IEEE Standard for
Local and metropolitan area networks—

Media Access Control (MAC) Service Definition

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

IEEE Std 802.1AC™-2016
(Revision of
IEEE Std 802.1AC-2012)

IEEE Std 802.1AC™-2016
(Revision of
IEEE Std 802.1AC-2012)

IEEE Standard for
Local and metropolitan area networks—

Media Access Control (MAC) Service Definition

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 7 December 2016
IEEE-SA Standards Board

Recognized as an American National Standard

Abstract: The MAC Service and the Internal Sublayer Service (ISS) are defined in this standard. This standard specifies media-dependent convergence functions that map IEEE 802® MAC interfaces to the ISS. The MAC Service is derived from the ISS.

Keywords: IEEE 802, IEEE 802.1AC, Internal Sublayer Service, ISS, LAN, local area network, MAC Service, MAN, metropolitan area network

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

PDF: ISBN 978-1-5044-3697-7 STD22395
Print: ISBN 978-1-5044-3698-4 STDPD22395

Important Notices and Disclaimers Concerning IEEE Standards Documents

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

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

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

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

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

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

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

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

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

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

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

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

Errata

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

Patents

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

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

Participants

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

Glenn Parsons, *Chair*

John Messenger, *Vice Chair, Maintenance Task Group Chair, Editor*

SeoYoung Baek
Shenghua Bao
Jens Bierschenk
Steinar Bjornstad
Christian Boiger
Paul Bottorff
David Chen
Feng Chen
Weiying Cheng
Rodney Cummings
János Farkas
Norman Finn
Geoffrey Garner
Eric W. Gray
Craig Gunther
Marina Gutierrez
Stephen Haddock
Mark Hantel
Patrick Heffernan
Marc Holness
Lu Huang
Tony Jeffree
Michael Johas Teener
Hal Keen
Stephan Kehrer
Philippe Klein
Jouni Korhonen
Yizhou Li
Christophe Mangin
Tom McBeath
James McIntosh
Tero Mustala
Hiroki Nakano
Bob Noseworthy
Donald R. Pannell
Walter Pienciak
Michael Potts
Karen Randall
Maximilian Riegel
Dan Romascanu
Jessy V. Rouyer
Eero Ryytty
Soheil Samii
Behcet Sarikaya
Frank Schewe
Michael Seaman
Johannes Specht
Wilfried Steiner
Patricia Thaler
Paul Unbehagen
Hao Wang
Karl Weber
Brian Weis
Jordon Woods
Nader Zein
Helge Zinner
Juan Carlos Zuniga

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

Carlos Aldana
Thomas Alexander
Butch Anton
Lee Armstrong
Stefan Aust
Christian Boiger
Nancy Bravin
William Byrd
Juan Carreon
Minho Cheong
Keith Chow
Yezid Donoso
Janos Farkas
Michael Fischer
Yukihiro Fujimoto
Gregory Gillooly
Eric W. Gray
Randall Groves
Craig Gunther
Stephen Haddock
Marek Hajduczenia
Mark Hamilton
Jerome Henry
Marco Hernandez
Werner Hoelzl
Tetsushi Ikegami
Noriyuki Ikeuchi
Sergiu Iordanescu
Atsushi Ito
Tony Jeffree
Michael Johas Teener
Peter Jones
Shinkyo Kaku
Piotr Karocki
Stuart Kerry
Yongbum Kim
Tero Kivinen
Bruce Kraemer
Paul Lambert
James Lepp
Joseph Levy
Arthur H. Light
William Lumpkins
Elvis Maculuba
Syam Madanapalli
Roger Marks
Arthur Marris
Richard Mellitz
Jose Morales
Michael Newman
Nick S. A. Nikjoo
Satoshi Obara
Satoshi Oyama
Alon Regev
Robert Robinson
Jessy V. Rouyer
Richard Roy
Bartien Sayogo
Michael Seaman
Shusaku Shimada
Ju-Hyung Son
Kapil Sood
Thomas Starai
Adrian Stephens
Walter Struppler
Pedro Tonhozi de Oliveira
Mark-Rene Uchida
John Vergis
George Vlantis
Khurram Waheed
Karl Weber
Hung-Yu Wei
Natalie Wienckowski
Chun Yu Charles Wong
Tan Pek Yew
Oren Yuen
Zhen Zhou

When the IEEE-SA Standards Board approved this standard on 7 December 2016, it had the following membership:

Introduction

This introduction is not part of IEEE Std 802.1AC-2016, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Service Definition.

During the history of IEEE 802, several different MAC types have been developed, all of which have a core of functionality that is common to IEEE 802 MACs in general, but all of which also provide functionality that extends beyond that common core. An example can be found in the way priority information is conveyed in different MACs; some have no means of conveying priority, some can convey two different priority code points, some can convey eight priority code points.

While such differences are not an issue in a Local Area Network (LAN) that employs a single MAC technology, they can become an issue in LANs where more than one MAC technology is employed, for example in Bridged LANs. It was therefore important at an early stage of MAC Bridge development to develop a clear definition of the MAC Service that would facilitate the definition of a common Bridging technology that could apply to all MAC types.

The MAC Service definition was first standardized as ISO/IEC 15802-1:1995 [B3]. When the ISO/IEC standard reached its 5-year revision point, IEEE 802 was asked to take over the document and revise it to reflect changes since publication. This revision emphasizes the fundamental relayable nature of the MAC Service provided to end stations by defining it in terms of the service, common to bridges and end stations, previously documented as the Internal Sublayer Service (ISS) in IEEE Std 802.1D™. In addition to the material that was contained in ISO/IEC 15802-1, this standard documents the ISS that was originally defined in IEEE Std 802.1D. This standard contains state-of-the-art material. The area covered by this standard is undergoing evolution. Revisions are anticipated within the next few years to clarify existing material, to correct possible errors, and to incorporate new related material. Information on the current revision state of this and other IEEE 802 standards may be obtained from

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

Contents

Figures

Tables

IEEE Standard for
Local and metropolitan area networks—

Media Access Control (MAC) Service Definition

1. Scope

The scope of this standard is to define the Media Access Control (MAC) Service provided by all IEEE 802® MACs, and the Internal Sublayer Service (ISS) provided within MAC Bridges, in abstract terms of the following:

a) Their semantics, primitive actions, and events; and

b) The parameters of, interrelationship between, and valid sequences of these actions and events.

2. Normative references

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

IEEE Std 802®, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.[1, 2]

IEEE Std 802.1AX™, IEEE Standard for Local and Metropolitan Area Networks—Link Aggregation.

IEEE Std 802.1D™, IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Bridges.

IEEE Std 802.1Q™, IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks.

IEEE Std 802.3™, IEEE Standard for Ethernet.

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

IEEE Std 802.16™, IEEE Standard for Air Interface for Broadband Wireless Access Systems.

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

IEEE Std 802.20™, IEEE Standard for Local and metropolitan area networks—Part 20: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility—Physical and Media Access Control Layer Specification.

ISO/IEC 7498-1, Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model.[3]

ISO/IEC 7498-3, Information technology—Open Systems Interconnection—Basic Reference Model: Naming and addressing.

ISO/IEC 10731, Information technology—Open Systems Interconnection—Basic Reference Model—Conventions for the definition of OSI services.

[1]IEEE publications are available from The Institute of Electrical and Electronics Engineers (http://standards.ieee.org/).
[2]The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.
[3]ISO/IEC publications are available from the ISO Central Secretariat (http://www.iso.org/). ISO publications are also available in the United States from the American National Standards Institute (http://www.ansi.org/).

3. Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.[4]

3.1 Basic reference model definitions

Although the MAC Service is not identified or defined in the Open Systems Interconnection (OSI) Basic Reference Model, this standard is based on the concepts developed in the Basic Reference Model and makes use of the following terms defined in ISO/IEC 7498-1 and ISO/IEC 7498-3, as they might apply to the MAC sublayer:[5]

a) (N)-entity
b) (N)-service

3.2 Service conventions definitions

Although the MAC Service is not identified or defined in the OSI Basic Reference Model, this standard makes use of the following terms defined in ISO/IEC 10731, as they might apply to the MAC sublayer:

a) Service user
b) Service provider
c) Primitive
d) Request
e) Indication

---

[4] *IEEE Standards Dictionary Online* subscription is available at: http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html.
[5] Information on references can be found in Clause 2.

4. Acronyms and abbreviations

For the purposes of this standard, the following acronyms and abbreviations apply:

CPS	Common Part sublayer
CS	Convergence sublayer
EPD	EtherType Protocol Discrimination
ISS	Internal Sublayer Service
LAN	Local Area Network
LLC	Logical Link Control
LPD	LLC Protocol Discrimination
LSAP	Link Service Access Point
MAC	Media Access Control
MSAP	Media Access Control Service Access Point
MSDU	Media Access Control Service Data Unit
OSI	Open Systems Interconnection
PMPN	Point-to-Multipoint Network
QoS	quality of service
RPR	Resilient Packet Ring
SAP	Service Access Point

5. Conformance

This clause specifies the mandatory and optional capabilities provided by conformant implementations of this standard. An implementation can

a) Compose all or part of the functionality of a system.
b) Provide, as specified by this standard, one or more instances of the MAC Service to other functional entities whose specification is outside the scope of this standard.
c) Provide, as specified by this standard, one or more instances of the MAC Internal Sublayer Service (ISS) to other implementations or instances of the same implementation that conform to this standard.

Accordingly, this clause specifies conformance requirements for common systems and for functional components within systems, possibly connected to other system components with interfaces that are not otherwise accessible.

5.1 Translation between media using different protocol discrimination methods

When receiving frames from or transmitting frames on a medium that uses LLC Protocol Discrimination (LPD), a conformant implementation shall translate the Media Access Control Service Data Unit (MSDU) as specified in Clause 12.

5.2 Support of the ISS by different MAC procedures

Systems interfacing to a network employing a media type listed in Table 5-1 shall conform to the requirements of Clause 13, conform to the applicable standard, and implement the convergence function specified in the table.

Table 5-1—MAC procedure and convergence conformance

Media type	Applicable standard	Convergence function
IEEE 802.3 Ethernet	IEEE Std 802.3-2015	13.1
IEEE 802.11 Wireless LAN	IEEE Std 802.11-2012	13.2
IEEE 802.16 WirelessMAN	IEEE Std 802.16-2012	13.3
IEEE 802.17 Resilient Packet Ring	IEEE Std 802.17-2011	13.4
IEEE 802.20 Mobile Broadband Wireless Access	IEEE Std 802.20-2008	13.5

6. Conventions

6.1 General considerations

This standard uses the descriptive conventions given in ISO/IEC 10731.

The service model, service primitives, and time-sequence diagrams used are abstract descriptions; they do not represent a specification for implementation.

6.2 Parameters

Service primitives, used to represent service user/service provider interactions (ISO/IEC 10731), convey parameters that indicate information available in the user/provider interaction, and are conveyed to one or more peer service users or used by the service provider when conveying that information (see 7.2).

7. Basic architectural concepts and terms

The architectural concepts used in this and other IEEE 802.1 standards are based on the layered protocol model introduced by the OSI Basic Reference Model (ISO/IEC 7498-1) and used in the MAC Service Definition (this standard), in IEEE Std 802, in other IEEE 802 standards, and elsewhere in networking. IEEE 802.1 standards in particular have developed terms and distinctions useful in describing the MAC Service and its support by protocol entities within the MAC sublayer.[6]

7.1 Protocol entities, peers, layers, services, and clients

The fundamental notion of the model is that each protocol entity within a system is instantiated at one of a number of strictly ordered layers, and communicates with peer entities (operating the same or an interoperable protocol within the same layer) in other systems by using the service provided by interoperable protocol entities within the layer immediately below, and thus provides a service to protocol entities in the layer above. The implied repetitive stacking of protocol entities is essentially unbounded at the lowest level and is bounded at the highest level by an application supported by peer systems. In descriptions of the model, the relative layer positions of protocol entities and services are conventionally referred to by N, designating a numeric level. The (N)-service is provided by an (N)-entity that uses the (N-1)-service provided by the (N-1)-entity, while the (N)-service user is an (N+1)-entity. Figure 7-1 illustrates these concepts with reference to the MAC sublayer, which contains MAC entities that provide the MAC Service to MAC Service users.

