IEEE P802.1AE/D2.01

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: For keywords refer to the title page proper, following the editors' foreword.

All rights reserved.This document is an unapproved draft of a proposed IEEE Standard. As such, this document is subject to change. USE AT YOUR OWN RISK! Because this is an unapproved draft, this document must not be utilized for any conformance/compliance purposes. Permission is hereby granted for IEEE Standards Committee participants to reproduce this document for purposes of IEEE standardization activities only. Prior to submitting this document to another standards development organization for standardization activities, permission must first be obtained from the Manager, Standards Licensing and Contracts, IEEE Standards Activities Department. Other entities seeking permission to reproduce this document, in whole or in part, must obtain permission from the Manager, Standards Licensing and Contracts, IEEE Standards Activities Department.

IEEE Standards Department
Copyright and Permissions
445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331, USA

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.

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; (978) 750-8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

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

Email:allyn@cisco.com

Dolors Sala
Chair, 802.1 Link Security Task Group

Email:dolors@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.
- 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 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.

>>

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

<<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/D2.01
October 19, 2004

IEEE P802.1AE/D2.01

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 Department
Copyright and Permissions
445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331, USA

IEEE Std 802.AE, 200X Edition

....

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

There is no intention that IEEE Std 802.1AE be used for IEEE 802.11, which has it's own security standard, IEEE Std 802.11i. Such a replacement is not within the scope of the IEEE 802.1AE PAR.

IEEE Std 802.1X specifies port based network access control.

IEEE Std 802.1af specifies key management and the establishment of secure associations used by IEEE Std 802.1AE.

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 incorporating MAC Security 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, authorization, 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 for MAC Security in terms of provision of the MAC Service and the preservation of the semantics and parameters of service requests and indications.
b) Describes the threats, both intentional and accidental, to correct provision of the service.
c) Specifies security services that prevent, or restrict the effect of attacks that exploit these threats.
d) 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.
e) 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 in End Stations and Bridges.
f) Specifies how SecYs are incorporated within the architectural structure of End Stations and Bridges.
g) 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.
h) Specifies the format of the MACsec Protocol Data Unit (MPDUs) used to provide secure service.
i) Specifies the interface/exchanges between a SecY and its associated and collocated Key Agreement Entity (KaY, P802.1af) that provides and updates cryptographic keying to the SecY.
j) Establishes the requirements for management of MAC Security, identifying the managed objects and defining the management operations for SecYs
k) Specifies performance requirements and recommends default values and applicable ranges for the operational parameters of a SecY.
l) Specifies the requirements to be satisfied by equipment claiming conformance to this standard.

This standard does not

m) specify how the relationships between MACsec protocol peers are discovered, authenticated, authorized, as supported by key management or key distribution protocols, but makes use of P802.1af Key Agreement for MAC security.

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.

ANSI X3.159-1989, American National Standards for Information Systems—Programming Language—C.[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-2001, IEEE Standards for Local and Metropolitan Area Networks—Port Based Network Access Control.

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 Edition, IEEE Standards for Local and Metropolitan Area Networks, Supplement to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications: Aggregation of Multiple Link Segments.

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.

<<802.1aa. If it is not yet a standard, will be removed before final draft>>

IETF RFC 2108[4], Definitions of Managed Objects for IEEE 802.3 Repeater Devices using SMIv2, de Graaf, K., and Romascanu, D., February 1997.

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

ITEF RFC 2737, Entity MIB (Version 2), McCloghrie, K., and Bierman, A., December 1999.

[1] ANSI publications are available from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

[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.

[4] Internet RFCs are retrievable by FTP at ds.internic.net/rfc/rfcnnnn.txt (where nnnn is a standards publication number, such as 1493), or by Web browser at http://www.ietf.org/ , or call InterNIC at 1-800-444-4345 for information about receiving copies through the mail.

IETF RFC 2922, Physical Topology MIB, Bierman, A., and Jones, K., November 1998.

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

IETF RFC 1155/STD 16, Structure and Identification of Management Information for TCP/IP-based Internets, Rose, M., and K. McCloghrie, May 1990.

IETF RFC 1157, Simple Network Management Protocol, Case, J., Fedor, M., Schoffstall, M., and Davin, J., SNMP Research, May 1990.

IETF RFC 1212, Concise MIB Definitions, Rose, M., and McCloghrie, K., March 1991.

IETF RFC 1213/STD 17, Management Information Base for Network Management of TCP/IP-based internets, McCloghrie K., and Rose, M., Editors, March 1991.

IETF RFC 1215, A Convention for Defining Traps for use with the SNMP, Rose, M., March 1991.

IETF RFC 1901, Introduction to Community-based SNMPv2, Case, J., McCloghrie, K., Rose, M., and Waldbusser, S., January 1996.

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 2674, Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions, Bell, E., Smith, A., Langille, P., Rijhsinghani, A., and McCloghrie, K., August 1999

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

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

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.

IETF RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), Case, J., Harrington, D., Presuhn, R., and Wijnen, B. December 2002.

IETF RFC 3413, Simple Network Management Protocol (SNMP) Applications, Levi, D., Meyer, P., and Stewart, B., December 2002.

IETF RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), Blumenthal, U., and Wijnen, B., December 2002.

IETF RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), Wijnen, B., Presuhn, R. and McCloghrie, K., December 2002.

IETF RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), Presuhn, R., Ed., December 2002.

IETF RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP), Presuhn, R., Ed., December 2002.

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

ISO 6937-2: 1983, Information processing—Coded character sets for text communication—Part 2: Latin alphabetic and non-alphabetic graphic characters.[5]

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

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.

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

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.

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

3. 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 AAA: Authentication, Authorization, and Accounting. Normally used in the context of the Radius or Diameter protocols.

3.2 Additional Authenticated Data (AAD): A sequence of octets supplied to a cryptographic function that are to be integrity protected using a secret key but that can be read in clear text without possession of the key.

3.3 AA Key: A secret key that embodies the result of authentication and authorization protocols, i.e. knowledge of the key by a protocol entity is not possible unless it is the entity identified and authorized for the purposes which peer entities also possessing the key are to use information securely bound to the key.

3.4 bidirectional: Operating in both of two opposite directions.

3.5 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 a explicit goal of this standard that MAC Security is transparent to the users of the MAC Service.

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

3.7 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.

3.8 controlled port: the access point used to provide the secure MAC Service to a client of a SecY.

3.9 data integrity: The condition or state in which data has not been altered. An algorithm that checks for integrity can detect tampering if it occurs, it does not guarantee against tampering.

3.10 connectionless data confidentiality: The protection of service data units from unauthorized disclosure during transmission from one entity to one or more entities, where there is no reliance of one protected date unit on any of its predecessors.

3.11 connectionless integrity: A service providing for the integrity of the parameters of a single service primitive, without reliance on preceding primitives.

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

3.13 initialization vector (IV): A value used to initialize a cryptographic algorithm or protocol, particularly block cipher modes of operation and stream ciphers.

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

3.14 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. Also known as a MAC.

3.15 key: A sequence of octets that controls the operation of cryptographic functions.

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

3.17 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.

3.18 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), and IEEE Std 8802.11 (Wireless).

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

3.20 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.

3.21 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.

3.22 man-in-the-middle attack: A class of active attack in which the attacker exploits inadequate authentication to become a proxy for data between two parties wishing to communicate. Acting as a proxy, the attacker may be able to modify data selectively without detection.

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 Message Authentication Code: A value generated by a symmetric cryptographic function. If the input data is changed, a value cannot be correctly computed without knowledge of the secret key. Thus, the secret key protects the input data from undetectable alteration. Known as an ICV in this Standard.

3.25 mode: A mode of operation, or mode, for short, is an algorithm that features the use of a symmetric key block cipher algorithm to provide one or more information services, such as confidentiality or message integrity.

3.26 nonce: A value that, given a particular key, must not be reused (except with negligible probability), without risking security compromise.

3.27 non-repudiation: The ability to establish that a message was generated by a particular entity. That is, a message is said to be non-reputable when an entity sends the message and some entity (usually not the same one) can demonstrate beyond a reasonable doubt that the entity sent the message. In practice, cryptography can only demonstrate that particular key material was used to produce a message, and does not protect against stolen credentials or duress.

3.28 Packet Number (PN): A monotonically increasing value used to uniquely identify a MACsec frame in the sequence of frames transmitted using an SA.

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

3.30 secret key: A cryptographic key known only to the communicating parties and used for both encipherment and decipherment.

3.31 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.

3.32 secure association identifier (SAI): An identifier for an SA, comprising the SCI concatenated with the Association Number (AN).

3.33 secure association key (SAK): The secret key used by an SA.

3.34 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.

3.35 secure channel identifier: 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.

3.36 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 to be supported by MACsec.

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

3.38 trust: When one party trusts the other party to not subvert the goals of the protocols, e.g., it will not attempt to perform the following attacks: spoofing, repudiation, information disclosure, denial of service, or elevation of privilege.

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

3.40 unidirectional: Operating in a single direction.

3.41 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.

4. Abbreviations

The following abbreviations are used in this standard.

AAD	Additional Authenticated Data
AES	Advanced Encryption Standard
CA	Secure Connectivity Association
CRC	Cyclic Redundancy Check
CTR	Counter mode
EA	Crypto algorithm that does both encryption and authentication
FCS	Frame Check Sequence
FIPS	Federal Information Processing Standard
ICV	Integrity Check Value
kb/s	Kilobit per second (1 kb/s is equivalent to 1000 bits per second)
KaY	MAC Security Key Agreement Entity
MAC	Media Access Control
MIC	Message Integrity Code
Mb/s	Megabit per second (1 Mb/s is equivalent to 1,000,000 bits per second)
MPDU	MACsec Protocol Data Unit
MSDU	MAC Service Data Unit
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OUI	Organizationally Unique Identifier
PAE	Port Access Entity
PBL	Packet Body Length (IEEE 802.1X)
PDU	Protocol Data Unit
PN	Packet Number
PMK	Pairwise Master Key
PRF	Pseudo-Random Function

PRNG	Pseudo Random Number Generator
PSK	Pre-Shared Key
RSN	Robust Security Network
RSTP	Rapid Spanning Tree Algorithm and Protocol
RST BPDU	Rapid Spanning Tree Bridge Protocol Data Unit
SA	Secure Association
SAI	Secure Association Identifier
SAK	Secure Association Key
SC	Secure Channel
SCI	Secure Channel Identifer
SecY	MAC Security Entity
SNAP	Sub-Network Access Protocol
Tb/s	Terabit per second (1 Tb/s is equivalent to 1,000,000 MB/s)

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 sytem 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 5.2 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. See 5.4 Recomendations.

5.1 Required Capabilities

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

a) Implement the MAC Security Protocol (MACsec), as specified in Clause 15.
b) Encode, decode, and validate MACsec PDUs as specified in Clauses 9 and 10.5.3.
c) Support the MAC status and point-to-point parameters for the Controlled and Uncontrolled Ports as specified in Clauses 6.5, 6.7, and 10.7.
d) Use a globally unique 48-bit MAC Address and a Port Identifier unique within the scope of that address assignment to identify the transmit SCI, as specified in Clause 8.2.1.
e) Satisfy the performance requirements specified in Table 10-2, and Clause 8.2.2.
f) Satisfy the undetected frame error rate requirement specified in Clause 10.4.
g) Provide the management functionality specified in Clause 12.
h) Support the Default Cipher Suite and Default Confidentiality Cipher Suite specified in Clause 14.
i) Specify the following parameters for each Cipher Suite implemented
    1) The maximum number of receive SCs supported
    2) The maximum number of receive keys
j) Specify the following performance characteristics of the implementation
    1) ....
    2) ....

An implementation of a MAC Security Entity (SecY) for which full conformance to this standard is claimed shall not implement Cipher Suites other than those specified in Clause 14.

5.2 Optional Capabilities

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

a) Support SNMP management using the MIB specified in Clause 13.
b) Support additional Cipher Suites specified in Clause 14.
c) Use Cipher Suites not specified in Clause 14, but meeting the criteria specified in 14.2, 14.3

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.

5.3 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 (normative) and shall provide the information necessary to identify both the supplier and the implementation.

5.4 Recommendations

<<On management - which may need to be mandatory, or at least a ban on implementing SNMP before V3?.>>

<<On advice, caveat emptor etc. on the assumption of security, of short enough words can be found.>>

<<On protocol policies to support security?>>

<<On the use, or non-use of additional Cipher Suites, partiicularly those that are proprietary or home grown.>>

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.

The goal of MAC Security is to provide transparently the same MAC Service as is offered without MAC Security, and to offer that service securely. The requirements for MACsec that are discussed in this clause, are informed by the goal of preserving the parameters of the MAC Service. Figure 6-1— Architectural Description, shows a schematic representation of MAC Security in relationship to the secure and insecure MAC Service interfaces. The MAC Service is preserved in the sense that the Service is the same at both interfaces, only it is secure at one interface and insecure at the the other. [REMOVE- See Figures 6-1 and 6-2 from .1AB and Figures 11.4 etc. here.]

NOTE 1—While it is possible to use cryptography to change the LAN topology, it is not only a non-goal to do so, but is strongly advised against. Any changes affecting the connectivity model should be done through the appropriate infrastructure mechanisms, and not as a side effect of cryptography.

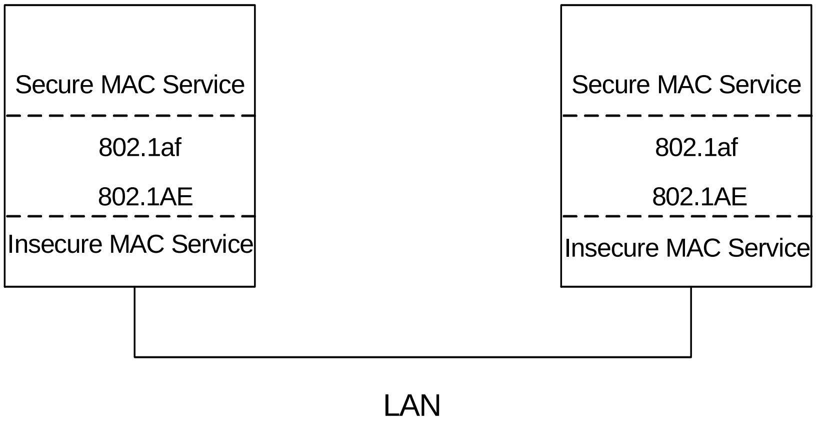


Figure 6-1—Architectural Description

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—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 (7.2), and on the security and trust placed in the MAC Bridges that interconnect those LANs (Clause 16.).

NOTE 2—Authentication and authorization is outside the scope of this standard, which ensures secure communication between mutually authenticated and authorized service access points.

NOTE 3—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 (6.2) 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.

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—MACsec Frame, VLAN TAG, and Quality of Service, shows the Priority field encapsulated in VLAN TAG and this 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.

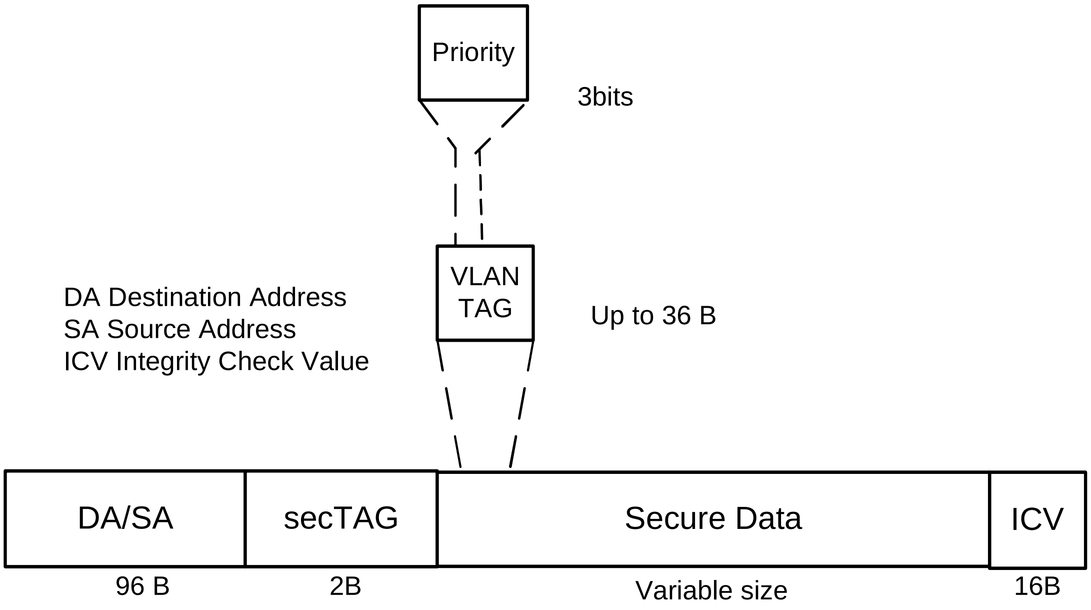


Figure 6-2—MACsec Frame, VLAN TAG, and Quality of Service

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 (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 LAN connectivity

The MAC Service provided by a point-to-multipoint LAN provides connectivity from a single distinguished point station to one or more multipoint stations, and from each of the multipoint stations to the point station. It does not provide connectivity from any multipoint station to any other multipoint station. Efficient multicast and broadcast to all multipoint stations is provided: a single service request with a given destination address at the point station can result in service indications at each multipoint station wishing to receive frames with that destination address.

NOTE—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.

NOTE1—KaY must check that it has an appropriate receive key for each active transmitter, and that it has handed out its key to those transmitters before asserting MAC_Operatl Ture, and allowing both transmission and reception. Frames validly received before the transmitter can be activated should be discarded.

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), MSTP (IEEE Std 802.1Q), and LACP (IEEE 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 media 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, such as configuration protocol transactions, 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 IEEE 802.1af 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 the MACsec operates within a single CA.

NOTE 1—In this standard, CA is the acronym for Secure Connectivity Association.

NOTE 2—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 3—EPON can be considered an exception with respect to symmetric connectivity. Discussion for the case of SCB for EPON is in (8.4).

b) If MAC_Operational is True in stations wanting to join a 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 time such that clients of the service are aware of the transition.
c) If MAC_Operation 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_Operation is False until the join is accomplished when it’s state transitions to MAC_Operational True.
d) If adminPointToPointMAC and MAC_Operational is True then operPointToPointMAC is True only if at most one other station is participating in the CA.

NOTE 4—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 parameter values supplied with the service request;
c) does not occur after a known bounded time has elapsed since the service request was made;

and can also ensure that

d) no more than one indication results from one service request;
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
   1) service requests,
   2) values of service request address parameters, or
   3) the number of octets that comprise the number of octets that comprise the MSDU

   from stations that are not members of the CA;
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 (c) is based on the frequency of distribution of cryptographic keying material, and is typically longer than required to enforce the maximum transit delay requirements of the MAC Service.

