

IEEE Standard for
Local and metropolitan area networks—

Media Access Control (MAC) Security

Amendment 2: Extended Packet Numbering

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 802.1AEbw™-2013
(Amendment to
IEEE Std 802.1AE™-2006)

12 February 2013

**IEEE Standard for
Local and metropolitan area networks—**

Media Access Control (MAC) Security

**Amendment 2:
Extended Packet Numbering**

Sponsor

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

Approved 6 February 2013

IEEE-SA Standards Board

Approved 24 October 2014

American National Standards Institute

Abstract: The optional use of Cipher Suites that make use of a 64-bit (PN) to allow more than 2^{32} MACsec protected frames to be sent with a single Secure Association Key are specified by this amendment.

Keywords: authorized port, confidentiality, data origin authenticity, IEEE 802.1AE, IEEE 802.1AEbw, 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

Copyright © 2013 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 12 February 2013. Printed in the United States of America.

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

PDF: ISBN 978-0-7381-8148-6 STD98100
Print: ISBN 978-0-7381-8149-3 STDPD98100

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

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

Notice and Disclaimer of Liability Concerning the Use of IEEE Documents: IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. 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 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.

Use of an IEEE Standard is wholly voluntary. IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon any IEEE Standard document.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied "AS IS."

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. 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 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.

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 the official position of IEEE or any of its committees and shall not be considered to be, nor 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 to ensure 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. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant IEEE working group at <http://standards.ieee.org/develop/wg/>.

Comments on standards should be submitted to the following address:

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

Photocopies: Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, 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.

Notice to users

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

This document is copyrighted by the IEEE. It is made available 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 this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE 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. 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](http://standards.ieee.org) or contact the IEEE at the address listed previously. For more information about the IEEE Standards Association or the IEEE standards development process, visit the [IEEE-SA Website](http://standards.ieee.org).

Errata

Errata, if any, for this and all other standards can be accessed 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.

Introduction

This introduction is not part of IEEE Std 802.1AEbw-2013, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Security—Amendment 2: Extended Packet Numbering.

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. This second amendment adds optional Cipher Suites, GCM-AES-XPB-128 and GCM-AES-XPB-256, that 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.

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.

This standard 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.

Participants

At the time this standard was submitted to the IEEE-SA Standard Board for approval, the IEEE P802.1 Working Group had the following membership:

Tony Jeffree, *Chair*

Glenn Parsons, *Vice-Chair*

Mick Seaman, *Editor and Task Group Chair*

Zehavit Alon	Anoop Ghanwani	John Morris
Yafan An	Franz Goetz	Eric Multanen
Ting Ao	Mark Gravel	David Olsen
Peter Ashwood-Smith	Eric Gray	Donald Pannell
Christian Boiger	Yingjie Gu	Mark Pearson
Brad Booth	Craig Gunther	Joseph Pelissier
Paul Bottorff	Stephen Haddock	Rene Raeber
Rudolf Brandner	Hitoshi Hayakawa	Karen T. Randall
Craig Carlson	Markus Jochim	Josef Roesse
Xin Chang	Michael Johas Teener	Dan Romascanu
Weiyang Cheng	Girault Jones	Jessy Rouyer
Paul Congdon	Daya Kamath	Ali Sajassi
Diego Crupnicoff	Hal Keen	Panagiotis Saltsidis
Rodney Cummings	Srikanth Keesara	Koichiro Seto
Claudio Desanti	Yongbum Kim	Rakesh Sharma
Donald Eastlake, III	Philippe Klein	Takeshi Shimizu
Janos Farkas	Oliver Kleineberg	Kevin Stanton
Donald Fedyk	Jeff Lynch	Patricia Thaler
Norman Finn	Ben Mack-Crane	Jeremy Touve
Andre Fredette	David Martin	Maarten Vissers
Geoffrey Garner	John Messenger	Yuehua Wei
		Min Xiao

