APPROVED DRAFT

P802.1Xck/D2.2
(DRAFT Amendment to IEEE Std 802.1X™–2010 as amended by
IEEE Std 802.1Xbx™–2014)
July 4, 2018

Draft Standard for
Local and metropolitan area networks—

Port-Based Network Access Control

Amendment 2: YANG Data Model

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Prepared by the Security Task Group of IEEE 802.1

Copyright © 2018 by the Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street
New York, NY 10017, USA
All rights reserved.

All rights reserved.This document is an unapproved draft of a proposed IEEE Standard. As such, this document is subject to change. USE AT YOUR OWN RISK! Because this is an unapproved draft, this document must not be utilized for any conformance/compliance purposes. Permission is hereby granted for IEEE Standards Committee participants to reproduce this document for purposes of IEEE standardization activities only. Prior to submitting this document to another standards development organization for standardization activities, permission must first be obtained from the Manager, Standards Licensing and Contracts, IEEE Standards Activities Department. Other entities seeking permission to reproduce this document, in whole or in part, must obtain permission from the Manager, Standards Licensing and Contracts, IEEE Standards Activities Department.

IEEE Standards Department
Copyright and Permissions
445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331, USA

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.

Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

Abstract: This amendment specifies a YANG data model that allows configuration and status reporting for port-based network access control in the scenarios described in Clause 7 of this standard and Clause 11 of IEEE Std 802.1AE™, using the information model previously specified in this standard.

Keywords: authorized port, confidentiality, data model, data origin authenticity, information model, integrity, LANs, local area networks, MAC Bridges, MAC security, MAC Service, MANs, metropolitan area networks, port based network access control, secure association, security, transparent bridging, YANG.

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

Copyright © 2018 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published x xxxxxxx 2018. Printed in the United States of America

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

PDF: ISBN xxxx
Print: ISBN xxxx

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.

Documents
Document Sharing Hub

This is an unapproved IEEE Standards draft, subject to change.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:48 UTC from IEEE Xplore. Restrictions apply.

Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

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 Notice" or "Important Notices and Disclaimers Concerning IEEE Standards Documents."

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. Volunteers 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 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.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.

Documents
Document Sharing Hub

Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

Translations

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

Official statements

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

Comments on standards

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

Comments on standards should be submitted to the following address:

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

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.

This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

Photocopies

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

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at http://ieeexplore.ieee.org/xpl/standards.jsp 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 © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

Introduction

This introduction is not part of IEEE Std 802.1Xck-20xx,
IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control—Amendment 2: YANG Data Model.

This second amendment to IEEE Std 802.1X-2010 specifies a YANG data model that allows configuration and status reporting for port-based network access control, in the scenarios described in Clause 7 of this standard and Clause 11 of IEEE Std 802.1AE™, using the information model previously specified in this standard.

The first edition of IEEE Std 802.1X was published in 2001. The second edition, IEEE Std 802.1X-2004 clarified areas related to mutual authentication and the interface between 802.1X specified state machine, and those specified by 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, clarifying and generalizing 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 in IETF RFCs. Further changes updated the standard to reflect best current practice, insisting, for example, upon 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 upon the security of the network accessed, and some prior provisions, with a more comprehensive treatment of segregating and limiting connectivity to unauthenticated systems. Applications of port-based network access that use IEEE Std 802.1AE MAC Security (MACsec) and/or MKA (MACsec Key Agreement protocol) are described.

Every effort was made to ensure that systems conformant to IEEE Std 802.1X-2010 will 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 in respect of 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. IEEE Std 802.1X-2010 includes 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.

IEEE Std 802.1Xbx-2014 MAC Security Key Agreement protocol (MKA) extensions, amended IEEE Std 802.1X-2010 by extending MKA to realize additional security and manageability capabilities made possible by the IEEE Std 802.1AEbw-2013 amendment that added extended packet numbering Cipher Suites to IEEE Std 802.1AE-2006. 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.

Participants

<<The lists of participants will be added in the usual way following approval of the standard.>>

Copyright © 2018 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
This is an unapproved IEEE Standards draft, subject to change.
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...
Documents
Document Sharing Hub

APPROVED DRAFT

Contents

1.Overview ... 3

1.3 Introduction ... 3
1.4 Provisions of this standard ... 3

2.Normative references ... 5

3.Definitions ... 8

5.Conformance ... 9

5.3 Conformant systems and system components ... 9
5.4 PAE requirements ... 10
5.10 MKA requirements ... 10
5.12 Virtual port requirements ... 11
5.23 Requirement for YANG data model of a PAE ... 11
5.24 Options for YANG data model of a PAE ... 11

6.Principles of port-based network access control operation ... 12

6.1 Port-based network access control architecture ... 12
6.4 Port Access Controller (PAC) ... 13

7.Port-based network access control applications ... 14

7.5 Host access with MACsec and a multi-access LAN ... 14

8.Authentication using EAP ... 15

8.11 EAP methods ... 15

9.MACsec Key Agreement protocol (MKA) ... 16

9.8 SAK generation, distribution, and selection ... 16
9.10 SAK installation and use ... 18
9.11 Connectivity change detection ... 20

11.EAPOL PDUs ... 21

11.1 EAPOL PDU transmission, addressing, and protocol identification ... 21
11.11 EAPOL-MKA ... 22

12.PAE operation ... 26

13.PAE MIB ... 28

13.4 Security considerations ... 28
13.5 Definitions for PAE MIB ... 29

14.YANG Data Model ... 78

14.1 PAE management using YANG ... 78
14.2 Security considerations ... 79
14.3 802.1X YANG model ... 81
14.4 Relationship to other YANG data models ... 81
14.5 Definition of the 802.1X YANG data model ... 94

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents
Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

14.6 YANG data model use in network access control applications 122

Annex A (normative) PICS Proforma 127

A.5 Major capabilities and options 127
A.6 PAE requirements and options 128
A.9 MKA requirements and options 129
A.15 YANG requirements and options 130

Annex B (informative) Bibliography 131

Annex E (informative) IEEE 802.1X EAP and RADIUS usage guidelines 135

E.1 EAP Session-Id 135
E.2 RADIUS Attributes for IEEE 802 Networks 135

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents
Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

Figures

Figure 12-3 PAE management information 27
Figure 14-1 YANG model structure 81
Figure 14-2 YANG object hierarchy with 802.1X 81
Figure 14-3 IETF system management YANG model 83
Figure 14-4 IETF interface management YANG model 85
Figure 14-5 Explicit Interface Model of Bridge Port 91
Figure 14-6 Augmented Interface Mode of Bridge Port..... 91
Figure 14-7 Bridge Port with LAG Interface stack model 91
Figure 14-8 Bridge Port YANG Interface stack model with MACSec 92
Figure 14-9 Augmented Interface Model of Bridge Port with MACSec 92
Figure 14-10 YANG Interface Model with MACSec and virtual ports 93
Figure 14-11 Explicit Interface Model of Bridge Port LAG with MACSec on members..... 93
Figure 14-12 Augmented Interface Model of Bridge Port LAG with MACSec on members..... 94
Figure 14-13 802.1X YANG model for host (7.1) 123
Figure 14-14 802.1X YANG model for network access point (7.1) 123
Figure 14-15 802.1X YANG model for network access point (7.3) 124

Copyright © 2018 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
This is an unapproved IEEE Standards draft, subject to change.
Documents
Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

Tables

Table 11-1 EAPOL group address assignments 22
Table 11-7 MKPDU parameter sets 23
Table 13-4 PAE managed object cross-reference table 28
Table 13-4 PAE managed object cross-reference table 28
Table 14-1 PAE System cross-reference table 84
Table 14-2 PAE cross-reference table 86

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

Draft Standard for
Local and metropolitan area networks—

Port-Based Network Access Control

Amendment 2: YANG Data Model

[This amendment is based on IEEE Std 802.1X™-2010 as amended by IEEE Std 802.1Xbx-2014.]

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 italic***. 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.

IIMPORTANT NOTICE: IEEE Standards documents are not intended to ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers 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.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...
Documents
Document Sharing Hub

APPROVED DRAFT

Copyright © 2018 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
This is an unapproved IEEE Standards draft, subject to change.
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

1. Overview

1.3 Introduction

Change the fourth paragraph of 1.3 as follows

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 3588 [B13]) or RADIUS (IETF RFC 2865 [B4]). Attributes supporting certain port-based network access control scenarios are described in IETF RFC 3580, IETF RFC 4675, ~~and~~ IETF RFC 4849, and IETF RFC 7268 [B26].

