INTERNATIONAL STANDARD

ISO/IEC/IEEE 8802-1X

First edition
2013-12-01

AMENDMENT 2
2020-11

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

Part 1X: Port-based network access control

AMENDMENT 2: YANG data model

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

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

AMENDEMENT 2: Modèle de données YANG

Reference number
ISO/IEC/IEEE 8802-1X:2013/Amd.2:2020(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

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

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

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted (see www.iso.org/directives).

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

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

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

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

ISO/IEC/IEEE 8802-1X:2013/Amd 2 was prepared by the LAN/MAN of the IEEE Computer Society (as IEEE Std 802.1Xck-2018) and drafted in accordance with its editorial rules. It was adopted, under the "fast-track procedure" defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

IEEE Std 802.1Xck™-2018
(Amendment to IEEE Std 802.1X™-2010
as amended by IEEE Std 802.1Xbx™-2014)

IEEE 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

Approved 27 September 2018

IEEE-SA Standards Board

Abstract: The YANG data model specified in this amendment to IEEE Std 802.1X™-2010 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™-2018, using the information model previously specified in this standard.

Keywords: amendment, authorized port, confidentiality, data model, data origin authenticity, IEEE 802.1X™, IEEE 802.1Xck™, 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

PDF: ISBN 978-1-5044-5213-7 STD23338
Print: ISBN 978-1-5044-5214-4 STDPD23338

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents." They can also be obtained on request from IEEE or viewed at https://standards.ieee.org/ipr/disclaimers.html.

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

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

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

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

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

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

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

Translations

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

Official statements

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

Comments on standards

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

Comments on standards should be submitted to the following address:

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

Laws and regulations

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

Copyrights

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

Photocopies

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

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. A current 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 IEEE Xplore at https://ieeexplore.ieee.org 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 https://standards.ieee.org.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: https://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 https://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.

Participants

At the time this amendment was submitted to the IEEE-SA Standards Board for approval, the IEEE 802.1 Working Group had the following membership:

Glenn Parsons, *Chair*
John Messenger, *Vice Chair*
Marc Holness, *Editor*
Mick Seaman, *Security Task Group Chair, Editor*

SeoYoung Baek
Shenghua Bao
Jens Bierschenk
Steinar Bjornstad
Christian Boiger
Paul Bottorff
David Chen
Feng Chen
Weiying Cheng
Rodney Cummings
János Farkas
Norman Finn
Geoffrey Garner
Eric W. Gray
Craig Gunther
Marina Gutierrez
Stephen Haddock
Mark Hantel
Patrick Heffernan
Lu Huang
Tony Jeffree
Michael Johas Teener
Hal Keen
Stephan Kehrer
Philippe Klein
Jouni Korhonen
Yizhou Li
Christophe Mangin
Tom McBeath
James McIntosh
Tero Mustala
Hiroki Nakano
Bob Noseworthy
Donald R. Pannell
Walter Pienciak
Michael Potts
Karen Randall
Maximilian Riegel
Dan Romascanu
Jessy V. Rouyer
Eero Ryytty
Soheil Samii
Behcet Sarikaya
Frank Schewe
Johannes Specht
Wilfried Steiner
Patricia Thaler
Paul Unbehagen
Hao Wang
Karl Weber
Brian Weis
Jordon Woods
Nader Zein
Helge Zinner
Juan Carlos Zuniga

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

Thomas Alexander
Butch Anton
Stefan Aust
Harry Bims
David Black
Nancy Bravin
Demetrio Bucaneg
William Byrd
Daniel Conte
Charles Cook
Richard Doyle
Sourav Dutta
János Farkas
Michael Fischer
Matthias Fritsche
Yukihiro Fujimoto
Eric W. Gray
Randall Groves
Stephen Haddock
Marco Hernandez
David Hess
Werner Hoelzl
Rita Horner
Noriyuki Ikeuchi
Osamu Ishida
Atsushi Ito
Raj Jain
Sangkwon Jeong
Piotr Karocki
Stuart Kerry
Evgeny Khorov
Yongbum Kim
Hyeong Ho Lee
James Lepp
Jon Lewis
Michael Lynch
Elvis Maculuba
Richard Mellitz
Michael Montemurro
Rick Murphy
Michael Newman
Nick S. A. Nikjoo
Satoshi Obara
Bansi Patel
Michael Peters
Clinton Powell
Karen Randall
Alon Regev
Maximilian Riegel
Robert Robinson
Jessy V. Rouyer
Frank Schewe
Mick Seaman
Di Dieter Smely
Daniel Smith
Thomas Starai
Walter Struppler
Mark-Rene Uchida
Dmitri Varsanofiev
George Vlantis
Hao Wang
Karl Weber
Brian Weis
Andreas Wolf
Chun Yu Charles Wong
Oren Yuen
Zhen Zhou

When the IEEE-SA Standards Board approved this amendment on 27 September 2018, it had the following membership:

Jean-Philippe Faure, *Chair*
Gary Hoffman, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Ted Burse
Guido R. Hiertz
Christel Hunter
Joseph L. Koepfinger*
Thomas Koshy
Hung Ling
Dong Liu
Xiaohui Liu
Kevin Lu
Daleep Mohla
Andrew Myles
Paul Nikolich
Ronald C. Petersen
Annette D. Reilly
Robby Robson
Dorothy Stanley
Mehmet Ulema
Phil Wennblom
Philip Winston
Howard Wolfman
Jingyi Zhou

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802.1Xck-2018, 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™-2018, 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 the IEEE 802.1X state machine and state machines 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, adds authenticated key agreement in support of IEEE 802.1AE™ MAC Security (MACsec) and clarifies and generalizes the relationship between the common architecture specified for port-based network access control and the functional elements and protocols that support that architecture as specified in IEEE Std 802.1X, other IEEE 802® standards, and IETF RFCs. Further changes update the standard to reflect best current practice, insisting, for example, on mutual authentication methods and using such methods in examples. A greater emphasis is placed on the security of systems accessing the network, as well as on 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 MACsec and/or MACsec Key Agreement protocol (MKA) 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 with respect to some existing implementations, not needing to support IEEE Std 802.1AE and already conforming to best current practice as of 2010, will continue to refer to IEEE Std 802.1X-2004. 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 is the first amendment to IEEE Std 802.1X-2010. Its MKA extensions make additional security and manageability capabilities possible based on the changes made by IEEE Std 802.1AEbw™-2013 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, in-service control plane software can be upgraded.

Contents

Figures

Tables

IEEE 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 italics***. Four editing instructions are used: change, delete, insert, and replace. ***Change*** is used to make corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using ~~strikethrough~~ (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Deletions and insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editing instructions, change markings, and this note will not be carried over into future editions because the changes will be incorporated into the base standard.[1]

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 6733 [B26]) or RADIUS (IETF RFC 2865 [B5]). Attributes supporting certain port-based network access control scenarios are described in IETF RFC 3580 [B13], IETF RFC 4675 [B17], ~~and~~ IETF RFC 4849 [B18], and IETF RFC 7268 [B28].[2]

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

[2] The numbers in brackets preceded by the letter B correspond to the numbers in the bibliography in Annex B.

1.4 Provisions of this standard

Change 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 F (informative) uses the same concepts to describe the architectural modeling of unsecured multi-access LANs, a widely deployed form of authenticated port-based network access control that does not meet the security requirements of this standard. Administrative connectivity to unauthenticated devices, as required for use of industry standard 'Wake-on-LAN' (WoL) protocols, is described for the scenarios of Clause 7; Annex E (informative) provides background information on WoL.

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

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

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

The basic architectural concepts, such as 'port', on which this standard relies are reviewed in IEEE Std 802.1AC ~~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 D (informative) provides EAP and RADIUS usage guidelines.

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

2. Normative references

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

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

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

~~IEEE Std 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.

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.

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.

IEEE Std 802.3™, IEEE Standard for Ethernet.

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

[3] https://www.iana.org/assignments/iana-if-type/iana-if-type.xhtml.
[4] IEEE publications are available from The Institute of Electrical and Electronics Engineers (https://www.standards.ieee.org).
[5] The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.

~~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., and Waldbusser, S., April 1999.[6]

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

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

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

IETF RFC 3394, Advanced Encryption Standard (AES) Key Wrap Algorithm, Schaad, J., and Housley, R., 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, Diercks, T., Rescorla, E., April 2006.~~

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

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

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

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

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

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

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

ISO/IEC 18033-3: 2010, Information technology—Security techniques—Encryption algorithms—Part 3:Block ciphers.[7]

NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions, Chen, L., November 2008.[8]

[6] IETF RFCs are available from the Internet Engineering Task Force (https://www.ietf.org/rfc.html).

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

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

3. Definitions

Change the following definitions in Clause 3 as shown:

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).

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

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)~~.

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

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 correspond to any other identifier, index, or port number. There can be more than one SC for a physical port, identifying frames transmitted by separate virtual ports, and more than one SC for a physical or virtual port if that port uses different SCs to transmit frames of different priorities.

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.

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

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

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.

Insert the following term and definition into Clause 3 in alphabetic order:

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

5. Conformance

5.3 Conformant systems and system components

Change 5.3 as follows:

This clause (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.

5.4 PAE requirements

Change 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) ~~c)~~ Implement the Logon Process functionality specified in 12.5.
c) ~~d)~~ Implement the CP state machine as specified in 12.4.
d) ~~e)~~ Maintain and allow retrieval of the EAPOL frame reception statistics specified in 12.8.1.
e) ~~f)~~ Maintain and allow retrieval of the EAPOL frame reception diagnostics specified in 12.8.2.

f) ~~g)~~ Maintain and allow retrieval of the EAPOL frame transmission statistics specified in 12.8.3.
g) ~~h)~~ Support the system configuration functions specified in 12.9.

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

h) ~~i)~~ 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) ~~j)~~ 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) ~~k)~~ 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 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).

5.12 Virtual port requirements

Change the last paragraph 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 the following subclauses (5.23 and 5.24) after 5.22:

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.

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 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 Key hierarchy

6.2.2 Using EAP for CAK key derivation

Change the fourth paragraph of 6.2.2 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

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 Port Access Entity (PAE)

6.3.6 Multi-access LANs

Change the note in 6.3.6 as follows:

NOTE—The addressing (individual or group) for each EAPOL Packet Type is specified in ~~Table J1-1 and~~ Table 11-4. For compatibility with prior revisions of this standard, Supplicants attached to IEEE 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 the introductory text 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

7. Port-based network access control applications

7.5 Host access with MACsec and a multi-access LAN

Change NOTE 1 and NOTE 3 in the introductory text of 7.5 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.

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.

8. Authentication using EAP

8.11 EAP methods

Insert the following paragraph at the end of the introductory text of 8.11:

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.

9. MACsec Key Agreement protocol (MKA)

9.2 Protocol support requirements

9.2.2 SC identification

Change 9.2.2 as follows:

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.

9.4 MKA transport

9.4.5 Addressing

Change 9.4.5 as follows:

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, make~~s it more difficult to~~ attack~~ing~~ MKA from a distance more difficult.

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 the introductory text 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 shall distribute 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 and NOTE 3 of the introductory text of 9.8 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.

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.

9.10 SAK installation and use

Change the first two paragraphs of the introductory text 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 IEEE Std 802.1AEcg-2016, 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).

Change the note ("Enforcement of ....") after the fourth paragraph of the introductory text of 9.10 to "NOTE 2."

Insert the following paragraphs after NOTE 2 in the introductory text of 9.10:

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 IEEE Std 802.1AEbw-2013.

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 occurs 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 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 convey information for only 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 has the value 0x00.

9.10.1 MKPDU application data

Change the beginning of 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).

Insert the following paragraph at the end 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.

9.11 Connectivity change detection

Change 9.11 as follows:

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.

11. EAPOL PDUs

11.1 EAPOL PDU transmission, addressing, and protocol identification

Change the introductory text of 11.1 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 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-2009 [B3].~~

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 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-2018.
[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 IEEE 802.1X PAE address in IEEE Std 802.1Q-2003, IEEE Std 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 paragraph in the introductory text 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 NOTE 3 after NOTE 2 in the introductory text of 11.11:

NOTE 3—The MKA Version Identifier was incremented to 3 by IEEE Std 802.1Xck-2018, which did not add any new parameter sets to this standard but did impose an ordering on entries in the Live Peer List and add the Key Server SSCI to the Live Peer List parameter set (9.10, Figure 11-9).

11.11.1 MKA parameter encoding

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

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[de]	O	Announcement TLVs	M	M	M	11.12
XPN	8	—	O[ed]	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[fe]	M[fe]					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] [e] Mandatory to implement if EAPOL-Announcements are sent [5.10 i)].

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

[f] [e] 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.

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 ~~a~~
Message Number								

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

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

11.11.3 Encoding MKPDUs

Change the beginning of the first paragraph 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 list item 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.

12. PAE operation

12.9 PAE management

Change Figure 12-3 as shown on the next page.

12.9.2 Identifying PAEs and their capabilities

Change 12.9.2 as follows:

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 among 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.

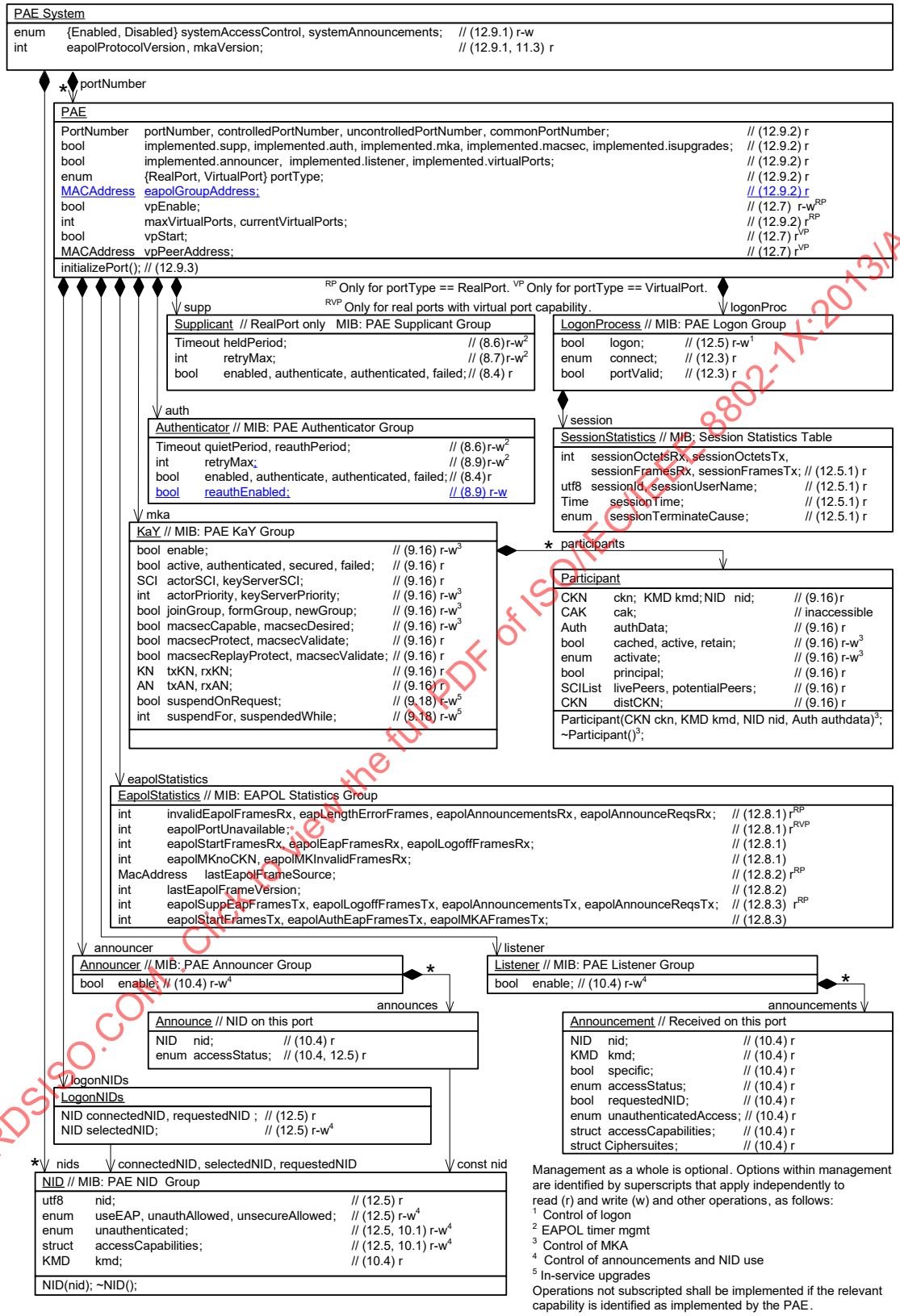


Figure 12-3—PAE management information

13. PAE MIB

13.2 Structure of the MIB

Change the following row of Table 13-4 as shown:

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 row into Table 13-4 after the commonPortNumber row:

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 in 13.4 as follows:

NOTE—IEEE Std 802.1Xbx-2014 added the in-service upgrade (9.18) group (ieee8021XPaeKaYIsupgradeGroup) to this standard. IEEE Std 802.1Xck-2018 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.

13.5 Definitions for PAE MIB

After the introductory paragraph of 13.5, delete the entire text of the MIB definition, 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).

            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.

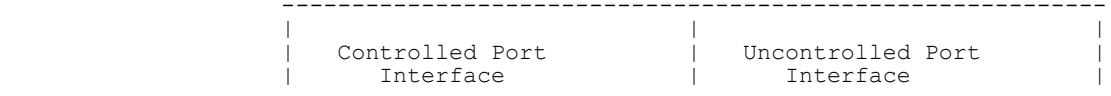
MPDU : MAC Protocol Data Unit.

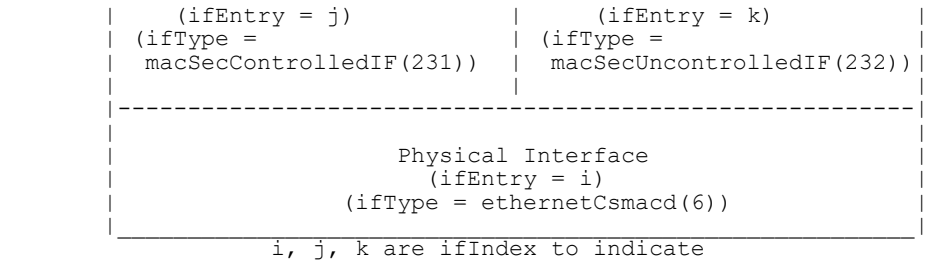
NID : Network Identity, a UTF-8 string identifying an network or network service.

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 :





i, j, k are ifIndex to indicate
an interface stack in the ifTable.
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.

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"
    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
        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.

        ‘expectedAccess’ : The Controlled Port is operational, and
            access provided is as expected for successful
            authentication and authorization for the NID.”

    REFERENCE       “IEEE 802.1X Clause 10.1, Table 11-8”
    SYNTAX          INTEGER  {
                        noAccess(0),
                        remedialAccess(1),
                        restrictedAccess(2),
                        expectedAccess(3)
                    }

Ieee8021XPaeNIDUnauthenticatedStatus ::= TEXTUAL-CONVENTION
    STATUS          current
    DESCRIPTION
        “This textual convention indicates the access capabilities of
        the port’s clients without authentication.

        ‘noAccess’ : Other than to authentication services (see
            Ieee8021XPaeNIDCapabilites information.

        ‘fallbackAccess’ : Limited access can be provided after
            authentication failure.

        ‘limitedAccess’ : Immediate limited access is available
            without authentication.

        ‘openAccess’ : Immediate access is available without
            authentication.”
```

```
    REFERENCE       "IEEE 802.1X Clause 10.1, Table 11-8"
    SYNTAX          INTEGER  {
                        noAccess(0),
                        fallbackAccess(1),
                        limitedAccess(2),
                        openAccess(3)
                    }

-- ---------------------------------------------------------- --
-- Groups in the IEEE 802.1X MIB
-- ---------------------------------------------------------- --

ieee8021XPaeMIBNotifications  OBJECT IDENTIFIER
    ::= { ieee8021XPaeMIB 0 }

ieee8021XPaeMIBObjects  OBJECT IDENTIFIER
    ::= { ieee8021XPaeMIB 1 }

ieee8021XPaeMIBConformance  OBJECT IDENTIFIER
    ::= { ieee8021XPaeMIB 2 }

-- ---------------------------------------------------------- --
-- Management Objects in the IEEE 802.1X MIB
-- ---------------------------------------------------------- --

ieee8021XPaeSystem  OBJECT IDENTIFIER
    ::= { ieee8021XPaeMIBObjects 1 }

ieee8021XPaeLogon  OBJECT IDENTIFIER
    ::= { ieee8021XPaeMIBObjects 2 }

ieee8021XPaeAuthenticator  OBJECT IDENTIFIER
    ::= { ieee8021XPaeMIBObjects 3 }

ieee8021XPaeSupplicant  OBJECT IDENTIFIER
    ::= { ieee8021XPaeMIBObjects 4 }

ieee8021XPaeEapol  OBJECT IDENTIFIER
    ::= { ieee8021XPaeMIBObjects 5 }

ieee8021XPaeKaY  OBJECT IDENTIFIER
    ::= { ieee8021XPaeMIBObjects 6 }

ieee8021XPaeNetworkIdentifier  OBJECT IDENTIFIER
    ::= { ieee8021XPaeMIBObjects 7 }


-- ---------------------------------------------------------- --
-- The 802.1X PAE System Group
-- ---------------------------------------------------------- --
--
-- ---------------------------------------------------------- --
-- The 802.1X PAE System Objects
-- ---------------------------------------------------------- --

ieee8021XPaeSysAccessControl OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "This object enables or disables port-based network access
        control for all the system's ports.  Setting this control
        object to 'false' causes the following actions :
            . Deletes any virtual ports previously instantiated.
            . Terminates authentication exchanges and MKA instances'
              operation.
            . Each real port PAE behaves as if no virtual ports
              created.
            . All the PAEs' Supplicant, Authenticator, and KaY are
              disabled.
            . Logon Process(es) behave as if the object
```

```
                ieee8021XNidUnauthAllowed was 'immediate'.
              . Announcements can be transmitted, both periodically and
                in response to announcement requests (conveyed by
                EAPOL-Starts or EAPOL-Announcement-Reqs) but are sent
                with a single NULL NID.
              . Objects announcementAccessStatus and announceAccessStatus
                have the 'noAccess' value, announcementAccessRequested is
                'false', object announcementUnauthAccess has the
                'openAccess' value.

            The control variable settings for each real port PAE in the
            ieee8021XPaePortTable are unaffected, and will be used once the
            object is set to 'true'.

            This configured value for this object shall be stored in
            persistent memory and remain unchanged across a
            re-initialization of the management system of the entity."
        REFERENCE
            "IEEE 802.1X Clause 12.9.1, Figure 12-3 PAE
                System.systemAccessControl"
        ::= { ieee8021XPaeSystem 1 }

    ieee8021XPaeSysAnnouncements OBJECT-TYPE
        SYNTAX          TruthValue
        MAX-ACCESS      read-write
        STATUS          current
        DESCRIPTION
            "Setting this control object to 'false' causes each PAE in this
            system to behave as if the PAE's Announcement functionality is
            disabled.  The independent controls for each PAE apply if
            this object is 'true'.