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

Thomas Alexander	Atsushi Ito	Benjamin Rolfe
Arthur Astrin	Tony Jeffree	Randall Safier
Nancy Bravin	Michael Johas Teener	Bartien Sayogo
William Byrd	Shinkyō Kaku	Mick Seaman
Radhakrishna Canchi	Piotr Karocki	Gil Shultz
Juan Carreon	Stuart Kerry	Dorothy Stanley
Keith Chow	Yongbum Kim	Thomas Starai
Charles Cook	Bruce Kraemer	Walter Struppler
Rodney Cummings	Geoff Ladwig	Joseph Tardo
Ray Davis	Shen Loh	William Taylor
Sourav Dutta	William Lumpkins	Patricia Thaler
Donald Fedyk	Greg Luri	Solomon Trainin
Yukihiro Fujimoto	Elvis Maculuba	Dmitri Varsanofiev
Devon Gayle	Jonathon McLendon	Prabodh Varshney
Eric Gray	Michael S. Newman	John Vergis
Randall Groves	Charles Ngethe	Hung-Yu Wei
Michael Gundlach	Satoshi Obara	Brian Weis
Chris Guy	Yoshihiro Ohba	Oren Yuen
Russell Housley	Karen Randall	Daidi Zhong
Noriyuki Ikeuchi	Maximilian Riegel	

When the IEEE-SA Standards Board approved this standard on 7 February 2013, it had the following membership:

John Kulick, *Chair*
Richard H. Hulett, *Past Chair*
Konstantinos Karachalios, *Secretary*

Masayuki Ariyoshi	Mark Halpin	Ron Peterson
Peter Balma	Gary Hoffman	Gary Robinson
Farooq Bari	Paul Houzé	Jon Walter Rosdahl
Ted Burse	Jim Hughes	Adrian Stephens
Wael William Diab	Michael Janezic	Peter Sutherland
Stephen Dukes	Joseph L. Koepfinger*	Yatin Trivedi
Jean-Philippe Faure	David J. Law	Phil Winston
Alexander Gelman	Oleg Logvinov	Yu Yuan

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Richard DeBlasio, *DOE Representative*
Michael Janezic, *NIST Representative*

Catherine Berger
IEEE Senior Standards Program Manager, Document Development

Kathryn Bennett
IEEE Standards Program Manager, Technical Program Development

Contents

3. Definitions	2
4. Abbreviations and acronyms	3
7. Principles of secure network operation.....	4
8. MAC Security Protocol (MACsec).....	5
8.3 MACsec operation	5
9. Encoding of MACsec protocol data units.....	7
9.8 Packet Number (PN)	7
9.9 Secure Channel Identifier (SCI)	7
10. Principles of MAC Security Entity (SecY) operation	8
10.5 Secure frame generation	8
10.6 Secure frame verification.....	9
10.7 SecY management	12
13. Management protocol	16
13.7 Use of the MIB with extended packet numbering	16
14. Cipher Suites.....	17
14.1 Cipher Suite use	17
14.2 Cipher Suite capabilities	18
14.4 Cipher Suite conformance	18
14.6 GCM–AES–256.....	18
14.7 GCM–AES–XPN-128	19
14.8 GCM–AES–XPN-256	20
Annex A (normative) PICS Proforma.....	22
A.13 Additional variant Cipher Suite capabilities	22
Annex B (informative) Bibliography	23
Annex C (informative) MACsec Test Vectors	25
C.1 Integrity protection (54-octet frame)	26
C.2 Integrity protection (60-octet frame)	31
C.3 Integrity protection (65-octet frame)	34
C.4 Integrity protection (79-octet frame)	37
C.5 Confidentiality protection (54-octet frame).....	40
C.6 Confidentiality protection (60-octet frame).....	45
C.7 Confidentiality protection (61-octet frame).....	48
C.8 Confidentiality protection (75-octet frame).....	51

