Draft Standard P802-REVc/D1.1
August, 2023
(Revision of IEEE Std 802®-2014 as amended by
IEEE Std 802d™-2017, IEEE Std 802c™-2017
and IEEE Std 802f™-20xx)

Draft Standard for Local and metropolitan area networks—

Overview and Architecture

Prepared by the
Maintenance Task Group of IEEE 802.1

Sponsor
LAN/MAN Standards Committee
of the
IEEE Computer Society

This and the following cover pages are not part of the draft. They provide revision and other information for IEEE 802.1 Working Group members and participants in the IEEE Standards Association ballot process, and will be updated as convenient. New participants: Please read these cover pages, they contain information that should help you contribute effectively to this standards development project.

The text proper of this draft begins with the Title Page.

Editors' Foreword

Throughout this document any notes presented between angle braces are temporary, inserted by the Editors for a variety of purposes. They will be removed prior to Sponsor Ballot and are not part of the normative text. The records of participants in the development of the standard will be added at an appropriate time.

Participation in 802.1 standards development

All participants in the standardization activities of IEEE 802.1 should be aware of the Working Group Policies and Procedures, and the fact that they have obligations under the IEEE Patent Policy, the IEEE Standards Association (SA) Copyright Policy, and the IEEE SA Participation Policy. For information on these policies see 1.ieee802.org/rules/ and the slides presented at the beginning of each of our Working Group and Task Group meeting.

As part of our IEEE 802® process, the text of the PAR (Project Authorization Request) and CSD (Criteria for Standards Development) of each project is reviewed regularly to ensure their continued validity. A link is provided to the full text of the PAR (no CSD was produced for this project as no new features are planned). A vote of "Approve" on this draft is also an affirmation that the PAR for this project are still valid.

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

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

http://ieee802.org/1/

Use of the email distribution list is not presently restricted to 802.1 members, and the working group has a policy of considering comments from all who are interested and willing to contribute to the development of the draft. Individuals not attending meetings have helped to identify sources of misunderstanding and ambiguity in past projects. The email lists exist primarily to allow the members of the working group to develop standards, and are not a general forum. All contributors to the work of 802.1 should familiarize themselves with the IEEE patent policy and anyone using the email distribution list will be assumed to have done so. Information can be found at http://standards.ieee.org/db/patents/

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

James Gilb
Editor, P802-REVc
Email:Gilb_IEEE@yahoo.com

Paul Congdon
Chair, 802.1 Maintenance Task Group
Email:paul.congdon@tallac.com

Glenn Parsons
Chair, 802.1 Working Group
Email: glenn.parsons@ericsson.com

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

All participants in IEEE standards development have responsibilities under the IEEE patent policy and should familiarize themselves with that policy, see http://standards.ieee.org/about/sasb/patcom/materials.html

Draft development

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

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

During the early stages of draft development the proposed text can be moved around a great deal, and even minor rearrangement can lead to a lot of 'change', not all of which is noteworthy from the point of the reviewer, so the use of automatic change bars is not very effective. In early drafts change bars may be omitted or applied manually, with a view to drawing the readers attention to the most significant areas of change. Readers interested in viewing every change are encouraged to use Adobe Acrobat to compare the document with their selected prior draft. Note that the FrameMaker change bar feature is useless when it comes to indicating changes to Figures.

Project Authorization Request, Scope, Purpose, and Criteria for Standards Development (CSD)

The complete PAR, as approved by IEEE NesCom 13th February 2020, can be found at:

https://development.standards.ieee.org/myproject-web/app#viewpar/12800/9288

A CSD (Criteria for Standards Development) was not produced for this project as the goal is to only include the approved amendments and fix errors.

Introduction to the current draft

This introduction is not part of the draft, and will be revised for SA ballot. A set of cover pages will be retained for use during SA ballot.

This is the third draft of the revision intended for ballot. This draft merged in two amendments. The changes from the first, IEEE Std 802c™-2017 are focused on sublcause 8.2, with new material in 8.4.1, 9.6 and Annex E.3. The second, IEEE Std 802d™-2017, added a new Clause 11.

This page intentionally left blank.

Draft standard P802®-REVc
(Revision of IEEE Std 802®-2014 as amended by
IEEE Std 802d™-2017, IEEE Std 802c™-2017
and IEEE Std 802f™-20xx)

Draft Standard for Local and Metropolitan Area Networks: Overview and Architecture

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Abstract: This standard provides an overview to the family of IEEE 802® standards. It describes the reference models for the IEEE 802 standards and explains the relationship of these standards to the higher layer protocols; it provides a standard for the structure of IEEE 802 MAC addresses; it provides a standard for identification of public, private, prototype, and standard protocols; it specifies an object identifier hierarchy used within IEEE 802 for uniform allocation of object identifiers used in IEEE 802 standards; and it specifies a method for higher layer protocol identification.

Keywords: BANs, body area networks, EtherTypes, IEEE 802®, IEEE 802 architecture, IEEE 802 reference model, LANs, local area networks, MANs, metropolitan area networks, object identifiers, PANs, personal area networks, RANs, regional area networks, protocol development, protocol types

---

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

PDF: ISBN 978-0-7381-9219-2 STD98723
Print: ISBN 978-0-7381-9220-8 STDPD98723

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 (https://standards.ieee.org/ipr/disclaimers.html), 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 are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA 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 makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. 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 the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s).

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, 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 subcommittees of the IEEE SA Board of Governors 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 evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the IEEE SA myProject system.[1] An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.[2]

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.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

[1] Available at: https://development.standards.ieee.org/myproject-web/public/view.html#landing.
[2] Available at: https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US 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, neither IEEE or its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, 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; https://www.copyright.com/. 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 10 years. When a document is more than 10 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 tIEEE Xplore or contact IEEE.[3] For more information about the IEEE SA or IEEE's standards development process, visit the IEEE-SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website.[4] Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata .

Patents

IEEE Standards are developed in compliance with the IEEE SA Patent Policy.[5]

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

[3]Available at: https://ieeexplore.ieee.org/browse/standards/collection/ieee.
[4]Available at: https://standards.ieee.org/standard/index.html.
[5]Available at: https://standards.ieee.org/about/sasb/patcom/materials.html.

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.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants

At the time this standard was completed, the IEEE 802.1 Working Group had the following membership:

Glenn Parsons, *Chair*
Jessy Rouyer, *Vice Chair*
Jessy Rouyer, *Recording Secretary*
James P. K. Gilb, *802-Rev Technical Editor*

In addition to the members of the IEEE 802.1 Working Group, significant contributions were received from the following individuals:

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

When the IEEE SA Standards Board approved this standard on <to be filled in>, it had the following membership:

, *Chair*
, *Vice-chair*
, *Past Chair*
Konstantinos Karachalios, *Secretary*

*Member Emeritus

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

<to be filled in by IEEE Editorial Staff>

Historical participants

When the IEEE Std 802-1990 was approved on 31 May 1990, the IEEE 802.1 Working Group had the following officer:

William P. Lidinsky, *Chair*

When the IEEE Std 802-2001 was approved on 6 December 2001, the IEEE 802.1 Working Group had the following officers:

William P. Lidinsky, *Chair*
Tony Jeffree, *Vice Chair and Editor*
Alan Chambers, Tony Jeffree, *Editors*

When the IEEE Std 802a-2003 was approved on 12 June 2003, the IEEE 802.1 Working Group had the following officers:

Tony Jeffree, *Chair and Editor*
Neil Jarvis, *Vice Chair*

When the IEEE Std 802b-2004 was approved on 25 March 2004, the IEEE 802.1 Working Group had the following officers:

Tony Jeffree, *Chair and Editor*
Neil Jarvis, *Vice Chair*

When the IEEE Std 802-2014 was approved on 12 June 2014, the IEEE 802.1 Working Group had the following officers:

Glenn Parsons, *Chair*
John Messenger, *Vice Chair*
Eric Gray, *Recording Secretary*
James P. K. Gilb, *IEEE 802-2014 Technical Editor*

When the IEEE Std 802c-2017 was approved on 15 June 2017, the IEEE 802.1 Working Group had the following officers:

Glenn Parsons, *Chair*
John Messenger, *Vice Chair*
Pat Thaler, *Chair, Data Center Bridging Task Group*
Roger B Marks, *IEEE 802c Technical Editor*

When the IEEE Std 802d-2017 was approved on 14 February 2017, the IEEE 802.1 Working Group had the following officers:

Glenn Parsons, *Chair*
John Messenger, *Vice Chair*
János Farkas, *Chair, Time-Sensitive Networking Task Group*
Tony Jeffree, *Editor*

The following individuals participated in the IEEE 802.1 working group during various stages of the standard's development. Since the initial publication, many IEEE standards have added functionality or provided updates to material included in this standard. The following is a historical list of participants who have dedicated their valuable time, energy, and knowledge to the creation of this standard:

Steve Adams
Fumio Akashi
Paul D. Amer
Charles Arnold
Floyd Backes
Ann Ballard
Richard Bantel
John Bartlett
Sy Bederman
Les Bell
Amatzia Ben-Artzi
Michael Berger
James S. Binder
Robert Bledsoe
Kwame Boakye
Paul Bottorff
Laura Bridge
Juan Bulnes
Bill Bunch
Fred Burg
Jim Burns
Peter Carbone
Paul Carroll
Jeffrey Catlin
Dirceu Cavendish
Alan Chambers
David W. Chang
Ken Chapman
Alice Chen
Jade Chien
Hon Wah Chin
Chris Christ
Paul Congdon
Glenn Connery
Jim Corrigan
Paul Cowell
David Cullerot
Ted Davies
Peter Dawe
Stan Degen
Fred Deignan
David Delaney
Ron Dhondy
Jeffrey Dietz
Eiji Doi
Barbara J. Don Carlos
Peter Ecclesine
J. J. Ekstrom
Hesham Elbakoury
Walder Eldon
Norman W. Finn
David Frattura
Lars Henrik Frederiksen
Eldon D. Feist
Len Fishler
Kevin Flanagan
Anoop Ghanwani
Pat Gonia
Gerard Goubert
Richard Graham
Michael A. Gravel
Steve Haddock
Sharam Hakimi
Mogens Hansen
Harold Harrington
John Hart
Mike Harvey
Richard Hausman
David Head
Deepak Hegde
Ariel Hendel
Bob Herbst
Steve Horowitz
Robert W. Hott
Jack R. Hung
Altaf Hussain
Thomas Hytry
Ran Ish-Shalom
Jay Israel
Vipin K. Jain
Neil Jarvis
Tony Jeffree
Shyam Kaluve
Toyoyuki Kato
Hal Keen
Kevin Ketchum
Alan Kirby
Kimberly Kirkpatrick
Keith Klamm
Steve Kleiman
Bruce Kling
Dan Krent

James Kristof
H. Eugene Latham
Bing Liao
William P. Lidinsky
George Lin
Paul Lachapelle
Bill Lane
Paul Langille
Roger Lapuh
Loren Larsen
Johann Lindmeyr
Andy Luque
Philip Magnuson
Bruce McClure
Tom McGowan
Milan Merhar
Margaret A. Merrick
John Messenger
Colin Mick
Dinesh Mohan
John Montrose
Bob Moskowitz
Yaron Nachman
Krishna Narayanaswamy
Lawrence Ng
Henry Ngai
Satoshi Obara
Don O'Connor
Jerry O'Keefe
Toshio Ooka
Jorg Ottensmeyer
Richard Patti
Luc Pariseau
Glenn Parsons
Roger Pfister
Thomas L. Phinney
John Pickens
Dinel Pitt
Ron L. G. Prince
Steve Ramberg
Nigel Ramsden
Shlomo Reches
Frank Reichstein
Trudy Reusser
James Richmond
Anil Rijsinghani
Eduoard Rocher
John Roese
Allyn Romanow
Dan Romascanu
Paul Rosenblum
Dolors Sala
John Salter
Alan Sarsby
Ayman Sayed
Susan Schannning
Mick Seaman
Gerry Segal
Rich Seifert
Lee Sendelbach
Himanshu Shah
Howard Sherry
Wu-Shi Shung
Phil Simmons
Curtis Simonson
Paramjeet Singh
Rosemary V. Slager
Alexander Smith
Andrew Smith
M. Soha
Larry Stefani
Dan Stokesberry
Stuart Soloway
Sundar Subramaniam
Lennart Swartz
Kazuo Takagi
Kenta Takumi
Robin Tasker
Angus Telfer
Pat Thaler
Dave Thompson
Geoffrey O. Thompson
Michel Thorsen
Nathan Tobol
Wendell Turner
Steve Van Seters
Dono van-Mierop
Paul Videcrantz
Dennis Volpano
Paul Wainright
John Wakerly
Peter Wang
Y. C. Wang
Trevor Warwick
Scott Wasson
Daniel Watts
Karl Weber
Alan Weissberger
Deborah Wilbert
Keith Willette
Michael Witkowski
Edward Wong
Michael D. Wright
Michele Wright
Allen Yu
Wayne Zakowski
Igor Zhovnirovosky
Carolyn Zimmer
Nick Zucchero

Introduction

This introduction is not part of IEEE Std 802-20xx, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.

This document is the third major revision of the IEEE 802® overview and architecture. This revision integrates into the previous revision of the standard, IEEE Std 802®-2014, the three subsequent amendments:

— IEEE Std 802d™-2017: Specifying a Uniform Resource Name (URN) root identifier for YANG data models

— IEEE Std 802c™-2017: Specifying an optional local medium access control (MAC) address space structure

— IEEE Std 802f-™20xx: Specifying a YANG moudle that contains EtherType information

Contents

IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture

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

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

1. Overview

1.1 Scope

This standard contains descriptions of the IEEE 802® standards published by the IEEE for frame-based data networks as well as a reference model (RM) for protocol standards. A specification for the identification of public, private, and standard protocols is included.

1.2 Purpose

This standard serves as the foundation for the family of IEEE 802 standards published by IEEE for local area networks (LANs), metropolitan area networks (MANs), personal area networks (PANs), and regional area networks (RANs), etc.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used; therefore, each referenced document is cited in 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 (included any amendments or corrigenda) applies.

IEEE Std 802.1Q™, IEEE Standard for Local and metropolitan area networks—Bridges and Bridged Networks.[1, 2]

IEEE Std 802.1AC™, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Service Definition.

IETF RFC 2578, Structure of Management Information Version 2 (SMIv2).[3]

IETF RFC 3406, Uniform Resource Names (URN) Namespace Definition Mechanisms, October 2002.

IETF RFC 8069, URN Namespace for IEEE, February 2017.

ISO/IEC 8802-2:1998, Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.[4] (ISO/IEC version of withdrawn standard IEEE Std 802.2)

ITU-T Recommendation X.660, Information technology—Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree.[5]

[1]The IEEE standards referred to in Clause 2 are trademarks owned by The Institute of Electrical and Electronics Engineers, Incorporated.

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

[3]IETF documents (i.e., RFCs) are available the Internet Engineering Task Force (https://www.rfc-archive.org/).

[4]ISO/IEC publications are available from the International Organization for Standardization (https://www.iso.org/standards.html) and the International Electrotechnical Commission (https://www.iec.ch/). ISO/IEC publications are also available in the United States from the American National Standards Institute (https://www.ansi.org/).

[5]ITU-T publications are available from the International Telecommunications Union (https://www.itu.int/).

3. Definitions, acronyms and abbreviations

3.1 Definitions

For this document, the following terms and definitions apply. *The IEEE Standards Dictionary Online*[6] should be consulted for terms not defined in this clause.[7]

access domain: A set of stations in an IEEE 802® network together with interconnecting data transmission media and functional units (e.g., repeaters), in which the stations use the same medium access control (MAC) protocol to communicate over a common physical medium.

bridge: A functional unit that interconnects two or more IEEE 802® networks that use the same data link layer (DLL) protocols above the medium access control (MAC) sublayer, but can use different MAC protocols. Forwarding and filtering decisions are made on the basis of layer 2 information.

canonical format: The format of a medium access control (MAC) data frame in which the octets of any 48-bit Extended Unique Identifiers (EUI-48s) or 64-bit Extended Unique Identifiers (EUI-64s) conveyed in the MAC user data field have the same bit ordering as in the hexadecimal representation.

end station: A functional unit in an IEEE 802® network that acts as a source of, and/or destination for, link layer data traffic carried on the network.

Ethernet: A communication protocol specified by IEEE Std 802.3™.

EtherType: A 2-octet value, assigned by the IEEE Registration Authority (RA), which provides data field context for frame interpretation (protocol identification).

filtering: A function in a bridge that is used to determine if a received medium access control (MAC) frame is to be forwarded or discarded on any given outbound port.

forwarding: A function in a bridge that transfers a received medium access control (MAC) frame to one or more outbound ports.

frame: The unit of data transfer between peer medium access control (MAC) sublayer entities.

handover: The process by which a mobile node obtains facilities and preserves traffic flows when traffic is switched from one link to another. Different types of handover are specified based on the way facilities for supporting traffic flows are preserved.

interconnection: A data communication path between stations in an IEEE 802® network.

interworking: The use of interconnected stations in a network for the exchange of data, by means of protocols operating over the underlying data transmission paths.

local area network (LAN): A network of devices, whether indoors or outdoors, covering a limited geographic area, e.g., a building or campus.

---

[6]The IEEE Standards Dictionary Online is not a dictionary but rather is a compendium of balloted definitions from individual approved standards.

[7]The *IEEE Standards Dictionary Online* is available at https://dictionary.ieee.org. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

local medium access control (MAC) address: A medium access control (MAC) address with the universally or locally administered (U/L) bit set to one.

logical link: A logical communication connection between two devices.

medium access control (MAC) data frame: A data structure consisting of fields in accordance with a MAC protocol, for the communication of user data and control information in a network; one of the fields contains a sequence of octets of user data.

medium access control (MAC) protocol: A protocol that governs access to the transmission medium in a network, to enable the exchange of data between stations in a network.

media-independent control function: A parallel control plane that provides control functions for different medium access control (MAC) and physical layer (PHY) sublayers and provides a media-independent abstraction to higher layer protocols.

media-independent handover function: A function that provides the ability to relocate traffic flows between different medium access technologies and associated physical media.

metropolitan area network (MAN): A network of devices, extending over a large geographical area such as an urban area, often providing integrated communication services such as data, voice, and video.

Network Unique Identifier (NUI): An identifier that is unique within the IEEE 802® local area network (LAN).

noncanonical format: The format of a medium access control (MAC) data frame in which the octets of 48-bit Extended Unique Identifiers (EUI-48s) or 64-bit Extended Unique Identifiers (EUI-64s) conveyed in the MAC user data field have the same bit ordering as in the bit-reversed representation.

personal area network (PAN): A network of devices extending over a very limited geographical area, used to convey information among a group of participant stations.

private protocol: A protocol whose use and specification are controlled by a private organization.

public protocol: A protocol whose specification is published and known to the public, but controlled by an organization other than a formal standards body.

regional area network (RAN): A network of devices that generally covers a service area that is larger than metropolitan area networks (MANs), typically in sparsely populated areas.

repeater: A device used to interconnect segments of the physical communications media, for example, to extend the range of a network when the physical specifications of the technology would otherwise be exceeded, while providing a single access domain for the attached stations.

service data unit: Information that is delivered between layers or sublayers.

single access domain: A set of stations such that, at most, only one can transmit at a given time, with all other stations acting as (potential) receivers.

standard protocol: A protocol whose specification is published and known to the public and is controlled by a standards body.

station: An end station or bridge. *See also*: **bridge**; **end station**.

Structured Local Address Plan (SLAP): An optional standardized specification to assign locally administered medium access control (MAC) addresses.

universal address: A 48-bit Extended Unique Identifier (EUI-48) or 64-bit Extended Unique Identifier (EUI-64) that is used as a unique address.

3.2 Acronyms and abbreviations

AAI	Administratively Assigned Identifier
AAI-48	48-bit AAI
AAI-64	64-bit AAI
BS	base station
BSS	basic service set
CID	Company ID
CPE	customer-premises equipment
CS	convergence sublayer
C-SAP	control service access point
DLL	data link layer
DCN	data center networking
ELI	Extended Local Identifier
ELI-48	48-bit ELI
ELI-64	64-bit ELI
EPD	EtherType protocol discrimination
EPON	Ethernet passive optical networks
EUI	Extended Unique Identifier
EUI-48	48-bit EUI
EUI-64	64-bit EUI
HLPDE	higher layer protocol discrimination entity
IANA	Internet Assigned Numbers Authority[8]
IEEE RA	Institute of Electrical and Electronic Engineers Registration Authority
IEEE RAC	Institute of Electrical and Electronic Engineers Registration Authority Committee
I/G	individual/group
IM	implementation model
IoT	Internet of things
IP	Internet Protocol
LAN	local area network
LLC	logical link control
LPD	LLC protocol discrimination
LSAP	link service access point
LSB	least significant bit
MAC	medium access control, media access control[9]
MA-L	MAC Address Block Large
MA-M	MAC Address Block Medium
MAN	metropolitan area network

[8] https://www.iana.org

[9] Both forms are used, with the same meaning. This standard uses medium.

MA-S	MAC Address Block Small
MCPS	MAC common part sublayer
MCPS-SAP	MAC common part sublayer data service access point
MIB	management information base
MICF	media-independent control function
MICLSAP	media-independent control link service access point
MICPSAP	media-independent control physical service access point
MICSAP	media-independent control service access point
MIH	media-independent handover
MIHF	media-independent handover function
MLME	MAC sublayer management entity
MSAP	MAC service access point
M-SAP	management service access point
MSB	most significant bit
MSTP	multiple spanning tree protocol
NCMS	network control and management system
NETCONF	Network Configuration Protocol
NID	Namespace Identifier
NUI	Network Unique Identifier
NUI-48	48-bit NUI
NUI-64	64-bit NUI
OAM	operations, administration, and maintenance
OID	object identifier
OLT	optical line terminal
OMG	Object Management Group
ONU	optical network unit
OSI/RM	Open Systems Interconnection basic reference model
OUI	Organizationally Unique Identifier
PAN	personal area network
PDU	protocol data unit
PHY	physical layer (OSI reference model and IEEE 802® reference model)
PHY	physical layer device or entity (IEEE 802.3™ reference model)
PICS	protocol implementation conformance statement
PLME	physical layer management entity
PMD	physical medium dependent
PSAP	physical service access point
RAN	regional area network
RM	reference model
RSTP	rapid spanning tree protocol
SAP	service access point
SAI	Standard Assigned Identifier
SAI-48	48-bit Standard Assigned Identifier
SAI-64	64-bit Standard Assigned Identifier
SLAP	Structured Local Address Plan
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol

SPB	shortest path bridging
SSF	spectrum sensing function
SS/MS	subscriber station/mobile subscriber station
TSN	Time-Sensitive Networking
U/L	universally or locally administered
UML	unified modeling language
URN	Uniform Resource Name
VLAN	virtual local area network
VOIP	voice over Internet protocol
WAN	wide area network
WLAN	wireless local area network
WPAN	wireless personal area network
WRAN	wireless regional area network
YANG	The name of the data modeling language defined in IETF RFC 6020 [B10][10] and IETF RFC 7950 [B12].

[10]The numbers in brackets correspond to the numbers of the bibliography in Annex A.

4. Family of IEEE 802 standards

4.1 Key concepts

IEEE 802 networks use frame-based communications over a variety of media to connect various digital apparatus regardless of computer technology and data type. However, the scope of IEEE 802 standards is not limited to the physical layers (PHYs) and data link layers (DLLs). The family of IEEE 802 standards is the collection of standards that have been developed under the IEEE 802 LMSC, see 4.4 for a list of the IEEE 802 standards current as of the publication of this standard.

The basic communications capabilities provided by all IEEE 802 standards are frame based with source and destination addressing and asynchronous timing of the frames[11]. In a frame-based system, the format is a variable-length sequence of data octets. By contrast, cell-based communication transmits data in fixed-length units in specified time intervals while isochronous communication transmits data as a steady stream of octets, or groups of octets, at equal time intervals. Some IEEE 802 networks can provide scheduled frame transmissions in addition to or alternatively to asynchronous frame transmissions. Scheduled frame transmissions use a network wide time for the transmission schedule which is synchronized over the network.

User and management data flowing within IEEE 802 networks can be secured by a variety of authentication, secure key exchange, and encryption mechanisms that are described in the various IEEE 802 standards. In addition, IEEE 802 standards specify mechanisms by which a station is able to discover neighboring networks information that may include IEEE 802 and non-IEEE 802 technologies. IEEE 802 standards also specify mechanisms to achieve service discovery (e.g., support for Internet or virtual private network service) and session continuity [e.g., a voice over Internet Protocol (VOIP) or multimedia session] in a heterogeneous networking environment when stations, while either stationary or in motion, have a choice of connecting to multiple access networks.

The early IEEE 802 local area network (LAN) wired technologies used shared-medium communication, with information broadcast for all stations to receive. That approach has evolved over the years, but in ways that preserve the appearance of simple peer-to-peer communications behavior for end stations. In particular, the use of bridges, as described in 5.3.2, for interconnecting IEEE 802 networks is now widespread. These bridges allow the construction of networks with much larger numbers of end stations and much higher aggregate throughput than would be achievable with a single shared medium. End stations attached to such a bridged IEEE 802 network can communicate with each other just as though they were attached to a single shared medium; however, the ability to communicate with other stations can be limited by use of management facilities in the bridges, particularly where broadcast or multicast transmissions are involved. A further stage in this evolution has led to the use of point-to-point full duplex communication in LANs, either between an end station and a bridge or between a pair of bridges.

Some IEEE 802 technologies, in particular wireless-based technologies, are inherently shared-medium communication systems. They too have been augmented over time. Many wireless local area networks (WLANs) support mobile node mobility and hence dynamic topologies. These additional facilities may, depending on the IEEE 802 technology in use, restrict bridged LAN interconnects to the static topology nodes within the wireless portion of a heterogeneous technology LAN. Additionally, it is common to interconnect individual networks and bridged networks at Layer 3 in the protocol stack with devices called routers. The specification of routers is outside the scope of IEEE 802 standards.

An IEEE 802 LAN is a peer-to-peer communication network that enables stations to communicate directly on a point-to-point, or point-to-multipoint, basis without requiring them to communicate with any

[11]Some IEEE 802 standards have asynchronous symbol timing within a frame.

intermediate stations that perform forwarding or filtering above the PHY. LAN communication takes place at moderate to high data rates and with short transit delays, on the order of a few milliseconds or less.

A LAN is generally owned, used, and operated by a single organization. This is in contrast to wide area networks (WANs) that interconnect communication facilities in different parts of a country or are used as a public utility. LANs are useful for deployment on a variety of scales, whether indoors or outdoors, including covering a scale up to a large building or campus environment.

