

1
2
3
4

5

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

9 Sponsor
10 **LAN/MAN Standards Committee**
11 of the
12 **IEEE Computer Society**
13

Important Notice

This document is an unapproved draft of a proposed IEEE Standard. IEEE hereby grants the named IEEE SA Working Group or Standards Committee Chair permission to distribute this document to participants in the receiving IEEE SA Working Group or Standards Committee, for purposes of review for IEEE standardization activities. No further use, reproduction, or distribution of this document is permitted without the express written permission of IEEE Standards Association (IEEE SA). Prior to any review or use of this draft standard, in part or in whole, by another standards development organization, permission must first be obtained from IEEE SA (stds-copyright@ieee.org). This page is included as the cover of this draft, and shall not be modified or deleted.

IEEE Standards Association
445 Hoes Lane
Piscataway, NJ 08854, USA

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

8 **Keywords:** BANs, body area networks, EtherTypes, IEEE 802[®], IEEE 802 architecture, IEEE 802
9 reference model, LANs, local area networks, MANs, metropolitan area networks, object identifiers,
10 PANs, personal area networks, RANs, regional area networks, protocol development, protocol
11 types

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

Copyright © 2023 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published xx Month 20xx. Printed in the United States of America.

IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

Object Management Group[®], OMG[®], UML[®] and Unified Modeling Language[™] are either registered trademarks or trademarks of Object Management Group, Inc. in the United States and/or other countries.

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

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

1 Important Notices and Disclaimers Concerning IEEE Standards Documents

2 IEEE documents are made available for use subject to important notices and legal disclaimers. These notices
3 and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all
4 standards and may be found under the heading “Important Notice” or “Important Notices and Disclaimers
5 Concerning IEEE Standards Documents.”

6 Notice and Disclaimer of Liability Concerning the Use of IEEE Standards 7 Documents

8 IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards
9 Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus
10 development process, which brings together volunteers representing varied viewpoints and interests to
11 achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic,
12 and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE
13 or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and
14 establishes rules to promote fairness in the consensus development process, IEEE does not independently
15 evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained
16 in its standards.

17 IEEE makes no warranties or representations concerning its standards, and expressly disclaims all
18 warranties, express or implied, concerning this standard, including but not limited to the warranties of
19 merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or
20 represent that the use of the material contained in its standards is free from patent infringement. IEEE
21 standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

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

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

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

41

42

1 Translations

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

5 Official statements

6 A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board
7 Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its
8 committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures,
9 symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall
10 make it clear that the presenter's views should be considered the personal views of that individual rather
11 than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements
12 made by volunteers may not represent the formal position of their employer(s) or affiliation(s).

13 Comments on standards

14 Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of
15 membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations,**
16 **consulting information or advice pertaining to IEEE Standards documents.**

17 Suggestions for changes in documents should be in the form of a proposed change of text, together with
18 appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is
19 important that any responses to comments and questions also receive the concurrence of a balance of
20 interests. For this reason, IEEE and the members of its Societies and subcommittees of the IEEE SA Board
21 of Governors are not able to provide an instant response to comments, or questions except in those cases
22 where the matter has previously been addressed. For the same reason, IEEE does not respond to
23 interpretation requests. Any person who would like to participate in evaluating comments or in revisions to
24 an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a
25 working group using the Interests tab in the Manage Profile & Interests area of the [IEEE SA myProject](#)
26 [system](#).¹ An IEEE Account is needed to access the application.

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

28 Laws and regulations

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

34 Data privacy

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

¹Available at: <https://development.standards.ieee.org/myproject-web/public/view.html#landing>.

²Available at: <https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html>.

1 Copyrights

2 IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws.
3 They are made available by IEEE and are adopted for a wide variety of both public and private uses. These
4 include both use, by reference, in laws and regulations, and use in private self-regulation, standardization,
5 and the promotion of engineering practices and methods. By making these documents available for use and
6 adoption by public authorities and private users, neither IEEE or its licensors waive any rights in copyright
7 to the documents.

8 Photocopies

9 Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license
10 to photocopy portions of any individual standard for company or organizational internal use or individual,
11 non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance
12 Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; [https://](https://www.copyright.com/)
13 www.copyright.com/. Permission to photocopy portions of any individual standard for educational
14 classroom use can also be obtained through the Copyright Clearance Center.

15 Updating of IEEE Standards documents

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

20 Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years
21 old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of
22 some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that
23 they have the latest edition of any IEEE standard.

24 In order to determine whether a given document is the current edition and whether it has been amended
25 through the issuance of amendments, corrigenda, or errata, visit [IEEE Xplore](#) or [contact IEEE](#).³ For more
26 information about the IEEE SA or IEEE's standards development process, visit the IEEE-SA Website.

27 Errata

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

32 Patents

33 IEEE Standards are developed in compliance with the [IEEE SA Patent Policy](#).⁵

34 Attention is called to the possibility that implementation of this standard may require use of subject matter
35 covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the

³Available at: <https://ieeexplore.ieee.org/browse/standards/collection/ieee>.

⁴Available at: <https://standards.ieee.org/standard/index.html>.

⁵Available at: <https://standards.ieee.org/about/sasb/patcom/materials.html>.

1 existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has
2 filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-
3 SA Website at <http://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate
4 whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or
5 under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair
6 discrimination to applicants desiring to obtain such licenses.

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

14 **IMPORTANT NOTICE**

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

1 Participants

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

3 **Glenn Parsons, *Chair***
4 **Jessy Rouyer, *Vice Chair***
5 **Jessy Rouyer, *Recording Secretary***
6 **James P. K. Gilb, *802-REVC Technical Editor***

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

¹ The following members of the individual balloting committee voted on this standard. Balloters may have
² voted for approval, disapproval, or abstention.

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

3 , *Chair*
4 , *Vice-chair*
5 , *Past Chair*
6 , *Secretary*

7 *Member Emeritus

⁸ Also included are the following nonvoting IEEE SA Standards Board liaisons:

9 <to be filled in by IEEE Editorial Staff>

1 Historical participants

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

4 **William P. Lidinsky, *Chair***

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

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

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

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

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

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

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

20 **Glenn Parsons, *Chair***
21 **John Messenger, *Vice Chair***
22 **Eric Gray, *Recording Secretary***
23 **James P. K. Gilb, *IEEE 802-2014 Technical Editor***
24

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

27 **Glenn Parsons, *Chair***
28 **John Messenger, *Vice Chair***
29 **Pat Thaler, *Chair, Data Center Bridging Task Group***
30 **Roger B Marks, *IEEE 802c Technical Editor***
31

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

34 **Glenn Parsons, *Chair***
35 **John Messenger, *Vice Chair***
36 **János Farkas, *Chair, Time-Sensitive Networking Task Group***
37 **Tony Jeffree, *Editor***
38

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

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

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

1 Introduction

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

3

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

- 7 — IEEE Std 802d[™]-2017: Specifying a Uniform Resource Name (URN) root identifier for YANG data
8 models
- 9 — IEEE Std 802c[™]-2017: Specifying an optional local medium access control (MAC) address space
10 structure
- 11 — IEEE Std 802f[™]-2023: Specifying a YANG module that contains EtherType information

12

Contents

2	1.	Overview.....	18
3	1.1	Scope.....	18
4	1.2	Purpose.....	18
5	1.3	Word usage	18
6	2.	Normative references.....	20
7	3.	Definitions, acronyms and abbreviations.....	21
8	3.1	Definitions	21
9	3.2	Acronyms and abbreviations	23
10	4.	Family of IEEE 802 standards	26
11	4.1	Key concepts.....	26
12	4.2	Application and support.....	27
13	4.3	An international family of standards	28
14	4.4	IEEE 802 standards.....	28
15	5.	Reference models (RMs)	30
16	5.1	Introduction.....	30
17	5.2	RM description for end stations.....	31
18	5.2.1	SAPs.....	32
19	5.2.2	LLC sublayer	32
20	5.2.3	MAC sublayer.....	33
21	5.2.4	PHY	34
22	5.2.5	Layer and sublayer management	34
23	5.3	Interconnection and interworking.....	34
24	5.3.1	Interconnection at the PHY.....	34
25	5.3.2	MAC-sublayer interconnection: Bridges.....	35
26	5.3.3	Network-layer interconnection: Routers.....	38
27	6.	General requirements for an IEEE 802 network.....	39
28	6.1	Services supported	39
29	6.2	Error ratios	39
30	7.	IEEE 802 network management	40
31	7.1	General.....	40
32	7.2	General-purpose IEEE 802 network management.....	40
33	7.2.1	Management functions.....	40
34	7.2.2	Management architecture.....	40
35	7.2.3	Managed object definitions.....	41
36	7.3	Special-purpose IEEE 802 network management standards	41
37	8.	MAC addresses	42
38	8.1	Terms and notational conventions	42
39	8.2	Universal addresses.....	42

1	8.2.1	Concept and overview	42
2	8.2.2	Assignment of universal addresses	43
3	8.2.3	Assignment by organizations	45
4	8.2.4	Uniqueness of address assignment	45
5	8.3	Interworking with 48-bit and 64-bit MAC addresses	45
6	8.4	Local MAC addresses	46
7	8.4.1	Concept and overview	46
8	8.4.2	Local MAC address assignment protocols	46
9	8.4.3	Structured Local Address Plan (SLAP)	46
10	8.4.4	SLAP local identifier types	48
11	8.4.5	Network Unique Identifier (NUI)	51
12	8.5	Standardized group MAC addresses	51
13	8.6	Bit-ordering and different MACs	51
14	9.	Protocol identifiers and context-dependent identifiers	52
15	9.1	Introduction	52
16	9.2	EtherTypes	52
17	9.2.1	Format, function, and administration	52
18	9.2.2	Public EtherType assignments subset	52
19	9.2.3	EtherTypes for prototype and vendor-specific protocol development	53
20	9.2.4	Local Experimental EtherTypes	53
21	9.2.5	OUI Extended EtherType	55
22	9.3	OUI, CID and OUI-36 as protocol identifiers	56
23	9.4	LSAP encoding of EtherType protocol identifier	57
24	9.5	SNAP	57
25	9.5.1	SNAP identifier	57
26	9.5.2	SNAP address	58
27	9.5.3	SNAP data unit format	58
28	9.6	Context-dependent identifiers	59
29	10.	Allocation of OID values in IEEE 802 standards	60
30	10.1	General	60
31	10.2	OIDs and ISO standards	60
32	10.3	The OID hierarchy for IEEE 802 standards	61
33	10.4	The OID hierarchy under iso(1) std(0) iso8802(8802)	62
34	10.5	Migration from previous OID allocations	62
35	11.	Allocation of Uniform Resource Name (URN) values in IEEE 802 standards	63
36	11.1	Introduction	63
37	11.2	The IEEE Namespace ID and Namespace Specific String	63
38	11.3	ResourceSpecificString values in IEEE 802 standards	63
39	Annex A	Bibliography	65
40	Annex B	RAMs for IEEE 802 standards	67
41	B.1	IEEE 802.3 RAMs	67
42	B.2	IEEE 802.11 RAM	69
43	B.3	IEEE 802.15™ RAMs	71
44	B.3.1	IEEE 802.15.3™ RAM	71
45	B.3.2	IEEE 802.15.4™ RAM	73

1	B.3.3	IEEE 802.15.6™ RM.....	73
2	B.3.4	IEEE 802.15.7™ RM.....	73
3	B.4	IEEE 802.16™ RM.....	74
4	B.4.1	Protocol RM.....	74
5	B.4.2	Network RM.....	75
6	B.5	IEEE 802.21™ RM.....	76
7	B.6	IEEE 802.22™ RM.....	77
8	B.6.1	Data plane.....	78
9	B.6.2	Management/control plane.....	78
10	B.6.3	Cognitive plane.....	78
11	Annex C Examples of bit ordering for addresses.....		79
12	C.1	General.....	79
13	C.2	Illustrative examples.....	79
14	Annex D List of IEEE 802 standards.....		82
15	Annex E History.....		84
16	E.1	Universal addresses.....	84
17	E.2	IEEE RA address block products.....	84
18	E.3	Local MAC addresses.....	85
19	Annex F EtherType Listing Subset.....		86
20	F.1	Introduction.....	86
21	F.2	Tabular format.....	86
22	F.3	YANG module for EtherType subset.....	89
23	F.3.1	YANG Framework.....	89
24	F.3.2	Definition for ieee802-ethertype YANG module.....	90
25	Annex G Wake-on-LAN.....		102

1

2

3 IEEE Standard for Local and 4 Metropolitan Area Networks: 5 Overview and Architecture

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

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

16 1. Overview

17 1.1 Scope

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

21 1.2 Purpose

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

25 1.3 Word usage

26 The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard
27 and from which no deviation is permitted (*shall* equals *is required to*).

28 The word *should* indicates that among several possibilities one is recommended as particularly suitable,
29 without mentioning or excluding others; or that a certain course of action is preferred but not necessarily
30 required (*should* equals *is recommended that*).¹

¹ The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).²

³ The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

¹The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.

²The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.

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 (including any amendments or corrigenda) applies.

IEEE Std 802.1Q™, IEEE Standard for Local and metropolitan area networks—Bridges and Bridged Networks.^{3, 4}

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).⁵

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.⁶ (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.⁷

18

³The IEEE standards referred to in Clause 2 are trademarks owned by The Institute of Electrical and Electronics Engineers, Incorporated.

⁴IEEE publications are available from The Institute of Electrical and Electronics Engineers (<https://standards.ieee.org/>).

⁵IETF documents (i.e., RFCs) are available the Internet Engineering Task Force (<https://www.rfc-archive.org/>).

⁶ISO/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/>).

⁷ITU-T publications are available from the International Telecommunications Union (<https://www.itu.int/>).

1 3. Definitions, acronyms and abbreviations

2 3.1 Definitions

3 For this document, the following terms and definitions apply. *The IEEE Standards Dictionary Online*⁸
4 should be consulted for terms not defined in this clause.⁹

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

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

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

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

16 **Ethernet:** A communication protocol specified by IEEE Std 802.3[™].

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

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

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

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

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

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

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

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

⁸The IEEE Standards Dictionary Online is not a dictionary but rather is a compendium of balloted definitions from individual approved standards.

⁹The *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.

- 1 **logical link:** A logical communication connection between two devices.
- 2 **medium access control (MAC) data frame:** A data structure consisting of fields in accordance with a
3 MAC protocol, for the communication of user data and control information in a network; one of the fields
4 contains a sequence of octets of user data.
- 5 **medium access control (MAC) protocol:** A protocol that governs access to the transmission medium in a
6 network, to enable the exchange of data between stations in a network.
- 7 **media-independent control function:** A parallel control plane that provides control functions for different
8 medium access control (MAC) and physical layer (PHY) sublayers and provides a media-independent
9 abstraction to higher layer protocols.
- 10 **media-independent handover function:** A function that provides the ability to relocate traffic flows
11 between different medium access technologies and associated physical media.
- 12 **metropolitan area network (MAN):** A network of devices, extending over a large geographical area such
13 as an urban area, often providing integrated communication services such as data, voice, and video.
- 14 **Network Unique Identifier (NUI):** An identifier that is unique within the IEEE 802[®] local area network
15 (LAN).
- 16 **noncanonical format:** The format of a medium access control (MAC) data frame in which the octets of 48-
17 bit Extended Unique Identifiers (EUI-48s) or 64-bit Extended Unique Identifiers (EUI-64s) conveyed in the
18 MAC user data field have the same bit ordering as in the bit-reversed representation.
- 19 **personal area network (PAN):** A network of devices extending over a very limited geographical area, used
20 to convey information among a group of participant stations.
- 21 **private protocol:** A protocol whose use and specification are controlled by a private organization.
- 22 **public protocol:** A protocol whose specification is published and known to the public, but controlled by an
23 organization other than a formal standards body.
- 24 **regional area network (RAN):** A network of devices that generally covers a service area that is larger than
25 metropolitan area networks (MANs), typically in sparsely populated areas.
- 26 **repeater:** A device used to interconnect segments of the physical communications media, for example, to
27 extend the range of a network when the physical specifications of the technology would otherwise be
28 exceeded, while providing a single access domain for the attached stations.
- 29 **service data unit:** Information that is delivered between layers or sublayers.
- 30 **single access domain:** A set of stations such that, at most, only one can transmit at a given time, with all
31 other stations acting as (potential) receivers.
- 32 **standard protocol:** A protocol whose specification is published and known to the public and is controlled
33 by a standards body.
- 34 **station:** An end station or bridge. *See also:* **bridge**; **end station**.
- 35 **Structured Local Address Plan (SLAP):** An optional standardized specification to assign locally
36 administered medium access control (MAC) addresses.

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

3 3.2 Acronyms and abbreviations

4	AAI	Administratively Assigned Identifier
5	AAI-48	48-bit AAI
6	AAI-64	64-bit AAI
7	BS	base station
8	BSS	basic service set
9	CID	Company ID
10	CPE	customer-premises equipment
11	CS	convergence sublayer
12	C-SAP	control service access point
13	DCN	data center networking
14	DLL	data link layer
15	ELI	Extended Local Identifier
16	ELI-48	48-bit ELI
17	ELI-64	64-bit ELI
18	EPD	EtherType protocol discrimination
19	EPON	Ethernet passive optical networks
20	EUI	Extended Unique Identifier
21	EUI-48	48-bit EUI
22	EUI-64	64-bit EUI
23	HLPDE	higher layer protocol discrimination entity
24	IANA	Internet Assigned Numbers Authority ¹⁰
25	IEEE RA	Institute of Electrical and Electronic Engineers Registration Authority
26	IEEE RAC	Institute of Electrical and Electronic Engineers Registration Authority Committee
27	I/G	individual/group
28	IM	implementation model
29	IoT	Internet of things
30	IP	Internet Protocol
31	LAN	local area network
32	LLC	logical link control
33	LPD	LLC protocol discrimination
34	LSAP	link service access point
35	LSB	least significant bit
36	MAC	medium access control, media access control ¹¹
37	MA-L	MAC Address Block Large
38	MA-M	MAC Address Block Medium
39	MAN	metropolitan area network
40	MA-S	MAC Address Block Small
41	MCPS	MAC common part sublayer
42	MCPS-SAP	MAC common part sublayer data service access point

¹⁰<https://www.iana.org>

¹¹Both forms are used, with the same meaning. This standard uses medium.

