IEEE P802.1AE/D3.5

Draft Standard for Local and Metropolitan Area Networks—

Media Access Control (MAC) Security

Sponsor

LAN MAN Standards Committee
of the
IEEE Computer Society

Prepared by the Security Task Group of IEEE 802.1

Abstract: This standard specifies how all or part of a network can be secured transparently to peer protocol entities that use the MAC Service provided by IEEE 802® LANs to communicate. MAC security (MACsec) provides connectionless user data confidentiality, frame data integrity, and data origin authenticity.
Keywords: local area networks, LANs, metropolitan area networks, MANs, security, MAC security confidentiality, integrity, data origin authenticity, port based network access control, MAC Service, MSAP, service access point, transparent bridging, MAC Bridges, port based network access control, authorized port, secure association.

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.

Use of an IEEE Standard is wholly voluntary. The 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 this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, 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 herein 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 five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, 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 this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received 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 interpretation requests except in those cases where the matter has previously received formal consideration.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Note: 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 with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

IEEE is the sole entity that may authorize the use of certification marks, trademarks, or other designations to indicate compliance with the materials set forth herein.

Editors' Foreword

<<Notes>>

<<Throughout this document, all notes such as this one, presented between angle braces, are temporary notes inserted by the Editors for a variety of purposes; these notes and the Editors' Foreword will all be removed prior to publication and are not part of the normative text.>>

<<Comments and participation in 802.1 standards development

Comments on this draft are encouraged. **PLEASE NOTE: All issues related to IEEE standards presentation style, formatting, spelling, etc. are routinely handled between the 802.1 Editor and the IEEE Staff Editors prior to publication, after balloting and the process of achieving agreement on the technical content of the standard is complete.** Readers are urged to devote their valuable time and energy only to comments that materially affect either the technical content of the document or the clarity of that technical content. Comments should not simply state what is wrong, but also what might be done to fix the problem.

Full participation in the development of this draft requires individual attendance at IEEE 802 meetings. Information on 802.1 activities, working papers, and email distribution lists etc. can be found on the 802.1 website:

http://ieee802.org/1/

Use of the email distribution list is not presently restricted to 802.1 members, and the working group has had a policy of considering ballot comments from all who are interested and willing to contribute to the development of the draft. Individuals not attending meetings have helped to identify sources of misunderstanding and ambiguity in past projects. Non-members are advised that the email lists exist primarily to allow the members of the working group to develop standards, and are not a general forum.

Comments on this document may be sent to the 802.1 email exploder, to the editors, or to the Chairs of the 802.1 Working Group and Link Security Task Group.

Allyn Romanow
Editor, P802.1AE MAC Security

+1 408 525 8836 (Tel)

Email: allyn@cisco.com

Frank Chao
Editor, MIB P802.1AE MAC Security

Email: fchao@cisco.com

Mick Seaman
Chair, 802.1 Link Security Task Group

Email:mick_seaman@ieee.org

Tony Jeffree
Chair, 802.1 Working Group
11A Poplar Grove
Sale
Cheshire
M33 3AX
UK
+44 161 973 4278 (Tel)
+44 161 973 6534 (Fax)
Email: tony@jeffree.co.uk

PLEASE NOTE: Comments whose distribution is restricted in any way cannot be considered, and may not be acknowledged.
>>

<<The draft text and accompanying information

This document currently comprises:

- A temporary cover page, preceding the Editors' Forewords. This cover page will be removed following working group approval of this draft, i.e. prior to sponsor ballot.
- IEEE boilerplate text.
- The editors' forewords, including this text. These include an unofficial and informal appraisal of history and status, introductory notes to each draft that summarize the progress and focus of each successive draft, and requests for comments and contributions on major issues.
- A title page for the proposed standard including an Abstract and Keywords. This title page will be retained following approval.
- IEEE boilerplate text (identical to the above).
- The introduction to this standard.
- A record of participants (not included in early drafts but added prior to publication).
- The proposed revision proper.
- Annexes A, B
- An Annex Z comprising the editors' discussion of issues. This annex will be deleted from the document prior to sponsor ballot.

During the early stages of draft development, 802.1 editors have a responsibility to attempt to craft technically coherent drafts from the resolutions of ballot comments and the other discussions that take place in the working group meetings. Preparation of drafts often exposes inconsistencies in editors instructions or exposes the need to make choices between approaches that were not fully apparent in the meeting. Choices and requests by the editors' for contributions on specific issues will be found in the editors' introductory notes to the current draft, at appropriate points in the draft, and in Annex Z. Significant discussion of more difficult topics will be found in the last of these.

The ballot comments received on each draft, and the editors' proposed and final disposition of comments, are part of the audit trail of the development of the standard and are available, along with all the revisions of the draft on the 802.1 website (for address see above).

>>

<<History and Scope

A PAR (Project Authorization Request) for this project was drafted at the June 2003 802.1 interim meeting, forwarded for SEC consideration by vote of the 802.1 Working Group at its closing plenary during the July 2003 meeting of P802, and approved by the IEEE-SA Standards Board on 11th September 2003, with the following Scope and Purpose:

Scope of Proposed Project:

> The scope of this project is to specify provision of connectionless user data confidentiality, frame data integrity, and data origin authenticity by media access independent protocols and entities that operate transparently to MAC Clients**. Key management and the establishment of secure associations is outside the scope but will be referenced by this project. **As specified in IEEE Standards 802, 802.2, 802.1D, 802.1Q, and 802.1X.

Purpose of Proposed Project:

> This standard will facilitate secure communication over publicly accessible LAN/MAN media for which security has not already been defined, and allow the use of IEEE Std 802.1X, already widespread and supported by multiple vendors, in additional applications.

A first draft, P802.1AE/D1, was the subject of a Task Group Ballot closing 4th January 2004, and ballot comments were discussed during the January 2004 802.1 interim meeting.>>

<<Introductory notes to the current draft

This editor's draft, P802.1AE/D3.5 makes changes based on the May meeting. There is no D3.4. The edits include:

Clarification of the two levels of conformance in cl 5.2.

Clarification language in 7.1 pertaining to KaY's behavior,

Statistics counters were reduced in version 3.1, but there it was not noted here in the editor's clause until now.

Clause 10.5.3 was modified to add the management variables useES and useSCB. They are needed to tell the SecY whether it should set the ES bit or whether it should set the SCB bit in the PDU. Clause 10.7.17 has useES and useSCB added to the list of Frame Generation controls. Clause 9.5 was also modified to say explicitly what the Port Identifier is when the SCB is set and the ES bit is not.

The use of the words "shall" and "may" was inappropriate in a number of places; this has been fixed.

>>

<<Notes to prior drafts (excerpts of continuing relevance).

This interim editor's draft, P802.1AE/D3.3, introduces the changes for multi-access, in clause 11. In addition, Clause 13 corrects an error in D3.2, here using the correct values of 30 and 50 for optional confidentiality offset.

This interim editor's draft, P802.1AE/D3.2 is primarily to introduce the changes necessary for optional confidentiality offsets, as discussed at the May interim. This includes changes to clauses 5, 10, 13 and 14. In addition Figure 10-3 was updated to reflect the deletion of AAD.

This interim editor's draft, P802.1AE/D3.1, includes changes based on the proposed Disposition of Comments for P802.1AE/D3.0

The following informative annexes were deleted as per direction:

Annex W, Perimeter Security Methods - unnecessary

Annex X, Deployment Notes - unnecessary

Annex Y, Secure Policy for RSTP - unnecessary

Annex Z, Commentary - unnecessary

The document was cleaned up from an editorial viewpoint - editor's notes were either accomplished or deleted, references were filled in.

The concept of AAD was removed, while instead specifying which fields need to be integrity protected when not confidentiality protected.

Support for multi-access was explicitly included, primarily an additional subclause 11.7 was added.

Definitions were changed to security standards definitions with appropriate references

=====

This version, P802.1AE/D3.0 is the first working group ballot draft.

The following clauses were deleted, as per direction at the January 2005 Interim meeting.

Cl 16, Securing Networks -unnecessary

Cl 15, MACsec state machines - unnecessary

Cl 12, Management of MAC security entities - management is covered in Cl 10.

Cl 10A, MACsec and EPON was renamed to Cl 12.

Cl 10 has been edited further. A replayWindow size has been introduced. Clauses 5 and 11 have been updated.

==========

This document, P802.1AE/D2.02 (there is no D2.1 due to an editorial error) is an interim version which will be updated to D3 for the a Group ballot in March of 2005.

The significant changes include:

-Management - Cl 10 is edited and enhanced, Cl 13 includes first draft of the MIB. Clause 12 will be updated based on comments on the MIB, hopefully for the next version of the document

-New clause for EPON, still called Cl 10A, so as not to renumber, but will make it Cl 11 and renumber subsequent clauses at next draft

-Changes made because default Cipher Suite is capable of both Integrity and Confidentiality+ integrity include

Removed SH bit from TCI

Changed the E bit to Changed Text (C) bit, in TCI and all prior references to E bit

Added new Encryption (E) bit to TCI, in place of the SH bit. The frame order is E, C.

-Decided to put only the KaY protocol (KSP) in .1af, and have all of the necessary context, i.e., architecture in .1AE. It is still unclear if the text does this adequately

The things that still need to be addressed are

-policy and possibly authorization?

-clause 15 state machine

-clause 16, Securing Networks

==========

This document, P802.1AE/D2.0 will be the subject of a further Task Group ballot, as agreed at the March 2004 meeting. It incorporates the editor's proposed resolution of comments to the prior ballot, and discussion in the January and March 2004 meeting. While it contains all the technical material from the editor's interim draft D1.2, it became apparent that the document would benefit from significant reorganization to introduce concepts in the best order, reduce digressions, and resolve an increasing duplication of content.

The order of clauses 8 (SecY operation) and 10 (MACsec protocol) has been reversed, and the state machine description of the protocol given its own later clause (15). The section on support of the EPON SCB capability has been moved to the new clause 8. Clause 7 has been divided, with the material on incorporating the SecY in system interface stacks now in its own clause (11) after the SecY itself has been discussed.Other material from the prior clause 7 on using MACsec to secure the network as a whole has also been given its own clause (16). Hopefully this new structure should prove durable.

The concept of the Null Cipher Suite was found, on detailed examination of inconsistencies, to be overloaded and has been removed in favour of specific management controls to facilitate deployment, including running with MACsec enabled but while still debugging the key agreement infrastructure, together with (at least some of the) necessary counters to figure out what is wrong. Some of what was in prior drafts with regard to authorization levels and replay counter exhaustion would clearly be more cleanly handled in the KaY (which can get MACsec to run on following PN exhaustion by simply providing a new key for an integrity only Cipher Suite, rather than have MACsec make this decision on its own), and has been removed. This, together with discussion of deployment, debugging, and other management should be useful topics for the Barcelona meeting.

With the exception of the clauses on management (including the MIB) and the formal specification of the state machines and procedures the document should now be substantially complete.
>>

<<Editors' final checklist (items noted in development, to be applied to final text.

The published standards are inconsistent and a bit of a mess when it comes to PDF bookmarks, this makes using them rather than final working group text difficult. P802.1p/D9 was very good. In particular it provides bookmarks for all figures at the end of a clause (see clause 7 for an example), need to copy that example.
>>

IEEE P802.1AE/D3.5

Draft Standard for Local and Metropolitan Area Networks—

Media Access Control (MAC) Security

Sponsor

LAN MAN Standards Committee
of the
IEEE Computer Society

Prepared by the Security Task Group of IEEE 802.1

Abstract: This standard specifies how all or part of a network can be secured transparently to peer protocol entities that use the MAC Service provided by IEEE 802® LANs to communicate. MAC security (MACsec) provides connectionless user data confidentiality, frame data integrity, and data origin authenticity.
Keywords: local area networks, LANs, metropolitan area networks, MANs, security, MAC security confidentiality, integrity, data origin authenticity, port based network access control, MAC Service, MSAP, service access point, transparent bridging, MAC Bridges, port based network access control, authorized port, secure association.

Introduction

[This introduction is not part of IEEE Std 802.1AE-200X, IEEE Standard for Local and Metropolitan Area Networks Media Access Control (MAC) Security.]

This is the first edition of this standard.

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

Another IEEE standard, IEEE Std 802.1XT-2004, specifies Port-based Network Access Control, and provides a means of authenticating and authorizing devices attached to a LAN. Use of this standard in conjunction with architecture and protocols of IEEE Std 802.1X-2004 extends the applicability of the latter to publicly accessible LAN/MAN media for which security has not already been defined. A proposed amendment, P802.1af, to IEEE Std 802.1X-2004 is being developed to specify the additional protocols and interfaces necessary.

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-2004, thus facilitating the use of a common authentication and authorization framework for LAN media to which this standard applies and for Wireless LANs.

Contents

IEEE P802.1AE

Draft Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security

1. Overview

1.1 Introduction

IEEE 802® Local Area Networks (LANs) are often deployed in networks that support mission critical applications. These include corporate networks of considerable extent, and public networks that support many customers with different economic interests. The protocols that configure, manage, and regulate access to these networks typically run over the networks themselves. Preventing disruption and data loss arising from transmission and reception by unauthorized parties is highly desirable, since it is not practical to secure the entire network against physical access by determined attackers.

MAC Security (MACsec), as defined by this Standard, allows authorized systems that attach to and interconnect LANs in a network to maintain confidentiality of transmitted data and to take measures against frames transmitted or modified by unauthorized devices.

MACsec facilitates

a) Maintenance of correct network connectivity and services
b) Isolation of denial of service attacks
c) Localization of any source of network communication to the LAN of origin
d) The construction of public networks, offering service to unrelated or possibly mutually suspicious customers, using shared LAN infrastructures
e) Secure communication between organizations, using a LAN for transmission
f) Incremental and non-disruptive deployment, protecting the most vulnerable network components.

To deliver these benefits MACsec has to be used in conjunction with appropriate policies for higher level protocol operation in networked systems, an authentication and authorization framework, and network management. P802.1af, Key Agreement for MAC Security, provides authentication and cryptographic key distribution.

MACsec protects communication between trusted components of the network infrastructure, thus protecting the network operation. MACsec cannot protect against attacks facilitated by the trusted components themselves, and is complementary to, rather than a replacement for, end to end application to application security protocols. The latter can secure application data independent of network operation, but cannot necessarily defend the operation of network components, or prevent attacks using unauthorized communication from reaching the systems that operate the applications.

1.2 Scope

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

NOTE—The MAC Clients are as specified in IEEE Standards 802, 802.2, 802.1D, 802.1Q, and 802.1X.

To this end it

a) Specifies the requirements to be satisfied by equipment claiming conformance to this standard.
b) Specifies the requirements for MAC Security in terms of provision of the MAC Service and the preservation of the semantics and parameters of service requests and indications.
c) Describes the threats, both intentional and accidental, to correct provision of the service.
d) Specifies security services that prevent, or restrict, the effect of attacks that exploit these threats.
e) Examines the potential impact of both the threats and the use of MAC Security on the Quality of Service, specifying constraints on the design and operation of MAC Security entities and protocols.
f) Models support of the secure MAC Service in terms of the operation of media access control method independent MAC Security Entities (SecYs) within the MAC Sublayer.
g) Specifies the format of the MACsec Protocol Data Unit (MPDUs) used to provide secure service.
h) Identifies the functions to be performed by each SecY, and provides an architectural model of its internal operation in terms of Processes and Entities that provide those functions.
i) Specifies the interface/exchanges between a SecY and its associated and collocated MAC Security Key Agreement Entity (KaY, P802.1af) that provides and updates cryptographic keys.
j) Specifies performance requirements and recommends default values and applicable ranges for the operational parameters of a SecY.
k) Specifies how SecYs are incorporated within the architectural structure within end stations and bridges.
l) Establishes the requirements for management of MAC Security, identifying the managed objects and defining the management operations for SecYs.
m) Specifies the Management Information Base (MIB) for managing the operation of MAC Security in TCP/IP networks.
n) Specifies requirements, criteria and choices of Cipher Suites for use with this standard.

This standard does not

o) Specify how the relationships between MACsec protocol peers are discovered and authenticated, as supported by key management or key distribution protocols, but makes use of P802.1af Key Agreement for MAC security to achieve these functions.

2. References

The following standards contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of ISO and IEC maintain registers of currently valid International Standards.

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

The Galois Counter Mode of Operation (GCM), David A. McGrew, John Viega.[1]

IEEE Std 802-2001, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture.[2]

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

IEEE Std 802.1Q-2003, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.

IEEE Std 802.1X-2004, IEEE Standards for Local and Metropolitan Area Networks: Port Based Network Access Control.

IEEE Std 802.1ad-200X, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks—Amendment 4: Provider Bridges.

IEEE Std 802.1AB-200X, IEEE Standards for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity and Discovery.

IEEE Std 802.2, 1998 Edition [ISO/IEC 8802-2: 1998], Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.[3]

IEEE Std 802.3-2002, Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications: Aggregation of Multiple Link Segments.

IEEE Std 802.3-2002, Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks.

IEEE Std 802.11, 1999 Edition [ISO/IEC 8802-11: 1999], Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

---

[1]This document can be downloaded from http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/gcm/gcm-spec.pdf.

[2]IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA. IEEE publications can be ordered on-line from the IEEE Standards Website: http://www.standards.ieee.org

[3]ISO [IEEE] and ISO/IEC [IEEE] documents are available from ISO Central Secretariat, 1 rue de Varembé, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA. ISO [IEEE] and ISO/IEC [IEEE] documents can be ordered on-line from the IEEE Standards Website: http://www.standards.ieee.org.

IEEE Std 802.11i-2004, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications—Media Access Control (MAC) Security Enhancements.

IEEE Std 802.17-2004 IEEE Standard for Information Technology--Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 17: Resilient packet ring (RPR) access method & physical layer specifications.

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

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

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

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

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

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

IISO/IEC 7498-1: 1994, Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 1: The Basic Mode.

ISO/IEC 15802-1: 1995, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 1: Medium Access Control (MAC) service definition.

ISO/IEC 14882: 1998, Information Technology—Programming languages—C++.

3. Definitions

For the purposes of this standard, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standards Terms,* Seventh Edition [B1][1], should be referenced for terms not defined in this clause.

3.1 Association Number (AN): A number that is concatenated with the Secure Channel Identifier to identify a Secure Association.

3.2 bounded receive delay: A guarantee that a frame will not be delivered after a known bounded time, in the case of protocols designed to use the MAC Service this is typically assumed to be less that two seconds.

3.3 Bridged Local Area Network: A concatenation of individual IEEE 802 LANs interconnected by MAC Bridges.

NOTE—Unless explicitly specified the use of the word 'network' in this Standard refers to a Bridged Local Area Network. The term Bridged Local Area Network is not otherwise abbreviated. The term Local Area Network and the abbreviation LAN are used exclusively to refer to an individual LAN specified by a MAC technology without the inclusion of Bridges. This precise use of terminology within this specification allows a Bridged Local Area Network to be distinguished from an individual LAN that has been bridged to other LANs in the network. In more general usage such precise terminology is not required, as it is an explicit goal of this standard that MAC Security is transparent to the users of the MAC Service.

3.4 Cipher Suite: A set of one or more algorithms, designed to provide any number of the following: data confidentiality, data authenticity, data integrity, replay protection.

3.5 Common Port: an instance of the MAC Internal Sublayer Service used by the SecY to provide transmission and reception of frames for both the controlled and uncontrolled ports.

3.6 Controlled Port: the access point used to provide the secure MAC Service to a client of a SecY.

3.7 cryptographic key: A parameter that determines the operation of a cryptographic function such as:

a) The transformation from plain text to cipher text and vice versa
b) Synchronized generation of keying material
c) Digital signature computation or validation.[2]

3.8 cryptographic mode of operation: Also referred to as mode. An algorithm for the cryptographic transformation of data that features a symmetric key block cipher algorithm.[3]

3.9 data integrity: A property whereby data ha not been altered in an unauthorized manner since it was created, transmitted or stored.[4]

3.10 entity authentication: The process of identifying and verifying the identity of an entity, using credentials issued to entities (e.g. username/password, token card, public-key-certificates, etc.).

3.11 initialization vector (IV): A vector used in defining the starting point of an encryption process within a cryptographic algorithm.[5]

---

[1]The numbers in brackets correspond to those of the bibliography in Annex B.

[2]This and other definitions in this clause have been drawn from ASC TR1/X9, Technical Report for ABA AXC/X9 Standards Definitions, Acronyms, and Symbols, 2002.

[3]This and other definitions in this clause have been drawn from Federal Information Processing Standard (FIPS) 300-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001.

[4]This and other definitions in this clause have been drawn from Federal Information Processing Standard (FIPS) 800-57, Recommendation for Key Management, 2005.

[5]This and other definitions in this clause have been drawn from Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, 2001.

3.12 integrity: See data integrity.

3.13 integrity check value (ICV): A value that is derived by performing an algorithmic transformation on the data unit for which data integrity services are provided. The ICV is sent with the protected data unit and is recalculated and compared by the receiver to detect data modification.

3.14 key: See cryptographic key.

3.15 key management: The generation, storage, distribution, deletion, archiving, and application of keys in accordance with a security policy.

3.16 Layer Management Interface (LMI): the interface between a protocol entity in a system and the system management, providing for the exchange of parameters with other system entities that are not attached to the service access points used and provided by the protocol entity.

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

3.18 MAC Security Entity (SecY): The entity that operates the MAC Security protocol within a system.

3.19 MAC Security TAG (SecTAG): A protocol header, comprising a number of octets and beginning with an EtherType, that is prepended to the service data unit supplied by the client of the protocol, and is used to provide security guarantees.

3.20 MAC service data unit (MSDU): A sequence of zero or more octets that compose the data to be communicated with a single MAC Service request or indication.

3.21 man-in-the-middle attack: An attack on the authentication protocol run, in which the attacker positions himself between the claimant and verifier so that he can intercept and alter data traveling between them.[6]

3.22 master key: A secret key that is used to derive one or more cryptographic keys that are used directly to protect data transfer.

3.23 message authentication: If the message arrives authenticated, the cryptographic guarantee is that the message was not modified in transit and that the message originated from an entity with the proper cryptographic credentials.

3.24 mode: See cryptographic mode of operation.

3.25 multipoint: Involving or potentially involving more than one participant in the role of receiver, or in the role of transmitter, in a single data transfer or set of related data transfers.

3.26 nonce: A non-repeating value, such as a counter, used in key management protocols to thwart replay and other types of attack.

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.

[6]This and other definitions in this clause have been drawn from Federal Information Processing Standard (FIPS) 800-63: Electronic Authentication Guideline, 2004.

3.28 plaintext key: An unencrypted cryptographic key.[7]

3.29 Port Identifier: A 16-bit number that is unique within the scope of the address of the port.

3.30 protocol data unit (PDU): A unit of data specified in a protocol and consisting of protocol information and, possibly, user data.

3.31 secret key: A cryptographic key used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public.[8]

3.32 Secure Association (SA): A security relationship that provides security guarantees for frames transmitted from one member of a CA to the others. Each SA is supported by a single secret key, or a single set of keys where the cryptographic operations used to protect one frame require more than one key.

3.33 Secure Association Identifier (SAI): An identifier for an SA, comprising the SCI concatenated with the Association Number (AN).

3.34 Secure Association key (SAK): The secret key used by an SA.

3.35 Secure Channel (SC): A security relationship used to provide security guarantees for frames transmitted from one member of a CA to the others. An SC is supported by a sequence of SAs thus allowing the periodic use of fresh keys without terminating the relationship.

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

3.37 secure Connectivity Association (CA): A security relationship, established and maintained by key agreement protocols, that comprises a fully connected subset of the service access points in stations attached to a single LAN that are to be supported by MACsec.

3.38 spoofing: Claiming a fraudulent identity for purposes of mounting an attack.

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

3.40 wiretapping: An attack that intercepts and accesses data and other information contained in a flow in a communication system. The term is used to refer to reading information from any sort of medium used for a link or even directly from a node, such as a gateway or subnetwork switch. “Active wiretapping” attempts to alter the data or otherwise affect the flow; “passive wiretapping” only attempts to observe the flow and gain knowledge of information it contains.

[7]FIPS 140-2.
[8]FIPS 140-2.

4. Abbreviations

The following abbreviations are used in this standard.

AAD	Additional Authenticated Data
AES	Advanced Encryption Standard
AN	Association Number
CA	Secure Connectivity Association
CRC	Cyclic Redundancy Check
CTR	Counter mode
DA	Destination Address
EPON	Ethernet Passive Optical Network
ES	End Station
FCS	Frame Check Sequence
FIPS	Federal Information Processing Standard
GCM	Galois Counter Mode
Gb/s	Gigabit per second (1 Gb/s is equivalent to 1 000 000 000 bits per second)
ICV	Integrity Check Value
ISS	Internal Sublayer Service
IV	Initialization Vector
KaY	MAC Security Key Agreement Entity
LACP	Link Aggregation Control Protocol
LAN	IEEE 802 Local Area Network
LLDP	Link Level Discovery Protocol
LMI	Layer Management Interface
MAC	Media Access Control
Mb/s	Megabit per second (1 Mb/s is equivalent to 1 000 000 bits per second)
MIB	Management Information Base
MPDU	MACsec Protocol Data Unit

MSDU	MAC Service Data Unit
MSTP	Multiple Spanning Tree Protocol
NESSIE	New European Schemes for Signatures, Integrity, and Encryption
NIST	National Institute of Standards and Technology
OLT	Optical Line Terminator
ONU	Optical Network Unit
PAE	Port Access Entity
PDU	Protocol Data Unit
PN	Packet Number
RADIUS	Remote Authentication Dial-In User Service
RSTP	Rapid Spanning Tree Algorithm and Protocol
SA	Secure Association
SAI	Secure Association Identifier
SAK	Secure Association Key
SC	Secure Channel
SCB	Secure Channel Broadcast
SCI	Secure Channel Identifier
SecTAG	MAC Security TAG
SecY	MAC Security Entity
SNMP	Simple Network Management Protocol

5. Conformance

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

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

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

5.1 Requirements terminology

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

a) ***shall*** is used for mandatory requirements;
b) ***may*** is used to describe implementation or administrative choices (may means is permitted to, and hence, may and may not mean precisely the same thing);
c) ***should*** is used for recommended choices (the behaviors described by should and should not are both permissible but not equally desirable choices).

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

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

5.2 Protocol Implementation Conformance Statement

The supplier of an implementation that is claimed to conform to this standard shall complete a copy of the PICS proforma provided in Annex A and shall provide the information necessary to identify both the supplier and the implementation.

5.3 Required capabilities

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

a) Support the Controlled and Uncontrolled Ports, and use a Common Port as specified in Clause 10.
b) Support the MAC status and point-to-point parameters for the Controlled and Uncontrolled Ports as specified in clauses 6.4, 6.5, and 10.7.
c) Process transmit requests from the Controlled Port as required by the specification of Secure Frame Generation (10.5).

d) Process receive indications from the Common Port as required by the specification of Secure Frame Verification (10.6), prior to causing receive indications at the Controlled Port.
e) Encode and decode MACsec PDUs as specified in Clause 9.
f) Use a globally unique 48-bit MAC Address and a 16-bit Port Identifier unique within the scope of that address assignment to identify the transmit SCI, as specified in clause 8.2.1.
g) Satisfy the performance requirements specified in Table 10-1 and clause 8.2.2.
h) Support the LMI operations required by the Kay Agreement Entity as specified in Clause 10.
i) Provide the management functionality specified in clause 10.7.
j) Protect and validate MACsec PDUs by using Cipher Suites as specified in clause 14.1.
k) Support Integrity Protection using the Default Cipher Suite specified in Clause 14.
l) For each Cipher Suite implemented, support a minimum of
    1) One receive SC
    2) Two receive SAKs
    3) One of the two receive SAKs at a time for transmission, with the ability to change from one to the other within the time specified in Table 10-1
m) Specify the following parameters for each Cipher Suite implemented
    1) The maximum number of receive SCs supported
    2) The maximum number of receive SAKs

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

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

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

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

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

5.4 Optional Capabilities

An implementation of a SecY for which conformance to this standard is claimed may

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

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

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

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

6. Secure provision of the MAC Service

MACsec provides secure communications between stations that are attached to the same LAN. An authenticated and authorized peer MAC Security Entity (SecY) within each station uses the unsecured MAC Service provided by the LAN to provide the secure MAC Service to its client (see Figure 6-1). The requirements for MACsec discussed in this clause are informed by the goal of preserving the MAC Service.

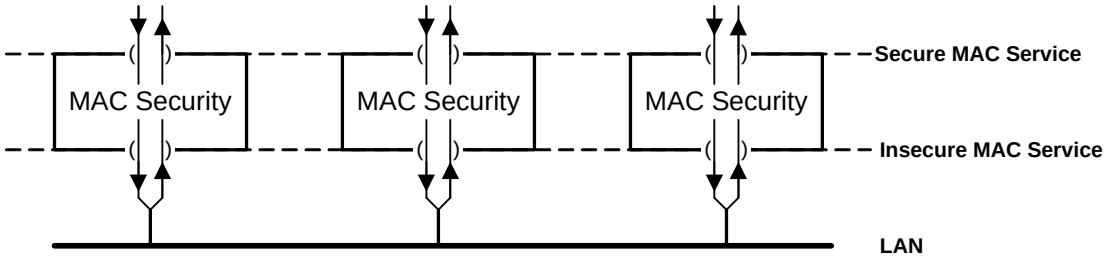


Figure 6-1—MACsec secured LAN with three stations

This clause discusses the

a) Primitives, parameters, connectivity, and status parameters provided by the MAC Service
b) Security threats posed by abuses of the MAC Service
c) Connectivity used and provided by the MAC Security Protocol (MACsec)
d) Service guarantees provided by MACsec and the security services they support
e) Quality of Service issues addressed in the design, implementation, and use of MACsec

NOTE 1—In order to introduce the concepts used in this standard, this clause can repeat or summarize the specification in other clauses, however it contains no normative provisions that apply either to the subject matter of those other clauses or to the other standards referenced. For conformance to this standard see Clause 5.

NOTE 2—MACsec does not itself guarantee the security of a Bridged Local Area Network, as that security depends on the security of the individual LANs that comprise the network, on the policies adopted by clients of the secure MAC Service (7.3), and on the security of the MAC Bridges that interconnect those LANs.

NOTE 3—Authentication and authorization are outside the scope of this standard, which ensures secure communication between mutually authenticated and authorized service access points.

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

6.1 MAC Service primitives and parameters

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

Each request and indication primitive has four parameters

— Destination Address

- Source Address
- Priority
- MAC Service Data Unit (MSDU)

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

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

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

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

The MAC Service provided by a single LAN preserves the relative order of service requests and corresponding service indications with the same requested priority. Each instance of the MAC Service provided using an instance of the EISS preserves the relative order of requests and indications with the same destination address, source address, and priority if the destination address is an individual address, and the relative order of requests and indications with the same destination address and priority if the destination address is a group address.

NOTE 4—A Provider Bridged Network can use the EISS to provide instances of the MAC Service that appear, with the exception of ordering constraints, to be a single LAN and are used as such by MACsec.

The address and MSDU parameters delivered with a service indication have identical values to those supplied with the corresponding service request. The MAC Service does not validate the parameters supplied with the request, for example it does not provide any assurance that the source address used by an LLC client is the individual address previously allocated to the station.

NOTE 5—For example, in the absence of policies that require authorization to use an address, or check that a MACsec participant does not change its address, the use of MACsec will not protect against ARP spoofing.

The priority parameter delivered with a service indication has an identical value to that supplied with the corresponding service request, where the media access control method used supports communication of priority. The access to the LAN granted by the media access control method can take the requested priority value into account, but can also be based on other factors. The 802.3 media access control method does not convey priority, and the priority value delivered with the service indication is determined by management of the receiving station. However, where the EISS is used to support an instance of the MAC Service, the priority parameter of the EISS is encoded within a VLAN TAG (IEEE Std 802.1Q) that forms the initial octets of the MSDU accompanying a service request to the instance of the ISS used to support the EISS. Figure 6-2 shows the priority field encapsulated in the VLAN TAG within the Secure Data portion of the

MACsec frame. In this case, the value of the priority parameter delivered with the service indication will be identical to that provided with the corresponding request.