7.2 Service interface primitives, parameters, and frames

Each (N)-service is described in terms of service primitives and their parameters, each primitive corresponding to an atomic interaction between the (N)-service user and the (N)-service provider, with each invocation of a primitive by a service user resulting in the service issuing corresponding primitives to peer service users. The purpose of the model is to provide a framework and requirements for the design of protocols while not unnecessarily constraining the internal design of systems; primitives and their parameters are limited to (but include all of) the information elements conveyed to corresponding peer protocol entities or required by other systems (and not supplied by protocols in lower layers) to identify (address) those entities and deliver the information. The parameters of service primitives do not include information that is used only locally (within the same system) e.g., to identify entities or organize resources.[7]

The primitives of the MAC Service comprise a data request and a corresponding data indication, each with MAC destination address, MAC source address, a MAC Service Data Unit (MSDU) comprising one or more octets of data, and priority parameters. Taken together these parameters are conveniently referred to as a *frame,* although this does not imply that they are physically encoded by a continuous signal on a communication medium, that no other fields are added or inserted by other protocol entities prior to transmission, or that the priority is always encoded with the other parameters transmitted.

[6]Drawing on prior network layer standards, including ISO/IEC 7498-1, wherever possible.

[7]These points are frequently misunderstood by those unfamiliar with the reference model, who take it as simply restating common sense principles of modular engineering. Early variants of the MAC Service, for example, omitted the source MAC address parameter on the grounds that it was a fixed property of the transmitting station and should be supplied by the MAC entity itself, despite the fact that communicating peer service users (and the protocols they operate) required that information. The introduction of MAC Bridges necessitated the development of a MAC ISS with the required parameter and has led to a restatement of the service definition included in a number of standards. However the source address parameter would still have been required even if MAC Bridges did not exist. Similarly, versions of the MAC Service have included local acknowledgment primitives or status return codes for primitives issued. These play no part in defining the peer-to-peer communication and do not conform to the reference model. The scope of some IEEE 802 standards does include the definition of interfaces, particularly electrical interfaces, within systems. These play a valuable role in defining components used to build those systems, but should not be confused with OSI service interfaces.

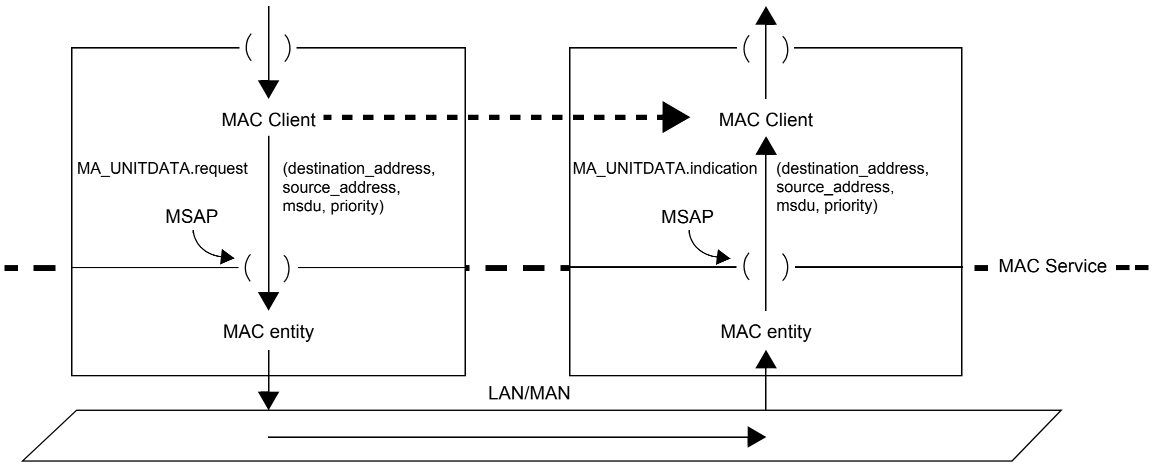

Figure 7-1—MAC entities, the MAC Service, and MAC Service users (clients)

7.3 Layer management interfaces

A given (N)-entity can have many associated management controls, counters, and status parameters that are not communicated to its user's peers and whose values are either not determined by its user or not required to change synchronously with the occurrence of individual (N)-service primitives to ensure successful (N+1)-protocol operation. Communication of the values of these parameters to and from local entities, i.e., within the same system, is modeled as occurring not through service primitives but through a layer management interface.[8] One protocol entity, for example a Simple Network Management Protocol (SNMP) entity, can be used to establish the operational parameters of another. Communication of the results of Fault Alarms to entities responsible for managing the network is one of the uses of layer management interfaces.

7.4 Service access points, interface stacks, and ports

Each service is provided to a single protocol entity at a Service Access Point (SAP) within a system. A given (N)-entity can support a number of N-SAPs and use one or more (N-1)-SAPs. The SAP serves to delineate the boundary between protocol specifications and to specify the externally observable relationship between entities operating those protocols. A SAP is an abstraction and does not necessarily correspond to any concrete realization within a system, but an (N)-entity often associates management counters with the SAP and provides status parameters that can be used by the (N+1)-entity using the SAP. Examples include the MAC_Operational and operPointToPointMAC status parameters (11.2, 11.3). Each SAP has an identifier with a value that is local to the system and uniquely identifies the SAP within the system.

The network layer and data link layer of the reference model accommodate many different real networks, subnetworks, and links with the requirements for bandwidth, multiplexing, security, and other aspects of communication differing from network to network.[9] A given service, e.g., the MAC Service, is often provided by a number of protocols, layered to achieve the desired result. Together the entities that support a

[8]This would require considerable enlargement and continuous modification of service interfaces, obscuring their original purpose, not to mention the creation of many additional interfaces and the addition of "pass-through" functions to others.

[9]The data link layer, as originally envisaged in the OSI reference model, contained no addressing and caused some involved in its development to reject the idea of LANs at the link layer. There is a sound argument for regarding LANs as simply subnetworks within the network layer, and in practice this is how they are treated. However this would have been unpalatable to many more people at a time when correspondence between LLC (ISO/IEC 8802-2:1998 [B2]) and high-level data link control (HDLC) was sought, together with the adoption of a unique network layer protocol [ITU-T X.25 (1996)]. Continuing to regard the MAC sublayer as part of the OSI Data Link Layer does relatively little harm (except when duplication of network layer functionality is proposed) and is convenient given the mass of historic documentation.

particular SAP compose an interface stack. Figure 7-2 provides an example, showing the use of Link Aggregation (IEEE Std 802.1AX).

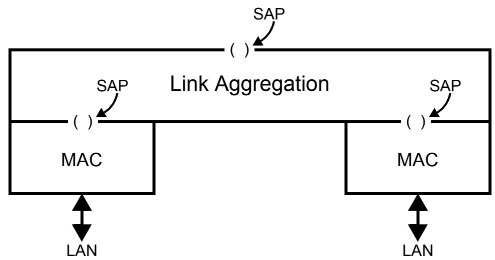

Figure 7-2—An interface stack

The term *port* is used to refer to the interface stack for a given SAP. Often the interface stack comprises a single protocol entity attached to a single Local Area Network (LAN), and port can be conveniently used to refer to several aspects of the interface stack, including the physical interface connector for example. In more complex situations—such as that in Figure 7-2, where the parts of the interface stack provided by the MAC entities effectively compose two ports that are then used by link aggregation to provide a single port to its user—the port has to be clearly specified in terms of the particular SAP supported.

7.5 MAC method independent protocols and shims

Some protocols, such as those specified in IEEE Std 802.3, IEEE Std 802.11, and other IEEE 802 standards, are specific to their LAN media or to the way access to that media is controlled. Other protocols and functions within the MAC sublayer, such as link aggregation and bridging, are MAC method independent—thus providing consistent management and interoperability across a range of media.

IEEE 802.1 standards use the term “shim” to refer to a protocol entity that provides the same service to its user as it uses from its provider. Shims can be inserted into an interface stack to provide functions such as aggregation (e.g., IEEE Std 802.1AX), security (e.g., IEEE Std 802.1AE™ [B1]), or multiplexing.

7.6 MAC Service clients

The protocol entity that uses the service provided at a Media Access Control Service Access Point (MSAP) is commonly referred to as the *client* of the MAC Service or of the entity providing the MAC Service. Within a Bridge, the MAC Relay Entity is a client of the Internal Sublayer Service (ISS), and a Logical Link Control (LLC) Entity is a client of the MAC Service. The LLC sublayer and protocol entities are described in IEEE Std 802 and provide~~s~~ protocol identification, multiplexing, and demultiplexing to and from a number of clients that use a common MSAP. The clients of LLC are also often referred to as *clients of the MAC*.

7.7 Stations and systems

A LAN station comprises a single media access method specific entity, operating the MAC procedures specified in the applicable IEEE 802 standard, together with other protocol entities mandated by those standards (e.g., an LLC Entity) or commonly used in conjunction with that entity.

A system is a collection of hardware and software components whose intercommunication is not directly externally observable and outside the scope of the IEEE 802 standards that specify the system behavior as a whole. Management of a system, when supported, is typically provided through a single management entity.

A system (such as a bridge) can contain many media access method specific entities, of the same or a variety of types, attached to different LANs. A system can therefore be said to include one or more LAN stations.

7.8 Connectionless connectivity

The MAC Service supported by an IEEE 802 LAN provides connectionless connectivity, i.e., communication between attached stations occurs without explicit prior agreement between service users. The potential connectivity offered by a connectionless service composes a connectivity association that is established prior to the exchange of service primitives between service users (see IETF RFC 787 [B4]). The way in which such a connectivity association is established depends on the particular protocols and resources that support it, and can be as simple as making a physical attachment to a wire. However simple or complex, the establishment of a connectivity association for connectionless data transfer involves only a two-party interaction between the service user and the service provider (though it can result in exchanges between service-providing entities in several systems) and not a three-party user-service-user interaction as is the case for connection-oriented communication. With the continual increase in the number of ways that IEEE 802 LAN connectivity can be supported, it is no longer useful to regard a LAN as a definite set of physical equipment. Instead, a LAN is defined by the connectivity association that exists between a set of MSAPs.[10]

[10]A LAN is thus defined in terms of its external observable behavior, not by an abstraction of its internal operation.

8. Overview of the MAC Service

The MAC Service provides a connectionless-mode service for the transparent transfer of data between MAC Service users. It makes invisible to these MAC Service users the way that supporting communications resources are used to achieve this transfer.

In particular, the MAC Service provides for the following:

a) Independence of the underlying MAC sublayer and Physical Layer—the MAC Service relieves MAC Service users from all concerns, with the exception of quality of service (QoS) considerations, regarding the MAC technology that is available.

b) Transparency of transferred information—the MAC Service provides for the transparent transfer of MAC Service user data. It does not restrict the content, format, or coding of the information, nor does it ever need to interpret its structure or meaning. It may however restrict the maximum number of octets of the MAC Service user data that can be supplied in a user/provider interaction.

c) Priority selection—the MAC Service makes available to MAC Service users a means to request the transfer of data at a specified priority.

d) Addressing—the MAC Service provides means for the MAC Service user to identify its MSAP and to specify the MSAP or MSAPs to which data is to be transferred. MAC address formats and encoding are specified in IEEE Std 802.

e) Connectionless data transfer—the MAC Service provides a means by which MSDUs of limited length are delimited and transparently transmitted from one source MSAP to one or more destination MSAPs in a single MAC Service access, without establishing or later releasing a connection.

9. Model of the MAC Service

Although the MAC Service is not identified or defined in the OSI Basic Reference Model, this standard uses the abstract model for a layer service defined in Clause 5 of ISO/IEC 10731:1994 as it might apply to the MAC sublayer. The model defines the interactions between the MAC Service users and the MAC Service provider that take place at the two MSAPs. Information is passed between the MAC Service user and the MAC Service provider by service primitives that convey parameters.

9.1 Model of a MAC connectionless-mode transmission

A defining characteristic of MAC Service connectionless-mode is a preexisting connectivity association amongst a set of MSAPs.

Only one type of object, the unitdata object, can be handed over to the MAC Service provider via an MSAP. In Figure 9-1, MAC Service User A represents the MAC Service user that passes objects to the MAC Service provider. MAC Service User B represents the MAC Service user that accepts objects from the MAC Service provider.