Figures

Figure 8-2 MACsec operation 6

Figure 9-2 SecTAG format 7

Figure 10-5 Management controls and counters for secure frame verification 9

Figure 14-1 Cipher Suite Protect and Validate operations 17

Tables

Table 10-1	Extended packet number recovery (examples).....	11
Table 14-1	MACsec Cipher Suites.....	18
Table C-1	Unprotected frame (example)	26
Table C-2	Integrity protected frame (example)	26
Table C-3	GCM-AES-128 Key and calculated ICV (example)	27
Table C-4	GCM-AES-256 Key and calculated ICV (example)	28
Table C-5	GCM-AES-XPB-128 Key and calculated ICV (example)	29
Table C-6	GCM-AES-XPB-256 Key and calculated ICV (example)	30
Table C-7	Unprotected frame (example)	31
Table C-8	Integrity protected frame (example)	31
Table C-11	GCM-AES-XPB-128 Key and calculated ICV (example)	32
Table C-12	GCM-AES-XPB-256 Key and calculated ICV (example)	33
Table C-13	Unprotected frame (example)	34
Table C-14	Integrity protected frame (example)	34
Table C-17	GCM-AES-XPB-128 Key and calculated ICV (example)	35
Table C-18	GCM-AES-XPB-256 Key and calculated ICV (example)	36
Table C-19	Unprotected frame (example)	37
Table C-20	Integrity protected frame (example)	37
Table C-23	GCM-AES-XPB-128 Key and calculated ICV (example)	38
Table C-24	GCM-AES-XPB-256 Key and calculated ICV (example)	39
Table C-25	Unprotected frame (example)	40
Table C-26	Confidentiality protected frame (example)	40
Table C-27	GCM-AES-128 Key, Secure Data, and ICV (example)	41
Table C-28	GCM-AES-256 Key, Secure Data, and ICV (example)	42
Table C-29	GCM-AES-XPB-128 Key, Secure Data, and ICV (example)	43
Table C-30	GCM-AES-XPB-256 Key, Secure Data, and ICV (example)	44
Table C-31	Unprotected frame (example)	45
Table C-32	Confidentiality protected frame (example)	45
Table C-35	GCM-AES-XPB-128 Key, Secure Data, and ICV (example)	46
Table C-36	GCM-AES-XPB-256 Key, Secure Data, and ICV (example)	47
Table C-37	Unprotected frame (example)	48
Table C-38	Confidentiality protected frame (example)	48
Table C-41	GCM-AES-XPB-128 Key, Secure Data, and ICV (example)	49
Table C-42	GCM-AES-XPB-256 Key, Secure Data, and ICV (example)	50
Table C-43	Unprotected frame (example)	51
Table C-44	Confidentiality protected frame (example)	51
Table C-47	GCM-AES-XPB-128 Key, Secure Data, and ICV (example)	52
Table C-48	GCM-AES-XPB-256 Key, Secure Data, and ICV (example)	53

IEEE Standard for Local and metropolitan area networks— Media Access Control (MAC) Security Amendment 2: Extended Packet Numbering

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

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

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 ~~strike~~ (to remove old material) and under (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.

3. Definitions

Change the definition of packet number as follows:

3.27 packet number (PN): A monotonically increasing value ~~used to uniquely identify a MACsec frame in the sequence of frames transmitted using an SA~~ that is guaranteed unique for each MACsec frame transmitted using a given SAK.

Insert the following definition, in the appropriate collating order:

3.xx Short Secure Channel Identifier (SSCI): A 32-bit value, managed by the key agreement protocol, that is unique for each SCI within the context of all SecYs using a given SAK.

4. Abbreviations and acronyms

Insert the following abbreviation(s), in the appropriate collating sequence:

MKA MACsec Key Agreement protocol

SSCI Short SCI

7. Principles of secure network operation

Change the note that appears in 7.1 as follows:

NOTE—An SC can be required to last for many years without interruption, since interrupting the MAC Service can cause client protocols to re-initialize and recalculate aggregations, spanning trees, and routes (for example). An SC lasts through a succession of SAs, each using a new SAK, to defend against a successful attack on a key while it is still in use. In contrast it is desirable to use a new SAK at periodic intervals to defend against a successful attack on a key while it is still in use. In addition, the MACsec protocol (Clause 8 and Clause 9) only allows ~~a limited number of~~ $2^{32}-1$ frames to be protected with a single key unless a Cipher Suite that supports extended packet numbering is used. Since 2^{32} minimum-sized IEEE 802.3 frames can be sent in approximately 5 min at 10 Gb/s, this can force the use of a new SA.

7.1.2 Secure Channel (SC)

Change the first paragraph of 7.1.2 as follows:

Each SecY transmits frames conveying secure MAC Service requests 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.

8. MAC Security Protocol (MACsec)

Change 8.2.7 as follows:

8.2.7 Key exchange and maintenance

The KaY delivers ~~transmit and receive~~ SAKs via the LMI (10.7.26).

