INTERNATIONAL STANDARD

ISO/IEC/IEEE 8802-1AE

First edition
2013-12

AMENDMENT 3
2018-10

Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks —

Part 1AE: Media access control (MAC) security

AMENDMENT 3: Ethernet data encryption devices

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Réseaux locaux et métropolitains —

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

AMENDEMENT 3:

Reference number
ISO/IEC/IEEE 8802-1AE:2013/Amd.3:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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 8802-1AE:2013/FDAmd 3 was prepared by the LAN/MAN of the IEEE Computer Society (as IEEE Std 802.1AEcg-2017) 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 802.1AEcg™-2017
(Amendment to
IEEE Std 802.1AE™-2006
as amended by
IEEE Std 802.1AEbn™-2011
and IEEE Std 802.1AEbw™-2013)

IEEE Standard for
Local and metropolitan area networks—

Media Access Control (MAC) Security

Amendment 3:
Ethernet Data Encryption devices

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 14 February 2017
IEEE-SA Standards Board

Abstract: Ethernet Data Encryption devices (EDEs) are specified in this amendment. An EDE is a two-port bridge that uses MACsec to provide secure connectivity for attached customer bridges, or for attached provider bridges. EDEs may allow the customer (or provider) bridges to continue to use a VLAN Identifier (VID) in transmitted frames to select (as already specified in IEEE Std 802.1Q™) between provider network or provider backbone network services.

Keywords: amendment, authorized port, confidentiality, data origin authenticity, EDE, Ethernet Data Encryption device, IEEE 802.1AE, IEEE 802.1AEcg, 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

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

PDF: ISBN 978-1-5044-3725-7 STD22415
Print: ISBN 978-1-5044-3726-4 STDPD22415

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Standards Documents."

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

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

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

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

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

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

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. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

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

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at http://ieeexplore.ieee.org/browse/standards/collection/ieee or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE-SA Website at http://standards.ieee.org.

Errata

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

Patents

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

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

Participants

At the time this standard was completed, the IEEE 802.1 working group had the following membership:

Glenn Parsons, *Chair*
John Messenger, *Vice Chair*
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
Marc Holness
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 standard. Balloters may have voted for approval, disapproval, or abstention.

Thomas Alexander
Richard Alfvin
Johann Amsenga
Butch Anton
Nancy Bravin
William Byrd
Juan Carreon
Keith Chow
Charles Cook
Rodney Cummings
Janos Farkas
Matthias Fritsche
Yukihiro Fujimoto
Joel Goergen
Randall Groves
Joseph Gwinn
Stephen Haddock
Marco Hernandez
Werner Hoelzl
Noriyuki Ikeuch
Osamu Ishida
Atsushi Ito
Raj Jain
SangKwon Jeong
Piotr Karocki
Jeritt Kent
Stuart Kerry
Yongbum Kim
Hyeong Ho Lee
James Lepp
Jon Lewis
Elvis Maculuba
Michael McInnis
Michael Montemurro
Michael Newman
Satoshi Obara
Bansi Patel
Arumugam Paventhan
Karen Randall
Alon Regev
Maximilian Riegel
Robert Robinson
Jessy Rouyer
Richard Roy
Mick Seaman
Thomas Starai
Walter Struppler
Patricia Thaler
Thomas Tullia
Mark-Rene Uchida
Prabodh Varshney
George Vlantis
Khurram Waheed
Hung-Yu Wei
Andreas Wolf
Chun Yu Charles Wong
Oren Yuen
Zhen Zhou

When the IEEE-SA Standards Board approved this standard on 14 February 2017, it had the following membership:

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

Chuck Adams
Masayuki Ariyoshi
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Gary Hoffman
Michael Janezic
Thomas Koshy
Joseph L. Koepfinger1
Kevin Lu
Daleep Mohla
Damir Novosel
Ronald C. Petersen
Annette D. Reilly
Robby Robson
Dorothy Stanley
Adrian Stephens
Mehmet Ulema
Phil Wennblom
Howard Wolfman
Yu Yuan

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802.1AEcg-2017, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Security—Amendment 3: Ethernet Data Encryption devices.

The first edition of IEEE Std 802.1AE™ was published in 2006. A first amendment, IEEE Std 802.1AEbn™-2011, added the option of using the GCM-AES-256 Cipher Suite. A second, IEEE Std 802.1AEbw™-2013 added the GCM-AES-XPN-128 and GCM-AES-XPN-256 Cipher Suites. These extended packet numbering Cipher Suites allow more than 2^{32} frames to be protected with a single Secure Association Key (SAK) and so ease the timeliness requirements on key agreement protocols for very high speed (100 Gb/s plus) operation. This third amendment, IEEE Std 802.1AEcg™-2017, specifies Ethernet Data Encryption devices (EDEs).

Relationship between IEEE Std 802.1AE and other IEEE Std 802 standards

IEEE Std 802.1X™-2010 specifies Port-based Network Access Control, and provides a means of authenticating and authorizing devices attached to a LAN, and includes the MACsec Key Agreement protocol (MKA) necessary to make use of IEEE 802.1AE.

IEEE Std 802.1AE is not intended for use with IEEE Std 802.11™ Wireless LAN Medium Access Control. An amendment to that standard, IEEE Std 802.11i™-2004, also makes use of IEEE Std 802.1X™, thus facilitating the use of a common authentication and authorization framework for LAN media to which this standard applies and for Wireless LANs.

Contents

Figures

Tables

IEEE Standard for
Local and metropolitan area networks—

Media Access Control (MAC) Security

Amendment 3:
Ethernet Data Encryption devices

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

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

1. Overview

1.2 Scope

Change 1.2 as follows:

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

NOTE—The MAC Clients are as specified in IEEE Std 802, ~~IEEE Std 802.2™, IEEE Std 802.1D™,~~ IEEE Std 802.1Q™, and IEEE Std 802.1X™.[1]

To this end it

a) Specifies the requirements to be satisfied by equipment claiming conformance to this standard.
b) Specifies the requirements for MAC Security in terms of provision of the MAC Service and the preservation of the semantics and parameters of service requests and indications.
c) Describes the threats, both intentional and accidental, to correct provision of the service.
d) Specifies security services that prevent, or restrict, the effect of attacks that exploit these threats.
e) Examines the potential impact of both the threats and the use of MAC Security on the Quality of Service (QoS), specifying constraints on the design and operation of MAC Security ~~entities and protocols~~.
f) Models support of the secure MAC Service in terms of the operation of media access control method independent MAC Security Entities (SecYs) within the MAC Sublayer.
g) Specifies the format of the MACsec Protocol Data Unit (MPDUs) used to provide secure service.
h) Identifies the functions to be performed by each SecY, and provides an architectural model of its internal operation in terms of Processes and Entities that provide those functions.
i) ~~Specifies the interface/exchanges between a SecY and its associated and collocated MAC Security Key Agreement Entity (KaY, IEEE Std 802.1X) that provides and updates cryptographic keys.~~
i) Specifies each SecY's use of an associated and collocated Port Access Entity (PAE, IEEE Std 802.1X™) to discover and authenticate MACsec protocol peers, and its use of that PAE's Key Agreement Entity (KaY) to agree and update cryptographic keys.
j) Specifies performance requirements and recommends default values and applicable ranges for the operational parameters of a SecY.
k) Specifies how SecYs are incorporated within the ~~architectural structure within~~ architecture of end stations, ~~and~~ bridges, and two-port Ethernet Data Encryption devices (EDEs).
l) Establishes the requirements for management of MAC Security, identifying the managed objects and defining the management operations for SecYs.
m) Specifies the Management Information Base (MIB) module for managing the operation of MAC Security in TCP/IP networks.
n) Specifies requirements, criteria, and choices of Cipher Suites for use with this standard.

~~This standard does not~~

o) ~~Specify how the relationships between MACsec protocol peers are discovered and authenticated, as supported by key management or key distribution protocols, but makes use of IEEE IEEE Std 802.1X™ to achieve these functions.~~

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

2. Normative references

Change the Normative references clause as follows:

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

~~Federal Information Processing Standards FIPS 197, Advanced Encryption Standard, 2001, Advanced Encryption Standard Cyclic Block Chaining (AES-CBC).[1]~~

IEEE Std 802®, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture.[2, 3]

~~IEEE Std 802.1D-2003, IEEE Standards for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges.~~

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

IEEE Std 802.1X-2010™, IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control.

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

IEEE Std 802.1AB™~~-2005~~, IEEE Standards 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 802.2™, IEEE Standard for 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~~Information technology—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.~~

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

~~IEEE Std 802.11i™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11:~~

[1] ~~FIPS publications are available from the National Technical Information Service (NTIS), U. S. Dept. of Commerce, 5285 Port Royal Rd., Springfield, VA 22161 (http://www.ntis.org/).~~

[2] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, ~~P.O. Box 1331,~~ Piscataway, NJ 0885~~45-1331~~, USA. IEEE publications can be ordered on-line from the IEEE Standards website: http://www.standards.ieee.org. Through the IEEE Standards Association, industry, and government support, select IEEE standards are available for download at no charge, see http://www.standards.ieee.org/about/get.

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

~~Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Media Access Control (MAC) Security Enhancements.~~

~~IEEE Std 802.17™, 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 & physical layer specifications.~~

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

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

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

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

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

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

~~ISO/IEC 7498-1, Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 1: The Basic Model[4].~~

~~ISO/IEC 7498-2, Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security architecture.~~

ISO/IEC 14882, Information Technology—Programming languages—C++.[4]

~~ISO/IEC 15802-1, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 1: Medium Access Control (MAC) service definition.~~

NIST SP 800-38D, Nov 2007, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.[5]

[4]ISO/IEC publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse (http://www.iso.ch/). ISO/IEC publications are also available in the United States from Global Engineering Documents, 15 Inverness Way East, Englewood, Colorado 80112, USA (http://global.ihs.com/). Electronic copies are available in the United States from the American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (http://www.ansi.org/).

[5]This document is available at http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

3. Definitions

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

3.1 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 the MAC Service defined in ~~ISO/IEC 15802-1~~ IEEE Std 802.1AC. IEEE 802 LANs include IEEE Std 802.3 (CSMA/CD), IEEE Std 802.11 (Wireless), IEEE Std 802.17 (Resilient Packet Ring).

Change the definition of Port Identifier as follows:

3.29 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 port number, identifier, or index. 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.

Change the definition of Secure Channel Identifier as follows:

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

NOTE—Key agreement protocols such as MKA (see IEEE Std 802.1X) 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). SCI uniqueness does not rely on MAC Address allocation procedures.

Insert the following definition(s), in the appropriate collating order, renumbering notes as required:

3.41 Ethernet Data Encryption device (EDE): A two-port bridge that transmits and receives frames that are assumed to be unprotected to and from one red-side port, and conditionally relays those frames to and from its other black-side port, protecting and verifying frames transmitted and received on the black-side port using MACsec.

3.42 black-side: Identifies the EDE port that uses MACsec to protect transmitted frames and verify received frames.

3.43 red-side: Identifies the EDE port that does not use MACsec to protect transmitted frames or verify received frames.

3.44 Reserved Address: A group address filtered by a bridge component to restrict the scope of the control protocols using that destination address.

3.45 user priority: In this standard, the priority associated with a transmit request received by a SecY's Controlled Port. The priority associated with a transmit request received by a protocol entity, often a shim, in an interface stack (see IEEE Std 802.1AC).

3.46 access priority: In this standard, the priority associated with a transmit request made by a SecY at its Common Port. The priority associated with a transmit request made by a protocol entity, often a shim, in an interface stack (see IEEE Std 802.1AC).

3.47 edge component: The bridge component in an EDE-CS, EDE-CC, or EDE-SS that is attached to the red-side port.

3.48 network component: The bridge component in an EDE-CS, EDE-CC, or EDE-SS that is attached to the black-side port.

3.49 Customer Edge Port: The red-side port of an EDE-CS, EDE-CC, or EDE-SS.

NOTE—The terms *customer* and *provider* applied to the external and internal ports of an EDE-CS are those used by IEEE Std 802.1Q in its description of Provider Edge Bridges and reflect the role of those ports in the layered network architecture. They do not indicate control or ownership of the equipment. In this standard it is convenient to extend the use of those terms to ports that have the same relative relationship to the edge and network components of an EDE-CC or EDE-SS. This is not a suggestion that further variants of PEBs and BEBs be specified, as the existence of additional variants would complicate interoperability, service provision, and the task of this standard.

3.50 Provider Edge Port: A port on the edge component of an EDE-CS, EDE-CC, or EDE-SS that provides internal connectivity to the network component of that EDE.

3.51 Customer Network Port: A port on the network component of an EDE-CS, EDE-CC, or EDE-SS that provides internal connectivity to the edge component of that EDE.

3.52 Provider Network Port: The black-side port of an EDE-CS, EDE-CC, or EDE-SS.

4. Abbreviations and acronyms

Insert the following abbreviations in the appropriate collating sequence:

EDE	Ethernet Data Encryption device
EDE-CC	Ethernet Data Encryption device with red-side recognition of C-TAGs and black-side addition and removal of C-TAGs
EDE-CS	Ethernet Data Encryption device with red-side recognition of C-TAGs and black-side addition and removal of S-TAGs
EDE-M	VLAN-unaware Ethernet Data Encryption device operating as a Customer Bridge
EDE-SS	Ethernet Data Encryption device with red-side recognition of S-TAGs and black-side addition and removal of S-TAGs
MKA	MACsec Key Agreement protocol (IEEE Std 802.1X)
PCP	Priority Code Point (IEEE Std 802.1Q)
UNI	User Network Interface (IEEE Std 802.1Q)

5. Conformance

Change Clause 5 as follows:

A claim of conformance to this standard is a claim that the behavior of an implementation of a MAC Security Entity (SecY) meets the requirements of this standard as they apply to the operation of the MACsec protocol, management of its operation, and provision of service to the protocol clients of the SecY, as revealed through externally observable behavior of the system of which the SecY forms a part.

A claim of conformance may be a claim of full conformance, or a claim of conformance with Cipher Suite variance, as specified in 5.4.

Conformance to this standard does not ensure that the system of which the MAC Security implementation forms a part is secure, or that the operation of other protocols used to support MAC Security, such as key management and network management do not provide a way for an attacker to breach that security.

Conformance to this standard does not require any restriction as to the nature of the system of which a SecY forms part other than as constrained by the SecY's required and optional capabilities (5.3, 5.4). Clause 11 describes the use of SecYs within a number of different types of systems. These include, but are not limited to, systems specified in IEEE Std 802.1Q and those that make use of IEEE Std 802.1X. Successful interoperable use of MACsec in those systems also requires conformance to those standards. In addition Clause 15 of this standard makes use of components specified in IEEE Std 802.1Q to define further systems, Ethernet Data Encryption devices (EDEs), whose purpose is to secure the MAC Service within networks comprising bridging systems specified by IEEE Std 802.1Q in a way that is transparent to the operation of those bridging systems. Additional claims of conformance can be made to this standard in respect of EDEs (5.5–5.7).

5.1 Requirements terminology

For consistency with existing IEEE and IEEE 802.1 standards, requirements placed upon conformant implementations of this standard are expressed using the following terminology:

a) ***shall*** is used for mandatory requirements;

b) ***may*** is used to describe implementation or administrative choices (***may*** means ***is permitted to***, and hence, ***may*** and ***may not*** mean precisely the same thing);

c) ***should*** is used for recommended choices (the behaviors described by ***should*** and ***should not*** are both permissible but not equally desirable choices).

The PICS proforma (see Annex A) reflects the occurrences of the words *shall, may,* and *should* within the standard.

The standard avoids needless repetition and apparent duplication of its formal requirements by using ***is***, ***is not***, ***are***, and ***are not*** for definitions and the logical consequences of conformant behavior. Behavior that is permitted but is neither always required nor directly controlled by an implementor or administrator, or whose conformance requirement is detailed elsewhere, is described by ***can***. Behavior that never occurs in a conformant implementation or system of conformant implementations is described by ***cannot***. ~~The word ***allow*** is used as a replacement for the cliche Support the ability for, and the word ***capability*** means can be configured to.~~

5.2 Protocol Implementation Conformance Statement (PICS)

The supplier of a~~n~~ MAC Security Entity (SecY) implementation that is claimed to conform to this standard shall complete a copy of the PICS proforma provided in Annex A (normative) and shall provide the information necessary to identify both the supplier and the implementation.

The supplier of an EDE that is claimed to conform to this standard shall complete a copy of the PICS proforma provided in Annex D (normative) and shall provide the information necessary to identify both the supplier and the implementation. The supplier of an EDE implementation shall also complete or provide copies of the following PICS proforma(s) adhering to any restrictions required by conformance to this standard and marking any exceptions required by conformance to this standard.

a) For all types of EDE, the PICS proforma for each SecY implementation provided in Annex A of this standard.

b) For all types of EDE, the PICS proforma specified by IEEE Std 802.1X.

c) For an EDE-M: the IEEE Std 802.1Q PICS proforma as required for a VLAN-unaware MAC Bridge.

d) For an EDE-CS: the IEEE Std 802.1Q PICS proforma as required for a Provider Edge Bridge.

e) For an EDE-CC: the IEEE Std 802.1Q PICS proforma as required for each of the two C-VLAN components.

f) For an EDE-SS: the IEEE Std 802.1Q PICS proforma as required for each of the two S-VLAN components.

5.3 ~~Required capabilities~~MAC Security Entity requirements

An implementation of a MAC Security Entity (SecY) for which conformance to this standard is claimed shall

a) Support the Controlled and Uncontrolled Ports, and use a Common Port as specified in Clause 10.

b) Support the MAC status and point-to-point parameters for the Controlled and Uncontrolled Ports as specified in 6.4, 6.5, and 10.7.

c) Process transmit requests from the Controlled Port as required by the specification of Secure Frame Generation (10.5).

d) Process receive indications from the Common Port as required by the specification of Secure Frame Verification (10.6), prior to causing receive indications at the Controlled Port.

e) Encode and decode MACsec PDUs as specified in Clause 9.

f) Use a ~~globally unique~~ 48-bit MAC Address and a 16-bit Port Identifier unique within the scope of that address assignment to identify ~~the~~ each transmit SCI, as specified in 8.2.1.

g) Satisfy the performance requirements specified in Table 10-1 and 8.2.2.

h) Support the Layer Management Interface (LMI) operations required by the Key Agreement Entity as specified in Clause 10.

i) Provide the management functionality specified in 10.7.

j) Protect and validate MACsec PDUs by using Cipher Suites as specified in 14.1.

k) Support Integrity Protection using the Default Cipher Suite specified in Clause 14.

l) For each Cipher Suite implemented, support a minimum of
   1) One receive SC
   2) Two receive SAKs
   3) One transmit SC
   4) One of the two receive SAKs at a time for transmission, with the ability to change from one to the other within the time specified in Table 10-1

m) Specify the following parameters for each Cipher Suite implemented
   1) The maximum number of receive SCs supported
   2) The maximum number of receive SAKs
   3) The maximum number of transmit SCs supported

An implementation of a ~~MAC Security Entity (~~SecY~~)~~ for which conformance to this standard is claimed shall not

n) Introduce an undetected frame error rate greater than that achievable by preserving the original FCS, as required by 10.4.
o) Implement any Cipher Suite that is additional to those specified in Clause 14 and does not meet all the criteria specified in 14.2, 14.3, and 14.4.1.
p) Support access to MACsec parameters by a management agent using any version of SNMP prior to v3.

An implementation of a ~~MAC Security Entity (~~SecY~~)~~ for which full conformance to this standard is claimed shall not:

q) Implement Cipher Suites other than those specified in Clause 14.

NOTE—Conformance with Cipher Suite variance is allowed, as specified in 5.4 and in 14.4.1.

5.4 ~~Optional capabilities~~MAC Security Entity options

An implementation of a MAC Security Entity (SecY) for which conformance to this standard is claimed may

a) ~~Support network management using the MIB specified in Clause 13.~~
b) ~~Support access to the MIB specified in Clause 13 using SNMP version v3 or higher.~~
a) Support access to MACsec parameters by a management agent using SNMP version v3 and the MIB module specified in Clause 13.
b) Support more than one receive SC.
c) Support more than two receive SAKs.
d) Support more than one transmit SC.
e) Support Confidentiality Protection using the Default Cipher Suite without a confidentiality offset, as specified in Clause 14.
f) Support Confidentiality Protection using the Default Cipher Suite with a confidentiality offset, as specified in Clause 14.
g) Include Cipher Suites that are specified in Clause 14 in addition to the Default Cipher Suite.

An implementation of a SecY that supports more than one transmit SC shall:

h) Support a Traffic Class Table and an Access Priority Table as specified in 10.7.17.

An implementation of a ~~MAC Security Entity (~~SecY~~)~~ for which conformance with Cipher Suite variance is claimed may:

i) Use Cipher Suites not specified in Clause 14, but meeting the criteria specified in 14.2, 14.3, 14.4.1.

~~NOTE—The term *capability* is used to describe a set of related detailed provisions of this standard. Each capability can comprise both mandatory provisions, required if implementation of the capability is to be claimed, and optional provisions. Each detailed provision is specified in one or more of the other clauses of this standard. The PICS, described in Annex A, provides a useful checklist of these provisions~~

5.5 EDE conformance

Ethernet Data Encryption devices (EDEs) of various types comprise bridging systems and bridge components used as specified in this standard. Clause 15 provides a taxonomy, specification, and a description of the intended use of each type (EDE-M, EDE-CC, EDE-CS, or EDE-SS).

The bridging system and/or bridge components that comprise an implementation of an EDE that is claimed to conform to this standard shall conform to the requirements of (and may use any of the options and recommendations permitted by) IEEE Std 802.1Q, IEEE Std 802.1X, and the provisions of this standard for each MAC Security Entity that is part of the EDE implementation, with the restrictions, additions, exceptions, and clarifications specified in this standard for that type of EDE.

An implementation of any type of EDE that is claimed to conform to this standard shall

a) Have two and only two externally accessible Bridge Ports, a red-side port and a black-side port.

   NOTE—A red-side port can also be referred to as the *customer* or *edge* port and the black-side port as a *provider* or *network* port. The use of either or both of the pair of terms, *customer/provider* and *edge/network* to refer to an EDE-M's ports is consistent with the relative roles played by ports in multicomponent bridges and EDEs.

b) Associate a PAE that includes a KaY capable of operating MKA with each SecY required by this standard for the particular type of EDE (15.2, 15.4, 15.5, 15.6, 15.7).

5.6 EDE-M conformance

An implementation of an EDE-M (15.2, 15.4) that is claimed to conform to this standard shall

a) Comprise a VLAN-unaware MAC Bridge as specified by IEEE Std 802.1Q (IEEE Std 802.1Q-2014 5.14) with the constraints and exceptions specified in this standard.
b) Incorporate a SecY in the black-side port interface stack (15.2, 15.4).
c) Be capable of being configured to secure connectivity within a customer or provider network (as specified in 15.2), using the Nearest non-TPMR group address for group-addressed EAPOL PDUs, and filtering frames whose destination MAC Address is a TPMR component Reserved Address or the Nearest non-TPMR Bridge group address.
d) Be capable of being configured to secure connectivity across a PBN to a peer EDE-M, MACsec-capable Customer Bridge, or an EDE-CS (as specified in 15.4 and 15.5), using the Nearest Customer Bridge group address for group addressed EAPOL PDUs and filtering frames whose destination MAC Address is a C-VLAN component Reserved Address with the exception of the Nearest Customer Bridge group address.

and may

e) Be capable of being configured to secure connectivity across a PBN to a peer EDE-CC (as specified in 15.6), using the EDE-CC PAE group address for group addressed EAPOL PDUs, and filtering

frames whose destination MAC Address is a C-VLAN component Reserved Address or the EDE-CC PAE group address.

f) Be capable of being configured to recover signaled priority from a C-VLAN tag and to priority tag (or not) frames transmitted by the black-side port as specified in 15.4.

5.7 EDE-CS conformance

An implementation of an EDE-CS (15.5) that is claimed to conform to this standard shall

a) Comprise a Provider Edge Bridge as specified by IEEE Std 802.1Q (IEEE Std 802.1Q-2014 5.10.2) including one and only one C-VLAN component (identified by this standard as the edge component of the EDE) and an S-VLAN component (the network component of the EDE).
b) Incorporate a SecY in each of the internal Provider Edge Port interface stacks (15.5).
c) Be capable of being configured to use the Nearest Customer Bridge group address for group addressed EAPOL PDUs (15.5).

5.8 EDE-CC conformance

An implementation of an EDE-CC (15.6) that is claimed to conform to this standard shall

a) Comprise two C-VLAN components, each as specified by IEEE Std 802.1Q (IEEE Std 802.1Q-2014 5.5)—an edge component and a network component—internally connected as specified in 15.6.
b) Incorporate a SecY in each of the internal Provider Edge Port interface stacks (15.6).
c) Be capable of being configured to use the EDE-CC PAE group address as the destination MAC address of group addressed EAPOL PDUs for group addressed EAPOL PDUs (as specified in 15.6).
d) Filter and not forward all frames whose destination MAC address is either one of the addresses identified by IEEE Std 802.1Q as a C-VLAN component Reserved Address or the EDE-CC PAE group address.
e) Transmit frames received from the red-side customer port and relayed to the black-side network port untagged if they were received untagged and C-tagged with the same C-VID if they were C-tagged on receipt (15.6).

5.9 EDE-SS conformance

An implementation of an EDE-SS (15.7) that is claimed to conform to this standard shall

a) Comprise two S-VLAN components, each as specified by IEEE Std 802.1Q (IEEE Std 802.1Q-2014 5.6)—an edge component and a network component—internally connected as specified in 15.7.
b) Incorporate a SecY in each of the internal Provider Edge Port interface stacks (15.7).
c) Be capable of being configured to use the EDE-SS PAE group address as the destination MAC address of group addressed EAPOL PDUs for group addressed EAPOL PDUs (as specified in 15.7).
d) Filter and not forward all frames whose destination MAC address is either one of the addresses identified by IEEE Std 802.1Q as an S-VLAN component Reserved Address or the EDE-SS PAE group address.

Transmit frames received from the red-side customer port and relayed to the black-side network port untagged if they were received untagged and S-tagged with the same S-VID if they were S-tagged on receipt (15.7).

6. Secure provision of the MAC Service

Change the fourth note as follows:

NOTE 4—The MAC Service and the secure MAC Service are provided at a service access point to a single client. The client is either a logical link control (LLC) Entity or an entity that in turn provides the MAC Service or a MAC Internal Sublayer Service (IEEE Std ~~802.1D~~ 802.1AC, IEEE Std 802.1Q).

6.1 MAC Service primitives and parameters

Change the first paragraph of 6.1 as follows:

The MAC Service (~~ISO/IEC 15802-1~~ IEEE Std 802.1AC) provides unconfirmed connectionless-mode data transfer between source and destination stations. The invocation of a request primitive at a service access point within a source station results, with a high probability, in a corresponding indication primitive at selected service access points in destination stations. A single service request at one service access point results in no more than one service indication at each of the other service access points.

Change the third paragraph of 6.1 and the notes as follows:

The MAC Service can be provided by a single LAN or by a Bridged Local Area Network. The service provided to an LLC Client in an end station is specified in ~~ISO/IEC 15802-1~~ IEEE Std 802.1AC. The service provided by a LAN to a MAC Bridge is the MAC Internal Sublayer Service (ISS), ~~(see IEEE Std 802.1D),~~ an extension of the MAC Service that includes parameters necessary to the bridge relay function including the frame check sequence (FCS). Except as otherwise explicitly noted, the term *MAC Service* as used in the remainder of this clause refers both to the provision of the MAC Service to an LLC client and to provision of the ISS. Multiple instances of the MAC Service can be provided using a single instance of the ISS and supported in VLAN-aware Bridges using the Enhanced Internal Sublayer Service (EISS), (see ~~6.6 of~~ IEEE Std 802.1Q). When a VLAN TAG (IEEE Std 802.1Q) is used to distinguish the service instances supported, the additional parameters of the EISS are all encoded within the ISS MSDU.

NOTE 1—The MAC Service defined in ~~ISO/IEC 15802-1~~ IEEE Std 802.1AC is an abstraction of the features common to a number of specific media access control methods and is a guide to the development of client protocols.

NOTE 2—Some older descriptions of the MAC Service omit the source address parameter. With the addition of this parameter and removal of the frame_type parameter from the ISS (frames other than user_data_frames are always discarded by ISS clients, and thus can be discarded by the media access control method specific functions that provide the ISS), the definitions of the MAC Service and of the Internal Sublayer Service are expected to converge in the future.

NOTE 3—The priority parameter described in this clause is also referred to as the user_priority in some specifications. The functions that support the ISS can calculate an access_priority for use on a LAN in local support of the user_priority. ~~The access_priority parameter can be modified by media access control method specific functions and is not delivered as a MAC Service indication parameter, so is not a concern of this specification.~~

6.2 MAC Service connectivity

Change the third note as follows:

NOTE 3—The original Spanning Tree Protocol (STP) could create loops in the network if symmetric connectivity was not provided. The Rapid Spanning Tree Protocol (RSTP), (see IEEE Std 802.1~~D~~Q), detects non-symmetric connectivity between Bridges, but will deny service until the problem is resolved, and intermittent non-symmetric connectivity can result in data loops. For example, the operation of the OSPF routing protocol on a LAN is inefficient unless all participants can receive frames sent by each other. If a LAN that provides the ISS to attached MAC Bridges merely delivers frames to their intended destination instead of providing full connectivity, learning of source addresses can be inhibited and frames flooded throughout the bridged network for an indefinite period.

6.4 MAC status parameters

Change the fourth paragraph of 6.4 and the note as follows:

The value of the MAC_Enabled and MAC_Operational parameters are determined by the specific entity providing the MAC Service. ~~IEEE Std 802.1D~~ IEEE Std 802.1AC and IEEE Std 802.1Q specify how that determination is made for provision of the insecure ISS by specific media access control methods, and for provision of the insecure EISS. This standard specifies how these parameters are determined for the secure MAC Service.

NOTE—Correct provision and use of the MAC_Operational parameter is essential for high performance implementation of RSTP (IEEE Std 802.1~~D~~Q), Multiple Spanning Tree Protocol (MSTP, IEEE Std 802.1Q), and Link Aggregation Control Protocol (LACP, IEEE Std ~~802.3~~ 802.1AX). In the absence of this parameter, loss of connectivity is determined by repetitive loss of protocol frames that are normally transmitted at intervals of a few seconds, and it is assumed that frames transmitted immediately after a medium availability transition have a high probability of not being received by protocol peers.

6.5 MAC point-to-point parameters

Change the fourth paragraph of 6.5 and the note as follows:

IEEE Std ~~802.1D~~ 802.1AC and IEEE Std 802.1Q specify how the point-to-point status determination is made for provision of the insecure ISS by specific media access control methods, and for provision of the insecure EISS. This standard specifies how it is determined for the secure MAC Service.

NOTE—RSTP ~~(IEEE Std 802.1D)~~ and MSTP (IEEE Std 802.1Q) require the use of operPointToPointMAC to facilitate rapid reconfiguration in some network failure scenarios. LACP (IEEE Std ~~802.3~~ 802.1AX) does not aggregate links that are not point-to-point and ~~may~~ can use operPointToPointMAC to make this determination.