1.4 Provisions of this standard

Change the text of 1.4, as follows:

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).
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 G (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 F (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)

Copyright © 2018 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
This is an unapproved IEEE Standards draft, subject to change.
Documents
Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

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’, that this standard relies on are reviewed in IEEE Std 802.1AC ~~Annex D~~.

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 E (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 © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.

Documents
Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

2. Normative references

Change the text of Clause 2 Normative References, 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.[1, 2]

~~IEEE Std 802.1D™, IEEE Standard for Local and Metropolitan Area Networks: Media access control (MAC) Bridges.[1,2]~~

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 ~~Virtual Bridged Local Area 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 802.1AE™-2006, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security.[3]

IEEE Std 802.1AEbn™-2011, IEEE Standard for Local and Metropolitan Area Network — Media Access Control (MAC) Security — Amendment 1: Galois Counter Mode—Advanced Encryption Standard—256 (GCM–AES–256) Cipher Suite.

IEEE Std 802.1AEbw™-2013, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security — Amendment 2: Extended Packet Numbering.

IEEE Std 802.1AEcg™, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security — Amendment 3: Ethernet Data Encryption devices.

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.[4]

IEEE Std 802.3™, IEEE Standard for Ethernet.

---

[1]IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA. IEEE publications can be ordered on-line from the IEEE Standards Website: https://www.standards.ieee.org.

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

[3]This standard refers to the latest edition of IEEE Std 802.1AE in addition to referencing specific revisions and amendments.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

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 802.17™-2004 IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 17: Resilient packet ring (RPR) access method and physical layer 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., Waldbusser, S., April 1999.[5]

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., Waldbusser, S., April 1999.

IETF RFC 2580, STD 58, Conformance Statements for SMIv2, McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., 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, R. Housley, September 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 1.1, Dierekx, T., Rescorla, E., April 2006.~~

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

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

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

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

[R-Xck-1] draft-bjorklund-netmod-rfc7223bis-00, A YANG Data Model for Interface Management, M. Bjorklund, August 21, 2017

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

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

[4]ISO [IEEE] and ISO/IEC [IEEE] documents are available from ISO Central Secretariat, 1 rue de Varembé, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA. ISO [IEEE] and ISO/IEC [IEEE] documents can be ordered on-line from the IEEE Standards Website: https://www.standards.ieee.org.

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

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

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, November 2008[6].

iana-if-type YANG module, Internet Assigned Numbers Authority, https://www.iana.org/assignments/iana-if-type/iana-if-type.xhtml.

[6]National Institute of Standards and Technology, FIPS 140-2 is available at https://csrc.nist.gov/publications/detail/sp/800-108/final.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents
Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

3. Definitions

Change the definition of authentication exchange and the following NOTE as follows:

authentication exchange: ~~The two-party conversation between systems performing an authentication process~~ 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).[7]

Change the definition of Bridge Port as follows:

Bridge Port: A Port of an ~~IEEE 802.1D or~~ IEEE 802.1Q Bridge.

Change the definition of IEEE 802 Local Area Network as follows:

IEEE 802 Local Area Network (LAN): IEEE 802 LANs (also referred to in the text simply as LANs) are LAN technologies that provide a MAC Service equivalent to that defined in IEEE Std 802.1AC ~~ISO/IEC 15802-1~~. IEEE 802 LANs include IEEE Std 802.3 (CSMA/CD), and IEEE Std 802.11 (Wireless), ~~and IEEE Std 802.17 (Resilient Packet Ring)~~.

Change the definitions of Port Identifier and Secure Channel Identifier as follows:

Port Identifier: A 16-bit identifier ~~number~~ that ~~is unique within the scope of the address of the port~~ 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 corrrespond to any other identifier, index, or port number, and 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.

Secure Channel Identifier (SCI): A ~~globally~~ unique identifier for a secure channel, comprising a ~~globally unique~~ MAC Address and a Port Identifier~~, unique within the system allocated that address~~.

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.

Change the NOTE following the definition of Short Secure Channel Identifier (SSCI), as follows:

NOTE—IEEE Std 802.1AEbw-2013 specifie~~s~~d the calculation of SSCI and Salt values used by the IEEE Std 802.1AE GCM-AES-XPN Cipher Suites from other MKA values. The IEEE Std 802.1Xck amendment to this standard constrained the order of entries in the MKPDU Live Peer List to facilitate that calculation.

Change the definition of virtual port as follows:

virtual port: A MAC Service or Internal Sublayer service access point (~~D.4~~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.

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

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

5. Conformance

Change the text of 5.3 as follows:

5.3 Conformant systems and system components

This clause (5) specifies requirements and options for implementation of the following components:

a) Port Access Entity (PAE, see 6.3, Clause 12) (5.4, 5.5, 5.6–5.15, 5.18, 5.19)
b) Port Access Controller (PAC, see 6.4) (5.20)

A port for which conformance to this standard is claimed shall implement the mandatory functions of the PAE (5.4) and the mandatory functionality for at least one of the following PAE functions:

— Supplicant (5.6, 5.7)
— Authenticator (5.8, 5.9)
— MACsec Key Agreement (MKA) (5.10, 5.11)

That port may also implement the mandatory functionality for all or any of the following PAE functions:

— Announcement transmission (5.14, 5.15)
— Announcement reception (5.16, 5.17)
— SNMP access to the PAE MIB (5.18, 5.19)
— Network configuration protocol (e.g., NETCONF) access to the YANG configuration and operational state model of the PAE and PAE system (5.23, 5.24)

A port that implements Authenticator or MKA functionality may also implement the mandatory functionality for the following PAE function:

— Virtual ports (5.12)

A port may implement the optional functionality for any function for which the mandatory functionality has been implemented.

The operation of one or more MAC Security Entities (as specified by IEEE Std 802.1AE) can be required to secure communication for each port. A port that does not implement a SecY shall implement the PAC (5.20).

Any implementation that is claimed to conform to this standard shall not violate the provisions of 5.22 (Prohibitions).

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

5.4 PAE requirements

Change the text of 5.4 as follows:

A PAE shall

a) Encode, decode, address, and validate EAPOL PDUs as specified in Clause 11.
b) ~~Transmit group-addressed EAPOL PDUs using one, and only one, of the destination addresses specified in Table 11-1.~~
b) Implement the Logon Process functionality specified in 12.5.
c) Implement the CP state machine as specified in 12.4.
d) Maintain and allow retrieval of the EAPOL frame reception statistics specified in 12.8.1.
e) Maintain and allow retrieval of the EAPOL frame reception diagnostics specified in 12.8.2.
f) Maintain and allow retrieval of the EAPOL frame transmission statistics specified in 12.8.3.
g) Support the system configuration functions specified in 12.9.

A PAE that supports both EAP (Supplicant or Authenticator) and MKA functionality shall

h) Derive a CAK from each EAP MSK, and a corresponding CKN for the corresponding EAP session ID as specified in 6.2.2.

A claim that an implementation conforms to this standard shall specify

i) The group address used to transmit group addressed PDUs. If the implementation can be configured in a way that changes the address used, that configuration shall be specified.

A PAE shall not

j) Use ~~a~~ the MACsec protected Controlled Port controlled by the PAE to transmit EAPOL Packet Types other than EAPOL-Announcement (10.2).

5.10 MKA requirements

Change the initial text of 5.10 as follows:

A PAE that supports MKA shall

a) Be capable of maintaining 2 or more simultaneous MKA instances as specified in Clause 9.
b) Specify the maximum number of simultaneous MKA instances it supports.
c) Create, delete, and activate MKA participants as specified in 9.13 and 9.16.
d) Be capable of receiving and using Group CAKs distributed by a Key Server.
e) Meet the requirements for MKA parameter encoding and for MKPDU validation, encoding, and decoding, specified in 11.11.
f) Be capable of using 128 bit CAKs and derived keys as specified in 6.2 and 9.3.
g) Observe the restrictions on the use and disclosure of each CAK and derived keys specified in 6.2 and 9.16.
h) Protect each distributed CAK and SAK by AES Key Wrap, as specified in 9.8.2 and 9.12.1.
i) Include the parameters of EAPOL-Announcements in MKPDUs, as specified in 9.13.