A metropolitan area network (MAN) is optimized for a larger geographical area than is a LAN, ranging from several blocks of buildings to entire cities. As with local networks, MANs can also depend on communications channels of moderate to high data rates. A MAN might be owned and operated by a single organization, but it is usually used by many individuals and organizations. MANs might also be owned and operated as public utilities. They often provide means for internetworking of local networks.

Personal area networks (PANs) are used to convey information among a small group of participant stations. Unlike a LAN, a connection made through a PAN typically involves little or no infrastructure or direct connectivity to the world outside the connection. This approach allows small, power-efficient, inexpensive solutions to be implemented. In the context of the family of IEEE 802 standards, PANs are implemented with wireless technology and are, therefore, sometimes referred to as wireless personal area networks (WPANs).

Regional area networks (RANs) generally cover a service area that is larger than the MANs. A RAN is similar to a MAN in that it is typically owned and operated by a single organization, but it is usually used by many individuals and organizations. For wireless regional area networks (WRANs), the unique propagation characteristics of the frequency bands in which they operate, typically from 30 MHz to 1 GHz, require a specialized design of the PHY and the medium access control (MAC) that can absorb long channel impulse responses and large propagation delays. In some cases, operation in these bands is subject to coordination with existing users, e.g., television broadcast.

IEEE 802 networks can also be used to perform the task of an access network, i.e., to connect end stations to a larger, heterogeneous network, e.g., the Internet.

The early IEEE 802 standards for LAN and MAN technologies were all based on the use of copper or optical fiber cables as the physical transmission medium. However, in addition to the use of cable-based media, today’s IEEE 802 standards include technologies, radio and optical, that use free space as the physical transmission medium. IEEE 802 standards for wireless networks include wireless LANs, MANs, RANs, and PANs. These technologies also target usage scenarios for both fixed and mobile wireless. These IEEE 802 network solutions address challenges of mobility, higher error rates, and potentials for signal loss and interference that are inherent to using wireless medium, which is typically a constantly changing environment.

4.2 Application and support

IEEE 802 networks are intended to have wide applicability in many environments. The primary aim is to provide for low-cost devices and networks, suitable for consumer, commercial, educational, governmental, and industrial applications. The following lists are intended to show some applications and devices and, as such, are not intended to be exhaustive, nor do they constitute a set of required items. IEEE 802 networks can be found in the following environments:

- Client/server applications
- Database access
- Desktop publishing

— Electronic mail
— File transfer
— Graphics
— Handover services
— Multimedia
— Office automation
— Vehicular communication
— Process control
— Robotics
— Telecommunication
— Text processing
— Transaction processing

IEEE 802 networks are intended to support communication, for example, between:

— Networking equipment, such as bridges, routers, and gateways
— Desktop, laptop and tablet computers
— Video, audio and multimedia equipment
— Cloud computing services, including web servers and data storage
— Monitoring and control equipment
— Scanners and printers
— Mobile phones and VOIP phones (desk phones)
— Internet of Things (IoT) devices, such as: thermostats, switches, and light bulbs

4.3 An international family of standards

The terms *LAN*, *MAN*, *PAN*, and *RAN* encompass a number of data communications technologies and applications of these technologies. So it is with the IEEE 802 standards. In order to provide a balance between the proliferation of a very large number of different and incompatible local and metropolitan networks, on the one hand, and the need to accommodate rapidly changing technology and to satisfy certain applications or cost goals, on the other hand, several types of medium access technologies are currently specified in the family of IEEE 802 standards. In turn, these MAC standards are specified for a variety of physical media. A secure data exchange standard and MAC bridging standards are intended to be used in conjunction with the MAC standards. Architecture and protocols for the management of IEEE 802 networks are also specified.

The IEEE 802 standards have been developed and applied in the context of a global data communications industry. IEEE 802 standards are recognized to be international standards in their own right. In addition, some IEEE 802 standards have progressed to become standards within Joint Technical Committee 1 of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC 1), International Telecommunication Union Telecommunication Standardization Sector (ITU-T), International Telecommunication Union Radiocommunication Sector (ITU-R), and a wide variety of national body standards development organizations.

4.4 IEEE 802 standards

The IEEE 802 LAN/MAN Standards Committee sponsors a large number of standards projects. The current state of IEEE 802 standards[12] as of the approval of this standard is illustrated in Figure 1. IEEE 802 standards are under continuous development; for the latest status refer to https://www.ieee802.org.

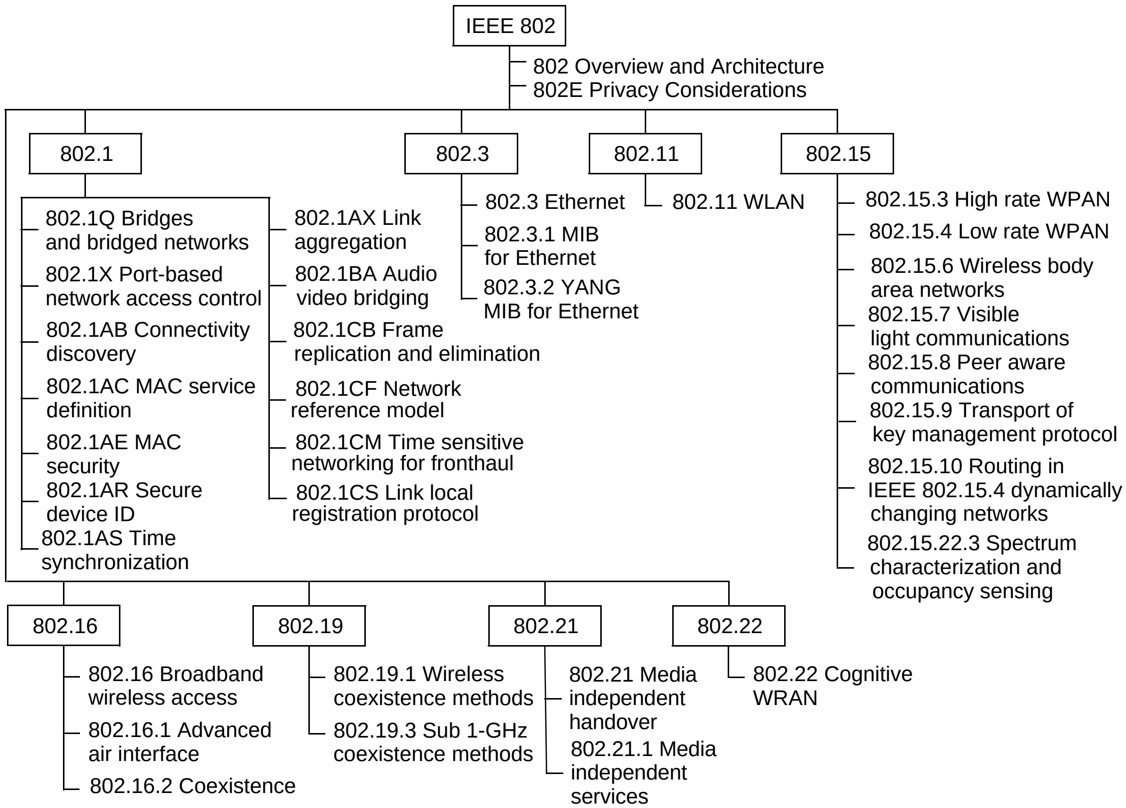


Figure 1—Current family of IEEE 802 standards

[12] Throughout this standard, the term IEEE 802 standard is interpreted to include standards, recommended practices and guides.

At any given time, an IEEE 802 standard may have one or more amendments related to it. Each amendment, once approved, is considered to be part of the base standard. At a future time, through the periodic IEEE-SA revision process, these amendments are incorporated into the base standard so that a new single document can be issued. This process is illustrated in Figure 2 for IEEE Std 802.15.4™-2011,[13] which incorporated the amendments IEEE Std 802.15.4a™-2007, IEEE Std 802.15.4c™-2009, and IEEE Std 802.15.4d™-2009 into the base standard IEEE Std 802.15.4-2006.

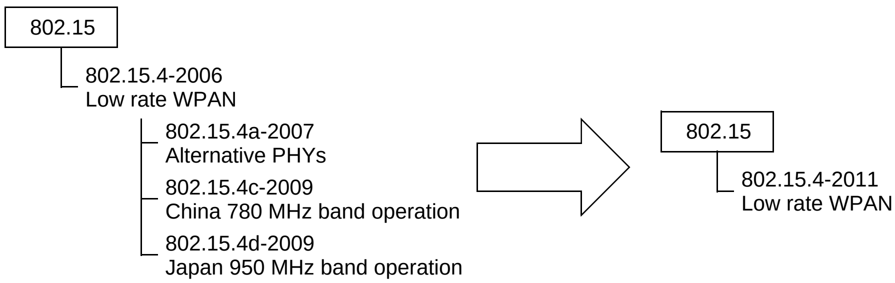


Figure 2—Issuance of IEEE Std 802.15.4-2011 from previous base standard and amendments

[13]See Annex D for a list of approved IEEE 802 standards that were current when this standard was completed.

5. Reference models (RMs)

5.1 Introduction

The IEEE 802 RM is derived from the Open Systems Interconnection basic reference model (OSI/RM), ISO/IEC 7498-1:1994 [B14][14]. It is assumed that the reader has some familiarity with the OSI/RM and its terminology. The IEEE 802 standards emphasize the functionality of the lowest two layers of the OSI/RM, i.e., PHY and DLL, and the higher layers as they relate to network management. The IEEE 802 RM is similar to the OSI/RM in terms of its layers and the placement of its service boundaries. Figure 3 shows the architectural view of IEEE 802 RM for end stations and its relation to the OSI/RM. A variation of the model applies within bridges, as described in 5.3.2.

MSAP MAC service access point
LSAP link service access point
PSAP PHY service access point

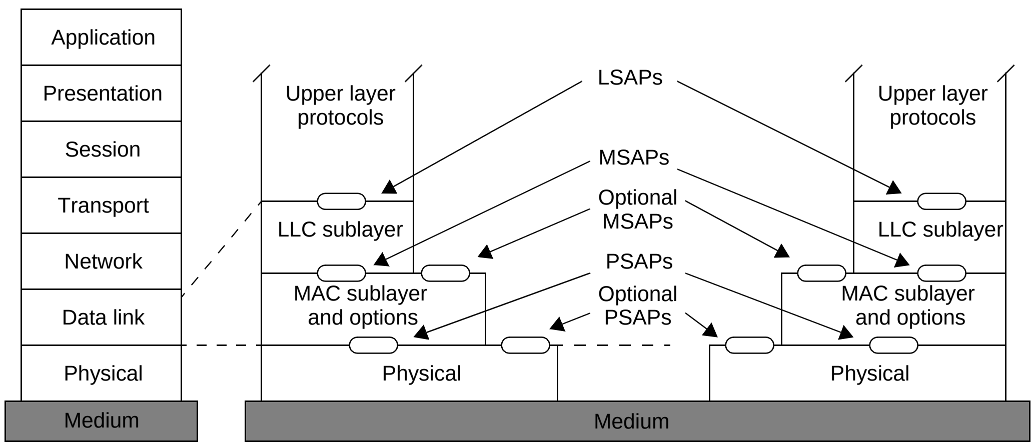


Figure 3—IEEE 802 RM for end stations

For the mandatory data services supported by all IEEE 802 networks, the DLL is structured as two sublayers, with the logical link control (LLC) sublayer, described in 5.2.2, operating over a MAC sublayer, described in 5.2.3.

Each IEEE 802 standard has RMs that are more detailed in order to describe the structure for that specific standard. The RMs for the IEEE 802 standards are given in Annex B.

IEEE 802 standards also provide implementation models (IMs), which are more specific than the IEEE 802 RMs, allowing differentiation between implementation approaches (e.g., different MAC protocols and PHYs). Figure 4 illustrates an IEEE 802.3 IM and its relation to the IEEE 802 RM.

Considerations of management, security, and media-independent handover (MIH) in IEEE 802 networks are also covered by IEEE 802 standards; these optional features lead to an elaboration of the RM, as illustrated in Figure 5. IEEE 802 network management provides protocols for exchange of management information between stations. The media-independent control function (MICF) is a parallel control plane that provides control functions for different MAC and PHY sublayers. Some examples of this MICF are the media-independent handover function (MIHF) of IEEE Std 802.21™ and the control functions proposed in the IEEE 802.19.1 Task Group and IEEE Std 802.22™. IEEE Std 802.1X™ forms part of the LLC sublayer and provides a secure, connectionless service immediately above the MAC sublayer.

[14]The numbers in brackets correspond to those of the bibliography in Annex A.

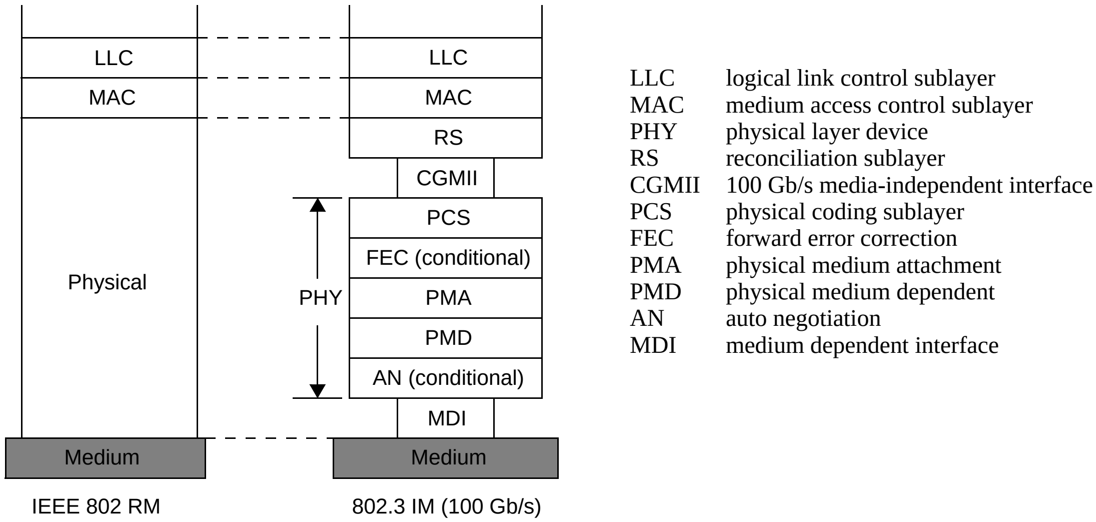


Figure 4—IEEE 802 RM and an example of an end-station IM (100 Gb/s)

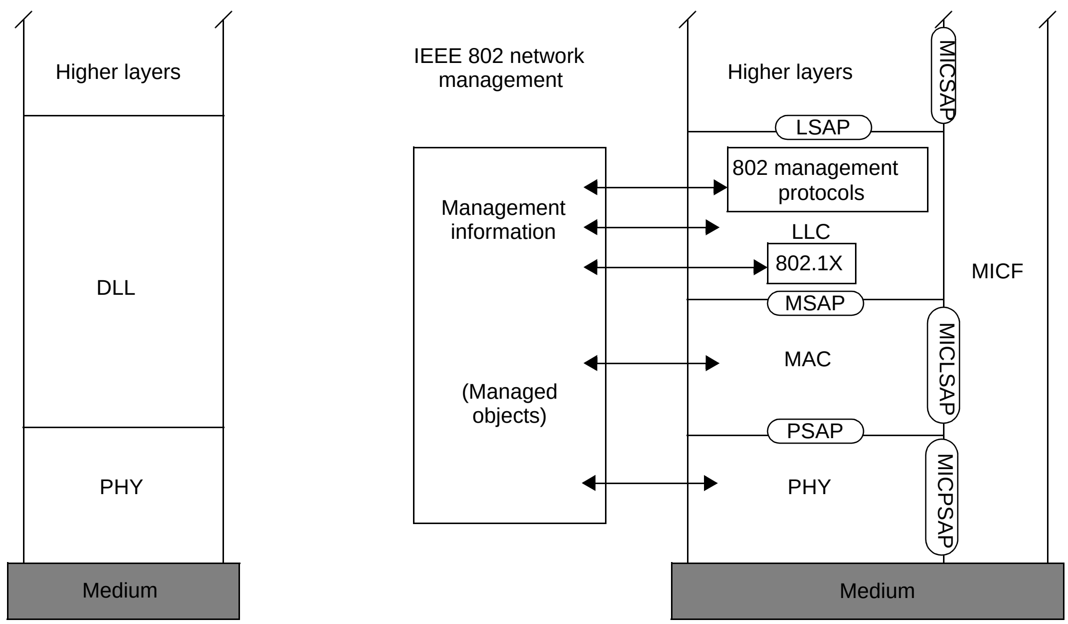


Figure 5—IEEE 802 RM with end-station management, security, and MIH

5.2 RM description for end stations

The IEEE 802 RM maps to the OSI/RM as shown in Figure 3. The applicable part of the OSI/RM consists of the lowest two layers: the DLL and the PHY. These map onto the same two layers in the IEEE 802 RM. The MAC sublayer of the IEEE 802 RM exists between the PHY and the LLC sublayer to provide a service for the LLC sublayer (certain MAC types provide additional MAC service features that can be used by LLC sublayer, in addition to the common core features). Service access points (SAPs) for connecting the layers and sublayers are shown in Figure 3.

5.2.1 SAPs

One or more link service access points (LSAPs) provide interface ports to support one or more higher layer users above the LLC sublayer.

In addition, the end station optionally provides one or more media-independent control service access points (MICSAPs) that interface between one or more higher layers and the control and management planes enabling higher layer information to pass to the MICF and vice versa.

The MAC sublayer provides one or more MAC service access points (MSAPs) as interfaces to the LLC sublayer in an end station. Clause 8 provides details of how broadcast and group addresses are constructed. The MAC sublayer optionally provides a media-independent control link service access point (MICLSAP), which is used to provide an interface to support control of the MAC by the MICF.

The PHY provides a PHY service access point (PSAP). In addition, the PHY optionally provides a media-independent control PHY service access point (MICPSAP), which is used to provide an interface port for the control of the PHY by the MICF.

5.2.2 LLC sublayer

The LLC sublayer contains a variety of entities, as illustrated in Figure 6.

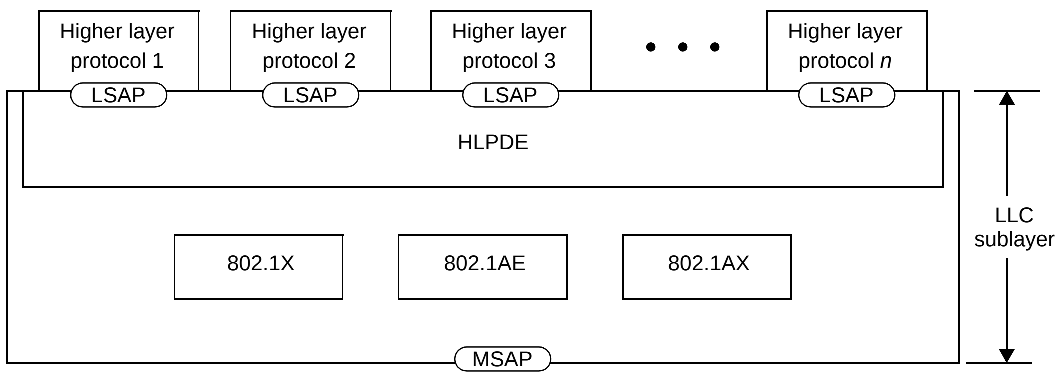


Figure 6—LLC sublayer in 802 RM

The higher layer protocol discrimination entity (HLPDE) is used by the LLC sublayer to determine the higher layer protocol to which to deliver an LLC sublayer protocol data unit (PDU). Two methods may be used in the HLPDE. The two methods are:

1) EtherType protocol discrimination (EPD), which uses the EtherType value made available to the LLC sublayer through the MSAP
2) LLC protocol discrimination (LPD), which uses the addresses defined in ISO/IEC 8802-2, including the Subnetwork Access Protocol (SNAP) format

IEEE Std 802.3™ is capable of natively representing the EtherType within its MAC frame format, which is used to support EPD. IEEE Std 802.3 also natively supports ISO/IEC 8802-2 LPD (over a limited range of frame sizes). In other IEEE 802 networks, such as IEEE Std 802.11™, LPD with SNAP is used. In either of these techniques, the EtherType is effectively being used as a means of identifying an LSAP that provides LLC sublayer service to the protocol concerned. For further details, refer to Clause 12 of IEEE Std 802.1AC-2016.

New IEEE 802 standards shall support protocol discrimination in the LLC sublayer using EPD.

IEEE Std 802.1AE™ provides MAC security with connectionless user data confidentiality, frame data integrity, and data origin authenticity by media access independent protocols and entities that operate transparently to MAC clients.

IEEE Std 802.1AX™ provides the ability to aggregate two or more links together to form a single logical link at a higher data rate.

IEEE Std 802.1X provides authentication, authorization, and cryptographic key agreement mechanisms to support secure communication between end stations connected by IEEE 802 networks.

5.2.3 MAC sublayer

The MAC sublayer provides a data transfer service to the LLC sublayer; a data unit received by the MAC sublayer from the LLC sublayer is transferred to a peer MAC sublayer for delivery to its LLC sublayer. The unit that carries the data for transfer between MAC sublayer entities is referred to as a MAC frame or simply a frame. In some MAC types, frames are also used to support other MAC sublayer functionality, such as the transfer of control or management information.

The principal functions of the MAC sublayer comprise the following:

- — Frame delimiting and recognition
- — Addressing of destination stations (both as individual stations and as groups of stations)
- — Conveyance of source-station addressing information
- — Transparent data transfer of PDUs from the next higher sublayer
- — Protection against errors, generally by means of generating and checking frame check sequences
- — Control of access to the physical transmission medium

Other functions of the MAC sublayer—applicable particularly when the supporting implementation includes interconnection devices such as bridges—include flow control between an end station and an interconnection device, as described in 5.3, and forwarding of frames according to their destination addresses to reduce the extent of propagation of frames in parts of an IEEE 802 network that do not contain communication paths leading to the intended destination end station(s).

The functions listed are those of the MAC sublayer as a whole. Responsibility for performing them is distributed across the transmitting and receiving end stations and any interconnection devices such as bridges. Devices with different roles, therefore, can behave differently in support of a given function. For example, the basic transmission of a MAC frame by a bridge is very similar to transmission by an end station, but not identical. Principally, the handling of source-station addressing is different.

The various MAC specifications all specify MAC frame formats in terms of a serial transmission model for the service provided by the supporting PHY. This model supports concepts such as “first bit (e.g., of a particular octet) to be transmitted” and a strict order of octet transmission in a uniform manner. However, the ways in which the model has been applied in different MAC specifications are not completely uniform with respect to bit-ordering within octets (see Clause 8, and particularly 8.6, for examples and explanation). The serial transmission model does not preclude current or future MAC specifications from using partly or wholly octet-oriented specifications of frame formats or of the interface to the PHY.

5.2.4 PHY

MAC entities use their respective PHY entities to exchange bits with their peers. The PHY provides the capability to transmit and receive modulated signals assigned to one or more channels for broadband.

Whereas the service offered to the MAC sublayer is expressed as the transfer of bits (in sequences representing MAC frames), the symbols that are encoded for transmission do not always represent individual bits. Particularly at speeds of 100 Mb/s and above or for wireless transmission, the PHY can map blocks of multiple bits to different multi-element symbols. In some PHY encodings, these symbols are subject to further transformation before transmission, and in some cases, the transmission is spread over multiple physical data paths.

5.2.5 Layer and sublayer management

The LLC, MAC, and PHY standards also include a management component that specifies managed objects and aspects of the protocol machine that provides the management view of these resources. See Clause 7 for further information.

5.3 Interconnection and interworking

In some cases, the end stations in an IEEE 802 network have no need to communicate with end stations on other networks. However, there are many cases in which end stations on an IEEE 802 network need to communicate with end stations on other networks; therefore, devices that interconnect the IEEE 802 network with other kinds of networks are required. In addition, several standard methods have been developed that permit a variety of interconnection devices to operate transparently to end stations on a network in order to extend the capabilities available to end stations, particularly in terms of the geographical extent and/or total number of end stations that can be supported.

Standard methods of interworking fall into the following three general categories, depending on the layer at which the corresponding interconnection devices operate:

— PHY interconnection, using devices usually termed *repeaters*, as described in 5.3.1
— MAC interconnection, using devices termed *bridges*, as described in 5.3.2
— Network-layer interconnection, using devices usually termed *routers*, as described in 5.3.3

5.3.1 Interconnection at the PHY

The original IEEE 802 standards were for end stations attached to a shared communication medium. This basic configuration is referred to as a *single access domain*; the domain consists of the set of stations such that, at most, only one can transmit at a given time, with all other stations acting as (potential) receivers. In this situation, the function of handling the “one-at-a-time” access arbitration is performed by the set of MACs on a shared medium.

A repeater is a device used to interconnect segments of the physical communications media, for example, to extend the range of a network when the physical specifications of the technology would otherwise be exceeded, while providing a single access domain for the attached stations.

5.3.2 MAC-sublayer interconnection: Bridges

5.3.2.1 Bridges and bridged IEEE 802 networks

Bridges are stations that interconnect multiple access domains. IEEE Std 802.1Q[15] provides the basic specification for bridge interworking among IEEE 802 networks. A bridged IEEE 802 network consists of one or more bridges together with the complete set of access domains that they interconnect. A bridged IEEE 802 network provides end stations belonging to any of its access domains with the connectivity of a network that contains the whole set of attached end stations.

A bridged network can provide for the following:

[15]Information on normative references can be found in Clause 2.

- — Communication between stations attached to networks of different MAC types that conform to the Internal Sublayer Service as specified in IEEE Std 802.1AC.
- — An increase in the total throughput of a network over that of a purely shared media network
- — An increase in the physical extent of, or number of permissible attachments to, a network
- — Partitioning of the physical network for administrative or maintenance reasons
- — Virtual local area networks (VLANs)
- — Provider bridging
- — Transfer of priorities between peer MAC entities
- — Support of latency, loss, and delay variation guarantees
- — Support for traffic management and virtualization within data center networks

NOTE—The term switch is sometimes used in the industry to refer to products that include an IEEE 802.1Q Bridge capability. The term Bridge, capitalized, refers to a bridge compliant with IEEE Std 802.1Q.

5.3.2.2 Bridge relaying and filtering

A Bridge processes protocols in the MAC sublayer and is functionally transparent to LLC sublayer and higher layer protocols. MAC frames are forwarded between access domains, or filtered (i.e., not forwarded to certain access domains), on the basis of addressing and protocol information contained in the MAC frame. Figure 7 shows the position of the bridging functions within the MAC sublayer; note particularly that relaying and filtering are considered to belong entirely within the MAC sublayer.

