INTERNATIONAL STANDARD

ISO/IEC/ IEEE 8802-1AE

First edition
2013-12-01

AMENDMENT 2
2015-05-01

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

Part 1AE: **Media access control (MAC) security**

AMENDMENT 2: Extended Packet Numbering

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 2

Reference number
ISO/IEC/IEEE 8802-1AE:2013/Amd.2:2015(E)

ISO copyright office
Case postale 56
CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
E-mail inmail@iec.ch
Web www.iec.ch

Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York
NY 10016-5997, USA
E-mail stds.ipr@ieee.org
Web 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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.

The main task of ISO/IEC JTC 1 is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is called to the possibility that implementation of this standard may require the use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. ISO/IEEE is not responsible for identifying essential patents or patent claims for which a license may be required, for conducting inquiries into the legal validity or scope of patents or patent claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance or a Patent Statement and Licensing Declaration Form, 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 ISO or the IEEE Standards Association.

Amendment 1 to ISO/IEC/IEEE 8802-11 was prepared by the LAN/MAN Standards Committee of the IEEE Computer Society (as IEEE Std 802.11ae-2012). It was adopted by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*, in parallel with its approval by the ISO/IEC national bodies, under the “fast-track procedure” defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE. IEEE is responsible for the maintenance of this document with participation and input from ISO/IEC national bodies.

(blank page)

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

12 February 2013

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

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

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 7 February 2013

IEEE-SA Standards Board

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

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

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 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.

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-XPN-128 and GCM-AES-XPN-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
Yafan An
Ting Ao
Peter Ashwood-Smith
Christian Boiger
Brad Booth
Paul Bottorff
Rudolf Brandner
Craig Carlson
Xin Chang
Weiying Cheng
Paul Congdon
Diego Crupnicoff
Rodney Cummings
Claudio Desanti
Donald Eastlake, III
Janos Farkas
Donald Fedyk
Norman Finn
Andre Fredette
Geoffrey Garner
Anoop Ghanwani
Franz Goetz
Mark Gravel
Eric Gray
Yingjie Gu
Craig Gunther
Stephen Haddock
Hitoshi Hayakawa
Markus Jochim
Michael Johas Teener
Girault Jones
Daya Kamath
Hal Keen
Srikanth Keesara
Yongbum Kim
Philippe Klein
Oliver Kleineberg
Jeff Lynch
Ben Mack-Crane
David Martin
John Messenger
John Morris
Eric Multanen
David Olsen
Donald Pannell
Mark Pearson
Joseph Pelissier
Rene Raeber
Karen T. Randall
Josef Roese
Dan Romascanu
Jessy Rouyer
Ali Sajassi
Panagiotis Saltsidis
Koichiro Seto
Rakesh Sharma
Takeshi Shimizu
Kevin Stanton
PatriciaThaler
Jeremy Touve
Maarten Vissers
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
Arthur Astrin
Nancy Bravin
William Byrd
Radhakrishna Canchi
Juan Carreon
Keith Chow
Charles Cook
Rodney Cummings
Ray Davis
Sourav Dutta
Donald Fedyk
Yukihiro Fujimoto
Devon Gayle
Eric Gray
Randall Groves
Michael Gundlach
Chris Guy
Russell Housley
Noriyuki Ikeuchi
Atsushi Ito
Tony Jeffree
Michael Johas Teener
Shinkyo Kaku
Piotr Karocki
Stuart Kerry
Yongbum Kim
Bruce Kraemer
Geoff Ladwig
Shen Loh
William Lumpkins
Greg Luri
Elvis Maculuba
Jonathon Mclendon
Michael S. Newman
Charles Ngethe
Satoshi Obara
Yoshihiro Ohba
Karen Randall
Maximilian Riegel
Benjamin Rolfe
Randall Safier
Bartien Sayogo
Mick Seaman
Gil Shultz
Dorothy Stanley
Thomas Starai
Walter Struppler
Joseph Tardo
William Taylor
Patricia Thaler
Solomon Trainin
Dmitri Varsanofiev
Prabodh Varshney
John Vergis
Hung-Yu Wei
Brian Weis
Oren Yuen
Daidi Zhong

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

Contents

Figures

Tables

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 ~~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.

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).

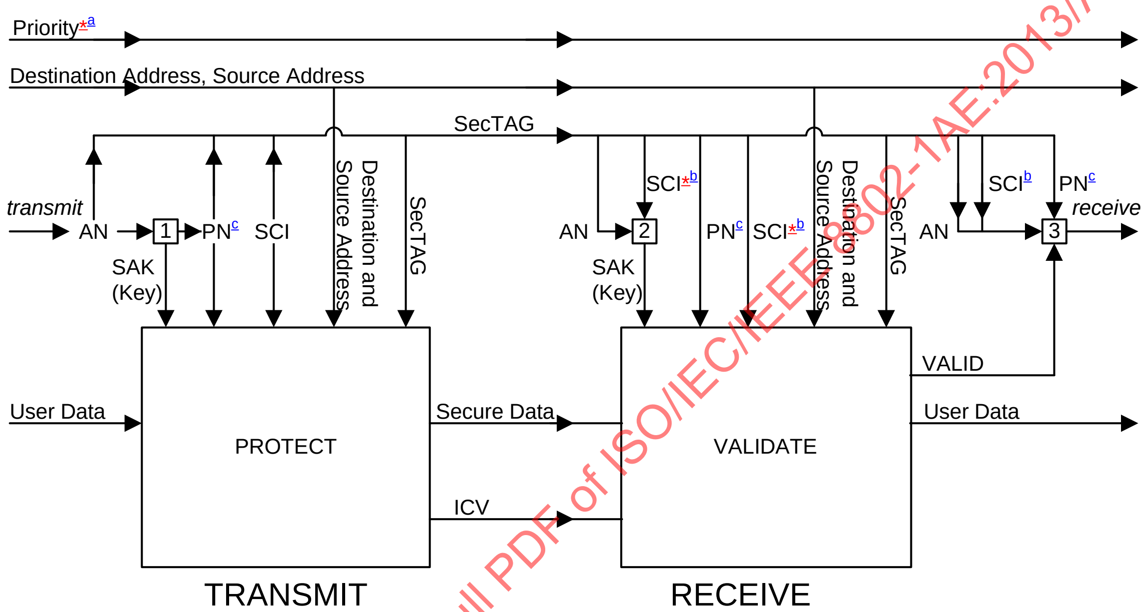
The protection function (14.1) of the Current Cipher Suite is presented with the SAK, the PN and SCI, the destination and source addresses of the frame together with the octets of the SecTAG, and the User Data. It returns the Secure Data and the ICV.

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:

.

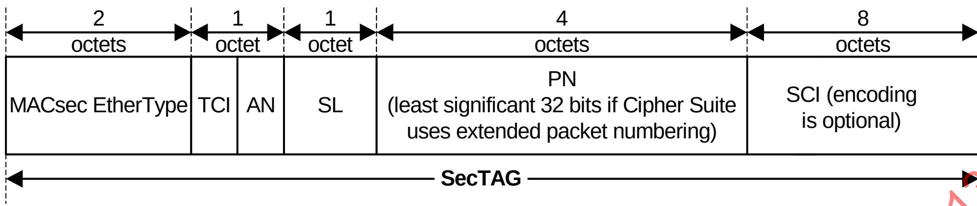


Figure 9-2—SecTAG format

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-XPN 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.

10. Principles of MAC Security Entity (SecY) operation

Change 10.5 as follows:

10.5 Secure frame generation

For each transmit request at the Controlled Port, the Secure Frame Generation process

a) Assigns the frame to an SA (10.5.1)

b) Assigns the nextPN variable for that SA to be used as the value of the PN ~~in the SecTAG~~ for that protected frame (10.5.2)

c) Encodes the octets of the SecTAG including the least significant 32 bits of the PN in the PN field (10.5.3)

d) Provides the protection function (14.1, 10.5.4) of the Current Cipher Suite with

   1) The SA Key (SAK)

   2) The SCI for the SC used by the SecY to transmit

   3) The PN

   4) The SecTAG

   5) The sequence of octets that compose the User Data

e) Receives the following parameters from the Cipher Suite protection operation

   6) The sequence of octets that compose the Secure Data

   7) The ICV

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 management control protectFrames is False, the preceding steps are omitted, an identical transmit request is made to the Transmit Multiplexer, and the OutPktsUntagged counter incremented.