6.10 Quality of service maintenance

Change the fourth paragraph of 6.10 and split it into two paragraphs as follows:

The operation of MACsec introduces no additional frame loss on individual LAN segments other than that expected for a specific media access control method as a consequence of a small increase in frame size. The operation of MACsec between two customer systems across a provider bridged network can introduce additional frame loss caused by possible frame reordering from expedited forward or link aggregations within the provider bridged network. The reception of misordered frames can cause MACsec implementations to discard additional frames depending upon the configuration of replay protection parameters. MACsec can use separate secure channels to transmit frames with different access priorities and thus reduce or eliminate undesirable frame discard resulting from the mutual reordering of those frames.

Conforming implementations of MACsec are capable of applying a new keying material starting with any frame in a sequence that is received with the minimum intervening spacing specified by the specific media access control method in use. Each frame protected by MACsec remains independent of its predecessors and successors, so loss of a single frame does not imply loss of additional frames.

Change the tenth paragraph of 6.10 as follows:

Use of MACsec on each of a MAC Bridge's Ports will force a change in the data covered by an FCS, even if the frame is being relayed between LANs that use the same media access control method. Application of the techniques described in ~~Annex F of IEEE Std 802.1D~~ Annex O of IEEE Std 802.1Q allow an

implementation to achieve an arbitrarily small increase in undetected frame error rate, even in cases where the data that is within the coverage of the FCS is changed.

Change the twelfth paragraph of 6.10 as follows:

Where MACsec is used to support an instance of the ISS that in turn supports the EISS, encoding of the priority parameter of the EISS within the ISS MSDU ensures that priority can be communicated unchanged between service access points that are attached to a single LAN. Since MACsec is terminated ~~on each of the Ports of MAC Bridges attached to such LANs, a Bridge~~ at each of those service access points, a bridge that makes use of that ISS instance to support one of its ports can access or change the priority even if the two instances of MACsec encrypt the MSDU in order to provide confidentiality. An Access Priority Table (10.7.17) can be used to derive the access priority requested from the medium supporting the ISS from the priority requested by the user of the EISS.

7. Principles of secure network operation

7.1 Support of the secure MAC Service by an individual LAN

Insert the following paragraph after the last paragraph of 7.1:

In the above examples (Figure 7-3, Figure 7-6), each station transmits frames using a single SC. A station can also use multiple transmit SCs, using each transmitted frame's priority to allocate to it one of the SCs. Each of these transmit SCs supports secure transmission for frames of one or more priorities from the transmitting station to all the others in the CA. This use of multiple transmit SCs allows MACsec to enforce in-order delivery (or the use of a smaller replay window than might otherwise be the case) for frames of any given priority.

7.1.2 Secure Channel (SC)

Change 7.1.2 as follows:

Each SecY transmits frames conveying secure MAC Service requests of any given priority on a single SC. Each SC provides unidirectional point-to-multipoint communication, and it can be long lived, persisting through SAK changes. Each SC is identified by a Secure Channel Identifier (SCI) comprising a ~~uniquely allocated~~ 48-bit MAC address concatenated with a 16-bit ~~port number~~ Port Identifier.

NOTE 1—Including the Port Identifier ~~Using an SC identifier that includes a port number~~ component would appear to be unnecessary in the case of a simple system ~~that comprises a single LAN station,~~ with a ~~uniquely allocated 48-bit~~ MAC address~~,~~ and a single SecY for each port. However, some systems require support for more SecYs than they have uniquely allocated addresses, ~~either~~ because they make use of technologies that support virtual MACs, ~~or~~ because their interface stacks include the possibility of including multiple SecYs at different sublayers (as do Provider Bridges [IEEE Std 802.1Q], for example), or because they transmit frames of different priorities using different SCs. ~~Provider bridges (IEEE Std 802.1Q) provide examples of the latter.~~

NOTE 2—An EPON Optical Line Terminator (OLT) can use a distinct SC to support the Single Copy Broadcast (SCB) capability (Clause 12). The formal identifier for this SC comprises a System Identifier for the OLT and a reserved Port ~~Number~~ Identifier. ~~b~~Both can be represented in the secured frame by a single SCB bit (Clause 9).

MACsec Key Agreement is responsible for informing each SecY of the identifier to be used for ~~the~~ each transmitting ~~SecY~~ SC, and of the existence and identifier of each of the SCs for which the SecY is to receive frames. While the structure of the communication facilitated by each SC is point-to-multipoint (which encompasses point-to-point as a special case) the SecY does not have to be aware that its transmissions can reach multiple receivers, that the frames that it receives could be received by other SecYs, or of any relationship or lack of relationship between the inbound SCs (except in determining the value of the operPointToPointMAC status parameter, 6.5, 10.7.4). The operation of the MACsec Key Agreement protocol (MKA; specified in IEEE Std 802.1X) is defined in terms of the behavior of participants, each representing a single KaY and a single transmit SCI. When a SecY uses multiple transmit SCIs, each SCI is represented by a separate participant that sends and receives MKPDUs to and from all the other participants just as if it were representing a separate SecY in the same group CA, see Annex E (informative).

NOTE 3—The point-to-multipoint nature of the SC does have technical consequences, in particular the decision to change from one SA to another is made by the transmitter using the SC, not by one or some number of the receivers.

7.1.3 Secure Association (SA)

Change the first paragraph of 7.1.3 as follows:

Each SC comprises a succession of SAs, each with a different SAK. Each SA is identified by the SC identifier concatenated with a two-bit Association Number (AN, Figure 7-7). The Secure Association

Identifier (SAI) thus created allows the receiving SecY to identify the SA and thus the SAK used to decrypt and authenticate the received frame. The ~~AN, and hence the~~ SAI~~,~~ is only unique for the SAs ~~that can be~~ used ~~or recorded~~ by ~~participating~~ SecYs participating in a given CA at any instant.

Change the third and fourth paragraphs of 7.1.3 as follows:

The decision to replace one SA with its successor is made by the SecY that transmits using the SC, after MACsec Key Agreement has informed it that all the other SecYs are prepared to receive using that SA. No notification, other than receipt of a secured frame with a different SAI is sent to the receiver. At any one instant a SecY has to be capable of storing SAKs for two SAs for each inbound SC, and of swapping from one SA to another without notice. Certain LAN technologies can reorder frames of different priority, so reception of frames on a single SC can use interleaved SAs. The time bound within which a receiver can accept interleaved SAs is 0.5 s.

The transmitting SecY does not interleave frames for different SAs on a given SC.

NOTE—When MKA (see IEEE Std 802.1X) is used to distribute the SAKs used by each of the SCs supporting a given CA, the same SAK is used for all SAs with a given AN (at any given time). The transmit SA for each SC is replaced with its successor at approximately the same time so that there is no need for any SecY participating in the CA to support more than two SAKs at a time.

Replace Figure 7-7 with the following:

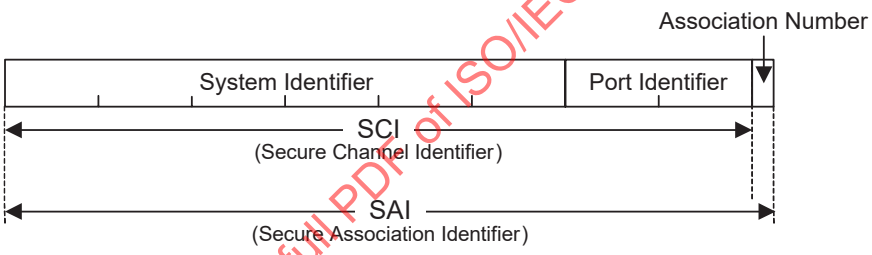


Figure 7-7—Secure Channel and Secure Association Identifiers

7.3 Use of the secure MAC Service

Change the fourth and fifth paragraphs of 7.3 as follows:

The client policies in use at any time should reflect the intersection of the capabilities permitted to the members of the CA. Policies can be

a) Selected by the client on the basis of the level of authorization, as provided by the ~~KaY~~ PAE through a layer management interface (LMI) (see 10.7) or
b) Selected by a central server that forms part of the management framework for the network, and
   1) Securely downloaded or
   2) Communicated to the client using a secure connection

~~MACsec Key Agreement supports mechanisms that securely bind downloads and secure connections to their intended client, thus protecting against a rights amplification attack.~~

7.3.1 Client policies

Delete NOTE 1 as follows, renumbering the subsequent note:

~~NOTE 1—To facilitate policy selection by clients of the secure MAC Service, IEEE Std 802.1X specifies authorized permissions, including those required by MAC Bridges (IEEE Std 802.1D) and VLAN aware Bridges (IEEE Std 802.1Q) to support the secure MAC Service in Bridged and Virtually Bridged Local Area Networks.~~

7.3.2 Use of the secure MAC Service by bridges

Change the second paragraph of 7.3.2 and the accompanying note as follows:

~~MACsec Key Agreement can use discovery protocols to identify SecYs that can participate in a CA. These protocols use a Reserved Group MAC Address that is normally filtered by bridges to restrict each instance of the secure MAC Service to an individual LAN.~~

PAEs and KaYs use group addressed frames to identify and communicate with peers whose SecYs are potential participants in the same CA. Frames with the group addresses used for this purpose are filtered by certain bridges and EDEs (Clause 15) to restrict each instance of the secure MAC Service to the appropriate LAN scope. By default PAEs and KaYs for MAC Bridges, VLAN Bridges, Provider Bridges, and Provider Backbone Bridges use the PAE group address specified by IEEE Std 802.1X (also identified as the Nearest Non-TMPR group address by IEEE Std 802.1Q). Use of this address restricts each instance of the secure MAC Service to an individual customer LAN.

~~NOTE 2—Use of this address ensures that the physical topology as perceived by spanning tree protocols aligns with that provided by MAC Security. In Provider Bridged Networks, the Provider Bridge Group Address is used. An exception to the alignment rule occurs with certain types of interface that are supported by Provider Bridge Networks, where a provider operated C-VLAN (see IEEE Std 802.1Q) aware component provides the customer interface.~~

NOTE 2—Use of Reserved Group MAC Addresses helps to ensure that the physical topology as perceived by spanning tree and other configuration protocols aligns with that provided by MAC Security.

Change the third note in 7.3.2 as follows:

NOTE 3—A Bridge Port is one of the bridge's points of attachment to an instance of the MAC Internal Sublayer Service (ISS), and is used by the MAC Relay Entity and associated Higher-Layer Entities as specified in ~~IEEE Std 802.1D and~~ IEEE Std 802.1Q.

8. MAC Security Protocol (MACsec)

8.1.1 Security requirements

Delete the note in 8.1.1 as follows:

~~NOTE—Key lifetimes are a property of the authentication and authorization provided by key agreement, and can therefore be restricted independently by any system in the CA.~~

8.2.1 SC identification requirements

Change 8.2.1 as follows:

~~The system shall have a globally unique 48-bit MAC Address, the Secure System Address, that can be used to compose the SCI (7.1.2, 9.9), and be capable of allocating a unique 16-bit Port Identifier within the scope of that address.~~

~~NOTE—The Secure System Address can be used for other purposes.~~

Each SecY shall be capable of identifying each of its transmit SCs with an SCI that comprises a unique 48-bit MAC Address and a 16-bit Port Identifier that is unique within the scope of that address (7.1.2, 9.9).

NOTE—MKA (IEEE Std 802.1X) verifies that each participant in any given CA has a unique SCI, as part of satisfying Cipher Suite requirements prior to establishing secure communication.

8.2.5 Authentication requirements

Change 8.2.5 as follows:

The ~~KaY~~ PAE supports mutual authentication of peer stations, and the SecY assumes that such authentication has taken place.

8.2.6 Authorization requirements

Change 8.2.6 as follows:

The ~~KaY~~ PAE provides authorization of services to be delivered to a peer station. ~~The minimum authorization provided should be Host and Infrastructure. Communication of authorization to users of the MAC service occurs via the LMI.~~

~~The KaY provides information to local services to allow cryptographic binding of configuration tunnels (for example, VLAN) to the authenticated connection.~~

The ~~KaY~~ PAE provides information to local services about the currently selected Cipher Suite.

8.3 MACsec operation

Change the fourth paragraph of 8.3 as follows:

On transmission, the frame is first assigned to a transmit SC and to the ~~an~~ SA (7.1.3), identified ~~locally~~ by its Association Number (AN) (see 7.1.3, 9.6), that will be used by that SC to protect the transmitted frame. The AN is used to identify the SAK (7.1.3) and the next PN (3.27, 9.8) for that SA. The AN, the SCI (7.1.2), and the PN are encoded in the SecTAG (the SCI can be omitted for point-to-point CAs if only one transmit SC is

in use) along with the MACsec EtherType (9.8) and the number of octets in the frame following the SecTAG (SL, 9.7) if less than 48 (8.1.3).

9. Encoding of MACsec protocol data units

9.9 Secure Channel Identifier (SCI)

Change 9.9 as follows:

If the SC bit in the TCI is set, the SCI (7.1.2, 8.2.1) is encoded in octets 9 through 16 of the SecTAG, and facilitates

a) Identification of the SA where the CA comprises three or more ~~peers~~ SCs
b) Network management identification of the SecY that has transmitted the frame

Octets 9 through 14 of the SecTAG encode the System Identifier component of the SCI. This comprises the six octets of a ~~globally unique~~ MAC address ~~uniquely~~ associated with the system that includes the transmitting SecY. The octet values and their sequence conform to the Canonical Format specified by IEEE Std 802.

Octets 15 and 16 of the SecTAG encode the Port Identifier component of the SCI, as an integer.

NOTE—The 64-bit value FF-FF-FF-FF-FF-FF-FF-FF is never used as an SCI and is reserved for use by implementations to indicate the absence of an SC or an SCI in contexts where an SC can be present.

An explicitly encoded SCI field in the SecTAG is not required on point-to-point links, which are identified by the operPointToPointMAC status parameter of the service provider, if the transmitting SecY uses only one transmit SC. In ~~the point-to-point~~ that case, the secure association created by the SecY for the peer SecYs, together with the direction of transmission of the secured MPDU, can be used to identify the transmitting SecY. ~~and t~~Therefore, an explicitly encoded SCI is unnecessary. Although the SCI does not have to be repeated in each frame when only two SecYs participate in a CA (see Clause 8, Clause 9, and Clause 10), the SCI (for Cipher Suites using a 32-bit PN) or the SSCI (for Cipher Suites using a 64-bit PN) still forms part of the cryptographic computation.

10. Principles of MAC Security Entity (SecY) operation

Change the note following the initial paragraph of Clause 10 as follows:

NOTE—Clause 6 defines the properties of the secure MAC Service, Clause 7 describes the security relationships used to support the service and how the service is used, providing the context within which each SecY operates, Clause 8 sets out requirements for the MACsec protocol and introduces the operation of the protocol, and Clause 9 specifies the encoding of parameters in MPDUs. This clause does not repeat all the information provided in those prior clauses, but includes sufficient reference to facilitate an understanding of SecY operation. IEEE Std 802.1AC-2012 Clause 7 and IEEE Std 802.1X-2010 Annex D describe the basic architectural concepts and terms used in this clause, including service, service access point, service primitive, and ports.

10.1 SecY overview

Change the sixth and following paragraphs and notes of 10.1 as follows:

The KaY is part of the Port Access Entity (IEEE Std 802.1X) associated with the SecY and uses the service provided by the Uncontrolled Port to transmit and receive frames that support key agreement protocols. These frames are distinguished by EtherType, so other selected protocol entities can also communicate using insecure frames by making use of ~~an~~ the Uncontrolled Port ~~provided by the KaY as illustrated in Figure 10-2~~.

~~The KaY also uses the Controlled Port provided by the SecY, providing its own Controlled Port for use by other protocols. This allows the KaY to provide MAC status parameters (6.4) that correctly reflect the secure connectivity to those users. The KaY does not modify frames that pass between its Controlled Port and the SecY's Controlled Port. However the KaY can use the secure service provided by the SecY to complete authentication, authorization, or the acquisition of client policies, prior to enabling transmission and reception through its Controlled Port.~~

The KaY determines the value of the MAC Operational parameter (IEEE Std 802.1AC) associated with Controlled Port (10.7.4, 10.7.5) consistent with the provisions of this standard (6.4, 6.5, 6.7, 7.1.3, 7.2, 10.5.1, 10.5.2, 10.7.14, 10.7.2, 10.7.25).

~~NOTE 2—Operation of the SecY without protection or validation allows the same interfaces and relationships to be maintained between entities within a system when SecY functionality is not required. This provides a useful migration path for networks comprising systems that will incorporate SecY functionality at different times.~~

The KaY communicates transmit and receive keys and other information (10.2) to the SecY through its Layer Management Interface (LMI) ~~as illustrated in Figure 10-2~~. The LMI is also used to exchange information with local protocol entities responsible for network management, such as an SNMP Agent.

NOTE ~~2~~3—The term *local* refers to any other entity residing within the same system. Information exchange with a local entity can be modelled as occurring through its LMI (10.1, 10.3, 10.4, Figure 10-1~~, Figure 10-2~~), thus facilitating information exchange between entities not necessarily adjacent in a protocol layer reference model. No constraints are placed on the information exchanged, but there is no synchronization with any particular invocation of service at a service access point, so LMI exchanges do not effectively add to the parameters of a service such as the MAC service.

Delete Figure 10-2, renumbering subsequent figures as required.

10.2 SecY functions

Change bullet h) of 10.2 as follows:

h) ~~A replay window to support use of MACsec over provider networks that misorder frames with different transmission priority and or addresses. Frames within the window can be received out of~~

~~order, but are not replay protected. The window size can be set to zero to enforce strict reception ordering and replay protection.~~

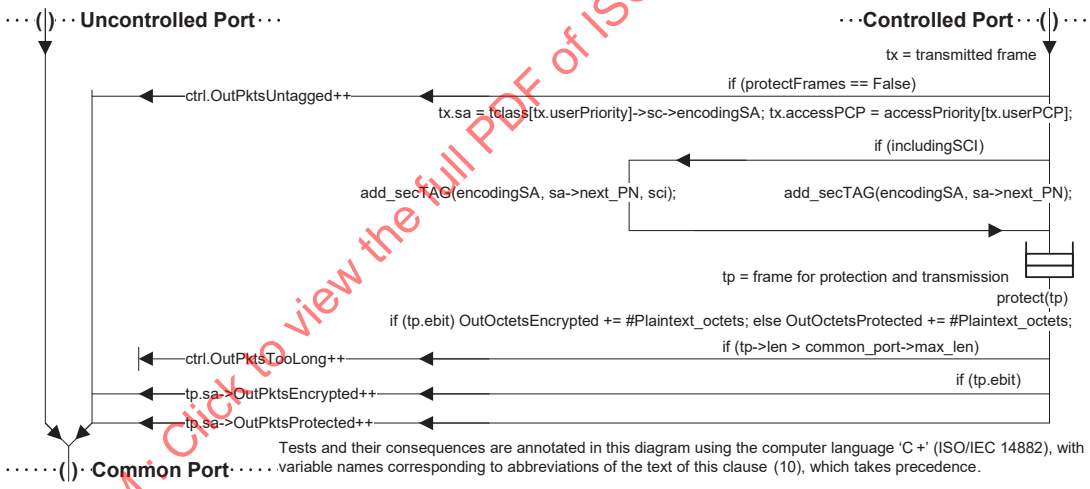
h) Use of multiple transmit SCs and a configurable replayWindow to support media access control methods and provider networks that can misorder frames with different priorities and/or addresses.

10.4 SecY architecture

Change the fifth paragraph of 10.4 as follows:

Management controls are provided to allow a SecY to be incorporated in a network system before MACsec is deployed, and to facilitate staged deployment. If protectFrames is not set, frames submitted to the Controlled Port are transmitted without modification. The validateFrames control allows untagged frames to be received, and Cipher Suite validation of tagged frames to be disabled or its result simply counted without frame discard. The protectFrames and validateFrames controls can also be set to allow the SecY to function completely transparently. The replayProtect and replayWindow controls allows replay protection to be disabled, to operate on a packet number window, or to enforce strict frame order. If replayProtect is set but the replayWindow is not zero, frames within the window can be received out of order, however they are not replay protected. Management counters allow configuration and operational errors to be identified and rectified before enabling secure operation. The effect of the controls, and the counters maintained, are summarized in Figure 10-4 and Figure 10-5.

Replace Figure 10-4 with the following figure:



NOTE 1—Secure generation frame counters are identified as reported by management. Confidentiality or integrity only protection is selected for an SA when it is created, so either but not both of the OutOctetsEncrypted or OutOctetsProtected counts and either OutPktsEncrypted or the OutPktsProtected will be incremented while that SA is in use, and the current value of the packet counter can be derived from nextPN for the SA less any change in the value of OutPktsTooLong since that SA has been used for protection, allowing an implementation to optimize counter resources.

Figure 10-4—Management controls and counters for secure frame generation

10.5 Secure frame generation

Change bullet f) of 10.5 as follows:

f) Issues a request to the Transmit Multiplexer with the destination and source MAC addresses~~, and priority of the frame as received from the Controlled Port,~~ and an MPDU comprising the octets of the SecTAG, Secure Data, and the ICV concatenated in that order (10.5.5). If the SecY does not

implement an Access Priority Table (10.7.17) the priority of the request is the same as that received from the Controlled Port, otherwise it is the access priority given by the table for the received priority.

10.5.1 Transmit SA assignment

Change 10.5.1 as follows:

~~Each SA is identified by its Association Number (AN).~~ Each frame is assigned to the SA identified by the current value of the encodingSA variable for the selected transmit SC. If the SecY does not implement a Traffic Class Table it uses a single transmit SC. If implemented, the Traffic Class Table specifies the value of the most significant four bits of the SCI's Port Identifier component for each possible transmit request user priority, allowing selection of one of up to eight distinct SCs (see 10.7.17).

The encodingSA ~~This~~ is updated following an LMI request from the KaY to start transmitting using the SA and can be read but not written by network management. Frames will be protected using the encodingSA immediately after the last frame assigned to the previous SA has been protected. If the SA ~~identified by the encodingSA~~ is not available for use, and the management control protectFrames is set, MAC_Operational transitions to False for the Controlled Port, and frames are neither accepted or delivered using the port.

Replace Figure 10-5 with the following figure:

Tests and their consequences are annotated in this diagram using the computer language 'C +' (ISO/IEC 14882), with variable names corresponding to abbreviations of the text of this clause (10), which takes precedence.

NOTE 1—Secure verification frame counters are identified as reported by management. Whether a given counter can be incremented depends on the management control validateFrames and on whether received frames are confidentiality protected, allowing an implementation to optimize resources. As shown in the figure, only one counter for each of the sets {InPktsUntagged, InPktsNoTag} and {InPktsUnusedSA, InPktsNotUsingSA} for the Controlled Port as a whole and only one counter for each of the sets {InPktsLate, InPktsDelayed}, {InPktsInvalid, InPktsNotValid}, and {InPktsUnchecked, InPktsOK} for each received SC can be incremented while validateFrames and confidentiality policy remain unchanged.

Figure 10-5—Management controls and counters for secure frame verification

10.5.3 SecTAG encoding

Change 10.5.3 as follows:

The SecTAG is encoded as specified in Clause 9.

The SC bit in the SecTAG shall be set and the SCI explicitly encoded in the SecTAG, and the management status parameter includingSCI set to True, if and only if

a) The management control alwaysIncludeSCI is True,
   or
b) The number of transmit SCs is greater than one,
   or
c) The number of receive SCs enabled for reception is greater than one, and
   1) The management control useES is False,
      and
   2) The management control useSCB is False.

If the management control useES is True and ~~alwaysIncludeSCI~~ includingSCI is False, the ES bit in the SecTAG shall be set. Otherwise, if useES is False or alwaysIncludeSCI is True, the ES bit shall be clear.

If the management control useSCB is True and ~~alwaysIncludeSCI~~ includingSCI is False, the SCB bit in the SecTAG shall be set. Otherwise, if useSCB is False or ~~alwaysIncludeSCI~~ includeSCI is True, the SCB bit shall be clear.

NOTE—These rules cover the case where useSCB is True and the number of active receive channels is greater than one. However SCB bit use is currently restricted to supporting a transmit only EPON interface (see Clause 12).

Table 10-1 summarizes the rules [a) through c) above], with each of the columns to the right representing a valid combination of controls, number of SCs, and SecTAG encoding.

Insert a new Table 10-1 as follows, renumbering subsequent tables as required:

Table 10-1—Management controls and SecTAG encoding

Mgmt controls	alwaysIncludeSCI	T[a]	F	F	F	F	F
	useES	—	—	F	T	T	F
	useSCB	—	—	F	T	F	T
#SCs	#transmitSCs > 1	—	T	—	F	F	F
	#receiveSCs enabled for reception > 1	—	—	T	—	—	—
Mgmt status	includingSCI	T	T	T	F	F	F
SecTAG encoding	SC bit set? (SCI explicitly encoded)	Y	Y	Y	N	N	N
	ES bit set?	N	N	N	Y	Y	N
	SCB bit set?	N	N	N	Y	N	Y

[a]T = True, F = False, — = don't care, Y= Yes, N = No

~~If the management control alwaysIncludeSCI is set, or the number of receive SCs with SAs enabled for reception is greater than one and both useES and useSCB are False, the SC bit in the SecTAG shall be set and the SCI explicitly encoded in the SecTAG; otherwise, the SC bit shall be clear and the SCI not explicitly encoded.~~

The values of useES, useSCB, and alwaysIncludeSCI can be written and read by management. The read-only management status parameter includeSCI is True if an SCI is explicitly encoded in each SecTAG, and False otherwise. The number of active receive SCs is controlled by the KaY but can be read by management.

If a frame is to be integrity protected, but not encrypted, with the number and value of the octets of the Secure Data exactly the same as those of the User Data and an ICV of 16 octets, then the E bit shall be clear and the C bit clear. The E bit shall be clear and the C bit set if the frame is not encrypted but the octets of the Secure Data differ from those of the User Data or the ICV is not 16 octets.

If both confidentiality (through encryption) and integrity protection are applied to a frame, then both the E bit and the C bit shall be set. The SecY shall not encode a SecTAG that has both the E bit set and the C bit clear for any frame received from the Controlled Port for transmission.

~~If the alwaysIncludeSCI control is set or the number of receive SCs with SAs enabled for reception is greater than 1, the SCI is included in the SecTAG; otherwise, it is omitted. The value of alwaysIncludeSCI can be written and read by management. The number of active receive SCs is controlled by the KaY, but can be read by management.~~

10.6 Secure frame verification

Change the second paragraph of 10.6 as follows:

If the management control validateFrames is not Strict, frames without a SecTAG are received, counted, and delivered to the Controlled Port; otherwise, they are counted and discarded. If validateFrames is Disabled, cryptographic validation is not applied to tagged frames, but frames whose original service user data can be recovered are delivered. Frames with a SecTAG that has the TCI E bit set but the C bit clear are discarded, as this reserved encoding is used to identify frames with a SecTAG that are not to be delivered to the Controlled Port. If validateFrames is Null, all received frames are delivered to the Controlled Port without modification, irrespective of the absence, presence, or validity of a SecTAG, and the processing described in a) through j) above and in 10.6.1 through 10.6.5 is not performed. Figure 10-5 summarizes the operation of secure frame verification management controls and counters.

Setting validateFrames to Null shall also cause the secure frame generation control protectFrames (10.5) to become False, thus allowing a port that includes a SecY to behave as if the SecY were not present. In particular, it allows a MACsec-capable bridge or EDE to forward frames that have a SecTAG but no other outer tag (such as a VLAN tag).

10.6.1 Receive SA assignment

Change the first and second paragraphs of 10.6.1 as follows:

An SCI is associated with the received frame and used to locate the receive SC. If an SCI is not explicitly encoded in the SecTAG, the ~~default~~ value established by the KaY for a single peer is used.

If the SC is not found, ~~it~~ the received SCI may be recorded to assist network management resolution of the problem, and:

a) If validateFrames is Strict or the C bit in the SecTAG is set, the ~~InPktsNoSCI~~ InPktsNoSAError counter is incremented and the frame is discarded; otherwise

b) The ~~InPktsUnknownSCI~~ InPktsNoSA counter is incremented and the frame (with the SecTAG and ICV removed) is delivered to the Controlled Port.

If the receive SC has been identified, the frame's AN is used to locate the receive SA for the received frame and processing continues with the preliminary replay check. If the SA is not in use:

c) If validateFrames is Strict or the C bit is set, the frame is discarded and the ~~InPktsNotUsingSA~~ InPktsNoSAError counter incremented; otherwise
d) The ~~InPktsUnusedSA~~ InPktsNoSA counter is incremented and the frame delivered to the Controlled Port.

NOTE—The short phrase "the frame is discarded" is commonly used to express the more formal notion of not processing a service primitive (an indication or request) further and recovering the resources that embody the parameters of that service primitive. No further processing is applied. However, if a duplicate of the primitive has been submitted to another process (by the Receive Demultiplexer in this case), processing of that duplicate is unaffected.

10.7 SecY management

Change the initial paragraph and bullet list of 10.7 as follows:

The SecY management process controls, monitors, and reports on the operation of the SecY, providing access to operational controls and statistics for network management and the KaY through the LMI. It

a) Reports the value of the SCI for the SecY's default traffic class SC (10.7.1)
b) Maintains the MAC Status (6.4) parameters and point-to-point MAC parameters (6.5) for the Uncontrolled (10.7.2) and Controlled (10.7.4) Ports
c) Provides interface statistics for the Uncontrolled (10.7.3) and Controlled Ports (10.7.6), deriving the latter from the detailed statistics maintained by the SecY
d) Provides information on the frame verification (10.7.7) and generation (10.7.16) capabilities
e) Supports control of frame verification (10.7.8) and generation (10.7.17), including management of a Traffic Class Table that allows the user priority associated with the Controlled Port transmit request to select one of a number of transmit SCs, and an Access Priority Table
f) Supports creation of transmit SCs (10.7.20), each corresponding to one of the values appearing in Traffic Class Table entries
g) Supports creation of transmit SAs (10.7.22), each associated with an SAK, for the transmit SC
h) Supports creation of receive SCs (10.7.11), each corresponding to potential member of the CA
i) Supports creation of receive SAs (10.7.13) for each receive SC, each associated with an SAK
j) Supports control over reception (10.7.15) and transmission (10.7.23) using individual SAs, and allows the nextPN variable to be set and updated for transmission and the lowest acceptable PN to be set and update for reception
k) Maintains ~~detail~~ statistics for receive and transmit SCs and SAs, accumulating statistics from past SAs ~~and SCs~~
l) Provides a list of the Cipher Suites ~~implemented, together~~ with their basic capabilities and properties, and list of those Cipher Suites implemented by the SecY with management control over their use (10.7.25)
m) Allows selection of the current Cipher Suite, from those implemented
n) Supports installation of SAKs for the current Cipher Suite, for transmission, reception, or both

Insert the following text as a new paragraph after the existing NOTE that immediately follows the second paragraph of 10.7:

In Figure 10-6 the management information for each SecY is indexed by controlledPortNumber within a SecY System. This containment relationship complements that specified in IEEE Std 802.1X, where the management information for each PAE is indexed by portNumber (IEEE Std 802.1X-2010 12.9.2) within a

PAE System and includes the controlledPortNumber that identifies the Controlled Port of the associated SecY. The containment relationship also matches that specified in Clause 13, with a SecY System corresponding to a SecY MIB module instance, and each controlledPortNumber to the ifIndex (RFC 2863) value used to identify a SecY within that module (13.3.2, 13.5).