            This configured value for this object shall be stored in
            persistent memory and remain unchanged across a
            re-initialization of the management system of the entity."
        REFERENCE
            "IEEE 802.1X Clause 12.9.1, Figure 12-3 PAE
                System.systemAnnouncements"
        ::= { ieee8021XPaeSystem 2 }

    ieee8021XPaeSysEapolVersion OBJECT-TYPE
        SYNTAX          Unsigned32
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The EAPOL protocol version for this system."
        REFERENCE
            "IEEE 802.1X Clause 12.9.1, Clause 11.3, Figure 12-3 PAE
                System.eapolProtocolVersion"
        ::= { ieee8021XPaeSystem 3 }

    ieee8021XPaeSysMkaVersion OBJECT-TYPE
        SYNTAX          Unsigned32
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The MKA protocol version for this system."
        REFERENCE       "IEEE 802.1X Clause 12.9.1"
        ::= { ieee8021XPaeSystem 4 }
    -- ------------------------------------------------------------------ --
    -- The 802.1X PAE Port Table
    -- ------------------------------------------------------------------ --

    ieee8021XPaePortTable OBJECT-TYPE
        SYNTAX          SEQUENCE OF Ieee8021XPaePortEntry
        MAX-ACCESS      not-accessible
        STATUS          current
        DESCRIPTION
            "A table of system level information for each port supported by
            the Port Access Entity.  An entry appears in this table for
            each port of this system.
```

```
        For the writeable objects in this table, the configured value
        shall be stored in persistent memory and remain unchanged
        across a re-initialization of the management system of the
        entity."
    REFERENCE       "802.1X Clause 12.9.2, Figure 12-3 PAE"
    ::= { ieee8021XPaeSystem 5 }

ieee8021XPaePortEntry OBJECT-TYPE
    SYNTAX          Ieee8021XPaePortEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "The Port number, protocol version, and
        initialization control for a Port.

         If the PAE has been dynamically instantiated to support an
         existing or potential virtual port, the Uncontrolled Port
         interface and Controlled Port interface are allocated by the
         real port's PAE."
    INDEX           { ieee8021XPaePortNumber }
    ::= { ieee8021XPaePortTable 1 }

Ieee8021XPaePortEntry ::= SEQUENCE {
        ieee8021XPaePortNumber               InterfaceIndex,
        ieee8021XPaePortType                 INTEGER,
        ieee8021XPaeControlledPortNumber     InterfaceIndex,
        ieee8021XPaeUncontrolledPortNumber   InterfaceIndex,
        ieee8021XPaeCommonPortNumber         InterfaceIndex,
        ieee8021XPaePortInitialize           TruthValue,
        ieee8021XPaePortCapabilities         BITS,
        ieee8021XPaePortVirtualPortsEnable   TruthValue,
        ieee8021XPaePortMaxVirtualPorts      Unsigned32,
        ieee8021XPaePortCurrentVirtualPorts Gauge32,
        ieee8021XPaePortVirtualPortStart     TruthValue,
        ieee8021XPaePortVirtualPortPeerMAC  MacAddress,
        ieee8021XPaePortLogonEnable          TruthValue,
        ieee8021XPaePortAuthenticatorEnable TruthValue,
        ieee8021XPaePortSupplicantEnable     TruthValue,
        ieee8021XPaePortKayMkaEnable         TruthValue,
        ieee8021XPaePortAnnouncerEnable      TruthValue,
        ieee8021XPaePortListenerEnable       TruthValue,
        ieee8021XPaeEapolGroupMACMacAddress
}

ieee8021XPaePortNumber OBJECT-TYPE
    SYNTAX          InterfaceIndex
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "An interface index indicates the port number associated with
        this port.  Each PAE is uniquely identified by a port number.
        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 indicates a real port, ieee8021XPaePortType object
        in the same row is 'realPort', the port number shall be the
        same as the ieee8021XPaeCommonPortNumber object in the same row
        for the associated PAC or SecY.

        If the PAE indicates a virtual port, ieee8021XPaePortType
        object in the same row is 'virtualPort', this port number
        should be the same as the uncontrolledPortNumber object in the
        same row for the associated PAC or SecY."
    REFERENCE       "802.1X Clause 12.9.2, Figure 12-3"
    ::= { ieee8021XPaePortEntry 1 }

ieee8021XPaePortType OBJECT-TYPE
    SYNTAX          INTEGER  {
                        realPort(1),
                        virtualPort(2)
                    }
```

```
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The port type of the PAE.

        realPort(1) : indicates the PAE is for a real port.

        virtualPort(2) : indicates the PAE is for a virtual port."
    REFERENCE       "802.1X Clause 12.9.2, Figure 12-3"
    ::= { ieee8021XPaePortEntry 2 }

ieee8021XPaeControlledPortNumber OBJECT-TYPE
    SYNTAX          InterfaceIndex
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "An interface index indicates the port number associated with
        PAC or SecY's Controlled Port."
    REFERENCE       "802.1X Clause 12.9.2, Figure 12-3"
    ::= { ieee8021XPaePortEntry 3 }

ieee8021XPaeUncontrolledPortNumber OBJECT-TYPE
    SYNTAX          InterfaceIndex
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "An interface index indicates the port number associated with
        PAC or SecY's Uncontrolled Port.  If the PAE supports a
        real port, this port number can be the same as the
        ieee8021XPaeCommonPortNumber object in the same row, otherwise
        it shall not be the same."
    REFERENCE       "802.1X Clause 12.9.2, Figure 12-3"
    ::= { ieee8021XPaePortEntry 4 }

ieee8021XPaeCommonPortNumber OBJECT-TYPE
    SYNTAX          InterfaceIndex
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "An interface index indicates the port number associated with
        PAC or SecY's 'Common Port'.  All the virtual ports created
        for a given real port share the same 'Common Port' and
        ieee8021XPaeCommonPortNumber in the same row."
    REFERENCE       "802.1X Clause 12.9.2, Figure 12-3"
    ::= { ieee8021XPaePortEntry 5 }

ieee8021XPaePortInitialize OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "The initialization control for this Port. Setting this object
        'true' causes the Port to be reinitialized, terminating (and
        potentially restarting) authentication exchanges and MKA
        operation.

        If the port is a real port, any virtual ports previously
        instantiated are deleted.  Virtual ports can be reinstantiated
        through normal protocol operation.

        The object value reverts to 'false' once initialization
        has completed."
    REFERENCE       "802.1X Clause 12.9.3, Figure 12-3"
    ::= { ieee8021XPaePortEntry 6 }

ieee8021XPaePortCapabilities OBJECT-TYPE
    SYNTAX          BITS {
                        suppImplemented(0),
                        authImplemented(1),
                        mkaImplemented(2),
                        macsecImplemented(3),
                        announcementsImplemented(4),
```

```
                        listenerImplemented(5),
                        virtualPortsImplemented(6)
                    }
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The capabilities of this PAE port.

        'suppImplemented' : A PACP EAP supplicant functions are
            implemented in this PAE if this bit is on.

        'authImplemented' : A PACP EAP authenticator functions are
            implemented in this PAE if this bit is on.

        'mkaImplemented' : The KaY MKA functions are implemented
            in this PAE if this bit is on.

        'macsecImplemented' : The MACsec functions in the
            Controlled Port are implemented in this PAE if this
            bit is on.

        'announcementsImplemented' : The EAPOL announcement can be
            sent in this PAE if this bit is on.

        'listenerImplemented' : This PAE can receive EAPOL announcement
            if this bit is on.

        'virtualPortsImplemented' : Virtual Port functions are
            implemented in this PAE if this bit is on."
    REFERENCE       "802.1X Clause 12.9.2, Figure 12-3"
    ::= { ieee8021XPaePortEntry 7 }

ieee8021XPaePortVirtualPortsEnable OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "Enable or disable to Virtual Ports function for this Real Port
        PAE, the object ieee8021XPaePortType in the same row has the
        value 'realPort'.  If this PAE is not a Real Port, this object
        should be read only and returns 'false'.

        This object will be read only and returns 'false' if the value
        of the object ieee8021XPaePortCapabilities in the same row has
        the bit 'virtualPortsImplemented' off."
    REFERENCE       "802.1X Clause 12.8.1, Figure 12-3"
    ::= { ieee8021XPaePortEntry 8 }

ieee8021XPaePortMaxVirtualPorts OBJECT-TYPE
    SYNTAX          Unsigned32
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The maximum number of virtual ports can be supported in this
        port."
    REFERENCE       "802.1X Clause 12.9.2, Figure 12-3"
    ::= { ieee8021XPaePortEntry 9 }

ieee8021XPaePortCurrentVirtualPorts OBJECT-TYPE
    SYNTAX          Gauge32
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The current number of virtual ports is running in this port."
    REFERENCE       "802.1X Clause 12.9.2, Figure 12-3"
    ::= { ieee8021XPaePortEntry 10 }

ieee8021XPaePortVirtualPortStart OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
```

```
        "This object will be 'true' if the virtual port is created by
        receipt of an EAPOL-Start packet."
    REFERENCE       "802.1X Clause 12.7, Figure 12-3"
    ::= { ieee8021XPaePortEntry 11 }

ieee8021XPaePortVirtualPortPeerMAC OBJECT-TYPE
    SYNTAX          MacAddress
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The source MAC address of the received EAPOL-Start if
        ieee8021XPaePortVirtualPortStart is set 'true'.

        If ieee8021XPaePortVirtualPortStart is not 'true' in the same
        row, the value of this object should be 00-00-00-00-00-00."
    REFERENCE       "802.1X Clause 12.7, Figure 12-3"
    ::= { ieee8021XPaePortEntry 12 }

ieee8021XPaePortLogonEnable OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "Enable or disable to transmit network announcement
        information."
    REFERENCE       "802.1X Clause 12.5, Figure 12-3"
    ::= { ieee8021XPaePortEntry 13 }

ieee8021XPaePortAuthenticatorEnable OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "True if the Authenticator is enabled.

        This object is read only. It returns 'false' if the value
        of the object ieee8021XPaePortCapabilities in the same row has
        the bit 'authImplemented' Off, or if the local control variable
        'enable' has not been set by the Logon Process."
    REFERENCE       "802.1X Clause 8.4 'enabled', Figure 12-3"
    ::= { ieee8021XPaePortEntry 14 }

ieee8021XPaePortSupplicantEnable OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "True if the Suppplicant is enabled.

        This object is read only. It returns 'false' if the PAE lacks
        supplicant functionality (ieee8021XPaePortCapabilities in the
        same row has the bit 'suppImplemented' off), or if the local
        control variable'enable' has not been set by the Logon Process
        (perhaps because the supplicant is designed to authenticate a
        human user and that user is not present)."
    REFERENCE       "802.1X Clause 8.4 'enabled', Figure 12-3"
    ::= { ieee8021XPaePortEntry 15 }

ieee8021XPaePortKayMkaEnable OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "Enable or disable the MKA protocol function in this PAE.

        This object will be read only and returns 'false' if the value
        of the object ieee8021XPaePortCapabilities in the same row has
        the bit 'mkaImplemented' off."
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    ::= { ieee8021XPaePortEntry 16 }

ieee8021XPaePortAnnouncerEnable OBJECT-TYPE
```

```
        SYNTAX          TruthValue
        MAX-ACCESS      read-write
        STATUS          current
        DESCRIPTION
            "Enable or disable the network Announcer function in this PAE.

            This object will be read only and returns 'false' if the value
            of the object ieee8021XPaePortCapabilities in the same row has
            the bit 'announcementsImplemented' off."
        REFERENCE       "802.1X Clause 10.4, Figure 12-3"
        ::= { ieee8021XPaePortEntry 17 }

    ieee8021XPaePortListenerEnable OBJECT-TYPE
        SYNTAX          TruthValue
        MAX-ACCESS      read-write
        STATUS          current
        DESCRIPTION
            "Enable or disable the network Listener function in this PAE.

            This object will be read only and returns 'false' if the value
            of the object ieee8021XPaePortCapabilities in the same row has
            the bit 'listenerImplemented' off."
        REFERENCE       "802.1X Clause 10.4, Figure 12-3"
        ::= { ieee8021XPaePortEntry 18 }

    ieee8021XPaeEapolGroupMAC OBJECT-TYPE
        SYNTAX          MacAddress
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The destination Group MAC Address used by this PAE when
            transmitting EAPOL frames."
        REFERENCE       "802.1X Clause 12.9, Figure 12-3"
        ::= { ieee8021XPaePortEntry 19 }


    -- ------------------------------------------------------------------ --
    -- The 802.1X PAC Port Table
    -- ------------------------------------------------------------------ --

    ieee8021XPacPortTable OBJECT-TYPE
        SYNTAX          SEQUENCE OF Ieee8021XPacPortEntry
        MAX-ACCESS      not-accessible
        STATUS          current
        DESCRIPTION
            "A table of system level information for each interface
            supported by PAC.

            This table will be instantiated if the value of the object
            ieee8021XPaePortCapabilities in the corresponding entry of the
            ieee8021XPaePortTable has the bit 'macsecImplemented' off.

            For the writeable objects in this table, the configured value
            shall be stored in persistent memory and remain unchanged
            across a re-initialization of the management system of the
            entity."
        REFERENCE       "IEEE 802.1X Clause 6.4, Clause 14"
        ::= { ieee8021XPaeSystem 6 }

    ieee8021XPacPortEntry OBJECT-TYPE
        SYNTAX          Ieee8021XPacPortEntry
        MAX-ACCESS      not-accessible
        STATUS          current
        DESCRIPTION
            "An entry containing PAC management information applicable to
            a particular interface."
        INDEX           { ieee8021XPacPortControlledPortNumber }
        ::= { ieee8021XPacPortTable 1 }

    Ieee8021XPacPortEntry ::= SEQUENCE {
            ieee8021XPacPortControlledPortNumber    InterfaceIndex,
            ieee8021XPacPortAdminPt2PtMAC           INTEGER,
```

```
        ieee8021XPacPortOperPt2PtMAC            TruthValue
}

ieee8021XPacPortControlledPortNumber OBJECT-TYPE
    SYNTAX          InterfaceIndex
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "The index to identify the 'Controlled Port' interface for a PAC."
    REFERENCE       "IEEE 802.1X Clause 6.4"
    ::= { ieee8021XPacPortEntry 1 }

ieee8021XPacPortAdminPt2PtMAC OBJECT-TYPE
    SYNTAX          INTEGER  {
                        forceTrue(1),
                        forceFalse(2),
                        auto(3)
                    }
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "An object to control the service connectivity to at most one
        other system.  The ieee8021XPacPortOperPt2PtMAC indicates
        operational status of the service connectivity for this PAC.

        'forceTrue' : allows only one service connection to the
                      other system.

        'forceFalse' : no restriction on the number of service
                       connections to the other systems.

        'auto' : means the service connectivity is determined by the
                 service providing entity."
    REFERENCE       "IEEE 802.1X Clause 6.4"
    DEFVAL          { auto }
    ::= { ieee8021XPacPortEntry 2 }

ieee8021XPacPortOperPt2PtMAC OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "An object to reflect the current service connectivity status.

        'true' : means the service connectivity of this PAC
             Controlled Port provides at most one other system.

        'false' : means the service connectivity of this PAC could
             provide more than one other system."
    REFERENCE       "IEEE 802.1X Clause 6.4"
    ::= { ieee8021XPacPortEntry 3 }


-- ---------------------------------------------------------------- --
-- The 802.1X PAE Logon Process Group
-- ---------------------------------------------------------------- --
--
-- ---------------------------------------------------------------- --
-- The 802.1X PAE Logon Process Table
-- ---------------------------------------------------------------- --

ieee8021XPaePortLogonTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF Ieee8021XPaePortLogonEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "A table of system level information for each port to support
        the Logon Process(es) status information.

        This table will be instantiated if the object
        ieee8021XPaePortLogonEnable in the corresponding entry of the
        ieee8021XPaePortTable is 'true'."
```

```
    REFERENCE       "802.1X Clause 12.5, Figure 12-3"
    ::= { ieee8021XPaeLogon 1 }

ieee8021XPaePortLogonEntry OBJECT-TYPE
    SYNTAX          Ieee8021XPaePortLogonEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "An entry contains Logon Process status information for the
        PAE."
    INDEX           { ieee8021XPaePortNumber }
    ::= { ieee8021XPaePortLogonTable 1 }

Ieee8021XPaePortLogonEntry ::= SEQUENCE {
        ieee8021XPaePortLogonConnectStatus INTEGER,
        ieee8021XPaePortPortValid          TruthValue
}

ieee8021XPaePortLogonConnectStatus OBJECT-TYPE
    SYNTAX          INTEGER  {
                        pending(1),
                        unauthenticated(2),
                        authenticated(3),
                        secure(4)
                    }
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The Logon Process sets this variable to one of the following
        values, to indicate to the CP state machine if, and how,
        connectivity is to be provided through the Controlled Port :

        'pending' : Prevent connectivity by disabling the
            Controlled Port of this PAE.

        'unauthenticated' : Provide unsecured connectivity, enabling
            the Controlled Port of this PAE.

        'authenticated' : Provide unsecured connectivity but with
            authentication, enabling Controlled Port of this PAE.

        'secure' : Provide secure connectivity, using SAKs provided by
            the KaY (when available) and enabling Controlled Port when
            those keys are installed and in use."
    REFERENCE       "802.1X Clause 12.3, Figure 12-3"
    ::= { ieee8021XPaePortLogonEntry 1 }

ieee8021XPaePortPortValid OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "This object will be set 'true' if Controlled Port communication
        is secured as specified by the MACsec."
    REFERENCE       "802.1X Clause 12.3, Figure 12-3"
    ::= { ieee8021XPaePortLogonEntry 2 }

-- ---------------------------------------------------------------------- --
-- The 802.1X PAE Session Table
-- ---------------------------------------------------------------------- --

ieee8021XPaePortSessionTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF Ieee8021XPaePortSessionEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "A table of system level information for each port to support
        Logon Process(es) session information.  This table maintains
        session statistics for its associated Controlled Port,
        suitable for communication to a RADIUS or other AAA server at
        the end of a session for accounting purpose.
```

```
        This table will be instantiated if the object
        ieee8021XPaePortLogonEnable in the corresponding entry of the
        ieee8021XPaePortTable is 'true'."
    REFERENCE       "802.1X Clause 12.5.1, Figure 12-3"
    ::= { ieee8021XPaeLogon 2 }

ieee8021XPaePortSessionEntry OBJECT-TYPE
    SYNTAX          Ieee8021XPaePortSessionEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "An entry contains Logon Process session information for the
        PAE.  A session, an entry, begins when the operation of
        Controlled Port becomes 'true' and ends when it becomes
        'false'.

        The counts of frames and octets can be derived from those
        maintained to support from Interface MIB counters for the
        SecY's or the PAC's Controlled Port, but differs in that the
        counts are zeroed when the session begins."
    INDEX           { ieee8021XPaeSessionControlledPortNumber }
    ::= { ieee8021XPaePortSessionTable 1 }

Ieee8021XPaePortSessionEntry ::= SEQUENCE {
        ieee8021XPaeSessionControlledPortNumber   InterfaceIndex,
        ieee8021XPaePortSessionOctetsRx           Counter64,
        ieee8021XPaePortSessionOctetsTx           Counter64,
        ieee8021XPaePortSessionPktsRx             Counter64,
        ieee8021XPaePortSessionPktsTx             Counter64,
        ieee8021XPaePortSessionId                 SnmpAdminString,
        ieee8021XPaePortSessionStartTime          TimeStamp,
        ieee8021XPaePortSessionIntervalTime       TimeInterval,
        ieee8021XPaePortSessionTerminate          INTEGER,
        ieee8021XPaePortSessionUserName           SnmpAdminString
}

ieee8021XPaeSessionControlledPortNumber OBJECT-TYPE
    SYNTAX          InterfaceIndex
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "The index to identify the 'Controlled Port' interface's session
        information for a PAE."
    REFERENCE       "802.1X Clause 12.5.1, Figure 12-3"
    ::= { ieee8021XPaePortSessionEntry 1 }

ieee8021XPaePortSessionOctetsRx OBJECT-TYPE
    SYNTAX          Counter64
    UNITS           "Octets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of octets received in this session of this PAE.

        Discontinuities in the value of this counter can occur at
        re-initialization of the management system, and at
        other times as indicated by the value of
        ieee8021XPaePortSessionStartTime."
    REFERENCE       "802.1X Clause 12.5.1, Figure 12-3"
    ::= { ieee8021XPaePortSessionEntry 2 }

ieee8021XPaePortSessionOctetsTx OBJECT-TYPE
    SYNTAX          Counter64
    UNITS           "Octets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of octets transmitted in this session of this PAE.

        Discontinuities in the value of this counter can occur at
        re-initialization of the management system, and at
```

```
            other times as indicated by the value of
            ieee8021XPaePortSessionStartTime."
        REFERENCE       "802.1X Clause 12.5.1, Figure 12-3"
        ::= { ieee8021XPaePortSessionEntry 3 }

    ieee8021XPaePortSessionPktsRx OBJECT-TYPE
        SYNTAX          Counter64
        UNITS           "Packets"
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The number of packets received in this session of this PAE.

            Discontinuities in the value of this counter can occur at
            re-initialization of the management system, and at
            other times as indicated by the value of
            ieee8021XPaePortSessionStartTime."
        REFERENCE       "802.1X Clause 12.5.1, Figure 12-3"
        ::= { ieee8021XPaePortSessionEntry 4 }

    ieee8021XPaePortSessionPktsTx OBJECT-TYPE
        SYNTAX          Counter64
        UNITS           "Packets"
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The number of packets transmitted in this session of this PAE.

            Discontinuities in the value of this counter can occur at
            re-initialization of the management system, and at
            other times as indicated by the value of
            ieee8021XPaePortSessionStartTime."
        REFERENCE       "802.1X Clause 12.5.1, Figure 12-3"
        ::= { ieee8021XPaePortSessionEntry 5 }

    ieee8021XPaePortSessionId OBJECT-TYPE
        SYNTAX          SnmpAdminString (SIZE  (3..253))
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The session identifier for this session of the PAE.  A UTF-8
            string, uniquely identifying the session within the context of
            the PAE's system."
        REFERENCE       "802.1X Clause 12.5.1, Figure 12-3"
        ::= { ieee8021XPaePortSessionEntry 6 }

    ieee8021XPaePortSessionStartTime OBJECT-TYPE
        SYNTAX          TimeStamp
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The starting time of this session."
        REFERENCE       "802.1X Clause 12.5.1, Figure 12-3"
        ::= { ieee8021XPaePortSessionEntry 7 }

    ieee8021XPaePortSessionIntervalTime OBJECT-TYPE
        SYNTAX          TimeInterval
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The duration time of the session has been last."
        REFERENCE       "802.1X Clause 12.5.1, Figure 12-3"
        ::= { ieee8021XPaePortSessionEntry 8 }

    ieee8021XPaePortSessionTerminate OBJECT-TYPE
        SYNTAX          INTEGER  {
                            macOperFailed(1),
                            sysAccessDisableOrPortInit(2),
                            receiveEapolLogOff(3),
                            eapReauthFailure(4),
                            mkaFailure(5),
                            newSessionBegin(6),
```

```
                        notTerminateYet(7)
                    }
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The reason for the session termination, one of the following :

        'macOperFailed' : 'Common Port' for this PAE is not
            operational.

        'sysAccessDisableOrPortInit' : The ieee8021XPaeSysAccessControl
            object is set to 'false' or initialization process of this
            PAE is invoked.

        'receiveEapolLogOff' : The PAE has received EAPOL-Logoff
            frame.

        'eapReauthFailure' : EAP reauthentication has failed.

        'mkaFailure' : MKA failure or other MKA termination.

        'newSessionBegin' : New session beginning.

        'notTerminateYet' : Not Terminated Yet."
    REFERENCE       "802.1X Clause 12.5.1, Figure 12-3"
    ::= { ieee8021XPaePortSessionEntry 9 }

ieee8021XPaePortSessionUserName OBJECT-TYPE
    SYNTAX          SnmpAdminString (SIZE  (0..253))
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The session user name for this session in the PAE.  A UTF-8
        string, representing the identity of the peer Supplicant.

