IEEE STANDARDS ASSOCIATION

802®

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

IEEE Computer Society

REDLINE

Shows changes from the previous version!

Sponsored by the
LAN/MAN Standards Committee

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

IEEE Std 802®-2014
(Revision to
IEEE Std 802-2001)

This is a Redline Document produced by Techstreet, a business of Thomson Reuters.

This document is intended to provide users with an indication of changes from one edition to the next. It includes a full-text version of the new document, plus an indication of changes from the previous version.

Redlines are designed to save time and improve efficiencies by using the latest software technology to find and highlight document changes. More professionals are using valuable new technologies like redlines, to help improve outcomes in a fastpaced global business world.

Because it may not be technically possible to capture all changes accurately, it is recommended that users consult previous editions as appropriate. In all cases, only the current base version of this publication is to be considered the official document.

445 Hoes Lane, Piscataway, NJ 08854 USA | http://standards.ieee.org | Tel. +1 732-981-0060 Fax +1 732-562-1571

Redline Processing Notes:

1. ~~**Red Text**~~ **-** Red strikethrough text denotes deletions.

2. **Blue Text** **-** Blue underlined text denotes modifications and additions.

IEEE Std 802®-2014
(Revision of
IEEE Std 802-2001)

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

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 12 June 2014

IEEE-SA Standards Board

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

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

---

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

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

Important Notices and Disclaimers Concerning IEEE Standards Documents

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

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

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

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

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

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

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

Translations

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

Official statements

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

Comments on standards

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

Comments on standards should be submitted to the following address:

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

Laws and regulations

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

Copyrights

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

Photocopies

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

Updating of IEEE Standards documents

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

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

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

Errata

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

Patents

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

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

Participants

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

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

Ting Ao
Christian Boiger
Paul Bottorff
Weiying Cheng
Diego Crupnicoff
Rodney Cummings
Patrick Diamond
Aboubacar Kader Diarra
Janos Farkas
Norman Finn
Andre Fredette
Geoffrey Garner
Anoop Ghanwani
Franz Goetz
Mark Gravel
Craig Gunther
Stephen Haddock
Hitoshi Hayakawa
Jeremy Hitt
Rahil Hussain
Mirko Jakovljevic
Tony Jeffree
Markus Jochim
Michael Johas Teener
Hal Keen
Marcel Kiessling
Philippe Klein
Jeff Lynch
Ben Mack-Crane
James McIntosh
Anatoly Moldovansky
Eric Multanen
Henry Muyshondt
Donald Pannell
Karen Randall
Dan Romascanu
Jessy Rouyer
Panagiotis Saltsidis
Rick Schell
Michael Seaman
Daniel Sexton
Johannes Specht
Kevin Stanton
Wilfried Steiner
Patricia Thaler
Jeremy Touve
Albert Tretter
Karl Weber
Yuehua Wei
Jordon Woods

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

Peter Anslow
Arthur Astrin
David Bagby
Subir Das
James P. K. Gilb
Robert Grow
Marek Hajduczenia
Tony Jeffree
Patrick Kinney
Bruce Kraemer
Marek Hajduczenia
Mark Hamilton
David Hunter
David J. Law
Roger B. Marks
Apurva Mody
Paul Nikolich
Glenn Parsons
Clinton Powell
Ivan Reede
Malcolm Reynolds
Benjamin Rolfe
Richard Roy
Pat Thaler
Geoffrey O. Thompson
Juan Carlos Zuniga

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

Katsuhiro Ajito
Thomas Alexander
Nobumitsu Amachi
Peter Anslow
Butch Anton
Danilo Antonelli
Arthur Astrin
Michael Bahr
Hugh Barrass
Harry Bims
Christian Boiger
Ralf-Peter Braun
Nancy Bravin
Vern Brethour
Monique Brown
William Byrd
Brent Cain
Edgar Callaway
William Carney
Keith Chow
Rodney Cummings
Alessandro De Filippo
Michael Denson
Wael Diab
Patrick Diamond
Carlo Donati
Peter Ecclesine
Donald Fedyk
Andrew Fieldsend
Avraham Freedman
Yukihiro Fujimoto
James P. K. Gilb
Gregory Gillooly
Tim Godfrey
Patrick Gonia
Randall Groves
Robert Grow
Michael Gundlach
Craig Gunther
Chris Guy
Rainer Hach
Stephen Haddock
Marek Hajduczenia
Mark Hamilton
Jerome Henry
Marco Hernandez
Werner Hoelzl
David Howard
David Hunter
Tetsushi Ikegami
Noriyuki Ikeuchi
James Innis
Akio Iso
Atsushi Ito
Raj Jain
Tony Jeffree
Steven Jillings
Michael Johas Teener
Peter Jones
Vincent Jones
Joe Natharoj Juisai
Shinkyo Kaku
Chol Kang
Piotr Karocki
Stuart Kerry
Yongbum Kim
Patrick Kinney
Scott Kipp
Jarkko Kneckt
Bruce Kraemer
Thomas Kurihara
Geoff Ladwig
Richard Lancaster
Mark Laubach
David J. Law
Kyu Ha Lee
Hyeong Ho Lee
David Lewis
Arthur H. Light
Ru Lin
William Lumpkins
Greg Luri
Michael Lynch
Thomas Mack-Crane
Elvis Maculuba
Syam Madanapalli
Wayne Manges
Roger Marks
Stephen McCann
Brett McClellan
Michael McInnis
Jonathon McLendon
Neal Mellen
Steven Methley
Jose Morales
Ronald Murias
Rick Murphy
Peter Murray
Nabil Nasser
Michael Newman
Nicks.A. Nikjoo
Paul Nikolich
Mitsuo Nohara
Satoshi Obara
Mi-Kyung Oh
Yoshihiro Ohba
David Olsen
Satoshi Oyama
Thomas Palkert
Sandhya Patil
Brian Phelps
Clinton Powell
James Reilly
Maximilian Riegel
Robert Robinson
Benjamin Rolfe
Jon Walter Rosdahl
Jessy Rouyer
M. K. Sajeev
Osman Sakr
John Santhoff
Naotaka Sato
Peter Saunderson
Bartien Sayogo
Michael Seaman
Shusaku Shimada
Dorothy Stanley
Thomas Starai
Adrian Stephens
Rene Struik
Walter Struppler
Mark Sturza
Patrik Sundstrom
Jun Ichi Takada
Joseph Tardo
William Taylor
Geoffrey Thompson
Michael Thompson
Ha-Nguyen Tran
Kazuyoshi Tsukada
Dmitri Varsanofiev
Prabodh Varshney
Srinivasa Vemuru
John Vergis
George Vlantis
Haiming Wang
Lei Wang
Xiang Wang
Stephen Webb
Karl Weber
Hung-Yu Wei
Stephen Whitesell
Ludwig Winkel
Andreas Wolf
Chun Yu Charles Wong
Forrest Wright
Michael Wright
Oren Yuen
Janusz Zalewski
Daidi Zhong

When the IEEE-SA Standards Board approved this standard on 12 June 2014, it had the following membership:

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

Historical participants

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

William P. Lidinsky, *Chair*

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

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

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

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

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

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

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

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

James Kristof
H. Eugene Latham
Bing Liao
William P. Lidinsky
George Lin
Paul Lachapelle
Bill Lane
Paul Langille
Roger Lapuh
Loren Larsen
Johann Lindmeyr
Andy Luque
Philip Magnuson
Bruce McClure
Tom McGowan
Milan Merhar
Margaret A. Merrick
John Messenger
Colin Mick
Dinesh Mohan
John Montrose
Bob Moskowitz
Yaron Nachman
Krishna Narayanaswamy
Lawrence Ng
Henry Ngai
Satoshi Obara
Don O'Connor
Jerry O'Keefe
Toshio Ooka
Jorg Ottensmeyer
Richard Patti
Luc Pariseau
Glenn Parsons
Roger Pfister
Thomas L. Phinney
John Pickens

Dinel Pitt
Ron L. G. Prince
Steve Ramberg
Nigel Ramsden
Shlomo Reches
Frank Reichstein
Trudy Reusser
James Richmond
Anil Rijsinghani
Eduoard Rocher
John Roese
Allyn Romanow
Dan Romascanu
Paul Rosenblum
Dolors Sala
John Salter
Alan Sarsby
Ayman Sayed
Susan Schannning
Susan Schannning
Mick Seaman
Gerry Segal
Rich Seifert
Lee Sendelbach
Himanshu Shah
Howard Sherry
Wu-Shi Shung
Phil Simmons
Curtis Simonson
Paramjeet Singh
Rosemary V. Slager
Alexander Smith
Andrew Smith
M. Soha
Larry Stefani
Dan Stokesberry

Stuart Soloway
Sundar Subramaniam
Lennart Swartz
Kazuo Takagi
Kenta Takumi
Robin Tasker
Angus Telfer
Pat Thaler
Dave Thompson
Geoffrey O. Thompson
Michel Thorsen
Nathan Tobol
Wendell Turner
Steve Van Seters
Dono van-Mierop
Paul Videcrantz
Dennis Volpano
Paul Wainright
John Wakerly
Peter Wang
Y. C. Wang
Trevor Warwick
Scott Wasson
Daniel Watts
Karl Weber
Alan Weissberger
Deborah Wilbert
Keith Willette
Michael Witkowski
Edward Wong
Michael D. Wright
Michele Wright
Allen Yu
Wayne Zakowski
Igor Zhovnirovosky
Carolyn Zimmer
Nick Zucchero

Introduction

This introduction is not part of IEEE Std 802-2014, IEEE Standard for Local and metropolitan area networks: Overview and Architecture.

This document is the third major revision of the IEEE 802® overview and architecture. This revision integrates two earlier amendments, IEEE Std 802a™-2003 (covering Ethertypes for prototype and vendor-specific protocol development) and IEEE Std 802b™-2004 (covering registration of object identifiers), into the previous major revision of the standard, IEEE Std 802®-2001. In addition, there has been extensive rework in this document to bring forward the practice of protocol identification using the EtherType. While the protocol identification mechanism specified by ISO/IEC 8802-2 (IEEE Std 802.2™, withdrawn) is still used, its use for new standards has been deprecated. Further, material about physical layer addressing and universal addressing has been added along with information about the IEEE Registration Authority (RA) to facilitate user procurement of address assignments.

Since the 2001 revision of this standard, the IEEE 802 standards and working groups have undergone many changes. IEEE Std 802.5™ was withdrawn; therefore, references to it have been removed from this revision. IEEE Std 802 has also been broadened to include a variety of wireless standards; therefore, a new informative annex has been added to address the variety of IEEE 802 standards (Annex D). Data rates for IEEE 802 standards now range from tens of kilobits per second to hundreds of gigabits per second and encompass copper, optical fiber, wireless, and free-space optical media.

With the diversity of IEEE 802 standards, another goal of this revision was to bring the reference models from these various standards into this standard. This consolidation enables the user to quickly see the differences and similarities of the architecture of IEEE 802 standards. The reference models are included in a new informative annex (Annex B).

Contents

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

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

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

1. Overview

1.1 Scope ~~General~~

~~This document serves as the foundation for the family of IEEE 802® Standards published by IEEE for Local Area Networks (LANs) and Metropolitan Area Networks (MANs). It~~ This standard contains descriptions of the ~~networks considered~~ published by the IEEE for frame-based data networks as well as a reference model (RM) for protocol standards. ~~Compliance with the family of~~The IEEE 802® Standards architecture is defined, and a ~~standard~~ specification for the identification of public, private, and standard protocols is included.

1.2 Purpose

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

2. Normative references

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

IEEE Std 802.1D™, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Bridges.[1, 2]

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

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

ISO/IEC 8802-2:1998 ~~(IEEE Std 802.2-1998™)~~, Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.[3] (ISO/IEC version of withdrawn standard IEEE Std 802.2)

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

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

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

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.[4]

IETF RFC 2578, Structure of Management Information Version 2 (SMIv2).[5]

~~2. References~~

~~The following publications contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below.~~

~~ISO/IEC 7498-1:1994, Information technology—Open Systems Interconnection—Basic Reference Model:The basic model.[1]~~

~~ISO/IEC 8802-2:1998 (IEEE Std 802.2-1998™), Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical Link Control.~~

~~ISO/IEC TR 11802-1:1997, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Technical reports and guidelines—Part 1: The structure and coding of Logical Link Control addresses in Local Area Networks.~~

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

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

~~ISO/IEC TR 11802-2:1999, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Technical reports and guidelines—Part 2: Standard Group MAC Addresses.~~

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

~~ISO/IEC 15802-3:1998 (IEEE Std 802.1D-1998™), Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 3: Media Access Control (MAC) Bridges.~~

~~NOTE—Annex A lists, for information, the other LAN/MAN and related standards. Unlike those listed above, they do not contain detailed provisions that are used, by reference, by this standard.~~

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For ~~the purposes of~~ this ~~standard~~document, the following terms and definitions apply. *The ~~Authoritative Dictionary of~~ IEEE Standards ~~Terms, Seventh Edition [B2],~~*~~[2]~~ *Dictionary Online* should be ~~referenced~~consulted for terms not defined in this clause.[6]

access domain: A set of ~~LAN or MAN~~ stations in an IEEE 802® network together with interconnecting data transmission media and ~~related equipment~~functional units (e.g., ~~connectors,~~ repeaters), in which the ~~LAN or MAN~~ stations use the same ~~MAC~~medium access control (MAC) protocol to ~~establish the sequence of stations that are in temporary control of the shared transmission media~~communicate over a common physical medium.

~~**3.1.2 bit-reversed representation:** The representation of a sequence of octet values in which the values of the individual octets are displayed in order from left to right, with each octet value represented as a two-digit hexadecimal numeral, and with the resulting pairs of hexadecimal digits separated by colons. The order of the hexadecimal digits in each pair, and the mapping between the hexadecimal digits and the bits of the octet value, are derived by reversing the order of the bits in the octet value and interpreting the resulting bit sequence as a binary numeral using the normal mathematical rules for digit significance.~~

~~NOTE—The bit-reversed representation is applicable to LAN MAC addresses for use in a Token Ring (IEEE 802.5®) orFDDI environment. See Figure 8 for a comparative example of bit-reversed and hexadecimal representation.~~

~~[2]The numbers in brackets correspond to those of the bibliography in Annex A.~~

[6] *The IEEE Standards Dictionary Online* subscriptions are available at http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html.

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

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

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

~~**3.1.6 Ethernet frame:** A MAC data frame structured in accordance with ISO/IEC 8802-3 and containing an Ethernet type value in the LENGTH / TYPE field.~~

~~**3.1.7 fibre distributed data interface (FDDI) frame:** A MAC data frame structured in accordance with ISO/IEC 9314-2.~~

~~**3.1.8 hexadecimal representation:** The representation of a sequence of octet values in which the values of the individual octets are displayed in order from left to right, with each octet value represented as a two-digit hexadecimal numeral, and with the resulting pairs of hexadecimal digits separated by hyphens. The order of the hexadecimal digits in each pair, and the mapping between the hexadecimal digits and the bits of the octet value, are derived by interpreting the bits of the octet value as a binary numeral using the normal mathematical rules for digit significance.~~

~~NOTE—See Figure 8 for a comparative example of bit-reversed and hexadecimal representation.~~

~~**3.1.9 IEEE 802.3® frame, 802.3® frame:** A MAC data frame structured in accordance with ISO/IEC 8802-3 and containing a length value in the LENGTH / TYPE field.~~

~~**3.1.10 IEEE 802.5® frame, 802.5® frame:** A MAC data frame structured in accordance with ISO/IEC 8802-5.~~

~~**3.1.11 IEEE 802.n® frame, 802.n® frame:** A MAC data frame structured in accordance with ISO/IEC 8802-n.~~

~~NOTES~~

~~1—At the time of publication of this standard, relevant specifications, in addition to those cited explicitly in 3.1.9 and 3.1.10, are for n = 4, 6, 9, and 11.~~

~~2—ISO/IEC 8802-12 also defines a MAC protocol, but it does not specify its own MAC data frame format; instead, it uses the IEEE 802.3® and IEEE 802.5® frame formats.~~

~~**3.1.12 IEEE 802® LAN, 802® LAN:** A LAN consisting of an access domain using either a MAC protocol specified in one of the IEEE 802.n and ISO/IEC 8802-n Standards or the FDDI MAC protocol.~~

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

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

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

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

frame: The format of aggregated bits from a medium access control (MAC) sublayer entity that are transmitted together in time.