If a Bridge Port is supported by a SecY (11.3) the ifIndex value used to identify the SecY's Controlled Port will be that identifying the ISS interface (service access point) used by the Bridge Port. IEEE Std 802.1Q specifies Bridge Port Numbers that identify Bridge Ports from the point of view of a bridge's MAC Relay Entity, and port numbers in general to identify ISS interfaces. In simple, common, cases (11.3) each Bridge Port Number can and most likely will be the same as the port number (and ifIndex value) identifying the Controlled Port, though an optional mapping table is specified (IEEE Std 802.1Q-2014 12.5.1).

IEEE Std 802.1Q can constrain the relationship between Bridge Port Numbers and other bridging parameters (see, for example, IEEE Std 802.1Q-2014 12.13) and if RSTP or MSTP are implemented the maximum number of Bridge Ports is 4095 (IEEE Std 802.1Q-2014 17.3.2.2). In a system comprising multiple bridge components, each port is uniquely identified by a ComponentID and Port Number pair. The SCI values used by a SecYs supporting Bridge Ports do not have to be derived from the Bridge Port Numbers or (possibly different) controlledPortNumbers so do not further constrain those port numbers. However, the least significant 12 bits (if a SecY supports multiple traffic class SCs) and all 16 bits (otherwise) of the Port Identifier can be assigned—subject only to the requirement for SCI uniqueness (3.29), so that in the simple case of a bridge component with 4095 or fewer ports, each SCI's Port Identifier can convey the Bridge Port Number and use the Bridge Address for the MAC Address-based component of each SCI, if so desired.

NOTE 2—The IEEE Std 802.1AEcg-2017 amendment to this standard added the SecY System to Figure 10-6 and clarified the management use of port numbers and ifIndex values, but did not change any related normative provisions.

Change and renumber Figure 10-6 as follows:

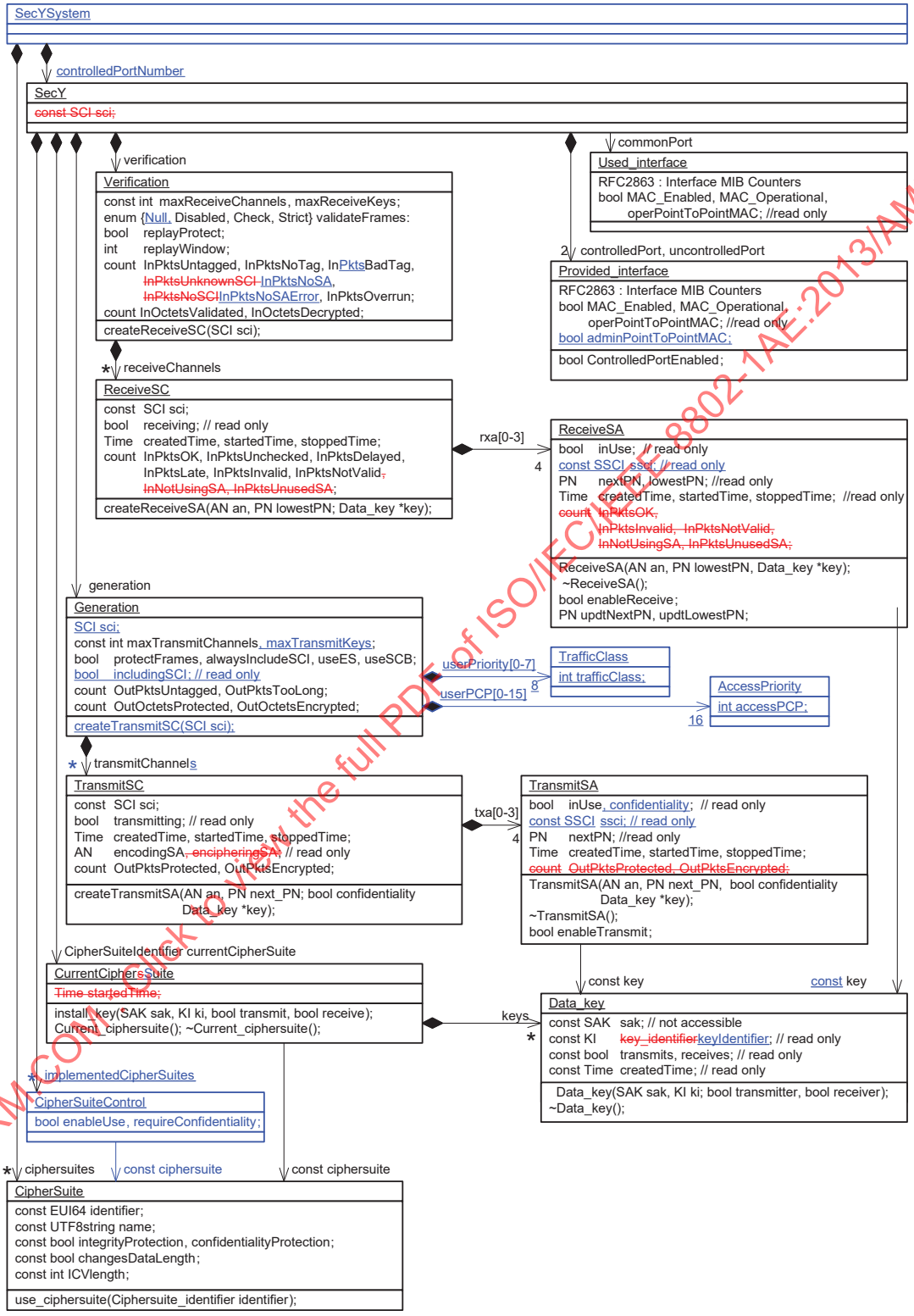


Figure 10-6—SecY managed objects

10.7.1 SCI

Change 10.7.1 as follows:

The SCI for the SecY's default traffic class~~, a constant parameter of the SecY~~ (7.1.2, 8.2.1)~~,~~ can be read but not written by management.

If the SecY supports more than one transmit SC [5.4(e), 10.7.1, 10.7.17], the four most significant bits of the Port Identifier component of this SCI are zero.

10.7.4 Controlled Port status

Change 10.7.4 as follows:

The following status parameters are provided to the user of the Controlled Port, and can be read but not directly written by management:

a) MAC_Enabled, True if and only if:
   1) ControlledPortEnabled (10.7.5) is True, and
   2) MAC_Enabled is True for the Common Port, and
   3) transmitting (10.7.21) is True for the transmit SC, and
   4) receiving (10.7.12) is True for at least one receive SC.

b) MAC_Operational, True if and only if:
   1) MAC_Enabled is True, and
   2) MAC_Operational is True for the Common Port

c) operPointToPointMAC~~,~~ If adminPointToPointMAC is Auto (6.5) operPointToPointMAC is True if and only if:
   1) validateFrames (10.7.8) is Strict, and receiving is enabled for ~~at most one~~ receive ~~channel~~SCs from at most one peer SecY, or
   2) validateFrames is not Strict, and operPointToPointMAC is True for the Common Port.

   Receive SCs are assumed to originate from the same peer SecY if their SCIs are the same with the exception of the four most significant bits of the Port Identifier component.

The following status parameter may be read and written by management:

d) adminPointToPointMAC (6.5).

   NOTE—Prior to the IEEE Std 802.1AEcg amendment to this standard, each SecY used a single transmit SC. The adminPointToPointMAC variable can be used to configure operPointToPointMAC in the event that an earlier implementation of this standard does not recognize two receive SCs as being from the same SecY or configures two distinct SecYs (in the same CA) with SCIs that differ only in the most significant bits of the Port Identifier.

10.7.6 Controlled Port statistics

Change the third paragraph of 10.7.6 as follows:

The ifInDiscards count is the sum of all the InPktsNoTag, InPktsLate, and InPktsOverrun counts. The ifInErrors count is the sum of all the InPktsBadTag, ~~InPktsNoSCI,~~InPktsNotUsingSA, and InPktsNotValid counts (10.6, Figure 10-5).

10.7.8 Frame verification controls

Change 10.7.8 as follows:

Frame verification is subject to the following controls, as specified in 10.6:

a) validateFrames, taking values of Null, Disabled, Check, or Strict, with a default of Strict
b) replayProtect, True or False, with a default of True
c) replayWindow, taking values between 0 and 2^{32}–1, with a default of 0

The validateFrames and replayProtect controls are provided to facilitate deployment. They can be read by management. Each may be written by management, but a conformant implementation shall provide a mechanism to allow write access by network management to be disabled for each parameter individually. If management access is prohibited to any of these parameters, its default value should be used.

If the Current Cipher Suite uses extended packet numbering, i.e., a 64-bit PN, the maximum value of replayWindow used in the Secure Frame Verification process (10.6) is 2^{30}–1, thus ensuring that the replayWindow does not encompass more than half of the range of PNs that can be correctly recovered (10.6.2). Any higher value set by network management is retained for possible subsequent use with a different Cipher Suite and will be reported if read by network management. This provision provides compatibility with prior revisions of this standard, though it is unlikely that such a high value of replayWindow would have been used.

10.7.9 Frame verification statistics

Change 10.7.9 as follows:

Any given received frame increments (10.6) exactly one of the following counts [item a) through item l)]. The following counts are maintained for the frame verification process as a whole:

a) InPktsUntagged
b) InPktsNoTag
c) InPktsBadTag
d) InPkts~~UnknownSCI~~NoSA
e) InPkts~~NoSCI~~NoSAError
f) InPktsOverrun

The following counts are maintained only for each receive SC and are discarded if the record of the SC is deleted by the KaY:

g) InPktsOK
h) InPktsUnchecked
i) InPktsInvalid
j) InPktsNotValid
k) InPktsDelayed
l) InPktsLate

~~The following are maintained for each receive SC, and for each of the four receive SAs corresponding to the last use of ANs 0 through 3 for that SC.~~

m) ~~InPktsOK~~
n) ~~InPktsInvalid~~
o) ~~InPktsNotValid~~
p) ~~InPktsNotUsingSA~~

q) ~~InPktsUnusedSA~~

The counts reported for each SC include those for current and prior SAs, with ANs that have since been reused. This allows useful counts to be maintained on high-speed LANs where an SA may be used for little more than 5 min, and an AN reused after 20 min.The times at which each SC and SA were, or are, in use are recorded (10.7.12, 10.7.14) and assist correlation of the statistics collected with network events.

~~NOTE—The counts can be correctly reported, without the need for each frame to increment separate real-time counters for the SC and an SA. A count for each SA is summed with that for the SC to respond to a request for the latter. When an SA is replaced by a successor with the same AN, its counts are added to those for the SC.~~

10.7.14 Receive SA status

Change 10.7.14 as follows:

The following parameters can be read, but not directly written, by management:

a) inUse
b) nextPN (10.6, 10.6.5)
c) lowestPN, the lowest acceptable PN value for a received frame (10.6, 10.6.2, 10.6.4, 10.6.5)
d) createdTime, the system time when the SA was created
e) startedTime, the system time when inUse last became True for the SA
f) stoppedTime, the system time when inUse last became False for the SA
g) keyIdentifier (10.7.28), identifying the SAK used by the SA

and, if the Current Cipher Suite uses extended packet numbering (14.7, 14.8), the following parameter:

h) ssci, the SSCI for this receive SA

If inUse is True, and MAC_Operational is True for the Common Port, the SA can receive frames.

The keyIdentifier is an octet string, whose format and interpretation depends on the key agreement protocol in use. It does not contain any information about the SAK other than that explicitly chosen by the key agreement protocol to publicly identify the key. If MKA is being used it is the 128-bit Key Identifier (KI) specified by IEEE 802.1X encoded in an octet string as specified by that standard.

10.7.16 Frame generation capabilities

Change 10.7.16 as follows:

The SecY's frame generation capabilities are represented by the following parameter(s):

a) Maximum number of transmit channels
b) Maximum number of keys in simultaneous use for transmission

Th~~i~~ese parameters can be read but not written by management.

NOTE—An individual SecY can support multiple traffic class SCs (10.7.17). When MKA is used (see Annex E), an SAK distributed by the Key Server is used by all newly created SAs (each supporting one of the SCs in the CA) so a SecY need only support two keys for transmission and reception at a time (allowing for rollover without frame loss, from one SAK to its successor), irrespective of the number of its traffic class SCs and peers in the CA.

10.7.17 Frame generation controls

Change 10.7.17 as follows:

Frame generation is subject to the following controls:

a) protectFrames (10.5), True or False, with a default of True
b) alwaysIncludeSCI (10.5.3), True or False, with a default of False
c) useES (10.5.3), True or False, with a default of False
d) useSCB (10.5.3), True or False, with a default of False

The protectFrames control is provided to facilitate deployment. The protectFrames, alwaysIncludeSCI, useES, and useSCB controls can be read by management and may be written, but a conformant implementation shall provide a mechanism to allow write access by network management to be disabled. If management access is prohibited, the default or a value determined by the KaY should be used.

The following status parameter can be read, but not written, by management:

e) includingSCI (10.5.3), True if and only if the SC bit is set and the SCI explicitly encoded in each SecTAG transmitted

The SecY may map each frame to a transmit SC using a Traffic Class Table and the frame's user priority. Up to eight transmit SCs may be implemented, allowing separate transmit SCs for each possible user priority. However, the reason for the possible use of multiple transmit SCs is to take advantage of the fact that their separate SAs use different PN values and thus to minimize the size of the replayWindow, and in particular to facilitate strict reception ordering and replay protection when the Common Port is supported by a service (such as a Provider Bridged Network, see 11.7) that can reorder frames of different priority. In such cases, the useful number of traffic classes might be two or three, corresponding to the differentiated classes of service provided. While the Traffic Class Table mirrors that specified by IEEE Std 802.1Q for the management of bridge queues, a SecY has a minimal implementation dependent buffering requirement and there is no reason to suppose that any given implementation might provide more timely service if the Common Port does not provide priority differentiated services.

NOTE 1—The IEEE Std 802.1AEcg amendment to this standard, introducing the use of multiple transmit SCs, was developed contemporaneously with IEEE P802.3 development of a capability that allows a high priority Ethernet frame to preempt one of lower priority and thus be received in its entirety prior to the latter. This provides another example of a service that can reorder frames on the basis of priority and for which the use of a separate transmit SC with separate PN number spaces can be used to allow strict ordering and strict replay protection for preemptible and preempting frames separately.

Each entry in the Traffic Class Table is a traffic class, represented by an integer from 0 (default) through 7 that also comprises the numeric value of the four most significant bits of the Port Identifier component of the SCI for the selected SC.

The SecY may map the user priority of each frame's transmit request at the Controlled Port to the access priority to be used for the corresponding transmit request at the Common Port using the Access Priority Table. The table index and its output both comprise 4 bits, representing both the priority (most significant three bits) and drop_eligible (least significant bit) of the user priority and access priority. The default value of each table entry is that of its index, thus leaving the priority and drop_eligible bits unchanged. This default is appropriate if the service provided by the Common Port already implements its own mapping from requested priority to its own priority or other parameters used to make decisions that affect frame reordering, and that mapping matches the Traffic Class Table's mapping of user priority to transmit SC. The default is also appropriate if the administrator is willing to tolerate the degree of misordering, and the replayWindow size that implies, resulting from allocating frames of different access priority to the same SC in the interest of providing a differentiated service to the higher priority frames without using additional transmit SCs. Otherwise it is recommended that the Access Priority Table be configured so that frames allocated to the same transmit SC use the same access priority.

NOTE 2—Where MACsec is used to support an instance of the ISS that in turn supports the EISS, the priority originally requested by the EISS user is encoded in the VLAN tag within the ISS MSDU and is thus protected by MACsec and is communicated unchanged to the peer EISS user, unaffected by local access priority mapping decisions.

10.7.18 Frame generation statistics

Change 10.7.18 as follows:

Any given transmitted frame (10.5) increments exactly one of the following counts [item a) through item d)]. The following counts are maintained for the frame generation process as a whole:

a) OutPktsUntagged
b) OutPktsTooLong

The following counts are maintained for ~~the~~ each transmit SC~~ and for each of the four transmit SAs corresponding to the last use of ANs 0 through 3 for that SC~~.

c) OutPktsProtected
d) OutPktsEncrypted

The counts reported for each SC include those for current and prior SAs, with ANs that have since been reused. This allows useful counts to be maintained on high-speed LANs where an SA may be used for little more than 5 min, and an AN reused after 20 min.The times at which each SC and SA were, or are, in use are recorded (10.7.21, 10.7.23) and assist correlation of the statistics collected with network events.

NOTE—The OutPktsProtected and OutPktsEncrypted counts can be correctly reported, without the need for each frame to increment separate real-time counters ~~for the SC and an SA~~. The packets for a given SA are either all encrypted (confidentiality protected) or all only integrity protected, so the counts for active SAs can be derived from the nextPN values (less any contribution to OutPktsTooLong made after PN assignment to discarded frames) and summed with that those previously accumulated for the SC. ~~Account for each SA is summed with that for the SC to respond to a request for the latter.~~ When an SA is replaced by a successor with the same AN, its counts are added to those accumulated for the SC.

Insert a new subclause 10.7.20 before the existing 10.7.20 Transmit SC status as follows:

10.7.20 Transmit SC creation

A transmit SC, with a given SCI that remains unchanged for the life of the SC, is created, as requested by the KaY, for the default traffic class SC and for each of the other SCs identified by the Traffic Class Table (if implemented). The KaY is responsible for ensuring the uniqueness of the SCI of any SC in a CA that might use the same SAK.

Transmit SCs and SAs (10.7.22) may also be created and controlled by management, but a conformant implementation shall provide a mechanism to allow creation and setting of control parameters by network management to be disabled.

Change the existing subclause 10.7.20 (now 10.7.21) as follows:

10.7.21 Transmit SC status

The following status parameters can be read, but not directly written, by management:

a) transmitting, True if inUse (~~10.7.14~~10.7.23) is True for any of the SAs for the SC, and False otherwise
b) encodingSA (10.5.1)
c) ~~encipheringSA (10.5.4)~~
c) createdTime, the system time when the SC was created
d) startedTime, the system time when transmitting last became True for the SC
e) stoppedTime, the system time when transmitting last became False for the SC

When the SC is created, transmitting is False and startedTime and stoppedTime are equal to createdTime.

Change 10.7.21(now 10.7.22) as follows:

10.7.22 Transmit SA creation

An SA is created for ~~the~~ a transmit SC on request from the KaY, with the following parameters:

a) AN, the association number for the SA
b) nextPN, the initial value of Transmit PN (10.5.2) for the SA
c) confidentiality, True if the SA is to provide confidentiality as well as integrity for transmitted frames
d) A reference to an SAK that is unchanged for the life of the SA

and, if the Current Cipher Suite uses extended packet numbering (14.7, 14.8), the KaY also supplies the following parameter:

e) SSCI for the SA
Each SA that uses the same SAK has a different SSCI when these Cipher Suites are used. When the SA is created, its SCI and SSCI are provided (for use in subsequent protection operations) to the instance of the Current Cipher Suite identified by the referenced SAK. A transmit SA will not be created if the SSCI supplied duplicates that for a different SCI (for the same SAK, for transmission or reception).

Frame generation statistics (10.7.18) for the SA are set to zero when the SA is created. Any prior SA with the same AN is deleted. Creation of the SA fails unless the referenced SAK exists and is installed (i.e., is available for use). A management protocol dependent reference is associated with each SA. This reference allows the transmit SA to be distinguished from any previously created with the same AN.

The MACsec Key Agreement (MKA) protocol specified in IEEE Std 802.1X-2010 does not distribute SSCIs explicitly. A KaY that uses MKA as specified in IEEE Std 802.1X-2010 assigns SSCI values as specified in 10.7.13.

Change 10.7.22 (now 10.7.23) as follows:

10.7.23 Transmit SA status

The following parameters can be read, but not directly written, by management:

a) inUse
b) createdTime, the system time when the SA was created
c) startedTime, the system time when inUse last became True for the SA
d) stoppedTime, the system time when inUse last became False for the SA

e) nextPN (10.5, 10.5.2)
f) confidentiality, True if the SA is providing confidentiality as well as integrity for transmitted frames
g) keyIdentifier (10.7.28), identifying the SAK used by the SA

and, if the Current Cipher Suite uses extended packet numbering (14.7, 14.8), the following parameter:

h) ssci, the SSCI for this transmit SA

If inUse is True, and MAC_Operational is True for the Common Port, the SA can transmit frames.

The keyIdentifier is an octet string, whose format and interpretation depends on the key agreement protocol in use. It does not contain any information about the SAK other than that explicitly chosen by the key agreement protocol to publicly identify the key. If MKA is being used it is the 128-bit Key Identifier (KI) specified by IEEE 802.1X encoded in an octet string as specified by that standard.

Change 10.7.24 (now 10.7.25) as follows:

10.7.25 Implemented Cipher Suites

The following read-only management per Cipher Suite implementation capability information is provided by the system of which the SecY is a part ~~for each Cipher Suite implemented~~:

a) Cipher Suite Identifier, a globally unique 64-bit (EUI-64) identifier
b) Cipher Suite Name, a human readable and displayable UTF-8 string
c) integrityProtection, True if integrity protection without confidentiality can be provided
d) confidentialityProtection, True if confidentiality with integrity protection can be provided
e) offsetConfidentiality, True if a selectable offset for confidentiality can be provided
f) changesDataLength, True if the data length is changed
g) ICVlength, number of octets in the ICV

The Cipher Suite Identifier and Cipher Suite Name are both assigned by the document that specifies use of the Cipher Suite with this standard. If the Cipher Suite provides integrityProtection and confidentialityProtection, the SecY shall be capable of receiving frames with either, as signaled by the E and C bits in the SecTAG.

The confidentialityProtection parameter shall be True if and only if the Cipher Suite implementation is capable of being configured so that, when confidentiality is selected, all the octets of the MSDU are integrity and confidentiality protected.

The offsetConfidentiality parameter shall be True if and only if the Cipher Suite implementation is capable of both integrityProtection and confidentialityProtection, and of being configured so that, when confidentiality is selected, a selectable number (0, 30, or 50) of the initial octets of the MSDU are only integrity protected, and appear in the MACsec PDU immediately after the SecTAG in the order and with the values in the MSDU (Figure 8-1), while the remaining octets are confidentiality and integrity protected.

NOTE— ~~The offsetConfidentiality capability and the specific offset values chosen are provided to facilitate deployment on IP version 4 and version 6 hosts that perform load balancing across multiple processors in a single system using the initial fields of those protocol stacks, and are not currently capable of terminating the secure association before distributing the load without incurring a significant performance penalty.~~ IEEE Std 802.1AE-2006 specified the confidentiality offset option to facilitate early MACsec deployment on systems that needed to examine the initial octets of IP version 4 or version 6 frames to decide where to store received frames, before decrypting the frame. The XPN Cipher Suites standardized in IEEE Std 802.1AEbw-2013 do not support confidentiality offsets.

Insert a new subclause 10.7.26 before 10.7.25 Cipher Suite selection, as follows:

10.7.26 SecY Cipher Suite use

The Cipher Suite capabilities implemented for each SecY can be read by management. The following controls may be written by management, but a conformant implementation shall provide a mechanism to allow write access by network management to be disabled for each parameter individually:

a) enableUse, True if use of the Cipher Suite is permitted
b) requireConfidentiality, True if the Cipher Suite can only be used to provide both confidentiality and integrity (and not integrity only, or confidentiality with an offset)

The MKA Key Server selects the Cipher Suite to be used to protect communication within a CA. If enableUse is False for the selected Cipher Suite, the SecY does not participate in the CA and MAC_Operational for the Controlled Port remains false. If the MKA Key Server has selected integrity protection and enableUse and requireConfidentiality are both True for the selected Cipher Suite, confidentiality protection is used.

NOTE—A system might contain distinct SecY implementations with differing detailed Cipher Suite capabilities. Each of the latter can be represented by a distinct set of Cipher Suite implementation capability information (10.7.25), with each SecY's capabilities represented by a list of references (each with separate use controls) to some of those sets.

Change 10.7.26 (now 10.7.28) as follows:

10.7.28 SAK creation

An SAK is installed, i.e., an instance of the Current Cipher Suite for a given SAK is created, on request from the KaY, with the following parameters:

a) The SAK value
b) ~~A Key Identifier~~keyIdentifier, used by network management to reference the key
c) transmit, True if the key is to be installed for transmission
d) receive, True if the key is to be installed for reception

and, if the Current Cipher Suite uses extended packet numbering, the following parameter:

e) Salt [B9], a 96-bit parameter provided to the Current Cipher Suite for subsequent protection and validation operations

The MACsec Key Agreement (MKA) protocol specified in IEEE Std 802.1X-2010 does not include explicit parameters for distributing a Salt. Each KaY that uses MKA as specified in IEEE Std 802.1X-2010 computes this parameter as follows. The 64 least significant bits of the Salt are the 64 least significant bits of the MKA Key Server's Member Identifier (MI), the 16 next most significant bits of the Salt comprise the exclusive-or of the 16 next most significant bits of that MI with the 16 most significant bits of the 32-bit MKA Key Number (KN), and the 16 most significant bits of the Salt comprise the exclusive-or of the 16 most significant bits of that MI with the 16 least significant bits of the KN. This way of obtaining a Salt is not necessarily applicable to any other key agreement protocol.

Delete subclause 10.7.28 SAK controls.

11. MAC Security in Systems

11.1 MAC Service interface stacks

Change the second paragraph of 11.1 as follows:

Alternatively, media access method independent functions, such as VLAN tagging of frames (IEEE Std 802.1Q) and MAC Security (as specified by this standard), can be used to support the MAC Service (IEEE Std 802.1AC), ~~or~~ the MAC Internal Sublayer Service (ISS~~, IEEE Std 802.1D~~IEEE Std 802.1AC), or the Enhanced Internal Sublayer Service (EISS, ~~(~~IEEE Std 802.1Q). These functions use an ISS access point provided by media access method independent or media access method dependent convergence functions~~, as specified in Clause 6.5 of IEEE Std 802.1D and IEEE Std 802.1Q~~. See Figure 11-2.

11.3 MACsec in MAC Bridges

Change the first paragraph of 11.3 as follows:

MAC Bridges are specified in IEEE Std 802.1~~D~~Q. The MAC Relay Entity forwards frames between the ISS access points supported by each of the Bridge Ports. To provide MAC Security for such a system, each of the insecure interfaces presented by a LAN supports MACsec, which in turn supports the functions described in ~~7.5 and 7~~ 8.5 of IEEE Std 802.1~~D~~Q. Figure 11-4 shows a bridge with and without MACsec.

Replace Figure 11-4 with the following figure and change the title as follows:

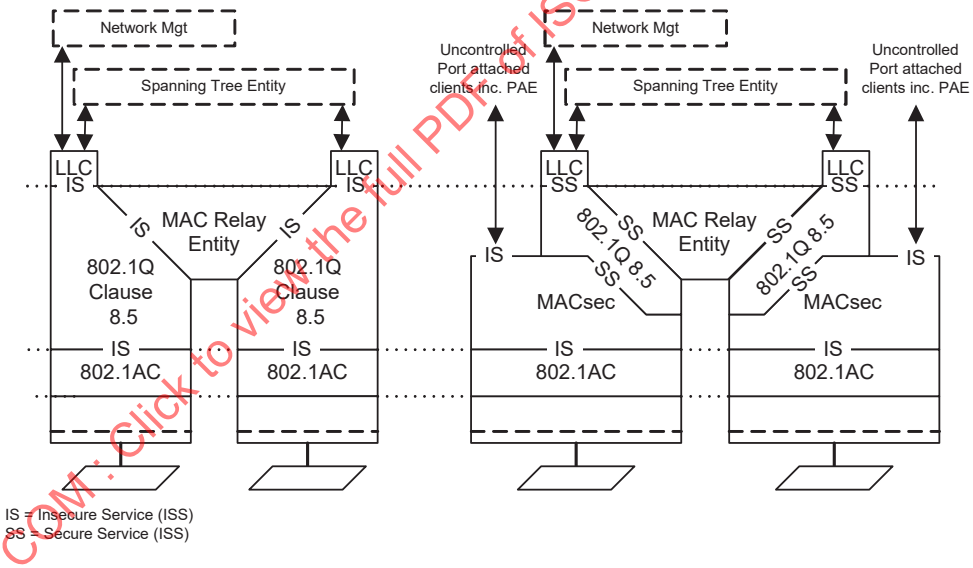


Figure 11-4—MACsec in a~~n IEEE 802.1D~~ VLAN-unaware MAC Bridge

Change the title of Figure 11-5 as follows:

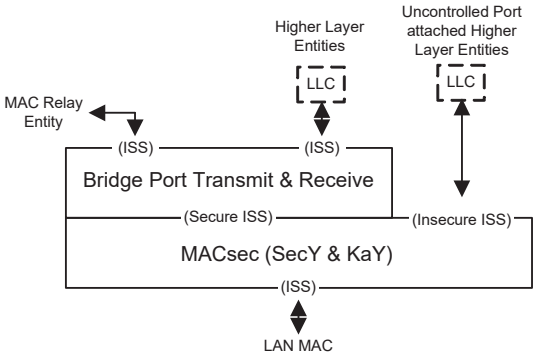


Figure 11-5— ~~IEEE 802.1D~~ VLAN-unaware MAC Bridge Port with MACsec

11.4 MACsec in VLAN-aware Bridges

Replace Figure 11-6 with the following figure:

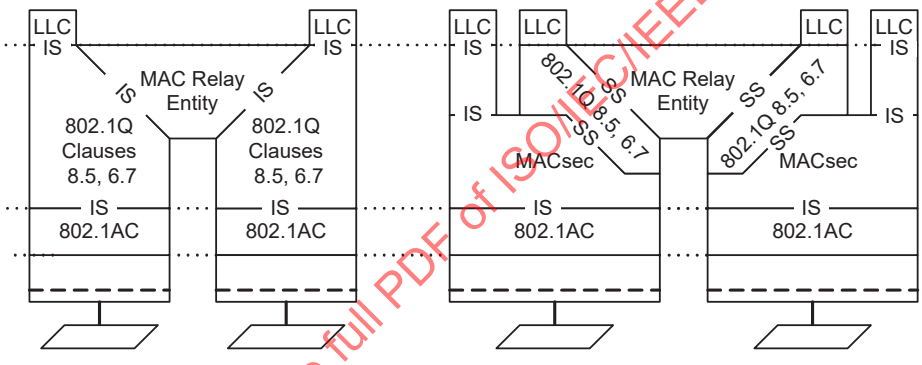


Figure 11-6—Addition of MAC Security to a VLAN-aware MAC Bridge

11.8 MACsec and multi-access LANs

Change 11.8 as follows:

MACsec can be used to support the equivalent of multiple LANs from one station to each of a number of others using the service provided by a single LAN. Each station that connects to more than one of the multiple LANs does so by using a distinct SecY for each of those connections. MACsec frames for each of the multiple LANs are distinguished from frames for the others by the SCI of the originating SecY. ~~The SecYs for any given station each have an SCI~~ If a station has more than one SecY, the SCIs for each SecY's transmit SC or SCs are based on the MAC Address allocated to that station but use a different Port Identifier component (9.9). Figure 11-15 shows one station (A in the figure) with two connections, one to each of two others (B, C).