A claim that an implementation conforms to this standard and supports MKA shall specify

j) The MKA Version supported (11.11, Table 11-7, 11.11.3).

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

5.12 Virtual port requirements

Change the last paragraph and bullet g) of 5.12 as follows:

A PAE implementation that creates virtual ports in a system that bridges frames to and from those ports as specified by ~~IEEE Std 802.1D or~~ IEEE Std 802.1Q shall

g) Support each of those virtual ports as specified by ~~that standard (IEEE 802.1D or~~ IEEE 802.1Q~~, as applicable)~~ for each Bridge Port, including support for Spanning Tree Protocol (see 7.6).

Insert new subclauses 5.23 and 5.24 as follows:

5.23 Requirement for YANG data model of a PAE

An implementation that is claimed to conform to the provisions of this standard for providing a YANG data model for configuration and operational state of a PAE, shall

a) Support access to the YANG model specified in Clause 14 using a network configuration protocol (such as NETCONF).
b) Support the configuration of PAEs within a PAE System using the YANG model (described in Clause 14).
c) Support the retrieval of operational state information of PAEs within a PAE System using the YANG model (described in Clause 14).

5.24 Options for YANG data model of a PAE

No options are specified for network configuration protocol access to the PAE YANG model.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

6. Principles of port-based network access control operation

Change the last paragraph of the introductory text of Clause 6 as follows:

An understanding of architectural concepts common to this and other IEEE 802.1 standards is essential to understanding this standard's specification of port-based network access control. The reader is encouraged to review ~~Annex D~~ Clause 7 of IEEE Std 802.1AC-2016 prior to reading the rest of this standard, and needs to be familiar with IEEE Std 802.1AE's description of secure LAN communication architecture including the fundamental concept of a Secure Connectivity Association (CA).

6.1 Port-based network access control architecture

Change the first paragraph and bullet list of 6.1 as follows:

The system architecture that supports port-based network access control includes the following:

a) The port, i.e., entities that compose an interface stack supporting a MAC Service access point, through which communication is controlled and secured.
b) The attached LAN, providing the MAC service to the port's client (IEEE Std 802.1AC~~D.6~~) and its peers.
c) Mechanisms that define a connectivity association between the port and a peer port or ports.

and, for each port that is a potential peer in secure access controlled communication, a protocol entity or entities that

d) Possess an authentication credential, is within or attached to the same system as the port, and has a secure relationship with the port and its clients ~~(D.6)~~.
e) Mutually authenticate peer ports, and whose operation results in
    1) Success or failure of the authentication.
    2) A token, comprising cryptographic keys and associated data, that can serve as a proof of mutual authentication in subsequent protocols.
    3) A binding to authorization data or to a secure channel that can be used to communicate authorization data to the access controlled port and its clients.
f) Communicate authorization data to the port's clients ~~(D.6)~~, so that each can permit or deny the use of manageable protocol capabilities appropriately.
g) Use the results of authentication to agree on keys to cryptographically protect communication, creating a secure connectivity association between peer ports.
h) Protect the data transferred within the secure connectivity association.
i) Enforce access control based on the success or failure of the authentication.

6.2.2 Using EAP for CAK key derivation

Change the third paragraph of 6.2.2 Algorithm Agility as follows:

For historical reasons MAC addresses, and the 24-bit OUIs assigned so that the assignee could derive a number of MAC addresses, were defined as bit-strings. mac1 and mac2 above are sequences of 6 octets, with the value of first octet derived from the first 8 bits of the 48-bit MAC address string, the second octet from second set of eight bits and so on, each set of 8 bits being taken to represent a binary number with its first bit being the least significant. The value of each octet in the sequence corresponds to that naturally associated with the Hexadecimal Representation of the LAN MAC Address defined in ISO/IEC 10039 (LAN MAC Service Definition) and referenced by IEEE Registration Authority tutorials, and the order of the octets corresponds to the left to right order in that representation. The first bit of the address string is the

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

Individual/Group address, and the bit order of the address is that originally used for transmission on IEEE 802.3 media. The octet sequence defined to represent the MAC address is used in a number of other IEEE 802.1 standards, including ~~IEEE Std 802.1D and~~ IEEE Std 802.1Q and the value and representation for an address is commonly known as the 'canonical format'. Users of this specification are warned that the long running 'endian' disputes about bit ordering and bit significance mean that some seemingly authoritative and generally available tutorials do reverse the bits of the 48-bit address string in eight bit groups, in order to show the most significant bit to the left (first according to some familiar conventions), though most now retain the bit significance necessary to this specification.

6.3.6 Multi-access LANs

Change the NOTE as follows:

NOTE—The addressing (individual or group) for each EAPOL Packet Type is specified in ~~Table 11-1 and~~ Table 11-4. For compatibility with prior revisions of this standard Supplicants attached to 802.3 networks use only group addresses in the destination address field of EAPOL frames supporting PACP.

6.4 Port Access Controller (PAC)

Change the first paragraph of 6.4 as follows:

The PAC is a protocol-less shim ~~(D.5)~~ (IEEE Std 802.1AC) that provides control over frame transmission and reception by clients attached to its Controlled Port, and uses the MAC Service provided by a Common Port. The access control decision is made by the PAE, typically taking into account the success or failure of mutual authentication and authorization of the PAE's peer(s), and is communicated by the PAE using the LMI to set the PAC's controlledPortEnabled variable. The PAE itself attaches to an Uncontrolled Port, provided by the PAC to support the authentication exchange prior to authorizing use of the Controlled Port. See Figure 6-6. Either or both of the SecY's in Figure 6-2 could be replaced with a PAC if cryptographically secured communication between the two systems were not required. A SecY can be configured, using the management controls specified in IEEE Std 802.1AE, to behave exactly like a PAC—thus facilitating interoperability when only one of the communicating systems implements MACsec.

6.4.2 Controlled Port transmission and reception

Change the second paragraph of 6.4.2 as follows:

MAC_Operational (IEEE Std 802.1AC~~D.4~~) for the Controlled Port is set *True* if and only if MAC_Operational for the Common Port is *True* and controlledPortEnabled is set.

6.4.3 PAC management

Change the second paragraph of 6.4.3 as follows:

The following status parameters (IEEE Std 802.1AC~~D.4~~) for the Uncontrolled Port and the Controlled Port are provided (separately) to the user(s) of those ports, and can be read by management:

- MAC_Enabled
- MAC_Operational
- operPointToPointMAC
- adminPointToPointMAC

Copyright © 2018 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
This is an unapproved IEEE Standards draft, subject to change.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

7. Port-based network access control applications

7.5 Host access with MACsec and a multi-access LAN

Change the first NOTE as follows:

NOTE 1—This standard specifies the procedures necessary to create virtual ports, but the instantiation of such ports within a bridge or router, though easy to envisage, is outside its scope. Creation of such virtual ports within the architecture specified in ~~IEEE Std 802.1D or~~ IEEE Std 802.1Q would require support for transmission of frames received on a physical Bridge Port through that same port if any two virtual ports can be members of the same VLAN.

Change the third NOTE as follows:

NOTE 3—This standard makes use of a layered protocol model (see ~~Annex D~~ IEEE Std 802.1AC), thus allowing the entities and protocols it specifies to be instantiated above a service access point supported by an arbitrary interfaces stack (see Figure 7-18, for example). If a single physical realization of an IEEE 802 LAN MAC were to be identified by more than one MAC Address, a separate MSAP would be provided for each address and the resulting system behavior would, for the purposes of this standard, be the same as that of a collection of separate stations each with a single address.

Change the NOTE to figure 7-16 as follows:

NOTE—Figure 7-16 is based on Figure 15-1 of IEEE Std 802.1Q-2018~~ (as amended by IEEE Std 802.1ad)~~.

Change the last sentence of the second paragraph of clause 7.7.2 as follows:

The interface stack shown includes the service access priority selection function described in 6.13 of IEEE Std 802.1Q-2018 ~~(as amended by IEEE Std 802.1ad)~~.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

8. Authentication using EAP

8.11 EAP methods

Insert the following paragraph after the first paragraph of this clause.

A passive adversary between a Supplicant and EAP authenticator can observe any information that an EAP method passes without confidentiality protection. This could be considered a privacy threat to the Supplicant. Some EAP methods (e.g., a “tunneled EAP” method such as TEAP (IETF RFC 7170)) protect the complete contents of the authentication process from a passive adversary.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

9. MACsec Key Agreement protocol (MKA)

Change 9.2.2 as follows:

9.2.2 SC identification

Each SC is identified by an SCI that comprises a ~~globally unique~~ MAC address and a Port Identifier, unique within the system that has been allocated that address.