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

IEEE 802® ~~**MAN, 802® MAN:** A MAN~~ **network:** A network consisting of one or more interconnected ~~sub~~networks each using a medium access control (MAC) protocol specified in an IEEE 802® ~~or ISO/IEC 8802 MAN~~ standard.

~~NOTE—Part of the data communication capability of an IEEE 802® MAN is the provision of a data service equivalent to that provided by an IEEE 802® LAN, over the extended geographical area of the MAN.~~

interconnection: ~~The provision of~~ A data communication path between ~~LAN or MAN~~ stations in an IEEE 802® network.

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

~~**3.1.16 LAN:** A computer network, located on a user's premises, within a limited geographical area.~~

~~**3.1.17 MAC control frame:** A data structure consisting of fields in accordance with a MAC protocol, for the communication of control information, only, in a LAN or MAN.~~

~~NOTE—ISO/IEC 8802-5® uses the term “MAC frame” in this sense.~~

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

logical link: A logical communication connection between two devices.

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

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

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

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

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

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

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

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

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

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

repeater: A device that interconnects segments of the physical medium by retransmitting a copy of the physical layer (PHY) frame.

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

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

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

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

universal address: A 48-bit extended unique identifier (EUI-48) or 64-bit extended unique identifier (EUI-64) that is used as a unique address.

~~**3.1.22 octet:** A sequence of eight bits, the ends of the sequence being identified as the most significant bit (MSB) and the least significant bit (LSB).~~

~~NOTE—This identification of the ends of the sequence defines an unambiguous mapping from octet values, via binary numerals, to the integers 0–255, and hence a mapping also from octet values to the expressions of those integers as numerals in hexadecimal notation. See: Hexadecimal Representation.~~

3.2 Acronyms and abbreviations

BS	base station
CID	company identifier
CPE	customer-premises equipment
CS	convergence sublayer
C-SAP	control service access point
DLL	data link layer
EPD	EtherType protocol discrimination
EPON	Ethernet passive optical networks
EUI-48	48-bit extended unique identifier
EUI-64	64-bit extended unique identifier
HLPDE	higher layer protocol discrimination entity

I/G	individual/group
IM	implementation model
IP	Internet Protocol
LAN	local area network
LLC	logical link control ~~(ISO/IEC 8802-2)~~
LPD	LLC protocol discrimination
LSAP	link service access point ~~(ISO/IEC 8802-2)~~
LSB	least significant bit
MAC	medium access control, media access control~~[3]~~[7]
MA-L	MAC address – large MA-M MAC address – medium
MAN	metropolitan area network
MA-S	MAC address – small
MCPS	MAC common part sublayer
MCPS-SAP	MAC common part sublayer data service access point

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

MIB management information base

MICF media-independent control function

MICLSAP media-independent control link service access point

MICPSAP media-independent control physical service access point

MICSAP media-independent control service access point

MIH media-independent handover

MIHF media-independent handover function

MLME MAC sublayer management entity

MSAP MAC service access point

M-SAP ~~MAC~~ management service access point

MSB most significant bit

NCMS network control and management system

OAM operations, administration, and maintenance

OID object identifier

OLT optical line terminal

ONU	optical network unit
OSI/RM	Open Systems Interconnection basic reference model~~(ISO/IEC 7498-1)~~
OUI	organizationally unique identifier
PAN	personal area network
PDU	protocol data unit
PHY	physical layer (OSI reference model and IEEE 802® reference model)
PHY	physical layer device or entity (IEEE 802.3™ reference model)
PICS	protocol implementation conformance statement
PLME	physical layer management entity
PMD	physical medium dependent
P~~h~~SAP	physical service access point
RA	Registration Authority
RAN	regional area network
RM	reference model
RSTP	rapid spanning tree protocol

SAP service access point

SNAP Subnetwork Access Protocol

SNMP Simple Network Management Protocol~~(RFC 1157[4])~~

SSF spectrum sensing function

SS/MS subscriber station/mobile subscriber station

U/L universally or locally administered

VLAN virtual local area network

WAN wide area network

WLAN wireless local area network

WPAN wireless personal area network

WRAN wireless regional area network

~~CMIP common management information protocol (ISO/IEC 9596-1)~~

~~CSMA/CD carrier sense multiple access with collision detection (ISO/IEC 8802-3)~~

~~DQDB distributed queue dual bus~~

~~[4]See A.1 for information on obtaining RFCs.~~

~~FDDI~~	~~fibre distributed data interface (ISO/IEC 9314)~~
~~ISDN~~	~~integrated services digital network~~
~~ISLAN~~	~~integrated services LAN (ISO/IEC 8802-9) LAN~~
~~MOCS~~	~~managed object conformance statement~~

4. Family of IEEE 802 standards

4.1 Key concepts

IEEE 802 networks use frame-based communications over a variety of media to connect various digital apparatus regardless of computer technology and data type. However, the scope of IEEE 802 standards is not limited to the physical layers (PHYs) and data link layers (DLLs).

The basic communications capabilities provided by all IEEE 802 standards are frame based with source and destination addressing and asynchronous timing. In a frame-based system, the format is a variable-length sequence of data octets. ~~LANs and MANs are packet-based, as opposed to either cell-based or isochronous. That is, the basic unit of transmission is a sequence of data octets, which can be of any length within a range that is dependent on the type of LAN; for all LAN types, the maximum length is in excess of 1000 octets.~~ By contrast, cell-based communication transmits data in fixed-length units in specified time intervals while isochronous communication transmits data as a steady stream of octets, or groups of octets, at equal time intervals.

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

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

Some IEEE 802 technologies, in particular wireless-based technologies, are inherently shared-medium communication systems. They too have been augmented over time. Many wireless local area networks (WLANs) support mobile node mobility and hence dynamic topologies. These additional facilities may, depending on the IEEE 802 technology in use, restrict bridged LAN interconnects to the static topology nodes within the wireless portion of a heterogeneous technology LAN.

~~The LANs described herein are distinguished from other types of data networks in that they are optimized for a moderate-sized geographic area, such as a single office building, a warehouse, or a campus.~~ An IEEE 802 LAN is a peer-to-peer communication network that enables stations to communicate directly on a point-to-point, or point-to-multipoint, basis without requiring them to communicate with any intermediate stations that perform forwarding or filtering above the PHY. ~~switching nodes.~~ LAN communication takes place at moderate to high data rates and with short transit delays, on the order of a few milliseconds or less.

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

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

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

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

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

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

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

~~Although primarily aimed at deployment on the scale of a large building or a campus, LANs are also frequently applied in smaller areas, such as small offices or single laboratories, and increasingly in homes. At the small-scale application level, a LAN is different from the type of network, such as a data bus or backplane bus, that is optimized for the interconnection of devices on a desktop or of components within a single piece of equipment. However, desktop-scale applications of LANs are also possible, particularly where the nature of the application is more suited to peer-to-peer communication among autonomous components, as opposed to a system structure with more centralized control.~~

~~The original IEEE 802® LAN technologies used shared-medium communication, with information broadcast for all stations to receive. That approach has been varied and augmented subsequently, but in ways that preserve the appearance of simple peer-to-peer communications behavior for end stations. In particular, the use of bridges (see 6.3.2) for interconnecting LANs is now widespread. These devices allow the construction of networks with much larger numbers of LAN end stations, and much higher aggregate throughput, than would be achievable with a single shared-medium LAN. End stations attached to such a bridged LAN can communicate with each other just as though they were attached to a single shared-medium LAN (however, the ability to communicate with other stations can be limited by use of management facilities in the bridges, particularly where broadcast or multicast transmissions are involved). A further stage in this evolution has led to the use of point-to-point full duplex communication in LANs, either between an end station and a bridge or as a typically high-speed link between a pair of bridges.~~

~~An optional function that may be offered by a LAN or a MAN is the provision of local networking of isochronous bearer services that are compatible with, or higher speed versions of, Integrated Services Digital Networks (ISDN) as defined by the ITU-T I-series Recommendations, to support voice, video, and data devices and terminals. These services are based on the use of end-user to end-user isochronous bearers that will span the supporting Integrated Services LAN (ISLAN) or MAN and an intervening ISDN-conformant WAN. Typically, the information streams for packet and isochronous services are multiplexed over the same physical media. In addition, capabilities are specified for a single integrated management of these various streams.~~

4.2 Application and support

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

- Client/server applications
- Database access
- Desktop publishing
- Electronic mail
- File transfer
- Graphics
- Handover services
- Multimedia
- Office automation
- Process control

— Robotics

— Telecommunication

— Text processing

— Transaction processing

— ~~Integrated Services (voice, video and data) applications~~

— IEEE 802 ~~The~~ networks are intended to support various data devices, such as the following:

— Bridges, routers, and gateways

— Computers

— Image and video monitors

— Mass storage devices

— Monitoring and control equipment

— Photocopiers and facsimile machines

— Printers and plotters

— Terminals

— Wireless terminals

— ~~Integrated Services devices, including ISDN terminals and end systems supporting combined voice, video, and data applications~~

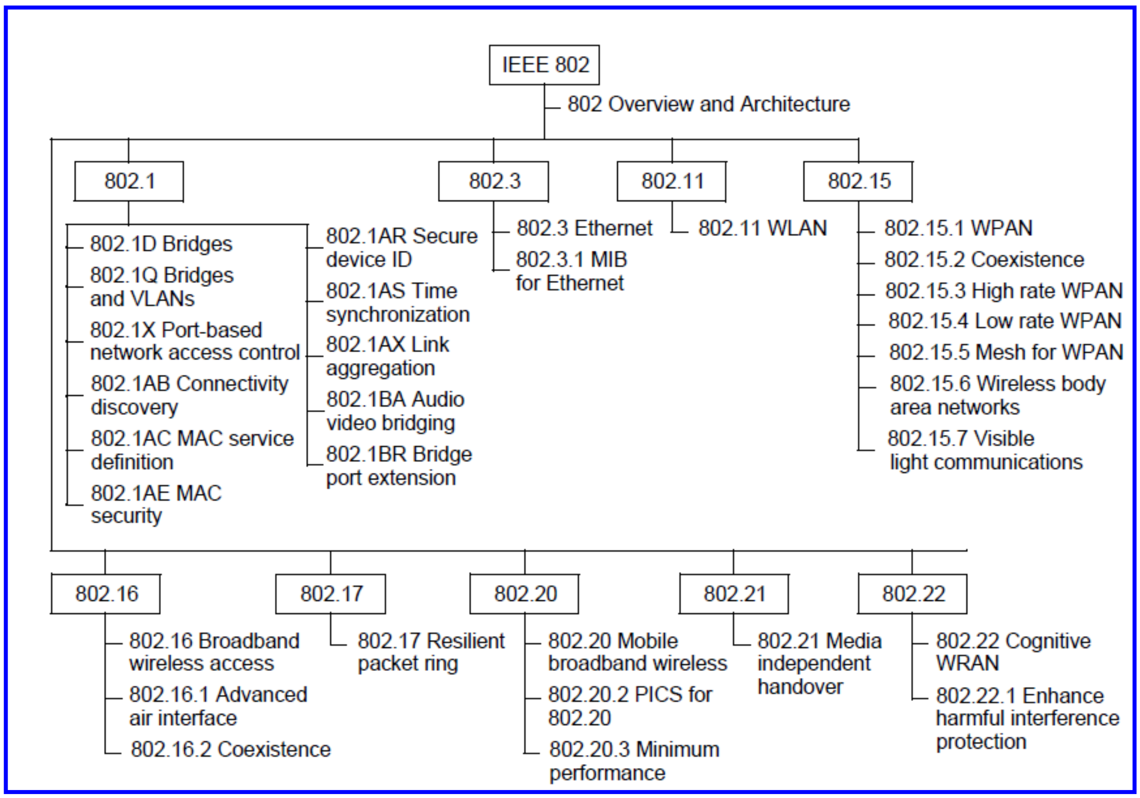
4.3 An international family of standards

The terms *LAN*, *MAN*, *PAN*, and *RAN* encompass a number of data communications technologies and applications of these technologies. So it is with the IEEE 802® standards. In order to provide a balance between the proliferation of a very large number of different and incompatible local and metropolitan networks, on the one hand, and the need to accommodate rapidly changing technology and to satisfy certain applications or cost goals, on the other hand, several types of medium access technologies are currently specified in the family of IEEE 802® standards. In turn, these MAC standards are specified for a variety of physical media. A ~~logical link control (LLC) standard~~ secure data exchange standard and MAC bridging standards are intended to be used in conjunction with the MAC standards. ~~In some ISLAN and MAN standards, provisions are made for optionally conveying isochronous bearer services in support of continuous voice, video, and synchronous data applications.~~ ~~An~~ Architecture and protocols for the management of IEEE 802® ~~LANs~~ networks are also specified ~~defined.~~

The IEEE 802® standards have been developed and applied in the context of ~~an increasingly~~ a global data communications industry. IEEE 802 standards are recognized to be international standards in their own right. In addition, some IEEE 802 standards have progressed to become standards within ~~ISO/IEC JTC 1~~Joint Technical Committee 1 ~~Information Technology,~~ of the International Organization for Standardization and the International Electrotechnical Commission ~~see Clause 2 and Annex A. This global context is recognized in that most IEEE 802® Standards are progressed to become also international~~ (ISO/IEC JTC 1), International Telecommunication Union Telecommunication Standardization Sector (ITU-T), International Telecommunication Union Radio communication Sector (ITU-R), and a wide variety of national body standards development organizations.

4.4 IEEE 802 standards

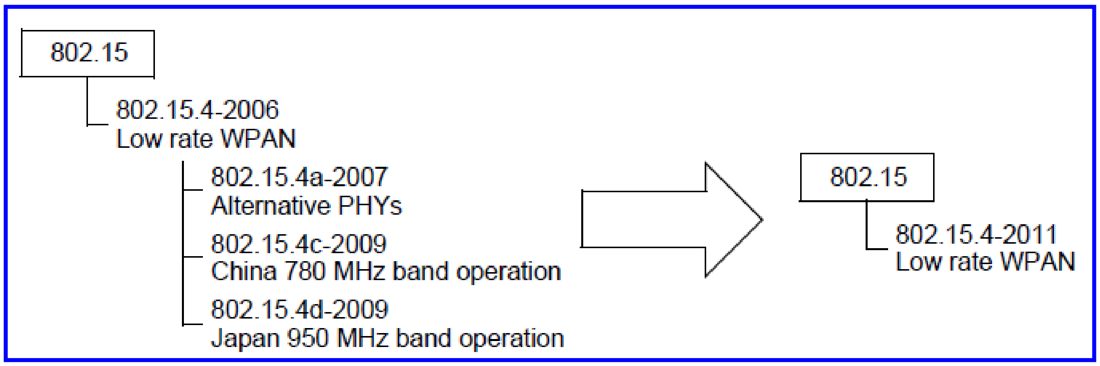
The IEEE 802 LAN/MAN Standards Committee sponsors a large number of standards projects. The current state of IEEE 802 standards and recommended practices is illustrated in Figure 1. The IEEE 802 committee is very active; therefore, for the latest status of the IEEE 802 working groups and standards, refer to http:// www.ieee802.org.



(New)

Figure 1—Current family of IEEE 802 standards and recommended practices

At any given time, an IEEE 802 standard may have one or more amendments related to it. Each amendment, once approved, is considered to be part of the base standard. At a future time, these amendments are incorporated into the base standard so that a new single document can be issued. This process is illustrated in Figure 2 for IEEE Std 802.15.4™-2011,[8] which incorporated the amendments IEEE Std 802.15.4a™-2007, IEEE Std 802.15.4c™-2009, and IEEE Std 802.15.4d™-2009 into the base standard IEEE Std 802.15.4-2006.