NOTE 1—The addition of explicit time indications to the SecTAG to provided 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 MACsec group”, rather than a particular individual station;
c) *confidentiality* (6.8(e));
d) *replay protection* (6.8(c), 6.8(d));
e) bounded receive delay;

and may 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.

<<As part of making one such policy easy to implement we should specify, in 802.1D, that a Filtering Database entry can be created for an Edge Port by functions that can make use of media specific management methods, and that learning can be turned off on that port - provided frames with additional source addresses are discarded. For discussion.>>

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 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 other than that expected for a specific media access control method as a consequence of a small increase in frame size. Conformant 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 the 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 10-2). 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 is additional delay is introduced by providing security. The typical bound on frame lifetime is approximately two seconds. See (10.11).

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 may be constrained by the owner of the LAN.

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).

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.

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 (7.2)

and delineates the responsibilities of the

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

NOTE 3—The term “individual LAN” (3.18) 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

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 SAI (Figure 7-7) are similar to but not exactly the same as those associated with the SPI defined by IPsec and the SAID previously defined by IEEE Std 802.11 (now withdrawn). The normative properties of all terms used in the standard are as defined by this standard.

Each station 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 the station between the SecY and its associated KaY is described in Clause 10 and Figure 10-2. Each KaY discovers the KaYs present in other stations attached to the same LAN, mutually authenticates and authorizes those stations, 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), one per LAN Service, is created to meet the requirements of the MAC Service (6.2) and MACsec (6.7) for connectivity between the stations

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). In contrast it is desirable to use a new SAK at periodic intervals to defend against a successful attack on an 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.

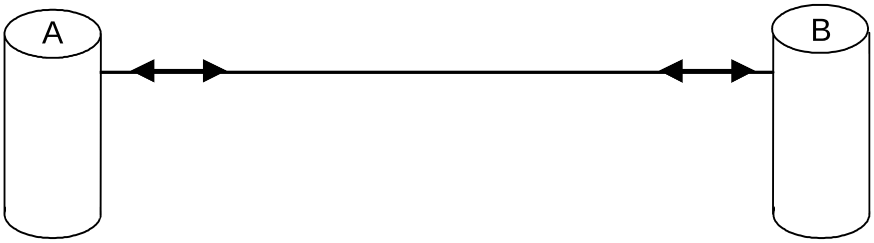


Figure 7-1—Two stations connected by a point to point LAN

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

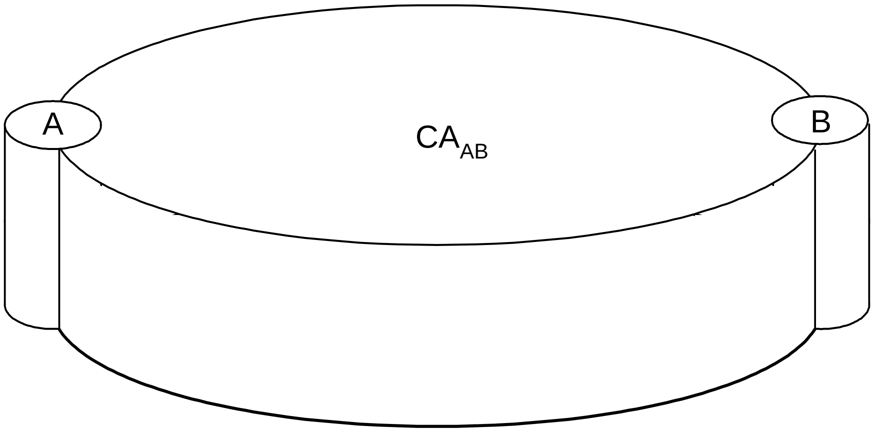


Figure 7-2—Two stations in a CA created by MACsec Key Agreement

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

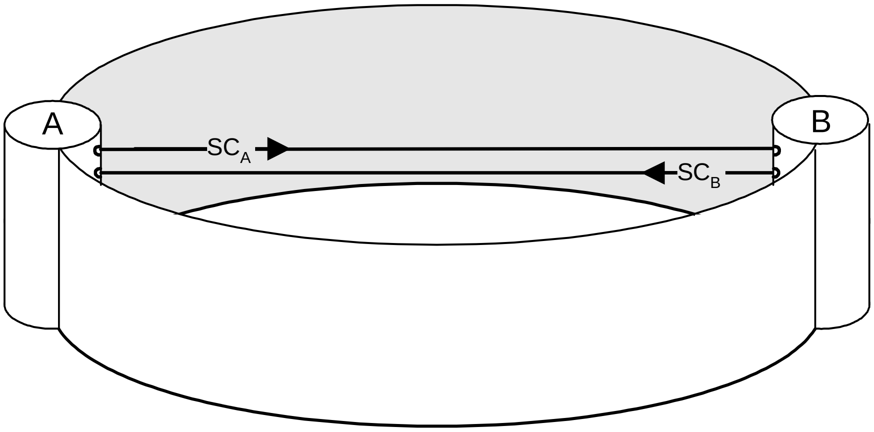


Figure 7-3—Secure communication between two stations

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

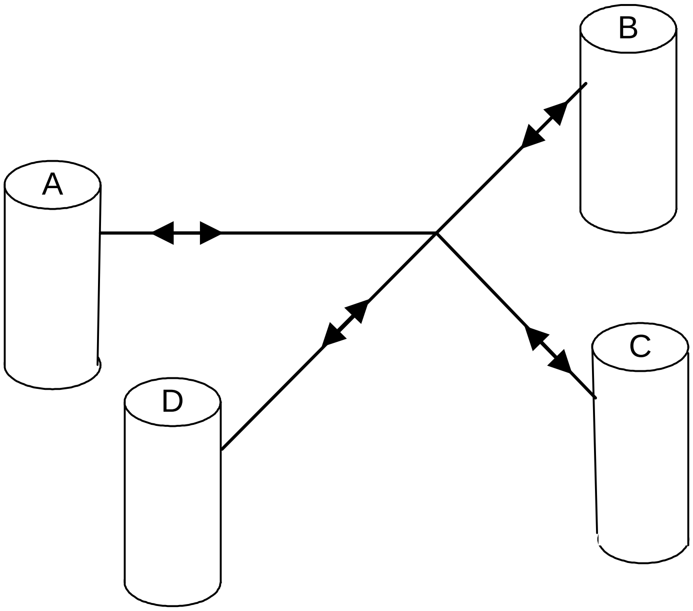


Figure 7-4—Four stations attached to a shared media LAN

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.

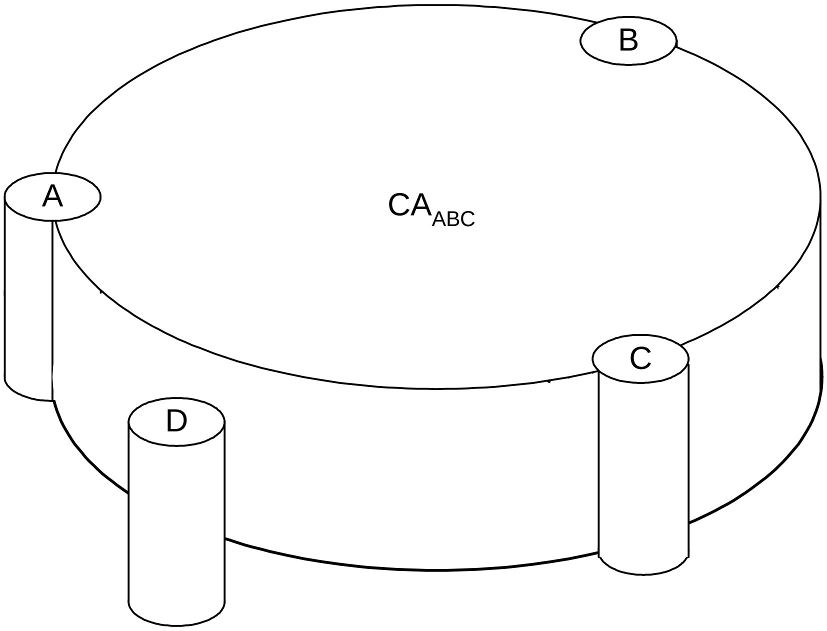


Figure 7-5—A CA including ports A, B, and C

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

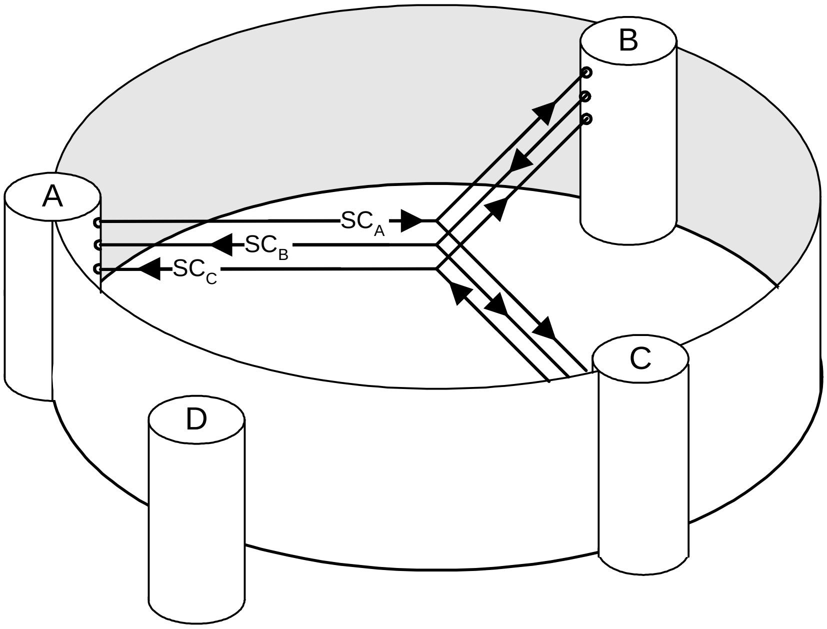


Figure 7-6—Secure communication between three stations

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.

There is only one CA per LAN Service, as discussed in (ref), and each SecY participates in only a single CA at any one time, since a SecY provides a single port of access to a LAN. 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, and receives frames conveying secure service indications on separate SCs, one for each of the other SecYs participating in the CA. Each SC provides unidirectional point to multipoint communication, and it can be long lived, persisting through SAK changes.

Each SC is identified by a Secure Channel Identifier (SCI), comprising a unique 48-bit Universally Administered MAC Address, identifying the system of which the transmitting SecY is part, concatenated with a 16-bit Port number, identifying the SecY within that system (Figure 7-7).

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 an 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 address, 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—The 64-bit value 00-00-00-00-00 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.

NOTE 3—An EPON OLT (8.4) can use a distinct SC to support the Single Copy Broadcast capability. The formal identifier for this SC comprises a System Identifier for the OLT and a reserved Port Number, both may be represented in the secured frame by a single SCB bit (Clause 9).

NOTE 4—The SCI field 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 PAE entity for the peer SecYs, together with the direction of transmission of the secured MPDU, can be used to identify the transmitting SecY and therefore the 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.

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 5—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 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 three 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 may accept interleaved SAs is .5 seconds.

NOTE—At the transmitter there should not be any interleaving.

If a SecY does not have a usable SA for its outbound SC, i.e. an SAK that all other SecYs are prepared to use for receipt, and a usable SA for each inbound SC, i.e. an SAK that it can use at no notice for frames received on that SC, then the MAC_Operational status parameter (6.4) is set FALSE.

When the service guarantees provided (6.8) include replay protection, the MACsec protocol requires a separate replay protection sequence number counter for each SA.

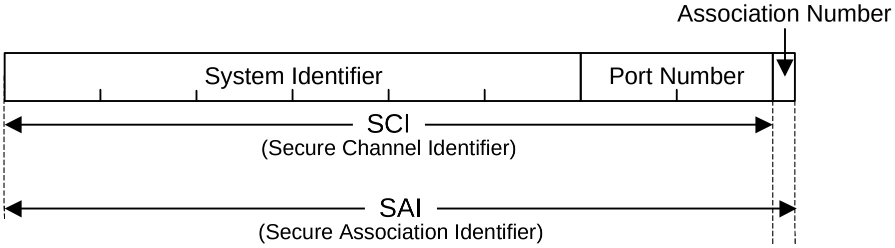


Figure 7-7—Secure Channel and Secure Association Identifiers

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

A secure MAC Service is constructed from a single instance of an insecure MAC Internal Sublayer Service, which suppports a single Common Port. It is not possible to have multiple Common Ports from a single ISS,. and as there is just one Common Port per LAN Service, there is only one secure MAC instance, that is, SecY, on a single LAN Service.

Multiple instances of secure MAC Service on a physical LAN require the creation of multiple instances of the LAN Service, or equivalently, the creation of multiple Common Ports. A single LAN can provide multiple instances of the secure MAC Service if 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 of which supports a distinct SecY.

The process of providing multiple MAC service instances is not part of MACsec, but occurs below the ISS provided to the SecY’s Common Port.

NOTE— Although multiple CAs can in principle be constructed on a single LAN by using different keys to separate connectivity without any underlying separation of service instances, that is a very bad idea. First such a scheme makes a hash of deploying MACsec, turning security on or off radically changes the network connectivity. This is hardly the behavior that is envisaged in the PAR, where it is stated that MACsec should operate transparently to its clients. Staged deployment scenarios using integrity protection without validation become impossible. Second such a scheme is an accident waiting to happen, if the keys for one CA ever coincide with or overlap the other, the CAs will merge for a period - and guarding against this problem simply exports a new and very unusual problem to key agreement. Third such a scheme requires explicit support from key agreement, which will have to carry an explicit multiplexing value to separate key agreement for the two separate instances. Fourth such a scheme requires explicit configuration of the ports attached to each "separate" CA if bridging is going to be provided between the instances. Fifth such a such a scheme will result in a high error rate, thus masking any other problems. We need to stick to one SecY being in one CA on one instance of an underlying service as far as possible. If multiple underlying services are to be realized on the same LAN then they should be supported as described in this clause.

Where multiple instances of service are supported by a single instance of physical media, a multiplexing function is required so that multiple Common Ports can be provided to separate SecYs. Identification of each service instance, and multiplexing and demultiplexing to and from the transmission capabilities provided by the LAN, are performed wholly below the ISS provided to the SecY’s Common Port (Clause 8), and thus can be accomplished by 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 (ref) . Also, see () for a discussion of the distinctions associated with Provider Bridges.

NOTE 1—Although the field or fields used to provide service instance multiplexing may not be parameters of the ISS, and thus 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 it’s membership. 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 must transition 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 the CA_y.

NOTE 2—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 each end station to identify each of a number of SecYs in the Bridge.

NOTE 3—This capability does not apply to the use of IEEE Std 802.11. That standard specifies its own mechanisms for identifying separate secure associations.

7.2 Use of the secure MAC Service

The secure MAC Service guarantees (6.8) the integrity of the parameters of each service indication, and that that each indication is a result of a request made by a SecY that is a member of the same CA as the receiver. 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.

NOTE 1—The secure MAC Service does not guarantee that the service request was made by any particular member of the CA.

NOTE 2—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 stations 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 (7.2.1) to support overall network security.

NOTE 3—Correct operation of spanning tree protocol depends, for example, 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)(8.X), 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 3—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 forwarded frames. In this case the trust is partly transitive, the question to be answered by each member of the CA being the degree of trust to place in the Bridge’s trust of systems that originate frames that the Bridge will forward.

7.2.1 Client policies

Client policies can include but are not limited to:

a) limiting the set of protocol procedures that can be invoked by the peer
b) segregating the communication from communication using different service instances
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.

7.2.2 Use of the secure MAC Service by Bridges

Each Bridge Port uses the service provided by an individual LAN, 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 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 4—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 proposed in P802.1ad 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 7.2) of the peer system(s) is not sufficient to allow full participation in determining the active topology of the network.

<<Using authorization time allocation of Bridge Ports to MAC service instances is efficient in terms of leveraging existing specifications but not entirely satisfactory in cases where one of a limited number of "port prototypes" is really desired to establish most of the parameters. Additionally a few of the parameters, the PVID for example, may not be conveniently pre-configured in every Bridge by port number. Some upgrade to the existing bridge specifications would seem to be required (outside of the MACsec activity), in concert with

the efforts to augment Radius parameters and to ensure cryptographic binding of other configuration tunnels to the authenticated MACsec Key Agreement peer(s).>>

Use of PVID, VLAN Translation Table, and Member Set policies in VLAN-aware Bridges, segregation of relayed frames by assigning them to differing VLANs on the basis of the authorization associated with the secure MAC Service instance supporting each receiving Bridge Port.

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.

<<Such a filtering capability is not currently present in 802.1D or 802.1Q. At the minimum a working group proposal to augment those specifications to support MAC Security, with this specific feature amongst others, would be required if the above capability is to feature in this proposed standard. The feature has been used in networks of significant size and complexity, and is known to be effective.>>

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. The state machines, variables, and procedures specified in Clause 15 constitute the normative specification of MACsec, and take precedence over the description in this clause in case of any conflict or ambiguity.

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).

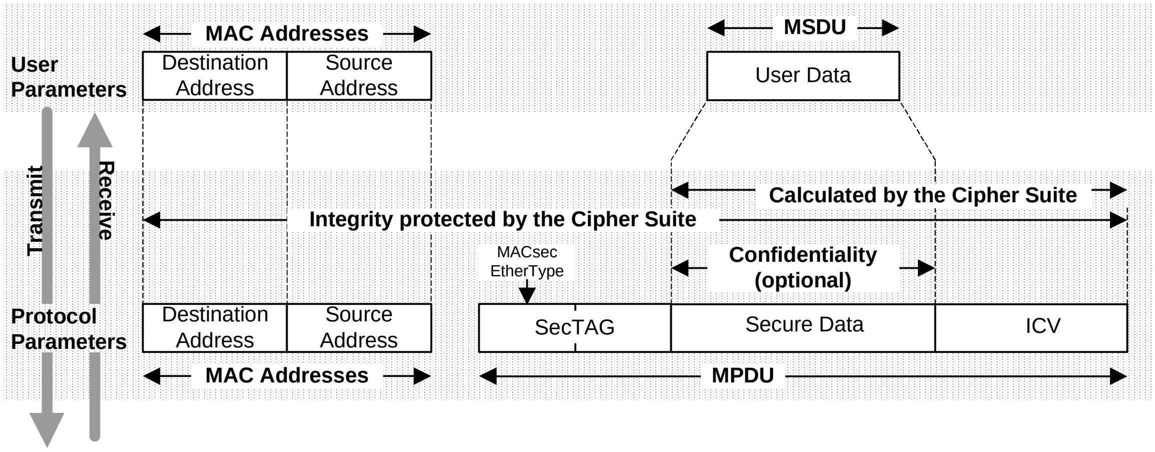


Figure 8-1—MACsec

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 media 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 on 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 disruption of 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, irrespective of the state of the MACsec state machines.
c) Allows operation of the Key Agreement protocol to be independent of MACsec. This, together with the capabilities above, allows authentication and authorization to be updated together with the AA keys (e.g. the PMKs provided by EAP) bound to the authentication and authorization information held by the communicating systems, and fresh SAKs derived from new AA keys, at any time, without unnecessarily disrupting communication.

