International Standard

ISO/IEC/IEEE 8802-1AE

Second edition
2020-08

AMENDMENT 4
2024-11

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

Part 1AE:
Media access control (MAC) security

AMENDMENT 4: MAC Privacy Protection

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

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

AMENDEMENT 4: Protection de la vie privée MAC

Reference number
ISO/IEC/IEEE 8802-1AE:2020/
Amd.4:2024(en)

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

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 document 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.

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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 8802-1AE:2020/Amd.4 was prepared by the LAN/MAN of the IEEE Computer Society (as IEEE Std 802.1AEdk-2023) 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.

Contents

Figures

Tables

IEEE Standard for
Local and Metropolitan Area Networks —

Media Access Control (MAC) Security

Amendment 4:
MAC Privacy Protection

[This amendment is based on IEEE Std 802.1AE™-2018.]

NOTE—The editing instructions contained in this amendment define how to merge the material contained therein into the existing base standard and its amendments to form the comprehensive standard.

The editing instructions are shown in ***bold italics***. Four editing instructions are used: change, delete, insert, and replace. ***Change*** is used to make corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using ~~strikethrough~~ (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Deletions and insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editing instructions, change markings, and this note will not be carried over into future editions because the changes will be incorporated into the base standard.

1. Overview

1.1 Introduction

Change 1.1 as follows:

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.

The MAC Security protocol (MACsec), as defined by this standard, allows authorized systems that attach to and interconnect LANs in a network to maintain confidentiality of transmitted data and to take measures against frames transmitted or modified by unauthorized devices.

MACsec facilitates

a) Maintenance of correct network connectivity and services

b) Isolation of denial of service attacks

c) Localization of any source of network communication to the LAN of origin

d) The construction of public networks, offering service to unrelated or possibly mutually suspicious customers, using shared LAN infrastructures

e) Secure communication between organizations, using a LAN for transmission

f) Incremental and non-disruptive deployment, protecting the most vulnerable network components

To deliver these benefits, MACsec has to be used in conjunction with appropriate policies for higher-level protocol operation in networked systems, an authentication and authorization framework, and network management. IEEE Std 802.1X™ provides authentication and cryptographic key distribution.[1]

MACsec protects communication between trusted components of the network infrastructure, thus protecting the network operation. MACsec cannot protect against attacks facilitated by the trusted components themselves, and is complementary to, rather than a replacement for, end-to-end application-to-application security protocols. The latter can secure application data independent of network operation, but cannot necessarily defend the operation of network components, or prevent attacks using unauthorized communication from reaching the systems that operate the applications.

MAC Privacy protection protocol, as defined by this standard, can be used in conjunction with MACsec to reduce the ability of adversaries to correlate the MAC addresses, sizes, and transmission timing of user data frames with individual persons, network applications, details of those applications, and levels of application activity.

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

1.2 Scope

Change 1.2 as follows:

The scope of this standard is to specify provision of connectionless user data confidentiality, frame data integrity, and data origin authenticity by media access independent protocols and entities that operate transparently to MAC Clients.

NOTE—The MAC Clients are as specified in IEEE Std 802, IEEE Std 802.1Q™, and IEEE Std 802.1X™.[2]

To this end it

a) Specifies the requirements to be satisfied by equipment claiming conformance to this standard.

b) Specifies the requirements for MAC Security ~~MACsec~~ in terms of provision of the MAC Service and the preservation of the semantics and parameters of service requests and indications.

c) Describes the threats, both intentional and accidental, to correct provision of the service.

d) Specifies security services that prevent, or restrict, the effect of attacks that exploit these threats.

e) Examines the potential impact of both the threats and the use of MACsec on the Quality of Service (QoS), specifying constraints on the design and operation of MAC Security entities and protocols.

f) Models support of the secure MAC Service in terms of the operation of media access control method independent MAC Security Entities (SecYs) within the MAC Sublayer.

g) Specifies the format of the MACsec Protocol Data Unit (MPDUs) used to provide secure service.

h) Identifies the functions to be performed by each SecY, and provides an architectural model of its internal operation in terms of Processes and Entities that provide those functions.

i) Specifies each SecY's use of an associated and collocated Port Access Entity (PAE, IEEE Std 802.1X) to discover and authenticate MACsec protocol peers, and its use of that PAE's Key Agreement Entity (KaY) to agree and update cryptographic keys.

j) Specifies performance requirements and recommends default values and applicable ranges for the operational parameters of a SecY.

k) Specifies how SecYs are incorporated within the architecture of end stations, bridges, and two-port Ethernet Data Encryption devices (EDEs).

l) Establishes the requirements for management of MAC Security, identifying the managed objects and defining the management operations for SecYs.

m) Specifies~~ the~~ a Management Information Base (MIB) module for SecY management ~~managing the operation of MAC Security in TCP/IP networks~~.

n) Specifies a YANG configuration and operational state model for SecY management.

o) Specifies requirements, criteria, and choices of Cipher Suites for use with this standard.

p) Describes threats to individual privacy that can result from an adversary's observation of individual frames, even if those frames are integrity protected and their data confidentiality protected.

q) Models support of a privacy protected secure MAC Service in terms of the operation of MAC Privacy protection Entities (PrYs) that encapsulate user data frames in MAC Privacy protection Protocol Data Units (MPPDUs) to hide the user source and destination MAC addresses and to reduce any correlation of the sizes and transmission timing of frames with user identities and communication purposes, applications, or content.

r) Specifies the addressing, encoding, and decoding of MPPDUs.

s) Identifies the functions to be performed by each PrY, and provides an architectural model of its internal operation in terms of Processes and Entities that provide those functions.

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

t) Specifies performance requirements and recommends default values and applicable ranges for the operational parameters of a PrY.

u) Specifies how PrYs can be incorporated within the architecture of end stations, bridges, two-port Ethernet Data Encryption devices (EDEs), and bridged networks.

v) Describes the requirements for management of MAC Privacy protection, identifying the managed objects and defining the manged objects for PrYs.

w) Specifies a Management Information Base (MIB) module for PrY management.

x) Specifies a YANG configuration and operational state model for PrY management.

2. Normative references

Change the list of normative references in Clause 2 as follows:

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.

IEEE Std 802®, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.[3,4]

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

IEEE Std 802.1X™, IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control.

~~IEEE Std 802.1Xbx™-2014, IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control—Amendment 1: MAC Security Key Agreement Protocol (MKA) Extensions.~~

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 802.3™, IEEE Standard for Ethernet.

IETF RFC 1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II, McCloghrie, K., and Rose, M. T., March 1991.[5]

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.

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.

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 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), Preshun, R., editor, December 2002.

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

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

[3] IEEE publications are available from The Institute of Electrical and Electronics Engineers (https://www.standards.ieee.org).
[4] The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.
[5] IETF RFCs are available from the Internet Engineering Task Force (https://www.ietf.org/rfc.html).

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

ISO/IEC 14882, Information Technology—Programming languages—C++.[6]

NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007.[7]

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

[7] NIST Special Publications are available from the National Institute of Standards and Technology (https://csrc.nist.gov/).