Change 9.4.5 as follows:

9.4.5 Addressing

A LAN can be an individual LAN, bounded by the extent of its supporting media access method and media access method procedures, or can be supported by bridges in a Bridged Local Area Network or Virtual Bridged Local Area Network. Interoperability, avoiding redundancy, protecting the infrastructure, and the need to support communication between stations in the network, all necessitate placing restrictions on where, within the interface stack that composes a port (IEEE Std 802.1AC~~D.4~~), SecYs are placed. IEEE Std 802.1AE-2006 Clause 11 specifies the use of MACsec within systems, and those restrictions, but explicitly recognizes that MACsec can be used across, within, and to secure access to a Provider Bridged Network. The destination address used by MKA has to be aligned with the placement of port-based network access control in the interface stack and the corresponding use of MACsec within the protocol stack, and shall be ~~one of the~~ a group address~~es specified in Table 11-1 and shall not be an individual address~~. Table 11-1 specifies group addresses that support the application scenarios described in this standard (Clause 7).

NOTE—Use of a group address that is filtered by bridges~~, as specified above,~~ and the inclusion of destination and source MAC addresses within the ICV calculation, makes it more difficult to attack MKA from a distance.

The source address of each MKPDU shall be ~~a globally unique~~ an individual MAC Address assigned to the port transmitting that MKPDU.

9.8 SAK generation, distribution, and selection

Change the first sentence of the third paragraph of 9.8 as follows:

If the Current Cipher Suite is not using extended packet numbering, t~~T~~he Key Server observes the Key Identifier and Lowest Acceptable PN ~~(LLPN) for the Latest Key~~ for the most recent SAK in use, as transmitted by each CA member (the LKI and LLPN if LRX is true, and the OKI and OLPN otherwise, <9.10.1>), and distributes a fresh SAK (subject to the constraints specified in <9.5> and this clause) if that Key Identifier ~~whenever a participant advertises an LKI that~~ matches the KI of the key ~~currently being~~ most recently distributed and ~~an LLPN~~ that Lowest Acceptable PN equals or exceeds the constant PendingPNExhaustion.

Change the fifth paragraph of 9.8 and the NOTE following as follows:

An MKA participant does not retain any record of SAKs used prior to initialization or re-initialization, and uses a fresh MI whenever it is initialized, thus forcing distribution of a fresh SAK whenever it has no record of prior SAK use. An MKA participant is re-initialized, or deleted and a fresh participant created, if the associated SCI is changed. An MKA participant accepts only SAKs distributed by Key Servers that are mutually live, i.e., shall not accept an SAK distributed in any MKPDU that does not contain that participant's MI and acceptably recent MN in the Live Peers List.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

NOTE 3—Inclusion in the Potential Peers List is sufficient to prove that the Key Server is live, but not that it has recognized the participant as live and updated the distributed key. Reinitializing and using a new MI if an SCI is changed prevents use of the new SCI in conjunction with a previously distributed SAK, allows the Key Server to check for SCI collision before distributing a fresh SAK, and means that the Key Server and other participants are aware of the change when calculating SSCI values.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents
Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

9.10 SAK installation and use

Change the first two paragraphs of 9.10 as follows:

Each CA member's KaY uses the LMI supported by the SecY (IEEE Std 802.1AE-2006, 10.7) to create a receive SC for each of its live peers' SCs, and a SA for each receive SC and its own transmit SC(s) using the distributed SAK and AN.

NOTE 1—As specified in the IEEE Std 802.1AEcg-2016 amendment to IEEE Std 802.1AE, an MKA participant is associated with each transmit SC even if multiple transmit SCs (each with its own SCI) are associated with one KaY. Only one of those participants can act as the Key Server at a time. MIs for the others are included in its Live Peer List.

Each ~~CA member~~ participant advertises the status of the receive SAs and its transmit SA. The Key Server will enable transmission for its transmit SA, immediately if it was not previously transmitting or receiving, and when all live peers report that they can receive using the corresponding SAK and AN otherwise. The other ~~CA members~~ participants enable transmission when they see that the Key Server is transmitting using the SAK and AN. See the CP state machine (12.4, Figure 12-2).

Insert the following new text immediately prior to 9.10.1, renumbering the prior NOTE as NOTE-2:

When MKA is used in conjunction with an XPN Cipher Suite, an SSCI is required for each SA. As specified in IEEE Std 802.1AE, the SA with the numerically greatest SCI uses the SSCI value 0x00000001, that with the next to the greatest SCI uses the SSCI value 0x00000002, and so on. The value 0x00000000 is not used.

NOTE 3—The XPN Cipher Suites and the derivation of SSCIs from SCI values were first specified in the IEEE Std 802.1AEbw-2013 amendment to IEEE Std 802.1AE.

PAEs that implement MKA Version 3 (or higher) order the MIs in the Live Peer List of transmitted MKPDUs. The MI associated with the numerically greatest SCI occurs first in the list, that with the next to greatest SCI second, and so on. The Key Server's own MI is not included in the Live Peer List. The SSID of the Key Server is also encoded in each MKPDU used to distribute an SAK for an XPN Cipher Suite, and indicates not only the value to be used by the Key Server, but also is corresponding to the position that it would otherwise occupy in the list. This information allows a receiving participant to determine the SCI to SSCI mappings for the transmit SAs used by it and each of the participants in the MKPDU's Live Peer List that are also in its own Live Peer List, even if those lists differ as a result of MKPDU loss or delay.

On receipt of a Version 3 or higher MKPDU distributing an SAK for an XPN Cipher Suite, a PAE implementing MKA Version 3 determines SSCI values as follows. The Key Server's SA takes the SSCI value explicitly encoded in the Live Peer List in the MKPDU. The SSCIs are then assigned in order to each of the SAs. The MI values that have a position ordinally lower than the Key Server's SSCI are given their ordinal value. The MI values that have a position in the Live Peer List of the Key Server's SSCI or greater are given an SSCI of their ordinal value + 1. So, for example, if the Key Server's transmit SA's SSCI is 0x00000002 and there are three MI values in the MKPDU Live Peer List, then their transmit SA's SSCIs are 0x00000001, 0x00000003, and 0x00000004 respectively. A receive SA is not created for any MI that is not in the Live List of a participant receiving a distributed SAK, but the ordered Live List from the MKPDU distributing that SAK is retained so the receive SA can be created when an MKPDU with that MI, proving liveness and conveying an SCI, is received.

NOTE 4—Since SSCIs are assigned sequentially and MKPDUs can only convey information for a limited number of participants, only the least significant octet of the Key Server's SSCI is encoded in MKPDUs, each of the more significant octets have the value 0x00.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

9.10.1 MKPDU application data

Insert the following new text after the existing text of 9.10.1:

PAEs that implement MKA Version 3 (or higher) order the MIs in the Live Peer List of transmitted MKPDUs as specified above (9.10), and encode the Key Server's transmit SA's SSCI in every MKPDU used to distribute an SAK for an XPN Cipher Suite.

Change the first paragraph of 9.10.1 as follows:

Each CA member encodes the following information in every MKPDU transmitted, for ~~both~~ the latest ~~(most recent) AN in use or about to be used,~~ and the old ~~(prior)~~ AN:

Change the second paragraph of 9.10.1 as follows:

A fixed format encoding is ~~supported by an 'In Service' flag, indicating that the fields for the respective SA are being~~ used. For convenience, these fields can be identified by the names and acronyms ~~Latest In Service/Old In Service (LIS/OIS),~~ Latest AN, Old AN (LAN, OAN), Latest Key Identifier/Old Key Identifier (LKI/OKI), Lowest Acceptable PN for the Latest Key/Lowest Acceptable PN for the Old Key (LLPN/OLPN), Latest Receiving/Old Receiving (LRX/ORX), Latest Transmitting/Old Transmitting (LTX/OTX).