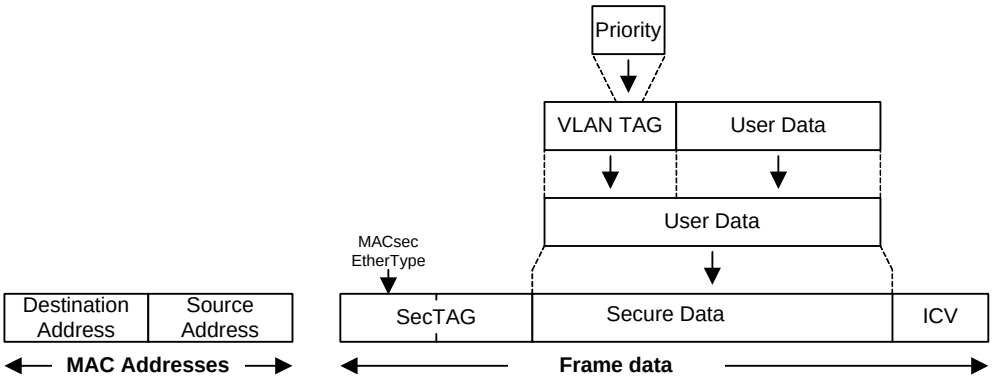


Figure 6-2—MACsec Frame, VLAN TAG, and Quality of Service

6.2 MAC Service connectivity

The MAC Service provided by a single point-to-point or shared media LAN provides symmetric and transitive connectivity between all the stations connected to that LAN. Following a service request at one service access point, a corresponding service indication occurs, with high probability, at all the MAC Internal Sublayer Service (ISS) access points in other stations attached to the same LAN. Service indications at service access points that provide the MAC Service to an LLC Entity are filtered by media access functions, generally within each receiving station, to exclude frames that are not destined to an individual or group address not used by the client.

NOTE 1—Symmetric connectivity means that if station A can communicate with station B, then B can also communicate with A. Transitive connectivity means that if station A can communicate with B, and B with C, then A can also communicate with C.

NOTE 2—Some media access control devices or methods, e.g. 802.17, are capable of not delivering some or all frames with unwanted destination addresses to some or all stations.

MAC Service clients and client protocols can operate incorrectly if the connectivity provided is not as expected. While some protocols can detect the lack of symmetric connectivity, they can simply deny service as a result. Protocols can operate inefficiently if transitive connectivity is not provided. While MAC Bridges can filter frames to restrict provision of service, the use of Virtual LANs (VLANs), with each VLAN providing full connectivity, is preferred to lessen the administrative burden of ensuring correct connectivity.

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

6.3 Point-to-multipoint LANs

A point-to-multipoint LAN provides connectivity from a single distinguished station to one or more other stations, i.e. from one point to multiple other points, and from each of the other stations to the distinguished station. The point-to-multipoint LAN does not provide direct connectivity between pairs of stations unless the distinguished station is one of the pair. Efficient multicast and broadcast from the distinguished station to all the others is provided: a single service request with a given destination address can result in service indications at each multipoint station wishing to receive frames with that destination address. Communication between the other stations occurs via the distinguished station, as specified by the relevant standard for the particular technology.

NOTE 1— Examples of point-to-multipoint LANs include IEEE Standard 802.3ah Ethernet Passive Optical Network (EPON, Clause 12), IEEE Standard 802.11, IEEE Standard 802.14, and certain provider network VLAN configurations. Depending on the particular LAN or network technology the distinguished stations are variously referred to as optical line terminators (OLTs), wireless access points (WAPs), head-ends, concentrators, star concentrators, or root nodes, and the other stations as optical network units (ONUs), stations, modems, or leaf nodes.

NOTE 2 — A point-to-multipoint LAN does not provide the MAC Service as currently specified. A suitable service specification is for future study. This specification attempts to bridge this much needed gap.

6.4 MAC status parameters

Each service access point can make available status parameters that reflect the operational state and administrative controls for the service instance provided at that access point.

The **MAC_Enabled** parameter is TRUE if use of the service is permitted; and is otherwise FALSE. The value of this parameter is determined by administrative controls specific to the entity providing the service.

The **MAC_Operational** parameter is TRUE if, and only if, service requests can be made and service indications can occur.

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

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

6.5 MAC point to point parameters

Each service access point can make available status parameters that reflect the point-to-point status for the service instance provided, and that allow administrative control over the use of that information.

If the **operPointToPointMAC** parameter is TRUE the service is used as if it provides connectivity to at most one other system, if FALSE the service is used as if it can provide connectivity to a number of systems.

The **adminPointToPointMAC** parameter can take one of three values. If it is

a) **ForceTrue**, operPointToPointMAC shall be TRUE, regardless of any indications to the contrary generated by the service providing entity.

b) **ForceFalse**, operPointToPointMAC shall be FALSE.
c) **Auto**, operPointToPointMAC is as currently determined by the service providing entity.

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

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

6.6 Security threats

The expected features of the MAC Service described above—the relationships between service requests and indications, preservation of the parameters of these primitives, the connectivity provided, and the relationship of the MAC status parameters to the connectivity—can be accidentally and unintentionally distorted through misconfiguration or deliberately abused. Misconfiguration or abuse can result in

a) Inability to issue service requests
b) Indiscriminate loss of service indications
c) Specifically targeted loss of service indications
d) Repeated service indications at the intended destinations
e) Service indications with modified address or data parameters
f) Additional service indications with unmodified or selectively modified parameters
g) Service indications at unintended recipients
h) Delayed service indications that can disrupt network operation

Deliberate abuse can serve as a basis for an attack upon the resources accessible from a LAN, through attacks on the protocols that use the service and provide access to or control over those resources. The effort required by an attacker to abuse the service in any particular way depends in general on the media access control method used by the LAN, and the particular devices and components that support it.

The MAC Service does not guarantee the origin or authenticity of service requests and the accompanying parameters. Since the sole use of the source address allocated to a station by that station and the restriction of service indications to intended recipients can depend on cooperative behavior from other stations, it is usually easy for an attacker that can attach a station to a LAN to receive any service indication and to issue additional service requests with parameters based on those indications. Other service abuses can require physical access to inconveniently located components.

It is beyond the scope of this standard to enumerate all the ways in which abuses of the service can be exploited, they include techniques commonly referred to as passive wiretapping, masquerading, and man-in-the middle attacks. The latter is facilitated by source address spoofing, usually after another station with that source address has been observed to have been granted access to some resource. Attacks can include

i) Denial of service, to all or to selected stations
j) Theft of service
k) Access to confidential information
l) Modification of confidential information
m) Access to or control over restricted resources.

MACsec does not protect against brute force denial of service attacks that can be mounted by abusing the operation of particular media access control methods through degrading the communication channel or transmitting erroneous media access method specific control frames.

6.7 MACsec connectivity

The connectivity provided (6.2) between the MAC Internal Sublayer Service (ISS) access points of stations connected to a single LAN composes an insecure association between communicating stations. Key agreement protocols as defined in P802.1af establish and maintain a secure Connectivity Association (CA), which is a fully (i.e. symmetric and transitive) connected subset of the ISS service access points. Each instance of MACsec operates within a single CA.

NOTE 1—ISO/IEC 15802, the MAC Service definition, introduces the term 'Connectivity Association' to discuss the relationship between service access points without referring to the details of particular media access control methods or to terms such as 'physical connection' or 'logical connection' that have other associated attributes and meanings.

MACsec itself does not provide comprehensive monitoring of the connectivity provided by a CA, although it can detect and will signal certain failures to the local MAC Security Key Agreement Entity (KaY). Together, operation of key agreement protocols and MACsec ensures that the status parameters provided by an instance of the secure MAC Service correctly reflect both the current connectivity and changes in the connectivity of the CA. Specifically

a) MAC_Operational is only True if the CA is complete (i.e. is symmetric and transitive), and the local MACsec Entity (SecY) can both receive and transmit.

NOTE 2—The Single Copy Broadcast (SCB) functionality of EPON can be considered an exception with respect to symmetric connectivity, as discussed in Clause 12.

b) If MAC_Operational is True in stations wanting to join a new CA and in stations already in the target CA, and if stations are added to the CA, MAC_Operational transitions to False in either all the stations originally participating in the CA or in all those added, for sufficient duration such that clients of the service are aware of the transition.

   Determining which group transitions MAC_Operational to False is outside the scope of this specification and is determined by the KaY and signaled through the Layer Management Interface (LMI).

c) If MAC_Operational is False in stations wanting to join a CA, and if these stations are added to a CA, there is no change in the MAC_Operational status of the stations already in the target CA, and MAC_Operational will transition to True in the joining stations after some period of time. This is the typical case for a single station joining a CA, in which its MAC_Operational is False until the join is accomplished when its state transitions to MAC_Operational True.

d) If adminPointToPointMAC is set to Auto and MAC_Operational is True, then operPointToPointMAC is True only if at most one other station is participating in the CA. If adminPointToPointMAC is set to forceFalse, then operPointToPointMAC must be False, regardless of the number of stations in the CA.

NOTE 3—Communication between KaYs in stations that compose a CA does not depend on the operation of MACsec.

6.8 MACsec guarantees

At each service access point that is a member of a CA, MACsec ensures that any service indication

a) Is the result of a service request at a service access point that is also a member of the same CA
b) Has the parameter values that are identical to those supplied with the service request

and can also ensure that

c) No more than one indication results from one service request

d) A service indication does not occur after a known bounded time has elapsed since the service request was made
e) The values of the octets that comprise the MAC Service Data Unit (MSDU) parameter cannot be ascertained except by members of the CA.

MACsec does not

f) Conceal the following from stations that are not members of the CA
   1) Service requests
   2) Values of service request address parameters
   3) The number of octets that comprises the MSDU
g) Validate the parameters provided with a service request

MACsec provides guarantees to within known bounds that are derived from the cryptographic methods and other mechanisms used.

The known bounded time in (d) is typically longer than required to enforce the maximum transit delay requirements of the MAC Service.

NOTE —The addition of explicit time indications to the SecTAG to provide tight bounds for transit delay was considered in the development of this standard, but the value delivered is small for the added complexity and the burden imposed on key agreement protocols. Higher layer protocols that have tight timing requirements typically add their own timing markers. As these markers are carried within the MSDU, their integrity is protected by MACsec.

6.9 Security services

The guarantees provided by MACsec support the following security services for stations participating in MACsec:

a) *Connectionless data integrity* (6.8(a), 6.8(b))
b) *Data origin authenticity* (6.8(a)). If the connectivity model is point to point, the originator is authenticated, but if the connectivity model is multipoint, then the authenticated originator is a member of the CA, rather than a particular individual station.
c) *Confidentiality* (6.8(d))
d) *Replay protection* (6.8(d), 6.8(c))
e) Bounded receive delay

and can be used to limit the nature and extent of

f) *Denial of service* attacks

MACsec does not support

g) *Non-repudiation*

or protect against

h) *Traffic analysis*

A MAC Bridge that forwards a frame with an erroneous source MAC address can unintentionally facilitate a denial of service or other attack on other LANs within a Bridged Local Area Network. The MAC Bridge should use MACsec in conjunction with an appropriate policy to verify the binding of the source MAC address to access to resources.

6.10 Quality of service maintenance

The quality of the MAC Service can be lowered by direct attacks on the operation of particular media access control methods and indirect attacks on their resource allocation procedures facilitated by masquerading and unauthorized data modification. MACsec does not provide guarantees for frames, known as MAC control frames, that are internal to the operation of a particular media access method and cannot defend against abuses that use or affect such frames. MAC control frames are not forwarded by MAC Bridges, so attacks that exploit them can be localized to particular LANs.

NOTE—Where, within the operation of a particular media access control method, it is possible to establish secure Connectivity Associations prior to performing certain control functions, those functions should be supported by frames transmitted using an instance of the ISS. The parameters of those frames can then be protected by MACsec, and the scope for abuse restricted. It is not a requirement of the Open Systems Interconnection (OSI) layer model (ISO 7498) that management and control of a particular layer be carried out purely within that layer by protocols whose identifiers and formats are specific to that layer. For example SNMP can be used to manage MAC Bridges.

Operation of a security protocol has the potential to lower some aspects of Quality of Service. The operation and design of MACsec is discussed below as it relates to

a) Service availability
b) Frame loss
c) Frame misordering
d) Frame duplication
e) Frame transit delay
f) Frame lifetime
g) Undetected frame error rate
h) Maximum service data unit size supported
i) Frame priority
j) Throughput

Use of MACsec can lower service availability if delays occur in the creation of Connectivity Associations or in the distribution and maintenance of cryptographic keying material. Failures or attacks upon the system that support authentication and authorization can result in denial of service.

The operation of MACsec introduces no additional frame loss on individual LAN segments other than that expected for a specific media access control method as a consequence of a small increase in frame size. The operation of MACsec between two customer systems across a provider bridged network can introduce additional frame loss caused by possible frame reordering from expedited forward or link aggregations within the provider bridged network. The reception of misordered frames can cause MACsec implementations to discard additional frames depending upon the configuration of replay protection parameters. Conforming implementations of MACsec are capable of applying a new keying material starting with any frame in a sequence that is received with the minimum intervening spacing specified by the specific media access control method in use. Each frame protected by MACsec remains independent of its predecessors and successors, so loss of a single frame does not imply loss of additional frames.

MACsec does not introduce any additional potential for duplicating or misordering frames. No retransmission mechanisms are added to relax requirements for distribution and use of MACsec related information. Any parallel processing of frames adopted by MACsec implementations is required to preserve the sequence of requests and indications between the secure service access point supported and the insecure service access point used.

Since the MAC Service is provided at an abstract interface within an end station, it is not possible to specify the total frame transit delay precisely. It is, however, possible to measure the additional transit delay introduced by an additional component or intermediate system.

The minimum additional transit delay introduced by MACsec is due to the increase in the MSDU size required to convey security information and essential buffering requirements required to meet the processing requirements of particular Cipher Suites. Specific limits are placed on the additional delays allowed to MACsec implementations (Table 10-1). The permitted delay is short compared with the upper bound mandated by the MAC Service, so does not threaten the correct operation of higher layer protocols.

Frame lifetime can be increased by MACsec if additional delay is introduced by providing security. The typical bound on frame lifetime is approximately two seconds.

MACsec does not increase the undetected frame error rate for frames received and transmitted on a single LAN. The frame check sequence (FCS) method used by each specific media access control method protects the entire frame including information added by MACsec. The integrity check added by MACsec can increase the probability of detecting unintentional frame modifications, particularly where those do not correspond to the expected noise characteristics for which the FCS was originally designed, but equally is not a substitute for the FCS since it is designed to ensure that an attacker has an exceedingly low chance of predicting how to make an undetected modification to the frame's parameters rather than to efficiently detect burst noise characteristics.

Use of MACsec on each of a MAC Bridge's Ports will force a change in the data covered by an FCS, even if the frame is being relayed between LANs that use the same media access control method. Application of the techniques described in IEEE Std 802.1D Annex F (informative) allow an implementation to achieve an arbitrarily small increase in undetected frame error rate, even in cases where the data that is within the coverage of the FCS is changed.

The Maximum Service Data Unit Size that can be supported by an IEEE 802 LAN varies with the media access control method and its associated parameters (speed, electrical characteristics, etc.), and can be constrained by the owner of the LAN. MACsec adds security information to a transmitted MSDU, and thus reduces the Maximum Service Data Unit Size available to users of the insecure MAC Service.

Where MACsec is used to support an instance of the ISS that in turn supports the EISS, encoding of the priority parameter of the EISS within the ISS MSDU ensures that priority can be communicated unchanged between service access points attached to a single LAN. Since MACsec is terminated on each of the Ports of MAC Bridges attached to such LANs, a Bridge can access or change the priority even if the two instances of MACsec encrypt the MSDU in order to provide confidentiality.

Cryptography can be computationally intensive, and the operation of MACsec has the potential to lower throughput. The Cipher Suite(s) mandated and recommended by this standard have been chosen, in part, for their ability to support economic implementation across the range of LAN MAC data rates.

7. Principles of secure network operation

This clause establishes the principles and a model of secure network operation. It describes the security relationships used to support the secure MAC Service (Clause 6), and how that service is used to provide overall network security. It provides the context necessary to understand the operation of the MAC Security Protocol (MACsec, Clause 8) and individual MAC Security Entities (SecYs, Clause 10).

Secure network operation comprises use of the secure MAC Service on each of the individual LANs that compose the network together with the application of appropriate security policies by the MAC Service clients in end stations and in intermediate systems that forward frames. This clause defines

a) The security relationships that support secure MAC Service

and describes how the secure MAC Service is

b) Supported on each of the individual LANs that compose the network (7.1)
c) Used by the protocol entities that are its Clients (7.3)

and delineates the responsibilities of the

d) MACsec Key Agreement Entities (P802.1af)
e) MAC Security Entities
f) Clients of the secure MAC Service.

Security relationships and the terms that identify them have been defined, in various ways, by a number of publicly available documents. This standard has deliberately chosen new terms to minimize confusion whenever differences could exist between previously used terms and the requirements. For example, the attributes associated with an Secure Association Identifier (SAI, Figure 7-7) are similar to but not exactly the same as those associated with the Security Parameter Index (SPI) defined by IPsec (IETF RFC 2406). The normative properties of all terms used in the standard are as defined by this standard.

NOTE 1—The use of the term ‘secure network’ in this clause refers to a network of end stations, LANs, bridges, routers and similar systems, and the servers and services that support these. The description and specification in this clause is limited to use of the secure MAC Service to contribute to overall system security (See Clause 1).

NOTE 2—In order to introduce the concepts used in this standard, this clause can repeat or summarize the specification in other clauses, however it contains no normative provisions that apply either to the subject matter of those other clauses or to the other standards referenced. For conformance to this standard see Clause 5.

NOTE 3—The term “individual LAN” (3.17) is used in this Standard to refer explicitly to an instance of media access method specific technologies providing the MAC Service directly. The term excludes larger networks or subsets of a network that are created by aggregation or concatenation of individual LANs by Link Aggregation or bridges.

NOTE 4—The examples presented in this Clause are intended to serve as a guide to best practice, however the use of MAC Security is not limited to the examples given. Limits to the use of MAC Security that are required for the successful operation of network configuration and other protocols are made explicit.

7.1 Support of the secure MAC Service by an individual LAN

Each port that is capable of participating in an instance of the secure MAC Service comprises both a MAC Security Key Agreement Entity (KaY) and a MAC Security Entity (SecY). The detailed relationship within a port between the SecY and its associated KaY is described in Clause 10 and Figure 10-2. Each KaY discovers or is made aware of the KaYs present in other stations attached to the same LAN, ensures that those stations are mutually authenticated and authorized, and creates and maintains the secure relationships between the stations that are used by the SecYs to transmit and receive frames. Specifically

a) A secure Connectivity Association (CA) is created to meet the requirements of the MAC Service (6.2) and MACsec (6.7) for connectivity between the stations attached to an individual LAN.

b) Each CA is supported by Secure Channels (SCs), each SC supporting secure transmission of frames, through the use of symmetric key cryptography, from one of the systems to all the others in the CA.

c) Each SC is supported by an overlapped sequence of Security Associations (SAs).

d) Each SA uses a fresh Secure Association Key (SAK) to provide the MACsec service guarantees (6.8) and security services (6.9) for a sequence of transmitted frames.

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 new independently derived master keys. 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 (Clauses 8, 9) only allows a limited number of frames to be protected with a single key. Since 2^{32} minimum sized 802.3 frames can be sent in approximately 5 minutes at 10 Gb/s, this can force the use of a new SA.

These security relationships (CAs, SCs, and SAs) and the information associated with each of them are further discussed below (7.1.1, 7.1.2, 7.1.3). Their mutual relationship, and the insecure connectivity provided by the LAN that supports them, are illustrated in Figure 7-1 through Figure 7-3 for a point to point LAN and in Figure 7-4 through Figure 7-6 for stations attached to a shared media LAN.

Figure 7-1 shows two stations, A and B, connected to a point to point LAN that provides insecure bidirectional connectivity.

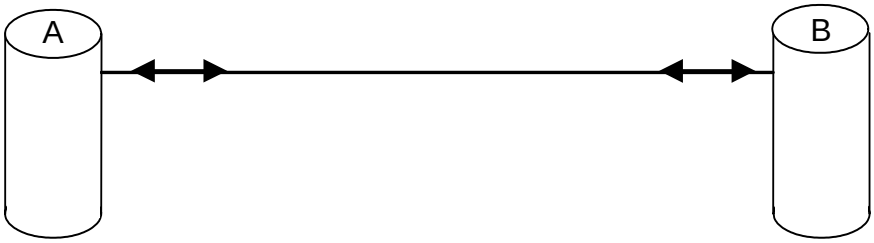


Figure 7-1—Two stations connected by a point to point LAN

Figure 7-2 depicts the CA created by MACsec Key Agreement following mutual authentication and authorization of A and B.

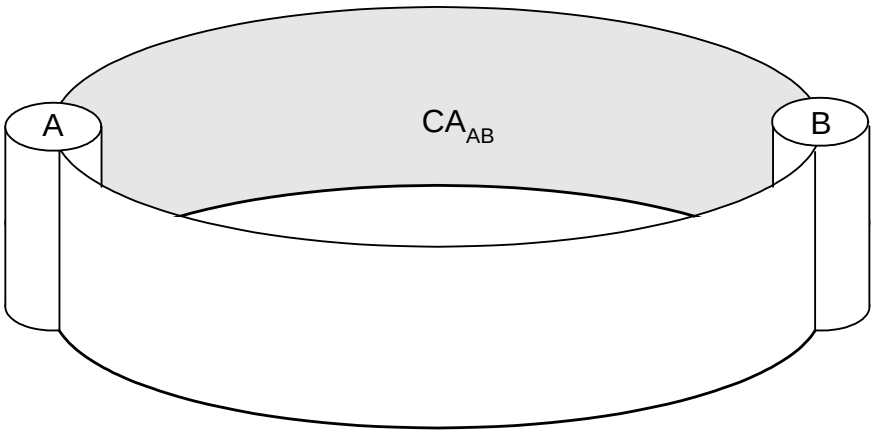


Figure 7-2—Two stations in a CA created by MACsec Key Agreement

Figure 7-3 shows the two SCs that support the CA.

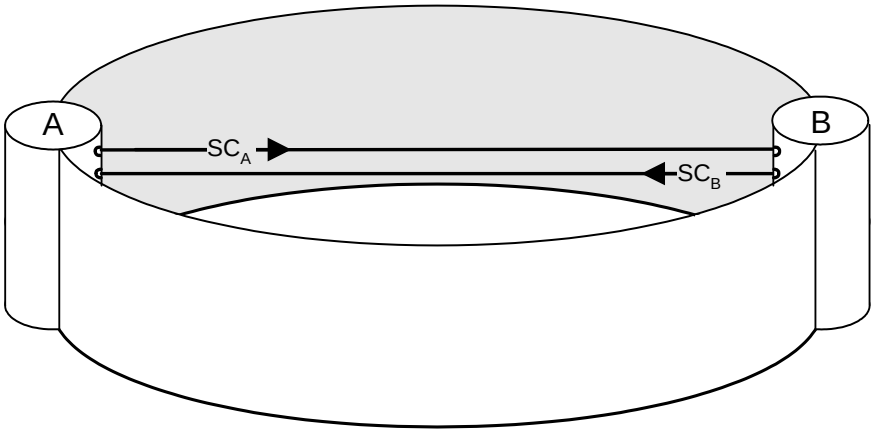


Figure 7-3—Secure communication between two stations

Figure 7-4 shows four stations, A, B, C, and D, attached to a shared media LAN that provides full but insecure connectivity between the stations

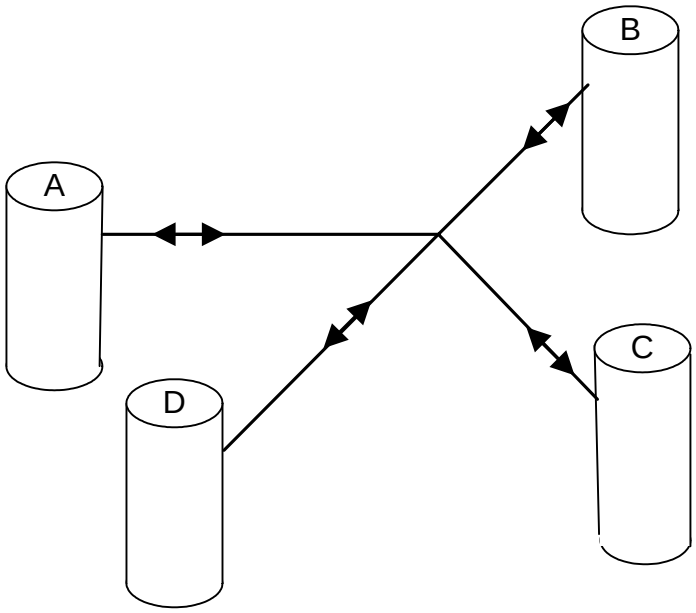


Figure 7-4—Four stations attached to a shared media LAN

Figure 7-5 depicts a CA created by MACsec Key Agreement following mutual authentication and authorization of A, B, and C. The CA excludes D.

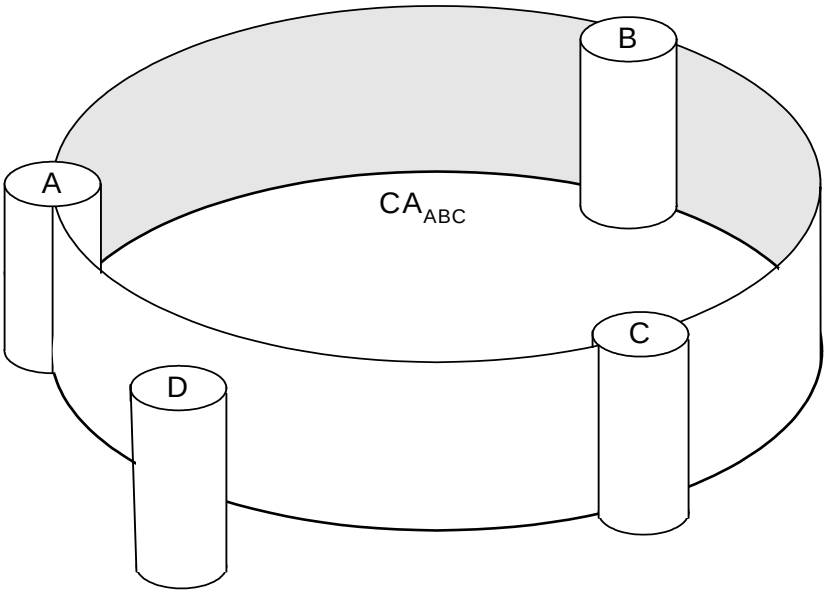


Figure 7-5—A CA including ports A, B, and C

Figure 7-6 shows the three SCs that support the CA, one for transmission by each of A, B, and C.

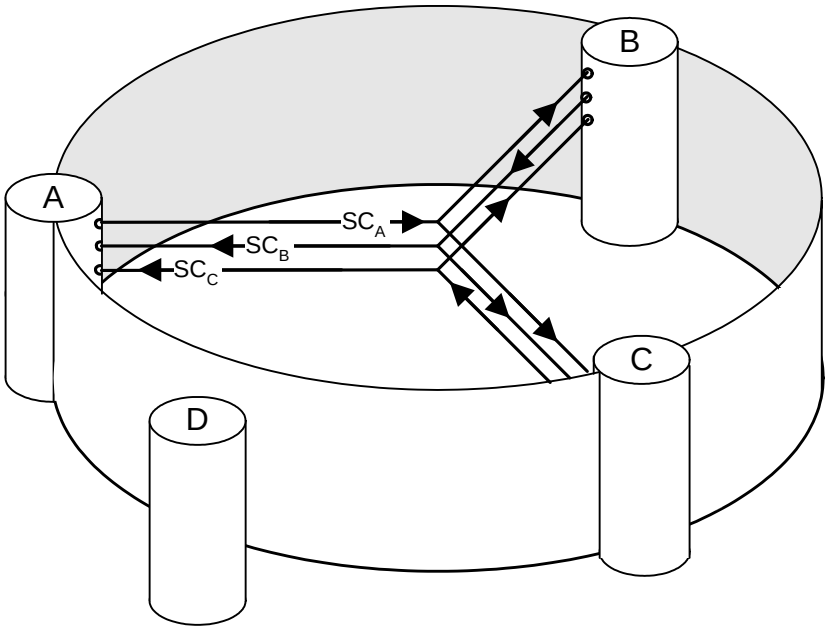


Figure 7-6—Secure communication between three stations

While D can send and receive frames using the insecure connectivity provided by the shared LAN, it does not have SAKs that would allow it to participate in any of the SAs that currently support SC_A, SC_B, or SC_C,

and therefore D cannot compromise the integrity, confidentiality, or origin of any of the frames being exchanged by A, B, and C.

7.1.1 Connectivity Association (CA)

MACsec Key Agreement is responsible for discovering, authenticating, and authorizing the potential participants in a CA. A SecY, as specified in this standard, does not need to be aware of the CA, except as a list of SCs in which it needs to participate. Since all the SCs in a CA use the same Cipher Suite at any one time, the Cipher Suite can be considered a property of the CA. A change in the Cipher Suite necessitates an interruption to the service provided by the CA.

Each SecY participates in only a single CA at any one time. Administrative controls can limit the number of peer SecYs that can participate in that CA.

NOTE—If this specification had allowed different SCs to use different Cipher Suites, a SecY implementing more than one Cipher Suite would have to be capable of simultaneous transmitting using one Cipher Suite and receiving using one or more other Cipher Suites.

7.1.2 Secure Channel (SC)

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.

NOTE 1—Using an SC identifier that includes a port number component would appear to be unnecessary in the case of a simple system that comprises a single LAN station, with a uniquely allocated 48-bit MAC address, and a single SecY. However some systems require support for more SecYs than they have uniquely allocated addresses, either because they make use of technologies that support virtual MACs, or because their interface stacks include the possibility of including multiple SecYs at different sublayers. Provider bridges (P802.1ad) provide examples of the latter.

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

MACsec Key Agreement is responsible for informing each SecY of the identifier to be used for the transmitting SecY, and of the existence and identifier of each of the SCs for which the SecY is to receive frames. While the structure of the communication facilitated by each SC is point to multipoint (which encompasses point to point as a special case) the SecY does not have to be aware that its transmissions can reach multiple receivers, that the frames that it receives could be received by other SecYs, or of any relationship or lack of relationship between the inbound SCs.

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

7.1.3 Secure Association (SA)

Each SC comprises a succession of SAs, each with a different SAK. Each SA is identified by the SC identifier concatenated with a two-bit Association Number (AN, Figure 7-7). The Secure Association Identifier (SAI) thus created allows the receiving SecY to identify the SA, and thus the SAK used to decrypt and authenticate the received frame. The AN, and hence the SAI, is only unique for the SAs that can be used or recorded by participating SecYs at any instant.

MACsec Key Agreement is responsible for creating and distributing SAKs to each of the SecYs in a CA. This key creation and distribution is independent of the cryptographic operation of each of the SecYs. The same SAK can be used for SAs that compose different SCs, provided that every IV used with the SAK is

unique. When the Default Cipher Suite(14.5) is used, the SCI is included in the IV to ensure uniqueness across SCs.

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

The transmitting SecY does not interleave frames.

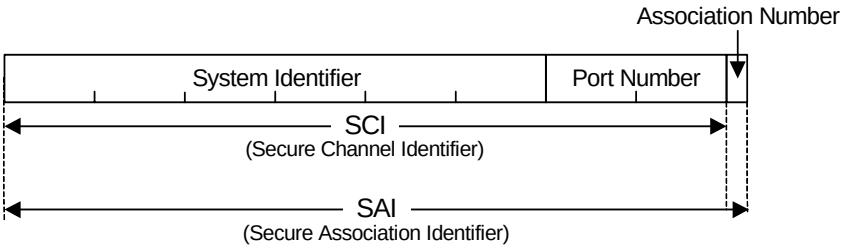


Figure 7-7—Secure Channel and Secure Association Identifiers

If a SecY does not have a usable SA for its outbound SC, i.e. an SA that can be used at no notice for frame transmission with a PN value that is not exhausted, and any of the current SAs for inbound SCs are not usable, then the MAC_Operational status parameter (6.4) is set FALSE.

7.2 Multiple instances of the secure MAC Service on a single LAN

Each service access point for an instance of the secure MAC Service is supported by a service access point for an instance of an insecure MAC Internal Sublayer Service. Multiple instances of the secure MAC Service can be provided by a single LAN, provided that each instance is uniquely identified by unencrypted fields contained in each received frame. These fields identify separate instances of the unsecured MAC Internal Sublayer Service, each capable of supporting a distinct service access point for MAC Security.

Identification of each insecure service instance, and multiplexing and demultiplexing to and from the transmission capabilities provided by the LAN, can performed wholly below the ISS by a media specific or media dependent functions. Some media are defined to support such a multiplexing function, e.g. the LLID used by P802.3ah EPON (See Clause 12). Provider Bridges are also capable of supporting multiple instances of the ISS over a network of individual LANs (See 11.6).

MAC Security should not be used to support multiple instances of the secure MAC Service on a single physical LAN without the use of unencrypted frame fields to identify separate instances of insecure service, each supporting a single instance of secure service. While the use of security to provide multiplexing is impossible to prevent (since different cryptographic keys can be used to separate connectivity) relying solely on security to define the connectivity makes deployment and fault management difficult - the topology of an entire network could change as security was enabled or disabled on a single LAN. Key agreement protocols that use the insecure MAC service can require a matching instance of that service for each secure service instance.