1	MIB	management information base
2	MICF	media-independent control function
3	MICLSAP	media-independent control link service access point
4	MICPSAP	media-independent control physical service access point
5	MICSAP	media-independent control service access point
6	MIH	media-independent handover
7	MIHF	media-independent handover function
8	MLME	MAC sublayer management entity
9	MSAP	MAC service access point
10	M-SAP	management service access point
11	MSB	most significant bit
12	MSTP	multiple spanning tree protocol
13	NCMS	network control and management system
14	NETCONF	Network Configuration Protocol
15	NID	Namespace Identifier
16	NUI	Network Unique Identifier
17	NUI-48	48-bit NUI
18	NUI-64	64-bit NUI
19	OAM	operations, administration, and maintenance
20	OID	object identifier
21	OLT	optical line terminal
22	OMG®	Object Management Group®
23	ONU	optical network unit
24	OSI/RM	Open Systems Interconnection basic reference model
25	OUI	Organizationally Unique Identifier
26	PAN	personal area network
27	PDU	protocol data unit
28	PHY	physical layer (OSI reference model and IEEE 802® reference model)
29	PHY	physical layer device or entity (IEEE 802.3™ reference model)
30	PICS	protocol implementation conformance statement
31	PLME	physical layer management entity
32	PMD	physical medium dependent
33	PSAP	physical service access point
34	RAN	regional area network
35	RM	reference model
36	RSTP	rapid spanning tree protocol
37	SAP	service access point
38	SAI	Standard Assigned Identifier
39	SAI-48	48-bit Standard Assigned Identifier
40	SAI-64	64-bit Standard Assigned Identifier
41	SLAP	Structured Local Address Plan
42	SNAP	Subnetwork Access Protocol
43	SNMP	Simple Network Management Protocol
44	SPB	shortest path bridging
45	SSF	spectrum sensing function
46	SS/MS	subscriber station/mobile subscriber station

1	TSN	Time-Sensitive Networking
2	U/L	universally or locally administered
3	UML™	unified modeling language®
4	URN	Uniform Resource Name
5	VLAN	virtual local area network
6	VOIP	voice over Internet protocol
7	WAN	wide area network
8	WLAN	wireless local area network
9	WPAN	wireless personal area network
10	WRAN	wireless regional area network
11	YANG	The name of the data modeling language defined in IETF RFC 6020 [B16] ¹² and IETF
12		RFC 7950 [B18].

¹²The numbers in brackets correspond to the numbers of the bibliography in Annex A.

1 4. Family of IEEE 802 standards

2 4.1 Key concepts

3 The family of IEEE 802 standards is the collection of standards that have been developed under the IEEE
4 802 LMSC, see 4.4 for a list of the IEEE 802 standards current as of the publication of this standard. The
5 scope of IEEE 802 standards is not limited to the physical layers (PHYs) and data link layers (DLLs). IEEE
6 802 networks use frame-based communications over a variety of media to connect various digital apparatus
7 regardless of computer technology and data type.

8 The basic communications capabilities provided by all IEEE 802 standards are frame based with source and
9 destination addressing and asynchronous timing of the frames¹³. In a frame-based system, the format is a
10 variable-length sequence of data octets. By contrast, cell-based communication transmits data in fixed-
11 length units in specified time intervals while isochronous communication transmits data as a steady stream
12 of octets, or groups of octets, at equal time intervals. Some IEEE 802 networks can provide scheduled frame
13 transmissions in addition to or alternatively to asynchronous frame transmissions.

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

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

33 Some IEEE 802 technologies, in particular wireless-based technologies, are inherently shared-medium
34 communication systems. They too have been augmented over time. Many wireless local area networks
35 (WLANs) support mobile node mobility and hence dynamic topologies. These additional facilities may,
36 depending on the IEEE 802 technology in use, restrict bridged LAN interconnects to the static topology
37 nodes within the wireless portion of a heterogeneous technology LAN. Additionally, it is common to
38 interconnect individual networks and bridged networks at layers above the DLL with devices called routers.
39 The specification of routers is not provided in IEEE 802 standards.

40 An IEEE 802 LAN is a peer-to-peer communication network that enables stations to communicate directly
41 on a point-to-point, or point-to-multipoint, basis without requiring them to communicate with any
42 intermediate stations that perform forwarding or filtering above the PHY. LAN communication takes place
43 at moderate to high data rates and with short transit delays, on the order of a few milliseconds or less.

¹³Some IEEE 802 standards have asynchronous symbol timing within a frame.

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

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

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

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

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

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

32 4.2 Application and support

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

- 38 — Client/server applications
- 39 — Database access
- 40 — Desktop publishing
- 41 — Electronic mail
- 42 — File transfer
- 43 — Graphics
- 44 — Handover services

- 1 — Multimedia
- 2 — Office automation
- 3 — Vehicular communication
- 4 — Process control
- 5 — Robotics
- 6 — Telecommunication
- 7 — Text processing
- 8 — Transaction processing

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

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

18 **4.3 An international family of standards**

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

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

34 **4.4 IEEE 802 standards**

35 The IEEE 802 LAN/MAN Standards Committee sponsors a large number of standards projects. The current
36 family of IEEE 802 standards¹⁴ as of the approval of this standard is illustrated in Figure 1. IEEE 802
37 standards are under continuous development; for the latest status refer to <https://www.ieee802.org>.

¹⁴Throughout this standard, the term IEEE 802 standard is interpreted to include standards, recommended practices and guides.

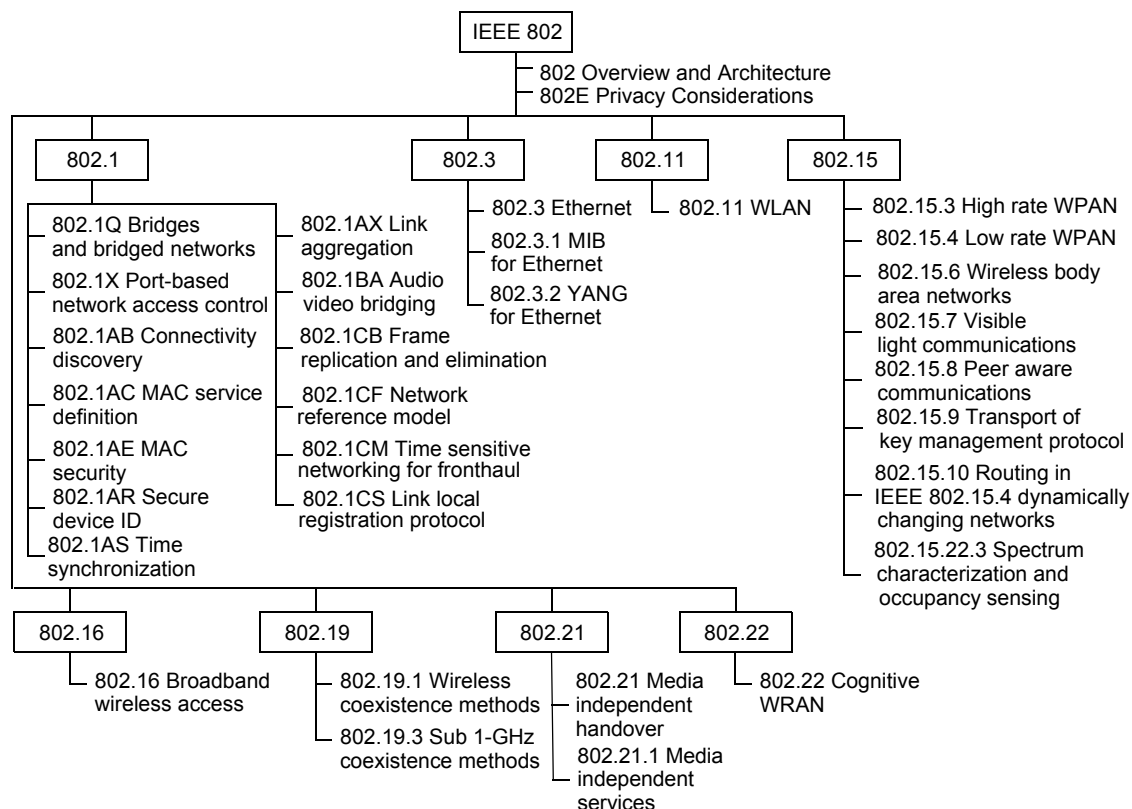


Figure 1—Current family of IEEE 802 standards

1 At any given time, an IEEE 802 standard may have one or more amendments related to it. Each amendment,
2 once approved, is considered to be part of the base standard. At a future time, through the periodic IEEE-SA
3 revision process, these amendments are incorporated into the base standard so that a new single document
4 can be issued. This process is illustrated in Figure 2 for IEEE Std 802.15.4TM-2011,¹⁵ which incorporated
5 the amendments IEEE Std 802.15.4aTM-2007, IEEE Std 802.15.4cTM-2009, and IEEE Std 802.15.4dTM-2009
6 into the base standard IEEE Std 802.15.4-2006.

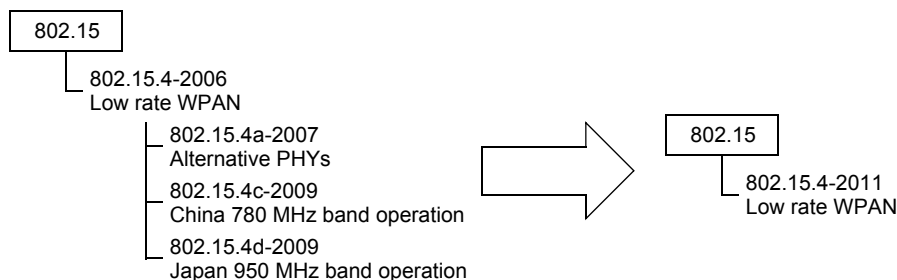


Figure 2—Issuance of IEEE Std 802.15.4-2011 from previous base standard and amendments

¹⁵See Annex D for a list of approved IEEE 802 standards that were current when this standard was completed.

1 5. Reference models (RMs)

2 5.1 Introduction

3 The IEEE 802 RM is derived from the Open Systems Interconnection basic reference model (OSI/RM),
4 ISO/IEC 7498-1:1994 [B20]¹⁶. It is assumed that the reader has some familiarity with the OSI/RM and its
5 terminology. The IEEE 802 standards emphasize the functionality of the lowest two layers of the OSI/RM,
6 i.e., PHY and DLL, and the higher layers as they relate to network management. The IEEE 802 RM is
7 similar to the OSI/RM in terms of its layers and the placement of its service boundaries. Figure 3 shows the
8 architectural view of IEEE 802 RM for end stations and its relation to the OSI/RM. A variation of the model
9 applies within bridges, as described in 5.3.2.

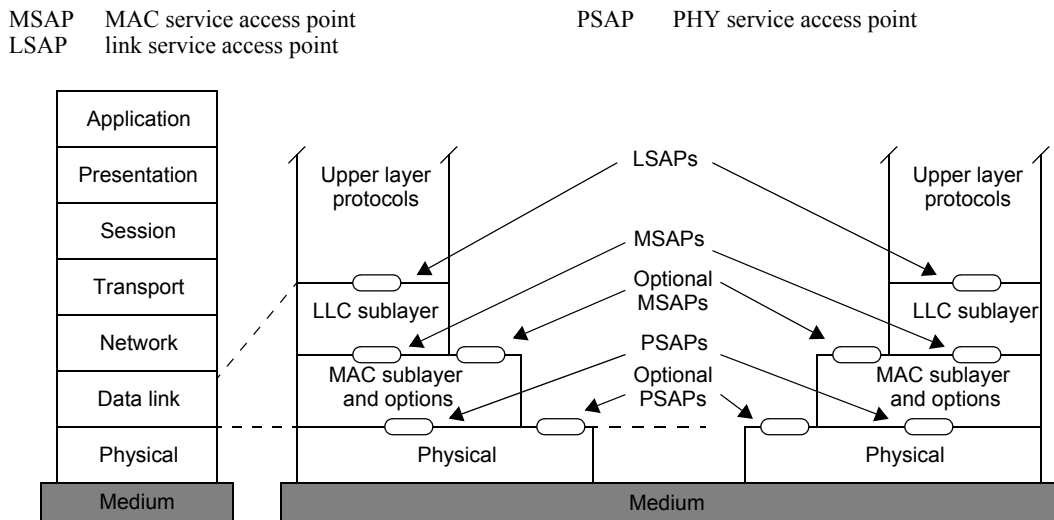


Figure 3—IEEE 802 RM for end stations

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

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

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

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

¹⁶The numbers in brackets correspond to those of the bibliography in Annex A.

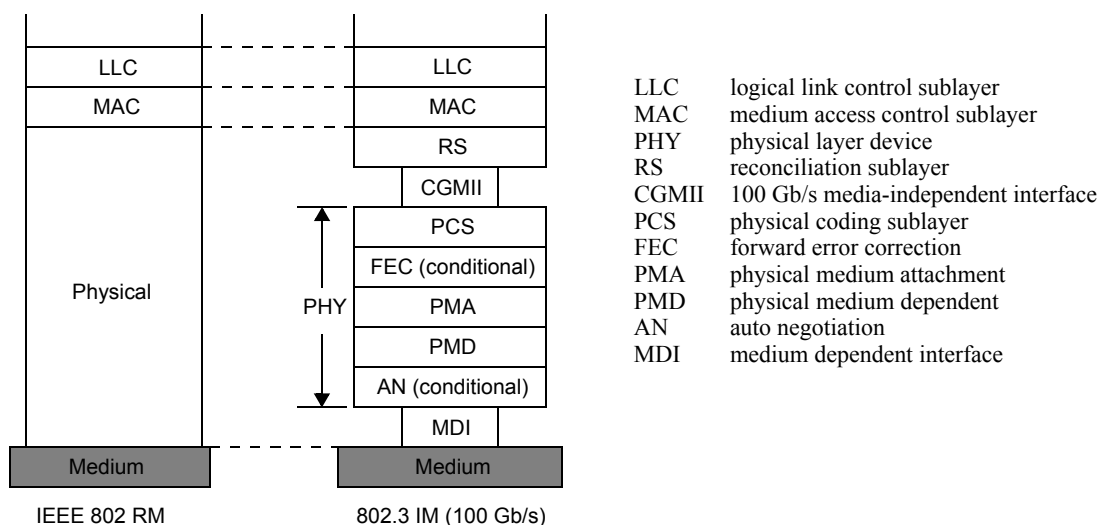


Figure 4—IEEE 802 RM and an example of an end-station IM (100 Gb/s)

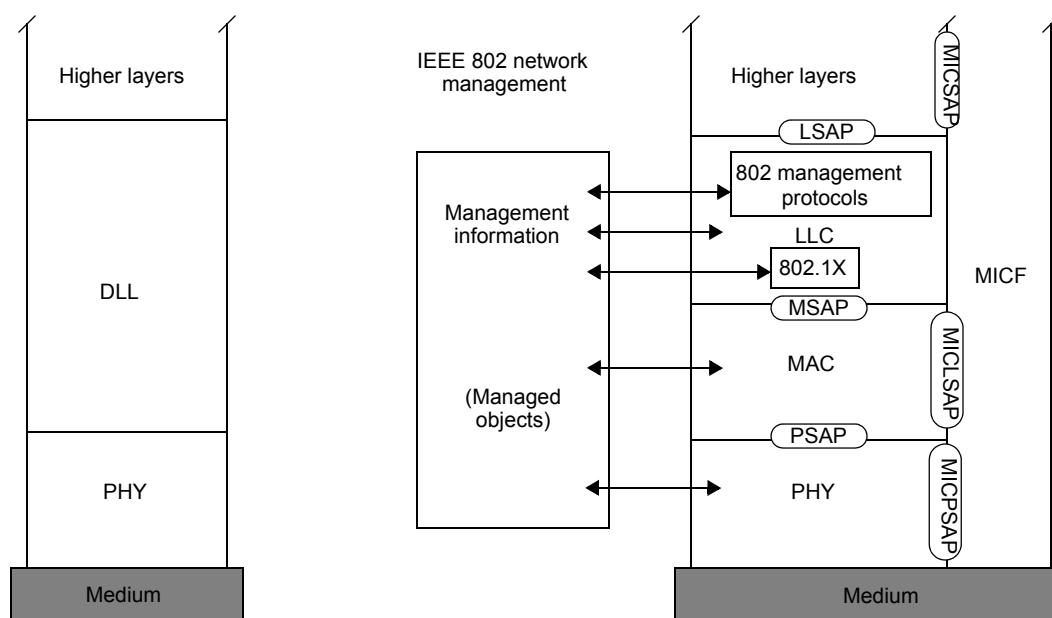


Figure 5—IEEE 802 RM with end-station management, security, and MIH

1 5.2 RM description for end stations

2 The IEEE 802 RM maps to the OSI/RM as shown in Figure 3. The applicable part of the OSI/RM consists of
3 the lowest two layers: the DLL and the PHY. These map onto the same two layers in the IEEE 802 RM. The
4 MAC sublayer of the IEEE 802 RM exists between the PHY and the LLC sublayer to provide a service for
5 the LLC sublayer (certain MAC types provide additional MAC service features that can be used by LLC
6 sublayer, in addition to the common core features). Service access points (SAPs) for connecting the layers
7 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.