(New)

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

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

~~5. Compliance~~

~~NOTE—IEEE policy with respect to claims of compliance, conformance, or compatibility with IEEE standards can be found in the Trademark Policy statement in the front matter. This clause will be deleted in the next revision of this standard.~~

5. Reference ~~and implementation~~ models (RMs)

5.1 Introduction

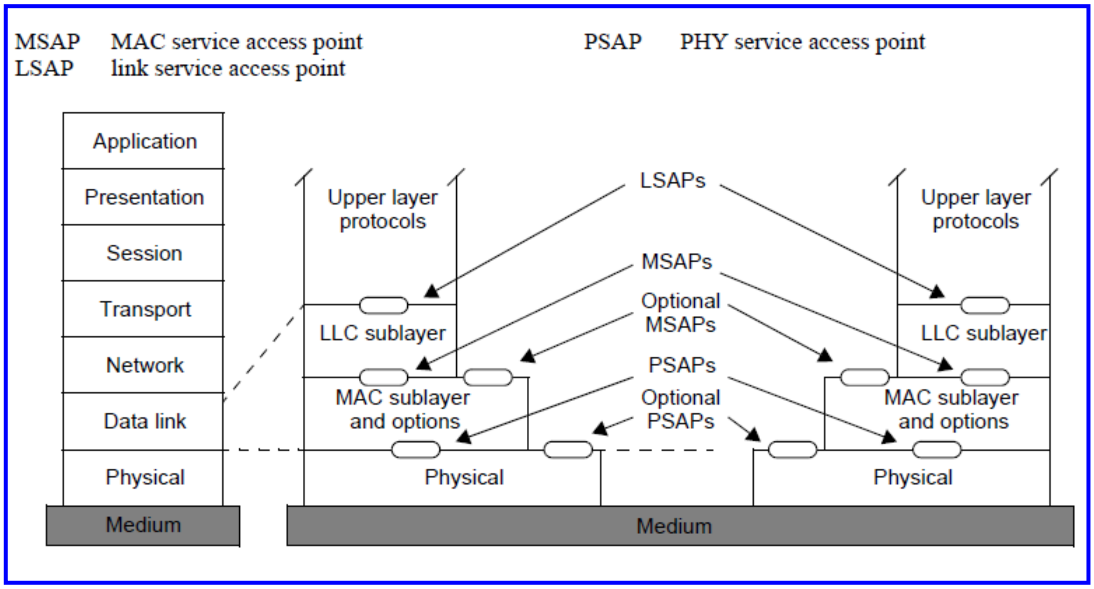
~~This clause defines The IEEE 802® LAN and MAN RM (LAN&MAN/ RM) and implementation model(LAN&MAN/IM). The intent of presenting these models is as follows:~~

~~a) To provide an overview of the standard~~

~~b) To serve as a guide to reading other IEEE 802® Standards~~

The IEEE 802® ~~LAN&MAN/RM is patterned after~~ derived from the Open Systems Interconnection ~~(OSI)~~ basic reference model (OSI/RM), ISO/IEC 7498-1:1994 [B7][9]. It is assumed that the reader has some familiarity with the OSI/RM and its terminology. The IEEE 802® ~~Standards encompass~~ standards emphasize the functionality of the lowest two layers of the OSI/RM, i.e., ~~Physical layer~~PHY and ~~Data Link layer)~~DLL, and the higher layers as they relate to ~~LAN~~network management. The ~~LAN&MAN/~~IEEE 802 RM is similar to the OSI/RM in terms of its layers and the placement of its service boundaries. Figure 3 shows the architectural view of IEEE 802 RM for end stations and its relation to the OSI/RM. A variation of the model applies within bridges, as described in 5.3.2.

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



(New)

Figure 3—IEEE 802 RM for end stations

For the mandatory ~~packet~~data services supported by all ~~LANs and MANs~~IEEE 802 networks, the ~~Data Link layer~~ DLL is structured as two sublayers, with the logical link control (LLC) sublayer, described in 5.2.2, operating over a MAC sublayer~~. In addition, some IEEE 802® LAN technologies provide direct support by the MAC sublayer for an alternative Ethernet sublayer operating at the same place in the architecture as does LLC; for the other IEEE 802® LAN technologies, the equivalent~~, described in 5.2.3.~~functionality is provided by encapsulation of the Ethernet sublayer information within LLC Protocol Data Units (PDUs), using the Subnetwork Access Protocol specified in Clause 10 of this Standard.~~

~~Optionally, some Integrated Service LANs and MANs may also support ITU-T compatible isochronous bearer services at the Physical layer.~~

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

~~The OSI/RM is referred to by the IEEE 802® Standards because of the following:~~

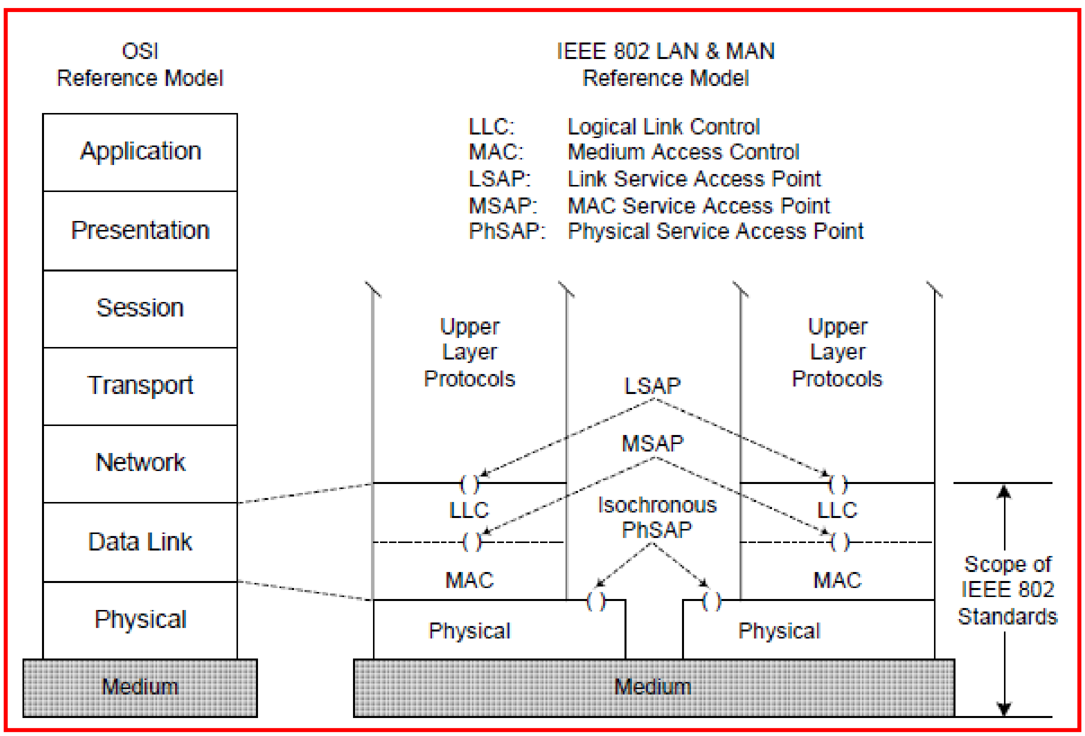
~~a) The OSI/RM provides a common vehicle for understanding and communicating the various components and interrelationships of the standards.~~

b) The OSI/RM helps define terms.

c) The OSI/RM provides a convenient framework to aid in ~~the development and enhancement of the standards~~.

~~d) The use of the OSI/RM facilitates a higher degree of interoperability than might otherwise be possible.~~

~~Figure 1 shows the architectural view of LAN&MAN/RM and its relation to the OSI/RM.~~

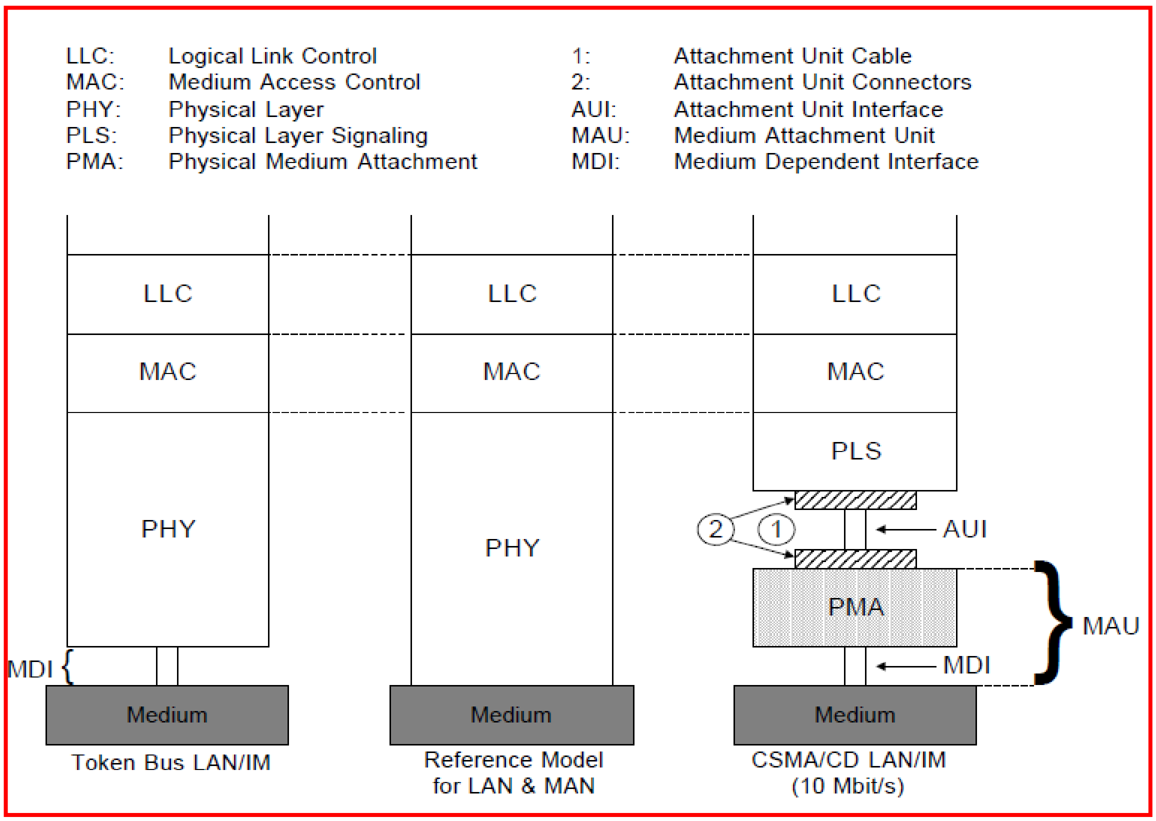


~~(Deleted)~~

~~**Figure 1—IEEE 802® RM for end stations (LAN&MAN/RM)**~~

~~The LAN&MAN/IM is~~ implementation models (IMs) are more specific than the ~~LAN&MAN/RM~~IEEE 802 RMs, allowing differentiation between implementation approaches (e.g., ~~of carrier sense multiple access with collision detection [CSMA/CD], and token passing). Figure 2 shows two implementation views of LAN&MAN/IMs and their~~ different MAC protocols and PHYs). Figure 4 illustrates an IEEE 802.3 IM and its relation to the ~~LAN&MAN/~~IEEE 802 RM.

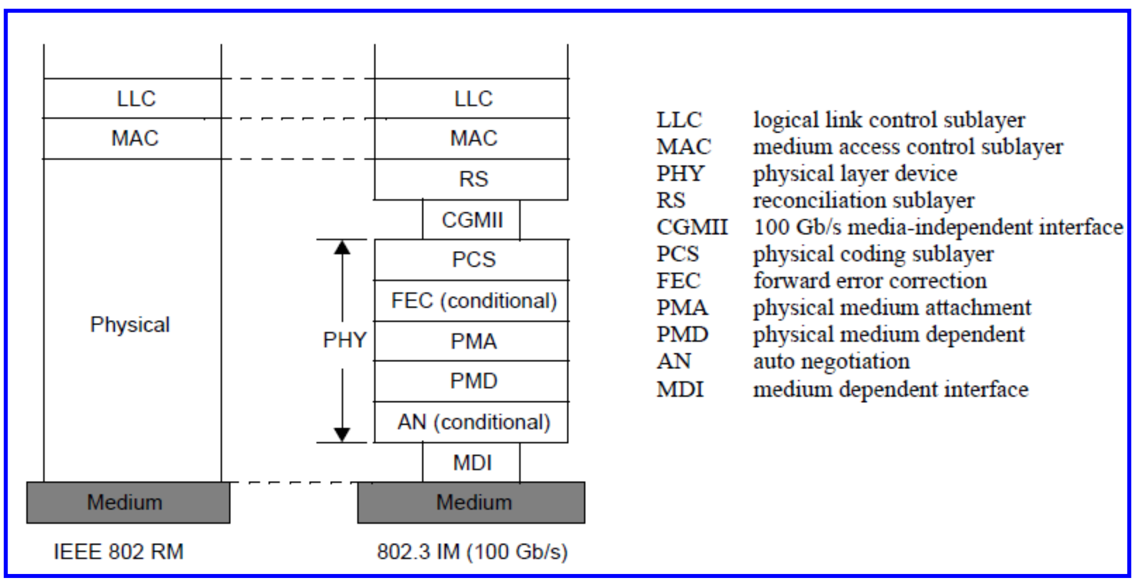
~~Both Figure 1 and Figure 2 illustrate the application of the models in LAN end stations. A variation of the model applies within bridges (see 6.3.2). Also, Figure 1 and Figure 2 illustrate only the basic transfer of user data between end stations.~~



~~(Deleted)~~

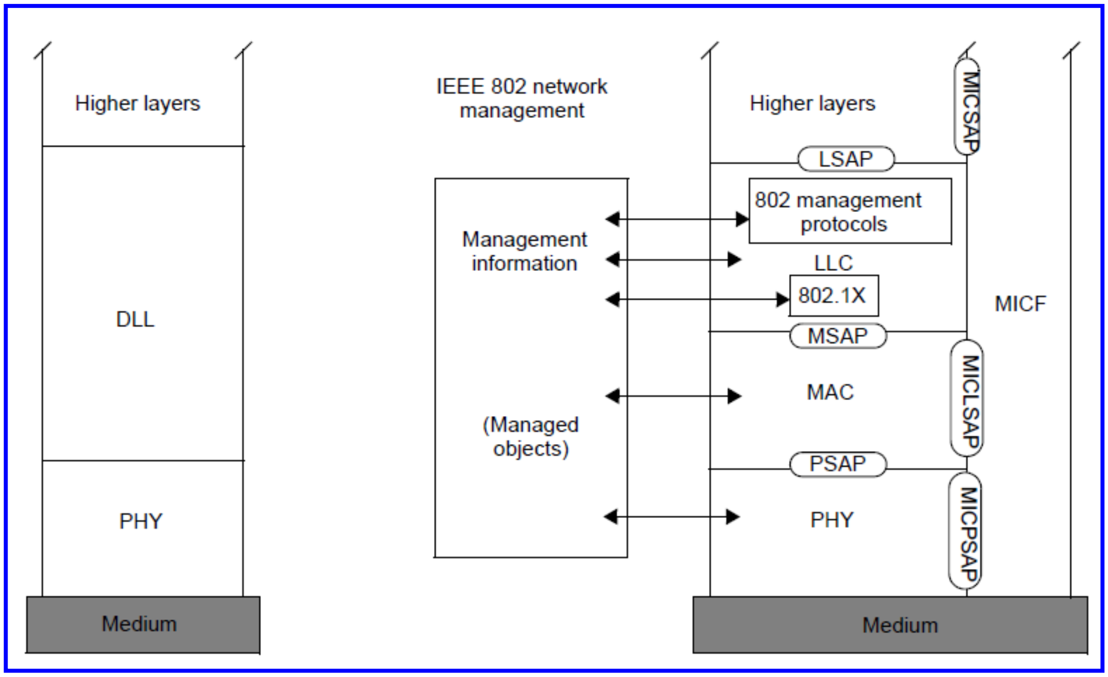
~~**Figure 2—IEEE 802® RM and two examples of end-station implementation model**~~

Considerations of management~~ and~~ security~~ in LANs and MANs~~, and media-independent handover (MIH) in IEEE 802 networks are also covered by IEEE 802® standards; these optional features lead to an elaboration of the RM, as illustrated in Figure ~~3). LAN/MAN~~5. IEEE 802 network management provides ~~a Data Link layer management~~ protocols for exchange of management information between ~~LAN~~ stations; ~~managed objects~~. The media-independent control function (MICF) is a parallel control plane that provides control functions for different MAC and PHY sublayers. Some examples of this MICF are ~~defined for all LAN/MAN protocol standards. The Secure Data Exchange (SDE) entity~~the media-independent handover function (MIHF) of IEEE Std 802.21™ and the control functions proposed in the IEEE 802.19.1 Task Group and IEEE Std 802.22™. IEEE Std 802.1X™ forms part of the LLC sublayer and provides a secure, connectionless service immediately above the MAC sublayer.