        If no such information, zero length string will return."
    REFERENCE       "802.1X Clause 12.5.1, Figure 12-3"
    ::= { ieee8021XPaePortSessionEntry 10 }


-- ---------------------------------------------------------------- --
-- The 802.1X PAE Logon Process NID Table
-- ---------------------------------------------------------------- --

ieee8021XLogonNIDTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF Ieee8021XLogonNIDEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "The Logon Process may use Network Identities (NIDs) to manage
        its use of authentication credentials, cached CAKs, and
        announcements.  This table provides the NID information for
        Logon Process.

        For the writeable objects in this table, the configured value
        shall be stored in persistent memory and remain unchanged
        across a re-initialization of the management system of the
        entity."
    REFERENCE       "802.1X Clause 12.5, Figure 12-3"
    ::= { ieee8021XPaeLogon 3 }

ieee8021XLogonNIDEntry OBJECT-TYPE
    SYNTAX          Ieee8021XLogonNIDEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "An entry provides the NID information for a Logon Process."
    INDEX           { ieee8021XPaePortNumber }
    ::= { ieee8021XLogonNIDTable 1 }

Ieee8021XLogonNIDEntry ::= SEQUENCE {
        ieee8021XLogonNIDConnectedNID Ieee8021XPaeNID,
```

```
        ieee8021XLogonNIDRequestedNID Ieee8021XPaeNIDOrNull,
        ieee8021XLogonNIDSelectedNID  Ieee8021XPaeNIDOrNull
}

ieee8021XLogonNIDConnectedNID OBJECT-TYPE
    SYNTAX          Ieee8021XPaeNID
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The NID associated with the current connectivity (possibly
        unauthenticated) provided by the operation of the CP state
        machine.

        This object can differ from both the ieee8021XLogonNIDSelectedNID and
        the ieee8021XLogonNIDRequestedNID objects in the same row if
        authenticated connectivity (either secure or unsecured) has
        already been established, and EAP authentication and MKA
        operation for both of the latter have not met the necessary
        conditions (as specified by the control variables unauthAllowed
        and unsecureAllowed)."
    REFERENCE       "802.1X Clause 12.5, Figure 12-3"
    ::= { ieee8021XLogonNIDEntry 1 }

ieee8021XLogonNIDRequestedNID OBJECT-TYPE
    SYNTAX          Ieee8021XPaeNIDOrNull
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The NID marked as access requested in announcements, as
        determined from EAPOL-Start frames.  The default of this object
        is as the configured value of object ieee8021XLogonNIDSelectedNID.

        This object information provides context for the PAE's EAP
        Authenticator.  If no EAPOL-Start frame has been received since
        the PAE's 'Common Port' became operational, or the last
        EAPOL-Start frame received for the port did not contain a
        requested NID, the object will take on the value of the object
        ieee8021XLogonNIDSelectedNID in the same row."
    REFERENCE       "802.1X Clause 12.5, Figure 12-3"
    ::= { ieee8021XLogonNIDEntry 2 }

ieee8021XLogonNIDSelectedNID OBJECT-TYPE
    SYNTAX          Ieee8021XPaeNIDOrNull
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "The NID currently configured for use by an access 'Controlled
        Port' when transmitting EAPOL-Start frames.  The default of
        this object is empty string.

        This object may be either explicitly configured by management
        or determined by the PAE using NID selection algorithms.  If no
        authentication is in progress, and the current connectivity is
        terminated and then starts again, ieee8021XLogonNIDConnectedNID will
        take on the value of ieee8021XLogonNIDRequestedNID (though a PAE
        NID's election algorithm, if used, can subsequently select
        another NID)."
    REFERENCE       "802.1X Clause 12.5, Figure 12-3"
    DEFVAL          { "" }
    ::= { ieee8021XLogonNIDEntry 3 }


-- ---------------------------------------------------------------------- --
-- The PAE Authenticator Group
-- ---------------------------------------------------------------------- --
--
-- ---------------------------------------------------------------------- --
-- The 802.1X PAE Authenticator Table
-- ---------------------------------------------------------------------- --

ieee8021XAuthenticatorTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF Ieee8021XAuthenticatorEntry
```

```
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "A table that contains the configuration objects for the
        Authenticator PAE associated with each port.  This table will
        be instantiated if the object ieee8021XPaePortAuthenticatorEnable in
        the corresponding entry of the ieee8021XPaePortTable is 'true'.

        For the writeable objects in this table, the configured value
        shall be stored in persistent memory and remain unchanged
        across a re-initialization of the management system of the
        entity."
    REFERENCE       "802.1X Clause 8, Figure 12-3"
    ::= { ieee8021XPaeAuthenticator 1 }

ieee8021XAuthenticatorEntry OBJECT-TYPE
    SYNTAX          Ieee8021XAuthenticatorEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "An entry that contains the Authenticator configuration objects
        for the PAE."
    INDEX           { ieee8021XPaePortNumber }
    ::= { ieee8021XAuthenticatorTable 1 }

Ieee8021XAuthenticatorEntry ::= SEQUENCE {
        ieee8021XAuthPaeAuthenticate  TruthValue,
        ieee8021XAuthPaeAuthenticated TruthValue,
        ieee8021XAuthPaeFailed        TruthValue,
        ieee8021XAuthPaeReAuthEnabled TruthValue,
        ieee8021XAuthPaeQuietPeriod   Unsigned32,
        ieee8021XAuthPaeReauthPeriod  Unsigned32,
        ieee8021XAuthPaeRetryMax      Unsigned32,
        ieee8021XAuthPaeRetryCount    Gauge32
}

ieee8021XAuthPaeAuthenticate OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "This object will be set 'true' by the PAE authenticator to
        request authentication, and if this object is 'true',
        reauthentication is allowed.

        This object will be 'false' while the PAE authenticator revokes
        authentication."
    REFERENCE       "IEEE 802.1X Clause 8, Figure 12-3"
    ::= { ieee8021XAuthenticatorEntry 1 }

ieee8021XAuthPaeAuthenticated OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "This object will be set 'true' by PACP if the PAE authenticator
        currently authenticated, and 'false' if the authentication
        fails or is revoked."
    REFERENCE       "IEEE 802.1X Clause 8, Figure 12-3"
    ::= { ieee8021XAuthenticatorEntry 2 }

ieee8021XAuthPaeFailed OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "This object will be set 'true' by PACP if the authentication
        has failed or has been terminated.  The cause could be a
        failure returned by EAP, either immediately or following a
        reauthentication, an excessive number of attempts to
        authenticate (either immediately or upon reauthentication), or
        the authenticator deasserting authenticate, the object
```

```
        authPaeAuthenticate in the same row is 'false'.  The PACP
        will set the object authPaeAuthenticated false as well as
        setting the object 'true'."
    REFERENCE       "IEEE 802.1X Clause 8, Figure 12-3"
    ::= { ieee8021XAuthenticatorEntry 3 }

ieee8021XAuthPaeReAuthEnabled OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "This object is set 'true' if PACP should initiate
        reauthentication periodically, 'false' otherwise."
    REFERENCE       "IEEE 802.1X Clause 8.9, Figure 12-3"
    ::= { ieee8021XAuthenticatorEntry 4 }

ieee8021XAuthPaeQuietPeriod OBJECT-TYPE
    SYNTAX          Unsigned32 (0..65535)
    UNITS           "seconds"
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "This object indicates a waiting period after a failed
        authentication attempt, before another attempt is permitted."
    REFERENCE       "IEEE 802.1X Clause 8.6, Figure 12-3"
    DEFVAL          { 60 }
    ::= { ieee8021XAuthenticatorEntry 5 }

ieee8021XAuthPaeReauthPeriod OBJECT-TYPE
    SYNTAX          Unsigned32 (0..65535)
    UNITS           "seconds"
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "This object indicates the time period of the reauthentication
        to the supplicant."
    REFERENCE       "IEEE 802.1X Clause 8.6, Figure 12-3"
    DEFVAL          { 3600 }
    ::= { ieee8021XAuthenticatorEntry 6 }

ieee8021XAuthPaeRetryMax OBJECT-TYPE
    SYNTAX          Unsigned32
    UNITS           "times"
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "The maximum number of authentication attempts before failure is
        reported to the Logon Process, and the authPaeQuietPeriod
        timer imposed before further attempts are permitted."
    REFERENCE       "IEEE 802.1X Clause 8.9, Figure 12-3"
    DEFVAL          { 2 }
    ::= { ieee8021XAuthenticatorEntry 7 }

ieee8021XAuthPaeRetryCount OBJECT-TYPE
    SYNTAX          Gauge32
    UNITS           "times"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The count of the number of authentication attempts."
    REFERENCE       "IEEE 802.1X Clause 8.9"
    ::= { ieee8021XAuthenticatorEntry 8 }


-- ---------------------------------------------------------------- --
-- The 802.1X PAE Supplicant Group
-- ---------------------------------------------------------------- --
--
-- ---------------------------------------------------------------- --
-- The 802.1X PAE Supplicant Table
-- ---------------------------------------------------------------- --
```

```
ieee8021XSupplicantTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF Ieee8021XSupplicantEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "A table that contains the configuration objects for the
        Supplicant PAE associated with each port.

        For the writeable objects in this table, the configured value
        shall be stored in persistent memory and remain unchanged
        across a re-initialization of the management system of the
        entity."
    REFERENCE       "802.1X Clause 8, Figure 8-6, Figure 12-3"
    ::= { ieee8021XPaeSupplicant 1 }

ieee8021XSupplicantEntry OBJECT-TYPE
    SYNTAX          Ieee8021XSupplicantEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "The configuration information for an Supplicant PAE."
    INDEX           { ieee8021XPaePortNumber }
    ::= { ieee8021XSupplicantTable 1 }

Ieee8021XSupplicantEntry ::= SEQUENCE {
        ieee8021XSuppPaeAuthenticate  TruthValue,
        ieee8021XSuppPaeAuthenticated TruthValue,
        ieee8021XSuppPaeFailed        TruthValue,
        ieee8021XSuppPaeHelloPeriod   Unsigned32,
        ieee8021XSuppPaeRetryMax      Unsigned32,
        ieee8021XSuppPaeRetryCount    Gauge32
}

ieee8021XSuppPaeAuthenticate OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "This object will be set 'true' by the PAE supplicant to request
        authentication, and if this object is 'true', reauthentication
        is allowed.

        This object will be 'false' while the PAE supplicant revokes
        authentication."
    REFERENCE       "IEEE 802.1X Clause 8.4, Figure 8-6, Figure 12-3"
    ::= { ieee8021XSupplicantEntry 1 }

ieee8021XSuppPaeAuthenticated OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "This object will be set 'true' by PACP if the PAE supplicant
        currently authenticated, and 'false' if the authentication
        fails or is revoked."
    REFERENCE       "IEEE 802.1X Clause 8.4, Figure 8-6, Figure 12-3"
    ::= { ieee8021XSupplicantEntry 2 }

ieee8021XSuppPaeFailed OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "This object will be set 'true' by PACP if the authentication
        has failed or has been terminated.  The cause could be a
        failure returned by EAP, either immediately or following a
        reauthentication, an excessive number of attempts to
        authenticate (either immediately or upon reauthentication), or
        the supplicant deasserting authenticate, the object
        ieee8021XSuppPaeAuthenticate in the same row is 'false'.  The PACP
        will set the object ieee8021XSuppPaeAuthenticated false as well as
        setting the object 'true'."
```

```
    REFERENCE       "IEEE 802.1X Clause 8.4, Figure 8-6, Figure 12-3"
    ::= { ieee8021XSupplicantEntry 3 }

ieee8021XSuppPaeHelloPeriod OBJECT-TYPE
    SYNTAX          Unsigned32 (0..65535)
    UNITS           "seconds"
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "This object indicated a waiting time period after a failed
        authentication attempt, before another attempt is permitted."
    REFERENCE       "IEEE 802.1X Clause 8.6, Figure 8-6, Figure 12-3"
    DEFVAL          { 60 }
    ::= { ieee8021XSupplicantEntry 4 }

ieee8021XSuppPaeRetryMax OBJECT-TYPE
    SYNTAX          Unsigned32
    UNITS           "times"
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "The maximum number of authentication attempts before failure is
        reported to the Logon Process, and the ieee8021XSuppPaeHelloPeriod
        timer imposed before further attempts are permitted."
    REFERENCE       "IEEE 802.1X Clause 8.7, Figure 8-6, Figure 12-3"
    DEFVAL          { 2 }
    ::= { ieee8021XSupplicantEntry 5 }

ieee8021XSuppPaeRetryCount OBJECT-TYPE
    SYNTAX          Gauge32
    UNITS           "times"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The count of the number of authentication attempts."
    REFERENCE       "IEEE 802.1X Clause 8.7, Figure 8-6, Figure 12-3"
    ::= { ieee8021XSupplicantEntry 6 }


-- ------------------------------------------------------------------ --
-- The 802.1X PAE EAPOL Statistics Table
-- ------------------------------------------------------------------ --

ieee8021XEapolStatsTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF Ieee8021XEapolStatsEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "A table in system level contains the EAPOL statistics and
        diagnostics information supported by PAE."
    REFERENCE       "802.1X Clause 12.8, Figure 12-3"
    ::= { ieee8021XPaeEapol 1 }

ieee8021XEapolStatsEntry OBJECT-TYPE
    SYNTAX          Ieee8021XEapolStatsEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "An entry contains the EAPOL statistics and diagnostics
        information for a PAE."
    INDEX           { ieee8021XPaePortNumber }
    ::= { ieee8021XEapolStatsTable 1 }

Ieee8021XEapolStatsEntry ::= SEQUENCE {
        ieee8021XEapolInvalidFramesRx         Counter32,
        ieee8021XEapolEapLengthErrorFramesRx  Counter32,
        ieee8021XEapolAnnouncementFramesRx    Counter32,
        ieee8021XEapolAnnouncementReqFramesRx Counter32,
        ieee8021XEapolPortUnavailableFramesRx Counter32,
        ieee8021XEapolStartFramesRx           Counter32,
        ieee8021XEapolEapFramesRx             Counter32,
        ieee8021XEapolLogoffFramesRx          Counter32,
```

```
        ieee8021XEapolMkNoCknFramesRx          Counter32,
        ieee8021XEapolMkInvalidFramesRx        Counter32,
        ieee8021XEapolLastRxFrameVersion       Unsigned32,
        ieee8021XEapolLastRxFrameSource        MacAddress,
        ieee8021XEapolSuppEapFramesTx          Counter32,
        ieee8021XEapolLogoffFramesTx           Counter32,
        ieee8021XEapolAnnouncementFramesTx     Counter32,
        ieee8021XEapolAnnouncementReqFramesTx Counter32,
        ieee8021XEapolStartFramesTx            Counter32,
        ieee8021XEapolAuthEapFramesTx          Counter32,
        ieee8021XEapolMkaFramesTx              Counter32
}

ieee8021XEapolInvalidFramesRx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of invalid EAPOL frames of any type that have been
        received by this PAE."
    REFERENCE       "802.1X Clause 12.8.1, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 1 }

ieee8021XEapolEapLengthErrorFramesRx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of EAPOL frames that the Packet Body Length does not
        match a Packet Body that is contained within the octets of the
        received EAPOL MPDU in this PAE."
    REFERENCE       "802.1X Clause 12.8.1, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 2 }

ieee8021XEapolAnnouncementFramesRx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of EAPOL-Announcement frames that have been received
        by this PAE."
    REFERENCE       "802.1X Clause 12.8.1, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 3 }

ieee8021XEapolAnnouncementReqFramesRx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of EAPOL-Announcement-Req frames that have been
        received by this PAE."
    REFERENCE       "802.1X Clause 12.8.1, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 4 }

ieee8021XEapolPortUnavailableFramesRx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of EAPOL frames that are discarded because their
        processing would require the creation of a virtual port, for
        which there are inadequate or constrained resources, or an
        existing virtual port and no such port currently exists.  If
        virtual port is not supported, this object should be always 0."
    REFERENCE       "802.1X Clause 12.8.1, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 5 }
```

```
ieee8021XEapolStartFramesRx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of EAPOL-Start frames that have been received by
        this PAE."
    REFERENCE       "802.1X Clause 12.8.1, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 6 }

ieee8021XEapolEapFramesRx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of EAPOL-EAP frames that have been received by
        this PAE."
    REFERENCE       "802.1X Clause 12.8.1, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 7 }

ieee8021XEapolLogoffFramesRx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of EAPOL-Logoff frames that have been received by
        this PAE."
    REFERENCE       "802.1X Clause 12.8.1, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 8 }

ieee8021XEapolMkNoCknFramesRx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of MKPDUs received with MKA not enabled or CKN not
        recognized in this PAE."
    REFERENCE       "802.1X Clause 12.8.1, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 9 }

ieee8021XEapolMkInvalidFramesRx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of MKPDUs failing in message authentication on
        receipt process in this PAE."
    REFERENCE       "802.1X Clause 12.8.1, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 10 }

ieee8021XEapolLastRxFrameVersion OBJECT-TYPE
    SYNTAX          Unsigned32
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The version of last received EAPOL frame by this PAE."
    REFERENCE       "802.1X Clause 12.8.2, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 11 }

ieee8021XEapolLastRxFrameSource OBJECT-TYPE
    SYNTAX          MacAddress
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The source MAC address of last received EAPOL frame by this
        PAE."
    REFERENCE       "802.1X Clause 12.8.2, Figure 12-3"
```

```
    ::= { ieee8021XEapolStatsEntry 12 }

ieee8021XEapolSuppEapFramesTx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of EAPOL-EAP frames that have been transmitted by
        the supplicant of this PAE."
    REFERENCE       "802.1X Clause 12.8.3, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 13 }

ieee8021XEapolLogoffFramesTx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of EAPOL-Logoff frames that have been transmitted by
        this PAE."
    REFERENCE       "802.1X Clause 12.8.3, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 14 }

ieee8021XEapolAnnouncementFramesTx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of EAPOL-Announcement frames that have been
        transmitted by this PAE."
    REFERENCE       "802.1X Clause 12.8.3, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 15 }

ieee8021XEapolAnnouncementReqFramesTx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of EAPOL-Announcement-Req frames that have been
        transmitted by this PAE."
    REFERENCE       "802.1X Clause 12.8.3, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 16 }

ieee8021XEapolStartFramesTx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of EAPOL-Start frames that have been transmitted by
        this PAE."
    REFERENCE       "802.1X Clause 12.8.3, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 17 }

ieee8021XEapolAuthEapFramesTx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The number of EAPOL-EAP frames that have been transmitted by
        the authenticator of this PAE."
    REFERENCE       "802.1X Clause 12.8.3, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 18 }

ieee8021XEapolMkaFramesTx OBJECT-TYPE
    SYNTAX          Counter32
    UNITS           "Packets"
    MAX-ACCESS      read-only
```

```
    STATUS          current
    DESCRIPTION
        "The number of EAPOL-MKA frames with no CKN information that
        have been transmitted by this PAE."
    REFERENCE       "802.1X Clause 12.8.3, Figure 12-3"
    ::= { ieee8021XEapolStatsEntry 19 }


-- ---------------------------------------------------------- --
-- The 802.1X PAE KaY Group
-- ---------------------------------------------------------- --
--
-- ---------------------------------------------------------- --
-- The 802.1X PAE KaY Table
-- ---------------------------------------------------------- --

ieee8021XKayMkaTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF Ieee8021XKayMkaEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "A table of system level information for each interface
        supported by the KaY (Key Agreement Entity).  This table will
        be instantiated if the object ieee8021XPaePortKayMkaEnable in
        the corresponding entry of the ieee8021XPaePortTable is 'true'.

        The following terms are used to identify roles within the MKA
        protocol or protocol scenarios and the MIB description :

        participant : An instance of MKA, transmitting and receiving
            frames protected by keys derived from a single CAK, and
            operating with positive intent, obeying the protocol.

        member: A participant that possesses the CAK that can be used
            to prove liveness and to obtain membership in the CA under
            discussion.

        actor: The participant under discussion, usually in the KaY
            being described.

        partners: Participants or members attached to the same LAN as
            the actor, excluding the actor.

        principal actor: The actor controlling the PAC or SecY
            associated with the KaY.

        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.

        For the writeable objects in this table, the configured value
        shall be stored in persistent memory and remain unchanged
        across a re-initialization of the management system of the
        entity."
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    ::= { ieee8021XPaeKaY 1 }

ieee8021XKayMkaEntry OBJECT-TYPE
    SYNTAX          Ieee8021XKayMkaEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "An entry containing KaY MKA management information applicable
        to a particular interface."
    INDEX           { ieee8021XPaePortNumber }
```

```
    ::= { ieee8021XKayMkaTable 1 }

Ieee8021XKayMkaEntry ::= SEQUENCE {
        ieee8021XKayMkaActive
            TruthValue,
        ieee8021XKayMkaAuthenticated
            TruthValue,
        ieee8021XKayMkaSecured
            TruthValue,
        ieee8021XKayMkaFailed
            TruthValue,
        ieee8021XKayMkaActorSCI
            SecySCI,
        ieee8021XKayMkaActorsPriority
            Ieee8021XMkaKeyServerPriority,
        ieee8021XKayMkaKeyServerPriority
            Ieee8021XMkaKeyServerPriority,
        ieee8021XKayMkaKeyServerSCI
            SecySCI,
        ieee8021XKayAllowedJoinGroup
            TruthValue,
        ieee8021XKayAllowedFormGroup
            TruthValue,
        ieee8021XKayCreateNewGroup
            TruthValue,
        ieee8021XKayMacSecCapability
            INTEGER,
        ieee8021XKayMacSecDesired
            TruthValue,
        ieee8021XKayMacSecProtect
            TruthValue,
        ieee8021XKayMacSecReplayProtect
            TruthValue,
        ieee8021XKayMacSecValidate
            TruthValue,
        ieee8021XKayMacSecConfidentialityOffset
            Integer32,
        ieee8021XKayMkaTxKN
            Ieee8021XMkaKN,
        ieee8021XKayMkaTxAN
            RowPointer,
        ieee8021XKayMkaRxKN
            Ieee8021XMkaKN,
        ieee8021XKayMkaRxAN
            RowPointer,
        ieee8021XKayMkaSuspendFor
            INTEGER,
        ieee8021XKayMkaSuspendOnRequest
            TruthValue,
        ieee8021XKayMkaSuspendedWhile
            INTEGER
}

ieee8021XKayMkaActive OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "This object will be 'true' if there is at least one MKA active
        actor, transmitting MKPDUs"
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    ::= { ieee8021XKayMkaEntry 1 }

ieee8021XKayMkaAuthenticated OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "This object will be 'true' if the principal actor,
        i.e. the actor controlling the PAC or SecY associated with
        the KaY, has determined that Controlled Port communication
        communication should proceed without MACsec."
```

```
        REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
        ::= { ieee8021XKayMkaEntry 2 }

    ieee8021XKayMkaSecured OBJECT-TYPE
        SYNTAX          TruthValue
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "This object will be 'true' if the principal actor has
            determined that communication should use MACsec."
        REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
        ::= { ieee8021XKayMkaEntry 3 }

    ieee8021XKayMkaFailed OBJECT-TYPE
        SYNTAX          TruthValue
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "This object will be 'true' if the object
            ieee8021XKayMkaSecured in
            the same row is 'false' and MKA Life Time has elapsed since an
            MKA participant was last created."
        REFERENCE       "IEEE 802.1X Clause 9.16, Table 9-3, Figure 12-3"
        ::= { ieee8021XKayMkaEntry 4 }

    ieee8021XKayMkaActorSCI OBJECT-TYPE
        SYNTAX          SecySCI
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The SCI assigned by the system to the port, applies to all the
            port's MKA actors."
        REFERENCE
            "IEEE 802.1X Clause 9.16, Figure 12-3
             IEEE 802.1AE Clause 7.1.2, 10.7.1"
        ::= { ieee8021XKayMkaEntry 5 }

    ieee8021XKayMkaActorsPriority OBJECT-TYPE
        SYNTAX          Ieee8021XMkaKeyServerPriority
        MAX-ACCESS      read-write
        STATUS          current
        DESCRIPTION
            "The Key Server priority for all the port's MKA actors.  Each
            participant encodes a key server priority, an 8-bit integer, in
            each MKPDU."
        REFERENCE       "IEEE 802.1X Clause 9.16, Table 9-2, Figure 12-3"
        ::= { ieee8021XKayMkaEntry 6 }

    ieee8021XKayMkaKeyServerPriority OBJECT-TYPE
        SYNTAX          Ieee8021XMkaKeyServerPriority
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The priority of the elected Key Server through MKA in the CA."
        REFERENCE       "IEEE 802.1X Clause 9.16, Table 9-2, Figure 12-3"
        ::= { ieee8021XKayMkaEntry 7 }

    ieee8021XKayMkaKeyServerSCI OBJECT-TYPE
        SYNTAX          SecySCI
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The SCI for key server for the MKA principal actor.  The length
            of this object is 0 if there is no principal actor, or that
            actor has no live peers.  This object matches the
            ieee8021XKayMkaActorSCI object in the same row if the actor is
            the key server."
        REFERENCE
            "IEEE 802.1X Clause 9.16, Figure 12-3
             IEEE 802.1AE Clause 7.1.2, 10.7.1"
        ::= { ieee8021XKayMkaEntry 8 }
```

```
ieee8021XKayAllowedJoinGroup OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "This object will be 'true' if the KaY will accept Group CAKs
        distributed by MKA protocol."
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    ::= { ieee8021XKayMkaEntry 9 }

ieee8021XKayAllowedFormGroup OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "This object will be 'true' if the KaY will attempt to use
        point-to-point CAKs to distribute a group CAK, if it is the
        Key Server for the MKA instances for all the point-to-point CAKs."
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    ::= { ieee8021XKayMkaEntry 10 }

ieee8021XKayCreateNewGroup OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "This object is set 'true' if a new Group CAK is to be
        distributed if the KaY is the Key Server for the MKA instances
        for all the point-to-point CAKs.  This object will be set 'false'
        by the KaY when distribution is complete."
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    ::= { ieee8021XKayMkaEntry 11 }

ieee8021XKayMacSecCapability OBJECT-TYPE
    SYNTAX          INTEGER {
                        noMACsec(0),
                        macSecCapability1(1),
                        macSecCapability2(2),
                        macSecCapability3(3)
                    }
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "This object indicates whether MACsec is implemented, and if so
        whether the implementation provides integrity protection only,
        integrity and integrity with confidentiality, or integrity and
        integrity with confidentiality with a selectable confidentiality offset
        of 0, 30, or 50 octets (see IEEE Std 802.1AE).