NOTE 1-The service access point for the secure MAC Service is referred to as Controlled Port of the MAC Security Entity (SecY, Clause 10) and the service access point for the insecure MAC Service as the SecY's Common Port. Access to the insecure service for protocol entities above MAC Security is provided at the Uncontrolled Port.

NOTE 2—Although the field or fields used to provide service instance multiplexing are not parameters of the ISS, and thus are not protected, the integrity of the secure MAC Service is not compromised. If the unprotected fields are modified, the frame can be delivered to the wrong SecY, but will subsequently fail integrity checks. Different SecYs use different security associations, keys, and cryptographic nonces. Additional management parameters are (cryptographically) bound to individual SecYs, not to the values of frame fields.

The secure MAC Service requirements for symmetric and transitive connectivity ensure that two or more service instances on the same LAN will appear as separate LANs to the clients of the SecYs. There is therefore no conflict between the use of bridges and the provision of multiple secure service instances.

When clients that are connected to a first service instance change and connect to a second service instance, the secure connectivity alters. MAC_Operational temporarily transitions to False for a minimum amount of time to allow the CA to re-establish its membership, (as determined by the KaY). In particular, each time membership of a CA changes, MAC_Operational transitions False for at least one of each pair of SecYs whose connectivity has changed. For example if members of CA_x leave CA_x and join CA_y and if CA_y has MAC_Operational True, then MAC_Operational transitions to False for either the members of CA_x who are joining CA_y, or for the original members of CA_y. MAC_Operational transitions to True once all the new members have joined CA_y.

NOTE 3—Two SecYs that connect to the same LAN and participate in the same CA appear connected to the same LAN (as one would expect) and appear connected to different LANs as they participate in distinct CAs. The effect is similar to partitioning a LAN by switching a repeater on or off.

Distinct instances of the secure point-to-point MAC Service can be provided by a bridge to different end stations connected to the same shared media by using the source address of the frames transmitted by each end station to identify one of a number of SecYs in the receiving bridge (11.7).

NOTE 4—This capability does not apply to the use of IEEE Std 802.11. That standard specifies its own mechanisms for identifying separate secure associations.

7.3 Use of the secure MAC Service

The secure MAC Service guarantees (6.8) the integrity of the parameters of each service indication, and that each indication is a result of a request made by a SecY that is a member of the same CA as the receiver, though not by any particular member. Management controls associated with each MACsec Key Agreement Entity (KaY) can require certain authentication and key management methods to ensure these guarantees. However the degree of trust placed in the security of the communication does not imply the degree of trust associated with the communicating peers. Accordingly, the MACsec Key Agreement framework facilitates authorization of each potential member, and allows management of the acceptable authorization for inclusion in the CA.

The secure MAC service does not itself provide any means to label or distinguish different levels of authorization, and does not associate different levels of authorization with individual invocations of the service. A station either participates in a service instance or it does not.

To ensure correct operation of client protocols, secure service indications are not filtered or modified by a SecY except as specified in Clause 8 and 9. Each protocol entity that is a client of the secure MAC Service should implement suitable policies (7.3.1) to support overall network security.

NOTE 1—For example, correct operation of Spanning Tree Protocol depends on the delivery of BPDUs to the Spanning Tree Protocol Entity of a given bridge from all the other bridges attached to the LAN that transmit frames that can be relayed by the given bridge. If a SecY were to require a higher level of authorization to pass received BPDUs through

the Controlled Port, data loops in the network could result. However the STP Entity can adopt a policy of discarding frames rather than permit another system that is not authorized as a bridge to be the Designated Bridge for the CA.

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

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

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

NOTE 2—If one of the members of the CA is a bridge (strictly speaking the Bridge Port is the CA member), the other members should adopt policies that reflect their confidence in the policies applied by the bridge to forward frames. In this case the trust is partly transitive— the question to be answered by each member of the CA is the degree of trust to place in the bridge's trust of systems that originate frames that the bridge will forward.

7.3.1 Client policies

Client policies, which are not specified in this standard, can include but are not limited to

a) Limiting the set of protocol procedures that can be invoked by the peer
b) Segregating communications between different sets of peer users of the MAC Service
c) Filtering, i.e. discarding, received frames

Clients of the secure MAC Service can also record any exceptional policy actions taken, so as to initiate further administrative action, outside the scope of this standard, with the entities legally and financially responsible for the operation of the authenticated peer systems.

NOTE 1—To facilitate policy selection by clients of the secure MAC Service, P802.1af Key Agreement for MAC Security, specifies authorized permissions, including those required by MAC Bridges (IEEE Std 802.1D) and VLAN-aware Bridges (IEEE Std 802.1Q) to support the secure MAC Service in Bridged and Virtually Bridged Local Area Networks.

NOTE 2—A VLAN-aware Bridge that assigns frames that have been received from a specific Bridge Port (the bridge's point of attachment to a service instance) to a VLAN on the basis of the authorization associated with the Port provides an example of policy of segregating communications, as described in (b) above.

7.3.2 Use of the secure MAC Service by bridges

Each Bridge Port uses the service provided by an individual LAN (see Clause 11), which is not dependent for its connectivity on the operation of other bridges. This ensures that the configuration protocols used by bridges, including the spanning tree protocol, operate over a physical topology (comprising a bipartite graph of bridges and individual LANs connected by Bridge Ports) that is not itself dependent on the active topology, or subsets of the active topology, calculated by those same configuration protocols.

NOTE 1—The apparent exception to this configuration restriction, which does not permit the creation of security associations to create "secure tunnels" through selected bridges in a Bridged Local Area Network, is the use of a Provider Bridged Network as specified in P802.1ad. However a Provider Bridged Network appears to Customer Bridges as a single LAN providing full connectivity independent of the operation of Customer Bridge protocols.

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

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

The policies applied by the Bridge Forwarding Process that is a client of each MAC service instance can include but are not limited to

a) Use of static Filtering Database Entries
b) Use of the RSTP and MSTP restrictedRole parameters
c) The PVID for the port
d) Configuration of the VLAN Translation Table (P802.1ad only)
e) Inclusion in the Member Set for any given VLAN and the setting of Enable Ingress Filtering
f) Identification of the Port as a Provider Edge Port
g) Port priority
h) Priority remapping tables

NOTE 3—A Bridge Port is one of the bridge's points of attachment to an instance of the MAC Internal Sublayer Service (ISS), and is used by the MAC Relay Entity and associated Higher Layer Entities as specified in IEEE Std 802.1D, IEEE Std 802.1Q, and P802.1ad.

NOTE 4—The RSTP and MSTP restrictedRole parameters in P802.1Q-REV ensure that the spanning tree active topology for other Bridge Ports is unaffected by BPDUs received on the Port, while continuing to protect against data loops and allowing the peer system to use the BPDUs it receives to select between redundant service instances. The restrictedRole parameter should be set if the authorization (see also 7.3) of the peer system(s) is not sufficient to allow full participation in determining the active topology of the network.

In response to a limited authorization on the Bridge Port, a bridge can be configured to discard frames other than from a specified number of MAC addresses, and to use additional services provided by the network administrator to ensure that these permitted addresses are not used by other end stations in the network.

8. MAC Security Protocol (MACsec)

MACsec provides the secure MAC Service (Clause 6) on a frame by frame basis, using cryptographic methods within the context of security relationships maintained by MACsec Key Agreement.

This clause

a) Sets out requirements for the design (8.1) and support (8.2) of MACsec
b) Provides an overview of its operation (8.3)

NOTE 1—The operation of MACsec Key Agreement Entity (KaY), and the protocols it uses are outside the scope of this standard. However the security relationships (Clause 7) it establishes are essential to the operation of MACsec, and form part of the support requirements.

Conformance to this standard is in terms of the observable protocol arising from the operation of a MAC Security Entity (SecY, Clause 10), including management of MACsec and the service provided to client protocols that use the secure MAC service.

Each of the possible sets of cryptographic algorithms used by MACsec to provide connectionless frame integrity and data confidentiality compose a Cipher Suite. This clause describes the result of Cipher Suite use by the SecY, illustrated in Figure 8-1. The normative specification of each Cipher Suite is provided in Clause 14. The Cipher Suite is selected as part of the establishment of the CA (7.1.1).

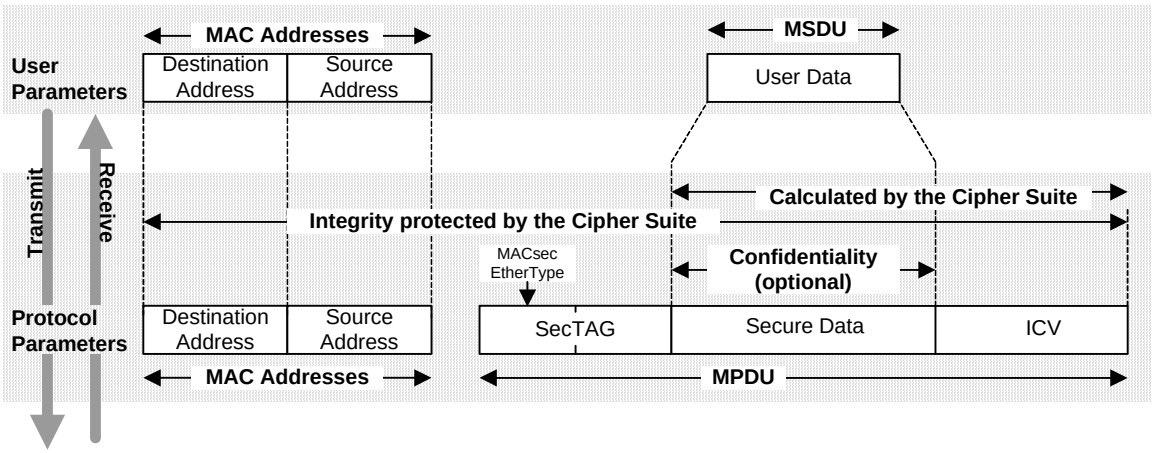


Figure 8-1—MACsec

NOTE 2—The Destination Address and Source Address parameters are shown as separate from the MPDU in Figure 8-1, as they are separate parameters of each service request. The encoding of these parameters into a transmitted frame on a medium is accomplished by the supporting service, which can interpose additional octets between those of the addresses and the MSDU. In the strict sense of externally visible transmission, this standard deals with parameters of service primitives, not with frames. However it is often convenient to talk of these parameters as a frame.

8.1 Protocol design requirements

MACsec operates in networks comprising end stations and individual point to point or shared media LANs, arbitrarily interconnected by intermediate systems, such as MAC Bridges, VLAN-aware Bridges, and routers. MACsec supports, preserves, and maintains the quality of the secure MAC Service in all its aspects as specified by Clause 6, meeting requirements for

a) Connectivity (6.7)
b) Security (6.8, 6.9, 8.1.1)
c) Manageability (8.1.2)
d) Interoperability (8.1.3)
e) Deployment (8.1.4)
f) Coexistence (8.1.5)
g) Scalability (8.1.6)
h) Intrusion detection (8.1.7)
i) Localization and isolation of attacks (8.1.8)
j) Implementation (8.1.9)

These requirements are met by the operation of MACsec (8.3) together with requirements placed on

k) The architecture that specifies how MAC Security Entities (SecYs) are placed within LAN stations and communicate with selected peers (Clause 11)
l) The choice of cryptographic methods that compose each MACsec Cipher Suite (Clause 14)
m) Support of the protocol by each SecY, and on the system that contains it (8.2)
n) The operation of the protocols that support MACsec Key Agreement, including aspects of authentication, authorization, and distribution of keys

8.1.1 Security requirements

In addition to providing the security guarantees (6.8) and services (6.9) required for support of the secure MAC service, the design of MACsec

a) Enables a succession of SAs, each with its own Secure Association Key (SAK) to be used to support the connectivity provided by each SC. Changing SAKs in this way, together with the use of Key Agreement protocols that provide Perfect Forward Secrecy, protects against the compromise of any single SAK, without disrupting service.
b) Ensures that a fresh SA, supporting an existing CA, can be used within a known bounded time (1 second, see 8.1.9) at intervals that are also bounded (keys can be changed as frequently as once every 10 seconds) after Key Agreement provides the associated SAK.
c) Allows operation of the Key Agreement protocol to be independent of MACsec. In particular allows fresh SAKs to be supplied at any time, without unnecessarily disrupting communication.

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

The security provided by each SAK rests on the security provided by the Cipher Suite, which in turn depends on the guarantees provide by the cryptographic mode of operation and its underlying block cipher, and on the protocols and procedures used to ensure that keys remain secret. Every implementation of MACsec that conforms to this standard uses only cryptographic modes of operation and block ciphers that have been the subject of open public scrutiny (see Clause 14 for requirements).

8.1.2 Manageability requirements

The design of MACsec ensures that the protocols that configure, and that run over media, individual LANs, and Bridged or Virtual Bridged Local Area Networks as a whole, can continue to operate with no diminution in the capabilities available to and customarily used by network administrators. Existing firewall and forwarding filters can still be applied to specific protocols.

When the Default Cipher Suite is used for integrity protection without confidentiality protection, protocol analyzers and other tools can understand the User Data transmitted, but cannot modify that data without the receiving SecY being aware of the intrusion. This capability is also available whenever the Secure Data remains the same as the User Data and the Integrity Check Value (ICV) length is the same as that of the Default Cipher Suite.

Where MACsec supports a shared media CA, or a point-to-point CA that uses shared transmission facilities, MACsec can convey the SCI (7.1.2, 8.2.1, 9.9), thus identifying the secure system that transmitted the MPDU both to the intended recipient and to network management systems.

8.1.3 Interoperability requirements

Interoperability between independent implementations of MACsec is facilitated by mandatory implementation of a Default Cipher Suite.

The use of Cipher Suites as a specification tool reduces the number of permutations of cryptographic algorithms and their parameters. Clause 14 mandates elements of Cipher Suite specification.

Where the underlying MAC Service used by MACsec is supported by a Provider Bridged Network (P802.1ad), communicating SecYs can be attached to different media operating (locally) at different transmission rates. Interoperability between, for example, 10 Gb/s and 1 Gb/s, and between 1 Gb/s and 100 Mb/s requires interoperability across the speed range. The design of MACsec facilitates interoperability from 1 Mb/s to 100 Gb/s without modification or negotiation of protocol formats and parameters. Operation at higher transmission rates depends on the capabilities of the Cipher Suite. The mandatory default Cipher Suite has been selected (Clause 14) in part because of its ability to perform across this range.

NOTE 1—Clearly additional ways of interconnecting different media access control methods could be standardized in the future. The above requirement mandates that interoperability be preserved between SecYs attached to a wide range of media operating over a wide speed range.

Communication between SecYs using different media access methods requires that MACsec not make use of any media specific additions to the MAC Service, or rely on any deficiencies in support of the service being common to all communicating participants. MACsec includes an explicit indication of the length of the Secure Data to avoid imposing the minimum frame size and padding requirements of IEEE Std 802.3 on all other media access methods that make use of MACsec.

8.1.4 Deployment requirements

The design of MACsec allows security to be introduced into a network one LAN at a time. Additionally the controls provided by a SecY (Clause 10) allow the deployment of MACsec capable systems one by one on a LAN, prior to enabling security. Integrity checking of MPDUs using the Default Cipher Suite can be disabled to facilitate testing of Key Agreement protocols prior to enabling security. Management counters allow a network system administrator to confirm that the connectivity provided by a SecY is complete and that enabling security will not disrupt existing required connectivity.

8.1.5 Coexistence requirements

The design of MACsec allows coexistence with other protocols on the same insecure LAN. This

a) Supports incremental deployment (8.1.4)
b) Allows fresh keys to be derived, using Key Agreement protocols that can be independently specified and use different frame formats, while MACsec is operating
c) Supports use of shared media providing independent services

8.1.6 Scalability requirements

The resources required to support MACsec in any single LAN station (an end station or a Bridge Port) are a function of the number of the SecY peers on the same LAN, but are independent of other systems attached to the same network but not the same LAN.

8.1.7 Intrusion detection

Intrusion detection is facilitated by integrity and replay protection, and the management counters (10.7) that record the receipt of invalid (presumably modified) and repeated and misordered (likely to be replayed) frames. Management for client policies (7.3) that use the guaranteed connectivity provided by MACsec should also record attempted violations.

8.1.8 Localization and isolation of attacks

MACsec discards frames sent by systems that are not authenticated and authorized members of the CA, thus localizing the traffic sent by those stations to a single LAN. The authorization accorded by the policies enforced by clients of MACsec (7.3.1) can restrict unauthorized attempts to affect protocols that control the network infrastructure. Where communication that does result in unauthorized behavior elsewhere in the network has been permitted, the use of MACsec by the intervening systems allows tracing of the source of that communication.

8.1.9 Implementation

The design of MACsec allows the SecY to function asynchronously with respect to other processes in the system. Key Agreement protocols and changes of SAKs are not tightly synchronized to the service requests and indications processed by the SecY. Delays in communication and variations in scheduling between the SecY and KaY can be as much as one second, allowing autonomous processing of frames in real time by the SecY while the KaY can operate as a normally scheduled software process. Time is also allowed for the KaY to compute keys and for the SecY to compute key schedules, and perform other preprocessing.

8.2 Protocol support requirements

The support of MACsec places requirements on

a) The secure system of which the SecY forms a part for
    1) SC identification (8.2.1)
    2) Support of transmit and receive SAKs (8.2.2)
b) The functionality provided by Key Agreement protocols, and the operation of the KaY for
    1) Independence of KaY operation from MACsec operation and state (8.2.3)
    2) Discovering connectivity (8.2.4)
    3) Authentication (8.2.5)
    4) Authorization (8.2.6)
    5) Key exchange and maintenance (8.2.7)

8.2.1 SC identification requirements

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

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

8.2.2 SA Key requirements

On transmit the Cipher Suite implementation shall be able to

a) Install, i.e. prepare for use, a new SAK within one second (8.1.9) of being given it by the KaY
b) Change from the use of one installed SAK to the next within the time normally taken to transmit one minimum sized frame, and shall not discard any frames as a result of the change

NOTE—Elsewhere in this standard the requirement for switching between SAKs is modelled as a requirement to support two SAKs for transmission, allowing management counters to reflect the continued use of a key after its successor has been provided by the KaY. The behavior of an implementation capable of accepting the new key and using it within one frame time is fully conforming, and will not cause any apparent management anomalies.

On receive the Cipher Suite implementation shall be able to

c) Receive any frame and its immediate successor using any one of two SAKs, allowing the selection of different keys switch without missing a frame.
d) Install, i.e. prepare for use, a new SAK within one second (8.1.9) of being given it by the KaY

The system does not need to be able to seamlessly switch between Cipher Suites.

8.2.3 KaY independence of MACsec

The KaY is aware of the required connectivity, identifying the SCs that compose the CA, independently of the design and state of MACsec.

The KaY operates resiliently in face of specifically identified denial of service attacks (as identified by the key agreement protocol specfiication).

These requirements are met in part by distinguishing key agreement frames from MACsec frames by using a different EtherType.

8.2.4 Discovering connectivity

The KaY discovers connections between peer stations, and recognizes potential connections.

NOTE 1— The MAC status parameters (6.4) indicate when connectivity changes. The status parameters provided by the KaY can also temporarily transition false to indicate a change in the authentication or authorization of its peers, preventing attacks that secretly degrade the trust.

The KaY accepts indications of which Cipher Suites are supported by the SecY via the LMI.

NOTE 2—The negotiation of which Cipher Suite is to be used on a connection is based on what Cipher Suites are available locally and at the peer SecY.

The KaY accepts indications of which connectivity capabilities are supported by the SecY via the LMI. The KaY delivers the connectivity selection to the SecY via the LMI.

8.2.5 Authentication requirements

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

8.2.6 Authorization requirements

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

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

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

8.2.7 Key exchange and maintenance

The KaY delivers transmit and receive SAKs via the LMI.

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.

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

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.

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

8.3 MACsec operation

MACsec comprises modification and additions to the MAC Service Data Unit (MSDU) conveyed by each frame transmitted by a user of the protocol, and illustrated in Figure 8-1. The MAC Security TAG (SecTAG) conveys parameters that identify the protocol, identify the key to be used to validate the received frame, and provide replay protection. The Secure Data field conveys the User Data, encrypted if confidentiality is provided. The ICV ensures the integrity of the MAC Destination Address, MAC Source Address, SecTAG, and User Data.

NOTE—The addition of the SecTAG and ICV to the MPDU, together with possible expansion of the User Data when conveyed in the Secure Data field can increase the size of a frame that could be insecurely transmitted using a media access method to the point that it no longer conforms to the maximum frame size specified by the media access method standard. If the implementation of the service used by MACsec cannot transmit the resulting MPDU, it is discarded.

MACsec does not transmit additional frames, such as keep alives or key exchanges. Each frame is delivered unmodified to peer users, subject to validation of the origin, destination and source address, and user data.

Figure 8-2 illustrates the transmission and reception of a frame by MACsec.

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

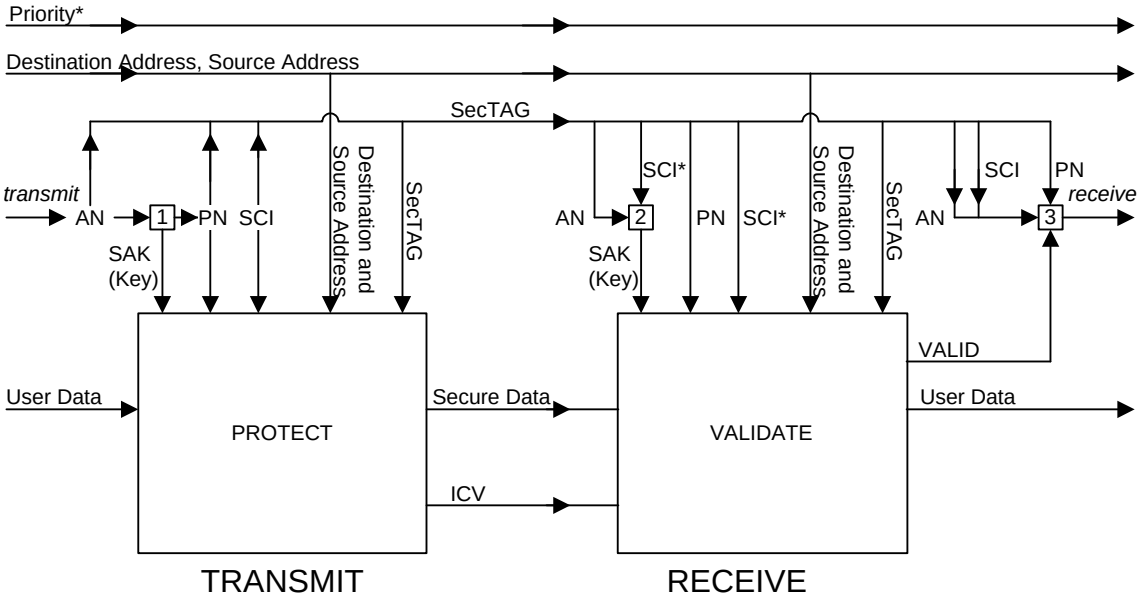
along with the MACsec Ethertype (9.8) and the number of octets in the frame following the SecTAG (SL, 9.7) if less than 64 (8.1.3).

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 ICV.

On receipt of a MACsec frame, the AN, SCI, PN, and SL field (if present) are extracted from the SecTAG (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.

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.

If the receive frame is valid, replay protection (if enabled) is applied, by checking that the received PN is not less than the lowest acceptable PN for the SA. If the check succeeds the parameters of the frame, unchanged from those transmitted, are presented to the MACsec client, and the lowest acceptable PN updated. The lowest acceptable PN can lag behind the received PN values, providing a window in which replay is tolerated, to allow receipt of frames that have been misordered by the network.



* Priority can be changed by media access method or receiving system and is not protected
* 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.

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

The format and encoding of each of the fields that comprise the SecTAG, including the support of different MACsec protocol versions is specified in Clause 9. The operation of the SecY that operates the MACsec protocol, the service that it provides, and the management control variables, error handling, and diagnostic information recorded is described in Clause 10.

9. Encoding of MACsec protocol data units

This clause specifies the structure and encoding of the MACsec Protocol Data Units (MPDUs) exchanged between MAC Security Entities (SecYs). It

a) Specifies rules for the representation and encoding of protocol fields
b) Specifies the major components of each MPDU, and the fields they comprise
c) Reviews the purpose of each field, and the functionality provided
d) Specifies validation of the MPDU on reception
e) Documents the allocation of an EtherType value, the MACsec Ethertype, to identify MPDUs

NOTE—The MPDU validation checks specified in this clause are deliberately limited to ensuring successful decoding, and do not overlap with the specification of SecY operation (Clause 10).

9.1 Structure, representation, and encoding

All MPDUs shall contain an integral number of octets.

The octets in a MPDU are numbered starting from 1 and increasing in the order they are put into the MAC Service Data Unit (MSDU) that accompanies a request to or indication from the instance of the MAC Internal Sublayer Service (ISS) used by a SecY.

The bits in an octet are numbered from 1 to 8 in order of increasing bit significance, where 1 is the least significant bit in the octet.

Where octets and bits within a MPDU are represented using a diagram, octets shown higher on the page than subsequent octets and octets shown to the left of subsequent octets at the same height on the page are lower numbered, bits shown to the left of other bits within the same octet are higher numbered.

Where two or more consecutive octets are represented as hexadecimal values, lower numbered octet(s) are shown to the left and each octet following the first is preceded by a hyphen, e.g. 01-80-C2-00-00-00.

When consecutive octets are used to encode a binary number, the lower octet number has the more significant value.When consecutive bits within an octet are used to encode a binary number, the higher bit number has the most significant value. When bits within consecutive octets are used to encode a binary number, the lower octet number composes the more significant bits of the number. A flag is encoded as a single bit, and is set (True) if the bit takes the value 1, and clear (False) otherwise. The remaining bits within the octet can be used to encode other protocol fields.

9.2 Major components

Each MPDU comprises

a) A Security TAG (SecTAG) (9.3)
b) Secure Data (9.10)
c) An Integrity Check Value (ICV) (9.11)

Each of these components comprises an integral number of octets and is encoded in successive octets of the MPDU as illustrated in Figure 9-1.

NOTE—The MPDU does not include the source and destination MAC addresses, as these are separate parameters of the service requests and indications to and from the insecure service that supports MACsec.

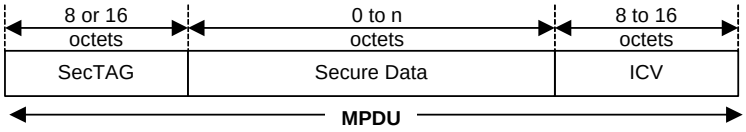


Figure 9-1—MPDU components

9.3 Security TAG

The Security TAG (SecTAG) is identified by the MACsec Ethertype (9.4), and conveys the

a) TAG Control Information (TCI, 9.5)
b) Association Number (AN, 9.6)
c) Short Length (SL, 9.7)
d) Packet Number (PN, 9.8)
e) Optionally encoded Secure Channel Identifier (SCI, 9.9).

The format of the SecTAG is illustrated in Figure 9-2.

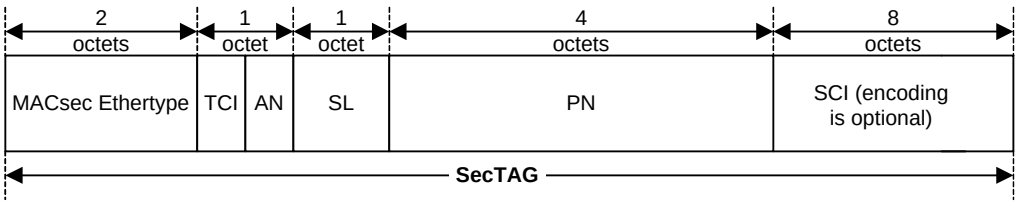


Figure 9-2—SecTAG format

9.4 MACsec Ethertype

The MACsec Ethertype (Table 9-1) comprises octet 1 and octet 2 of the SecTAG. It is included to allow

a) Coexistence of MACsec capable systems in the same environment as other systems
b) Incremental deployment of MACsec capable systems
c) Peer SecYs to communicate using the same media as other communicating entities
d) Concurrent operation of Key Agreement protocols that are independent of the MACsec protocol and the Current Cipher Suite
e) Operation of other protocols and entities that make use of the service provided by the SecY's Uncontrolled Port to communicate independently of the Key Agreement state

Table 9-1—MACsec EtherType allocation

Tag Type	Name	Value
802.1AE Security TAG	MACsec EtherType	<<to be assigned>>

The encoding of the MACsec Ethertype in the MPDU is illustrated in Figure 9-3.

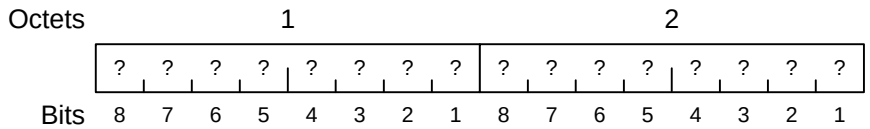


Figure 9-3—MACsec EtherType encoding

<<NOTE—The MACsec EtherType value will not be assigned until the start of the IEEE Sponsor Ballot. Delaying the assignment to this time, is established 802.1/802.3 policy and is explicitly intended to minimize the chance of sponsor ballot voters being effectively deprived of their vote by prior development of an 'installed base'. Implementors should note that other fields in MPDUs may be miscellaneously varied through the course of development of this standards project.>>

9.5 TAG Control Information (TCI)

The TCI field comprises bits 8 through 3 of octet 3 (Figure 9-4) of the SecTAG. These bits facilitate

a) Version numbering of the MACsec protocol without changing the MACsec Ethertype
b) Optional use of the MAC Source Address parameter to convey the SCI
c) Optional inclusion of an explicitly encoded SCI (7.1.2, Figure 7-7)
d) Use of the EPON (12) Single Copy Broadcast capability, without requiring an explicit SCI to distinguish the SCB Secure Channel
e) Extraction of the User Data from MPDUs by systems that do not possess the SAK (8.1.2, 8.1.4) when confidentiality is not being provided
f) Determination of whether confidentiality or integrity alone are in use

The encoding of the MACsec TCI in the MPDU is illustrated in Figure 9-4.

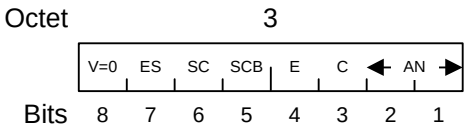


Figure 9-4—MACsec TCI and AN Encoding

The version number shall be 0 and is encoded in bit 8.

NOTE—Future versions of the MACsec protocol may use additional bits of the TCI to encode the version number. The fields and format of the remainder of the MPDU may change if the version number changes.

If the MPDU is transmitted by an end station and the first 6 octets of the SCI are equal to the value of the octets of MAC Source Address parameter of the ISS request in canonical format order, bit 7 (the End Station (ES) bit) of the TCI may be set. If the ES bit is set, bit 6 (the SC bit) shall not be set and an SCI shall not be explicitly encoded in the SecTAG. The ES bit is clear if the Source Address is not used to determine the SCI.

If an SCI (9.9, 7.1.2) is explicitly encoded in the SecTAG, bit 6 (the SC bit) of the TCI shall be set. The SC bit shall be clear if an SCI is not present in the SecTAG.

If and only if the MPDU is associated with the Secure Channel that supports the EPON Single Copy Broadcast capability, bit 5 (the SCB bit) of the TCI may be set. If the SCB is set, bit 6 (the SC bit) shall not be set and an SCI shall not be explicitly included in the SecTAG.

If the ES bit is set and the SCB is not set, the SCI comprises a Port Identifier (7.1.2) component of 00-01. If the SCB bit is set, the Port Identifier (7.1.2) component has the reserved SCB value of 00-00.

If the Encryption (E) bit is set and the Changed Text (C) bit is clear the frame is not processed by the SecY (10.6), but is reserved for use by the KaY. Otherwise, the E bit is set if and only if confidentiality is being provided and is clear if integrity only is being provided, and the C bit is clear if and only if the Secure Data is exactly the same as the User Data and the ICV is 16 octets long.

When the Default Cipher Suite (14.5) is used for integrity protection only the Secure Data is the unmodified User Data, and a 16 octet ICV is used. Both the E bit and the C bit are therefore clear, and the data conveyed by MACsec is available to applications, such as network management, that need to see the data but are not trusted with the SAK that would permit its modification. Other Cipher Suites may also integrity protect data without modifying it, and use a 16 octet ICV, enabling read access to the data by other applications. The E and C bits are also clear for such Cipher Suites when integrity only is provided.

Some cryptographic algorithms modify or add to the data even when integrity only is being provided, or use an ICV that is not 16 octets long. The C bit is never clear for such an algorithm, even if the E bit is clear to indicate that confidentiality is not provided. Recovery of the data from a MACsec frame with the E bit clear and the C bit set requires knowledge of the Cipher Suite at a minimum. That information is not provided in the MACsec frame.