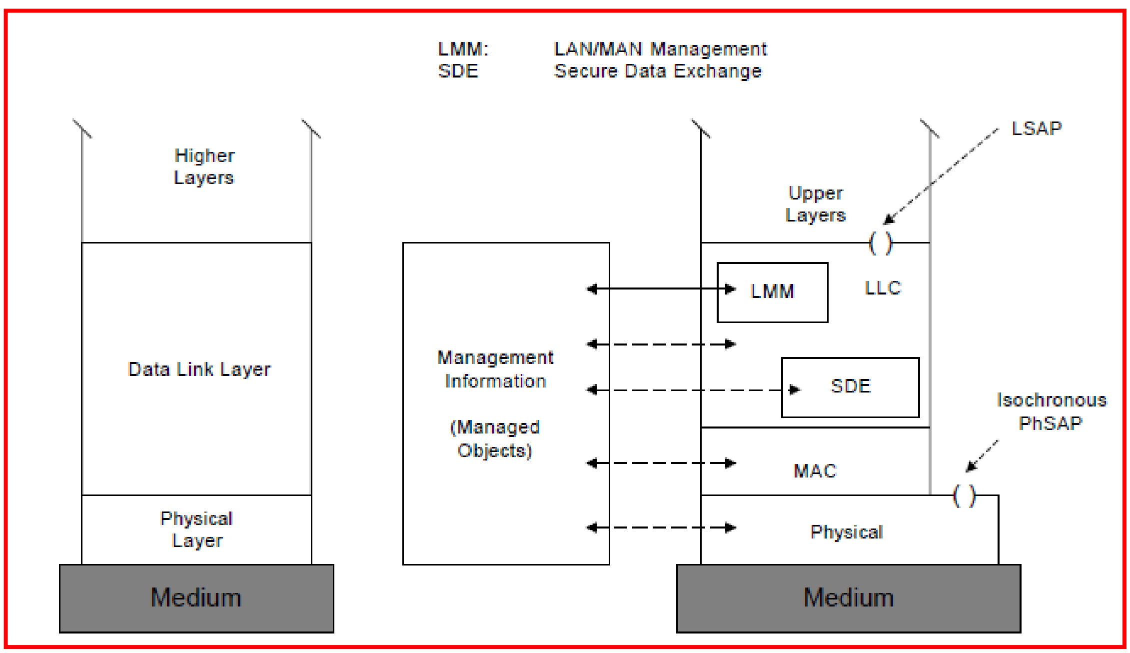


(New)

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



(New)



~~(Deleted)~~

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

5.2 RM description for end stations

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

5.2.1 ~~Service access points~~ (SAPs)

~~Multiple~~ One or more link service access points (LSAPs) provide interface ports to support ~~multiple~~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 ~~a single~~ one or more MAC service access ~~point (MSAP~~points (MSAPs) as ~~an interface port~~interfaces to the LLC sublayer in an end station. ~~In general, the MSAP~~ 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 ~~identified (~~used to provide an interface to support control of the MAC by the MICF.

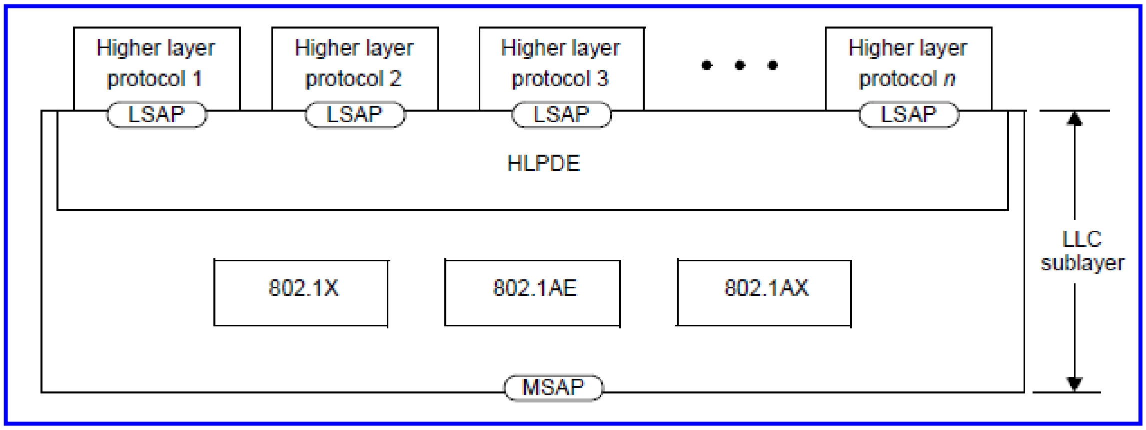
The PHY provides a PHY service access point (PSAP). In addition, the PHY optionally provides a media- independent control PHY service access point (MICPSAP), which is used to provide an interface port for ~~transmission and reception) by a single individual MAC address and (for reception)~~the control of the PHY by the ~~LAN-wide broadcast MAC address; it can~~MICF. ~~also be identified (for reception) by one or more group MAC addresses. Clause 9 provides details of how these MAC addresses are constructed and used; see also ISO/IEC 15802-1~~

~~A user of LLC is identified by, at a minimum, the logical concatenation of the MAC address field and the LLC address field in a frame. See ISO/IEC 8802-2 and ISO/IEC TR 11802-1 for a description of LLC addresses.~~

~~The Physical layer provides an interface port to a single MAC station, and in the case of ISLANs and MANs, it may optionally offer isochronous bearer services at multiple Physical service access points (PhSAPs). See 11.3 for a more detailed description of ISLAN and MAN PhSAP addressing requirements.~~

5.2.2 LLC sublayer

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



(New)

Figure 6—LLC sublayer in 802 RM

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

1) EtherType protocol discrimination (EPD), which uses the EtherType value made available to the LLC sublayer through the MSAP

2) LLC protocol discrimination (LPD), which uses the addresses defined in ISO/IEC 8802-2, including the Subnetwork Access Protocol (SNAP) format

IEEE Std 802.3™ is capable of natively representing the EtherType within its MAC frame format, which is used to support EPD. IEEE Std 802.3 also natively supports ISO/IEC 8802-2 LPD (over a limited range of frame sizes). In other IEEE 802 networks, such as for IEEE Std 802.11™, LPD is also achieved using SNAP, as described in Clause 9. In either of these techniques, the EtherType is effectively being used as a means of identifying an LSAP that provides LLC sublayer service to the protocol concerned. New IEEE 802 standards shall support protocol discrimination in the LLC sublayer using EPD.

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

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

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

~~The LLC sublayer standard, ISO/IEC 8802-2, describes three types of operation for data communication between service access points: unacknowledged connectionless-mode (type 1), connection-mode (type 2), and acknowledged connectionless-mode (type 3).~~

~~With type 1 operation, information frames are exchanged between LLC entities without the need for the prior establishment of a logical link between peers. The LLC sublayer does not provide any acknowledgments for these LLC frames, nor does it provide any flow control or error recovery procedures.~~

~~LLC type 1 also provides a TEST function and an Exchange Identification (XID) function. The capability to act as responder for each of these functions is mandatory: This allows a station that chooses to support initiation of these functions to check the functioning of the communication path between itself and any other station, to discover the existence of other stations, and to find out the LLC capabilities of other stations.~~

~~With type 2 operation, a logical link is established between pairs of LLC entities prior to any exchange of information frames. In the data transfer phase of operation, information frames are transmitted and delivered in sequence. Error recovery and flow control are provided, within the LLC sublayer.~~

~~With type 3 operation, information frames are exchanged between LLC entities without the need for the prior establishment of a logical link between peers. However, the frames are acknowledged to allow error recovery and proper ordering. Further, type 3 operation allows one station to poll another for data.~~

~~NOTE—ISO/IEC 8802-2 defines four classes of LLC, each of which groups together support for a different combination of LLC types. All classes include mandatory support of type 1.~~

~~The Secure Data Exchange (SDE) entity forms part of the LLC sublayer and provides a secure connectionless service immediately above the MAC sublayer. The operation of the SDE entity is described in IEEE Std 802.10®.~~

5.2.3 MAC sublayer

The MAC sublayer performs the functions necessary to provide ~~packet~~frame-based, connectionless-mode (datagram style) data transfer between stations in support of the ~~LLC~~next higher sublayer~~ or of the Ethernet sublayer (see 6~~, as described in 5.1), for ~~LANs~~networks that support it. The term *MAC frame*, or simply *frame*, is used to describe the ~~packets~~datagrams transferred ~~within the~~between peer MAC sublayer entities. In some MAC types~~ (e.g., Token Ring),~~, some MAC frames are used in support of the MAC sublayer functionality itself, rather than for transfer of ~~LLC data~~data from the next higher sublayer.

The principal functions of the MAC sublayer comprise the following:

— Frame delimiting and recognition

— Addressing of destination stations (both as individual stations and as groups of stations)

— Conveyance of source-station addressing information

— Transparent data transfer of ~~LLC~~ PDUs~~, or of equivalent information in~~ from the ~~Ethernet~~next higher sublayer

— Protection against errors, generally by means of generating and checking frame check sequences

— Control of access to the physical transmission medium

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

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

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

~~NOTE—~~The serial transmission model does not preclude current or future MAC specifications from using partly or wholly octet-oriented specifications of frame formats or of the interface to the ~~Physical layer~~PHY.

5.2.4 ~~Physical layer~~PHY

~~The Physical layer provides the capability of transmitting and receiving bits between Physical layer~~ MAC entities~~. A pair of Physical layer~~ use their respective PHY entities ~~identifies the peer-~~to~~-peer unit~~ exchange ~~of bits between two MAC users, and in the case of ISLANs and MANs, it may optionally support the exchange of~~ bits with ~~end-~~their peers. The PHY provides the capability to~~-end timing preserved between isochronous-service PhSAPs.~~

~~The Physical layer provides the capability of transmitting and receiving~~ transmit and receive modulated signals assigned to specific frequency channels~~, in the case of~~ for broadband or wireless, media or to a single~~ in the case of~~ baseband-channel.

~~Note that,~~ Whereas the service offered to the MAC sublayer is expressed as the transfer of bits (in sequences representing MAC frames), the ~~actual~~ symbols that are encoded for transmission do not always represent individual bits. Particularly at speeds of 100 ~~Mbit~~Mb/s and above~~,~~ or for wireless transmission, the ~~Physical layer~~PHY can map blocks of several bits (e.g., 4, 5, or 8 bits) to different multi-element symbols. In some ~~Physical layer~~PHY encodings, these symbols are subject to further transformation before transmission, and in some cases, the transmission is spread over multiple physical data paths. ~~The actual transmission on physical media can therefore be far removed from the simple bit serial representation of a MAC frame (as was specified, for example, in the original ISO/IEC 8802-3 and ISO/IEC 8802-5 Physical layers).~~

5.2.5 Layer and sublayer management

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

5.3 Interconnection and interworking

In some cases, the end ~~systems on a LAN or MAN~~stations in an IEEE 802 network have no need to communicate with end ~~systems~~stations on other networks ~~(other LANs, WANs, etc.).~~. However, ~~this is not expected to be the norm;~~ there are many cases in which end stations on ~~a LAN or MAN will~~an IEEE 802 network need to communicate with end ~~systems~~stations on other networks ~~and so~~; therefore, devices that interconnect the ~~LAN or MAN~~IEEE 802 network with other kinds of networks are required. In addition, several standard methods have been developed that permit a variety of interconnection devices to operate transparently to end stations on a ~~LAN or MAN~~network in order to extend the ~~LAN/MAN~~ capabilities available to end stations, particularly in terms of the geographical extent and/or total number of end stations that can be supported.

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

— ~~Physical layer~~PHY interconnection, using devices usually termed *repeaters* or *hubs*, as described in 5.3.1

— MAC ~~sublayer~~ interconnection, using devices termed *bridges*, as described in 5.3.2

— Network-layer interconnection, using devices usually termed *routers*, as described in 5.3.3

~~See also Clause 11 of this standard, for an outline of the optional methods by which ISLANs and MANs may support isochronous interworking with WANs and with remote ISLANs and MANs.~~

5.3.1 Interconnection at the PHY ~~Physical layer: repeaters and hubs~~

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

A repeater is a device used to interconnect segments of the physical communications media, for example, to extend the range of a ~~LAN~~network when the physical specifications of the technology would otherwise be exceeded, while providing a single access domain for the attached ~~LAN~~ stations. Repeaters used in support of multiple end stations attached by star-wired network topologies are frequently referred to as *hubs*.

5.3.2 MAC-sublayer interconnection: Bridges

5.3.2.1 Bridges and bridged ~~LANs~~IEEE 802 networks

Bridges ~~(see 3.1.3)~~ are ~~devices~~stations that interconnect multiple access domains. ~~ISO/IEC 15802-3~~IEEE Std 802.1D[10] provides the basic specification for bridge interworking among IEEE 802® networks. A bridged ~~LAN (see 3.1 of ISO/IEC 15802-3)~~IEEE 802 network consists of one or more bridges together with the complete set of access domains that they interconnect. A bridged ~~LAN~~IEEE 802 network provides end stations belonging to any of its access domains with the ~~appearance~~connectivity of a ~~LAN~~ network that contains the whole set of attached end stations. IEEE Std 802.1Q adds additional capabilities to the bridge specification in IEEE Std 802.1D including virtual local area networks (VLANs), priorities, and provider bridging, as described in 5.3.2.5.

A bridged ~~LAN~~network can provide for the following:

— Communication between stations attached to ~~LANs~~networks of different MAC types that conform to the Internal Sublayer Service as specified in IEEE Std 802.1AC.

— An increase in the total throughput of a ~~LAN~~network over that of a purely shared media network

— An increase in the physical extent of, or number of permissible attachments to, a ~~LAN~~network

— Partitioning of the physical ~~LAN~~network for administrative or maintenance reasons

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

The term *switch* is often used to refer to some classes of bridge. However, there is no consistent meaning applied to the distinction between the terms *bridge* and *switch*, and ~~ISO/IEC 15802-3~~IEEE Std 802.1D does not make any such distinction. Hence, this standard only uses the term *bridge*.