        'noMACsec' : the MACsec is not implemented.

        'macSecCapability1' :  capable in 'integrity protection without
            confidentiality'.

        'macSecCapability2' :  capable in 'integrity protection without
             confidentiality' and integrity protection and confidentiali
              with a confidentiality offset 0',.

        'macSecCapability3' :  capable in 'integrity protection without
             confidentiality' and integrity protection and confidentiali
              with a confidentiality offset 0, 30 or 50'."
    REFERENCE
        "IEEE 802.1X Clause 9.6.1, Clause 9.16, Figure 12-3, Table 11-6"
    ::= { ieee8021XKayMkaEntry 12 }

ieee8021XKayMacSecDesired OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "This object will be set 'true' if the MKA participants desire
        the use of MACsec to protect frames with this KaY."
```

```
    REFERENCE
        "IEEE 802.1X Clause 9.6.1, Clause 9.16, Figure 12-3"
    ::= { ieee8021XKayMkaEntry 13 }

ieee8021XKayMacSecProtect OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The status of the MACsec protection function for this KaY.

        'true' : then the status of the MACsec protection function will
            be as object secyIfProtectFramesEnable object configured
            in the IEEE8021-SECY-MIB.
        'false' : then the MACsec protection function is disabled by
            this KaY."
    REFERENCE
        "IEEE 802.1X Clause 9.6.1, Clause 9.16, Figure 12-2,
         Figure 12-3, IEEE 802.1AE IEEE8021-SECY-MIB"
    ::= { ieee8021XKayMkaEntry 14 }

ieee8021XKayMacSecReplayProtect OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The status of the MACsec replay protection function for this
        KaY.

        'true' : then the status of the MACsec replay protection
            function will be as secyIfReplayProtectEnable object
            configured in the IEEE8021-SECY-MIB.
        'false' : then the MACsec replay protection function is
            disabled by this KaY."
    REFERENCE
        "IEEE 802.1X Clause 9.6.1, Clause 9.16, Figure 12-2,
         Figure 12-3"
    ::= { ieee8021XKayMkaEntry 15 }

ieee8021XKayMacSecValidate OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The status of the MACsec validation function for this KaY.

        'true' : then the status of the MACsec validation function
            will be as secyIfValidateFrames object configured in the
            IEEE8021-SECY-MIB.
        'false' : then the MACsec validation function is enabled but
            only for checking without filtering out invalid frames by
            the SecY."
    REFERENCE
        "IEEE 802.1X Clause 9.6.1, Clause 9.16, Figure 12-2,
        Figure 12-3"
    ::= { ieee8021XKayMkaEntry 16 }

ieee8021XKayMacSecConfidentialityOffset OBJECT-TYPE
    SYNTAX          Integer32 (0 | 30 | 50)
    UNITS           "bytes"
    MAX-ACCESS      read-write
    STATUS          current
    DESCRIPTION
        "The confidentiality protection offset options for the selected
        cipher suite in the MACsec.  If the cipher suite does not have
        this capability, the configured value of the object will not
        apply to the cipher suite."
    REFERENCE
        "IEEE 802.1X Clause 9.7.1, Clause 9.16, Figure 12-3"
    ::= { ieee8021XKayMkaEntry 17 }

ieee8021XKayMkaTxKN OBJECT-TYPE
```

```
        SYNTAX          Ieee8021XMkaKN
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The key number assigned by the key server to the SAK currently
            being used for transmission.  This object will be 0 if MACsec
            is not being used or the key number is not available yet."
        REFERENCE       "IEEE 802.1X Clause 9.8, Clause 9.16, Figure 12-3"
        ::= { ieee8021XKayMkaEntry 18 }

    ieee8021XKayMkaTxAN OBJECT-TYPE
        SYNTAX          RowPointer
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The AN assigned by the key server for use with the key number
            for transmission.

            This row pointer will point to an entry in the secyTxSATable
            which the secyTxSCEncodingSA object also points to in the
            IEEE8021-SECY-MIB.

            If MACsec is not in use or the AN is not identified yet, the
            value of this object shall be set to the OBJECT IDENTIFIER
            { 0 0 }."
        REFERENCE
            "IEEE 802.1X Clause 9.9, Clause 9.16, Figure 12-3,
             IEEE8021-SECY-MIB"
        ::= { ieee8021XKayMkaEntry 19 }

    ieee8021XKayMkaRxKN OBJECT-TYPE
        SYNTAX          Ieee8021XMkaKN
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The key number assigned by the key server to the oldest SAK
            currently being used for reception.  It is the same as the key
            number for transmission if a single SAK is currently in use.
            This object will be 0 if MACsec is not being used or the key
            number is not available yet."
        REFERENCE       "IEEE 802.1X Clause 9.8, Clause 9.16, Figure 12-3"
        ::= { ieee8021XKayMkaEntry 20 }

    ieee8021XKayMkaRxAN OBJECT-TYPE
        SYNTAX          RowPointer
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The AN assigned by the key server for use with the key number
            for reception.  It is the same as AN for transmission if a
            single SAK is currently in use.

            This row pointer will point to an entry in the secyRxSATable
            which the secyRxSCCurrentSA object also points to in the
            IEEE8021-SECY-MIB.

            If MACsec is not in use or the AN is not identified yet, the
            value of this object shall be set to the OBJECT IDENTIFIER
            { 0 0 }."
        REFERENCE
            "IEEE 802.1X Clause 9.6.1, Clause 9.16, Figure 12-3,
             IEEE8021-SECY-MIB"
        ::= { ieee8021XKayMkaEntry 21 }

    ieee8021XKayMkaSuspendFor OBJECT-TYPE
        SYNTAX INTEGER (1..120)
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
            "Set by management to a non-zero number of seconds between 1
            and MKA Suspension Limit to initiate a suspension (9.18) of
            that duration (if the KaY's principal actor is the Key
```

```
            Server) or to request a suspension (otherwise)"
        REFERENCE "IEEE 802.1X Clause 9.16, Figure 12-3"
        ::= { ieee8021XKayMkaEntry 22 }

    ieee8021XKayMkaSuspendOnRequest OBJECT-TYPE
        SYNTAX TruthValue
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
            "The status of the suspendOnRequest function for this KaY.
            'true' : then the KaY's principal actor will initiate a
            suspension if it is the Key Server and another participant
            has requested a suspension by transmitting a non-zero value
            of its suspendFor parameter
            'false' : then the KaY will not initiate a suspension on
            request from another participant."
        REFERENCE "IEEE 802.1X Clause 9.16, Figure 12-3"
        ::= { ieee8021XKayMkaEntry 23 }

    ieee8021XKayMkaSuspendedWhile OBJECT-TYPE
        SYNTAX INTEGER (1..126)
        MAX-ACCESS read-write
        STATUS current
        DESCRIPTION
            "Read by management to determine if a suspension is in
            progress and to discover the remaining duration of that
            suspension. May be set directly to coordinate in-service
            upgrades."
        REFERENCE "IEEE 802.1X Clause 5.11.4, Clause 9.16, Clause 9.18.5,
                   Clause 9.18.6, Figure 12-3"
        ::= { ieee8021XKayMkaEntry 24 }

    -- ------------------------------------------------------------------ --
    -- The 802.1X PAE KaY MKA Participants Table
    -- ------------------------------------------------------------------ --

    ieee8021XKayMkaParticipantTable OBJECT-TYPE
        SYNTAX          SEQUENCE OF Ieee8021XKayMkaParticipantEntry
        MAX-ACCESS      not-accessible
        STATUS          current
        DESCRIPTION
            "A table for each MKA participant supported by the KaY MKA
            entity.

            For the writeable objects in this table, the configured value
            shall be stored in persistent memory and remain unchanged
            across a re-initialization of the management system of the
            entity."
        REFERENCE       "IEEE 802.1X Clause 9.14, Clause 9.16, Figure 12-3"
        ::= { ieee8021XPaeKaY 2 }

    ieee8021XKayMkaParticipantEntry OBJECT-TYPE
        SYNTAX          Ieee8021XKayMkaParticipantEntry
        MAX-ACCESS      not-accessible
        STATUS          current
        DESCRIPTION
            "An entry containing KaY MKA management information applicable
            to a MKA participant."
        INDEX           { ieee8021XPaePortNumber, ieee8021XKayMkaPartCKN }
        ::= { ieee8021XKayMkaParticipantTable 1 }

    Ieee8021XKayMkaParticipantEntry ::= SEQUENCE {
            ieee8021XKayMkaPartCKN             Ieee8021XPaeCKN,
            ieee8021XKayMkaPartKMD             Ieee8021XPaeKMD,
            ieee8021XKayMkaPartNID             Ieee8021XPaeNID,
            ieee8021XKayMkaPartCached          TruthValue,
            ieee8021XKayMkaPartActive          TruthValue,
            ieee8021XKayMkaPartRetain          TruthValue,
            ieee8021XKayMkaPartActivateControl INTEGER,
            ieee8021XKayMkaPartPrincipal       TruthValue,
            ieee8021XKayMkaPartDistCKN         Ieee8021XPaeCKNOrNull,
            ieee8021XKayMkaPartRowStatus       RowStatus
```

```
}

ieee8021XKayMkaPartCKN OBJECT-TYPE
    SYNTAX          Ieee8021XPaeCKN
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "The CKN information for this MKA participant."
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    ::= { ieee8021XKayMkaParticipantEntry 1 }

ieee8021XKayMkaPartKMD OBJECT-TYPE
    SYNTAX          Ieee8021XPaeKMD
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "The KMD information for this MKA participant."
    REFERENCE       "IEEE 802.1X Clause 9.16, Clause 12.6, Figure 12-3"
    ::= { ieee8021XKayMkaParticipantEntry 2 }

ieee8021XKayMkaPartNID OBJECT-TYPE
    SYNTAX          Ieee8021XPaeNID
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "The NID information for this MKA participant."
    REFERENCE       "IEEE 802.1X Clause 9.16, Clause 12.6, Figure 12-3"
    ::= { ieee8021XKayMkaParticipantEntry 3 }

ieee8021XKayMkaPartCached OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "This object is set 'true' by the KaY if the participant's
        parameters are cached.  If this object is 'true', this object
        can be set 'false' cleared by management to remove the
        participant's parameters from the cache."
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    ::= { ieee8021XKayMkaParticipantEntry 4 }

ieee8021XKayMkaPartActive OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "This object is set 'true' if the participant is active, i.e. is
        currently transmitting periodic MKPDUs."
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    DEFVAL { false }
    ::= { ieee8021XKayMkaParticipantEntry 5 }

ieee8021XKayMkaPartRetain OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "This object is set 'true' to retain the participant in the
        cache, even if the KaY would normally remove it (due to lack
        of use for example)"
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    ::= { ieee8021XKayMkaParticipantEntry 6 }

ieee8021XKayMkaPartActivateControl OBJECT-TYPE
    SYNTAX          INTEGER  {
                        default(1),
                        disabled(2),
                        onOperUp(3),
                        always(4)
                    }
    MAX-ACCESS      read-create
    STATUS          current
```

```
        DESCRIPTION
            "This object is for controlling the participant's behavior when
            the participant is activated.

            'default' : the participant is from cached entries created by
                the KaY as part of normal operation, without explicit
                management, and is activated according to the
                implementation dependent policies of the KaY.

            'disabled' : the participant allows the cache information to
                be retained, but disabled for indefinite period.

            'onOperUp' : causing the participant to be activated when the
                PAE's 'Uncontrolled Port' becomes operational and when the
                PAE resumes following suspension.

            'always' : causing the participant to remain active all the
                time, even in the continued absence of partners.

            If the object changed to disabled(1) or onOperUp(3), the
            participant ceases operation immediately and receipt of MKPDUs
            with a matching CKN during a subsequent period of twice MKA
            lifetime will not cause the participant to become active once
            more."
        REFERENCE       "IEEE 802.1X Clause 9.14, Clause 9.16, Figure 12-3"
        ::= { ieee8021XKayMkaParticipantEntry 7 }

    ieee8021XKayMkaPartPrincipal OBJECT-TYPE
        SYNTAX          TruthValue
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "This object is set 'true' if the participant is currently the
            principal actor."
        REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
        DEFVAL { false }
        ::= { ieee8021XKayMkaParticipantEntry 8 }

    ieee8021XKayMkaPartDistCKN OBJECT-TYPE
        SYNTAX          Ieee8021XPaeCKNOrNull
        MAX-ACCESS      read-only
        STATUS          current
        DESCRIPTION
            "The CKN for the last CAK distributed either by the actor or one
            of its partners.  Empty string for this object will be provided if
            this participant has not been used to distribute a CAK or the
            participant is not active, i.e. the object
            ieee8021XKayMkaPartActive in the same row is 'false'."
        REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
        DEFVAL { "" }
        ::= { ieee8021XKayMkaParticipantEntry 9 }

    ieee8021XKayMkaPartRowStatus OBJECT-TYPE
        SYNTAX          RowStatus
        MAX-ACCESS      read-create
        STATUS          current
        DESCRIPTION
            "The object to create the parameters for the supported
            participant information in the system.

            If the participant information is from downloaded policies,
            this object is 'active'."
        REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
        ::= { ieee8021XKayMkaParticipantEntry 10 }

    -- ---------------------------------------------------------------- --
    -- The 802.1X PAE MKA Peer List Table
    -- ---------------------------------------------------------------- --

    ieee8021XKayMkaPeerListTable OBJECT-TYPE
        SYNTAX          SEQUENCE OF Ieee8021XKayMkaPeerListEntry
        MAX-ACCESS      not-accessible
```

```
    STATUS          current
    DESCRIPTION
        "A table containing the lists of Live Peers and Potential Peers,
        for all MKA instances for which the KaY is active."
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    ::= { ieee8021XPaeKaY 3 }

ieee8021XKayMkaPeerListEntry OBJECT-TYPE
    SYNTAX          Ieee8021XKayMkaPeerListEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "A table entry for one of the peers for one of the MKA
        instances for which this KaY is an active participant."
    INDEX           { ieee8021XPaePortNumber, ieee8021XKayMkaPartCKN,
                      ieee8021XKayMkaPeerListMI }
    ::= { ieee8021XKayMkaPeerListTable 1 }

Ieee8021XKayMkaPeerListEntry ::= SEQUENCE {
        ieee8021XKayMkaPeerListMI   Ieee8021XMkaMI,
        ieee8021XKayMkaPeerListMN   Ieee8021XMkaMN,
        ieee8021XKayMkaPeerListType INTEGER,
        ieee8021XKayMkaPeerListSCI  SecySCI
}

ieee8021XKayMkaPeerListMI OBJECT-TYPE
    SYNTAX          Ieee8021XMkaMI
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "The peer entry's MI information in the peer list of this active
        participant in MKA protocol."
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    ::= { ieee8021XKayMkaPeerListEntry 1 }

ieee8021XKayMkaPeerListMN OBJECT-TYPE
    SYNTAX          Ieee8021XMkaMN
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The peer entry's latest MN information in the peer list of this
        active participant in MKA protocol."
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    ::= { ieee8021XKayMkaPeerListEntry 2 }

ieee8021XKayMkaPeerListType OBJECT-TYPE
    SYNTAX          INTEGER  {
                      livePeerList(1),
                      potentialPeerList(2)
                    }
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The peer entry's type in the peer list of this active
        participant in MKA protocol.

        'livePeerList' : the peer entry is in the Live Peer List.

        'potentialPeerList' : the peer entry is in the Potential
            Peer List."
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    ::= { ieee8021XKayMkaPeerListEntry 3 }

ieee8021XKayMkaPeerListSCI OBJECT-TYPE
    SYNTAX          SecySCI
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The SCI information of the peer entry in the peer list of this
        active participant in MKA protocol."
    REFERENCE       "IEEE 802.1X Clause 9.16, Figure 12-3"
    ::= { ieee8021XKayMkaPeerListEntry 4 }
```

```
-- ------------------------------------------------------------ --
-- The 802.1X PAE NID Group
-- ------------------------------------------------------------ --
--
-- ------------------------------------------------------------ --
-- The 802.1X PAE NID Configuration Table
-- ------------------------------------------------------------ --

ieee8021XNidConfigTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF Ieee8021XNidConfigEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "A table that contains the configuration objects for the network
        announcement information for the Logon Process.

        The detail operation of the Logon Process can vary depending on
        the port-based network access control applications, and on the
        capabilities supported by that implementation including, for
        example, network discovery and roaming.  This table specifies
        control variables that facilitate behaviors that are
        potentially useful in a range of applications.  Implementations
        may use and augment the variables specified, or may use
        variables specific to the implementation.

        For the writeable objects in this table, the configured value
        shall be stored in persistent memory and remain unchanged
        across a re-initialization of the management system of the
        entity."
    REFERENCE       "802.1X Clause 8, Figure 8-6, Figure 12-3"
    ::= { ieee8021XPaeNetworkIdentifier 1 }

ieee8021XNidConfigEntry OBJECT-TYPE
    SYNTAX          Ieee8021XNidConfigEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "An entry contains network announcement parameters for a NID."
    INDEX           { IMPLIED ieee8021XNidNID }
    ::= { ieee8021XNidConfigTable 1 }

Ieee8021XNidConfigEntry ::= SEQUENCE {
        ieee8021XNidNID                     Ieee8021XPaeNID,
        ieee8021XNidUseEap                  INTEGER,
        ieee8021XNidUnauthAllowed           INTEGER,
        ieee8021XNidUnsecuredAllowed        INTEGER,
        ieee8021XNidUnauthenticatedAccess Ieee8021XPaeNIDUnauthenticatedStatus,
        ieee8021XNidAccessCapabilities    Ieee8021XPaeNIDCapabilites,
        ieee8021XNidKMD                     Ieee8021XPaeKMD,
        ieee8021XNidRowStatus               RowStatus
}

ieee8021XNidNID OBJECT-TYPE
    SYNTAX          Ieee8021XPaeNID
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "The network identifier to identify NID configuration in the
        PAE."
    REFERENCE       "802.1X Clause 12.5, Figure 12-3"
    ::= { ieee8021XNidConfigEntry 1 }

ieee8021XNidUseEap OBJECT-TYPE
    SYNTAX          INTEGER  {
                        never(1),
                        immediate(2),
                        mkaFail(3)
                    }
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
```

```
            "Determines when the Logon Process will initiate EAP, if the
            Supplicant and or Authenticator are enabled, and takes one of
            the following values:

            'never' : Never.

            'immediate' : Immediately, concurrently with the use of MKA
                with any cached CAK(s).

            'mkaFail' : Not until MKA has failed, if a prior CAK has been
                cached."
        REFERENCE       "802.1X Clause 12.5, Figure 12-3"
        ::= { ieee8021XNidConfigEntry 2 }

    ieee8021XNidUnauthAllowed OBJECT-TYPE
        SYNTAX          INTEGER  {
                            never(1),
                            immediate(2),
                            authFail(3)
                        }
        MAX-ACCESS      read-create
        STATUS          current
        DESCRIPTION
            "Determines when the Logon Process will tell the CP state
            machine to provide unauthenticated connectivity, and takes one
            of the following values:

            'never' : Never.

            'immediate' : Immediately, independently of any current or
                future attempts to authenticate using the PAE or MKA.

            'authFail' : Not until an attempt has been made to
                authenticate using EAP, unless neither the Supplicant nor
                the Authenticator is enabled, and MKA has attempted to use
                any cached CAK (unless the Key is not enabled)."
        REFERENCE       "802.1X Clause 12.5, Figure 12-3"
        ::= { ieee8021XNidConfigEntry 3 }

    ieee8021XNidUnsecuredAllowed OBJECT-TYPE
        SYNTAX          INTEGER  {
                            never(1),
                            immediate(2),
                            mkaFail(3),
                            mkaServer(4)
                        }
        MAX-ACCESS      read-create
        STATUS          current
        DESCRIPTION
            "Determines when the Logon Process will tell the CP state
            machine to provide authenticated but unsecured connectivity,
            takes one of the following values:

            'never' : Never.

            'immediate' : Immediately, to provide connectivity
                concurrently with the use of MKA with any CAK acquired
                through EAP.

            'mkaFail' : Not until MKA has failed, or is not enabled.

            'mkaServer' : Only if directed by the MKA server."
        REFERENCE       "802.1X Clause 12.5, Figure 12-3"
        ::= { ieee8021XNidConfigEntry 4 }

    ieee8021XNidUnauthenticatedAccess OBJECT-TYPE
        SYNTAX          Ieee8021XPaeNIDUnauthenticatedStatus
        MAX-ACCESS      read-create
        STATUS          current
        DESCRIPTION
            "The configured access capability of the port's clients without
            authentication in this NID."
```

```
    REFERENCE       "802.1X Clause 12.5, Clause 10.1, Figure 12-3"
    ::= { ieee8021XNidConfigEntry 5 }

ieee8021XNidAccessCapabilities OBJECT-TYPE
    SYNTAX          Ieee8021XPaeNIDCapabilites
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "The authentication and protection capabilities supported for
        the NID."
    REFERENCE       "802.1X Clause 12.5, Clause 10.1, Figure 12-3"
    ::= { ieee8021XNidConfigEntry 6 }

ieee8021XNidKMD OBJECT-TYPE
    SYNTAX          Ieee8021XPaeKMD
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "The configured KMD information for this NID."
    REFERENCE       "802.1X Clause 10.4, Figure 12-3"
    ::= { ieee8021XNidConfigEntry 7 }

ieee8021XNidRowStatus OBJECT-TYPE
    SYNTAX          RowStatus
    MAX-ACCESS      read-create
    STATUS          current
    DESCRIPTION
        "The object to create the parameters for the supported Network
        Announcement information in the system.