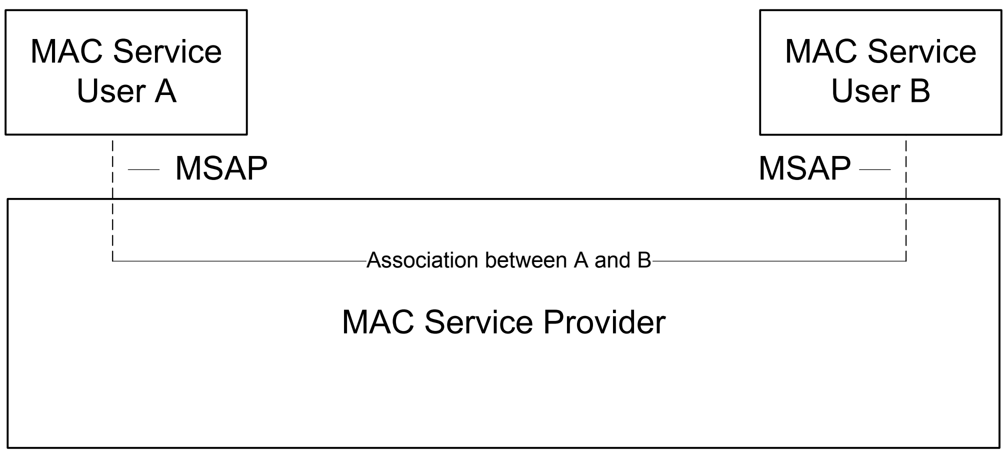

Figure 9-1—Model for a MAC Service connectionless-mode transmission

9.2 Service provided by the connectionless-mode MAC Service

In general, the MAC Service provider can perform any or all of the following actions:

— Discard objects
— Change the order of the objects

The MAC Service exhibits a negligible rate of the following:

— Object duplication
— Reordering of objects for a given priority

Awareness of the characteristics of the MAC Service provided, e.g., the rate at which objects can be discarded, duplicated, or misordered, is part of the MAC Service user's a priori knowledge of the environment.

10. Quality of connectionless-mode service

The term *quality of service* (QoS) refers to certain characteristics of a connectionless-mode transmission as observed between the MSAPs. QoS describes aspects of a connectionless-mode transmission that are solely attributable to the MAC Service provider; it can only be properly determined in the absence of MAC Service user behavior (which is beyond the control of the MAC Service provider) that specifically constrains or impedes the performance of the MAC Service.

Whether the QoS provided for each instance of the connectionless-mode transmission is the same for each MAC Service user depends on information concerning the nature of the service made available to the MAC Service user(s) by the MAC Service provider prior to the invocation of the service.

10.1 Determination of QoS for connectionless-mode service

A basic characteristic of a connectionless-mode service is that, unlike a connection-mode service, no specific association similar to that provided by a connection establishment is set up between the parties involved. Thus, characteristics of the service to be provided during the transfer are not negotiated between the MAC Service user and the MAC Service provider.

Associated with each MAC connectionless-mode transmission, certain measures of QoS are requested by the transmitting MAC Service user when the primitive action is initiated. The requested measures (or parameter values and options) are based on prior knowledge by the MAC Service user of the service(s) made available to it by the MAC Service provider. Knowledge of the characteristics and type of service provided (i.e., the parameters, formats, and options that affect the transfer of data) is made available to a MAC Service user through some layer management interaction prior to (any) invocation of the MAC connectionless-mode service. Thus, the MAC Service user not only has knowledge of the parties with which it may communicate, it also has explicit knowledge of the characteristics of the service it can expect for each invocation of the service.

10.2 Definition of connectionless-mode QoS parameters

QoS comprises the following:

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
i) Frame priority
j) Throughput

These parameters are discussed in detail in 6.5 of IEEE Std 802.1Q-2014.

11. Internal Sublayer Service

The Internal Sublayer Service (ISS) forms the basis of the MAC Service, providing elements necessary both to the performance of data transfer between MSAPs and the provision of MAC relay in IEEE 802.1D MAC Bridges and IEEE 802.1Q VLAN Bridges. Within an end-station, a subset of these elements provides the MAC Service specified in Clause 14. Within an IEEE 802.1Q VLAN Bridge, these elements are augmented to provide the Enhanced Internal Sublayer Service. The ISS excludes MAC-specific features and procedures whose operation is confined to an individual LAN.

11.1 Service primitives and parameters

The ISS is specified by two unit-data primitives, an M_UNITDATA.indication and an M_UNITDATA.request, together with the parameters of those primitives. Each M_UNITDATA indication corresponds to the receipt of an error-free MAC frame from a LAN. A data request primitive is invoked to transmit a frame to an individual LAN.

NOTE 1—Detailed specifications of error conditions in received frames are contained in the relevant MAC standards; for example, Frame Check Sequence (FCS) errors, length errors, and non-integral number of octets.[11]

```
M_UNITDATA.indication       (
                            destination_address,
                            source_address,
                            mac_service_data_unit,
                            priority,
                            drop_eligible,
                            frame_check_sequence,
                            service_access_point_identifier,
                            connection_identifier
                            )

M_UNITDATA.request          (
                            destination_address,
                            source_address,
                            mac_service_data_unit,
                            priority,
                            drop_eligible,
                            frame_check_sequence,
                            service_access_point_identifier,
                            connection_identifier
                            )
```

The destination_address parameter is the address of an individual MSAP or a group of MSAPs. If the local MSAP is designated by the destination address parameter of an M_UNITDATA.request primitive, the indication primitive is not also invoked by the MAC entity (see Clause 7) to the MAC Service user. For example, all frames transmitted to the broadcast address invoke M_UNITDATA.indication primitives at all MSAPs in the LAN except at the MSAP that generated the request.

NOTE 2—This non-reflective behavior is a change from that previously specified in ISO/IEC 15802-1 [B3], where an indication primitive was invoked by the MAC entity to the originating MAC Service user if the local MSAP was designated by the destination_address parameter. Consequently, if the former behavior is desired, it would be necessary to provide it locally. This change was made to bring the definition of the MAC Service into line with the requirements of

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

MAC bridging. In an underlying MAC whose natural behavior is for such local indications to be invoked, the MAC entity is the only point at which this reflection can be suppressed.

The source_address parameter is the individual address of the source MSAP.

The mac_service_data_unit parameter is the service user's data. This parameter allows the transmission of the MAC Service user data between MAC Service users, without modification by the MAC Service provider. The MAC Service user may transmit any integral number of octets greater than zero, up to a limit determined by the MAC Service provider. The value of this limit is made available to the MAC Service user by the use of management facilities or prior knowledge.

The default value of the priority parameter is 0. Values 1 through 7 form an ordered sequence of user_priorities, with 1 being the lowest value, 7 the highest, and 0 falling between 1 and 2. If the MAC Service user does not explicitly state a value for the priority parameter, or requests a value not supported by the provider, the MAC Service provider uses default values. The value of the priority parameter in the two primitives are related so that

a) In the request primitive, any defined value is allowed; and
b) In the indication primitive, the priority indicated is the value requested or as modified by the MAC Service provider.

The drop_eligible parameter provides guidance to the recipient of the service request or of an indication corresponding to the service request, and takes the values TRUE or FALSE. If drop_eligible is TRUE, the request can be discarded in preference to other requests in which drop_eligible is FALSE. The default drop_eligible value is FALSE.

The frame_check_sequence parameter is explicitly provided with the M_UNITDATA.indication so that it can be used in a related M_UNITDATA.request. The parameter comprises the Frame Check Sequence (FCS) value and sufficient information to determine whether the FCS value can be used. If the frame_check_sequence parameter is provided with an M_UNITDATA.request and the receiving and the transmitting service providers

1) Use the same algorithm to determine the FCS; and
2) Apply that algorithm to the same fields of the frame, i.e., the FCS coverage is the same; and
3) The data that is within the coverage of the FCS remains the same;

then the transmitting service provider uses the supplied FCS value.

NOTE 3—There are two possibilities for recreating a valid FCS. Annex F of IEEE Std 802.1D-2004 discusses these possibilities in more detail.

Unlike the other parameters of the service primitives, the service_access_point_identifier and connection_identifier are not parameters of the peer-to-peer service. The values of the service_access_point_identifier and connection_identifier are purely local to the system within which a given service request or service indication occurs, and are not conveyed to the communicating peer system. The values are opaque to the user of the ISS and are not manipulated by that service user, thus permitting independent operation of entities within the MAC sublayer as well as extending capabilities by the addition of protocol shims. The values are not conveyed in any external protocol, including management protocols; however, management protocols can convey externally visible data related to the SAP or connection. For example, there is a one-to-one association between service_access_point_identifier of a Bridge Port used by the MAC Relay Entity and the port number identifying that Bridge Port in management and control protocols.

The service_access_point_identifier parameter always identifies the SAP at which the service indication occurs or the service request is made, in the context of the receiving or transmitting system. In the common case of direct support of the ISS by a specific MAC procedure, it identifies the attached individual LAN. When a protocol entity in the interface stack either uses or supports multiple SAPs, the service_access_point_identifier parameter associates the service primitive with the appropriate SAP.

The connection_identifier can be null and is ignored by any specific MAC procedures except as explicitly specified in those procedures (see Clause 13). The connection_identifier is used where this standard specifically provides for efficient support of a single SAP by a number of connections, i.e., by dynamically created connectivity associations between peer entities. For example, a Provider Instance Port (6.10 of IEEE Std 802.1Q-2014) creates connections with peer Provider Instance Ports, and uses the connection_identifier to associate the backbone MAC address of the peer Provider Instance Port with Customer MAC Addresses that can be reached through that peer Provider Instance Port (26.4 of IEEE Std 802.1Q-2014). Following an M_UNITDATA.indication at a given SAP with a given source_address and connection_identifier, a subsequent M_UNITDATA.request at the same SAP with that source address as its destination_address and with the same connection_identifier will result in an M_UNITDATA.indication at the peer entity selected by the connection_identifier (in the absence of frame loss or reconfiguration of network components). The value of a connection_identifier is significant only at a single SAP. Any protocol entity in the interface stack that does not specify use of the connection_identifier assigns the connection_identifier value (if any) supplied with a request from the user of the protocol entity (or with an indication from the provider of the service used by the protocol entity) to the connection_identifier on associated requests made (or indications generated) by the protocol entity.

NOTE 4—The ISS specification in this standard omits the frame_type and access_priority parameters that are included in the ISS specification in IEEE Std 802.1D. The frame_type is not required as the receipt of a frame other than a user data frame does not cause a data indication, nor are such frames transmitted by the media independent bridge functions. The mapping of the ISS to particular access methods specified by this standard includes derivation of the access_priority parameter (for those media that require it) from the ISS priority parameter.

11.2 Status parameters

The ISS also makes available status parameters that reflect the operational state and administrative controls over each instance of the service provided.

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 the entity providing the service is capable of transmitting and receiving frames and its use is permitted by management, i.e., MAC_Enabled is also TRUE. Its value is otherwise FALSE. The value of this parameter is determined by the specific MAC procedures.

NOTE—These status parameters provide a common approach across MACs for handling the fact that

a) A MAC can inherently be working or not;

b) If the MAC is working, its operational state can be administratively overridden.

11.3 Point-to-point parameters

The ISS also makes available status parameters that reflect the point-to-point status of each instance of the service provided and provide 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 is always TRUE, regardless of any indications to the contrary generated by the service providing entity.
b) **ForceFalse**, operPointToPointMAC is always FALSE.
c) **Auto**, operPointToPointMAC is determined by the service providing entity.

The value of operPointToPointMAC is determined dynamically; i.e., it is reevaluated whenever adminPointToPointMAC or the status of the service providing entity changes.

11.4 Control primitives and parameters

The ISS provides two control primitives, an M_CONTROL.request and an M_CONTROL.indication, and their associated parameters.

NOTE—These control primitives are used in IEEE Std 802.1Q in order to support Priority-Based Flow Control (5.11 and Clause 36 of IEEE Std 802.1Q-2014).