NOTE—This model of operation supports the externally observable behavior that can result when the Cipher Suite implementation calculates the Secure Data and ICV parameters for a number of frames in parallel, and the responses to protection and validation requests are delayed. Transmitted frames are not misordered.

Change 10.5.2 as follows:

10.5.2 Transmit PN assignment

The frame's PN is set to the value of nextPN for the SA, and nextPN is incremented. If the nextPN variable for the encodingSA is zero (or 2^{32} if the Current Cipher Suite does not support extended packet numbering, 2^{64} if it does) and the protectFrames control is set, MAC_Operational transitions to False for the Controlled Port and frames are neither accepted or delivered. The initial value of nextPN is set by the KaY via the LMI prior to use of the SA, and its current value can be read both while and after the SA is used to transmit frames. The value of nextPN can be read, but not written, by network management.

Change Figure 10-5 as follows:

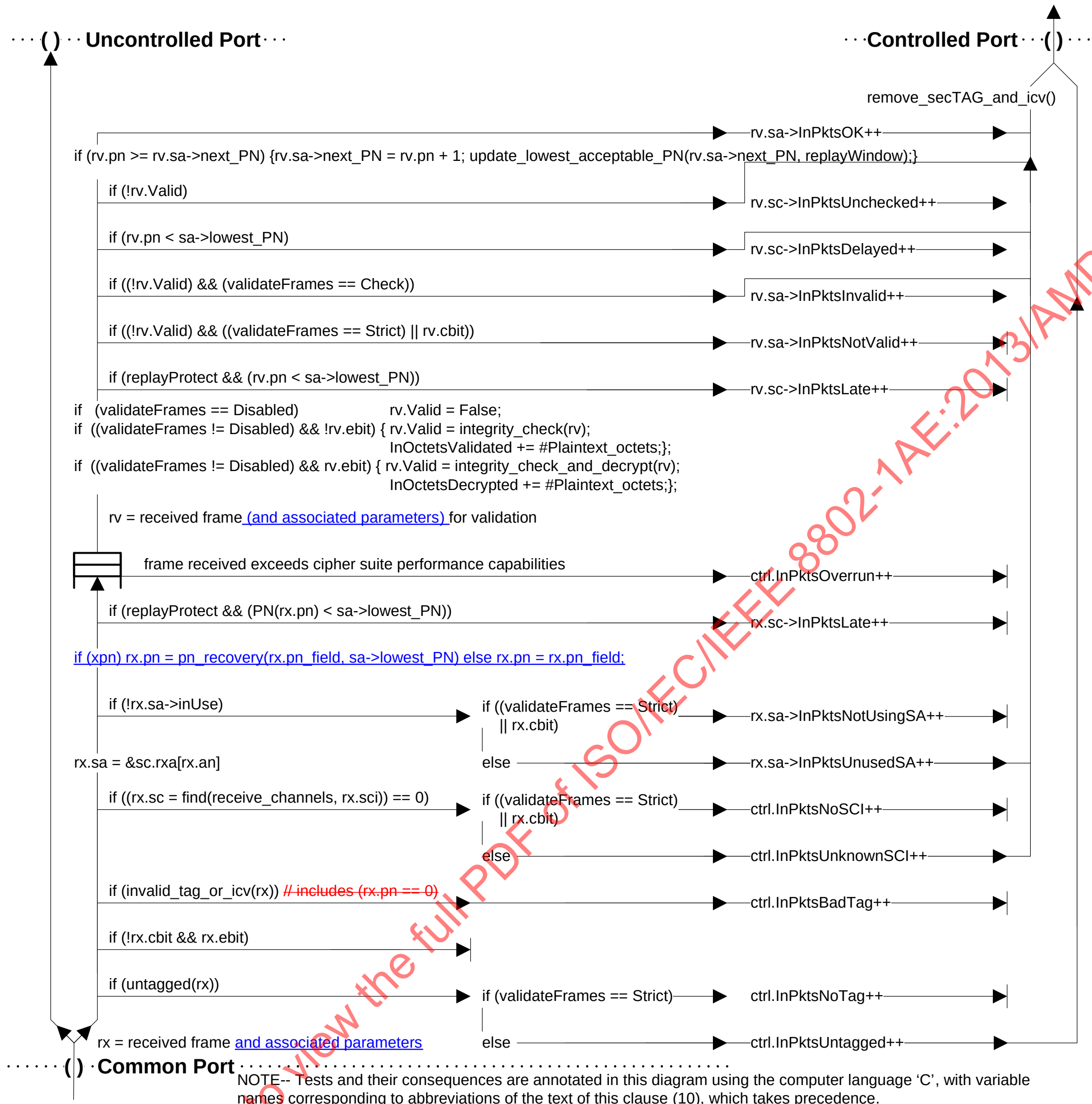


Figure 10-5—Management controls and counters for secure frame verification

10.6 Secure frame verification

Change the initial paragraphs of 10.6 as follows:

For each receive indication from the Receive Demultiplexer, the Secure Frame Verification process

a) Examines the user data for a SecTAG
b) Validates frames with a SecTAG as specified in 9.12
c) Extracts and decodes the SecTAG as specified in 9.3 through 9.9
d) Extracts the User Data and ICV as specified in 9.10 and 9.11
e) Assigns the frame to an SA (10.6.1)
f) Recovers the PN and p~~P~~erforms a preliminary replay check against the last validated PN for the SA (10.6.2)

g) Provides the validation function (14.1, 10.6.3) of the Current Cipher Suite with
   1) The SA Key (SAK)
   2) The SCI for the SC used by the SecY to transmit
   3) The PN
   4) The SecTAG
   5) The sequence of octets that compose the Secure Data
   6) The ICV
h) Receives the following parameters from the Cipher Suite validation operation
   7) A Valid indication, if the integrity check was valid and the User Data could be recovered
   8) The sequence of octets that compose the User Data
i) Updates the replay check (10.6.4)
j) Issues an indication to the Controlled Port with the DA, SA, and priority of the frame as received from the Receive Demultiplexer, and the User Data provided by the validation operation (10.6.5).

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. Figure 10-5 summarizes the operation of management controls and counters.

Change 10.6.2 and insert Table 10-1, renumbering and updating references to the subsequent table, as follows:

10.6.2 PN recovery and p~~P~~reliminary replay check

If the Current Cipher Suite does not use extended packet numbering, i.e., the PN comprises 32 bits, the value of the PN is that decoded from the 4 octet PN field in the SecTAG of the received frame (9.1, 9.8).

If the Current Cipher Suite supports extended packet numbering, the PN comprises 64 bits. The least significant 32 bits of the PN are those decoded from the PN field in the SecTAG of the received frame. The 32 most significant bits of the PN are recovered for each received frame by applying the assumption that they have remained unchanged since their use in the frame with the lowest acceptable PN—unless the most significant of the 32 least significant bits of the lowest acceptable PN is set and the corresponding bit of the received PN is not set, in which case the value of the 32 most significant bits of the PN is one more than the value of the 32 most significant bits of the lowest acceptable PN. Table 10-1 provides examples.

Table 10-1—Extended packet number recovery (examples)

SecTAG PN field value	0x 2A2B 5051
Lowest acceptable PN	0x 0000 0007 1234 DEF0
PN	0x 0000 0007 2A2B 5051
SecTAG PN field value	0x 2A2B 5051
Lowest acceptable PN	0x 0000 0007 8234 DEF0
PN	0x 0000 0008 2A2B 5051
SecTAG PN field value	0x 9A2B 5051
Lowest acceptable PN	0x 0000 0007 8234 DEF0
PN	0x 0000 0007 9A2B 5051
SecTAG PN field value	0x 9A2B 5051
Lowest acceptable PN	0x 0000 0007 2234 DEF0
PN	0x 0000 0007 9A2B 5051

The recovered PN value is not guaranteed to be the same as that used by the transmitter to protect the frame, but all PN values in the range lowest acceptable PN to lowest acceptable PN plus 2^{31} will be recovered correctly. If the recovered PN value is incorrect, the Cipher Suite validation operation will not return VALID and the frame will be discarded if validateFrames is Strict (10.6.5, 10.7.8). A recovered PN value is used to update the lowest acceptable PN only if the validation operation with that PN value returns VALID.

NOTE 1— For a discussion of the PN recovery algorithm, its incidental properties and alternatives, that goes beyond the normative requirements of this standard, see The XPN recovery algorithm [B17].

NOTE 2—If a large number of successive frames were to be lost (2^{30}–1, corresponding to approximately 9 seconds of full utilization of a 400 Gb/s link by minimum sized Ethernet frames) subsequent receipt of MACsec frames might fail to establish a correct PN value. MKA, the MACsec Key Agreement protocol specified in IEEE Std 802.1X and its amendments communicates the value of the high order bits periodically to recover from this eventuality.