NOTE 1—This last capability raises the number of SAKs required to be held by the receiver per SC from 2 (required to allow the transmitter to decide to change SAKs without disrupting reception), to 3 (since Key Agreement can provide a new SAK to a receiver just when a change in SAKs by the transmitter is already imminent or in progress).

NOTE 2—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 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 and block cipher 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, 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 for other Cipher Suites for which the Secure Data remains the same as the User Data and the 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, 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 and a Default Confidentiality 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 suites have been selected (Clause 14) in part because of their 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 independent of the total number of systems that compose the network. The required resources are a function of the number of the SecY peers on the same LAN. Resources are not necessary for systems that are not on the same LAN, but are part of the same network.

8.1.7 Intrusion detection

Intrusion detection can be faciltated by the management functions (ref). For example, an entity monitoring network traffic counts might be able to detect abnormal behavior.

Additional mechanisms for detecting abnormality based on management functions are possible, but are outside the scope of this specification.

<<Detection of attempts to break in, counting bad frames etc.>>

<<Intrusion detection based on supporting policies and detection mechanisms provided by client protocols. Some of this should simply be a forward reference to the management clause.>>

8.1.8 Localization and isolation of attacks

<<Simple responses to attacks using MACsec controls. Isolation of attacks using client policies. Support of localization and response using client policies (but check for overlap with clause 7.2)>>

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 1 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.

<<Is 1 second enough to allow precomputation of key schedules, or whatever other name is given to the table entries used by cryptographic algorithms?>>

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)

<<What MACsec depends on Key Agreement to achieve. Timeliness of operation etc. Mention the policy and authorization implications/needs, or the requirement for binding to a secure tunnel that can supply these. Timing of coordinated changes. Deployability criteria not to be mentioned here as will be covered by the Key Agreement PAR/Project.>>

<<A number of the KaY related requirements are independent both of the design of MACsec, and the functionality provided by Key Agreement to MACsec. They will be moved to P802.1af as that proposed standard is drafted.>>

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), 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 1 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 conformant, 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 1 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 shall be able to perform the following functions independently of the design and state of MACsec

a) discover the required connectivity, identifying the SCs that compose the CA
b) operate resiliently in face of most denial of service attacks.

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 must be able to discover connections between peer stations, and recognize what potential connections are available. The Discovery mechanism (protocol?) is within an individual LAN, and uses the Bridge Group Address.

NOTE 1— The MAC status parameters (6.4) indicate when there is a new connection, and when the connectivity provided by the CA has changed. If there is a change in the trust relationship, the line goes down and comes up again, so that the status parameter reflects the reset. The related policy engine sees the new trust status after the reset. This mechanism prevents attacks that secretly degrade the trust level.

The KaY must accept indications of which Cipher Suites are supported by the SecY via the LMI. The choice of Cipher Suites is controllable by management via the Cipher Suite Selectable parameter. The choice of negotiated Cipher Suite is delivered to 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 must accept indications of which connectivity capabilities are supported by the SecY via the LMI. The KaY will deliver the connectivity selection to the SecY via the LMI. (This will cause the setting of the Cipher Suite's Oper Multipoint Connectivity variable in the SecY.)

The KaY will set the Neighbors All SecYs variable if ...

8.2.5 Authentication requirements

The KaY may authenticate the peer station if there is no pre-shared key in place. When there is a pre-shared master key, there is no need to generate a master key via the authentication process. In this case, the key management process will find a preshared key and operate without the authentication process needing to generate the key.

In either case, 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 based on the outcome of the authentication and authorization process. 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

Symmetric MAC Service is maintained via a commit protocol.

The KaY will deliver transmit and receive SAKs via the LMI.

The KaY will create, manage, and maintain one CA that connects two or more KaYs and their corresponding SecYs. The KaY will create and maintain all of the point to multipoint SCs between itself and all the stations within the CA. For each SC, the KaY repeatedly creates and manages short-lived sequential overlapping pairs of SAs between two peers.

The KaY will accept indication of impending exhaustion of the SA from the SecY via the LMI. The KaY will efficiently derive new SAKs from the Master Key.

The KaY will accept 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 will accept indication from the SecY that a PN is close to exhaustion. (model as status variable setting) The KaY will select the Default Cipher Suite when the PN is exhausted and the local service is capable of invoking policies based on authorization.??

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 Integrity Check Value (ICV) ensures the *integrity* of the MAC Destination Address, MAC Source Address, SecTAG, and User Data.

NOTE 2—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.

<<Liaison with 802.3 on the subject of an increase in maximum frame size to allow successful deployment of security is ongoing. It seems likely that any future extension required for protocol headers will be distinguished from the maximum data unit size transmitted by conformant end stations, in attempt to avoid any provision for header space being used top transmit more data, thus requiring additional provision for headers, and so on.>>>>

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.

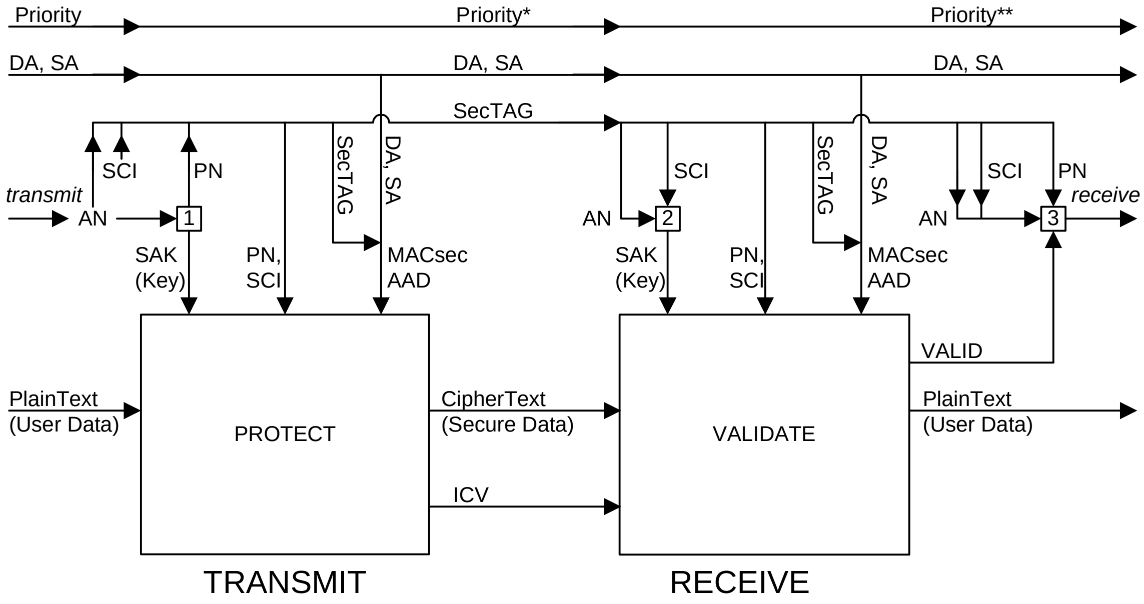
On transmission, the frame is first assigned to an SA (7.1.3), identified locally by its Association Number (AN, 7.1.3, 9.6). The AN is used to identify the SAK (7.1.3), and the next PN (3.28, 9.8) for that SA. The AN, the SCI (7.1.2), and the PN are encoded in the SecTAG (the SCI can be omitted for 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). Data, such as the Destination Address, the Source Address, and the SecTAG, that can be read in clear text but are integrity checked are called Additional Authenticated Data (AAD) (ref cl3).

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 Secure Data are returned.

If the receive frame is valid, replay protection (if enabled) is applied, by checking that the received PN is greater than the last PN received for a valid frame on the SA. If the check succeeds the parameters of the frame, unchanged from those transmitted, are presented to the MACsec client.



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

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 MAC Security Entity (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. clause specifies how the parameters encoded in the MPDU are generated, validated, and used. The normative specification of MACsec and SecY operation, including management, is specified in Clause 15.

8.4 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 ONU separate from the connectivity provided to other ONUs. An additional MAC instance provides a Single Copy Broadcast 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, 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 Single Copy Broadcast 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.

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, and the functionality provided by, each field
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) or the protocol state machines (Clause 15).

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.

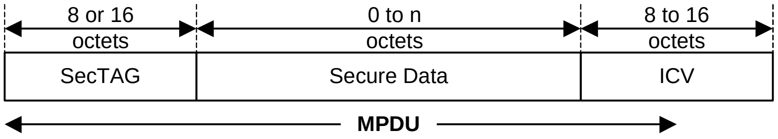


Figure 9-1—MPDU components

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) optional Secure Channel Identifier (SCI, 9.9).

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

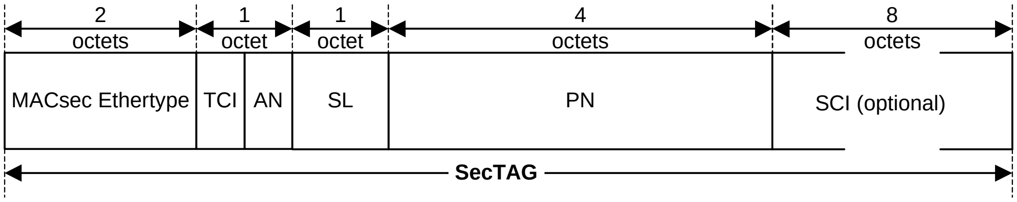


Figure 9-2—SecTAG format

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.

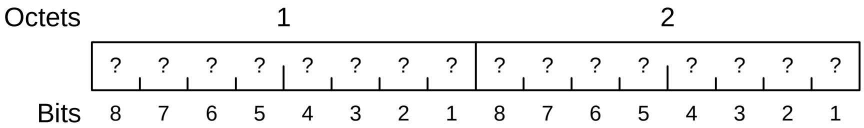


Figure 9-3—MACsec EtherType encoding

<<NOTE—The MACsec EtherType value will not be assigned until the completion 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 thru 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 explicit SCI (7.1.2, Figure 7-7)
d) use of the EPON (8.4) Single Copy Broadcast capability, without requiring an explicit SCI to distinguish the SCB Secure Channel
e) use of the Short Length field to determine the length of the Secure Data
f) 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.

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

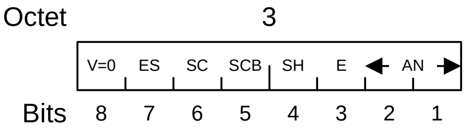


Figure 9-4—MACsec TCI and AN encoding

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 ES bit) of the TCI may be set. If ES bit is set, bit 6 (the SC bit) shall not be set and an SCI shall not be explicitly included in the SecTAG.

If an SCI (9.9, 7.1.2) is present in the SecTAG, bit 6 (the SC bit) of the TCI shall be set.

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 both the ES and the SCB bits are set, the Port Identifier (7.1.2) takes the reserved SCB value (8.4).

If the number of octets in the Secure Data field, i.e. the number of octets between the last octet of the SecTAG and the first octet of the ICV is less than 64, bit 4 (the SH bit) shall be set.

If and only if the Secure Data comprises 63 or fewer octets bit 4 (the SH bit) is set.

If and only if the number of octets and the value of each octet of the Secure Data are exactly the same as those of the User Data, and the ICV comprises the same number of octets as the Default Cipher Suite, bit 3 (the E bit) is clear, otherwise it is set.

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 thru 6 of octet 4 of the SecTAG, and is set to the number of octets in the Secure Data 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.

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) 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 should be a globally unique identifier for a SecY. To provide the IV uniqueness requirements of CTR mode, a fresh key should be 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) 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;
c) replay protection where multipoint connectivity is being provided.

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.

9.10 Secure Data

The Secure Data comprises all the octets that follow the MACsec TAG and precede the ICV.

NOTE 1—The minimum number of octets of Secure Data is set by the current Cipher Suite, and can vary by Cipher Suite. It can be zero. However if the MAC Service Data Unit composed by the operation of the current Cipher Suite following MPDU reception contains less than 2 octets it is highly to 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. The default Cipher Suite (GCM-AES) encrypts that MACsec's user's date into the same number of octets of Secure Data.

NOTE 2—Ethernet transport 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.

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 MPDU shall be processed on receipt as specified in Clauses 8 and 9, if and only if it comprises a valid Security TAG, zero or more octets of cryptographic component, and an Integrity Check Value, i.e.

a) it comprises at least 16 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) if the SC bit in the TCI is set, then the frame comprises at least 24 octets
f) if the SH bit in the TCI is clear, then the SL is zero
g) if the E bit is set the frame comprises at least 24 octets if the SC bit is clear, and at least 32 octets if the SC bit is set
h) bits 7 and 8 of octet 4 are clear.

Otherwise the received frame shall be discarded and the MACsecPDUFormatError count incremented.

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 (10.5 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 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).

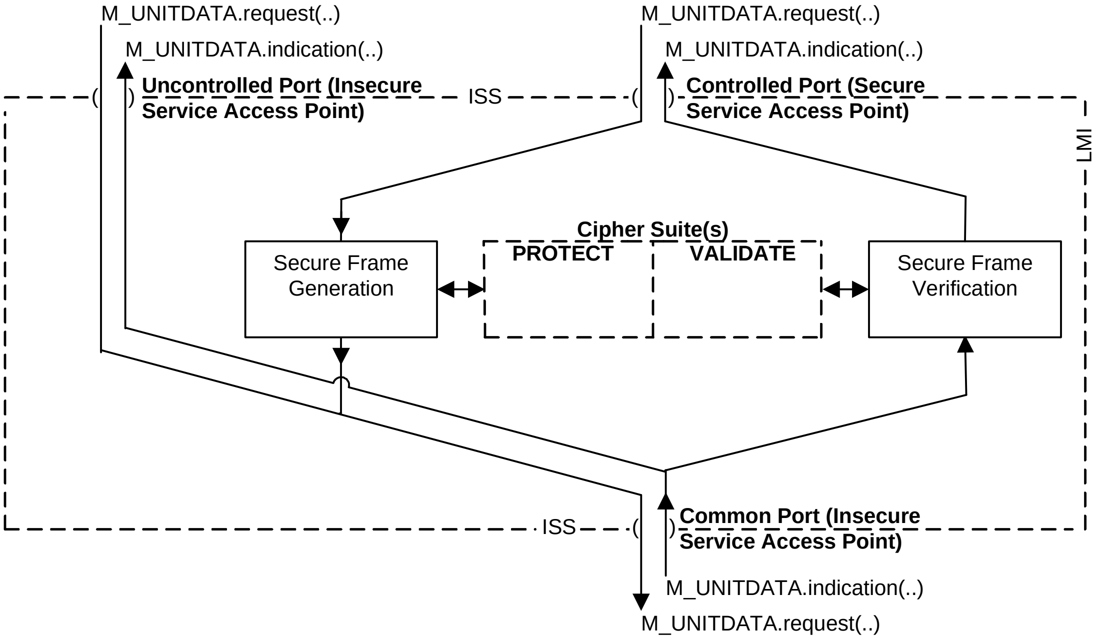

M_UNITDATA.request(..)
M_UNITDATA.indication(..)
Uncontrolled Port (Insecure Service Access Point)
ISS
M_UNITDATA.request(..)
M_UNITDATA.indication(..)
Controlled Port (Secure Service Access Point)
LMI
Cipher Suite(s)
PROTECT
VALIDATE
Secure Frame Generation
Secure Frame Verification
ISS
Common Port (Insecure Service Access Point)
M_UNITDATA.indication(..)
M_UNITDATA.request(..)

Figure 10-1—SecY

The integrity and origin (6.8) 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, 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 provider indications and the corresponding indications to the users of the Uncontrolled Port and the Controlled Port is not defined, save that the order of indications from any one Port to any one other Port is preserved. Similarly the relative order of user requests at the Uncontrolled Port and at the Controlled Port does not define the relative 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 10-2.

The specification of the cryptographic algorithms used at any time to provided 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 provides integrity, and a Cipher Suite that provides 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 users of the Uncontrolled Port and the Controlled Port can each be another entity within the MAC Sublayer or an instance of LLC that provides one or more LSAPs (Link Service Access Points), each to an application or higher layer protocol.

NOTE 1—Clause 11 specifies the incorporation of a SecY within a number of systems in more detail.

MACsec Key Agreement makes use of the service provided by the Uncontrolled Port, either directly or indirectly through an LLC Entity, as described in Clause 11. The frames transmitted and received by key agreement protocols are distinguished by EtherType, so that LLC Entity can also support other protocols. Direct use of the SecY's Uncontrolled port by a KaY that provides an Uncontrolled Port for the other protocols is illustrated in Figure 10-2.

NOTE 2—The term 'LLC', as used in this Standard, includes protocol identification by EtherType.

The KaY associated with a SecY can make direct use of the Controlled Port, and provide its own Controlled Port for use by other protocols as illustrated in Figure 10-2. This allows the KaY to 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 the Controlled Port used by other protocol entities.

Management controls are provided to allow the SecY to operate without modifications or additions to the MAC Service user data and thus without providing integrity, origin, or confidentiality protection. In this case the Controlled Port is controlled purely by the operation of MACsec Key Agreement (Figure 10-2); either all received frames give rise to service indications or none do.

NOTE 3—Operation of the SecY without cryptographic protection 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.

NOTE 4—The operation of MACsec Key Agreement together with a SecY that uses does not modify or add to the MAC Service user data provides the same functionality as IEEE Std 802.1X, and is similarly described.

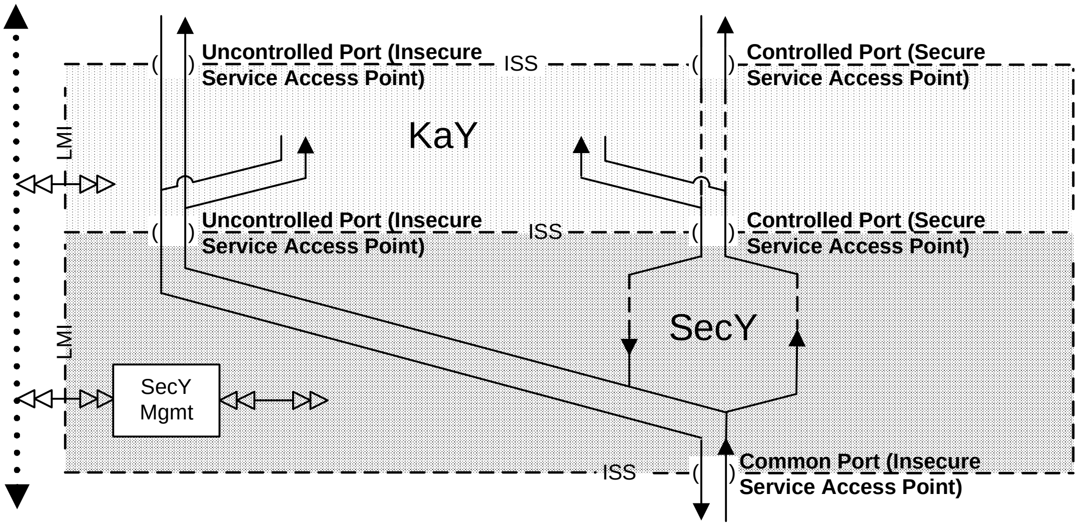

Uncontrolled Port (Insecure Service Access Point)
ISS
Controlled Port (Secure Service Access Point)
KaY
LMI
Uncontrolled Port (Insecure Service Access Point)
ISS
Controlled Port (Secure Service Access Point)
SecY
LMI
SecY Mgmt
ISS
Common Port (Insecure Service Access Point)

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

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

NOTE 5— The term 'local' used in discussion of a protocol entity refers to any other entity residing within the same system. Exchange of information 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 that are 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 including

f) Transmission and reception by the user of the Controlled Port without using MACsec.
g) Reception without integrity checking.

use of MACsec over LANs that misorder frames with different transmission priority and or addresses

h) Reception without replay protection.