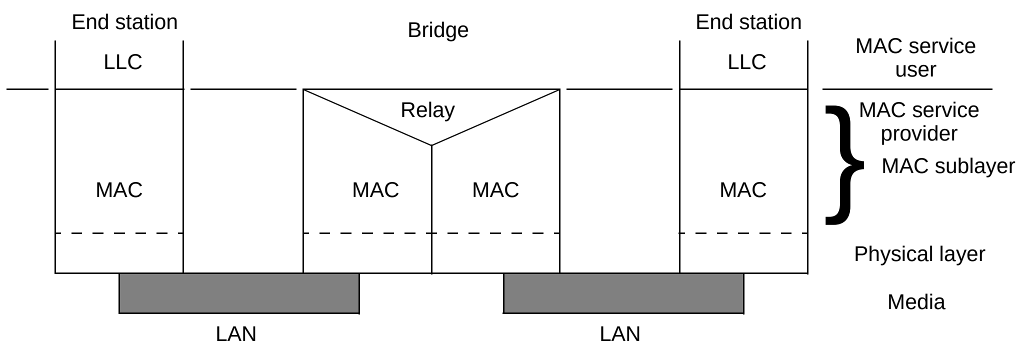


Figure 7—Internal organization of the MAC sublayer with bridging

Filtering by Bridges tends to confine traffic to only the parts of the bridged network that lie between transmitting end stations and the intended receivers. This permits a bridged network to support several transmitting end stations at any given time (up to the total number of access domains present).

5.3.2.3 Resolving topologies with multiple paths

A key aspect of IEEE Std 802.1Q is the specification of the spanning tree protocols and shortest path bridging (SPB) which are used by bridges to configure their interconnections in order to prevent looping data paths in the bridged IEEE 802 network. If the basic interconnection topology of bridges and networks contains multiple possible paths between certain points, use of the rapid spanning tree protocol (RSTP) blocks some paths in order to produce a simply connected active topology for the flow of MAC user traffic between end stations. For each point of attachment of a bridge to a network, the RSTP selects whether MAC user traffic is to be received and transmitted by the bridge at that point of attachment.

The RSTP adapts to changes in the configuration of the bridged IEEE 802 network, maintaining connectivity while avoiding data loops. Some configuration changes can cause temporary interruptions of connectivity between parts of the bridged IEEE 802 network, typically lasting for a few tens of milliseconds at most.

IEEE Std 802.1Q specifies a variant of RSTP, the multiple spanning tree protocol (MSTP), that can configure multiple, independent spanning trees within a bridged network. In addition, IEEE Std 802.1Q specifies SPB, which allows the use of shortest path communication within administratively defined network regions, while retaining concurrent support for all existing spanning tree protocols. The use of SPB, for unicast and multicast, allows multiple paths to be used simultaneously.

5.3.2.4 Transparent bridging

IEEE Std 802.1Q specifies transparent bridging operation, so called because the MAC bridging function does not require the MAC user frames transmitted and received to carry any additional information relating to the operation of the bridging functions; end-station operation is unchanged by the presence of bridges.

5.3.2.5 Provider bridging

IEEE Std 802.1Q specifies the method by which the MAC service is supported by virtual bridged LANs, the principles of operation of those networks, and the operation of VLAN-aware bridges, including management, protocols, and algorithms. The standard also enables a service provider to use the architecture and protocols specified in order to offer the equivalent of separate LANs, bridged LANs, or virtual bridged LANs to a number of customers, while requiring no cooperation between the customers and minimal cooperation between each customer and the service provider.

Provider backbone bridging further extends the concept of provider bridging by allowing a backbone network, under the administrative control of a single backbone service provider, to support multiple service providers, each administering its own distinct provider-bridged network to support distinct sets of customers.

5.3.2.6 Time sensitive networking (TSN)

TSN features are a set of protocols and mechanisms specified by IEEE 802 standards from which one can select the mechanisms that are best suited to meet the needs of the applications supported by a given network. These TSN mechanisms are add-ons to generic networking mechanisms in order to establish a common network that supports TSN Streams as well as other kinds of traffic. The goals of using TSN features typically include providing guaranteed data transport with low and bounded latency, low and bounded delay variation, and extremely low packet loss for TSN Streams. TSN features evolve and new capabilities are added as part of IEEE 802 standardization efforts. Therefore, the following list is incomplete and just provides a snapshot of TSN features:

a) Timing and Synchronization for Time-Sensitive Applications (IEEE Std 802.1AS-2020 [B1])
b) Credit-Based Shaper: (IEEE Std 802.1Q-2022, 5.4.1.5)
c) Frame Preemption (IEEE Std 802.3-2018 [B6] and IEEE Std 802.1Q-2022, 5.26)
d) Scheduled Traffic (IEEE Std 802.1Q-2022, 8.6.8.4)
e) Cyclic Queuing and Forwarding (IEEE Std 802.1Q-2022, 5.4.1.9)
f) Asynchronous Traffic Shaping (IEEE Std 802.1Q-2022, 5.4.1.10)
g) Per-Stream Filtering and Policing (IEEE Std 802.1Q-2022, 5.4.1.8)
h) Frame Replication and Elimination for Reliability (IEEE Std 802.1CB-2017 [B3])
i) Stream Reservation Protocol (IEEE Std 802.1Q-2022, clause 35.)
j) Link-local Registration Protocol (IEEE Std 802.1CS-2020 [B5])
k) Path Control and Reservation (IEEE Std 802.1Q-2022, 5.4.6)
l) TSN Configuration (IEEE Std 802.1Q-2022, 5.29)
m) Configuration Enhancements for Time-Sensitive Networking (IEEE Std 802.1Qdj-2023)

NOTE-There is no need to apply all the TSN features in a network and none of the TSN features are a requirement. The application area or actual deployment determine which TSN features are used in a given network, e.g., whether or not time synchronization is used. TSN profile standards, e.g., IEEE Std 802.1BA [B2] and IEEE Std 802.1CM [B4] select TSN features and give guidelines on their use in a particular application area.

5.3.2.7 Data center networking bridging

The IEEE 802.1 Working Group provides a series of standards and Bridging enhancements for data center networking (DCN). A data center is a facility composed of compute and storage servers interconnected by a high bandwidth network and located in a small area, typically not exceeding 100 m in diameter. DCN standards target network congestion for data centers and data center network virtualization. The DCN features can provide networks free of congestion loss and support for in server virtualized networking for attachment of containers and virtual machines. DCN features evolve and new capabilities are added as part of IEEE 802 standardization efforts. Therefore, the following list is incomplete and just provides a snapshot of DCN features:

a) Congestion Notification (IEEE Std 802.1Q-2022, Clause 30, Clause 31, Clause 32, Clause 33)
b) Priority-based Flow Control (IEEE Std 802.1Q-2022, Clause 36)
c) Enhanced Transmission Selection (IEEE Std 802.1Q-2022, Clause 37)
d) Congestion Isolation (IEEE Std 802.1Qcz-2023)
e) Edge Virtual Bridging (IEEE Std 802.1Q-2022, Clause 40, Clause 41, Clause 42, Clause 43)

5.3.2.8 Bridging example

Some Bridges are used to interconnect access domains that each contain a very small number of end stations (often, a single end station). Other Bridges interconnect multiple access domains that contain principally other Bridges. These Bridges and links are referred to as an IEEE 802 backbone network. Bridged IEEE 802 network configurations that involve these kinds of interconnection have become widespread as the technologies have developed. These configurations allow the construction of networks with much larger numbers of end stations and much higher aggregate throughput than was previously achievable.

Figure 8 illustrates an example of a bridged IEEE 802 network that can be configured with bridge-style interconnection. The Bridges A and B, and the IEEE 802.3 LAN configurations to which they attach, are typical of the older style of bridged IEEE 802 network in which a Bridge interconnects a small number of access domains, each containing many end stations, as is similar with K, L and M. The IEEE 802.3 connections to M and those between S and T and S and U form IEEE 802 backbone networks. On the other hand, the Bridges S, T, and U function as Bridges that combine IEEE 802.3 and IEEE 802.16™ networks. S and M are Bridges on an IEEE 802 backbone network, handling a number of network attachments. T and U are Bridges that support multiple end stations, with connection to an IEEE 802 backbone network. B and K also provide access to an IEEE 802 backbone network. The end station shown connected to S by a point-to-point link could be a server system.

5.3.3 Network-layer interconnection: Routers

Routers are interconnection devices that operate as IEEE 802 end stations. These process network layer protocols that operate directly above the LLC sublayer, with forwarding decisions based on network layer addresses. Details of this kind of interconnection lie outside the scope of IEEE 802 standards, but the various standard and proprietary network-layer protocols involved represent a substantial part of the user traffic on many IEEE 802 networks. In particular, IEEE 802 networks are often interconnected by routers for the IP and its related routing and management protocols, either directly to other IEEE 802 networks or by means of WAN connections.

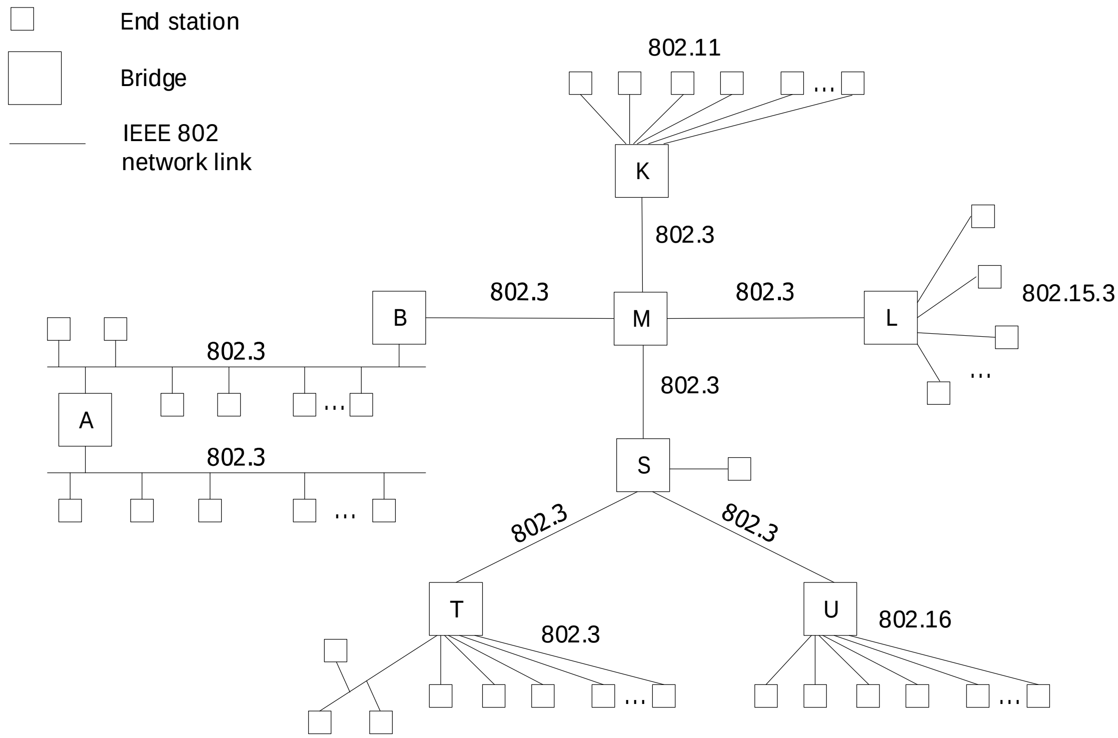


Figure 8—An example of a bridged IEEE 802 network

6. General requirements for an IEEE 802 network

6.1 Services supported

With the descriptions in Clause 5 as a basis, an IEEE 802 network can be characterized as a communication resource that provides sufficient capabilities to support the MAC service specified in IEEE Std 802.1AC, between two or more MSAPs. In particular, this requires the ability to convey LLC sublayer data from one MSAP to *n* other MSAPs, where *n* can be any number from 1 to the number of all of the other MSAPs on the network. An IEEE 802 network is required, at a minimum, to support the MAC Internal Sublayer Service specified in IEEE Std 802.1AC and support the use of EtherTypes for protocol identification at the LLC sublayer.

6.2 Error ratios

The error performance of IEEE 802 networks is as follows:

a) For wired or optical fiber physical media: Within a single access domain, the probability that a transmitted MAC frame (excluding any preamble) is not reported correctly at the PHY service interface of an intended receiving peer MAC entity, due only to operation of the PHY, shall be less than 8×10^{-8} per octet of MAC frame length.

b) For wired physical media with frames shorter than 2048 octets: The probability that an MAC service data unit (MSDU) delivered at an MSAP contains an undetected error, due to operation of the MAC service provider, shall be less than 5×10^{-14} per octet of MSDU length.

c) For wireless physical media, the error performance within a single access domain is variable over time, and no guarantee of service can be given.

NOTE—For example, the worst-case probability of losing a maximum-length IEEE 802.3 frame at the PHY is to be less than 1.21×10^{-4}, or approximately 1 in 8250. The worst-case probability that a similar frame, which contains an MSDU of 1500 octets, is delivered with an undetected error is to be less than 7.5×10^{-11}, or approximately 1 in 13 300 000 000.

7. IEEE 802 network management

7.1 General

The provision of an adequate means of remote management is an important factor in the design of today's network equipment. Such management mechanisms fall into two broad categories: those that provide general-purpose management capability, allowing control and monitoring for a wide variety of purposes, and those that provide specific capabilities aimed at a particular aspect of management. These aspects of management are discussed in 7.2 and 7.3, respectively.

7.2 General-purpose IEEE 802 network management

This subclause introduces the functions of management to assist in the identification of the requirements placed on IEEE 802 network equipment for support of management facilities, and it identifies general-purpose management standards that may be used as the basis of developing management specifications for such equipment.

7.2.1 Management functions

Management functions relate to users' needs for facilities that support the planning, organization, supervision, control, protection, and security of communications resources. These facilities may be categorized as supporting the functional areas of configuration, fault, performance, security, and accounting management. These can be summarized as follows:

- Configuration management provides for the identification of communications resources, initialization, reset and shut-down, the supply of operational parameters, and the establishment and discovery of the relationships between resources.
- Fault management provides for fault prevention, detection, diagnosis, and correction.
- Performance management provides for evaluation of the behavior of communications resources and of the effectiveness of communication activities.
- Security management provides for the protection of resources.
- Accounting management provides for the identification and distribution of costs and the setting of charges.

Management facilities in IEEE 802 network equipment address some or all of these areas, as appropriate to the needs of that equipment and the environment in which it is to be operated.

7.2.2 Management architecture

The management facilities specified in IEEE 802 standards are based on the concept of managed objects that model the semantics of management operations. Operations on a managed object supply information concerning, or facilitate control over, the managed object and thereby, indirectly, the process or entity associated with that object.

Operations on a managed object can be initiated by mechanisms local to the equipment being managed (e.g., via a control panel built into the equipment) or can be initiated from a remote management system by means of a general-purpose management protocol carried using the data services provided by the IEEE 802 network to which the equipment being managed is connected.

The Simple Network Management Protocol (SNMP), as described in IETF RFC 3411 [B8], and Network Configuration Protocol (NETCONF), as described in RFC 6241 [B11], are examples of general-purpose management protocol that can be used for the management of IEEE 802 network equipment.

7.2.3 Managed object definitions

In order for an IEEE 802 standard to specify management facilities, it is necessary for it to specify managed objects that model the operations that can be performed on the communications resources specified in the standard. The components of a managed object definition are as follows:

a) A definition of the functionality provided by the managed object, and the relationship between this functionality and the resource to which it relates.
b) A definition of the syntax that is used to convey management operations, and their arguments and results, in a management protocol.
c) An address that allows the management protocol to specifically communicate with the managed object in question. In IEEE 802 this is done with either an object identifier (OID), as described in Clause 10, or a Uniform Resource Name (URN), as described in Clause 11.

The functionality of a managed object can be described in a manner that is independent of the protocol that is used; this abstract definition can then be used in conjunction with a definition of the syntactic elements required in order to produce a complete definition of the object for use with specific management protocols.

SNMP is used in many cases together with the structure of management information known as SMIv2 (IETF RFC 2578, IETF RFC 2579 [B6], and IETF RFC 2580 [B7]), which uses a set of macros based on a subset of ASN.1 for defining managed objects. YANG (IETF RFC 7950 [B12]) is a data modeling language used to model configuration data, state data, remote procedure calls, and notifications for network management protocols. The YANG objects are modeled in IEEE 802 standards using the Object Management Group (OMG) unified modeling language (UML) diagrams.

IEEE 802 networks can support management with SNMP MIBs or YANG to describe management objects.

The choice of notational tools for defining managed objects depends on the available management protocols the standard supports.

7.3 Special-purpose IEEE 802 network management standards

Special-purpose protocols relating to the management functionality of IEEE 802 stations can be developed when the use of a general-purpose management protocol is inappropriate. Examples of special-purpose management protocols that can be found in the family of IEEE 802 standards include the Connectivity Fault Management Protocol specified in IEEE Std 802.1Q; the Operations, Administration, and Maintenance (OAM) Protocol specified in IEEE Std 802.3; and the Link Layer Discovery Protocol (LLDP) in IEEE Std 802.1AB™.

8. MAC addresses

8.1 Terms and notational conventions

In this standard, the term *MAC address* is used to refer to a 48-bit or 64-bit number that is used to identify the source and destination MAC entities. A MAC address may also be used to identify a MAC SAP. In many IEEE 802 standards, the term *MAC address* refers only to a 48-bit MAC address. In some IEEE 802 standards, the term *extended address* is used to refer to a 64-bit MAC address.

If interoperability through bridges is required for a standard, then 48-bit MAC addressing is required. New IEEE 802 standards that only require routed connectivity should use 64-bit MAC addressing.

Hexadecimal representation is a sequence of octet values in which the values of the individual octets are displayed in order from left to right, with each octet value represented as a 2-digit hexadecimal numeral and with the resulting pairs of hexadecimal digits separated by hyphens. The order of the hexadecimal digits in each pair, as well as the mapping between the hexadecimal digits and the bits of the octet value, is derived by interpreting the bits of the octet value as a binary numeral using the normal mathematical rules for digit significance.

Bit-reversed representation is a sequence of octet values in which the values of the individual octets are displayed in order from left to right, with each octet value represented as a 2-digit hexadecimal numeral and with the resulting pairs of hexadecimal digits separated by colons. The order of the hexadecimal digits in each pair, as well as the mapping between the hexadecimal digits and the bits of the octet value, is derived by reversing the order of the bits in the octet value and interpreting the resulting bit sequence as a binary numeral using the normal mathematical rules for digit significance.

NOTE—The bit-reversed representation is of historical interest only and is no longer applicable to any active IEEE 802 standard.

See 8.2.2 for a comparative example of bit-reversed and hexadecimal representation.

8.2 Universal addresses

8.2.1 Concept and overview

The concept of universal addressing is based on the idea that all potential members of a network need to have a unique identifier. The advantage of a universal address is that a station with such a MAC address can be attached to any IEEE 802 network in the world with an assurance that the MAC address is unique, if all stations adhere to the rules and the security of the network prevents malicious spoofing of MAC addresses.

NOTE—Other network standards that are not IEEE 802 standards also use MAC addresses as specified in this standard.

A universal address is a MAC address that is globally unique.[16] Two different lengths of universal addresses have been specified by the IEEE Registration Authority (RA): 48-bit Extended Unique Identifier (EUI-48) and 64-bit Extended Unique Identifier (EUI-64).

8.2.2 Assignment of universal addresses

The IEEE RA has the responsibility for the administration of IEEE 802 network universal addresses.[17] The IEEE RA is recognized by ISO/IEC as the registration authority for universal addresses for the ISO/IEC

[16]And beyond the earth as well. For example, IEEE Std 802.15.4 was deployed on the Mars helicopter.

[17]Interested applicants should contact the IEEE RA https://standards.ieee.org/regauth

8802 series of standards. The responsibility for defining the procedures is discharged by the IEEE Registration Authority Committee, which is chartered by the IEEE Standards Association Board of Governors.

The IEEE RA assigns universal addresses (i.e., EUI-48s and EUI-64s) in various address block sizes. Each block assigns a common value (leading bits) that is common to all addresses in the assignment as described in Table 1.[18]

Table 1—IEEE RA assignment summary

IEEE RA assignment	Number of assigned bits	Block size of EUI-48	Block size of EUI-64	Used for company or organization identifier?
Company ID (CID)	24	0 (zero)	0 (zero)	yes (CID)
MAC Address Block Large (MA–L)	24	2^{24}	2^{40}	yes [Organizationally Unique Identifier (OUI)]
MAC Address Block Medium (MA–M)	28	2^{20}	2^{36}	no
MAC Address Block Small (MA–S)	36	2^{12}	2^{28}	yes (OUI-36 only)

NOTE 1—The terms *OUI* and *OUI-36* were previously used by the IEEE RA to refer both to the globally unique 24-bit OUI and 36-bit identifiers and to the “products” that included the identifier and a block of addresses. The OUI "product" was replaced by the *MA-L* that, in addition to the address block, includes an assignment of an OUI; likewise, the OUI-36 was replaced by the *MA-S* that includes the assignment of an address block and an OUI-36. The use of these terms is not always consistent within IEEE standards.

NOTE 2—A CID assignment is used to identify a company or organization. It is not used to create universal addresses. For more information see 8.4.

The standard representation of MA-L, MA-M, and MA-S is to use the hexadecimal representation. See 8.6 for further specification relating to use of the bit-reversed representation.

The structure of an OUI is illustrated in Figure 9, which also highlights the structure of the first octet of an 802 network MAC address. The first octet of a MAC address has the same structure for all 802 network address, so this first octet structure applies to all address block assignments (MA-S, MA-M and MA-L); and also to 48-bit or 64-bit MAC addresses. The least significant bit (LSB) of the first octet is the individual/group (I/G) address bit. The next-to-lsb of the first octet for the MAC address is the universal/local (U/L) address bit.

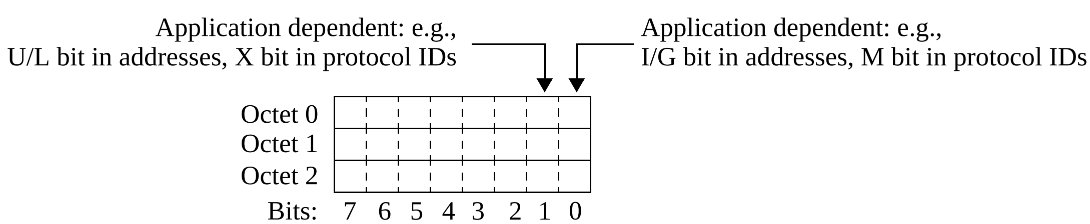


Figure 9—Structure of an OUI

[18]More information on MA-L, MA-M, and MA-S assignment can be found on the IEEE RA web site, https://standards.ieee.org/develop/regauth/.

The I/G address bit is used to identify the destination MAC address as an individual MAC address or a group MAC address. If the I/G address bit is zero, it indicates that the MAC address field is an individual MAC address. If this bit is one, the MAC address is a group MAC address that identifies one or more (or all) stations connected to the IEEE 802 network. The all-stations broadcast MAC address is a special group MAC address of all ones.

The U/L bit indicates whether the MAC address has been assigned by a local or universal administrator. Universal addresses have the U/L bit set to zero. If the U/L bit is set to one, the address is locally administered, as described in 8.4.

A universal address consists of two parts: the leading bits (24, 28, or 36) are assigned by the IEEE RA to an assignee with the U/L bit set to zero and the remaining bits from the assigned block of addresses. An example of an EUI-48 is shown in Figure 10. For MA-M and MA-S, the final 4 bits of the assigned number are in a nibble that is not adjacent to the other bits in the assigned number when displayed with LSB on the left and most significant bit (MSB) on the right. For example, when using an MA-S to create an EUI-48, the MA-S value is contained in octets 0, 1, 2, 3 and the most significant four bits of octet 4, and the value assigned by the assignee is contained in the least significant 4 bits of octet 4 and in octet 5.

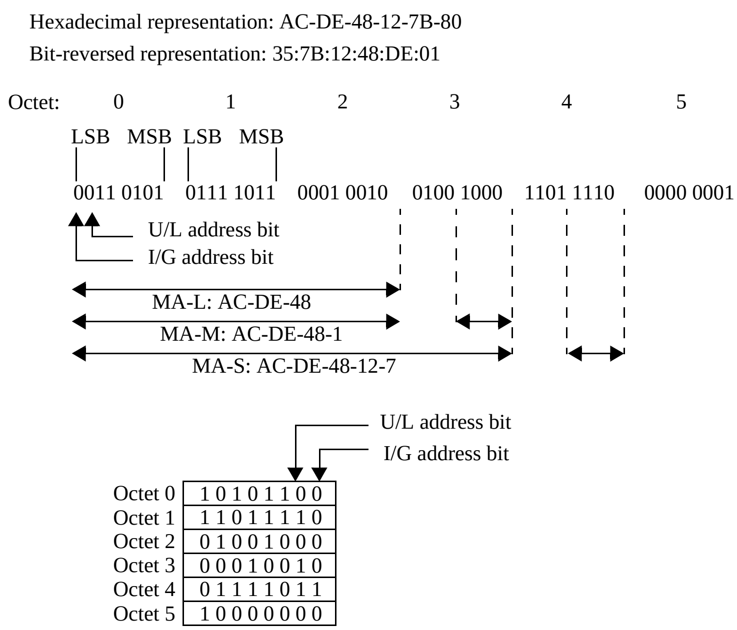


Figure 10—Example EUI-48

NOTE 3—The octet string AC-DE-48-12-7B-80 is used in this standard because it is clear when a bit pattern is reversed. This octet string could be in use and is not a reserved value. While AC-DE-48 is used as the same first 3 octets for the examples of MA-L, MA-M, and MA-S, the first 3 octets are different for valid assigned IEEE RA values.

An example of an EUI-64 is illustrated in Figure 11.

NOTE 4—The upper, bit-stream representation of the EUI-48 in Figure 10 and the EUI-64 in Figure 11 shows the LSB of each octet first; this corresponds to the data-communications convention for representing bit-serial transmission in left-to-right order, applied to the model for transmission of EUI-48 fields (see 5.2.3) and EUI-64 fields. See also 8.6 for further discussion of bit-ordering issues. The lower, octet-sequence representation shows the bits within each octet in the usual order for binary numerals; the order of octet transmission is from the top downward.