The KaY creates, manages, and maintains one CA that connects two or more KaYs and their corresponding SecYs. The KaY creates and maintains all of the point-to-multipoint SCs and SAs between itself and all the stations within the CA (10.2, 10.7.11–10.7.15, 10.7.20–10.7.23). An SAK delivered by a given KaY is not shared with any other KaY, is not used by the given KaY to support more than one CA, and once used to support an SA for a given SC is not re-used to support any other SA for that SC. A KaY can (and in the MACsec Key Agreement protocol (MKA) specified in IEEE Std 802.1X-2010 does) use a single SAK to support multiple SCs within a CA. It is recognized that two SAKs can have the same value with a probability of no less than 1 in 2^{keysize} when generated by an approved pseudorandom function.

~~The KaY accepts indication of impending exhaustion of the SA from the SecY via the LMI.~~

The KaY monitors the use of PNs by the SecY via the LMI in order to identify impending exhaustion of the transmitting SA (10.7.22). IEEE Std 802.1X-2010 specifies the distribution of a fresh SAK when the value of the PN exceeds that of the constant PendingPNExhaustion (0xC000 0000 for 32-bit PNs). If extended packet numbering (a 64-bit PN) is used in conjunction with IEEE Std 802.1X-2010, PendingPNExhaustion takes the value 0xC000 0000 0000 0000.

The KaY accepts indications that one SA is retired and a new one is started, in other words, when an overlapping pair of SAs is provisioned and the SecY switches from one to the next (10.7.20).

~~The KaY accepts an indication from the SecY that a PN is close to exhaustion.~~

8.3 MACsec operation

Change the fourth through seventh paragraphs as follows, renumbering the existing NOTE in 8.3 as NOTE 1:

On transmission, the frame is first assigned to an SA (7.1.3), identified locally by its Association Number (AN) (see 7.1.3, 9.6). 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 32 least significant bits of the PN are encoded in the SecTAG (the SCI can be omitted for point-to-point CAs) 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).

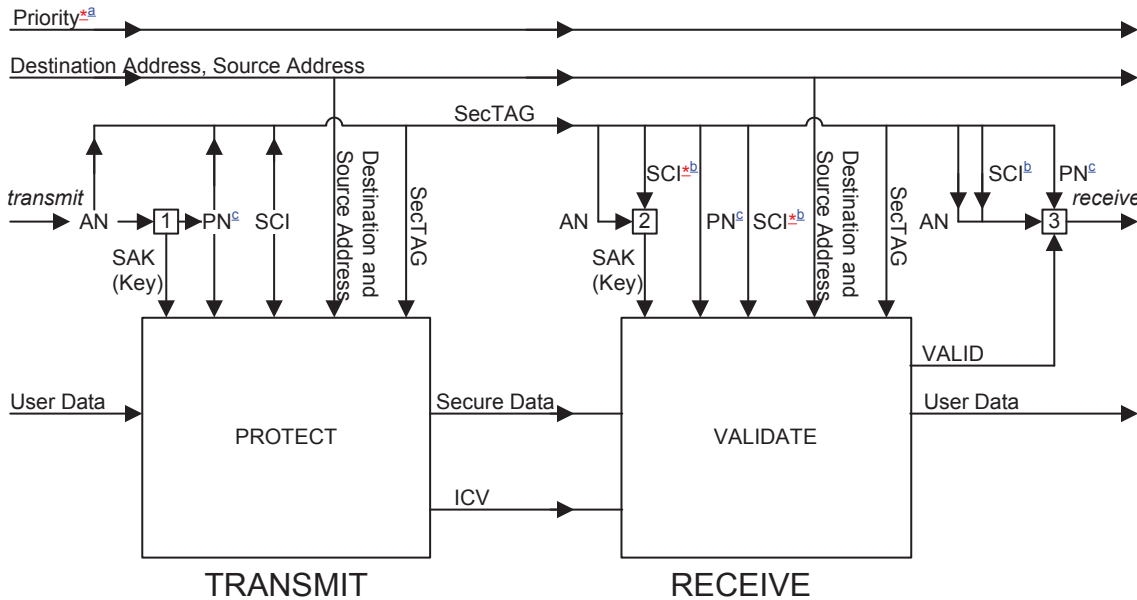
The protection function (14.1) of the Current Cipher Suite is presented with the SAK, the PN and SCI, the destination and source addresses of the frame together with the octets of the SecTAG, and the User Data. It returns the Secure Data and the ICV.