The M_CONTROL.request primitive has the following form:

```
M_CONTROL.request            (
                             destination_address,
                             opcode,
                             request_operand_list
                             )
```

The M_CONTROL.indication primitive has the following form:

```
M_CONTROL.indication         (
                             opcode,
                             indication_operand_list
                             )
```

12. Protocol discrimination and media

As described in Clause 9 of IEEE Std 802-2014, some media (e.g., IEEE 802.11) employ LLC Protocol Discrimination (LPD) and some media (e.g., IEEE 802.3) employ EtherType Protocol Discrimination (EPD) as the primary means for identifying the protocol that defines the format of the data parameter in their service definitions corresponding to the ISS's mac_service_data_unit parameter. On LPD media, the first three or four octets of the data are the destination and source Link Service Access Point (LSAP) identifiers and one or two Control octets that together identify the protocol. On EPD media, either the first two octets are the length of the user data in the frame, which is then followed by a three- or four-octet LLC that identifies the protocol, or the first two octets are an EtherType that identifies the protocol.

Since the ISS is Length/Type encoded, a Media Access Method Dependent convergence function (see Clause 13) for a medium employing EPD need not transform the mac_service_data_unit parameter when mapping to or from the ISS. A Media Access Method Dependent convergence function for a medium employing LPD shall perform the transformations specified in the following subclauses.

12.1 M_UNITDATA.request data transformation for LPD media

The following procedure shall be used to convert an ISS mac_service_data_unit parameter, which is Length/Type encoded, to the data parameter of a MAC employing LPD:

a) If the value of the first two octets of the mac_service_data_unit, treated as a 16-bit binary integer (with the first octet being the most significant), is in the range hexadecimal 0000–05DC (decimal 0–1500) inclusive, then they constitute a Length field. In that case:
   1) The Length field is removed from the mac_service_data_unit, reducing its size by 2 octets;
   2) If the value of the (removed) Length field is less than the number of octets remaining in the mac_service_data_unit, then the mac_service_data_unit is further truncated, from its last octets, to the length in the Length field.
b) Otherwise, if the value of the first two octets of the mac_service_data_unit (as above) is equal to the LLC encapsulation EtherType (Table 12-2), then those two octets are removed from the mac_service_data_unit.
c) Otherwise, if the value of the first two octets of the mac_service_data_unit (as above) is in the range hexadecimal 0600–FFFF (decimal 1536–65535) inclusive, then they constitute an EtherType. In that case, the six octets hexadecimal AA-AA-03-00-00-00 are inserted into the mac_service_data_unit before that EtherType, increasing its length by six octets.
d) This standard does not specify the behavior when the value of the first two octets of the mac_service_data_unit (as above) is in the range hexadecimal 05DD–05FF (decimal 1501–1535) inclusive.

12.2 M_UNITDATA.indication data transformation for LPD media

The following procedure shall be used to convert the data parameter of a data indication from a MAC employing LPD to an ISS mac_service_data_unit parameter, which is Length/Type encoded:

a) If the first six octets of the data parameter are hexadecimal AA-AA-03-00-00-00, then those six octets are removed from the data parameter to form the mac_service_data_unit, thus reducing its size by 6 octets.
b) Otherwise, if the length of the data parameter is in the range hexadecimal 0000–05DC (decimal 0–1500) inclusive, then that length is prepended to the data as a 16-bit binary integer (with the first octet being the most significant), to form the ISS mac_service_data_unit.
c) Otherwise, the LLC encapsulation EtherType shown in Table 12-2 is prepended to the data parameter to form the ISS mac_service_data_unit.

Table 12-2—LLC encapsulation EtherType

Assignment	Value
LLC encapsulation EtherType	C9-D1

NOTE—Without the LLC encapsulation EtherType, the Length of an indication with more than 1500 octets of data might be, and of an indication with more than 1536 octets would be, mistaken for an EtherType.

12.3 Tags in end stations

The result of the conversions specified in 12.1 and 12.2, when applied consistently by IEEE 802.1Q bridges, is that the mac_service_data_unit parameters are identical for the service interfaces of MACs employing both LPD and EPD, except for the encoding of the outermost tag (or the user data, if no tag is present). The outermost tag (or the user data, if no tag is present) is LPD encoded on LPD media and Length/Type encoded on EPD media, and all subsequent tags (and the user data, if there is at least one tag) are Length/Type encoded.

For this reason, end stations transmitting a tagged frame on LPD media shall encode only the outermost tag using LPD, and use Length/Type encoding for all subsequent tags and the user data. End stations transmitting an untagged frame on LPD media shall encode the user data using LPD.

13. Support of the Internal Sublayer Service by specific MAC procedures

This clause specifies Media Access Method Dependent convergence functions supporting the ISS using MAC Entities that use specific IEEE 802 media access methods, including the mapping to the MAC protocol and procedures for each access method, and the encoding of the parameters of the service in MAC frames. The mapping is specified by reference to the IEEE 802 standards that specify each access method. The mapping draws attention to any special responsibilities of Bridges attached to LANs of that type. MAC control frames, typically frames that control some aspect of the operation of the MAC, i.e., frames that do not convey MAC user data, do not give rise to ISS data indications and are therefore not forwarded by a Bridge to any LAN other than that on which they originated.

Each MAC entity examines all frames received on the LAN to which it is attached. All error-free received user data frames give rise to M_UNITDATA indication primitives. A frame that is in error, as defined by the relevant MAC specification, is discarded by the MAC entity without giving rise to any M_UNITDATA indication.

The mac_service_data_unit shall be Length/Type encoded, meaning that its first two octets contain either the number of octets of service user data in the mac_service_data_unit (and are immediately followed by an LLC protocol identifier), or an EtherType.

13.1 Ethernet convergence function

The Ethernet convergence function presents a single instance of the ISS to upper layers, and uses a single instance of the IEEE 802.3 MAC Service as defined in 2.3 of IEEE Std 802.3-2015.

When the convergence function receives an M_UNITDATA.request primitive, it generates a corresponding MA_DATA.request to the underlying MAC Service as follows:

— The destination_address and source_address parameters are passed unaltered.

— The mac_service_data_unit is processed as follows. IEEE Std 802.3 requires that transmitted frames have a 64-octet minimum length (3.2.8 of IEEE Std 802.3-2015), including the destination_address, source_address, mac_service_data_unit, and frame_check_sequence. The implementation is permitted to add pad octets to the mac_service_data_unit to meet the minimum length requirement, or padding may be left to the IEEE 802.3 MAC. If the mac_service_data_unit begins with an IEEE 802.1Q VLAN tag, the implementation is permitted to add pad octets to the mac_service_data_unit to bring the frame to a total length of up to 68 octets.

  NOTE—The purpose of this flexibility is to permit, but not require, an IEEE 802.1Q bridge to remove and/or alter pad octets rendered unnecessary when it adds a VLAN tag to a minimum-length frame.

— If a frame_check_sequence is included in the M_UNITDATA.request primitive, its value is adjusted to include any added padding (Annex G of IEEE Std 802.1Q-2014).

— The priority, drop_eligible, service_access_point_identifier, and connection_identifier parameters are ignored.

When the convergence function receives an MA_DATA.indication primitive from the underlying MAC Service, it generates a corresponding M_UNITDATA.indication as follows:

— The destination_address, source_address, mac_service_data_unit, and frame_check_sequence parameters are passed unaltered.

— The drop_eligible parameter of the M_UNITDATA.indication is FALSE.

— The priority parameter of the M_UNITDATA.indication shall take the value of the Default Priority parameter for the SAP on which the MA_DATA.indication was received. The default value of this parameter is 0. This parameter may be set by management in which case the capability to set it to any of the values 0 through 7 shall be provided.

The number of octets of data in the mac_service_data_unit parameter is either one of the following:

— Encoded in the Length/Type field of the MAC frame if the frame makes use of the Length interpretation of the Length/Type field (3.2.6 of IEEE Std 802.3-2015), or
— Determined from the length of the received MAC frame, if the frame makes use of the Type interpretation of the Length/Type field (3.2.6 of IEEE Std 802.3-2015).

The value of MAC_Enabled is always TRUE. The value of MAC_Operational is TRUE if there is an indication from the underlying medium that it is available, and FALSE otherwise. This indication is dependent on the type of the physical layer but is indicated in the aMediaAvailable managed object (see 30.5.1.1.4 of IEEE Std 802.3-2015).

From the point of view of determining the value of operPointToPointMAC (11.3), the MAC is considered to be connected to a point-to-point LAN if any of the following conditions are true:

— The MAC entity concerned supports auto negotiation (e.g., Clause 28, Clause 37, and Clause 73 of IEEE Std 802.3-2015), and the auto negotiation function has determined that the LAN is to be operated in full duplex mode; or
— The MAC entity has been configured by management means for full duplex operation.

Otherwise, the MAC is considered to be connected to a LAN that is not point-to-point.

On receipt of an M_CONTROL.request primitive, an IEEE 802.3 MA_CONTROL.request primitive is generated having the same parameters. On receipt of an IEEE 802.3 MA_CONTROL.indication primitive, an M_CONTROL.indication primitive is generated having the same parameters.

13.2 Wireless LAN convergence function

The wireless LAN access method is specified in IEEE Std 802.11-2012. Subclause 5.2 of that standard specifies the IEEE 802.11 MAC data service definition, 4.3.4 introduces the distribution system, and Clause 4 and Clause 5 specify the points in the IEEE 802.11 architecture at which the MAC Service is offered. The Media Access Method Dependent convergence functions used with IEEE Std 802.11 are as follows:

a) The IEEE 802.11 portal convergence function (13.2.1) supports an IEEE 802.11 portal, offers an instance of the ISS to the upper layers, and uses an instance of the Distribution Service SAP (DS SAP) offered by an IEEE 802.11 distribution system. The distribution system in turn provides connectivity to some number of IEEE 802.11 access points and IEEE 802.11 mesh gates, and via those, to some number of associated IEEE 802.11 non-AP stations (13.2.1).
b) The IEEE 802.11 station convergence function (13.2.3) offers an instance of the ISS to the upper layers, and uses an instance of the IEEE 802.11 MAC Service interface offered by an IEEE 802.11 non-AP STA, mesh STA, IBSS STA or DMG STSA.

NOTE—The native MAC Service provided by an IEEE 802.11 STA (9.2.8 of IEEE Std 802.11-2012) cannot be adapted to the ISS by a Media Access Method Dependent convergence function, because frames with a destination address that is a group address are reflected back to the station. This behavior is prohibited for an ISS (11.1).

All of the convergence functions defined in this clause use the same mapping of ISS parameters to and from IEEE 802.11 service instance primitives. This parameter mapping is defined in 13.2.4.

13.2.1 IEEE 802.11 portal convergence function

As shown in Figure 13-1, the IEEE 802.11 portal convergence function offers an instance of the ISS to upper layers, connecting to an IEEE 802.11 distribution system through an instance of the DS SAP interface defined in Annex R of IEEE Std 802.11-2012. An IEEE 802.11 non-AP infrastructure station is associated to the distribution system via an IEEE 802.11 access point. An IEEE 802.11 mesh station can be associated to the distribution system via one or more IEEE 802.11 mesh gates. For a description of the IEEE 802.11 architecture, see Clause 4 of IEEE Std 802.11-2012. The IEEE 802.11 portal convergence function, together with the upper layers to which it offers a service via the ISS, constitute one architecture for an IEEE 802.11 portal.

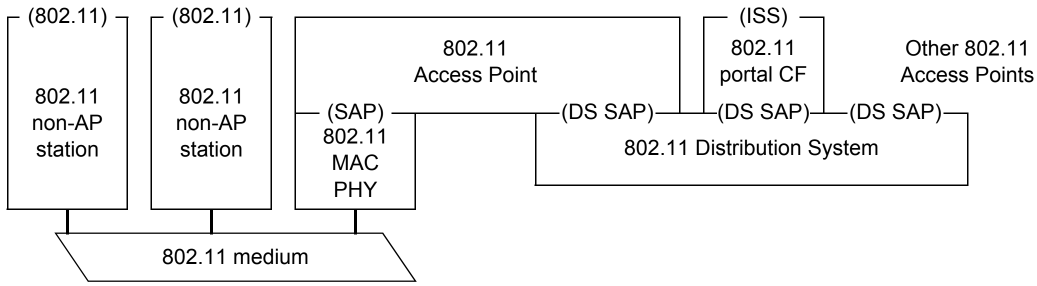

Figure 13-1—IEEE 802.11 portal convergence function method

The DS SAP offers the DS-UNITDATA.request and DS-UNITDATA.indication primitives, defined in Annex R of IEEE Std 802.11-2012. The "data" parameter of the request and indication use LPD. This convergence function uses the translation functions described in Clause 12 to supply the integration function required by Q.6 of IEEE Std 802.11-2012. The IEEE 802.11 portal convergence function makes no use of the DS-STA-NOTIFY.request primitive offered by the DS SAP.