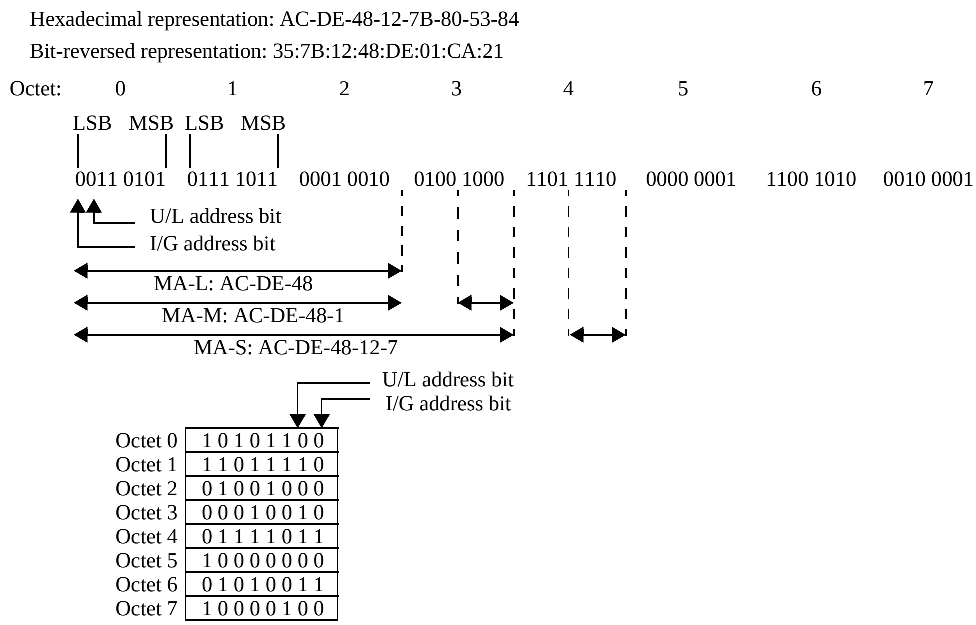


Figure 11—Example EUI-64

8.2.3 Assignment by organizations

The IEEE RA does not assign an MA-L, MA-M, or MA-S to any organization having previously received an address block assignment, unless specific requirements are met. The requirements are designed to assure that all addresses in an assigned block are used for network attachments. Requirements for an additional allocation include the organization certifying it has exhausted or will soon exhaust its previous assignment.

It is important to note that universal addresses created from MA-Ls, MA-Ms, or MA-Ss should not be used for purposes that would lead to skipping large numbers of them (for example, as product identifiers for the purpose of aiding company inventory procedures). The IEEE RA asks that organizations implement internal policies that minimize the misuse of addresses, that would unnecessarily exhaust an address block prematurely. There are sufficient identifiers to satisfy the intended needs for a long time, even as uses of IEEE 802 network stations grow – however, no address space is infinite.

The method that an assignee uses to ensure that no two of its stations carry the same universal address is not defined in this standard. However, the users of networks worldwide expect to have unique addresses. The ultimate responsibility for assuring that user expectations and requirements are met, therefore, lies with the organization offering such stations.

8.2.4 Uniqueness of address assignment

It is recommended that each MAC entity on an IEEE 802 network have its own unique MAC address.

NOTE—Some implementations have used a single MAC address to identify more than one of the system's MAC entities. This approach does meet the requirements of IEEE 802.1Q™ MAC bridging.

8.3 Interworking with 48-bit and 64-bit MAC addresses

In response to concerns that the EUI-48 space could be exhausted by the breadth of products requiring unique identifiers, 64-bit MAC addresses were introduced. Initially, new IEEE standards projects that did not require backward compatibility with EUI-48 were requested to use 64-bit MAC addresses. This led to some IEEE 802 standards adopting 64-bit MAC addressing, which cannot be bridged onto IEEE 802 networks that use 48-bit MAC addressing. Truncating a 64-bit MAC address into a 48-bit field can lead to two stations having the same 48-bit value. Instead, traffic between 64-bit and 48-bit MAC addressed networks needs to be routed at a layer above the DLL.

Bridging for an IEEE 802 network with 64-bit MAC addresses is currently not specified.

8.4 Local MAC addresses

8.4.1 Concept and overview

The U/L bit of a local MAC address is set to one, indicating that the remaining bits (i.e., all bits except the U/L bit and the I/G bit, which is set as described in 8.2.2) are locally administered. Local MAC addresses are not presumed globally unique across all IEEE 802 networks. The locally administered bits of local MAC addresses are arbitrarily assignable under the condition that local MAC addresses are unique within a LAN (which may be a bridged LAN or virtual bridged LAN). In a virtual bridged LAN wherein the bridges use Independent VLAN Learning, the uniqueness condition applies to each VLAN rather than to the entire virtual bridged LAN. Any failure of such uniqueness invalidates the fundamental premises of IEEE 802 network operation and can lead to disruption. Therefore, administrators should ensure that the probability of local MAC address non-uniqueness is acceptably small.

While a local administrator may assign addresses throughout the local range, the optional Structured Local Address Plan (SLAP) specifies different assignment approaches in four specified regions of the local MAC address space.

Unlike universal addresses, which are persistent to the MAC entity, local MAC addresses are not necessarily persistent. The local MAC address assigned to a MAC entity, including any subsequent change to that assignment, is entirely within the scope of the local administration.

8.4.2 Local MAC address assignment protocols

An address assignment protocol assigning local MAC addresses to devices on a LAN should ensure uniqueness of those addresses, per the description of F.1.2 of IEEE Std 802.1Q. That standard's Annex F also identifies risks of non-uniqueness.

When multiple address assignment protocols operate on a LAN without centralized administration, address duplication is possible, even if each protocol alone is designed to avoid duplication, unless such protocols assign addresses from disjoint address pools.

Administrators who deploy multiple protocols on a LAN in accordance with the SLAP enables the unique assignment of local MAC addresses within the LAN as long as each protocol maintains unique assignments within its own address subspace.

8.4.3 Structured Local Address Plan (SLAP)

The SLAP specifies use of local MAC address space. Under the SLAP, the use is specified differently in four quadrants of local MAC address space.

The least and second least significant bits of the initial octet of a MAC address are designated the M bit and X bit, respectively, as shown in Figure 12. The third and fourth least significant bits of the initial octet in the local MAC address are designated the Y bit and Z bit, respectively, as illustrated for a 48-bit address in Figure 12 (see NOTE 4 of 8.2.2).

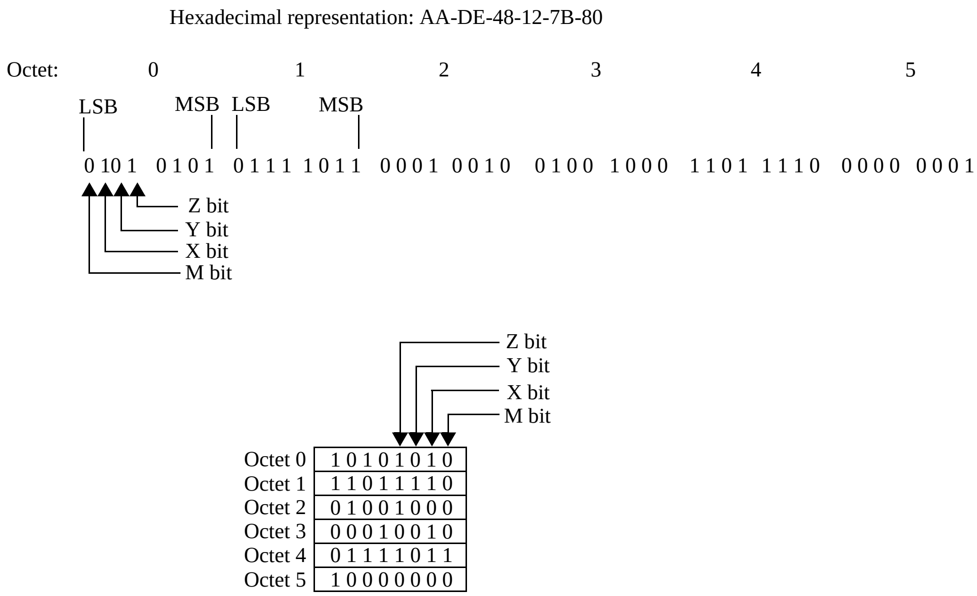


Figure 12—M, X, Y and Z bits of local MAC address

NOTE 1—The specific address used in Figure 12 and Figure 13 is not a reserved value.

NOTE 2—The bit-stream representation of the addresses in Figure 12 and Figure 13 show the LSB of each octet first; this corresponds to the data-communications convention for representing bit-serial transmission in left-to-right order. See also 8.6 for further discussion of bit-ordering issues.

A local MAC address exists in one of four SLAP quadrants, each identified by a different combination of the Y and Z bits, as indicated in Table 2. That table also indicates the SLAP local identifier type specified for each SLAP quadrant. The SLAP local identifier types are specified in 8.4.4.

Table 2—SLAP quadrants, addresses and bit settings

SLAP quadrant name	M bit	X bit	Y bit	Z bit	SLAP local identifier type	SLAP local addresses	Number of bits (including I/G and U/L) assigned by IEEE RA or IEEE Std 802
01	I/G	1	0	1	Extended Local	ELI-48, ELI-64	24 (CID)
11	I/G	1	1	1	Standard Assigned	SAI-48, SAI-64	4
00	I/G	1	0	0	Administratively Assigned	AAI-48, AAI-64	4
10	I/G	1	1	0	*Reserved*	*Reserved*	—

For compliance to the SLAP, local MAC addresses shall be assigned only as valid Extended Local Identifiers (ELIs), Standards Assigned Identifiers (SAIs) or Administratively Assigned Identifiers (AAIs).

While IEEE Std 802 assigns four SAI bits, additional SAI bits may also be assigned by IEEE 802 standards.

8.4.4 SLAP local identifier types

8.4.4.1 Extended Local Identifier (ELI)

A SLAP identifier of type “Extended Local” is known as an Extended Local Identifier (ELI). ELIs are in SLAP quadrant “01”. The X, Y and Z its of an ELI are defined in Table 2. An ELI may be used as a local MAC address; such an address is known as an ELI address.

The IEEE RA uniquely assigns a 24-bit identifier known as the Company ID (CID)[19] to identify a company, organization, entity, protocol, etc., as described in the IEEE RA tutorial [B2].

An ELI is based on an assigned CID. Two different lengths of ELI are specified: ELI-48 is a 48-bit ELI, and ELI-64 is a 64-bit ELI, as described in Table 3.

Table 3—IEEE RA CID and ELI summary

IEEE RA assignment	Number of bits (including I/G and U/L) assigned by IEEE RA	Address block size, ELI-48	Address block size, ELI 64
CID	24	2^{24}	2^{40}

The structure of the CID is identical to that of the OUI, which is illustrated in Figure 9. However, the CID is not used to create universal addresses. Each CID assignment provided by the IEEE RA has the X bit set to one, so that any MAC address created by extension of the CID, as shown in Figure 13, exists in locally administered address space. Changing the X bit of an OUI assigned by the IEEE RA is not authorized by the IEEE RA, does not result in a valid CID, can invalidly duplicate a valid CID assignment, and shall not be used as the basis of an ELI. Likewise, changing the X bit of an CID assigned by the IEEE RA is not authorized by the IEEE RA, does not result in a valid OUI, can invalidly duplicate a valid OUI assignment, and shall not be used as the basis of an EUI.

While each CID assignment provided by the IEEE RA has the M bit set to zero, the corresponding bit of the ELI address represents the I/G bit and is set as described in 8.2.2.

An ELI-48 or ELI-64 created as an extension of the CID consists of two parts: the leading 24 bits are assigned as the CID, with the I/G bit assignable as described in 8.2.2, and the remaining bits are specified as an extension by the CID assignee or by a protocol designated by the CID assignee.

Several CIDs are reserved as Administrator CIDs and not assigned exclusively. The local administrator is an implicitly authorized assignee of the Administrator CIDs and may, within the SLAP, create and assign an ELI as an extension of an Administrator CID. Administrator CIDs are specified in Table 4.

An example of an ELI-48 created by extension of a CID is shown in Figure 13 (see NOTE 4 of 8.2.2). An ELI-64 is created with the same method but using two additional octets.

NOTE—The specific CID and ELI-48 used in this example are not reserved values.

Figure 13 also illustrates the location of the Y bit and Z bit in a CID.

[19] More information on CIDs, follow the tutorial link from https://standards.ieee.org/regauth to locate the appropriate tutorial.

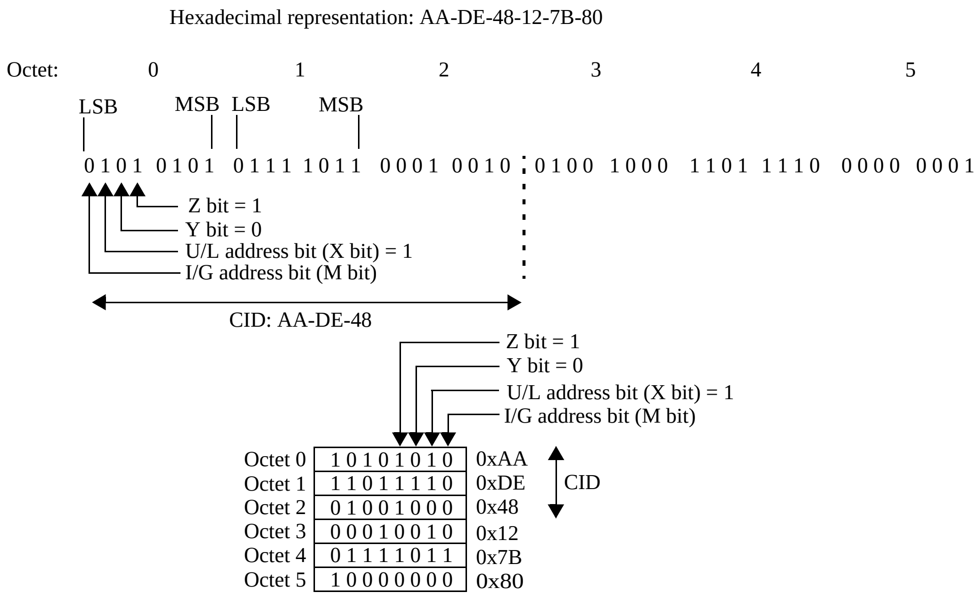


Figure 13—Example ELI-48 created as an extension of CID

Table 4—Administrator CIDs

Administrator CIDs
0x3AA3F8
0xCA30BF
0x4A07D6
0xFA94F1

IEEE 802 standards support the use of ELI-48 and ELI-64 based on CID only for CID values that specify zero for the Y bit and one for the Z bit. The IEEE RA assigns CIDs only with zero for the Y bit and one for the Z bit.

In some cases, an ELI assignment protocol may assign the 24-bit or 40-bit extension of the ELI to convey specific information. Such information may be interpreted by receivers and bridges that recognize the CID and are cognizant of the protocol identified by the CID. The functionality of receivers and bridges that do not recognize the protocol is not affected. Such address formats, and their interpretation, are outside the scope of this standard but may be specified by the entity to which the specific CID is assigned by the IEEE RA.

Note, in contrast to such uses of local addresses, IEEE RA policies (detailed in [B2]) intended to prevent premature exhaustion of the universal address space do not allow for similar subdivision of a universal address block. Such subdivision does not provide assurance that addresses in the block have been used for an identifiable physical instance per EUI-48 identifier

8.4.4.2 Standard Assigned Identifier (SAI)

A SLAP identifier of type “Standard Assigned” is known as a Standard Assigned Identifier (SAI). SAIs are in SLAP quadrant “11”. The X, Y and Z bits of an SAI are defined in Table 2. An SAI may be used as local MAC address; such an address is known as an SAI address. The specification of this quadrant is reserved for a future IEEE 802 standard (see E.3).

An SAI is assigned by a protocol specified in an IEEE 802 standard.

Two different lengths of an SAI are specified: SAI-48 is a 48-bit SAI, and SAI-64 is a 64-bit SAI.

Multiple protocols for assigning SAI may be specified within various IEEE 802 standards. Coexistence of such protocols may be supported by restricting each to assignments within a subspace of SAI space. In some cases, an SAI assignment protocol may assign the SAI to convey specific information. Such information may be interpreted by receivers and bridges that recognize the specific SAI assignment protocol, as identified by the subspace of the SAI. The functionality of receivers and bridges that do not recognize the protocol is not affected. SAI address formats, and their interpretation, are outside the scope of this standard but may be specified in other IEEE 802 standards.

8.4.4.3 Administratively Assigned Identifier (AAI)

A SLAP identifier of type “Administratively Assigned” is known as an Administratively Assigned Identifier (AAI). AAIs are in SLAP quadrant “00”. The X, Y and Z its of an AAI are defined in Table 2. An AAI may be used as local MAC address; such an address is known as an AAI address.

Administrators who wish to assign local MAC addresses in an arbitrary fashion (for example, randomly) and yet maintain compatibility with other assignment protocols operating under the SLAP on the same LAN may assign a local MAC address as an AAI.

Two different lengths of an AAI are specified: AAI-48 is a 48-bit AAI, and AAI-64 is a 64-bit AAI, as described in Table 5.

Table 5—AAI summary

IEEE 802 assignment	**Number of bits (including I/G and U/L) assigned by IEEE Std 802**	**Address block size, ELI-48**	**Address block size, ELI 64**
Bits M, X, Y, Z	4	2^{44}	2^{60}

Per IETF RFC 2464 [B5], a multicast IPv6 packet uses a Ethernet destination address whose first 2 octets are the value 0x3333. Such addresses lie within the AAI quadrant of the multicast local MAC address space. Therefore, administrators who wish to support IPv6 should not assign AAIs beginning with 0x3333.

8.4.4.4 SLAP quadrant “10”

Under the SLAP, the local identifiers in SLAP quadrant “10” are reserved for future use.

While SLAP quadrant “10” identifiers remain reserved, they may be administratively used and assigned in accordance with the considerations specified for AAI usage, without effect on SLAP assignments. However, administrators should be cognizant of possible future specifications regarding SLAP quadrant “10” that would render administrative assignment incompatible with the SLAP.

8.4.5 Network Unique Identifier (NUI)

Network Unique Identifier (NUI) is an identifier that is unique within the IEEE 802 LAN (which may be a bridged LAN or virtual bridged LAN). An NUI-48 is a 48-bit NUI that is an EUI-48, ELI-48, SAI-48 or AAI-48. An NUI-64 is a 64-bit NUI that is an EUI-64, ELI-64, SAI-64 or AAI-64.

8.5 Standardized group MAC addresses[20]

The previous subclauses described the assignment of individual and group MAC addresses and protocol identifiers for public or private use by private organizations. There is also a need for standardized 48-bit and 64-bit group MAC addresses to be used with standard protocols. The administration of these standardized 48-bit and 64-bit group MAC addresses, including the procedure for application and a list of currently assigned values, is described on the web pages for the IEEE RA[21]. Many standardized group MAC addresses used in standards are assigned within a block of universally administered addresses derived from an MA-L that has been assigned by the IEEE 802.1 Working Group for this purpose.

8.6 Bit-ordering and different MACs

Clause 5 describes the reference models for IEEE Std 802 networks. IEEE Std 802 interoperability is determined at the MAC Service Access Point (MSAP). Each IEEE Std 802 network standard specifies how octets from the LLC are transmitted and received. Most IEEE 802 network standards have multiple options for the Physical Layer, often with these Physical Layer options tied to different data rates. Though most IEEE 802 network Physical Layers encode multiple bits or multiple octets of the MAC frame for transmission on the medium, a few IEEE 802 network Physical Layers have a one-to-one mapping of a bit in the MAC frame to an encoded bit on the medium.

IEEE Std 802 specifies how MAC address I/G and U/L bits are positioned in the destination and source address fields (e.g., see Figure 10). Some MAC standards have specified serial transmission of the bits of an octet LSB first (historically referred to as canonical order), and other MAC standards specifying transmission of the MSB first (historically referred to as bit-reversed order), but both specifying the I/G bit as being the first bit of a frame to be transmitted with bit serial transmission. Historically, this has created problems when MAC addresses occur within the information field of a frame (e.g., a management frame).

It is strongly recommended that the historical problems observed with different serial bit transmission orders are best avoided by only transmitting the LSB of octets first. If though MSB (bit-reversed) serial transmission order is used, the standard shall assure that a MAC address will be the same at the MSAP whether it is a MAC address field or an address appearing in the information field.

[20] These were previously referred to as standard group MAC addresses.

[21] See the “Standard Group MAC addresses” at: https://standards.ieee.org/products-programs/regauth/tut/

9. Protocol identifiers and context-dependent identifiers

9.1 Introduction

This clause describes methods that allow multiple network layer protocols to be carried over an IEEE 802 network. These methods provide for the following:

- — The operation of multiple network layer protocols
- — The migration of existing networks to future standard protocols
- — The accommodation of future higher layer protocols

Within a given layer, entities can exchange data by a mutually agreed upon protocol mechanism. A pair of entities that do not support a common protocol cannot communicate with each other. For multiple protocols to operate within a layer, it is necessary to determine which protocol is to be invoked to process a service data unit delivered by the lower layer.

Various network and higher layer protocols have been assigned reserved LPD addresses or EtherTypes, as recorded by the IEEE RA[22]. These addresses permit multiple protocols to operate over a single MAC entity.

This clause describes the protocol identifiers used for the LPD and EPD methods as well as a protocol identifier based on OUI-36.

The EPD method shall be the primary specified means for protocol identification at the LLC sublayer in IEEE 802 standards developed after January 2011[23], excluding amendments to existing standards.

9.2 EtherTypes

9.2.1 Format, function, and administration

EtherType protocol identification values are assigned by the IEEE RA[24] and are used to identify the protocol that is to be invoked to process the user data in the frame. An EtherType is a sequence of 2 octets, interpreted as a 16-bit numeric value with the first octet containing the most significant 8 bits and the second octet containing the least significant 8 bits. Values in the 0–1535 range are not available for use.

Examples of EtherTypes are 08 00 and 86 DD, which are used to identify IPv4 and IPv6, respectively.

It is strongly recommended when designing new protocols to be identified by an EtherType, that fields are defined to provide for subtyping. The format used for subtyping in a protocol described in 9.2.4 is recommended.

9.2.2 Public EtherType assignments subset

The IEEE Registration Authority (RA) provides a public listing of EtherType assignments[25]. Many of these are for private or proprietary purposes. However, others are incorporated into well-known standards. In some cases, the IEEE RA Public Listing for an EtherType identifies an assignee without explicitly

[22]More information can be found at https://standards.ieee.org/products-programs/regauth/.

[23]IEEE Std 802.2™-1989 (reaffirmed 2003) was administratively withdrawn as an IEEE standard on 11 January 2011 in deference to the stabilized standard ISO/IEC 8802-2:1998 where the same material continues to be available.

[24]More information on EtherTypes can be found on the IEEE RA web site, https://standards.ieee.org/products-programs/regauth/ether-type/.and https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries.

[25]The EtherType public listing is the public view of the EtherType registry managed by the Registration Authority (see https://standards.ieee.org/regauth).

identifying the standards in which the use of that EtherType is specified. For ready reference by users and developers of such standards, Annex F identifies some well-known EtherTypes and the protocols they identify. This subset is derived by combining the EtherTypes listed in the ietf-ethertypes YANG module specified in IETF RFC 8519 [B13] with the subset of EtherTypes defined by IEEE 802 Standards (e.g., IEEE 802.1Q, 802.3, etc.) and as provided by participants that developed this standard. Information on products released after that date can be found on the IEEE SA Registration Authority web site: https://standards.ieee.org/products-programs/regauth/ethertype/ and https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries. The subset in Table F.1 and in F.3 is provided solely for the convenience of users of this standard and does not constitute an endorsement by IEEE of the listed protocols.

The EtherType public listing includes the following fields, specified by the EtherType assignee:

— **Assignment** — The hexadecimal representation of the EtherType.
— **Assignment Type** — The type is EtherType[26].
— **Company Name** — The registrant of the Assignment.
— **Company Address** — The address of the registrant.
— **Protocol** — A brief protocol description, as provided by the registrant.

This Standard includes the following fields in Table F.1 for use by the YANG module:

a) **Friendly Name** — A short alphanumeric name for the Assignment that is unique within the YANG module in F.2 and is used to enumerate the entry.
b) **Short Description** — A short description of the assigned protocol per its typical usage.
c) **Reference** — A reference to a standard associated with the EtherType assignment.

A YANG model representation can be found in F.3.2.

9.2.3 EtherTypes for prototype and vendor-specific protocol development

The EtherType identifier space is a finite resource. The vendor-specific protocol identifier is a means whereby protocol developers may assign permanent protocol identifier values without consuming type values from this limited resource. This can be useful for prototype, experimental, and private/proprietary protocols to be developed without impacting the rest of the EtherType namespace.

These objectives are supported by the following EtherType assignments and associated rules for their use:

a) Two EtherType values, known as the Local Experimental EtherTypes, as specified in 9.2.4, assigned, as the name implies, for experimental use within a local area
b) A single EtherType value, known as the OUI Extended EtherType, as specified in 9.2.5, assigned for the identification of vendor-specific protocols

The values of the Local Experimental EtherTypes and the OUI Extended EtherType are listed in Table 6.

9.2.4 Local Experimental EtherTypes

The Local Experimental EtherTypes are only intended for use in conjunction with experimental protocol development within a privately administered development network, for example, within an experimental network that has no wide area connectivity. Within that network, a local administrator is free to use a Local Experimental EtherType and to assign subtypes for protocol development purposes. However, by virtue of

[26]EtherType is the only assignment type for the records in the EtherType public listing.

Table 6—Assigned EtherType values

Name	Value
Local Experimental EtherType 1	88-B5
Local Experimental EtherType 2	88-B6
OUI Extended EtherType	88-B7

the way these EtherTypes are intended to be used, the following practical and administrative constraints apply to their use:

a) Since the format for protocols using the Local Experimental EtherTypes does not contain a means to identify the administrative domain, it might not be possible to identify the protocol of a frame if protocols developed within different administrative domains using Local Experimental EtherTypes are used in the same network. Hence, the use of these EtherTypes to identify protocols can only be achieved reliably if all uses of the EtherTypes are within the control of a single administrative domain. Therefore, these EtherTypes shall not be used in protocols or products that are to be released for use in the wider networking community, as freeware, shareware, or any part of a company's commercial product offering. Products shall be transitioned to a product EtherType before it is deployed in an environment outside the developing organization's administrative control, for example, when deployed with a customer or any other connected environments for testing.

b) Local Experimental EtherType shall not be permanently assigned for use with a given protocol or protocols.

c) End stations that bound any administrative domain should be configured to prevent frames containing a Local Experimental EtherType from passing either into or out of a domain in which its contents can be misinterpreted. For example, the default configuration of any firewall should be to not pass this EtherType.