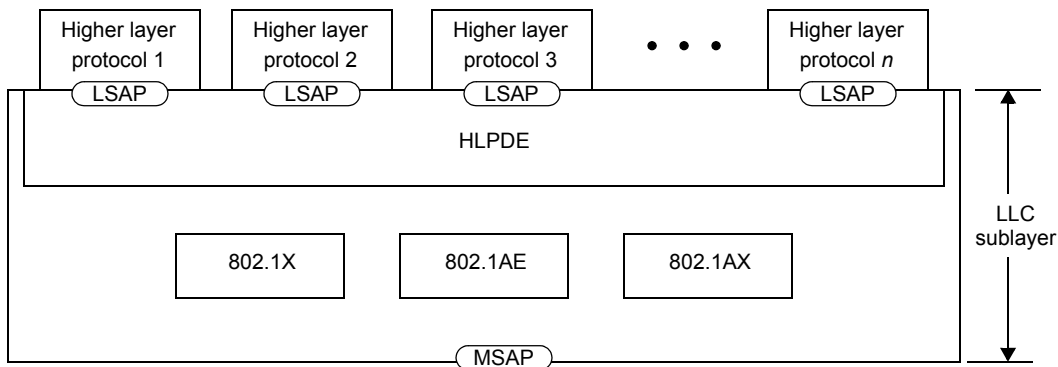


Figure 6—LLC sublayer in 802 RM

The higher layer protocol discrimination entity (HLPDE) is used by the LLC sublayer to determine the protocol identifier designating 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, as the protocol identifier, the EtherType value made available to the LLC sublayer through the MSAP; and
- 2) LLC protocol discrimination (LPD), which uses, as the protocol identifier the LLC address as specified in ISO/IEC 8802-2 or, using a particular form (described in 9.4) of the Subnetwork Access Protocol (SNAP) format, an EtherType.

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

LSAP encoding supports LPD, allowing the decoding of LSAP addresses. LSAP also supports EPD using the RFC 1042 form of SNAP, as described in 9.4. The general form of SNAP also allows the decoding of private protocol identifiers (neither LSAP addresses nor EtherTypes) under an assigned OUI or CID, as described in 9.5.

1 LSAP addresses and EtherTypes may be encoded as protocol identifiers using Length/Type encoding, as
2 exemplified in IEEE Std 802.3, which uses the value of a Length/Type field to distinguish between EPD and
3 LPD. Length/Type encoding also allows the decoding of protocol identifiers that are neither LSAP
4 addresses nor EtherTypes, namely:

- 5 — private protocol identifiers under the OUI Extended EtherType, as described in 9.2.4; and
- 6 — experimental protocol identifiers under the Local Experimental EtherType, as described in 9.2.3.

7 LPD/SNAP should not be used with Length/Type encoding. Length/Type encoding, using the LLC
8 encapsulation EtherType of IEEE Std 802.1AC, allows LSAP protocol identifiers to be encoded even when
9 the value of the Length/Type field indicates EPD.

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

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

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

17 **5.2.3 MAC sublayer**

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

23 The principal functions of the MAC sublayer comprise the following:

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

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

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

40 The various MAC specifications all specify MAC frame formats in terms of a serial transmission model for
41 the service provided by the supporting PHY. This model supports concepts such as “first bit (e.g., of a

1 particular octet) to be transmitted” and a strict order of octet transmission in a uniform manner. However,
2 the ways in which the model has been applied in different MAC specifications are not completely uniform
3 with respect to bit-ordering within octets (see Clause 8, and particularly 8.6, for examples and explanation).
4 The serial transmission model does not preclude current or future MAC specifications from using partly or
5 wholly octet-oriented specifications of frame formats or of the interface to the PHY.

6 **5.2.4 PHY**

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

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

15 **5.2.5 Layer and sublayer management**

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

19 **5.3 Interconnection and interworking**

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

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

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

32 **5.3.1 Interconnection at the PHY**

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

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

1 5.3.2 MAC-sublayer interconnection: Bridges

2 5.3.2.1 Bridges and bridged IEEE 802 networks

3 Bridges are stations that interconnect multiple access domains. IEEE Std 802.1Q¹⁷ provides the basic
4 specification for bridge interworking among bridgeable IEEE 802 networks. A bridged IEEE 802 network
5 consists of one or more bridges together with the complete set of access domains that they interconnect. A
6 bridged IEEE 802 network provides end stations belonging to any of its access domains with the
7 connectivity of a network that contains the whole set of attached end stations.

8 A bridged network can provide for the following:

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

19 NOTE—The term switch is sometimes used in the industry to refer to products that include an IEEE 802.1Q bridge
20 capability.

21 5.3.2.2 Bridge relaying and filtering

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

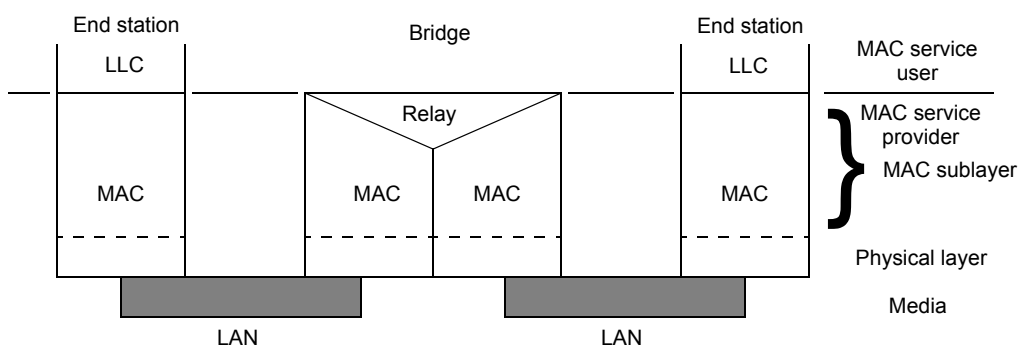


Figure 7—Internal organization of the MAC sublayer with bridging

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

¹⁷Information on normative references can be found in Clause 2.

1 5.3.2.3 Resolving topologies with multiple paths

2 A key aspect of IEEE Std 802.1Q is the specification of the spanning tree protocols and shortest path
3 bridging (SPB) which are used by bridges to configure their interconnections in order to prevent looping
4 data paths in the bridged IEEE 802 network.

5 If the basic interconnection topology of bridges and networks contains multiple possible paths between
6 certain points, use of the rapid spanning tree protocol (RSTP) blocks some paths in order to produce a
7 simply connected active topology for the flow of MAC user traffic between end stations. For each point of
8 attachment of a bridge to a network, the RSTP selects whether MAC user traffic is to be received and
9 transmitted by the bridge at that point of attachment.

10 The RSTP adapts to changes in the configuration of the bridged IEEE 802 network, maintaining
11 connectivity while avoiding data loops. Some configuration changes can cause temporary interruptions of
12 connectivity between parts of the bridged IEEE 802 network, typically lasting for a few tens of milliseconds
13 at most. IEEE Std 802.1Q specifies a variant of RSTP, the multiple spanning tree protocol (MSTP), that can
14 configure multiple, independent spanning trees within a bridged network.

15 In addition, IEEE Std 802.1Q specifies SPB, which allows the use of shortest path communication within
16 administratively defined network regions, while retaining concurrent support for all existing spanning tree
17 protocols. The use of SPB, for unicast and multicast, allows multiple paths to be used simultaneously.

18 5.3.2.4 Transparent bridging

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

22 5.3.2.5 Provider bridging

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

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

33 5.3.2.6 Time-Sensitive Networking (TSN)

34 Some IEEE 802 standards specify TSN capabilities to provide network protocols and mechanisms for use by
35 applications that need data transport with low and bounded latency, low and bounded delay variation, and
36 low packet loss. The TSN capabilities augment networking protocols and mechanisms to support both TSN
37 traffic streams as well as other traffic. Some TSN capabilities are described in the following standards:

- 38 a) Timing and Synchronization for Time-Sensitive Applications (IEEE Std 802.1AS-2020 [B3])
- 39 b) Credit-Based Shaper: (IEEE Std 802.1Q-2022, 5.4.1.5)
- 40 c) Frame Preemption (IEEE Std 802.3-2022 [B8] Clause 99 and IEEE Std 802.1Q-2022, 5.26)
- 41 d) Scheduled Traffic (IEEE Std 802.1Q-2022, 8.6.8.4)

- 1 e) Cyclic Queuing and Forwarding (IEEE Std 802.1Q-2022, 5.4.1.9)
- 2 f) Asynchronous Traffic Shaping (IEEE Std 802.1Q-2022, 5.4.1.10)
- 3 g) Per-Stream Filtering and Policing (IEEE Std 802.1Q-2022, 5.4.1.8)
- 4 h) Frame Replication and Elimination for Reliability (IEEE Std 802.1CB-2017 [B5])
- 5 i) Stream Reservation Protocol (IEEE Std 802.1Q-2022, clause 35.)
- 6 j) Link-local Registration Protocol (IEEE Std 802.1CS-2020 [B7])
- 7 k) Path Control and Reservation (IEEE Std 802.1Q-2022, 5.4.6)
- 8 l) TSN Configuration (IEEE Std 802.1Q-2022, 5.29)
- 9 m) Configuration Enhancements for Time-Sensitive Networking (IEEE Std 802.1Qdj-2023)

10 NOTE—There is no need to apply all the TSN features in a network and none of the TSN features are a requirement. The
11 application area or actual deployment determine which TSN features are used in a given network, e.g., whether or not
12 time synchronization is used. TSN profile standards, e.g., IEEE Std 802.1BA [B4] and IEEE Std 802.1CM [B6] select
13 TSN features and give guidelines on their use in a particular application area.

14 5.3.2.7 Data center networking bridging

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

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

28 5.3.2.8 Bridging example

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

35 Figure 8 illustrates an example of a bridged IEEE 802 network that can be configured with bridge-style
36 interconnection. The bridges A and B, and the IEEE 802.3 LAN configurations to which they attach, are
37 typical of the older style of bridged IEEE 802 network in which a bridge interconnects a small number of
38 access domains, each containing many end stations, as is similar with K, L, T and U. The IEEE 802.3
39 connections to M and those between S and T and S and U form IEEE 802 backbone networks. On the other
40 hand, the bridges T, and U function as bridges that combine IEEE 802.3 and IEEE 802.16™ networks. S and
41 M are bridges on an IEEE 802 backbone network, handling a number of network attachments. T and U are
42 bridges that support multiple end stations, with connection to an IEEE 802 backbone network. B and K also
43 provide access to an IEEE 802 backbone network. The end station shown connected to S by a point-to-point
44 link could be a server system. The wireless interfaces shown in Figure 8 are defined in each of the listed
45 standards. For example, a discussion of the 802.11 architecture is given in Annex B.2.

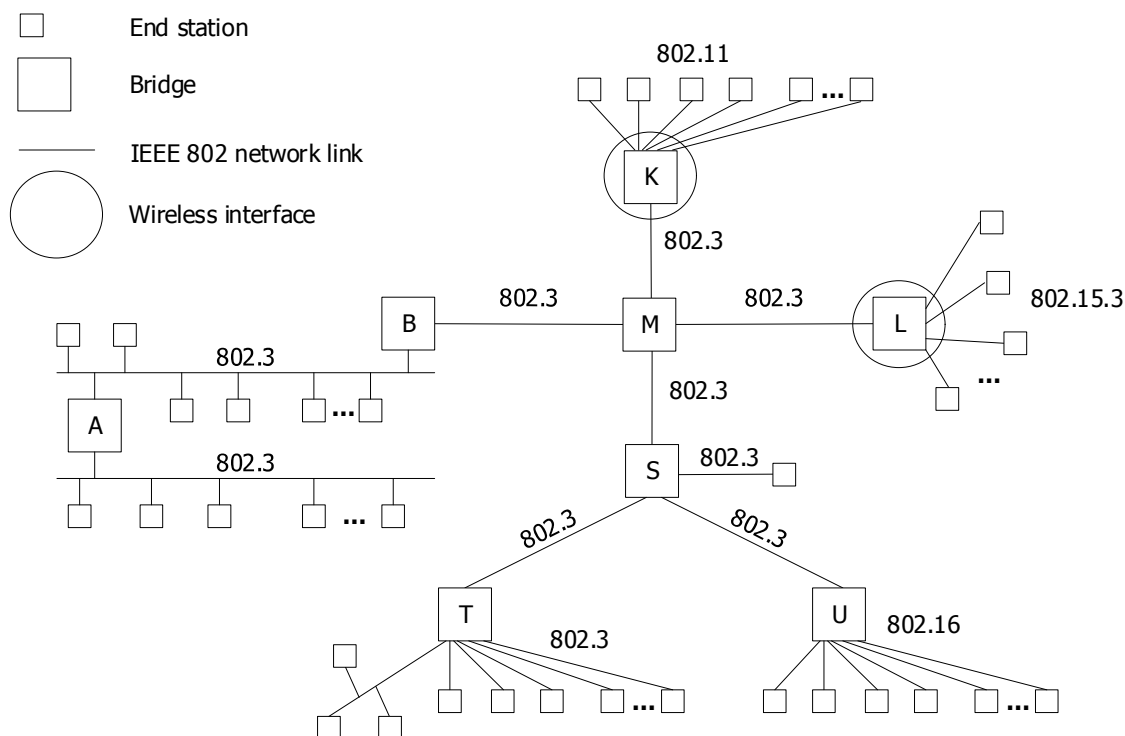


Figure 8—An example of a bridged IEEE 802 network

1 5.3.3 Network-layer interconnection: Routers

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

6. General requirements for an IEEE 802 network

6.1 Services supported

With the descriptions in Clause 5 as a basis, a bridgeable 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. A bridgeable 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.

NOTE—Some networks not specified in IEEE 802 standards meet these requirements and are therefore bridgeable IEEE 802 networks.

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.

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.

1 7. IEEE 802 network management

2 7.1 General

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

8 7.2 General-purpose IEEE 802 network management

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

13 7.2.1 Management functions

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

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

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

29 7.2.2 Management architecture

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

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

1 The Simple Network Management Protocol (SNMP), as described in IETF RFC 3411 [B14], and Network
2 Configuration Protocol (NETCONF), as described in RFC 6241 [B17], are examples of general-purpose
3 management protocol that can be used for the management of IEEE 802 network equipment.

4 **7.2.3 Managed object definitions**

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

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

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

18 SNMP is used in many cases together with the structure of management information known as SMIV2 (IETF
19 RFC 2578, IETF RFC 2579 [B12], and IETF RFC 2580 [B13]), which uses a set of macros based on a
20 subset of ASN.1 for defining managed objects. YANG (IETF RFC 7950 [B18]) is a data modeling language
21 used to model configuration data, state data, remote procedure calls, and notifications for network
22 management protocols. The YANG objects are modeled in IEEE 802 standards using the Object
23 Management Group® (OMG®) similar to those of Unified Modeling Language™ (UML®) diagrams.

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

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

27 **7.3 Special-purpose IEEE 802 network management standards**

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

1 8. MAC addresses

2 8.1 Terms and notational conventions

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

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

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

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

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

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

24 8.2 Universal addresses

25 8.2.1 Concept and overview

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

30 NOTE—Some network standards that are not IEEE 802 standards also use MAC addresses that are compliant with this
31 standard.

32 A universal address is a MAC address that is globally unique.¹⁸ Two different lengths of universal addresses
33 have been specified by the IEEE Registration Authority (RA): 48-bit Extended Unique Identifier (EUI-48)
34 and 64-bit Extended Unique Identifier (EUI-64).

¹⁸And beyond the earth as well. For example, IEEE Std 802.15.4 was deployed on the Mars helicopter.

8.2.2 Assignment of universal addresses

The IEEE RA has the responsibility for the administration of IEEE 802 network universal addresses.¹⁹ The IEEE RA is recognized by ISO/IEC as the registration authority for universal addresses 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 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 1.²⁰

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.

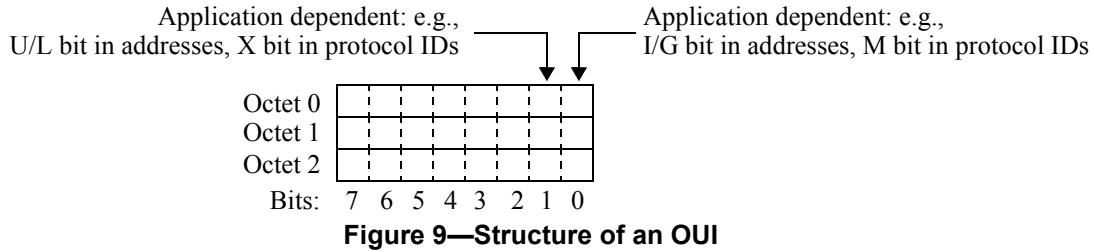
The standard representation of MA-L, MA-M, and MA-S is to use the hexadecimal representation. See 8.6 for further specification relating to use of the bit-reversed representation.

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.

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.

¹⁹Interested applicants should contact the IEEE RA <https://standards.ieee.org/regauth>

²⁰More 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/>.



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

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

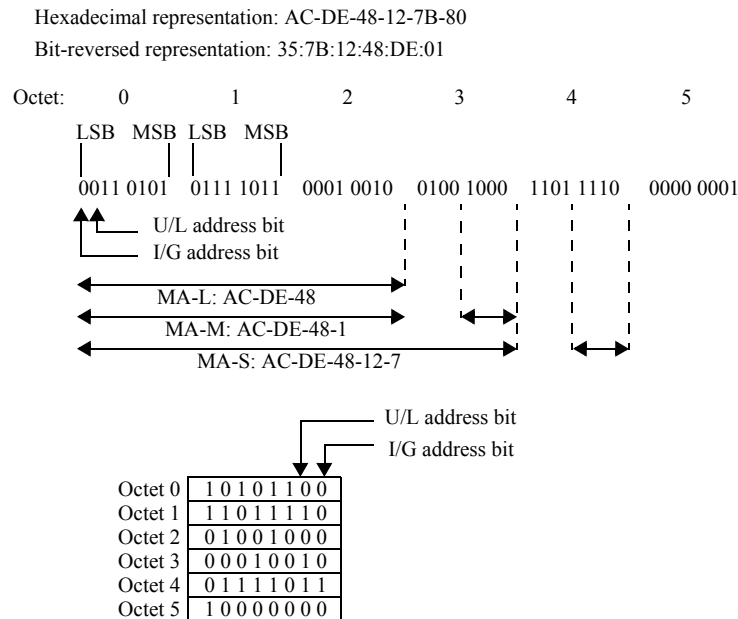


Figure 10—Example EUI-48

11 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.
12 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
13 examples of MA-L, MA-M, and MA-S, the first 3 octets are different for valid assigned IEEE RA values.