If both the C and E bits are set confidentiality of the original User Data is being provided.

9.6 Association Number (AN)

The AN is encoded as an integer in bits 1 and 2 of octet 3 (Figure 9-4) of the SecTAG, and identifies up to 4 different SAs within the context of an SC.

NOTE—Although each receiving SecY only needs to maintain two SAs per SC, the use of a 2 bit AN simplifies the design of protocols that update values associated with each of the SAs.

9.7 Short Length (SL)

SL is an integer encoded in bits 1 through 6 of octet 4 of the SecTAG, and is set to the number of octets in the Secure Data (9.10) field, i.e. the number of octets between the last octet of the SecTAG and the first octet of the ICV, if that number is less than 64. Otherwise SL is set to zero. If the number is zero then the frame is deemed not to have been short. The Secure Data field always comprises at least one octet.

Bits 7 and 8 of octet 4 shall be zero.

9.8 Packet Number (PN)

The PN is 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—As specified in Clause 9, the IV used by the default Cipher Suite (GCM-AES-128) comprises the SCI (even if the SCI is not transmitted in the SecTAG) and the 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.

9.9 Secure Channel Identifier (SCI)

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

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

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

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

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

An explicitly encoded SCI field in the SecTAG is not required on point to point links, which are identified by the operPointToPointMAC status parameter of the service provider. 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 Clauses 8, 9, 10), the SCI still forms part of the cryptographic computation.

9.10 Secure Data

The Secure Data comprises all the octets that follow the MACsec TAG and precede the ICV. The Secure Data field is never of zero length, since the primitives of the MAC Service require a non-null MSDU (User Data) parameter.

NOTE 1—In practice, if the MSDU composed by the operation of the current Cipher Suite following MPDU reception contains less than two octets, it will be discarded by the user of the SecY's controlled port, since it is too short to contain an EtherType or an LLC length field. Such discard is, however, determined by the user of the Controlled Port and not by the SecY itself.

NOTE 2—Ethernet transports frames of a minimum size, and provides no explicit indication of PDU length if the PDU is composed of fewer octets. The SL field allows the originator of the frame, which is not necessarily aware of the need of an intervening Ethernet component to pad the frame, to specify the number of octets in the MPDU, thus allowing the receiver to unambiguously locate the ICV.

9.11 Integrity Check Value (ICV)

The length of the ICV is Cipher Suite dependent, but is not less than 8 octets and not more than 16 octets, depending on the Cipher Suite.

NOTE—The ICV protects the destination and source MAC address parameters, as well as all the fields of the MPDU.

9.12 PDU validation

A received MPDU is valid if and only if it comprises a valid SecTAG, one or more octets of Secure Data, and an ICV, i.e.

a) It comprises at least 17 octets
b) Octets 1 and 2 compose the MACsec Ethertype
c) The V bit in the TCI is clear
d) If the ES or the SCB bit in the TCI is set, then the SC bit is clear
e) Bits 7 and 8 of octet 4 of the SecTAG are clear
f) If the C and SC bits in the TCI are clear, the MPDU comprises 24 octets plus the number of octets indicated by the SL field if that is non-zero and at least 88 octets otherwise
g) If the C bit is clear and the SC bit set, then the MPDU comprises 32 octets plus the number of octets indicated by the SL field if that is non-zero and at least 96 octets otherwise
h) If the C bit is set and the SC bit clear, then the MPDU comprises 8 octets plus the minimum length of the ICV as determined by the Cipher Suite in use at the receiving SecY, plus the number of octets indicated by the SL field if that is non-zero and at least 64 additional octets otherwise
i) If the C and SC bits are both set, the frame comprises at least 16 octets plus the minimum length of the ICV as determined by the Cipher Suite in use at the receiving SecY, plus the number of octets indicated by the SL field if that is non-zero and at least 64 additional octets otherwise

10. Principles of MAC Security Entity (SecY) operation

This clause

a) Provides an overview of the SecY (10.1), the service that it provides, and its relationship to other entities in a secure system including its associated MACsec Key Agreement Entity (KaY).
b) Describes the functionality of the SecY (10.2).
c) Provides a model of operation (10.3) comprising an architecture (10.4) and its constituent processes (through 10.7) that supports the detailed functionality including management controls.
d) Details the addressing requirements and specifies the addressing of SecYs (10.8).

NOTE—Clause 6 defines the properties of the secure MAC Service, Clause 7 described the security relationships used to support the service, and how the service is used, providing the context within which each SecY operates, Clause 8 sets out requirements for the MACsec protocol and introduces the operation of the protocol, and Clause 9 specifies the encoding of parameters in MPDUs. This clause does not repeat all the information provided in those prior clauses, but includes sufficient reference to facilitate an understanding of SecY operation.

10.1 SecY overview

Each SecY uses the MAC Service provided by a Common Port (10.4) to provide one instance of the secure MAC Service (Clause 6), to the user of its Controlled Port, and one instance of insecure service, to the user of its Uncontrolled Port (Figure 10-1).

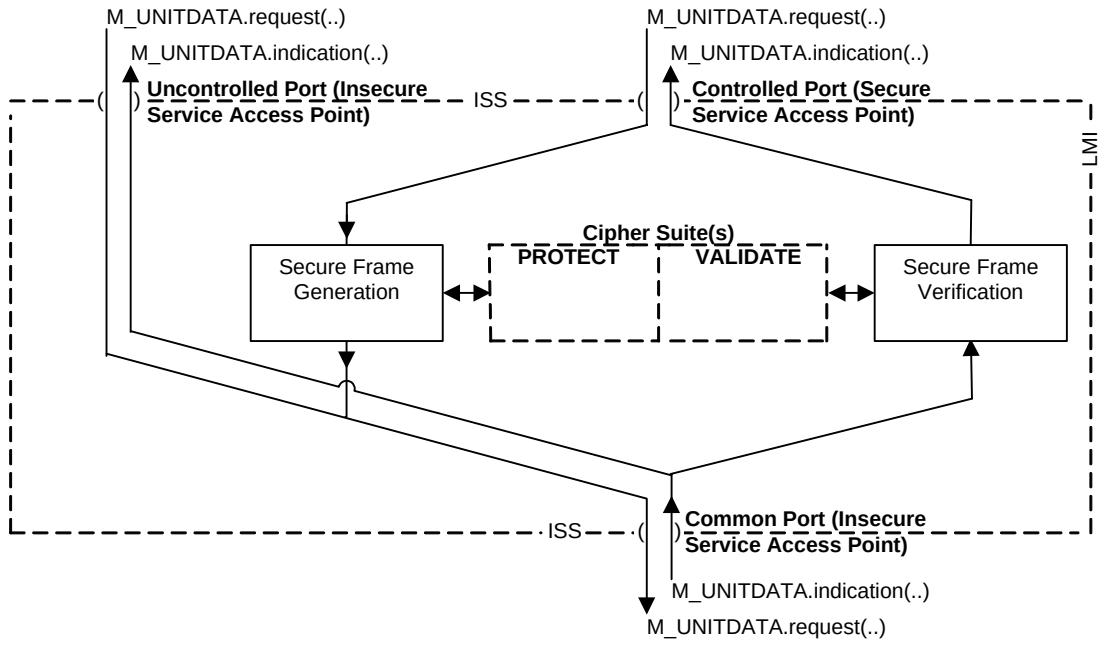


Figure 10-1—SecY

The integrity and origin of the parameters of each service request and indication accepted from and delivered to the Controlled Port are protected and validated by the SecY. The SecY may also encrypt to provide user data confidentiality. If the parameters that accompany a service indication at the Common Port are not successfully validated as required by management controls, no service indication will occur at the Controlled Port and the received parameters will be discarded.

Each service request made by the user of a SecY's Uncontrolled Port results in an identical request at the Common Port, and each service indication received from the Common Port results in an identical indication to the user of its Uncontrolled Port in addition to any indication at the Controlled Port.

The relative order of Common Port indications and the corresponding indications at the Uncontrolled Port and the Controlled Port is not defined, save that the order of indications from one Port to another Port is preserved. Similarly the relative order of user requests at the Uncontrolled and Controlled Ports does not define the order of requests to the Common Port. The interval between any request or indication and the SecY making a corresponding request or indication shall not exceed the bounds specified in Table 10-1.

The specification of the cryptographic algorithms used at any time to provide integrity and confidentiality, together with the values of parameters (for example, key size) used by those algorithms, compose a Cipher Suite (Clause 14). This standard mandates a default Cipher Suite that can provide integrity protection only or both integrity and confidentiality. A SecY may implement additional Cipher Suites. This standard only permits the use of Cipher Suites that meet well defined criteria (14.2, 14.3).

The KaY associated with the SecY uses the service provided by the Uncontrolled Port to transmit and receive frames that support key agreement protocols. These frames are distinguished by EtherType, so other selected protocol entities can communicate using unsecured frames by making use of an Uncontrolled Port provided by the KaY as illustrated in Figure 10-2.

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

NOTE 1—Operation of the SecY without protection or validation allows the same interfaces and relationships to be maintained between entities within a system when SecY functionality is not required. This provides a useful migration path for networks comprising systems that will incorporate SecY functionality at different times.

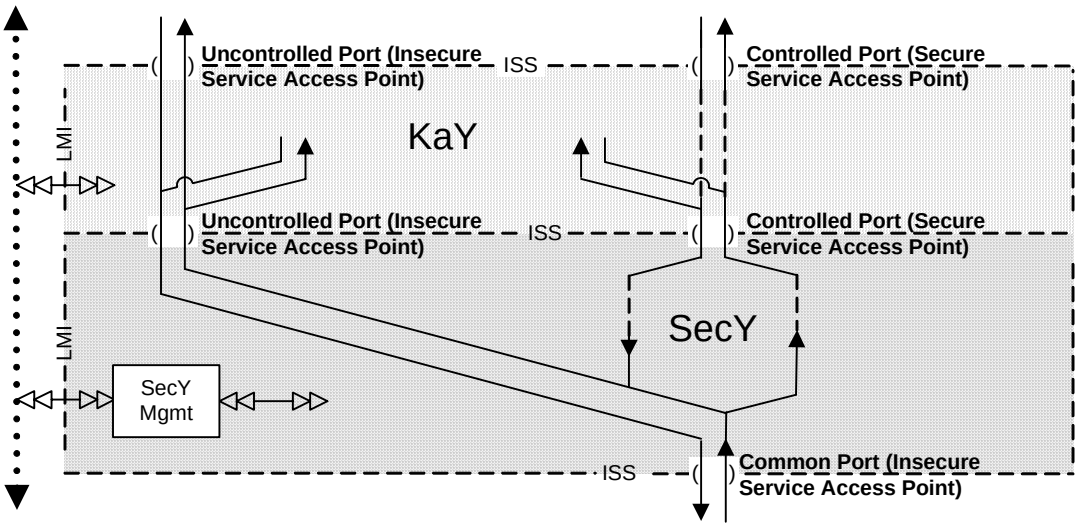


Figure 10-2—KaY use of SecY Uncontrolled and Controlled Ports

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

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

10.2 SecY functions

Each SecY supports

a) Secure transmission of the parameters of service requests made by the user of its Controlled Port.
b) Unsecured transparent transmission from the Uncontrolled Port.
c) Reception, verification, and delivery of secure service indications to the Controlled Port.
d) Reception and transparent delivery of service indications to the Uncontrolled Port.
e) MAC Status (6.4) and point-to-point parameters (6.5) for the Uncontrolled and Controlled Ports.

Management controls that support deployment (8.1.4) of MACsec include

f) Transmission and reception by the user of the Controlled Port without frame modifications.
g) Reception without integrity checking.
h) A replay window to support use of MACsec over provider networks that misorder frames with different transmission priority and or addresses. Frames within the window can be received out of order, but are not replay protected. The window size can be set to zero to enforce strict reception ordering and replay protection.

Selection of a Cipher Suite, CA establishment, and SA support, is supported by allowing the KaY to

i) Discover which Cipher Suites are implemented, and how many receive SCs each can support.
j) Select the Current Cipher Suite.
k) Identify the SCs to be used to support reception for the CA.
l) Provide transmit and receive SAKs for identified SAs.
m) Confirm that SAKs have been installed, i.e. are ready for use.
n) Monitor the PN used for transmission, in order to provide new SAKs prior to PN exhaustion.

Operational and diagnostic controls and statistics, provide

o) Administrative control over the optional security tagging capabilities of the SecY.
p) A count of frames intended for transmission but discarded as too long for the Common Port.
q) Counts of received frames without the MACsec Ethertype, discarded by validation checks, without SCIs when the LAN connectivity is not restricted to point-to-point communication, identified as belonging to unknown SCs, identified as belonging to an SA that is not in use, failing the replay check, failing the integrity check, and delivered to the user.

NOTE—Except where explicitly specified otherwise, throughout this Standard the term “user” refers to the user of the MAC service instance provided by the Controlled Port, and the term “provider” refers to the instance of protocol and procedures that provides the MAC service instance to the SecY at the Common Port.

10.3 Model of operation

The model of operation in this clause is simply a basis for describing the functionality of a SecY. It is in no way intended to constrain real implementations; these may adopt any internal model of operation compatible with the externally visible behavior that this standard specifies. Conformance of equipment to this standard is purely in respect of observable protocol.

10.4 SecY architecture

A SecY uses an instance of the MAC Internal Sublayer Service (ISS, 6.1), referred to as the Common Port, to provide a secured instance of the ISS, the Controlled Port, and an unsecured instance of the ISS, the Uncontrolled Port, that provides transparent transmission and reception through the Common Port.

The architecture of a SecY is illustrated in Figure 10-3, and comprises

a) The Controlled, Uncontrolled, and Common Ports together with their MAC Status parameters.
b) The Secure Frame Generation process ().
c) The Secure Frame Verification process (10.6).
d) Cipher Suite protection of transmitted frames and validation of received frames (8.2, 14).
e) A Transmit Multiplexer, and a Receive Demultiplexer.
f) Optional transmit and receive FCS Regenerators.
g) A SecY Management process (10.7).

The Transmit Multiplexer accepts transmit requests from the Uncontrolled Port and the Secure Frame Generation process for the Controlled Port, and submits corresponding requests to the Common Port. The Receive Demultiplexer submits each indication from the Common Port to the Uncontrolled Port and to the Secure Frame Verification process for the Controlled Port.

NOTE—This specification most clearly sets out the resulting behavior of a conforming implementation. Real implementations can implement the behavior in any way that yields the same externally visible behavior (including the values of management counters). For example, examination of the specification in this Clause shows that there need be no implementation burden corresponding to duplication of the received frame if protectFrames is set and none of the users of the Uncontrolled Port make use of the MACsec Ethertype.

A Layer Management Interface (LMI) is used by the SecY Management process to communicate the capabilities of the SecY, its controls, status, protocol and management events and counters to and from other entities that compose the secure system containing the SecY.

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

A frame check sequence (FCS) can be included as a parameter of an M_UNITDATA.request or M_UNITDATA.indication primitive. When the data that is within the FCS coverage is modified, by the addition of an integrity check value (ICV), or encryption of the user data, the FCS changes. The SecY shall not introduce an undetected frame error rate greater than that which would have been achieved by preserving the original FCS (6.10).

NOTE 2—There are number of possibilities for changing FCS without diminishing the coverage provided. One is to generate a new FCS by algorithmically modifying the received FCS, based on knowledge of the FCS algorithm and the transformations that the frame has undergone between reception and transmission.

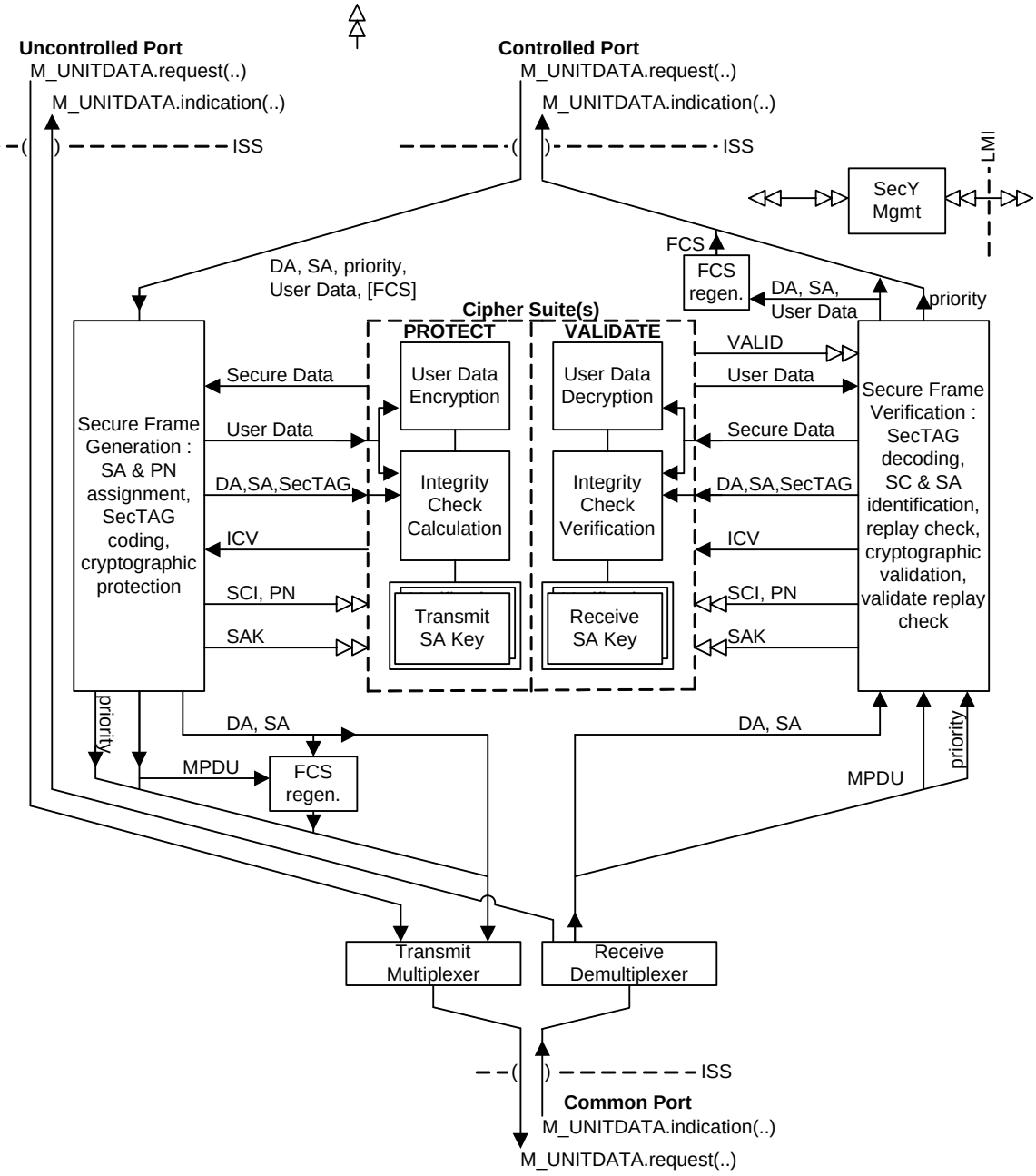


Figure 10-3—SecY architecture and operation

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 (10.5.2)
c) Encodes the octets of the SecTAG (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.

10.5.1 Transmit SA assignment

Each SA is identified by its Association Number (AN). Each frame is assigned to the SA identified by the current value of the encodingSA variable. This is updated following an LMI request from the KaY to start transmitting using the SA, and can be read but not written by network management. Frames will be protected using the encodingSA immediately after the last frame assigned to the previous SA has been protected.

If the SA identified by the encodingSA is not available for use, and the management control protectFrames is set, the SecY management process sets MAC_Operational false for the Controlled Port, and frames are neither accepted or delivered using the port.

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}) and the protectFrames control is set, MAC_Operational is set 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.

10.5.3 SecTAG encoding

The SecTAG is encoded as specified in Clause 9.

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

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

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

The values of useES, useSCB, and alwaysIncludeSCI can be written and read by management. The number of active receive SCs is controlled by the KaY, but can be read by management.

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

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

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

10.5.4 Cryptographic protection

If the Cipher Suite is currently protecting frames using the previous SA and its SA Key, as reflected by the value of the encipheringSA, the frame can be queued awaiting protection. The value of the encipheringSA is updated, and protection of the frame parameters is started within a minimum frame size transmission delay, after the last frame has been protected using the previous key.

The use of each of the Cipher Suites specified by this standard is specified in Clause 14. That clause takes precedence over any explanation in this or other clauses.

The appropriate octet counter is incremented by the number of octets in the User Data (OutOctetsEncrypted if confidentiality protection was provided, and OutOctetsProtected otherwise).

10.5.5 Transmit request

If the MPDU composed of the concatenated octets of the SecTAG, Secure Data, and ICV exceeds the size of the MSDU supported by the Common Port, the frame is discarded and a counter incremented. Details of the

discarded frame may be recorded to assist network management resolution of the problem. Otherwise the parameters of the service request are submitted to the Transmit Multiplexer.

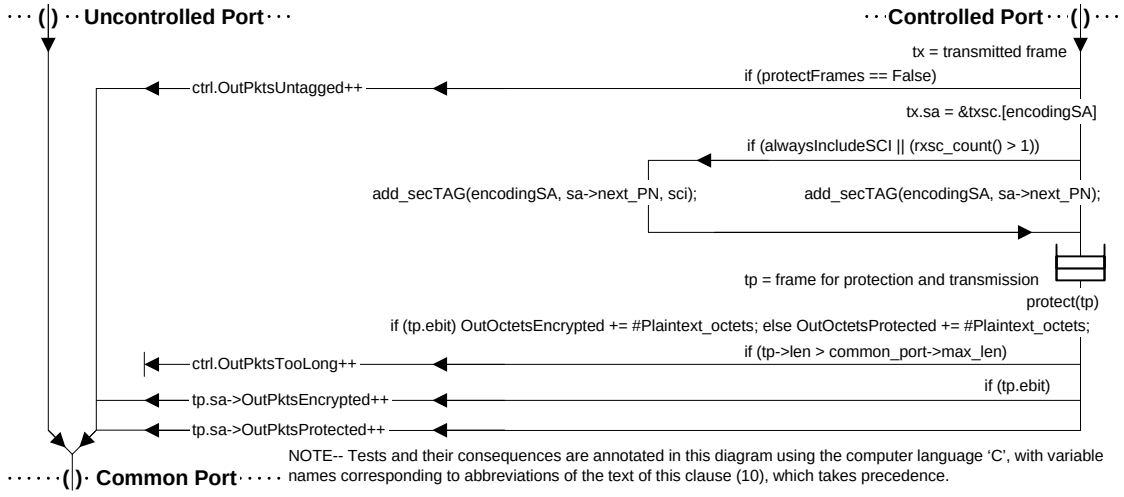


Figure 10-4—Management controls and counters for secure frame generation

10.6 Secure frame verification

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 clause 9.12
c) Extracts and decodes the SecTAG as specified in clauses 9.3 through 9.9
d) Extracts the User Data and ICV as specified in clauses 9.10 and 9.11
e) Assigns the frame to an SA (10.6.1)
f) Performs 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.

10.6.1 Receive SA assignment

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

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

a) If validateFrames is Strict or the C bit in the SecTAG is set, the InPktsNoSCI counter is incremented and the frame is discarded; otherwise
b) The InPktsUnknownSCI counter is incremented and the frame (with the SecTAG and ICV removed) is delivered to the Controlled Port.

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

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

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

10.6.2 Preliminary replay check

If replayProtect control is enabled and the PN 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—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.

10.6.3 Cryptographic validation

The frame can be queued awaiting validation. If the frame reception rate exceeds the Cipher Suite's validation capabilities the frame may be discarded, and the InPktsOverrun counter incremented.

If the validateFrames control is Disabled, the Cipher Suite validation is not used to validate the frame.

If validateFrames is not Disabled, and the E bit in the SecTAG is set, the Cipher Suite is used to validate and decrypt the frame. If the Cipher Suite does not provide confidentiality protection it shall not return VALID. The InOctetsDecrypted counter is incremented by the number of octets in the resulting User Data (or an estimate of that number, if VALID is not returned).

If validateFrames is not Disabled, and the E bit in the SecTAG is clear, the Cipher Suite is used to validate the frame. If the Cipher Suite does not provide integrity protection without confidentiality it shall not return VALID. The InOctetsValidated counter is incremented by the number of octets in the resulting User Data (or an estimate of that number, if VALID is not returned).

The frame is marked valid if the Cipher Suite is used and returns VALID, and is marked invalid otherwise. The use of each of the Cipher Suites specified by this standard is specified in Clause 14. That clause takes precedence over any explanation in this or other clauses.

10.6.4 Replay check update

If the PN of the received frame is less than the lowest acceptable packet number for the SA, and replayProtect is enabled, the frame is discarded and the InPktsLate counter incremented.

NOTE—This model of operation assumes that any queuing within the verification process occurs prior to frame validation, and the check described uses the lowest acceptable PN updated by prior frames as described below (10.6.5). Implementations can process frames as convenient, provided the externally observable result is the same.

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 PN value of zero as 2^{32}), 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, 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.

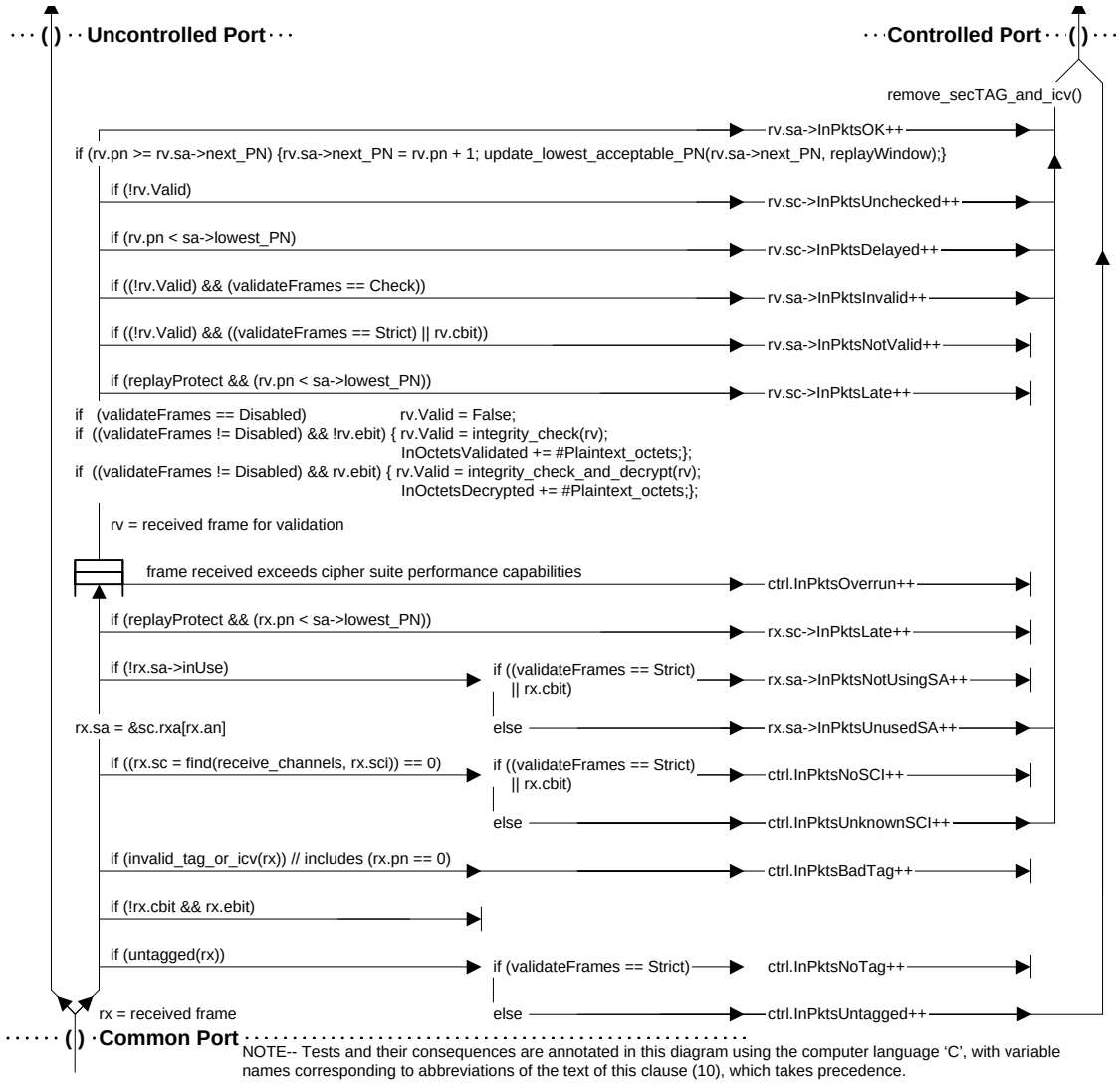


Figure 10-5—Management controls and counters for secure frame verification

10.7 SecY management

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

a) Reports the value of the SCI for the SecY (10.7.1)
b) Maintains the MAC Status (6.4) parameters and point-to-point MAC parameters (6.5) for the Uncontrolled (10.7.2) and Controlled (10.7.4) Ports
c) Provides interface statistics for the Uncontrolled (10.7.3) and Controlled Ports (10.7.5), deriving the latter from the detailed statistics maintained by the SecY
d) Provides information on the frame verification (10.7.7) and generation (10.7.16) capabilities
e) Supports control of frame verification (10.7.8) and generation (10.7.17)
f) Supports creation of transmit SAs (10.7.21), each associated with an SAK, for the transmit SC

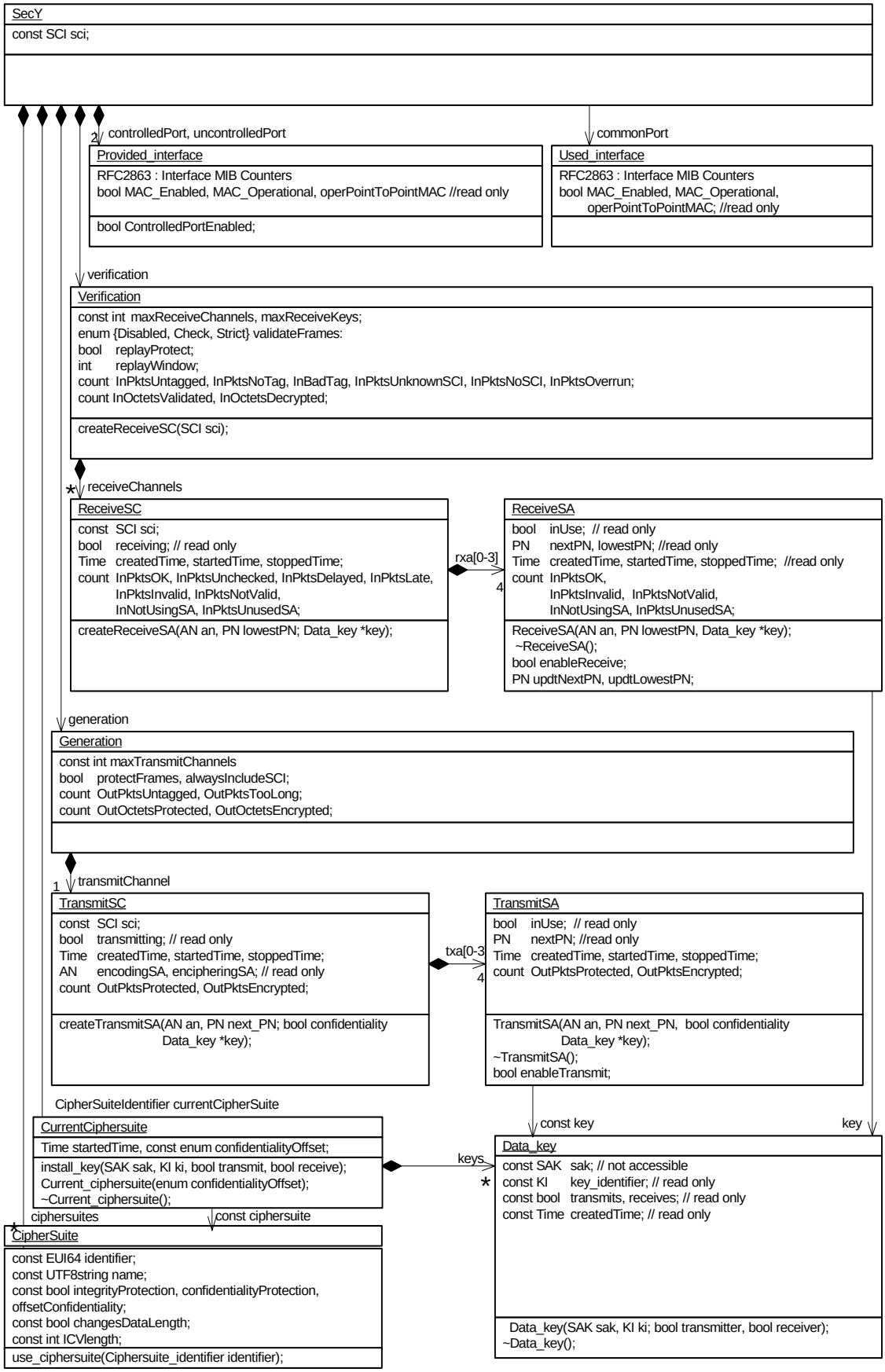


Figure 10-6—SecY managed objects

g) Supports creation of receive SCs (10.7.11), each corresponding to potential member of the CA
h) Supports creation of receive SAs (10.7.13) for each receive SC, each associated with an SAK
i) Supports control over reception (10.7.15) and transmission (10.7.23) using individual SAs, and allows the nextPN variable to be set and updated for transmission and the lowest acceptable PN to be set and update for reception
j) Maintains detail statistics for receive and transmit SCs and SAs, accumulating statistics from past SAs and SCs
k) Provides a list of the Cipher Suites implemented together with their basic capabilities and properties
l) Allows selection of the current Cipher Suite, from those implemented
m) Supports installation of SAKs for the current Cipher Suite, for transmission, reception, or both.