A Local Experimental EtherType is processed by the HLPDE in the same manner as other EtherType values.

In order to allow for different experimental protocols, sub-protocols, and versions to coexist within the same experimental network, a protocol subtype and a protocol version identifier shall be used in conjunction with the Local Experimental EtherType value. Figure 14 shows the format of an IEEE 802.3 frame carrying a Local Experimental EtherType. The lengths of the protocol subtype and the protocol version identifier fields, as well as their order of appearance within the frame, are not constrained by this standard.

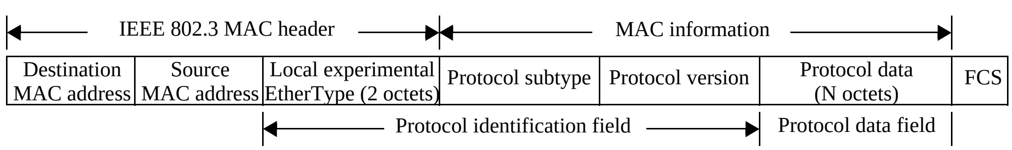


Figure 14—Example of an IEEE 802.3 frame carrying the Local Experimental EtherType

Two Local Experimental EtherType values are provided to allow protocols that need more than one distinct EtherType value, or two distinct protocols, to be developed within a single administrative domain. In particular, the provision of two Local Experimental EtherTypes allows for cases where it is necessary to be able to distinguish protocols or sub-protocols at the EtherType level in order to facilitate the use of filtering actions in bridges.

The combination of the Local Experimental EtherType value, the protocol subtype, and the protocol version provides the protocol identifier for the experimental protocol. The values assigned to the protocol subtype and protocol version are locally administered; their meaning cannot, therefore, be correctly interpreted outside of the administrative domain within which the value was allocated.

NOTE—The use of this format provides for a simple migration path to the use of a distinct EtherType permanently assigned to the protocol. The routine examination of proposals made to the IEEE RA for the allocation of EtherTypes includes a check that the proposed protocol format has sufficient subtype capability to withstand enhancement by the originator without the need for the assignment of a further EtherType in the future, and inclusion of the subtype and version values could be deemed to meet this requirement. While the existence of such a mechanism in the protocol specification is not in itself sufficient to ensure that an application for an EtherType succeeds, its existence is a necessary element of an acceptable protocol design. The subtyping mechanism described here offers one way that this requirement may be met.

9.2.5 OUI Extended EtherType

The OUI Extended EtherType provides a means of protocol identification similar to that offered by the SNAP identifier described in 9.5.1. Like the SNAP identifier, the OUI Extended EtherType allows an organization to use protocol identifiers, as described in 9.5. An organization allocates protocol identifiers to its own protocols in a manner that ensures that the protocol identifier is globally unique. An illustration of a protocol identifier created with an OUI or CID is illustrated in Figure 15.

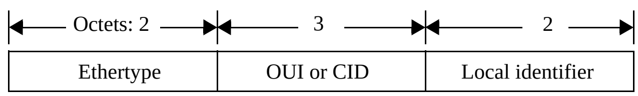


Figure 15—Protocol identifier composed of an OUI or CID

The EtherType field shall cointain the Vendor Specific EtherType value.

The OUI field shall contain the OUI or CID assigned to the entity.

The Local Identifier field shall contain a 2 octet numeric value assigned by the entity identified by the OUI or CID.

NOTE 1—The requirement for global uniqueness of protocol identifiers means that if protocol identifier X has been allocated for use by an organization’s protocol, then that protocol identifier can be used with either the SNAP identifier or the OUI Extended EtherType to identify that protocol. Conversely, it means that protocol identifier X cannot be used to identify any other protocol.

The OUI Extended EtherType is processed by the HLPDE. Immediately following the EtherType value is a protocol identifier, as described in 9.5, consisting of a 3-octet OUI or CID value followed by 2 octets administered by the OUI or CID assignee. The OUI or CID value provides an administrative context within which the assignee can allocate values to a 16-bit protocol subtype. This approach is closely similar to the LPD-based SNAP identifier mechanism specified in 9.5; however, the OUI Extended EtherType is used instead of the LPD method.

Figure 16 shows the format of an IEEE 802.3 frame carrying the OUI Extended EtherType in the Length/Type field. The value used for the OUI component of the protocol identifier is an OUI or CID value assigned to the organization that has developed the vendor-specific protocol. The combination of the OUI Extended EtherType, the OUI or CID value, and the 16-bit value administered by the OUI or CID assignee provides a unique protocol identification field for the vendor-specific protocol. The 16-bit values are administered by the organization to which the OUI or CID has been assigned; their meaning can, therefore, be correctly interpreted only by reference to the organization that owns the OUI or CID concerned.

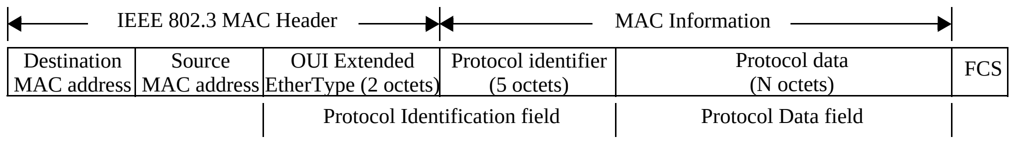


Figure 16—IEEE 802.3 frame with the OUI Extended EtherType encoded in the Length/Type field

NOTE 2—As the protocol designer is free to specify the structure of the Protocol Data field, pad octets can be included in the definition of this field, for example, for the purposes of alignment with 4-octet or 8-octet boundaries.

Good protocol development practice is to use a protocol subtype, along with a protocol version identifier in order to avoid having to allocate a new protocol identifier when a protocol is revised or enhanced. Users of the OUI Extended EtherType are, therefore, encouraged to include protocol subtype and version information in the specification of the protocol data for their protocols.

This method of protocol identification is intended to be used in products or protocols that are planned to be released into multi-vendor environments outside of the control of the administration that assigns the protocol identifier. The use of this mechanism allows such protocols to be developed and distributed without the need for a specific EtherType to be assigned for the use of each protocol.

As the OUI Extended EtherType is a normal EtherType value, it is possible to use the encoding described in 9.4 to carry its value within an LPD PDU, using a SNAP identifier with the IETF RFC 1042 [B3] OUI. Figure 17 shows the format of an IEEE 802.3 frame carrying the OUI Extended EtherType encoded in this way. In this case, it would be more appropriate to use the SNAP identifier directly (i.e., omit the RFC 1042 OUI and OUI Extended EtherType fields shown in Figure 17); however, this is a valid encoding of the OUI Extended EtherType that can result from the application of the encapsulation described in 9.4.

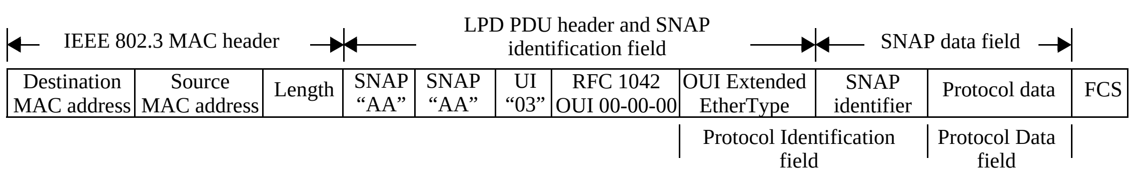


Figure 17—IEEE 802.3 frame with the OUI Extended EtherType encoded in an LPD PDU

9.3 OUI, CID and OUI-36 as protocol identifiers

An organization that has an OUI, CID or OUI-36 assigned to it may use its OUI, CID or OUI-36 to assign universally unique protocol identifiers (potentially with additional octets as part of the identifier) to identify its own protocols, and to use in protocols described in IEEE 802 standards.

The position of the M bit (see NOTE 4 of 8.2.2) for a CID is illustrated in Figure 18 and for an OUI-36 in Figure 19. All OUI, CID and OUI-36 identifiers assigned by the IEEE RA have the M bit set to zero; values with the M bit set to one are reserved.

The X bit of a protocol identifier is the bit of the first octet adjacent to the M bit. All OUI and OUI-36 identifiers assigned by the IEEE RA with the X bit set to zero may be used as OUI or OUI-36 protocol identifiers, respectively, and may also be used to create EUI-48 and EUI-64 addresses. All CIDs assigned by the IEEE RA have the X bit set to one and may be used as a protocol identifier.

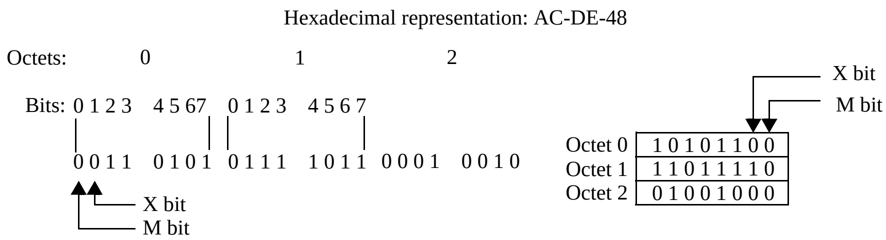


Figure 18—Format of an OUI or CID used as a protocol identifier

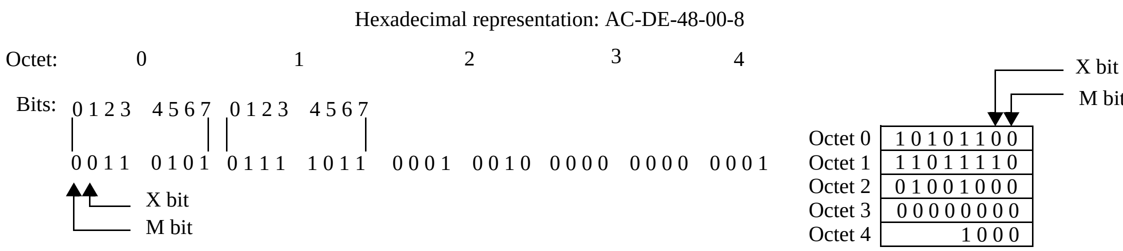


Figure 19—Format of an OUI-36 used as a protocol identifier

9.4 Encapsulation of Ethernet frames with LPD

This subclause specifies the standard method for conveying Ethernet frames across IEEE 802 networks that offer only the LPD function and not the EPD function in the LLC sublayer.

An Ethernet frame conveyed on an LPD-only IEEE 802 network shall be encapsulated in a SNAP data unit contained in an LPD PDU of type UI, as follows:

a) The Protocol Identification field of the SNAP data unit shall contain a SNAP identifier in which
   1) The three OUI octets each take the value zero.
   2) The two remaining octets take the values, in the same order, of the 2 octets of the Ethernet frame’s EtherType.
b) The Protocol Data field of the SNAP data unit shall contain the user data octets, in order, of the Ethernet frame.
c) The values of the Destination MAC Address field and Source MAC Address field of the Ethernet frame shall be used in the Destination MAC Address field and Source MAC Address field, respectively, of the MAC frame in which the SNAP data unit is conveyed.

NOTE—This encapsulation was originally specified in IETF RFC 1042 [B3], which contains recommendations relating to its use. Further recommendations are contained in IETF RFC 1390 [B4].

9.5 SNAP

SNAP provides a method for multiplexing and demultiplexing of private and public protocols among multiple users of the LLC sublayer. An organization that has an OUI or CID assigned to it may use its OUI or CID to assign universal protocol identifiers to its own protocols, for use in the protocol identification field of SNAP data units.

9.5.1 SNAP identifier

The SNAP identifier is 5 octets in length and follows the LPD header in a frame. The first 3 octets of the SNAP identifier consist of the OUI or CID. The remaining 2 octets are administered by the assignee. In the

SNAP identifier, an example of which is shown in Figure 20 (see NOTE 4 of 8.2.2), the OUI or CID is contained in octets 0, 1, and 2 with octets 3 and 4 being assigned by the assignee of the OUI or CID.

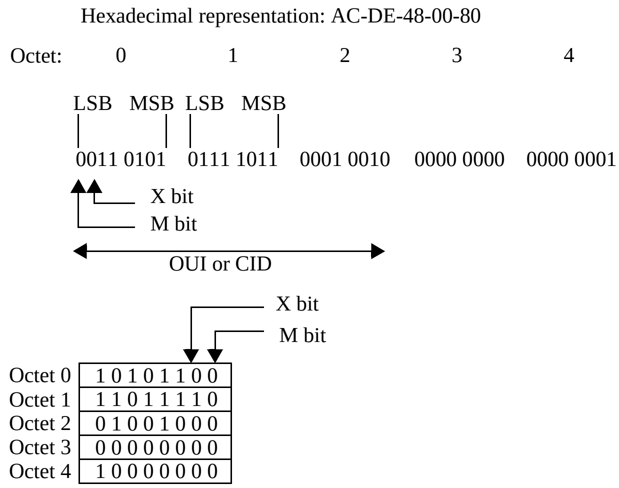


Figure 20—SNAP identifier

The standard representation of a SNAP identifier is as a string of 5 octets using the hexadecimal representation.

The LSB of the first octet of a SNAP identifier is referred to as the M bit. All SNAP identifiers derived from OUIs or CIDs assigned by the IEEE RA shall have the M bit set to zero; values with the M bit set to one are reserved.

SNAP identifiers may be assigned universally or locally. The X bit of a SNAP identifier is the bit of the first octet adjacent to the M bit. All universally assigned SNAP identifiers derived from OUIs have the X bit set to zero. All universally assigned SNAP identifiers derived from CIDs have the X bit set to one.

9.5.2 SNAP address

The reserved LPD address for use with SNAP is called the SNAP address. It is specified to be the bit pattern (starting with the LSB) Z1010101, in which the symbol Z indicates that either value 0 or 1 can occur, depending on the context in which the address appears (as specified in ISO/IEC 8802-2). The two possible values have hexadecimal representation AA.

The SNAP address identifies, at each MSAP, a single LSAP for standard, public, and private protocol usage. To permit multiple public and private network layer protocols to coexist at one MSAP, each public or private protocol using SNAP shall employ a protocol identifier that enables SNAP to discriminate among these protocols.

9.5.3 SNAP data unit format

Each SNAP data unit shall conform to the format shown in Figure 21 and shall form the entire content of the LPD information field.

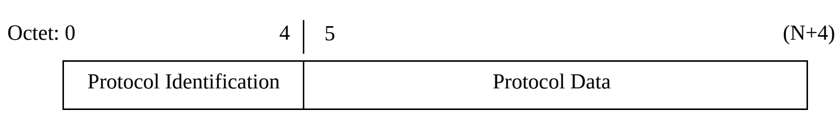


Figure 21—SNAP data unit format

In Figure 21, the Protocol Identification field contains a SNAP identifier whose format and administration are as described in 9.5.1. The Protocol Data field is a field whose length, format, and content are specified by a public or private protocol specification.

Figure 22 illustrates how a SNAP data unit appears in a complete MAC frame (the IEEE 802.3 MAC format is used for the example). The LPD control field (CTL) is shown for PDU type UI, Unnumbered Information, which is the most commonly used PDU type in this context; however, other information-carrying LPD PDU types may also be used with SNAP identifiers.

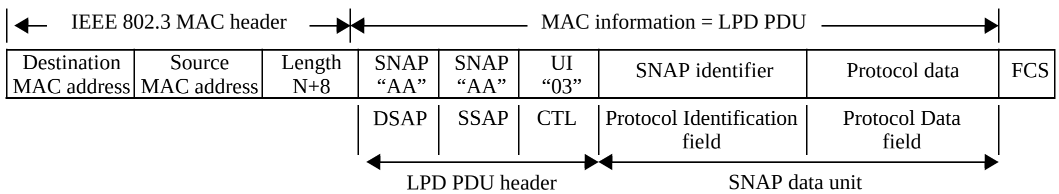


Figure 22—SNAP data unit in IEEE 802.3 MAC frame

9.6 Context-dependent identifiers

The IEEE RA tutorial [B2] explains the creation of context dependent identifiers. Just as the OUI is extended to create EUI-48 and EUI-64 identifiers, or a CID can be extended to create a locally administered MAC address, other extended identifiers can be created from an OUI or CID assignment. Such extended identifiers are referred to as context-dependent identifiers. These identifiers are not necessarily globally unique, but are intended to only be unique within a well specified context.

In some cases, the context of a context-dependent identifier is the IEEE 802 LAN. Since this is the same context in which local identifiers operate, the SLAP of Clause 8 provides a basis to assign unique context-dependent identifiers, such as NUI-48 and NUI- 64, within that context.

10. Allocation of OID values in IEEE 802 standards

10.1 General

From time to time, various IEEE 802 standards have a requirement to allocate OID values. The most common example is for defining management information base (MIB) objects for SNMP, but other examples exist. MIB modules describe the structure of the management data of a device subsystem and use a hierarchical name space based on OIDs to identify variables. This clause specifies a simple and consistent OID hierarchy, based on the use of the OID value that has been assigned by ISO to identify the IEEE 802 series of standards. This hierarchy should be used by all current and future IEEE 802 Working Groups and can be used flexibly to meet the needs of the standards developed by those working groups. This establishes a consistent practice within IEEE 802 for the development and allocation of OIDs. Consistency of OID allocation facilitates implementation and operation of IEEE 802-compliant equipment.

10.2 OIDs and ISO standards

An OID is an ASN.1 data type, specified in ITU-T Recommendation X.660, that is used as a means of defining unique identifiers for objects. Values of the OID data type can then be used to name the objects to which they relate.

The OID data type consists of a sequence of one or more non-negative integers, often referred to as arcs, that specify a hierarchy, or tree, of OID values. The first arc in the sequence identifies the registration authority responsible for allocating the values of the second and subsequent arcs. For example:

iso (1)

indicates that an initial arc value of 1 identifies ISO as the registration authority. Subsequent arcs in the sequence are determined by ISO or are allocated by registration authorities subordinate to ISO.

Under the iso arc, a second arc has been allocated to identify organizations recognized by ISO, such as the IEEE; hence, the two-integer sequence

iso (1) iso-identified-organization (3)

Under the iso-identified-organization arc, a subsequent arc has been allocated to identify the IEEE; hence, the three-integer sequence

iso (1) iso-identified-organization (3) ieee (111)

indicates that the fourth integer identifies a particular registry within the IEEE and that the allocation of the fourth and subsequent arcs is the responsibility of the IEEE. Under the ieee arc, the IEEE RA has specified an arc for the numbered series of IEEE standards; hence, the four-integer sequence

iso (1) iso-identified-organization (3) ieee (111)
standards-association-numbered-series-standards (2)

indicates that the fifth integer is used to identify a particular IEEE numbered series standard. The actual number corresponding to the numbered series standard is used in the fifth arc; hence, the following identifies the IEEE 802 series of standards:

iso (1) iso-identified-organization (3) ieee (111)
standards-association-numbered-series-standards (2) ieee-802 (802)

The responsibility for allocating the subsequent arcs under iso (1) iso-identified-organization (3) ieee (111) standards-association-numbered-series-standards (2) ieee-802 (802) lies with IEEE 802.

As the standard number 802 is used to identify the member of the family of IEEE 802 standards, this particular sequence of integer values can form the basis of an OID hierarchy for use by the individual standards in the IEEE 802 family. The act of assigning a number to a standard has the effect of automatically assigning an OID arc to that standard; therefore, no further administrative effort is needed before that standard can allocate OID values under that point in the tree, using the subsequent arcs.

10.3 The OID hierarchy for IEEE 802 standards

The OID value assigned to the family of IEEE 802 standards is:

> iso (1) iso-identified-organization (3) ieee (111)
> standards-association-numbered-series-standards (2) ieee-802 (802)

The next arc under iso (1) iso-identified-organization (3) ieee (111) standards-association-numbered-series-standards (2) ieee-802 (802) is used to differentiate between members of the family of IEEE 802 standards, by using it as a working group designator, as follows:

> iso (1) iso-identified-organization (3) ieee (111)
> standards-association-numbered-series-standards (2) ieee-802 (802) ieee802dotX (X)

where X is the working group number of the IEEE 802 Working Group responsible for that standard. These arcs are assigned for use in all current and future IEEE 802.X standards.

For example, under this hierarchy, the value used for standards developed by the IEEE 802.3 Working Group is:

> iso (1) iso-identified-organization (3) ieee (111)
> standards-association-numbered-series-standards (2) ieee-802 (802) ieee802dot3 (3)

and the value used for IEEE 802.11™ standards is:

> iso (1) iso-identified-organization (3) ieee (111)
> standards-association-numbered-series-standards (2) ieee-802 (802) ieee802dot11 (11)

The working group concerned is free to decide how further arcs are allocated within their standards, in a manner that makes sense for their particular needs.

It is the responsibility of each working group to ensure that any values that are allocated to the fifth and subsequent arcs are documented, in a manner that ensures that the same OID value cannot be assigned to two different objects. In the IEEE 802.1 Working Group, this has been achieved in the past by placing tables of OID allocations in an annex within the standard concerned[27]; in the IEEE 802.3 Working Group, a master spreadsheet of allocated OID values is maintained by the chair and posted on the working group's website. For future allocations, adopting a master spreadsheet approach is appropriate.

It is important that the allocation scheme for the fifth and subsequent arcs is constructed in a manner that leaves appropriate "escapes" for uses that cannot be foreseen. The simple expedient of allocating a "type of allocation" value as the fifth arc is sufficient to ensure that such an escape is always available.

---

[27] More information on IEEE 802.1 OIDs can be found on the working group web site, https://www.ieee802.org/1/pages/OIDS.html.

10.4 The OID hierarchy under iso(1) std(0) iso8802(8802)

The 2001 revision of this standard documented the use of iso(1) std(0) iso8802(8802) as the root arc under which IEEE 802 standards would develop their OID hierarchies. The use of this root arc is deprecated.

10.5 Migration from previous OID allocations

The OID hierarchy described in this clause need not have any effect upon existing IEEE 802 standards that have already solved this problem by using a specific allocation obtained elsewhere (for example, from ANSI).

With the hierarchy as specified in this clause, as each new working group is created in IEEE 802, its base OID arc is also created automatically; therefore, no administrative effort is required on the part of the working group, other than to determine how the fifth and subsequent arcs are used in its standards.

For those working groups that have already made use of other allocation schemes (e.g., IEEE 802.3 and IEEE 802.1), it may be considered appropriate to migrate existing allocations to the hierarchy specified in this clause. In considering this, the following should be borne in mind:

— While it might be perceived as “tidy” to have all IEEE 802 OIDs allocated under a single arc of the OID tree, this is not a requirement for any other reason; one OID value is no better or no worse than any other from a technical point of view (with the possible exception that the encoded length can vary with the number of arcs to be encoded), as long as any given OID identifies a single object.

— If migration is desired, there is no requirement to remove the old OID values[28]. Indeed, this is not permitted for objects in SNMP MIB modules that are not obsolete, as specified in IETF RFC 2578, nor is it permitted to associate such objects with more than one OID value. Instead, new definitions are required to be created and registered under the desired OID tree[29].

[28] There is no general requirement that an object should have only a single identifier; if it has more than one, then it can be “reached” by following more than one set of branches of the naming tree, just as a map can provide more than one path to a destination.

[29] This appears to contradict the earlier statement and footnote that indicate that it does not matter if multiple OIDs point at the same object; however, this is a specific requirement imposed on MIB objects for SNMP by the relevant IETF standards, and not a general rule.

11. Allocation of Uniform Resource Name (URN) values in IEEE 802 standards

11.1 Introduction

From time to time, some IEEE 802 standards have a requirement to allocate Uniform Resource Name (URN) values—the most common example being for the purpose of defining data models using the YANG data modeling language defined in IETF RFC 6020 [B10] and IETF RFC 7950 [B12], but other examples exist. This clause defines a simple and consistent URN hierarchy, based on the use of the base URN value that has been assigned by the Internet Assigned Numbers Authority (IANA) for use in IEEE standards. All current and future IEEE working groups can use this hierarchy flexibly to meet the needs of the standards defined by those working groups. This hierarchy provides a consistent practice within IEEE 802 for the development and allocation of URNs. Consistency of URN allocation facilitates implementation and operation of IEEE 802 compliant equipment.

NOTE—While the focus of this Clause is on the use of URN values in IEEE 802 standards, the base URN value identified in 11.2 and the hierarchy of values that follows forms a basis for the assignment of URN values in all IEEE standards, not just those developed by IEEE 802.

11.2 The IEEE Namespace ID and Namespace Specific String

URN values used in IEEE standards use the following Namespace ID (NID) value assigned to the IEEE (see IETF RFC 3406 and IETF RFC 8069):

ieee

The Namespace Specific String (NSS) of all URNs that use the IEEE NID shall use the following structure:

urn:ieee:{IEEEresource}:{ResourceSpecificString}

The strings used as values of IEEEresource and ResourceSpecificString are case-insensitive.

There are potential uses of URNs in the IEEE outside of standards use. Only standards use is considered in this standard; therefore, the IEEEresource is always as follows:

std

Hence, all URN values assigned for use in the context of IEEE standards are of the following form:

urn:ieee:std:{ResourceSpecificString}

NOTE—The mechanism for allocation of URN values used by the IEEE is fully conformant with IETF RFC 3406 and is documented in IETF RFC 8069.

11.3 ResourceSpecificString values in IEEE 802 standards

ResourceSpecificString values identify the IEEE standard that has assigned the URN value, and the particular resource defined by that standard that the URN value identifies. The structure of ResourceSpecificString is as follows:

{IEEE standard designation}:{resourceType}:{resourceIdentifier}

{IEEE standard designation} is the standard designation assigned to the base standard that defines the URN value. For example, in the case of IEEE Std 802.1Q, the standard designation is 802.1Q; in the case of IEEE Std 802.11, the standard designation is 802.11. Where URN values are assigned in amendments or corrigenda to a base standard, the base standard's IEEE standard designation shall be used, not the IEEE standard designation of the amendment or corrigendum. The IEEE standard designation shall not include any colons. The form of standard designation numbers is as specified in the IEEE SA Project Numbering Policy.[30]

{resourceType} identifies the type of resource to which the URN value applies. A single value of resourceType is defined for use across all IEEE 802 standards as follows:

yang

The yang resourceType shall be used to create any URN in YANG modules defined in IEEE 802 standards.

Should further resourceType values be required for consistent use across multiple IEEE 802 standards, they would be defined via future amendments to this standard. Further resourceType values that are specific to a designated IEEE 802 standard can be defined within that standard.

The {resourceIdentifier} identifies a specific resource, in the context of the designated IEEE standard and the resourceType. All resourceIdentifier values are specified within the designated standard.