        If the Network Announcement information of the entry is from
        downloaded policies, this object is 'active'."
    REFERENCE       "802.1X Clause 10.4, Figure 12-3"
    ::= { ieee8021XNidConfigEntry 8 }


-- ---------------------------------------------------------------------- --
-- The 802.1X PAE Announce Information Table
-- ---------------------------------------------------------------------- --

ieee8021XAnnounceTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF Ieee8021XAnnounceEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "A table contains the status information that the Announcers
        announce in the network announcement of the PAE system.

        This table will be instantiated if the object
        ieee8021XPaePortAnnouncerEnable in the corresponding entry of
        the ieee8021XPaePortTable is 'true'."
    REFERENCE       "802.1X Clause 8, Figure 8-6, Figure 12-3"
    ::= { ieee8021XPaeNetworkIdentifier 2 }

ieee8021XAnnounceEntry OBJECT-TYPE
    SYNTAX          Ieee8021XAnnounceEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "An entry contains an Announcer's status information."
    INDEX           { ieee8021XPaePortNumber,
                      IMPLIED ieee8021XAnnounceNID }
    ::= { ieee8021XAnnounceTable 1 }

Ieee8021XAnnounceEntry ::= SEQUENCE {
        ieee8021XAnnounceNID          Ieee8021XPaeNID,
        ieee8021XAnnounceAccessStatus Ieee8021XPaeNIDAccessStatus
}

ieee8021XAnnounceNID OBJECT-TYPE
    SYNTAX          Ieee8021XPaeNID
    MAX-ACCESS      not-accessible
```

```
    STATUS          current
    DESCRIPTION
        "The NID information to identify a transmitting network
        announcement for the PAE."
    REFERENCE       "802.1X Clause 10.4, Clause 12.5, Figure 12-3"
    ::= { ieee8021XAnnounceEntry 1 }

ieee8021XAnnounceAccessStatus OBJECT-TYPE
    SYNTAX          Ieee8021XPaeNIDAccessStatus
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The object information reflects connectivity as a result of
        authentication attempts of this NID for this Announcer."
    REFERENCE
        "802.1X Clause 10.4, Clause 10.1, Clause 12.5, Figure 12-3"
    ::= { ieee8021XAnnounceEntry 2 }


-- ----------------------------------------------------------------------
-- The 802.1X PAE Announcement Information Table
-- ---------------------------------------------------------------------- --

ieee8021XAnnouncementTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF Ieee8021XAnnouncementEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "A table contains the status information that the Listeners
        receive in the network announcement of the PAE system.

        This table will be instantiated if the object
        ieee8021XPaePortListenerEnable in the corresponding entry of the
        ieee8021XPaePortTable is 'true'."
    REFERENCE       "802.1X Clause 10.4, Figure 12-3"
    ::= { ieee8021XPaeNetworkIdentifier 3 }

ieee8021XAnnouncementEntry OBJECT-TYPE
    SYNTAX          Ieee8021XAnnouncementEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "An entry contains a Listener's status information."
    INDEX           { ieee8021XPaePortNumber,
                      IMPLIED ieee8021XAnnouncementNID }
    ::= { ieee8021XAnnouncementTable 1 }

Ieee8021XAnnouncementEntry ::= SEQUENCE {
        ieee8021XAnnouncementNID             Ieee8021XPaeNID,
        ieee8021XAnnouncementKMD             Ieee8021XPaeKMD,
        ieee8021XAnnouncementSpecific        TruthValue,
        ieee8021XAnnouncementAccessStatus    Ieee8021XPaeNIDAccessStatus,
        ieee8021XAnnouncementAccessRequested TruthValue,
                                               ieee8021XAnnouncementUnauthAccess
Ieee8021XPaeNIDUnauthenticatedStatus,
        ieee8021XAnnouncementCapabilities    Ieee8021XPaeNIDCapabilites
}

ieee8021XAnnouncementNID OBJECT-TYPE
    SYNTAX          Ieee8021XPaeNID
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "The NID information to identify a received network announcement
        for the PAE."
    REFERENCE       "802.1X Clause 10.4, Figure 12-3"
    ::= { ieee8021XAnnouncementEntry 1 }

ieee8021XAnnouncementKMD OBJECT-TYPE
    SYNTAX          Ieee8021XPaeKMD
    MAX-ACCESS      read-only
    STATUS          current
```

```
    DESCRIPTION
        "The KMD information for this received network announcement of
        the PAE."
    REFERENCE       "802.1X Clause 10.4, Figure 12-3"
    ::= { ieee8021XAnnouncementEntry 2 }

ieee8021XAnnouncementSpecific OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "This object indicates the received announcement information was
        specific to the receiving PAE, not generic for all systems attached
        to the LAN."
    REFERENCE       "802.1X Clause 10.1, 10.4, Figure 12-3"
    ::= { ieee8021XAnnouncementEntry 3 }

ieee8021XAnnouncementAccessStatus OBJECT-TYPE
    SYNTAX          Ieee8021XPaeNIDAccessStatus
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The object information reflects connectivity as a result of
        authentication attempts for this received network announcement
        of the PAE."
    REFERENCE       "802.1X Clause 10.4, Clause 10.1, Figure 12-3"
    ::= { ieee8021XAnnouncementEntry 4 }

ieee8021XAnnouncementAccessRequested OBJECT-TYPE
    SYNTAX          TruthValue
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The authenticated access has been requested for this particular
        NID or not."
    REFERENCE       "802.1X Clause 10.4, Clause 10.1, Figure 12-3"
    ::= { ieee8021XAnnouncementEntry 5 }

ieee8021XAnnouncementUnauthAccess OBJECT-TYPE
    SYNTAX          Ieee8021XPaeNIDUnauthenticatedStatus
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The access capability of the port's clients without
        authentication in this received network announcement of the
        PAE.

        'openAccess', 'limitedAccess' should not be returned if the
        object ieee8021XNidUnauthAllowed is 'immediate'."
    REFERENCE
        "802.1X Clause 10.1, Clause 12.5, Figure 12-3"
    ::= { ieee8021XAnnouncementEntry 6 }

ieee8021XAnnouncementCapabilities OBJECT-TYPE
    SYNTAX          Ieee8021XPaeNIDCapabilites
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The announcement capabilities of this received network
        announcement for this PAE."
    REFERENCE       "802.1X Clause 10.1, Clause 12.5, Figure 12-3"
    ::= { ieee8021XAnnouncementEntry 7 }

-- ---------------------------------------------------------------- --
-- The 802.1X PAE Announcement Cipher Suite Information Table
-- ---------------------------------------------------------------- --

ieee8021XAnnouncementCipherSuitesTable OBJECT-TYPE
    SYNTAX          SEQUENCE OF Ieee8021XAnnouncementCipherSuitesEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
```

```
        "A table contains the Cipher Suites information that the Listeners
        receive in the network announcement of the PAE system.

        This table will be instantiated if the object
        ieee8021XPaePortListenerEnable in the corresponding entry of the
        ieee8021XPaePortTable is 'true'."
    REFERENCE       "802.1X Clause 10.4, Clause 11.13.3, Figure 11-21, Figure 12-
3"
    ::= { ieee8021XPaeNetworkIdentifier 4 }

ieee8021XAnnouncementCipherSuitesEntry OBJECT-TYPE
    SYNTAX          Ieee8021XAnnouncementCipherSuitesEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "An entry contains the Cipher Suite information which a Listener has
        reveived from network announcement."
    INDEX           { ieee8021XPaePortNumber,
                      ieee8021XAnnouncementNID,
                      ieee8021XAnnouncementCipherSuite }
    ::= { ieee8021XAnnouncementCipherSuitesTable 1 }

Ieee8021XAnnouncementCipherSuitesEntry ::= SEQUENCE {
        ieee8021XAnnouncementCipherSuite         OCTET STRING,
        ieee8021XAnnouncementCipherCapability    Unsigned32
}

ieee8021XAnnouncementCipherSuite OBJECT-TYPE
    SYNTAX          OCTET STRING (SIZE (8))
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION
        "The identifier for the announced cipher suite.  This is a
        global unique 64-bit (EUI-64) identifier to identify a cipher
        suite."
    REFERENCE
        "802.1X Clause 10.4, Figure 12-3, 802.1AE-2006 Clause 14"
    ::= { ieee8021XAnnouncementCipherSuitesEntry 1 }

ieee8021XAnnouncementCipherCapability OBJECT-TYPE
    SYNTAX          Unsigned32 (0..65535)
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION
        "The capability of a Cipher Suite received from the network
        announcement by the Listener.

        A 2 octets Cipher Suite dependent implementation capability field
        precedes each Cipher Suite reference number. If the Cipher Suite,
        ieee8021XAnnouncementCipherSuite, identifies the Default Cipher
        Suite (specified in IEEE Std 802.1AE), the two least significant
        bits of the implementation capability field encode the MACsec
        Capability parameter specified in Table 11-7 and the fourteen more
        significant bits are as 0 and ignored on receipt."
    REFERENCE
        "802.1X Clause 11.13.3, Figure 11-21"
    ::= { ieee8021XAnnouncementCipherSuitesEntry 2 }

-- ---------------------------------------------------------------------- --
-- 802.1X Conformance
-- ---------------------------------------------------------------------- --

ieee8021XPaeCompliances  OBJECT IDENTIFIER
    ::= { ieee8021XPaeMIBConformance 1 }

ieee8021XPaeGroups  OBJECT IDENTIFIER
    ::= { ieee8021XPaeMIBConformance 2 }


-- ---------------------------------------------------------------------- --
-- 802.1X Compliance Statements
-- ---------------------------------------------------------------------- --
```

```
ieee8021XPaeCompliance MODULE-COMPLIANCE
    STATUS          current
    DESCRIPTION
        "The compliance statement for device support of
        Port Access Control."
    MODULE          -- this module
    MANDATORY-GROUPS {
                        ieee8021XPaeSystemGroup,
                        ieee8021XPaeLogonGroup,
                        ieee8021XPaeEapolStatsGroup
                    }

    GROUP           ieee8021XPacGroup
    DESCRIPTION
        "This group is mandatory for systems that do not support
        the MACsec functions of the PAE."

    GROUP           ieee8021XPaeAuthConfigGroup
    DESCRIPTION
        "This group is mandatory for systems that support the
        Authenticator functions of the PAE."

    GROUP           ieee8021XPaeSuppConfigGroup
    DESCRIPTION
        "This group is mandatory for systems that support the
        Supplicant functions of the PAE."

    GROUP           ieee8021XPaeKaYMkaGroup
    DESCRIPTION
        "This group is mandatory for systems that support the KaY
        MKA functions of the PAE."

    GROUP           ieee8021XPaeNetworkIdentifierGroup
    DESCRIPTION
        "This group is mandatory for systems that support the
        network announcement functions of the PAE."

    GROUP           ieee8021XPaeAnnouncerGroup
    DESCRIPTION
        "This group is mandatory for systems that support the
        network announcement and the Announcer functions of the
        PAE."

    GROUP           ieee8021XPaeListenerGroup
    DESCRIPTION
        "This group is mandatory for systems that support
        the network announcement and the Listener functions of the
        PAE."

    OBJECT          ieee8021XKayMacSecConfidentialityOffset
    MIN-ACCESS      read-only
    DESCRIPTION
        "read-write access is not required.  This may be read-only."

    OBJECT          ieee8021XNidUseEap
    MIN-ACCESS      read-only
    DESCRIPTION
        "read-create access is not required.  This may be
        read-only."

    OBJECT          ieee8021XNidUnauthAllowed
    MIN-ACCESS      read-only
    DESCRIPTION
        "read-create access is not required.  This may be
        read-only."

    OBJECT          ieee8021XNidUnsecuredAllowed
    MIN-ACCESS      read-only
    DESCRIPTION
        "read-create access is not required.  This may be
        read-only."
```

```
OBJECT          ieee8021XNidUnauthenticatedAccess
MIN-ACCESS      read-only
DESCRIPTION
    "read-create access is not required.  This may be
    read-only."

OBJECT          ieee8021XNidAccessCapabilities
MIN-ACCESS      read-only
DESCRIPTION
    "read-create access is not required.  This may be
    read-only."

OBJECT          ieee8021XNidKMD
MIN-ACCESS      read-only
DESCRIPTION
    "read-create access is not required.  This may be
    read-only."

OBJECT          ieee8021XNidRowStatus
MIN-ACCESS      read-only
DESCRIPTION
    "read-create access is not required.  This may be
    read-only."
::= { ieee8021XPaeCompliances 1 }

ieee8021XPaeV2Compliance MODULE-COMPLIANCE
STATUS          current
DESCRIPTION
    "The compliance statement for device support of
    Port Access Control as specified in 802.1X-2010
    amended by 802.1Xbx."
MODULE          -- this module
MANDATORY-GROUPS {
                    ieee8021XPaeSystemGroup,
                    ieee8021XPaeLogonGroup,
                    ieee8021XPaeEapolStatsGroup
                }

GROUP           ieee8021XPacGroup
DESCRIPTION
    "This group is mandatory for systems that does not support
    the MACsec functions of the PAE."

GROUP           ieee8021XPaeAuthConfigGroup
DESCRIPTION
    "This group is mandatory for systems that support the
    Authenticator functions of the PAE."

GROUP           ieee8021XPaeSuppConfigGroup
DESCRIPTION
    "This group is mandatory for systems that support the
    Supplicant functions of the PAE."

GROUP           ieee8021XPaeKaYMkaGroup
DESCRIPTION
    "This group is mandatory for systems that support the KaY
    MKA functions of the PAE."

GROUP           ieee8021XPaeNetworkIdentifierGroup
DESCRIPTION
    "This group is mandatory for systems that support the
    network announcement functions of the PAE."

GROUP           ieee8021XPaeAnnouncerGroup
DESCRIPTION
    "This group is mandatory for systems that support the
    network announcement and the Announcer functions of the
    PAE."

GROUP           ieee8021XPaeListenerGroup
DESCRIPTION
```

```
        "This group is mandatory for systems that support
        the network announcement and the Listener functions of the
        PAE."

    GROUP           ieee8021XPaeKaYIsupgradeGroup
    DESCRIPTION
        "This group is mandatory for systems that support KaY MKA
        in-service upgrades."

    OBJECT          ieee8021XKayMacSecConfidentialityOffset
    MIN-ACCESS      read-only
    DESCRIPTION
        "read-write access is not required.  This may be read-only."

    OBJECT          ieee8021XNidUseEap
    MIN-ACCESS      read-only
    DESCRIPTION
        "read-create access is not required.  This may be
        read-only."

    OBJECT          ieee8021XNidUnauthAllowed
    MIN-ACCESS      read-only
    DESCRIPTION
        "read-create access is not required.  This may be
        read-only."

    OBJECT          ieee8021XNidUnsecuredAllowed
    MIN-ACCESS      read-only
    DESCRIPTION
        "read-create access is not required.  This may be
        read-only."

    OBJECT          ieee8021XNidUnauthenticatedAccess
    MIN-ACCESS      read-only
    DESCRIPTION
        "read-create access is not required.  This may be
        read-only."

    OBJECT          ieee8021XNidAccessCapabilities
    MIN-ACCESS      read-only
    DESCRIPTION
        "read-create access is not required.  This may be
        read-only."

    OBJECT          ieee8021XNidKMD
    MIN-ACCESS      read-only
    DESCRIPTION
        "read-create access is not required.  This may be
        read-only."

    OBJECT          ieee8021XNidRowStatus
    MIN-ACCESS      read-only
    DESCRIPTION
        "read-create access is not required.  This may be
        read-only."
    ::= { ieee8021XPaeCompliances 2 }


ieee8021XPaeSystemGroup OBJECT-GROUP
    OBJECTS         {
                        ieee8021XPaeSysAccessControl,
                        ieee8021XPaeSysAnnouncements,
                        ieee8021XPaeSysEapolVersion,
                        ieee8021XPaeSysMkaVersion,
                        ieee8021XPaePortType,
                        ieee8021XPaeControlledPortNumber,
                        ieee8021XPaeUncontrolledPortNumber,
                        ieee8021XPaeCommonPortNumber,
                        ieee8021XPaePortInitialize,
                        ieee8021XPaePortCapabilities,
                        ieee8021XPaePortVirtualPortsEnable,
                        ieee8021XPaePortMaxVirtualPorts,
```

```
                        ieee8021XPaePortCurrentVirtualPorts,
                        ieee8021XPaePortVirtualPortStart,
                        ieee8021XPaePortVirtualPortPeerMAC,
                        ieee8021XPaePortLogonEnable,
                        ieee8021XPaePortAuthenticatorEnable,
                        ieee8021XPaePortSupplicantEnable,
                        ieee8021XPaePortKayMkaEnable,
                        ieee8021XPaePortAnnouncerEnable,
                        ieee8021XPaePortListenerEnable
                    }
    STATUS          current
    DESCRIPTION
        "A collection of objects providing system information for a PAE
        system and a PAE port status and control information."
    ::= { ieee8021XPaeGroups 1 }

ieee8021XPacGroup OBJECT-GROUP
    OBJECTS         {
                        ieee8021XPacPortAdminPt2PtMAC,
                        ieee8021XPacPortOperPt2PtMAC
                    }
    STATUS          current
    DESCRIPTION
        "A collection of objects providing information of a PAC in the
        system."
    ::= { ieee8021XPaeGroups 2 }

ieee8021XPaeLogonGroup OBJECT-GROUP
    OBJECTS         {
                        ieee8021XPaePortLogonConnectStatus,
                        ieee8021XPaePortPortValid,
                        ieee8021XPaePortSessionOctetsRx,
                        ieee8021XPaePortSessionOctetsTx,
                        ieee8021XPaePortSessionPktsRx,
                        ieee8021XPaePortSessionPktsTx,
                        ieee8021XPaePortSessionId,
                        ieee8021XPaePortSessionStartTime,
                        ieee8021XPaePortSessionIntervalTime,
                        ieee8021XPaePortSessionTerminate,
                        ieee8021XPaePortSessionUserName
                    }
    STATUS          current
    DESCRIPTION
        "A collection of objects providing information of a Logon
        Process in the system."
    ::= { ieee8021XPaeGroups 3 }

ieee8021XPaeAuthConfigGroup OBJECT-GROUP
    OBJECTS         {
                        ieee8021XAuthPaeAuthenticate,
                        ieee8021XAuthPaeAuthenticated,
                        ieee8021XAuthPaeFailed,
                        ieee8021XAuthPaeReAuthEnabled,
                        ieee8021XAuthPaeQuietPeriod,
                        ieee8021XAuthPaeReauthPeriod,
                        ieee8021XAuthPaeRetryMax,
                        ieee8021XAuthPaeRetryCount
                    }
    STATUS          current
    DESCRIPTION
        "A collection of objects providing configuration information of
        an Authenticator in the system."
    ::= { ieee8021XPaeGroups 4 }

ieee8021XPaeSuppConfigGroup OBJECT-GROUP
    OBJECTS         {
                        ieee8021XSuppPaeAuthenticate,
                        ieee8021XSuppPaeAuthenticated,
                        ieee8021XSuppPaeFailed,
                        ieee8021XSuppPaeHelloPeriod,
                        ieee8021XSuppPaeRetryMax,
                        ieee8021XSuppPaeRetryCount
```

```
                    }
    STATUS          current
    DESCRIPTION
        "A collection of objects providing configuration information of
        a Supplicant in the system."
    ::= { ieee8021XPaeGroups 5 }

ieee8021XPaeEapolStatsGroup OBJECT-GROUP
    OBJECTS         {
                        ieee8021XEapolInvalidFramesRx,
                        ieee8021XEapolEapLengthErrorFramesRx,
                        ieee8021XEapolAnnouncementFramesRx,
                        ieee8021XEapolAnnouncementReqFramesRx,
                        ieee8021XEapolPortUnavailableFramesRx,
                        ieee8021XEapolStartFramesRx,
                        ieee8021XEapolEapFramesRx,
                        ieee8021XEapolLogoffFramesRx,
                        ieee8021XEapolMkNoCknFramesRx,
                        ieee8021XEapolMkInvalidFramesRx,
                        ieee8021XEapolLastRxFrameVersion,
                        ieee8021XEapolLastRxFrameSource,
                        ieee8021XEapolSuppEapFramesTx,
                        ieee8021XEapolLogoffFramesTx,
                        ieee8021XEapolAnnouncementFramesTx,
                        ieee8021XEapolAnnouncementReqFramesTx,
                        ieee8021XEapolStartFramesTx,
                        ieee8021XEapolAuthEapFramesTx,
                        ieee8021XEapolMkaFramesTx
                    }
    STATUS          current
    DESCRIPTION
        "A collection of objects providing counters and diagnostic
        information for the EAPOL in the system."
    ::= { ieee8021XPaeGroups 6 }

ieee8021XPaeKaYMkaGroup OBJECT-GROUP
    OBJECTS         {
                        ieee8021XKayMkaActive,
                        ieee8021XKayMkaAuthenticated,
                        ieee8021XKayMkaSecured,
                        ieee8021XKayMkaFailed,
                        ieee8021XKayMkaActorSCI,
                        ieee8021XKayMkaActorsPriority,
                        ieee8021XKayMkaKeyServerPriority,
                        ieee8021XKayMkaKeyServerSCI,
                        ieee8021XKayAllowedJoinGroup,
                        ieee8021XKayAllowedFormGroup,
                        ieee8021XKayCreateNewGroup,
                        ieee8021XKayMacSecCapability,
                        ieee8021XKayMacSecDesired,
                        ieee8021XKayMacSecProtect,
                        ieee8021XKayMacSecReplayProtect,
                        ieee8021XKayMacSecValidate,
                        ieee8021XKayMacSecConfidentialityOffset,
                        ieee8021XKayMkaTxKN,
                        ieee8021XKayMkaTxAN,
                        ieee8021XKayMkaRxKN,
                        ieee8021XKayMkaRxAN,
                        ieee8021XKayMkaPartKMD,
                        ieee8021XKayMkaPartNID,
                        ieee8021XKayMkaPartCached,
                        ieee8021XKayMkaPartActive,
                        ieee8021XKayMkaPartRetain,
                        ieee8021XKayMkaPartActivateControl,
                        ieee8021XKayMkaPartPrincipal,
                        ieee8021XKayMkaPartDistCKN,
                        ieee8021XKayMkaPartRowStatus,
                        ieee8021XKayMkaPeerListMN,
                        ieee8021XKayMkaPeerListType,
                        ieee8021XKayMkaPeerListSCI
                    }
    STATUS          current
```