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

Change 9.11 as follows:

9.11 Connectivity change detection

Changes in CA membership represent changes in the topology of a network that would be accompanied by link level indications, if the connectivity association represented by the CA were a LAN supported directly by media access method specific procedures, modeled by changes in the MAC_Operational and OperPointToPointMAC status parameters (IEEE Std 802.1~~D~~AC, IEEE Std 802.1Q). The SecY that operates MACsec detects some of the conditions that cause such topology changes, and notifies the client of its Controlled Port through changes in the status parameters. Some of the changes that the SecY cannot detect are unimportant, and require no exceptional measures, while other information about CA membership can be accessed through the LMI to optimize the operation of certain client protocols—loss of connectivity to a Designated Router or Designated Bridge (for example) might be detected by MACsec more rapidly than by those protocols. A more significant change is the creation of new connectivity, which can only be detected by client protocols when it has occurred as opposed to when it is about to occur. New connectivity that is not signaled by MAC_Operational can cause temporary data loops in bridged networks, while a TRUE-FALSE-TRUE transition in MAC_Operational has the defined effect (for spanning tree protocols) of re-initializing state machines to deal with new connectivity.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

11. EAPOL PDUs

11.1 EAPOL PDU transmission, addressing, and protocol identification

Change the introductory text of 11.1 and the accompanying NOTEs as follows:

EAPOL PDUs are transmitted and received using the service provided by an LLC entity that uses, in turn, a single instance of the MAC Service provided at an MSAP. Each EAPOL PDU is transmitted as a single MAC service request, and received as a single MAC service indication, with the following parameters:

a) Destination address (11.1.1)
b) Source address (11.1.2)
c) MSDU
d) Priority (11.1.3)

The MSDU of each request and indication is the EAPOL MPDU (MAC Protocol Data Unit). This MPDU comprises an Ethertype protocol identification header (11.1.4) followed by the EAPOL PDU proper (11.3).

NOTE 1—For the purposes of this standard, the term "LLC entity" includes entities that support protocol discrimination using the Ethertype field as specified in IEEE Std 802~~a-2003 [B2]~~.

NOTE 2—The complete format of an EAPOL frame 'on the wire' or 'through the air' depends not only on the EAPOL MPDU format, as specified in this clause, but also on the procedures (both media access method dependent and independent) used to support the MAC Service in a particular application scenario, as specified in Clause 7. Clause 7 includes the interface stack specifications necessary for interoperability, these do not add VLAN tags to transmitted frames prior to submitting them to media access method dependent procedures unless tagging is shown explicitly.

11.1.1 Destination MAC address

Change the second paragraph of 11.1.1, the following bullets, and the NOTE as follows:

Where a group destination address is used, the choice of address depends on the potential scope of the connectivity association that includes the desired peer entities, and a given system could choose to use EAPOL in connectivity associations with potentially different scopes. Subclause 7.7 and IEEE Std 802.1AE-2006 Clause 11 discuss the use of MACsec to secure both access to a provider network and transmission between systems attached to that network. IEEE ~~Std 802.1D,~~ IEEE Std 802.1Q~~, and their amendments~~ recognizes connectivity associations between peer MAC service users with the following scopes:

a) Within a LAN or VLAN that potentially encompasses the whole of a Bridged Local Area Network. Connectivity between individual LANs in the network might be supported by one or more Provider Bridged Networks or Provider Backbone Networks, but the connectivity association typically excludes systems that compose those supporting networks.
b) Within a customer's LAN, and bounded by MAC Bridges~~ (IEEE Std 802.1D)~~, VLAN Bridges, or end stations.
c) Within a provider's LAN forming part of a Provider Bridged Network, or within a LAN providing access for a customer to a provider, and bounded by MAC Bridges, VLAN Bridges, Provider Bridges, Provider Backbone Edge Bridges, Provider Backbone Bridges, or end stations.
d) Within an individual LAN supporting the MAC service using media dependent access methods, and bounded by end stations and all systems that use media independent protocols or media dependent convergence protocols to support the MAC service, including MAC Bridges, VLAN Bridges, Provider Bridges, Provider Backbone Edge Bridges, Provider Backbone Bridges, and TPMRs.

~~NOTE—TPMRs (Two Port MAC Relays) are being specified by IEEE Std 802.1aj [B3].~~

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

Replace Table 11-1 with the following table:

Table 11-1—EAPOL group address assignments

Address assignment	Address value	Filtered by:[a]				
		EDE-CC Edge components				
			MAC Bridge & C-VLAN components[b]			
				PEB C-VLAN component w/ single PEP[c]		
					S-VLAN components	
						TPMR components
EDE-CC PEP Address[d]	01-80-C2-00-00-1F	Y				
Bridge Group Address, Nearest Customer Bridge group address[e]	01-80-C2-00-00-00	Y	Y			
EDE-SS PEP Address[e, f]	01-80-C2-00-00-0B	Y	Y	Y		
Nearest non-TPMR Bridge group address, IEEE Std 802.1X PAE address[e, g]	01-80-C2-00-00-03	Y	Y	Y	Y	
Individual LAN Scope group address, Nearest Bridge group address[e, h]	01-80-C2-00-00-0E	Y	Y	Y	Y	Y

[a]Y indicates, Yes, this address is filtered by the component.

[b]Including a C-VLAN component that supports more than one provider network service instance (multiple PEPs) in a PEB.

[c]As specified in IEEE Std 802.1Q.

[d]This address is assigned in Table 15-1 of IEEE Std 802.1AE as amended by IEEE Std 802.1AEcg-2017.

[e]These addresses are assigned in Table 8-1, Table 8-2, and Table 8-3 of IEEE Std 802.1Q.

[f]Address filtering by an EDE-SS Edge component is specified in IEEE Std 802.1AE as amended by IEEE Std 802.1AEcg-2017.

[g]Identified as the Nearest non-TPMR Bridge group address in IEEE Std 802.1Q, and as the 802.1X PAE address in IEEE 802.1Q-2003, 802.1Q-2005, and this standard..

[h]It is intended that no IEEE 802.1 relay device will be defined that will forward frames that carry this destination address.

11.11 EAPOL-MKA

Change the third paragraphs of 11.11 as follows:

MKPDU encoding, validation, and decoding follows EAPOL's versioning rules (11.2, 11.5). The Basic Parameter Set includes an MKA Version Identifier that (with other parameters in the basic set) advertises the capabilities of the transmitting MKA implementation. This information can be supplemented both by version specific parameters within the basic set and by optional sets. A consistent TLV encoding identifies each set and allows it to be skipped if unrecognized by the receiver. Addition of parameters to existing sets, and the addition of parameter sets whose support is mandatory for a given version, will be accompanied by an MKA Version Identifier increment. This standard specifies the use of MKA Version Identifier ~~2~~ 3.

Insert a new NOTE after the existing NOTE-2 as follows:

NOTE 3—The MKA Version Identifier was incremented to 3 by the IEEE Std 802.1Xck-2017 amendment to this standard which did not add any new parameter sets but imposed an ordering on entries in the Live Peer List and added the Key Server SSCI to the Live Peer List parameter set (9.10, Figure 11-9).

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

Change Table 11-7 as follows:

Table 11-7—MKPDU parameter sets

Parameter set and Parameter set type		Version		Parameters	Version			Parameter specification
		1[a]	2, 3		1[a]	2	3	
Basic Parameter Set See Figure 11-8	[b] –	M	M	MKA Version Identifier	M	M	M	11.11
				Key Server Priority	M	M	M	9.5
				Key Server	M	M	M	9.5.1
				MACsec Desired	M	M	M	9.6.1
				MACsec Capability	M	M	M	9.6.1
				SCI	M	M	M	IEEE Std 802.1AE
				Actor's Member Identifier	M	M	M	
				Actor's Message Number	M	M	M	
				Algorithm Agility	M	M	M	
				CAK Name	M	M	M	9.3.1, 6.2.2, 6.3.3
Live Peer List See Figure 11-9	1	M	M	Member Identifier, Message Number tuples	M	M	M	9.4.3, 9.10
				Key Server's SSCI	—	—	M[c]	9.10
Potential Peer List See Figure 11-9	2	M	M	Member Identifier, Message Number tuples	M	M	M	9.4.3
MACsec SAK Use See Figure 11-10	3	M	M	Latest Key AN	M	M	M	9.8, 9.10
				Latest Key tx	M	M	M	9.10
				Latest Key rx	M	M	M	9.10
				Old Key AN	M	M	M	9.10
				Old Key tx	M	M	M	9.10
				Old Key rx	M	M	M	9.10
				Plain tx	M	M	M	—
				Plain rx	M	M	M	—
				Delay protect	M	M	M	9.10.1
				Latest Key Identifier (Key Server Member Identifier, Key Number)	M	M	M	9.8, 9.10.1
				Latest Key Lowest Acceptable PN	M	M	M	9.8, 9.10.1
				Old Key Identifier (Key Server Member Identifier, Key Number)	M	M	M	9.8, 9.10.1
				Old Key Lowest Acceptable PN	M	M	M	9.8, 9.10.1