If replayProtect control is enabled and the PN recovered from ~~of~~ the received frame is less than the lowest acceptable packet number (see 10.6.5) for the SA, the frame is discarded and the InPktsLate counter incremented.

NOTE 3—If the SC is supported by a network that includes buffering with priority queueing, such as a provider bridged network, delivered frames can be reordered.

Change 10.6.5 as follows:

10.6.5 Receive indication

If the received frame is marked as invalid, and the validateFrames control is Strict or the C bit in the SecTAG was set, the frame is discarded and the InPktsNotValid counter incremented. Otherwise the frame is delivered to the Controlled Port, and the appropriate counter incremented as follows:

a) If the frame is not valid and validateFrames is set to Check, InPktsInvalid, otherwise
b) If the received PN is less than the lowest acceptable PN (treating a 32-bit PN value of zero as 2^{32}, and a 64-bit PN value of zero as 2^{64}), InPktsDelayed, otherwise
c) If the frame is not valid, InPktsUnchecked, otherwise
d) InPktsOK

If the PN for the frame was equal to or greater than the nextPN variable for the SA and the frame is valid, nextPN is set to the value for the received frame, incremented by one. The lowest acceptable PN variable is set to the greater of its existing value and the value of nextPN minus the replayWindow variable.

NOTE—The lowest acceptable packet number can also be set or incremented by the KaY to ensure timely delivery.

10.7 SecY management

Insert the following NOTE after the second paragraph (beginning "Figure 10-6 illustrates the management information ...") of 10.7:

NOTE—Figure 10-6 omits parameters specific to extended packet numbering [used by some but not all Cipher Suites (14.7, 14.8)] and not accessible by network management. Specifically: 1) the createReceiveSA(), ReceiveSA(), createTransmitSA(), and TransmitSA() procedures all take an additional SSCI parameter, whose value becomes a parameter of the created SA; 2) the install_key() procedure takes an additional Salt parameter, whose value becomes an inaccessible parameter of the Data_key object. These parameters are specified in 10.7.13, 10.7.21, and 10.7.26.

Change 10.7.8 as follows:

10.7.8 Frame verification controls

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

a) validateFrames, taking values of 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.

Change 10.7.13 and 10.7.14 as follows:

10.7.13 Receive SA creation

A receive SA is created for an existing SC on request from the KaY, with the following parameters:

a) The association number, AN, for the SA
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) 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 validation operations) to the instance of the Current Cipher Suite identified by the referenced SAK. A receive SA will not be created if the SSCI supplied duplicates that for a different SCI (for the same SAK, for transmission or reception).

Frame verification statistics (10.7.9) for the SA are set to zero when the SA is created. Any prior SA with the same AN for the SC 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 each SA to be distinguished from any previously created for the same SCI and 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 follows. The KaY with numerically greatest SCI uses the SSCI value 0x00000001, the KaY with the next to the greatest SCI uses the SSCI value 0x00000002, and so on. This assignment procedure is not necessarily applicable to any other key agreement protocol.

NOTE—At any given time (when configured by a KaY using the MACsec Key Agreement protocol (MKA) specified in IEEE Std 802.1X) this and other Cipher Suites (including those specified in 14.5, 14.6, and 14.7) use the same SAK for all SAs (each with a different SCI) within the same CA and with the same AN. MKA guarantees that each KaY that uses a given SAK has a unique SCI, and these SCIs are present in every MKPDU that conveys a (key-wrapped) SAK.The number of SCIs (and hence the number of SSCIs) is ultimately limited by the maximum number of current members in a group CA that MKA can support (less than 100) but is likely to be further limited by the port-based network control application (see IEEE Std 802.1X Clause 7).

10.7.14 Receive SA status

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

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

Change 10.7.21 and 10.7.22, as follows:

10.7.21 Transmit SA creation

An SA is created for the 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.

10.7.22 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 (~~10.6, 10.6.5~~ 10.5, 10.5.2)

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

Change 10.7.26, 10.7.27, and 10.7.28 as follows:

10.7.26 SAK creation

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

a) The SAK value
b) A Key Identifier, 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, 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.

10.7.27 SAK status

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

a) transmits, True if the key has been installed for transmission, i.e., can be used ~~referenced~~ by a transmit SA
b) receives, True if the key has been installed for reception, i.e., can be used ~~referenced~~ by a receive SA
c) createdTime, the system time when the SAK record was created

~~10.7.28 SAK controls~~

~~The KaY uses the following parameters to control the use of each SAK:~~

~~a) enableTransmit, install the key for transmission~~
~~b) enableReceive, install the key for reception~~

13. Management protocol

Insert a new subclause 13.7 as follows:

13.7 Use of the MIB with extended packet numbering

Although originally defined prior to the specification of Cipher Suites using extended packet numbering, the MAC Security MIB is applicable both when such Cipher Suites are implemented and when they are not. A conformant implementation with extended packet numbering Cipher Suites also includes the Default Cipher Suite (to provide interoperability) and retention of the existing MIB minimizes any disruption to deployed network management. The MIB accommodates the addition and identification of new Cipher Suites.

The addition of the SSCI (10.7.13, 10.7.21) and Salt (10.7.26) parameters in support of extended packet numbering does not require any addition to the MIB. Determination of the Salt and allocation of the SSCI are matters for key agreement protocol, and are monitored (if at all) by the management arrangements for that protocol.

The MIB contains a number of 32-bit statistic counters for each active SA (10.7.14, 10.7.22, 10.7.9). As an active SA is replaced by its successor these statistics are accumulated into a 64-bit counter for the parent SC, and each of the statistics reported by management for an SC comprise the sum of past accumulated values and the active SA values. If the Current Cipher Suite uses a 32-bit PN, none of these 32-bit counters can overflow. If the Current Cipher Suite uses extended packet numbering, each SC statistic is incremented each time a counter for a corresponding SA statistic overflows and wraps. Each of the counters for an SA statistic thus holds the 32 least significant bits of the value accumulated since the creation of the SA. The createdTime for the SA remains unchanged when and if any counter wraps. Similarly the 32-bit SA object for the nextPN reports the 32 least significant bits of that parameter. The relevant MIB objects are as follows:

```
secyTxSANextPN                  Unsigned32
secyRxSANextPN                  Unsigned32
secyTxSAStatsProtectedPkts      Counter32
secyTxSAStatsEncryptedPkts      Counter32
secyRxSAStatsUnusedSAPkts       Counter32
secyRxSAStatsNoUsingSAPkts      Counter32
secyRxSAStatsNotValidPkts       Counter32
secyRxSAStatsInvalidPkts        Counter32
secyRxSAStatsOKPkts             Counter32
```


14. Cipher Suites

Change the introductory text of Clause 14 as follows:

A Cipher Suite is an interoperable specification of cryptographic algorithms together with the values of parameters (for example, key size) to be used by those algorithms. Specification of the cryptographic functions required by MAC Security in terms of Cipher Suites increases interoperability by providing a clear default and a limited number of alternatives.

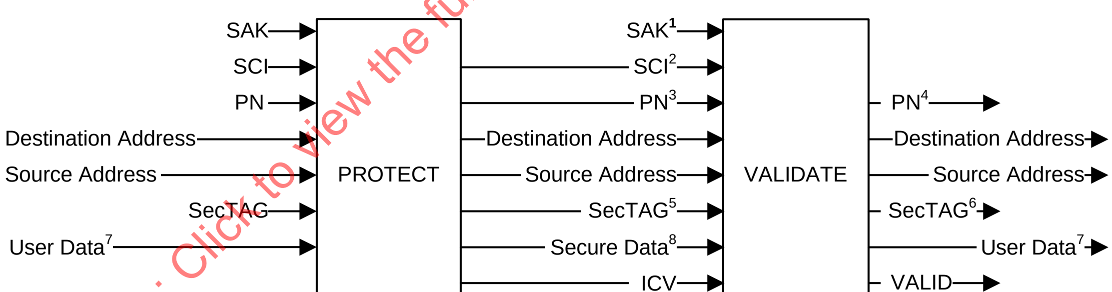
This clause specifies

a) Terms that describe the use of each Cipher Suite by the MAC Security Entity (SecY).
b) Capabilities required of each Cipher Suite.
c) Requirements this standard places on Cipher Suite specification.
d) Mandatory and optional Cipher Suites for use in conjunction with this standard.
e) Criteria for the use of additional Cipher Suites in conjunction with MAC Security for implementations for which a claim of conformance to this standard is made.