When an M_UNITDATA.request primitive is received, the IEEE 802.11 portal convergence function generates a corresponding IEEE 802.11 DS-UNITDATA.request as described in 13.2.4.1.

When an IEEE 802.11 DS-UNITDATA.indication primitive is received, the IEEE 802.11 portal convergence function generates a corresponding M_UNITDATA.indication as described in 13.2.4.2.

NOTE—As shown in Figure 13-1, this convergence function does not supply the Controlled and Uncontrolled Ports of the IEEE 802.11 Security architecture (13.2.2). This is because the DS SAP is a service offered by the IEEE 802.11 distribution system, not the IEEE 802.11 MAC/PHY.

The MAC_Operational status parameter (11.2) is TRUE if the MAC_Enabled parameter is TRUE; otherwise MAC_Operational is FALSE.

If the adminPointToPointMAC parameter has the value Auto (11.3), then the operPointToPointMAC parameter for any ISS offered by the IEEE 802.11 portal convergence function is FALSE.

13.2.2 IEEE 802.11 Security architecture

The IEEE 802.1AE Security Entity (SecY) is illustrated in Figure 13-2, which is a simplified version of Figure 10-1 of IEEE Std 802.1AE-2006. The SecY provides two instances of the ISS to the layers above it, and utilizes a single instance of the ISS to access the layers below it. The two ISS instances above the SecY are the Controlled Port (C) and the Uncontrolled Port (U). The Controlled Port can supply cryptologically secured MAC Service, and the Uncontrolled Port supplies unsecured MAC Service.

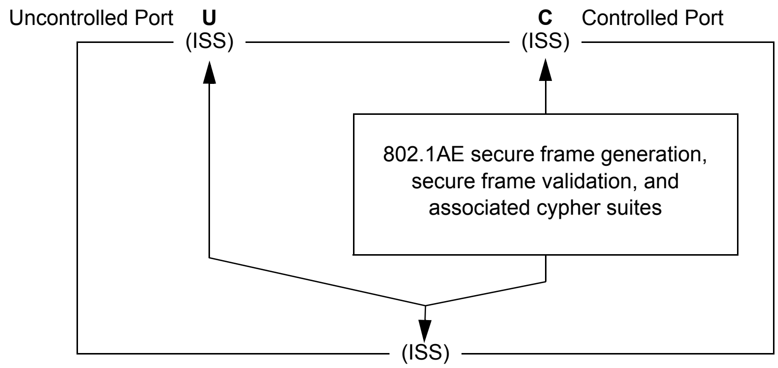

Figure 13-2—Simplified IEEE 802.1AE SecY

The SecY is used on some IEEE 802 media, including IEEE 802.3, but not including IEEE 802.11, in the manner illustrated in part 1 of Figure 13-3. IEEE 802.11, however, necessarily places its security layer, with Controlled and Uncontrolled ports similar to those of the IEEE 802.1AE SecY, below the IEEE 802.11 SAP. This is because IEEE 802.11 systems protect fragments of frames, not whole frames, and those segments are created or assembled in layers between the SAP and the security layer. Therefore, the IEEE 802.1AE SecY is not typically used on IEEE 802.11 media.

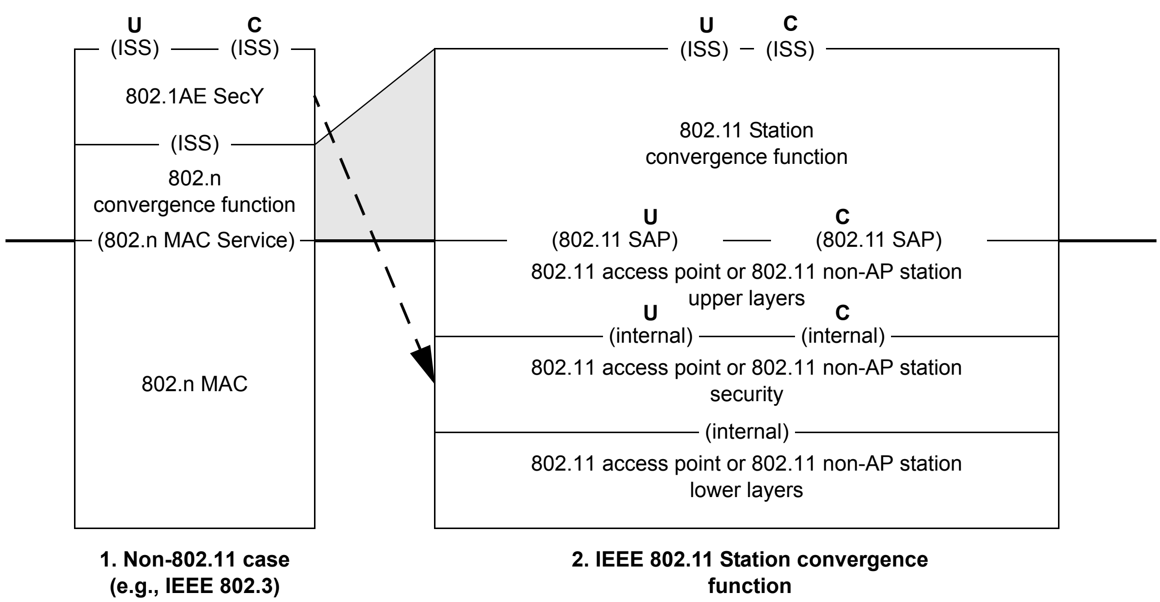

Figure 13-3—IEEE 802.11 Security architecture

13.2.3 IEEE 802.11 station convergence function

This convergence function offers an instance of the ISS to the upper layers, and uses an instance of the MA-UNITDATA service offered by an underlying IEEE 802.11 station. In order to use the IEEE 802.11 security layer, but provide the same services to the upper layers for IEEE 802.11 media that are provided by the SecY for other media, this convergence function provides an Uncontrolled Port and a Controlled Port, each mapped to their equivalents at the service offered by the IEEE 802.11 station.

When an M_UNITDATA.request primitive is received, the IEEE 802.11 parameter mapping generates a corresponding IEEE 802.11 MA-UNITDATA.request as described in 13.2.4.1.

When an IEEE 802.11 MA-UNITDATA.indication primitive is received, the IEEE 802.11 parameter mapping generates a corresponding M_UNITDATA.indication as described in 13.2.4.2.

13.2.4 IEEE 802.11 parameter mapping

13.2.4.1 IEEE 802.11 parameter mapping (requests)

When an M_UNITDATA.request primitive is received, the IEEE 802.11 convergence function (13.2.1 or 13.2.3) generates a corresponding IEEE 802.11 MA-UNITDATA.request or IEEE 802.11 DS-UNITDATA.request as follows:

a) The destination_address, source_address, and priority parameters are passed unaltered as the destination address, source address and priority, respectively.
b) The M_UNITDATA mac_service_data_unit parameter is translated as specified in 12.1 and passed as the MA-UNITDATA or DS-UNITDATA data parameter.
c) The ISS M_UNITDATA drop_eligible, frame_check_sequence, service_access_point_identifier, and connection_identifier parameters are ignored.

   NOTE—Drop eligibility is a capability defined in IEEE Std 802.11aa. However, it is not represented in the MA-UNITDATA service interfaces.

d) The IEEE 802.11 MA-UNITDATA or DS-UNITDATA routing information parameter is null.
e) The value of the IEEE 802.11 MA-UNITDATA or DS-UNITDATA service class parameter is QoSAck.

13.2.4.2 IEEE 802.11 parameter mapping (indications)

When an IEEE 802.11 MA-UNITDATA.indication or DS-UNITDATA.indication primitive is received, the IEEE 802.11 convergence function (13.2.1 or 13.2.3) generates a corresponding M_UNITDATA.indication as follows:

a) The destination address, source address, and priority parameters are passed unaltered as the destination_address, source_address, and priority parameters, respectively.
b) The MA-UNITDATA or DS-UNITDATA data parameter is translated as specified in 12.2 and passed as the mac_service_data_unit parameter.
c) The drop_eligible parameter is FALSE.
d) The frame_check_sequence, service_access_point_identifier, and connection_identifier parameters are null.
e) The MA-UNITDATA or DS-UNITDATA routing information, reception status, and service class parameters are ignored.

13.3 WirelessMAN convergence function

The WirelessMAN MAC access method is specified in IEEE Std 802.16-2012. Clause 5 of that standard addresses the Service-Specific Convergence sublayer (CS) that implements the MAC Service, including multiple service-specific convergence specifications. Subclause 5.2.4, specifying the IEEE 802.3/Ethernet-specific part of the Packet CS specification, describes the IEEE 802.3/Ethernet CS Mode. The IEEE 802.3/ Ethernet CS Mode supports the ISS. Subclause 5.2.5 (the IP specific part of the Packet CS specification) does not support the ISS.

Clause 6 of IEEE Std 802.16-2012 specifies the MAC Common Part sublayer (MAC CPS) transmission and reception procedures and Annex C describes the MAC CPS service definition.

IEEE Std 802.16 includes no explicit definition of the MAC Service definition for the IEEE 802.3/Ethernet CS Mode. The IEEE 802.3/Ethernet CS Mode MAC Service is defined in Clause 2 of IEEE Std 802.3-2015.

The IEEE 802.16 MAC CPS presents a connection-oriented MAC Service. The IEEE 802.3/Ethernet CS Mode utilizes this service to present the IEEE 802.3/Ethernet service. A pair of communicating peer CS entities between an IEEE 802.16 BS and an IEEE 802.16 SS create a point-to-point LAN as specified in 11.3.

Since the IEEE 802.3/Ethernet CS Mode does not forward the frame_check_sequence parameter of the M_UNITDATA.indication, then

a) Any service flow using this MAC CS shall enable the IEEE 802.16 MAC CRC.
b) PHS validation shall not be turned off for this service flow (since IEEE 802.16 MAC CRC cannot protect suppressed MAC header fields).

13.3.1 Support for Internal Sublayer Service under IEEE Std 802.16 and IEEE 802.3/Ethernet CS Mode

The destination_address, source_address, priority, drop_eligible, and mac_service_data_unit parameters of the M_UNITDATA primitives are encoded as described in 13.1.

The value of operPointToPointMAC (11.3) shall be TRUE.

The value of MAC_Enabled shall be determined by the procedure described in 11.2.

After the IEEE 802.16 SS has registered with the BS, authenticated, and performed capabilities negotiation, and after the IEEE 802.3/Ethernet CS Mode has established the active MAC CPS service flows necessary to carry IEEE 802 frames, then the value of the MAC_Operational parameter shall be determined by the procedure described in 11.2. Beforehand, the value of MAC_Operational shall be FALSE.

Frame size limits are determined by IEEE Std 802.3.

13.4 Resilient Packet Ring convergence function

The Resilient Packet Ring (RPR) MAC access method is specified in IEEE Std 802.17-2011. Clause 6 of that standard specifies the MAC Service interface and reference model. Clause 7 specifies the MAC transmission and reception procedures. Clause 9 specifies the MAC frame structure.

On receipt of an M_UNITDATA.request primitive, the local MAC entity performs transmit data encapsulation, which assembles a MAC frame (Clause 9 of IEEE Std 802.17-2011) with the parameters supplied as specified in the paragraphs that follow.

On receipt of a valid MAC frame (Clause 9 of IEEE Std 802.17-2011), an M_UNITDATA.indication primitive is generated, with parameter values derived from the frame fields as specified in the paragraphs that follow.

The destination_address parameter is encoded in the *da* field of the MAC frame (9.2.2.3 of IEEE Std 802.17-2011). For request primitives from a client (e.g., MAC Relay Entity) where the source_address parameter does not equal the MAC's address, the destination_address parameter is encoded in both the *da* and the *daExtended* fields of the MAC frame (9.2.2.8 of IEEE Std 802.17-2011).