CA establishment, Cipher Suite selection, and SA support 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, providing

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 on shared media, 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 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 (10.5).
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 Secure Frame Selector, Transmit Multiplexer, and a Receive Demultiplexer.
f) Optional transmit and receive FCS Regenerators.
g) A SecY Management process (10.7).

A Layer Management Interface (LMI) is used by the SecY Management process to communicate the capabilities of the SecY, its status, its protocol and management events and counters to other Entities, including a KaY, that compose the secure system of which the SecY forms a part. The LMI also receives parameters from those Entities.

The Secure Frame Selector allows a SecY to be incorporated into a system before MACsec is deployed in the network of which the system forms a part. If the ControlledReceivesAll management control is set, the Secure Frame Selector submits all transmits requests from the Controlled Port directly to the Transmit Multiplexer, and all receive indications from the Receive Demultiplexer directly to the Controlled Port without adding a SecTAG or and ICV, or modifying, protecting, or validating the User Data.

The Transmit Multiplexer accepts transmit requests from the Uncontrolled Port, from the Secure Frame Selector, and from 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. In addition each receive indication is also submitted directly to the Secure Frame Selector if the ControlledReceivesAll management control is set, and is submitted to the Secure Frame Verification process otherwise.

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 ControlledReceivesAll is False and none of the users of the LLC Entity supported by the Uncontrolled Port make use of the MACsec Ethertype.

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—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.

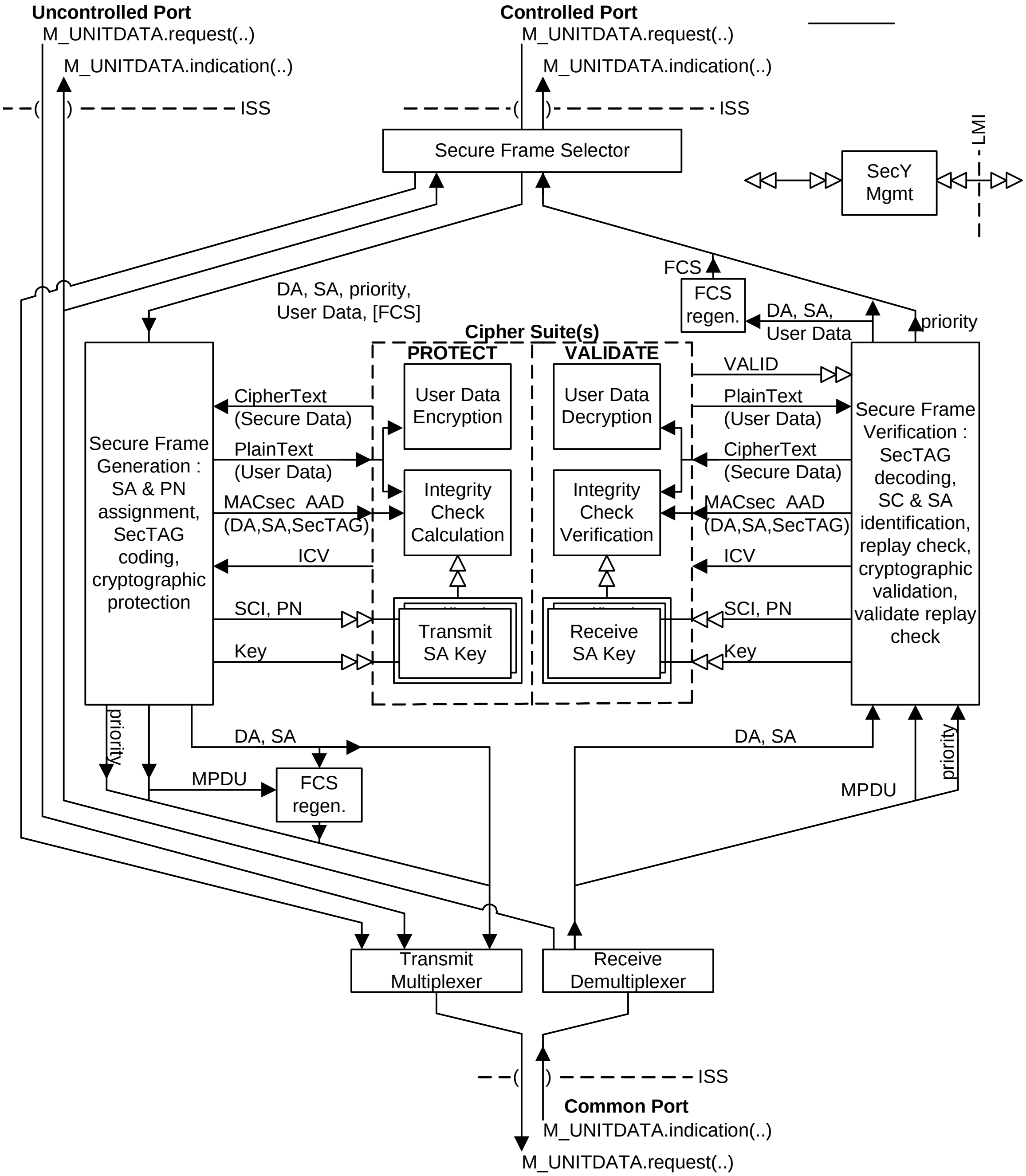


Figure 10-3—SecY architecture and operation

10.5 Secure Frame Generation

For each transmit request from the Secure Frame Selector, 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, 10.5.3) 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) MACsec AAD (10.5.4)
   5) PlainText, the sequence of octets that compose the User Data
e) receives the following parameters from the Cipher Suite protection operation
   6) CipherText, the sequence of octets that compose the Secure Data
   7) the ICV
f) issues a request to the Transmit Multiplexer with the DA, SA, and priority of the frame as received from the Secure Frame Selector, and an MPDU comprising the octets of the SecTAG, Secure Data, and the ICV concatenated in that order (10.5.2).

Management controls are provided to allow some of the above checks to be skipped.

NOTE—This model of operation and the state machines (Clause 14) 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. The order of responses is assumed to remain the same, since the protection and validation operations do not misorder frames.

10.5.1 Transmit SA assignment

Each SA is identified by its Association Number (AN). The KaY assigns each frame to SA identified by the current value of the encodingSA variable. This state machine variable is updated by the SecY management process after the key corresponding to the SA has been installed, i.e. the Cipher Suite implementation has completed any preliminary calculations required for it to use the SA Key immediately after the last frame assigned to the previous SA has been protected. The value of encodingSA can be read but not written by network management.

10.5.2 Transmit PN assignment

The PN value associated with the frame is assigned the value of the nextPN variable for the SA. If nextPN is zero (or 2^{32}), the frame is discarded and the management variable DiscardTransmitPNExhausted is incremented. Otherwise the value of nextPN is incremented. nextPN is set to 1 by the SecY management process after the SA Key has been received via the LMI and before the first use of that key in a protect operation. The value of nextPN can be read, but not written, by network management. The value reported is synchronized with the reported value of encodingSA.

10.5.3 SecTAG encoding

The SecTAG is encoded as specified in Clause 9.

The SL parameter is set to the number of octets of Secure Data plus the number of octets of the ICV that will be returned by the Current Cipher Suite, if that would cause the short indication (SH) to be set.

If the Current Cipher Suite provides integrity, but not confidentiality, and the number of octets of the CipherText will be exactly the same as those of the PlainText, and the ICV will be 16 octets long, then the E bit shall be clear. Otherwise the E bit shall be set.

If the IncludeSCI variable has the value MultipointOnly and connectivity provide by the CA is point-to-point, i.e. the number of receive SCs in the CA is 1 and ValidateReceivedFrames is set, the SCI is not included in the SecTAG, otherwise the SCI is included.

The value of the IncludeSCI variable can be written and read by network management. The number of receive SCs in the CA is controlled by the KaY, but can be read from the SecY by network management. The ValidateReceivedFrames control can be written and can read by network 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 encipheringSA is updated and the protection of the frame parameters started within a minimum frame size transmission delay after the last frame has been protected using the previous key.

The MACsec AAD (Additional Authenticated Data) provided to the Current Cipher Suite consists of a sequence of octets comprising the six octets of the Destination MAC Address, in canonical format order, followed by the six octets of the Source MAC Address, followed by the octets of the SecTAG in their transmission sequence, followed by 4 octets of PN and optionally 8 octets of SCI.

NOTE—MACsec AAD is not transmitted.

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, then the frame is discarded and the counter DiscardProtectedFrameTooLong is incremented. Details of the discarded frame, similar to those specified in 802.1D’s “Discard On Error Details” structure may be recorded to assist network management resolution of the problem. The DiscardProtectedFrameTooLong counter can be read but not written by network management.

Otherwise the parameters of the service request are submitted to the Transmit Multiplexer.

10.6 Secure Frame Verification

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

a) validates the MPDU as specified in clause 9.12
b) extracts and decodes the SecTAG as specified in clauses 9.3 through 9.9
c) extracts the User Data and ICV as specified in clauses 9.10 and 9.11
d) assigns the frame to an SA (10.6.1)
e) performs a preliminary replay check against the last validated PN for the SA (10.6.2)
f) 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 MACsec AAD (10.5.4)
    5) CipherText, the sequence of octets that compose the Secure Data
    6) the ICV

g) 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) PlainText, the sequence of octets that compose the User Data
h) updates the replay check (10.6.4)
i) issues an indication to the Secure Frame Selector with the DA, SA, and priority of the frame as received from the Receive Demultiplexer, and the User Data provided by the verification operation.

Management controls are provided to allow some of the above checks to be skipped.

10.6.1 Receive SA assignment

An SCI is first associated with the received frame. If the SCI was explicitly encoded in the SecTAG then that value is used. Otherwise, and if and only if the CA is point-to-point and the KaY has established a value of the SCI for the peer SecY, that value is associated with the frame.

If an SCI is not assigned the management counter UnknownSCI is incremented, and the frame is discarded if the management control ValidateReceivedFrames is set or the E bit in the TCI is set.

If an SCI has been assigned it is used to locate the associated receive SC, if this is not found the management counter UnknownSC is incremented and the frame is discarded if either ValidateReceivedFrames or the E bit are set. A record of the SCI may be kept to assist network management resolution of the presumed problem.

If the receive SC has been identified, then the receive SAI is composed of the SCI extended by the AN, and used to locate the receive SA. If the SA is marked NotInUse, the management counter UnknownSA is incremented and the frame is discarded if either ValidateReceivedFrames or the E bit are set. A record of the SAI may be kept to assist network management resolution of the presumed problem.

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 the receive SA been identified and ReplayProtect is set, and if the PN of the received frame is less than or equal to the lastValidatedPN for the SA, then the ReplayViolations count for that SA is incremented, and the frame discarded if ValidateReceivedFrames is set.

10.6.3 Cryptographic validation

If the validation function provided by the Current Cipher Suite does not return VALID, the management counter InvalidReceivedFrames is incremented, and the frame discarded if either ValidateReceivedFrames or the E bit are set.

10.6.4 Replay check update

If ValidateReceivedFrames and ReplayProtect are both set and the PN of the received frame is less than or equal to the lastValidatedPN for the SA, then the ReplayViolations count for that SA is incremented and the frame discarded. If the validation function returned VALID and the PN is greater than lastValidatedPN, lastValidatedPN is set to the value of the received PN.

If a Bridge in the CA is using priority queueing to support priorities, then the necessary re-ordering of frames will obviate replay protection. Therefore, it is recommended to have only one of either replay protection or priorities active at a time. This situation is likely to arise if MACsec frames are tunneled through a Provider Bridge and multiple classes of service are in use.

10.7 SecY Management

The SecY management process controls, monitors, and reports on the operation of the SecY. It ensures that the MAC Status (6.4) and point-to-point parameters (6.5) for the Uncontrolled and Controlled Ports, reflect the connectivity (6.7) provided, and uses the LMI to provide network management access to operational parameters to network management and an interface with the KaY.

The management process maintains and uses information for

a) the SecY as a whole
b) the CA
c) each SC in the CA
d) each of the SAs that support an SC

<<Some or all of this should migrate to the management section. What belongs here is any description of active interaction with the SecY, including the details of setting the MAC status parameters.>>

<<Diagram of containment structure, or implied containment structure (database join) and variables that identify it.>>

NOTE—While the KaY can operate discovery and key management and exchange protocols to change the CA membership while SecY is providing the secure MAC Service, the temporary states that can result are not shared between the KaY and the SecY.

10.7.1 SecY parameters

List of Cipher Suites—identified by reference number
Current Cipher Suite —selected by SecY
If the Current Cipher Suite is changed, the Controlled Port will go down.

10.7.2 Cipher Suite parameters

Cipher suite identifier
Confidentiality provided?
Secure Data Length == User Data Length?
ICV length

The KaY is responsible for selecting the current Cipher Suite, and communicating that choice to the SecY via the LMI. If the Current Cipher Suite becomes inoperable for any SC and for any reason, the SecY shall cease transmission and reception to and from the Controlled Port and set MAC_Operational (<ref>) False for that Port.

NOTE —Two communicating SecYs can implement a number of Cipher Suites in common. Specification of the process of selection from amongst the selectable Cipher Suites provided by a SecY is outside the scope of this standard, and is modeled occurring through the operation of a KaY. A user of services provided through the Controlled Port can retrieve parameters from the KaY to characterize both the Current Cipher Suite and the authorized capabilities of the users of the peer SecY(s). Selection of an inferior Cipher Suite can therefore result in restrictions in communication being imposed by that user.

10.7.3 CA parameters

Transmit SC—identified by SCI
List of Receive SCs—each identified by SCI

10.7.4 Transmit SC

SCI
encodingSA
enciphering SA

10.7.5 Receive SC

SCI
Transmit or Receive
SAs (set of 4)
statistics (since SAs may be too temporary to hold stats)

10.7.6 Transmit SA

SCI
AN
InUse?
SAK
nextPN

10.7.7 Receive SA

SCI
AN
In use?
SAK
lastValidatedPN

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 (<ref clause 6>). 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 Performance parameter management

Table 10-1 specifies default values and ranges for timer and transmission rate limiting performance parameters. Defaults are specified to avoid the need to set values prior to operation in most cases, and have been chosen for their wide applicability to maximize ease of operation. Ranges are specified to ensure that the protocol operates correctly, and provide guidance to implementors.

Table 10-1—SecY performance parameters

Parameter	Recommended or Default value	Permitted Range	Compatibility Range

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

10.11 SecY performance requirements

This clause (10.11) places requirements on the performance of the SecYs to ensure that MACsec operates correctly.

Table 10-2—SecY performance requirements

Parameter	Permitted values
SecY transmit delay	< Wire transmit time for MPDU + 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	
SecY receive delay variance	
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.

10.A. MACsec and EPON-will go after cl 10

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 ONU separate from the connectivity provided to other ONUs. An additional MAC instance provides a Single Copy Broadcast 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, 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 Single Copy Broadcast 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.

11. MAC Security in Systems

This clause (11) specifies how MAC Security is incorporated within the architecture of

a) end stations (11.1)

b) systems that incorporate Link Aggregation (IEEE Std 802.3 Clause 43) (11.2)

c) MAC Bridges (IEEE Std 802.1D) (11.4)

d) VLAN-aware MAC Bridges (IEEE Std 802.1Q) (11.1)

e) Provider Bridges (P802.1ad) (11.1).

The figures in this clause illustrate the relative position of major architectural components within each of these systems, without and with the incorporation of MAC Security Entities (SecYs). The latter figures show both the secure MAC Service provide by each SecY's Controlled Port, and the insecure service provided by the Uncontrolled Port for use by each MACsec Key Agreement Entity.

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

11.1 MACsec in end stations

Figure 11-1 provides two views of the architecture in a end station that uses a generic LAN media access controlled method, referred to in this and following figures as 802.X.

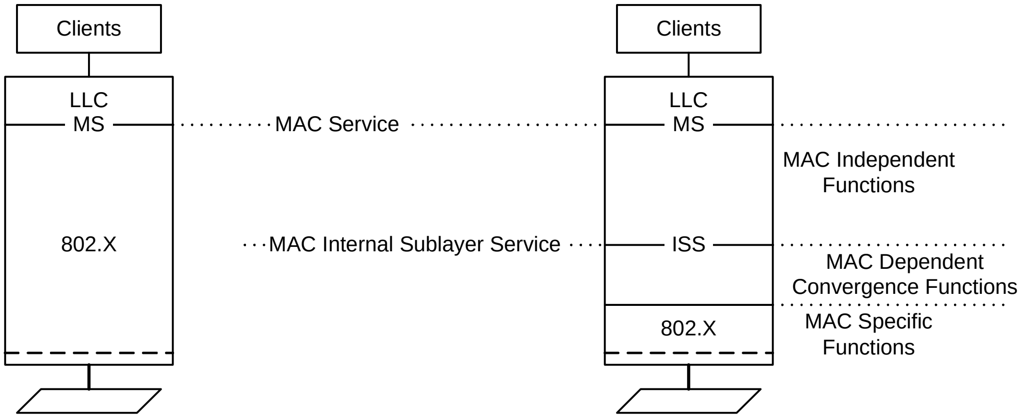

Clients
LLC
MS
802.X
MAC Service
MAC Internal Sublayer Service
Clients
LLC
MS
ISS
802.X
MAC Independent Functions
MAC Dependent Convergence Functions
MAC Specific Functions

Figure 11-1—Two views of the MAC sublayer in an end station

On the left, 802.X is shown as supporting the insecure MAC Service directly. On the right, the media access method specific functions of 802.X provide an interface to media access method dependent convergence functions, which in turn provide an insecure instance of the MAC Internal Sublayer Service (ISS). Media access method independent functions use the ISS to provide the MAC Service to LLC and its clients. If the media access method independent functions are trivial and provide only a straight forward mapping between the parameters of the MAC Service and ISS service access points, the externally observed behavior of the end station is the same for both the left and right hand views.