NOTE—The choice and combination of cryptographic methods is notorious for the introduction of unexpected security exposures. Each Cipher Suite ~~is~~ uses an algorithm or combination of algorithms whose interactions have been studied by the professional security community. Each Cipher Suite specification (14.5–14.8) in this clause comprises the necessary combination (e.g., concatenation of named strings) and mapping of parameters and parameter names used in the other clauses of this standard to the parameters and parameter names used by a public established standard that specifies the cryptographic operations.

14.1 Cipher Suite use

Change footnote2 and footnote 3 in Figure 14-1 as follows:



[1] The SAK to be used on receipt of the frame is identified by the SCI and the AN.

[2] 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.
In the GCM-AES-128 and GCM-AES-256 Cipher Suites (14.5, 14.6), the SCI is always included in the IV parameter whether included in the SecTAG or not (and thus always contributes to the ICV). However the Cipher Suite parameter A includes the SCI if and only if the SCI is included in the SecTAG.
In the GCM-AES-XPN-128 and GCM-AES-XPN-256 Cipher Suites (14.7, 14.8), the {SCI, SAK} tuple (or equivalently the SA) identifies the SSCI (conveyed by key agreement) that is included in the IV parameter, and the Cipher Suite parameter A includes the SCI if and only if the SCI is included in the SecTAG.

[3] The 32 least significant bits of the PN are ~~is~~ conveyed in the SecTAG

[4] The validated PN can be used for replay protection.

[5] All the transmitted octets of the SecTAG are protected, including the optional SCI field if present

[6] The validated received SecTAG contains bits of the TCI, and optionally the SCI, these can be used for service multiplexing (11.7).

[7] The length, in octets, of the User Data is conveyed by the User Data parameter, and is protected by Cipher Suite operation.

[8] The length, in octets, of the Secure Data is conveyed by the MACsec frame, unless it is short, when it is conveyed by the SL parameter in the SecTAG TCI

Figure 14-1—Cipher Suite Protect and Validate operations

Change the fourth paragraph of 14.1 as follows:

The PN (Packet Number, 3.27, 8.3) is a ~~32-bit~~ number that is never zero, is incremented each time a protect request is made for a given SCI, and is never repeated for an SCI unless the SAK is changed. The size of the PN depends on the Cipher Suite, and is 32 bits unless otherwise specified. Cipher Suites that provide extended packet numbering use a 64-bit PN. Irrespective of the size of the PN, only the least significant 32 bits are conveyed in the SecTAG. If extended packet numbering is used, the most significant 32 bits are recovered for each received frame as specified in 10.6.2.

14.2 Cipher Suite capabilities

Change bullet b) as follows:

b) Provide integrity and confidentiality (if specified) for at least ~~up to~~ 2^{32}– 1 invocations, each with a different PN, without requiring a fresh SAK.

14.4 Cipher Suite conformance

Change Table 14-1 as follows:

Table 14-1—MACsec Cipher Suites

Cipher Suite # Identifier	Cipher Suite Name	Services provided		Mandatory/Optional	Defining Clause
		Integrity without confidentiality	Integrity and confidentiality		
00-80-C2-00-01-00-00-01	GCM–AES–128	Yes	Yes	Mandatory	14.5
00-80-C2-00-01-00-00-02	GCM-AES-256	Yes	Yes	Optional	14.6
00-80-C2-00-01-00-00-03	GCM–AES–XPN-128	Yes	Yes	Optional	14.7
00-80-C2-00-01-00-00-04	GCM-AES-XPN-256	Yes	Yes	Optional	14.8

Change 14.6 as follows:

14.6 GCM–AES–256

GCM-AES-256 uses the Galois/Counter Mode of operation with the AES-256 symmetric block cipher, as specified in this clause by reference to the terms *K, IV, A, P, C, T* used in NIST SP 800-38D.

K is the 256-bit SAK. The 64 most significant bits of the 96-bit *IV* are the octets of the SCI, encoded as a binary number (9.1). The 32 least significant bits of the 96-bit *IV* are the octets of the PN, encoded as a binary number (9.1). *T* is the ICV, and is 128 bits long. When the bit-strings *A*, *P*, and *C* are specified in terms of octet strings, earlier octets compose earlier bits, and more significant bits in each octet are earlier.

NOTE—The bit strings obtained by transforming MAC Address and data octets using these rules do not correspond to IEEE 802.3 “wire order” for frame transmission.

When ~~the Default~~ this Cipher Suite is used for Integrity Protection

— *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG and User Data concatenated in that order.
— *P* is null.
— The Secure Data is the octets of the User Data, without modification.

When ~~the Default~~ this Cipher Suite is used for Confidentiality Protection without a confidentiality offset

— *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG concatenated in that order.
— *P* is the octets of the User Data.
— The Secure Data is *C*.

When ~~the Default~~ 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 concatenated in that order.
— *P* is the remaining octets of the User Data.
— The Secure Data is the first confidentialityOffset octets of the User Data concatenated with *C*, in that order.

Insert a new subclause 14.7 as follows:

14.7 GCM–AES–XPN-128

Each instance of the GCM-AES-XPN-128 Cipher Suite, i.e., the protection and validation capabilities created for a given SAK at the request of the KaY (10.7.26, Figure 10-6) maintains an instance of the following parameter as specified in 10.7.26:

a) Salt, a 96-bit value distributed by key agreement protocol to all members of the CA.

and an instance of the following parameter for each SCI, as supplied by the KaY when an SA that uses the SCI and the given SAK is created (10.7.13, 10.7.21):

b) SSCI, a 32-bit value that is unique for each SCI using a given SAK.

NOTE 1—The maximum number of SSCIs for a given SAK is thus limited by the maximum number of SCIs (equivalently, by the maximum number of simultaneous members in a CA as requirements placed on the KaY (8.2.7) prohibit the use of the same SAK in multiple CAs). A claim of conformance to this standard requires a statement of the maximum number of receive SCs supported (5.3m, A.5, A.12, A.13). The total number of SCIs will be one greater (to include the transmit SC) or two greater [for an EPON OLT supporting an SCB (Clause 12.)]. Whether and to what extent the same SAK is used by different SAs (each with a different SCI, and hence a different SSCI for that SAK) depends on the key agreement protocol, and the number of members in a CA will also be ultimately limited by the capabilities of the key agreement protocol. The practical requirements of the port-based network control application (see IEEE Std 802.1X Clause 7) are likely to be more limited.

GCM-AES-XPN-128 uses the Galois/Counter Mode of operation with the AES-128 symmetric block cipher, as specified in this clause by reference to the terms *K, IV, A, P, C, T* used in NIST SP 800-38D.

K is the 128-bit SAK. The 32 most significant bits of the 96-bit *IV* are the octets of the SSCI for the SCI, encoded as a binary number (9.1) and exclusive-or’d with the 32 most significant bits of the Salt. The 64 least significant bits of the 96-bit *IV* are the octets of the PN, encoded as a binary number (9.1) and exclusive-or'd with the 64 least significant bits of the Salt. *T* is the ICV, and is 128 bits long. When the bit-strings *A*, *P*, and *C* are specified in terms of octet strings, earlier octets compose earlier bits, and more significant bits in each octet are earlier.

NOTE 2—The bit strings obtained by transforming MAC Address and data octets using these rules do not correspond to IEEE 802.3 "wire order" for frame transmission.

When this Cipher Suite is used for Integrity Protection

— *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG and User Data concatenated in that order.
— *P* is null.
— The Secure Data is the octets of the User Data, without modification.

When this Cipher Suite is used for Confidentiality Protection without a confidentiality offset

— *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG concatenated in that order.
— *P* is the octets of the User Data.
— The Secure Data is *C*.

This Cipher Suite does not provide Confidentiality Protection with a confidentiality offset.

Insert a new subclause 14.8 as follows:

14.8 GCM–AES–XPN-256

Each instance of the GCM-AES-XPN-256 Cipher Suite, i.e., the protection and validation capabilities created for a given SAK at the request of the KaY (10.7.26, Figure 10-6) maintains an instance of the following parameter as specified in 10.7.26:

a) Salt, a 96-bit value distributed by key agreement protocol to all members of the CA.

and an instance of the following parameter for each SCI, as supplied by the KaY when an SA that uses the SCI and the given SAK is created (10.7.13, 10.7.21):

b) SSCI, a 32-bit value that is unique for each SCI using a given SAK.