For example, in IEEE Std 802.1Q, a URN value for use in a YANG module would take the following form:

urn:ieee:std:802.1Q:yang:{resourceIdentifier}

Or in IEEE Std 802.11, a URN value for use in a YANG module would take the following form:

urn:ieee:std:802.11:yang:{resourceIdentifier}

[30]The current IEEE SA Numbering Policy Document is found at https://mentor.ieee.org/myproject/Public/mytools/init/parnum.pdf. Some IEEE projects use a numbering method that predates this policy

Annex A

(informative)

Bibliography

Bibliographic references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] IEEE Project Authorization Request (PAR) P802.1CQ, Draft Standard for Local and Metropolitan Area Networks: Multicast and Local Address Assignment, February 2016.[31]

[B2] IEEE Registration Authority Tutorial, "Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI) and Company ID (CID)".[32]

[B3] IETF RFC 1042, A Standard for the Transmission of IP Datagrams over IEEE 802 Networks. Postel, J., and J. Reynolds, Feb. 1988.[33]

[B4] IETF RFC 1390, Transmission of IP and ARP over FDDI Networks. Katz, D., Jan. 1993.

[B5] IETF RFC 2464, Transmission of IPv6 Packets over Ethernet Networks.

[B6] IETF RFC 2579, STD 58, Textual Conventions for SMIv2. McCloghrie, K., D. Perkins, J. Schoenwaelder, J. Case, M. Rose, and S. Waldbusser, Apr. 1999.

[B7] IETF RFC 2580, STD 58, Conformance Statements for SMIv2. McCloghrie, K., D. Perkins, J. Schoenwaelder, J. Case, M. Rose, and S. Waldbusser, Apr. 1999.

[B8] IETF RFC 3411, STD 62, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.

[B9] IETF RFC 5677, IEEE 802.21 Mobility Services Framework Design (MSFD). Melia, T., G. Bajko, S. Das, N. Golmie, and J. C. Zuniga, Dec. 2009.

[B10] IETF RFC 6020, YANG—A Data Modeling Language for the Network Configuration Protocol (NETCONF), October 2010.

[B11] IETF RFC 6241, Network Configuration Protocol (NETCONF), June 2011.

[B12] IETF RFC 7950, The YANG 1.1 Data Modeling Language, August 2016.

[B13] IETF RFC 8519, YANG Data Model for Network Access Control Lists (ACLs), March 2019.

[B14] IISO/IEC 7498-1:1994, Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model.

[31]IEEE publications are available from The Institute of Electrical and Electronics Engineers (https://standards.ieee.org/)
[32]The tutorial is available at https://standards.ieee.org/regauth. Follow the tutorial link and search for the tutorial title.
[33]IETF documents (i.e., RFCs) are available the Internet Engineering Task Force (https://www.rfc-archive.org/).

Annex B

(informative)

RMs for IEEE 802 standards

B.1 IEEE 802.3 RMs

IEEE Std 802.3 offers multiple options, each of which has a different RM.

The basic RM for IEEE 802.3 stations without optional sublayers is illustrated in Figure B.1.

RS	reconciliation sublayer	MSAP	MAC service access point
LSAP	link service access point	PSAP	PHY service access point

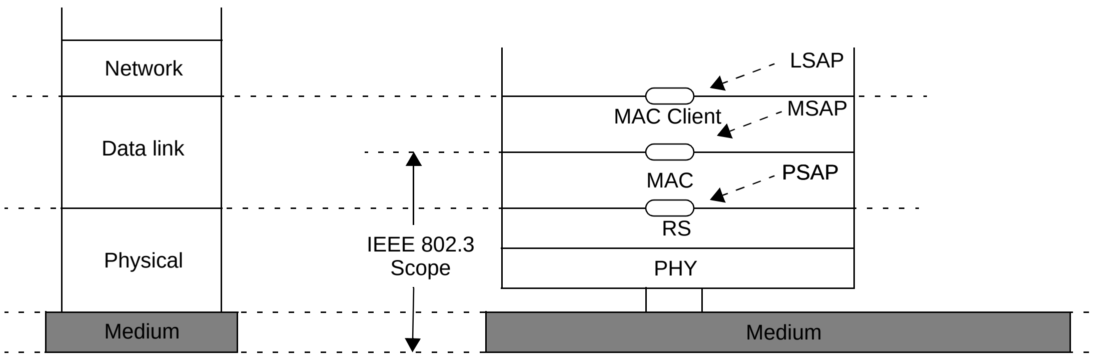


Figure B.1—Basic RM for IEEE 802.3 stations

The RM for IEEE Std 802.3 is illustrated in Figure B.2.

OAM	operations, administration and maintenance sublayer	MSAP	MAC service access point
		OSAP	OAM service access point
RS	reconciliation sublayer	MCSAP	MAC control service access point
LSAP	link service access point	PSAP	PHY service access point

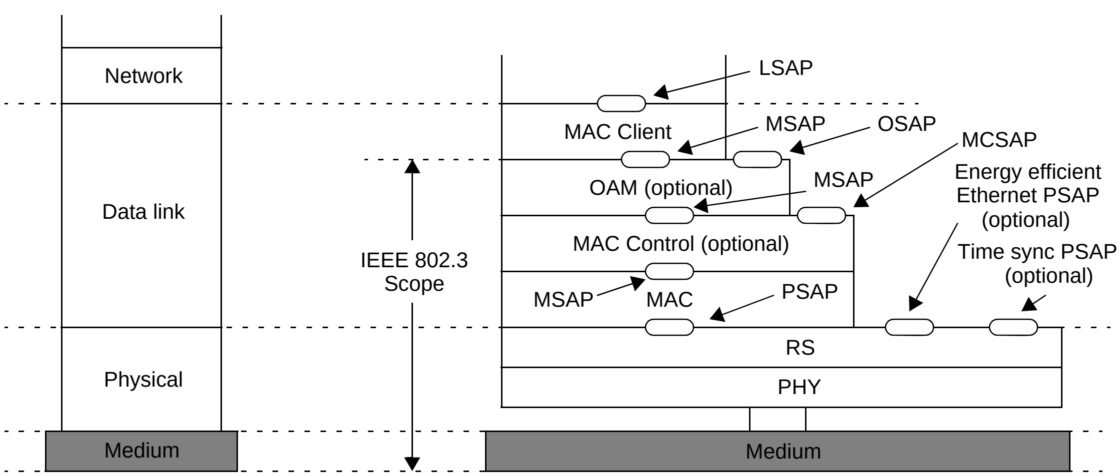


Figure B.2—The RM for IEEE 802.3 point-to-point stations

The RM for IEEE 802.3 Ethernet passive optical networks (EPON) optical line terminal (OLT) is illustrated in Figure B.3.

OAM	operations, administration and maintenance sublayer	MSAP	MAC service access point
RS	reconciliation sublayer	OSAP	OAM service access point
LSAP	link service access point	MCSAP	MAC control service access point
		PSAP	PHY service access point

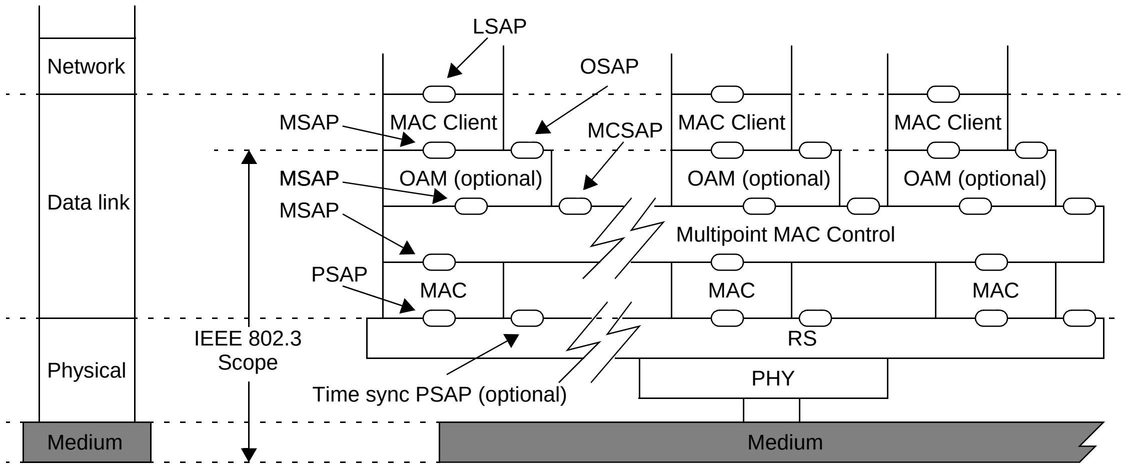


Figure B.3—IEEE 802.3 RM for point-to-multipoint OLT

The RM for IEEE 802.3 EPON optical network unit (ONU) is illustrated in Figure B.4.

OAM	operations, administration and maintenance sublayer	MSAP	MAC service access point
RS	reconciliation sublayer	OSAP	OAM service access point
LSAP	link service access point	MCSAP	MAC control service access point
		PSAP	PHY service access point

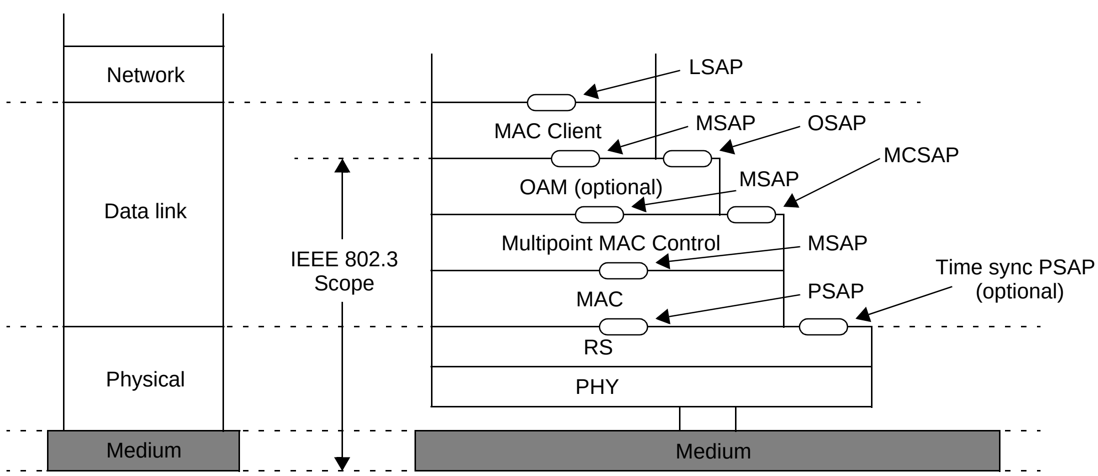


Figure B.4—The RM for IEEE 802.3 point-to-multipoint ONU

IEEE Std 802.3 was amended in 2004 to introduce the concept of subscriber access network.[34] The purpose of Ethernet in the first mile (EFM), as well as its distinction from traditional Ethernet networks, is that it specifies functionality required for the subscriber access network, i.e., public network access. Network

[34]The amendment was IEEE Std 802.3ah™-2004, which is no part of the current IEE Std 802.3.

design considerations for public access that may differ from traditional Ethernet LANs include the OAM function and the regulatory requirements.

B.2 IEEE 802.11 RM

The IEEE 802.11 RM is based on the functional station (STA) model, as shown in Figure B.5.

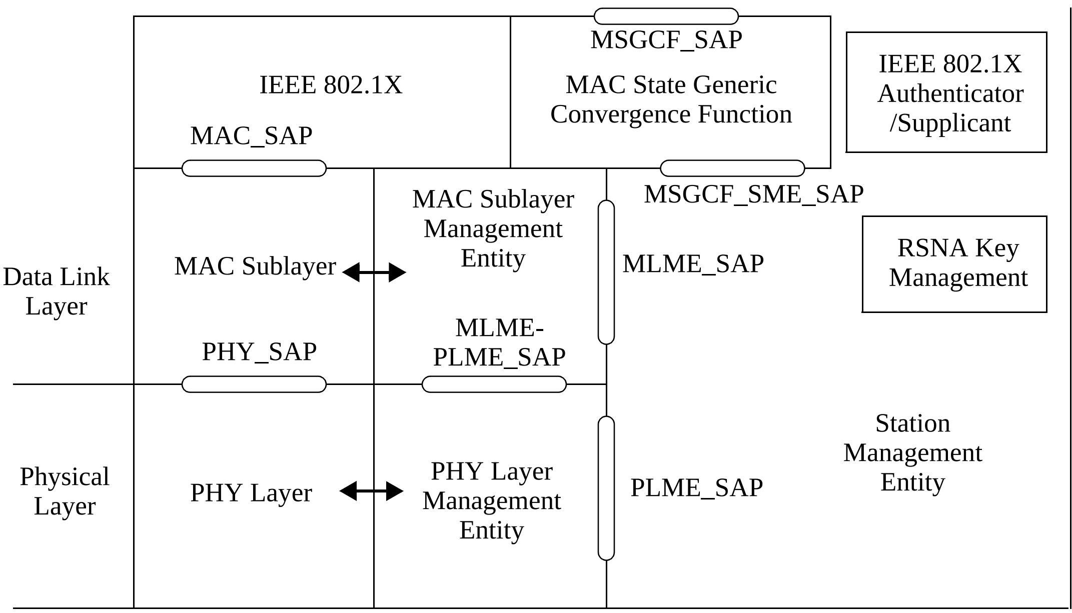


Figure B.5—IEEE 802.11 STA RM

The interconnections between IEEE 802.11 STAs follow three general connection models.

The first interconnection model provides several types of peer-to-peer, direct, pair-wise communication between STAs, each applicable in differing use scenarios. In these direct communications the STAs in each pair have symmetrical operations, with each STA matching the functional STA model, although they can take on different behavioral roles to establish and maintain the interconnection link.

The second interconnection model, the infrastructure model, supports multiple STAs, collected into one or more wireless access domains, called basic service sets (BSSs). These access domains (BSSs) are interconnected via the distribution system and can interwork with other IEEE 802 networks via a portal.

Each access domain in the infrastructure model is established by an access point (AP), which extends the basic STA model to include repeating and forwarding functions that allow communications between non-AP STAs that do not directly interconnect. The AP, acting in cooperation with the distribution system, is a forwarding entity that enables communications between non-AP STAs within the access domain (intra-BSS relay) and also to different IEEE 802.11 wireless access domains established by other APs connected to the same distribution system (inter-BSS relay).

The third interconnection model, is a mesh model consisting of autonomous STAs. Inside the mesh, STAs establish peer-to-peer wireless links with neighbor STAs to mutually exchange messages. Further, using the mesh’s multi-hop capability, messages can be transferred between STAs that are not in direct communication with each other over a single instance of the wireless medium. From the data delivery point of view, it appears as if all STAs in a mesh are directly connected at the MAC layer even if the STAs are not within range of each other. A mesh might have an interface to the distribution system, through a Mesh Gate, and thereby can enable communication to non-AP STAs in infrastructure access domains, and/or via a portal to non-IEEE 802.11 networks.

Figure B.6 illustrates the infrastructure model for APs, the distribution system and portal. The arrows indicate the intra-BSS and inter-BSS relay functions for MSDUs as well as interconnection to other IEEE 802 networks.

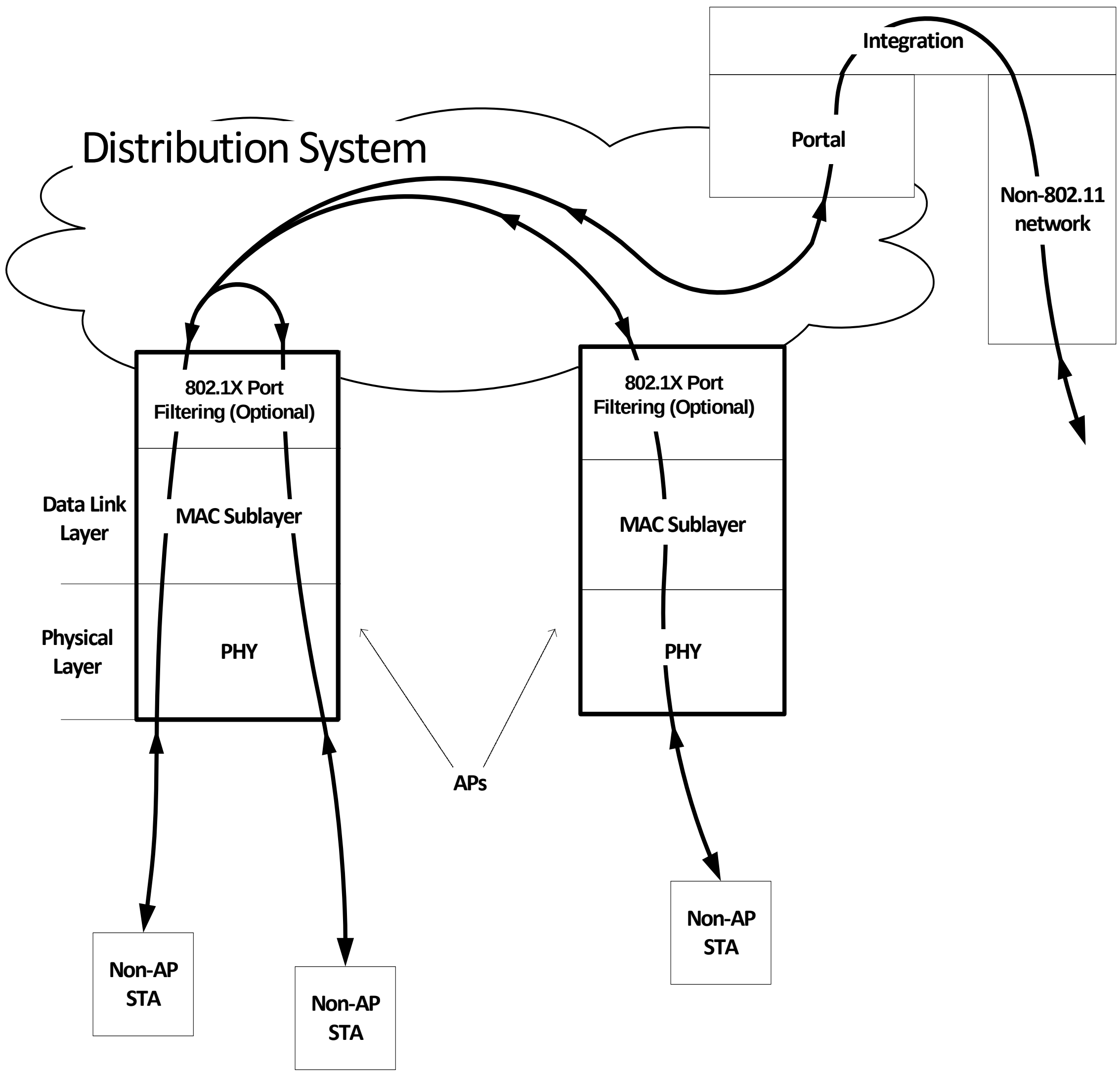


Figure B.6—IEEE 802.11 infrastructure model

B.3 IEEE 802.15™ RMs

B.3.1 IEEE 802.15.3™ RM

The RM for IEEE Std 802.15.3 is illustrated in Figure B.7.

The PHY SAP and physical layer management entity (PLME) SAP are not specified in IEEE Std 802.15.3 as they are rarely, if ever, exposed in a typical implementation. The PHY management objects and attributes are accessed through the MAC sublayer management entity (MLME) SAP with the generic management primitives used to access the MAC management objects and attributes.

The MAC SAP and MLME SAP are specified as logical interfaces to access the services provided by IEEE 802.15.3 end stations.

The PLME and MLME are logical entities that control the PHY and MAC, respectively, based on request from the higher layers.

The frame convergence sublayer (FCSL) is used to allow multiple protocols to simultaneously access the services of an IEEE 802.15.3 PAN. IEEE Std 802.15.3 specifies an FCSL for connection to the ISO/IEC 8802-2 LPD.

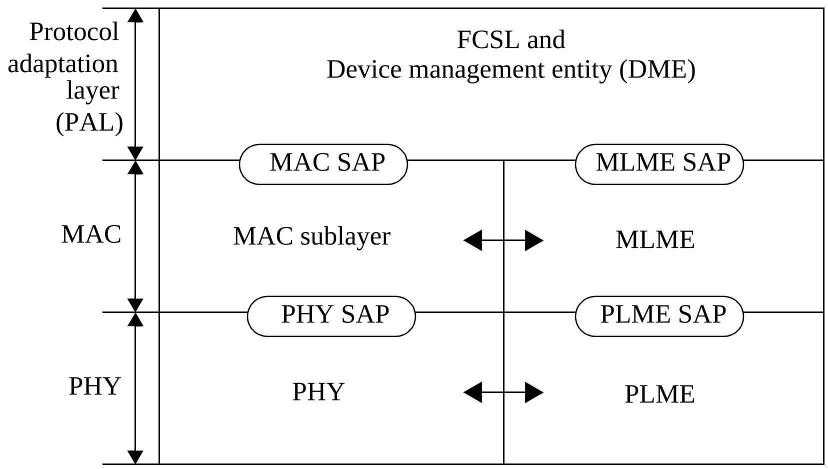


Figure B.7—IEEE 802.15.3 RM

B.3.2 IEEE 802.15.4™ RM

The RM for IEEE Std 802.15.4 is illustrated in Figure B.8.

The upper layers shown in Figure B.8 consist of a network layer (which provides network configuration, manipulation, and message routing) and an application layer (which provides the intended function of the device). The upper layers are not specified in IEEE Std 802.15.4.

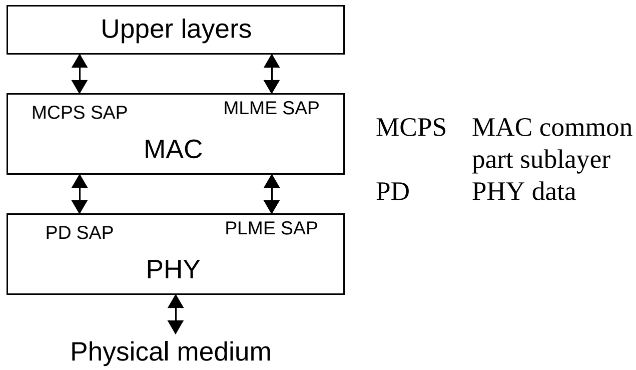


Figure B.8—IEEE 802.15.4 RM

B.3.3 IEEE 802.15.6™ RM

The RM for IEEE 802.15.6 hub or node are shown in Figure B.9.

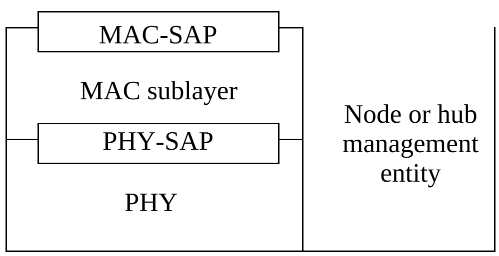


Figure B.9—IEEE 802.15.6 RM

B.3.4 IEEE 802.15.7™ RM

The RM for IEEE Std 802.15.7™ is shown in Figure B.10.

The MAC sublayer provides the following two services, accessed through two SAPs:

— The MAC data service, accessed through the MAC common part sublayer (MCPS) data SAP (MCPS-SAP)

— The MAC management service, accessed through the MLME-SAP

In addition to these external interfaces, an implicit interface also exists between the MLME and the MCPS that allows the MLME to use the MAC data service.

The PHY provides two services, accessed through two SAPs:

— The PHY data service, accessed through the PHY data SAP (PD-SAP)

— The PHY management service, accessed through the PLME’s SAP (PLME-SAP).

The optical SAP (OPTICAL-SAP) provides an interface between the PHY and the optical channel and is not specified in the standard.

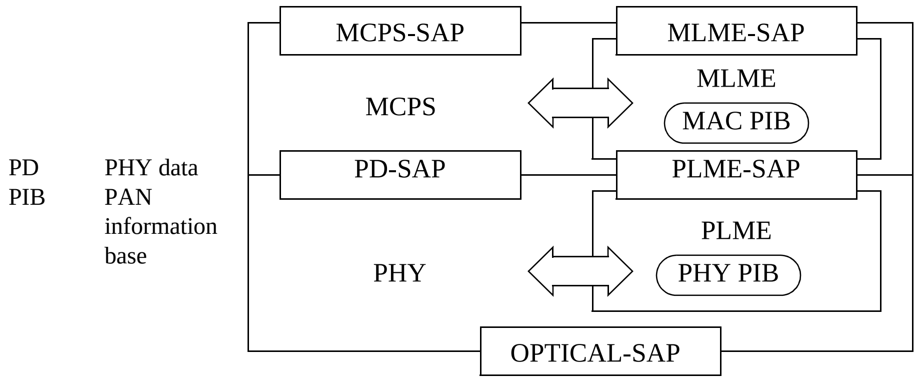


Figure B.10—IEEE 802.15.7 RM

B.4 IEEE 802.16™ RM

B.4.1 Protocol RM

Figure B.11 illustrates the protocol RM for IEEE Std 802.16.

The service-specific convergence sublayer (CS) provides any transformation or mapping of external network data, received through the CS SAP, into MSDUs received by the MCPS through the MAC SAP. This includes classifying external network service data units and associating them to the proper MAC service flow identifier and connection identifier. Multiple CS specifications are provided for interfacing with various protocols.

The MAC CPS provides the core MAC functionality of system access, bandwidth allocation, connection establishment, and connection maintenance. Quality of service is applied to the transmission and scheduling of data over the PHY.

The security sublayer in the MAC provides authentication, secure key exchange, and encryption.

Data, PHY control, and statistics are transferred between the MAC CPS and the PHY via the PHY SAP (which is implementation specific).

The PHY definition includes multiple specifications, each appropriate to a particular frequency range and application.