The source_address parameter is encoded in the *sa* field of the MAC frame (9.2.2.4 of IEEE Std 802.17-2011) when supplied in the request primitive and when the source_address is equal to the MAC's address. When the source_address is supplied in the request primitive, and when the source_address is not equal to the MAC's address, then the source_address is encoded in the *saExtended* field of the MAC frame (9.2.2.9 of IEEE Std 802.17-2011).

The mac_service_data_unit parameter is the service user data that includes the protocol type and is encoded in the *protocolType* and *serviceDataUnit* fields of the MAC frame (9.2.2.10 and 9.2.2.11 of IEEE Std 802.17-2011).

The priority parameter provided in the data request primitive is encoded into the service class (*sc*) subfield of the *baseControl* field (9.6.4 of IEEE Std 802.17-2011) of the MAC frame. This encoding is done in accordance with the priority to MAC Service class mapping shown in Table 13-1.

Table 13-1—Priority to MAC Service class mapping

Priority	MAC Service class
0	classC
1	classC
2	classC
3	classC
4	classB
5	classB
6	classA
7	classA

In the case of the indication primitive, the priority parameter is directly derived from the *sc* subfield of the *baseControl* field of the MAC frame. The mapping between the service class and the priority parameter of the indication primitive is provided in Table 13-2.

Table 13-2—MAC Service class to priority mapping

MAC Service class	Priority
classC	0
classB	4
classA	6

The frame_check_sequence parameter found in the data request primitive is encoded in the *fcs* field of the MAC frame (9.2.2.12 of IEEE Std 802.17-2011). The *fcs* is calculated as a 32-bit CRC starting from the first byte following the header checksum field (*hec*) (9.2.2.7 of IEEE Std 802.17-2011) to the end of the payload (9.2.2.11 of IEEE Std 802.17-2011) in accordance with E.2 of IEEE Std 802.17-2011. If an M_UNITDATA.request primitive is not accompanied by this parameter, it is calculated in accordance with E.2 of IEEE Std 802.17-2011.

No special action, above that specified in IEEE Std 802.17-2011, is required for the support of the MAC ISS by the RPR access method.

The IEEE 802.17 MAC Service interface supports a number of optional parameters that are specific to the IEEE 802.17 MAC. These parameters take on default values in M_UNITDATA.request primitive during transmission, and they are ignored by the MAC Relay on reception. The default values and procedures for handling RPR specific parameters are defined in 6.4.1, Clause 7, and F.3.1 of IEEE Std 802.17-2011.

13.5 Mobile Broadband Wireless Access Method convergence function

13.5.1 Support by Wideband Mode of IEEE Std 802.20-2008 (MBWA)

The Mobile Broadband Wireless Access Method for the IEEE 802.20 Wideband Mode is specified in 5.4 and Clause 6 through Clause 17 of IEEE Std 802.20-2008. Clause 8 of the standard specifies the Wideband Mode Lower MAC Layer Frame structure and protocol procedures. Clause 7 specifies the Radio Link Sublayer protocol, and Clause 6 defines the Services sublayer of the Wideband Mode. Clause 11 defines the Connection Control Plane that controls the state of the air-link by managing the states of individual Lower MAC Layer protocols, and by providing individual Lower MAC Layer protocols with operating parameters.

The Basic Packet Consolidation Protocol (8.2 of IEEE Std 802.20-2008) provides packet consolidation on the transmit side and provides packet de-multiplexing on the receive side. It provides an interface for the Radio Link sublayer to transport user information from the Services sublayer.

For packets to be transmitted over the air interface (wireless medium) from either the Access Node (AN) or Access Terminal (AT), the Lower MAC sublayer shall accept Radio Link sublayer data and control packets and shall generate Lower MAC sublayer control packets of its own. For packets leaving the air interface (wireless medium) for the AN or AT, the Lower MAC sublayer shall de-multiplex the received packets and shall deliver the payload to the Radio Link sublayer. The Radio Link sublayer shall deliver the payload to the Services sublayer, which includes support for different IEEE 802.3 frame-based protocols.

13.5.1.1 Support for Internal Sublayer Service under Wideband Mode of IEEE Std 802.20

The destination_address, source_address, mac_service_data_unit, and priority parameters of the M_UNITDATA primitive are encoded as described in 11.1.

The value of operPointToPointMAC (11.3) shall be TRUE.

The value of MAC_Enabled shall be determined by the procedure described in 11.2.

After the IEEE 802.20 AT has registered with the AN, authenticated, and performed capabilities negotiation, and after the stream is established to carry IEEE 802 frames, then the value of the MAC_Operational parameter shall be determined by the procedure described in 11.2. Beforehand, the value of MAC_Operational shall be FALSE.

Frame size limits are determined by IEEE Std 802.3.

13.5.2 Support by 625k-MC mode of IEEE Std 802.20-2008 (MBWA)

The Mobile Broadband Wireless Access Method for 625k-MC mode is specified in 5.5, Clause 18 through Clause 31, and Annex A of IEEE Std 802.20-2008. Clause 19 of the standard specifies 625k-MC Mode MAC Frame structure. Clause 23 specifies the MAC Protocol Sublayer function to implement the 625k-MC mode MAC Service. Clause 25 specifies the L3 protocol, and Clause 26 defines all the primitives used in 625k-MC Mode.

The L3 protocol layer is made up of components with distinct roles in supporting a connection across the air interface. The L3 Connection Management (CM) module provides an application level interface to the higher layer. The L3 protocol creates logical connections to transport the higher layer L4 data packets. The L3 Registration Management (RM) module takes the L4 data packets provided by the higher layer (through L3 CM) and converts them into a form that can be sent over the air interface. On the receiving side, L3 RM converts packets received from the air interface back into network packets before giving them to L3 CM.

Clause 26 defines the higher layer to L3 CM Interface Primitives for the SAP that shall be provided by L3 CM for the use of the higher layer. Clause 26 defines L3 CM to L4 Interface Primitives for the SAP provided by the higher layer for the use of L3 CM.

For packets entering air interface (wireless medium) from either base station (BS) network or End User Device (EUD), L3 shall accept L4 data and L4 control packets and shall generate L3 control packets of its own, and shall then send them to L2 RLC. For packets leaving air interface (wireless medium) for BS network or EUD, L3 shall accept byte streams from L2 RLC, shall determine whether the packet is a data packet, an L3 control packet, or an L4 control packet, and shall route the L4 control and data packets to the higher layer.

13.5.2.1 Support for ISS under 625k-MC mode of IEEE Std 802.20-2008

The destination_address, source_address, mac_service_data_unit, and priority parameters of the M_UNITDATA primitive are encoded as described in 11.1 and presented as an ISS-supported IEEE 802.3 MAC to the higher layer. The higher layer triggers the L3 protocol of 625k-MC. The L3 CM module state machine shall respond to requests from the higher layer for virtual connections across the air interface and requests registrations from the L3 RM to allow the virtual connections to use physical channels (streams).

The value of operPointToPointMAC (11.3) shall be TRUE.

The value of MAC_Enabled shall be determined by the procedure described in 11.2.

Initially, the value of MAC_Operational shall be FALSE. After the user terminal (UT) has registered with the BS, authenticated, and performed capabilities negotiation, and after the stream is established to carry IEEE 802 frames, then the value of the MAC_Operational parameter shall be determined by the procedure described in 11.2. Frame size limits are determined by IEEE Std 802.3.

13.6 Point-to-Multipoint Network convergence function

13.6.1 Point-to-Multipoint Networks

A Point-to-Multipoint Network (PMPN) is a time-division multiplexed-access network that supports two types of transmissions—unicast transmission for node-to-node transmission and multicast/broadcast transmission for one-node-to-other/all-nodes transmission. Each node-to-node link has its own bandwidth characteristics that could change over time.

A PMPN is physically a shared network, in that a PMPN node has a single physical port connected to the half-duplex medium, but is also a logically fully-connected one-hop mesh network, in that every node could transmit to every other node using its own link profile over the medium.

In order to easily adapt a PMPN to the large number of existing networking technologies that are optimized for networks consisting of point-to-point LANs, the PMPN convergence function makes the PMPN appear, to the higher layers, to consist of some number of virtual point-to-point LANs. The networking technologies enabled by this simulation include routing, bridging, and protection switching, along with a wide range of associated networking protocols.

13.6.2 PMPN convergence function

A system can connect to a PMPN node via the PMPN convergence function. The PMPN convergence function provides zero or more ISS SAPs to the upper layers, each one attached to a virtual point-to-point LAN connecting to another PMPN node. If the PMPN incorporates its own link security capability, rather than utilizing IEEE Std 802.1X and/or IEEE Std 802.1AE, then the PMPN convergence function offers two instances of the ISS to the system for each virtual point-to-point LAN—a Controlled Port and an Uncontrolled Port. (See 13.2.2 for an example.)

The PMPN convergence function makes use of a single PMPN SAP offered by the PMPN node. The PMPN SAP is similar to the ISS, except that it includes a station vector parameter, specifying to which of the PMPN nodes (equivalently, to which of the virtual point-to-point LANs) the request is directed, or from which the indication is presented.

A PMPN SAP request primitive can be directed to any non-empty subset of the PMPN nodes, including all of them. The station vector is supplied with the request primitive so that the PMPN node can make the determination of whether to execute the request in a single transmission or more than one transmission, in order to balance considerations such as bandwidth usage. For the PMPN SAP indication primitive, the station vector always indicates from which single PMPN node the indication was received.

The number of virtual point-to-point LANs implemented, and thus the number of SAPs offered to the upper layers by the PMPN convergence function, are an implementation choice. PMPN nodes can be dynamically added and removed from the PMPN network, and direct links between PMPN nodes can be created or destroyed. An implementation can choose, as these events occur, to create and destroy virtual point-to-point LANs and SAPs, or it can manipulate the MAC_Operational parameters of the SAPs to make them available for use or not.

NOTE—Subclause 8.6 of IEEE Std 802.1Q discusses the process of forwarding frames through a bridge in terms of the creation, at the time a frame is received, of a vector of ports on which the frame can be output. The process of deciding on what port or ports the frame is to be output is described in terms of removing ports from this vector. The following paragraph is a formalism, not a description of an intended implementation method. The purpose of this formalism is to resolve the conflict between multiple virtual Bridge Ports and a single physical interface.

Upon (in theory) the simultaneous receipt of one or more identical M_UNITDATA.request primitives on the ISS instances from the upper layers, the PMPN convergence function passes those parameters along to the PMPN SAP along with a station vector, indicating from which ISS instances the request primitive was received (and thus, to which virtual point-to-point LANs it is directed), and constructs an PMPN request primitive, mapping the parameters as required by the particular medium.

On receipt of a valid PMPN indication primitive and station vector, the PMPN convergence function generates an M_UNITDATA.indication primitive on the ISS instance specified by the station vector, mapping the parameters as required by the particular medium.

The ISS MAC_Operational status parameter (11.2) for both the Controlled Port and the Uncontrolled Port offered by a given PMPN virtual LAN is TRUE if virtual point-to-point LAN between the two PMPN nodes is established and authenticated, and the MAC_Enabled status parameter is TRUE, otherwise MAC_Operational is FALSE.

If the adminPointToPointMAC parameter has the value Auto (11.3), then the operPointToPointMAC parameter for any ISS offered by the PMPN General Link convergence function is TRUE.

14. MAC Service

14.1 Function

The MAC connectionless-mode transmission service (the MAC Service) is provided using a subset of the elements of the ISS (Clause 11). The primitives defined in this clause can be used to transmit an independent, self-contained MSDU from one MSAP to another MSAP in a single service access. It is self-contained in that all of the information required to deliver the MSDU is presented to the MAC Service provider in a single service access; thus no initial establishment or subsequent release of a connection is required.

An MSDU transmitted using MAC connectionless-mode transmission is not considered by the MAC Service provider to be related in any way to any previously transmitted MSDU. Although the MAC Service maintains the integrity of individual MSDUs, it does not necessarily deliver them to the receiving MAC Service user in the order in which they are presented by the transmitting MAC Service user, for example in cases where they have different priorities.

The MAC Service provider is not required to maintain state information for flow control between specific combinations of MSAPs.