Frames transmitted by each SecY's Uncontrolled Port can include a SecTAG, with ~~the~~ an ~~same~~ SCI value used by the SecY's Controlled Port. These frames are distinguished by setting the E bit in the SecTAG TCI True and the C bit False, and are discarded by the frame verification process for the Controlled Port (10.6). The connectivity between Uncontrolled Ports using the SecTAG thus matches the secure connectivity provided between the corresponding Controlled Ports. The protocol entities attached to the SecY's Uncontrolled Port add and remove this SecTAG as required.

NOTE—Frames including a SecTAG and E bit True and C bit False were not used by any standard protocol at the time of the development of the IEEE Std 802.1AEcg amendment to this standard, but this normative provision remains for possible future use by protocols that need to associate Uncontrolled Port frames with individual SCIs.

Frames transmitted through a SecY's Uncontrolled Port to a multi-access LAN can omit the SecTAG, provided that only one bidirectional unicast communication is supported between any pair of stations. The recipient uses the source address of the frame to identify the peer SecY.

Each multi-access capable station also supports an Uncontrolled Port (shown to the left in station A in Figure 11-15) that allows arbitrary frames to be transmitted on the LAN and received, if they are not MACsec frames, by any of the systems. These Uncontrolled Ports support the protocols required to discover peer multi-access capable systems and to associate SCIs (and hence SecYs and KaYs) with each connection. The entities that operate such discovery and association protocols in stations, such as station A, that are capable of supporting multiple SecYs on a single LAN, are typically capable of instantiating some number of SecYs and associated entities on demand. The Controlled Ports thus provided to higher-layer entities can be transient and are referred to as "virtual Ports".

Where a protocol entity for each SecY's Uncontrolled Port transmits frames without a SecTAG, it is possible for there to be no externally observable difference between the operation of entities attached to those ports and of an equivalent entity or entities attached to the Uncontrolled Port for the station as a whole. Whether to emphasize common functions or peer relationships is a choice for each protocol's specification.

Figure 11-16 shows part of an interface stack for a multi-access capable system. The 'Y' function can simply copy all indications from its lower service access point to all upper access points, and any request from an upper service access point to the lower access point. Each KaY and SecY will discard indications for SCIs that do not match one of their receive SCs. Alternatively, the 'Y' function can selectively deliver indications for known SCIs to the appropriate SecY, as instructed by the higher-layer entity responsible for virtual port creation and its association. Its detailed specification is determined by the specification of that entity.

The connectivity provided by a multi-access LAN depends on the security provided and can change as security is deployed, enabled, or disabled. Because this can lead to difficulties in the management of bridged networks, multi-access LANs should not be used to support LANs with two or more attached bridges. They are appropriate for the attachment of end stations or hosts at the periphery of the network.

Replace Figure 11-15 with the following figure:

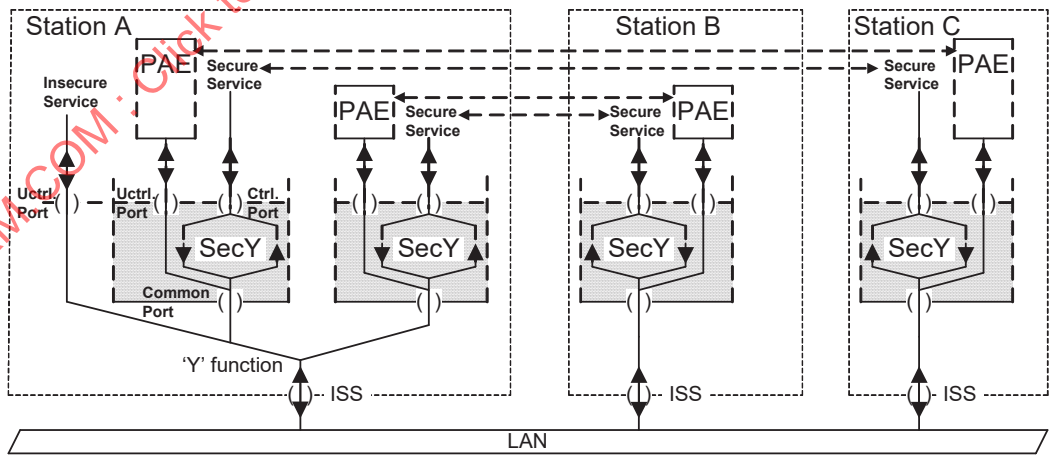


Figure 11-15—An example multi-access LAN

Change the title of Clause 13 as follows:

13. ~~Management protocol~~ MAC Security Entity MIB

13.1 Introduction

Change the text of 13.1 as follows:

This clause ~~defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes managed objects~~ contains an SMIv2 Management Information Base (MIB) for managing the operation of a MAC Security Entity (SecY), based on the specifications contained in Clause 10 and Clause 11. This clause includes a MIB module that is compliant to SMIv2.

13.4 Security considerations

Change the text of the first four paragraphs and accompanying list items in 13.1 as follows:

There are a number of management objects defined in this MIB module with a MAX-ACCESS clause of read-write and/or read-create. ~~Such~~ All such objects ~~may be considered~~ are sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. These are the tables and objects and their sensitivity/vulnerability:

a) secyIfTable, secyIfCipherTable, secyIfICVTable, and secyIfAPTable contain~~s~~ system-level information for each interface supported by the MAC security entity. SET access to ~~this~~ these tables by unauthorized persons can disable the MAC security protection functions, block network connectivity, and impact network performance. ~~Examination of this table in comparison with~~ A comparison of the secyIfTable and the IF-MIB can identify which ports are not protected by ~~the~~ a MAC security entity.
b) secyRxSANextPN (deprecated) in secyRxSATable provides the capability to change the replay protection window. SET access to this object by unauthorized persons can affect the MACsec replay protection function, block network connectivity, and impact network performance.

Some of the readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) ~~may be considered~~ are sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and ~~possible~~ to ~~even~~ encrypt the values of these objects when sending them over the network via SNMP.

The MIB module provides statistics from the interface level (SecY) to each secure association (SA). These statistics provide information for the diagnosis or debugging of the migration from a non-secure environment to a secure environment and can be used to observe the activities of MACsec operation. This information is useful for security monitoring by authorized personnel, but is also potentially useful to attackers so ~~should~~ need to be protected against unauthorized access.

These are the tables and objects and their sensitivity/vulnerability:

c) secyTSATable (and secyTxSATable, deprecated) provides information on~~controls~~ each transmitting SA. secyT~~x~~SAConfidentiality exposes whether confidentiality is supported or not for the SA. This information could help an attacker focus their attacks on traffic without confidentiality protection.

d) secyRxSATable contains information about receiving SAs. secyRxSANextPN is~~parameters~~ used in replay protection to determine which frames should be discarded. Read access to these related parameters could allow an attacker to know the PN range that an attempted replay must fall within.
e) secyCipherSuiteTable provides information about the capabilities of the cipher suites supported by the implementation. Access to this information could allow an attacker to focus their attacks on implementations with specific cipher suites and specific weaknesses~~, e.g., those that lack confidentiality support, or those that only support short integrity check values~~.
f) secyRxSAStatsTable (deprecated) and secyRxSCStatsTable contain statistics for each receiving SA and each receiving SC. Read access could allow an attacker to compare these statistics with Figure 10-5 to determine which aspect of their attack failed, and to modify their attack until a different counter is incremented, indicating that they have succeeded in meeting a particular requirement.
g) secyStatsTable contains statistics about the MAC security entity. This information is SecY interface-level statistics information, and also read access to this information can help an attacker determine if a system might be vulnerable.
h) The global parameters secyIfMaxPeerSCs, secyIfRxMaxKeys, and secyIfTxMaxKeys might be used by an attacker when attempting to overload the system capabilities to cause a denial of service attack.

13.5 Structure of the MIB module

Change 13.5 as follows:

~~A single MIB module is defined in this clause. Objects in the MIB are arranged into groups. Each group is organized as a set of related objects. The overall structure and assignment of objects to their groups is shown in Table 13-1. Table 13-2 contains cross references between the objects defined in 10.7 and the MIB objects defined in 13.6.~~

A single MIB module is defined in this clause. Within the MIB module, each SecY is identified by the InterfaceIndex used by the Interfaces MIB (13.3.2, Figure 13-1) for the Controlled Port sublayer interface. This facilitates identification of the SecY when investigating an interface stack, and discovery of the other entities (via the Interfaces MIB) that are related to a particular SecY, including the associated PAE.

Insert the following text after the initial paragraph of 13.5:

At the top level, the MIB module identifies MIB notifications, MIB objects, and MIB conformance information, though no notifications are defined. Figure 13-1 illustrates the structure of the MIB module, as described in this clause.

NOTE 1—MIB conformance is represented by objects, with an initial OID (object identifier) of secyMIBConformance, but in this MIB description the term *MIB objects* refers specifically to objects with an initial OID of secyMIBObjects.

MIB objects are arranged in a number of tables (in MIB terms a SEQUENCE OF entries) with each entry in the table comprising an number of basic objects (in MIB terms a SEQUENCE OF objects such as truth values, integers, text strings). MIB objects are further classified into management and statistics objects.

The entries in each of the management object tables are indexed in one of the following ways:

a) By the interface index, if the objects in each entry are for the SecY identified by that index)
b) By the interface index and SCI, if the objects are for an SCI used by the SecY
c) By the interface index, SCI, and AN, if the objects are for an SA used by the SecY
d) By a cipher suite index, defined in the module, for information specific to a given cipher suite but applicable to all SecYs in the system

e) By a cipher suite index and SCI, for cipher suite information for a given SecY

Insert a new Figure 13-1 as follows:

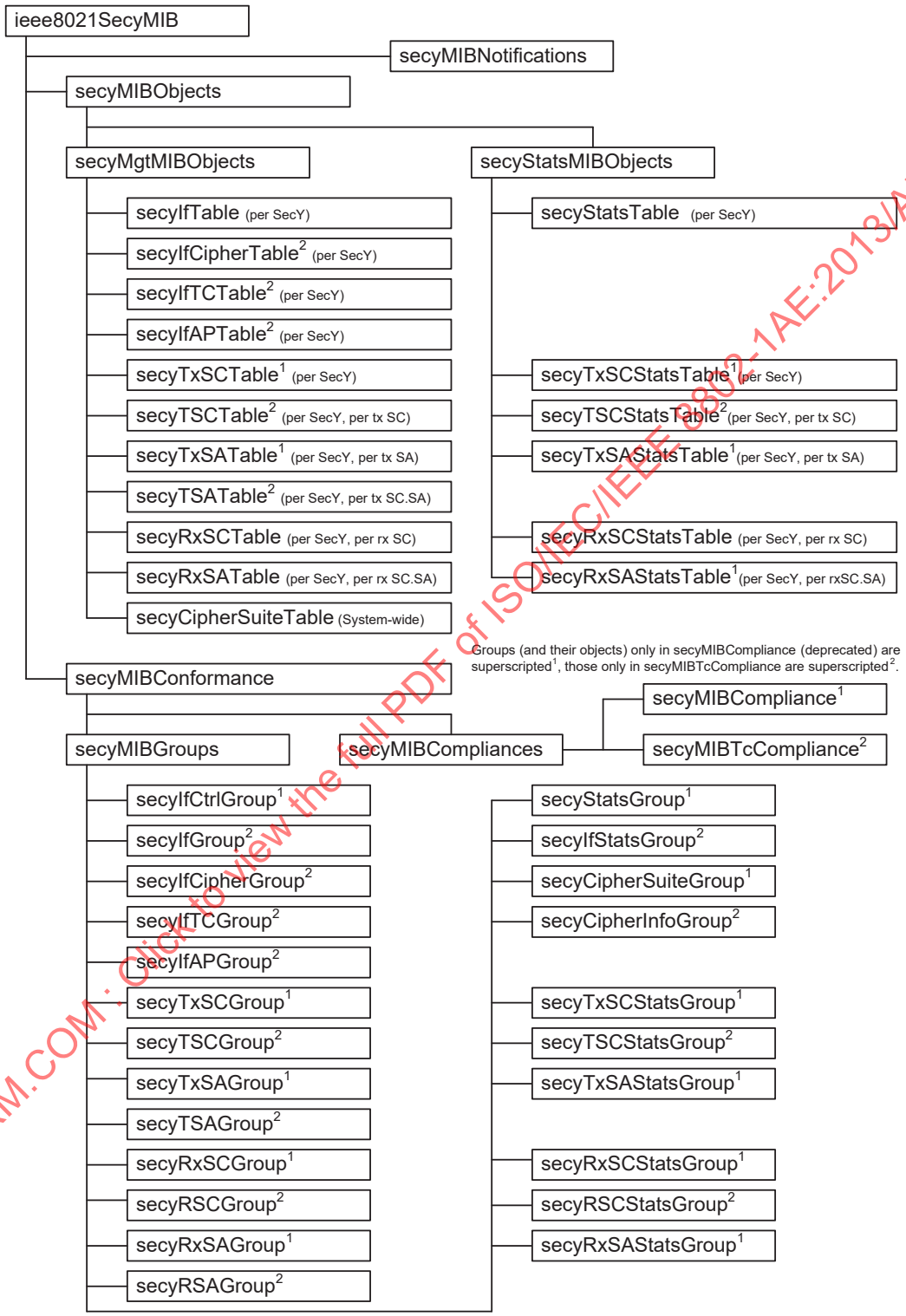


Figure 13-1—Secy MIB structure

Each of the statistics object table entries augments a particular management object table entry, effectively using the same index. The per SecY, per SC, and per SA management tables for Controlled Port transmission and reception are summarized in Table 13-1 and Table 13-2, and the corresponding statistics tables in Table 13-3. Management tables for system-wide and per SecY Cipher Suite information are summarized in Table 13-4.

The MIB conformance objects are organized into compliance statements and conformance groups.

The compliance statement (secyMIBCompliance) for the original revision of this MIB module, published in IEEE Std 802.1AE-2006, mandated implementation of each of the groups specified in that revision, and each of the management object tables and statistics object tables specified has a corresponding group that includes all the objects for each entry in the table, though read-only access is permitted for a number of objects. This compliance statement and some of the tables have now been deprecated, and implementation of all the tables and objects it specifies is no longer a requirement of this standard for a conformance claim of network management MIB support. Implementations may continue to support this original compliance statement to support interoperability, either as an additional or as the only supported compliance statement, but it is expected to become obsolete in some future revision.

The current revision of this MIB module adds support for multiple traffic classes (with a complementary reduction in per SC statistics collection) and extended packet number reporting, with an additional compliance statement (secyMIBTcCompliance) and new conformance groups for additional tables. An implementation of a SecY for which support of network management using the MIB module is claimed should support secyMIBTcCompliance. An implementation that does not require multiple traffic class support can still benefit from reduced statistics collection and from the resolution of minor inconsistencies with the normative text elsewhere in the standard (which takes precedence).

NOTE 2—Annex G provides additional information on the management and MIB revisions.

Delete existing Table 13-1 and Table 13-2.

Insert a new Table 13-1 as follows:

Table 13-1—Controlled Port service management

Table	Table Entry objects	Figure 10-5 reference and definition
secyIfTable secyIfEntry [secyIfInterfaceIndex] secyIfCtrlGroup[1a] secyIfGroup[2]	secyIfInterfaceIndex secyIfSCI[2] secyIfMaxPeerSCs secyIfRxMaxKeys secyIfTxMaxKeys secyIfProtectFramesEnable secyIfValidateFrames secyIfReplayProtectEnable secyIfReplayProtectWindow secyIfCurrentCipherSuite secyIfAdminPt2PtMAC secyIfOperPt2PtMAC secyIfIncludeSCIEnable secyIfUseESEnable secyIfUseSCBEnable secyIfIncludingSCI[2] secyIfMaxTSCs[2]	Aligned with IF-MIB InterfaceIndex (10.1) Generation.sci (7.1.2, 8.2.1, 10.7.1) Verification.maxReceiveChannels (10.7.7) Verification.maxReceiveKeys (10.7.7) Generation.maxTransmitKeys (10.7.16) Generation.protectFrames (10.7.17, Fig 10-4) Verification.validateFrames (10.7.8, Fig 10-5) Verification.replayProtect (10.7.8, Fig 10-5) Verification.replayWindow (10.7.8, Fig 10-5) CurrentCipherSuite.ciphersuite (10.7.25) controlledPort.adminPointToPointMAC (6.5, 10.7.4) controlledPort.operPointToPointMAC (6.5, 10.7.4) Generation.alwaysIncludeSCI (10.5.3,10.7.17) Generation.useES (10.5.3,10.7.17) Generation.useSCB (10.5.3, 10.7.17) Generation.includingSCI (10.5.3, 10.7.17, Fig 10-4) Generation.maxTransmitChannels (10.7.16)
secyIfCipherTable[2] secyIfCipherEntry[2] [secyIfInterfaceIndex, secyCipherSuiteIndex] secyIfCipherGroup[2]	secyIfCipherImplemented[2b] secyIfCipherEnableUse[2] secyIfCipherRqConfidentiality[2]	implementedCipherSuites (10.7.26) CipherSuiteControl.enableUse (10.7.26) CipherSuiteControl.requireConfidentiality (10.7.26)
secyIfTCTable[2] secyIfTCEntry[2] [secyIfInterfaceIndex, secyTCUserPriority[2]] secyTCGroup[2]	secyIfTCUserPriority[2] secyIfTCTrafficClass[2]	Generation.userpri (10.5.1, 10.7.17) TrafficClass.trafficClass (10.5.1, 10.7.17)
secyIfAPTable[2] secyAPEntry[2] [secyIfInterfaceIndex, secyAPUserPCP[2]] secyIfAPGroup[2]	secyIfAPUserPCP[2] secyIfAPAccessPCP[2]	Generation.userpcp (10.5, 10.7.17) AccessPriority.accessPCP (10.5, 10.7.17)

[a]Tables, table entries, groups and objects that appear only in secyMIBCompliance (deprecated) are superscripted[1], and those that appear only in secyTcMIBCompliance (recommended) are superscripted[2]. Those that are used in both are not superscripted.

[b]If the CipherSuite referenced by secyCipherSuiteIndex is not implemented for the SecY identified by the secyIfInterfaceIndex, the corresponding instance of this object is not required, if it is present secyCipherSuiteAvailable (read-only) and secyCipherSuiteEnable (normally read-write) will be False and not writable.

Insert a new Table 13-2 as follows:

Table 13-2—Transmit and receive SC management

Table	Table Entry objects	Figure 10-5 reference and definition
secyTxSCTable[1a] secyTxSCEntry[1] [secyIfInterfaceIndex] secyTxSCGroup[1]	secyTxSCI[1] secyTxSCState[1] secyTxSCEncodingSA[1] secyTxSCEncipheringSA[1] secyTxSCCreatedTime[1] secyTxSCStartedTime[1] secyTxSCStoppedTime[1]	TransmitSC.sci (7.1.2, 10.7.1) TransmitSC.transmitting (10.7.21, 10.7.23) TransmitSC.encodingSA (10.5.1, 10.7.21) deprecated (10.5.4) TransmitSC.createdTime (10.7.21) TransmitSC.startedTime (10.7.21) TransmitSC.stoppedTime (10.7.21)
secyTSCTable secyTSCEntry[2] [secyIfInterfaceIndex, secyTSCI] secyTSCGroup[2]	secyTSCI[2] secyTSCState[2] secyTSCEncodingSA[2] secyTSCCreatedTime[2] secyTSCStartedTime[2] secyTSCStoppedTime[2]	TransmitSC.sci (7.1.2, 10.7.17, 10.7.20) TransmitSC.transmitting (10.7.21, 10.7.23) TransmitSC.encodingSA (10.5.1, 10.7.21) TransmitSC.createdTime (10.7.21) TransmitSC.startedTime (10.7.21) TransmitSC.stoppedTime (10.7.21)
secyTxSATable[1] secyTxSAEntry[1] [secyIfInterfaceIndex, secyTxSA] secyTxSAGroup[1]	secyTxSA[1] secyTxSAState[1] secyTxSANextPN[1] secyTxSAConfidentiality[1] secyTxSASAKUnchanged[1] secyTxSACreatedTime secyTxSAStartedTime secyTxSAStoppedTime	TransmitSC.txa (10.7.22) TransmitSA.inUse (10.7.23) TransmitSA.nextPN (10.5, 10.7.23) TransmitSA.confidentiality (10.7.23) deprecated TransmitSA.createdTime (10.7.23) TransmitSA.startedTime (10.7.23) TransmitSA.stoppedTime (10.7.23)
secyTSATable[2] secyTSAEntry[2] [secyIfInterfaceIndex, secyTSCI, secyTSA] secyTSAGroup[2]	secyTSA[2] secyTSAState[2] secyTSANextXPN[2] secyTSAConfidentiality[2] secyTSACreatedTime[2] secyTSAStartedTime[2] secyTSAStoppedTime[2] secyTSAKeyIdentifier[2] secyTSASSCI[2]	TransmitSC.txa (10.7.22) TransmitSA.inUse (10.7.23) TransmitSA.nextPN (10.5, 10.7.23) TransmitSA.confidentiality (10.7.23) TransmitSA.createdTime (10.7.23) TransmitSA.startedTime (10.7.23) TransmitSA.stoppedTime (10.7.23) TransmitSA.keyIdentifier (10.7.23) TransmitSA.ssci (10.7.23)
secyRxSCTable secyRxSCEntry [secyIfInterfaceIndex, secyRxSCI] secyRxSCGroup[1] secyRcSCGroup[2]	secyRxSCI secyRxSCState secyRxSCCurrentSA[1] secyRxSCCreatedTime secyRxSCStartedTime secyRxSCStoppedTime	ReceiveSC.sci (10.7.11) ReceiveSC.receiving (10.7.12, 10.7.14, 10.7.15) deprecated ReceiveSC.createdTime (10.7.12) ReceiveSC.startedTime (10.7.12) ReceiveSC.stoppedTime (10.7.12)
secyRxSATable secyRxSAEntry [secyIfInterfaceIndex, secyRxSCI, secyRxSA] secyRxSAGroup[1] secyRSAGroup[2]	secyRxSA secyRxSAState secyRxSANextPN[1] secyRxSANextXPN[2] secyRxSALowestXPN[2] secyRxSASAKUnchanged[1] secyRxSACreatedTime secyRxSAStartedTime secyRxSAStoppedTime secyRxSAKeyIdentifier[2] secyRxSASSCI[2]	ReceiveSC.rxa (10.7.13) ReceiveSA.inUse (10.7.14) deprecated ReceiveSA.nextPN (10.7.14) ReceiveSA.lowestPN (10.6.2, 10.6.4, 10.6.5, 10.7.14, Fig 10-5) deprecated ReceiveSA.createdTime (10.7.14) ReceiveSA.startedTime (10.7.14) ReceiveSA.stoppedTime (10.7.14) ReceiveSA.keyIdentifier (10.7.14) ReceiveSA.ssci (10.7.14)

[a]Tables, table entries, groups and objects that appear only in secyMIBCompliance (deprecated) are superscripted[1], and those that appear only in secyTcMIBCompliance (recommended) are superscripted[2]. Those that are used in both are not superscripted.

Insert a new Table 13-3 as follows:

Table 13-3—Transmit and receive statistics

Table	Table Entry objects	Figure 10-5 reference and definition
secyStatsTable secyStatsEntry augments secyIfEntry secyStatsGroup[1a] secyIfStatsGroup[2] secyCipherStatsGroup[2]	secyStatsTxUntaggedPkts secyStatsTxTooLongPkts secyStatsRxUntaggedPkts secyStatsRxNoTagPkts secyStatsRxBadTagPkts secyStatsRxUnknownSCIPkts[1] secyStatsRxNoSCIPkts[1] secyStatsRxOverrunPkts secyStatsRxNoSAPkts[2] secyStatsRxNoSAErrorPkts[2] secyStatsTxOctetsProtected[2] secyStatsTxOctetsEncrypted[2] secyStatsRxOctetsValidated[2] secyStatsRxOctetsDecrypted[2]	Generation.OutPktsUntagged (10.7.18, Fig 10-4) Generation.OutPktsTooLong (10.7.18, Fig 10-4) Verification.InPktsUntagged (10.7.18, Fig 10-4) Verification.InPktsNoTag (10.7.9, Fig 10-5) Verification.InPktsBadTag (10.7.9, Fig 10-5) deprecated deprecated Verification.InPktsOverrun (10.7.9, Fig 10-5) Verification.InPktsNoSA (10.7.9, Fig 10-5) Verification.InPktsNoSAError(10.7.9, Fig 10-5) Generation.OutOctetsProtected (10.7.9, Fig 10-4) Generation.OutsOctetsEncrypted (10.7.9, Fig 10-4) Verification.InOctetsValidated (10.6.3, Fig 10-5) Verification.InOctetsValidated (10.6.3, Fig 10-5)
secyTxSCStatsTable[1] secyTxSCStatsEntry[1] augments secyTxSCEntry secyTxSCStatsGroup[1]	secyTxSCStatsProtectedPkts [1] secyTxSCStatsEncryptedPkts[1] secyTxSCStatsOctetsProtected[1] secyTxSCStatsOctetsEncrypted[1]	TransmitSC.OutPktsProtected (10.7.18, Fig 10-4) TransmitSC.OutPktsEncrypted (10.7.18, Fig 10-4) deprecated deprecated
secyTSCStatsTable[2] secyTSCStatsEntry[2] augments secyTSCEntry secyTSCStatsGroup[2]	secyTSCStatsProtectedPkts[2] secyTSCStatsEncryptedPkts[2]	TransmitSC.OutPktsProtected (10.7.18, Fig 10-4) TransmitSC.OutPktsEncrypted (10.7.18, Fig 10-4)
secyTxSAStatsTable[1] secyTxSAStatsEntry[1] augments secyTxSAEntry[1] secyTxSAStatsGroup[1]	secyTxSAStatsProtectedPkts[1] secyTxSAStatsEncryptedPkts[1]	deprecated deprecated
secyRxSCStatsTable secyRxSCStatsEntry augments secyRxSCEntry secyRxSCStatsGroup[1] secyRSCStatsGroup[2]	secyRxSCStatsUnusedSAPkts[1] secyRxSCStatsNoUsingSAPkts[1] secyRxSCStatsLatePkts secyRxSCStatsNotValidPkts secyRxSCStatsInvalidPkts secyRxSCStatsDelayedPkts secyRxSCStatsUncheckedPkts secyRxSCStatsOKPkts secyRxSCStatsOctetsValidated[1] secyRxSCStatsOctetsDecrypted[1]	deprecated deprecated ReceiveSC.InPktsLate (10.7.9, Fig 10-5) ReceiveSC.InPktsNotValid (10.7.9, Fig 10-5) ReceiveSC.InPktsInvalid (10.7.9, Fig 10-5) ReceiveSC.InPktsDelayed (10.7.9, Fig 10-5) ReceiveSC.InPktsUnchecked (10.7.9, Fig 10-5) ReceiveSC.InPktsOK(10.7.9, Fig 10-5) deprecated deprecated
secyRxSAStatsTable[1] secyRxSAStatsEntry augments secyRxSAEntry secyRxSAStatsGroup[1]	secyRxSAStatsUnusedSAPkts[1] secyRxSAStatsNotUsingSAPkts[1] secyRxSAStatsNotValidPkts[1] secyRxSAStatsInvalidPkts[1] secyRxSAStatsOKPkts[1]	deprecated deprecated deprecated deprecated deprecated

[a]Tables, table entries, groups and objects that appear only in secyMIBCompliance (deprecated) are superscripted[1], and those only in secyTcMIBCompliance (recommended) are superscripted[2]. Those that are used in both are not superscripted.