Figure 10-6 illustrates the management information that represents a SecY's capabilities, and provides control over and reporting on its operation. For convenience the figure uses UML 2.0 conventions together with C++ language constructs. For an explanation of these conventions, see [Fowler, 2004]. The containment relationships in Figure 10-6 have been chosen primarily to reflect the necessary relationships between lifetimes of potentially transient objects. For example, a receive SC can contain a succession of SAs, but never more than one per AN at a time, and all receive SAs for an SC are deleted when the receive SC ceases to exist. A paradigm of object creation and deletion is used, instead of one of data structure reuse, to express the required bounding of the lifetime of key information.

Conformance to this standard is strictly in terms of the external behavior required by this standard, as revealed through the relationship of the operation of the SecY to the operations supported by the SMIv2 MIB module (Clause 13) and to the specifications of protocols operated by the KaY. Interactions with the KaY through the LMI are wholly contained within the secure system, and there is no conformance in respect of syntactic elements that are used to describe that interface in this clause. Table 10-1 specifies performance requirements for SecY operation, including maximum delays for the execution of management operations.

In some situations it can be desirable to substitute control using SNMP for the operation of key agreement protocols, and Clause 13 provides all the necessary operations as an option. However misuse of these operations can compromise security, and their availability (including the ability of an administrator to configure access to these operations) may be forbidden in some systems.

10.7.1 SCI

The SCI, a constant parameter of the SecY (7.1.2, 8.2.1), can be read but not written by management.

10.7.2 Uncontrolled Port status

The following status parameters are provided to the user(s) of the Uncontrolled Port, including the KaY, and can be read but not written by management:

a) MAC_Enabled
b) MAC_Operational
c) operPointToPointMAC.

Their values are identical to those for the Common Port. They can be read but not written by management.

10.7.3 Uncontrolled Port statistics

The following statistics are provided to support RFC2863 interface MIB Counters:

a) ifInOctets
b) ifInUcastPkts, ifInMulticastPkts, and ifInBroadcastPkts
c) ifInDiscards
d) ifInErrors
e) ifOutOctets
f) ifOutUcastPkts, ifOutMulticastPkts, ifOutBroadcastPkts
g) ifOutErrors

The ifInOctets, ifInUcastPkts, ifInMulticastPkts, and ifInBroadcastPkts counts are identical to those of Common Port, and are not separately recorded. The ifInDiscards and ifInErrors counts are zero, as the operation of the Uncontrolled Port provides no error checking or occasion to discard packets, beyond that provided by its users or by the entity supporting the Common Port.

The ifOutErrorscount is zero, as no checking is applied to frames transmitted by the Uncontrolled Port.The ifOutOctets, ifOutUcastPkts, ifOutMulticastPkts, ifOutBroadcastPkts counts are the same as those for the user of the Uncontrolled Port.

10.7.4 Controlled Port status

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

a) MAC_Enabled, true if and only if
    1) ControlledPortEnabled (10.7.5) is true, and
    2) MAC_Enabled is true for the Common Port, and
    3) transmitting is true for the transmit SC, and
    4) receiving is true for at least one receive SC.
b) MAC_Operational, true if and only if
    1) MAC_Enabled is true, and
    2) MAC_Operational is true for the Common Port
c) operPointToPointMAC, true if and only if:
    1) validateFrames (10.7.8) is Strict, and receiving is enabled for at most one receive channel, or
    2) validateFrames is not Strict, and operPointToPointMAC is true for the Common Port.

10.7.5 Controlled Port controls

The KaY uses the following parameter(s):

a) ControlledPortEnabled

By setting ControlledPortEnabled False, the KaY can prohibit use of the Controlled Port until the secure connectivity required has been configured.

10.7.6 Controlled Port statistics

The following statistics are provided to support RFC2863 interface MIB Counters:

a) ifInOctets
b) ifInUcastPkts, ifInMulticastPkts, and ifInBroadcastPkts
c) ifInDiscards
d) ifInErrors
e) ifOutOctets
f) ifOutUcastPkts, ifOutMulticastPkts, ifOutBroadcastPkts
g) ifOutErrors

The ifInOctets count is the sum of all the octets of the MSDUs delivered to the user of the Controlled Port by the Secure Frame Verification process (10.6), plus the octets of the destination and source MAC addresses.

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

The ifOutOctets count is the sum of the all octets of the MSDUs delivered by the user of the Controlled Port to the Secure Frame Generation process (), plus the octets of the destination and source MAC addresses.

The ifOutErrors count is equal to the OutPktsTooLong count (, Figure 10-4). If ifOutDiscards is reported as part of RFC2863 counts, it is zero.

10.7.7 Frame verification capabilities

The SecY's frame verification capabilities are represented by the following parameters:

a) Maximum number of receive channels
b) Maximum number of keys in simultaneous use for reception

These parameters can be read but not written by management.

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.

10.7.9 Frame verification statistics

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

a) InPktsUntagged,
b) InPktsNoTag
c) InPktsBadTag
d) InPktsUnknownSCI
e) InPktsNoSCI
f) InPktsOverrun

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

g) InPktsUnchecked
h) InPktsDelayed
i) InPktsLate

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

j) InPktsOK
k) InPktsInvalid
l) InPktsNotValid
m) InPktsNotUsingSA
n) InPktsUnusedSA

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

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

10.7.10 Frame validation statistics

Investigation or validation of the performance of the cryptographic functions is supported by maintaining counts of packets (InPktsOverrun, 10.6.3, 10.7.9) that have been discarded due to inability to validate frames at the received rate, and by accumulation of the following counts:

a) InOctetsValidated, the number of octets of User Data recovered from received frames that were integrity protected but not encrypted;
b) InOctetsDecrypted, the number of octets of User Data recovered from received frames that were both integrity protected and encrypted.

These counts are incremented even if the User Data recovered failed the integrity check or could not be recovered. In the latter case an estimate of the number of User Data octets is used, as judged by the load imposed on the validation function.

10.7.11 Receive SC creation

A receive SC, with a given SCI that remains unchanged for the life of the SC, is created following a request from the KaY. Each SC has a unique SCI.

Receive SCs and SAs (10.7.13) may also be created and controlled by management, but a conformant implementation shall provide a mechanism to allow creation and setting of control parameters by network management to be disabled.

10.7.12 Receive SC status

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

a) receiving, True if inUse (10.7.14) is True for any of the SAs for the SC, and False otherwise
b) createdTime, the system time when the SC was created
c) startedTime, the system time when receiving last became True for the SC
d) stoppedTime, the system time when receiving last became False for the SC.

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

The record of the SC should be retained after it is no longer used, subject to the availability of system resources, to provide information about immediate past operation.

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.

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.

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.

10.7.15 Receive SA control

The KaY uses the following parameters to control the use of each receive SA:

a) enableReceive
b) updtNextPN
c) updtLowestPN

When the SA is created, enableReceive and inUse are False, and the SA cannot be used to receive frames. The SA shall be able to receive, and inUse shall be True, when enableReceive is set. The SA shall stop receiving, and inUse shall be False, when enableReceive is reset.

The value of nextPN (or lowestPN as appropriate) shall be set to the greater of its existing value and the supplied of updtNextPn (or updtLowestPN).

10.7.16 Frame generation capabilities

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

a) Maximum number of keys in simultaneous use for transmission

This parameter can be read but not written by management

10.7.17 Frame generation controls

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

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

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

10.7.18 Frame generation statistics

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

a) OutPktsUntagged
b) OutPktsTooLong

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

c) OutPktsProtected
d) OutPktsEncrypted

The counts reported for each SC include those for current and prior SAs, with ANs that have since been reused. This allows useful counts to be maintained on high speed LANs where an SA may be used for little more than 5 minutes, and an AN reused after 20 minutes.The times at which each SC and SA was, or are, in use are recorded (10.7.20, 10.7.22), and assist correlation of the statistics collected with network events.

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

10.7.19 Frame protection statistics

Investigation or validation of the performance of the cryptographic functions is supported by accumulation of the following counts:

a) OutOctetsProtected, the number of octets of User Data in transmitted frames that were integrity protected but not encrypted;
b) OutOctetsEncrypted, the number of octets of User Data in transmitted frames that were both integrity protected and encrypted.

10.7.20 Transmit SC status

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

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

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

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 (, 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.

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.

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.

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

10.7.23 Transmit SA controls

The KaY uses the following parameters to control the use of each receive SA:

a) enableTransmit

When the SA is created, enableTransmit and inUse are False, and the SA is not used to receive frames. The SC parameter encodingSA shall be set to the value of the AN for the SA and inUse set True, when enableTransmit is set. The SA shall stop transmitting, and inUse reset, when enableTransmit is reset.

10.7.24 Implemented Cipher Suites

The following read only management information is provided for each Cipher Suite implemented:

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

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

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

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

NOTE— The offsetConfidentiality capability and the specific offset values chosen are provided to facilitate deployment on IP version 4 and version 6 hosts that perform load balancing across multiple processors in a single system using the initial fields of those protocol stacks, and are not currently capable of terminating the secure association before distributing the load without incurring a significant performance penalty.

10.7.25 Cipher Suite selection

The KaY uses the following parameter to select the Current Cipher Suite:

a) currentCipherSuite, the Cipher Suite Identifier (10.7.24) for the cipher suite.

If offsetConfidentiality (10.7.24) is not false for the Cipher Suite, the following parameter is specified:

b) confidentialityOffset, the number of initial octets of each MSDU without confidentiality protection.

The CurrentCipherSuite is selected by the KaY. The Current Cipher Suite may also be selected and keys created by management, but a conformant implementation shall provide a mechanism to allow such

selection and creation by network management to be disabled. The confidentialityOffset applies to all frames transmitted and received with confidentiality protection. If both confidentialityProtection and offsetConfidentiality are supported, then it takes the values 0, 30, and 50.

If the Current Cipher Suite is changed, all keys created for that Cipher Suite are deleted, and (as a consequence) inUse will become False for all SAs, with the further consequence that MAC_Operational will become False for the Controlled Port.

10.7.26 SAK creation

An 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

10.7.27 SAK status

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

a) transmits, True if the key has been installed for transmission, i.e. can be referenced by a transmit SA
b) receives, True if the key has been installed for reception, i.e. can be 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.

10.8 Addressing

Frames transmitted between end stations using the MAC Service carry the MAC Address of the source and destination peer end stations in the source and destination address fields of the frames, respectively. Communicating peer SecYs can secure communication for all or part of the path used by such frames, and are not directly addressed by the communicating peers, nor are the frames modified to include additional addresses. Each SecY does not have a MAC Address of its own, but is associated with a local entity that forms part of the secure system.

The addressing used by Key Agreement Entities and the means they use to identify SecYs within the same secure system are outside the scope of this specification.

While destination and source MAC addresses are not required to identify SecYs, they are parameters of the MAC Internal Sublayer Service (ISS) used and provided by a SecY, and are covered by the ICV (Integrity Check Value), generated by a Cipher Suite implementation while remaining unencrypted. To facilitate ICV calculation and verification, all frames processed by SecYs use 48-bit MAC addresses.

10.9 Priority

While priority is a parameter of both an ISS M_UNITDATA.request and corresponding M_UNITDATA.indications, end to end communication of the requested priority is not a service attribute (6.1). Protocols supporting the ISS can use the requested priority to perform local actions in the originating station, and do not necessarily attempt to communicate the parameter. Accordingly, the requested and

indicated priorities do not contribute to the ICV, and are not explicitly included in the encoded MSDU by a transmitting SecY.

NOTE—If communication of priority is desired, either guaranteed unchanged or available to a service provider for possible modification to meet the admission control and service characteristics of a particular network, use of the EISS in conjunction with the ISS is indicated. See Clause 7, Principles of Network Operation.

10.10 SecY performance requirements

Table 10-1 places requirements on SecY performance to ensure that MACsec operates correctly.

Table 10-1—SecY performance requirements

Parameter	Permitted values
SecY transmit delay	< Wire transmit time for maximum sized MPDU + (4 times wire transmit time for 64 octet MPDUs)
SecY transmit delay variance	< SecY transmit delay
SecY receive delay	< Wire transmit time for maximum sized MPDU + (4 times wire transmit time for 64 octet MPDUs)
SecY receive delay variance	< SecY receive delay
SC and SA creation and control delay	< 0.1 second
Transmit SAK install delay	<1 second (8.2.2)
Transmit SAK switch delay	< Wire transmit time for 64 octet MPDU (8.2.2)
Receive SAK install delay	<1 second
Receive SAK switch delay	No frame loss

All times are in seconds. —Not applicable, value is fixed.

11. MAC Security in Systems

This clause specifies how MAC Security is incorporated within the architecture of

a) End stations (11.2)
b) MAC Bridges (11.3)
c) VLAN-aware Bridges(11.4)
d) Systems that incorporate Link Aggregation (11.5)
e) Systems that incorporate Link Layer Discovery Protocol (11.6)
f) Provider Bridges and VLAN-aware Bridges attached to Provider Bridged Networks (11.7).
g) LANs that provide independently secured access for multiple end stations (11.8).

The figures in this clause illustrate the relative position of components within the MAC Service interface stacks (11.1) of each of these systems. Both the secure MAC Service provided by the Controlled Port, and the insecure service provided to the Uncontrolled Port are shown. This clause shows MACsec as a whole, including both a SecY and its associated KaY. See Figure 10-2 for their interrelationship.

NOTE—For more information on the Controlled and Uncontrolled Ports and the operation of the SecY, see Clause 10.

11.1 MAC Service interface stacks

Each LAN MAC, e.g. that specified in IEEE Std 802.3, is capable of providing the MAC Service directly to LLC and its clients, as illustrated in Figure 11-1.

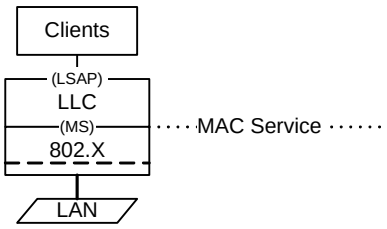


Figure 11-1—Direct support of the MAC Service by a media access method

NOTE—The term 802.X refers to any one of the IEEE 802 LAN media access control method technologies.

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

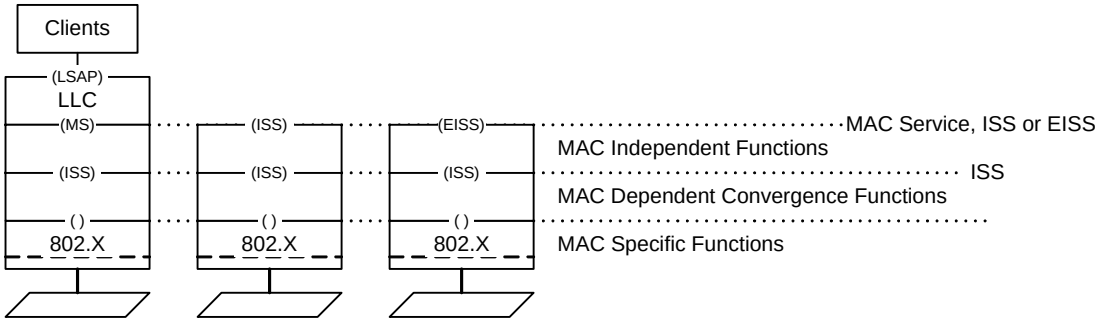


Figure 11-2—Provision of MAC Service with media independent functions

Each SecY uses an ISS access point and provides the ISS at its Controlled and Uncontrolled Ports. This allows use of MAC Security with other media independent functions. However, interoperability between systems using MAC Security requires not only interoperability between SecY implementations and use of the same LAN MAC technology, but also that the same, or compatible, media interface functions are used with the same relative position within the interface stack, as specified in this clause.

NOTE—MAC Bridges and VLAN-aware Bridges provide interoperability between access points for the MAC Service, the ISS, and the EISS, using the following common elements of those service specifications. The MAC Service, the ISS, and the EISS all use the same request and indication primitives. The parameters used by the ISS for each primitive are a superset of those of the MAC Service. An EISS access point effectively provides access to multiple ISS instances.

11.2 MACsec in end stations

The ISS provided by the SecY is trivially mapped to and from the MAC Service provided within an end station. Service indications for unwanted destination MAC addresses are discarded, and the source MAC address of service requests is that of the station. Figure 11-3 shows MAC Security as the sole media independent function within a station.

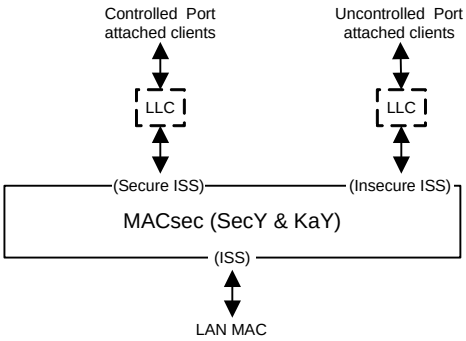


Figure 11-3—MACsec in an end station

11.3 MACsec in MAC Bridges

MAC Bridges are specified in IEEE Std 802.1D. The MAC Relay Entity forwards frames between the ISS access points supported by each of the Bridge Ports. To provide MAC Security for such a system, each of the insecure interfaces presented by a LAN supports MACsec, which in turn supports the functions described in clauses 7.5 and 7.6 of IEEE Std 802.1D. Figure 11-4 shows a bridge with and without MACsec.

NOTE—If the MAC Bridge aggregates multiple LANs to support a single Bridge Port, each individual LAN supports its own SecY, which provides the secure MAC Service to the Link Aggregation sublayer, as specified below (11.5). Each aggregated port then provides secure service to the Bridge Port transmit and receive functions.

Figure 11-5 shows the interface stack for each of the Bridge Ports.

11.4 MACsec in VLAN-aware Bridges

VLAN-aware Bridges are specified in IEEE Std 802.1Q. Figure 11-6 illustrates the addition of MAC Security.

Figure 11-7 shows the interface stack for each of the VLAN-aware Bridge Ports.

Figure 11-8 shows the frame format and placement of the VLAN tag within the frame relative to MACsec. Thus if there is encryption, the VLAN tag is not in the clear.

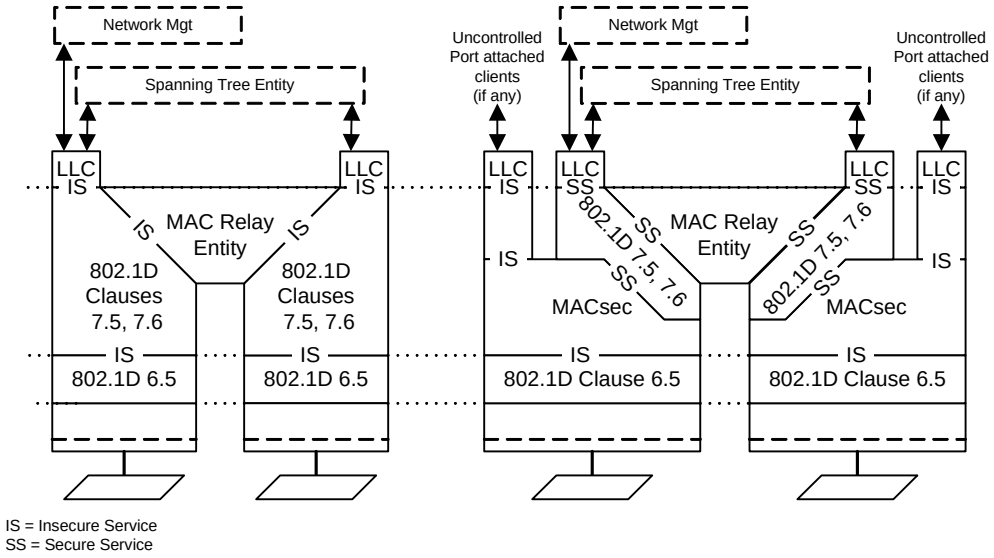


Figure 11-4—MACsec in an 802.1D MAC Bridge

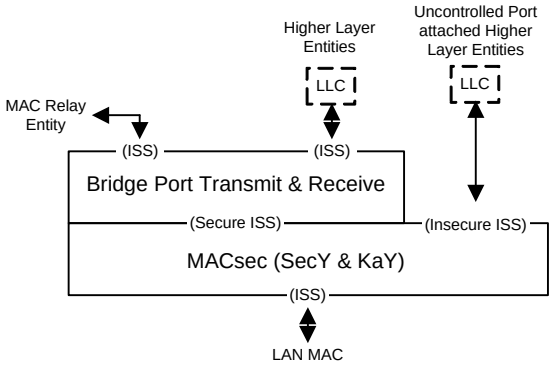


Figure 11-5— 802.1D MAC Bridge Port with MACsec

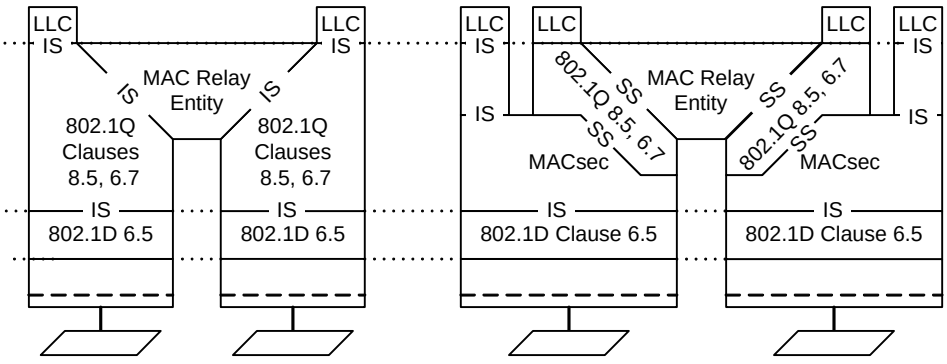


Figure 11-6—Addition of MAC Security to a VLAN-aware MAC Bridge

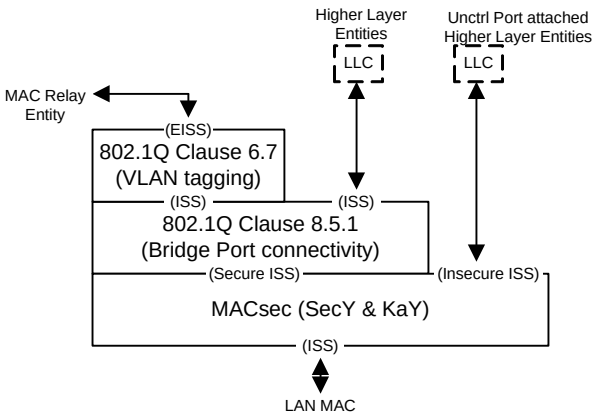


Figure 11-7— 802.1Q VLAN-aware Bridge Port with MACsec

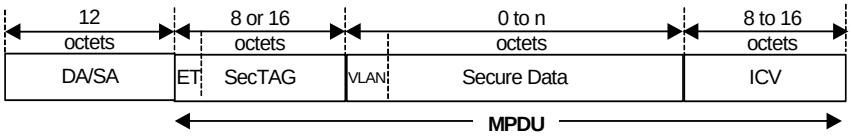


Figure 11-8—MACsec frame format showing VLAN Tag

The position of MACsec, below both the Bridge Port connectivity and VLAN tagging functions, has the following consequences:

a) Each Bridge Port uses a single SecY, with a single transmit SC and a single receive SC for each of the other bridges attached to the LAN, to support all VLANs.
b) Interoperability with MAC Bridges, that are not VLAN-aware, is supported in the same way as VLAN-aware and unaware bridges without MAC Security.
c) Higher layer entities attached to the Bridge Port, such as the Spanning Tree Protocol Entity and protocol stacks for network management, do not need to be supported by separate SecYs. In particular a MACsec protected point-to-point link between two bridges continues to function as a point-to-point link despite the end station functions associated with each Bridge Port.
d) Changes in the operation of MAC Security do not cause differences in the network connectivity used by the MAC Relay Entity and in the network connectivity perceived by the Controlled Port attached higher layer entities that execute control protocols for the relay function.

11.5 MACsec and Link Aggregation

Link Aggregation is specified in IEEE Std 802.3 Clause 43. The service provided by two separate point to point LANs is combined to provide a single service interface. To provide MAC Security for such a system, two independent SecYs operate below the link aggregation sublayer. If the two links are being aggregated dynamically, as provided for by the Link Aggregation Control Protocol (LACP), the operation of LACP will be protected. In addition, if the authentication provided by the KaYs determines that the two links do not connect to the same partner system, local system management can change the aggregation keys. Changes in link aggregation do not cause changes to the MACsec CAs, SCs, SAs, or SAKs.

NOTE 1—LACP aggregation keys have nothing to do with cryptography. See IEEE Std 802.3 Clause 43 for details.

NOTE 2—Although specified in IEEE Std 802.3, Link Aggregation is a media access method independent function.

Figure 11-9 shows part of an interface stack with MAC Security and Link Aggregation. The insecure service access points for each of the SecYs are independently provided to the KaY associated with each SecY, and may or may not be aggregated separately.

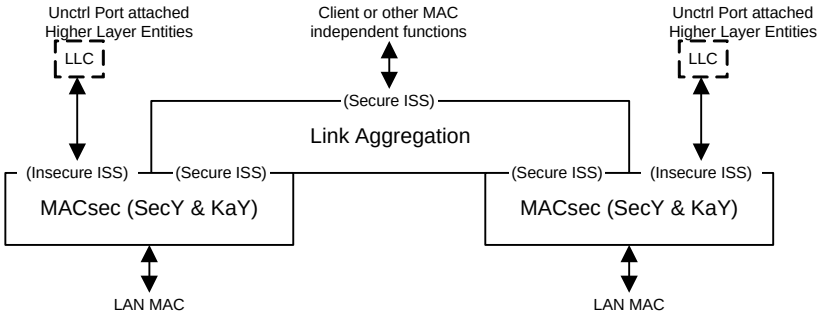


Figure 11-9—MACsec and Link Aggregation in an interface stack

Figure 11-10 shows the addition of link aggregation to the interface stack for a VLAN-aware Bridge Port that also uses MACsec.

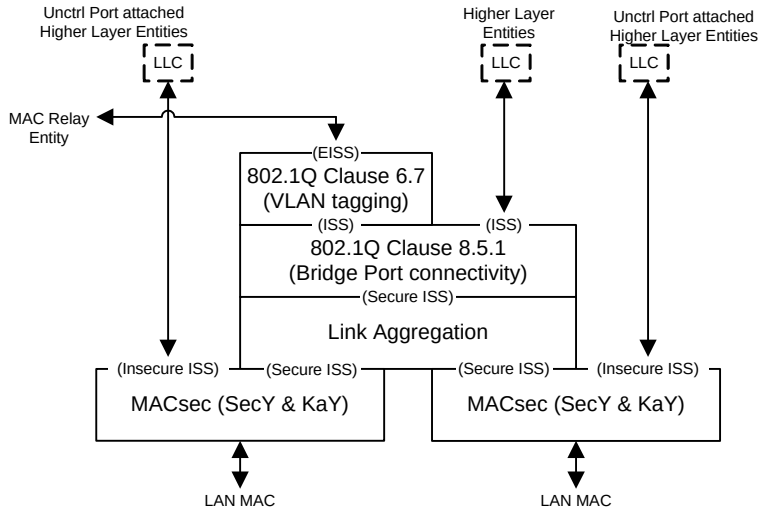


Figure 11-10—802.1Q VLAN-aware Bridge Port with MACsec and Link Aggregation

11.6 Link Layer Discovery Protocol (LLDP)

LLDP is specified in IEEE Std 802.1AB. When used in conjunction with MACsec each LLDP Agent should make use of the Secure ISS provided by MACsec for the attached LAN as shown in Figure 11-11.

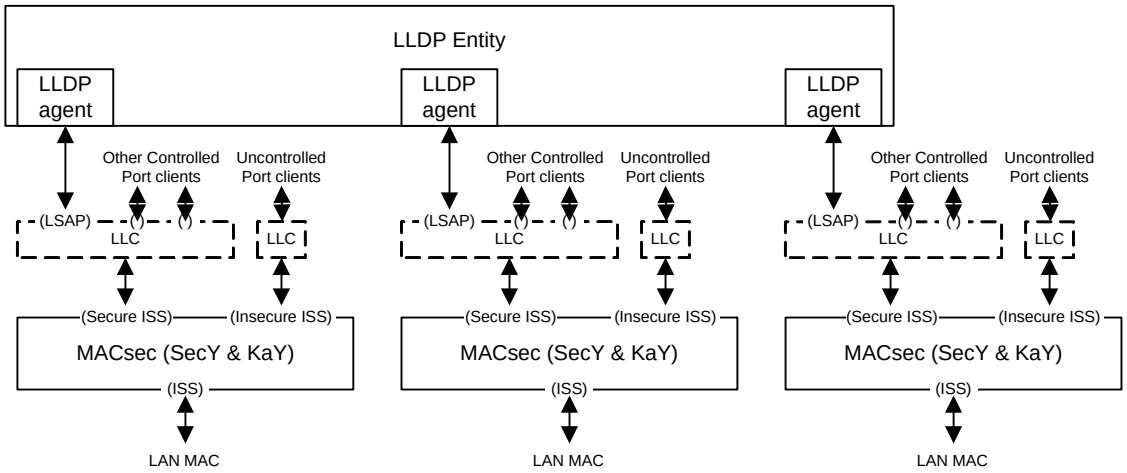


Figure 11-11—MACsec with LLDP

11.7 MACsec in Provider Bridged Networks

Provider Bridges are specified in the IEEE Std 802.1ad amendment to IEEE Std 802.1Q. Provider Bridges enable service providers to use VLANs to offer the equivalent of separate LANs to different users. Data for each of the virtual LANs is segregated within the provider's network by using a Service VLAN TAG (S-TAG) that is distinguished, by EtherType from the Customer VLAN-TAGs (C-TAGs) used within each customer's network. See Figure 11-12.

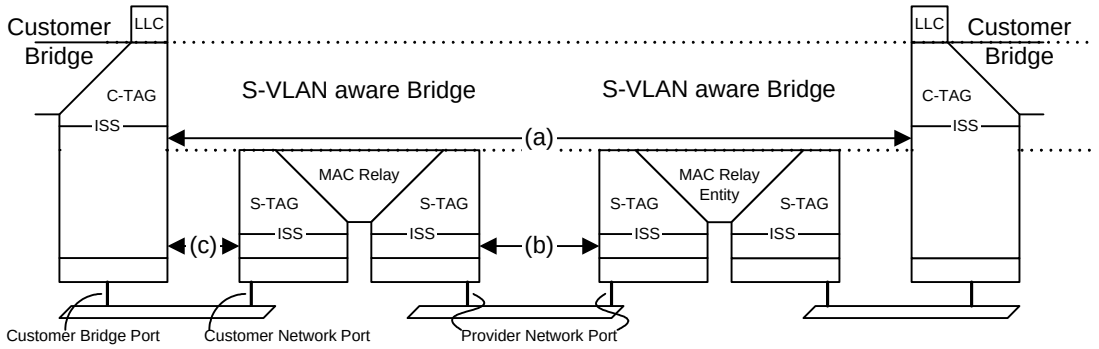


Figure 11-12—Internal organization of the MAC sublayer in a Provider Bridged Network

NOTE—Figure 11-12 is based on Figure 15-1 of IEEE Std 802.1ad-2005.

MACsec can be used to secure communication between

a) A customer's bridges or other equipment, across the provider's network;
b) Adjacent S-VLAN aware Bridges, within the provider's network.
c) A customer's bridge and the provider's network.

If it is the customer's intention to secure only one of (a) or (c), then the use of one of the interface stacks illustrated in Figure 11-3 (for an end station), Figure 11-5 (for a MAC Bridge), or Figure 11-7 (for a VLAN-aware Bridge) within the customer equipment is sufficient.