On receipt of a MACsec frame, the AN, SCI, PN, and SL field (if present) are extracted from the SecTAG. If ~~(if the CA is point-to-point and the SCI is not present, the value previously communicated by the KaY will be used).~~ The AN and SCI are used to assign the frame to an SA, and hence to identify the SAK. If the Current Cipher Suite uses extended packet numbering (a 64-bit PN), the full PN is recovered (as specified in 10.6) using the 32 least significant bits conveyed in the SecTAG and the 32 most significant bits used in a prior successful frame validation.

The validation function of the Current Cipher Suite is presented with the SAK, the PN and SCI, the destination and source addresses of the frame together with the octets of the SecTAG, and the Secure Data and ICV. If the integrity of the frame has been preserved and the User Data can be successfully decoded from the Secure Data, a VALID indication and the octets of the User Data are returned.

NOTE 2—If the Current Cipher Suite supports extended packet numbering, the PN comprises 64 bits. The validation functions of the GCM-AES-XPN Cipher Suites (14.7, 14.8) use the SCI to identify a 32 bit SSCI supplied by the KaY and construct a 96-bit IV using that SSCI and the PN.

Change Figure 8-2 as follows:



- ^{*a} Priority can be changed by media access method or receiving system and is not protected
- ^{*b} The SCI is extracted from the SCI field of the SecTAG if present. A value conveyed by key agreement (point-to-point only) is used otherwise.
- ^c The SecTAG carries only the least significant 32 bits of the PN. When a 64 bit PN (extended packet numbering) is used, the most significant 32 bits are recovered on receipt, and the complete 64 bit PN is presented to PROTECT, VALIDATE, and the replay check.
- Functions
- 1 Lookup Key and next PN for transmit SA identified by AN
 - 2 Lookup Key PN for receive SA identified by SCI, AN
 - 3 Discard if received frame not VALID. Discard if replay check of PN for receive SA identified by SCI, AN fails. Updated replay check.

Figure 8-2—MACsec operation

9. Encoding of MACsec protocol data units

Replace Figure 9-2 with the following:

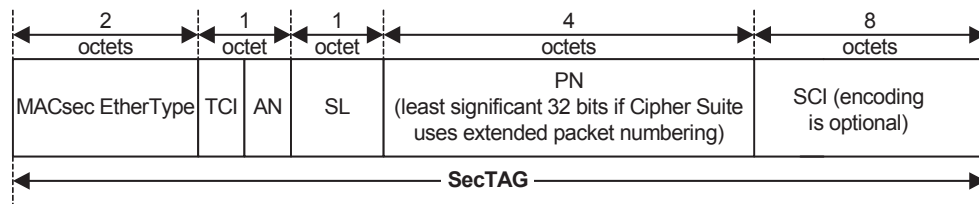


Figure 9-2—SecTAG format

Change 9.8 as follows:

9.8 Packet Number (PN)

The 32 least significant bits of the PN ~~is~~ are encoded in octets 5 through 8 of the SecTAG to

- a) Provide a unique IV PDU for all MPDUs transmitted using the same SA
- b) Support replay protection

NOTE 1—The IV used by the Default Cipher Suite GCM-AES-128 (14.5) and the GCM-AES-256 Cipher Suite (14.6) comprises the SCI (even if the SCI is not transmitted in the SecTAG) and ~~the a 32-bit~~ PN. Subject to proper unique MAC Address allocation procedures, the SCI is a globally unique identifier for a SecY. To satisfy the IV uniqueness requirements of CTR mode of operation, a fresh key is used before PN values are reused.

NOTE 2—If the Current Cipher Suite provides extended packet numbering, i.e. uses a 64-bit PN, the 32 least significant bits of the PN are conveyed in this SecTAG field and the 32 most significant bits are recovered on receipt as specified in 10.6. The IV used by the GCM-AES-XPB Cipher Suites (14.7, 14.8) is constructed from a 32-bit SSCI distributed by key agreement protocol and unique for each SCI within the scope of the CA (and hence within potential users of the same SAK) and the 64-bit non-repeating PN.

9.9 Secure Channel Identifier (SCI)

Change the last paragraph of 9.9 as follows:

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. In the point-to-point 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 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.