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

15 NOTE 4—The upper, bit-stream representation of the EUI-48 in Figure 10 and the EUI-64 in Figure 11 shows the LSB
16 of each octet first; this corresponds to the data-communications convention for representing bit-serial transmission in
17 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

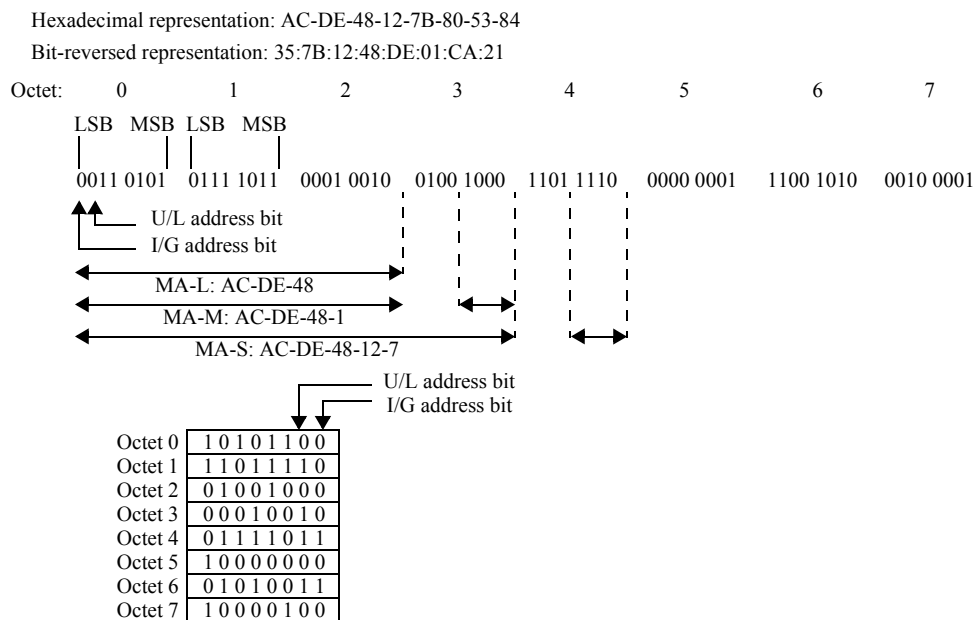


Figure 11—Example EUI-64

1 further discussion of bit-ordering issues. The lower, octet-sequence representation shows the bits within each octet in the
2 usual order for binary numerals; the order of octet transmission is from the top downward.

3 8.2.3 Assignment by organizations

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

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

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

18 8.2.4 Uniqueness of address assignment

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

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

22 8.3 Interworking with 48-bit and 64-bit MAC addresses

23 In response to concerns that the EUI-48 space could be exhausted by the breadth of products requiring
24 unique identifiers, 64-bit MAC addresses were introduced. Initially, new IEEE standards projects that did

1 not require backward compatibility with EUI-48 were requested to use 64-bit MAC addresses. This led to
2 some IEEE 802 standards adopting 64-bit MAC addressing, which cannot be bridged onto IEEE 802 net-
3 works that use 48-bit MAC addressing. Truncating a 64-bit MAC address into a 48-bit field can lead to two
4 stations having the same 48-bit value. To avoid this, traffic between a 64-bit MAC addressed network and a
5 48-bit MAC addressed network needs to be routed at a layer above the DLL..

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

7 **8.4 Local MAC addresses**

8 **8.4.1 Concept and overview**

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

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

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

24 **8.4.2 Local MAC address assignment protocols**

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

28 When multiple address assignment protocols operate on a LAN without centralized administration, address
29 duplication is possible, even if each protocol alone is designed to avoid duplication, unless such protocols
30 assign addresses from disjoint address pools. Administrators who deploy multiple protocols on a LAN in
31 accordance with the SLAP enable the unique assignment of local MAC addresses within the LAN as long as
32 each protocol maintains unique assignments within its own address subspace.

33 **8.4.3 Structured Local Address Plan (SLAP)**

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

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

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

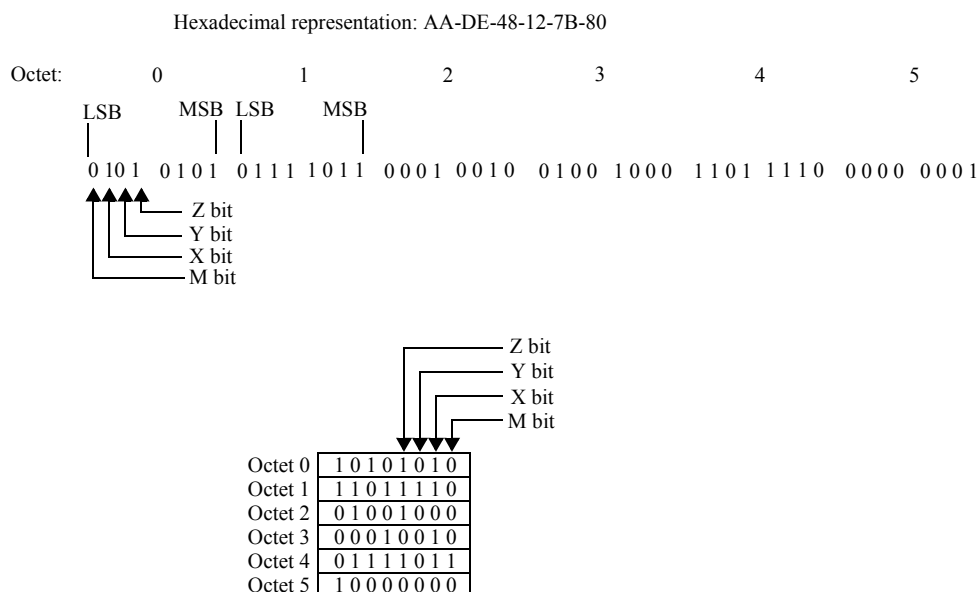


Figure 12—M, X, Y and Z bits of local MAC address

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

4 A local MAC address exists in one of four SLAP quadrants, each identified by a different combination of the
5 Y and Z bits, as indicated in Table 2. That table also indicates the SLAP local identifier type specified for
6 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	<i>Reserved</i>	<i>Reserved</i>	—

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

9 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 bits 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)²¹ 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.

²¹For more information on CIDs, follow the tutorial link from <https://standards.ieee.org/regauth> to locate the appropriate tutorial.

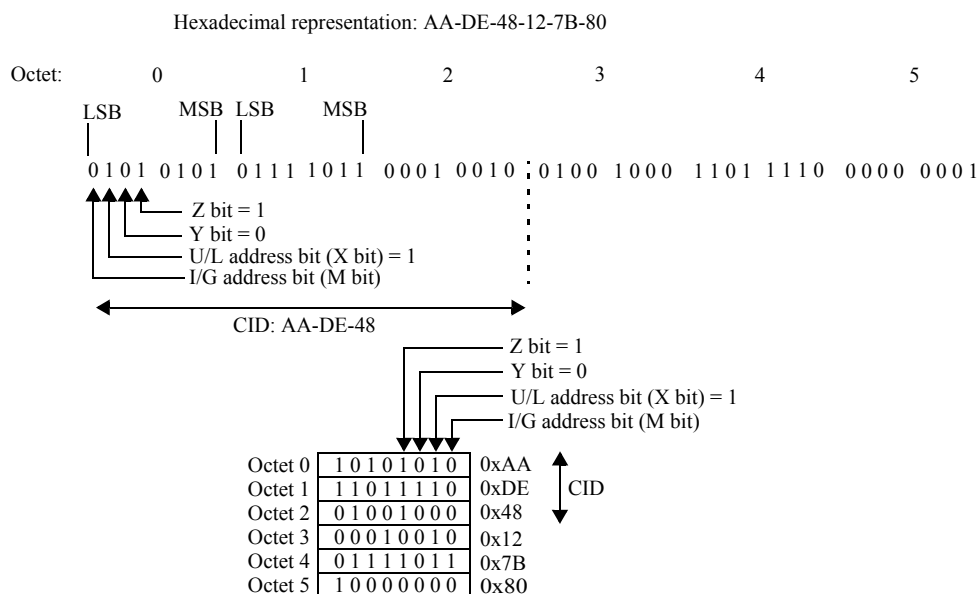


Figure 13—Example ELI-48 created as an extension of CID

Table 4—Administrator CIDs

Administrator CIDs
0x3AA3F8
0xCA30BF
0x4A07D6
0xFA94F1

1 IEEE 802 standards support the use of ELI-48 and ELI-64 based on CID only for CID values that specify
2 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
3 the Z bit.

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

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

1 8.4.4.2 Standard Assigned Identifier (SAI)

2 A SLAP identifier of type “Standard Assigned” is known as a Standard Assigned Identifier (SAI). SAIs are
3 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
4 MAC address; such an address is known as an SAI address. The specification of this quadrant is reserved for
5 a future IEEE 802 standard (see E.3).

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

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

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

15 8.4.4.3 Administratively Assigned Identifier (AAI)

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

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

22 Two different lengths of an AAI are specified: AAI-48 is a 48-bit AAI, and AAI-64 is a 64-bit AAI, as
23 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}

24 Per IETF RFC 2464 [B11], a multicast IPv6 packet uses a Ethernet destination address whose first 2 octets
25 are the value 0x3333. Such addresses lie within the AAI quadrant of the multicast local MAC address space.
26 Therefore, administrators who wish to support IPv6 should not assign AAIs beginning with 0x3333.

27 8.4.4.4 SLAP quadrant “10”

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

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

1 8.4.5 Network Unique Identifier (NUI)

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

5 8.5 Standardized group MAC addresses²²

6 The previous subclauses described the assignment of individual and group MAC addresses and protocol
7 identifiers for public or private use by private organizations. There is also a need for standardized 48-bit and
8 64-bit group MAC addresses to be used with standard protocols. The administration of these standardized
9 48-bit and 64-bit group MAC addresses, including the procedure for application and a list of currently
10 assigned values, is described on the web pages for the IEEE RA²³. Many standardized group MAC
11 addresses used in standards are assigned within a block of universally administered addresses derived from
12 an MA-L that has been assigned by the IEEE 802.1 Working Group for this purpose.

13 8.6 Bit-ordering and different MACs

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

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

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

²²These were previously referred to as standard group MAC addresses.

²³See the “Standard Group MAC addresses” at: <https://standards.ieee.org/products-programs/regauth/tut/>

1 9. Protocol identifiers and context-dependent identifiers

2 9.1 Introduction

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

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

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

12 Various network and higher layer protocols have been assigned reserved LPD addresses or EtherTypes, as
13 recorded by the IEEE RA²⁴. These addresses permit multiple protocols to operate over a single MAC entity.

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

16 The EPD method shall be the primary specified means for protocol identification at the LLC sublayer in
17 IEEE 802 standards developed after January 2011²⁵, excluding amendments to existing standards.

18 9.2 EtherTypes

19 9.2.1 Format, function, and administration

20 EtherType protocol identification values are assigned by the IEEE RA²⁶ and are used to identify the
21 protocol that is to be invoked to process the user data in the frame. An EtherType is a sequence of 2 octets,
22 interpreted as a 16-bit numeric value with the first octet containing the most significant 8 bits and the second
23 octet containing the least significant 8 bits. Values in the 0–1535 range are not available for use.

24 Examples of EtherTypes are 0x08-00 and 0x86-DD, which are used to identify IPv4 and IPv6, respectively.

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

28 9.2.2 Public EtherType assignments subset

29 The IEEE Registration Authority (RA) provides a public listing of EtherType assignments²⁷. Many of these
30 are for private or proprietary purposes. However, others are incorporated into well-known standards. In
31 some cases, the IEEE RA Public Listing for an EtherType identifies an assignee without explicitly

²⁴More information can be found at <https://standards.ieee.org/products-programs/regauth/>.

²⁵IEEE 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.

²⁶More 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>.

²⁷The EtherType public listing is the public view of the EtherType registry managed by the Registration Authority (see <https://standards.ieee.org/regauth/>).

1 identifying the standards in which the use of that EtherType is specified. For ready reference by users and
2 developers of such standards, Annex F identifies some well-known EtherTypes and the protocols they
3 identify. This subset is derived by combining the EtherTypes listed in the ietf-ethertypes YANG module
4 specified in IETF RFC 8519 [B19] with the subset of EtherTypes defined by IEEE 802 Standards (e.g.,
5 IEEE 802.1Q, 802.3, etc.) and as provided by participants that developed this standard. Information on
6 products released after that date can be found on the IEEE SA Registration Authority web site: [https://
7 standards.ieee.org/products-programs/regauth/ethertype/](https://standards.ieee.org/products-programs/regauth/ethertype/) and [https://regauth.standards.ieee.org/standards-
9 ra-web/pub/view.html#registries](https://regauth.standards.ieee.org/standards-
8 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.

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

- 11 — **Assignment** — The hexadecimal representation of the EtherType.
- 12 — **Assignment Type** — The type is EtherType²⁸.
- 13 — **Company Name** — The registrant of the Assignment.
- 14 — **Company Address** — The address of the registrant.
- 15 — **Protocol** — A brief protocol description, as provided by the registrant.

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

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

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

22 9.2.3 EtherTypes for prototype and vendor-specific protocol development

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

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

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

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

33 9.2.4 Local Experimental EtherTypes

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

²⁸EtherType 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.

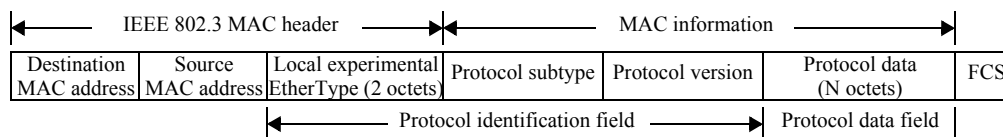


Figure 14—Example of an IEEE 802.3 frame carrying the Local Experimental EtherType

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.

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

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

13 9.2.5 OUI Extended EtherType

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

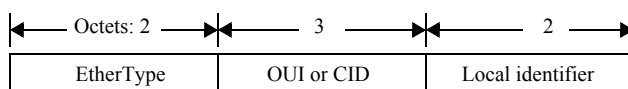


Figure 15—Protocol identifier composed of an OUI or CID

19 The EtherType field shall contain the Vendor Specific EtherType value.

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

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

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

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

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

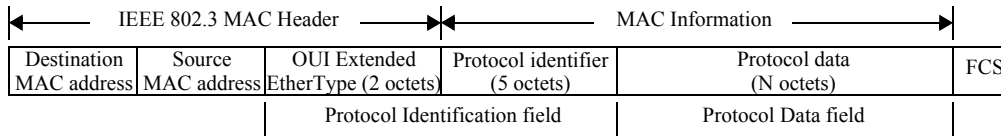


Figure 16—IEEE 802.3 frame with the OUI Extended EtherType encoded in the Length/Type field

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

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

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

11 As the OUI Extended EtherType is a normal EtherType value, it is possible to use the encoding described in
12 9.4 to carry its value within an LPD PDU, using a SNAP identifier with the IETF RFC 1042 [B9] OUI.
13 Figure 17 shows the format of an IEEE 802.3 frame carrying the OUI Extended EtherType encoded in this
14 way. In this case, it would be more appropriate to use the SNAP identifier directly (i.e., omit the RFC 1042
15 OUI and OUI Extended EtherType fields shown in Figure 17); however, this is a valid encoding of the OUI
16 Extended EtherType that can result from the application of the encapsulation described in 9.4.

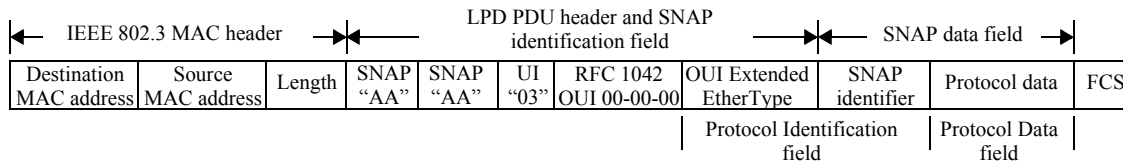


Figure 17—IEEE 802.3 frame with the OUI Extended EtherType encoded in an LPD PDU

17 9.3 OUI, CID and OUI-36 as protocol identifiers

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

21 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
22 Figure 19. All OUI, CID and OUI-36 identifiers assigned by the IEEE RA have the M bit set to zero; values
23 with the M bit set to one are reserved.

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

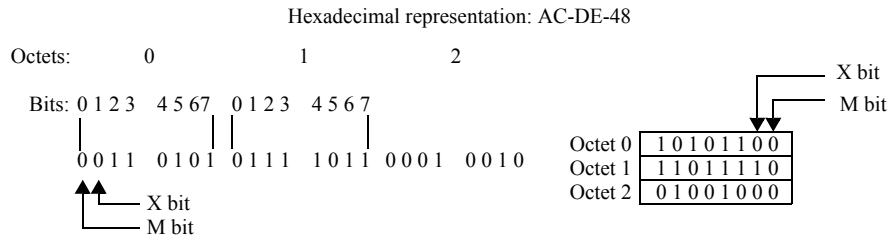


Figure 18—Format of an OUI or CID used as a protocol identifier

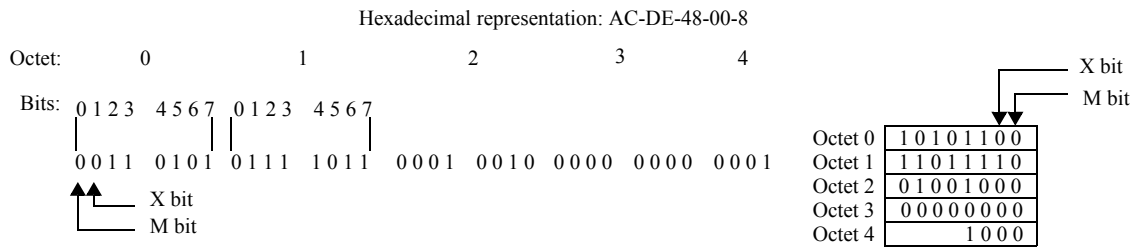


Figure 19—Format of an OUI-36 used as a protocol identifier

9.4 LSAP encoding of EtherType protocol identifier

This subclause specifies the standard method for conveying EtherType protocol identifiers using LSAP encoding.

