenticator, the Supplicant, or both.

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

NOTE—The Port Identifier is not constrained to correspond to any other identifier, index, or port number. There can be more than one SC for a physical port, identifying frames transmitted by separate virtual ports, and more than one SC for a physical or virtual port if that port uses different SCs to transmit frames of different priorities.

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

real port: A port that is not created on demand, but that can transmit and receive frames for one or more virtual ports.

Salt: A 96-bit secret value communicated by key agreement protocol for use by the protection and verification operations of the IEEE Std 802.1AE GCM-AES-XPN Cipher Suites.

secret key: A cryptographic key used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public.[16]

Copyright © 2020 IEEE. All rights reserved.

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

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

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

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

Secure Channel Identifier (SCI): A unique identifier for a secure channel, comprising a MAC Address and a Port Identifier.

NOTE—Key agreement protocols such as MKA are responsible for ensuring that each SCI used with a given SAK is unique where a Cipher Suite requires that for nonce construction, as does the Default Cipher Suite (14.5 of IEEE Std 802.1AE-2018). SCI uniqueness does not rely on MAC Address allocation procedures.

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

secure Connectivity Association Key (CAK): A secret key possessed by members of a given CA.

secure Connectivity Association Key Name (CKN): A text that identifies a CAK.

secured connectivity: Data transfer between two or more Controlled Ports that is protected by MACsec.

NOTE—MACsec requires mutual authentication between communicating peers, so secured connectivity is always authenticated. Connectivity that is not secured could have been preceded by mutual authentication, but is not proof against intrusion.

set: When applied to a Boolean variable, **set** means to make the value of the variable true. *See also:* **clear**.

Short Secure Channel Identifier (SSCI): A 32-bit value that is unique for each SCI within the context of all SecYs using a given SAK.

NOTE—IEEE Std 802.1AEbw-2013 specified the calculation of SSCI and Salt values used by the IEEE Std 802.1AE GCM-AES-XPN Cipher Suites from other MKA values. IEEE Std 802.1Xck-2018 constrained the order of entries in the MKPDU Live Peer List to facilitate that calculation.

Supplicant: An entity at one end of a point-to-point LAN segment that seeks to be authenticated by an Authenticator attached to the other end of that link.

NOTE—The term *Supplicant* is used in this standard in place of the term *peer*, used in other access control-related specifications, as peer is used throughout IEEE 802.1 standards and elsewhere to denote a protocol entity of equal status in a layered protocol model.

system: A device that is attached to a LAN by one or more Ports. Examples of systems include end stations, servers, MAC Bridges, and routers.

unauthenticated connectivity: Data transfer between peers that are not mutually authenticated (such data transfer cannot be secured by MACsec).

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

[16]FIPS 140-2.

Copyright © 2020 IEEE. All rights reserved.

unsecured connectivity: Data transfer that is not protected by MACsec, but has been preceded by mutual authentication between the (supposedly) communicating peers.

virtual port: A MAC Service or Internal Sublayer service access point (IEEE Std 802.1AC) that is created on demand. Virtual ports can be used to provide separate secure connectivity associations over the same LAN.

YANG: A data modeling language, published as IETF RFC 7950.

Copyright © 2020 IEEE. All rights reserved.