Use of the interface stack illustrated in Figure 11-7 within the provider's S-VLAN aware Bridge Ports is sufficient to secure either (b) or (c) as required. If (c) is not to be secured, MACsec is either omitted from the interface stack for the Customer Network Port (see Figure 11-12), or the Bridge Port connectivity function (IEEE Std 802.Q Clause 8.5.1) uses the service provided by the Uncontrolled Port.

If it is the intention to secure both (a) and (c) from the Customer Bridge Port, then the use of two independent SecY's within the port's interface stack is required as shown in Figure 11-13.

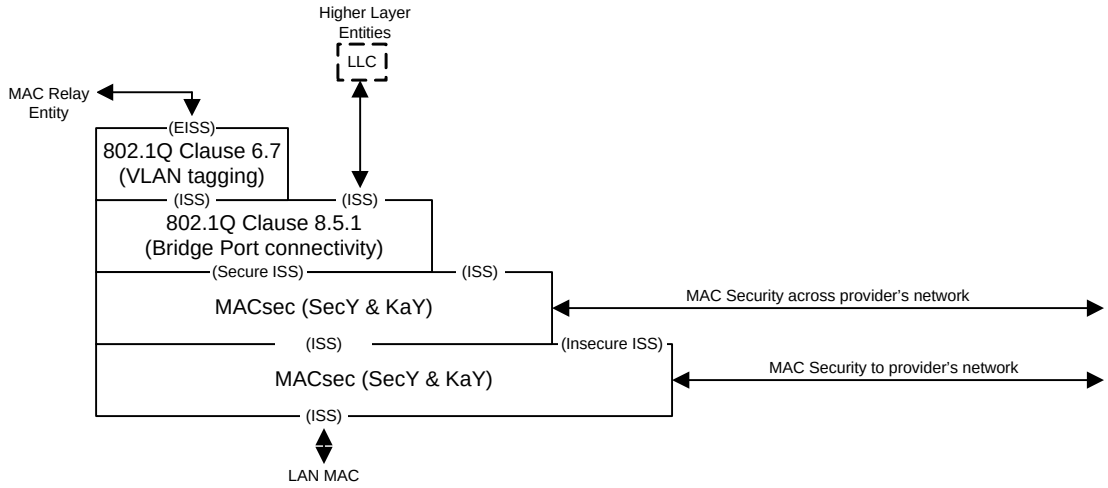


Figure 11-13—Interface stack for MAC Security to and across provider's network

Figure 11-14 shows the addition of the service access priority selection function described in clause 6.9 of IEEE Std 802.1ad to the interface stack of Figure 11-13, together with the use of Link Aggregation to support attachment to the provider's network with two LANs.

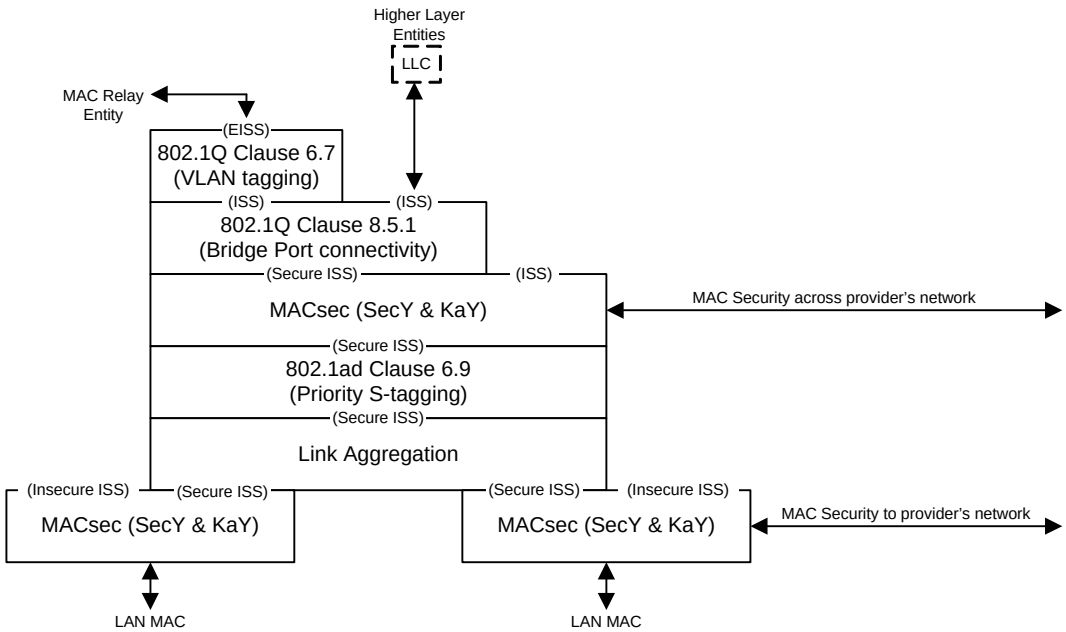


Figure 11-14—Provider network with priority selection and aggregation

11.8 MACsec and multi-access LANs

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

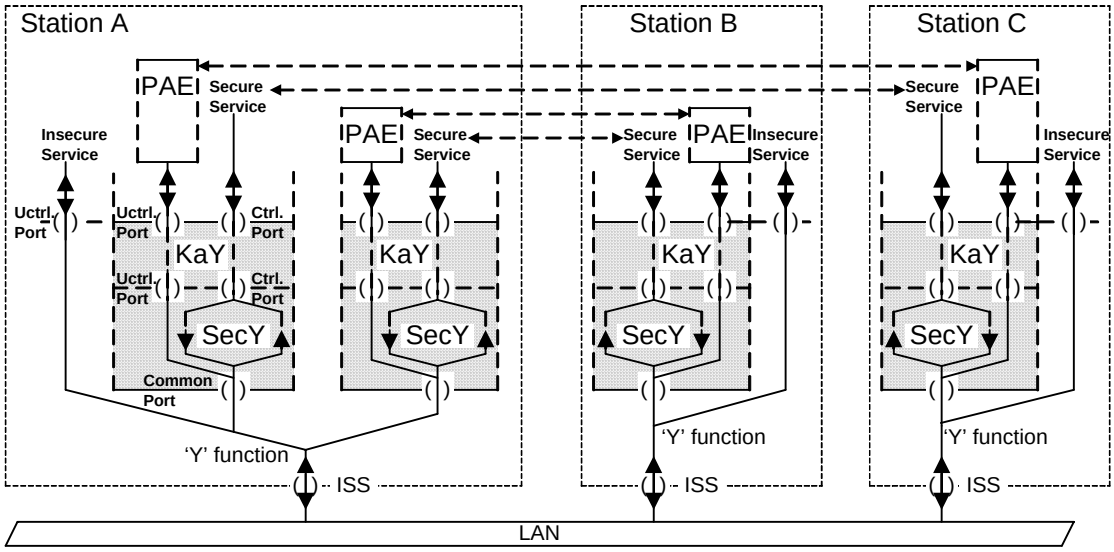


Figure 11-15—An example multi-access LAN

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

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

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

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

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

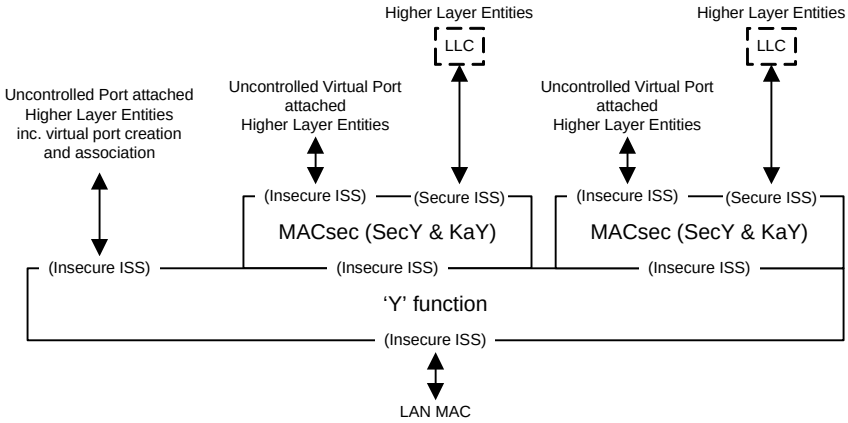


Figure 11-16—Multi-access LAN interface stack

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

12. MACsec and EPON

IEEE Std 802.3 Clauses 64 and 65 specify an Ethernet passive optical network (EPON) that uses a physical fiber tree topology to provide efficient point to multipoint connectivity from a single OLT to one or more ONUs. Clause 64 specifies the instantiation of multiple MAC entities within the OLT, each with an associated service access point that provides point to point connectivity to a specific Optical Network Unit (ONU) separate from the connectivity provided to other ONUs. An additional MAC instance provides a Single Copy Broadcast (SCB) service access point that allows a single copy of a frame to be received by all ONUs.

MACsec provides a separate instance of the secure MAC Service to provide bidirectional connectivity between each ONU and the OLT, as illustrated in Figure 12-17, and thus ensures the confidentiality, integrity, and origin authenticity of each data frame sent and received by the OLT and each ONU. These guarantees are provided irrespective of the ability of an attacker to transmit or receive frames to or from the OLT or any ONU, even if that attacker can exactly mimic the EPON media access method specific behavior of any of the securely communicating participants.

In the OLT, each instance of the secure MAC Service is provided by a distinct SecY that uses the insecure instance of the MAC Service provided by one of the point to point MAC entities in the OLT.

The MAC Service, as specified in ISO/IEC 15802-1, does not provide point to multipoint unidirectional connectivity. However MACsec can support the SCB service access point with a dedicated SC. Appropriate distribution to the ONUs of the encryption and authentication keys for the sequence of SAs that compose the SC ensures the confidentiality, integrity, and origin of each frame sent using the SCB.

NOTE 1—Since the SCB MAC interfaces in the OLT lacks a peer interface in each ONU, the keys for the sequence of SAs that support them are distributed to the Key Agreement Entities of all authorized ONUs using the unsecured bidirectional MAC Service associated with each of the point to point MAC instances.

NOTE 2—An ONU can elect to discard frames from the SCB as these are readily identifiable by the EPON MAC. However if such frames are received, their integrity and origin should be secured, particularly if the system comprising the ONU bridges or routes such frames. Otherwise an attacker could use frames that appear to be sent using the SCB to penetrate the attached network, even if the point to point EPON connectivity has been correctly secured.

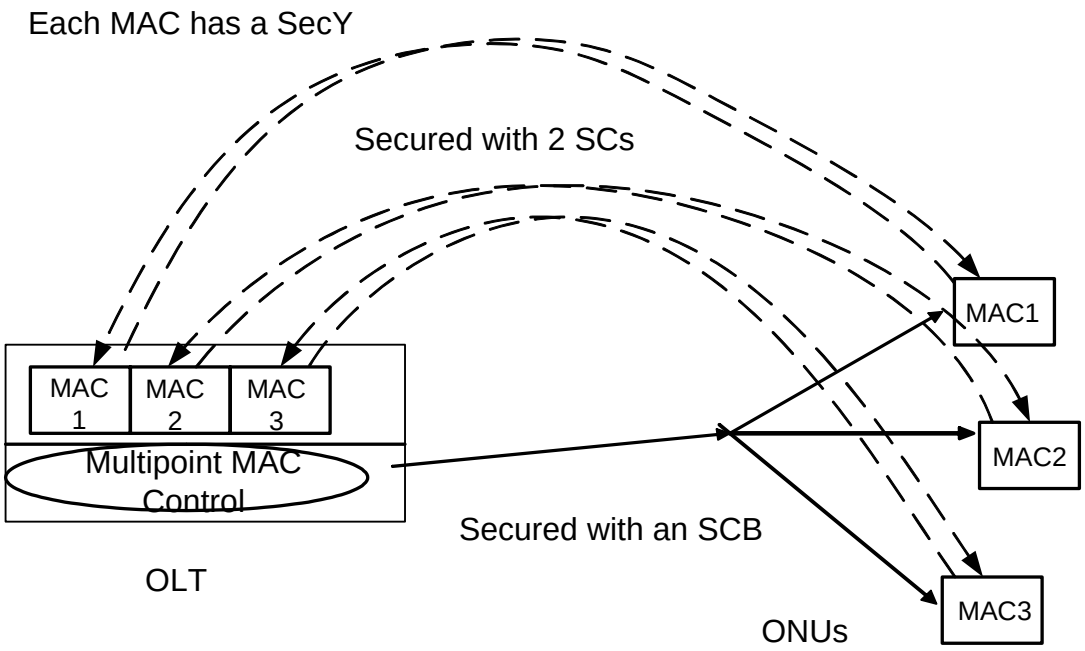


Figure 12-17—MACsec with EPON, showing SCs and SCB

13. Management protocol

13.1 Introduction

This clause defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it describes managed objects for managing the operation of MAC Security, based on the specifications contained in Clause 10 and Clause 1. This clause includes a MIB module that is compliant to SMIv2.

13.2 The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to section 7 of [IETF RFC 3410].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIv2, which is described in [IETF RFC 2578], [IETF RFC 2578],[IETF RFC 2579], [IETF RFC 2579] and [IETF RFC 2580].

13.3 Relationship to other MIBs

13.3.1 System MIB

It is assumed that a system implementing this MIB will also implement the “system” group defined in [IETF RFC 3418] (or at least that subset of the system group defined in[IETF RFC 1213]).

13.3.2 Relationship to the Interfaces MIB

It is assumed that a system implementing this MIB module will implement the “interfaces” group defined in [IETF RFC 2863], the Interfaces Group MIB. This MIB includes the clarifications mandated by [IETF RFC 2863] for any MIB that is medium-specific or an adjunct of the Interfaces Group MIB.

13.4 Security considerations

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

secyIfTable contains system level information for each interface supported by the MAC security entity. SET access to this table by unauthorized persons can disable the MAC security protection functions, block network connectivity, and impact network performance. Examination of this table in comparison with the IF-MIB can identify which ports are not protected by the MAC security entity.

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

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

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

secyTxSATable controls each transmitting SA. secyTxSAConfidentiality exposes whether confidentiality is supported or not for the SA. This information could help an attacker focus their attacks on traffic without confidentiality protection.

secyRxSATable contains information about receiving SAs. secyRxSANextPN is parameters used in replay protection to determine which frames should be discarded. Read access to these related parameters could allow an attacker to know the PN range that an attempted replay must fall within.

secyCipherSuiteTable provides information about the capabilities of the cipher suites supported by the implementation. Access to this information could allow an attacker to focus their attacks on implementations with specific cipher suites and specific weaknesses, e.g. those which lack confidentiality support, or those which only support short integrity check values.

secyRxSAStatsTable and secyRxSCStatsTable contain statistics for each receiving SA and each receiving SC. Read access could allow an attacker to compare these statistics to Figure 10-5 to determine which aspect of their attack failed, and to modify their attack until a different counter is incremented, indicating that they have succeeded in meeting a particular requirement.

secyStatsTable contains statistics about the MAC security entity. This information is SecY interface level statistics information, and also read access to this information can help an attacker determine if a system might be vulnerable.

The global parameters secyMaxPeerSCs and secyMaxKeys might be used by an attacker when attempting to overload the system capabilities to cause a denial of service attack.

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPSec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

Implementers should consider the security features as provided by the SNMPv3 framework (see [IETF RFC 3410], section 8), including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

Further, implementers should not deploy SNMP versions prior to SNMPv3. Instead, implementers should deploy SNMPv3 to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

13.5 Definitions for MAC Security MIB

In the MIB definition below, should any discrepancy between the DESCRIPTION text and the corresponding definition in Clause 10 occur, the definition in Clause 10 shall take precedence.

```
-- ****************************************************************
```

```
-- IEEE8021-SECY-MIB
--
-- Definitions of managed objects supporting IEEE 802.1AE MACsec.
--
-- May 2005
--
-- ****************************************************************

IEEE8021-SECY-MIB DEFINITIONS ::= BEGIN

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

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

ieee8021SecyMIB MODULE-IDENTITY
    LAST-UPDATED   "200505080000Z"
    ORGANIZATION   "IEEE 802.1 Working Group"
    CONTACT-INFO
        "http:/grouper.ieee.org/groups/8021/index.html"
    DESCRIPTION
        "The MAC security entity (SecY) module for managing IEEE
         802.1AE.  An SecY is the entity that operates the MAC Security
         protocol within the system.

         Each SecY transmits frames conveying secure MAC Service
         requests on a single Secure Channel (SC), and receives frames
         conveying secure service indications on separate SCs (one for
         each of the other SecYs participating in the Secure
         Connectivity Association (CA)).  A CA is a security
         relationship, established and maintained by key agreement
         protocols that comprise a fully connected subset of the
         service access points in stations attached to a single MACsec
         supported LAN.  An SC is a security relationship used to
         provide security guarantees for frames transmitted from one
         member of a CA to the others.  It is a unidirectional point to
         multipoint communication, and can be long lived, persisting
         through Secure Association Key (SAK) changes.  Each SC is
         supported by a sequence of Secure Associations (SAs) thus
         allowing the periodic use of fresh keys without terminating
         the relationship.  Each SA is supported by a single secret
```

```
            key, or a set of keys where the cryptographic operations used
            to protect one frame require more than one key."
        REVISION        "200505080000Z"
        DESCRIPTION
            "Initial version of this MIB module.  Published as part of
             IEEE standard 802.1AE"
    -- Editorial note xxx will be replaced by the value allocated for
    -- the ieee8021SecyMIB module sub-tree of the standard publication; and
    -- also, this note will be removed.
        ::= { iso(1) std(0) iso8802(8802) ieee802dot1(1)
              ieee802dot1mibs(1) xxx }

    secyMIBNotifications OBJECT IDENTIFIER ::= { ieee8021SecyMIB 0 }

    secyMIBObjects OBJECT IDENTIFIER ::= { ieee8021SecyMIB 1 }

    secyMIBConformance OBJECT IDENTIFIER ::= { ieee8021SecyMIB 2 }


    --
    -- Textual Convention
    --

    SecySCI ::= TEXTUAL-CONVENTION
        STATUS current
        DESCRIPTION
            "This textual convention indicates a Secure Channel
             Identifier (SCI).

             Each SC is identified by an SCI, comprised of a unique 48-bit
             Universally Administered MAC Address, identifying the system
             to which the transmitting SecY belongs, concatenated with a
             16-bit Port number, identifying the SecY within that system."
        REFERENCE
            "IEEE 802.1AE Clause 7.1.2, 10.7.1 and figure 7.7"
        SYNTAX OCTET STRING (SIZE (8))

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

             Each SC is comprised of a succession of SAs, each with a
             different SAK.  Each SA is identified by the SC identifier
             concatenated with a two-bit AN.  The Secure Association
             Identifier (SAI) thus created allows the receiving SecY to
             identify the SA, and the SAK used to decrypt and authenticate
             the received frame. The AN, and the SAI, is only unique for
             the SAs that can be used or recorded by participating SecYs
             at any instant."
        REFERENCE
             "IEEE 802.1AE Clause 8.1.3 and figure 7.7"
        SYNTAX Unsigned32 (0..3)
```

```
--
-- SecY global objects
--

secyMaxPeerSCs    OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "security connections"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Maximum number of peer SCs per SecY that this system can
         support."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.7"
    ::= { secyMIBObjects 1 }

secyMaxKeys    OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "keys"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Maximum number of keys in simultaneous use that this system
         can support."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.7"
    ::= { secyMIBObjects 2 }

--
-- SecY Management Table
--

secyIfTable    OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyIfEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table of system level information for each interface
        supported by the MAC security entity.  An entry appears in this
        table for each interface with MAC security capability in this
        system.

        For those writable SecY management information, the configured
        value should remain constant at least from one re-initialization
        of the entity's network management system to the next
        re-initialization."
    REFERENCE
        "IEEE 802.1AE Clause 10.7"
    ::= { secyMIBObjects 3 }

secyIfEntry    OBJECT-TYPE
    SYNTAX      SecyIfEntry
    MAX-ACCESS  not-accessible
```

```
        STATUS      current
        DESCRIPTION
             "An entry containing SecY management information applicable to
              a particular interface."
        INDEX   { secyIfInterfaceNumber }
        ::= { secyIfTable 1 }

    SecyIfEntry ::= SEQUENCE {
        secyIfInterfaceNumber              InterfaceIndex,
        secyIfProtectFramesEnable          TruthValue,
        secyIfValidateFrames               INTEGER,
        secyIfReplayProtectEnable          TruthValue,
        secyIfReplayProtectWindow          Unsigned32,
        secyIfCurrentCipherSuite           Unsigned32,
        secyIfAdminPt2PtMAC                INTEGER,
        secyIfOperPt2PtMAC                 TruthValue,
        secyIfIncludeSCIEnable             TruthValue
    }

    secyIfInterfaceNumber    OBJECT-TYPE
        SYNTAX      InterfaceIndex
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "An interface index for a port with SecY management ability.

             This interface index should be aligned with ifIndex in the
             ifTable to point to the same port entity."
        REFERENCE
            "IEEE 802.1AE Clause 10.1"
        ::= { secyIfEntry 1 }

    secyIfProtectFramesEnable    OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "An object to enable or disable the protection function for
             egress frames."
        REFERENCE
            "IEEE 802.1AE Clause 10.5"
        DEFVAL { true }
        ::= { secyIfEntry 2 }

    secyIfValidateFrames    OBJECT-TYPE
        SYNTAX      INTEGER {
                        disabled(1),
                        check(2),
                        strict(3)
                    }
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "An object to control the validation function for ingress
```

```
            frames.

            disabled(1) : means to disable the validation function.

            check(2) : means to enable the validation function but only
                       for checking without filtering out invalid frames.

            strict(3) : means to enable the validation function and also
                        strictly filter out those invalid frames."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.8"
        DEFVAL { strict }
        ::= { secyIfEntry 3 }

    secyIfReplayProtectEnable    OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "An object to enable or disable the replay protection function."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.8, 10.7.17"
        DEFVAL { true }
        ::= { secyIfEntry 4 }

    secyIfReplayProtectWindow    OBJECT-TYPE
        SYNTAX      Unsigned32
        UNITS       "Packets"
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "An object to indicate the replay protection window size.  This
             object only takes effect if the object secyReplayProtectEnable
             is true."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.8"
        DEFVAL { 0 }
        ::= { secyIfEntry 5 }

    secyIfCurrentCipherSuite    OBJECT-TYPE
        SYNTAX      Unsigned32
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "An object that points to an entry of the secyCipherSuiteTable
             to indicate the cipher which this SecY is currently using.  By
             default, this object should point to the default cipher suite
             which system provides."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.25"
        ::= { secyIfEntry 6 }

    secyIfAdminPt2PtMAC    OBJECT-TYPE
        SYNTAX      INTEGER {
```

```
                    forceTrue(1),
                    forceFalse(2),
                    auto(3)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "An object to control the service connectivity to at most one
         other system.  The secyOperPt2PtMAC indicates operational
         status of the service connectivity for this SecY.

         forceTrue(1) : allows only one service connection to the
                        other system.

         forceFalse(2) : no restriction on the number of service
                         connections to the other systems.

         auto(3) : means the service connectivity is determined by the
                   service providing entity."
    REFERENCE
        "IEEE 802.1AE Clause 6.5"
    ::= { secyIfEntry 7 }

secyIfOperPt2PtMAC    OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "An object to reflect the current service connectivity status.

         true(1) : means the service connectivity of this SecY provides
                   at most one other system.

         false(2) : means the service connectivity of this SecY could
                    provide more than one other system."
    REFERENCE
        "IEEE 802.1AE Clause 6.5"
    ::= { secyIfEntry 8 }

secyIfIncludeSCIEnable    OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "An object indicates to include the SCI information in
         security TAG (SecTAG) field while transmitting MACsec
         frames."
    REFERENCE
        "IEEE 802.1AE Clause 9.3, 10.5.3, 10.7.17"
    DEFVAL { false }
    ::= { secyIfEntry 9 }

--
-- Tx SC Management Table
```

```
--

secyTxSCTable    OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyTxSCEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table for providing information about the status of each
         transmitting SC supported by the MAC security entity."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.17, 10.7.20"
    ::= { secyMIBObjects 4 }

secyTxSCEntry    OBJECT-TYPE
    SYNTAX      SecyTxSCEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing transmitting SC management information
         applicable to a particular SecY."
    INDEX   { secyIfInterfaceNumber }
    ::= { secyTxSCTable 1 }

SecyTxSCEntry ::= SEQUENCE {
    secyTxSCI              SecySCI,
    secyTxSCState          INTEGER,
    secyTxSCCurrentSA      RowPointer,
    secyTxSCCreatedTime    TimeStamp,
    secyTxSCStartedTime    TimeStamp,
    secyTxSCStoppedTime    TimeStamp
}

secyTxSCI    OBJECT-TYPE
    SYNTAX      SecySCI
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The SCI information for transmitting MACsec frames of the
         transmitting SC in the SecY."
    REFERENCE
        "IEEE 802.1AE Clause 7.1.2, 8.2.1, 10.7.1"
    ::= { secyTxSCEntry 1 }

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

         inUse(1) : means any of SAs for this SC is in use.
```

```
1
2                notInUse(2) : means no SAs for this SC is in use."
3            REFERENCE
4                "IEEE 802.1AE Clause 10.7.20"
5            ::= { secyTxSCEntry 2 }
6
7        secyTxSCCurrentSA    OBJECT-TYPE
8            SYNTAX      RowPointer
9            MAX-ACCESS  read-only
10           STATUS      current
11           DESCRIPTION
12               "The current transmitting SA in use.  The row pointer will point
13                to an entry in the secyTxSATable.  If no such information is
14                available, the value shall be the OBJECT IDENTIFIER { 0 0 }."
15           REFERENCE
16               "IEEE 802.1AE Clause 10.5.1, 10.7.20"
17           ::= { secyTxSCEntry 3 }
18
19       secyTxSCCreatedTime    OBJECT-TYPE
20           SYNTAX      TimeStamp
21           MAX-ACCESS  read-only
22           STATUS      current
23           DESCRIPTION
24               "The system time when this transmitting SC was created."
25           REFERENCE
26               "IEEE 802.1AE Clause 10.7.20"
27           ::= { secyTxSCEntry 4 }
28
29       secyTxSCStartedTime    OBJECT-TYPE
30           SYNTAX      TimeStamp
31           MAX-ACCESS  read-only
32           STATUS      current
33           DESCRIPTION
34               "The system time when this transmitting SC last started
35                transmitting MACsec frames."
36           REFERENCE
37               "IEEE 802.1AE Clause 10.7.20"
38           ::= { secyTxSCEntry 5 }
39
40       secyTxSCStoppedTime    OBJECT-TYPE
41           SYNTAX      TimeStamp
42           MAX-ACCESS  read-only
43           STATUS      current
44           DESCRIPTION
45               "The system time when this transmitting SC last stopped
46                transmitting MACsec frames."
47           REFERENCE
48               "IEEE 802.1AE Clause 10.7.20"
49           ::= { secyTxSCEntry 6 }
50
51       --
52       -- Tx SA Management Table
53       --
54
```

```
secyTxSATable    OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyTxSAEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table for providing information about the status of each
         transmitting SA supported by the MAC security entity."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.21"
    ::= { secyMIBObjects 5 }

secyTxSAEntry    OBJECT-TYPE
    SYNTAX      SecyTxSAEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing transmitting SA management information
         applicable to a particular SA."
    INDEX   { secyIfInterfaceNumber, secyTxSA }
    ::= { secyTxSATable 1 }

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

secyTxSA    OBJECT-TYPE
    SYNTAX      SecyAN
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The association number (AN) for identifying a transmitting
         SA."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.21"
    ::= { secyTxSAEntry 1 }

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

         inUse(1) : means this SA is in use.
```

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

    secyTxSANextPN    OBJECT-TYPE
        SYNTAX      Unsigned32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The next packet number (PN) that will be used in transmitting
             MACsec frames in the SA."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.21"
        ::= { secyTxSAEntry 3 }

    secyTxSAConfidentiality    OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "Whether this SA supports the confidentiality as well as
             integrity function in transmitting frames."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.21"
        ::= { secyTxSAEntry 4 }

    secyTxSACreatedTime    OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The system time when this transmitting SA was created."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.22"
        ::= { secyTxSAEntry 5 }

    secyTxSAStartedTime    OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The system time when this transmitting SA last started
             transmitting MACsec frames."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.22"
        ::= { secyTxSAEntry 6 }

    secyTxSAStoppedTime    OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The system time when this transmitting SA last stopped
```

```
            transmitting MACsec frames."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.22"
        ::= { secyTxSAEntry 7 }

    --
    -- Rx SC Management Table
    --

    secyRxSCTable    OBJECT-TYPE
        SYNTAX      SEQUENCE OF SecyRxSCEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "A table for providing information about the status of each
             receiving SC supported by the MAC security entity."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.11"
        ::= { secyMIBObjects 6 }

    secyRxSCEntry    OBJECT-TYPE
        SYNTAX      SecyRxSCEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "An entry containing receiving SC management information
             applicable to a particular SC."
        INDEX    { secyIfInterfaceNumber, secyRxSCI }
        ::= { secyRxSCTable 1 }

    SecyRxSCEntry ::= SEQUENCE {
        secyRxSCI              SecySCI,
        secyRxSCState          INTEGER,
        secyRxSCCurrentSA      RowPointer,
        secyRxSCCreatedTime    TimeStamp,
        secyRxSCStartedTime    TimeStamp,
        secyRxSCStoppedTime    TimeStamp
    }

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

    secyRxSCState    OBJECT-TYPE
        SYNTAX      INTEGER {
                        inUse(1),
                        notInUse(2)
                    }
```

```
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The state of the receiving SC in the SecY.

             inUse(1) : means any of SAs for this SC is in use.

             notInUse(2) : means no SAs for this SC is in use."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.12"
        ::= { secyRxSCEntry 2 }

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

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

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

    secyRxSCStoppedTime    OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The system time when this receiving SC last stopped
             receiving MACsec frames."
```

```
        REFERENCE
            "IEEE 802.1AE Clause 10.7.12"
        ::= { secyRxSCEntry 6 }

    --
    -- Rx SA Management Table
    --

    secyRxSATable    OBJECT-TYPE
        SYNTAX      SEQUENCE OF SecyRxSAEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "A table for providing information about the status of each
             receiving SA supported by the MAC security entity."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.13"
        ::= { secyMIBObjects 7 }

    secyRxSAEntry    OBJECT-TYPE
        SYNTAX      SecyRxSAEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "An entry containing receiving SA management information
             applicable to a particular SA."
        INDEX    { secyIfInterfaceNumber, secyRxSCI, secyRxSA }
        ::= { secyRxSATable 1 }

    SecyRxSAEntry ::= SEQUENCE {
        secyRxSA               SecyAN,
        secyRxSAState          INTEGER,
        secyRxSANextPN         Unsigned32,
        secyRxSACreatedTime    TimeStamp,
        secyRxSAStartedTime    TimeStamp,
        secyRxSAStoppedTime    TimeStamp
    }

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

    secyRxSAState    OBJECT-TYPE
        SYNTAX      INTEGER {
                        inUse(1),
                        notInUse(2)
                    }
```

```
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The current state for the receiving SA."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.14"
        ::= { secyRxSAEntry 2 }

    secyRxSANextPN    OBJECT-TYPE
        SYNTAX      Unsigned32
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The stored packet number (PN) for replay protection
             in the SA.  If the PN of any receiving frames is less
             than the value of this object minus the value of
             secyReplayProtectWindow and secyReplayProtectEnable
             is true, the receiving frames should be discarded."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.14"
        ::= { secyRxSAEntry 3 }

    secyRxSACreatedTime    OBJECT-TYPE
        SYNTAX      TimeStamp
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The system time when this receiving SA was created."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.14"
        ::= { secyRxSAEntry 4 }