An EtherType protocol identifier conveyed on an IEEE 802 network using LSAP encoding 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 first three octets each take the value zero.
 - 2) The two remaining octets take the values, in the same order, of the 2 octets of the EtherType.
- b) The Protocol Data field of the SNAP data unit shall contain the user data octets, in order.

NOTE—This method was originally specified in IETF RFC 1042 [B9], which contains recommendations relating to its use. Further recommendations are contained in IETF RFC 1390 [B10].

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.

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

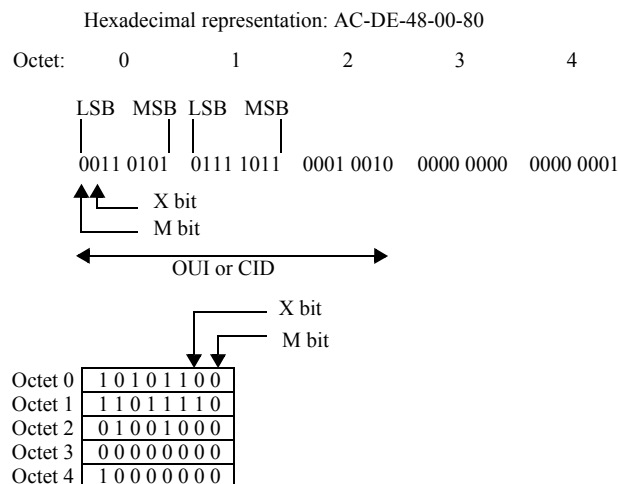


Figure 20—SNAP identifier

1 The LSB of the first octet of a SNAP identifier is referred to as the M bit. All SNAP identifiers derived from
2 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
3 reserved.

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

7 9.5.2 SNAP address

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

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

16 9.5.3 SNAP data unit format

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

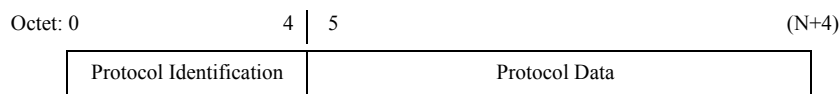


Figure 21—SNAP data unit format

19 In Figure 21, the Protocol Identification field contains a SNAP identifier whose format and administration
20 are as described in 9.5.1. The Protocol Data field is a field whose length, format, and content are specified
21 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.

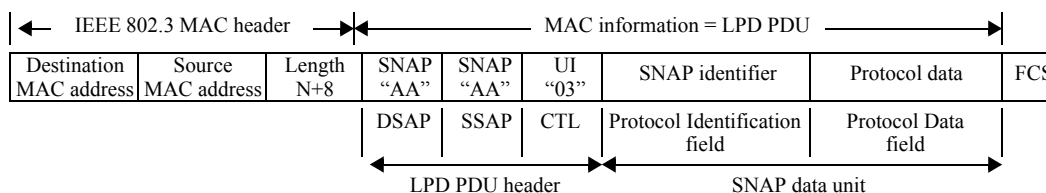


Figure 22—SNAP data unit in IEEE 802.3 MAC frame

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)

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

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

8 **10.3 The OID hierarchy for IEEE 802 standards**

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

10 iso (1) iso-identified-organization (3) iee (111)
11 standards-association-numbered-series-standards (2) iee-802 (802)

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

15 iso (1) iso-identified-organization (3) iee (111)
16 standards-association-numbered-series-standards (2) iee-802 (802) iee802dotX (X)

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

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

21 iso (1) iso-identified-organization (3) iee (111)
22 standards-association-numbered-series-standards (2) iee-802 (802) iee802dot3 (3)

23 and the value used for IEEE 802.11™ standards is:

24 iso (1) iso-identified-organization (3) iee (111)
25 standards-association-numbered-series-standards (2) iee-802 (802) iee802dot11 (11)

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

28 It is the responsibility of each working group to ensure that any values that are allocated to the fifth and
29 subsequent arcs are documented, in a manner that ensures that the same OID value cannot be assigned to
30 two different objects. In the IEEE 802.1 Working Group, this has been achieved in the past by placing tables
31 of OID allocations in an annex within the standard concerned²⁹; in the IEEE 802.3 Working Group, a master
32 spreadsheet of allocated OID values is maintained by the chair and posted on the working group's website.
33 For future allocations, adopting a master spreadsheet approach is appropriate.

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

²⁹More 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 values³⁰. 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 tree³¹.

³⁰There 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.

³¹This 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 [B16] and IETF RFC 7950 [B18], 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}

1 {IEEE standard designation} is the standard designation assigned to the base standard that defines the URN
2 value. For example, in the case of IEEE Std 802.1Q, the standard designation is 802.1Q; in the case of IEEE
3 Std 802.11, the standard designation is 802.11. Where URN values are assigned in amendments or
4 corrigenda to a base standard, the base standard's IEEE standard designation shall be used, not the IEEE
5 standard designation of the amendment or corrigendum. The IEEE standard designation shall not include
6 any colons. The form of standard designation numbers is as specified in the IEEE SA Project Numbering
7 Policy.³²

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

10 yang

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

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

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

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

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

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

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

³²The 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 2016.³³

[B2] IEEE Registration Authority Tutorial, “Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI) and Company ID (CID)”.³⁴

[B3] IEEE Std 802.1AS™-2020, IEEE Standard for Local and metropolitan area networks—Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks.

[B4] IEEE Std 802.1BA™, IEEE Standard for Local and metropolitan area networks—Audio Video Bridging (AVB) Systems.

[B5] IEEE Std 802.1CB™-2017, IEEE Standard for Local and metropolitan area networks—Frame Replication and Elimination for Reliability.

[B6] IEEE Std 802.1CM™, IEEE Standard for Local and metropolitan area networks—Time-Sensitive Networking for Fronthaul.

[B7] IEEE Std 802.1CS™-2020, IEEE Standard for Local and metropolitan area networks—Link-local Registration Protocol.

[B8] IEEE Std 802.3™-2022, IEEE Standard for Ethernet.

[B9] IETF RFC 1042, A Standard for the Transmission of IP Datagrams over IEEE 802 Networks. Postel, J., and J. Reynolds, Feb. 1988.³⁵

[B10] IETF RFC 1390, Transmission of IP and ARP over FDDI Networks. Katz, D., Jan. 1993.

[B11] IETF RFC 2464, Transmission of IPv6 Packets over Ethernet Networks.

[B12] IETF RFC 2579, STD 58, Textual Conventions for SMIV2. McCloghrie, K., D. Perkins, J. Schoenwaelder, J. Case, M. Rose, and S. Waldbusser, Apr. 1999.

[B13] IETF RFC 2580, STD 58, Conformance Statements for SMIV2. McCloghrie, K., D. Perkins, J. Schoenwaelder, J. Case, M. Rose, and S. Waldbusser, Apr. 1999.

[B14] IETF RFC 3411, STD 62, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.

³³IEEE publications are available from The Institute of Electrical and Electronics Engineers (<https://standards.ieee.org/>)

³⁴The tutorial is available at <https://standards.ieee.org/regauth>. Follow the tutorial link and search for the tutorial title.

³⁵ETF documents (i.e., RFCs) are available the Internet Engineering Task Force (<https://www.rfc-archive.org/>).

¹ [B15] IETF RFC 5677, IEEE 802.21 Mobility Services Framework Design (MSFD). Melia, T., G. Bajko,
² S. Das, N. Golmie, and J. C. Zuniga, Dec. 2009.

³ [B16] IETF RFC 6020, YANG—A Data Modeling Language for the Network Configuration Protocol
⁴ (NETCONF), October 2010.

⁵ [B17] IETF RFC 6241, Network Configuration Protocol (NETCONF), June 2011.

⁶ [B18] IETF RFC 7950, The YANG 1.1 Data Modeling Language, August 2016.

⁷ [B19] IETF RFC 8519, YANG Data Model for Network Access Control Lists (ACLs), March 2019.

⁸ [B20] IISO/IEC 7498-1:1994, Information technology—Open Systems Interconnection—Basic Reference
⁹ Model: The Basic Model.

1 **Annex B**

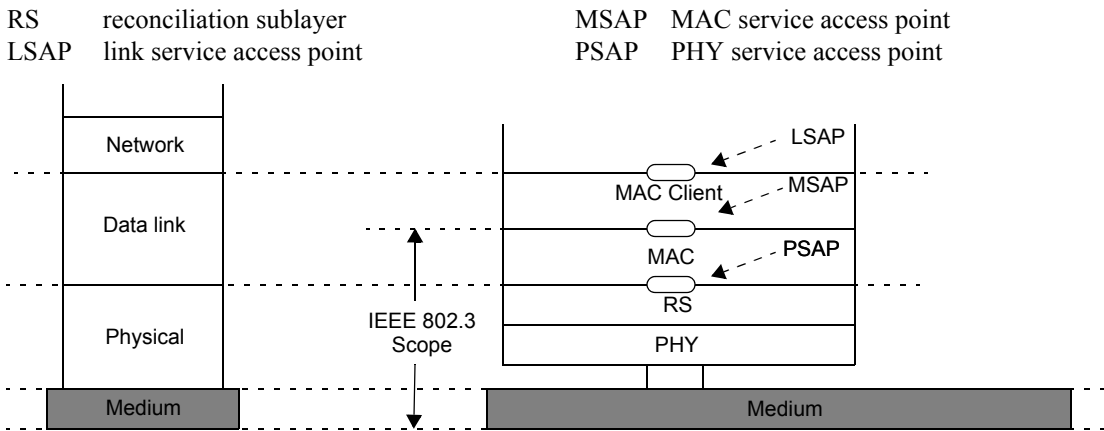
2 (informative)

3 **RM for IEEE 802 standards**

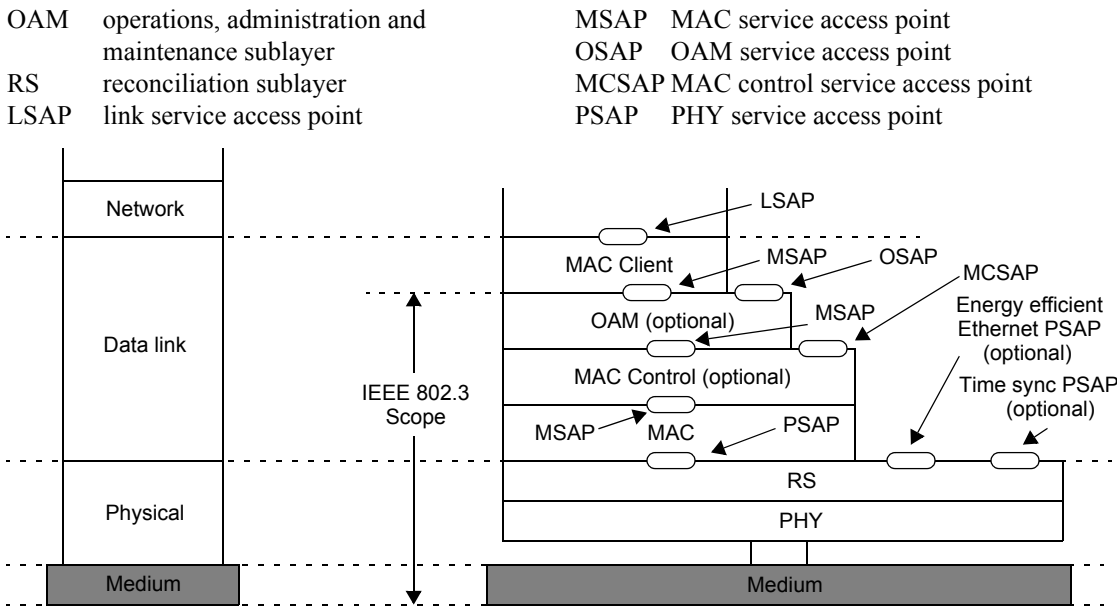
4 **B.1 IEEE 802.3 RMs**

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

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



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



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

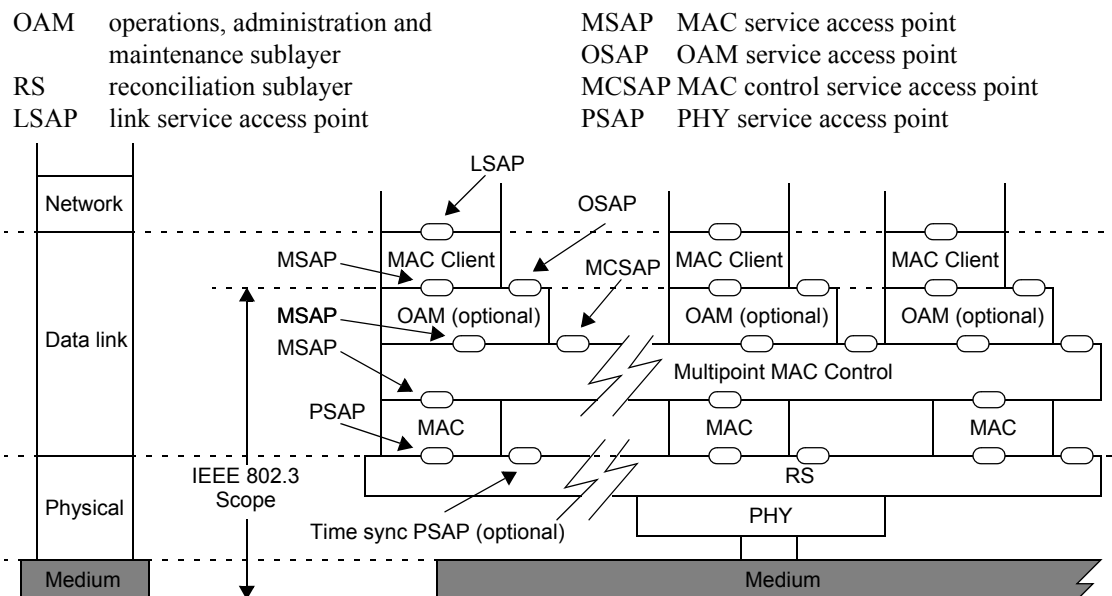


Figure B.3—IEEE 802.3 RM for point-to-multipoint OLT

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

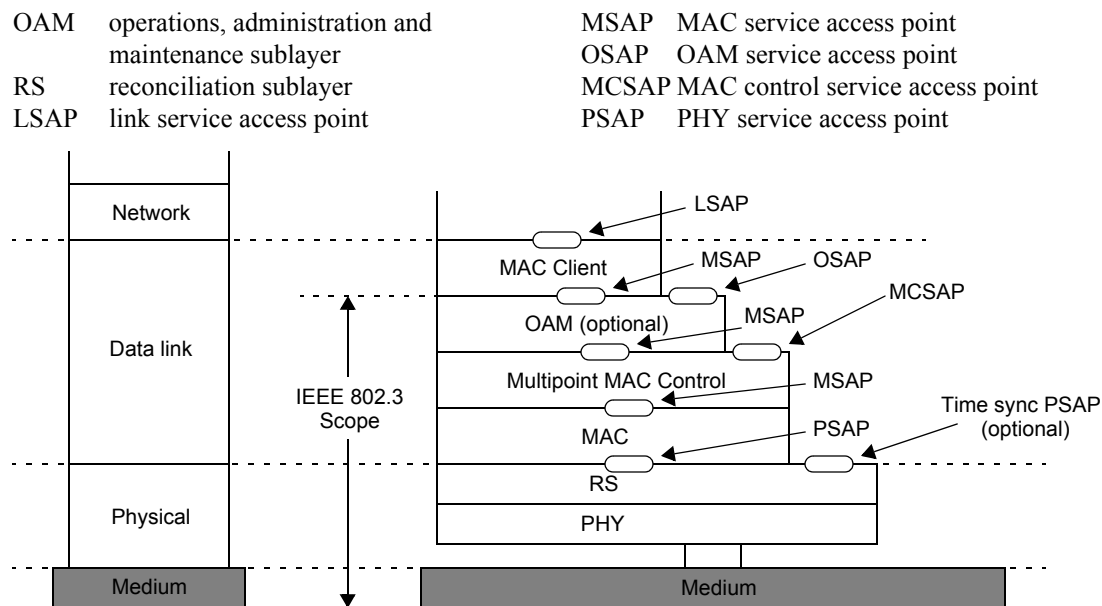


Figure B.4—The RM for IEEE 802.3 point-to-multipoint ONU

4 IEEE Std 802.3 was amended in 2004 to introduce the concept of subscriber access network.³⁶ The purpose
5 of Ethernet in the first mile (EFM), as well as its distinction from traditional Ethernet networks, is that it
6 specifies functionality required for the subscriber access network, i.e., public network access. Network

³⁶The amendment was IEEE Std 802.3ah™-2004, which is now part of the current IEE Std 802.3.