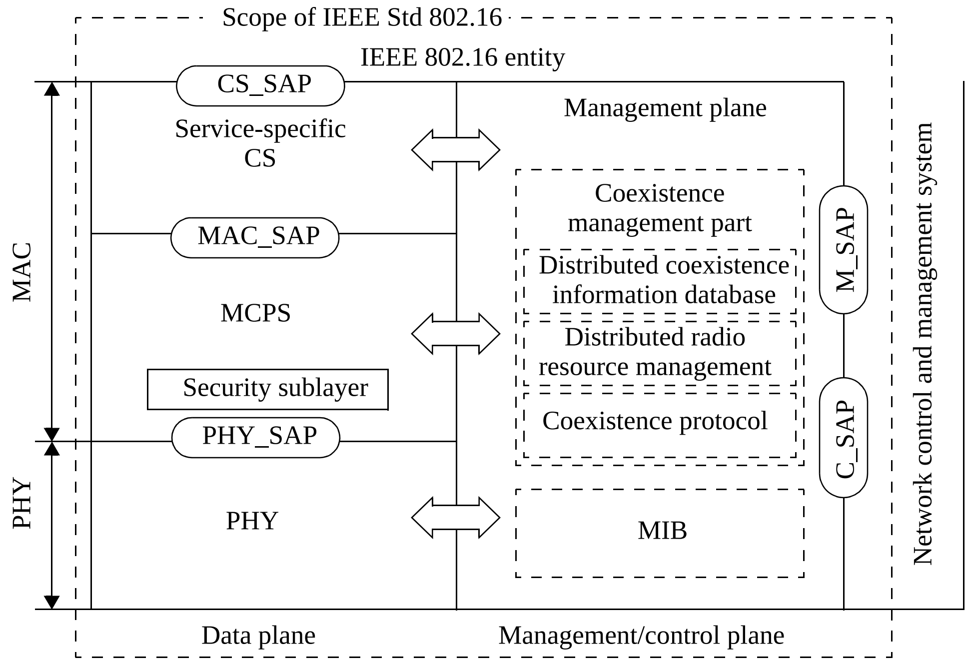


Figure B.11—IEEE 802.16 protocol RM

B.4.2 Network RM

Figure B.12 describes a simplified network RM for IEEE Std 802.16.

The network control and management system (NCMS) abstraction allows the PHY/MAC layers specified in IEEE Std 802.16 to be independent of the network architecture, the transport network, and the protocols used at the backend and, therefore, allows greater flexibility.

NCMS logically exists at base station (BS) side and subscriber station/mobile subscriber station (SS/MS) side of the radio interface, termed *NCMS(BS)* and *NCMS(SS/MS)*, respectively. Any necessary inter-BS coordination is handled through the NCMS(BS).

The control service access point (C-SAP) and management service access point (M-SAP) expose the control plane and management plane functions to upper layers. The NCMS uses the C-SAP and M-SAP to interface with the IEEE 802.16 entity. In order to provide correct MAC operation, NCMS is present within each SS/MS. The NCMS is a layer independent entity that may be viewed as a management entity or control entity. General system management entities can perform functions through NCMS, and standard management protocols can be implemented in the NCMS.

An IEEE 802.16 entity is the logical entity in an SS/MS or BS that comprises the PHY and MAC layers of the data plane and the management/control plane. The IEEE 802.16 end stations can include SS, MS or BS. Multiple SS or MS may be attached to a BS.

SS or MS communicate to the BS over the U interface using a primary management connection, a basic connection, or a secondary management connection.

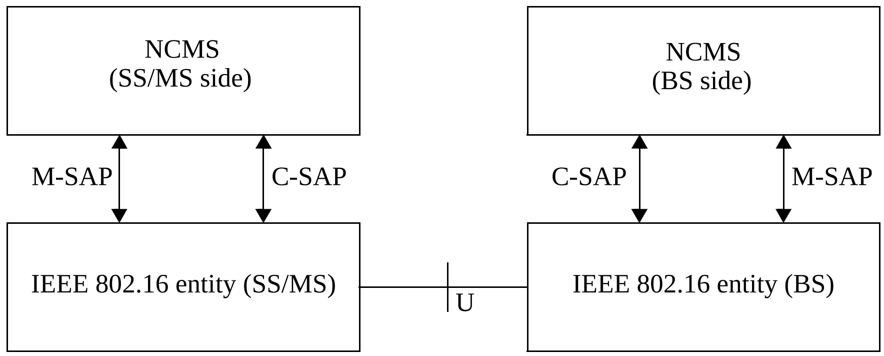


Figure B.12—IEEE 802.16 network RM

B.5 IEEE 802.21™ RM

Figure B.13 shows an implementation view of a dual-mode IEEE 802.11/IEEE 802.16 station with IEEE 802.21 MIH functionality. The MIHF provides the required services to perform handovers between IEEE 802.11 and IEEE 802.16 access technologies. Also, the MIHF becomes a higher layer when it requires data transport services to communicate with an IEEE 802.21 MIH peer. For layer 2 transport of MIH data, services are provided by the IEEE 802.16 CS_SAP or the IEEE 802.11 LSAP. For layer 3 transport, services are provided as described in IETF RFC 5677 [B9].

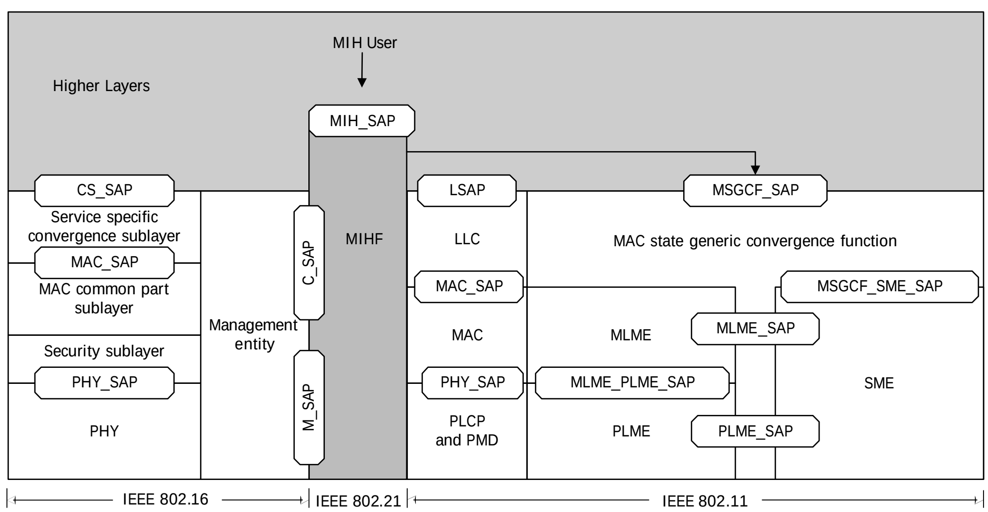


Figure B.13—Example of dual-mode IEEE 802.11 and IEEE 802.16 end station with IEEE 802.21 end-station RM

B.6 IEEE 802.22™ RM

The RM of IEEE Std 802.22 is depicted in Figure B.14. A unique characteristic of this architecture is its cognitive components, which are used to allow for dynamic frequency selection and avoid interference to incumbents on a real-time basis.

AAA	authentication, authorization and accounting
C-SAP	control service access point
CS SAP	convergence sublayer service access point
M-SAP	management service access point
NCMS	network control and management system
MAC SAP	MAC sublayer service access point
PHY SAP	PHY service access point
SM-SSF SAP	spectrum manager, spectrum sensing function service access point
SM-GL SAP	spectrum manager, geolocation service access point

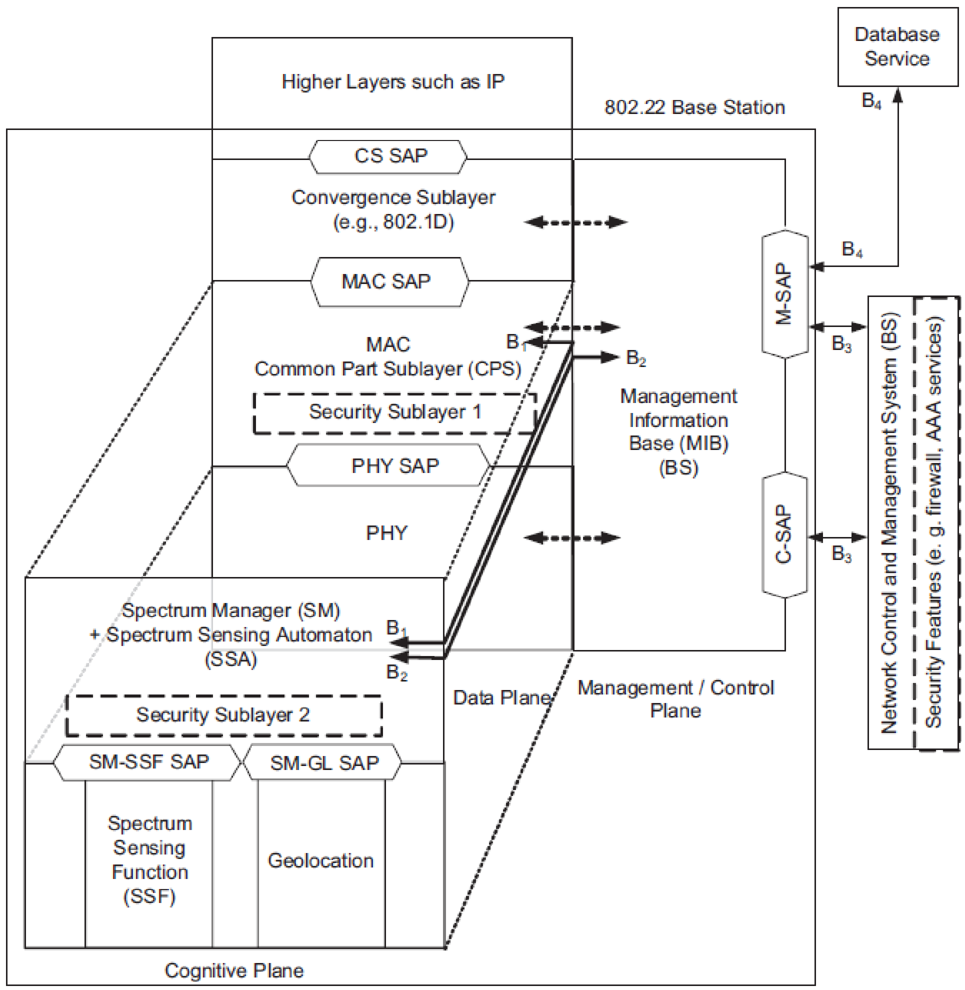


Figure B.14—IEEE 802.22 RM for the BS and CPE

B.6.1 Data plane

The service-specific CS provides the transformation or mapping of external network data that is received through the CS SAP into MSDUs and data that is received by the MAC CPS through the MAC SAP. Multiple CS specifications are provided for interfacing with various protocols.

The MAC CPS provides the core MAC functionality of system access, connection establishment, and connection maintenance. The data that the MAC layer receives from the various CSs through the MAC SAP is classified according to the particular MAC connections.

The security sublayer 1 provides mechanisms for authentication, secure key exchange, encryption, etc.

Data, PHY control, and radio statistics are transferred between the MAC CPS and the PHY via the PHY SAP.

B.6.2 Management/control plane

The management/control plane contains the MIB. SNMP is used to communicate with the MIB database, and some of its primitives can be used to manage the network entities, e.g., BS, customer-premises equipment (CPE), bridges, routers. The MIB at the CPE is a subset of MIB at the BS.

B.6.3 Cognitive plane

The SM maintains spectrum availability information, manages channel lists, manages quiet periods scheduling, implements self-coexistence mechanisms, and processes requests from the MAC/PHY. The SM is the central point at the BS where all the information on the spectrum availability resulting from the database service and the spectrum sensing function (SSF) is gathered. Based on this combined information, local regulations, and predefined SM policies, the SM provides the necessary configuration information to the BS MAC, which then remotely configures all the registered CPEs. Connection B2 is used to configure the SM at the BS, to transmit the available television channel list to the SM, and to report the RF environment information via the MIB objects. Connection B1 is used by the SM to initiate a channel move, to configure the SSA at the CPE (e.g., backup/candidate channel list) and to gather information from the CPEs (e.g., local sensing information, local geolocation information).

The spectrum sensing automaton (SSA) is present at the BS and at the CPEs and independently implements specific procedures for sensing the RF environment at initialization of the BS and before the registration of a CPE with the BS. The SSA at the CPE also includes features to allow proper operation when the CPE is not under the control of a BS. At any other time, the SSA at the CPE is under the control of the SM. The SSA at the BS is also active when the BS is not transmitting to conduct out-of-band sensing. The SSA located at the BS can also carry out sensing to clear channels when the BS is not transmitting.

The SSF implements spectrum sensing algorithms while the geolocation module provides the information to determine the location of the IEEE 802.22 end station (BS or CPE).

The role of the security sublayer 2 is to provide enhanced protection to the incumbents as well as necessary protection to the IEEE 802.22 stations.

Annex C

(informative)

Examples of bit ordering for addresses

C.1 General

This annex illustrates the various bit- and octet-transmission scenarios that can occur, and it is intended as a basis for clarifying the issue of bit-ordering for EUI-48s across different MACs. Throughout, the examples make use of the OUI value AC-DE-48, introduced in 8.2.2. This 3-octet value is considered in its two possible roles: as the first part of a 5-octet protocol identifier and as the first part of a 6-octet EUI-48. The consistent representations of the OUI in its role as part of a protocol identifier are contrasted with the sometimes variable representations that apply to its role as part of an EUI-48.

NOTE—Protocol identifiers always form part of the normal user data in a MAC Information field; hence, there is nothing special about OUI octets in their protocol identifier role.

C.2 Illustrative examples

For the examples, the bit significance of an OUI in general is illustrated in Figure C.1.

	MSB							LSB
Octet 0	h	g	f	e	d	c	b	a
Octet 1	p	o	n	m	l	k	j	i
Octet 2	x	w	v	u	t	s	r	q

When used in an address field:
Bit “a” of the OUI = I/G address bit. Bit “b” of the OUI = U/L address bit.

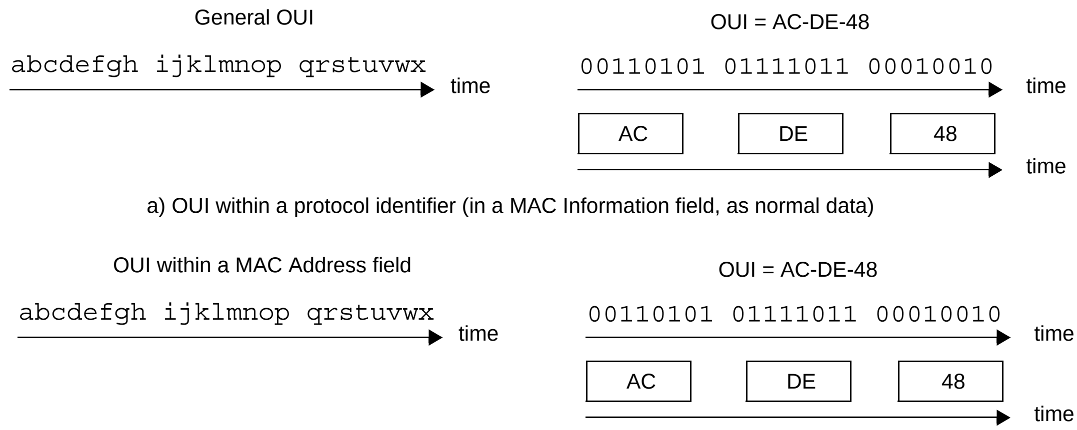
When used in a protocol identifiers:
Bit “a” of the OUI (always zero) = M bit. Bit “b” of the OUI = X bit.

Figure C.1—Bit significance of an OUI

When transmitted on a network with all data octets of the OUI transmitted LSB first, the OUI portions of a protocol identifier and of an EUI-48 appear as in Figure C.2. When transmitted on a network with the data octets of the OUI transmitted MSB first, the OUI portions of a protocol identifier and of an EUI-48 contained in a MAC Address field appear as in Figure C.3.

In some circumstances, it is necessary to convey EUI-48s as data within MAC Information fields, e.g., as part of a management protocol or a network layer routing protocol.

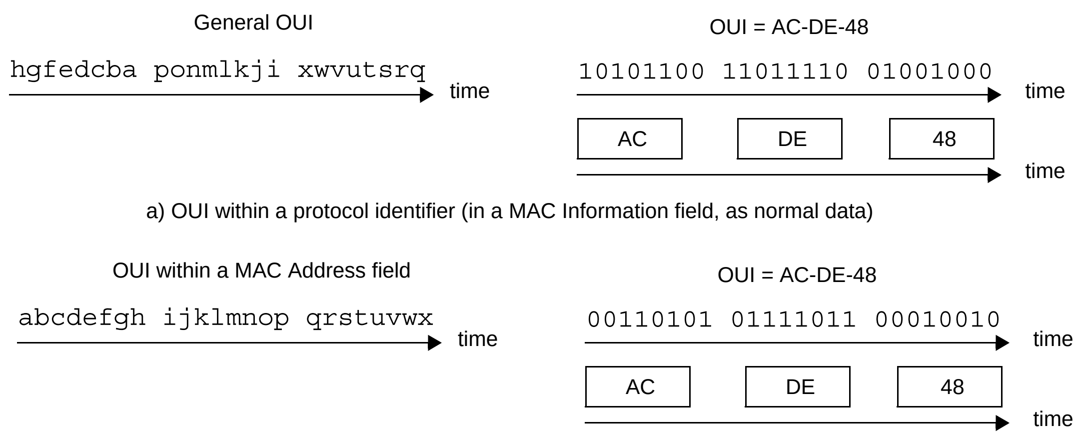
For network types in which Figure C.2 applies, such as IEEE Std 802.3, the bit-ordering within the octets of an EUI-48 conveyed as data is the same as both the ordering when the address appears in a MAC Address field and the ordering for octets of non-address information.



a) OUI within a protocol identifier (in a MAC Information field, as normal data)

b) OUI within a MAC Address field

Figure C.2—Order of bit and octet transmission for an OUI with LSB transmitted first



a) OUI within a protocol identifier (in a MAC Information field, as normal data)

b) OUI within a MAC Address field

Figure C.3—Order of bit and octet transmission for an OUI with MSB transmitted first

For network types in which Figure C.3 applies, there appears to be a choice of representations for EUI-48s conveyed as data, as follows:

— Canonical format: The octets of the EUI-48 can be treated like any other data octets and transmitted with the bit-ordering of Figure C.3(a). The canonical format is illustrated in Figure C.4.

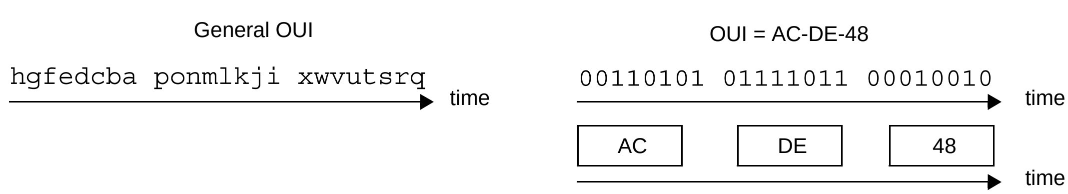


Figure C.4—Order of bit and octet transmission for an OUI in an EUI-48 with MSB transmitted first, canonical format.

— Noncanonical format: The bit-ordering of Figure C.3(b) is treated as a property of the EUI-48 rather than of the MAC Address field as transmitted in MAC frames, and the EUI-48 octets are transmitted with the bit-ordering reversed compared with normal data octets. The noncanonical format is illustrated in Figure C.5.

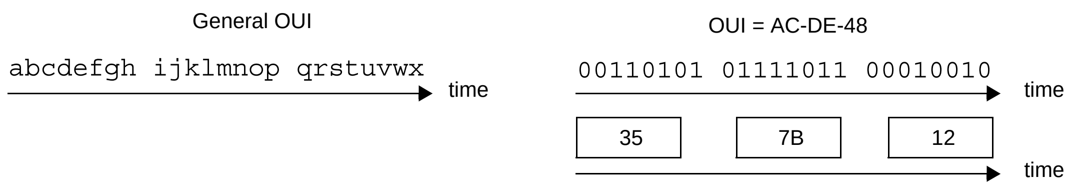


Figure C.5—Order of bit and octet transmission for an OUI in an EUI-48 with MSB transmitted first, noncanonical format.

The noncanonical format has the unfortunate consequence that applications operating in environments containing a mixture of LAN types have to handle different representations of EUI-48s, according to the environment in which the EUI-48 is to be used.

In Figure C.2, Figure C.3, Figure C.4, and Figure C.5, it can be seen that the interpretation of OUI bits as octet values is consistent. This reversal of the bit order applies only to all 6 octets (not just the OUI) of an EUI-48 placed in the MAC Information field of a frame by a protocol that uses the bit-reversed view of the EUI-48s derived from Figure C.3(b). Frames containing, or possibly containing, such EUI-48s are described as having noncanonical format. Frames that cannot contain such EUI-48s are described as having canonical format.

Note that there is no way of knowing, from MAC layer information only, whether a particular frame is in canonical or noncanonical format. In general, this depends on which higher layer protocols are present in the frame.

Annex D

(informative)

List of IEEE 802 standards

This annex contains a list of approved IEEE 802 standards. The list was current when this standard was completed.

IEEE Std 802.1AB™, IEEE Standard for Local and metropolitan area networks—Station and Medium Access Control Connectivity Discovery.[35, 36]

IEEE Std 802.1AC™, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Service Definition.

IEEE Std 802.1AE™, IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Security.

IEEE Std 802.1AR™, IEEE Standard for Local and metropolitan area networks—Secure Device Identity.

IEEE Std 802.1AS™, IEEE Standard for Local and metropolitan area networks—Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks.

IEEE Std 802.1AX™, IEEE Standard for Local and metropolitan area networks—Link Aggregation.

IEEE Std 802.1BA™, IEEE Standard for Local and metropolitan area networks—Audio Video Bridging (AVB) Systems.

IEEE Std 802.1BR™, IEEE Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks – Bridge Port Extension.

IEEE Std 802.1Q™, IEEE Standard for Local and metropolitan area networks—Bridges and Bridged Networks.

IEEE Std 802.1X™, IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control.

IEEE Std 802.3™, IEEE Standard for Ethernet.

IEEE Std 802.3.1™, IEEE Standard for Management Information Base (MIB) Definitions for Ethernet.

IEEE Std 802.3.2™, IEEE Standard for Ethernet - YANG Data Model Definitions.

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 802.15.3™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.3:

[35]The IEEE standards and products referred to in Annex D are trademarks owned by The Institute of Electrical and Electronics Engineers, Incorporated.

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

Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs).

IEEE Std 802.15.4™, IEEE Standard for Local and metropolitan area networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).

IEEE Std 802.15.6™, IEEE Standard for Local and metropolitan area networks—Part 15.6: Wireless Body Area Networks.

IEEE Std 802.15.7™, IEEE Standard for Local and metropolitan area networks—Part 15.7: Short-Range Wireless Optical Communication Using Visible Light.

IEEE 802.15.8™, IEEE Standard for Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Peer Aware Communications (PAC).

IEEE 802.15.9™, IEEE Standard for Transport of Key Management Protocol (KMP) Datagrams.

IEEE 802.15.10™, IEEE Recommended Practice for Routing Packets in IEEE 802.15.4 Dynamically Changing Wireless Networks.

IEEE 802.15.22.3™, IEEE Standard for Spectrum Characterization and Occupancy Sensing.

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

IEEE Std 802.16.1™, IEEE Standard for WirelessMAN-Advanced Air Interface for Broadband Wireless Access Systems.

IEEE Std 802.16.2™, IEEE Recommended Practice for Local and Metropolitan Area Networks—Coexistence of Fixed Broadband Wireless Access Systems.

IEEE 802.19.1™, IEEE Standard for Information technology--Telecommunications and information exchange between systems--Local and metropolitan area networks--Specific requirements--Part 19: Wireless Network Coexistence Methods.

IEEE 802.19.3™, IEEE Recommended Practice for Local and Metropolitan Area Networks--Part 19: Coexistence Methods for IEEE 802.11 and IEEE 802.15.4 Based Systems Operating in the Sub-1 GHz Frequency Bands

IEEE Std 802.21™, IEEE Standard for Local and metropolitan area networks—Media Independent Services Framework.

IEEE Std 802.21.1™, IEEE Standard for Local and metropolitan area networks--Part 21.1: Media Independent Services.

IEEE Std 802.22™, IEEE Standard for Information Technology—Telecommunications and information exchange between systems Wireless Regional Area Networks (WRAN)—Specific requirements Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands.

Annex E

(informative)

History

E.1 Universal addresses

The universal administration of MAC addresses began with the Xerox Corporation administering Block Identifiers (Block IDs) for Ethernet addresses. Block IDs, subsequently referred to as OUI by the IEEE RA, were assigned by the Ethernet Administration Office. The Block IDs were 24 bits in length, and an organization developed addresses by assigning the remaining 24 bits. For example, the address as represented by the 6 octets P-Q-R-S-T-U comprises the Block ID, P-Q-R, and the locally assigned octets S-T-U.

The IEEE RA, because of the work in IEEE 802 on standardizing networking technologies, assumed the responsibility of defining and carrying out procedures for the universal administration of these addresses. The IEEE RA has also been designated by ISO/IEC to act as a registration authority for the ISO/IEC 8802 series of standards. The responsibility for defining the procedures is discharged by the IEEE Registration Authority Committee, which is chartered by the IEEE Standards Association Board of Governors.

The IEEE RA has the responsibility for the administration of universal addresses. There are agreements and processes in place for IEEE 802 standards to also become ISO/IEC standards. Most of these standards are in the ISO/IEC 8802 series. The IEEE was designated by ISO/IEC to act as the registration authority for the ISO/IEC 8802 series of standards. IEEE established the IEEE Registration Authority to manage the administration of universal addresses (as well as other registries defined in IEEE standards. When the IEEE Standards Association was created, 1998, responsibility for management of the IEEE RA was assigned to the IEEE SA. The IEEE SA Board of Governors in turn delegates responsibility for technical oversight of the IEEE RA to a a subcommittee, the IEEE Registration Authority Committee (RAC).

E.2 IEEE RA address block products

When the IEEE RA took over administration of universal addresses, blocks of addresses were allocated by assigning an OUI to companies and organizations that requested them. When the Internet began to grow exponentially, it seemed as if the currently allocated address space using 24-bit OUIs would run out quickly. The IEEE RA addressed one part of this concern by introducing 64-bit addressing and recommending this addressing scheme for new standards that did not require 48-bit addressing for backwards compatibility.

In addition, the IEEE RA looked for ways to make the original OUI space last longer. Many times, a company or organization would be allocated an OUI, but would not use a significant portion of the 2^{24} (16 777 216) EUI-48 addresses or 2^{40} (1 099 511 627 776) EUI-64 addresses available in the address block. The addresses would be “lost”, never being assigned. To avoid this situation, the IEEE RA created the OUI-36, which could be used as an identifier as well as for creating universal addresses (up to 4096 EUI-48s or 268 435 456 EUI-64s).

Based on customer requests, beginning on January 1, 2014, the IEEE RA added a 28-bit identifier (MA-M) and renamed the products to be MA-L (24 bits, previously OUI), MA-M (28 bits), and MA-S (36 bits, also referred to as OUI-36). The MA-L assignment includes the assignment of an OUI, whereas the MA-M and MA-S do not. The MA-M assignment is derived from an OUI that is assigned to IEEE.