NOTE—IEEE Std 802.1D Clause 6.5 specifies the ISS together with media access dependent mappings for a number of 802 LAN technologies.

Figure 11-2 incorporates a SecY into the architecture depicted by the right hand view in Figure 11-1. For simplicity the distinction between the ISS and the MAC Service is omitted from this following figures, which simply show insecure (IS) and secure (SS) service access points.

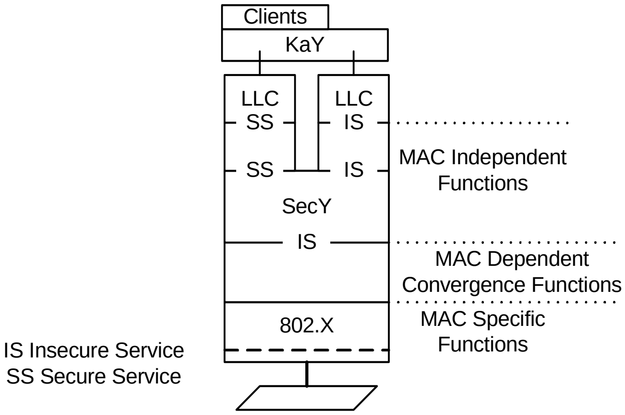


Figure 11-2—An end station with MAC security

11.2 MACsec and Link Aggregation

The left hand side of Figure 11-3 depicts an end station using Link Aggregation, as specified in IEEE Std 802.3 Clause 43. The service provided by two separate point to point LANs is combined by the link aggregation sublayer to provide a single service interface to LLC and its clients. To provide MAC Security for such a system, two independent SecYs operate below the Link Aggregation sublayer, as shown on the right hand side of the figure. If the two links are being aggregated dynamically as provided by the Link Aggregation Control Protocol (LACP), the operation of LACP will be protected by the secure MAC Service. 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 be informed and can change the aggregation keys.

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

The insecure service access points for each of the SecYs are independently provided to the KaY associated with each SecY, and are not candidates for aggregation.

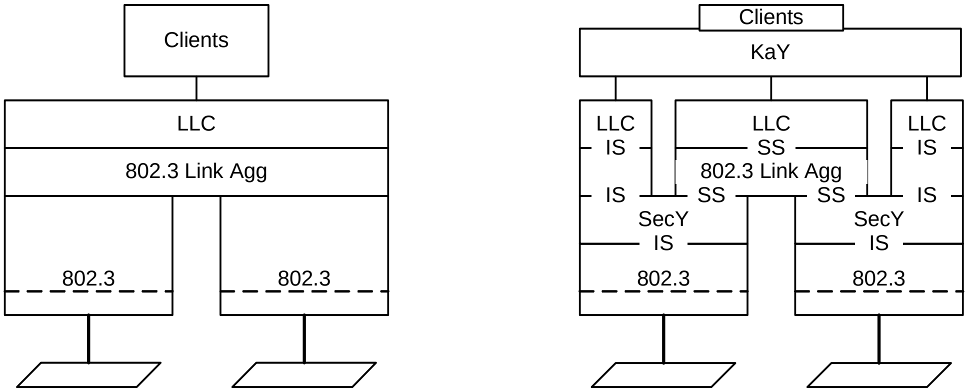


Figure 11-3—MACsec and Link Aggregation in a station

11.3 MACsec and LLDP

Figure 11-4 shows a diagram of LLDP (ref) with MACsec.

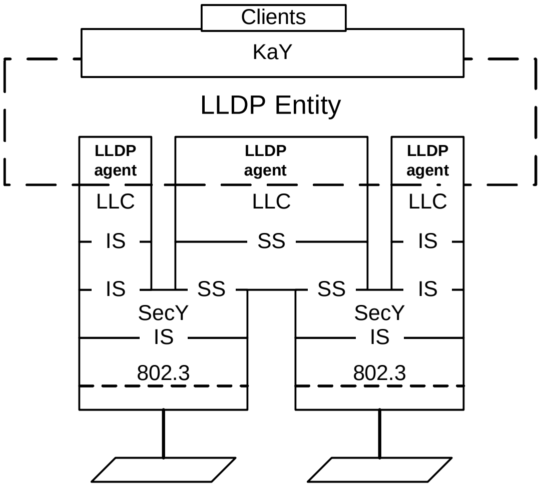


Figure 11-4—MACsec and LLDP

11.4 MACsec in MAC Bridges

The left hand side of Figure 11-5 depicts a MAC Bridge, as specified in IEEE Std 802.1D. The MAC Relay Entity forwards frames between service access points presented by the instances of the ISS that are 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 a SecY, which in turn supports the functions described in clauses 7.5 and 7.6 of IEEE Std 802.1D, as shown on the right hand side of the figure.

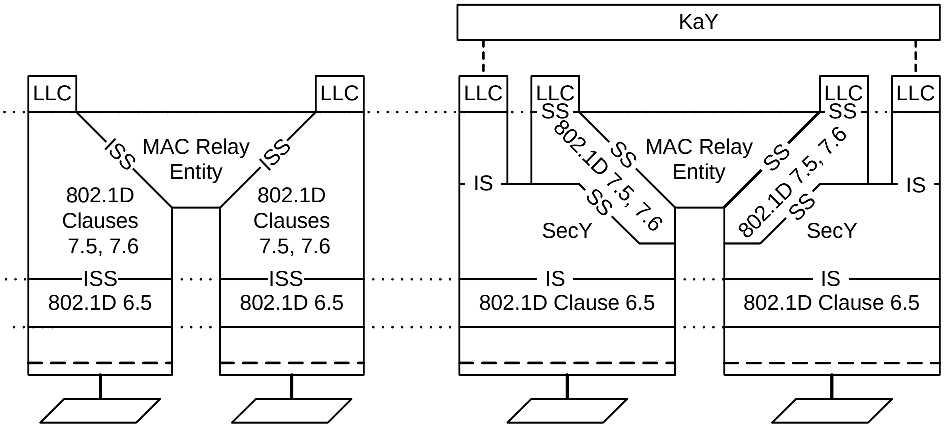


Figure 11-5—MACsec in an 802.1D MAC Bridge

NOTE—If the MAC Bridge can aggregate multiple LANs to support a single Bridge Port, each individual LAN provides the insecure MAC Service to its own SecY, which then provides the secure MAC Service to the Link Aggregation sublayer, as specified above (11.2). Each aggregated port then provides secure service to 802.1D 7.5 and 7.6.

Figure 11-6 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.

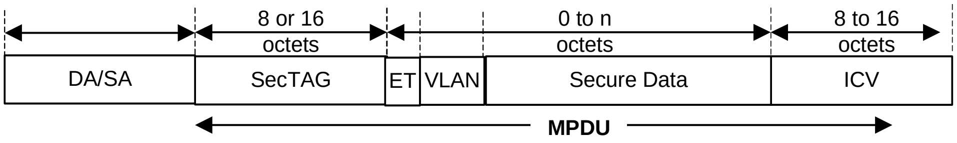


Figure 11-6—Frame Format showing VLAN Tag

11.5 MACsec in VLAN-aware Bridges

Figure 11-8 illustrates the incorporation of MAC Security in a VLAN-aware MAC Bridge.

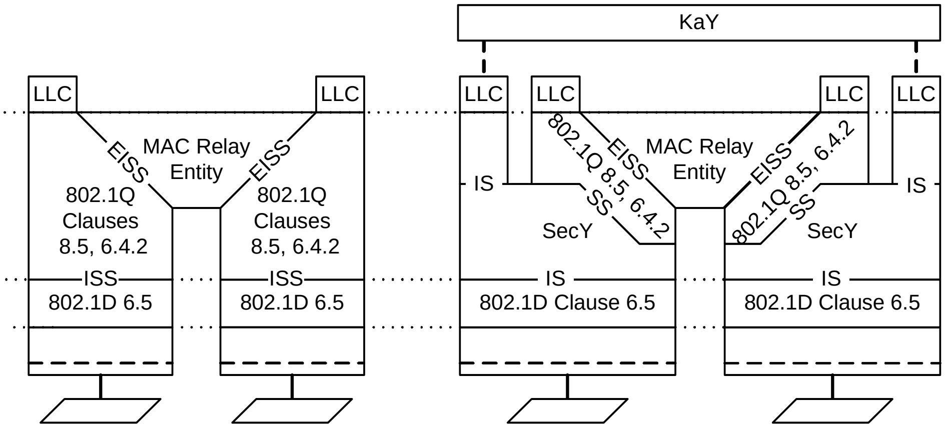


Figure 11-8—Addition of MAC Security to a VLAN-aware MAC Bridge

11.6 MACsec in Provider Bridges

Figure <tbs> illustrates the incorporation MAC Security in Provider Bridges and Provider Edge Bridged.

12. Management of MAC Security Entities

This clause defines the set of managed objects, and their functionality, that allow administrative configuration and monitoring of MAC Security Entities.

<<management referring to security protection, response, reaction. here's how we tell someone is doing a DoS attack. rapidly fluctuating numbers. Replay. think of clause 9 first. improving stuff in model. so there are specific places for counting things. get a feel for all counts. before state machine. what counters are good for. bottoms up. detection of replay attacks. cl 11. the management stuff. space to develop tops down view of what watching out for and trying to prevent.>>

This clause

a) Introduces the functions of management to assist in the identification of the requirements placed on MAC Security Entities for the support of management facilities
b) Establishes the correspondence between the state machines used to model the operation of a SecY and its managed objects
c) Specifies the management operations supported by each managed object

12.1 Management functions

Management functions relate to the users' needs for facilities that support the planning, organization, supervision, control, protection, and security of communications resources, and account for their use. These facilities may be categorized as supporting the functional areas of Configuration, Fault, Performance, Security, and Accounting Management. Each of these is summarized in 12.1.1 through 12.1.5, together with the facilities commonly required for the management of communication resources, and the particular facilities provided in that functional area by SecY Management.

12.1.1 Configuration Management

Configuration Management provides for the identification of communications resources, initialization, reset and close-down, the supply of operational parameters, and the establishment and discovery of the relationship between resources. The facilities provided by SecY Management in this functional area are as follows:

a) Configuration of the operational parameters for the SECy (12.4.1.1 and 12.4.1.2)
b) Initialization of the state machines for the SECy ()

12.1.2 Fault Management

Fault Management provides for fault prevention, detection, diagnosis, and correction. The facilities provided by SecY Management in this functional area are as follows:

a) Retrieval of SECy statistical information ()
b) Configuration of the operational parameters for the SECy (12.4.1.1 and 12.4.1.2)

12.1.3 Performance Management

Performance Management provides for evaluation of the behavior of communications resources and of the effectiveness of communication activities. The facilities provided by SecY Management in this functional area are

a) Retrieval of statistical information ()
b) Configuration of the operational parameters (12.4.1.1 and 12.4.1.2)

12.1.4 Security Management

Security Management provides for the protection of resources. The facilities provided by SecY Management in this functional area are as follows:

a) ???

12.1.5 Accounting Management

Accounting Management provides for the identification and distribution of costs and the setting of charges. The facilities provided by SecY Management in this functional area is as follows:

a) Retrieval of accounting statistics (12.4.1.3)

12.2 Managed objects

Managed objects model the semantics of management operations. Operations upon a managed object supply information concerning, or facilitate control over, the Process or Entity associated with that managed object.

Management of SecY is described in terms of the managed resources that are associated with individual Ports that support MAC Security. The managed resources of a SecY are those of the Processes and Entities established in... Specifically,

a) first sort of resource....................
b) ....

The management of these resources is described in terms of managed objects and operations defined below.

NOTE—The values specified in this clause, as inputs and outputs of management operations, are abstract information elements. Questions of format or encoding are a matter for particular protocols that convey or otherwise represent this information.

12.3 Data types

This sub clause specifies the semantics of operations independent of their encoding in management protocol. The data types of the parameters of operations are defined only as required for that specification.

The following data types are used:

a) Boolean
b) Enumerated, for a collection of named values
c) Unsigned, for all parameters specified as “the number of” some quantity
d) MAC Address
e) Time Interval, an Unsigned value representing a positive integral number of 10 milliseconds, for all protocol time-out parameters
f) Counter, for all parameters specified as a “count” of some quantity (a counter increments and wraps with a modulus of 2 to the power of 64)

12.4 SecY first sort of resource managed objects

The..........are described in........

The objects that comprise this managed resource are as follows:

a) ....
b) ...

A SecY that supports.......... functionality shall support the management functionality defined by the... managed object. A SecY that supports.......... functionality may support the management functionality defined by the............. managed objects.

The means by which this management functionality is provided (e.g., the management protocol supported) shall be stated in the PICS associated with the implementation.

12.4.1 first resource first object

The.... managed object models the operations that modify, or enquire about, the configuration of the SecY's resources. There is a single SecY Configuration managed object for each SecY.

The management operations that can be performed on the.... managed object are

a) Read.. Configuration (12.4.1.1)
b) Set.. Configuration (12.4.1.2)
c) ...(12.4.1.3)

12.4.1.1 Read... Configuration

12.4.1.1.1 Purpose

To solicit configuration information regarding the configuration of the SecY.

12.4.1.1.2 Inputs

— **Identifier....**

12.4.1.1.3 Outputs

a) **Identifier...** The identification number assigned to the SecY**...**.
b) **...........**

12.4.1.2 Set... Configuration

12.4.1.2.1 Purpose

To configure the parameters that control the operation of the SecY.

12.4.1.2.2 Inputs

Any parameters marked as (optional) may be omitted from the operation to allow selective modification of a subset of the configuration parameters. However, implementations shall support the ability to include all of the parameters identified below.

a) **....**
b)
c)

12.4.1.2.3 Outputs

None.

12.4.1.3 .....

12.4.1.3.1 Purpose

...

12.4.1.3.2 Inputs

a) **...**

12.4.1.3.3 Outputs

None.

12.4.1.3.4 Effect

This operation...

13. Management protocol

13.1 Introduction

This clause defines a portion of the Management Information Base (MIB) for use with network management protocols in TCP/IP-based internets. In particular, it defines objects for managing the operation of MAC Security, based on the specification contained in Clause 10 and Clause 1. This clause includes a MIB module that is SNMPv3 SMI compliant.

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 RFC 3410 [RFC3410].

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 STD 58, RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] and STD 58, RFC 2580 [RFC2580].

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 RFC1213).

<<get from mick>>

13.3.2 Relationship to the Interfaces MIB

It is assumed that a system implementing this MIB will also implement the “interfaces” group defined defined in IETF RFC 2863.

It is assumed that a system implementing this MIB will also implement the “system” group defined in IETF RFC3418 (or at least that subset of the system group defined in IETF RFC1213), and the “interfaces” group defined in IETF RFC 2863.

IETF RFC 2863, the Interface MIB Evolution, requires that any MIB that is an adjunct of the Interface MIB clarify specific areas within the Interface MIB. These areas were intentionally left vague in IETF RFC 2863 to avoid over constraining the MIB, thereby precluding management of certain media types.

Section 3.3 of IETF RFC 2863 enumerates several areas that a media-specific MIB must clarify. Each of these areas is addressed in a following subsection. The implementor is referred to IETF RFC 2863 in order to understand the general intent of these areas.

In IETF RFC 2863, the “interfaces” group is defined as being mandatory for all systems and contains information on an entity’s interfaces, where each interface is thought of as being attached to a *subnetwork*. (Note that this term is not to be confused with *subnet*, which refers to an addressing partitioning scheme used in the Internet suite of protocols.) The term *segment* is sometimes used to refer to such a subnetwork.

13.3.3 Relationships to Bridge MIB and IEEE Std 802.1X MIB

<<tbd>>

13.4 Security considerations

<<Use Security Guidelines for IETF MIB Modules at http://www.ops.ietf.org/mib-security.html. To be done when MIB is written.>>

13.5 Relationship to the managed objects defined in Clause 12

Table 13-1 contains cross-references between the objects defined in Clause 12 and the MIB objects defined in this clause.

Table 13-1—Managed object cross-reference table

Definition in Clause 11	MIB object(s)
12.4.1first resource, first object	**dot1aeMACsecY**
....	
....	
....	
....	
Initialize SecY	
Statistics	**dot1aeStatsTable**

Table 13-1—Managed object cross-reference table ***(continued)***

Definition in Clause 11	MIB object(s)
Diagnostics	**dot1aeDiagTable**

13.6 Structure of the MIB

A single MIB module is defined in this clause. Objects in the MIB are arranged into groups. Each group is organized as a set of related objects. The overall structure and assignment of objects to their groups is shown in the following sub clauses.

13.6.1 The...........Group

This group of objects provides management functionality that is not specific to the operation of......

13.6.2 The... Group

This group of objects provides......

13.7 Definitions for MAC Security MIB

In the MIB definition below, should any discrepancy between the DESCRIPTION text and the corresponding definition in Clause 12 occur, the definition in Clause 12 shall take precedence.

```
IEEE8021-SECY-MIB DEFINITIONS ::= BEGIN


-- ---------------------------------------------------------- --
-- IEEE 802.1AE MIB
-- ---------------------------------------------------------- --
```

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 1—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.

NOTE 2—The criteria adopted during the development of this standard for Cipher Suite selection, leading to the inclusion of GCM-AES and GMAC-AES as the mandatory and only Cipher Suites specified for full conformance, are recorded in Annex V. Annex V also makes recommendations concerning the use of additional Cipher Suites.

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.

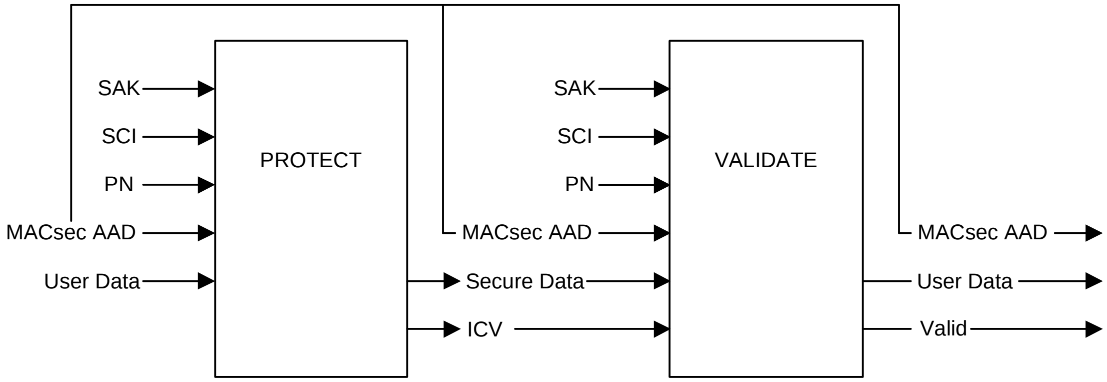


Figure 14-1—Cipher Suite Protect and Validate operations

```
Protect (  SAK,                          Validate(  SAK,
           SCI,                                     SCI,
           PN,                                      PN,
           MACsec AAD,                              MACsec AAD,
           User Data                                Secure Data, ICV
         )                                        )
         Secure Data, ICV                          User Data, Valid
```

The SAK (Secure Association Key, 3.35, 7.1) is the value of the Cipher Suite dependent key(s).