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

3 **B.2 IEEE 802.11 RM**

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

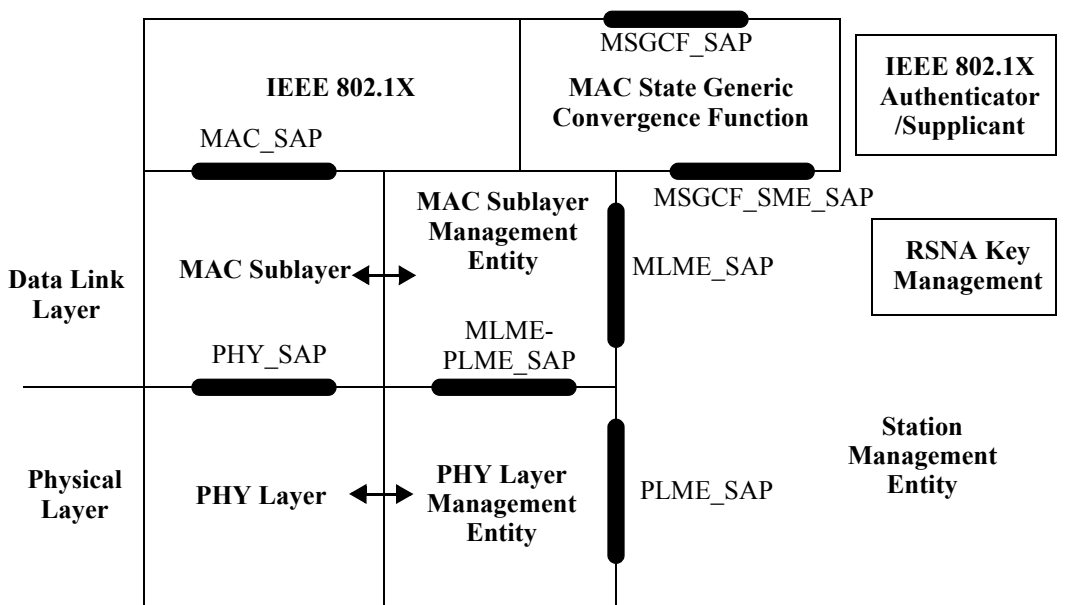


Figure B.5—IEEE 802.11 STA RM

5 The interconnections between IEEE 802.11 STAs follow four general connection models.

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

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

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

20 The third interconnection model, is a mesh model consisting of autonomous STAs. Inside the mesh, STAs
21 establish peer-to-peer wireless links with neighbor STAs to mutually exchange messages. Further, using the
22 mesh's multi-hop capability, messages can be transferred between STAs that are not in direct
23 communication with each other over a single instance of the wireless medium. From the data delivery point

1 of view, it appears as if all STAs in a mesh are directly connected at the MAC layer even if the STAs are not
2 within range of each other. A mesh might have an interface to the distribution system, through a Mesh Gate,
3 and thereby can enable communication to non-AP STAs in infrastructure access domains, and/or via a portal
4 to non-IEEE 802.11 networks.

5 The fourth interconnection model, is the general link (GLK) model consisting of GLK STAs connected by
6 IEEE 802.11 general links that are suitable to be used as links inside an IEEE 802.1Q bridged network. A
7 GLK STA coordinates with a GLK convergence function to provide an instance of Internal Sublayer
8 Service, as defined in IEEE Std 802.1AC-2016, to an IEEE 802.1Q bridge for each peer GLK STA with
9 which it is communicating. GLK STAs also provide link metrics for the use of external path selection
10 protocols such as spanning tree protocol. GLK operation does not involve a DS. Instead, the general links
11 formed with GLK operation are a point-to-point connection between pairs of instances of Internal Sublayer
12 Service SAPs.

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

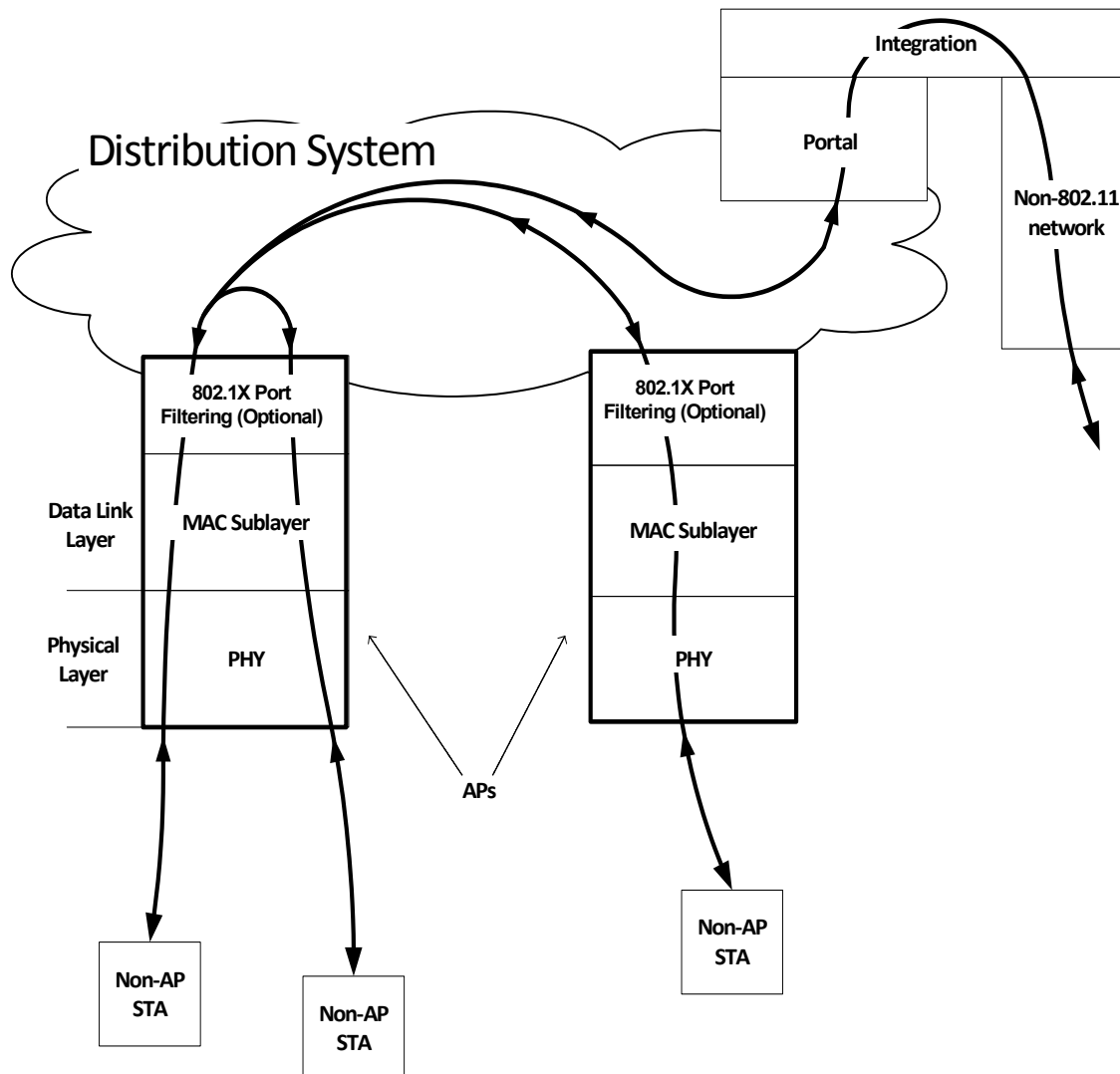


Figure B.6—IEEE 802.11 infrastructure model

Figure B.7 illustrates the infrastructure model for GLK APs and GLK non-APs STA s, the general links shown connect the IEEE 802.1Q MAC relay entities shown with each other or the LLC sublayer of the end stations shown.

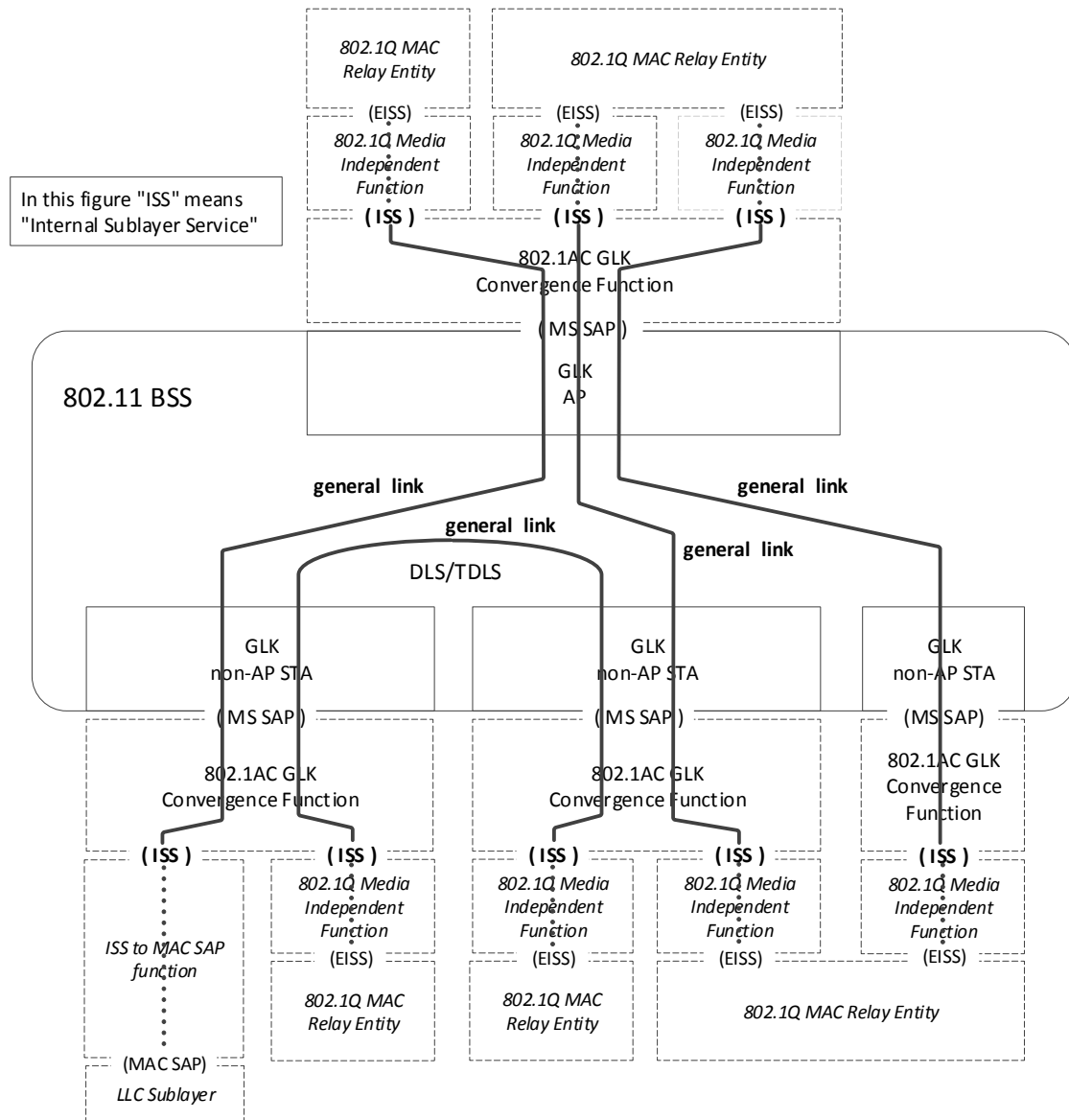


Figure B.7—Example of infrastructure BSS with general links

4 B.3 IEEE 802.15™ RMs

5 B.3.1 IEEE 802.15.3™ RM

⁶ The RM for IEEE Std 802.15.3 is illustrated in Figure B.8.

7 The PHY SAP and physical layer management entity (PLME) SAP are not specified in IEEE Std 802.15.3
8 as they are rarely, if ever, exposed in a typical implementation. The PHY management objects and attributes

1 are accessed through the MAC sublayer management entity (MLME) SAP with the generic management
2 primitives used to access the MAC management objects and attributes.

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

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

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

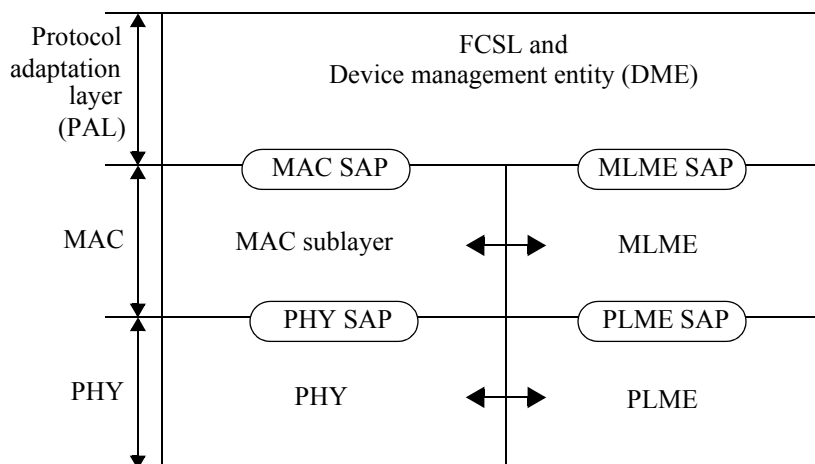


Figure B.8—IEEE 802.15.3 RM

1 B.3.2 IEEE 802.15.4™ RM

2 The RM for IEEE Std 802.15.4 is illustrated in Figure B.9.

3 The upper layers shown in Figure B.9 consist of a network layer (which provides network configuration,
4 manipulation, and message routing) and an application layer (which provides the intended function of the
5 device). The upper layers are not specified in IEEE Std 802.15.4.

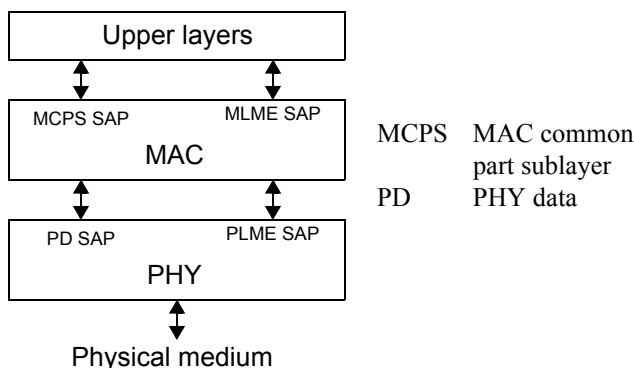


Figure B.9—IEEE 802.15.4 RM

6 B.3.3 IEEE 802.15.6™ RM

7 The RM for IEEE 802.15.6 hub or node are shown in Figure B.10.

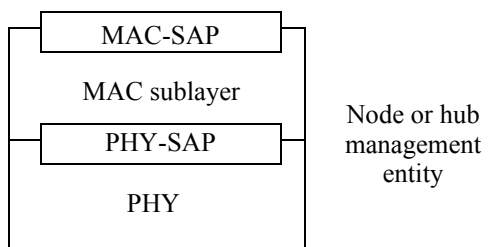


Figure B.10—IEEE 802.15.6 RM

8 B.3.4 IEEE 802.15.7™ RM

9 The RM for IEEE Std 802.15.7™ is shown in Figure B.11.

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

- 11 — The MAC data service, accessed through the MAC common part sublayer (MCPS) data SAP (MCPS-SAP)
- 12
- 13 — The MAC management service, accessed through the MLME-SAP

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

16 The PHY provides two services, accessed through two SAPs:

- 17 — The PHY data service, accessed through the PHY data SAP (PD-SAP)
- 18 — The PHY management service, accessed through the PLME's SAP (PLME-SAP).

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

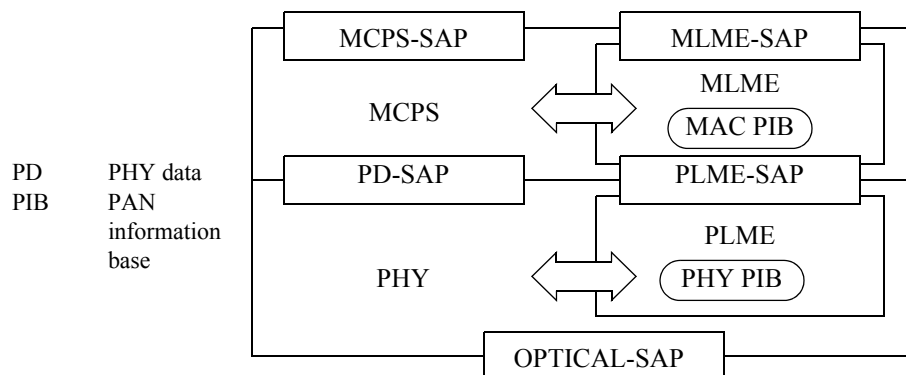


Figure B.11—IEEE 802.15.7 RM

3 **B.4 IEEE 802.16™ RM**

4 **B.4.1 Protocol RM**

5 Figure B.12 illustrates the protocol RM for IEEE Std 802.16.

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

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

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

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

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

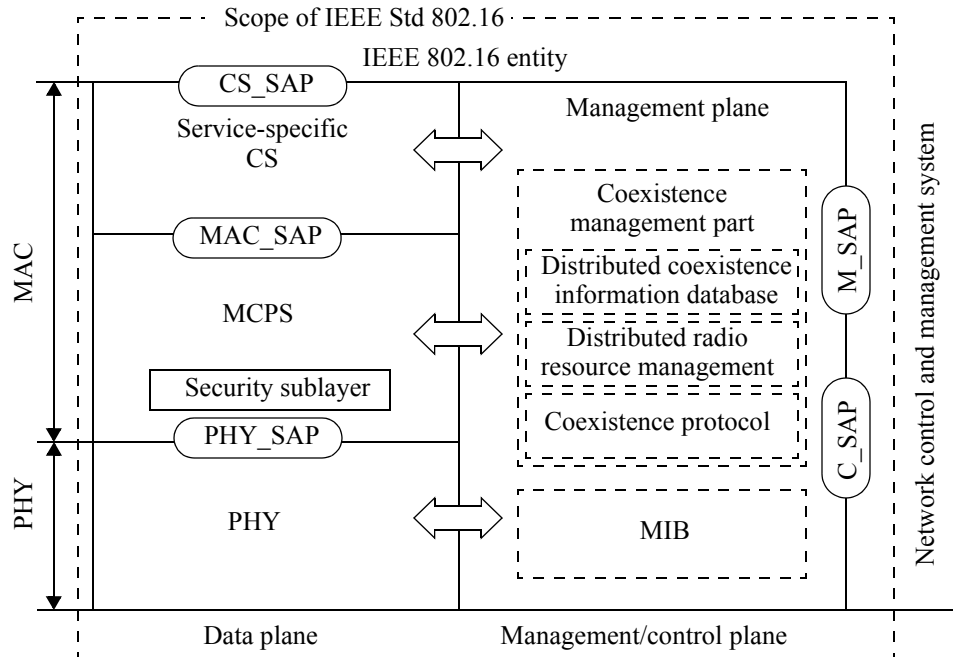


Figure B.12—IEEE 802.16 protocol RM

1 B.4.2 Network RM

² Figure B.13 describes a simplified network RM for IEEE Std 802.16.