NOTE 1—The maximum number of SSCIs for a given SAK is thus limited by the maximum number of SCIs (equivalently, by the maximum number of simultaneous members in a CA as requirements placed on the KaY (8.2.7) prohibit the use of the same SAK in multiple CAs). A claim of conformance to this standard requires a statement of the maximum number of receive SCs supported (5.3m, A.5, A.12, A.13). The total number of SCIs will be one greater (to include the transmit SC) or two greater [for an EPON OLT supporting an SCB (Clause 12.)]. Whether and to what extent the same SAK is used by different SAs (each with a different SCI, and hence a different SSCI for that SAK) depends on the key agreement protocol, and the number of members in a CA will also be ultimately limited by the capabilities of the key agreement protocol. The practical requirements of the port-based network control application (see IEEE Std 802.1X Clause 7) are likely to be more limited.

GCM-AES-XPN-256 uses the Galois/Counter Mode of operation with the AES-256 symmetric block cipher, as specified in this clause by reference to the terms *K, IV, A, P, C, T* used in NIST SP 800-38D.

K is the 256-bit SAK. The 32 most significant bits of the 96-bit *IV* are the octets of the SSCI for the SCI, encoded as a binary number (9.1) and exclusive-or'd with the 32 most significant bits of the Salt. The 64 least significant bits of the 96-bit *IV* are the octets of the PN, encoded as a binary number (9.1), and exclusive-or'd with the 64 least significant bits of the Salt. *T* is the ICV, and is 128 bits long. When the bit-strings *A*, *P*, and *C* are specified in terms of octet strings, earlier octets compose earlier bits, and more significant bits in each octet are earlier.

NOTE 2—The bit strings obtained by transforming MAC Address and data octets using these rules do not correspond to IEEE 802.3 “wire order” for frame transmission.

When this Cipher Suite is used for Integrity Protection

— *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG and User Data concatenated in that order.
— *P* is null.
— The Secure Data is the octets of the User Data, without modification.

When this Cipher Suite is used for Confidentiality Protection without a confidentiality offset

— *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG concatenated in that order.
— *P* is the octets of the User Data.
— The Secure Data is *C*.

This Cipher Suite does not provide Confidentiality Protection with a confidentiality offset.

Annex A

(normative)

PICS Proforma

A.13 Additional variant Cipher Suite capabilities

Change Item CSV-12 as follows:

Does the Cipher Suite provide protection for at least ~~up to~~ $2^{32}–1$ invocations without requiring a fresh SAK?

Annex B

(informative)

Bibliography

Change the text of this annex as follows, updating cross-references as necessary:

[B1] Fowler, M., "UML Distilled: A Brief Guide to the Standard Object Modeling Language, Third Edition," Pearson Education Inc., Boston, 2004, ISBN 0-321-19368-7.

[B2] Generation of Deterministic Initialization Vectors (IVs) and Nonces, McGrew, D., August 2012.[1]

[B3] ~~IEEE 100,~~ *The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition.

[B4] IETF RFC 2279, UTF-8, a Transformation format of ISO 10646, Yergeau, F., January 1998.

[B5] IETF RFC 2406, IP Encapsulating Security Payload (ESP), Kent, S., Atkinson, R., November 1998.

[B6] IETF RFC 2737, Entity MIB (Version 2), McCloghrie, K., Bierman, A., December 1999.

[B7] IETF RFC 3232, Assigned Numbers: RFC 1700 is Replaced by an On-line Database, Reynolds, J., January 2002.

[B8] IETF RFC 3410, Introduction and Applicability Statements for Internet-Standard Management Framework, Case, J., Mundy, R., Partain, D., and Stewart, B., December 2002.

[B9] IETF RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, Harrington, D., Presuhn, R., and Wijnen, B., December 2002.

[B10] IETF RFC 4302, IP Authentication Header, Kent, S., December 2005.

[B11] IETF RFC 4303, IP Encapsulating Security Payload (ESP), Kent, S., December 2005. Appendix A.

[B12] IETF RFC 5116, An Interface and Algorithms for Authenticated Encryption, McGrew, D., January 2008.

[B13] ISO 6937-2: 1983, Information processing—Coded character sets for text communication—Part 2: Latin alphabetic and non-alphabetic graphic characters.[2]

[B14] ISO/IEC TR 11802-2: 1997, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Technical reports and guidelines—Part 2: Standard Group MAC addresses.

[B15] The Galois/Counter Mode of Operation (GCM), David A. McGrew and J. Viega. May 31, 2005.[3]

[1]Available at http://tools.ietf.org/html/draft-mcgrew-iv-gen-02

[2]ISO and ISO/IEC documents are available from the ISO Central Secretariat, 1 rue de Varembé, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

[3]A prior revision of this document was the normative reference for GCM in IEEE Std 802.1AE-2006, but has been superseded by NIST SP 800-38D for that purpose. It does contain additional background information, and can be downloaded from http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-revised-spec.pdf

[B16] The Security and Performance of the Galois/Counter Mode (GCM) of Operation. D. McGrew and J. Viega. Proceedings of INDOCRYPT ’04, Springer-Verlag, 2004. [4]

~~[B17] McGrew, D. A., Viega, J., “The Security and Performance of the Galois/Counter Mode (GCM) of Operation (Full Version), http://eprint.iacr.org/2004/193.pdf.~~

[B17] The XPN recovery algorithm, Mick Seaman. June 2012.[5]

[4]Available from the IACR Cryptology ePrint Archive: Report 2004/193, http://eprint.iacr.org/2004/193
[5]Available at http://www.ieee802.org/1/files/public/docs2012/aebw-seaman-xpn-recovery-0612-v02.pdf

Annex C

(informative)

MACsec Test Vectors

Change the third paragraph of the initial text of this annex, as follows:

Test cases are provided for ~~both~~ the Default Cipher Suite (GCM-AES-128, 14.5), ~~and~~ GCM-AES-256 (14.6), GCM-AES-XPN-256 (14.7), and GCM-AES-XPN-256 (14.8). The notation used in this annex is that specified in Clause 14 (Cipher Suites) and NIST SP 800-38D. Fields in the MACsec header are specified in Clause 9. Summaries of the computation and intermediate outputs are provided.

C.1 Integrity protection (54-octet frame)

Change the initial paragraphs and tables of C.1 as follows:

The MAC Destination Address, MAC Source Address, and MAC Service Data Unit (MSDU, User Data) of a MAC Service data request and a corresponding data indication are shown in Table C-1. These comprise the octets of an unprotected frame when concatenated in the order given (with the addition of any media dependent additional fields such as padding). The User Data shown includes the IP EtherType.

Table C-1—Unprotected frame (example)

Field	Value
MAC DA	D6 09 B1 F0 56 63
MAC SA	7A 0D 46 DF 99 8D
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 00 01

The MAC Security TAG (SecTAG) comprises the MACsec EtherType, the TCI, the AN, the SL, the PN (32 least significant bits for Cipher Suites using extended packet numbering), and the (optional) SCI. The PN differs for each protected frame transmitted with any given SAK (*K*) and has been arbitrarily chosen (for this and in other examples) as have the other parameter values. The fields of the protected frame are shown (in the order transmitted) in Table C-2.

Table C-2—Integrity protected frame (example)

Field	Value
MAC DA	D6 09 B1 F0 56 63
MAC SA	7A 0D 46 DF 99 8D
MACsec EtherType	88 E5
TCI and AN	22
SL	2A
PN	B2 C2 84 65
SCI	12 15 35 24 C0 89 5E 81
Secure Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 00 01
ICV	Cipher Suite and Key (SAK) dependent (see Table C-3~~ and~~, Table C-4, Table C-5, and Table C-6)

~~The GCM parameter *A*, the additional data to be authenticated, is formed by concatenating the MAC DA, the MAC SA, the SecTAG, and the User Data. This input is then processed through the authentication only operation of the GCM module. The SCI and the PN are concatenated (in that order) to form the 96-bit *IV* used by GCM. The computed GCM parameter *T* is the ICV.~~

Change C.1.1 and C.1.2 as follows:

C.1.1 GCM-AES-128 (54-octet frame integrity protection)

Table C-3 specifies an arbitrary 128-bit key (SAK), and the ICV generated by the GCM-AES-128 Cipher Suite when that key is used in conjunction with the frame field data of Table C-2. The GCM parameter *A*, the additional data to be authenticated, is formed by concatenating the MAC DA, the MAC SA, the SecTAG, and the User Data. This input is then processed through the authentication only operation of the GCM module. The SCI and the PN are concatenated (in that order) to form the 96-bit *IV* used by GCM. The computed GCM parameter *T* is the ICV. Details of the computation follow the table.