14.2 Service primitives and parameters

Two unit-data primitives are specified for the connectionless-mode data transmission service, an MA_UNITDATA.indication and an MA_UNITDATA.request, together with the parameters of those primitives. Each MA_UNITDATA indication corresponds to the receipt of an error-free MAC frame from a LAN. A data request primitive is invoked to transmit a frame to an individual LAN.

NOTE 1—Detailed specifications of error conditions in received frames are contained in the relevant MAC standards; for example, FCS errors, length errors, and non-integral number of octets.

```
MA_UNITDATA.indication      (
                            destination_address,
                            source_address,
                            mac_service_data_unit,
                            priority
                            )

MA_UNITDATA.request         (
                            destination_address,
                            source_address,
                            mac_service_data_unit,
                            priority
                            )
```

The destination_address parameter is the address of an individual MSAP or a group of MSAPs. The source_address parameter is the individual address of the source MSAP.

The mac_service_data_unit parameter is the service user data. The default value of the priority parameter is 0. Values 1 through 7 form an ordered sequence of user_priorities, with 1 being the lowest value, 7 the highest, and 0 falling between 1 and 2.

NOTE 2—The specification in this standard differs from that of IEEE Std 802.1D as it omits the frame_type and access_priority parameters. The frame_type is not required as the receipt of a frame other than a user data frame does not cause a data indication. The mapping of these primitives to particular access methods specified by this standard includes derivation of the access_priority parameter (for those media that require it) from the priority parameter specified here.

NOTE 3—The remaining parameters associated with the M_UNITDATA.request and M_UNITDATA.indication primitives (frame_check_sequence, drop_eligible, service_access_point_identifier, and connection_identifier) are unspecified.

14.3 Status parameters

The connectionless-mode transmission service also makes available status parameters that reflect the operational state and administrative controls over each instance of the service provided.

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 the entity providing the service is capable of transmitting and receiving frames and its use is permitted by management, i.e., MAC_Enabled is also TRUE. Its value is otherwise FALSE. The value of this parameter is determined by the specific MAC procedures.

NOTE—These status parameters provide a common approach across MACs for handling the fact that

a) A MAC can inherently be working or not;
b) If the MAC is working, its operational state can be administratively overridden.

14.4 Sequence of primitives

The sequence of primitives in a successful MAC sublayer connectionless-mode transmission is defined in the time sequence diagram in Figure 14-1.

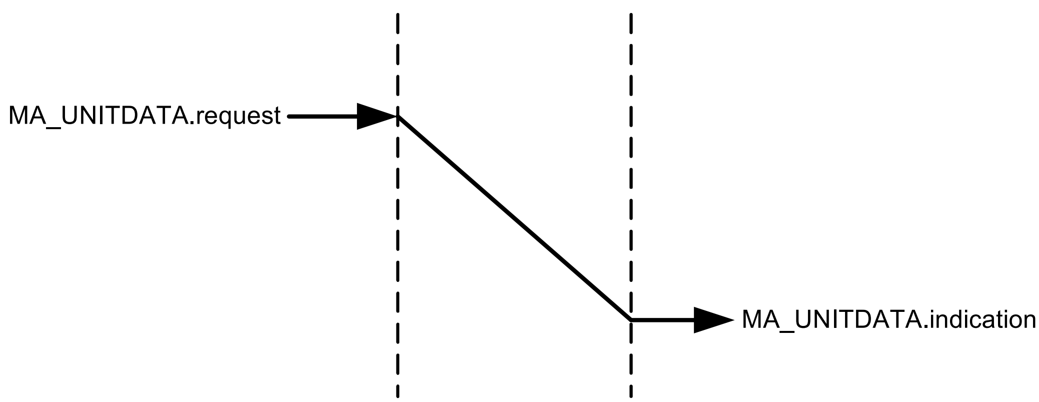

Figure 14-1—Sequence of primitives

Annex A

(informative)

Bibliography

[B1] IEEE Std 802.1AE™-2006, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Security.[12, 13]

[B2] 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.[14]

[B3] ISO/IEC 15802-1, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 1: Medium Access Control (MAC) service definition.

[B4] IETF RFC 787 (July 1981), *Connectionless Data Transmission Survey/Tutorial*, A. Lyman Chapin.[15]

[12]IEEE publications are available from The Institute of Electrical and Electronics Engineers (http://standards.ieee.org/).

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

[14]ISO/IEC publications are available from the ISO Central Secretariat (http://www.iso.org/). ISO publications are also available in the United States from the American National Standards Institute (http://www.ansi.org/).

[15]Internet RFCs are retrievable at http://www.ietf.org/rfc/rfcNNNN.txt (where nnnn is a standard's publication number such as 1042).

Annex B

(informative)

Support of the Internal Sublayer Service by specific MAC procedures

NOTE—The convergence function specified in this annex provides a framework to allow IEEE 802.11 media to be used in the interior of an IEEE 802.1Q bridged LAN.

B.1 General wireless LAN convergence function

The wireless LAN access method is specified in IEEE Std 802.11-2012. Subclause 5.2 of that standard specifies the IEEE 802.11 MAC Service definition, 4.3.5 introduces the distribution system, and Clause 4 and Clause 5 specify the points in the IEEE 802.11 architecture at which the MAC Service is offered. The Media Access Method Dependent convergence functions used with IEEE Std 802.11 and amendments are as follows:

a) The IEEE 802.11 portal convergence function (B.1.1) supports an IEEE 802.11 portal, offers an instance of the ISS to the upper layers, and uses an instance of the Distribution Service SAP (DS SAP) offered by an IEEE 802.11 distribution system. The distribution system in turn provides connectivity to some number of IEEE 802.11 access points and IEEE 802.11 mesh gates, and via those, to some number of associated IEEE 802.11 non-AP stations (B.1.1).
b) The IEEE 802.11 General Link (GLK) convergence function (B.1.4) attached to an IEEE 802.11 GLK access point or IEEE 802.11 GLK non-AP STA presents a set of ISS SAPs, each corresponding to a virtual point-to-point LAN. These ISS SAPs are mapped onto an IEEE 802.11 MAC SAP, which provides access to the corresponding set of virtual point-to-point LANs, where each LAN connects to one of the following:
    1) Zero or one associated IEEE 802.11 GLK non-AP STAs when the LANs are provided by an access point; or
    2) Zero or one associated IEEE 802.11 access points, or zero or one other GLK non-AP STAs, when the LANs are provided by a GLK non-AP STA.
c) The IEEE 802.11 non-GLK convergence function (B.1.3) offers an instance of the ISS to the upper layers, and uses an instance of the IEEE 802.11 MAC Service interface offered by an IEEE 802.11 non-AP STA, mesh STA, IBSS STA, or DMG STSA.

NOTE—The native service provided by an IEEE 802.11 non-GLK station (9.2.8 of IEEE Std 802.11-2012) cannot be adapted to the ISS by a Media Access Method Dependent convergence function, because frames with a destination address that is a group address are reflected back to the station. This behavior is prohibited for an ISS (11.1).

All of the convergence functions defined in this clause use the same mapping of ISS parameters to and from IEEE 802.11 service instance primitives, which is defined in B.1.5.

B.1.1 IEEE 802.11 portal convergence function

As shown in Figure B.1, this convergence function offers an instance of the ISS to upper layers, connecting to an IEEE 802.11 distribution system through an instance of the DS SAP interface defined in Annex R of IEEE Std 802.11-2012. An IEEE 802.11 non-AP infrastructure station is associated to the distribution system via an IEEE 802.11 access point. An IEEE 802.11 mesh station can be associated to the distribution system via one or more IEEE 802.11 mesh gates. For a description of the IEEE 802.11 architecture, see Clause 4 of IEEE Std 802.11-2012. The IEEE 802.11 portal convergence function, together with the upper layers to which it offers a service via the ISS, constitute one architecture for an IEEE 802.11 portal.

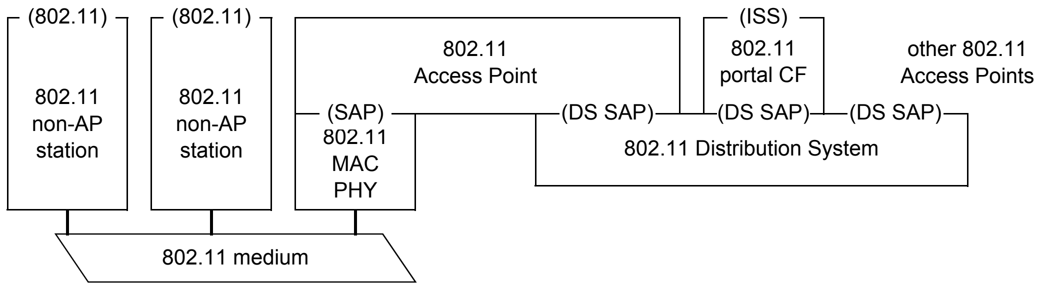

Figure B.1—IEEE 802.11 portal convergence function method

The DS SAP offers the DS-UNITDATA.request and DS-UNITDATA.indication primitives, defined in Annex R of IEEE Std 802.11-2012. The "data" parameter of the request and indication uses LPD. This convergence function uses the translation functions described in Clause 12 to supply the integration function required by Annex Q.6 of IEEE Std 802.11-2012. The IEEE 802.11 portal convergence function makes no use of the DS-STA-NOTIFY.request primitive offered by the DS SAP.

When an M_UNITDATA.request primitive is received, the IEEE 802.11 portal convergence function generates a corresponding IEEE 802.11 DS-UNITDATA.request as described in B.1.5.1.

When an IEEE 802.11 DS-UNITDATA.indication primitive is received, the IEEE 802.11 portal convergence function generates a corresponding M_UNITDATA.indication as described in B.1.5.2.

NOTE—As shown in Figure B.1, this convergence function does not supply the Controlled and Uncontrolled Ports of the IEEE 802.11 Security architecture (B.1.2). This is because the DS SAP is a service offered by the IEEE 802.11 distribution system, not the IEEE 802.11 MAC/PHY.

The MAC_Operational status parameter (11.2) is TRUE if the MAC_Enabled parameter is TRUE, otherwise MAC_Operational is FALSE.

If the adminPointToPointMAC parameter has the value Auto (11.3), then the operPointToPointMAC parameter for any ISS offered by the IEEE 802.11 portal convergence function is FALSE.

B.1.2 IEEE 802.11 Security architecture

The IEEE 802.1AE Security Entity (SecY) is illustrated in Figure B.2, which is a simplified version of Figure 10-1 of IEEE Std 802.1AE-2006. The SecY provides two instances of the ISS to the layers above it, and utilizes a single instance of the ISS to access the layers below it. The two ISS instances above the SecY are the Controlled Port (C) and the Uncontrolled Port (U). The Controlled Port can supply cryptologically secured MAC Service, and the Uncontrolled Port supplies unsecured MAC Service.

The SecY is used on some IEEE 802 media, including IEEE 802.3, but not including IEEE 802.11, in the manner illustrated in part 1 of Figure B.4. IEEE 802.11, however, necessarily places its security layer, with Controlled and Uncontrolled ports similar to those of the IEEE 802.1AE SecY, below the IEEE 802.11 SAP. This is because IEEE 802.11 systems protect fragments of frames, not whole frames, and those segments are created or assembled in layers between the SAP and the security layer. Therefore, the IEEE 802.1AE SecY is not typically used on IEEE 802.11 media.