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

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

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

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

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

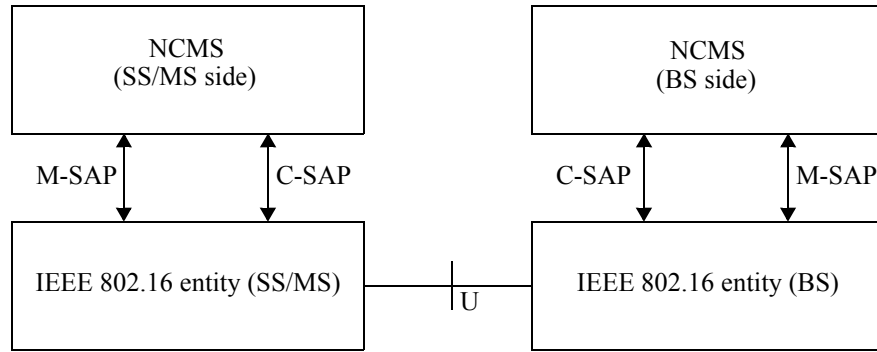


Figure B.13—IEEE 802.16 network RM

1 B.5 IEEE 802.21™ RM

2 Figure B.14 shows an implementation view of a dual-mode IEEE 802.11/IEEE 802.16 station with
3 IEEE 802.21 MIH functionality. The MIHF provides the required services to perform handovers between
4 IEEE 802.11 and IEEE 802.16 access technologies. Also, the MIHF becomes a higher layer when it requires
5 data transport services to communicate with an IEEE 802.21 MIH peer. For layer 2 transport of MIH data,
6 services are provided by the IEEE 802.16 CS_SAP or the IEEE 802.11 LSAP. For layer 3 transport, services
7 are provided as described in IETF RFC 5677 [B15].

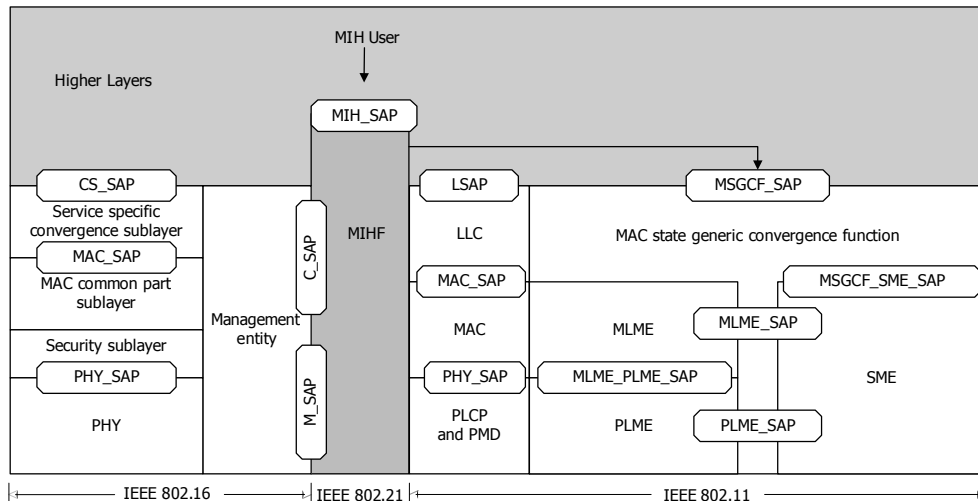


Figure B.14—Example of dual-mode IEEE 802.11 and IEEE 802.16 end station with IEEE 802.21 end-station RM

1 B.6 IEEE 802.22™ RM

2 The RM of IEEE Std 802.22 is depicted in Figure B.15. A unique characteristic of this architecture is its
3 cognitive components, which are used to allow for dynamic frequency selection and avoid interference to
4 incumbents on a real-time basis.

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

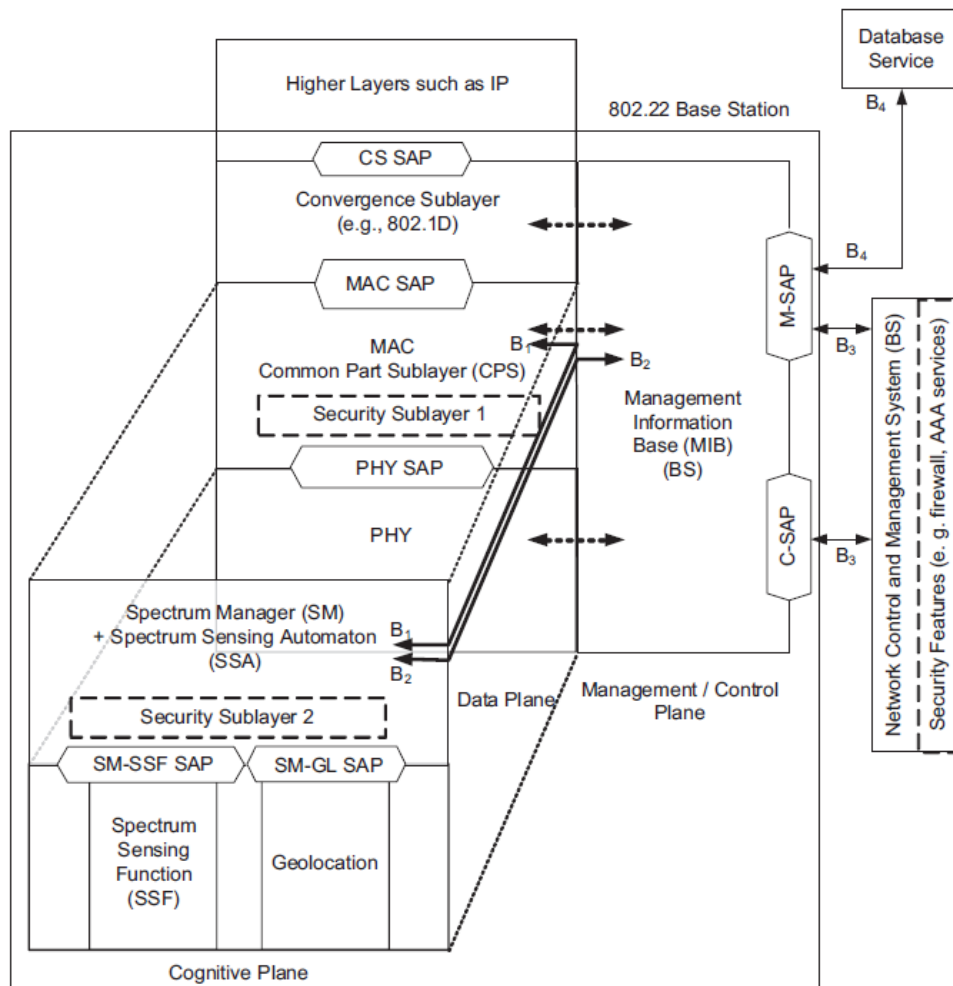


Figure B.15—IEEE 802.22 RM for the BS and CPE

1 **B.6.1 Data plane**

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

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

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

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

11 **B.6.2 Management/control plane**

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

15 **B.6.3 Cognitive plane**

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

26 The spectrum sensing automaton (SSA) is present at the BS and at the CPEs and independently implements
27 specific procedures for sensing the RF environment at initialization of the BS and before the registration of a
28 CPE with the BS. The SSA at the CPE also includes features to allow proper operation when the CPE is not
29 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
30 the BS is also active when the BS is not transmitting to conduct out-of-band sensing. The SSA located at the
31 BS can also carry out sensing to clear channels when the BS is not transmitting.

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

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

1 Annex C

2 (informative)

3 Examples of bit ordering for addresses

4 C.1 General

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

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

13 C.2 Illustrative examples

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

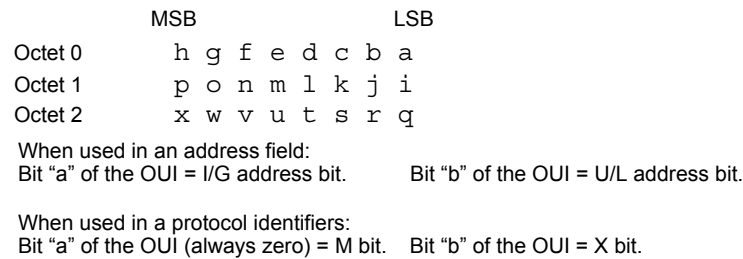


Figure C.1—Bit significance of an OUI

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

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

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

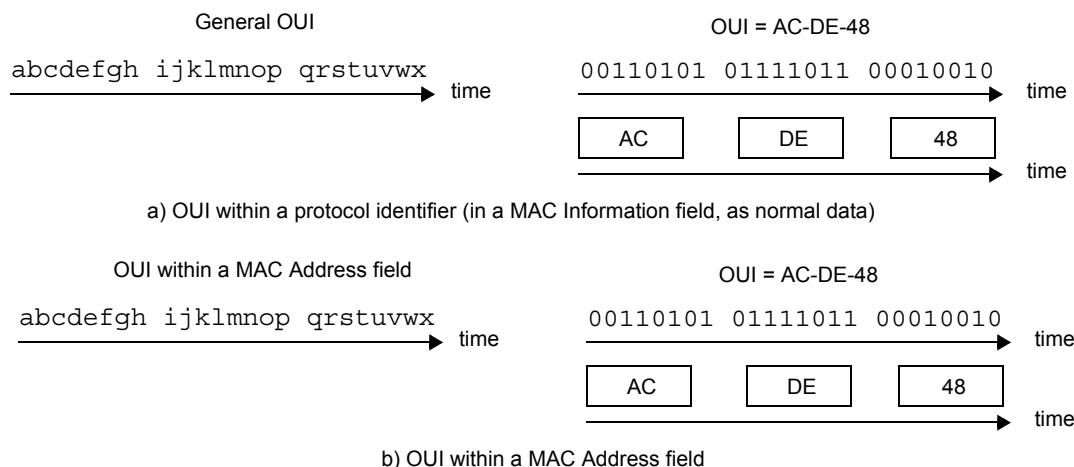


Figure C.2—Order of bit and octet transmission for an OUI with LSB transmitted first

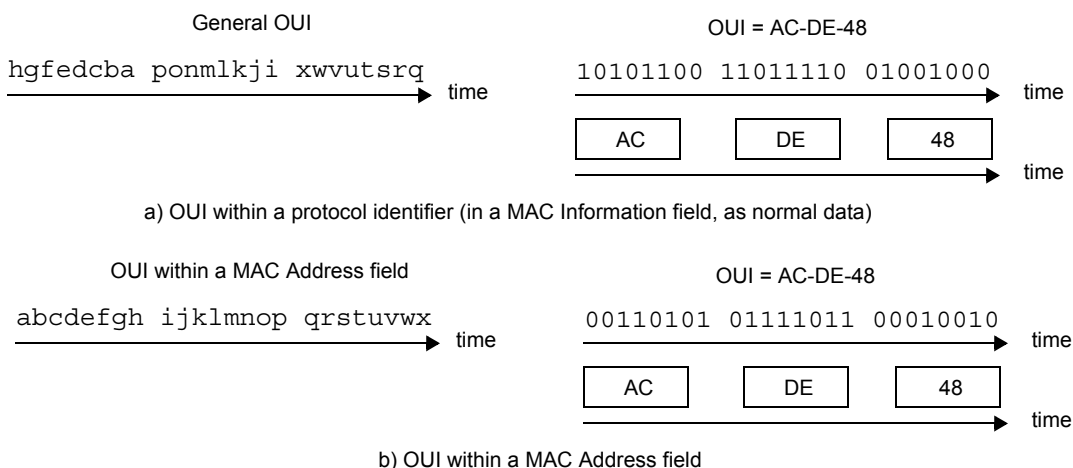


Figure C.3—Order of bit and octet transmission for an OUI with MSB transmitted first

¹ For network types in which Figure C.3 applies, there appears to be a choice of representations for EUI-48s
² conveyed as data, as follows:

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

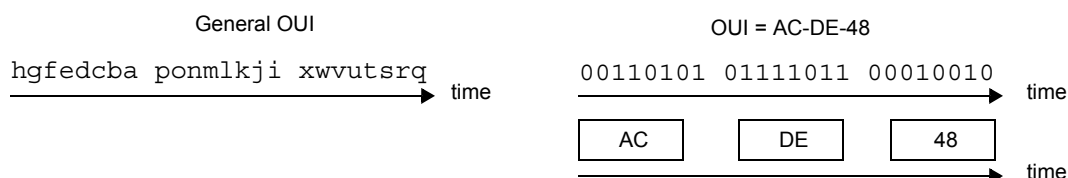


Figure C.4—Order of bit and octet transmission for an OUI in an EUI-48 with MSB transmitted first, canonical format.

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

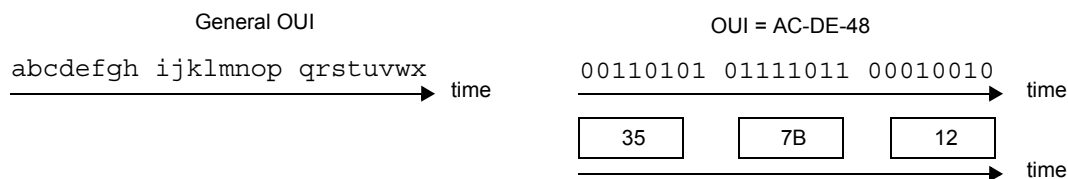


Figure C.5—Order of bit and octet transmission for an OUI in an EUI-48 with MSB transmitted first, noncanonical format.

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

8 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
9 octet values is consistent. This reversal of the bit order applies only to all 6 octets (not just the OUI) of an
10 EUI-48 placed in the MAC Information field of a frame by a protocol that uses the bit-reversed view of the
11 EUI-48s derived from Figure C.3(b). Frames containing, or possibly containing, such EUI-48s are described
12 as having noncanonical format. Frames that cannot contain such EUI-48s are described as having canonical
13 format.

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

1 Annex D

2 (informative)

3 List of IEEE 802 standards

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

6 IEEE Std 802.1AB™, IEEE Standard for Local and metropolitan area networks—Station and Medium
7 Access Control Connectivity Discovery.^{37, 38}

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

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

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

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

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

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

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

20 IEEE Std 802.1CB™, IEEE Standard for Local and metropolitan area networks—Frame Replication and
21 Elimination for Reliability.

22 IEEE Std 802.1CF™, IEEE Recommended Practice for Network Reference Model and Functional
23 Description of IEEE 802® Access Network

24 IEEE Std 802.1CM™, IEEE Standard for Local and metropolitan area networks—Time-Sensitive
25 Networking for Fronthaul.

26 IEEE Std 802.1CS™, IEEE Standard for Local and metropolitan area networks—Link-local Registration
27 Protocol.

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

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

³⁷The IEEE standards and products referred to in Annex D are trademarks owned by The Institute of Electrical and Electronics Engineers, Incorporated.

³⁸IEEE publications are available from The Institute of Electrical and Electronics Engineers (<https://standards.ieee.org/>).

1 IEEE Std 802.3™, IEEE Standard for Ethernet.

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

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

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

7 IEEE Std 802.15.3™, IEEE Standard for Information technology—Telecommunications and information
8 exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.3:
9 Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless
10 Personal Area Networks (WPANs).

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

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

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

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

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

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

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

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

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

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

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

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

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

1 Annex E

2 (informative)

3 History

4 E.1 Universal addresses

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

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

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

24 E.2 IEEE RA address block products

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

30 In addition, the IEEE RA looked for ways to make the original OUI space last longer. Many times, a
31 company or organization would be allocated an OUI, but would not use a significant portion of the 2^{24}
32 (16 777 216) EUI-48 addresses or 2^{40} (1 099 511 627 776) EUI-64 addresses available in the address block.
33 The addresses would be “lost”, never being assigned. To avoid this situation, the IEEE RA created the OUI-
34 36, which could be used as an identifier as well as for creating universal addresses (up to 4096 EUI-48s or
35 268 435 456 EUI-64s).

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

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

5 **E.3 Local MAC addresses**

6 Local addresses were included in the initial series of IEEE 802 standards (published in 1985). IEEE Std
7 802.5-1985 included an annex for hierarchical addressing (dividing an address into a ring number and a
8 node number both being locally administered). Pre-standard Ethernet did not include local addresses. A few
9 Block IDs assigned by Xerox Corporation prior to the definition of local addresses (circa 1981) had the X bit
10 equal to one. The vendors assigned such Block IDs participated in remediation of problems created by the
11 definition of local addresses for all IEEE 802 networks.

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

21 The IEEE RA opened its CID registry on 1 January 2014. Later that year, the IEEE introduced an expanded
22 version of its tutorial “Guidelines for use of the 24-bit Organizationally Unique Identifiers (OUI)” as
23 “Guidelines for Use Organizationally Unique Identifier (OUI) and Company ID (CID)”³⁹, including
24 explanatory material regarding CIDs. Using language similar to that of IEEE Std 802-2014, the tutorial also
25 suggested the possibility of building a local MAC address from a CID.

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

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

32

³⁹The tutorial has been updated again to include EUIs, [B2]

1 Annex F

2 (informative)

3 EtherType Listing Subset

4 F.1 Introduction

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

8 F.2 Tabular format

9 A subset of EtherType assignments by the IEEE RA is given in Table F.1. Each Friendly Name in Table F.1
10 is unique and is used as an identifier in the YANG module. The Short Description identifies the protocol,
11 protocol message, or protocol field that uses the assignment as specified in the Reference, or the EtherType
12 assignment itself as named in the Reference. Where the Reference specifies more than one name or use
13 (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	misp	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)	Internetwork Packet Exchange - Novell, Inc.
82-04	qnx	QNX Qnet	QNX - Quantum Software Systems, Ltd.
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	INT51X1 datasheet
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

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

EtherType Assignment (HEX)	Friendly Name	Short Description	Reference
88-A8	s-tag	Service VLAN Tag (S-TAG) or Backbone VLAN Tag (B-TAG)	IEEE Std 802.1Q
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	Link Layer Discovery Protocol (LLDP)	IEEE Std 802.1AB
88-CD	sercos	Sercos Interface	IEC 61158-4-19
88-DC	wsmpp	WAVE Short Message Protocol (WSMP)	IEEE Std 1609
88-E1	homeplug-av-mme	HomePlug AV Mobile Management Entity (MME)	HomePlug AV Specification
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	T11 FC-BB-5

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	drp	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.