The SCI (Secure Channel Identifier, 3.35, 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, 3.28, 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 MACsec AAD (Additional Authenticated Data, 3.2) is a string of 20, or 28 octets. If the string is 20 octets long the last four octets encode the PN. If the string is 28 octets long, the last 8 octets encode the SCI, and the prior 4 octets encode the PN.

NOTE 1—The PN and SCI must be in Clear Text and therefore not encrypted. There are two general strategies for protecting the PN and the SCI. The first is to use the PN and the SCI as part of an IV (Initialization Vector); thus they will be integrity checked, whether or not they are included in the AAD. The second method is to include the PN and the SCI in the MACsec AAD so that it is the integrity protected. This latter strategy is appropriate if the SCI and PN cannot form part of the IV, as is the case if the Cipher Suite mandates a random IV. In MACsec, the PN is included in the AAD, and the SCI is optionally in the AAD.

Optional SCI in AAD--?

The PlainText is a string of octets.

The CipherText is a string of octets. If the Cipher Suite is providing confidentiality it is hard (in the cryptographic sense) for someone who learns the CipherText to recover the PlainText without the SAK.

The ICV (Integrity Check Value, 3.14, 8.3) is a string of octets.

Valid is a boolean parameter. If TRUE the validation was successful.

Given the SAK, SCI, PN, MACsec AAD, and PlainText, the Protect returns the CipherText and ICV.

Given the same SAK, SCI, PN, MACsec AAD, CipherText, and ICV, the Verify operation returns the original PlainText and Valid True. If any of the parameters to were modified, Valid is returned False.

14.2 Cipher Suite Capabilities

Any Cipher Suite used with MACsec shall

a) provide integrity protection for the PN, the first 16 octets of the MACsec AAD, and from 0 thru 2^{16}-1 octets of PlainText on each invocation

NOTE—Recall that the AAD includes the SecTAG.

b) provide integrity protection for the SCI if the latter is included in the MACsec AAD
c) provide integrity and confidentiality (if specified) for up to 2^{32}-1 invocations, each with a different PN, without requiring a fresh SAK.
d) given any specific number of octets of PlainText, generate a predictable number of octets of CipherText and ICV

and may

e) provide confidentiality protection for the PlainText
f) provided integrity protection for the SCI, even if the latter is not included in the MACsec AAD

and shall not

g) generate a CipherText that when added to the number of octets in the ICV contains more than <896> octets more than the PlainText.

NOTE 1—<<explain how the above figure was arrived at>>.

NOTE 2—A Cipher Suite may introduce additional fields into the Cipher Text even if confidentiality is not provided.

h) modify or constrain the values of the SCI, PN, or MACsec AAD other than as specified by this Standard
i) require an SAK exceeding 1024 bits long (in total for all keys that compose the SAK)
j) require different keys for the protect and validate operations

A implementation of MACsec for which conformance to this Standard is claimed shall include at least one Cipher Suite that provides integrity and not confidentiality, with the CipherText the same as the PlainText, 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) <<adequacy of reference material>>

and shall state

c) whether confidentiality of the PlainText is provided
d) the maximum difference in the lengths of the PlainText and CipherText
e) the length of the ICV
f) the length and properties of the keys required, including assumptions of the scope of uniqueness

NOTE—While a further clauses of this Standard provides definitive specifications of the Cipher Suites that support full conformance, that specification makes the greatest possible use of other public and established standards, and is 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 is required to be able to operate at least one cryptographic Cipher Suite that does not encrypt User Data.

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.

Table 14-1—MACsec Cipher Suites

Cipher Suite #	Name	Type	Services provided		Mandatory/ Optional	Defining Clause
			Integrity	Confidentiality		
1	Default Cipher Suite	GMAC	Yes	No	Mandatory	14.5
2	Default Confidentiality Cipher Suite	GCM	Yes	Yes	Mandatory	14.6

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 8-1, 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 have been adopted by the NIST modes process <ref>, and shall not implement any other Cipher Suite, or other combination of cryptographic algorithms and parameters.

14.5 Default Cipher Suite (GMAC-AES-128)

<<To be specified by reference to the GCM spec submitted to the NIST modes process [1]

AES-128 is used as the underlying block cipher

[1] Section 2.1	K	= SAK
[1] Section 2.1	IV	= SCI || PN
[1] Section 2.1	A	= MACsec AAD (first 16 octets only) || User Data
[1] Section 2.1	P	= <null>
[1] Section 2.1	C	= Secure Data
[1] Section 2.1	T	= ICV

T is 128 bits long

>>

14.6 Default Confidentiality Cipher Suite (GCM-AES-128)

<<To be specified by reference to the GCM spec submitted to the NIST modes process [1]

AES-128 is used as the underlying block cipher

[1] Section 2.1	K	= SAK
[1] Section 2.1	IV	= SCI || PN
[1] Section 2.1	A	= MACsec AAD (first 16 octets only)
[1] Section 2.1	P	= User Data
[1] Section 2.1	C	= Secure Data
[1] Section 2.1	T	= ICV

T is 128 bits long

>>

15. MACsec state machines

This clause provides the normative specification of the behavior of a MAC Security Entity (SecY) in terms of protocol state machines, procedures and parameters, including the specification of the relationship of management controls and counters to both expected behavior and protocol errors.

The behavior of a SecY implementation is specified by a number of cooperating state machines. Figure 15-1 is not itself a state machine, but illustrates the machines, their interrelationships, the principal variables used to communicate between them, their local variables, and performance parameters.

<<Need state machine showing what happens when out of synch, missing frame, part of PN doesn't appear in packet, management events, rate limiting management events, key failure>>

15.1 Notational conventions used in state diagrams

State diagrams are used to represent the operation of the protocol by a number of cooperating state machines each comprising a group of connected, mutually exclusive states. Only one state of each machine can be active at any given time.

Each state is represented in the state diagram as a rectangular box, divided into two parts by a horizontal line. The upper part contains the state identifier, written in upper case letters. The lower part contains any procedures that are executed on entry to the state.

All permissible transitions between states are represented by arrows, the arrowhead denoting the direction of the possible transition. Labels attached to arrows denote the condition(s) that must be met in order for the transition to take place. All conditions are expressions that evaluate to TRUE or FALSE; if a condition evaluates to TRUE, then the condition is met. The label UCT denotes an unconditional transition (i.e., UCT always evaluates to TRUE). A transition that is global in nature (i.e., a transition that occurs from any of the possible states if the condition attached to the arrow is met) is denoted by an open arrow; i.e., no specific state is identified as the origin of the transition. When the condition associated with a global transition is met, it supersedes all other exit conditions including UCT. The special global condition BEGIN supersedes all other global conditions, and once asserted remains asserted until all state blocks have executed to the point that variable assignments and other consequences of their execution remain unchanged.

On entry to a state, the procedures defined for the state (if any) are executed exactly once, in the order that they appear on the page. Each action is deemed to be atomic; i.e., execution of a procedure completes before the next sequential procedure starts to execute. No procedures execute outside of a state block. The procedures in only one state block execute at a time, even if the conditions for execution of state blocks in different state machines are satisfied, and all procedures in an executing state block complete execution before the transition to and execution of any other state block occurs, i.e. the execution of any state block appears to be atomic with respect to the execution of any other state block and the transition condition to that state from the previous state is TRUE when execution commences. The order of execution of state blocks in different state machines is undefined except as constrained by their transition conditions. A variable that is set to a particular value in a state block retains this value until a subsequent state block executes a procedure that modifies the value.

On completion of all of the procedures within a state, all exit conditions for the state (including all conditions associated with global transitions) are evaluated continuously until one of the conditions is met. The label ELSE denotes a transition that occurs if none of the other conditions for transitions from the state are met (i.e., ELSE evaluates to TRUE if all other possible exit conditions from the state evaluate to FALSE). Where two or more exit conditions with the same level of precedence become TRUE simultaneously, the choice as to which exit condition causes the state transition to take place is arbitrary.

Figure 15-1—MACsec state machines - overview and interrelationships

Where it is necessary to split a state machine description across more than one diagram, a transition between two states that appear on different diagrams is represented by an exit arrow drawn with dashed lines, plus a reference to the diagram that contains the destination state. Similarly, dashed arrows and a dashed state box are used on the destination diagram to show the transition to the destination state. In a state machine that has been split in this way, any global transitions that can cause entry to states defined in one of the diagrams are deemed to be potential exit conditions for all of the states of the state machine, regardless of which diagram the state boxes appear in.

Should a conflict exist between the interpretation of a state diagram and either the corresponding global transition tables or the textual description associated with the state machine, the state diagram takes precedence. The interpretation of the special symbols and operators used in the state diagrams is as defined in Table 15-2; these symbols and operators are derived from the notation of the "C++" programming language, ISO/IEC 14882. If a boolean variable is described in this clause as being set it has or is assigned the value TRUE, if reset or clear the value FALSE.

Table 15-2—State machine symbols

Symbol	Interpretation
( )	Used to force the precedence of operators in Boolean expressions and to delimit the argument(s) of actions within state boxes.
;	Used as a terminating delimiter for actions within state boxes. Where a state box contains multiple actions, the order of execution follows the normal English language conventions for reading text.
=	Assignment action. The value of the expression to the right of the operator is assigned to the variable to the left of the operator. Where this operator is used to define multiple assignments, e.g., a = b = X the action causes the value of the expression following the right-most assignment operator to be assigned to all of the variables that appear to the left of the right-most assignment operator.
!	Logical NOT operator.
&&	Logical AND operator.
||	Logical OR operator.
if...then...	Conditional action. If the Boolean expression following the if evaluates to TRUE, then the action following the then is executed.
!=	Inequality. Evaluates to TRUE if the expression to the left of the operator is not equal in value to the expression to the right.
==	Equality. Evaluates to TRUE if the expression to the left of the operator is equal in value to the expression to the right.
*	Arithmetic multiplication operator.
-	Arithmetic subtraction operator.

15.2 State machine timers

The timer variables declared in this clause, 15.2, are part of the specification of the operation of the SecY. The accompanying descriptions of their meaning and use are provided to aid in the comprehension of the protocol only, and are not part of the specification. A SecY implementation shall implement a single instance of each timer variable.

Each timer variable represents an integral number of seconds before timer expiry.

15.2.1 Timer 1

Timer 1.

15.3 State machine variables

The variables declared in this clause, 15.3, are part of the specification of the operation of the SecY. The accompanying descriptions of their use are provided to aid in the comprehension of the protocol only, and are not part of the specification.

15.3.1 BEGIN

A boolean controlled by the system initialization (15.1). If TRUE causes all state machines, including per Port state machines, to continuously execute their initial state.

15.3.2 AdminMultiPoint

15.3.3 CipherSuiteSelectable

15.3.4 DuplicateDetected

15.3.5 IncludeSCI

15.3.6 IncludeSecTAG

15.3.7 NeighborsAllSecYs

15.3.8 PortEnabled

A boolean. Set if the SecY can use the MAC Service provided by the Port’s MAC entity to transmit and receive frames to and from the attached LAN, i.e. portEnabled is TRUE if and only if:

a) MAC_Operational (IEEE Std 802.1D Clause 6.4.2) is TRUE.

15.4 State machine conditions and parameters

The following variable evaluations are defined for notational convenience in the state machines.

15.4.1 Condition 1.

Condition 1.

15.5 State machine procedures

The following naming convention is used for the names of procedures that modify multiple variables (either multiple variables of a single Port or variables of multiple Ports):

a) ***set***: The procedure sets the value of the variables to TRUE.
b) ***clear:*** The procedure clears (resets) the value of the variables to FALSE.
c) ***updt:*** The procedure updates the variables in some other way.

The suffix “Tree” is used for procedures that can modify a variable in all Ports of the Bridge. For example, ***setSyncTree()*** is the name of a procedure that sets a variable TRUE for all Bridge Ports.

Where procedures are used to determine the value of a single variable, the procedure’s returned value is explicitly assigned to the variable in the state machine concerned.

15.5.1 proc1()

Returns TRUE if....

15.6 XXX state machine

The XXX state machine shall implement the function specified by the state diagram in Figure 15-1, the definitions in 15.1, and the variable declarations and procedures specified in 15.2 through 15.5.

Figure 15-1—XXX state machine

15.7 SecY performance requirements

This clause (15.7) places requirements on the performance of the SecYs to ensure that MACsec operates correctly.

16. Securing Networks

<<The following is still to be updated.>>

16.1 Securing Bridged Local Area Networks

Each user of the secured MAC Service provided by a Bridged Local Area Network is assured that communication through the Controlled Port providing the service is either directly with an authenticated and authorized system, or with an authenticated and authorized Bridge that in turn provides the same level of assurance. It is convenient to configure such a network to provide perimeter security. For example, then policy decisions (7.2) that support the security of each network protocol can be taken either by the end stations connected to the network, or by ingress and egress policies applied by the Bridge Forwarding Process (IEEE Std 802.1D, IEEE Std 802.1Q) at the edge ports that provide connectivity to those end stations. Figure 16-1 illlustrates such a network.

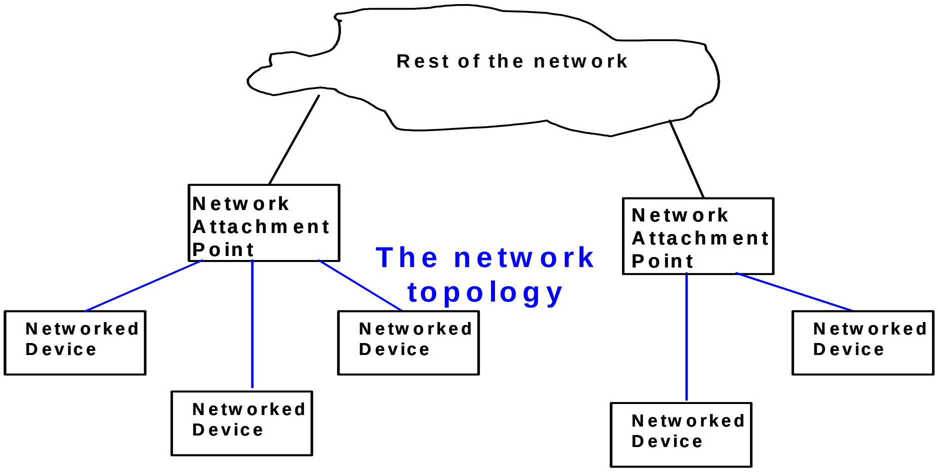


Figure 16-1—Network Topology

In environments where a small number of systems are all fully under the control of a single administration, ingress and egress policies can be unnecessary. Where controls are desirable to prevent some network hosts attacking the network infrastructure, or masquerading as a provider of network services to other hosts, the MAC Security key agreement protocols and supporting services should, at a minimum, be capable of distinguishing Host and Infrastructure authorization. This distinction can be useful in alternative methods for providing perimeter security, as described in Annex W.

16.2 Securing Provider Bridged Networks

<<Short intro. some of the points already made above. include figure.>>

Annex A (normative)

PICS Proforma[1]

<<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 will all be removed prior to publication and are not part of the normative text.>>

<<Material borrowed from 802.1D is scattered through this clause as a prompt to the editor and reviewers to supply analagous material for MAC Security, if appropriate.>>

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
MACP	Does the implementation provide the MAC Service, as specified in <ref>, for use by end system functionality in the containing system?	M	A.6	
EISSP	Does the implementation provide the Extended Internal Sublayer Service as specified in IEEE Std 802.1Q to support the MAC Bridge functionality?	O	A.7	
EISSU	Is each specific MAC Technology used as specified by IEEE Std 802.1Q for the support of the MAC Extended Internal Sublayer Service for that MAC Technology? (The PICS Proforma(s) required by IEEE Std 802.1Q shall also be completed.) (If support of a specific MAC technology is claimed any PICS Proforma(s) required by the Standard specifying that technology shall also be completed.)	M	IEEE Std 802.1Q 6.4, . A.8	Yes [ ]
SECS	Does the implementation support the full range of security services specified in Clause 6 of this standard?	M	<<ref>> A.9	
EX1	Does the implemention provide this mandatory major capability?	M	<<ref>> A.10	Yes [ ]
EX2	Is this major capability supported?	O	<<ref>> A.11	Yes [ ] No [ ]
EX3	Does the implementation do what is supposed to do in respect of this major capability?	**EX2:**M	<<ref>> A.12	Yes [ ] N/A[ ]

A.6 Provision of the MAC Service

Item	Feature	Status	References	Support
MACP-1	Has it been done right?	M		Yes [ ]
MACP-2	First detail?	M		Yes[ ]
MACP-3	Second detail?	M	6.4, .	Yes [ ]
MACP-4	Are the MAC status parameters implemented on all Ports?	M	6.4, .	Yes [ ]

Predicates:
GOOK= GOOK_SPEC[Yes]

A.7 Provision of the Extended Internal Sublayer Service

Item	Feature	Status	References	Support
EISSP-1	Has it been done right?	**EISSP:**M		Yes [ ]
EISSP-2		M		Yes[ ]

A.8 Use of the Extended Internal Sublayer Service

Item	Feature	Status	References	Support
EISSU-1				
EISSU-2				

A.9 Security services

Item	Feature	Status	References	Support
SECS-1				Yes [ ]
SECS-2				Yes [ ]

A.10 Major Capability 1

Item	Feature	Status	References	Support
EX1-1				Yes [ ]
EX1-2				Yes [ ]

A.11 Major Capability 2

Item	Feature	Status	References	Support
EX2-1				Yes [ ]
EX2-2				Yes [ ]

A.12 Major Capability 3

Item	Feature	Status	References	Support
EX3-1				Yes [ ]
EX3-2				Yes [ ]

Annex B (informative)

Bibliography

<<Items in the References clause should only be those that are definitely referenced by the document, not just useful background reading. The latter should go here.>>

ANSI X3.159-1989, American National Standards for Information Systems—Programming Language—C.[1]

IETF RFC 2108[2], Definitions of Managed Objects for IEEE 802.3 Repeater Devices using SMIv2, de Graaf, K., and Romascanu, D., February 1997.

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

ITEF RFC 2737, Entity MIB (Version 2), McCloghrie, K., and Bierman, A., December 1999.

IETF RFC 2922, Physical Topology MIB, Bierman, A., and Jones, K., November 1998.

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

[1] ANSI publications are available from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

[2] Internet RFCs are retrievable by FTP at ds.internic.net/rfc/rfcnnnn.txt (where nnnn is a standards publication number, such as 1493), or by Web browser at http://www.ietf.org/ , or call InterNIC at 1-800-444-4345 for information about receiving copies through the mail.