Insert a new Table 13-4 as follows:

Table 13-4—Cipher Suite information

Table Table Entry [Index]	Table Entry Objects	Figure 10-5 reference and definition
secyCipherSuiteTable secyCipherSuiteEntry [secyCipherSuiteIndex] secyCipherSuiteGroup[1] secyCipherInfoGroup[2]	secyCipherSuiteIndex secyCipherSuiteId secyCipherSuiteName secyCipherSuiteCapability secyCipherSuiteProtection[1] secyCipherSuiteProtectionOffset[1] secyCipherSuiteDataLengthChange secyCipherSuiteICVLength secyCipherSuiteRowStatus[1]	 CipherSuite.identifier (10.7.25, Table 14-1) CipherSuite.name (10.7.25, Table 14-1) CipherSuite.integrityProtection, confidentialityProtection (10.7.25) deprecated deprecated CipherSuite.changesDataLength (10.7.25) CipherSuite.ICVlength (10.7.25) deprecated

Change the title of 13.6 as follows:

13.6 ~~Definitions for~~ MAC Security Entity (SecY) MIB definitions

Delete the entire text of the MIB definition in 13.6, following the introductory sentence, and insert the following text:

```
-- ****************************************************************
-- IEEE8021-SECY-MIB
--
-- Definitions of managed objects supporting IEEE 802.1AE MACsec.
-- ****************************************************************

IEEE8021-SECY-MIB DEFINITIONS ::= BEGIN

-- ----------------------------------------------------------------
-- IEEEE802.1AE MIB
-- ----------------------------------------------------------------

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

ieee8021SecyMIB MODULE-IDENTITY
    LAST-UPDATED    "201605102049Z"
    ORGANIZATION    "IEEE 802.1 Working Group"
    CONTACT-INFO    "http:/grouper.ieee.org/groups/8021/index.html"
    DESCRIPTION
    "The MAC security entity (SecY) MIB module. A SecY is a protocol
     shim providing MAC Security (MACsec) in an interface stack.
```

```
        Each SecY transmits MACsec protected frames on one or more
        Secure Channels (SCs) to each of the other SecYs attached to the
        same LAN and participating in the same Secure Connectivity
        Association (CA). The CA is a security relationship, that is
        established and maintained by key agreement protocols and supported
        by MACsec to provide full connectivity between its participants.
        Each SC provides unidirectional point to multipoint connectivity
        from one participant to all the others and is supported by a
        succession of similarly point to multipoint Secure Associations
        (SAs). The Secure Association  Key (SAK) used to protect frames is
        changed as an SA is replaced by its (overlapping) successor so
        fresh keys can be used without disrupting a long lived SC and CA.

        Two different upper interfaces, a Controlled Port (for frames
        protected by MACsec, providing an instance of the secure MAC
        service) and an Uncontrolled Port (for frames not requiring
        protection, like the key agreement frames used to establish the
        CA and distribute keys) are associated with a SecY  shim. For each
        instance of a SecY 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)'.

        ____________________________________|____________________________________
        |                                   |                                   |
        |  Controlled Port Interface        |   Uncontrolled Port Interface     |
        |  (ifEntry = j,ifType =            |   (ifEntry = k, ifType =          |
        |   macSecControlledIF(231))        |    macSecUncontrolledIF(232))     |
        |___________________________________|___________________________________|
        |                                                                       |
        |                      Physical Interface                               |
        |                        (ifEntry = i)                                  |
        |                  (ifType = ethernetCsmacd(6))                         |
        |_______________________________________________________________________|
           Example MACsec Interface Stack. i, j, k are ifIndexes each
           indicating a row in the ifTable.
    "
    REVISION    "201605102049Z"
    DESCRIPTION
    "Updated by the IEEE Std 802.1AEcg amendment. Object DESCRIPTIONs
     and references aligned with text of the standard (including prior
     amendments). IEEE 802.1AEcg Annex G details changes.
     The initial version of this ieee8021SecyMIB used the object
     name prefix 'secy' rather than 'ieee8021secy' (recommended by
     RFC 4181). The 'secy' prefix has been retained in this revision for
     for backwards compatbility and internal consistency."

    REVISION    "200601100000Z"
    DESCRIPTION "Initial version of this MIB in IEEE 802.1AE-2006"
    ::= { iso(1) std(0) iso8802(8802) ieee802dot1(1)
          ieee802dot1mibs(1) 3 }

secyMIBNotifications OBJECT IDENTIFIER ::= { ieee8021SecyMIB 0 }

secyMIBObjects OBJECT IDENTIFIER ::= { ieee8021SecyMIB 1 }

secyMIBConformance OBJECT IDENTIFIER ::= { ieee8021SecyMIB 2 }

--
-- Textual Conventions
--

SecySCI ::= TEXTUAL-CONVENTION
    STATUS current
    DESCRIPTION
```

```
        "Textual convention for a Secure Channel Identifier (SCI).

         Each SC is identified by an SCI comprising a 48-bit MAC Address,
         allocated to the transmitting system and a 16-bit Port Identifier."
        REFERENCE   "IEEE 802.1AE Clause 7.1.2 and figure 7.7"
        SYNTAX OCTET STRING (SIZE (8))

    SecyAN ::= TEXTUAL-CONVENTION
        DISPLAY-HINT "d"
        STATUS current
        DESCRIPTION
        "Textual convention for an Association Number (AN).

         Each SC is comprised of a succession of SAs, each with a different
         SAK, identified by a Secure Association Identifier (SAI) comprising
         an SCI concatenated with a two-bit AN.  The SAI is unique for SAs
         used by SecYs participating in a given CA at any instant."
        REFERENCE   "IEEE 802.1AE Clause 7.1.3, Figure 7.7"
        SYNTAX Unsigned32 (0..3)

    secyMgmtMIBObjects OBJECT IDENTIFIER ::= { secyMIBObjects 1 }

    secyStatsMIBObjects OBJECT IDENTIFIER ::= { secyMIBObjects 2 }

    --
    -- SecY Interface Management Table
    --

    secyIfTable    OBJECT-TYPE
        SYNTAX      SEQUENCE OF SecyIfEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
        "A table with an entry for each service interface in this system
         with MAC Security capability, i.e. for each SecY.

         The configured value of writable objects in each table entry
         shall be stored in persistent memory and remain unchanged across
         a re-initialization of the system's management entity."
        REFERENCE "IEEE 802.1AE Clause 10.7, Table 13-1"
        ::= { secyMgmtMIBObjects 1 }

    secyIfEntry    OBJECT-TYPE
        SYNTAX      SecyIfEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
        "A table entry with service information for a particular SecY."
        INDEX   { secyIfInterfaceIndex }
        ::= { secyIfTable 1 }

    SecyIfEntry ::= SEQUENCE {
        secyIfInterfaceIndex            InterfaceIndex,
        secyIfMaxPeerSCs                Unsigned32,
        secyIfRxMaxKeys                 Unsigned32,
        secyIfTxMaxKeys                 Unsigned32,
        secyIfProtectFramesEnable       TruthValue,
        secyIfValidateFrames            INTEGER,
        secyIfReplayProtectEnable       TruthValue,
        secyIfReplayProtectWindow       Unsigned32,
        secyIfCurrentCipherSuite        Unsigned32,
        secyIfAdminPt2PtMAC             INTEGER,
        secyIfOperPt2PtMAC              TruthValue,
        secyIfIncludeSCIEnable          TruthValue,
```

```
    secyIfUseESEnable               TruthValue,
    secyIfUseSCBEnable              TruthValue,
    secyIfSCI                       SecySCI,      -- 802.1AEcg
    secyIfIncludingSCI              TruthValue,   -- 802.1AEcg
    secyIfMaxTSCs                   Unsigned32    -- 802.1AEcg
}

secyIfInterfaceIndex    OBJECT-TYPE
    SYNTAX      InterfaceIndex
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An interface index, aligned with ifIndex in the
                 ifTable, pointing to the SecY's Controlled Port."
    REFERENCE   "IEEE 802.1AE Clause 10.1"
    ::= { secyIfEntry 1 }

secyIfMaxPeerSCs    OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "security connections"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The maximum number of peer SCs for this SecY."
    REFERENCE   "IEEE 802.1AE Clause 10.7.7"
    ::= { secyIfEntry 2 }

secyIfRxMaxKeys    OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "keys"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The maximum number of keys in simultaneous use for
                 reception for this SecY."
    REFERENCE   "IEEE 802.1AE Clause 10.7.7"
    ::= { secyIfEntry 3 }

secyIfTxMaxKeys    OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "keys"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The maximum number of keys in simultaneous use for
                 transmission for this SecY."
    REFERENCE   "IEEE 802.1AE Clause 10.7.16"
    ::= { secyIfEntry 4 }

secyIfProtectFramesEnable    OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Enables or disables protection of transmitted frames."
    REFERENCE   "IEEE 802.1AE Clause 10.7.17, Figure 10-3"
    DEFVAL { true }
    ::= { secyIfEntry 5 }

secyIfValidateFrames    OBJECT-TYPE
    SYNTAX      INTEGER {
                    disabled(1),
                    check(2),
                    strict(3),
                    null(4)    -- 802.1AEcg
                }
    MAX-ACCESS  read-write
    STATUS      current
```

```
        DESCRIPTION
        "Controls validation of received frames.

         disabled(1) : disable validation, remove SecTAGs and ICVs (if
                       present) from received frames.
         check(2)    : enable validation, do not discard invalid frames.
         strict(3)   : enable validation and  discard invalid frames.
         null(4)     : no processing, do not remove SecTAGs or ICVs."
        REFERENCE   "IEEE 802.1AE Clause 10.7.8, Figure 10-4"
        DEFVAL { strict }
        ::= { secyIfEntry 6 }

    secyIfReplayProtectEnable    OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION "Enables or disables replay protection."
        REFERENCE   "IEEE 802.1AE Clause 10.7.8, Figure 10-4"
        DEFVAL { true }
        ::= { secyIfEntry 7 }

    secyIfReplayProtectWindow    OBJECT-TYPE
        SYNTAX      Unsigned32
        UNITS       "Packets"
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION "The replay protection window size."
        REFERENCE   "IEEE 802.1AE Clause 10.7.8, Figure 10-4"
        DEFVAL { 0 }
        ::= { secyIfEntry 8 }

    secyIfCurrentCipherSuite    OBJECT-TYPE
        SYNTAX      Unsigned32
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION "The Cipher Suite currently used by this SecY,
                     identified by the secyCipherSuiteTable entry index.
                     Should be read-only if secyIfCipherTable implemented."
        REFERENCE   "IEEE 802.1AE Clause 10.7.25"
        ::= { secyIfEntry 9 }

    secyIfAdminPt2PtMAC    OBJECT-TYPE
        SYNTAX      INTEGER {
                      forceTrue(1),
                      forceFalse(2),
                      auto(3)
                    }
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
        "Controls the value of operPointToPointMAC (secyOperPt2PtMAC)
        reported to the user(s) of this SecY's Controlled Port.

         forceTrue(1)  : operPointToPointMAC is True, regardless of the
                         configuration and status of the SecY.
         forceFalse(2) : operPointToPointMAC is False, regardless of the
                         configuration and status of the SecY.
         auto(3)       : OperPointMAC is True if secyIfvalidateFrames is
                         strict and reception is from at most one peer SecY,
                         or if secyIfvalidateFrames is not strict and
                         operPointToPointMAC is True for the Common Port,
                         and is False otherwise."
        REFERENCE   "IEEE 802.1AE Clause 6.5, 10.7.4"
        DEFVAL { auto }
```

```
    ::= { secyIfEntry 10 }

secyIfOperPt2PtMAC    OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
    "Reflects the current service connectivity to be assumed by the
     user(s) of the SecY's Controlled Port.

     true(1)  : connectivity is to at most one other system.
     false(2) : connectivity is to one or more other systems."
    REFERENCE   "IEEE 802.1AE Clause 6.5, 10.7.4"
    ::= { secyIfEntry 11 }

secyIfIncludeSCIEnable    OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION "Mandates inclusion of an explicit SCI in the SecTAG
                 when transmitting protected frames."
    REFERENCE   "IEEE 802.1AE Clause 10.5.3 alwaysIncludeSCI, 10.7.17"
    DEFVAL { false }
    ::= { secyIfEntry 12 }

secyIfUseESEnable    OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION "Enables use of the ES bit in the SecTAG when
                 transmitting protected frames."
    REFERENCE   "IEEE 802.1AE Clause 10.5.3 useES, 10.7.17"
    DEFVAL { false }
    ::= { secyIfEntry 13 }

secyIfUseSCBEnable    OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION "Enables use of the SCB bit in the SecTAG when
                 transmitting protected frames."
    REFERENCE   "IEEE 802.1AE Clause 10.5.3 useSCB, 10.7.17"
    DEFVAL { false }
    ::= { secyIfEntry 14 }

secyIfSCI     OBJECT-TYPE
    SYNTAX      SecySCI
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The SCI for the SecY's default traffic class."
    REFERENCE   "IEEE 802.1AE Clause 7.1.2, 10.7.1"
    ::= { secyIfEntry 15 }

secyIfIncludingSCI    OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "True if an explicit SCI is included in the SecTAG when
                 transmitting protected frames."
    REFERENCE   "IEEE 802.1AE Clause 10.5.3 includingSCI, 10.7.17"
    DEFVAL { false }
    ::= { secyIfEntry 16 }

secyIfMaxTSCs    OBJECT-TYPE
```

```
    SYNTAX      Unsigned32
    UNITS       "security connections"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The maximum number of transmit SCs for this SecY."
    REFERENCE   "IEEE 802.1AE Clause 10.7.16"
    ::= { secyIfEntry 17 }

--
-- Tx SC Management Table : systems not supporting traffic class SCs
--

secyTxSCTable   OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyTxSCEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "A table with an entry for each SecY's transmit SC."
    REFERENCE   "IEEE 802.1AE Clause 10.7.17, 10.7.20, Table 13-2"
    ::= { secyMgmtMIBObjects 2 }

secyTxSCEntry    OBJECT-TYPE
    SYNTAX      SecyTxSCEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry with transmit SC information for a SecY."
    INDEX { secyIfInterfaceIndex }
    ::= { secyTxSCTable 1 }

SecyTxSCEntry ::= SEQUENCE {
    secyTxSCI               SecySCI,
    secyTxSCState           INTEGER,
    secyTxSCEncodingSA      RowPointer,
    secyTxSCEncipheringSA   RowPointer, -- deprecated
    secyTxSCCreatedTime     TimeStamp,
    secyTxSCStartedTime     TimeStamp,
    secyTxSCStoppedTime     TimeStamp
}

secyTxSCI       OBJECT-TYPE
    SYNTAX      SecySCI
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The SCI for the SecY's transmit SC."
    REFERENCE   "IEEE 802.1AE Clause 7.1.2, 10.7.1"
    ::= { secyTxSCEntry 1 }

secyTxSCState   OBJECT-TYPE
    SYNTAX      INTEGER {
                    inUse(1),
                    notInUse(2)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The transmitting state of the SecY's transmit SC.
                 inUse(1) : one or more SAs are in use.
                 notInUse(2) : no SAs are in use."
    REFERENCE   "IEEE 802.1AE Clause 10.7.21 transmitting, 10.7.23"
    ::= { secyTxSCEntry 2 }

secyTxSCEncodingSA    OBJECT-TYPE
    SYNTAX      RowPointer
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
```

```
        "The SA currently used to encode the SecTAG for frames awaiting
         transmission. The row pointer will point to an entry in the
         secyTxSATable. If no such information is available, the value shall
         be the OBJECT IDENTIFIER { 0 0 }."
        REFERENCE   "IEEE 802.1AE Clause 10.5.1, 10.7.21"
        ::= { secyTxSCEntry 3 }

    secyTxSCEncipheringSA    OBJECT-TYPE
        SYNTAX      RowPointer
        MAX-ACCESS  read-only
        STATUS      deprecated -- 802.1AEcg
        DESCRIPTION
        "The SA currently used to encipher frames for transmission.
         The row pointer will point to an entry in the secyTxSATable.
         If no such information is available, the value shall be the
         OBJECT IDENTIFIER { 0 0 }."
        REFERENCE   "IEEE 802.1AE Clause 10.5.4"
        ::= { secyTxSCEntry 4 }

    secyTxSCCreatedTime    OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The system time when this transmitting SC was created."
        REFERENCE   "IEEE 802.1AE Clause 10.7.21"
        ::= { secyTxSCEntry 5 }

    secyTxSCStartedTime    OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The system time when this transmitting SC last started
                     transmitting MACsec frames."
        REFERENCE   "IEEE 802.1AE Clause 10.7.21"
        ::= { secyTxSCEntry 6 }

    secyTxSCStoppedTime    OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The system time when this transmitting SC last stopped
                     transmitting MACsec frames."
        REFERENCE   "IEEE 802.1AE Clause 10.7.21"
        ::= { secyTxSCEntry 7 }

    --
    -- Traffic Class capable transmit SC Management Table : 802.1AEcg
    --

    secyTSCTable   OBJECT-TYPE
        SYNTAX      SEQUENCE OF SecyTSCEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION "A table of entries for each SecY's traffic class SCs."
        REFERENCE   "IEEE 802.1AE Clause 7.1.2, 10.7.17, 10.7.20"
        ::= { secyMgmtMIBObjects 10 }

    secyTSCEntry   OBJECT-TYPE
        SYNTAX      SecyTSCEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION "An entry with transmit SC information for one of the
                     system's SecYs and one of its traffic classes."
        INDEX { secyIfInterfaceIndex, secyTSCI }
```

```
    ::= { secyTSCTable 1 }

SecyTSCEntry ::= SEQUENCE {
    secyTSCI                SecySCI,
    secyTSCState            INTEGER,
    secyTSCEncodingSA       RowPointer,
    secyTSCCreatedTime      TimeStamp,
    secyTSCStartedTime      TimeStamp,
    secyTSCStoppedTime      TimeStamp
}

secyTSCI        OBJECT-TYPE
    SYNTAX       SecySCI
    MAX-ACCESS   not-accessible
    STATUS       current
    DESCRIPTION "The SCI for the transmit SC for this SecY and
                 traffic class."
    REFERENCE    "IEEE 802.1AE Clause 7.1.2, 10.7.17, 10.7.20"
    ::= { secyTSCEntry 1 }

secyTSCState    OBJECT-TYPE
    SYNTAX       INTEGER {
                     inUse(1),
                     notInUse(2)
                 }
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
    "The state of the transmit SC for this SecY and traffic class.

     inUse(1)     : one or more SAs for the traffic class SC are in use.
     notInUse(2) : no SAs for the traffic class SC are in use."
    REFERENCE    "IEEE 802.1AE Clause 10.7.20"
    ::= { secyTSCEntry 2 }

secyTSCEncodingSA    OBJECT-TYPE
    SYNTAX       RowPointer
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
    "The SA currently used to encode the SecTAG for frames awaiting
     transmission. The row pointer will point to an entry in the
     secyTxSATable. If no such information is available, the value shall
     be the OBJECT IDENTIFIER { 0 0 }."
    REFERENCE    "IEEE 802.1AE Clause 10.5.1, 10.7.21"
    ::= { secyTSCEntry 3 }

secyTSCCreatedTime    OBJECT-TYPE
    SYNTAX       TimeStamp
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "The system time when this transmitting SC was created."
    REFERENCE    "IEEE 802.1AE Clause 10.7.21"
    ::= { secyTSCEntry 4 }

secyTSCStartedTime    OBJECT-TYPE
    SYNTAX       TimeStamp
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION "The system time when this transmitting SC last started
                 transmitting MACsec frames."
    REFERENCE    "IEEE 802.1AE Clause 10.7.21"
    ::= { secyTSCEntry 5 }
```

```
secyTSCStoppedTime    OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The system time when this transmitting SC last stopped
                 transmitting MACsec frames."
    REFERENCE   "IEEE 802.1AE Clause 10.7.21"
    ::= { secyTSCEntry 6 }

--
-- Tx SA Management Table : systems not supporting traffic class SCs
--

secyTxSATable   OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyTxSAEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "A table with an entry for each transmit SA for each of
                 the system's SecYs."
    REFERENCE   "IEEE 802.1AE Clause 10.7.22, Table 13-2"
    ::= { secyMgmtMIBObjects 3 }

secyTxSAEntry    OBJECT-TYPE
    SYNTAX      SecyTxSAEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry for a transmit SA."
    INDEX   { secyIfInterfaceIndex, secyTxSA }
    ::= { secyTxSATable 1 }

SecyTxSAEntry ::= SEQUENCE {
    secyTxSA                    SecyAN,
    secyTxSAState               INTEGER,
    secyTxSANextPN              Unsigned32,
    secyTxSAConfidentiality     TruthValue,
    secyTxSASAKUnchanged        TruthValue, -- deprecated
    secyTxSACreatedTime         TimeStamp,
    secyTxSAStartedTime         TimeStamp,
    secyTxSAStoppedTime         TimeStamp
}

secyTxSA    OBJECT-TYPE
    SYNTAX      SecyAN
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "The association number (AN) for this transmit SA."
    REFERENCE   "IEEE 802.1AE Clause 10.7.22"
    ::= { secyTxSAEntry 1 }

secyTxSAState    OBJECT-TYPE
    SYNTAX      INTEGER {
                    inUse(1),
                    notInUse(2)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The current status of the transmitting SA.

                 inUse(1)    : this SA is in use.
                 notInUse(2) : this SA is not in use."
    REFERENCE   "IEEE 802.1AE Clause 10.7.22"
    ::= { secyTxSAEntry 2 }

secyTxSANextPN    OBJECT-TYPE
```

```
        SYNTAX      Unsigned32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The next packet number (PN) for this SA."
        REFERENCE   "IEEE 802.1AE Clause 10.5, 10.7.23"
        ::= { secyTxSAEntry 3 }

    secyTxSAConfidentiality    OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "True if the SA provides confidentiality as well as
                     integrity for transmitted frames."
        REFERENCE   "IEEE 802.1AE Clause 10.7.23"
        ::= { secyTxSAEntry 4 }

    secyTxSASAKUnchanged    OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-only
        STATUS      deprecated -- 802.1AEcg
        DESCRIPTION "A reference to an SAK that is unchanged for the life
                     of the transmitting SA."
        REFERENCE   "IEEE 802.1AE Clause 10.7.22"
        ::= { secyTxSAEntry 5 }

    secyTxSACreatedTime    OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The system time when this transmit SA was created."
        REFERENCE   "IEEE 802.1AE Clause 10.7.23"
        ::= { secyTxSAEntry 6 }

    secyTxSAStartedTime    OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The system time when this transmit SA last started
                     transmitting MACsec frames."
        REFERENCE   "IEEE 802.1AE Clause 10.7.23"
        ::= { secyTxSAEntry 7 }

    secyTxSAStoppedTime    OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The system time when this transmit SA last stopped
                     transmitting MACsec frames."
        REFERENCE   "IEEE 802.1AE Clause 10.7.23"
        ::= { secyTxSAEntry 8 }

    --
    -- Trafffic Class capable transmit SA Management Table : 802.1AEcg
    --

    secyTSATable   OBJECT-TYPE
        SYNTAX      SEQUENCE OF SecyTSAEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION "A table with an entry for each transmit SA for each of
                     the system's SecYs."
        REFERENCE   "IEEE 802.1AE Clause 10.7.22, Table 13-2"
        ::= { secyMgmtMIBObjects 11 }
```

```
secyTSAEntry    OBJECT-TYPE
    SYNTAX      SecyTSAEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry for a transmit SA."
    INDEX   { secyIfInterfaceIndex, secyTSCI, secyTSA }
    ::= { secyTSATable 1 }

SecyTSAEntry ::= SEQUENCE {
    secyTSA                     SecyAN,
    secyTSAState                INTEGER,
    secyTSANextXPN              Counter64,
    secyTSAConfidentiality      TruthValue,
    secyTSAKeyIdentifier        SnmpAdminString,
    secyTSASSCI   Integer32,
    secyTSACreatedTime          TimeStamp,
    secyTSAStartedTime          TimeStamp,
    secyTSAStoppedTime          TimeStamp
}

secyTSA     OBJECT-TYPE
    SYNTAX      SecyAN
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "The association number (AN) for this transmit SA."
    REFERENCE   "IEEE 802.1AE Clause 10.7.22"
    ::= { secyTSAEntry 1 }

secyTSAState   OBJECT-TYPE
    SYNTAX      INTEGER {
                    inUse(1),
                    notInUse(2)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The current status of the transmit SA.

                 inUse(1) : this SA is in use.
                 notInUse(2) : this SA is not in use."
    REFERENCE   "IEEE 802.1AE Clause 10.7.23"
    ::= { secyTSAEntry 2 }

secyTSANextXPN  OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The next packet number (PN) for this SA."
    REFERENCE   "IEEE 802.1AE Clause 10.5, 10.7.23"
    ::= { secyTSAEntry 3 }

secyTSAConfidentiality    OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "True if the SA provides confidentiality as well as
                 integrity for transmitted frames."
    REFERENCE   "IEEE 802.1AE Clause 10.7.23"
    ::= { secyTSAEntry 4 }

secyTSAKeyIdentifier    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (1..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The Key Identifier (KI) for the SAK for this SA."
```

```
        REFERENCE   "IEEE 802.1X, IEEE 802.1AE Clause 10.7.23"
        ::= { secyTSAEntry 5 }

    secyTSASSCI     OBJECT-TYPE
        SYNTAX      Integer32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The SSCI for this SA, 0 if an XPN Cipher Suite is not
                    being used."
        REFERENCE   "IEEE 802.1X, IEEE 802.1AE Clause 10.7.23"
        ::= { secyTSAEntry 6 }

    secyTSACreatedTime    OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The system time when this transmit SA was created."
        REFERENCE   "IEEE 802.1AE Clause 10.7.23"
        ::= { secyTSAEntry 7 }

    secyTSAStartedTime    OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The system time when this transmit SA last started
                     transmitting MACsec frames."
        REFERENCE   "IEEE 802.1AE Clause 10.7.23"
        ::= { secyTSAEntry 8 }

    secyTSAStoppedTime    OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The system time when this transmit SA last stopped
                     transmitting MACsec frames."
        REFERENCE   "IEEE 802.1AE Clause 10.7.23"
        ::= { secyTSAEntry 9 }

    --
    -- Rx SC Management Table
    --

    secyRxSCTable   OBJECT-TYPE
        SYNTAX      SEQUENCE OF SecyRxSCEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION "A table for the system's SecY's receive SCs."
        REFERENCE   "IEEE 802.1AE Clause 10.7.11, Table 13-2"
        ::= { secyMgmtMIBObjects 4 }

    secyRxSCEntry   OBJECT-TYPE
        SYNTAX      SecyRxSCEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION "An entry for one of the SCs used by one of the system's
                     SecY's to receive protected frames."
        INDEX    { secyIfInterfaceIndex, secyRxSCI }
        ::= { secyRxSCTable 1 }

    SecyRxSCEntry ::= SEQUENCE {
        secyRxSCI              SecySCI,
        secyRxSCState          INTEGER,
        secyRxSCCurrentSA      RowPointer,
        secyRxSCCreatedTime    TimeStamp,
```

```
    secyRxSCStartedTime     TimeStamp,
    secyRxSCStoppedTime     TimeStamp
}

secyRxSCI       OBJECT-TYPE
    SYNTAX      SecySCI
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "The SCI for the receive SC."
    REFERENCE   "IEEE 802.1AE Clause 10.7.11"
    ::= { secyRxSCEntry 1 }

secyRxSCState   OBJECT-TYPE
    SYNTAX      INTEGER {
                    inUse(1),
                    notInUse(2)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The state of the receive SC.

                 inUse(1) : one or more SAs for this SC are in use.
                 notInUse(2) : no SAs for this SC is in use."
    REFERENCE   "IEEE 802.1AE Clause 10.7.12 receiving,
                                      10.7.14 inUse, 10.7.15"
    ::= { secyRxSCEntry 2 }

secyRxSCCurrentSA    OBJECT-TYPE
    SYNTAX      RowPointer
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION
    "The current receiving association number of the SC in use.
     The row pointer will point to an entry in the secyRxSATable.  If no
     such information can be identified, the value of this object shall
     be the OBJECT IDENTIFIER {0 0 }."
    REFERENCE   "IEEE 802.1AE Clause 10.6.1, 10.7.13"
    ::= { secyRxSCEntry 3 }

secyRxSCCreatedTime    OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The system time when this receiving SC was created."
    REFERENCE   "IEEE 802.1AE Clause 10.7.12"
    ::= { secyRxSCEntry 4 }

secyRxSCStartedTime    OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The system time when this receiving SC last started
                 receiving MACsec frames."
    REFERENCE   "IEEE 802.1AE Clause 10.7.12"
    ::= { secyRxSCEntry 5 }

secyRxSCStoppedTime    OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The system time when this receiving SC last stopped
                 receiving MACsec frames."
    REFERENCE   "IEEE 802.1AE Clause 10.7.12"
    ::= { secyRxSCEntry 6 }
```

```
--
-- Rx SA Management Table
--

secyRxSATable   OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyRxSAEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "A table with entries for the system's receive SAs."
    REFERENCE   "IEEE 802.1AE Clause 10.7.13"
    ::= { secyMgmtMIBObjects 5 }

secyRxSAEntry   OBJECT-TYPE
    SYNTAX      SecyRxSAEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry for one of the SAs used by one of the system's
                 SecY's to receive protected frames."
    INDEX    { secyIfInterfaceIndex, secyRxSCI, secyRxSA }
    ::= { secyRxSATable 1 }

SecyRxSAEntry ::= SEQUENCE {
    secyRxSA               SecyAN,
    secyRxSAState          INTEGER,
    secyRxSANextPN         Unsigned32,
    secyRxSASAKUnchanged   TruthValue,
    secyRxSACreatedTime    TimeStamp,
    secyRxSAStartedTime    TimeStamp,
    secyRxSAStoppedTime    TimeStamp,
    secyRxSANextXPN        Counter64,         -- 802.1AEcg
    secyRxSALowestXPN      Counter64,         -- 802.1AEcg
    secyRxSAKeyIdentifier  SnmpAdminString, -- 802.1AEcg
    secyRxSASSCI   Integer32 -- 802.1AEcg
}

secyRxSA        OBJECT-TYPE
    SYNTAX      SecyAN
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "The association number (AN) for this receive SA."
    REFERENCE   "IEEE 802.1AE Clause 10.7.13"
    ::= { secyRxSAEntry 1 }

secyRxSAState   OBJECT-TYPE
    SYNTAX      INTEGER {
                    inUse(1),
                    notInUse(2)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The current state for this receive SA."
    REFERENCE   "IEEE 802.1AE Clause 10.7.14"
    ::= { secyRxSAEntry 2 }

secyRxSANextPN    OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-write
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION
    "One more than the highest PN conveyed in the SecTAG of a frame
     received on this SA that has been successfully validated (if
     validateFrames has not been disabled). Deprecated: use
     secyRxSANextXPN for both 32-bit PN and 64-bit XPN PN values. If
```

```
        this object is implemented and an XPN Cipher Suite is used, it
        contains the lowest 32-bits of the XPN."
    REFERENCE   "IEEE 802.1AE Clause 10.6.5, 10.7.14, Figure 10-4"
    ::= { secyRxSAEntry 3 }

secyRxSASAKUnchanged    OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION "A reference to an SAK that is unchanged for the life
                 of the receiving SA."
    REFERENCE   "IEEE 802.1AE Clause 10.7.13"
    ::= { secyRxSAEntry 4 }

secyRxSACreatedTime    OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The system time when this receiving SA was created."
    REFERENCE   "IEEE 802.1AE Clause 10.7.14"
    ::= { secyRxSAEntry 5 }

secyRxSAStartedTime    OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The system time when this receiving SA last started
                 receiving MACsec frames."
    REFERENCE   "IEEE 802.1AE Clause 10.7.14"
    ::= { secyRxSAEntry 6 }

secyRxSAStoppedTime    OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The system time when this receiving SA last stopped
                 receiving MACsec frames."
    REFERENCE   "IEEE 802.1AE Clause 10.7.14"
    ::= { secyRxSAEntry 7 }

secyRxSANextXPN    OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "One more than the highest PN conveyed in the SecTAG of
                 successfully validates frames received on this SA."
    REFERENCE   "IEEE 802.1AE Clause 10.6.5, 10.7.14, Figure 10-4"
    ::= { secyRxSAEntry 8 }

secyRxSALowestXPN    OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The lowest acceptable packet number. A received frame
                 with a lower PN is  discarded if
                 secyIfReplayProtectEnable is enabled."
    REFERENCE   "IEEE 802.1AE Clause 10.6.2, 10.6.4, 10.6.5, 10.7.14,
        Figure 10-4"
    ::= { secyRxSAEntry 9 }

secyRxSAKeyIdentifier    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (1..32))
    MAX-ACCESS  read-only
    STATUS      current
```

```
        DESCRIPTION "The Key Identifier (KI) for the SAK for this SA."
        REFERENCE   "IEEE 802.1X, IEEE 802.1AE Clause 10.7.14"
        ::= { secyRxSAEntry 10 }

    secyRxSASSCI    OBJECT-TYPE
        SYNTAX      Integer32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The SSCI for this SA, 0 if an XPN Cipher Suite is not
                     being used."
        REFERENCE   "IEEE 802.1X, IEEE 802.1AE Clause 10.7.14"
        ::= { secyRxSAEntry 11 }

    --
    --  SecY Selectable Cipher Suites
    --

    secyCipherSuiteTable    OBJECT-TYPE
        SYNTAX      SEQUENCE OF SecyCipherSuiteEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
        "A table of the system's Cipher Suite capabilities, which can differ
         by Cipher Suite implementation, so there can be more than one entry
          with the same secyCipherSuiteId. The secyIfCipherTable lists
          available entries by SecY, avoiding the need for remote network
          management to  write objects or create rows in this table. Any
          configured values shall be stored in persistent memory and remain
          unchanged across a re-initialization of the management system."
        REFERENCE   "IEEE 802.1AE Clause 10.7.25"
        ::= { secyMgmtMIBObjects 6 }

    secyCipherSuiteEntry    OBJECT-TYPE
        SYNTAX      SecyCipherSuiteEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION "An entry for a Cipher Suite implementation."
        INDEX { secyCipherSuiteIndex }
        ::= { secyCipherSuiteTable 1 }

    SecyCipherSuiteEntry ::= SEQUENCE {
        secyCipherSuiteIndex                Unsigned32,
        secyCipherSuiteId                   OCTET STRING,
        secyCipherSuiteName                 SnmpAdminString,
        secyCipherSuiteCapability           BITS,
        secyCipherSuiteProtection           BITS,
        secyCipherSuiteProtectionOffset     INTEGER,
        secyCipherSuiteDataLengthChange     TruthValue,
        secyCipherSuiteICVLength            Unsigned32,
        secyCipherSuiteRowStatus            RowStatus
    }

    secyCipherSuiteIndex    OBJECT-TYPE
        SYNTAX      Unsigned32 (1..4294967295)
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION "The CipherSuiteTable entry index."
        ::= { secyCipherSuiteEntry 1 }

    secyCipherSuiteId    OBJECT-TYPE
        SYNTAX      OCTET STRING (SIZE (8))
        MAX-ACCESS  read-create
        STATUS      current
        DESCRIPTION "A unique 64-bit (EUI-64) identifier for the Cipher
```

```
                Suite."
    REFERENCE   "IEEE 802.1AE Clause 10.7.25, Table 14-1"
    ::= { secyCipherSuiteEntry 2 }

secyCipherSuiteName    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (1..128))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION "The Cipher Suite Name, 128 octets or fewer."
    REFERENCE   "IEEE 802.1AE Clause 10.7.25, Table 14-1"
    ::= { secyCipherSuiteEntry 3 }

secyCipherSuiteCapability    OBJECT-TYPE
    SYNTAX      BITS {
                    integrity(0),
                    confidentiality(1),
                    offsetConfidentiality(2)
                }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION "Cipher Suite implementation capability information.

                 integrity(0)             : integrity protection.
                 confidentiality(1)       : confidentiality protection.
                 offsetConfidentiality(2) : offset confidentiality
                                            protection."
    REFERENCE   "IEEE 802.1AE Clause 10.7.24, 10.7.25"
    ::= { secyCipherSuiteEntry 4 }

secyCipherSuiteProtection    OBJECT-TYPE
    SYNTAX      BITS {
                    integrity(0),
                    confidentiality(1),
                    offsetConfidentiality(2)
                }
    MAX-ACCESS  read-create
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION
    "The secyIfCipherSuite table should be used instead of this object
     to allow per SecY cipher Suite configuration.

     The options provided by this control are a subset of those
     defined by the object secyCipherSuiteCapability.
     If secyCipherSuiteCapability has the integrity bit on,the integrity
     bit can be turned on for this object.
     If secyCipherSuiteCapability has the integrity and confidentiality
     bits on, the confidentiality bit of this object can be turned on
     and the integrity bit must be on.
     If secyCipherSuiteCapability has the integrity and
     offsetConfidentiality bits on, the offsetConfidentiality bit can be
     turned on and the integrity bit must be on.

     integrity(0) : on or off the function of supporting integrity
                    protection for this cipher suite.

     confidentiality(1) : on or off the function of supporting
                    confidentiality for this cipher suite.

    offsetConfidentiality(2) : on or off the function of supporting
                    offset confidentiality for this cipher suite."
    REFERENCE   "IEEE 802.1AE Clause 10.7.25"
    DEFVAL { { integrity } }
    ::= { secyCipherSuiteEntry 5 }
```

```
secyCipherSuiteProtectionOffset    OBJECT-TYPE
    SYNTAX      Integer32 (0 | 30 | 50)
    UNITS       "bytes"
    MAX-ACCESS  read-create
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION
   "The confidentiality protection offset options of this cipher suite.
    Options should depend on the choice of secyCipherSuiteProtection.
    If the value of secyCipherSuiteProtection only turns on integrity
    bit, users can only choose 0 byte for this object.
    If the value of secyCipherSuiteProtection only turns on integrity
    and confidentiality bits, users can only choose 0 byte for this
    object.
    If the value of secyCipherSuiteProtection only turns on integrity
    and offsetConfidentiality bits, users can choose 30 or 50 bytes for
    this object.
    If the value of secyCipherSuiteProtection turns on integrity and
    confidentiality and offsetConfidentiality bits, users can choose 0
    or 30 or 50 bytes for this object."
    REFERENCE   "IEEE 802.1AE Clause 10.7.25, 10.7.26"
    DEFVAL { 0 }
    ::= { secyCipherSuiteEntry 6 }

secyCipherSuiteDataLengthChange    OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION "True if cipher suite changes the length of the data."
    REFERENCE   "IEEE 802.1AE Clause 10.7.25, Figure 9-1"