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

Table 11-7—MKPDU parameter sets *(continued)*

Parameter set and Parameter set type		Version		Parameters	Version			Parameter specification
		1[a]	2, 3		1[a]	2	3	
Distributed SAK See Figure 11-11, Figure 11-12	4	M	M	AES Key Wrap of SAK	M	M	M	9.8
				Distributed AN	M	M	M	9.9
				Offset Confidentiality		M	M	9.7
				Key Number	M	M	M	9.8
				MACsec Cipher Suite	M	M	M	9.7
Distributed CAK See Figure 11-13	5	M	M	AES Key Wrap of CAK	M	M	M	9.5
				CA Key Name	M	M	M	9.3.1
KMD See Figure 11-14	6	M	M	KMD	M	M	M	12.6
Announcement See Figure 11-15	7	O[d]	O	Announcement TLVs	M	M	M	11.12
XPN	8	—	O[e]	MKA suspension time	—	M	M	9.18
				Latest Key: Lowest Acceptable PN (msbs)	—	M	M	
				Old Key: Lowest Acceptable PN (msbs)	—	M	M	
ICV Indicator See Figure 11-17		M[f]	M[f]	—	—			11.11.3,11.11.4

[a]M = mandatory to implement. O = optional. – = ignore on receipt.

[b]The Basic Parameter Set is identified by its position at the start of the MKPDU, the first octet encodes the MKA Version Identifier.

[c]Only encoded in MKPDUs that contain a Distributed SAK, and ignored on receipt otherwise.

[d]Mandatory to implement if EAPOL-Announcements are sent (5.10 (i)).

[e]Mandatory to implement if support for Extended Packet Numbering is claimed (5.11.4).

[f]The ICV Indicator will not be encoded unless the Algorithm Agility parameter specifies the use of an ICV that is not 16 octets in length (11.11.3) and there is no requirement to implement such an algorithm, however 11.11.4 states the requirement for processing the parameter set should it be received.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

Change Figure 11-9 as follows:

Bit: 8	7	6	5	4	3	2	1	Octet:
Parameter set type = 1 or 2								1
~~X~~ Key Server's SSCI[a]								2
X	X	X	X	Parameter set body length				3
Parameter set body length (cont)								4
Member Identifier								5 – 16
Message Number								17 – 20
Member Identifier								b
Message Number								

Figure 11-9—Live Peer List and Potential Peer List parameter sets

[a]The least-significant octet of the Key Server's transmit SSCI is encoded in MKPDUs containing a Distributed SAK parameter set for use with an XPN Cipher Suite, otherwise 0 is encoded. The Key Server's SSCI is distributed only in Live Peer Lists, and is transmitted as zero and ignored on receipt in Potential Peer Lists.

[b]Member Identifier, Message Number tuples are repeated to the end of the parameter set.

11.11.3 Encoding MKPDUs

Change the first sentence of 11.11.3 as follows:

An implementation that transmits MKPDU PDUs with an MKA Version Identifier of 1, 2, or 3 shall encode the protocol parameters provided by the KaY as follows:

Change the text of bullet c) of 11.11.3 as follows:

c) If there are one or more Live Peers, their Member Identifier, Message Number tuples are encoded within a Live Peer List as specified in Figure 11-9. An implementation that transmits MKPDUs with an MKA Version Identifier of 3 shall order the entries in the Live Peer List, and shall encode the least significant octet of the Key Server's SSCI in Octet 2 of the Live Peer List parameter set of MKPDUs containing a Distributed SAK parameter set for use with an XPN Cipher Suite, as specified in 9.10.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

12. PAE operation

Change 12.9.2 as follows:

12.9.2 Identifying PAEs and their capabilities

Each PAE and its major components and capabilities are identified by the following variables:

- portNumber: Each PAE is uniquely identified by a port number (see IEEE Std 802.1AC ~~D.4~~). The port number used is unique amongst all port numbers for the system, and directly or indirectly identifies the Uncontrolled Port that supports the PAE. If the PAE has been dynamically instantiated to support an existing or potential virtual port, this portNumber, the uncontrolledPortNumber and the controlledPortNumber are allocated by the real port's PAE, and this portNumber is the uncontrolledPortNumber. If the PAE supports a real port, this portNumber is the commonPortNumber for the associated PAC or SecY.
- portType: Either RealPort or VirtualPort.
- controlledPortNumber: The port number for the associated PAC or SecY's Controlled Port.
- uncontrolledPortNumber: The port number for the associated PAC or SecY's Uncontrolled Port.
- commonPortNumber: The port number for the associated PAC or SecY's Common Port. All the virtual ports created for a given real port share the same Common Port and commonPortNumber.

  NOTE—These port numbers, with the value constraints specified, not only allow each PAE and the associated ports to be identified uniquely, but also allow a network manager to locate the real port PAE responsible for instantiating a given virtual port, and the virtual ports instantiated for a given real port.

- eapolGroupAddress: The group address used for EAPOL frames (including MKA frames). For a virtual port instantiated by a real port PAE, the same as that for the real port PAE.
- implemented.supp: Set iff a PACP EAP Supplicant is implemented (Clause 8).
- implemented.auth: Set iff a PACP EAP Authenticator is implemented (Clause 8).
- implemented.mka: Set iff MKA is implemented.
- implemented.macsec: Set iff the Controlled Port is supported by MACsec.
- implemented.isupgrades: Set iff the MKA supports in-service upgrades (9.18).
- implemented.announcements: Set iff EAPOL announcement can be sent.
- implemented.listener: Set iff received EAPOL announcements can be used.
- implemented.virtualPorts: Set for a RealPort iff virtual ports are implemented.

If a RealPort has implemented virtual ports, the following information may be provided:

- maxVirtualPorts: The guaranteed maximum number of virtual ports.
- currentVirtualPorts: The current number of virtual ports.

Change Figure 12-3 as follows:

Copyright © 2018 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
This is an unapproved IEEE Standards draft, subject to change.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