5.3.2.2 Bridge relaying and filtering

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

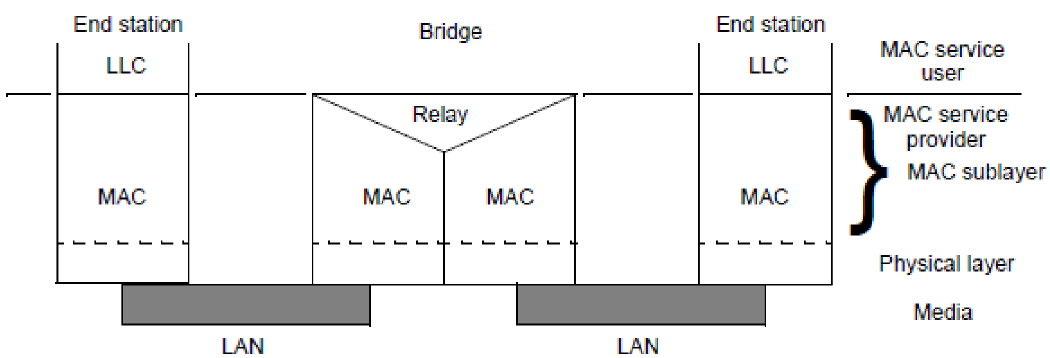


Figure 7—Internal organization of the MAC sublayer with bridging

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

5.3.2.3 ~~The Spanning Tree Protocol~~Resolving topologies with multiple paths

A key aspect of ~~ISO/IEC 15802-3~~IEEE Std 802.1D and IEEE Std 802.1Q is ~~its~~ the specification of the ~~Spanning Tree Protocol,~~rapid spanning tree protocol (RSTP), which is used by bridges to configure their interconnections in order to prevent looping data paths in the bridged ~~LAN. In the event that~~IEEE 802 network. If the basic interconnection topology of bridges and ~~LANs~~networks contains multiple possible paths between certain points, use of the ~~Spanning Tree Protocol~~RSTP blocks some paths in order to produce a simply connected active topology for the flow of MAC user traffic between end stations. For each point of attachment of a bridge to a ~~LAN~~network, the ~~Spanning Tree Protocol~~RSTP selects whether ~~or not~~ MAC user traffic is to be received and transmitted by the bridge at that point of attachment.

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

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

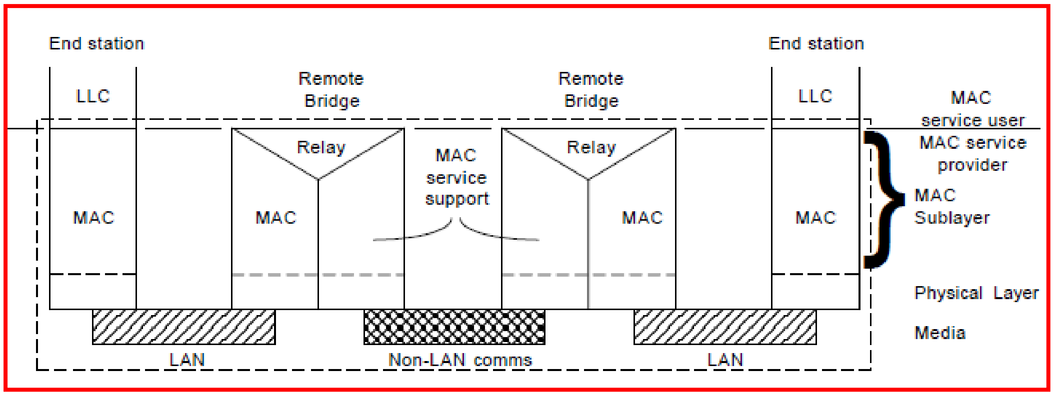
5.3.2.4 Transparent bridging~~ and source routing~~

~~ISO/IEC 15802-3 specifies~~IEEE Std 802.1D and IEEE Std 802.1Q specify transparent bridging operation, so called because the MAC bridging function does not require the MAC user frames transmitted and received to carry any additional information relating to the operation of the bridging functions; end-station operation is unchanged by the presence of bridges.

~~Also specified, in an annex to ISO/IEC 15802-3, is the operation of a Source Routing Transparent (SRT) bridge. This adds the ability for a *source routing* function in a bridge to use explicit MAC sublayer routing information contained in MAC user frames; this source-routing information is inserted by the transmitting end station. Source routing is specified only for ISO/IEC 8802-5 Token Ring and ISO/IEC 9314 FDDI LANs, and for IEEE 802.12® Demand Priority LANs when operating with 8802-5 format frames.~~

~~6.3.2.5 Remote MAC bridging~~

~~ISO/IEC 15802-5 extends the specification in ISO/IEC 15802-3 to cover remote MAC bridging, where non-IEEE 802® communications technologies are used to interconnect bridges, for example, to allow a bridged LAN to include WAN links to provide greatly extended geographical range. Figure 5 shows the corresponding organization of the MAC sublayer.~~



~~(Deleted)~~

~~**Figure 5—Internal organization of MAC sublayer with remote bridges**~~

5.3.2.5 Provider bridging

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

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

5.3.2.6 Bridging example

Some bridges are used to interconnect access domains that each contain a very small number of end stations (often, a single end station). Others interconnect multiple access domains that contain principally other bridges, thus, forming a backbone for the bridged ~~LAN. (Hybrid~~IEEE 802 networks. Bridged IEEE 802 network configurations~~, with characteristics of both kinds of bridge, are of course possible.) Bridged LAN configurations involving~~ that involve these kinds of interconnection have become widespread as the ~~IEEE 802® LAN~~ technologies have developed. ~~As noted in 1.2, they~~These configurations allow the construction of networks with much larger numbers of end stations and much higher aggregate throughput than was previously achievable.

Figure 8 illustrates ~~the kind~~an example of a bridged ~~LAN~~IEEE 802 network that can be configured with bridge-style interconnection. The bridges A and B, and the ~~CSMA/CD~~IEEE 802.3 LAN configurations to which they attach, are typical of the older style of bridged ~~LAN~~IEEE 802 network in which a bridge interconnects a small number of access domains, each containing many end stations, as is similar with K~~, L,~~ and ~~M~~L and their ~~Token Ring LANs.~~ IEEE 802.17™ ring. The IEEE 802.17 ring and the IEEE 802.3 connections between S and T and S and U form backbone networks. On the other hand, the bridges S, T, and U function as bridges ~~in a high-speed backbone~~ that combines ~~FDDI and 100 Mbit/s~~IEEE 802.17, IEEE 802.3® ~~LANs.~~, and IEEE 802.16™ networks. S is a backbone bridge, handling a number of ~~high-speed LAN~~network attachments. T and U are bridges that support multiple end stations, with connection to ~~the~~a backbone network. B and K also provide access to ~~the~~a backbone network. The end station shown connected to S by a point-to- point link could be a server system~~, as might the end stations attached to the FDDI LAN~~.

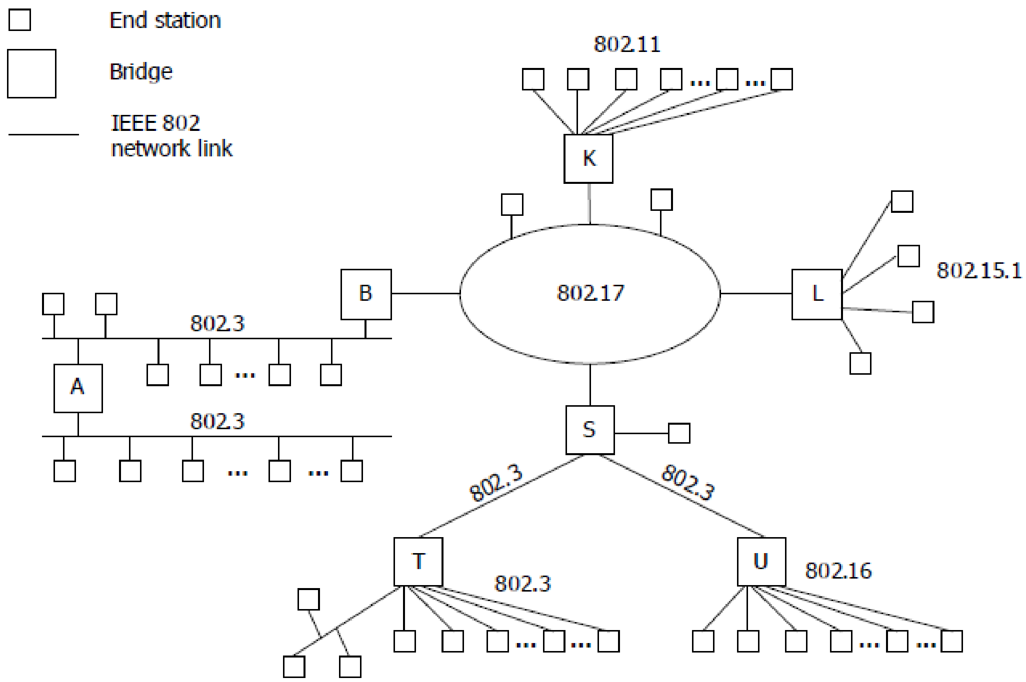


Figure 8—An example of a bridged ~~LAN~~IEEE 802 network

5.3.3 Network-layer interconnection: Routers

~~The third category of interconnection uses Network-layer~~ Routers are interconnection devices, generally known as routers, that operate as ~~LAN/MAN~~IEEE 802 end stations. These process network layer protocols that operate directly above the LLC sublayer ~~or equivalent~~, with forwarding decisions based on network layer addresses. Details of this kind of interconnection lie outside ~~of~~ the scope of IEEE 802® ~~LAN/MAN~~ standards, but the various standard and proprietary network-layer protocols involved represent a ~~very~~ substantial part of the user traffic on many ~~real~~ IEEE 802® networks. In particular, IEEE 802® ~~LANs and MANs~~ networks are often interconnected by routers for the ~~Internet Protocol~~ (IP) and its related routing and management protocols, either directly to other ~~LANs~~IEEE 802 networks or by means of WAN ~~links~~connections.

6. General requirements for an IEEE 802® ~~LAN or MAN~~ network

6.1 Services supported

With the descriptions in Clause 5 as a basis, an IEEE 802® ~~LAN or MAN~~ network can be characterized as a communication resource that provides sufficient capabilities to support the MAC service ~~defined~~specified in ~~ISO/IEC 15802-1~~IEEE Std 802.1AC, between two or more MSAPs. In particular, this requires the ability to convey LLC sublayer data from one MSAP to *n* other MSAPs, where *n* can be any number from 1 to the number of all of the other MSAPs on the network. An IEEE 802® ~~LAN~~ network is required, at a minimum, to support ~~both LLC Type 1 and~~ the MAC Internal Sublayer Service ~~defined~~specified in ~~ISO/IEC 15802-3. In addition, an ISLAN or MAN may optionally~~ IEEE Std 802.1AC and support ~~isochronous bearer services compatible with ISDN services as defined in the ITU-T I-series Recommendations~~the use of EtherTypes for protocol identification at the LLC sublayer.

~~7.2 Size and extent~~

~~The original IEEE 802® LAN and MAN technologies were designed to be capable of supporting access domains containing at least 200 end stations and with geographical extent of at least 2 km for LANs (using Physical-layer repeaters if necessary) and 50 km for MANs. Subsequent developments in IEEE 802® LAN technology and performance have been accompanied by a reduction in the size and extent required in individual access domains, recognizing that these can readily and cost-effectively be interconnected in bridged LANs that are capable of offering at least the original minimum size and extent, with increased overall bandwidth and performance. Size and extent requirements for future IEEE 802® LAN technologies are, similarly, expected to be determined by application needs and opportunities.~~

6.2 Error ratios ~~rates~~

~~Error performance of IEEE 802® LANs and MANs is required to be such as follows:~~ For wired or optical fiber physical medium, 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 ~~Physical Service interface~~PHY service inter-face of an intended receiving peer MAC entity, due only to operation of the ~~Physical layer~~PHY, shall be less than8×10^{-8} per octet of MAC frame length.

NOTE—For some applications and data rates, better performance than this may be required.

~~b) For wireless physical media: Within a single access domain, the probability that a MAC Service Data Unit (MSDU) is not delivered correctly at an MSAP of an intended receiving MAC service user, due to the operation of the Physical layer and the MAC protocol, shall be less than 8 × 10^-8 per octet of MSDU 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.

~~NOTE—The performance measure stated in (a) defines a highly desirable characteristic of LAN performance, as it has a bearing on other aspects of the delivered service, such as frame loss and transmission delays caused by the need to retransmit. However, this measure is not realistic for all physical media; for example, wireless media may be unable to meet this level of physical layer performance due to the inherent transmission characteristics of the medium. In such cases, the operation of the MAC protocol must employ additional mechanisms, for example, error detection and correction mechanisms, in order to enable the MAC service provider to meet the performance levels implied by this condition in the service offered at the MAC service boundary.~~

NOTE—For example, ~~(a)~~ the worst-case probability of losing a maximum-length IEEE 802.3® frame ~~(1518 octets) through physical layer damage~~at the PHY is to be less than 1.21×10^{-4}, or approximately 1 in 8250~~; (c)~~. 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 7.5×0^{-11}, or approximately 1 in 13 300 000 000.

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

6.3 Transient service interruption ~~availability~~

Insertion of a ~~device~~station into, or removal of a ~~device~~station from, ~~a LAN or MAN~~an IEEE 802 network shall cause at most a transient loss of availability of the access domain(s) to which the ~~device~~station attaches, lasting not more than 1 s. Failure of a ~~device~~station, including loss of power, shall ~~not~~ cause ~~more than~~at most a transient fault for the access domain(s) to which it ~~attaches~~was attached, with duration ~~of~~ on the order of 1 s. The preceding requirements assume that the new configuration of the network without the lost station is valid.

~~NOTE—In a bridged LAN, reconfiguration of the topology in response to logical insertion or removal of a bridge, or to changes in a bridge's Configuration parameters, can cause loss of communication between some access domains for longer periods, typically a few tens of seconds; ISO/IEC 15802-3 contains the full specification~~.

~~7.5 Safety, and lightning and galvanic protection~~

~~Equipment implementing IEEE 802® LAN and MAN standards is typically subject to guidance and requirements relating to safety and to protection of the equipment and its users from lightning and galvanic effects. Such guidance and requirements are outside of the scope of IEEE 802® standardization; they are typically specified by other organizations with different legal, geographical, and industrial scope. However, the general underlying concerns can have an influence on the Physical layer aspects can ® LAN and MAN standards.~~

6.4 Regulatory requirements

While regulatory compliance is out of the scope of IEEE 802 standards, the need to comply with regulations can influence the regulations can standards.

~~Equipment implementing IEEE 802® LAN and MAN standards may be subject to regulations imposed within particular geographical and political domains. For example, the deployment of equipment implementing IEEE802® wireless LAN standards may be subject to local regulations that pertain to the use of radio-frequencytransmission. Such regulations are outside of the scope of IEEE 802® standardization; they are typically specified by other organizations with different legal, geographical, and industrial scope. However, the general underlying concerns can have an influence on the Physical layer aspects of IEEE 802® LAN and MAN standards.~~

7. IEEE 802 ~~LAN/MAN~~ network management

7.1 General

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

7.2 General-purpose ~~LAN/MAN~~IEEE 802 network management

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

7.2.1 Management functions

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

— Configuration management provides for the identification of communications resources, initialization, reset and ~~close~~shut-down, the supply of operational parameters, and the establishment and discovery of the relationships between resources.

— Fault management provides for fault prevention, detection, diagnosis, and correction.

— Performance management provides for evaluation of the behavior of communications resources and of the effectiveness of communication activities.

— Security management provides for the protection of resources.

— Accounting management provides for the identification and distribution of costs and the setting of charges.

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

7.2.2 Management architecture

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

Operations on a managed object can be initiated by mechanisms local to the equipment being managed (e.g., via a control panel built into the equipment) or can be initiated from a remote management system by means of a general-purpose management protocol carried using the data services provided by the ~~LAN or MAN~~IEEE 802 network to which the equipment being managed is connected. The entity that does both the network communication of the management protocol and the interaction to and from the managed objects is called the *agent*.

~~There are two general-purpose management protocols of relevance to the management of LAN/MANequipment, as follows:~~

The Simple Network Management Protocol (SNMP), as described in IETF RFC 3411 [B5], provides a general-purpose management protocol that can be used for the management of IEEE 802 network equipment.

~~The OSI common1157 common management information protocol (CMIP), as described in ISO/IEC 9595 and ISO/IEC 9596 and related standards~~

~~NOTE—In addition to operation of CMIP over a full OSI protocol stack, two standards define the use of CMIP over simpler protocol support. ISO/IEC 15802-2 (IEEE Std 802.1B-1995™) defines a means of using CMIP over a simple Data Link layer protocol stack in LANs; RFC 1095 describes the use of CMIP over a TCP/IP protocol stack~~.