```
    DESCRIPTION
        "A collection of objects providing monitoring and controlling
        information of a KaY MKA in the system."
    ::= { ieee8021XPaeGroups 7 }

ieee8021XPaeNetworkIdentifierGroup OBJECT-GROUP
    OBJECTS         {
                        ieee8021XLogonNIDConnectedNID,
                        ieee8021XLogonNIDRequestedNID,
                        ieee8021XLogonNIDSelectedNID,
                        ieee8021XNidUseEap,
                        ieee8021XNidUnauthAllowed,
                        ieee8021XNidUnsecuredAllowed,
                        ieee8021XNidUnauthenticatedAccess,
                        ieee8021XNidAccessCapabilities,
                        ieee8021XNidKMD,
                        ieee8021XNidRowStatus
                    }
    STATUS          current
    DESCRIPTION
        "A collection of objects providing monitoring and controlling
        information of an NID in the system."
    ::= { ieee8021XPaeGroups 8 }

ieee8021XPaeAnnouncerGroup OBJECT-GROUP
    OBJECTS         { ieee8021XAnnounceAccessStatus }
    STATUS          current
    DESCRIPTION
        "A collection of objects providing status information for
        an Announcer in the system."
    ::= { ieee8021XPaeGroups 9 }

ieee8021XPaeListenerGroup OBJECT-GROUP
    OBJECTS         {
                        ieee8021XAnnouncementKMD,
                        ieee8021XAnnouncementSpecific,
                        ieee8021XAnnouncementAccessStatus,
                        ieee8021XAnnouncementAccessRequested,
                        ieee8021XAnnouncementUnauthAccess,
                        ieee8021XAnnouncementCapabilities,
                        ieee8021XAnnouncementCipherCapability
                    }
    STATUS          current
    DESCRIPTION
        "A collection of objects providing status information for
        a Listener in the system."
    ::= { ieee8021XPaeGroups 10 }

ieee8021XPaeKaYIsupgradeGroup OBJECT-GROUP
    OBJECTS         {
                        ieee8021XKayMkaSuspendFor,
                        ieee8021XKayMkaSuspendOnRequest,
                        ieee8021XKayMkaSuspendedWhile
                    }
    STATUS          current
    DESCRIPTION
        "A collection of objects providing monitoring and control
        for MKA support of in-service upgrades."
    ::= { ieee8021XPaeGroups 11 }

ieee8021XPaeSystemAddGroup OBJECT-GROUP
  OBJECTS     {
                        ieee8021XPaeEapolGroupMAC
                    }
  STATUS      current
  DESCRIPTION
      "Objects previously overlooked, added by maintenance."
  ::= { ieee8021XPaeGroups 12 }

END
```

Insert the following text (Clause 14) after Clause 13:

14. YANG data model

14.1 PAE management using YANG

This clause specifies a YANG data model that facilitates control and monitoring of the component protocol entities and processes for a system's PAEs by providing access to the operational controls, statistics, and diagnostic capabilities specified in 12.9 and summarized in the Unified Modeling Language (UML) information model in Figure 12-3. The data model also supports management of a system's PACs for access controlled ports that are not using MACsec.

NOTE 1—The MIBs specified in Clause 13 were also derived directly from 12.9 and Figure 12-3; therefore, the capabilities and structure of the YANG data model are closely aligned with that represented by the MIBs. However, the data model has not been derived from the MIB, and no attempt has been made to include data or modeling constructs that might appear in the MIB but not in the information model.

The development of Clause 14 has been guided by the YANG guidelines published in IETF RFC 6087 [B22] as applicable to IEEE standards.

Hierarchy has been introduced by the YANG framework in the following areas:

a) The uniform resource name (URN), as specified in IEEE Std 802d, has a structure where ieee is the root (i.e., name-space identifier), followed by the standard and then the working group developing the standard.
b) The YANG objects form a hierarchy of configuration and operational data structures that define the YANG model. These hierarchical relationships are described in 14.3.
c) The Interface YANG model is augmented by the PAE YANG sub-tree model. This provides PAE specific configuration and operational data extensions that can be associated with a designated Interface.

Network interfaces are central to the management of protocols supported over the interface. Thus, it is important to establish a common data model for how interfaces are identified, configured, and monitored. The IETF Interface Management YANG data model (IETF RFC 8343) defines a generic YANG data model for the management of network interfaces. Additionally, common system level properties within a device (containing a network configuration protocol server) are provided in the IETF System Management YANG data model (IETF RFC 7317).

In general, interface type specific YANG data models (e.g., PAE) should augment the generic interfaces data model defined by the IETF Interface Management YANG data model (IETF RFC 8343). Additionally, system level properties within a device (such as a PAE System) should augment the generic system data model defined by the IETF System Management YANG data model (IETF RFC 7317).

NOTE 2—UML 2.5 [B33] conventions together with C++ language constructs are used in Clause 14 as a representation to convey model structure and relationships.

It is expected that the PAE YANG modules and PAE MIBs will not co-exist as a means to manage PAEs and PAE Systems.

NOTE 3—This standard does not preclude the support of the PAE MIB and PAE YANG module at the same time on the device. However, it is expected that the user will either use YANG or the MIB for configuration and/or state retrieval. An implementation is not required to do both.

14.2 Security considerations

The YANG modules defined in Clause 14 are designed to be accessed via the NETCONF protocol (IETF RFC 6241 [B23]). The lowest NETCONF layer is the secure transport layer. It is mandatory to implement secure transport via the NETCONF Protocol over Secure Shell (SSH) (IETF RFC 6242 [B24]). The NETCONF access control model (IETF RFC 6536 [B25]) provides the means to restrict access for particular NETCONF users to a pre-configured subset of all available NETCONF protocol operations and content.

A number of data nodes defined in this YANG module are writable/creatable/deletable (i.e., config true, which is the default). These data nodes may be considered sensitive or vulnerable in some network environments. Write operations (e.g., edit-config) to these data nodes without proper protection can have a negative effect on network operations. Listed below are the subtrees and data nodes and their sensitivity/vulnerability:

a) */system/pae-system/system-access-control*: Turning off network access control completely could render a network or a system accessing a network open to attack.
b) */interfaces/interface/pae/kay:enable*: Turning off MKA operation would prevent use of MACsec and, in turn, either deny service or render communication open to attack.
c) */nid-group*: Modifying policies for unsecured or unauthenticated communication renders the system open to attack or denies the service (and thus encourages security to be disabled).

Some of the readable data nodes in this YANG module may be considered sensitive or vulnerable in some network environments. It is thus important to control read access (e.g., via get, get-config, or notification) to these data nodes. Listed below are the subtrees and data nodes and their sensitivity/vulnerability:

d) */system/pae-system/system-access-control*: Identify network access points that are not configured to secure access.
e) */nid-group*: Identify network access points that permit unauthenticated or unsecured access to certain network services.

MACsec could also be used to provide security for network configuration protocol functions when applied to this YANG model.

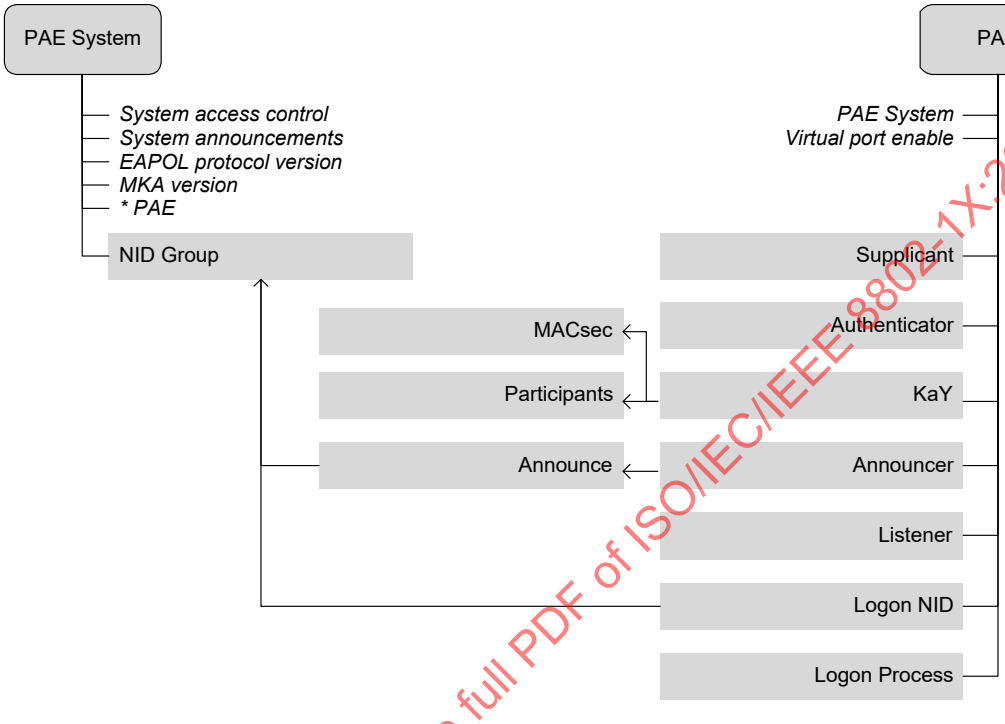
It is the responsibility of a system's implementor and administrator to ensure that the protocol entities in the system that support NETCONF, and any other remote configuration protocols that make use of these YANG modules, are properly configured to allow access only to the principals (users) that have legitimate rights to read or write data nodes. This standard does not specify how the credentials of those users are to be stored or validated.

The subject of this standard is network access control, and the YANG module(s) specified in Clause 14 that provide information can be presumed to include information that might be of use to an attacker, even if that attacker cannot directly control data that determines access rules or credentials. All the YANG module data nodes that are useful for operational management leak information about the configuration or performance of the system and might be used to direct attacks or evaluate their success. That being said, access to some data poses more significant risks, and that data is the focus of this subclause.

This standard does not specify any management operations that provide read access to certain variables, such as secret keys, that are stored and used without being disclosed directly. Extensions to this data model, or to others in the system, that could provide such access are likely to compromise the security provided and could negate the purpose of this standard. Implementations of this standard should include mechanisms to ensure such keys can be used only for specified operations (such as calculating an ICV).

14.3 802.1X YANG model structure

A single YANG module is defined in this subclause. The model is composed of two primary YANG sub-trees: a PAE System sub-tree and a PAE sub-tree (as illustrated in Figure 14-2). The overall structure and assignment of PAE objects to their groups are set out in Figure 14-1.



YANG nodes shaded in gray are containers that encompass additional leaf configuration or operational attributes. YANG nodes in white are leaf nodes that can be configurable (i.e., read-write) or operational (i.e., read-only) attributes.

Figure 14-1—YANG model structure

The PAE System YANG nodes augment the IETF System Management YANG data model (IETF RFC 7317), while the PAE YANG nodes augment the IETF Interface Management YANG data model (IETF RFC 8343), as illustrated in Figure 14-2.

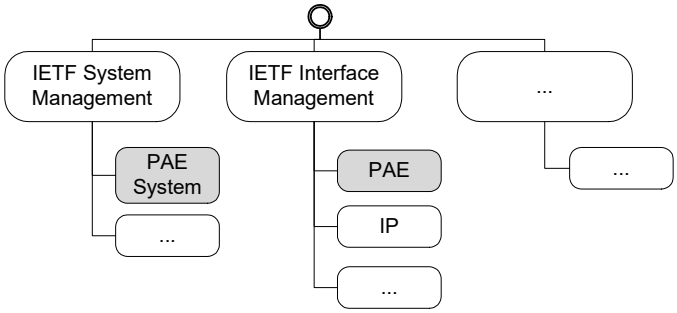


Figure 14-2—YANG object hierarchy with IEEE Std 802.1X

14.4 Relationship to other YANG data models

14.4.1 General

This standard specifies both a framework for port-based network control and particular details within that framework.

The IEEE 802.1X YANG data model augments the following key YANG models:

— IETF System Management YANG data model (IETF RFC 7317, 14.4.2)
— IETF Interface Management YANG data model (IETF RFC 8343, 14.4.3)

The use of the IEEE 802.1X YANG data model in a number of applications is described in 14.6. In some scenarios, that model is itself sufficient to meet the port-based network access control YANG data modeling requirements for particular devices. Stand-alone infrastructure devices can, for example, use pre-shared CAKs (PSKs) exclusively (i.e., require the use of MKA, but not EAP) and operate in scenarios where PSK installation by remote network management is not considered desirable. In other application scenarios, YANG data models can be required to support management of the following:

a) EAP, including the selection of EAP methods.
b) EAP credentials.
c) Trust roots to support EAP mutual authentication.
d) Provisioning and management of PSKs.
e) Policy based settings of other network parameters, depending on authorization associated with or following authentication, such as VLANs.

NOTE 1—At the time of publication of IEEE Std 802.1Xck-2018, no IEEE or IETF standards tracked any RFC YANG data model addressing the requirements for a) through e) above.

Alternately, in some scenarios for some types of devices, one or more of these requirements might continue to be met by other management frameworks, as follows:

— For a personal device such as a laptop, some information [e.g., passwords used as EAP credentials; see b) above] might be entered directly at the keyboard by a human user, while other information can be displayed for checking. Equally, information supporting secure network access might be stored or captured for later reuse in the same way that the device handles other device settings. A device that is used for a range of tasks, e.g., both personal and work-related activities, might use information provided and controlled by a number of different management frameworks.

  NOTE 2—In the model of PAE operation (12.1, Figure 12-1), the Logon Process is responsible for controlling and coordinating the use of EAP, the CAK Cache, and MKA and includes the acquisition and provision of the necessary credentials to EAP. The implementation of the Logon Process can vary to meet the needs of particular devices.

— Remote Authentication Dial-In User Service (RADIUS) (IETF RFC 2865 [B5], IETF RFC 3579 [B12]) can provide the EAP Authenticator with VLAN and other attribute settings (IETF RFC 3580 [B13], IETF RFC 4675 [B17]) to support e) above.

  NOTE 3—At the time of publication of IEEE Std 802.1Xck-2018, YANG models and YANG based management were not expected to supersede the use of RADIUS and RADIUS attributes, although a YANG model might facilitate the creation of policy profiles for use by EAP Authenticators and Supplicants or by CA members in scenarios where EAP is not used.

14.4.2 Relationship to the IETF System Management YANG data model (IETF RFC 7317)

A system implementing the IEEE 802.1X YANG data model shall also implement the IETF System Management YANG data model defined in IETF RFC 7317. The IETF System Management YANG data model defines the configuration and identification of some common system properties within a device containing a network configuration protocol (e.g., NETCONF or other mechanisms). A representation of the IETF System Management YANG data model in UML format is illustrated in Figure 14-3.

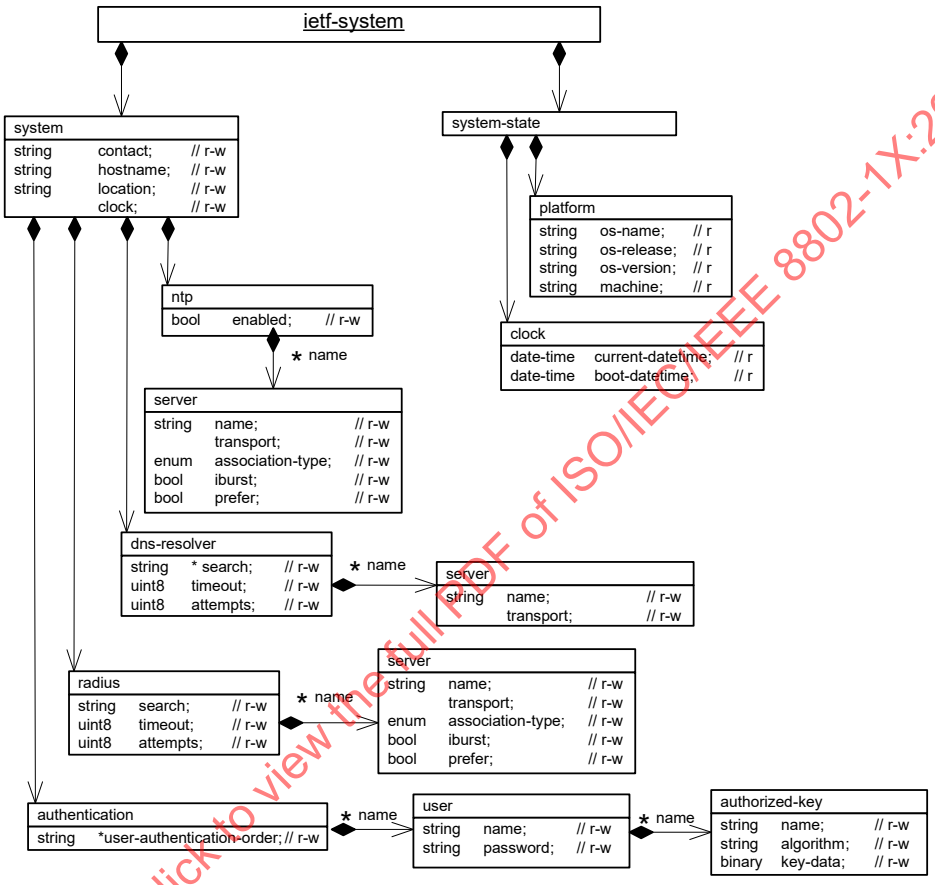


Figure 14-3—IETF System Management YANG data model

The PAE System YANG nodes augment the IETF System Management YANG data model with PAE system attributes. The system level PAE management entities outlined in 12.9.1 are contained within the PAE System YANG sub-tree. In addition, a list of PAEs that are governed by the PAE System is maintained, and a list of NIDs, which identifies the network services available to other systems attached to the same LAN, is included.

NOTE—A device can have multiple PAE Systems configured.

The PAE System cross-reference table, shown in Table 14-1, provides an association between the managed objects to the YANG module attributes.

Table 14-1—PAE System cross-reference table

PAE management information (Figure 12-3)	YANG node(s)
PAE System	**ietf-system:system:ieee802-dot1x:pae-system**
—	name
systemAccessControl (12.9.1) r-w	system-access-control
systemAnnouncements (12.9.1) r-w	system-announcements
eapolProtocolVersion (12.9.1, 11.3) r	eapol-protocol-version
mkaVersion (12.9.1, 11.3) r	mka-version
—	* pae[a]
*** NID**	**ietf-system:system:ieee802-dot1x:pae-system:nid-group**
nids (12.5)	nid — KEY
useEAP (12.5) r-w	use-eap
unauthAllowed (12.5) r-w	unauth-allowed
unsecureAllowed (12.5) r-w	unsecure-allowed
unauthenticated (12.5, 10.1) r-w	unauthenticated-access
accessCapabilities (12.5, 10.1) r-w	access-capabilities
kmd (10.4) r	kmd

[a] The asterisk (*) prior to an entity in this table represents a list of entities.

14.4.3 Relationship to the IETF Interface Management YANG data model (IETF RFC 8343)

A system implementing the IEEE 802.1X YANG data model shall also implement the IETF Interface Management YANG data model defined in IETF RFC 8343. The IETF Interface Management YANG data model defines the management of network interfaces. A representation of the IETF Interface Management YANG data model in UML format is illustrated in Figure 14-4.

NOTE—Since network interfaces are central to the management of many Internet protocols, it is important to establish a common data model for how interfaces are identified, configured, and monitored.

The PAE YANG data model augments the IETF Interface Management YANG data model with PAE configuration and state data described in Figure 12-3. If the PAE utilizes a MAC Security Entity, then the interface stack would include a SecY shim. However, if there is no MAC Security Entity, then the interface stack would include a PAC (6.4), which is a protocol-less shim. The PAC managed objects specify attributes of a shim in an interface stack (IEEE Std 802.1AC). The Controlled Port and Uncontrolled Ports are service access points provided by the PAC. Following IETF RFC 2863, these two service access points are defined as supported by separate sublayers in the interface stack, and each has an individual conceptual Interface definition. The two interfaces are created together and co-exist without interference; one is not “on the top” of the other. The IETF Interface Management YANG data model leaf nodes *higher-layer-if* and *lower-layer-if* (as illustrated in Figure 14-4, interfaces-state object),[9] are used to identify the layer relationships between the (upper) Controlled Port interface provided by the PAC and the (lower) Common Port interface that it uses.