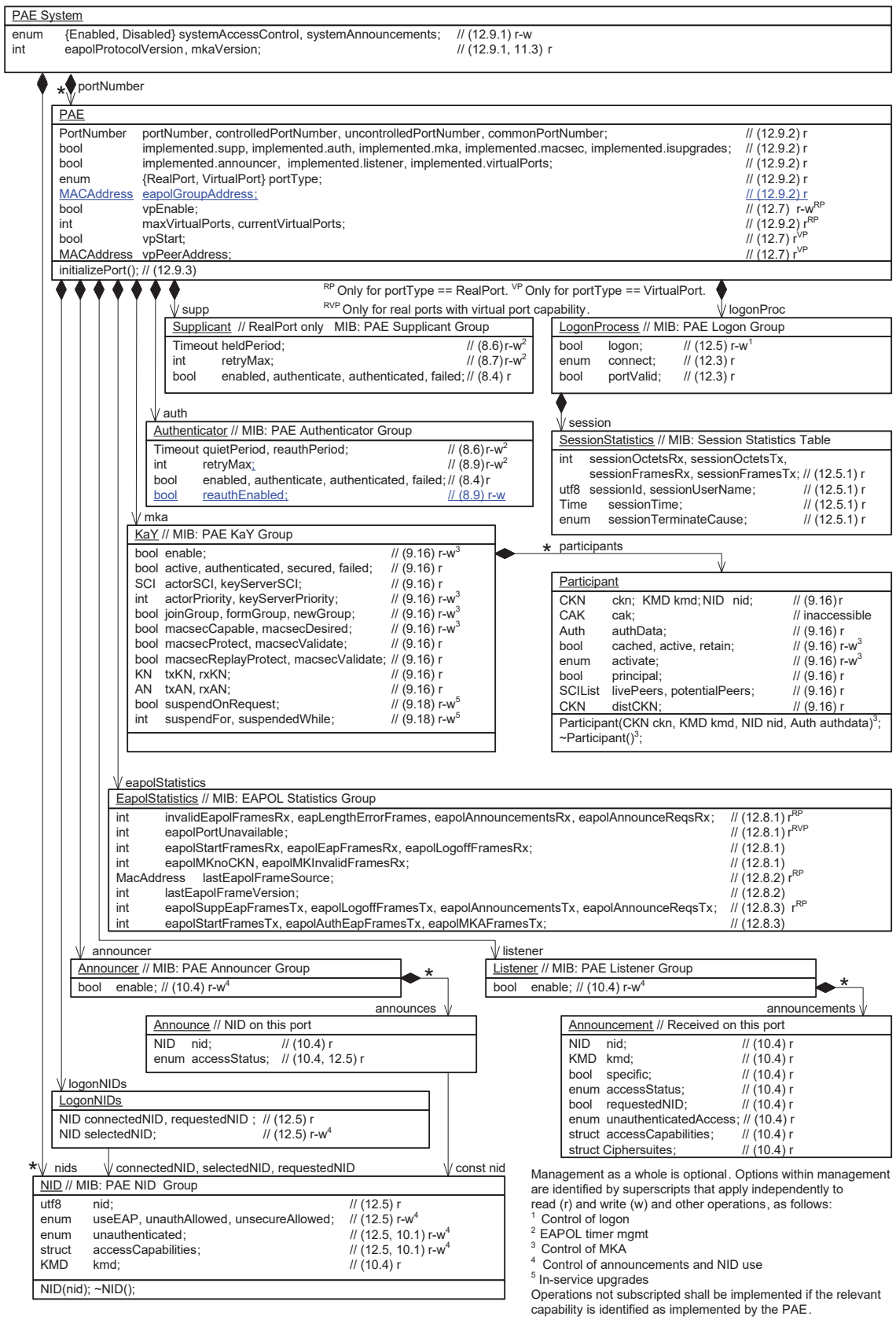


Figure 12-3—PAE management information

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

13. PAE MIB

Change the following row in Table 13-4 after vpStart:

Table 13-4—PAE managed object cross-reference table

PAE management information (Figure 12-3)	MIB object(s)
vpPeerAddress (12.17) r	ieee8021XPaePortVirtualPortPeerMAC~~Address~~

Insert the following rows into Table 13-4 after commonPortNumber:

Table 13-4—PAE managed object cross-reference table

PAE management information (Figure 12-3)	MIB object(s)
eapolGroupAddress (12.9.2) r	ieee8021XPaeEapolGroupMAC

13.4 Security considerations

Change the NOTE as follows:

NOTE—The IEEE 802.1Xbx amendment to this standard added the in-service upgrade (9.18) group (ieee8021XPaeKaYIsupgradeGroup). The IEEE 802.1Xck amendment added the EAPOL Group Address used by each PAE (12.9.2) (ieee8021XPaeEapolGroup).Th~~is~~ese additions do~~es~~ not affect the security considerations to be taken into account when making use of this standard.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

13.5 Definitions for PAE MIB

Delete the entire text of the MIB definition, following the introductory sentence, and insert the following text:

```
-- ****************************************************************
--
-- IEEE8021X-PAE-MIB : IEEE 802.1X (802.1X-2010 + 802.1Xbx + 802.1Xck)
--
-- ****************************************************************

IEEE8021X-PAE-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Gauge32,
    Counter32,
    Counter64,
    Unsigned32,
    Integer32
        FROM SNMPv2-SMI
    MacAddress,
    TEXTUAL-CONVENTION,
    TruthValue,
    RowPointer,
    TimeStamp,
    TimeInterval,
    RowStatus
        FROM SNMPv2-TC
    MODULE-COMPLIANCE,
    OBJECT-GROUP
        FROM SNMPv2-CONF
    SnmpAdminString
        FROM SNMP-FRAMEWORK-MIB
    InterfaceIndex
        FROM IF-MIB
    SecySCI
        FROM IEEE8021-SECY-MIB;

ieee8021XPaeMIB MODULE-IDENTITY
    LAST-UPDATED    "201710281457Z"
    ORGANIZATION    "IEEE 802.1 Working Group"
    CONTACT-INFO
      " WG-URL: http://grouper.ieee802.org/1
        WG-EMail: stds-802-1-L@ieee.org
        Contact: IEEE 802.1 Working Group Chair
        Postal: C/O IEEE 802.1 Working Group
                IEEE Standards Association
                445 Hoes Lane
                P.O. Box 1331
                Piscataway
                NJ 08855-1331
                USA
                E-mail: STDS-802-1-L@LISTSERV.IEEE.ORG"
    DESCRIPTION
        "The MIB module for managing the Port Access Entity (PAE)
        functions of IEEE 802.1X (Revision of 802.1X-2004).
        The PAE functions managed are summarized in Figure 12-3 of
        IEEE 802.1X and include EAPOL PACP support for authentication
        (EAP Supplicant and/or Authenticator), MACsec Key Agreement
        (MKA), EAPOL, and transmission and reception of network
        announcements.

        The following acronyms and definitions are used in this MIB.

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


Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

Announcer : EAPOL-Announcement transmission functionality.

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

CA : secure Connectivity Association: 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.

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

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

Common Port : An instance of the MAC Internal Sublayer Service used by the SecY or PAC 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 PAC or SecY.

CP state machine : Controlled Port state machine is capable of controlling a SecY or a PAC. The CP supports interoperability with unauthenticated systems that are not port-based network access control capable, or that lack MKA. When the access controlled port is supported by a SecY, the CP is capable of controlling the SecY so as to provide unsecured connectivity to systems that implement a PAC.

EAP : Extensible Authentication Protocol, RFC3748.

EAPOL : EAP over LANs.

KaY : Key Agreement Entity, a PAE entity responsible for MKA.

Key Server : Elected by MKA, to transport a succession of SAKs, for use by MACsec, to the other member(s) of a CA.

KMD : Key Management Domain, a string identifying systems that share cached CAKs.

Listener : The role is to receive the network announcement parameters in the authentication process.

Logon Process : The Logon Process is responsible for the managing the use of authentication credentials, for initiating use of the PAE's Supplicant and or Authenticator functionality, for deriving CAK, CKN tuples from PAE results, for maintaining PSKs (Pre-Sharing Keys), and for managing MKA instances. In the absence of successful authentication, key agreement, or support for MAC Security, the Logon Process determines whether the CP state machine should provide unauthenticated connectivity or authenticated but unsecured connectivity.

MKA : MACsec Key Agreement protocol allows PAEs, each associated with a port that is an authenticated member of a secure connectivity association (CA) or a potential CA, to discover other PAEs attached to the same LAN, to confirm mutual possession of a CAK and hence to prove a past mutual authentication, to agree the secret keys (SAKs) used by MACsec for symmetric shared key cryptography, and to ensure that the data protected by MACsec has not been delayed.

MKPDU : MACsec Key Agreement Protocol Data Unit.

MPDU : MAC Protocol Data Unit.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT

NID : Network Identity, a UTF-8 string identifying an network or network service.

PAE : Port Access Entity, the protocol entity associated with a Port. It can support the protocol functionality associated with the Authenticator, the Supplicant, or both.

PAC : Port Access Controller, a protocol-less shim that provides control over frame transmission and reception by clients attached to its Controlled Port, and uses the MAC Service provided by a Common Port. The access control decision is made by the PAE, typically taking into account the success or failure of mutual authentication and authorization of the PAE's peer(s), and is communicated by the PAE using the LMI to set the PAC's Controlled Port enabled/disable. Two different interfaces 'Controlled Port' and 'Uncontrolled Port', are associated with a PAC, and that for each instance of a PAC, two ifTable rows (one for each interface) run on top of an ifTable row representing the 'Common Port' interface, such as a row with ifType = 'ethernetCsmacd(6)'.

For example :

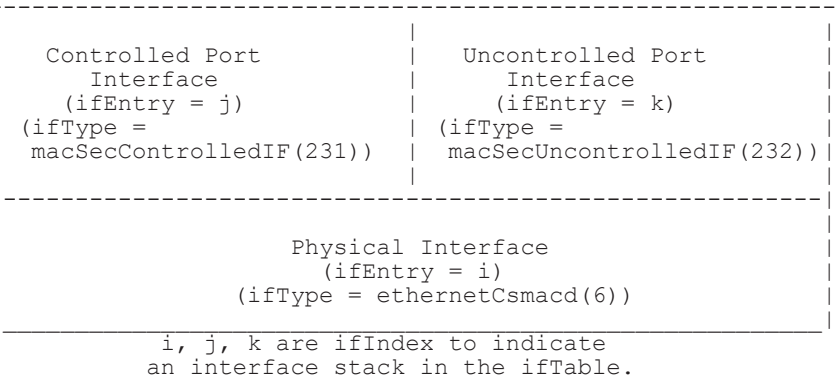


Figure : PAC Interface Stack

The 'Controlled Port' is the service point to provide one instance of the secure MAC service in a PAC. The 'Uncontrolled Port' is the service point to provide one instance of the insecure MAC service in a PAC.

PACP : Port Access Controller Protocol.

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.

Real Port : Indicates the PAE is for a real port. A port that is not created on demand by the mechanisms specified in this standard, but that can transmit and receive frames for one or more virtual ports.

SC : Secure Channel, 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.

SA : Secure Association, 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.

Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT


```
        SAK : Secure Association key, the secret key used by an SA.