~~Of the two protocols, SNMP is the more significant in terms of its wide application across the spectrum of LAN/MAN products in today's marketplace; however, in some markets, and where it is desirable to integrate LAN management with management of wide-area networking and telephony equipment, use of the OSI management protocols may be important.~~

7.2.3 Managed object definitions

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

a) A definition of the functionality provided by the managed object, and the relationship between this functionality and the resource to which it relates.

b) A definition of the syntax that is used to convey management operations, and their arguments and results, in a management protocol.

c) An address that allows the management protocol to specifically communicate with the managed object in question. In IEEE 802 this is done with an object identifier (OID), as described in Clause 10.

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

~~Each management protocol has its notation for defining managed objects, as follows:~~

SNMP ~~has standards for~~is used in many cases together with the structure of management information known as ~~SMIv1 (RFC 1155, RFC 1212 and RFC 1215) and~~ SMIv2 (IETF RFC ~~1902,~~2578, IETF RFC ~~1903~~2579 [B3], and IETF RFC ~~1904),~~2580 [B4]), which ~~provides ASN.1-based~~ uses a set of macros based on ~~with~~subset of ASN.1 for defining managed objects.

b) ~~CMIP has a standard language, known as GDMO (ISO/IEC 10165-4), which is used along with ASN.1 to define both the syntactic and semantic aspects of managed objects.~~

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

~~NOTES~~

~~1—IEEE Std 802.1F® provides additional guidance for use of GDMO in LAN/MAN standards.~~

~~2—Some IEEE 802® standards have used GDMO as the notation for their managed object definitions, with SNMP management information base (MIB) definitions being developed subsequently within the IETF, using automatic tools for translating GDMO definitions into equivalent SNMP definitions.~~

7.3 Special-purpose ~~LAN/MAN~~IEEE 802 network management standards

Special-purpose protocols relating to the management functionality of IEEE 802® stations can be developed ~~where~~when the use of a general-purpose management protocol is inappropriate. ~~An~~ Examples of ~~a~~ special-purpose management ~~protocol is ISO/IEC 15802-4, which defines the services and~~ protocols ~~for remote station loading~~that can be found in ~~a LAN/MAN environment. This protocol permits~~the family of IEEE 802 standards include the ~~simultaneous loading of multiple stations by~~Connectivity Fault Management Protocol specified in IEEE Std 802.1Q; the Operations, Administration, and Maintenance (OAM) Protocol specified in IEEE Std 802.3; and the Link Layer Discovery Protocol (LLDP) in IEEE Std 802.1AB™. ~~use of the group addressing capability in IEEE 802® technologies.~~

8. MAC addresses

8.1 Terms and notational conventions

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

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

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

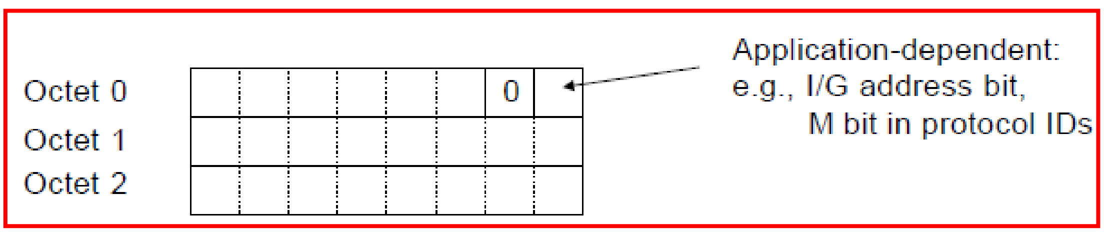
Bit-reversed representation is a sequence of octet values in which the values of the individual octets are displayed in order from left to right, with each octet value represented as a 2-digit hexadecimal numeral and with the resulting pairs of hexadecimal digits separated by colons. The order of the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

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

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

~~9. Universal addresses and protocol identifiers~~

~~The IEEE makes it possible for organizations to employ unique individual LAN MAC addresses, group addresses, and protocol identifiers. It does so by assigning Organizationally Unique Identifiers (OUIs), which are three octets (24 bits) in length. Because the assignment of the OUI in effect reserves a block of each derivative identifier (i.e., blocks of individual LAN MAC addresses, group addresses, and protocol identifiers), the address space of the OUI is chosen to be large. Although the OUIs are 24 bits in length, their true address space is 22 bits. The LSB of the first octet can be set to 1 or 0 depending on the application. The next-to-LSB of the first octet is 0, for all assignments. The remaining 22 bits, which shall not be changed by the assignee, result in 2 22 (approximately 4 million) identifiers; see Figure 7.~~



~~(Deleted)~~

~~Figure 7—OUI~~

~~The universal administration of LAN MAC addresses began with the Xerox Corporation administering Block Identifiers (Block IDs) for Ethernet addresses. Block IDs were assigned by the Ethernet Administration Office and were 24 bits in length (three octets). An organization developed addresses by assigning the remaining 24 bits. For example, the address as represented by the six octets P-Q-R-S-T-U comprises the Block ID, P-Q-R, and the locally assigned octets S-T-U.~~

~~The IEEE, because of the work in Project 802® on standardizing LAN technologies, has assumed the responsibility of defining and carrying out procedures for the universal administration of addresses for IEEE and ISO/IEC LANs (e.g., CSMA/CD, Token Bus, Token Ring, and FDDI). In carrying out the procedures, the IEEE acts as the Registration Authority for OUIs.[5] The responsibility for defining the procedures is discharged by the IEEE Registration Authority Committee (RAC), which is chartered by the IEEE Standards Association Board of Governors.~~

~~The IEEE honors the Block ID assignments made by the predecessor administration office where those assignments fall as the great majority of them do within the space administered by the IEEE. The Block ID is referred to as the OUI by the IEEE.~~

~~9.1 OUI~~

~~OUIs allow a general means of assuring unique identifiers for a number of purposes. Currently, the IEEE assigns OUIs to be used for generating LAN MAC addresses and protocol identifiers. Assuming correct administration by the IEEE Registration Authority and the assignee, the LAN MAC addresses and protocol identifiers will be universally unique.~~

~~OUIs are assigned as three-octet values. Both values (0, 1) are assigned to the LSB of the first octet. The next-to-LSB of the first octet is set to 0; this bit of the OUI being set to 0 indicates that the assignment is universal. Three-octet values occupying the same fields as OUIs can occupy, but with the next-to-LSB of the first octet set to 1, are locally assigned and have no relationship to the IEEE-assigned values (as described herein).~~

~~[5] Interested applicants should contact the IEEE Registration Authority, Institute of Electrical and Electronic Engineers Inc., 445 HoesLane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA.~~

~~The standard representation of the OUI is as a string of three octets, using the hexadecimal representation(see 3.1.8).~~

8.2 ~~48 bit~~ universal ~~LAN MAC~~ addresses

8.2.1 Concept and overview

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

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

8.2.2 Assignment of universal addresses

The IEEE RA has the responsibility of defining and carrying out procedures for the administration of universal addresses.[11] The IEEE RA has also been designated by ISO/IEC to act as a registration authority for the ISO/IEC 8802 series of standards. The responsibility for defining the procedures is discharged by the IEEE Registration Authority Committee, which is chartered by the IEEE Standards Association Board of Governors.

[11] Interested applicants should contact the IEEE RA, http://standards.ieee.org/develop/regauth/oui.

The IEEE RA enables the creation of universal addresses, i.e., EUI-48s and EUI-64s, by assigning identifiers of various lengths, as described in Table 1.[12]

Table 1—IEEE RA assignment summary

IEEE RA assignment	Number of IEEE 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 addresses – large (MA–L)	24	2^{24}	2^{40}	yes [organizationally unique identifier (OUI)]
MAC addresses–medium (MA–M)	28	2^{20}	2^{36}	no
MAC addresses – small (MA–S)	36	2^{12}	2^{28}	yes (OUI-36 only)

(New)

NOTE 1—The terms *OUI* and *OUI-36* were previously used by the IEEE RA to refer to what are now called *MA–L* and *MA–S*, respectively. The acronym OUI without modification was used to refer to the 24-bit field assigned by the IEEE RA. However, while not appropriate, the acronym OUI has been used to refer to generally to all IEEE RA assignments. As a result, the use of OUI is not always consistent within all IEEE standards.

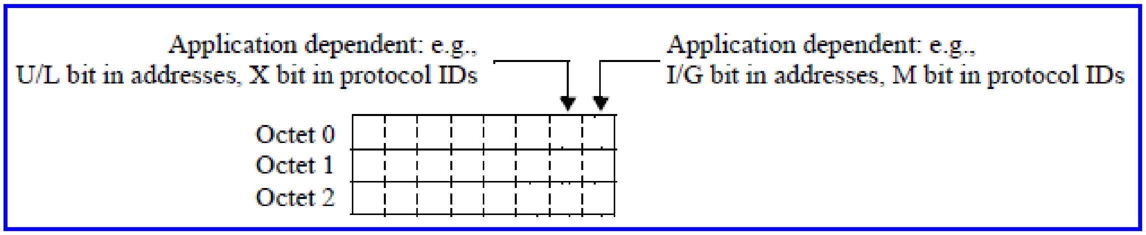
NOTE 2—The CID comes from the same 24-bit space as the MA-L/OUI. A CID assignment is used to identify a company or organization, but is not used to create universal addresses. A CID assignment has the X bit (the U/L address bit in a MAC address) set to one, which would place any address created with a CID in the locally administered address space.[13]

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

[13] More information on CIDs can be found on the IEEE RA tutorial web page, http://standards.ieee.org/develop/regauth/tut/index.html.

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 MA-L is illustrated in Figure 9. The structure for the first octet of MA-M and MA-S is the same as for MA-L. For MA-L, MA-M, and MA-S, 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 assignment is the universal/local (U/L) address bit.



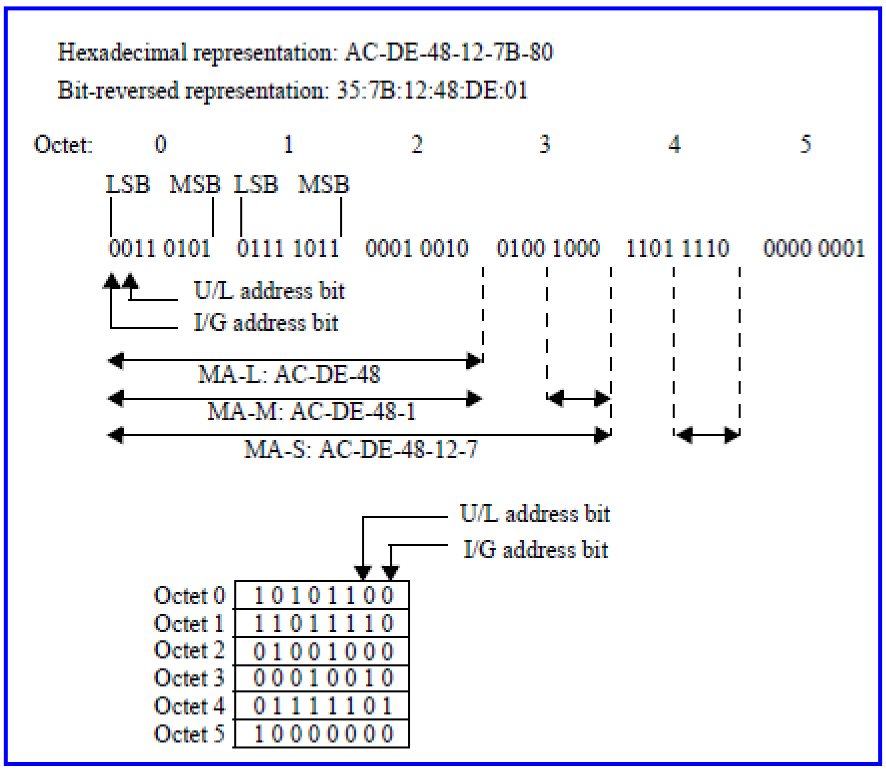
(New)

Figure 9—Structure of MA-L/OUI

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 0, it indicates that the MAC address field is an individual MAC address. If this bit is 1, 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 1's.

The U/L bit indicates whether the MAC address has been assigned by a local or universal administrator. Universal addresses have the U/L bit set to 0. If the U/L bit is set to 1, the remaining bits (i.e., all bits except the I/G and U/L bits) are locally administered and should not be expected to meet the uniqueness requirement of the IEEE RA-assigned values.

A universal address consists of two parts~~. The first 24~~: the leading bits ~~correspond to the OUI as~~(24, 28, or 36) are assigned by the IEEE~~, except~~ RA with the U/L bit set to zero and the remaining bits by that ~~the~~ assignee ~~may set the LSB of the first octet to 1 for group addresses or set it to 0 for individual addresses. The second part, comprising the remaining 24 bits, is administered by the assignee. In the 48-bit LAN MAC address, an~~ . An example of ~~which~~an EUI-48 is shown in Figure ~~8, the OUI is~~ 10. For MA-M and MA-S, the final 4 bits of the assigned number are in a nibble that is not adjacent to the other bits in the assigned number when displayed with LSB on the left and most significant bit (MSB) on the right. For example, when using an MA-S to create an EUI-48, the MA-S value is contained in octets 0, 1, 2, 3 and the least significant nibble of octet 4, and the value assigned by the assignee is contained in the most significant nibble of octet 4 and octet 5.



(New)

Figure 10—Example EUI-48

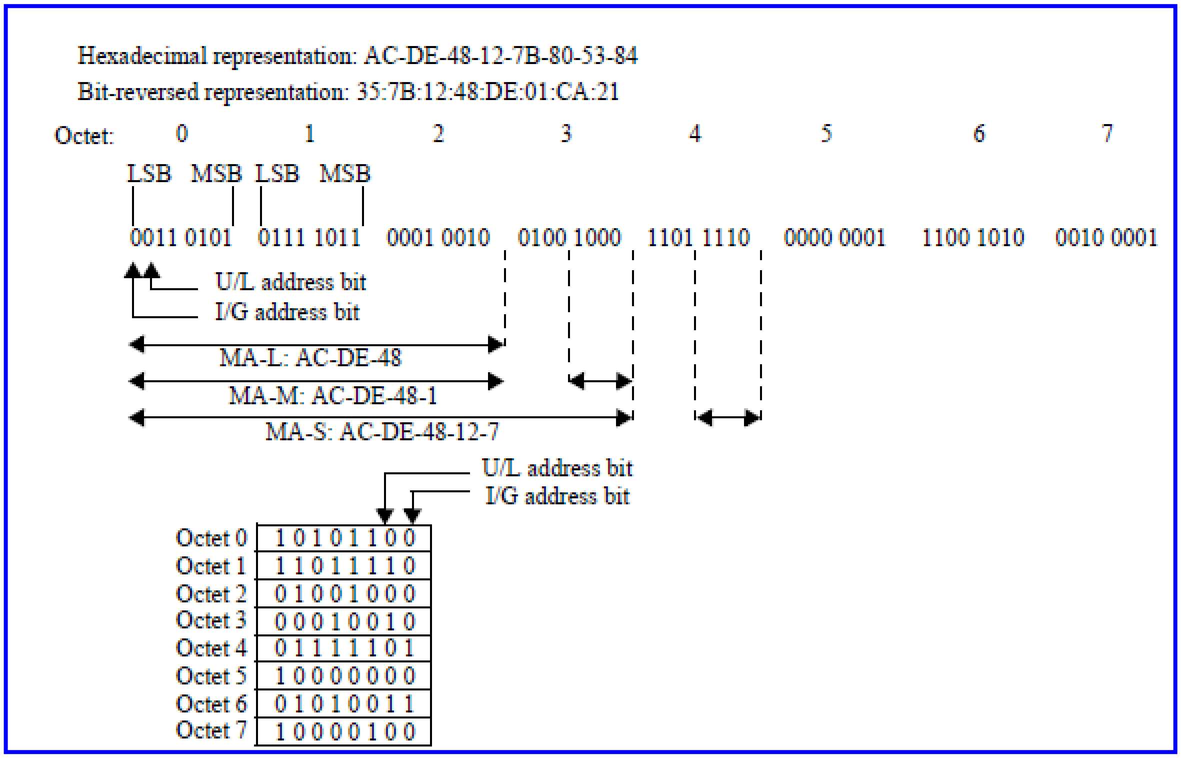
NOTE—The octet string AC-DE-48-12-7B-80 is used in this standard because it is clear when a bit pattern is reversed. This octet string could be in use and is not a reserved value. While AC-DE-48 is used as the same first 3 octets ~~3, 4, 5. This address, including its OUI, is used throughout this document as the basis for~~ for the examples of ~~LAN MAC addresses and protocol identifiers~~MA-L, MA-M, and MA-S, the first 3 octets are different for valid assigned RA values.