The MA-S assignment is derived from an OUI that is assigned to IEEE and encompasses both the Individual Address Block and the OUI-36 assignments offered prior to January 1, 2014. An MA-S assignment includes an OUI-36 that is specified in some standards for identification of a company or organization and used in creation of extended identifiers.

E.3 Local MAC addresses

Local addresses were included in the initial series of IEEE 802 standards (published in 1985). IEEE Std 802.5-1985 included an annex for hierarchical addressing (dividing an address into a ring number and a node number both being locally administered). Pre-standard Ethernet did not include local addresses. A few Block IDs assigned by Xerox Corporation prior to the definition of local addresses (circa 1981) had the X bit equal to one. The vendors assigned such Block IDs participated in remediation of problems created by the definition of local addresses for all IEEE 802 networks.

The amendment IEEE Std 802c-2017 (now included in IEEE Std 802) on local MAC address usage introduced the SLAP, ELI, AAI, and SAI. Prior to that amendment, IEEE Std 802 provided little normative content regarding the use of local MAC address space beyond the description of the U/L bit. A brief subclause on local MAC addresses was introduced in the revision IEEE Std 802-2014, stating that local MAC addresses "need to be unique on a LAN or bridged LAN unless the bridges support VLANs with independent learning." That revision also introduced the Company ID (CID), referring to the IEEE RA for details. It did not specify the creation of local MAC addresses based on CID, but it did hint at the possibility, stating that "A CID assignment has the X bit (the U/L address bit in a MAC address) set to one, which would place any address created with a CID in the locally administered address space."

The IEEE RA opened its CID registry on 1 January 2014. Later that year, the IEEE introduced an expanded version of its tutorial "Guidelines for use of the 24-bit Organizationally Unique Identifiers (OUI)" as "Guidelines for Use Organizationally Unique Identifier (OUI) and Company ID (CID)"[37], including explanatory material regarding CIDs. Using language similar to that of IEEE Std 802-2014, the tutorial also suggested the possibility of building a local MAC address from a CID.

All CIDs publicly listed by the IEEE RA are assigned with the Y and Z bits equal to zero and one, respectively. Local MAC addresses based on CIDs are in SLAP quadrant "01", in accordance with the specification of the ELI, 8.4.4.1.

In February 2016, the IEEE SA initiated a project, P802.1CQ [B1], regarding multicast and local MAC address assignments to specify protocols, procedures, and management objects for locally unique assignment of 48-bit and 64-bit addresses in IEEE 802 networks.

[37]The tutorial has been updated again to include EUIs, [B2]

Annex F

(informative)

EtherType Listing Subset

F.1 Introduction

This Annex lists the subset of EtherType assignments described in 9.2.2 in tabular form, Table F.1, and in the form of a YANG module, F.3. This subset is provided solely for the convenience of the users of this standard and does not constitute an endorsement by IEEE of the listed protocols.

F.2 Tabular format

A subset of EtherType assignments by the IEEE RA is given in Table F.1. Each Friendly Name in Table F.1 is unique and is used as an identifier in the YANG module. The Short Description identifies the protocol, protocol message, or protocol field that uses the assignment as specified in the Reference, or the EtherType assignment itself as named in the Reference. Where the Reference specifies more than one name or use (distinguished for example by sub-type) these are included in the Short Description field.

Table F.1—EtherType listing subset*

EtherType Assignment (HEX)	Friendly Name	Short Description	Reference
08-00	ipv4	Internet Protocol version 4 (IPv4)	IETF RFC 894
08-06	arp	Address Resolution Protocol (ARP)	IETF RFC 826, IETF RFC 7042
08-42	wol	Wake-on-LAN	IEEE Std 802
22-E2	msp	MAC Status Protocol (MSP)	IEEE Std 802.1Q
22-E7	cnm	Congestion Notification Message (CNM)	IEEE Std 802.1Q
22-E9	cn-tag	Congestion Notification Tag (CN-TAG)	IEEE Std 802.1Q
22-EA	msrp	Multiple Stream Reservation Protocol (MSRP)	IEEE Std 802.1Q
22-F3	trill	Transparent Interconnection of Lots of Links	IETF RFC 6325
60-03	decnet	DECnet DNA Routing	DECnet DIGITAL Network Architecture - Ethernet Data Link Architectural Specification v1.0.0
80-35	rarp	Reverse Address Resolution Protocol	IETF RFC 903

Table F.1—EtherType listing subset* (continued)

EtherType Assignment (HEX)	Friendly Name	Short Description	Reference
80-9B	appletalk	Appletalk (Ethertalk)	Inside Appletalk, Second Edition
80-F3	aarp	Appletalk Address Resolution Protocol	Inside Appletalk, Second Edition
81-00	c-tag	Customer VLAN Tag (C-TAG)	IEEE Std 802.1Q
81-37	ipx	Internetwork Packet Exchange (IPX)	IETF RFC 8519
82-04	qnx	QNX Qnet	IETF RFC 8519
86-DD	ipv6	Internet Protocol Version 6 (IPv6)	IETF RFC 2464
88-08	efc	Multipoint Control Protocol (MPCP)	IEEE Std 802.3
88-09	esp	Ethernet Slow Protocol	IEEE Std 802.3
88-19	cobranet	CobraNet CobraNet	Programmer's Reference, Version 2.5
88-47	mpls-unicast	Multiprotocol Label Switching (MPLS) unicast traffic	IETF RFC 3031
88-48	mpls-multicast	Multiprotocol Label Switching (MPLS) multicast	IETF RFC 3031
88-63	pppoe-discovery	Point-to-Point Protocol over Ethernet (PPPoE) Discovery Stage	IETF RFC 2516
88-64	pppoe-session	Point-to-Point Protocol over Ethernet (PPPoE) Session Stage	IETF RFC 2516
88-6D	intel-ans	Intel Advanced Networking Services Probe Packets	Intel® Advanced Network Services (Intel® ANS) Advanced Settings for Teams
88-70	llc-encaps	LLC Encapsulation	IEEE Std 802.1AC
88-7B	homeplug	Homeplug	IETF RFC 8519
88-8E	eap	Port Access Entity (PAE) EtherType, Extensible Authentication Protocol over LANs (EAPOL)	IEEE Std 802.1X
88-92	profinet	PROFINET	IEC 61158-6-10
88-9A	hyperscsi	Small Computer System Interface (SCSI) over Ethernet.	An Ethernet Based Data Storage Protocol for Home Network
88-A2	aoe	Advanced Technology Attachment (ATA) over Ethernet	ATA over Ethernet (AoE)
88-A4	ethercat	Ethernet for Control Automation Technology (EtherCAT)	IEC 61158-4-12
88-A8	s-tag	Service VLAN Tag (S-TAG) or Backbone VLAN Tag (B-TAG)	IEEE Std 802.1Q

Table F.1—EtherType listing subset* (continued)

EtherType Assignment (HEX)	Friendly Name	Short Description	Reference
88-AB	ethernet-powerlink	Ethernet Powerlink	IEC 61158-4-13
88-B5	exp1	Local experimental EtherType 1	IEEE Std 802
88-B6	exp2	Local experimental EtherType 2	IEEE Std 802
88-B7	oui-ext	OUI Extended EtherType	IEEE Std 802
88-B8	goose	IEC 61850 Generic Object Oriented Substation Event (GOOSE)	IEC 61850-8-1
88-B9	gse	IEC 61850 Generic Substation Events (GSE) management services	IEC 61850-8-1
88-BA	sv	IEC 61850 Sampled Value Transmission (SV)	IEC 61850-8-2
88-C7	pre-auth	RSNA Pre-Authentication	IEEE Std 802.11
88-CC	lldp	ink Layer Discovery Protocol (LLDP)	IEEE Std 802.1AB
88-CD	sercos	Sercos Interface	IEC 61158-4-19
88-DC	wsmp	WAVE Short Message Protocol (WSMP)	IEEE Std 1609
88-E1	homeplug-av-mme	HomePlug AV Mobile Management Entity (MME)	IETF RFC 8519
88-E3	mrp	Media Redundancy Protocol	IEC 62439-2
88-E5	macsec	MACsec EtherType	IEEE Std 802.1AE
88-E7	i-tag	Backbone Service Instance Tag	IEEE Std 802.1Q
88-F5	mvrp	Multiple VLAN Registration Protocol (MVRP)	IEEE Std 802.1Q
88-F6	mmrp	Multiple MAC Registration Protocol (MMRP)	IEEE Std 802.1Q
88-F7	ptp	Precision Time Protocol	IEEE Std 1588
89-02	cfm	IEEE 802.1Q Connectivity Fault Management (CFM) PDU Encapsulation EtherType	IEEE Std 802.1Q
89-06	fcoe	Fibre Channel over Ethernet (FCoE)	T11 FC-BB-5
89-0D	wlan-mgmt	802.11 Management Protocol	IEEE Std 802.11
89-10	encap	Backbone Service Encapsulated Addresses	IEEE Std 802.1Q
89-14	fip	FCoE Initialization Protocol	IETF RFC 8519

Table F.1—EtherType listing subset* *(continued)*

EtherType Assignment (HEX)	Friendly Name	Short Description	Reference
89-15	roce	Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCEv1)	InfiniBand™ Architecture Specification
89-17	mis	Media Independent Service (MIS) Protocol	IEEE Std 802.21
89-1D	tte	TTEthernet Protocol Control Frame (TTE)	SAE AS6802
89-29	mirp	Multiple I-SID Registration Protocol (MIRP)	IEEE Std 802.1Q
89-2F	hsr	High-availability Seamless Redundancy (HSR)	IEC 62439-3
89-3F	e-tag	Bridge Port Extension Tag (E-TAG)	IEEE Std 802.1BR
89-40	ecp	Edge Control Protocol	IEEE Std 802.1Q
89-4B	f-tag	Flow Filtering Tag (F-TAG) IEEE	Std 802.1Q
89-52	drcp	Distributed Relay Control Protocol (DRCP)	IEEE Std 802.1AX
89-A2	cim	Congestion Isolation Message (CIM)	IEEE Std 802.1Q
C9-D1	llc-legacy	LLC Encapsulation (obsolete)	IEEE Std 802.1AC
F1-C1	r-tag	Frame Replication and Elimination for Reliability (FRER) Redundancy Tag (R-TAG)	IEEE Std 802.1CB

*Hexadecimal values in the Assignment field are provided from the public listing, while the information in the other fields (i.e., Friendly Name, Short Description, and Reference) is specified herein.

F.3 YANG module for EtherType subset

F.3.1 YANG Framework

The YANG module representation of the EtherType subset (as defined in Table F.1) is provided in this subclause.

Changes to the ieee802-ethertypes.yang module, adding or revising entries, are made by amending or revising this standard and will add a new revision statement to the module. YANG augmentation should not be used to extend the module.

NOTE — The ietf-ethertypes.yang module (as defined in rfc8519) is currently used by the ietf-packet-fields.yang module (as defined in rfc8519) and the ietf-detnet.yang module. Moving forward it is anticipated that the YANG module (ieee802-ethertype.yang) defined in F.3.2 will supersede ietf-ethertypes.yang, which would result in ietf-ethertypes.yang being deprecated.

F.3.2 Definition for ieee802-ethertype YANG module[38,39]

```
module ieee802-ethertype {

  namespace "urn:ieee:std:802.1Q:yang:ieee802-ethertype";
  prefix "ieee-ethertype";

  organization
    "IEEE 802.1 Working Group";

  contact
    "WG-URL: http://ieee802.org/1/
     WG-EMail: stds-802-1@ieee.org

     Contact: IEEE 802.1 Working Group Chair
     Postal: C/O IEEE 802.1 Working Group
             IEEE Standards Association
             445 Hoes Lane
             Piscataway
             NJ 08854
             USA

     E-mail: stds-802-1-chairs@ieee.org";

  description
    "This module contains a subset of commonly used 802 network Ether-
Types.

     Copyright (C) IEEE (2023).

     This version of this YANG module is part of the IEEE Std 802;
     see the standard itself for full legal notices.";

  revision "2023-04-17" {
    description
      "Initial revision.";
    reference
      "IEEE Std 802f, Overview and Architecture -
       YANG Data Model for EtherTypes";
  }

  typedef ethertype {
    type enumeration {
      enum ipv4 {
        value 2048;
        description
          "08-00 Internet Protocol version 4 (IPv4)";
        reference
          "Organization: Xerox, US
```

[38]Copyright release for YANG: Users of this standard may freely reproduce the YANG modules contained in this standard so that they can be used for their intended purpose.

[39]An ASCII version of the YANG module is attached to the PDF of this standard and can also be obtained from the IEEE 802.1 website at https://1.ieee802.org/yang-modules/.

```
          Standard: IETF RFC 894";
      }
      enum arp {
        value 2054;
        description
          "08-06 Address Resolution Protocol (ARP)";
        reference
          "Organization: Symbolics, Inc.
          Standard: IETF RFC 826, IETF RFC 7042";
      }
      enum wol {
        value 2114;
        description
          "08-42 Wake-on-LAN";
        reference
          "Organization: None
          Standard: IEEE Std 802";
      }
      enum msp {
      value 8930;
      description
        "22-E2 MAC Status Protocol (MSP)";
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE Std 802.1Q";
      }
      enum cnm {
        value 8935;
        description
          "22-E7 Congestion Notification Message (CNM)";
        reference
          "Organization: IEEE 802.1 Working Group
          Standard: IEEE Std 802.1Q";
      }
      enum cn-tag {
        value 8937;
        description
          "22-E9 Congestion Notification Tag (CN-TAG)";
        reference
          "Organization: IEEE 802.1 Working Group
          Standard: IEEE Std 802.1Q";
      }
      enum msrp {
         value 8938;
        description
          "22-EA Multiple Stream Reservation Protocol (MSRP)";
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE Std 802.1Q";
      }
      enum trill {
        value 8947;
        description
          "22-F3 Transparent Interconnection of Lots of Links";
```

```
        reference
          "Organization: IETF TRILL Working Group
          Standard: IETF RFC 6325";
      }
      enum decnet {
        value 24579;
        description
          "60-03 DECnet DNA Routing";
        reference
          "Organization: DEC
          Standard: DECnet DIGITAL Network Architecture - Ethernet
          Data Link Architectural Specification v1.0.0";
      }
      enum rarp {
        value 32821;
        description
          "80-35 Reverse Address Resolution Protocol";
        reference
          "Organization: Private
            Standard: IETF RFC 903";
      }
      enum appletalk {
      value 32923;
      description
        "80-9B Appletalk (Ethertalk)";
      reference
        "Organization: Private
        jStandard: Inside Appletalk, Second Edition";
      }
      enum aarp {
        value 33011;
        description
"          80-F3 Appletalk Address Resolution Protocol";
        reference
          "Organization: Private
          Standard: Inside Appletalk, Second Edition";
      }
      enum c-tag {
        value 33024;
        description
          "81-00 Customer VLAN Tag (C-TAG)";
        reference
          "Organization: IEEE 802.1 Working Group
          Standard: IEEE Std 802.1Q";
      }
      enum ipx {
        value 33079;
        description
          "81-37 Internetwork Packet Exchange (IPX)";
        reference
          "Organization: Novell, Inc.
          Standard: IETF RFC 8519";
      }
      enum qnx {
```

```
      value 33284;
      description
        "82-04 QNX Qnet";
      reference
        "Organization: Quantum Software Systems, Ltd.
        Standard: IETF RFC 8519";
    }
    enum ipv6 {
      value 34525;
      description
        "86-DD Internet Protocol Version 6 (IPv6)";
      reference
        "Organization: USC/ISI
        Standard: IETF RFC 2464";
    }
    enum efc {
      value 34824;
    description
      "88-08 Multipoint Control Protocol (MPCP)";
    reference
      "Organization: IEEE 802.3 Working Group
      Standard: IEEE Std 802.3";
    }
    enum esp {
      value 34825;
      description
        "88-09 Ethernet Slow Protocol";
      reference
        "Organization: IEEE 802.3 Working Group
        Standard: IEEE Std 802.3";
    }
    enum cobranet {
      value 34841;
      description
        "88-19 CobraNet";
      reference
        "Organization: Peak Audio
        Standard: CobraNet Programmer's Reference, Version 2.5";
    }
    enum mpls-unicast {
      value 34887;
      description
        "88-47 Multiprotocol Label Switching (MPLS) unicast
        traffic";
      reference
        "Organization: Cisco Systems
        Standard: IETF RFC 3031";
    }
    enum mpls-multicast {
      value 34888;
      description
        "88-48 Multiprotocol Label Switching (MPLS) multicast";
      reference
        "Organization: Cisco Systems
```

```
        Standard: IETF RFC 3031";
    }
    enum pppoe-discovery {
      value 34915;
      description
        "88-63 Point-to-Point Protocol over Ethernet (PPPoE)
        Discovery Stage";
      reference
        "Organization: UUNET Technologies, Inc.
        Standard: IETF RFC 2516";
    }
    enum pppoe-session {
      value 34916;
      description
        "88-64 Point-to-Point Protocol over Ethernet (PPPoE)
        Session Stage";
      reference
        "Organization: UUNET Technologies, Inc.
        Standard: IETF RFC 2516";
    }
    enum intel-ans {
      value 34925;
      description
        "88-6D Intel Advanced Networking Services Probe Packets";
      reference
        "Organization: Intel Corporation
        Standard: Intel® Advanced Network Services (Intel® ANS)
    }
    enum llc-encaps {
      value 34928;
      description
        "88-70 LLC Encapsulation";
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE Std 802.1AC";
    }
    enum homeplug {
      value 34939;
      description
        "88-7B Homeplug";
      reference
        "Organization: Intellon Corporation
        Standard: IETF RFC 8519";
    }
    enum eapol {
      value 34958;
      description
        "88-8E Port Access Entity (PAE) EtherType, Extensible
        Authentication Protocol over LANs (EAPOL)";
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE Std 802.1X";
    }
    enum profinet {
```

```
      value 34962;
      description
        "88-92 PROFINET";
      reference
        "Organization: PROFIBUS International
        Standard: IEC 61158-6-10";
    }
    enum hyperscsi {
      value 34970;
      description
        "88-9A Small Computer System Interface (SCSI) over
        Ethernet.";
      reference
        "Organization: Data Storage Institute
        Standard: An Ethernet Based Data Storage Protocol for Home
        Network";
    }
    enum aoe {
      value 34978;
      description
        "88-A2 Advanced Technology Attachment (ATA) over Ethernet.";
      reference
        "Organization: Coraid Inc
        Standard: AoE (ATA over Ethernet)";
    }
    enum ethercat {
      value 34980;
      description
        "88-A4 Ethernet for Control Automation Technology
        (EtherCAT)";
      reference
        "Organization: Beckhoff Automation GmbH & Co KG
        Standard: IEC 61158-4-12";
    }
    enum s-tag {
      value 34984;
      description
        "88-A8 Service VLAN Tag (S-TAG) or Backbone VLAN Tag
        (B-TAG)";
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE Std 802.1Q";
    }
    enum ethernet-powerlink {
      value 34987;
      description
        "88-AB Ethernet Powerlink";
      reference
        "Organization: Ethernet Powerlink Standardization Group
        (EPSG)
        Standard: IEC 61158-4-13";
  }
    enum exp1 {
      value 34997;
```

```
      description
        "88-B5 Local experimental EtherType 1";
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE Std 802";
    }
    enum exp2 {
      value 34998;
      description
        "88-B6 Local experimental EtherType 2";
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE Std 802";
    }
    enum oui-ext {
      value 34999;
      description
        "88-B7 OUI Extended EtherType";
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE Std 802";
    }
    enum goose {
      value 35000;
      description
        "88-B8 IEC 61850 Generic Object Oriented Substation Event
        (GOOSE)";
      reference
        "Organization: IEC TC57
        Standard: IEC 61850-8-1";
    }
    enum gse {
      value 35001;
      description
        "88-B9 IEC 61850 Generic Substation Events (GSE) management
        services";
      reference
        "Organization: IEC TC57
        Standard: IEC 61850-8-1";
    }
    enum sv {
      value 35002;
      description
        "88-BA IEC 61850 Sampled Value Transmission (SV)";
      reference
        "Organization: IEC TC57
        Standard: IEC 61850-8-2";
    }
    enum pre-auth {
      value 35015;
      description
        "88-C7 RSNA Pre-Authentication";
      reference
        "Organization: IEEE 802.11 Working Group
```

```
        Standard: IEEE Std 802.11";
    }
    enum lldp {
      value 35020;
      description
        "88-CC Link Layer Discovery Protocol (LLDP)";
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE Std 802.1AB";
    }
    enum sercos {
      value 35021;
      description
        "88-CD Sercos Interface";
      reference
        "Organization: sercos international e.V.
        Standard: IEC 61158-4-19";
    }
    enum wsmp {
      value 35036;
      description
        "88-DC WAVE Short Message Protocol (WSMP)";
      reference
        "Organization: IEEE P1609 WG
        Standard: IEEE Std 1609";
    }
    enum homeplug-av-mme {
      value 35041;
      description
        "88-E1 HomePlug AV Mobile Management Entity (MME)";
      reference
        "Organization: HomePlug Powerline Alliance, Inc.
        Standard: IETF RFC 8519";
    }
    enum mrp {
      value 35043;
      description
        "88-E3 Media Redundancy Protocol";
      reference
        "Organization: Siemens AG
        Standard: IEC 62439-2";
    }
    enum macsec {
      value 35045;
      description
        "88-E5 MACsec EtherType";
      reference
        "Organization: IEEE 802 LAN/MAN Standards Committee
        Standard: IEEE Std 802.1AE";
    }
    enum i-tag {
      value 35047;
      description
        "88-E7 Backbone Service Instance Tag";
```

```
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE Std 802.1Q";
    }
    enum mvrp {
      value 35061;
      description
        "88-F5 Multiple VLAN Registration Protocol (MVRP)";
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE Std 802.1Q";
    }
    enum mmrp {
      value 35062;
      description
        "88-F6 Multiple MAC Registration Protocol (MMRP)";
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE Std 802.1Q";
    }
    enum ptp {
      value 35063;
      description
        "88-F7 Precision Time Protocol";
      reference
        "Organization: IEEE I&M Society TC9
        Standard: IEEE Std 1588";
    }
    enum cfm {
      value 35074;
      description
        "89-02 IEEE 802.1Q Connectivity Fault Management (CFM) PDU
        Encapsulation EtherType";
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE 802.1Q";
    }
    enum fcoe {
      value 35078;
      description
        "89-06 Fibre Channel over Ethernet (FCoE)";
      reference
        "Organization: Cisco Systems, Inc
        Standard: T11 FC-BB-5";
    }
    enum wlan-mgmt {
      value 35085;
      description
        "89-0D 802.11 Management Protocol";
      reference
        "Organization: IEEE 802.11 Working Group
        Standard: IEEE Std 802.11";
    }
    enum encap {
```

```
      value 35088;
      description
        "89-10 Backbone Service Encapsulated Addresses";
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE Std 802.1Q";
    }
    enum fip {
      value 35092;
      description
        "89-14 FCoE Initialization Protocol";
      reference
        "Organization: Brocade Communications Systems LLC
        Standard: IETF RFC 8519";
    }
    enum roce {
      value 35093;
      description
        "89-15 Remote Direct Memory Access (RDMA) over Converged
        Ethernet (RoCE)";
      reference
        "Organization: Mellanox Technologies, Inc.
        Standard: IBTA Specification";
    }
    enum mis {
      value 35095;
      description
        "89-17 Media Independent Service (MIS) Protocol";
      reference
        "Organization: IEEE 802.21 Working Group
        Standard: IEEE Std 802.21";
    }
    enum tte {
      value 35101;
      description
        "89-1D Time-Triggered Ethernet (TTE) Protocol Control
        Frame";
      reference
        "Organization: TTTech Computertechnik AG
        Standard: SAE AS6802";
    }
    enum mirp {
      value 35113;
      description
        "89-29 Multiple I-SID Registration Protocol (MIRP)";
      reference
        "Organization: IEEE 802.1 Working Group
        Standard: IEEE Std 802.1Q";
    }
    enum hsr {
      value 35119;
      description
        "89-2F High-availability Seamless Redundancy (HSR)";
      reference
```

```
          "Organization: International Electrotechnical Commission
          Standard: IEC 62439-3";
      }
      enum e-tag {
        value 35135;
        description
          "89-3F Bridge Port Extension Tag (E-TAG)";
        reference
          "Organization: IEEE 802.1 Working Group
          Standard: IEEE Std 802.1BR";
      }
      enum ecp {
        value 35136;
        description
          "89-40 Edge Control Protocol";
        reference
          "Organization: IEEE 802.1 Working Group
          Standard: IEEE Std 802.1Q";
      }
      enum f-tag {
        value 35147;
        description
          "89-4B Flow Filtering Tag (F-TAG)";
        reference
          "Organization: IEEE 802.1 Working Group
          Standard: IEEE Std 802.1Q";
      }
      enum drcp {
        value 35154;
        description
          "89-52 Distributed Relay Control Protocol (DRCP)";
        reference
          "Organization: IEEE 802.1 Working Group
          Standard: IEEE Std 802.1AX";
      }
      enum cim {
        value 35234;
        description
          "89-A2 Congestion Isolation Message (CIM)";
        reference
          "Organization: IEEE 802.1 Working Group
          Standard: IEEE Std 802.1Q";
      }
      enum llc-legacy {
        value 51665;
        description
          "C9-D1 LLC Encapsulation (obsolete)";
        reference
          "Organization: IEEE 802.1 Working Group
          Standard: IEEE Std 802.1AC";
      }
      enum mpp {
        value 57915;
        description
```

```
          "E2-3B MAC Privacy protection Protocol";
        reference
          "Organization:
          Standard: IEEE Std 802.1AE";
      }
      enum r-tag {
        value 61889;
        description
          "F1-C1 Frame Replication and Elimination for Reliability
          (FRER) Redundancy Tag (R-TAG)";
        reference
          "Organization: IEEE 802.1 Working Group
          Standard: IEEE Std 802.1CB";
      }
    }
    description
      "IEEE Std 802 EtherTypes subset.";
  }

}
```

Annex G

(informative)

Wake-on-LAN

Wake-on-LAN (WoL) is a common protocol to wake up devices from a very low power mode remotely. It can be implemented over IEEE 802 networks as a frame using the EtherType 08-42. The payload of a WoL packet following the EtherType is shown in Figure G.1.

6 octets	96 octets	0, 4 or 6 octets
Synchronization Stream	Target MAC	Password (optional)

Figure G.1—Wake-on-LAN packet payload fields

The Synchronization Stream contains the all-stations broadcast MAC address, as specified in 8.2.2. The Target MAC contains 16 duplications of the destination MAC address. The Password field is optional, but if present, contains either 4 octets (for an IPv4 address) or 6 octets (for a MAC address).