Table C-3—GCM-AES-128 Key and calculated ICV (example)

Field	Value
Key (SAK)	AD7A2BD03EAC835A6F620FDCB506B345
ICV	F0 94 78 A9 B0 90 07 D0 6F 46 E9 B6 A1 DA 25 DD

```
key size = 128 bits
P:     0 bits
A:     560 bits
IV:    96 bits
ICV:   128 bits
K:     AD7A2BD03EAC835A6F620FDCB506B345
P:
A:     D609B1F056637A0D46DF998D88E5222A
       B2C2846512153524C0895E8108000F10
       1112131415161718191A1B1C1D1E1F20
       2122232425262728292A2B2C2D2E2F30
       313233340001
IV:    12153524C0895E81B2C28465
GCM-AES Authentication
H:     73A23D80121DE2D5A850253FCF43120E
Y[0]:  12153524C0895E81B2C2846500000001
E(K,Y[0]): EB4E051CB548A6B5490F6F11A27CB7D0
X[1]:  6B0BE68D67C6EE03EF7998E399C01CA4
X[2]:  5AABADF6D7806EC0CCCB028441197B22
X[3]:  FE072BFE2811A68AD7FDB0687192D293
X[4]:  A47252D1A7E09B49FB356E435DBB4CD0
X[5]:  18EBF4C65CE89BF69EFB4981CEE13DB9
GHASH(H,A,C): 1BDA7DB505D8A165264986A703A6920D
C:
T:     F09478A9B09007D06F46E9B6A1DA25DD
```

C.1.2 GCM-AES-256 (54-octet frame integrity protection)

Table C-4 specifies an arbitrary 256-bit key (SAK), and the ICV generated by the GCM-AES-256 Cipher Suite when that key is used in conjunction with the frame field data of Table C-2. The GCM parameter *A*, the additional data to be authenticated, is formed by concatenating the MAC DA, the MAC SA, the SecTAG,and the User Data. This input is then processed through the authentication only operation of the GCM module. The SCI and the PN are concatenated (in that order) to form the 96-bit *IV* used by GCM. The computed GCM parameter *T* is the ICV. Details of the computation follow the table.

Table C-4—GCM-AES-256 Key and calculated ICV (example)

Field	Value
Key (SAK)	E3C08A8F06C6E3AD95A70557B23F7548 3CE33021A9C72B7025666204C69C0B72
ICV	2F 0B C5 AF 40 9E 06 D6 09 EA 8B 7D 0F A5 EA 50

```
key size = 256 bits
P:      0 bits
A:      560 bits
IV:     96 bits
ICV:    128 bits
K:      E3C08A8F06C6E3AD95A70557B23F7548
        3CE33021A9C72B7025666204C69C0B72
P:
A:      D609B1F056637A0D46DF998D88E5222A
        B2C2846512153524C0895E8108000F10
        1112131415161718191A1B1C1D1E1F20
        2122232425262728292A2B2C2D2E2F30
        313233340001
IV:     12153524C0895E81B2C28465
GCM-AES Authentication
H:      286D73994EA0BA3CFD1F52BF06A8ACF2
Y[0]:   12153524C0895E81B2C2846500000001
E(K,Y[0]): 714D54FDCFCEE37D5729CDDAB383A016
X[1]:   BA7C26F578254853CF321281A48317CA
X[2]:   2D0DF59AE78E84ED64C3F85068CD9863
X[3]:   702DE0382ABF4D42DD62B8F115124219
X[4]: DAED65979342F0D155BFDFE362132078
X[5]: 9AB4AFD6344654B2CD23977E41AA18B3
GHASH(H,A,C): 5E4691528F50E5AB5EC346A7BC264A46
C:
T: 2F0BC5AF409E06D609EA8B7D0FA5EA50
```


Insert new subclauses C.1.3, C.1.4 as follows, renumbering subsequent tables as required:

C.1.3 GCM-AES-XPN-128 (54-octet frame integrity protection)

Table C-5 specifies an arbitrary value for the SSCI, the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), a 96-bit Salt, and 128-bit key (SAK), with the ICV generated by the GCM-AES-XPN-128 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-2. The GCM parameter *A*, the additional data to be authenticated, is formed by concatenating the MAC DA, the MAC SA, the SecTAG, and the User Data. This input is then processed through the authentication only operation of the GCM module. The 32 most significant bits of the 96-bit *IV* are the octets of the SSCI, encoded as a binary number (9.1) and exclusive-or'd with the 32 most significant bits of the Salt. The 64 least significant bits of the 96-bit *IV* are the octets of the PN, encoded as a binary number (9.1) and exclusive-or'd with the 64 least significant bits of the Salt. The computed GCM parameter *T* is the ICV. Details of the computation follow the table.

Table C-5—GCM-AES-XPN-128 Key and calculated ICV (example)

Field	Value
SSCI	7A30C118
PN (ms 32 bits)	B0DF459C
Salt	E630E81A48DE86A21C66FA6D
Key (SAK)	AD7A2BD03EAC835A6F620FDCB506B345
ICV	17 FE 19 81 EB DD 4A FC 50 62 69 7E 8B AA 0C 23

```
key size = 128 bits
P:     0 bits
A:     560 bits
IV:    96 bits
ICV:   128 bits
K:     AD7A2BD03EAC835A6F620FDCB506B345
P:
A:     D609B1F056637A0D46DF998D88E5222A
       B2C2846512153524C0895E8108000F10
       1112131415161718191A1B1C1D1E1F20
       2122232425262728292A2B2C2D2E2F30
       313233340001
IV:    9C002902F801C33EAEA47E08
GCM-AES Authentication
H:     73A23D80121DE2D5A850253FCF43120E
Y[0]:  9C002902F801C33EAEA47E0800000001
E(K,Y[0]): 0C246434EE05EB99762BEFD9880C9E2E
X[1]:  6B0BE68D67C6EE03EF7998E399C01CA4
X[2]:  5AABADF6D7806EC0CCCB028441197B22
X[3]:  FE072BFE2811A68AD7FDB0687192D293
X[4]:  A47252D1A7E09B49FB356E435DBB4CD0
X[5]:  18EBF4C65CE89BF69EFB4981CEE13DB9
GHASH(H,A,C): 1BDA7DB505D8A165264986A703A6920D
C:
T:     17FE1981EBDD4AFC5062697E8BAA0C23
```

C.1.4 GCM-AES-XPN-256 (54-octet frame integrity protection)

Table C-6 specifies an arbitrary value for the SSCI, the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), a 96-bit Salt, and 256-bit key (SAK), with the ICV generated by the GCM-AES-XPN-256 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-2. The GCM parameter *A*, the additional data to be authenticated, is formed by concatenating the MAC DA, the MAC SA, the SecTAG, and the User Data. This input is then processed through the authentication only operation of the GCM module. The 32 most significant bits of the 96-bit *IV* are the octets of the SSCI, encoded as a binary number (9.1) and exclusive-or'd with the 32 most significant bits of the Salt. The 64 least significant bits of the 96-bit *IV* are the octets of the PN, encoded as a binary number (9.1) and exclusive-or'd with the 64 least significant bits of the Salt. The computed GCM parameter *T* is the ICV. Details of the computation follow the table.

Table C-6—GCM-AES-XPN-256 Key and calculated ICV (example)

Field	Value
SSCI	7A30C118
PN (ms 32 bits)	B0DF459C
Salt	E630E81A48DE86A21C66FA6D
Key (SAK)	E3C08A8F06C6E3AD95A70557B23F7548 3CE33021A9C72B7025666204C69C0B72
ICV	4D BD 2F 6A 75 4A 6C F7 28 CC 12 9B A6 93 15 77

```
key size = 256 bits
P:      0 bits
A:      560 bits
IV:     96 bits
ICV:    128 bits

K:      E3C08A8F06C6E3AD95A70557B23F7548
        3CE33021A9C72B7025666204C69C0B72

P:

A:      D609B1F056637A0D46DF998D88E5222A
        B2C2846512153524C0895E8108000F10
        1112131415161718191A1B1C1D1E1F20
        2122232425262728292A2B2C2D2E2F30
        313233340001

IV:     9C002902F801C33EAEA47E08

GCM-AES Authentication
H:      286D73994EA0BA3CFD1F52BF06A8ACF2
Y[0]:   9C002902F801C33EAEA47E0800000001
E(K,Y[0]): 13FBBE38FA1A895C760F543C1AB55F31
X[1]:   BA7C26F578254853CF321281A48317CA
X[2]:   2D0DF59AE78E84ED64C3F85068CD9863
X[3]:   702DE0382ABF4D42DD62B8F115124219
X[4]:   DAED65979342F0D155BFDFE362132078
X[5]:   9AB4AFD6344654B2CD23977E41AA18B3
GHASH(H,A,C): 5E4691528F50E5AB5EC346A7BC264A46

C:

T:      4DBD2F6A754A6CF728CC129BA6931577
```


C.2 Integrity protection (60-octet frame)

Change the initial paragraphs and tables of C.2 as follows:

The MAC Destination Address, MAC Source Address, and MAC Service Data Unit (MSDU, User Data) of a MAC Service data request and a corresponding data indication are shown in ~~Table C-5~~ Table C-7. These comprise the octets of an unprotected frame when concatenated in the order given (with the addition of any media dependent additional fields such as padding). The User Data shown includes the IP EtherType.