[9] For example, the Interface stack relationship for a Link Aggregation Group (LAG) member, which is an Ethernet port, would be such that the *higher-layer-if* would reference the Interface representing the LAG, while the *lower-layer-if* would reference the Interface representing the Ethernet port.

The YANG model can be used to manage an interface stack in one of two ways. The simplest management requirements can be met by augmenting an interface whose *ifType* (iana-if-type) is that of the PAC's or SecY's Common Port (typically *ethernetCsmacd*). Frames transmitted and received by the PAE, modeled in this standard by its use of an Uncontrolled Port, are not subject to PAC or SecY control and do not contribute to the YANG Interface counters. Those interface counters reflect the use of the PAC's or SecY's Controlled Port, and the *ifType* of the augmented interface is *macSecControlledIF*.[10,11]

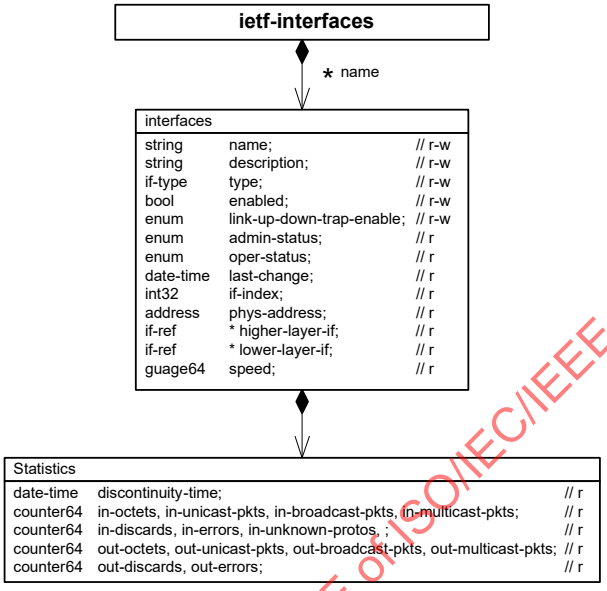


Figure 14-4—IETF Interface Management YANG data model

This simple model allows IEEE 802.1X functionality to be enabled or disabled on a port-by-port basis without any change to the interface stack and with the desirable attribute that the interface stack for an IEEE 802.1X capable Ethernet Port with IEEE 802.1X disabled (temporarily or permanently) does not differ from that for a port without IEEE 802.1X capability. Any further augmentation to the interface is assumed to be using the Controlled Port unless it is specified as using the Common Port or includes controls that specify which port it uses in the absence of a suitable default or controls that the following flexible management model needs to be used.

The MAC_Enabled and MAC_Operational parameters (6.4) are mapped to the *admin-status* and *oper-status* leaf operational nodes found within the IETF Interface Management YANG data model.

Additionally, a pointer to the PAE System by which the PAE is governed is maintained. A PAE can be associated with an end station and/or MAC Bridges, where authentication, authorization, and secure communications (in accordance with this standard) are applied on one of its ports to any other system attached to the same LAN.

The PAE cross-reference table, shown in Table 14-2, provides an association between the managed objects to the YANG module attributes.

[10] Even if PAC is used.

[11] When IEEE Std 802.1X is used in conjunction with IEEE Std 802.11, the interface type is as specified by IEEE 802.11 standards.

Table 14-2—PAE cross-reference table

PAE management information (Figure 12-3)	YANG node(s)
*** PAE[a]**	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae**
—	pae-system
vpEnable (12.7) r-w	vp-enable
r	port-name
portNumber (12.9.2) r	port-number
r	controlled-port-name
controlledPortNumber (12.9.2) r	controlled-port-number
r	uncontrolled-port-name
uncontrolledPortNumber (12.9.2) r	uncontrolled-port-number
r	common-port-name
commonPortNumber (12.9.2) r	common-port-number
implemented.supp (12.9.2) r	port-capabilities:supp
implemented.auth (12.9.2) r	port-capabilities:auth
implemented.mka (12.9.2) r	port-capabilities:mka
implemented.macsec (12.9.2) r	port-capabilities:macsec
implemented.isupgrades (12.9.2) r	port-capabilities:in-service-upgrades
implemented.announcer (12.9.2) r	port-capabilities:annoucements
implemented.listener (12.9.2) r	port-capabilities:listener
implemented.virtualPorts (12.9.2) r	port-capabilities:virtual-ports
portType (12.9.2) r	port-type
maxVirtualPorts (12.9.2) r	virtual-port:max
currentVirtualPorts (12.9.2) r	virtual-port:current
vpStart (12.7) r	virtual-port:start
vpPeerAddress (12.7) r	virtual-port:peer-address
Supplicant	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:supplicant**
heldPeriod (8.6) r-w	held-period
retryMax (8.7) r-w	retry-max
enabled (8.4) r	enabled
authenticate (8.4) r	authenticated
authenticated (8.4) r	authenticated
failed (8.4) r	failed

Table 14-2—PAE cross-reference table (*continued*)

PAE management information (Figure 12-3)	YANG node(s)
Authenticator	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:authenticator**
quietPeriod (8.6) r-w	quiet-period
reauthPeriod (8.6) r-w	reauth-period
reauthEnable (8.1) r-w	reauth-enable
retryMax (8.9) r-w	retry-max
enabled (8.4) r	enabled
authenticate (8.4) r	authenticate
authenticated (8.4) r	authenticated
failed (8.4) r	failed
KaY	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:kay**
enable (9.16) r-w	enable
actorPriority (9.16) r-w	actor:priority
keyServerPriority (9.16) r-w	key-server:priority
joinGroup (9.16) r-w	group:join
formGroup (9.16) r-w	group:form
newGroup (9.16) r-w	group:new
macsecCapable (9.16) r-w	macsec:capable
macsecDesired (9.16) r-w	macsec:desired
suspendOnRequest (9.18) r-w	suspend-on-request
suspendFor (9.18) r-w	suspend-for
actorSCI (9.16) r	actor:sci
keyServerSCI (9.16) r	key-server:sci
macsecProtect (9.16) r	macsec:protect
macsecValidate (9.16) r	macsec:validate
macsecReplayProtect (9.16) r	macsec:replay-protect
suspendedWhile (9.18) r	suspended-while
active (9.16) r	active
authenticated (9.16) r	authenticated
secured (9.16) r	secured
failed (9.16) r	failed
txKN (9.16) r	key-number:tx
rxKN (9.16) r	key-number:rx
txAN (9.16) r	association-number:tx
rxAN (9.16) r	association-number:rx

Table 14-2—PAE cross-reference table (*continued*)

PAE management information (Figure 12-3)	YANG node(s)
*** Participant**	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:kay:participant**
—	participants — KEY
cached (9.16) r-w	cached
active (9.16) r-w	active
retain (9.16) r-w	retain
activate (9.16) r-w	activate
livePeers (9.16) r	peers:*live
potentialPeers (9.16) r	peers:*potential
ckn (9.16) r	ckn
kmd (9.16) r	kmd
nid (9.16) r	nid
authData (9.16) r	auth-data
principal (9.16) r	principal
distCKN (9.16) r	dist-ckn
LogonNIDs	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:logon-nid**
selectedNID (12.5) r-w	selected
connectedNID (12.5) r	connected
requestedNID (12.5) r	requested
*** NID**	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:logon-nid:nid-group**
connectedNID, selectedNID, requestedNID (12.5)	nid — KEY
useEAP (12.5) r-w	use-eap
unauthAllowed (12.5) r-w	unauth-allowed
unsecureAllowed (12.5) r-w	unsecure-allowed
unauthenticated (12.5, 10.1) r-w	unauthenticated-access
accessCapabilities (12.5, 10.1) r-w	access-capabilities
kmd (10.4) r	kmd

Table 14-2—PAE cross-reference table (*continued*)

PAE management information (Figure 12-3)	YANG node(s)
Announcer	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:announcer**
enable (10.4) r-w	enable
*** Announce**	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:announcer.announce**
—	announces — KEY
nid (10.4) r	nid
accessStatus (10.4, 12.5) r	access-status
*** NID**	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:announcer.announce:nid-group**
nid (12.5)	nid — KEY
useEAP (12.5) r-w	use-eap
unauthAllowed (12.5) r-w	unauth-allowed
unsecureAllowed (12.5) r-w	unsecure-allowed
unauthenticated (12.5, 10.1) r-w	unauthenticated-access
accessCapabilities (12.5, 10.1) r-w	access-capabilities
kmd (10.4) r	kmd
Listener	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:listener**
enable (10.4) r-w	enable
*** Announcement**	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:listener:annoucement**
—	announcements — KEY
nid (10.4) r	nid
kmd (10.4) r	kmd
specific (10.4) r	specific
accessStatus (10.4) r	access-status
requestedNID (10.4) r	requested-nid
unauthenticatedAccess (10.4) r	unauthenticated-access
accessCapabilities (10.4) r	access-capabilities
* Ciphersuites (10.4) r	cipher-suites
—	index — KEY
—	cipherSuite
—	cipherSuiteCapability

Table 14-2—PAE cross-reference table (*continued*)

PAE management information (Figure 12-3)	YANG node(s)
EapolStatistics	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:eapol-statistics**
invalidEapolFramesRx (12.8.1) r	invalid-eapol-frame-rx
eapLengthErrorFrames (12.8.1) r	eap-length-error-frames
eapolAnnouncementsRx (12.8.1) r	eapol-announcements-rx
eapolAnnounceReqsRx (12.8.1) r	eapol-announce-reqs-rx
eapolPortUnavailable (12.8.1) r	eapol-port-unavailable
eapolStartFramesRx (12.8.1) r	eapol-start-frames-rx
eapolEapFramesRx (12.8.1) r	eapol-eap-frames-rx
eapolLogoffFramesRx (12.8.1) r	eapol-logoff-frames-rx
eapolMKnoCKN (12.8.1) r	eapol-mk-no-cfn
eapolMkInvalidFramesRx (12.8.1) r	eapol-mk-invalid-frames-rx
lastEapolFrameSource (12.8.2) r	last-eapol-frame-source
lastEapolFrameVersion (12.8.2) r	last-eapol-frame-version
eapolSuppEapFramesTx (12.8.3) r	eapol-supp-eap-frames-tx
eapolLogoffFramesTx (12.8.3) r	eapol-logoff-frames-tx
eapolAnnouncementsTx (12.8.3) r	eapol-announcements-tx
eapolAnnounceReqsTx (12.8.3) r	eapol-announce-reqs-tx
eapolStartFramesTx (12.8.3) r	eapol-start-frames-tx
eapolAuthEapFramesTx (12.8.3) r	eapol-auth-eap-frames-tx
eapolMKAFramesTx (12.8.3) r	eapol-mka-frames-tx
LogonProcess	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:logon-process**
logon (12.5) r-w	logon
connect (12.3) r	connect
portValid (12.3) r	port-valid

Table 14-2—PAE cross-reference table (*continued*)

PAE management information (Figure 12-3)	YANG node(s)
*** SessionStatistics**	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:logon-process:session-statistics**
sessionId (12.5.1) r	session-id — KEY
sessionUserName (12.5.1) r	user-name
sessionOctetsRx (12.5.1) r	octets-rx
sessionOctetsTx (12.5.1) r	octets-tx
sessionFramesRx (12.5.1) r	frames-rx
sessionFramesTx (12.5.1) r	frames-tx
sessionTime (12.5.1) r	time
sessionTerminateCause (12.5.1) r	terminate-cause
*** NID**	**ietf-interfaces:interfaces:interface:ieee802-dot1x:pae:nid-group**
nids (12.5)	nid — KEY
useEAP (12.5) r-w	use-eap
unauthAllowed (12.5) r-w	unauth-allowed
unsecureAllowed (12.5) r-w	unsecure-allowed
unauthenticated (12.5, 10.1) r-w	unauthenticated-access
accessCapabilities (12.5, 10.1) r-w	access-capabilities
kmd (10.4) r	kmd

[a] The asterisk (*) prior to an entity in this table represents a list of entities.

14.4.4 The Interface Stack Models

The YANG model supports both explicit and augmented interface models. An explicitly modeled interface represents a single shim or sublayer in an interface stack. An augmented interface combines adjacent shims or sublayers into a single interface to simplify configuration. Figure 14-5, for example, represents the structure of a simple Bridge Port explicitly, using one interface to model the IEEE 802.3 attributes of the port and another to represent attributes associated with their use as a Bridge Port. The small alphanumeric circles overlaying the larger clear circles represent the index used to identify the Interface. Here, Interface A would be an ifType of *bridge*, with a lower-layer-if of Interface B, while Interface B would be an ifType of *ethernetCsmacd* with a higher-layer-if of Interface A.

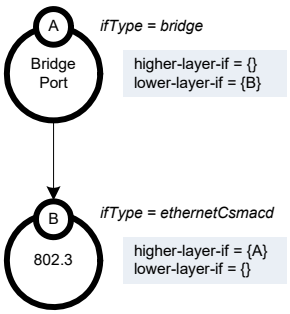


Figure 14-5—Explicit Interface Model of Bridge Port

Figure 14-6 shows the IEEE 802.3 interface, Interface A, augmented with Bridge Port configuration and operational data. Shaded circles represent protocol entities, while clear circles represent service access points (SAPs). Dashed ovals represent the set of protocol entities sharing the same Interface as the SAP.

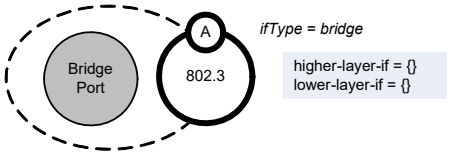


Figure 14-6—Augmented Interface Mode of Bridge Port

NOTE—In Figure 14-6, it is assumed that the network manager has overwritten the ifType to reflect the service provided by the augmented interface, i.e., that of a Bridge Port.

The support of Link Aggregation (IEEE Std 802.1AX) will also introduce further variations in the Interface Stack that can be supported. For example, as illustrated in Figure 14-7, Interface A, which is a link aggregation port, would have an ifType of *bridge* because it is augmented by the Bridge Port. The link aggregation members are represented by Interface B and Interface C, both of which are of ifType *ethernetCsmacd*. The lower-layer-if of Interface A would comprise Interface B and Interface C. The higher-layer-if of Interface B and Interface C would be Interface A.

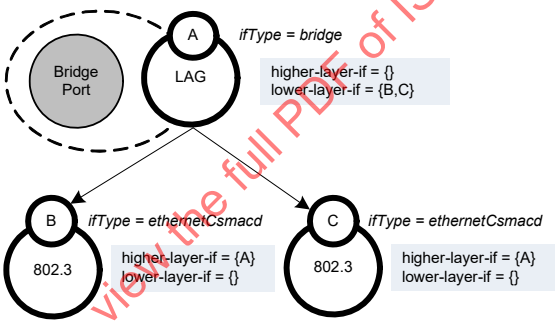


Figure 14-7—Bridge Port with LAG Interface stack model

More exacting management requirements are met with interface stacks that comprise two or more tiered YANG interfaces. For example, Figure 14-8 provides an illustration of the YANG model with MACsec. The service that provides the Common Port to a PAC or SecY is associated with an Interface and the Controlled Port; or, as in the case of Virtual Ports, the multiple Control Ports that make use of a single Common Port are separate YANG interfaces. This tiered interface stack is required for Virtual Port management and also allows use of the Controlled Port or the Common Port by other protocol entities (such as LLDP) to be specified without augmenting the YANG models for those entities.

The Interface with index of B would have an ifType of *macSecControlledIF*. The higher-layer-if of Interface B would be Interface A, while the lower-layer-if is Interface C.

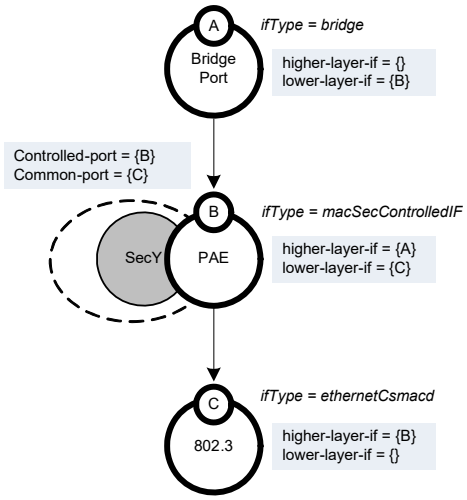


Figure 14-8—Bridge Port YANG Interface stack model with MACsec

A system can support one or both (e.g., explicit or augmented interface model) of these interface stack styles, but any change from one to another occurs only as a result of explicit management configuration, not as a side effect or as a result of dynamic conditions. The use and configuration of other YANG models can depend on the use of a simple, single-tiered, interface stack or a multi-tiered stack.

Figure 14-9 provides an illustration of an augmented interface of a Bridge Port with a PAE. The Bridge Port is the result of an augmentation of Interface A, which was of ifType *ethernetCsmacd*. Subsequently, the PAE augments Interface A.

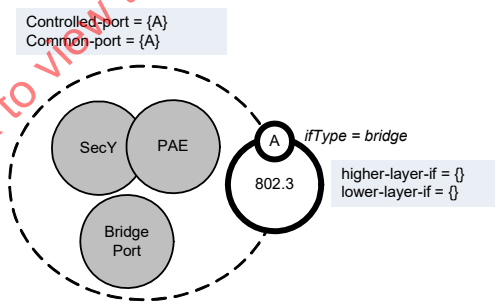


Figure 14-9—Augmented Interface Model of Bridge Port with a PAE

Figure 14-10 provides an example illustration of the YANG Interface model representing a real port and multiple virtual ports.

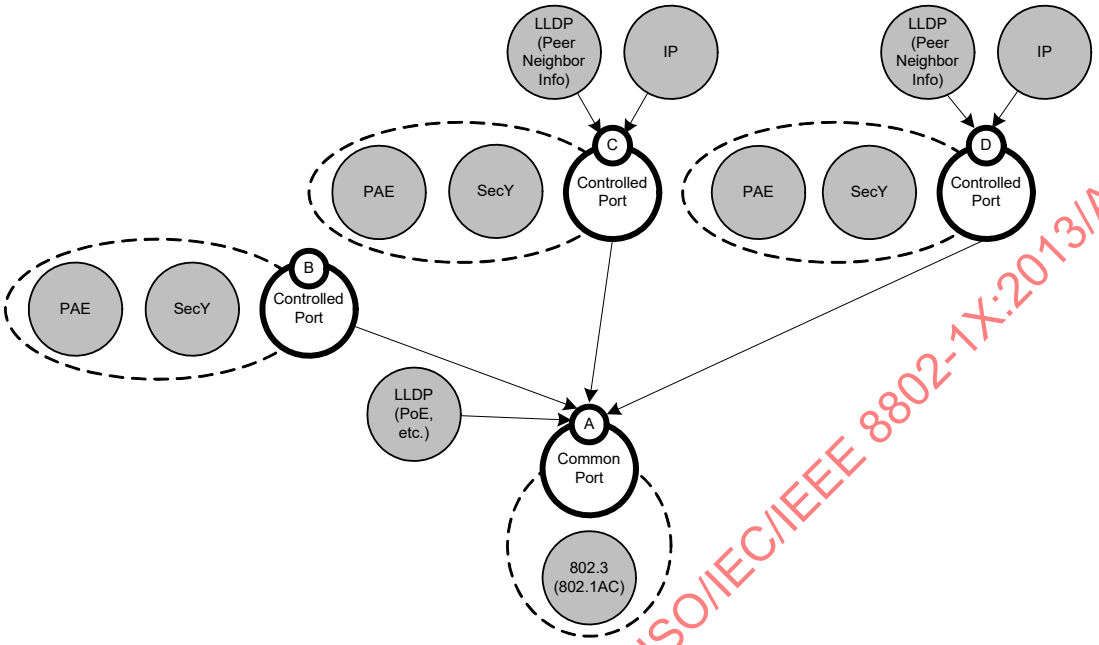


Figure 14-10—YANG Interface Model with MACsec and virtual ports

The introduction of MACsec on link aggregation members can be expressed as an explicit or augmented interface model. Figure 14-11 provides an illustration of interfaces being explicitly modeled within the interface stack of MACsec configured on aggregation members of a Bridge Port that is a LAG. Interface A of ifType *bridge* is a LAG interface augmented by Bridge Port. PAE Interface B and Interface M are inserted above Interface C and Interface N, respectively, in the stack. The Controlled-ports are Interface B and Interface M, each of which have an ifType of *macSecControlledIF*. The interface stack is very clear and explicit.

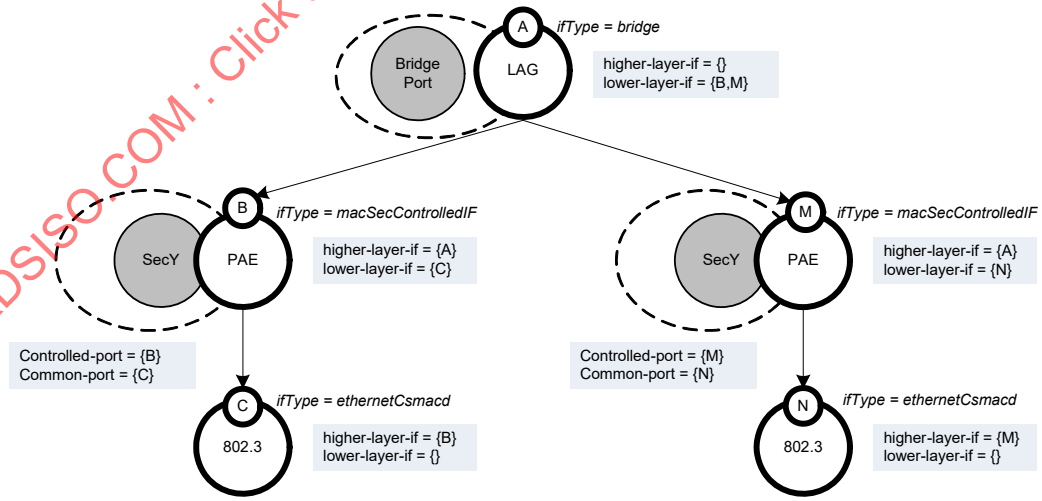


Figure 14-11—Explicit Interface Model of Bridge Port LAG with MACsec on members

Conversely, Figure 14-12 provides an illustration of an augmented interface model where the interface stack represents MACsec on aggregation members of a Bridge Port that is a LAG. Interface A of ifType *bridge* is an LAG interface augmented by Bridge Port. The PAE augments Interface B and Interface C, respectively, each of which have an ifType of *ethernetCsmacd*.

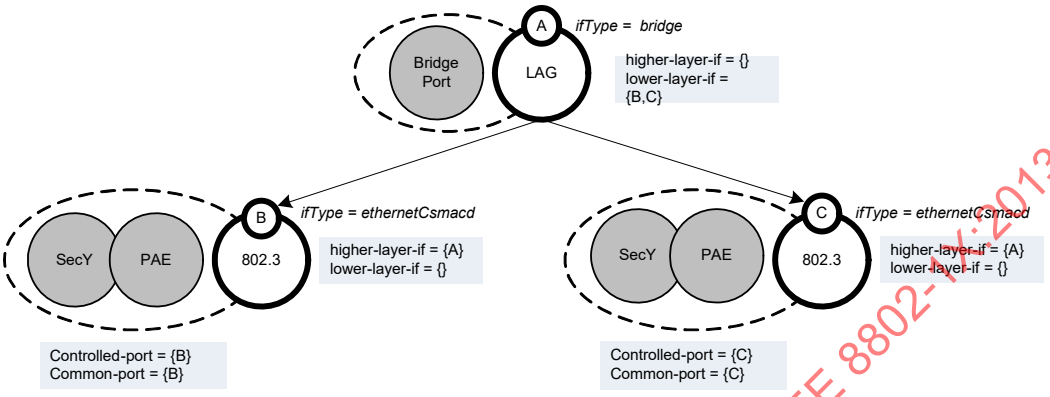


Figure 14-12—Augmented Interface Model of Bridge Port LAG with MACsec on members

The YANG models (defined in 14.5.2) support the various Interface augmentation and interface stacking strategies. Interface stacking models ranging from explicitly modeling interfaces to augmentation of interfaces can be supported. The controller (e.g., NETCONF client) can dictate which interface stack model should be used. Consideration needs to be made to select the interface stack model that is right for the usage scenario. For example, starting with an augmented interface model of a Bridge Port, as illustrated in Figure 14-6, and transitioning to a Bridge Port LAG interface stack (with or without MACsec), as illustrated in Figure 14-7, require the initial Bridge Port Interfaces to be torn down (e.g., deleted) and re-instantiated (e.g., created) to support the transition. This is not the case when starting from an explicit interface model of the Bridge Port (as illustrated in Figure 14-5).

14.5 Definition of the IEEE 802.1X YANG data model[12]

14.5.1 YANG tree schema

The YANG tree associated with the *ieee802-dot1x* module is shown below:

```
module: ieee802-dot1x
    +--rw nid-group
       +--rw pae-nid-group* [nid]
          +--rw nid                          pae-nid
          +--rw use-eap?                     enumeration
          +--rw unauth-allowed?              enumeration
          +--rw unsecure-allowed?            enumeration
          +--rw unauthenticated-access?      enumeration
          +--rw access-capabilities?         pae-nid-capabilities
          +--ro kmd?                         pae-kmd
  augment /sys:system:
    +--rw pae-system
       +--rw name?                       string
       +--rw system-access-control?      enumeration
       +--rw system-announcements?       enumeration
       +--ro eapol-protocol-version?     uint32
       +--ro mka-version?                uint32
       +--ro pae*                        if:interface-ref
  augment /if:interfaces/if:interface:
```

[12]Copyright release for YANG: Users of this standard may freely reproduce the YANG modules contained in this clause so that they can be used for their intended purpose.

```
+--rw pae
   +--rw pae-system?                dot1x:pae-system-ref
   +--rw vp-enable?                 boolean
   +--rw port-capabilities
   |  +--rw supp?                   boolean
   |  +--rw auth?                   boolean
   |  +--rw mka?                    boolean
   |  +--rw macsec?                 boolean
   |  +--rw announcements?          boolean
   |  +--rw listener?               boolean
   |  +--rw virtual-ports?          boolean
   |  +--rw in-service-upgrades?    boolean
   +--ro port-name?                   if:interface-ref
   +--ro port-number?                 pae-if-index
   +--ro controlled-port-name?        if:interface-ref
   +--ro controlled-port-number?      pae-if-index
   +--ro uncontrolled-port-name?      if:interface-ref
   +--ro uncontrolled-port-number?    pae-if-index
   +--ro common-port-name?            if:interface-ref
   +--ro common-port-number?          pae-if-index
   +--ro port-type?                   enumeration
   +--ro virtual-port
   |  +--ro max?             uint32
   |  +--ro current?         yang:gauge32
   |  +--ro start?           uint32
   |  +--ro peer-address?    ieee:mac-address
   +--rw supplicant
   |  +--rw held-period?     uint16
   |  +--rw retry-max?       uint8
   |  +--ro enabled?         boolean
   |  +--ro authenticate?    boolean
   |  +--ro authenticated?   boolean
   |  +--ro failed?          boolean
   +--rw authenticator
   |  +--rw quiet-period?    uint16
   |  +--rw reauth-period?   uint16
   |  +--rw reauth-enable?   boolean
   |  +--rw retry-max?       uint8
   |  +--ro enabled?         boolean
   |  +--ro authenticate?    boolean
   |  +--ro authenticated?   boolean
   |  +--ro failed?          boolean
   +--rw kay
   |  +--rw enable?               boolean
   |  +--rw actor
   |  |  +--rw priority?   uint8
   |  |  +--ro sci?        sci-list-entry
   |  +--rw key-server
   |  |  +--rw priority?   uint8
   |  |  +--ro sci?        sci-list-entry
   |  +--rw group
   |  |  +--rw join?   boolean
   |  |  +--rw form?   boolean
   |  |  +--rw new?    boolean
   |  +--rw macsec
   |  |  +--rw capable?          boolean
   |  |  +--rw desired?          boolean
   |  |  +--ro protect?          boolean
   |  |  +--ro validate?         boolean
   |  |  +--ro replay-protect?   boolean
   |  +--rw suspend-on-request?   boolean
   |  +--rw suspend-for?          uint8
   |  +--ro suspended-while?      uint8
   |  +--ro active?               boolean
   |  +--ro authenticated?        boolean
   |  +--ro secured?              boolean
   |  +--ro failed?               boolean
   |  +--ro key-number
   |  |  +--ro tx?   mak-kn
   |  |  +--ro rx?   mak-kn
   |  +--ro association-number
   |  |  +--ro tx?   mak-an
   |  |  +--ro rx?   mak-an
   |  +--rw participants* [participant]
   |     +--rw participant    uint32
   |     +--rw cached?        boolean
   |     +--rw active?        boolean
   |     +--rw retain?        boolean
   |     +--rw activate?      enumeration
   |     +--ro peers
   |     |  +--ro live*        sci-list-entry
```

```
|     |  +--ro potential*   sci-list-entry
|     +--ro ckn?           pae-ckn
|     +--ro kmd?           pae-kmd
|     +--ro nid?           pae-nid
|     +--ro auth-data?     pae-auth-data
|     +--ro principal?     boolean
|     +--ro dist-ckn?      pae-ckn
+--rw logon-nid
|  +--rw selected?        pae-nid
|  +--rw pae-nid-group* [nid]
|  |  +--rw nid                        pae-nid
|  |  +--rw use-eap?                   enumeration
|  |  +--rw unauth-allowed?            enumeration
|  |  +--rw unsecure-allowed?          enumeration
|  |  +--rw unauthenticated-access?    enumeration
|  |  +--rw access-capabilities?       pae-nid-capabilities
|  |  +--ro kmd?                       pae-kmd
|  +--ro connected?       pae-nid
|  +--ro requested?       pae-nid
+--rw announcer
|  +--rw enable?     boolean
|  +--rw announce* [announces]
|     +--rw announces        uint32
|     +--rw pae-nid-group* [nid]
|     |  +--rw nid                        pae-nid
|     |  +--rw use-eap?                   enumeration
|     |  +--rw unauth-allowed?            enumeration
|     |  +--rw unsecure-allowed?          enumeration
|     |  +--rw unauthenticated-access?    enumeration
|     |  +--rw access-capabilities?       pae-nid-capabilities
|     |  +--ro kmd?                       pae-kmd
|     +--ro nid?             pae-nid
|     +--ro access-status?   pae-access-status
+--rw listener
|  +--rw enable?         boolean
|  +--ro announcement* [announcements]
|     +--ro announcements             uint32
|     +--ro nid?                      pae-nid
|     +--ro kmd?                      pae-kmd
|     +--ro specific?                 boolean
|     +--ro access-status?            pae-access-status
|     +--ro requested-nid?            boolean
|     +--ro unauthenticated-access?   pae-access-status
|     +--ro access-capabilities?      pae-nid-capabilities
|     +--ro cipher-suites* [index]
|        +--ro index                    uint16
|        +--ro cipherSuite?             string
|        +--ro cipherSuiteCapability?   uint32
+--ro eapol-statistics
|  +--ro invalid-eapol-frame-rx?       yang:counter32
|  +--ro eap-length-error-frames?      yang:counter32
|  +--ro eapol-announcements-rx?       yang:counter32
|  +--ro eapol-announce-reqs-rx?       yang:counter32
|  +--ro eapol-ppdu-unavailable?       yang:counter32
|  +--ro eapol-start-frames-rx?        yang:counter32
|  +--ro eapol-eap-frames-rx?          yang:counter32
|  +--ro eapol-logoff-frames-rx?       yang:counter32
|  +--ro eapol-mk-no-cfn?              yang:counter32
|  +--ro eapol-mk-invalid-frames-rx?   yang:counter32
|  +--ro last-eapol-frame-source?      ieee:mac-address
|  +--ro last-eapol-frame-version?     yang:counter32
|  +--ro eapol-supp-eap-frames-tx?     yang:counter32
|  +--ro eapol-logoff-frames-tx?       yang:counter32
|  +--ro eapol-announcements-tx?       yang:counter32
|  +--ro eapol-announce-reqs-tx?       yang:counter32
|  +--ro eapol-start-frames-tx?        yang:counter32
|  +--ro eapol-auth-eap-frames-tx?     yang:counter32
|  +--ro eapol-mka-frames-tx?          yang:counter32
+--rw logon-process
   +--rw logon?                 boolean
   +--ro connect?               enumeration
   +--ro port-valid?            boolean
   +--ro session-statistics* [session-id]
      +--ro session-id          pae-session-id
      +--ro user-name?          pae-session-user-name
      +--ro octets-rx?          yang:counter64
      +--ro octets-tx?          yang:counter64
      +--ro frames-rx?          yang:counter64
      +--ro frames-tx?          yang:counter64
      +--ro time?               yang:timeticks
      +--ro terminate-cause?    enumeration
```

14.5.2 YANG module definition

The IEEE 802.1X YANG model is provided below:

```
module ieee802-dot1x {

  namespace "urn:ieee:std:802.1X:yang:ieee802-dot1x";
  prefix "dot1x";

  import ieee802-types { prefix "ieee"; }
  import ietf-yang-types { prefix "yang"; }
  import ietf-interfaces { prefix "if"; }
  import ietf-system { prefix "sys"; }
  import iana-if-type { prefix "ianaift"; }

  organization
    "Institute of Electrical and Electronics Engineers";

  contact
       "WG-URL: http://grouper.ieee.org/groups/802/1/
    WG-EMail: stds-802-1@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
    "Port-based network access control allows a network administrator
    to restrict the use of IEEE 802 LAN service access points (ports)
    to secure communication between authenticated and authorized
    devices. IEEE Std 802.1X specifies an architecture, functional
    elements, and protocols that support mutual authentication
    between the clients of ports attached to the same LAN and secure
    communication between the ports. The following control allows a
    port to be reinitialized, terminating (and potentially
    restarting) authentication exchanges and MKA operation, based on
    a data model described in a set of YANG modules.";

  revision 2017-10-15 {
    description
      "Updates based upon comment resolution on draft
      D1.1 of P802.1Xck.";
    reference
      "IEEE 802.1X-2010, Port-Based Network Access Control.";
  }

  /* ----------------------------------------
   * List of features that may be optionally
   * implemented/supported
   * ----------------------------------------
   */
  feature pacp-eap-supplicant {
    description
      "This feature indicates that the device supports a PACP EAP
      Supplicant.";
    reference
      "IEEE 802.1X-2010 Clause 12.9.2";
  }
  feature pacp-eap-authenticator {
    description
      "This feature indicates that the device supports a PACP EAP
      Authenticator.";
    reference
      "IEEE 802.1X-2010 Clause 12.9.2";
  }
  feature mka {
    description
      "This feature indicates that the device supports MKA";
    reference
      "IEEE 802.1X-2010 Clause 12.9.2";
  }
  feature macsec {
```

```
  description
    "This feature indicates that the device supports MACsec on the
    Controlled Port.";
  reference
    "IEEE 802.1X-2010 Clause 12.9.2";
}
feature announcements {
  description
    "This feature indicates that the device supports the ability to
    send EAPOL announcements.";
  reference
    "IEEE 802.1X-2010 Clause 12.9.2";
}
feature listener {
  description
    "This feature indicates that the device supports the ability to
    use receive EAPOL announcements.";
  reference
    "IEEE 802.1X-2010 Clause 12.9.2";
}
feature virtual-ports {
  description
    "This feature indicates that the device supports the virtual
    ports for a real port.";
  reference
    "IEEE 802.1X-2010 Clause 12.9.2";
}
feature in-service-upgrades {
  description
    "This feature indicates that the device supports MKA in-service
    upgrades.";
  reference
    "IEEE 802.1Xbx-2014 Clause 12.9.2";
}

/* ------------------------------------------------
 * Type definitions used by dot1X YANG module
 * ------------------------------------------------
 */

typedef pae-system-ref {
  type leafref {
    path "/sys:system/dot1x:pae-system/dot1x:name";
  }
  description
    "This type is used by data models that need to reference
    configured PAE systems.";
}

typedef pae-nid {
  type string {
    length "0..100";
  }
  description
    "Network Identify, which is a UTF-8 string identifying a
    network or network service.";
  reference
    "IEEE 802.1X-2010 Clause 3, Clause 10.1, Clause 12.6";
}

typedef pae-session-user-name {
  type string {
    length "0..253";
  }
  description
    "Session user name, which is a utf8 string, representing the
    identify of the peer Supplicant.";
  reference
    "IEEE 802.1X-2010 Clause 12.5.1";
}

typedef pae-session-id {
  type string {
    length "3..253";
  }
  description
    "Session Identifier, which is a utf8 string, uniquely
    identifying the session within the context of the PAEs
    system.";
  reference
    "IEEE 802.1X-2010 Clause 12.5.1";
```

```
}

typedef pae-nid-capabilities {
  type bits {
    bit eap {
      position 0;
      description
        "EAP";
    }
    bit eapMka {
      position 1;
      description
        "EAP + MKA";
    }
    bit eapMkaMacSec {
      position 2;
      description
        "EAP + MKA + MACsec";
    }
    bit mka {
      position 3;
      description
        "MKA";
    }
    bit mkaMacSec {
      position 4;
      description
        "MKA + MACsec";
    }
    bit higherLayer {
      position 5;
      description
        "Higher Layer (WebAuth)";
    }
    bit higherLayerFallback {
      position 6;
      description
        "Higher Layer Fallback (WebAuth)";
    }
    bit vendorSpecific {
      position 7;
      description
        "Vendor specific authentication mechanisms";
    }
  }
  description
    "Authentication and protection capabilities supported for the
    NID. Indicates the combinations of authentication and
    protection capabilities supported for a NID. Any set of these
    combinations can be supported.";
  reference
    "IEEE 802.1X-2010 Clause 10.1, Clause 11.12.3";
}

typedef pae-access-status {
  type enumeration {
    enum no-access {
      description
        "Other than to authentication services, and to services
        announced as available in the absence of authentication
        (unauthenticated).";
    }
    enum remedial-access {
      description
        "The access granted is severely limited, possibly to
        remedial services.";
    }
    enum restricted-access {
      description
        "The Controlled Port is operational, but restrictions have
        been applied by the network that can limit access to some
        resources.";
    }
    enum expected-access {
      description
        "The Controlled Port is operational, and access provided is
        as expected for successful authentication and authorization
        for the NID.";
    }
  }
  description
```

```
    "Indicates the transmitters Controlled Port operational status
    and current level of access resulting from authentication and
    the consequent authorization controls applied by that ports
    clients.";
  reference
    "IEEE 802.1X-2010 Clause 10.4, Clause 12.5";
}

typedef mak-kn {
  type uint32;
  description
    "Indicates a Key Number (KN) used in MKA. It is assigned by
    the Key Server (sequentially beginning with 1).";
  reference
    "IEEE 802.1X-2010 Clause 9.8, Clause 9.16";
}

typedef mak-an {
  type uint32;
  description
    "A number that is concatenated with a MACsec Secure Channel
    Identifier to identify a Secure Association. Indicates an
    Association Number (AN) assigned by the Key Server for use with
    the key number for transmission.";
  reference
    "IEEE 802.1X-2010 Clause 9.8, Clause 9.16";
}

typedef pae-ckn {
  type string {
    length "1..32";
  }
  description
    "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-2010 Clause 9.3.1, Clause 6.2";
}

typedef pae-kmd {
  type string {
    length "0..253";
  }
  description
    "A Key Management Domain (KMD). A string of up to 253 UTF-8
    characters that names the transmitting authenticators key
    management domain.";
  reference
    "IEEE Clause 12.6";
}

typedef pae-auth-data {
  type string;
  description
    "Authorization data associated with the CAK.";
  reference
    "IEEE 802.1X-2010 Clause 9.16";
}

typedef sci-list-entry {
  type string {
    length "8";
  }
  description
    "8 octet string, where the first 6 octets represents the MAC
    Address (in canonical format), and the next 2 octets represents
    the Port Identifier.";
  reference
    "IEEE 802.1AE Clause 7.1.2, Clause 10.7.1";
}

typedef pae-if-index {
     type int32 {
    range "1..2147483647";
  }
     description
            "The interface index value represented by this interface.";
}
```

```
grouping nid-group {
  description
    "The PAE NID Group configuration and operational inforamtion.";
  list pae-nid-group {
    key "nid";
    description
      "A list that contains the configuration and operational
      nodes for the network announcement information for the
      Logon Process.";
    leaf nid {
      type pae-nid;
      description
        "Identification of the network or network service.";
      reference
        "IEEE 802.1X-2010 Clause 12.5";
    }
    leaf use-eap {
      type enumeration {
        enum never {
          description
            "Never.";
        }
        enum immediate {
          description
            "Immediately, concurrently with the use of MKA with any
            cached CAK(s).";
        }
        enum mka-fail {
          description
            "Not until MKA has failed, if a prior CAK has been
            cached.";
        }
      }
      default "immediate";
      description
        "Determines when the Logon Process will initiate EAP, if
        the Supplicant and or Authenticator are enabled, and takes
        one of the above values.";
      reference
        "IEEE 802.1X-2010 Clause 12.5";
    }
    leaf unauth-allowed {
      type enumeration {
        enum never {
          description
            "Never.";
        }
        enum immediate {
          description
            "Immediately, independently of any current or future
            attempts to authenticate using the PAE or MKA.";
        }
        enum auth-fail {
          description
            "Not until an attempt has been made to authenticate
            using EAP, unless neither the supplicant nor the
            authenticator is enabled, and MKA has attempted to use
            any cached CAK (unless the KaY is not enabled).";
        }
      }
      default "immediate";
      description
        "Determines when the Logon Process will tell the CP state
        machine to provide unauthenticated connectivity, and takes
        one of the above values.";
      reference
        "IEEE 802.1X-2010 Clause 12.5";
    }
    leaf unsecure-allowed {
      type enumeration {
        enum never {
          description
            "Never.";
        }
        enum immediate {
          description
            "Immediately, to provide connectivity concurrently with
            the use of MKA with any CAK acquired through EAP.";
        }
        enum mka-fail {
          description
```

```
            "Not until MKA has failed, or is not enabled.";
          }
          enum mka-server {
            description
              "Only if directed by the MKA server.";
          }
        }
        default "immediate";
        description
          "Determines when the Logon Process will tell the CP state
          machine to provide authenticated but unsecured
          connectivity, takes one of the above values.";
        reference
          "IEEE 802.1X-2010 Clause 12.5";
      }
      leaf unauthenticated-access {
        type enumeration {
          enum no-access {
            description
              "Other than to authentication services.";
          }
          enum fallback-access {
            description
              "Limited access can be provided after authentication
              failure.";
          }
          enum limited-access {
            description
              "Immediate limited access is available without
              authentication.";
          }
          enum open-access {
            description
              "Immediate access is available without
              authentication.";
          }
        }
        default "no-access";
        description
          "Unauthenticated access capabilities provided by the NID.";
        reference
          "IEEE 802.1X-2010 Clause 10.1";
      }
      leaf access-capabilities {
        type pae-nid-capabilities;
        description
          "Authentication and protection capabilities supported for
          the NID.";
        reference
          "IEEE 802.1X-2010 Clause 10.1";
      }

      leaf kmd {
        type pae-kmd;
        config false;
        description
          "The Key Management Domain for the NID.";
        reference
          "IEEE 802.1X-2010 Clause 10.4";
      }
    }
  }

  grouping port-capabilities {
    description
      "Per port PAE feature capabilities.";
    leaf supp {
      type boolean;
      description
        "Indicates if PACP EAP Supplicant is supported.";
      reference
        "IEEE 802.1X-2010 Clause 12.9.2";
    }
    leaf auth {
      type boolean;
      description
        "Indicates if PACP EAP Authenticator is supported.";
      reference
        "IEEE 802.1X-2010 Clause 12.9.2";
    }
    leaf mka {
```

```
      type boolean;
      description
        "Indicates if MKA is supported.";
      reference
        "IEEE 802.1X-2010 Clause 12.9.2";
    }
    leaf macsec {
      type boolean;
      description
        "Indicates if MACsec on the Controlled port is supported.";
      reference
        "IEEE 802.1X-2010 Clause 12.9.2";
    }
    leaf announcements {
      type boolean;
      description
        "Indicates if the ability to send EAPOL announcements is
        supported.";
      reference
        "IEEE 802.1X-2010 Clause 12.9.2";
    }
    leaf listener {
      type boolean;
      description
        "Indicates if the ability to use received EAPOL
        announcements is supported.";
      reference
        "IEEE 802.1X-2010 Clause 12.9.2";
    }
    leaf virtual-ports {
      type boolean;
      description
        "Indicates if virtual ports for a real port is supported.";
      reference
        "IEEE 802.1X-2010 Clause 12.9.2";
    }
    leaf in-service-upgrades {
      type boolean;
      description
        "Indicates if MKA in-service upgrades is supported.";
      reference
        "IEEE 802.1Xbx-2014 Clause 12.9.2";
    }
  }

  /* ------------------------------------------------
   * Configuration objects used by 802.1X YANG module
   * ------------------------------------------------
   */
  augment "/sys:system" {
    description
      "Augment system with 802.1X PAE System specific configuration
      nodes.";
    container pae-system {
      description
        "Contains all 802.1X PAE System specific related
        configuration and operational data.";
      leaf name {
        type string;
        description
          "The name which uniquely identifies the PAE System.";
      }
      leaf system-access-control {
        type enumeration {
          enum disabled {
            description
              "Deletes any virtual ports previously instantiated, and
              terminates authentication exchanges and MKA
              operation.";
          }
          enum enabled {
            description
              "Enables PAE system access control.";
          }
        }
        description
          "Setting this control to disabled deletes any virtual ports
          previously instantiated, and terminates authentication
          exchanges and MKA operation. Each real port PAE behaves as
          if enabledVirtualPorts was clear, the PAEs Supplicant,
          Authenticator, and KaY as if their enabled controls were
```

```
          clear, and Logon Process(es) as if unauthAllowed was
          Immediate. Announcements can be transmitted (subject to
          other controls), both periodically and in response to
          announcement requests (conveyed by EAPOL-Starts or
          EAPOL-Announcement-Reqs) but are sent with a single NID
          Set, with a null NID, and the Access Information TLV (and
          no other) with an pae-access-status of No Access,
          accessRequested false, OpenAccess, and no
          accessCapabilities. The control variable settings for each
          real port PAE are unaffected, and will be used once
          systemAccessControl is set to enabled.";
        reference
          "IEEE 802.1X-2010 Clause 12.9.1";
      }
      leaf system-announcements {
        type enumeration {
          enum disabled {
            description
              "Causes each PAE to behave as if enabled were clear
              for the PAEs Announcement functionality.";
          }
          enum enabled {
            description
              "Enables PAE system announcements.";
          }
        }
        description
          "Setting this control to Disabled causes each PAE to behave
          as if enabled were clear for the PAE's Announcement
          functionality. The independent controls for each PAE apply
          if systemAnnouncements is Enabled.";
        reference
          "IEEE 802.1X-2010 Clause 12.9.1";
      }
      leaf eapol-protocol-version {
        type uint32;
        config false;
        description
          "The EAPOL protocol version for this system.";
        reference
          "IEEE 802.1X-2010 Clause 12.9.1, Clause 11.3";
      }
      leaf mka-version {
        type uint32;
        config false;
        description
          "The MKA protocol version for this system.";
        reference
          "IEEE 802.1X-2010 Clause 12.9.1, Clause 11.3";
      }
      leaf-list pae {
        type if:interface-ref;
        config false;
        description
          "List of PAE references.";
      }
    }
}

/*
 *  Port Authentication Entity (PAE) Nodes
 */
augment "/if:interfaces/if:interface" {
  when "if:type = 'ianaift:ethernetCsmacd' or
        if:type = 'ianaift:ilan' or
        if:type = 'ianaift:macSecControlledIF' or
        if:type = 'ianaift:ptm'" {
    description
      "Applies to the Controlled Port of SecY or PAC shim or
      Ethernet related Interface.";
  }
  description
    "Augment interface model with PAE configuration and
     operational nodes.";
  reference
    "IEEE 802.1AE Clause 11.7 and IEEE 802.1X-2010 Clause 6.5 and
    Clause 13.3.2";
  container pae {
    description
      "Contains PAE configuration and operational related nodes.";
    leaf pae-system {
```

```
    type dot1x:pae-system-ref;
    description
      "The PAE system that this PAE is a member of.";
  }
  leaf vp-enable {
    when "../port-type = 'real-port' and
          ../port-capabilities/virtual-ports = 'true'" {
      description
        "Applies when port is Real Port and virtual port
        capabilities are supported.";
    }
    type boolean;
    default "false";
    description
      "A real ports PAE may be configured to create virtual
      ports to support multi-access LANs provided that MKA and
      MACsec operation is enabled for that port.";
    reference
      "IEEE 802.1X-2010 Clause 12.7";
  }
  container port-capabilities {
    description
      "Per port PAE feature capabilities.";
    uses port-capabilities;
  }

  leaf port-name {
    type if:interface-ref;
    config false;
    description
      "Each PAE is uniquely identified by a port name.";
    }
  leaf port-number {
    type pae-if-index;
    config false;
    description
      "Each PAE is uniquely identified by a port number. The
      port number used is unique amongst all port names 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 ports 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.";
    reference
      "IEEE 802.1X-2010 Clause 12.9.2";
    }
  leaf controlled-port-name {
    type if:interface-ref;
    config false;
    description
      "Each PAE is uniquely identified by a port name.";
  }
  leaf controlled-port-number {
    type pae-if-index;
    config false;
    description
      "The port for the associated PAC or SecYs Controlled
      Port.";
    reference
      "IEEE 802.1X-2010 Clause 12.9.2";
  }
  leaf uncontrolled-port-name {
    type if:interface-ref;
    config false;
    description
      "The uncontrolled port name reference.";
  }
  leaf uncontrolled-port-number {
    type pae-if-index;
    config false;
    description
      "The port for the associated PAC or SecYs Uncontrolled
      Port.";
    reference
      "IEEE 802.1X-2010 Clause 12.9.2";
  }
  leaf common-port-name {
```

```
    type if:interface-ref;
    config false;
    description
      "The common port name reference.";
  }
  leaf common-port-number {
    type pae-if-index;
    config false;
    description
      "The port for the associated PAC or SecYs Common Port. All
      the virtual ports created for a given real port share the
      same Common Port and commonPortNumber.";
    reference
      "IEEE 802.1X-2010 Clause 12.9.2";
  }
  leaf port-type {
    type enumeration {
      enum real-port {
        description
          "Real Port type.";
      }
      enum virtual-port {
        description
          "Virtual Port type.";
      }
    }
    //config false;
    description
      "The port type of the PAE.";
    reference
      "IEEE 802.1X-2010 Clause 12.9.2";
  }
  container virtual-port {
    when "../port-capabilities/virtual-ports = 'true'" {
      description
        "Applies when the virtual ports port capability is
        supported.";
    }
    config false;
    description
      "Contains Virtual Port operational state information.";
    leaf max {
      when "../../port-type = 'real-port'" {
        description
          "Applies when Port is a Real Port.";
      }
      type uint32;
      description
        "The guaranteed maximum number of virtual ports.";
      reference
        "IEEE 802.1X-2010 Clause 12.9.2";
    }
    leaf current {
      when "../../port-type = 'real-port'" {
        description
          "Applies when Port is a Real Port.";
      }
      type yang:gauge32;
      description
        "The current number of virtual ports.";
      reference
        "IEEE 802.1X-2010 Clause 12.9.2";
    }
    leaf start {
      when "../../port-type = 'virtual-port'" {
        description
          "Applies when Port is a Virtual Port.";
      }
      type uint32;
      description
        "Set if the virtual port was created by receipt of an
        EAPOL-Start frame.";
      reference
        "IEEE 802.1X-2010 Clause 12.9.7";
    }
    leaf peer-address {
      when "../../port-type = 'virtual-port'" {
        description
          "Applies when Port is a Virtual Port.";
      }
      type ieee:mac-address;
```