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

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

```
--
--  SecY Selectable Cipher Suites
--

secyCipherSuiteTable    OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyCipherSuiteEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The table of selectable cipher suites for the MAC security
         entity."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.24"
    ::= { secyMIBObjects 8 }

secyCipherSuiteEntry    OBJECT-TYPE
    SYNTAX      SecyCipherSuiteEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing the management information for a cipher
         suite."
    INDEX { secyCipherSuiteId }
    ::= { secyCipherSuiteTable 1 }

SecyCipherSuiteEntry ::= SEQUENCE {
    secyCipherSuiteId                   Unsigned32,
    secyCipherSuiteName                 SnmpAdminString,
    secyCipherSuiteCapability           BITS,
    secyCipherSuiteProtection           BITS,
    secyCipherSuiteProtectionOffset     INTEGER,
    secyCipherSuiteDataLengthChange     TruthValue,
    secyCipherSuiteICVLength            Unsigned32
}

secyCipherSuiteId    OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The identifier for the cipher suite."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.24"
    ::= { secyCipherSuiteEntry 1 }

secyCipherSuiteName    OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (1..128))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The name of the cipher suite.  If the name is composed of
         multi-byte characters, the total length  must fit within 128
         octets."
    REFERENCE
```

```
            "IEEE 802.1AE Clause 10.7.24"
        ::= { secyCipherSuiteEntry 2 }

    secyCipherSuiteCapability    OBJECT-TYPE
        SYNTAX      BITS {
                        integrity(0),
                        confidentiality(1),
                        offsetConfidentiality(2)
                    }
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The capability of this cipher suite.

             integrity(0) : integrity protection capability for this
                 cipher suite..

             confidentiality(1) : confidentiality protection
                 capability for this cipher suite.

             offsetConfidentiality(2) : offset confidentiality protection
                 capability for this cipher suite."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.24, 10.7.25"
        ::= { secyCipherSuiteEntry 3 }

    secyCipherSuiteProtection    OBJECT-TYPE
        SYNTAX      BITS {
                        integrity(0),
                        confidentiality(1),
                        offsetConfidentiality(2)
                    }
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "The protection options of this cipher suite.  The options
             should depend on the object secyCipherSuiteCapability.

             If the value of secyCipherSuiteCapability is only integerity
             bit on, users can only choose to turn on integrity bit for
             this object.

             If the value of secyCipherSuiteCapability is integrity and
             confidentiality bits on, users can choose to turn on
             integrity or confidentiality bits, but if confidentiality
             bit is on, the integrity bit has to be on.

             If the value of secyCipherSuiteCapability is integrity and
             offsetConfidentiality bits on, users can choose to turn on
             integrity or offsetConfidentiality bits, but if
             offsetConfidentiality bit is on, the integrity bit has to be
             on.

             If the value of secyCipherSuiteCapability is integrity and
```

```
            confidentiality and offsetConfidentiality bits on, users can
            choose to turn on integrity or confidentiality or
            offsetConfidentiality bits, but if confidentiality or
            offsetConfidentiality bits are on, the integrity bit has to
            be on.

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

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

            offsetConfidentiality(2) : on or off the function of
                supporting offset confidentiality for this cipher suite."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.24, 10.7.25"
        ::= { secyCipherSuiteEntry 4 }

    secyCipherSuiteProtectionOffset    OBJECT-TYPE
        SYNTAX      Integer32 (0 | 30 | 50)
        UNITS       "bytes"
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "The confidentiality protection offset options of this
             cipher suite.  The options should depend on the choice of
             secyCipherSuiteProtection.

             If the value of secyCipherSuiteProtection only turns on
             integrity bit, users can only choose 0 byte for this
             object.

             If the value of secyCipherSuiteProtection only turns on
             integrity and confidentiality bits, users can only choose
             0 byte for this object.

             If the value of secyCipherSuiteProtection only turns on
             integrity and offsetConfidentiality bits, users can choose
             30 or 50 bytes for this object.

             If the value of secyCipherSuiteProtection turns on
             integrity and confidentiality and offsetConfidentiality
             bits, users can choose 0 or 30 or 50 bytes for this object."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.24, 10.7.25"
        ::= { secyCipherSuiteEntry 5 }

    secyCipherSuiteDataLengthChange    OBJECT-TYPE
        SYNTAX      TruthValue
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "This indicates whether the data length will be
             changed after encryption by the cipher suite."
```

```
        REFERENCE
            "IEEE 802.1AE Clause 10.7.24"
        ::= { secyCipherSuiteEntry 6 }

    secyCipherSuiteICVLength    OBJECT-TYPE
        SYNTAX      Unsigned32 (8..16)
        UNITS       "octets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The length of integrity check value (ICV) field."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.24"
        ::= { secyCipherSuiteEntry 7 }

    --
    -- Statistics Information
    --


    --
    -- TX SA Statistics Information
    --

    secyTxSAStatsTable    OBJECT-TYPE
        SYNTAX      SEQUENCE OF SecyTxSAStatsEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "A table that contains the statistics objects for each
             transmitting SA in the MAC security entity."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.18, figure 10.4"
        ::= { secyMIBObjects 9 }

    secyTxSAStatsEntry    OBJECT-TYPE
        SYNTAX      SecyTxSAStatsEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "The entry holds the statistics for a transmitting SA.  An SA
             may be reused once a while.

             When starting using the SA, the counters of the SA should
             start at 0.

             When stopping using the SA, the counters will be stopped
             incrementing.

             The timestamps of starting and stopping time are recorded in
             the secyTxSATable."
        INDEX { secyIfInterfaceNumber, secyTxSA }
        ::= { secyTxSAStatsTable 1 }

    SecyTxSAStatsEntry ::= SEQUENCE {
```

```
    secyTxSAStatsProtectedPkts    Counter32,
    secyTxSAStatsEncryptedPkts    Counter32
}

secyTxSAStatsProtectedPkts    OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of integrity protected but not encrypted packets
         for this transmitting SA."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.18, figure 10.4"
    ::= { secyTxSAStatsEntry 1 }

secyTxSAStatsEncryptedPkts    OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of integrity protected and encrypted packets for
         this transmitting SA."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.18, figure 10.4"
    ::= { secyTxSAStatsEntry 2 }

--
-- TX SC Statistics Information
--

secyTxSCStatsTable    OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyTxSCStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table that contains statistics information for each
         transmitting SC in the MAC security entity."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.18, 10.7.19, figure 10.4"
    ::= { secyMIBObjects 10 }

secyTxSCStatsEntry    OBJECT-TYPE
    SYNTAX      SecyTxSCStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The entry contains the transmitting SC's counters.  Since some
         counters in the transmitting SA will be reset while the SA is
         reused, in order to maintain complete statistics information
         for the SC, the counters information on the SAs need to be kept
         in the SC.
```

```
            Those counters that may be reset are :
            secyTxSAStatsProtectedPkts,
            secyTxSAStatsEncryptedPkts

            Each counter for a SC is in the summation of the corresponding
            counter information for all the SAs, current and prior SAs,
            belonging to this SC."
        INDEX { secyIfInterfaceNumber }
        ::= { secyTxSCStatsTable 1 }

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

    secyTxSCStatsProtectedPkts    OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The number of integrity protected but not encrypted packets
             for this transmitting SC."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.18, figure 10.4"
        ::= { secyTxSCStatsEntry 1 }

    secyTxSCStatsEncryptedPkts    OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The number of integrity protected and encrypted packets for
             this transmitting SC."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.18, figure 10.4"
        ::= { secyTxSCStatsEntry 4 }

    secyTxSCStatsOctetsProtected    OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Octets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The number of plain text octets that are integrity protected
             but not encrypted on the transmitting SC."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.19, figure 10.4"
        ::= { secyTxSCStatsEntry 10 }

    secyTxSCStatsOctetsEncrypted    OBJECT-TYPE
```

```
        SYNTAX      Counter64
        UNITS       "Octets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The number of plain text octets that are integrity protected
             and encrypted on the transmitting SC."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.19, figure 10.4"
        ::= { secyTxSCStatsEntry 11 }

    --
    -- RX SA Statistics Information
    --

    secyRxSAStatsTable    OBJECT-TYPE
        SYNTAX      SEQUENCE OF SecyRxSAStatsEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "A table that contains the statistics objects for each
             receiving SA in the MAC security entity."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9, figure 10.5"
        ::= { secyMIBObjects 11 }

    secyRxSAStatsEntry    OBJECT-TYPE
        SYNTAX      SecyRxSAStatsEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "The entry holds the statistics for a receiving SA.  An SA
             may be reused once a while.

             When starting using the SA, the counters of the SA should
             start at 0.

             When stopping using the SA, the counters will be stopped
             incrementing.

             The timestamps of starting and stopping time are recorded in
             the secyRxSATable."
        INDEX { secyIfInterfaceNumber, secyRxSCI, secyRxSA }
        ::= { secyRxSAStatsTable 1 }

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

    secyRxSAStatsUnusedSAPkts    OBJECT-TYPE
```

```
        SYNTAX      Counter32
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "For this SA which is not currently in use, the number of
             received, unencrypted, packets with secyValidateFrames
             not in the strict mode."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9, figure 10.5"
        ::= { secyRxSAStatsEntry 1 }

    secyRxSAStatsNoUsingSAPkts   OBJECT-TYPE
        SYNTAX      Counter32
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "For this SA which is not currently in use, the number of
             received packets that have been discarded, and have
             either the packets encrypted or the secyValidateFrames set to
             strict mode."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9, figure 10.5"
        ::= { secyRxSAStatsEntry 4 }

    secyRxSAStatsNotValidPkts     OBJECT-TYPE
        SYNTAX      Counter32
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "For this SA, the number discarded packets with the
             condition that the packets are not valid and one of the
             following conditions are true: either secyValidateFrames in
             strict mode or the packets encrypted."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9, figure 10.5"
        ::= { secyRxSAStatsEntry 13 }

    secyRxSAStatsInvalidPkts     OBJECT-TYPE
        SYNTAX      Counter32
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "For this SA, the number of packets with the condition
             that the packets are not valid and secyValidateFrames is in
             check mode."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9, figure 10.5"
        ::= { secyRxSAStatsEntry 16 }

    secyRxSAStatsOKPkts          OBJECT-TYPE
```

```
        SYNTAX      Counter32
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "For this SA, the number of validated packets."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9, figure 10.5"
        ::= { secyRxSAStatsEntry 25 }

    --
    -- RX SC Statistics Information
    --

    secyRxSCStatsTable    OBJECT-TYPE
        SYNTAX      SEQUENCE OF SecyRxSCStatsEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "A table for each receiving SC's statistics information
             supported by the MAC security entity."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9, 10.7.10, figure 10.5"
        ::= { secyMIBObjects 12 }

    secyRxSCStatsEntry    OBJECT-TYPE
        SYNTAX      SecyRxSCStatsEntry
        MAX-ACCESS  not-accessible
        STATUS      current
        DESCRIPTION
            "The entry contains the receiving SC's counters.  Since some
             counters in the receiving SA will be reset while the SA is
             reused, in order to maintain complete statistics information
             for the SC, the counters information on the SAs need to be kept
             in the SC.

             Those counters that may be reset are :
             secyRxSAStatsUnusedSAPkts,
             secyRxSAStatsNoUsingSAPkts,
             secyRxSAStatsNotValidPkts,
             secyRxSAStatsInvalidPkts,
             secyRxSAStatsOKPkts

             Each counter for a SC is in the summation of the corresponding
             counter information for all the SAs, current and prior SAs,
             belonging to this SC."
        INDEX { secyIfInterfaceNumber, secyRxSCI }
        ::= { secyRxSCStatsTable 1 }

    SecyRxSCStatsEntry ::= SEQUENCE {
        secyRxSCStatsUnusedSAPkts         Counter64,
        secyRxSCStatsNoUsingSAPkts        Counter64,
        secyRxSCStatsLatePkts             Counter64,
        secyRxSCStatsNotValidPkts         Counter64,
```

```
    secyRxSCStatsInvalidPkts          Counter64,
    secyRxSCStatsDelayedPkts          Counter64,
    secyRxSCStatsUncheckedPkts        Counter64,
    secyRxSCStatsOKPkts               Counter64,
    secyRxSCStatsOctetsValidated      Counter64,
    secyRxSCStatsOctetsDecrypted      Counter64
}

secyRxSCStatsUnusedSAPkts    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The summation of counter secyRxSAStatsUnusedSAPkts
         information for all the SAs which belong to this SC.

         Since the secyRxSAStatsUnusedSAPkts counters in the SAs
         will be reset, in order to maintain complete statistics
         information for the SC, the counter information on the SAs
         need to be kept in the SC."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.9, figure 10.5"
    ::= { secyRxSCStatsEntry 1 }

secyRxSCStatsNoUsingSAPkts    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The summation of counter secyRxSAStatsNoUsingSAPkts
         information for all the SAs which belong to this SC.

         Since the secyRxSAStatsNoUsingSAPkts counters in the SAs
         will be reset, in order to maintain complete statistics
         information for the SC, the counter information on the SAs
         need to be kept in the SC."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.9, figure 10.5"
    ::= { secyRxSCStatsEntry 2 }

secyRxSCStatsLatePkts        OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "For this SC, the number of received packets that have
         been discarded with the condition : secyReplayProtect is equal
         to true and the packet's PN is lower than the lower bound
         replay check PN."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.9, figure 10.5"
```

```
        ::= { secyRxSCStatsEntry 3 }

    secyRxSCStatsNotValidPkts     OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The summation of counter secyRxSAStatsNotValidPkts
             information for all the SAs which belong to this SC.

             Since the secyRxSAStatsNotValidPkts counters in the SAs
             will be reset, in order to maintain complete statistics
             information for the SC, the counter information on the SAs
             need to be kept in the SC."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9, figure 10.5"
        ::= { secyRxSCStatsEntry 4 }

    secyRxSCStatsInvalidPkts     OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The summation of counter secyRxSAStatsInvalidPkts
             information for all the SAs which belong to this SC.

             Since the secyRxSAStatsInvalidPkts counters in the SAs
             will be reset, in order to maintain complete statistics
             information for the SC, the counter information on the SAs
             need to be kept in the SC."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9, figure 10.5"
        ::= { secyRxSCStatsEntry 5 }

    secyRxSCStatsDelayedPkts     OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "For this SC, the number of packets with the condition
             that the PN of the packets is lower than the lower bound
             replay protection PN."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9, figure 10.5"
        ::= { secyRxSCStatsEntry 6 }

    secyRxSCStatsUncheckedPkts   OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
```

```
        DESCRIPTION
            "For this SC, the number of packets with the following
             condition:
             -secyValidateFrames is disabled or
             -secyValidateFrames is not disabled and the packet is not
             encrypted and the integrity check has failed or
             -secyValidateFrames is not disable and the packet is
             encrypted and integrity check has failed."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9, figure 10.5"
        ::= { secyRxSCStatsEntry 7 }

    secyRxSCStatsOKPkts          OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The summation of counter secyRxSAStatsOKPkts
             information for all the SAs which belong to this SC.

             Since the secyRxSAStatsOKPkts counters in the SAs
             will be reset, in order to maintain complete statistics
             information for the SC, the counter information on the SAs
             need to be kept in the SC."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9, figure 10.5"
        ::= { secyRxSCStatsEntry 8 }

    secyRxSCStatsOctetsValidated     OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Octets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The number of octets of plaintext recovered from received
             packets that were integrity protected but not encrypted."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.10, figure 10.5"
        ::= { secyRxSCStatsEntry 9 }

    secyRxSCStatsOctetsDecrypted    OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Octets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The number of octets of plaintext recovered from received
             packets that were integrity protected and encrypted."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.10, figure 10.5"
        ::= { secyRxSCStatsEntry 10 }

    --
```

```
-- SecY statistics table
--

secyStatsTable    OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table for each SecY's statistics information supported by
         the MAC security entity."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.9, 10.7.18, figure 10.4, 10.5"
    ::= { secyMIBObjects 13 }

secyStatsEntry    OBJECT-TYPE
    SYNTAX      SecyStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing counters for statistics or diagnosis for
         a SecY."
    INDEX { secyIfInterfaceNumber }
    ::= { secyStatsTable 1 }

SecyStatsEntry ::= SEQUENCE {
    secyStatsTxUntaggedPkts     Counter64,
    secyStatsTxTooLongPkts      Counter64,
    secyStatsRxUntaggedPkts     Counter64,
    secyStatsRxNoTagPkts        Counter64,
    secyStatsRxBadTagPkts       Counter64,
    secyStatsRxUnknownSCIPkts   Counter64,
    secyStatsRxNoSCIPkts        Counter64,
    secyStatsRxOverrunPkts      Counter64
}

secyStatsTxUntaggedPkts    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of transmitted packets without the MAC
         security tag (SecTAG) because secyProtectFramesEnable is
         configured as false."
    REFERENCE
        "IEEE 802.1AE Clause 10.7.18, figure 10.4"
    ::= { secyStatsEntry 1 }

secyStatsTxTooLongPkts    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
```

```
            "The number of transmitted packets discarded because the packet
             length is greater than that supported by the common port."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.18, figure 10.4"
        ::= { secyStatsEntry 2 }

    secyStatsRxUntaggedPkts    OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The number of received packets without the MAC security tag
             (SecTAG) with secyValidateFrames which is not in the
             strict mode."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9 , figure 10.5"
        ::= { secyStatsEntry 3 }

    secyStatsRxNoTagPkts       OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The number of received packets discarded without the
             MAC security tag (SecTAG) with secyValidateFrames which is
             in the strict mode."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9 , figure 10.5"
        ::= { secyStatsEntry 4 }

    secyStatsRxBadTagPkts      OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The number of received packets discarded with an invalid
             SecTAG or a zero value PN or an invalid ICV."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9 , figure 10.5"
        ::= { secyStatsEntry 5 }

    secyStatsRxUnknownSCIPkts  OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The number of received packets with unknown SCI with the
             condition :
             secyValidateFrames is not in the strict mode and the
             C bit in the SecTAG is not set."
```

```
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9 , figure 10.5"
        ::= { secyStatsEntry 6 }

    secyStatsRxNoSCIPkts       OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The number of received packets discarded with unknown SCI
             information with the condition :
             secyValidateFrames is in the strict mode or the C bit
             in the SecTAG is set."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9 , figure 10.5"
        ::= { secyStatsEntry 7 }

    secyStatsRxOverrunPkts       OBJECT-TYPE
        SYNTAX      Counter64
        UNITS       "Packets"
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
            "The number of packets discarded because the number of
             received packets exceeded the cryptographic performance
             capabilities."
        REFERENCE
            "IEEE 802.1AE Clause 10.7.9 , figure 10.5"
        ::= { secyStatsEntry 8 }

    --
    -- Conformance
    --

    secyMIBCompliances  OBJECT IDENTIFIER ::= { secyMIBConformance 1 }

    secyMIBGroups  OBJECT IDENTIFIER ::= { secyMIBConformance 2 }

    -- Compliance

    secyMIBCompliance MODULE-COMPLIANCE
        STATUS current
        DESCRIPTION
            "The compliance statement for entities which implement
             the IEEE8021-SECY-MIB."
        MODULE  -- this module
            MANDATORY-GROUPS {
                secyGlobalGroup,
                secyIfCtrlGroup,
                secyTxSCGroup,
                secyTxSAGroup,
                secyRxSCGroup,
                secyRxSAGroup,
```

```
                secyCipherSuiteGroup,
                secyTxSAStatsGroup,
                secyTxSCStatsGroup,
                secyRxSAStatsGroup,
                secyRxSCStatsGroup,
                secyStatsGroup
            }
        ::= { secyMIBCompliances 1 }

    -- Units of Conformance

    secyGlobalGroup    OBJECT-GROUP
        OBJECTS {
            secyMaxPeerSCs,
            secyMaxKeys
        }
        STATUS      current
        DESCRIPTION
            "A collection of objects providing a SecY control management
             information."
        ::= { secyMIBGroups 1 }

    secyIfCtrlGroup    OBJECT-GROUP
        OBJECTS {
            secyIfProtectFramesEnable,
            secyIfValidateFrames,
            secyIfReplayProtectEnable,
            secyIfReplayProtectWindow,
            secyIfCurrentCipherSuite,
            secyIfAdminPt2PtMAC,
            secyIfOperPt2PtMAC,
            secyIfIncludeSCIEnable
        }
        STATUS      current
        DESCRIPTION
            "A collection of objects providing a SecY control management
             information."
        ::= { secyMIBGroups 2 }

    secyTxSCGroup    OBJECT-GROUP
        OBJECTS {
            secyTxSCI,
            secyTxSCState,
            secyTxSCCurrentSA,
            secyTxSCCreatedTime,
            secyTxSCStartedTime,
            secyTxSCStoppedTime
        }
        STATUS      current
        DESCRIPTION
            "A collection of objects providing a transmitting SC control
             management information."
        ::= { secyMIBGroups 3 }
```

```
secyTxSAGroup    OBJECT-GROUP
    OBJECTS {
        secyTxSAState,
        secyTxSANextPN,
        secyTxSAConfidentiality,
        secyTxSACreatedTime,
        secyTxSAStartedTime,
        secyTxSAStoppedTime
    }
    STATUS      current
    DESCRIPTION
        "A collection of objects providing a transmitting SA control
         management information."
    ::= { secyMIBGroups 4 }

secyRxSCGroup    OBJECT-GROUP
    OBJECTS {
        secyRxSCState,
        secyRxSCCurrentSA,
        secyRxSCCreatedTime,
        secyRxSCStartedTime,
        secyRxSCStoppedTime
    }
    STATUS      current
    DESCRIPTION
        "A collection of objects providing a receiving SC control
         management information."
    ::= { secyMIBGroups 5 }

secyRxSAGroup    OBJECT-GROUP
    OBJECTS {
        secyRxSAState,
        secyRxSANextPN,
        secyRxSACreatedTime,
        secyRxSAStartedTime,
        secyRxSAStoppedTime
    }
    STATUS      current
    DESCRIPTION
        "A collection of objects providing a receiving SA control
         management information."
    ::= { secyMIBGroups 6 }

secyCipherSuiteGroup    OBJECT-GROUP
    OBJECTS {
        secyCipherSuiteName,
        secyCipherSuiteCapability,
        secyCipherSuiteProtection,
        secyCipherSuiteProtectionOffset,
        secyCipherSuiteDataLengthChange,
        secyCipherSuiteICVLength
    }
    STATUS      current
    DESCRIPTION
```

```
            "A collection of objects providing a cipher suite information."
        ::= { secyMIBGroups 7 }

    secyTxSAStatsGroup    OBJECT-GROUP
        OBJECTS {
            secyTxSAStatsProtectedPkts,
            secyTxSAStatsEncryptedPkts
        }
        STATUS      current
        DESCRIPTION
            "A collection of objects providing a transmitting SA statistics
             information."
        ::= { secyMIBGroups 8 }

    secyRxSAStatsGroup    OBJECT-GROUP
        OBJECTS {
            secyRxSAStatsUnusedSAPkts,
            secyRxSAStatsNoUsingSAPkts,
            secyRxSAStatsNotValidPkts,
            secyRxSAStatsInvalidPkts,
            secyRxSAStatsOKPkts
        }
        STATUS      current
        DESCRIPTION
            "A collection of objects providing a receiving SA statistics
             information."
        ::= { secyMIBGroups 9 }

    secyTxSCStatsGroup    OBJECT-GROUP
        OBJECTS {
            secyTxSCStatsProtectedPkts,
            secyTxSCStatsEncryptedPkts,
            secyTxSCStatsOctetsProtected,
            secyTxSCStatsOctetsEncrypted
        }
        STATUS      current
        DESCRIPTION
            "A collection of objects providing a transmitting SC statistics
             information."
        ::= { secyMIBGroups 10 }

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

```
        STATUS      current
        DESCRIPTION
            "A collection of objects providing a receiving SC statistics
             information."
        ::= { secyMIBGroups 11 }

    secyStatsGroup    OBJECT-GROUP
        OBJECTS {
            secyStatsTxUntaggedPkts,
            secyStatsTxTooLongPkts,
            secyStatsRxUntaggedPkts,
            secyStatsRxNoTagPkts,
            secyStatsRxBadTagPkts,
            secyStatsRxUnknownSCIPkts,
            secyStatsRxNoSCIPkts,
            secyStatsRxOverrunPkts
        }
        STATUS      current
        DESCRIPTION
            "A collection of objects providing a SecY statistics
             information."
        ::= { secyMIBGroups 12 }

    END
```

14. Cipher Suites

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.

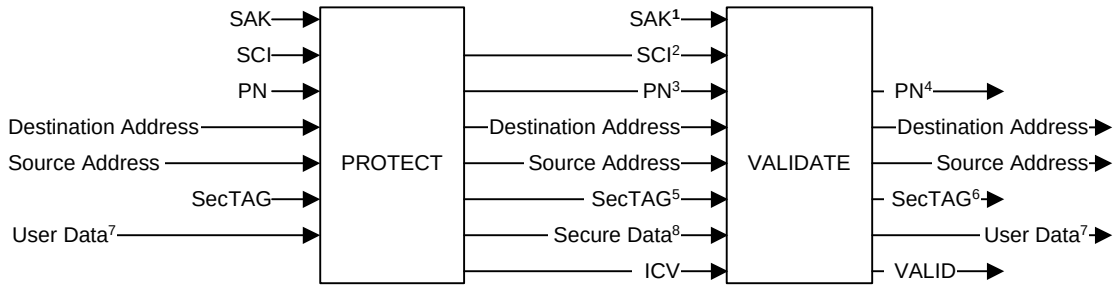
This clause specifies:

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 an algorithm or combination of algorithms whose interactions have been studied by the professional security community.

14.1 Cipher Suite Use

A Cipher Suite is initialized with one or more Cipher Suite dependent keys, and then used to protect protocol parameters. Any implementation of the same Cipher Suite, initialized with the same key values, can be used to validate and recover the protected parameters. The protect and validate operations are illustrated in Figure 14-1, and their inputs and outputs specified below.



[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.
[3] The PN 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