~~NOTE–The requirement for the use of 64-bit addresses in new applications is under consideration by the IEEE Registration Authority (RAC).~~

~~The standard representation of a 48-bit LAN MAC address is as a string of six octets, using the hexadecimal representation (3.1.8). In certain contexts associated with use of IEEE 802.5® frame formats, LAN MAC addresses may be represented using the alternative bit-reversed representation (3.1.2). See 9.5 for further specification relating to use of the bit-reversed representation.~~

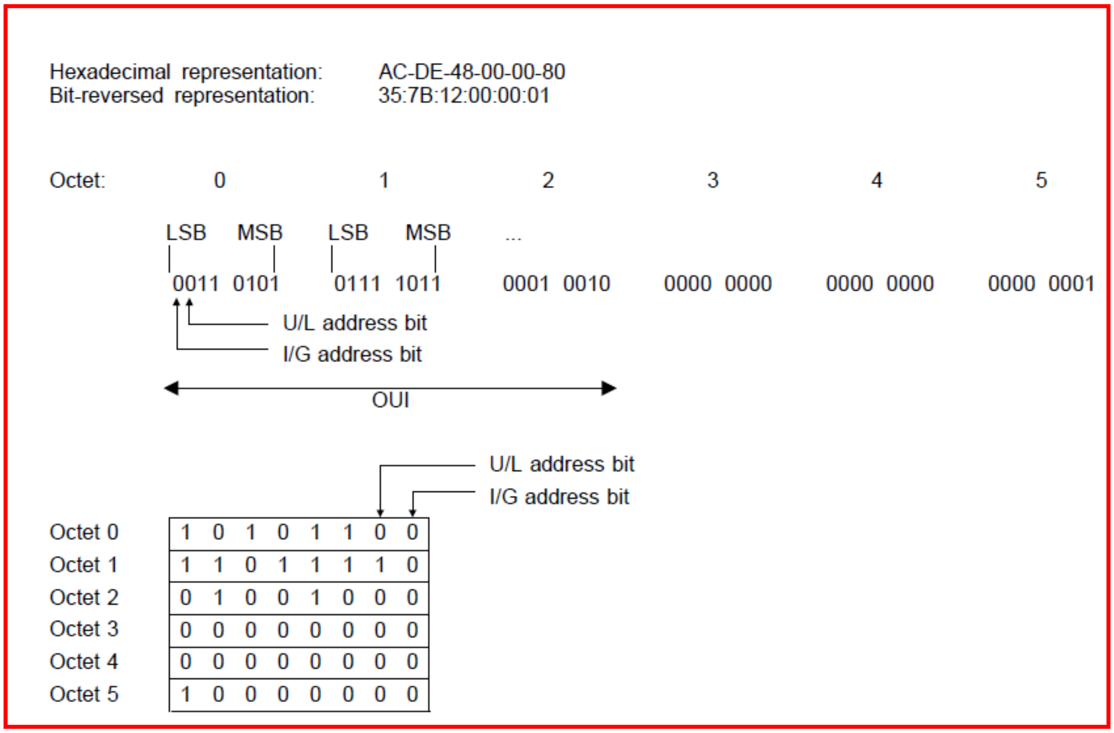
An example of an EUI-64 is illustrated in Figure 11.

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



(New)

Figure 11—Example EUI-64



~~(Deleted)~~

~~8—Universal address~~

~~The Individual/Group (I/G) address bit (LSB of octet 0) is used to identify the destination address as an individual address or a group address. If the I/G address bit is 0, it indicates that the address field contains an individual address. If this bit is 1, the address field contains a group address that identifies one or more (or all) stations connected to the LAN. The all-stations broadcast address is a special, predefined group address of all 1's.~~

~~The Universally or Locally administered (U/L) address bit is the bit of octet 0 adjacent to the I/G address bit. This bit indicates whether the address has been assigned by a local or universal administrator. Universally administered addresses have this bit set to 0. If this bit is set to 1, the entire address (i.e., 48 bits) has been locally administered.~~

8.2.3 Assignment by organizations

~~Varying the last 24 bits in the block of MAC addresses for a given OUI allows the OUI assignee approximately16 million unique individual addresses and 16 million unique group addresses that no other organization may assign (i.e., universally unique).~~ The IEEE ~~intends~~does not intend to assign additional ~~OUIs~~MA-Ls, MA-Ms, or MA-Ss to any organization unless the organization has exhausted ~~this address block. Therefore, it is important for the IEEE to maintain a single point of contact with each assignee to avoid complicating the assignment process.~~ use of the address block or blocks already assigned to that organization.

It is important to note that ~~in no way~~universal addresses created from MA-Ls, MA-Ms, or MA-Ss should ~~these addresses~~not be used for purposes that would lead to skipping large numbers of them (for example, as product identifiers for the purpose of aiding company inventory procedures). The IEEE asks that organizations not misuse the assignments of the ~~last 24~~remaining bits and thereby unnecessarily exhaust the block. There are sufficient identifiers to satisfy most needs for a long time, even in volume production; however, no address space is infinite.

The method that an assignee uses to ensure that no two of its ~~devices~~stations carry the same universal address ~~will, of course, depend on the assignment or manufacturing process, the nature of the organization, and the organization's philosophy.~~is not defined in this standard. However, the users of networks worldwide expect to have unique addresses. The ultimate responsibility for assuring that user expectations and requirements are met, therefore, lies with the organization offering such ~~devices~~stations.

8.2.4 Uniqueness of address assignment

~~An issue to be considered is the nature of the device to which uniqueness of address assignment applies.~~

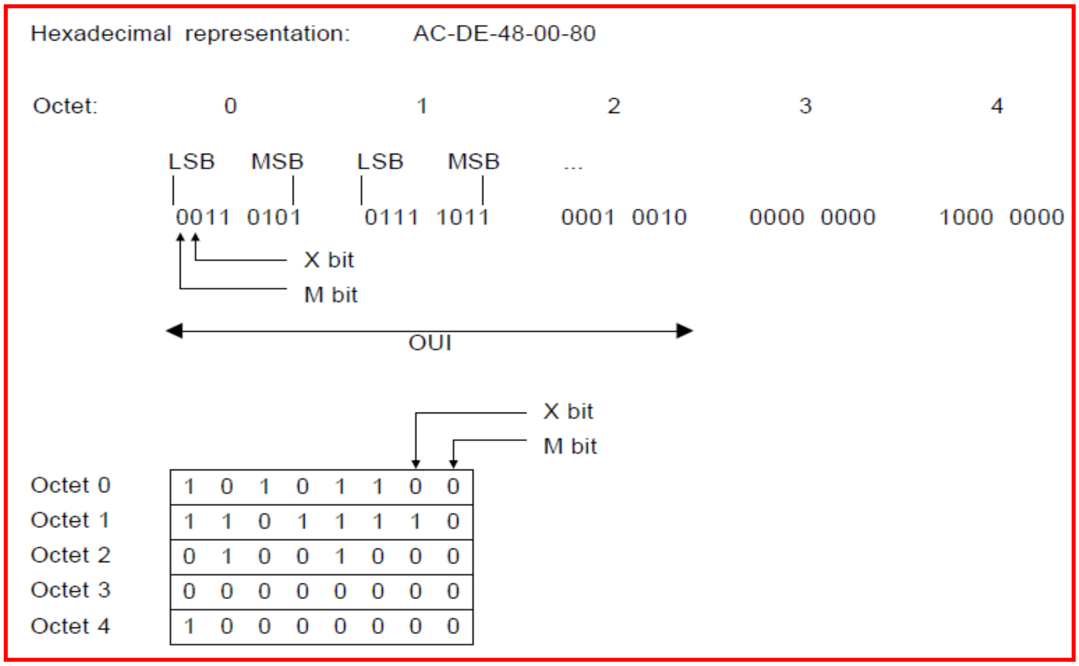
~~The~~ It is recommended ~~approach is for~~that each ~~device associated with a~~ distinct point of attachment to ~~a LAN to~~an IEEE 802 network have its own unique ~~MAC address.~~EUI-48 or EUI-64. Typically, therefore, ~~a LAN~~an IEEE 802 network adapter card (or, e.g., an equivalent chip or set of chips on a motherboard) should have one unique ~~MAC address~~EUI-48 or EUI-64 for each ~~LAN~~IEEE 802 network attachment that it can support at a given time.

NOTE—~~It is recognized that an alternative approach has gained currency in~~ While some ~~LAN~~ implementations~~, in which the device is interpreted as a complete computer system, which can~~ have ~~multiple attachments to different LANs. Under this interpretation, a~~ used a single ~~LAN MAC address is used~~EUI-48 or EUI-64 to identify all of the system's points of attachment to ~~the LANs in question. This~~IEEE 802 networks, this approach~~, unlike the recommended one,~~ does not ~~automatically~~inherently meet the requirements of IEEE ~~Std~~ 802.1D~~-1998~~™ MAC bridging.

8.3 ~~Protocol identifiers~~ Interworking with 48-bit ~~LAN~~and 64-bit MAC addresses

~~Clause 10 specifies the Subnetwork Access Protocol (SNAP), which permits multiplexing and demultiplexing of private and public protocols (see 10.1) among multiple users of a data link. An organization that has an OUI assigned to it may use its OUI to assign universally unique protocol identifiers to its own protocols, for use in the protocol identification field of SNAP PDUs (see 10.3).~~

~~The protocol identifier is five octets (40 bits) in length and follows the LLC header in a frame. The first three octets of the protocol identifier consist of the OUI in exactly the same fashion as in. The remaining two octets (16 bits) are administered by the assignee. In the protocol identifier, an example of which is shown in Figure 9, the OUI is contained in octets 0, 1, 2 with octets 3, 4 being assigned by the assignee of the OUI.~~



~~(Deleted)~~

~~Figure 9—Protocol identifier~~

In response to concerns that the EUI-48 space could be exhausted by the breadth of products requiring unique identifiers, 64-bit MAC addresses were introduced. Initially, new IEEE standards projects that did not require backward compatibility with EUI-48 were requested to use 64-bit MAC addresses. This led to some IEEE 802 standards adopting 64-bit MAC addressing, which cannot be bridged onto IEEE 802 networks that use 48-bit MAC addressing. The reason is that the bridging function in IEEE Std 802.1D and IEEE Std 802.1Q assumes that 48-bit MAC addresses are unique among all the connected networks. Truncating an 64-bit MAC address into an 48-bit field can lead to two stations having the same 48-bit value. Instead, traffic between 64-bit and 48-bit MAC addressed networks needs to be routed at a layer above the DLL.

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

8.4 Local MAC addresses

Local MAC addresses are 48-bit or 64 bit MAC addressees for which there is no guarantee that the MAC address is unique in all IEEE 802 networks. Local MAC addresses may be assigned any value that has the U/L bit set to indicate a local MAC addresses and an I/G bit value that indicates whether the MAC address is individual or group. Local MAC addresses need to be unique on a LAN or bridged LAN unless the bridges support VLANs with independent learning.

The I/G bit is set as described in 8.2.2.

NOTE— MA-L, MA-M, and MA-S assignments do not apply to local MAC addresses. Refer to the IEEE RA web site[14] for recommendations for management of the local MAC address space.

~~The standard representation of a protocol identifier is as a string of five octets, using the hexadecimal representation (3.1.8).~~

~~The LSB of the first octet of a protocol identifier is referred to as the M bit. All identifiers derived from OUIs assigned by the IEEE shall have the M bit set to 0. Values with the M bit set to 1 are reserved.~~

~~Protocol identifiers may be assigned universally or locally. The X bit of a protocol identifier is the bit of the first octet adjacent to the M bit. All identifiers derived from OUIs assigned by the IEEE will have the X bit set to 0 and are universally assigned. Values with the X bit set to 1 are locally assigned and have no relationship to the IEEE assigned values. They may be used, but there is no assurance of uniqueness.~~

[14] http://standards.ieee.org/develop/regauth.

8.5 Standardized group MAC addresses[15]

The previous subclauses described the assignment of individual and group MAC addresses, and protocol identifiers for public or private use by private organizations. There is also a need for standardized 48-bit and64-bit group MAC addresses to be used with standard protocols. The administration of these standardized48-bit and 64-bit group MAC addresses, including the procedure for application and a list of currently assigned values, is ~~defined in ISO/IEC TR 11802-2.~~described on the web pages for the IEEE RA[16]. These standardized group MAC addressees come from a block of universally administered ~~LAN MAC~~ addresses derived from ~~an OUI~~a MA-L that has been assigned by the IEEE for this purpose.

~~ISO/IEC 8802-5 also defines *functional addresses*, for use in Token Ring LAN environments to identify well-known functional entities. These addresses are a subset of the locally administered group MAC addresses, identified by having the 15 address bits that follow the I/G and U/L address bits set to zero. Certain values are used consistently throughout Token Ring LAN environments and, therefore, play a very similar role to standard group MAC addresses; these functional address values are also recorded in ISO/IEC TR 11802-2.~~

8.6 Bit-ordering and different MACs

~~NOTE—~~Throughout this subclause, considerations relating to the order of bit and/or octet transmission refer to the basic bit-serial model of transmission that applies to the representation of MAC frames at the boundary between the MAC ~~sublayer~~ and the ~~Physical layer; see 6.2.3~~PHY.

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

[16] http://standards.ieee.org/develop/regauth/grpmac.

8.6.1 General considerations

The transmission of data on IEEE 802.3®~~ and 802.4® LAN types~~ networks is represented~~ (6.~~, as described in 5.2.3, as occurring LSB first within each octet. This is true for the entire frame: ~~LAN MAC~~ source and destination address fields, MAC-specific fields (e.g., Length/Type field~~ in IEEE 802.3® LANs~~), and the MAC Information field.~~ (The MAC Information field is defined to be that part of the frame starting directly after the MAC header and ending immediately before the frame check sequence: e.g., LLC information, such as the Protocol Identification field, is contained in the MAC Information field.)~~

On some other ~~LAN types, for which IEEE 802.5® is here used as the typical example~~network types, each octet of the MAC Information field is represented as being transmitted MSB first. The ~~LAN MAC~~ source and destination address fields, however, are represented as being transmitted with the LSB of each octet first. Thus, the first bit transmitted is the I/G address bit, as ~~on~~ in IEEE 802.3® ~~and IEEE 802.4® LANs.~~ networks. For frames that originate within the MAC (e.g., MAC-embedded management frames), the ordering of bits within the MAC Information field is ~~defined~~specified by the MAC ~~specification—ISO/IEC 8802-5, etc~~standard.

For most purposes, the difference in the bit~~ orderings~~ ordering used to represent transmission of the octets of the MAC Information field is of no consequence, whether considered within a given MAC type, or across different MAC types. Each octet of user data is mapped to and from the appropriate ordering, symmetrically by the transmitting and receiving MAC entities. An unfortunate exception has occurred, however, where the octets concerned are those of a MAC address that is embedded, as user data, in the MAC Information field.