Annex V (informative)

Cipher Suites (this Clause is not sorted out yet)

V.1 Criteria for Selection of Mandatory Cipher Suites

Principle goal is to maximize interoperability, allow communication between unlike systems at different speeds. Picking one mandatory Cipher Suite simplifies achieving this goal. It is best to have a minimum number of madatory suites for interoperability across interworking/interconnection scenarios, where the scenarios are direct connection over a MAC, a transparent infrastructure.

<<Provide a list of algorithms that have been considered and the decision based on selection criteria.>>

CCM format is specific to 802.11

CCM broader. CCM can’t go above 3Gbs in hardware.

suggested major goal is to maximize interoperability. communicate with unlike systems at different speeds. speed translations. pick one mandatory, simplifies.

one mandatory, others admitted because systems are built using them. got to be able to plug in. Formally talk about one suite, make sure others can fit in.

ccm format is specific to .11.

Minimum number of mandatory suites for interoperability across interworking/interconnection scenarios, where the scenarios are direct connection over a MAC, a transparent infrastructure, like not limited to provider bridge nets for speed reande of 10 G to 1 Mbs. transp infra can cause operation between any point in speed range, then these criteria are best met with one choice. Potential .11 specific solutions are not believed extensively useful for this.

Export issues for strong ciphers? in US not an issue. common treaty, for most countries can do what want. not for China. define an operational suite that has a reduced key size. eg aes-128 with 64 bits fixed, may not get through. can do as vendor inspired option.

V.2 Cryptographic suites

Crypto choices include:

1) parameters: - what are they and what are their sizes- PN (packet number) length, ICV length,.
2) privacy, confidentiality modes: CTR, CBC,.
3) integrity modes: HMAC-SHA1, MD5, OMAC, PMAC,...
4) encryption algorithms, block ciphers: AES-128, DES, 3DES-EDE,.
5) combination modes: CCM, OCB, CWC, GCM, EAX

V.3 Cipher suites

It is better to use Cipher Suites rather than to choose individual algorithms to match together to provide different functions, such as, confidentiality, integrity, key management, and replay protection. The algorithms within a given Cipher Suite are well-understood to work together, and the set of algorithms is verifiability secure for some set of configured parameters. On the contrary, to not use a Cipher Suite would open the choices for providing key management, integrity and confidentiality to an arbitrary combination of algorithms and parameter settings, which are not necessarily known to work well together and be secure. For example, past experience suggests that using modes differently than in their default configurations has led to poor security.

Here is a suggested Table of Cipher Suites for confidentiality.

Table 1—Suggested Confidentiality Ciphers

EUI-48	Cipher #	Type	Mandatory/ Optional	Defined in
XX-XX-XX	0	NULL	Mandatory	x.y.z
XX-XX-XX	1	AES-128 in GCM Mode	Mandatory	
XX-XX-XX	2	AES-128 in OCB Mode	Optional	
XX-XX-XX	3	OMAC	O	
XX-XX-XX	4	PMAC	O	
XX-XX-XX	5	CWC	O	
XX-XX-XX	...	TBD		
XX-XX-XX	...-32767	Reserved		
XX-XX-XX	32768-65535	Playpen		
XX-XX-XX	0-65535	Vendor Proprietary		

A Null encryption Cipher Suite is necessary, see Cl 8.

It is argued that a minimal number of Cipher Suites should be mandatory, while the rest are optional. Optional Cipher Suites might be mandatory for some devices for technical reasons, e.g., parallelizability. It is necessary to make sure the dividing line is well-defined. Define the dividing line, e.g., OCB is mandatory above 1.1. Gb/ps.

Sets of ciphers for port authentication and for key exchange are also necessary, but will be under another PAR.

V.3.1 Cipher Suite Selection Criteria

A Cipher Suite provides a set of cryptographic methods that provide confidentiality/privacy and integrity/message authentication. Due to constraints imposed by implementation of these algorithms in hardware, we define a minimal default set of features mandatory to implement.

The important criteria for choosing cryptographic algorithms include:

1) crypto strength, provably secure << how is it measured?>>
2) peer review among cryptographers <<how measured?>>
3) exportability
4) interoperability <<??>>
5) ease of hardware implementation- memory, gate count
6) encumbrance status
7) speed - parallelizability

A safe method of choosing cryptographic algorithms is to use Cipher Suites. A Cipher Suite fulfills the requirements for a well-defined minimal mandatory set of security features. It specifies a set of algorithms for some or each of key exchange, data confidentiality, data origin (message) authentication, and replay protection. The interaction between the various algorithms that constitute the set of modes in a given Cipher Suite have been shown to interact well together and are well understood within the cryptography community. Each Cipher Suite can be shown to be verifiably secure by security experts using formal methods.

<<Some of the combination mode stuff needs mentioning in 9.3 Cipher Suites>>

Some modes are called combination modes. These modes consist of cryptographic algorithms which offer multiple crypto functions within the same algorithm. For example, Encryption Authentication (EA) modes provide both confidentiality and integrity into one “combined” algorithm. The tag in a combined mode replaces the ICV. These modes can be included in Cipher Suites with other algorithms to provide additional functionality.

We will use only bona fide Cipher Suites, including combined modes. We will not make our own choice of cryptographic algorithms outside those which appear together in a given Cipher Suite, i.e., we will not mix and match crypto algorithms. This is to prevent security breaches similar to those that experience has shown are likely to occur when crypto algorithms are matched with each other.

<<See Appendix Z>>

One way to decide whether a crypto algorithm has various criteria is to follow guidance of FIPS/NIST.<<how to judge whether crypto algorithms meet criteria? We should better understand FIPS process>>

The size of parameter fields in crypto algorithms: the Cipher Suite entry should specify the lengths of all the parameters for all algorithms used in the Cipher Suite. We will not dynamically vary parameter lengths. Different size parameters may be necessary for different media types. These can be handled by specifying different Cipher Suites offer different parameter sizes. See Appendix Z.

When parameter lengths are fixed, they algorithms are amenable to mathematical techniques, and can be provably secure.

Provider Bridges result in end-to-end connections (and SAs) between dissimilar technologies (e.g., 802.11 vs. 802.3). This difference in media technologies causes variations in cryptographic needs, such as the PN length, parallelizability, etc.

A and B will have the same default Cipher Suite, and either use that, or choose a vendor mode that is different than the default. Reason to negotiate even when on the same media is if can do better than the default.

V.3.2 Observations on cryptographic algorithms

1) AES is the block cipher du jour

2) RC4-40 used for exportability, but is not good for engineering reasons, as it has a heavily serial algorithm
3) DES is deprecated (by FIPS) for new equipment
4) CTR (privacy mode) is parallelizable
5) FIPS has not yet chosen an integrity mode. It is thought likely to choose OMAC, which is not parallelizable
6) integrity modes that are parallelizable are often encumbered - PMAC,...
7) it is possible to use an authentication specific algorithm, HMAC-SHA1. However it requires independent hardware
8) combo mode CCM- not parallelizable, not encumbered, used in 802.11i
9) combo mode OCB - parallelizable, encumbered, requires more gates to do AES decrypting
10) combo mode CWC - parallelizable, not encumbered,...

Annex W (informative)

Perimeter Security Methods

The following discussion indicates some of the ways in which the distinction provided by MACsec between host and infrastructure authorization can be used in providing perimeter security.

W.1 Private VLANs

All the hosts can be prevented from communicating directly with one another, as follows. Each Bridge edge port that connects to a host admits only untagged frames and uses a PVID A (say). Each Bridge edge port that connects to an Infrastructure component other than a Bridge uses a PVID B. Only VLAN B is permitted to egress to hosts, while both VLAN A and B egress to Infrastructure components. VLANs A and B are configured for Shared VLAN Learning (SVL).

NOTE 1—The partial connectivity provided to hosts by preventing their direct interconnection while permitting infrastructure components to transparently communicate with both hosts can interfere with the normal operation of some protocols, e.g. OSPF, if attached hosts are permitted to operate such protocols. Use of multiple instances of the secure MAC Service on a single LAN, as described in the following clause, is one way to address that requirement.

W.2 Other methods

Alternatively edge ports connecting to hosts can limit their participation in DHCP, ARP and other similar protocols that provide subnetwork support for routing. A discussion of such approaches is presented here.

<<If someone is willing to volunteer to draft it.>>

Hosts can be prevented from using more than one MAC Address....as can Infrastructure stations other than Bridges although the latter is problematic with VRRP...

Annex X (informative)

Draft Changes

ch 1.2 added scope verbatim from PAR

ch 1.4 Definitions - note to fill in

ch. 6 typo, "the EISS is derived from the ISS"

added annex X to keep changes, will throw away

Annex Y (informative)

Secure RSTP

This note is an preliminary look at using MACsec to secure RSTP. It proposes a deployment plan and security policies for use with RSTP/MSTP in conjunction with MACsec.

Y.1 Overview

This annex

a) Summarizes the challenges and ingredients required for a successful deployment plan.
b) Puts the argument for ensuring that standard management encompasses deployment.
c) Lists challenges that might occur in a MACsec deployment.
d) Suggests a step by step deployment plan that allows these challenges to be encountered and investigated while maintaining network connectivity.
e) Describes RSTP policies that ensure that only authorized systems can perturb the spanning tree configuration and learnt address information.
f) Considers early deployment of software based MACsec protection for configuration protocols in advance of full rate hardware, with special reference to RSTP.

Y.2 Protocol Deployment

Network administrators rarely have the freedom to take entire networks of significant size out of service for an extended period to perform simultaneous upgrades of systems. At the same time the number of things that could go wrong on a big bang transition from undeployed to fully deployed is large. So large in fact that a ìjust try it and fallback if it all doesnít workî approach is both unlikely to succeed and unlikely to provide enough diagnostic data for success on a second or subsequent attempts.

A staged deployment plan is required. Each stage should:

a) be a small step toward the end goal
b) be easily reversible
c) provide positive feedback, and diagnostic data
   1) confirming that the step occurred
   2) pinpointing the cause of any network problem introduced
   3) identifying problems that should be fixed before taking the next step.

In an ideal world each stage can be made risk free, i.e. the network will continue to work as expected, provided any problems identified in the prior stage were addressed. In most deployments the diagnostic capabilities have to be more powerful than would be required if a methodical staged plan had been used. It is rare, for example, that an adequate inventory of network devices and their current state is produced until after a deployment problem has occurred.

Y.3 Specifying management

Management controls are clearly needed to support staged deployment. Counters of both normal and error events are required to confirm that each stage is proceeding to plan, and to diagnose failures.

There are alternative ways of introducing MACsec. If these are not explicitly discussed, it is likely that the management controls provided by the standard will be selection of those required by a number of these, but insufficient to support any one of them. Whether proprietary management from any vendor will be sufficient is anyone's guess, but the chance of multi-vendor staged deployment is low, so practical interoperability will be confined to those cases where the network has magically sprung into being in its final complete and debugged form.

Y.4 MACsec deployment challenges

MACsec secures a network one LAN at a time, which greatly helps deployment by reducing the number of inter-system dependencies, particularly if the LAN is truly point-to-point. LANs most open to attack can be secured first, and a secure perimeter implemented.

Deployment might still be disrupted because

a) Stations, most likely bridges, routers, or servers, that provide or require connectivity and are essential to service delivery are attached to the LAN but have been missed in the upgrade process.

NOTE 1—This is much more likely when the LAN is "virtual", as in the case of a service instance provided by a Provider Bridged Network.

b) Cipher suite selection has failed.

NOTE 2—This is largely dealt with by requiring a mandatory default Cipher Suite for all conformant implementations.

c) Key agreement protocols fail.

NOTE 3—One of the worst cases is intermittent failure of key agreement protocols due to intermittent failure of the infrastructure components that support them.

d) Authorization is incorrectly set or not correctly bound to authenticities.
e) Authentication credentials are not properly distributed or maintained.
f) Incorrect client policies have been implemented.

<<As is readily apparent this is just a top-of-mind list. A structured and time tested decomposition of failure causes would be appreciated.>>

Y.5 Full MACsec deployment

The plan to secure RSTP operation on a LAN is somewhat simpler if it can be assumed that full MACsec capabilities are available in each of the systems attached to the LAN, so that will be described first.

We will also assume that the risk of missing stations from the pre-upgrade network baseline process is low. This assumption is reasonable if point-to-point links are being upgraded, but to help it we plan to upgrade one LAN at a time, so when the network breaks we have a good chance of identifying where (provided that not too much else, unconnected to MACsec, is being changed at the same time).

The 'standard' interface stack configuration is used to support this deployment, i.e. both the MAC Relay Entity and the RSTP Entity (in Bridges) are attached to the Controlled Port of the SecY providing the interface to the LAN.

The upgrade steps are:

1. Upgrade all the system attached to the target LAN so they are MACsec capable. The management parameters of the SecY are set as follows:

— Secure Frame Selector:
ControlledReceives = Both
ControlledSends = Untagged
— Secure Frame Verification:
ValidateReceivedFrames = False
ReplayProtect = False

<<These follow P802.1AE/D2 very loosely. That spec also needs to describe which parameters are expected to be set directly, and which should be set by the Kay.>>

NOTE—The SecY verifies frames with the MACsec Ethertype, but transparently receives all other frames. Other possible settings are All (bypasses the SecY, even frames with MACsec EtherType are transparently passed), Untagged, and Tagged.

The KaY management parameters are set as follows:

— CipherSuiteSelectable = True only for the Default Cipher Suite

This step should not break anything, unless there is illicit use of the MACsec EtherType.

NOTE—It would be nice at this step if the KaY provided sufficient controls and recording for its Discovery process to allow connectivity to be confirmed. Some testing of key agreement protocols is also possible at this stage. Both of these suggestions lie outside the scope of this note.

2. For the next step, the KaY has to be set so that it will generate a stream of SAKs even if the key agreement protocols are not working properly. Change the SecY management parameters as follows:

— Secure Frame Selector:
ControlledReceives = Both 8
ControlledSends = Tagged
— Secure Frame Verification:
ValidateReceivedFrames = False
ReplayProtect = False

NOTE—The SecY verifies frames with the MACsec Ethertype, but transparently receives all other frames. Other possible settings are All (bypasses the SecY, even frames with MACsec EtherType are transparently passed), Untagged, and Tagged.

This step shouldn't break anything either. The counts of SecTAG'd frames received should go up, and those of untagged frames should go down. Monitoring those counts together with knowledge of protocols that run over the Uncontrolled Port should be sufficient to confirm that all Controlled Port traffic on the LAN is now being sent tagged.

3. Change the SecY management parameters as follows:

— Secure Frame Selector:
ControlledReceives = Tagged 9
ControlledSends = Tagged
— Secure Frame Verification:
ValidateReceivedFrames = False
ReplayProtect = False

NOTE—The SecY verifies frames with the MACsec Ethertype, but transparently receives all other frames. Other possible settings are All (bypasses the SecY, even frames with MACsec EtherType are transparently passed), Untagged, and Tagged.

Check that the connectivity is indeed not being disrupted, that the spanning tree has not reconfigured etc. A deadman timer protected change is a useful tool here, as it will recover an inband managed network if connectivity was broken.

This is a good time to get the KaY and the key agreement protocol infrastructure really working. When it is working, the InvalidReceivedFrames count should stop incrementing. Check the UnknownSCI and UnknownSC counts if problems persist (Discovery may not be working correctly). If there are none of these, check the per SA counters to see if SAs are being used correctly by the transmitter, otherwise suspect the keys. Look at the KaY to monitor key agreement and SAK derivation.

4. Allow the KaY to select other Cipher Suites, including those which set the E bit, i.e. require Cipher Suite selection, and possibly the SAK, to be known at receivers if connectivity is not to break.

Confirm that frames are not being discarded as invalid on receipt.

5. Set ValidateReceivedFrames = True. If the previous steps were OK, nothing should change. Check the ReplayViolations count. If it is not incrementing, then Replay Protect can be set.

6. Check the spanning tree roles and the authorization provided by the KaY against those that would be permitted by RSTP policies. Set the restrictedRole (controlling whether the Port can be a Root Port) and restrictedTCN policies. Verify that the spanning tree configuration has not changed.

Done.

Y.6 RSTP policies

Secure RSTP implements policies that use the authorization provided by P802.1af and the associated integrity and origin guarantees provided by MACsec. RSTP policies are applied to received BPDUs and control whether or not:

a) The receiving port can be a Root Port (restrictedRole)
b) Topology changes are accepted (restrictedTcn)

If restrictedRole is set for a port, then the RSTP’s updateRoles procedure will not select it as a Root Port, but only as a Designated, Alternate, or Backup Port.

NOTE—This a proposal not part of the current RSTP specification in IEEE Std 802.1D-2004.

If a BPDU has been received that would become a Root Port (i.e., if restrictedRole were not set, then) it becomes an Alternate Port instead. This means that the spanning tree configuration of the network ‘behind’ the bridge port cannot be changed by receipt of a BPDU by the port.

NOTE—This has to be checked to ensure that no proposal-agreement handshakes can be initiated.

It also means that there will be no connectivity through the port, if a BPDU is received that conveys a priority vector suggesting a better Root or better path to the Root.

If the restrictedTcn parameter is set, no topology changes are propagated through the port to the other ports of a bridge.

Y.7 Unauthorized Bridges

It may be the case that there are unauthorized bridges attached to the LAN, and that the intent is to deploy MACsec to exclude these. Since both the MAC Relay and RSTP use the Controlled Port, the unauthorized bridges will be excluded from both the control protocol and the data when ValidateReceivedFrames is turned on.

To minimize the chance of those unauthorized bridges blindly passing MACsec frames and causing a loop in the network, the SecYs for all Ports that are not yet attached to secure LANs, and are not currently participating in deployment to a specific LAN, should have ControlledReceives = Untagged.

Y.8 Staging capabilities

It is useful if deployment plans not only recognize the challenge of upgrading different systems at different times, but also the opportunities presented by the staged availability of capabilities within a single system. While these may only provide a fraction of the anticipated benefits of protocol deployment, they present an opportunity to debug a large part of the deployment.

However such fractional ability may also require additional controls and different system configurations. Their benefits should be balanced against the complexity of incorporating them into the system.

Y.9 Soft MACsec deployment

The term ‘soft deployment’ is used here for the idea that a software based MACsec implementation might be used to protect control protocols, in advance of the availability of full rate hardware capable of protecting all the data

<<A major point of this note is to describe how this can be done for RSTP. The idea that it could be done was advanced by Norm Finn. I am not sure if the description of how given here fits Norm’s ideas on the subject..

If anyone can think of a better term for this I would appreciate it.>>

Soft deployment definitely has its problems, as it threatens to divorce the connectivity provided to the control protocols from that of the data that they are meant to be controlling. For bridging that could be disastrous, therefore special care is required.