    ::= { secyCipherSuiteEntry 7 }

secyCipherSuiteICVLength    OBJECT-TYPE
    SYNTAX      Unsigned32 (8..16)
    UNITS       "octets"
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION "The length of the integrity check value (ICV) field."
    REFERENCE   "IEEE 802.1AE Clause 10.7.25, Figure 9-1"
    ::= { secyCipherSuiteEntry 8 }

secyCipherSuiteRowStatus    OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
    "The secyIfCipherTable (if implemented) avoids the need for
     network manager creation of entries in the secyCipherSuiteTable,
     and RowStatus should always be valid(1), with any per SecY
     unavailability indicated by an absence of a corresponding
     secyIfCipherTable entry or one with secyCipherSuiteAvailable
     false (the latter can indicate temporay unavailability)."
    REFERENCE   "IEEE 802.1AE Clause 10.7.25"
    ::= { secyCipherSuiteEntry 9 }

--
-- SecY Interface Ciphers Table : 802.1AEcg
--

secyIfCipherTable    OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyIfCipherEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "A table with an entry for the Cipher Suite capabilities
```

```
            implemented for each SecY in this system, providing per SecY
            control of Cipher Suite use.

            The configured value of writable objects in each table entry
            shall be stored in persistent memory and remain unchanged across
            a re-initialization of the system's management entity."
        REFERENCE   "IEEE 802.1AE Clause 10.7.26, Table 13-1"
        ::= { secyMgmtMIBObjects 7 }

    secyIfCipherEntry    OBJECT-TYPE
        SYNTAX      SecyIfCipherEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION "A table entry with Cipher Suite control for a SecY."
        INDEX   { secyIfInterfaceIndex, secyCipherSuiteIndex }
        ::= { secyIfCipherTable 1 }

    SecyIfCipherEntry ::= SEQUENCE {
        secyIfCipherImplemented         TruthValue,
        secyIfCipherEnableUse           TruthValue,
        secyIfCipherRqConfidentiality   TruthValue
    }

    secyIfCipherImplemented    OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "True if the Cipher Suite implementation can be used by
                     this SecY (if secIfCipherEnablUse is true)."
        REFERENCE   "IEEE 802.1AE Clause 10.7.26"
        DEFVAL { true }
        ::= { secyIfCipherEntry 1 }

    secyIfCipherEnableUse    OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION "Enables use of the Cipher Suite by this SecY."
        REFERENCE   "IEEE 802.1AE Clause 10.7.26"
        DEFVAL { true }
        ::= { secyIfCipherEntry 2 }

    secyIfCipherRqConfidentiality    OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION "True if confidentiality protection (without an offset)
                     is required if this Cipher Suite is used."
        REFERENCE   "IEEE 802.1AE Clause 10.7.26"
        DEFVAL { true }
        ::= { secyIfCipherEntry 3 }

    --
    -- SecY Interface Traffic Class Table : 802.1AEcg
    --

    secyIfTCTable   OBJECT-TYPE
        SYNTAX      SEQUENCE OF SecyIfTCEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
           "The Traffic Class Table for each SecY in this system.

            The configured value of writable objects in each table entry
```

```
        shall be stored in persistent memory and remain unchanged across
        a re-initialization of the system's management entity."
    REFERENCE   "IEEE 802.1AE Clause 10.5.1, 10.7.17, Table 13-1"
    ::= { secyMgmtMIBObjects 8 }

secyIfTCEntry   OBJECT-TYPE
    SYNTAX      SecyIfTCEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "A table entry providing Traffic Class selection for a
                 given SecY and User Priority."
    INDEX   { secyIfInterfaceIndex, secyIfTCUserPriority }
    ::= { secyIfTCTable 1 }

SecyIfTCEntry ::= SEQUENCE {
    secyIfTCUserPriority           Integer32,
    secyIfTCTrafficClass           Integer32
}

secyIfTCUserPriority    OBJECT-TYPE
    SYNTAX      Integer32 (0..7)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "One of the possible User Priority values for a frame."
    REFERENCE   "IEEE 802.1AE Clause 10.7.17"
    ::= { secyIfTCEntry 1 }

secyIfTCTrafficClass    OBJECT-TYPE
    SYNTAX      Integer32 (0..7)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "The Traffic Class for this SecY and User Priority, as
        transmitted in the four most significant bits of the Port
        Identifier component of the SCI of protected frames."
    REFERENCE   "IEEE 802.1AE Clause 10.7.17"
    DEFVAL { 0 }
    ::= { secyIfTCEntry 2 }

--
-- SecY Interface Access Priority Table : 802.1AEcg
--

secyIfAPTable   OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyIfAPEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "The Access Priority Table for each SecY in this system.

        The configured value of writable objects in each table entry
        shall be stored in persistent memory and remain unchanged across
        a re-initialization of the system's management entity."
    REFERENCE   "IEEE 802.1AE Clause 10.5.1, 10.7.17, Table 13-1"
    ::= { secyMgmtMIBObjects 9 }

secyIfAPEntry   OBJECT-TYPE
    SYNTAX      SecyIfAPEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "A table entry selecting the  Access Priority Code Point
                 for a given SecY and User Priority Code Point."
    INDEX   { secyIfInterfaceIndex, secyIfAPUserPCP }
    ::= { secyIfAPTable 1 }
```

```
SecyIfAPEntry ::= SEQUENCE {
    secyIfAPUserPCP             Integer32,
    secyIfAPAccessPCP           Integer32
}

secyIfAPUserPCP OBJECT-TYPE
    SYNTAX      Integer32 (0..15)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "A User Priority Code Point."
    REFERENCE   "IEEE 802.1AE Clause 10.5, 10.7.17"
    ::= { secyIfAPEntry 1 }

secyIfAPAccessPCP    OBJECT-TYPE
    SYNTAX      Integer32 (0..15)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION "The Access Priority Code Point for this SecY and User
                 PCP. Defaults to the User PCP value. "
    REFERENCE   "IEEE 802.1AE Clause 10.5, 10.7.17"
    ::= { secyIfAPEntry 2 }

--
-- TX SA Statistics : systems not supporting traffic class SCs
--

secyTxSAStatsTable    OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyTxSAStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION "A table of statistics for each transmit SA for each of
                 the system's SecYs."
    REFERENCE   "IEEE 802.1AE Clause 10.7.18, figure 10-4"
    ::= { secyStatsMIBObjects 1 }

secyTxSAStatsEntry    OBJECT-TYPE
    SYNTAX      SecyTxSAStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION
       "An entry with statistics for a transmit SA.  The AN that
        identifies an SA (for a given SC) and this corresponding entry
        can be reused. When creating the SA and before (re)using the
        entry, the SA counters are (re)set to 0. When the SA is stopped
        (secyTxSA notInuse) the counters will be stop incrementing.

        The secyTxSATable timestamps SA creation, start, and stop."
    AUGMENTS { secyTxSAEntry }
    ::= { secyTxSAStatsTable 1 }

SecyTxSAStatsEntry ::= SEQUENCE {
    secyTxSAStatsProtectedPkts    Counter32,
    secyTxSAStatsEncryptedPkts    Counter32
}

secyTxSAStatsProtectedPkts    OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION "The number of integrity protected but not encrypted
                 packets for this transmit SA. Zero if
                 secyTxSAConfidentiality is True, and one less than
```

```
                secyTxSANextPN otherwise."
    REFERENCE   "IEEE 802.1AE Clause 10.7.18, figure 10-4"
    ::= { secyTxSAStatsEntry 1 }

secyTxSAStatsEncryptedPkts    OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION "The number of integrity protected and encrypted packets
                 for this transmit SA. Zero if secyTxSAConfidentiality
                 is False, and one less than secyTxSANextPN otherwise."
    REFERENCE   "IEEE 802.1AE Clause 10.7.18, Figure 10-4"
    ::= { secyTxSAStatsEntry 2 }


--
-- TX SC Statistics : systems not supporting traffic class SCs
--

secyTxSCStatsTable    OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyTxSCStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "A table of statistics for each SecY's transmit SC."
    REFERENCE   "IEEE 802.1AE Clause 10.7.18, 10.7.19, Figure 10-3"
    ::= { secyStatsMIBObjects 2 }

secyTxSCStatsEntry    OBJECT-TYPE
    SYNTAX      SecyTxSCStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "An entry containing counts for a transmit SC. SA counters are
        reset when the SA's AN is reused, so these SC counts are
        a summation for all current and prior SAs belonging to the SC."
    AUGMENTS { secyTxSCEntry }
    ::= { secyTxSCStatsTable 1 }

SecyTxSCStatsEntry ::= SEQUENCE {
    secyTxSCStatsProtectedPkts      Counter64,
    secyTxSCStatsEncryptedPkts      Counter64,
    secyTxSCStatsOctetsProtected    Counter64, -- deprecated
    secyTxSCStatsOctetsEncrypted    Counter64  -- deprecated
}

secyTxSCStatsProtectedPkts    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The number of integrity protected but not encrypted
                 packets for this transmit SC."
    REFERENCE   "IEEE 802.1AE Clause 10.7.18, Figure 10-3"
    ::= { secyTxSCStatsEntry 1 }

secyTxSCStatsEncryptedPkts    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The number of integrity protected and encrypted packets
                 for this transmit SC."
    REFERENCE   "IEEE 802.1AE Clause 10.7.18, Figure 10-3"
```

```
    ::= { secyTxSCStatsEntry 4 }

secyTxSCStatsOctetsProtected    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Octets"
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION "The number of plain text octets that are integrity
                 protected but not encrypted for this transmit SC."
    REFERENCE   "IEEE 802.1AE Clause 10.7.19, Figure 10-3"
    ::= { secyTxSCStatsEntry 10 }

secyTxSCStatsOctetsEncrypted    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Octets"
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION
        "The number of plain text octets that are integrity protected
         and encrypted on the transmit SC."
    REFERENCE   "IEEE 802.1AE Clause 10.7.19, Figure 10-3"
    ::= { secyTxSCStatsEntry 11 }
--
-- Traffic Class capable transmit SC Statistics : 802.1AEcg
--

secyTSCStatsTable    OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyTSCStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of statistics for each SecY's transmit SCs."
    REFERENCE   "IEEE 802.1AE Clause 10.7.18, 10.7.19, Figure 10-3"
    ::= { secyStatsMIBObjects 12 }

secyTSCStatsEntry    OBJECT-TYPE
    SYNTAX      SecyTSCStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A entry containing counts for a transmit SC, since SA counters
         are reset when the SA's AN  is reused these are a summation for
         all current and prior SAs belonging to the SC."
    AUGMENTS { secyTSCEntry }
    ::= { secyTSCStatsTable 1 }

SecyTSCStatsEntry ::= SEQUENCE {
    secyTSCStatsProtectedPkts      Counter64,
    secyTSCStatsEncryptedPkts      Counter64
}

secyTSCStatsProtectedPkts    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of integrity protected but not encrypted packets
         for this transmit SC."
    REFERENCE   "IEEE 802.1AE Clause 10.7.18, Figure 10-3"
    ::= { secyTSCStatsEntry 1 }

secyTSCStatsEncryptedPkts    OBJECT-TYPE
    SYNTAX      Counter64
```

```
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of integrity protected and encrypted packets for
         this transmit SC."
    REFERENCE   "IEEE 802.1AE Clause 10.7.18, Figure 10-3"
    ::= { secyTSCStatsEntry 2 }


--
-- RX SA Statistics Information
--

secyRxSAStatsTable    OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyRxSAStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      deprecated
    DESCRIPTION
        "A table that contains the statistics objects for each
         receiving SA in the MAC security entity."
    REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
    ::= { secyStatsMIBObjects 3 }

secyRxSAStatsEntry    OBJECT-TYPE
    SYNTAX      SecyRxSAStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION
       "An entry with statistics for a receive SA.  The AN that
        identifies an SA (for a given SC) and this corresponding entry
        can be reused. When creating the SA and before (re)using the
        entry, the SA counters are (re)set to 0. When the SA is stopped
        (secyRxSA notInuse) the counters will be stop incrementing.

        The secyRxSATable timestamps SA creation, start, and stop."
    AUGMENTS { secyRxSAEntry }
    ::= { secyRxSAStatsTable 1 }

SecyRxSAStatsEntry ::= SEQUENCE {
    secyRxSAStatsUnusedSAPkts    Counter32, -- deprecated
    secyRxSAStatsNoUsingSAPkts   Counter32, -- deprecated
    secyRxSAStatsNotValidPkts    Counter32, -- deprecated
    secyRxSAStatsInvalidPkts     Counter32, -- deprecated
    secyRxSAStatsOKPkts          Counter32  -- deprecated
}

secyRxSAStatsUnusedSAPkts    OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "For this SA which is not currently in use, the number of
         received, unencrypted, packets with secyValidateFrames
         not in the strict mode."
    REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
    ::= { secyRxSAStatsEntry 1 }

secyRxSAStatsNoUsingSAPkts   OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      deprecated
```

```
        DESCRIPTION
            "For this SA which is not currently in use, the number of
             received packets that have been discarded, and have
             either the packets encrypted or secyValidateFrames set to
             strict mode."
        REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
        ::= { secyRxSAStatsEntry 4 }

    secyRxSAStatsNotValidPkts     OBJECT-TYPE
        SYNTAX      Counter32
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      deprecated
        DESCRIPTION
            "For this SA, the number discarded packets with the
             condition that the packets are not valid and one of the
             following conditions are true: either secyValidateFrames in
             strict mode or the packets encrypted."
        REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
        ::= { secyRxSAStatsEntry 13 }

    secyRxSAStatsInvalidPkts     OBJECT-TYPE
        SYNTAX      Counter32
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      deprecated
        DESCRIPTION
            "For this SA, the number of packets with the condition
             that the packets are not valid and secyValidateFrames is in
             check mode."
        REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
        ::= { secyRxSAStatsEntry 16 }

    secyRxSAStatsOKPkts          OBJECT-TYPE
        SYNTAX      Counter32
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      deprecated
        DESCRIPTION
            "For this SA, the number of validated packets."
        REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
        ::= { secyRxSAStatsEntry 25 }

    --
    -- RX SC Statistics Information
    --

    secyRxSCStatsTable    OBJECT-TYPE
        SYNTAX      SEQUENCE OF SecyRxSCStatsEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION "A table of statistics for each receive SC for each of
                     the system's SecYs."
        REFERENCE   "IEEE 802.1AE Clause 10.7.9, 10.7.10, Figure 10-4"
        ::= { secyStatsMIBObjects 4 }

    secyRxSCStatsEntry    OBJECT-TYPE
        SYNTAX      SecyRxSCStatsEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
           "An entry containing counts for a receive SC. SA counters are
            reset when the SA's AN  is reused, so these SC counts are a
            summation for all current and prior SAs belonging to the SC."
```

```
    AUGMENTS { secyRxSCEntry }
    ::= { secyRxSCStatsTable 1 }

SecyRxSCStatsEntry ::= SEQUENCE {
    secyRxSCStatsUnusedSAPkts          Counter64, -- deprecated
    secyRxSCStatsNoUsingSAPkts         Counter64, -- deprecated
    secyRxSCStatsLatePkts              Counter64,
    secyRxSCStatsNotValidPkts          Counter64,
    secyRxSCStatsInvalidPkts           Counter64,
    secyRxSCStatsDelayedPkts           Counter64,
    secyRxSCStatsUncheckedPkts         Counter64,
    secyRxSCStatsOKPkts                Counter64,
    secyRxSCStatsOctetsValidated       Counter64, -- deprecated
    secyRxSCStatsOctetsDecrypted       Counter64  -- deprecated
}

secyRxSCStatsUnusedSAPkts    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION "The sum of secyRxSAStatsUnusedSAPkts counts for all
                 current and prior SAs belonging to this SC."
    REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
    ::= { secyRxSCStatsEntry 1 }

secyRxSCStatsNoUsingSAPkts    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION "The sum of secyRxSAStatsNoUsingSAPkts counts for all
                 current and prior SAs belonging to this SC."
    REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
    ::= { secyRxSCStatsEntry 2 }

secyRxSCStatsLatePkts        OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of packets discarded, for this SC, because the
         the received PN was lower than the lowest acceptable PN
         (secyRxSALowestXPN) and secyIfReplayProtectEnable was true."
    REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
    ::= { secyRxSCStatsEntry 3 }

secyRxSCStatsNotValidPkts     OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "The number of packets discarded, for this SC, because validation
        failed and secyIfvalidateFrames was 'strict' or the data was
        encrypted (so the original frame could not be recovered)."
    REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
    ::= { secyRxSCStatsEntry 4 }

secyRxSCStatsInvalidPkts     OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
```

```
        STATUS      current
        DESCRIPTION
           "The number of packets, for this SC, that failed validation but
           could be received because secyIfvalidateFrames  was 'check' and
           the  data was not encrypted (so the original frame could be
           recovered)."
        REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
        ::= { secyRxSCStatsEntry 5 }

    secyRxSCStatsDelayedPkts     OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
           "The number of received packets, for this SC, with PN lower
            than the lowest acceptable PN (secyRxSALowestXPN) and
            secyIfReplayProtectEnable false."
        REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
        ::= { secyRxSCStatsEntry 6 }

    secyRxSCStatsUncheckedPkts   OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The number of packets received for this SC,  while
                     secyValidateFrames was 'disabled'."
        REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
        ::= { secyRxSCStatsEntry 7 }

    secyRxSCStatsOKPkts          OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The number of packets received for this SC
                     successfully validated and within the replay window."
        REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
        ::= { secyRxSCStatsEntry 8 }

    secyRxSCStatsOctetsValidated     OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Octets"
        MAX-ACCESS  read-only
        STATUS      deprecated -- 802.1AEcg
        DESCRIPTION "The number of plaintext octets recovered from packets
                     that were integrity protected but not encrypted."
        REFERENCE "Deprecated, the secyIsStatsTable has per SecY counts
                   for cryptographic performance management."
        ::= { secyRxSCStatsEntry 9 }

    secyRxSCStatsOctetsDecrypted    OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Octets"
        MAX-ACCESS  read-only
        STATUS      deprecated -- 802.1AEcg
        DESCRIPTION "The number of plaintext octets recovered from packets
                     that were integrity protected and encrypted."
        REFERENCE  "Deprecated, the secyIsStatsTable has per SecY counts
                    for cryptographic performance management."
        ::= { secyRxSCStatsEntry 10 }

    --
```

```
-- SecY statistics table
--

secyStatsTable    OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "A table of statistics for each of the system's SecYs."
    REFERENCE   "IEEE 802.1AE Clause 10.7.9, 10.7.18, Figure 10-3, 10.5"
    ::= { secyStatsMIBObjects 5 }

secyStatsEntry    OBJECT-TYPE
    SYNTAX      SecyStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing counts for a SecY."
    AUGMENTS { secyIfEntry }
    ::= { secyStatsTable 1 }

SecyStatsEntry ::= SEQUENCE {
    secyStatsTxUntaggedPkts     Counter64,
    secyStatsTxTooLongPkts      Counter64,
    secyStatsRxUntaggedPkts     Counter64,
    secyStatsRxNoTagPkts        Counter64,
    secyStatsRxBadTagPkts       Counter64,
    secyStatsRxUnknownSCIPkts   Counter64, -- deprecated
    secyStatsRxNoSCIPkts        Counter64, -- deprecated
    secyStatsRxOverrunPkts      Counter64,
    secyStatsRxNoSAPkts         Counter64, -- 802.1AEcg
    secyStatsRxNoSAErrorPkts    Counter64, -- 802.1AEcg
    secyStatsTxOctetsProtected  Counter64, -- 802.1AEcg
    secyStatsTxOctetsEncrypted  Counter64, -- 802.1AEcg
    secyStatsRxOctetsValidated  Counter64, -- 802.1AEcg
    secyStatsRxOctetsDecrypted  Counter64  -- 802.1AEcg
}

secyStatsTxUntaggedPkts    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The number of packets transmitted without a SecTAG
                 because secyProtectFramesEnable is configured false."
    REFERENCE   "IEEE 802.1AE Clause 10.7.18, Figure 10-3"
    ::= { secyStatsEntry 1 }

secyStatsTxTooLongPkts    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The number of transmit packets discarded because their
                 length is greater than the ifMtu of the Common Port."
    REFERENCE   "IEEE 802.1AE Clause 10.7.18, Figure 10-3"
    ::= { secyStatsEntry 2 }

secyStatsRxUntaggedPkts    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The number of packets without the MACsec tag (SecTAG)
                 received while secyValidateFrames was not 'strict'."
```

```
    REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
    ::= { secyStatsEntry 3 }

secyStatsRxNoTagPkts       OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The number of received packets  without a SecTAG
                 discarded because secyValidateFrames was 'strict'."
    REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
    ::= { secyStatsEntry 4 }

secyStatsRxBadTagPkts      OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The number of received packets discarded with an
                 invalid SecTAG, zero value PN, or invalid ICV."
    REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
    ::= { secyStatsEntry 5 }

secyStatsRxUnknownSCIPkts  OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION "The number of received packets with an unknown SCI."
    REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
    ::= { secyStatsEntry 6 }

secyStatsRxNoSCIPkts       OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION "The number of discarded packets with an unknown SCI."
    REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
    ::= { secyStatsEntry 7 }

secyStatsRxOverrunPkts         OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The number of packets discarded because they exceeded
                 cryptographic performance capabilities."
    REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
    ::= { secyStatsEntry 8 }

secyStatsRxNoSAPkts       OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The number of received packets with an unknown SCI
                 or for an unused SA."
    REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
    ::= { secyStatsEntry 9 }

secyStatsRxNoSAErrorPkts       OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
```

```
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The number of packets discarded because the received
                     SCI is unknown or the SA is not in use."
        REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
        ::= { secyStatsEntry 10 }

    secyStatsTxOctetsProtected       OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Octets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The number of plain text octets integrity protected
                     but not encrypted in transmitted frames."
        REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
        ::= { secyStatsEntry 11 }

    secyStatsTxOctetsEncrypted       OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Octets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The number of plain text octets integrity protected
                     and encrypted in transmitted frames."
        REFERENCE   "IEEE 802.1AE Clause 10.7.9, Figure 10-4"
        ::= { secyStatsEntry 12 }

    secyStatsRxOctetsValidated       OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Octets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The number of plaintext octets recovered from packets
                     that were integrity protected but not encrypted."
        REFERENCE   "IEEE 802.1AE Clause 10.6.3, Figure 10-3"
        ::= { secyStatsEntry 13 }

    secyStatsRxOctetsDecrypted       OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Octets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION "The number of plaintext octets recovered from packets
                     that were integrity protected and encrypted."
        REFERENCE   "IEEE 802.1AE Clause 10.6.3, Figure 10-3"
        ::= { secyStatsEntry 14 }
    --
    -- Conformance
    --

    secyMIBCompliances  OBJECT IDENTIFIER ::= { secyMIBConformance 1 }

    secyMIBGroups  OBJECT IDENTIFIER ::= { secyMIBConformance 2 }

    -- Compliance

    secyMIBTcCompliance MODULE-COMPLIANCE
        STATUS current -- 802.1AEcg
        DESCRIPTION
        "The compliance statement for an IEEE8021-SECY-MIB supporting
         traffic class transmit SCs, added by IEEE 802.1AEcg."
        MODULE IF-MIB
            MANDATORY-GROUPS {
                ifCounterDiscontinuityGroup
```

```
            }
        MODULE  -- this module
            MANDATORY-GROUPS {
                secyIfGroup,
                secyIfCipherGroup,
                secyIfTCGroup,
                secyIfAPGroup,
                secyTSCGroup,
                secyTSAGroup,
                secyRSCGroup,
                secyRSAGroup,
                secyCipherInfoGroup,
                secyCipherStatsGroup,
                secyTSCStatsGroup,
                secyRSCStatsGroup,
                secyIfStatsGroup
            }
            OBJECT secyIfCurrentCipherSuite
                MIN-ACCESS    read-only
                DESCRIPTION "should be read-only, use the secyIfCipherTable
                             to control ciper suite use."
            OBJECT    secyCipherSuiteId
                MIN-ACCESS    read-only
                DESCRIPTION "read-create not required, may be read-only."
            OBJECT    secyCipherSuiteName
                MIN-ACCESS    read-only
                DESCRIPTION "read-create not required, should be read-only."
            OBJECT    secyCipherSuiteCapability
                MIN-ACCESS    read-only
                DESCRIPTION "read-create not required, should be read-only."
            OBJECT    secyCipherSuiteDataLengthChange
                MIN-ACCESS    read-only
                DESCRIPTION "read-create not required, should be read-only."
            OBJECT    secyCipherSuiteICVLength
                MIN-ACCESS    read-only
                DESCRIPTION "read-create not required, should be read-only."
        ::= { secyMIBCompliances 2 }

    secyMIBCompliance MODULE-COMPLIANCE
        STATUS deprecated -- 802.1AEcg
        DESCRIPTION
        "The compliance statement for the IEEE8021-SECY-MIB as specified in
         IEEE Std 802.1AE-2006."
        MODULE  -- this module
            MANDATORY-GROUPS {
                secyIfCtrlGroup,
                secyTxSCGroup,
                secyTxSAGroup,
                secyRxSCGroup,
                secyRxSAGroup,
                secyCipherSuiteGroup,
                secyTxSAStatsGroup,
                secyTxSCStatsGroup,
                secyRxSAStatsGroup,
                secyRxSCStatsGroup,
                secyStatsGroup
            }
            OBJECT secyIfCurrentCipherSuite
                MIN-ACCESS    read-only
                DESCRIPTION "write access not required, may be read-only."
            OBJECT    secyCipherSuiteId
                MIN-ACCESS    read-only
                DESCRIPTION "read-create not required, may be read-only."
            OBJECT    secyCipherSuiteName
```

```
            MIN-ACCESS    read-only
            DESCRIPTION "read-create not required, may be read-only."
        OBJECT    secyCipherSuiteCapability
            MIN-ACCESS    read-only
            DESCRIPTION "read-create not required, may be read-only."
        OBJECT    secyCipherSuiteProtection
            MIN-ACCESS    read-only
            DESCRIPTION "read-create not required, may be read-only."
        OBJECT    secyCipherSuiteProtectionOffset
            MIN-ACCESS    read-only
            DESCRIPTION "read-create not required, may be read-only."
        OBJECT    secyCipherSuiteDataLengthChange
            MIN-ACCESS    read-only
            DESCRIPTION "read-create not required, may be read-only."
        OBJECT    secyCipherSuiteICVLength
            MIN-ACCESS    read-only
            DESCRIPTION "read-create not required, may be read-only."
        OBJECT    secyCipherSuiteRowStatus
            MIN-ACCESS    read-only
            DESCRIPTION "read-create not required, may be read-only."
    ::= { secyMIBCompliances 1 }
--
-- Units of Conformance
-- Controlled Port service management MIB Groups

secyIfGroup    OBJECT-GROUP
    OBJECTS {
        secyIfMaxPeerSCs,
        secyIfRxMaxKeys,
        secyIfTxMaxKeys,
        secyIfProtectFramesEnable,
        secyIfValidateFrames,
        secyIfReplayProtectEnable,
        secyIfReplayProtectWindow,
        secyIfCurrentCipherSuite,
        secyIfAdminPt2PtMAC,
        secyIfOperPt2PtMAC,
        secyIfIncludeSCIEnable,
        secyIfUseESEnable,
        secyIfUseSCBEnable,
        secyIfSCI,                  -- 802.1AEcg
        secyIfIncludingSCI,         -- 802.1AEcg
        secyIfMaxTSCs               -- 802.1AEcg
    }
    STATUS      current --- 802.1AEcg, updates secyIfCtrlGroup
    DESCRIPTION "SecY service management (secyIfTable objects) for
                 systems supporting traffic class SCs."
    ::= { secyMIBGroups 12 }

secyIfCtrlGroup    OBJECT-GROUP
    OBJECTS {
        secyIfMaxPeerSCs,
        secyIfRxMaxKeys,
        secyIfTxMaxKeys,
        secyIfProtectFramesEnable,
        secyIfValidateFrames,
        secyIfReplayProtectEnable,
        secyIfReplayProtectWindow,
        secyIfCurrentCipherSuite,
        secyIfAdminPt2PtMAC,
        secyIfOperPt2PtMAC,
        secyIfIncludeSCIEnable,
        secyIfUseESEnable,
        secyIfUseSCBEnable
```

```
    }
    STATUS      deprecated
    DESCRIPTION "SecY service management (secyIfTable) objects."
    ::= { secyMIBGroups 1 }

secyIfTCGroup    OBJECT-GROUP
    OBJECTS {
        secyIfTCTrafficClass
    }
    STATUS      current --- 802.1AEcg
    DESCRIPTION "Traffic class control (secyIfTCTable)."
    ::= { secyMIBGroups 14 }

secyIfAPGroup    OBJECT-GROUP
    OBJECTS {
        secyIfAPAccessPCP
    }
    STATUS      current --- 802.1AEcg
    DESCRIPTION "Access Priority Code Point control (secyIfAPTable)."
    ::= { secyMIBGroups 15 }

-- Transmit SC and SA MIB Groups

secyTSCGroup    OBJECT-GROUP
    OBJECTS {
        secyTSCState,
        secyTSCEncodingSA,
        secyTSCCreatedTime,
        secyTSCStartedTime,
        secyTSCStoppedTime
    }
    STATUS      current --- 802.1AEcg, updates secyTxSCGroup
    DESCRIPTION "Transmit SC management (secyTSCTable objects) for
                 systems supporting traffic class SCs."
    ::= { secyMIBGroups 16 }

secyTxSCGroup    OBJECT-GROUP
    OBJECTS {
        secyTxSCI,
        secyTxSCState,
        secyTxSCEncodingSA,
        secyTxSCEnciphieringSA,
        secyTxSCCreatedTime,
        secyTxSCStartedTime,
        secyTxSCStoppedTime
    }
    STATUS      deprecated
    DESCRIPTION "Transmit SC management objects (for systems without
                 traffic class SC capabilities)."
    ::= { secyMIBGroups 2 }

secyTSAGroup    OBJECT-GROUP
    OBJECTS {
        secyTSAState,
        secyTSANextXPN,
        secyTSAConfidentiality,
        secyTSAKeyIdentifier,
        secyTSASSCI,
        secyTSACreatedTime,
        secyTSAStartedTime,
        secyTSAStoppedTime
    }
    STATUS      current --- 802.1AEcg, updates secyTxSAGroup
    DESCRIPTION "Transmit SA management (secyTSATable objects) for
```

```
                systems supporting traffic class SCs."
    ::= { secyMIBGroups 17 }

secyTxSAGroup    OBJECT-GROUP
    OBJECTS {
        secyTxSAState,
        secyTxSANextPN,
        secyTxSAConfidentiality,
        secyTxSASAKUnchanged,
        secyTxSACreatedTime,
        secyTxSAStartedTime,
        secyTxSAStoppedTime
    }
    STATUS      deprecated
    DESCRIPTION "Transmit SA management objects (for systems without
                 traffic class SC capabilities)."
    ::= { secyMIBGroups 3 }

-- Receive SC and SA MIB Groups

secyRSCGroup    OBJECT-GROUP
    OBJECTS {
        secyRxSCState,
        secyRxSCCreatedTime,
        secyRxSCStartedTime,
        secyRxSCStoppedTime
    }
    STATUS      current --- 802.1AEcg, updates secyRxSCGroup
    DESCRIPTION "Receive SC management (secyRxSCTable objects)."
    ::= { secyMIBGroups 18 }

secyRxSCGroup    OBJECT-GROUP
    OBJECTS {
        secyRxSCState,
        secyRxSCCurrentSA,
        secyRxSCCreatedTime,
        secyRxSCStartedTime,
        secyRxSCStoppedTime
    }
    STATUS      deprecated
    DESCRIPTION "Receive SC management objects."
    ::= { secyMIBGroups 4 }

secyRSAGroup    OBJECT-GROUP
    OBJECTS {
        secyRxSAState,
        secyRxSANextXPN,
        secyRxSALowestXPN,
        secyRxSAKeyIdentifier,
        secyRxSASSCI,
        secyRxSACreatedTime,
        secyRxSAStartedTime,
        secyRxSAStoppedTime
    }
    STATUS      current --- 802.1AEcg, updates secyRxSAGroup
    DESCRIPTION "Receive SA (secyRxSATable objects)."
    ::= { secyMIBGroups 19 }

secyRxSAGroup    OBJECT-GROUP
    OBJECTS {
        secyRxSAState,
        secyRxSANextPN,
        secyRxSASAKUnchanged,
        secyRxSACreatedTime,
```

```
            secyRxSAStartedTime,
            secyRxSAStoppedTime
        }
        STATUS      deprecated
        DESCRIPTION "Receive SA management objects."
        ::= { secyMIBGroups 5 }

    -- Cipher information, use, and statistics MIB Groups

    secyCipherInfoGroup    OBJECT-GROUP
        OBJECTS {
            secyCipherSuiteId,
            secyCipherSuiteName,
            secyCipherSuiteCapability,
            secyCipherSuiteDataLengthChange,
            secyCipherSuiteICVLength
        }
        STATUS      current --- 802.1AEcg, updates secyCipherSuiteGroup
        DESCRIPTION "Cipher Suite implementation information
                     (secyCipherSuiteTable objects)."
        ::= { secyMIBGroups 21 }

    secyCipherSuiteGroup    OBJECT-GROUP
        OBJECTS {
            secyCipherSuiteId,
            secyCipherSuiteName,
            secyCipherSuiteCapability,
            secyCipherSuiteProtection,
            secyCipherSuiteProtectionOffset,
            secyCipherSuiteDataLengthChange,
            secyCipherSuiteICVLength,
            secyCipherSuiteRowStatus
        }
        STATUS      deprecated
        DESCRIPTION "Cipher Suite information objects."
        ::= { secyMIBGroups 6 }

    secyIfCipherGroup    OBJECT-GROUP
        OBJECTS {
            secyIfCipherImplemented,
            secyIfCipherEnableUse,
            secyIfCipherRqConfidentiality
        }
        STATUS      current --- 802.1AEcg
        DESCRIPTION "Cipher Suite use control (secyIfCipherTable  objects)."
        ::= { secyMIBGroups 13 }

    secyCipherStatsGroup    OBJECT-GROUP
        OBJECTS {
            secyStatsTxOctetsProtected,
            secyStatsTxOctetsEncrypted,
            secyStatsRxOctetsValidated,
            secyStatsRxOctetsDecrypted
        }
        STATUS      current --- 802.1AEcg
        DESCRIPTION
            "Cipher Suite performance statistics (from secyStatsTable)."
        ::= { secyMIBGroups 24 }

    -- Transmit and Receive SA and SC statistics MIB Groups

    secyTxSAStatsGroup    OBJECT-GROUP
        OBJECTS {
            secyTxSAStatsProtectedPkts,
```

```
            secyTxSAStatsEncryptedPkts
        }
        STATUS      deprecated
        DESCRIPTION "Transmit SA statistics objects."
        ::= { secyMIBGroups 7 }

    secyRxSAStatsGroup    OBJECT-GROUP
        OBJECTS {
            secyRxSAStatsUnusedSAPkts,
            secyRxSAStatsNoUsingSAPkts,
            secyRxSAStatsNotValidPkts,
            secyRxSAStatsInvalidPkts,
            secyRxSAStatsOKPkts
        }
        STATUS      deprecated
        DESCRIPTION "Receive SA statistics objects."
        ::= { secyMIBGroups 8 }

    secyTSCStatsGroup    OBJECT-GROUP
        OBJECTS {
            secyTSCStatsProtectedPkts,
            secyTSCStatsEncryptedPkts
        }
        STATUS      current --- 802.1AEcg, updates secyTxSCStatsGroup
        DESCRIPTION "Transmit SC statistics (secyTSCStatsTable objects)."
        ::= { secyMIBGroups 22 }

    secyTxSCStatsGroup    OBJECT-GROUP
        OBJECTS {
            secyTxSCStatsProtectedPkts,
            secyTxSCStatsEncryptedPkts,
            secyTxSCStatsOctetsProtected,
            secyTxSCStatsOctetsEncrypted
        }
        STATUS      deprecated
        DESCRIPTION "Transmit SC statistics objects."
        ::= { secyMIBGroups 9 }

    secyRSCStatsGroup    OBJECT-GROUP
        OBJECTS {
            secyRxSCStatsLatePkts,
            secyRxSCStatsNotValidPkts,
            secyRxSCStatsInvalidPkts,
            secyRxSCStatsDelayedPkts,
            secyRxSCStatsUncheckedPkts,
            secyRxSCStatsOKPkts
        }
        STATUS      current --- 802.1AEcg, updates secyRxSCStatsGroup
        DESCRIPTION "Receive SC statistics (secyRxSCStatsTable objects)."
        ::= { secyMIBGroups 23 }

    secyRxSCStatsGroup    OBJECT-GROUP
        OBJECTS {
            secyRxSCStatsUnusedSAPkts,
            secyRxSCStatsNoUsingSAPkts,
            secyRxSCStatsLatePkts,
            secyRxSCStatsNotValidPkts,
            secyRxSCStatsInvalidPkts,
            secyRxSCStatsDelayedPkts,
            secyRxSCStatsUncheckedPkts,
            secyRxSCStatsOKPkts,
            secyRxSCStatsOctetsValidated,
            secyRxSCStatsOctetsDecrypted
        }
```

```
        STATUS      deprecated
        DESCRIPTION
            "Receive SC statistics objects."
        ::= { secyMIBGroups 10 }

    -- Controlled Port service statistics MIB Groups

    secyIfStatsGroup    OBJECT-GROUP
        OBJECTS {
            secyStatsTxUntaggedPkts,
            secyStatsTxTooLongPkts,
            secyStatsRxUntaggedPkts,
            secyStatsRxNoTagPkts,
            secyStatsRxBadTagPkts,
            secyStatsRxNoSAPkts,
            secyStatsRxNoSAErrorPkts,
            secyStatsRxOverrunPkts
        }
        STATUS      current --- 802.1AEcg, updates secyRxSCStatsGroup
        DESCRIPTION
            "SecY statistics (secyStatsTable objects)."
        ::= { secyMIBGroups 20 }

    secyStatsGroup    OBJECT-GROUP
        OBJECTS {
            secyStatsTxUntaggedPkts,
            secyStatsTxTooLongPkts,
            secyStatsRxUntaggedPkts,
            secyStatsRxNoTagPkts,
            secyStatsRxBadTagPkts,
            secyStatsRxUnknownSCIPkts,
            secyStatsRxNoSCIPkts,
            secyStatsRxOverrunPkts
        }
        STATUS      deprecated
        DESCRIPTION
            "SecY statistics objects."
        ::= { secyMIBGroups 11 }

    END
```