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

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

        SecY : MAC Security Entity, the entity that operates the MAC
            Security protocol within a system.

        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.

        Suspension: Temporary suspension of MKA operation to facilitate
            in-service control plane software upgrades without
            disrupting existing secure connectivity.

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

        Virtual Port : Indicates the PAE is for a virtual port.  A MAC
            Service or Internal Sublayer service access point that is
            created on demand.  Virtual ports can be used to provide
            separate secure connectivity associations over the same
            LAN."
    REVISION        "201710281457Z"
    DESCRIPTION
        "Published as part of IEEE 802.1Xck.
         Minor DESCRIPTION clarifications as required by resolution
         of maintenance items 154, 155, 157 (see 802.1 maintenance
         process discussion). Added ieee8021XPaeEapolGroupMAC Address."
    REVISION        "201404101619Z"
    DESCRIPTION
        "Update published as part of IEEE 802.1Xbx (Amendment to
        IEEE 802.1X-2010)"
    REVISION        "200910011650Z"
    DESCRIPTION
        "Initial version of this MIB module.  Published as part of
        IEEE P802.1X (Revision of IEEE Standard 802.1X-2009)"
    ::= { iso(1) iso-identified-organization(3) ieee(111)
          standards-association-numbered-series-standards(2)
          lan-man-stds(802) ieee802dot1(1) ieee802dot1mibs(1) 15 }

-- ------------------------------------------------------------------ --
-- Textual Conventions
-- ------------------------------------------------------------------ --

Ieee8021XPaeCKN ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "This textual convention indicates the CAK name to identify
        the Connectivity Association Key (CAK) which is the root key
        in the MACsec Key Agreement key hierarchy.  All potential
        members of the CA use the same CKN."

    REFERENCE       "IEEE 802.1X Clause 5.4, Clause 9.3.1, Clause 6.2"
    SYNTAX          OCTET STRING (SIZE (1..16))

Ieee8021XPaeCKNOrNull ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "This textual convention indicates the CAK name to identify
        the Connectivity Association Key (CAK) which is the root key
        in the MACsec Key Agreement key hierarchy.  All potential
        members of the CA use the same CKN.

        If this is a zero length value, then the NULL string means
        CKN information is applicable."

    REFERENCE       "IEEE 802.1X Clause 5.4, Clause 9.3.1, Clause 6.2"
```


Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT


```
    SYNTAX          OCTET STRING (SIZE (0..16))

Ieee8021XPaeKMD ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "This textual convention indicates a Key Management Domain
        (KMD).

        KMD is a string of UTF-8 characters that names the transmitting
        authenticator's key management domain."

    REFERENCE       "IEEE 802.1X Clause 12.6"
    SYNTAX          OCTET STRING (SIZE (0..253))

Ieee8021XPaeNID ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "This textual convention indicates a Network Identifier (NID).

        Each network is identified by a NID, a UTF-8 string used by
        network attached systems to select a network profile."

    REFERENCE       "IEEE 802.1X Clause 12.6, Clause 10.1"
    SYNTAX          OCTET STRING (SIZE (1..100))

Ieee8021XPaeNIDOrNull ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "This textual convention indicates a Network Identifier (NID).

        Each network is identified by a NID, a UTF-8 string used by
        network attached systems to select a network profile.

        If this is a zero length value, then the NULL string for
        NID information is applicable."

    REFERENCE       "IEEE 802.1X Clause 12.6, Clause 10.1"
    SYNTAX          OCTET STRING (SIZE (0..100))

Ieee8021XMkaKeyServerPriority ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "This textual convention indicates a Key Server priority
        information.

        Each MKA participant encodes a Key Server Priority, an 8-bit
        integer, in each MKPDU.  Each participant selects the live
        participant advertising the highest priority as its Key Server
        provided that participant has not selected another as its Key
        Server or is unwilling to act as the Key Server.  If a Key
        Server cannot be selected SAKs are not distributed.  In the
        event of a tie for highest priority Key Server, the member with
        the highest priority SCI is chosen.  For consistency with other
        uses of the SCI's MAC Address component as a priority,
        numerically lower values of the Key Server Priority and SCI are
        accorded the highest priority.  The Table 9-2 contains
        recommendations for the use of priority values for various
        system roles. Participants that will never act as a Key Server
        should advertise priority 0xFF."

    REFERENCE       "IEEE 802.1X Clause 9.5, Table 9-2"
    SYNTAX          OCTET STRING (SIZE (1))

Ieee8021XMkaMI ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "This textual convention indicates a Member Identifier (MI).

        The MI is a 96-bit random value chosen when the MKA Instance
        begins, used with a 32-bit MN to protect against replay attacks
        and to record liveliness in the Live Peer List or potential
        liveliness in the Potential Peer List. If the MN wraps, a new
```


Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Documents Document Sharing Hub
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...

APPROVED DRAFT


```
        random MI value is chosen and the MN begins again at 1."

    REFERENCE       "IEEE 802.1X Clause 9.4.2"
    SYNTAX          OCTET STRING (SIZE (12))

Ieee8021XMkaMN ::= TEXTUAL-CONVENTION
    DISPLAY-HINT    "d"
    STATUS          current
    DESCRIPTION
        "This textual convention indicates a Member Number (MN).

        The MN is a 32-bit value which begins at 1 and increases for
        each MKPDU transmitted.  It is used with the MI to protect
        against replay attacks and to record liveliness in the Live
        Peers List or potential liveliness in the Potential Peer List.
        If the MN wraps, a new random MI value is chosen and the MN
        begins again at a value of 1."

    REFERENCE       "IEEE 802.1X Clause 9.4.2"
    SYNTAX          Unsigned32 (1..2147483648)

Ieee8021XMkaKN ::= TEXTUAL-CONVENTION
    DISPLAY-HINT    "d"
    STATUS          current
    DESCRIPTION
        "This textual convention indicates a Key Number (KN) used in
        MKA.

        The MN is a 32-bit integer assigned by that Key Server
        (sequentially, beginning with 1)."

    REFERENCE       "IEEE 802.1X Clause 9.8"
    SYNTAX          Unsigned32 (1..2147483648)

Ieee8021XPaeNIDCapabilites ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "This textual convention indicates the combinations of
        authentication and protection capabilities supported for a
        NID. Any set of these combinations can be supported."

    REFERENCE       "IEEE 802.1X Clause 10.1, Table 11-8"
    SYNTAX          BITS {
                        eap(0),
                        eapMka(1),
                        eapMkaMacSec(2),
                        mka(3),
                        mkaMacSec(4),
                        higherLayer(5), -- WebAuth
                        higherLayerFallback(6), -- WebAuth
                        vendorSpecific(7)
                    }

Ieee8021XPaeNIDAccessStatus ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        "This textual convention indicates the transmitter's
        Controlled Port operational status and current level of
        access resulting from authentication and the consequent
        authorization controls applied by that port's clients.

        'noAccess' : Other than to authentication services, and to
            services announced as available in the absence of
            authentication (unauthenticated).

        'remedialAccess' : The access granted is severely limited,
            possibly to remedial services.

        'restrictedAccess' : The Controlled Port is operational, but
            restrictions have been applied by the network that can
            limit access to some resources.
```


Copyright © 2018 IEEE. All rights reserved.
This is an unapproved IEEE Standards draft, subject to change.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 28,2026 at 19:08:45 UTC from IEEE Xplore. Restrictions apply.
Full document details: P802.1Xck/D2.2, Jul 2018 - IEEE Approved Draft Standard for Local and Metropolitan Area Networks - Port-Based Network Access Co...