Soft deployment can

a) Ensure that the network as a whole is not disrupted by an unauthorized bridge that claims to be the Root Bridge or provide a path to the Root, or that injects unwanted topology change notifications into the rest of the network.
b) Detect bridges that are unauthorized but have not been attached to the network with any malicious intent.

and what soft deployment cannot do is to protect data.

The MAC Relay is connected to the Uncontrolled Port.

The RSTP entity is connected to both the Controlled and Uncontrolled Ports. It always transmits and receives frames using the Controlled Port, and also receives BPDUs on the Uncontrolled Port when ControlledReceives is set to Tagged.

If the goal is simply to restrict the impact of BPDUs from unauthorized bridges, BPDUs are also transmitted using the Uncontrolled Port when ControlledSends is set to Tagged.

.A slightly higher priority and subtly different identity are associated with BPDUs received from the Controlled Port, thus ensuring that they, and their associated authorizations, are not immediately displaced by the Uncontrolled BPDU from the same transmitter.

Different levels of authorization are naturally attached to BPDUs received from the Controlled and Uncontrolled Ports. MACsec protected BPDUs are used to establish spanning tree port states for Uncontrolled Port data, the two are not treated as separate Bridge Ports. All the bridges attached to a LAN have to use the same relative priority for BPDUs if data connectivity is provided, so there can be times when the reception of an Uncontrolled BPDU can displace a priority vector received in a Controlled BPDU and cause the receiving port not to be a Root Port. The authorization associated with each received priority vector is maintained along with the RSTP “infoIs” variable for the port to ensure that the policy control is applied correctly.

Annex Z (informative)

Commentary

<<Editor's Note: This is a temporary Annex, included as a record of technical issues and their disposition. This annex will be removed prior to Sponsor Ballot, and preserved on the 802.1 web site for future reference[1].>>

<<The order of discussion of issues is intended to help the reader understand first what is the draft, secondly what may be added, and thirdly what has been considered but will not be included. In pursuit of this goal, issues where the proposed disposition is “no change” will be moved to the end. The description of issues is updated to reflect our current understanding[2] of the problem and its solution: where it has been considered useful to retain the original comment, in whole or part, either to ensure that its author does not feel that it has not been sufficiently argued or the editor suspects there may be further aspects to the issue, that has been done as a footnote.>>

Z.1 Multiple CAs on a single LAN

Strictly speaking multiple CAs can exist on a single LAN, in the sense that it is possible to use cryptography to create distinct CA groups by having more than one key set. However, this is to be strongly advised against. It changes the connectivity of the LAN as a by-product of security. For example, if you have 5 stations in a LAN, they are all connected. If you use cryptography to separate them into two CAs, one with 2 members and one with 3 members, by issuing separate keys, then all the members in the LAN will no longer be able to communicate with each other. If security is on, all 5 members can’t communicate, when security is turned off, all members of the LAN will be able to communicate. So, the connectivity will be dependent on the security service. It is precisely this sort of change in MAC Service that we do not want to be a result of providing secure service. The reason is that it will make difficult to debug and is likely to lead to causing secure service to be “blamed” for anything that goes wrong.

Although multiple CAs can in principle be constructed on a single LAN by using different keys to separate connectivity without any underlying separation of service instances, that is a very bad idea, and text needs to be added to this clause and potentially elsewhere in the document to disparage the idea. First such a scheme makes a hash of deploying MACsec, turning security on or off radically changes the network connectivity. This is hardly the behavior that is envisaged in the PAR, where it is stated that MACsec should operate transparently to its clients. Staged deployment scenarios using integrity protection without validation become impossible.

Second such a scheme is an accident waiting to happen, if the keys for one CA ever coincide with or overlap the other, the CAs will merge for a period - and guarding against this problem simply exports a new and very unusual problem to key agreement.

Third such a scheme requires explicit support from key agreement, which will have to carry an explicit multiplexing value to separate key agreement for the two separate instances.

Fourth such a scheme requires explicit configuration of the ports attached to each "separate" CA if bridging is going to be provided between the instances.

[1] The footnotes in this annex provide further background to its development. Most of the highly subjective material, who said what and were they were right etc. together with temporary notes on blind alleys will be put into the footnotes so that they can be easily stripped out when the final annex is preserved.

[2] This annex is not intended therefore to be a complete historical record of the development of the draft. The formal record is largely captured in the Disposition of Comments on each ballot.

Fifth such a such a scheme will result in a high error rate, thus masking any other problems.

We need to stick to one SecY being in one CA on one instance of an underlying service as far as possible. If multiple underlying services are to be realized on the same LAN then they should be supported as already described in this clause.

Concepts are “logical” and “physical” LAN, but 802.1 doesn’t want to use term “logical” which is problematic.

Z.2 Position of the Security Shim

The position of the security shim will be in different places in a regular bridge and a provider bridge. Weakness of a shim model is that it can be put anywhere, ncluding foolish places. We need to focus on certain use cases and say where to put the shim.

Z.3 Replay protection

Notwithstanding the emphasis on “connectionless” confidentiality and integrity in the PAR, and the implication that not only is the service provided connectionless (i.e., one request primitive has no relationship to any other except for quality of service aspects), but also the service support is connectionless, i.e., there is no relationship between one frame and another, it has been agreed that the discussion, and potential provision, of replay protection falls within the scope of the PAR.

Replay protection is provided through including a sequence number, such as the Packet Number PN, in the frame header. Determining whether this PN has been received before is usually done in one of two ways. First, by keeping a list of numbers that have been seen. Alternatively, an upper and lower window size could be kept, and any packet outside the window is dropped. If the packet is in the window, it is checked to see whether it was previously received or not.

The PNs cannot be changed without detection because they are protected by the ICV.

Z.3.1 Disposition

And this is what we have decided so far- we will have Replay protection. It’s useful and it comes ‘for free’ with the Packet Number.

Z.4 Crypto issues

The crypto needs of different media types are different -speed, cost, processing power needs. Provider bridges require that different media types interact, on both ends of an SA. How should the differing crypto needs be treated?

Security establishment: There is a chicken and egg situation that needs to be considered on a MAC specific basis. How does a link get established if it needs to be secure to be established and you can only do security on an established link? Which parts of the frame are protected and which are not? Must avoid setting up a race condition by design. For 802.3, the decision is to apply security transform only to data, not to control frames

Z.5 Vulnerabilities

IEEE 802 technologies are vulnerable at the interfaces between L2 and L3. Vulnerability is created where there is loose coupling between layers, where there is difference of address spaces, where there is security at layer n-1 but not layer n. ARP spoofing occurs because of the need for an unprotected discovery protocol to discover the lower layer address. MACsec probably cannot offer any help.

Z.5.1 ARP Spoofing

We cannot offer protection against disclosure due to ARP spoofing, in which an attacker sends gratuitous ARP messages claiming to have IP addresses of other stations. The attacker can then intercept, read, and alter messages between any two points in a point to point topology. The ICV will be recalculated and the altered data will pass integrity check. If the message is cryptographically protected above L2, for example with IPsec, the data cannot be read or changed by the attacker. This threat occurs at the intersection between the L2 and L3 layers.

There is no protection against legitimate users - in ARP spoofing, the attacker has legitimate use of the LAN. It is a case of legitimate user with bad intent. MACsec does offer the ability to identify the bad user. If the bad behavior is unintentional, for example, due to misconfiguration, it can be corrected, but if it is unintentional, then MACsec only identifies the attacker, but cannot prevent the attack.

The ICV is recomputed every time the frame presented to the MAC layer, so a man-in-the-middle can make unauthorized changes and it will pass the integrity check. Thus, we have point to point integrity, but not global integrity.

Z.6 Parameters and Frame Format

Z.6.1 Requirements

What should the parameters be bound to? A Cipher Suite.

If the parameters are variable, then the frame formatter might need to behave dynamically, redefine MTU, etc.

Parameter choices

1) A sequence counter - Packet Number (PN), Initial Value (IV) - how long?
2) An integrity check - Message Integrity Code, MIC, Message Authentication Code MAC, Integrity Check Value (ICV) - length?
3) What kind of ciphertext?
4) How much of packet should be in ciphertext?
5) Security Association ID (SAID)

Different media technologies give rise to different cryptographic needs, such as length of the PN and whether parallelizability is necessary. This arises in the context of Provider Bridges, which may result in end-to-end connections between dissimilar technologies. One suggestion is that we should have a global default set of parameters to be present on all devices. This however creates challenges to meet the criteria of both technologies, such as needing speed (802.3) and also requiring low cost (802.11).

Vendor proprietary area and playpen areas, with appropriate EUI-48s should be included.

Parameter values: Parameter values need to be constant during the life of an Security Association (SA). Parameter values that can change dynamically create vulnerabilities. Rather than attacking the cryptographic algorithm, an attacker can attack the negotiation, so that a weaker type of cryptography is chosen, which the attacker can then break more easily. For example, in wireless, an attacker could cause WEP to be chosen rather than something more secure. Therefore, once parameters values have been established, there should not be a mechanism for changing them.

Variable parameters (e.g., variable tag size in CCM, ref.) creates a vulnerability and therefore also leads to poor security. [say more, example to make clear what is meant].

Should parameter values be negotiable? There can be reasons for making some parameters negotiable at setup time. For example, PN length might be negotiated because different priorities exist for different MAC/PHYs. One way to incorporate this need is by including the various options within the set of defined Cipher Suites.

The way to provide for different parameter values is through different Cipher Suites -- for example one might have 128-bit value and another 256-bit value. Using Cipher Suites in this way is a simple way to allow policy.

Z.6.2 Header data

The MAC level header fields are not in MSDU, but are in the MPDU, except in the one case shown above in Figure.., where the SecY is the... The header fields are defined by the various IEEE 802 MAC/PHY specifications. Thus they are different for different IEEE 802 technologies.

Header data consists of authenticated parts, covered by the ICV, and non-authenticated parts, not covered by the ICV. Not all fields in the header require authentication. See Figure 8.1

Placement: Ideally the header data would be placed after the PN just before the ciphertext in order to allow some time between nonce construction and data encryption.

Not all fields in the header require authentication. For example, the Header Check Sequence (HCS) in IEEE 802.16 would not be authenticated as the field is itself computed from the first 5 bytes of the header in order to discover bit errors. In fact, it would prove problematic in implementation to authenticate. The HCS is generated after authentication has been done. Another example is from 802.11. The upper four bits of the sequence control field, SC, cannot be authenticated for implementation reasons; the value of the bits is known only a moment before transmission.

Z.6.3 Secure Channel Identifier (SCI)

Source and destination addresses, SA and DA, in the MPDU are the original addresses, the end to end addresses. In a multipoint or Provider Bridge network,. the SA and DA are not the addresses of intermediate devices that are doing the encryption and decryption. The SecY is part of the bridge stack, and thus it’s address is not seen. It would be useful in the PB case in particular, to make available the knowledge of where the encryption was applied. This is what the SCI provides. It is the address of the Bridge port, which is used both by the Bridge and the SecY, called a Common Port, see Cl 8.

Z.6.4 Packet Number (PN)

Placement: The packet number should go as early as possible in the frame because a nonce needs to be constructed before any cryptographic operations can happen.

Size: The PN strength is measured in the time to re-key, which is directly dependent on the length of the PN. Therefore, longer is better than shorter. The time to re-key is inversely proportional to the packet rate.

There is a discrepancy in what is a good PN size for different cases, there is no good PN size for all cases. Compare the slowest IEEE 802 technology with the fastest to see the magnitude of the difference between optimal in each case. The minimum rate is approximately 10kb/ps (IEEE 802.15), maximum rate approximately 100 Gb/ps (arbitrary optical medium). There is a 10^7 difference, which is approximately 23.5 bits. so the slowest links will want 24 fewer bits to achieve the same re-keying rate as the fastest link will want for optimal operation. The gap will only widen in the future.

How can this issue of choosing the PN size be resolved? A number of options were considered:

1) Pick suitable case for highest packet rate interface. Make it 8 bytes. The problem here is that then slower devices suffer, which may have as a consequence poor adoption rate.
2) Tie the PN size to the PHY type. Provider bridges span between different PHY types, so this option won’t work.
3) Variable length encoding. The PN size could grow with the PN magnitude. This is expensive to do in hardware implementation. The savings is not great because most occupancy is caused by large sized values.
4) Variable PN size, coded in the header. This option has bad security implications. An attacker spoofing the packet can make the PN size smaller and thereby easier to crack.
5) Variable PN size negotiated between stations during setup. Negotiated at the time of SA formation and remain constant for the lifetime of the SA.

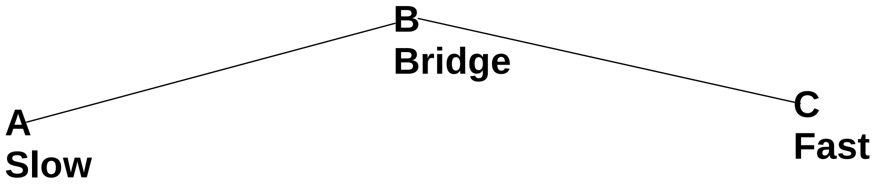
Agreement to negotiate a priori for the life of the SA. The PN size should be a parameter in the Cipher Suite, so that two sizes create two Cipher Suites. It was decided to chose the PN sizes to differ maximally, the largest and the smallest - either 64 bits or 24 bits. The rationale is that it is usually desirable to either maximize security with a large size, or to minimize the damaging effect on throughput with the smaller size.

For a given technology, the PN size should have a default value based on the maximum packet rate. Therefore, in the case where there is not a Provider Bridge, the negotiation will be brief, both sides agreeing on the default.

Provider Bridges causes some complexity with respect to the PN size. What about negotiating PN size in the case of Provider Bridges? If the PN size is by default the smaller PN choice of the two ends, then the slower device limits the maximum packet rate.

Negotiating the size of the PN in the Provider Bridge case causes a vulnerability. Attackers can attack the negotiation rather than the cryptography, in order to get the PN size smaller and thus make the cryptography easier to crack. Requirements for cryptography should include assurance that the negotiation leads to a chosen size no smaller than the minimum acceptable to the slower device.

With Provider Bridges a vulnerability can be caused. A and C negotiate a small PN in accordance with A, the slower device. An active attacker on the fast side of B is capable of breaking a small PN. If the slower transmission rate is used in security assumptions, they become invalid if the link from B to C has a faster data rate.



Negotiating the PN size as a parameter for a particular algorithm is not a good idea. The negotiation might lead to the improper use of a cryptographic function. For example, a security proof may assume that the PN size is a particular value.

Choosing between Cipher Suites would work since we are limited to known good cases. Assume that each Cipher Suite configuration had been validated.

Negotiating PN size exposes the existence of a Provider Bridge PB. If there is not a PB, then there is a single medium and the default PN will quickly be established, so any negotiation between stations exposes the fact that they are separated by a PB.

Two proposals for PN negotiation:

1) When operating across Provider Bridges, the slower device yields to the faster device PN length and suffers throughput drop. This minimizes security risk on the fast side, and makes impersonating a Provider Bridge pointless, since the more secure length is chosen.
When on a non-provider Bridge link, negotiation leads to the default for that MAC/PHY.

2) When operating across Provider Bridges, the faster device yields to the slower device PN length and suffers the potential increase in re-keying rate. This prevents imposing an undue overhead on a slow link.
When on a non-provider Bridge link, negotiations leads to the default for that MAC/PHY, or to a shared enhanced mode value.

<<example of two Cipher Suites that differ only in a parameter value>>

Z.6.5 Ciphertext

Placement: The placement of the ciphertext in the frame is similar to the placement of the plaintext.

Z.6.6 Integrity Check Value (ICV)

When to compute the ICV: Is the ICV going to be computed over encrypted data, or cleartext? A big issue to consider. Although this will be decided as part of a Cipher Suite choice, we should understand the implications. Computing the ICV over encrypted data makes it possible for the ICV to be okay, but the data to be meaningless.

Intuitively, you would do the ICV over cleartext, but there are significant advantages to computing it over encrypted text. If it is computed over encrypted data, then it allows rapid recognition that the packet does not pass the ICV. Such rapid recognition is paramount in thwarting DOS attacks. On the other hand, if the ICV is on cleartext, and then the frame is encrypted, then you have the cost of decryption prior to computing the ICV, which takes considerable time. If the ICV is over encrypted text, then you first compute the ICV, so you learn quickly if the frame is not authentic.

The principal issue involved in whether to encrypt before or after computing the ICV is the trade-off between the cost of computing the ICV value and the cost of decrypting. Since these vary for different algorithms, different Cipher Suites will differ in when they compute the ICV.

Placement: It is easier for implementation to place the ICV at the end of the frame for both transmission and reception. On transmission, if the ICV is placed at the end of the packet, it can be computed on the fly. On reception, if the ICV is at the end of the packet, it does not need to be stored during ICV computation.

Size: Some modes are susceptible to birthday attacks [delete ref. to birthday attacks] and some modes are not susceptible to such offline attacks. For example HMAC SHA1, as a digest, is subject to a birthday attack, because the ICV is in the clear, whereas CCM is not vulnerable to a birthday attack because the ICV is encrypted.

For a mode that is susceptible to an offline attack, the crypto strength is proportional to sqrt(2^n), where n is the number of bits in the ICV. A mode that is not susceptible to birthday attack has crypto strength proportional to 2^n. For a given level of security, the ICV for a susceptible mode needs to be twice as long as the ICV for a non-susceptible mode. In a birthday attack, the number of cases that need to be examined before finding a match is the square root of the number of states of the ICV.

Thus if we avoid modes susceptible to birthday attacks, the size of the ICV can be at least less than half the length for the same strength.

Another consideration with respect to the size of the ICV, is that it is difficult computationally to do a large number of guesses, 2^80, say. If a mode is not subject to offline attacks, it forces the attacker to launch an active attack, which is more likely to be detected.

The implication of this discussion is that we should choose modes that are not subject to birth attacks because then the ICV can be half as long. This is particularly an advantage for media technologies for whom the longer ICV uses up scarce bandwidth resources, e.g., wireless 802.11 and 802.16.

Z.6.7 Frame Expansion

Due to additional fields, frame expansion is required and needs to be considered by 802.3. Theoretically, there are 3 alternatives: expansion, fragmentation, MTU limitation. Practically, only expansion is acceptable. We are asking 802.3 for a larger frame size.

An alternative to fragmentation is to limit the MTU size, thereby forcing the higher layer protocol to fragment the packet. In the wireless domain this requirement is not an issue since such MTU limitation is normal. An MTU of any size is accepted at the MAC layer and is fragmented later. However some wired standards do not have a means of signaling MTU variation to the next higher layer.

The former IEEE 802.10 specification fragmented the packet into two when MTU adjustment was not supported. Fragmentation by the security protocol is not natural function for a security sublayer, should be done by media access control as media need and dictate.

It is felt that there is a need for a generic service to propagate MTU size upwards.