Delete subclause 13.7.

14. Encoding of MACsec protocol data units

14.5 Default Cipher Suite (GCM–AES–128)

Insert the following NOTE after the first paragraph of 14.5, renumbering subsequent NOTEs.

NOTE 1—[B7], [B10] and [B12] provide additional information about GCM, its security properties and use.

Change the last paragraph of 14.5 as follows:

When the Default Cipher Suite is used for Confidentiality Protection with a confidentiality offset

- *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG and the first confidentialityOffset (10.7.24) octets of the User Data (or all the octets of the User Data if that comprises fewer than confidentialityOffset octets) concatenated in that order.
- *P* is the remaining octets (if any) of the User Data.
- The Secure Data is the first confidentialityOffset octets of the User Data concatenated with *C,* in that order (or all the octets of the User Data if that comprises fewer than confidentialityOffset octets).

NOTE 3— IEEE Std 802.1AE-2006 specified the confidentiality offset option to facilitate early MACsec deployment on systems that needed to examine the initial octets of IP version 4 or version 6 frames to decide where to store received frames, before decrypting the frame. The XPN Cipher Suites standardized in IEEE Std 802.1AEbw-2013 do not support confidentiality offsets.

14.6 GCM-AES-256

Change the last paragraph of 14.6 as follows, renumbering the preceding NOTE as required:

When this Cipher Suite is used for Confidentiality Protection with a confidentiality offset

- *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG and the first confidentialityOffset (10.7.24) octets of the User Data (or all the octets of the User Data if that comprises fewer than confidentialityOffset octets) concatenated in that order.
- *P* is the remaining octets (if any) of the User Data.
- The Secure Data is the first confidentialityOffset octets of the User Data concatenated with *C,* in that order (or all the octets of the User Data if that comprises fewer than confidentialityOffset octets).

NOTE 2— IEEE Std 802.1AE-2006 specified the confidentiality offset option to facilitate early MACsec deployment on systems that needed to examine the initial octets of IP version 4 or version 6 frames to decide where to store received frames, before decrypting the frame. The XPN Cipher Suites standardized in IEEE Std 802.1AEbw-2013 do not support confidentiality offsets.

Insert the following new Clause 15 after the existing Clause 14.

15. Ethernet Data Encryption devices

An Ethernet Data Encryption device (EDE) is a frame forwarding device with two physical ports that uses IEEE Std 802.1Q, IEEE Std 802.1AE, and IEEE Std 802.1X to provide integrity and confidentiality for frames forwarded on network hops open to attack. One port (red side) receives and transmits unprotected frames, while frames transmitted and received on the other (black side) are protected by MACsec.

This clause describes and specifies:

a) The common characteristics of EDEs—the rationale for identifying some of the many possible MACsec capable bridging systems as EDEs—and provides an EDE taxonomy (15.1).
b) How connectivity between adjacent bridges in a customer bridged network or a Provider Bridged Network (PBN) can be secured by an EDE-M (15.2) comprising a two-port VLAN-unaware MAC Bridge with a MAC Security Entity (SecY) supporting one port.
c) Requirements for securing connectivity across a PBN (15.3).
d) How connectivity across a PBN can be secured by an EDE-M (15.4), or by an EDE-CS (15.5), EDE-CC (15.6), or EDE-SS (15.7)—each comprising two VLAN bridge components, and each using MACsec to preserve frame data integrity, data origin authenticity, and confidentiality, while allowing the provider to use the frame's VLAN tag to perform service selection and to convey priority code point (PCP) and drop-eligible (DEI) information.
e) Interoperability between EDEs and other MACsec-capable bridging systems (15.8).
f) Considerations applicable to UNI access and CFM use when EDEs are used (15.9).

An understanding of architectural concepts common to this and other IEEE 802.1 standards is essential to understanding this standard's specification of EDEs. The reader is encouraged to review Annex D of IEEE Std 802.1X and IEEE Std 802.1Q's use of bridge components in its specification of Provider Edge Bridges (PEBs), Backbone Edge Bridges (BEBs), PBNs, and provider network service interfaces (see, in particular, IEEE Std 802.1Q-2014 Clause 15, Clause 16, Clause 25, 15.2, and 25.2).

15.1 EDE characteristics

The specification of EDEs arises from the desire to separate, so far as is possible, the implementation and use of MAC security within bridged networks from other implementation and management concerns. Reduction of the scope (in terms both of quantity and variety) of the functionality co-resident with the implementation and management of MACsec and its associated authentication, authorization, and key agreement functions can have two benefits. First, there is less software to validate, and fewer people and organizations might have to be involved in the development of each EDE. Second, it might be possible to assign management responsibility for EDEs and other bridging systems to separate smaller administrative organizations, each with its own particular expertise. Against these benefits are to be set the costs arising from additional items of equipment and the operational coordination necessary. This standard does not attempt to judge the balance of these benefits and costs, which are implementation and deployment specific. In particular there is no suggestion that the specification of EDEs means that these are always preferred to the use of other bridging systems specified in IEEE Std 802.1Q with MACsec supporting particular ports.

Restricting an EDE to having two and only two physical ports reduces the requirement for traffic class processing, particularly if the ports operate at close to the same data rate. A two-port EDE might also have no need to appear as a node in certain protocols at all, with frames for those protocols (or specific instances of those protocols as identified by destination group MAC address) being relayed simply from one port to another. Since other types of bridging systems will be usually attached to an EDE, there is no need to learn from the source address of frames.

NOTE 1—IEEE Std 802.1Q provides for some functional simplification in two-port systems or components. Provider Edge Bridges can simply forward frames addressed to the Nearest Customer Bridge Address if the C-VLAN component of a PEB has a single Provider Edge Port, i.e., it provides connectivity to a single provider network service instance (stated in terms of the equivalent condition of connecting to the S-VLAN component through a single Customer Network Port in IEEE Std 802.1Q-2014 subclause 13.41). If the enhanced filtering utility criteria (IEEE Std 802.1Q-2014 8.7.2) can never be met (a common condition for a two-port component supporting point-to-point connectivity), no source address learning need ever occur, and the size of the Filtering Database can be restricted to that necessary to accommodate the Permanent Database.

This standard specifies various types of EDE, distinguishing them by their bridging components. An EDE-M comprises a single VLAN-unaware MAC Bridge component, an EDE-CS (both a C-VLAN and an S-VLAN component), an EDE-CC two C-VLAN components, and an EDE-SS two S-VLAN components. The architecture and use of each type is explained in the following clauses (15.2–15.7).

NOTE 2—The first-time reader of this specification is encouraged to read 15.2 through 15.7 before attempting to understand this taxonomy and its inherent possibilities in detail. In brief, describing each type of EDE in terms of existing components (just as IEEE Std 802.1Q specifies a Provider Edge Bridge in terms of the C-VLAN and S-VLAN components that comprise Customer Bridges and Provider Bridges respectively) makes for economy of specification and simplifies analysis. Since the existing components can already be connected in a network, and any part of a valid network can be considered a valid (if large) system, no new interoperability challenges arise.

15.2 Securing LANs with EDE-Ms

In the simplest EDE network configuration, the protected (black-side) of each of a pair of EDE-Ms is attached to a single LAN providing point-to-point connectivity between the EDEs as shown in Figure 15-1.

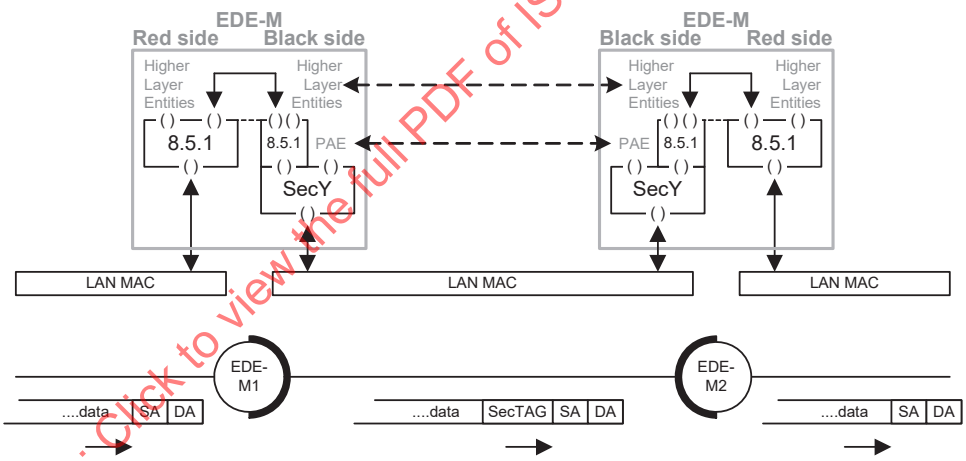


Figure 15-1—EDE-Ms connected by a point-to-point LAN

The upper part of Figure 15-1 shows the interface stacks, each attached to a LAN, in two EDE-Ms. The lower part shows the path, from the red side of one of the EDEs through to the red side of the other, and the change to a frame transmitted along that path.

NOTE 1—The architecture of a bridge is often drawn as in Figure 11-4, showing the MAC Relay entity below the MAC Service boundary to show that the relay is transparent to higher layer protocols. In this clause (Clause 15) it is convenient to use figures that focus on the interface stacks supporting relay and higher layer entities as in Figure 11-5. Numbers in the figures in this clause (e.g., 8.5.1 in Figure 15-1, 6.9 in Figure 15-2) refer to relevant clauses of IEEE Std 802.1Q-2014. The representation of EDE-M1 and EDE-M2 in Figure 15-1 provides a simple indication that frames transmitted and received by their black-side ports have had SecTAGs (and MACsec processing) applied. Similarly, other figures in this clause use light and dark patterns to indicate the possible presence of a C-VLAN or an S-VLAG tag respectively. For example, in Figure 15-3 an untagged or C-tagged frame from B1 is Sec-tagged by EDE-1, has an

S-TAG added by PB1, and passes through PB2 before the outer tags are processed and removed en-route to B2. This notation can be used in larger network diagrams where showing the frame on each connecting link is inconvenient.

A pair of EDE-Ms can secure a point-to-point LAN connecting the ports of two Customer Bridges or Provider Bridges, as in Figure 15-2.

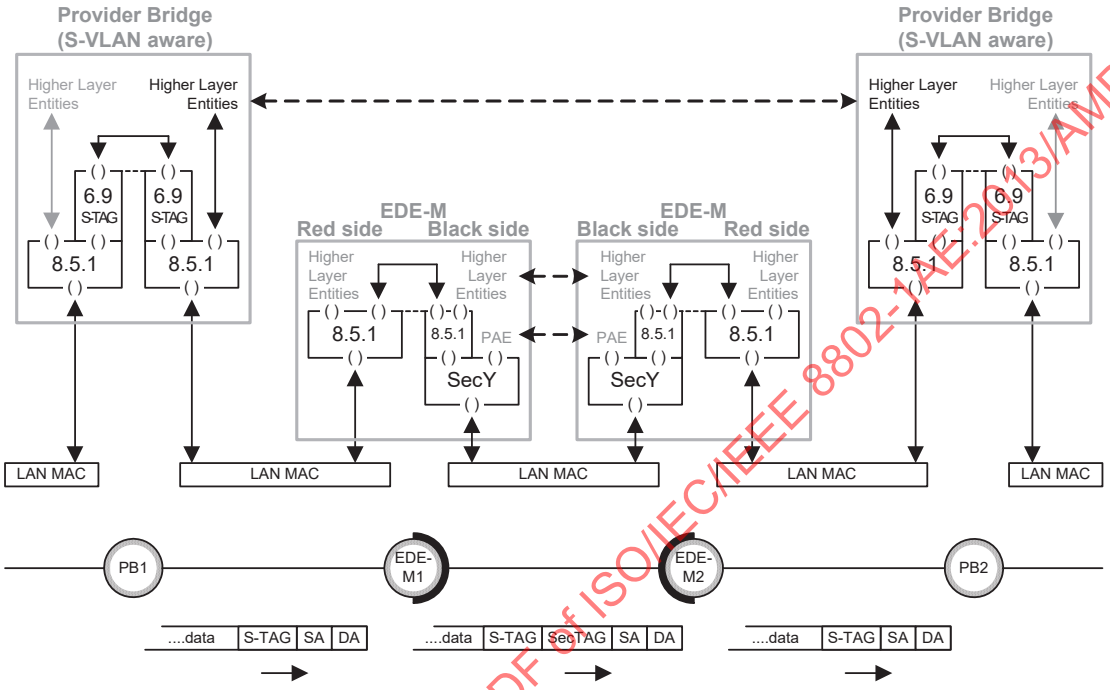


Figure 15-2—EDE-Ms securing a point-to-point LAN between Provider Bridges

Each EDE-M's PAE uses the Nearest non-TPMR group address[6] (01-80-C2-00-00-03) as the destination address for EAPOL PDUs. Frames with this destination address are filtered by all bridges specified in IEEE 802.1 standards (including EDEs) other than TPMRs. A PAE receiving a frame with this destination address can be certain that no IEEE 802.1 standards-conformant bridge lies between itself and the originator of the frame. If such a bridge is interposed between the EDE-Ms, they will not exchange EAPOL PDUs and will not, as a consequence, use MACsec to protect the frames (if any) that they forward. This avoids unintended use of the EDE-Ms in a misconfigured network. Similarly neither EDE-M shown can receive EAPOL-PDUs from other EDEs connected to PB1 or PB2. This helps to prevent accidental creation of MACsec protected connectivity through (but without the participation of) an intervening bridge, and the undesirable consequence of making it impossible for that bridge to understand frames that it was intended to receive.

NOTE 2—EAPOL PDUs are used to initiate and reinitiate EAP authentication exchanges, convey EAP PDUs in support of those exchanges, and convey MACsec Key Agreement PDUs (MKPDUs). At the time of the development of the IEEE Std 802.1AEcg-2016 amendment to this standard, EAPOL destination addresses were specified in IEEE Std 802.1X-2010 11.1 and Table 11-1, and filtering of Reserved Addresses by bridges was specified in IEEE Std 802.1Q-2014 8.6.3, 8.13.4, and Table 8-1, Table 8-2, and Table 8-3.

Each EDE-M also filters the addresses specified by IEEE Std 802.1Q as TMPR component Reserved Addresses. When an EDE-M's PAE is configured to use the Nearest non-TPMR group address, the other Reserved Addresses specified for MAC Bridge, C-VLAN, and S-VLAN components are forwarded, making the EDE-Ms and the connection they protect transparent to protocols using those addresses.

[6]This address was identified as the 802.1X PAE address in IEEE Std 802.1Q-2005. That name is still used in IEEE 802.1X-2010.

15.3 Securing connectivity across PBNs

IEEE Std 802.1Q specifies support of the MAC Service by Provider Bridged Networks and their principles of operation. Individual instances of the MAC Service are segregated within the PBN by S-VLAN tag, and access to those instances are provided by port-based, C-tagged, or S-tagged service interfaces. A given service instance can support service interfaces of more than one type. For example, in a hub-and-spoke configuration, it might be convenient to use a C-tagged service interface at the central site but a port-based interface at the remote sites, since the latter communicate directly only with the central site. Such an arrangement avoids having to configure each remote site differently. Alternately, each remote site might be configured to use the same identical S-TAG value. In the first of these alternatives, the PBN adds or removes the tag at the service interface; in the latter, it is translated. S-VLAN tag translation within the PBN also allows the service provider to re-allocate service instances without changing the customers' service instance selection. The VLAN tags used for service selection also carry priority and drop_eligible fields that can be policed and changed by the service provider.

NOTE—This summary of PBN service instance selection, segregation, and priority handling serves only to provide context for the provisions for this standard. For an authoritative specification, refer to IEEE Std 802.1Q.

Since VLAN tags used for communicating priority information and for service instance selection can be modified by the PBN service provider, they cannot be protected by MACsec, as any change would then result in discard on verification failure. It is also preferable for the service provider not to have to make any change to accommodate MACsec-protected frames. From the service provider's point of view, a frame whose initial EtherType is the MACsec EtherType is untagged (unless the provider's interface is itself a member of the CA that is protecting frames between the interface and customer's equipment). Figure 15-3 illustrates the passage of two MACsec-protected frames from one customer bridge network to another through port-based interfaces provided by a PBN. The first frame comprises a MAC DA, SA, and arbitrary data, with each of these frame fields reaching its destination unmodified. The second comprises a MAC DA and SA, a C-VLAN tag, and arbitrary data. Each of these frame fields also reaches its destination unmodified—the C-VLAN tag is just one possibility for the initial octets of the arbitrary data of the first example frame—and its protection ensures that an attacker cannot simply change the VLAN assignment of the frame.

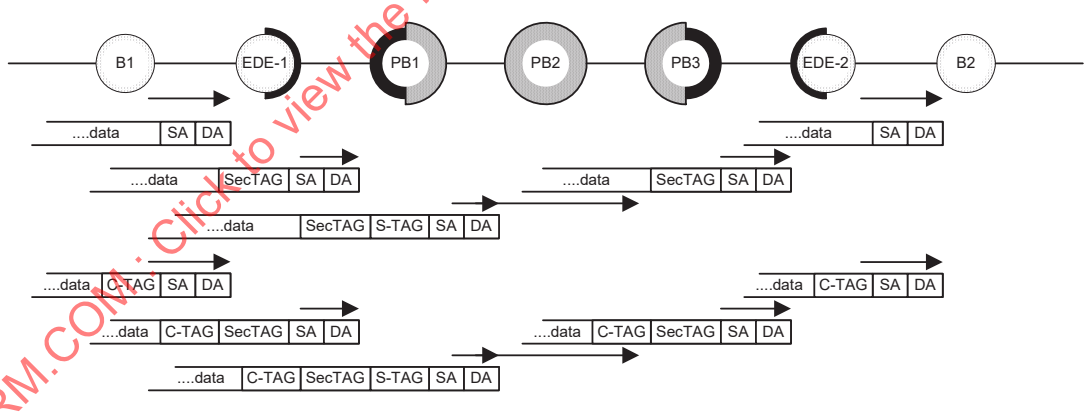


Figure 15-3—MACsec protected frame traversing a PBN

Since the PBN service provider (operating PB1) sees frames received from the customer as untagged, Figure 15-3 does not provide a way for EDE-1 to communicate each frame's priority to PB1. This can be done by priority tagging the frame after protecting it with MACsec. This requirement to communicate priority is so common as to be a required EDE-M capability (15.4, Figure 15-4). Other types of EDE, including the EDE-CS (15.5, Figure 15-6), add a full VLAN tag that depends on the protected VLAN tag so that the service provider can support service selection without requiring access to the protected data.

15.4 Securing PBN connectivity with an EDE-M

The point-to-point connectivity between the EDEs shown in Figure 15-1 could equally be provided by a Provider Bridged Network (PBN). Figure 15-4 illustrates the use of a pair of EDE-Ms to secure connectivity between Customer Bridges attached to port-based service interfaces provided by a PBN. (Numeric references in the figure are to clauses in IEEE Std 802.1Q-2014.)