1 F.3 YANG module for EtherType subset

2 F.3.1 YANG Framework

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

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

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

1 F.3.2 Definition for ieee802-ethertype YANG module^{40,41}

```
2 module ieee802-ethertype {
3
4   namespace "urn:ieee:std:802.1Q:yang:ieee802-ethertype";
5   prefix "ieee-ethertype";
6
7   organization
8     "IEEE 802.1 Working Group";
9
10  contact
11    "WG-URL: http://ieee802.org/1/
12    WG-EMail: stds-802-1@ieee.org
13
14    Contact: IEEE 802.1 Working Group Chair
15    Postal: C/O IEEE 802.1 Working Group
16            IEEE Standards Association
17            445 Hoes Lane
18            Piscataway
19            NJ 08854
20            USA
21
22    E-mail: stds-802-1-chairs@ieee.org";
23
24  description
25    "This module contains a subset of commonly used 802 network Ether-
26 Types.
27
28    Copyright (C) IEEE (2023).
29
30    This version of this YANG module is part of the IEEE Std 802;
31    see the standard itself for full legal notices.";
32
33  revision "2023-04-17" {
34    description
35      "Initial revision.";
36    reference
37      "IEEE Std 802f, Overview and Architecture -
38      YANG Data Model for EtherTypes";
39  }
40
41  typedef ethertype {
42    type enumeration {
43      enum ipv4 {
44        value 2048;
45        description
46          "08-00 Internet Protocol version 4 (IPv4)";
47        reference
48          "Organization: Xerox, US
```

⁴⁰Copyright 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.

⁴¹An 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/>.

```
1      Reference: IETF RFC 894";
2  }
3  enum arp {
4      value 2054;
5      description
6          "08-06 Address Resolution Protocol (ARP)";
7      reference
8          "Organization: Symbolics, Inc.
9      Reference: IETF RFC 826, IETF RFC 7042";
10 }
11 enum wol {
12     value 2114;
13     description
14         "08-42 Wake-on-LAN";
15     reference
16         "Organization: None
17     Reference: IEEE Std 802";
18 }
19 enum msp {
20     value 8930;
21     description
22         "22-E2 MAC Status Protocol (MSP)";
23     reference
24         "Organization: IEEE 802.1 Working Group
25     Reference: IEEE Std 802.1Q";
26 }
27 enum cnm {
28     value 8935;
29     description
30         "22-E7 Congestion Notification Message (CNM)";
31     reference
32         "Organization: IEEE 802.1 Working Group
33     Reference: IEEE Std 802.1Q";
34 }
35 enum cn-tag {
36     value 8937;
37     description
38         "22-E9 Congestion Notification Tag (CN-TAG)";
39     reference
40         "Organization: IEEE 802.1 Working Group
41     Reference: IEEE Std 802.1Q";
42 }
43 enum msrp {
44     value 8938;
45     description
46         "22-EA Multiple Stream Reservation Protocol (MSRP)";
47     reference
48         "Organization: IEEE 802.1 Working Group
49     Reference: IEEE Std 802.1Q";
50 }
51 enum trill {
52     value 8947;
53     description
54         "22-F3 Transparent Interconnection of Lots of Links";
```

```
1      reference
2      "Organization: IETF TRILL Working Group
3      Reference: IETF RFC 6325";
4  }
5  enum decnet {
6      value 24579;
7      description
8      "60-03 DECnet DNA Routing";
9      reference
10     "Organization: DEC
11     Reference: DECnet DIGITAL Network Architecture - Ethernet
12     Data Link Architectural Specification v1.0.0";
13 }
14 enum rarp {
15     value 32821;
16     description
17     "80-35 Reverse Address Resolution Protocol";
18     reference
19     "Organization: Private
20     Reference: IETF RFC 903";
21 }
22 enum appletalk {
23     value 32923;
24     description
25     "80-9B Appletalk (Ethertalk)";
26     reference
27     "Organization: Private
28     jReference: Inside Appletalk, Second Edition";
29 }
30 enum aarp {
31     value 33011;
32     description
33     "80-F3 Appletalk Address Resolution Protocol";
34     reference
35     "Organization: Private
36     Reference: Inside Appletalk, Second Edition";
37 }
38 enum c-tag {
39     value 33024;
40     description
41     "81-00 Customer VLAN Tag (C-TAG)";
42     reference
43     "Organization: IEEE 802.1 Working Group
44     Reference: IEEE Std 802.1Q";
45 }
46 enum ipx {
47     value 33079;
48     description
49     "81-37 Internetwork Packet Exchange (IPX)";
50     reference
51     "Organization: Novell, Inc.
52     Reference: Internetwork Packet Exchange - Novell, Inc.";
53 }
54 enum qnx {
```

```
1      value 33284;
2      description
3          "82-04 QNX Qnet";
4      reference
5          "Organization: Quantum Software Systems, Ltd.
6          Reference: QNX - Quantum Software Systems, Ltd.";
7  }
8  enum ipv6 {
9      value 34525;
10     description
11         "86-DD Internet Protocol Version 6 (IPv6)";
12     reference
13         "Organization: USC/ISI
14         Reference: IETF RFC 2464";
15 }
16 enum efc {
17     value 34824;
18     description
19         "88-08 Multipoint Control Protocol (MPCP)";
20     reference
21         "Organization: IEEE 802.3 Working Group
22         Reference: IEEE Std 802.3";
23 }
24 enum esp {
25     value 34825;
26     description
27         "88-09 Ethernet Slow Protocol";
28     reference
29         "Organization: IEEE 802.3 Working Group
30         Reference: IEEE Std 802.3";
31 }
32 enum cobranet {
33     value 34841;
34     description
35         "88-19 CobraNet";
36     reference
37         "Organization: Peak Audio
38         Reference: CobraNet Programmer's Reference, Version 2.5";
39 }
40 enum mpls-unicast {
41     value 34887;
42     description
43         "88-47 Multiprotocol Label Switching (MPLS) unicast
44         traffic";
45     reference
46         "Organization: Cisco Systems
47         Reference: IETF RFC 3031";
48 }
49 enum mpls-multicast {
50     value 34888;
51     description
52         "88-48 Multiprotocol Label Switching (MPLS) multicast";
53     reference
54         "Organization: Cisco Systems
```

```
1      Reference: IETF RFC 3031";
2  }
3  enum pppoe-discovery {
4      value 34915;
5      description
6          "88-63 Point-to-Point Protocol over Ethernet (PPPoE)
7          Discovery Stage";
8      reference
9          "Organization: UUNET Technologies, Inc.
10         Reference: IETF RFC 2516";
11  }
12  enum pppoe-session {
13      value 34916;
14      description
15          "88-64 Point-to-Point Protocol over Ethernet (PPPoE)
16          Session Stage";
17      reference
18          "Organization: UUNET Technologies, Inc.
19         Reference: IETF RFC 2516";
20  }
21  enum intel-ans {
22      value 34925;
23      description
24          "88-6D Intel Advanced Networking Services Probe Packets";
25      reference
26          "Organization: Intel Corporation
27         Reference: Intel® Advanced Network Services (Intel® ANS)
28  }
29  enum llc-encaps {
30      value 34928;
31      description
32          "88-70 LLC Encapsulation";
33      reference
34          "Organization: IEEE 802.1 Working Group
35         Reference: IEEE Std 802.1AC";
36  }
37  enum homeplug {
38      value 34939;
39      description
40          "88-7B Homeplug";
41      reference
42          "Organization: Intellon Corporation
43         Reference: INT51X1 datasheet";
44  }
45  enum eapol {
46      value 34958;
47      description
48          "88-8E Port Access Entity (PAE) EtherType, Extensible
49          Authentication Protocol over LANs (EAPOL)";
50      reference
51          "Organization: IEEE 802.1 Working Group
52         Reference: IEEE Std 802.1X";
53  }
54  enum profinet {
```

```
1      value 34962;
2      description
3          "88-92 PROFINET";
4      reference
5          "Organization: PROFIBUS International
6          Reference: IEC 61158-6-10";
7  }
8  enum hyperscsi {
9      value 34970;
10     description
11         "88-9A Small Computer System Interface (SCSI) over
12         Ethernet.";
13     reference
14         "Organization: Data Storage Institute
15         Reference: An Ethernet Based Data Storage Protocol for Home
16         Network";
17 }
18 enum aoe {
19     value 34978;
20     description
21         "88-A2 Advanced Technology Attachment (ATA) over Ethernet.";
22     reference
23         "Organization: Coraid Inc
24         Reference: AoE (ATA over Ethernet)";
25 }
26 enum ethercat {
27     value 34980;
28     description
29         "88-A4 Ethernet for Control Automation Technology
30         (EtherCAT)";
31     reference
32         "Organization: Beckhoff Automation GmbH & Co KG
33         Reference: IEC 61158-4-12";
34 }
35 enum s-tag {
36     value 34984;
37     description
38         "88-A8 Service VLAN Tag (S-TAG) or Backbone VLAN Tag
39         (B-TAG)";
40     reference
41         "Organization: IEEE 802.1 Working Group
42         Reference: IEEE Std 802.1Q";
43 }
44 enum ethernet-powerlink {
45     value 34987;
46     description
47         "88-AB Ethernet Powerlink";
48     reference
49         "Organization: Ethernet Powerlink Standardization Group
50         (EPSG)
51         Reference: IEC 61158-4-13";
52 }
53 enum exp1 {
54     value 34997;
```

```
1      description
2      "88-B5 Local experimental EtherType 1";
3      reference
4      "Organization: IEEE 802.1 Working Group
5      Reference: IEEE Std 802";
6  }
7  enum exp2 {
8      value 34998;
9      description
10     "88-B6 Local experimental EtherType 2";
11     reference
12     "Organization: IEEE 802.1 Working Group
13     Reference: IEEE Std 802";
14 }
15 enum oui-ext {
16     value 34999;
17     description
18     "88-B7 OUI Extended EtherType";
19     reference
20     "Organization: IEEE 802.1 Working Group
21     Reference: IEEE Std 802";
22 }
23 enum goose {
24     value 35000;
25     description
26     "88-B8 IEC 61850 Generic Object Oriented Substation Event
27     (GOOSE)";
28     reference
29     "Organization: IEC TC57
30     Reference: IEC 61850-8-1";
31 }
32 enum gse {
33     value 35001;
34     description
35     "88-B9 IEC 61850 Generic Substation Events (GSE) management
36     services";
37     reference
38     "Organization: IEC TC57
39     Reference: IEC 61850-8-1";
40 }
41 enum sv {
42     value 35002;
43     description
44     "88-BA IEC 61850 Sampled Value Transmission (SV)";
45     reference
46     "Organization: IEC TC57
47     Reference: IEC 61850-8-2";
48 }
49 enum pre-auth {
50     value 35015;
51     description
52     "88-C7 RSNA Pre-Authentication";
53     reference
54     "Organization: IEEE 802.11 Working Group
```



```
1      Reference: IEEE Std 802.11";
2  }
3  enum lldp {
4      value 35020;
5      description
6          "88-CC Link Layer Discovery Protocol (LLDP)";
7      reference
8          "Organization: IEEE 802.1 Working Group
9      Reference: IEEE Std 802.1AB";
10 }
11 enum sercos {
12     value 35021;
13     description
14         "88-CD Sercos Interface";
15     reference
16         "Organization: sercos international e.V.
17     Reference: IEC 61158-4-19";
18 }
19 enum wsmpp {
20     value 35036;
21     description
22         "88-DC WAVE Short Message Protocol (WSMP)";
23     reference
24         "Organization: IEEE P1609 WG
25     Reference: IEEE Std 1609";
26 }
27 enum homeplug-av-mme {
28     value 35041;
29     description
30         "88-E1 HomePlug AV Mobile Management Entity (MME)";
31     reference
32         "Organization: HomePlug Powerline Alliance, Inc.
33     Reference: HomePlug AV Specification";
34 }
35 enum mrp {
36     value 35043;
37     description
38         "88-E3 Media Redundancy Protocol";
39     reference
40         "Organization: Siemens AG
41     Reference: IEC 62439-2";
42 }
43 enum macsec {
44     value 35045;
45     description
46         "88-E5 MACsec EtherType";
47     reference
48         "Organization: IEEE 802 LAN/MAN Standards Committee
49     Reference: IEEE Std 802.1AE";
50 }
51 enum i-tag {
52     value 35047;
53     description
54         "88-E7 Backbone Service Instance Tag";
```

```
1      reference
2      "Organization: IEEE 802.1 Working Group
3      Reference: IEEE Std 802.1Q";
4  }
5  enum mvrp {
6      value 35061;
7      description
8      "88-F5 Multiple VLAN Registration Protocol (MVRP)";
9      reference
10     "Organization: IEEE 802.1 Working Group
11     Reference: IEEE Std 802.1Q";
12 }
13 enum mmrp {
14     value 35062;
15     description
16     "88-F6 Multiple MAC Registration Protocol (MMRP)";
17     reference
18     "Organization: IEEE 802.1 Working Group
19     Reference: IEEE Std 802.1Q";
20 }
21 enum ptp {
22     value 35063;
23     description
24     "88-F7 Precision Time Protocol";
25     reference
26     "Organization: IEEE I&M Society TC9
27     Reference: IEEE Std 1588";
28 }
29 enum cfm {
30     value 35074;
31     description
32     "89-02 IEEE 802.1Q Connectivity Fault Management (CFM) PDU
33     Encapsulation EtherType";
34     reference
35     "Organization: IEEE 802.1 Working Group
36     Reference: IEEE 802.1Q";
37 }
38 enum fcoe {
39     value 35078;
40     description
41     "89-06 Fibre Channel over Ethernet (FCoE)";
42     reference
43     "Organization: Cisco Systems, Inc
44     Reference: T11 FC-BB-5";
45 }
46 enum wlan-mgmt {
47     value 35085;
48     description
49     "89-0D 802.11 Management Protocol";
50     reference
51     "Organization: IEEE 802.11 Working Group
52     Reference: IEEE Std 802.11";
53 }
54 enum encap {
```

```
1      value 35088;
2      description
3          "89-10 Backbone Service Encapsulated Addresses";
4      reference
5          "Organization: IEEE 802.1 Working Group
6          Reference: IEEE Std 802.1Q";
7  }
8  enum fip {
9      value 35092;
10     description
11         "89-14 FCoE Initialization Protocol";
12     reference
13         "Organization: Brocade Communications Systems LLC
14         Reference: T11 FC-BB-5";
15 }
16 enum roce {
17     value 35093;
18     description
19         "89-15 Remote Direct Memory Access (RDMA) over Converged
20         Ethernet (RoCE)";
21     reference
22         "Organization: Mellanox Technologies, Inc.
23         Reference: IBTA Specification";
24 }
25 enum mis {
26     value 35095;
27     description
28         "89-17 Media Independent Service (MIS) Protocol";
29     reference
30         "Organization: IEEE 802.21 Working Group
31         Reference: IEEE Std 802.21";
32 }
33 enum tte {
34     value 35101;
35     description
36         "89-1D Time-Triggered Ethernet (TTE) Protocol Control
37         Frame";
38     reference
39         "Organization: TTTech Computertechnik AG
40         Reference: SAE AS6802";
41 }
42 enum mirp {
43     value 35113;
44     description
45         "89-29 Multiple I-SID Registration Protocol (MIRP)";
46     reference
47         "Organization: IEEE 802.1 Working Group
48         Reference: IEEE Std 802.1Q";
49 }
50 enum hsr {
51     value 35119;
52     description
53         "89-2F High-availability Seamless Redundancy (HSR)";
54     reference
```

```
1      "Organization: International Electrotechnical Commission
2      Reference: IEC 62439-3";
3  }
4  enum e-tag {
5      value 35135;
6      description
7          "89-3F Bridge Port Extension Tag (E-TAG)";
8      reference
9          "Organization: IEEE 802.1 Working Group
10         Reference: IEEE Std 802.1BR";
11  }
12  enum ecp {
13      value 35136;
14      description
15          "89-40 Edge Control Protocol";
16      reference
17          "Organization: IEEE 802.1 Working Group
18         Reference: IEEE Std 802.1Q";
19  }
20  enum f-tag {
21      value 35147;
22      description
23          "89-4B Flow Filtering Tag (F-TAG)";
24      reference
25          "Organization: IEEE 802.1 Working Group
26         Reference: IEEE Std 802.1Q";
27  }
28  enum drcp {
29      value 35154;
30      description
31          "89-52 Distributed Relay Control Protocol (DRCP)";
32      reference
33          "Organization: IEEE 802.1 Working Group
34         Reference: IEEE Std 802.1AX";
35  }
36  enum cim {
37      value 35234;
38      description
39          "89-A2 Congestion Isolation Message (CIM)";
40      reference
41          "Organization: IEEE 802.1 Working Group
42         Reference: IEEE Std 802.1Q";
43  }
44  enum llc-legacy {
45      value 51665;
46      description
47          "C9-D1 LLC Encapsulation (obsolete)";
48      reference
49          "Organization: IEEE 802.1 Working Group
50         Reference: IEEE Std 802.1AC";
51  }
52  enum mpp {
53      value 57915;
54      description
```

```
1      "E2-3B MAC Privacy protection Protocol";
2      reference
3      "Organization:
4      Reference: IEEE Std 802.1AE";
5      }
6      enum r-tag {
7      value 61889;
8      description
9      "F1-C1 Frame Replication and Elimination for Reliability
10     (FRER) Redundancy Tag (R-TAG)";
11     reference
12     "Organization: IEEE 802.1 Working Group
13     Reference: IEEE Std 802.1CB";
14     }
15     }
16     description
17     "IEEE Std 802 EtherTypes subset.";
18     }
19
20 }
21
```

¹ **Annex G**

² (informative)

³ **Wake-on-LAN**

⁴ Wake-on-LAN (WoL) is a common protocol to wake up devices from a very low power mode. It can be
⁵ implemented over IEEE 802 networks as a frame using the EtherType 08-42. WoL is not standardized in an
⁶ IEEE 802 standard.