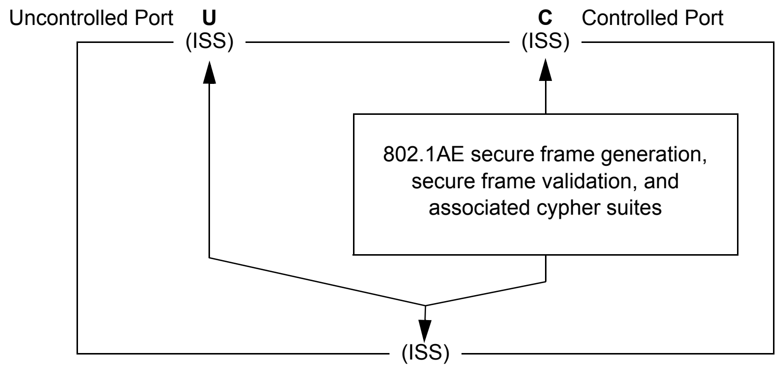

Figure B.2—Simplified IEEE 802.1AE SecY

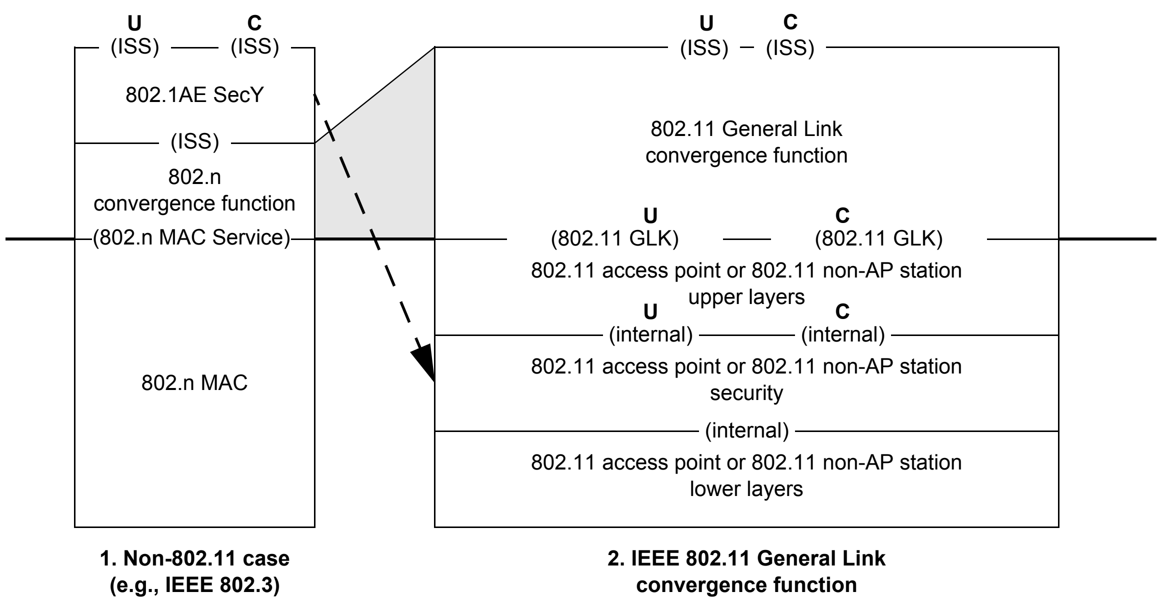

Figure B.3—IEEE 802.11 Security architecture

B.1.3 IEEE 802.11 non-GLK station convergence function

This convergence function offers an instance of the ISS to the upper layers, and uses an instance of the MA-UNITDATA service offered by an underlying non-GLK IEEE 802.11 station. In order to use the IEEE 802.11 security layer, but provide the same services to the upper layers for IEEE 802.11 media that are provided by the SecY for other media, this convergence function provides an Uncontrolled Port and a Controlled Port, each mapped to their equivalents at the service offered by the IEEE 802.11 station.

When an M_UNITDATA.request primitive is received, the IEEE 802.11 parameter mapping generates a corresponding IEEE 802.11 MA-UNITDATA.request as described in B.1.5.1.

When an IEEE 802.11 MA-UNITDATA.indication primitive is received, the IEEE 802.11 parameter mapping generates a corresponding M_UNITDATA.indication as described in B.1.5.2.

B.1.4 IEEE 802.11 General Link convergence function

A system may connect to an IEEE 802.11 station via the IEEE 802.11 General Link (GLK) convergence function. The General Link convergence function provides connections to zero or more virtual point-to-point LANs, each to another IEEE 802.11 station. In order to utilize the IEEE 802.11 security layer, but provide the same services to the upper layers for IEEE 802.11 media that are provided by the SecY for other media, this convergence function provides an Uncontrolled Port and a Controlled Port for each virtual point-to-point LAN, which is to say, for each of the other IEEE 802.11 stations to which its access point or non-AP station is associated. Figure B.4, part 2, illustrates the infrastructure method applied to an IEEE 802.11 access point (or non-AP station) with *n* associated IEEE 802.11 stations.

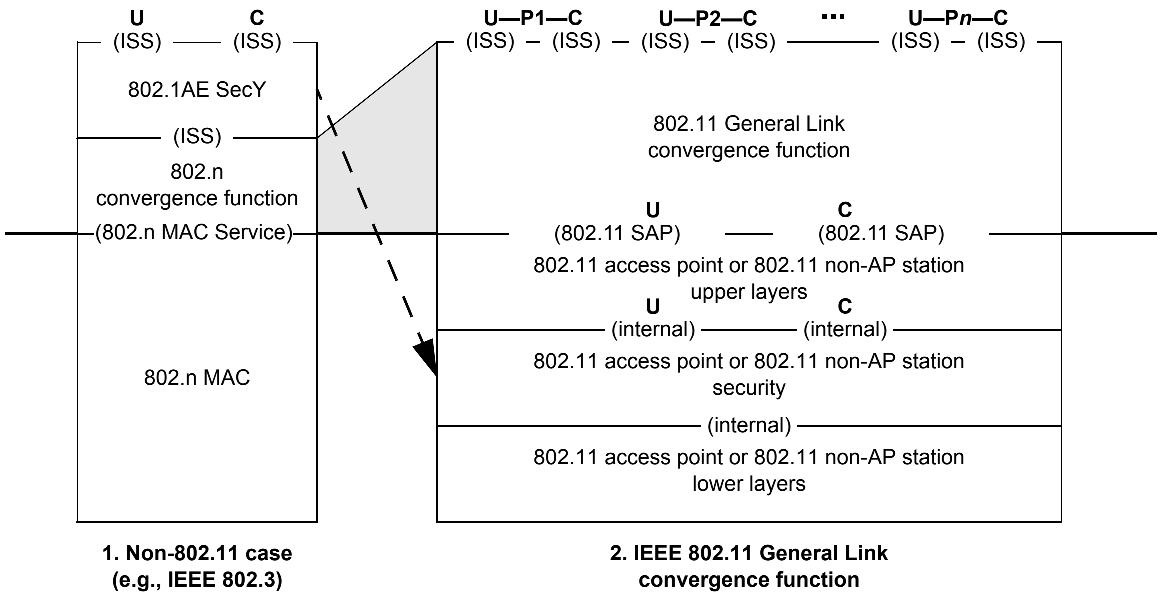

Figure B.4—MAC security and IEEE 802.11 media

The service interface presented by the IEEE 802.11 station (whether an access point or a non-AP station) to the General Link convergence function includes a station vector parameter in the MA-UNITDATA.request and MA-UNITDATA.indication primitives, specifying to which of the IEEE 802.11 stations the request is directed, or from which the indication is presented. A request can be directed to any non-empty subset of the associated IEEE 802.11 stations, including to all of them. The station vector is supplied with a request primitive so that the IEEE 802.11 station can make the determination of whether to execute the request in a single transmission or more than one transmission, in order to balance considerations such as reliability of delivery versus bandwidth utilized. For the indication primitive, the station vector always indicates arrival from a single IEEE 802.11 station.

The number of virtual point-to-point LANs implemented, and thus the number of Controlled and Uncontrolled Ports and ultimately, Bridge Ports, are an implementation choice. IEEE 802.11 non-AP stations can be associated and disassociated with IEEE 802.11 access points, and direct links among non-AP stations can be created or destroyed. An implementation can choose, as these events occur, to create and destroy virtual point-to-point LANs and ports, or it can manipulate the MAC_Operational parameters of the SAPs to make them available for use or not.

NOTE—Subclause 8.6 of IEEE Std 802.1Q-2014 discusses the process of forwarding frames through a bridge in terms of the creation, at the time a frame is received, of a vector of ports on which the frame can be output. The process of deciding on what port or ports the frame is to be output is described in terms of removing ports from this vector. It is intended that this vector of ports be mapped to an IEEE 802.11 service parameter providing similar functions. The following paragraph is a formalism, not a description of an intended implementation method. The purpose of this formalism is to resolve the conflict between multiple virtual Bridge Ports and a single physical interface.

Upon (in theory) the simultaneous receipt of one or more identical M_UNITDATA.request primitives on the ISS instances from the upper layers, the General Link convergence function passes a single MAC Service Data Unit and a station vector, indicating from which ISS instances the request primitive was received, and constructs an IEEE 802.11 MA-UNITDATA.request primitive, mapping the parameters as specified in B.1.5.1.

On receipt of a valid IEEE 802.11 MA-UNITDATA.indication primitive and station vector, the General Link convergence function generates an M_UNITDATA.indication primitive on the ISS instance specified by the station vector, mapping the parameters as specified in B.1.5.2.

The ISS MAC_Operational status parameter (11.2) for both the Controlled Port and the Uncontrolled Port offered by a given IEEE 802.11 infrastructure virtual LAN is TRUE if the IEEE 802.11 access point or non-AP station is both associated to (4.5.3.3 of IEEE Std 802.11-2012) and authenticated to (4.5.4.2 of IEEE Std 802.11-2012) the remote station, and the MAC_Enabled status parameter is TRUE. Otherwise, MAC_Operational is FALSE.

If the adminPointToPointMAC parameter has the value Auto (11.3), then the operPointToPointMAC parameter for any ISS offered by the IEEE 802.11 General Link convergence function is TRUE.

B.1.5 IEEE 802.11 parameter mapping

B.1.5.1 IEEE 802.11 parameter mapping (requests)

When an M_UNITDATA.request primitive is received, the IEEE 802.11 convergence function (B.1.1, B.1.3, or B.1.4) generates a corresponding IEEE 802.11 MA-UNITDATA.request or IEEE 802.11 DS-UNITDATA.request as follows:

a) The destination_address, source_address, and priority parameters are passed unaltered as the destination address, source address and priority, respectively.
b) The M_UNITDATA mac_service_data_unit parameter is passed unaltered as the MA-UNITDATA or DS-UNITDATA data parameter.
c) The ISS M_UNITDATA drop_eligible, frame_check_sequence, service_access_point_identifier, and connection_identifier parameters are ignored.

   NOTE—Drop eligibility is a capability defined in IEEE Std 802.11aa. However, it is not represented in the MA-UNITDATA service interfaces.

d) The IEEE 802.11 MA-UNITDATA or DS-UNITDATA routing information parameter is null.
e) The value of the IEEE 802.11 MA-UNITDATA or DS-UNITDATA service class parameter is QoSAck.
f) The IEEE 802.11 MA-UNITDATA MSDU_format parameter is EPD.
g) If one or more MA_UNITDATA.request primitives for the same frame type are being serviced by the General Link convergence function (B.1.4), then an IEEE 802.11 MA-UNITDATA station_vector parameter is supplied to indicate on which virtual point-to-point LANs the frame is to be transmitted.

B.1.5.2 IEEE 802.11 parameter mapping (indications)

When an IEEE 802.11 MA-UNITDATA.indication or DS-UNITDATA.indication primitive is received, the IEEE 802.11 convergence function (B.1.1, B.1.3, or B.1.4) generates a corresponding M_UNITDATA.indication as follows:

a) For the General Link convergence function (B.1.4), the MA-UNITDATA station_vector parameter is used to determine on which ISS instance the M_UNITDATA.indication primitive is to be generated.
b) The destination address, source address, and priority parameters are passed unaltered as the destination_address, source_address, and priority parameters, respectively.
c) If the MSDU_format parameter of the MA-UNITDATA.indication specifies LPD, then the data parameter is translated as specified in 12.2 to form the mac_service_data_unit parameter. Otherwise, the MA-UNITDATA or DS-UNITDATA data parameter is passed unaltered as the mac_service_data_unit parameter.
d) The drop_eligible parameter is FALSE.
e) The frame_check_sequence, service_access_point_identifier, and connection_identifier parameters are null.
f) The MA-UNITDATA or DS-UNITDATA routing information, reception status and service class parameters are ignored.

Consensus

WE BUILD IT.

Connect with us on:

Facebook: https://www.facebook.com/ieeesa

Twitter: @ieeesa

LinkedIn: http://www.linkedin.com/groups/IEEESA-Official-IEEE-Standards-Association-1791118

IEEE-SA Standards Insight blog: http://standardsinsight.com

YouTube: IEEE-SA Channel

IEEE
standards.ieee.org
Phone: +1 732 981 0060 Fax: +1 732 562 1571