Table C-7—Unprotected frame (example)

Field	Value
MAC DA	E2 01 06 D7 CD 0D
MAC SA	F0 76 1E 8D CD 3D
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 00 03

The MAC Security TAG comprises the MACsec EtherType, the TCI, the AN, the SL, the PN. In this example the optional SCI has been omitted. The fields of the protected frame are shown (in the order transmitted) in ~~Table C-6~~ Table C-8.

Table C-8—Integrity protected frame (example)

Field	Value
MAC DA	E2 01 06 D7 CD 0D
MAC SA	F0 76 1E 8D CD 3D
MACsec EtherType	88 E5
TCI and AN	40
SL	00
PN	76 D4 57 ED
Secure Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 00 03
ICV	Cipher Suite and Key (SAK) dependent (see ~~Table C-7 and Table C-8~~ Table C-9, Table C-10, Table C-11, and Table C-12)

Insert new subclauses C.2.3, C.2.4 as follows, renumbering subsequent tables as required:

C.2.3 GCM-AES-XPN-128 (60-octet frame integrity protection)

Table C-11 specifies arbitrary values for the SSCI, the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), 96-bit Salt, and 128-bit key (SAK), with the ICV generated by the GCM-AES-XPN-128 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-7.

Table C-11—GCM-AES-XPN-128 Key and calculated ICV (example)

Field	Value
SSCI	7A30C118
PN (ms 32 bits)	B0DF459C
Salt	E630E81A48DE86A21C66FA6D
Key (SAK)	071B113B0CA743FECCCF3D051F737382
ICV	AB C4 06 85 A3 CF 91 1D 37 87 E4 9D B6 A7 26 5E

```
key size = 128 bits
P:      0 bits
A:      544 bits
IV:     96 bits
ICV:    128 bits
K:      071B113B0CA743FECCCF3D051F737382
P:
A:      E20106D7CD0DF0761E8DCD3D88E54000
        76D457ED08000F101112131415161718
        191A1B1C1D1E1F202122232425262728
        292A2B2C2D2E2F303132333435363738
        393A0003
IV:     9C002902F801C33E6AB2AD80
GCM-AES Authentication
H:      E4E01725D724C1215C7309AD34539257
Y[0]:   9C002902F801C33E6AB2AD8000000001
E(K,Y[0]): 5BE02ED3987877610007A055C2EEA9A6
X[1]:   8DAD4981E33493018BB8482F69E4478C
X[2]:   5B0BFA3E67A3E080CB60EA3D523C734A
X[3]:   051F8D267A68CF88748E56C5F64EF503
X[4]:   4187F1240DB1887F2A92DDAB8903A0F6
X[5]:   C7D64941A90F02FA9FCDECC083B4B276
GHASH(H,A,C): F02428563BB7E67C378044C874498FF8
C:
T:      ABC40685A3CF911D3787E49DB6A7265E
```


C.2.4 GCM-AES-XPN-256 (60-octet frame integrity protection)

Table C-12 specifies arbitrary values for the SSCI, the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), a 96-bit Salt, and 256-bit key (SAK), with the ICV generated by the GCM-AES-XPN-256 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-7.

Table C-12—GCM-AES-XPN-256 Key and calculated ICV (example)

Field	Value
SSCI	7A30C118
PN (ms 32 bits)	B0DF459C
Salt	E630E81A48DE86A21C66FA6D
Key (SAK)	691D3EE909D7F54167FD1CA0B5D76908 1F2BDE1AEE655FDBAB80BD5295AE6BE7
ICV	AC 21 95 7B 83 12 AB 3C 99 AB 46 84 98 79 C3 F3

```
key size = 256 bits
P:     0 bits
A:     544 bits
IV:    96 bits
ICV:   128 bits
K:     691D3EE909D7F54167FD1CA0B5D76908
       1F2BDE1AEE655FDBAB80BD5295AE6BE7
P:
A:     E20106D7CD0DF0761E8DCD3D88E54000
       76D457ED08000F101112131415161718
       191A1B1C1D1E1F202122232425262728
       292A2B2C2D2E2F303132333435363738
       393A0003
IV:    9C002902F801C33E6AB2AD80
GCM-AES Authentication
H:     1E693C484AB894B26669BC12E6D5D776
Y[0]:  9C002902F801C33E6AB2AD8000000001
E(K,Y[0]): 1EE16A68524D7D515FE89FEC1E11B4D6
X[1]:  20107B262134C35B60499E905C532004
X[2]:  D7A468F455F09F947884E35A2C80CD7F
X[3]:  A82D607070F2E4470FD94C0EECA9FCC1
X[4]:  03C3C8725883EB355963BD53B515C82D
X[5]:  8FF6F0311DDE274FFA936965C0C905B4
GHASH(H,A,C): B2C0FF13D15FD66DC643D96886687725
C:
T: AC21957B8312AB3C99AB46849879C3F3
```

C.3 Integrity protection (65-octet frame)

Change the initial paragraphs and tables of C.3 as follows:

The MAC Destination Address, MAC Source Address, and MAC Service Data Unit (MSDU, User Data) of a MAC Service data request and a corresponding data indication are shown in ~~Table C-9~~Table C-13. These comprise the octets of an unprotected frame when concatenated in the order given (with the addition of any media dependent additional fields such as padding). The User Data shown includes the IP EtherType.

Table C-13—Unprotected frame (example)

Field	Value
MAC DA	84 C5 D5 13 D2 AA
MAC SA	F6 E5 BB D2 72 77
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 00 05

The MAC Security TAG comprises the MACsec EtherType, the TCI, the AN, the SL, the PN, and the (optional) SCI. The fields of the protected frame are shown (in the order transmitted) in ~~Table C-10~~Table C-14.

Table C-14—Integrity protected frame (example)

Field	Value
MAC DA	84 C5 D5 13 D2 AA
MAC SA	F6 E5 BB D2 72 77
MACsec EtherType	88 E5
TCI and AN	23
SL	00
PN	89 32 D6 12
SCI	7C FD E9 F9 E3 37 24 C6
Secure Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 00 05
ICV	(see ~~Table C-11 and Table C-12~~ Table C-15, Table C-16, Table C-17, and Table C-18)

Insert new subclauses C.3.3, C.3.4 as follows, renumbering subsequent tables as required:

C.3.3 GCM-AES-XPN-128 (65-octet frame integrity protection)

Table C-17 specifies arbitrary values for the SSCI, the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), 96-bit Salt, and 128-bit key (SAK), with the ICV generated by the GCM-AES-XPN-128 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-13.