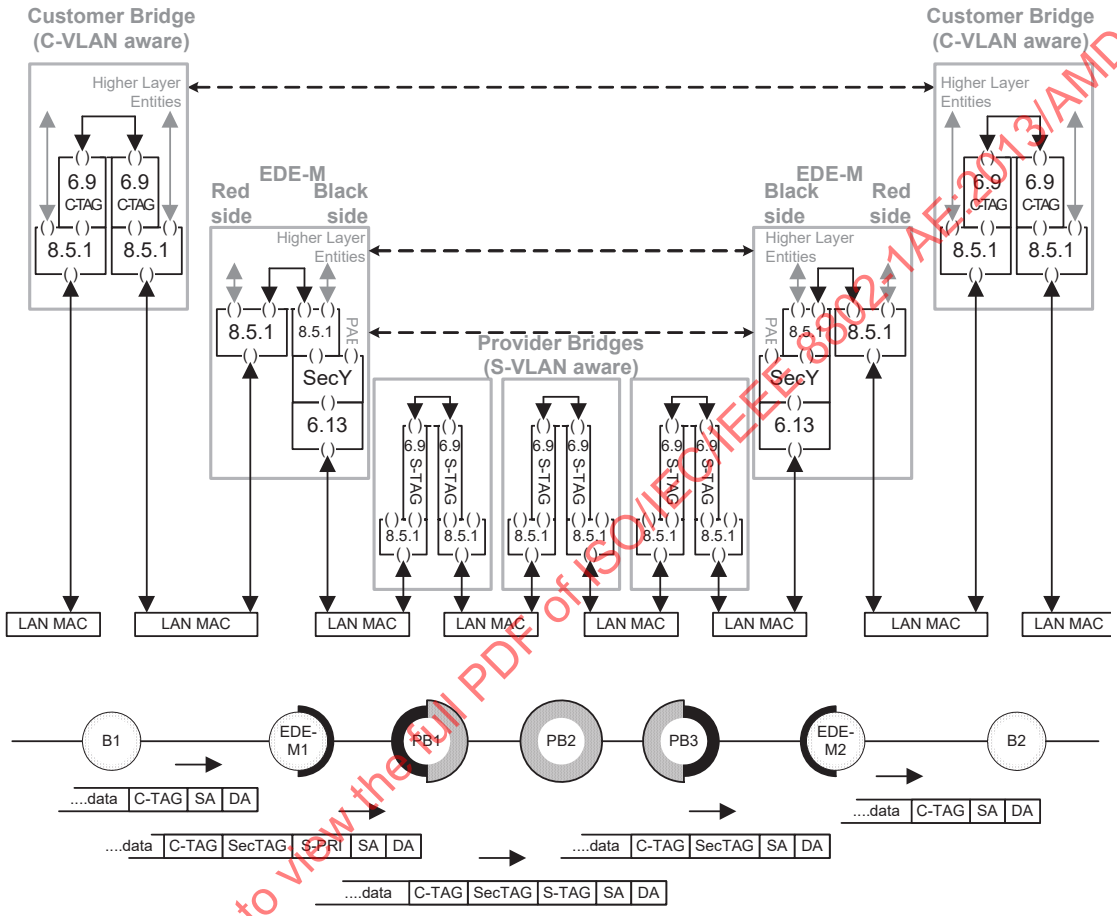


Figure 15-4—EDE-Ms securing point-to-point LAN connectivity across a PBN

As shown in the figure, EDE-M1 (on the left) may recover the signaled priority from the C-VLAN tag (if present) of the received frame as specified by IEEE Std 802.1Q (IEEE Std 802.1Q-2014 6.20 Support of the ISS with signaled priority) before protecting the frame using MACsec. If the EDE-M1 is capable of recovering signaled priority, it shall also be capable of being configured to priority tag (IEEE Std 802.1Q-2014 6.13 Support of the ISS for attachment to a PBN) or not priority tag frames transmitted by the black-side port. EDE-M2 (on the left) receives the frame and (if it is capable of recognizing signaled priority and priority tagging frames) removes any S-TAG immediately following the MAC SA and DA (not shown in the figure, which assumes the service provider interface has been configured to deliver frames that are not S-tagged). It validates the frame using MACsec before recovering the priority originally signaled by B1 in the C-VLAN tag (if present, and if capable of recovering signaled priority) and forwarding the frame.

In this scenario, each EDE-M's PAE uses the Bridge Group Address (01-80-C2-00-00-00) as the destination address of EAPOL PDUs transmitted to its peer PAE. The use of this address is specified in IEEE

Std 802.1X, and it is also identified as the Nearest Customer Bridge group address by IEEE Std 802.1Q. Each EDE-M filters any frame with a destination address that is one of the Reserved Addresses specified by IEEE Std 802.1Q as filtered by MAC Bridge and C-VLAN components (IEEE Std 802.1Q-2014 Table 8-1) with the exception of the Nearest Customer Bridge group address.

NOTE—A frame that is received on the red-side port and not forwarded by the MAC Relay Entity will not be received by the PAE for the black-side port or transmitted on the black-side port. A frame that is received on the black-side port and not forwarded will not be transmitted on the red-side port but can be received by the PAE for the black-side port.

The PBN service is not necessarily limited to point-to-point connectivity, Figure 15-5 illustrates the secure use of a multi-point service to connect three customer bridges.

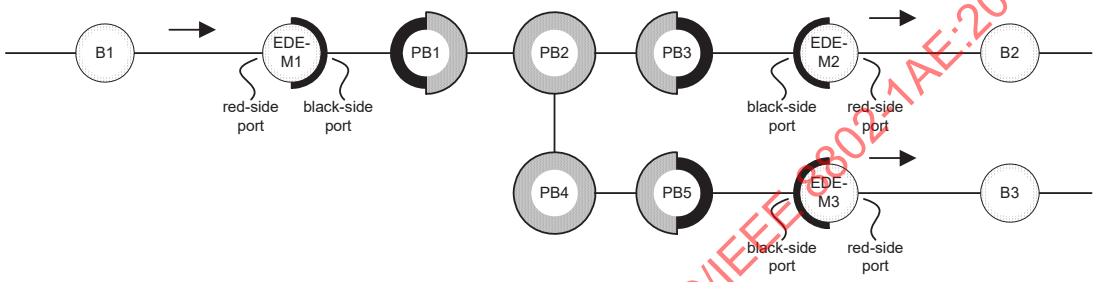


Figure 15-5—EDE-Ms securing multi-point PBN connectivity

In the figure the provider bridge ports attached to the black-side ports of each of the EDEs are assumed to be configured to provide connectivity between each of the latter.

15.5 Securing PBN connectivity with an EDE-CS

An EDE-CS provides a red-side C-tagged service interface and uses a black-side S-tagged service interface. It allows an attached customer network to use C-VIDs to select between provider service instances, protects each of those service instances with a separate CA, and identifies frames for each with a single S-VID. An EDE-CS comprises both a C-VLAN and an S-VLAN component, just as in a Provider Edge Bridge (PEB), with the following additions and restrictions. A single C-VLAN component provides a single red-side Customer Edge Port and one or more Provider Edge Ports, each supported by a SecY. Each of the Provider Edge Ports is attached to one of the Customer Network Ports of the S-VLAN component, which supports a single black-side Provider Network Port.

NOTE—The terms *customer* and *provider* applied to the external and internal ports of an EDE-CS are those used by IEEE Std 802.1Q in its description of PBs, PEBs, and BEBs and reflect the role of those ports in the layered network architecture. They do not indicate control or ownership of the equipment.

Figure 15-6 depicts an example network, with a single provider operated bridge (PB) that provides S-tagged service interfaces to two customer operated EDE-CSs and a customer operated PEB, and a port-based interface to a customer owned EDE-M. Consider EDE-CS1, on the left of the figure. This has a C-VLAN component, with a single Customer Edge Port connected to bridge B1 and three Provider Edge Ports, and an S-VLAN component, with a Provider Network Port attached to the provider's S-tagged service interface and three Customer Network Ports. Each of the three Provider Edge Ports has a SecY that protects transmitted and received frames and connects to one of the Customer Network Ports. EDE-CS1's C-VLAN component is constrained, as required by IEEE Std 802.1Q's specification of PEB operation, to forward frames received on its Customer Edge Port for a given VLAN to at most one of its Provider Edge Ports, and hence to at most

one Customer Network Port. Each of the Customer Network Ports does not have a SecY, and thus treats each received frame as untagged and assigns it to the S-VLAN identified by the port's PVID as follows:

— The upper port's PVID is configured with the S-VID used by the point-to-point service instance that provides connectivity to EDE-M2 (thus protecting communication between B1 and B2)

— The middle port's PVID provides connectivity to the upper Provider Edge Port in EDE-CS3 (protecting communication between B1 and B3).

— The lower port's PVID provides connectivity to the upper C-VLAN component in PEB4 (with a SecY on its Provider Edge Port, protecting communication between B1 and B4.1).

Not all the protected traffic has to pass through EDE-CS1 or be associated with one of its protected service instances; the figure also shows EDE-CS3 and PEB4 (with a SecY on the Provider Edge Port of its lower C-VLAN component) protecting traffic between B3 and B4.2.

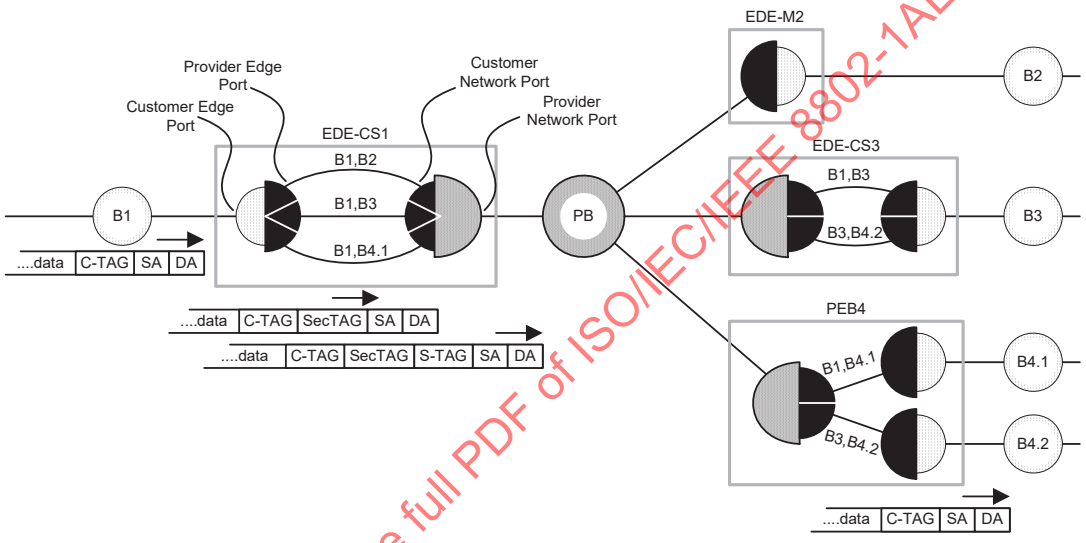


Figure 15-6—Example network with an EDE-CS

Figure 15-7 shows the internal architecture of an EDE-CS together with that of a Customer Bridge and a Provider Bridge (attached to the EDE-CS's Customer Edge Port and Provider Network Port respectively). This view of the interface stacks involved in the connection of the EDE-CS to an S-tagged interface depicts just one path through the network.

The PAE of each EDE-CS's Provider Edge Port shall be capable of being configured to use the Bridge Group Address (01-80-C2-00-00-00, also known as the Nearest Customer Bridge group address) as the destination address of EAPOL PDUs that it transmits and receives. The C-VLAN component of an EDE-CS filters any frame with a destination address that is one of the Reserved Addresses specified by IEEE Std 802.1Q as filtered by MAC Bridge and C-VLAN components (IEEE Std 802.1Q-2014 Table 8-1), including the Nearest Customer Bridge group address. The S-VLAN component filters any frame with a destination address that is one of the Reserved Addresses specified by IEEE Std 802.1Q as filtered by S-VLAN components.

NOTE—Because the EDE-CS's C-VLAN component provides connectivity to multiple service instances, it does not offer the same level of transparency to protocols using the Nearest Customer Bridge group address as does an EDE-M.

In Figure 15-6 the PAE associated with the uppermost Provider Edge Port on EDE-CS1 is connected (over an S-VLAN supported by the Provider Bridge PB) to the PAE for the black-side port of EDE-M2, and exchanges EAPOL PDUs with that PAE. The path between the PAEs is supported by the S-VLAN components (the network component in EDE-CS1 and the Provider Bridge PB) that do not filter frames with the destination MAC address used by the EAPOL PDUs. Similarly EAPOL PDUs are exchanged between

the PAE for the middle Provider Edge Port of EDE-CS1 exchanges EAPOL PDUs with the PAE for the upper Provider Edge Port of EDE-CS3 (over another S-VLAN), between the PAE for lower Provider Edge Port of EDE-CS1 and that for the upper Provider Edge Port of PEB4, and between the PAEs for the lower Provider Edge Ports for EDE-CS3 and PEB4.

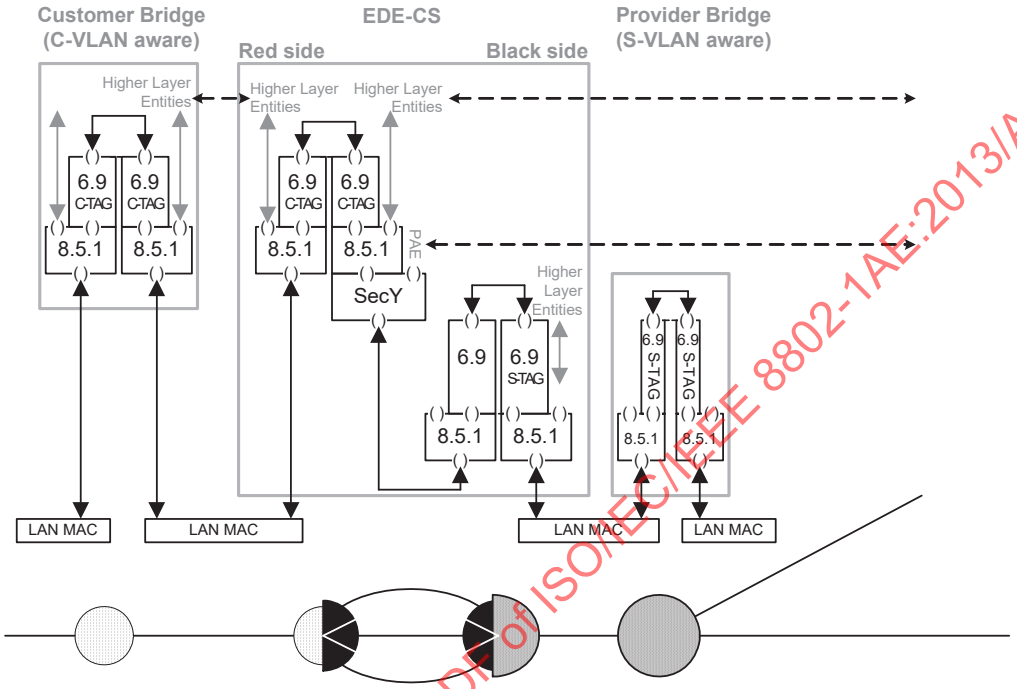


Figure 15-7—EDE-CS connected to a PBN S-tagged interface

15.6 Securing PBN connectivity with an EDE-CC

A service provider might offer C-tagged service interfaces but not S-tagged interfaces. Equally it might be desirable to secure existing network connectivity by adding an EDE between a Customer Bridge and the provider network while retaining the C-VLAN service selection capability. Figure 15-8 illustrates this before and after scenario.

The upper half of the figure depicts a Customer Bridge attached to a PEB that provides access to three point-to-point service instances, each selected by one or more C-VIDs or by the PVID used by the PEB's Customer Edge Port to classify frames received untagged. Frames with any given VID are forwarded through at most one of the PEB's Provider Edge Ports and hence through at most one Customer Network Port. The PEB's S-VLAN component sees each of these frames as untagged (as it does not recognize a C-TAG) and assigns each to the S-VLAN (and thus to the point-to-point service instance) identified by the Customer Network Port's PVID. The frame is S-tagged with the selected S-VID as it passes through the PEB's Provider Network Port into the PBN. In the other direction, each frame received from the PBN is directed by the PEB's S-VLAN component to Customer Network Port whose PVID matches the received S-VID. The S-TAG is removed on transmission through the Customer Network Port, revealing the C-tagged frame, which is then forwarded by the PEB's C-VLAN component. Within the PEB, one C-VLAN can be carried without a tag on each of the *internal LANs* that connects a Provider Edge Port with a Customer Network Port, which leads to the possibility of frames for each of these C-VLANs being carried without a C-TAG within the PBN.

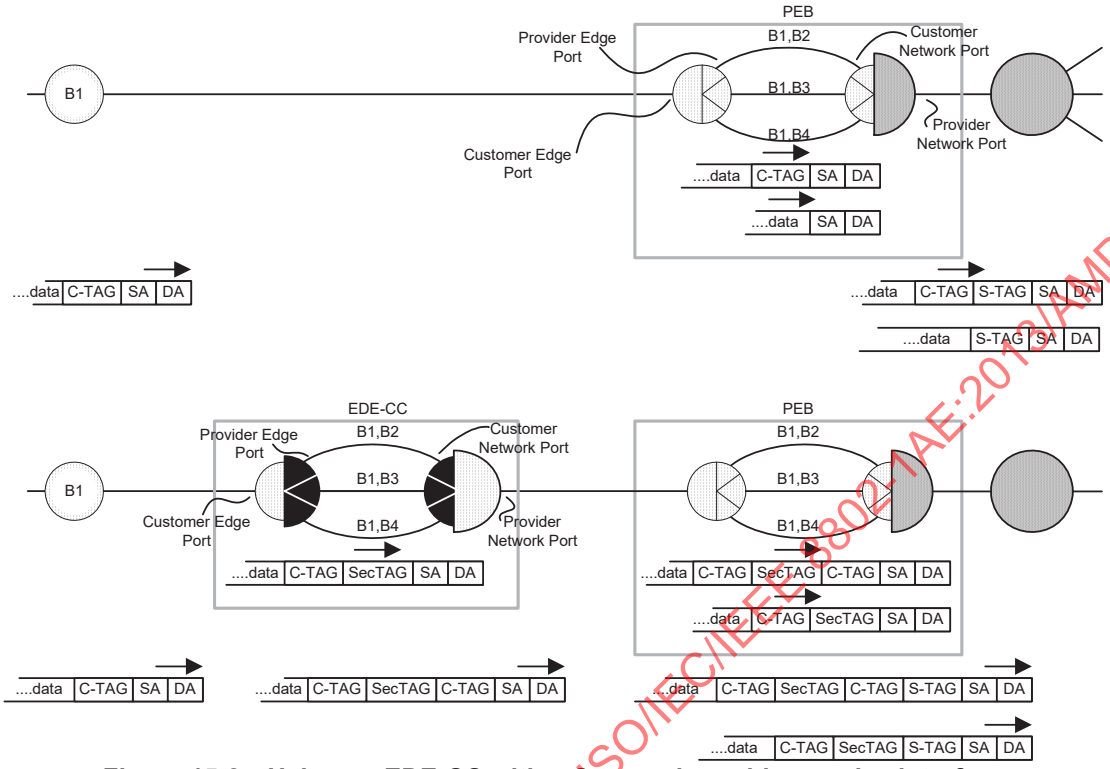


Figure 15-8—Using an EDE-CC with a C-tagged provider service interface

In the lower half of Figure 15-8 an EDE-CC has been added between the Customer Bridge and the PEB. In the figure the PEB is shown as supporting three service provider instances, protecting communication between B1 and B2, B1 and B3, and between B1 and B4 (B2, B3, and B4 lying elsewhere in the network), and the EDE-CC's edge component has three Provider Edge Ports, each participating in a CA that protects one of the service instances. In this scenario, it is unnecessary to carry the additional C-TAG, added by the EDE-CC's network component, over the PBN—it can be removed by the PEB's Provider Edge Port as the attached internal LAN suffices to identify the provider service instance within the PEB. The PBN frame format for each of the service instances is then as shown in the bottom right of the figure. If the PEB had been configured to map these CAs to one or two service instances, a C-TAG would be required to distinguish those carried over a common service instance.

Figure 15-9 shows the architecture of the EDE-CC in more detail. This standard extends the use of the terms Customer Edge Port, Provider Edge Port, Customer Network Port, and Provider Network Port (initially defined in IEEE Std 802.1Q for Provider Edge Bridges) to identify ports that play similar roles in EDE-CSs, EDE-CCs, and EDE-SSs. However, if a SecY associated with a EDE-CC's Provider Edge Port is configured not to protect frames (as might be done to facilitate initial deployment), a SecTAG will not be added to transmit frames, and the EDE-CC's Customer Network Port component will see the received frames as already C-VLAN-tagged and will not add a further tag. The externally observable behavior of the EDE-CC would then resemble that of a single Customer Bridge, not a Provider Edge Bridge.

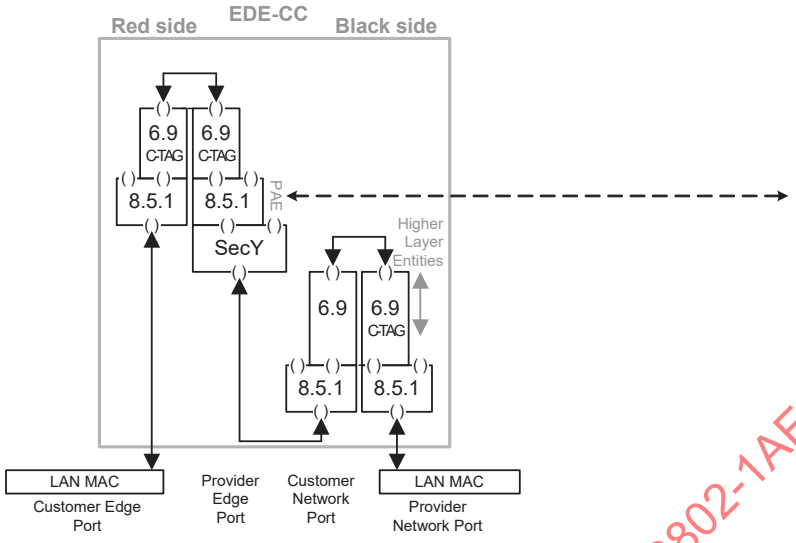


Figure 15-9—EDE-CC architecture

The PAE of each Provider Edge Port for an EDE-CC's edge component shall be capable of being configured to use the EDE-CC PEP Address (see Table 15-1) as the destination address of EAPOL PDUs that it transmits and receives. In Figure 15-9, the EDE-CC's C-VLAN network component (shown on the right in the figure, with a Customer Network Port and a Provider Network Port) is shown at a lower level than its accompanying edge component to emphasize the fact that it is transparent to the operation of the Provider Edge Port PAEs and other edge component protocol entities. It filters any frame with a destination address that is one of the Reserved Addresses specified by IEEE Std 802.1Q as filtered by S-VLAN components. The EDE-CC's C-VLAN edge component (shown on the left in the figure, with a Customer Edge Port and a Provider Edge Port) filters any frame with a destination address that is either one of the Reserved Addresses specified by IEEE Std 802.1Q as filtered by MAC Bridge and C-VLAN components (IEEE Std 802.1Q-2014 Table 8-1) or the EDE-CC PEP Address.

The configuration of an EDE-CC is constrained to restrict egress for each Provider Edge Port to a single C-VID and to restrict the PVID for the internally connected Customer Network Port to the same value, with the consequence that the outer C-VID will always match the inner C-VID. The PVID for the Customer Edge Port is constrained to be the same as that for the Provider Network Port and the Static VLAN Registration Entry (IEEE Std 802.1Q 8.8.2) for that and other VIDs are constrained so that frames for that VID are transmitted untagged on both ports, with the consequence that frames received untagged on either port are forwarded (if at all) untagged on the other. These restrictions simplify EDE management, supporting the desired separation of concerns (15.1) and maintaining the scope of address learning within each C-VLAN. If the desired secured connectivity between the EDE-CC and its potential (provider network attached) peers depends only on their characteristics and does not vary by C-VLAN, an EDE can create that secure connectivity on demand—initiating EAP or starting MKA instances to authenticate and authorize the VLAN connectivity as frames for each VLAN are received—reducing the need to communicate VLAN specific details between administrative organizations. Further restrictions on the use of EAPOL and MKA to support such dynamically created connectivity—including use of pre-shared or cached CAKs and announcements—are beyond the scope of this specification (see IEEE Std 802.1X for detailed capabilities).

NOTE—The descriptive advantage of the two component architecture of PEBs and EDEs is not limited to VLAN multiplexing over service instances. It allows existing and developing port-based queue servicing specifications to be applied in the context of the resources available to each provider service instance, for example.

15.7 Securing PBN connectivity with an EDE-SS

An EDE-SS addresses a similar requirement to that for an EDE-CC—securing existing network connectivity with minimal change to existing systems, in this case retaining S-VLAN service selection capability, using the same architecture with two S-VLAN components instead of two C-VLAN components. The same configurations restrictions apply: the value of the outer S-VID added and removed by the EDE's network component matches that of the inner S-VID, and frames received untagged by the Customer Edge Port are transmitted untagged by the Provider Network Port and vice versa.

The PAE of each EDE-SS's Provider Edge Port shall be capable of being configured to use the EDE-SS PEP Address (see Table 15-1) as the destination address of EAPOL PDUs that it transmits and receives. The S-VLAN network component filters any frame with a destination address that is one of the Reserved Addresses specified by IEEE Std 802.1Q as filtered by S-VLAN components. The S-VLAN edge component filters any frame with a destination address that is one of these addresses or the EDE-SS PEP Address.

NOTE—An EDE device with red-side recognition of S-TAGs and black-side addition and removal of I-TAGs and B-TAGs, used to secure connectivity across a Provider Bridged Backbone Network (PBBN), would not differ from a BEB with an EDE-SS on the customer side and is therefore not described in this standard.

15.8 EDE Interoperability

The PAEs specified above for each EDE type (15.2, 15.4, 15.6, 15.7) can be configured to use the group MAC address typically used by a potential peer MACsec capable system. Table 15-1 summarizes the group addresses specified by this standard and IEEE Std 802.1X, and their filtering by bridge components.

Table 15-1—PAE Group Addresses

Address assignment	Address value	Address filtering				
EDE-CC PEP Address	01-80-C2-00-00-1F	Y[a]				
Bridge Group Address, Nearest Customer Bridge group address	01-80-C2-00-00-00	Y	Y			
EDE-SS PEP Address	01-80-C2-00-00-0B	Y	Y	Y		
Nearest non-TPMR Bridge group address, IEEE Std 802.1X PAE address[b]	01-80-C2-00-00-03	Y	Y	Y	Y	
Individual LAN Scope group address, Nearest Bridge group address[c]	01-80-C2-00-00-0E	Y	Y	Y	Y	Y
						EDE-CC Edge components
					MAC Bridge & C-VLAN components (Customer Bridges, PEB w/multiple PEPs[d])	
				PEB C-VLAN components w/ single PEP		
			S-VLAN components (Provider Bridges, Provider Backbone Bridges, PEBs)			
		TPMR components				

[a]Y indicates, Yes, this address is filtered by the component.
[b]Identified as the 802.1X PAE address in IEEE Std 802.1Q-2003, IEEE Std 802.1Q-2005, and IEEE Std 802.1X.
[c]It is intended that no IEEE 802.1 relay device will be defined that will forward frames that carry this destination address.
[d]A PEB's C-VLAN component with multiple PEPs supports more than one provider network service instance.

Table 15-2 summarizes the use of these addresses in various scenarios. In each case, the choice of address is constrained by the need for it to be forwarded (and not filtered) by intervening components. For example, a PAE for an EDE-M connected via a port-based interface providing access to a single provider service instance can use the Nearest Customer Bridge group address to communicate to a peer PAE in a similarly

connected EDE-M or Customer Bridge, but cannot use that address to communicate to an EDE-CC connected to a C-tagged interface. Where connectivity is impossible or undesirable, an address is not given. For example, securing connectivity between a EDE-CC connected to a provider network and a TPMR connected to a distant LAN might be possible using the EDE-CC PAE address, but could render traffic relayed by the TPMR unintelligible to neighboring Customer Bridges, which operate at a higher sublayer in the network's connectivity. The network administrator should take care not to introduce a similar (sub)layering violation by configuring the PAE of an EDE-M that is not directly connected to a PBN with the EDE-CC PAE address, as that could interfere with the operation of configuration protocols between the EDE-M and its immediate neighbors.

Table 15-2—PAE Group Address use

System	Connectivity	Address[a,b]							
EDE-CC	C-tagged PBN i/f	-1F	-1F	-1F					
EDE-M	Port-based PBN i/f	-1F	-00	-00	-00				
Customer Bridge	Port-based PBN i/f	-1F	-00	-00	-00				
EDE-CS	S-tagged PBN i/f		-00	-00	-00				
EDE-SS	S-tagged PBN i/f					-0B			
Provider Bridge	Individual LAN						-03	-03	-03	-0E
EDE-M	Individual LAN						-03	-03	-03	-0E
Customer Bridge	Individual LAN						-03	-03	-03	-0E
TPMR	Individual LAN						-0E	-0E	-0E	-0E

[a]The system connected as shown in the *i*th row of the table interoperates with that in the *j*th row (also connected as shown in that row) using the group address in *i*th row and *j*th column.
[b]For convenience the EDE-CC PEP Address is shown as -1F, the Nearest Customer Bridge group address as -00, the EDE-SS PEP address as -0B, the Nearest non-TPMR group address as -03, and the Nearest Bridge group address as 0E.

NOTE—Table 15-2 is not intended to cover all MACsec interoperability scenarios.

In addition to agreeing on the group addresses to be used by their PAEs, MACsec-capable systems connected to a PBN can only interoperate if the use, addition, removal, or modification of VLAN tags by the provider network is appropriate. EDE-CCs (for example) rely on the presence of VLAN tags to distinguish provider network service instances. EDE-Ms (on the other hand) need to receive frames from the attached single provider network service instance untagged. When EDE-Ms (or MACsec-capable Customer Bridges) are connected across a PBN in a hub-and-spoke configuration to an EDE-CC acting a hub, the PBN has to be configured to add a C-VLAN tag prior to EDE-CC reception so that the latter can separate frames from each spoke and has to remove the outer C-VLAN tag from frames transmitted by the EDE-CC before they are delivered to each spoke.

Any outer C-VLAN (or S-VLAN in the case of an EDE-SS) tag only facilitates service selection and connectivity across the PBN. This tag is neither used or trusted by systems attached to red-side ports. The level of trust associated with connectivity between EDEs is based on contents of each MACsec-protected frame, including (where appropriate) the VLAN tag. For example, red-side traffic can be separated by VLAN according to the use made of each VLAN. If an EDE-CC's PEP's PAE establishes connectivity across a PBN and the level of authorization (based on authentication attributes) associated with the remote EDE is sufficient only to permit limited access (perhaps to a *guest VLAN*), then the EDE-CC's Edge Components VLAN ingress controls for the PEP can be configured to deny access to other VLANs.

15.9 EDEs, CFM, and UNI Access

Provider network operators typically define a User Network Interface (UNI) that enables autoconfiguration of devices attached to provider network services and provides service status information. One set of