```
Protect ( SAK,                              Validate (  SAK,
          SCI, PN,                                      SCI, PN,
          Destination Address, Source Address,          Destination Address, Source Address,
          SecTAG,                                       SecTAG,
          User Data                                     Secure Data, ICV
        ) Secure Data, ICV                          )   User Data, VALID
```

The SAK (Secure Association Key, 3.36, 7.1) is the value of the Cipher Suite dependent key(s).

The SCI (Secure Channel Identifier, 3.36, 7.1.2) is a 64-bit identifier that is globally unique amongst all correctly configured Cipher Suite implementation instances protecting MACsec protocol parameters.

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 Destination Address and Source Address are the MAC addresses of the frame. MAC Addresses are specified as octet strings, using the canonical format specified in IEEE Std 802.

The SecTAG is as specified in Clause 9.

The ICV (Integrity Check Value, 3.13, 8.3) is a string of octets. VALID is a boolean parameter. If TRUE the validation was successful.

Given the SAK, SCI, PN, Source Address, Destination Address, SecTAG, and the User Data, the Protect operation returns the Secure Data and ICV.

Given the same SAK, SCI, PN, Source Address, Destination Address, and SecTAG, and the Secure Data and ICV, the Verify operation returns the original User Data and VALID. If any of the parameters were modified, VALID is returned False.

14.2 Cipher Suite Capabilities

Any Cipher Suite used with MACsec shall

a) Provide integrity protection for the SCI, PN, Source Address, Destination Address, SecTAG, and from 0 through 2^{16}-1 octets of User Data on each invocation.
b) Provide integrity and confidentiality (if specified) for up to 2^{32}-1 invocations, each with a different PN, without requiring a fresh SAK.
c) Given any specific number of octets of User Data, generate a predictable number of octets of Secure Data and ICV.

and may

d) Provide confidentiality protection for all the octets of the User Data.
e) Provide confidentiality protection for all the octets of the User Data following an initial number of octets, as specified in clause (10.7.24).

and shall not

f) Generate Secure Data that when added to the number of octets in the ICV contains more than 896 octets more than the User Data.

NOTE—A Cipher Suite may introduce additional fields into the Secure Data even if confidentiality is not provided.

g) Modify or constrain the values of the SCI, PN, Source Address, Destination Address, or SecTAG fields, other than as specified in this Clause (14).
h) Require an SAK exceeding 1024 bits long (in total for all keys that compose the SAK).
i) Require different keys for the protect and validate operations.

An implementation of MACsec for which conformance to this Standard is claimed includes at least one Cipher Suite that provides integrity without confidentiality, with the Secure Data the same as the User Data, and the ICV comprising 16 octets. This requirement is met by the mandatory Default Cipher Suite.

14.3 Cipher Suite Specification

Each Cipher Suite specification shall

a) Comprise an interoperable specification of the protection and verification procedures in terms of the parameters specified in 14.1 above.
b) Be publicly available and the subject of a review process under the aegis of an accredited standards committee.

and shall state

c) Whether confidentiality of the User Data is provided
d) The maximum difference in the lengths of the User Data and Secure Data
e) The length of the ICV
f) The length and properties of the keys required, including assumptions of the scope of uniqueness.

NOTE—While this Standard provides definitive specifications of the Cipher Suites that support full conformance, those specifications make the greatest possible use of other public and established standards, and are principally concerned with ensuring unambiguous application of those standards in the context of MAC Security.

14.4 Cipher Suite Conformance

An implementation of MAC Security that claims full conformance to this standard shall implement the Mandatory Cipher Suites in Table 14-1, may implement one or more of the Optional Cipher Suites in the Table, and shall not implement any other Cipher Suite. Every conformant implementation shall include at least one Cipher Suite that does not encrypt User Data.

Table 14-1—MACsec Cipher Suites

Cipher Suite #	Name	Type	Services provided		Mandatory/ Optional	Defining Clause
			Integrity without confidentiality	Integrity and confidentiality		
1	MACsec Default Cipher Suite	GCM–AES–128	Yes	Yes	Mandatory	14.5

NOTE —At this revision of this standard Table 14-1 does not include any Optional Cipher Suites.

Table 14-1 assigns a Cipher Suite reference number for use in protocol identification within a MACsec context, provides a short name for use in this standard, indicates the type of cryptographic algorithm used and the security services provided, specifies whether the Cipher Suite is mandatory or optional for conformance to this standard, and references the clause of this standard that provides the definitive description of the Cipher Suite.

14.4.1 Conformance with Cipher Suite variance

An implementation of MAC Security that claims conformance to this standard with Cipher Suite variance, shall implement the Mandatory Cipher Suites in Table 14-1, may implement one or more of the Optional Cipher Suites in Table 14-1, and may implement alternate Cipher Suites that meet the requirements of Clauses 14.2 and 14.3, and the following guidelines, and shall not implement any other Cipher Suite, or other combination of cryptographic algorithms and parameters.

The use of additional Cipher Suites shall meet the following guidelines:

a) Algorithms chosen have an effective key length of at least 128 bits. In schemes built on block ciphers, the underlying block cipher has a block width of at least 128 bits.
b) The underlying cryptographic cipher is approved either by NIST or the NESSIE standards project.
c) The Cipher Suite provides message authentication using a message authentication algorithm with an academically peer-reviewed proof of security against forgery attacks, even in a model where the attacker has the ability to choose messages for the sender.
d) If confidentiality is provided, the confidentiality mechanism has an academically peer-reviewed proof of security in a model where the attacker has the ability to adaptively choose both plaintext and cipher text.
e) Mechanisms for confidentiality and message authentication are used in a way that is consistent with their proof of security. For example, if using the Cipher Block Chaining (AES-CBC) mode of operation the IV is performed through keystream generation.
f) Mechanisms for confidentiality and message authentication are used in a way that is consistent with their proof of security. For instance, if using the Cipher Block Chaining (AES-CBC) mode of operation, the IV is randomly selected with each message, and not sequentially.
g) If serviced by separate algorithms, the properties of the authentication and confidentiality mechanisms are combinable in accordance with well-established security results. Either the encryption happens before authentication, or the encryption is performed through keystream generation.

14.5 Default Cipher Suite (GCM–AES–128)

The Default Cipher Suite 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 section 2.1 of the GCM specification (GCM) as submitted to NIST.

K is the 128 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 802.3 'wire order' for frame transmission.

When the Default 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 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 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.

Annex A (normative)

PICS Proforma[1]

A.1 Introduction

The supplier of a protocol implementation which is claimed to conform to this standard shall complete the following Protocol Implementation Conformance Statement (PICS) proforma.

A completed PICS proforma is the PICS for the implementation in question. The PICS is a statement of which capabilities and options of the protocol have been implemented. The PICS can have a number of uses, including use

a) By the protocol implementor, as a checklist to reduce the risk of failure to conform to the standard through oversight;

b) By the supplier and acquirer—or potential acquirer—of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the standard PICS proforma;

c) By the user—or potential user—of the implementation, as a basis for initially checking the possibility of interworking with another implementation (note that, while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible PICSs);

d) By a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

A.2 Abbreviations and special symbols

A.2.1 Status symbols

M	mandatory
O	optional
O.n	optional, but support of at least one of the group of options labelled by the same numeral *n* is required
X	prohibited
pred:	conditional-item symbol, including predicate identification: see A.3.4
¬	logical negation, applied to a conditional item's predicate

A.2.2 General abbreviations

N/A	not applicable
PICS	Protocol Implementation Conformance Statement

[1]*Copyright release for PICS proformas:* Users of this standard may freely reproduce the PICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed PICS.

A.3 Instructions for completing the PICS proforma

A.3.1 General structure of the PICS proforma

The first part of the PICS proforma, implementation identification and protocol summary, is to be completed as indicated with the information necessary to identify fully both the supplier and the implementation.

The main part of the PICS proforma is a fixed-format questionnaire, divided into several subclauses, each containing a number of individual items. Answers to the questionnaire items are to be provided in the rightmost column, either by simply marking an answer to indicate a restricted choice (usually Yes or No), or by entering a value or a set or range of values. (Note that there are some items where two or more choices from a set of possible answers can apply; all relevant choices are to be marked.)

Each item is identified by an item reference in the first column. The second column contains the question to be answered; the third column records the status of the item—whether support is mandatory, optional, or conditional; see also A.3.4 below. The fourth column contains the reference or references to the material that specifies the item in the main body of this standard, and the fifth column provides the space for the answers.

A supplier may also provide (or be required to provide) further information, categorized as either Additional Information or Exception Information. When present, each kind of further information is to be provided in a further subclause of items labelled *Ai* or *Xi,* respectively, for cross-referencing purposes, where *i* is any unambiguous identification for the item (e.g., simply a numeral). There are no other restrictions on its format and presentation.

A completed PICS proforma, including any Additional Information and Exception Information, is the Protocol Implementation Conformation Statement for the implementation in question.

NOTE—Where an implementation is capable of being configured in more than one way, a single PICS may be able to describe all such configurations. However, the supplier has the choice of providing more than one PICS, each covering some subset of the implementation's configuration capabilities, in case that makes for easier and clearer presentation of the information.

A.3.2 Additional information

Items of Additional Information allow a supplier to provide further information intended to assist the interpretation of the PICS. It is not intended or expected that a large quantity will be supplied, and a PICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations, or information about aspects of the implementation that are outside the scope of this standard but that have a bearing upon the answers to some items.

References to items of Additional Information may be entered next to any answer in the questionnaire, and may be included in items of Exception Information.

A.3.3 Exception information

It may occasionally happen that a supplier will wish to answer an item with mandatory status (after any conditions have been applied) in a way that conflicts with the indicated requirement. No pre-printed answer will be found in the Support column for this: instead, the supplier shall write the missing answer into the Support column, together with an *Xi* reference to an item of Exception Information, and shall provide the appropriate rationale in the Exception item itself.

An implementation for which an Exception item is required in this way does not conform to this standard.

NOTE—A possible reason for the situation described above is that a defect in this standard has been reported, a correction for which is expected to change the requirement not met by the implementation.

A.3.4 Conditional status

A.3.4.1 Conditional items

The PICS proforma contains a number of conditional items. These are items for which both the applicability of the item itself, and its status if it does apply—mandatory or optional—are dependent upon whether or not certain other items are supported.

Where a group of items is subject to the same condition for applicability, a separate preliminary question about the condition appears at the head of the group, with an instruction to skip to a later point in the questionnaire if the "Not Applicable" answer is selected. Otherwise, individual conditional items are indicated by a conditional symbol in the Status column.

A conditional symbol is of the form "**pred:** S" where **pred** is a predicate as described in A.3.4.2 below, and S is a status symbol, M or 0.

If the value of the predicate is true (see A.3.4.2), the conditional item is applicable, and its status is indicated by the status symbol following the predicate: the answer column is to be marked in the usual way. If the value of the predicate is false, the "Not Applicable" (N/A) answer is to be marked.

A.3.4.2 Predicates

A predicate is one of the following:

a) An item-reference for an item in the PICS proforma: the value of the predicate is true if the item is marked as supported, and is false otherwise;
b) A predicate-name, for a predicate defined as a boolean expression constructed by combining item-references using the boolean operator OR: the value of the predicate is true if one or more of the items is marked as supported;
c) A predicate-name, for a predicate defined as a boolean expression constructed by combining item-references using the boolean operator AND: the value of the predicate is true if all of the items are marked as supported;
d) The logical negation symbol "¬" prefixed to an item-reference or predicate-name: the value of the predicate is true if the value of the predicate formed by omitting the "¬" symbol is false, and vice versa.

Each item whose reference is used in a predicate or predicate definition, or in a preliminary question for grouped conditional items, is indicated by an asterisk in the Item column.

A.4 PICS proforma for IEEE Std 802.1AE

A.4.1 Implementation identification

Supplier	
Contact point for queries about the PICS	
Implementation Name(s) and Version(s)	
Other information necessary for full identification—e.g., name(s) and version(s) of machines and/or operating system names	
NOTE 1—Only the first three items are required for all implementations; other information may be completed as appropriate in meeting the requirement for full identification. NOTE 2—The terms Name and Version should be interpreted appropriately to correspond with a supplier's terminology (e.g., Type, Series, Model).	

A.4.2 Protocol summary, IEEE Std 802.1AE

Identification of protocol specification	IEEE Std 802.1AE, Standards for Local and Metropolitan Area Networks: Media Access Control (MAC) Security
Identification of amendments and corrigenda to the PICS proforma which have been completed as part of the PICS	Amd. : Corr. : Amd. : Corr. :
Have any Exception items been required? (See A.3.3: the answer Yes means that the implementation does not conform to IEEE Std 802.1AE.)	No [ ] Yes [ ]

Date of Statement	

A.5 Major capabilities

Item	Feature	Status	References	Support
SAP	Does the implementation of each MAC Security Entity support the Controlled and Uncontrolled Ports, and use a Common Port as specified in Clause 10?	M	5.3(a), 10, A.6	Yes [ ]
STAT	Does the implementation support the MAC status and point-to-point parameters for the Controlled and Uncontrolled Ports as specified in clauses 6.4, 6.5, and 10.7?	M	5.3(b), 6.4, 6.5, 10.7, A.7	Yes [ ]
GEN	Does the implementation process transmit requests from the Controlled Port as required by the specification of Secure Frame Generation (10.5)?	M	5.3(c), 10.5, A.8	Yes [ ]
VER	Does the implementation process receive indications from the Common Port as required by the specification of Secure Frame Verification (10.6), prior to causing receive indications at the Controlled Port?	M	5.3(d), 10.6, A.9	Yes[ ]
FMT	Does the implementation encode and decode MACsec PDUs as specified in in Clause 9?	M	5.3(e), 9, A.10	Yes [ ]
SCI	Does the implementation use a globally unique 48-bit MAC Address and a 16-bit Port Identifier unique within the scope of that address assignment to identify the transmit SCI, as specified in clause 8.2.1?	M	5.3(f), 8.2.1	Yes [ ]
PERF	Does the implementation satisfy the performance requirements specified in Table 10-1 and clause 8.2.2?	M	5.3(g), 10.1, Table 10-1, 8.2.2	Yes [ ]
FCS	Does the implementation introduce an undetected frame error rate greater than that achievable by preserving the original FCS, as required by clause 10.4?	X	5.3(n), 10.4, 6.10	No []
KAY	Does the implementation support the LMI operations required by the Key Agreement Entity as specified in Clause 10?	M	5.3(h), 10, A.11	Yes [ ]
MGT	Does the implementation provide the management functionality specified in Clause 10.7?	M	5.3(i), 10.7, A.12.1	Yes [ ]
MIB	Does the implementation support network management using the MIB specified in Clause 13?	O	5.4(a), 13	Yes [ ] No[ ]
SNMP	Does the implementation support access to the MIB specified in Clause 13 using SNMP v3 or higher?	O	5.4(b), 13	Yes [ ] No[ ]
SNMX	Does the implementation support access to MACsec parameters using any version of SNMP prior to v3?	X	5.3(p)	No[ ]
MSC	Does the implementation support more than one receive SC?	O	5.4(c)	Yes [ ] No[ ]
MSAK	Does the implementation support more than two receive SAKs?	O	5.4(d)	Yes [ ] No[ ]

A.5 Major capabilities *(continued)*

Item	Feature	Status	References	Support
CS	Does the implementation protect and validate MACsec PDUs by using implemented Cipher Suites as specified in clause 14.1?	M	5.3(j), 14.1	Yes [ ]
CSI	Does the implementation support Integrity Protection using the Default Cipher Suite specified in Clause 14?	M	5.3(k), 14, 14.5,	Yes [ ]
CSC	Does the implementation support Confidentiality Protection using the Default Cipher Suite without a Confidentiality Offset as specified in Clause 14?	¬CSO:O CSO:M	5.4(e), 14, 14.5,	Yes [ ]
CSO	Does the implementation support Confidentiality Protection using the Default Cipher Suite with a Confidentiality Offset as specified in Clause 14?	O	5.4(f), 14, 14.5,	Yes [ ]
CSA	Does the implementation include Cipher Suites that are specified in Clause 14 in addition to the Default Cipher Suite? (This PICS requires the completion of a copy of Table A.13 for each such Cipher Suite implemented.)	O	5.4(g), A.13	Yes [ ] No[ ]
CSX	Does the implementation include any Cipher Suite that is additional to those specified in Clause 14 and does not meet all the criteria specified in 14.2, 14.3, 14.4.1?	X	5.3(o), 14.2, 14.3, 14.4.1	No[ ]
CSV	Does the implementation include Cipher Suites other than those specified in Clause 14, but meeting the criteria specified in 14.2, 14.3, 14.4.1? (This PICS requires the completion of a copy of Table A.14 for each such Cipher Suite implemented.)	O	5.4(h), A.14	Yes [ ] No[ ]
CSR	Does the implementation support a minimum of one receive SC and two receive SAKs, and one of the two receive SAKs at a time for transmission as specified in 5.3(l), for each Cipher Suite implemented?	M	5.3(l), 14	Yes [ ]
CSS	Does this completed PICS specify the maximum number of receive SCs and SAKs for each Cipher Suite implemented?	M	5.3(m), A.13, A.14	Yes [ ]
CSRC	What is the maximum number of receive SCs supported by the Default Cipher Suite implementation? _ _ _ _ _		5.3(i)	
CSRK	What is the maximum number of receive SAKs supported by the Default Cipher Suite implementation? _ _ _ _ _		5.3(i)	
FULL	Is a claim for full conformance being made for the implementation?	**CSV**:X ¬**CSV**:O	5.3	Yes [ ] No[ ]
VAR	Is a claim for conformance with cipher suite variance being made for the implementation?		5.3	Yes [ ] No[ ]

A.6 Support and use of Service Access Points

Item	Feature	Status	References	Support
SAP-1	Does each transmit request from the Uncontrolled Port result in a single request to the Common Port with the same parameters?	M	10.4	Yes []
SAP-2	Does each receive indication from the Common Port result in a single indication to the Uncontrolled Port with the same parameters if any of the users of the Common Port wishes to receive the indication?	M	10.4	Yes []
SAP-3	Does each transmit request from the Controlled Port result in at most one request to the Common Port?	M	10.4	Yes []
SAP-4	Does each receive indication from the Common Port result in at most one indication to the Controlled Port?	M	10.4	Yes []
SAP-5	Are any transmit requests made to the Common Port that do not correspond to requests made at the Uncontrolled or Controlled Port?	X	10.4	No []
SAP-6	Are any receive indications caused at the Uncontrolled or Controlled Port that do not correspond to indications from the Common Port?	X	10.4	No []
SAP-7	Is the order of requests made at the Common Port unchanged from the order of corresponding requests from the Uncontrolled Port?	M	10.4	Yes []
SAP-8	Is the order of requests made at the Common Port unchanged from the order of corresponding requests from the Controlled Port?	M	10.4	Yes []
SAP-9	Is the order of receive indications caused at the Uncontrolled Port the same as the order of reception from the Common Port?	M	10.4	Yes []
SAP-10	Is each transmit request from the Controlled Port processed in accordance with the specification of the Secure Frame Generation process, prior to discarding the request or making a corresponding request to the Common Port?	M	10.4, 10.5	Yes []
SAP-11	Is each receive indication from the Common Port processed in accordance with the specification of the Secure Frame Verification process prior to causing a possible corresponding indication at the Controlled Port?	M	10.4, 10.6	Yes []

A.7 MAC status and point to point parameters

Item	Feature	Status	References	Support
STAT-1	Are the values for MAC_Operational and operPointToPointMAC for the Uncontrolled Port identical to those for the Common Port?	M	6.4, 10.7.2	Yes [ ]
STAT-2	Is MAC_Operational false for the Controlled Port, and frames neither accepted or delivered on the port, if the SA identified by the encodingSA is not available for use and protectFrames is set?	M	6.4, 10.5.1, 7.1	Yes [ ]
STAT-3	Is MAC_Operational false for the Controlled Port and frames neither accepted nor delivered, if the nextPN for the encodingSA is zero or 2^{32}?	M	6.4, 10.5.2	Yes [ ]
STAT-4	Is MAC_Operational true only if MAC_Enabled is true and MAC_Operational for the Common Port is true?	M	6.4, 10.7.4	Yes [ ]
STAT-5	Is the value of operPointToPointMAC for the Controlled Port always as specified in 10.7.4.	M	6.5, 10.7.4	Yes [ ]

A.8 Secure Frame Generation

Item	Feature	Status	References	Support
GEN-1	Does each transmit request from the Controlled Port result in an identical transmit request at the Common Port if the management control protectFrames is false?	M	10.5	Yes []
GEN-2	Does each transmit request at the Common Port resulting from a request at the Common Port convey request parameters, i.e. a frame, protected in accordance with Clause 10.5 if the management control protectFrames is true?	M	10.5	Yes[ ]
GEN-3	Is each protected frame assigned to the SA with AN corresponding to the current value of encodingSA as specified by the KaY?	M	10.5.1	Yes[ ]
GEN-4	Are frames to be protected discarded if the assigned SA cannot be used?	M	10.5.1	Yes[ ]
GEN-5	Is the PN value of zero used?	X	10.5.2	No []
GEN-6	Following assignment of a PN to a protected frame, is the next frame to be protected for the same SA assigned the next higher value of PN?	M	10.5.2	Yes[ ]
GEN-7	Is the SecTAG encoded as specified in Clause 9?	M	10.5.3, 9	
GEN-8	Is the ES bit set or clear as required by the management controls useES and alwaysIncludeSCI?	M	10.5.3	
GEN-9	Is the SC bit set or clear and the SCI explicitly encoded or not as required by the management controls useES, use SCB, alwaysIncludeSCI, and by the number of receive SCs?	M	10.5.3	
GEN-10	Is the SCB bit set or clear as required by the management controls useSCB and alwaysIncludeSCI?	M	10.5.3	
GEN-11	Is the E bit set if the frame is confidentiality protected, and clear otherwise?	M	9.5	
GEN-12	Is the C bit set if the octets of the Secure Data differ from those of the User Data or the ICV is not 16 octets, and clear otherwise?	M	9.5	
GEN-13	Is each frame transmitted from the Controlled Port protected using a Cipher Suite as specified in Clause 14 if protectFrames is set?	M	10.5	
GEN-14	Is OutOctetsEncrypted incremented by the number of octets in the User Data if confidentiality protections is provided, and OutOctetsProtected incremented otherwise?	M	10.5.4	
GEN-15	Is the protected frame transmitted if the MACsec PDU (SecTAG, Secure Data, and ICV) does not exceed the maximum data unit size supported by the Common Port and discarded otherwise?	M	10.5.5	

A.9 Secure Frame Verification

Item	Feature	Status	References	Support
VER-1	For each receive indication, does the Secure Frame Verification process examine the user data for a SecTAG and validate frames with a SecTAG as specified in 9.12, extracting and decoding the SecTAG as specified in Clauses 9.3 through 9.9, and extracting the User Data and ICV as specified in clauses 9.10 and 9.11?	M	10.6, 9.3 through 9.9, 9.10, 9.11	Yes[ ]
VER-2	Is a received frame without a SecTAG delivered to the Controlled Port if validateFrames is not Strict, and discarded otherwise?	M	10.6	Yes[ ]
VER-3	Is a received frame with the SecTAG E bit set and C bit clear discarded and not delivered to the Controlled Port?	M	10.6	Yes[ ]
VER-4	Is the received frame discarded if the SC is unknown and validateFrames is Strict or the C bit is set, and delivered to the Controlled Port otherwise?	M	10.6.1	Yes[ ]
VER-5	Is the received frame discarded if the SA is unused and validateFrames is Strict or the C bit is set, and delivered to the Controlled Port otherwise?	M	10.6.1	Yes[ ]
VER-6	Is the received frame discarded if the PN is less than the lowest acceptable packet number for the SA and replayProtect is enabled?	M	10.6.2, 10.6.4	Yes[ ]
VER-7	Is the InPktsOverrun counter incremented if a received frame is discarded for reasons not attributed to the data conveyed?	M	10.6.3	Yes[ ]
VER-8	If validateFrames is Disabled, is Cipher Suite validation omitted and a received frame delivered to the Controlled Port if the C bit is not set?	M	10.6.3, 10.6.5	Yes[ ]
VER-9	If validateFrames is not Disabled is the Cipher Suite used to validated the received frame?	M	10.6.3	Yes[ ]
VER-10	Are frames that are not successfully validated discarded if validateFrames is Strict or the C bit is set?	M	10.6.5	Yes[ ]
VER-11	Are the values for the next expected and lowest acceptable PN updated as specified in 10.6.5 following receipt of a MACsec PDU successfully validate by the Cipher Suite, and not modified by received frames otherwise?	M	10.6.5	Yes[ ]
VER-12	Are received frames not discarded by Secure Frame Verification delivered to the Controlled Port after removal of a SecTAG and ICV?	M	10.6	Yes[ ]

A.10 MACsec PDU encoding and decoding

Item	Feature	Status	References	Support
FMT-1	Does each MACsec PDU transmitted contain an integral number of octets?	M	9.1	Yes[ ]
FMT-2	Does each MACsec PDU transmitted comprise a SecTAG, formatted as specified in Clause 9, one or more octets of Secure Data, and an ICV of the length specified by the Cipher Suite in use?	M	9.1, 9.2, 9.3, Figure 9-1, 10.5.3	Yes[ ]
FMT-3	Is the EtherType encoded in the SecTAG the value specified in Table 9-1?	M	9.3, 9.4	Yes[ ]
FMT-4	Is the version number in the SecTAG encoded as zero?	M	9.5	Yes[ ]
FMT-5	Is the SC bit clear and the SCI not explicitly encoded if the ES bit is set?	M	9.5	Yes[ ]
FMT-6	Is the SC bit set if an SCI is explicitly encoded and clear otherwise?	M	9.5	Yes[ ]
FMT-7	Is the SC bit clear if the SCB bit is set?	M	9.5	Yes[ ]
FMT-8	Are bits 7 and 8 of octet 4 of the SecTAG zero?	M	9.7	Yes[ ]
FMT-9	Is each received MACsec PDU validated as specified in clause 9.12.	M	9.5	Yes[ ]

A.11 Key Agreement Entity LMI

Item	Feature	Status	References	Support
KAY-1	Does the implementation allow the KaY to read the values of the MAC_Enabled, MAC_Operational, and operPointToPointMAC parameters?	M	10.7.2	Yes[ ]
KAY-2	Does the implementation allow the KaY to set and clear the ControlledPortEnabled parameter, acting on the parameter as specified?	M	10.7.5, 10.7.4	Yes[ ]
KAY-3	Does the implementation allow the KaY to discover which Cipher Suites are implemented and how many receive SCs each can support?	M	10.2, 10.7.24, 10.7.7, 10.7.16	Yes[ ]
KAY-4	Does the implementation allow the KaY to create a receive SC?	M	10.7.11, 10.6.1	Yes[ ]
KAY-5	Does the implementation allow the KaY to create receive SAs as specified in 10.7.13?	M	10.7.13	Yes[ ]
KAY-6	Does the implementation allow the KaY to control the use of each receive SA and to update the values of the next expected PN and lowest acceptable PN as specified in 10.7.15?	M	10.7.15	Yes[ ]
KAY-7	Does the implementation allow the KaY to create transmit SAs as specified in 10.7.21?	M	10.7.21, 10.5.2	Yes[ ]
KAY-8	Does the implementation allow the KaY to control the use of each transmit SA as specified in 10.7.23?	M	10.7.23, 10.5.1, 10.5.2	Yes[ ]
KAY-9	Does the implementation allow the KaY to monitor the nextPN associated with each transmit SA in order to create a new SA with a fresh SAK prior to PN exhaustion?	M	10.7.2	Yes[ ]
KAY-10	Does the implementation allow the KaY to select the Current Cipher Suite as specified in 10.7.25?	M	10.7.25	Yes[ ]
KAY-11	Does the implementation allow the KaY to create and control an SAK as specified in 10.7.26 and 10.7.28?	M	10.7.2	Yes[ ]

A.12 Management

A.12.1 Management - control and status information

Item	Feature	Status	References	Support
Can each of the following parameter values be read by management?				
MGT1-1	The SCI for the SecY	M	10.7.1	Yes[ ]
MGT1-2	MAC_Enabled, MAC_Operational, and operPointToPointMAC for the Uncontrolled Port	M	10.7.2	Yes[ ]
MGT1-3	MAC_Enabled, MAC_Operational, and operPointToPointMAC for the Controlled Port	M	10.7.4	Yes[ ]
MGT1-4	The maximum number of receive SCs and SAKs that can be in simultaneous use	M	10.7.7	Yes[ ]
MGT1-5	validateFrames, replayProtect, and replayWindow	M	10.7.8	Yes[ ]
MGT1-6	The SCI, receiving, createdTime, startedTime, and stoppedTime for each receive SC	M	10.7.12	Yes[ ]
MGT1-7	inUse, nextPN, lowestPN, createdTime, startedTime, stoppedTime, and Key Identifer for each receive SA	M	10.7.14	Yes[ ]
MGT1-8	The maximum number of SAKs that can be in simultaneous use for transmission	M	10.7.16	Yes[ ]
MGT1-9	protectFrames, useES, useSCB, and alwaysIncludeSCI	M	10.7.17	Yes[ ]
MGT1-10	transmitting, createdTime, startedTime, and stoppedTime for the transmit SC	M	10.7.20	Yes[ ]
MGT1-11	inUse, nextPN, lowestPN, createdTime, startedTime, stoppedTime, and Key Identifier for each transmit SA	M	10.7.22	Yes[ ]
MGT1-12	The currentCipherSuite identifer and the confidentialityOffset for frames with confidentiality protection	M	10.7.25	Yes[ ]
MGT1-13	transmits, receives, and createdTime for each SAK	M	10.7.27	Yes[ ]
MGT1-14	Can the management information for each implemented Cipher Suite be read?	M	10.7.24	Yes[ ]

A.12.2 Management - basic controls

Item	Feature	Status	References	Support
Can the following parameters be written by management?				
MGT2-1	validateFrames	O	10.7.8, 10.6	Yes[ ] No []
MGT2-2	replayProtect	O	10.7.8, 10.62, 10.6.4	Yes[ ] No []
MGT2-3	replayWindow	O	10.7.8,10.6.5	Yes[ ] No []
MGT2-4	protectFrames	O	10.7.17, 10.5	Yes[ ] No []
MGT2-5	useES	O	10.7.17, 10.5.3	Yes[ ] No []
MGT2-6	useSCB	O	10.7.17, 10.5.3	Yes[ ] No []
MGT2-7	alwaysIncludeSCI	O	10.7.17, 10.5.3	Yes[ ] No []
Can write access by management to each of the following parameters be disabled individually?				
MGT2-8	validateFrames	MGT2-1:M	10.7.8	Yes[ ]
MGT2-9	replayProtect	MGT2-2:M	10.7.8	Yes[ ]
MGT2-10	replayWindow	MGT2-3:M	10.7.8	Yes[ ]
MGT2-11	protectFrames	MGT2-4:M	10.7.17	Yes[ ]
MGT2-12	useES	MGT2-5:M	10.7.17	Yes[ ]
MGT2-13	useSCB	MGT2-6:M	10.7.17	Yes[ ]
MGT2-14	alwaysIncludeSCI	MGT2-7:M	10.7.17	Yes[ ]

A.12.3 Management - control over secure communication

Item	Feature	Status	References	Support
Can the following be created, controlled, or selected by management?				
MGT3-1	Receive SCs and SAs	O	10.7.11, 10.7.13, 10.7.15	Yes[ ] No []
MGT3-2	Transmit SAs	O	10.7.21, 10.7.23	Yes[ ] No []
MGT3-3	The current CipherSuite	O	10.7.25	Yes[ ] No []
MGT3-4	confidentialityOffset	O	10.7.25	Yes[ ] No []
MGT3-5	SAKs	O	10.7.26, 10.7.28	Yes[ ] No []
Can creation, control, or selection by management of the following be disabled individually?				
MGT3-1	Receive SCs and SAs	MGT3-1:M	10.7.11	Yes[ ]
MGT3-2	Transmit SAs	MGT3-2:M	10.7.21, 10.7.23	Yes[ ]
MGT3-3	The current CipherSuite	MGT3-3:M	10.7.25	Yes[ ]
MGT3-4	confidentialityOffset	MGT3-4:M	10.7.25	Yes[ ]
MGT3-5	SAKs	MGT3-5:M	10.7.25	Yes[ ]

A.12.4 Management - statistics

Item	Feature	Status	References	Support
Are each of the following interface statistics provided for the Controlled Port as specified in clause 10.7.6?				
MGT4-1	ifInOctets	M	10.7.6	Yes[ ]
MGT4-2	ifInUcastPkts, ifInMulticastPkts, ifInBroadcastPkts	M	10.7.6	Yes[ ]
MGT4-3	ifInDiscards	M	10.7.6	Yes[ ]
MGT4-4	ifInErrors	M	10.7.6	Yes[ ]
MGT4-5	ifOutOctets	M	10.7.6	Yes[ ]
MGT4-6	ifOutUcastPkts, ifOutMulticastPkts, ifOutBroadcastPkts	M	10.7.6	Yes[ ]
MGT4-7	ifOutErrors	M	10.7.6	Yes[ ]
Are each of the following frame verification statistics recorded as specified in clause 10.6 and maintained for the frame verification process as a whole?				
MGT4-8	InPktsUntagged	M	10.7.9, 10.6, Figure 10-5	Yes[ ]
MGT4-9	InPktsNoTag	M	10.7.9, 10.6, Figure 10-5	Yes[ ]
MGT4-10	InPktsBadTag	M	10.7.9, 10.6, Figure 10-5	Yes[ ]
MGT4-11	InPktsUnknownSCI	M	10.7.9, 10.6.1	Yes[ ]
MGT4-12	InPktsNoSCI	M	10.7.9, 10.6.1	Yes[ ]
MGT4-13	InPktsOverrun	M	10.7.9, 10.6.3	Yes[ ]
Are each of the following frame verification statistics recorded as specified in clause 10.6 and maintained for each receive SC?				
MGT4-14	InPktsUnchecked	M	10.7.9, 10.6.5	Yes[ ]
MGT4-15	InPktsDelayed	M	10.7.9, 10.6.5	Yes[ ]
MGT4-16	InPktsLate	M	10.7.9, 10.6.2, 10.6.4	Yes[ ]
Are each of the following frame verification statistics recorded as specified in clause 10.6 and maintained for each receive SC and for each of the four receive SAs corresponding to the last use of AN for that SC?				
MGT4-17	InPktsOK	M	10.7.9, 10.6.5	Yes[ ]
MGT4-18	InPktsInvalid	M	10.7.9, 10.6.5	Yes[ ]
MGT4-19	InPktsNotValid	M	10.7.9, 10.6.5	Yes[ ]
MGT4-20	InPktsNotUsingSA	M	10.7.9, 10.6.1	Yes[ ]
MGT4-21	InPktsUnusedSA	M	10.7.9, 10.6.1	Yes[ ]

A.12.4 Management - statistics *(continued)*

Item	Feature	Status	References	Support
Are each of the following frame validation statistics recorded as specified in clause 10.7?				
MGT4-22	InOctetsValidated	M	10.7.10	Yes[ ]
MGT4-23	InOctetsDecrypted	M	10.7.10	Yes[ ]
Are each of the following frame generation statistics recorded as specified in clause 10.5 and maintained for the frame verification process as a whole?				
MGT4-24	OutPktsUntagged	M	10.7.18, 10.5	Yes[ ]
MGT4-25	OutPktsTooLong	M	10.7.18, 10.5.5, Figure 10-4	Yes[ ]
Are each of the following frame generation statistics recorded as specified in clause 10.5 and maintained for each of the four transmit SAs corresponding to the last use of AN for the transmit SC?				
MGT4-26	OutPktsProtected	M	10.7.18, 10.5.4	Yes[ ]
MGT4-27	OutPktsEncrypted	M	10.7.18, 10.5.4	Yes[ ]
Are each of the following frame protection statistics recorded as specified in clause 10.7?				
MGT4-28	OutOctetsProtected	M	10.7.19	Yes[ ]
MGT4-29	OutOctetsEncrypted	M	10.7.19	Yes[ ]

A.13 Additional fully conformant Cipher Suite capabilities

Item	Feature	Status	References	Support
CSA-1	Name of Cipher Suite as specified in Clause 14. _			
CSA-2	Does the Cipher Suite implementation provide integrity without confidentiality?	O	14.2(	Yes[ ] No []
CSA-3	Does the Cipher Suite implementation provide confidentiality for all the octets of the User Data?	¬CSV-19: O CSV-19: M	14.2(d), 14.3(c)	Yes[ ] No []
CSA-4	Does the Cipher Suite implementation provide offset confidentiality for the User Data?	O	14.2(e), 14.3(c)	Yes[ ] No []
CSA-5	What is the maximum number of receive SCs supported by the Cipher Suite implementation? _ _ _ _ _		5.3(i)	
CSA-6	What is the maximum number of receive SAKs supported by the Cipher Suite implementation? _ _ _ _ _		5.3(i)	

A.14 Additional variant Cipher Suite capabilities

Item	Feature	Status	References	Support
CSV-1	Name of Cipher Suite or other commonly used identification (to be supplied) _			
CSV-2	Identify the specification(s) of the Cipher Suite, including any additional information necessary to acquire the specification(s) (supply items of Additional Information if necessary) _ _ _ _	M	14.3	
CSV-3	Does the specification include interoperable protection and verification procedures specified in terms of the parameters of clause 14.1?	M	14.3(a), 14.1	Yes [ ]
CSV-4	Is the specification publicly available and the sunject of a review process under the aegis of an accredited standards committee?	M	14.3(b)	Yes [ ]
CSV-5	Do the Cipher Suite algorithms have an effective key length of at least 128 bits, and does any block cipher used have a block width of at least 128 bits?	M	14.4.1(a)	Yes[ ]
CSV-6	Has NIST approved the cryptographic cipher(s)?	CSV-7:O ¬CSV-7:M	14.4.1(b)	Yes[ ] No[ ]
CSV-7	Has NESSIE approved the cryptographic cipher(s)?	CSV-6:O ¬CSV-6:M	14.4.1(b)	Yes[ ] No[ ]
CSV-8	Does the Cipher Suite satisfy the message authentication requirements of clause 14.4.1? Identify the proof of security, including any additional information necessary to acquire the proof _ _	M	14.4.1(c)	Yes [ ]
CSV-9	Does the Cipher Suite satisfy the confidentiality requirements of clause 14.4.1? Identify the proof of security, including any additional information necessary to acquire the proof _ _	CSV-N OR CSV-N:M	14.4.1(d)	Yes [ ]
CSV-10	Does the Cipher Suite use mechanisms for confidentiality and authentication in a way that is consistent with the the proofs of security?	M	14.4.1(e)	Yes[ ]
CSV-11	Does the Cipher Suite provide integrity protection for the SCI, PN, Source Address, Destination Address, SecTAG, and User Data?	M	14.2(a)	Yes[ ]
CSV-12	Does the Cipher Suite provide protection for up to 2^{32}-1 invocations without requiring a fresh SAK?	M	14.2(b)	Yes[ ]

A.14 Additional variant Cipher Suite capabilities *(continued)*

Item	Feature	Status	References	Support
CSV-13	Does the Cipher Suite generate a predictable number of octets of Secure Data and ICV given any specific number of octets of User Data?	M	14.2(c)	Yes[ ]
CSV-14	Does the maximum difference in length of the User Data and the Secure Data plus ICV exceed 896 octets?	X	14.2(f)	Yes[ ]
CSV-15	What is the maximum difference in length of the User Data and the Secure Data? _ _ _ _ _ octets		14.3(b)	
CSV-16	What is the length of the ICV _ _ _ _ _ octets		14.3(e)	
CSV-17	Does the specification specify the length and properties of the keys required, including assumptions of the scope of uniqueness?	M	14.3(f)	Yes[ ]
CSV-18	Does the Cipher Suite implementation provide confidentiality for all the octets of the User Data?	¬CSV-19: O CSV-19: M	14.2(d), 14.3(c)	Yes[ ] No []
CSV-19	Does the Cipher Suite implementation provide offset confidentiality for the User Data?	O	14.2(e), 14.3(c)	Yes[ ] No []
CSV-20	Does the Cipher Suite modify or constrain the values of the SCI, PN, Source Address, Destination Address, or SecTAG fields other than as specified in Clause14?	X	14.2(g)	No []
CSV-21	Does the Cipher Suite require an SAK exceeding 1024 bits long?	X	14.2(h)	No []
CSV-22	Does the Cipher Suite require different keys for the protect and validate operations?	X	14.2(i)	No []
CSV-23	What is the maximum number of receive SCs supported by the Cipher Suite implementation? _ _ _ _ _		5.3(i)	
CSV-24	What is the maximum number of receive SAKs supported by the Cipher Suite implementation? _ _ _ _ _		5.3(i)	

Annex B (informative)

Bibliography

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

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

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

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

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

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

ISO 6937-2: 1983, Information processing—Coded character sets for text communication—Part 2: Latin alphabetic and non-alphabetic graphic characters.[1]

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.

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.

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.

[1]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.