Table C-17—GCM-AES-XPN-128 Key and calculated ICV (example)

Field	Value
SSCI	7A30C118
PN (ms 32 bits)	B0DF459C
Salt	E630E81A48DE86A21C66FA6D
Key (SAK)	013FE00B5F11BE7F866D0CBBC55A7A90
ICV	67 85 59 B7 E5 2D B0 06 82 E3 B8 30 34 CE BE 59

```
key size = 128 bits
P:     0 bits
A:     648 bits
IV:    96 bits
ICV:   128 bits

K:     013FE00B5F11BE7F866D0CBBC55A7A90

P:

A:     84C5D513D2AAF6E5BBD2727788E52300
       8932D6127CFDE9F9E33724C608000F10
       1112131415161718191A1B1C1D1E1F20
       2122232425262728292A2B2C2D2E2F30
       3132333435363738393A3B3C3D3E3F00
       05

IV:    9C002902F801C33E95542C7F

GCM-AES Authentication
H:     EB28DCB361EE1110F98CA0C9A07C88F7
Y[0]:  9C002902F801C33E95542C7F00000001
E(K,Y[0]): 0857C6B6369497B8879CB7FC8F177E1C
X[1]:  279344E391DB8834EFA68FD3F1BA5CD8
X[2]:  DC35B123F4D387BBB076D0822BD60816
X[3]:  8AB3B52963CC15C9C2DB3E4C801CB65A
X[4]:  CAB6A261225F42578E6B86ABA9F0DD18
X[5]:  6ABDBB3ECAC0458F116A82AA0DAC563F
X[6]:  8F39EF45985C691E35814202B6BB6EF6
GHASH(H,A,C): 6FD29F01D3B927BE057F0FCCBBD9C045

C:

T:     678559B7E52DB00682E3B83034CEBE59
```

C.3.4 GCM-AES-XPN-256 (65-octet frame integrity protection)

Table C-18 specifies arbitrary values for the SSCI, the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), a 96-bit Salt, and 256-bit key (SAK), with the ICV generated by the GCM-AES-XPN-256 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-13.

Table C-18—GCM-AES-XPN-256 Key and calculated ICV (example)

Field	Value
SSCI	7A30C118
PN (ms 32 bits)	B0DF459C
Salt	E630E81A48DE86A21C66FA6D
Key (SAK)	83C093B58DE7FFE1C0DA926AC43FB360 9AC1C80FEE1B624497EF942E2F79A823
ICV	84 BA C8 E5 3D 1E A3 55 A5 C7 D3 34 84 0A E9 62

```
key size = 256 bits
P:     0 bits
A:     648 bits
IV:    96 bits
ICV:   128 bits
K:     83C093B58DE7FFE1C0DA926AC43FB360
       9AC1C80FEE1B624497EF942E2F79A823
P:
A:     84C5D513D2AAF6E5BBD2727788E52300
       8932D6127CFDE9F9E33724C608000F10
       1112131415161718191A1B1C1D1E1F20
       2122232425262728292A2B2C2D2E2F30
       3132333435363738393A3B3C3D3E3F00
       05
IV:    9C002902F801C33E95542C7F
GCM-AES Authentication
H:     D03D3B51FDF2AACB3A165D7DC362D929
Y[0]:  9C002902F801C33E95542C7F00000001
E(K,Y[0]): 032500E383A7A99F250344CAD546A331
X[1]:  22C28F4DF8D09267EA3E11F019F5932C
X[2]:  3D02CFE5FC6A8A9E65B8FFD63E525083
X[3]:  78466AE4A3490819A08645DDC95B143B
X[4]:  6FE4921A6F0A1D5DD90A100A40206142
X[5]:  C880DEC2FF2C44F8AD611692AF6D1069
X[6]:  CF4D709A4D020BA876F4371BAA788444
GHASH(H,A,C): 879FC806BEB90ACA80C497FE514C4A53
C:
T: 84BAC8E53D1EA355A5C7D334840AE962
```


C.4 Integrity protection (79-octet frame)

Change the initial paragraphs and tables of C.4 as follows:

The MAC Destination Address, MAC Source Address, and MAC Service Data Unit (MSDU, User Data) of a MAC Service data request and a corresponding data indication are shown in ~~Table C-13~~ Table C-19. These comprise the octets of an unprotected frame when concatenated in the order given (with the addition of any media dependent additional fields such as padding). The User Data shown includes the IP EtherType.

Table C-19—Unprotected frame (example)

Field	Value
MAC DA	68 F2 E7 76 96 CE
MAC SA	7A E8 E2 CA 4E C5
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 00 07

The MAC Security TAG comprises the MACsec EtherType, the TCI, the AN, the SL, and the PN. In this example the optional SCI has been omitted. The fields of the protected frame are shown (in the order transmitted) in ~~Table C-14~~ Table C-20.

Table C-20—Integrity protected frame (example)

Field	Value
MAC DA	68 F2 E7 76 96 CE
MAC SA	7A E8 E2 CA 4E C5
MACsec EtherType	88 E5
TCI and AN	41
SL	00
PN	2E 58 49 5C
Secure Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 00 07
ICV	(see ~~Table C-15 and Table C-16~~ Table C-21, Table C-22, Table C-23, and Table C-24)

Insert new subclauses C.4.3, C.4.4 as follows, renumbering subsequent tables as required:

C.4.3 GCM-AES-XPN-128 (79-octet frame integrity protection)

Table C-23 specifies arbitrary values for the SSCI, the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), 96-bit Salt, and 128-bit key (SAK), with the ICV generated by the GCM-AES-XPN-128 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-19.

Table C-23—GCM-AES-XPN-128 Key and calculated ICV (example)

Field	Value
SSCI	7A30C118
PN (ms 32 bits)	B0DF459C
Salt	E630E81A48DE86A21C66FA6D
Key (SAK)	88EE087FD95DA9FBF6725AA9D757B0CD
ICV	D0 DC 89 6D C8 37 98 A7 9F 3C 5A 95 BA 3C DF 9A

```
key size = 128 bits
P:      0 bits
A:      696 bits
IV:     96 bits
ICV:    128 bits

K:      88EE087FD95DA9FBF6725AA9D757B0CD

P:

A:      68F2E77696CE7AE8E2CA4EC588E54100
        2E58495C08000F101112131415161718
        191A1B1C1D1E1F202122232425262728
        292A2B2C2D2E2F303132333435363738
        393A3B3C3D3E3F404142434445464748
        494A4B4C4D0007

IV:     9C002902F801C33E323EB331

GCM-AES Authentication
H:      AE19118C3B704FCE42AE0D15D2C15C7A
Y[0]:   9C002902F801C33E323EB33100000001
E(K,Y[0]): 051CB848B04A95168858F67B22FB45CD
X[1]:   CA0CAE2BEE8F19845DCB7FE3C5E713AB
X[2]:   5D3F9C7A3BC869457EA5FDFD404A415F
X[3]:   760E6A2873ACC0515D4901B5AC1C85E4
X[4]:   5A40A8425165E3D1978484F07AFC70D8
X[5]:   D9687630FC4436EE582A90A8E4AFC504
X[6]:   311CE361065F86403CDA5DB00798B961
GHASH(H,A,C): D5C03125787D0DB11764ACEE98C79A57

C:

T:      D0DC896DC83798A79F3C5A95BA3CDF9A
```


C.4.4 GCM-AES-XPN-256 (79-octet frame integrity protection)

Table C-24 specifies arbitrary values for the SSCI, the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), a 96-bit Salt, and 256-bit key (SAK), with the ICV generated by the GCM-AES-XPN-256 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-19.

Table C-24—GCM-AES-XPN-256 Key and calculated ICV (example)

Field	Value
SSCI	7A30C118
PN (ms 32 bits)	B0DF459C
Salt	E630E81A48DE86A21C66FA6D
Key (SAK)	4C973DBC7364621674F8B5B89E5C1551 1FCED9216490FB1C1A2CAA0FFE0407E5
ICV	04 24 9A 20 8A 65 B9 6B 3F 32 63 00 4C FD 86 7D

```
key size = 256 bits
P:      0 bits
A:      696 bits
IV:     96 bits
ICV:    128 bits

K:      4C973DBC7364621674F8B5B89E5C1551
        1FCED9216490FB1C1A2CAA0FFE0407E5

P:

A:      68F2E77696CE7AE8E2CA4EC588E54100
        2E58495C08000F101112131415161718
        191A1B1C1D1E1F202122232425262728
        292A2B2C2D2E2F303132333435363738
        393A3B3C3D3E3F404142434445464748
        494A4B4C4D0007

IV:     9C002902F801C33E323EB331

GCM-AES Authentication
H:      9A5E559A96459C21E43C0DFF0FA426F3
Y[0]:   9C002902F801C33E323EB33100000001
E(K,Y[0]): 35F6654C6A3A1D45F1D3C3E5C6B4CAC5
X[1]:   06A9019B44B76FFEC18978E8B21513E2
X[2]:   89A6401E39EAB6EE5B8159570139F54D
X[3]:   0A5E22BA54F282CE464C334D1AF598EF
X[4]:   4514D8A5C15E15CABC3D2A0E24FC758E
X[5]:   6F98DE3369B88F25AACBF3A993003E78
X[6]:   8183B21C0A932A2D5F598E1B2967564B
GHASH(H,A,C): 31D2FF6CE05FA42ECEE1A0E58A494CB8

C:

T: 04249A208A65B96B3F3263004CFD867D
```