~~The consequences particularly affect the use of MAC addresses in mixed environments containing Token Ring LANs and non-Token Ring LANs.~~

~~The following subclauses describe the problem and some of the issues arising from it.~~

~~9.5.2 Illustrative examples~~

~~This subclause illustrates the various bit- and octet transmission scenarios that can occur, and it is intended as a basis for clarifying the issue of bit ordering for LAN MAC addresses across different MACs. Throughout, the examples make use of the OUI value AC-DE-48, introduced in 9.2.1. This three-octet value is considered in its two possible roles: as the first part of a five-octet protocol identifier, and as the first part of a six-octet LAN MAC address. The consistent representations of the OUI in its role as part of a protocol identifier are contrasted with the sometimes variable representations that apply to its role as part of a MAC address.~~

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

~~For the examples, the bit significance of an OUI in general is defined to be as in Figure 10.~~

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

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

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

~~(New)~~

~~**Figure 10—Bit significance of an OUI**~~

~~When transmitted on an IEEE 802.3® or IEEE 802.4® LAN (all data octets transmitted LSB first), the OUI portions of a protocol identifier and of a LAN MAC address appear as in Figure 11. When transmitted on an IEEE 802.5® LAN (data octets in the MAC Information field transmitted MSB first), the OUI portions of a protocol identifier, and of a LAN MAC address contained in a MAC Address field, appear as in Figure 12~~

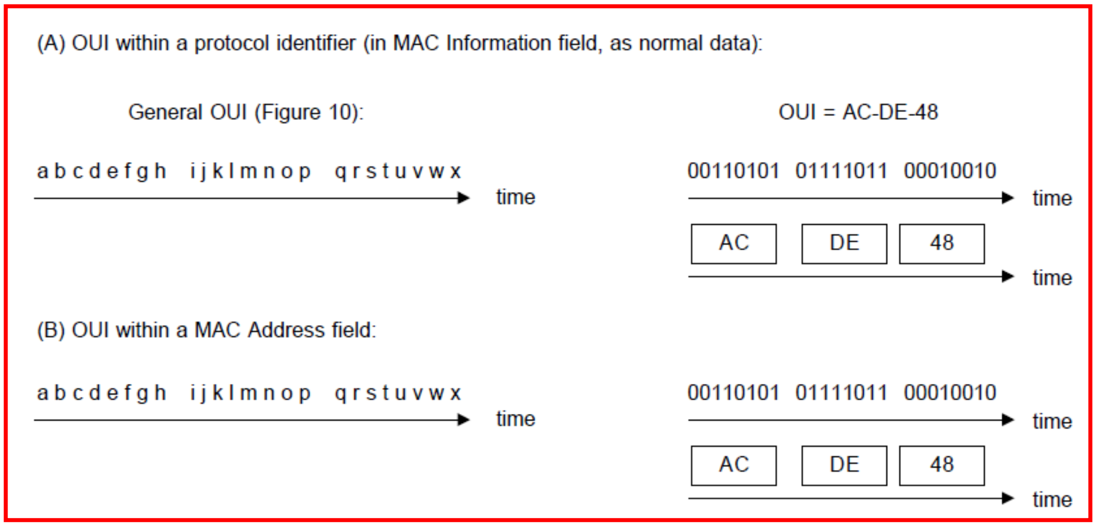
~~In some circumstances, it is necessary to convey LAN MAC addresses as data within MAC Information fields, e.g., as part of a management protocol or a Network layer routing protocol.~~

~~For LAN types in which Figure 11 applies, such as IEEE 802.3®, the bit ordering within the octets of a LAN MAC address conveyed as data is the same as both the ordering when the address appears in a MAC address field and the ordering for octets of nonaddress information (see Figure 13).~~

~~For LAN types in which Figure 12 applies, such as IEEE 802.5® and FDDI, there appears to be a choice of representations for MAC addresses conveyed as data, as follows:~~

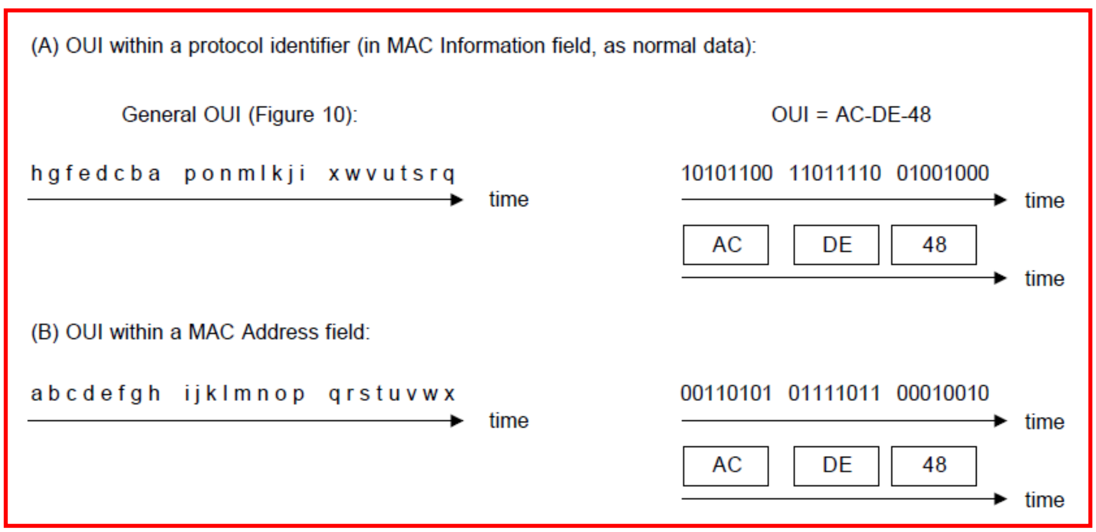
~~a) The octets of the MAC address can be treated like any other data octets and transmitted with the bit ordering of Figure 12 (A)~~

~~b) The bit ordering of Figure 12 (B) can be treated as a property of the MAC address rather than of the MAC address field as transmitted in MAC frames, and the MAC address octets can be transmitted with the bit ordering reversed compared with normal data octets~~



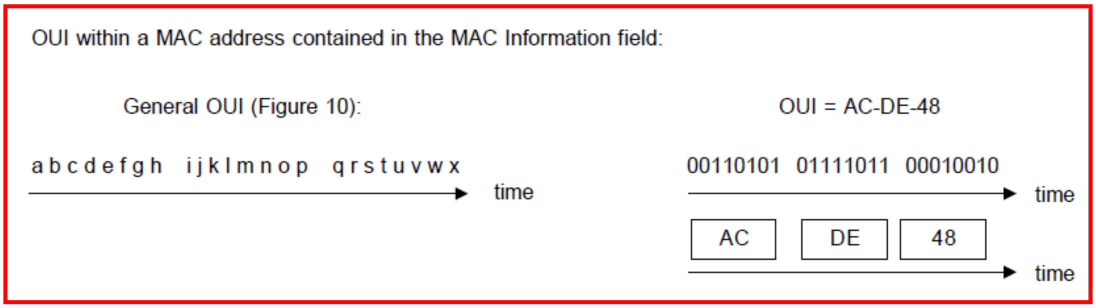
~~(Deleted)~~

~~Figure 11—IEEE 802.3®, etc., frame: Order of bit and octet transmission for an OUI~~



~~(Deleted)~~

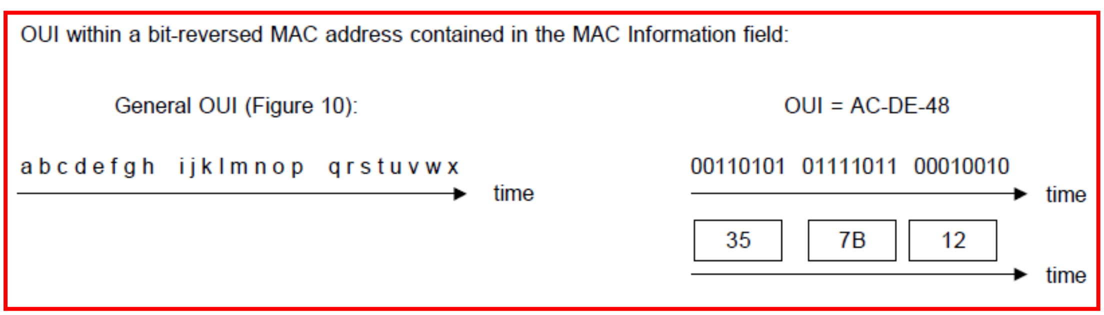
~~Figure 12—IEEE 802.5®, etc., frame: Order of bit and octet transmission for an OUI~~



~~(Deleted)~~

~~Figure 13—IEEE 802.3®, etc., frame: Order of bit and octet transmission for an OUI in aMAC address contained in a MAC Information field~~

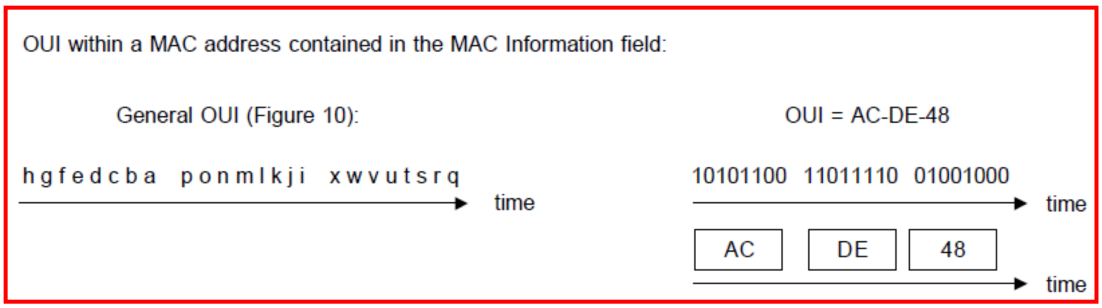
~~In the case of IEEE 802.5® Token Ring LANs, approach b) was adopted early in the development and deployment of Token Ring technology. This has the unfortunate consequence that applications operating in environments containing a mixture of LAN types have to handle different representations of MAC addresses, according to the environment in which the MAC address is to be used; see Figure 14.~~



~~(Deleted)~~

~~Figure 14—IEEE 802.5®, etc., frame: Order of bit and octet transmission for an OUI in aMAC address contained in a MAC Information field (noncanonical format)~~

~~For other LAN types in which Figure 12 applies, including, in particular, FDDI, approach a) was adopted (Figure 15), at least in environments involving interconnection with IEEE 802.3®, and so on, LANs. However, where FDDI LANs are used in an IEEE 802.5® Token Ring environment, approach b) is used for consistency with the interconnected IEEE 802.5® LANs. In a mixed environment of FDDI, IEEE 802.3® and IEEE 802.5® LANs, frames constructed according to both approaches can occur on the FDDI LANs, at least; some care is needed in managing such an installation to avoid confusion between the formats.~~



~~(Deleted)~~

~~Figure 15—FDDI frame: Order of bit and octet transmission for an OUI in a MAC address contained in a MAC Information field (canonical format)~~

~~In Figure 11 through Figure 15, it can be seen that the interpretation of OUI bits as octet values is consistent in every case except Figure 14, in which the octet values are bit reversed. This reversal of the bit order applies only to all six octets (not just the OUI) of a MAC address placed in the MAC Information field of a frame by a protocol that uses the Token Ring Bit reversed view of MAC addresses derived from Figure 12 (B). Frames containing, or possibly containing, such MAC addresses are described as having noncanonical format. Frames (on any LAN or LAN type) that cannot contain such MAC addresses are described as having canonical format.~~

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

8.6.2 Recommendation

Designers of protocols that operate above the ~~Data Link layer~~DLL are strongly recommended to avoid specifying new protocols that result in frames of noncanonical format~~, except where such a protocol is clearly an extension of existing practice in a strongly Token Ring environment~~.

9. Protocol identifiers~~discrimination above the MAC sublayer: Subnetwork Access Protocol (SNAP) and Ethernet types~~

9.1 Introduction

~~This clause outlines the mechanisms for the coexistence of multiple standard, public, and private network layer protocols within a single 802® station (10.2). It then describes the functions, features, and protocol format conventions for public and private protocols sharing a single LSAP (10.3). All public and private protocols using the IEEE 802® reserved LLC address assigned for public and private protocol use shall conform to this standard.~~

~~This clause further describes Ethernet types used to identify different protocols operating over the alternative Ethernet sublayer (10.4), and it describes the standard encapsulation specified for conveyance of such Ethernet-supported protocols on IEEE 802® LANs that do not intrinsically support an Ethernet sublayer (10.5).~~

~~A standard protocol is defined to be a protocol whose specification is published and known to the public but controlled by a standards body. A public protocol is defined to be a protocol whose specification is published and known to the public, but controlled by an organization other than a formal standards body. A private protocol is defined to be a protocol whose use and specification are controlled by a private organization.~~

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

— ~~By providing for~~ The coexistence of multiple network layer protocols

— The migration of existing ~~LANs~~networks to future standard protocols~~ is facilitated, and multiple~~

— The accommodation of future higher layer protocols~~ are more easily~~

~~10.2 Basic concepts~~

~~10.2.1 Coexistence of multiple protocols~~

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

~~The following subclauses specify mechanisms for use when the LLC sublayer is present above the MAC layer, and when the alternative Ethernet sublayer is present above the MAC sublayer.~~

~~10.2.2 Multiple protocols above the LLC sublayer~~

~~Standard Network~~Various network and higher layer protocols have been assigned reserved ~~LLC~~LPD addresses or EtherTypes, as recorded ~~in ISO/IEC TR11802-1.~~by the IEEE RA[17]. These addresses permit multiple ~~standard network layer~~ protocols to coexist at a single MAC station.~~ One half of the LLC address space is reserved for such assignment.~~

[17] More information can be found at http://standards.ieee.org/develop/regauth/llc.

~~Other protocols are accommodated in two ways. One way is by local assignment of LSAPs, for which the other half of the LLC address space is available. Thus, users can agree to use locally assigned LSAPs for either an instance of communication or a type of communication.~~

~~The second way is through the use of a particular reserved LLC address value that has been assigned for use in conjunction with the Subnetwork Access Protocol (SNAP, specified in 10.3), which provides for multiplexing and demultiplexing of public and private protocols among multiple users of a data link.~~

~~10.2.3 Multiple protocols above the Ethernet sublayer~~

~~The Ethernet MAC frame format includes a 16-bit type value, whose function is to identify the particular protocol pertaining to the user data contained in the frame. See 10.4 for further details.~~

~~10.3 Subnetwork Access Protocol~~

~~10.3.1 SNAP address~~

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

~~The SNAP address identifies, at each MSAP, a single LSAP for standard, public, and private protocol usage. To permit multiple public and private network layer protocols to coexist at one MSAP, each public or private protocol using SNAP must employ~~ This clause describes the protocol identifiers used for the LPD and EPD methods as well as a protocol identifier ~~that enables SNAP to discriminate among these protocols~~based on OUI-36.

~~10.3.2 SNAP PDU format~~

~~Each SNAP PDU~~The EPD method shall ~~conform to~~ be the ~~format shown in Figure 16 and shall form the entire content of the LLC information field.~~

~~In Figure 16, the Protocol Identification field is a five-octet field containing a~~ primary specified means for protocol ~~identifier whose format and administration are as described in 9.3. The Protocol Data field is a field whose length, format, and content are defined by a public or private protocol specification. Each public or private protocol begins its PDU format with the Protocol Identification field, which shall contain the protocol identifier assigned to the protocol.~~identification at the LLC sublayer in IEEE 802 standards developed after January 2011[18], excluding amendments to existing standards.

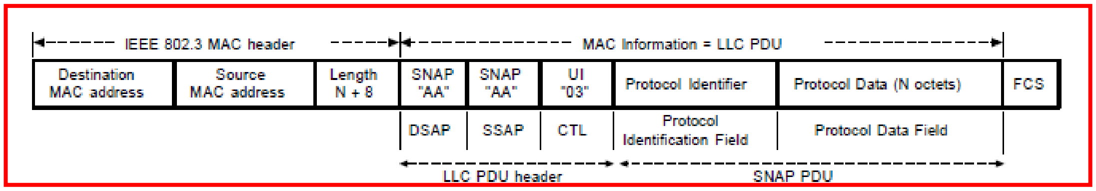
Octet: 0	...	4	5	...	(N+4)
Protocol Identification (5 octets)			Protocol Data (N octets)		

~~(Deleted)~~

~~**Figure 16—SNAP PDU format**~~

~~Figure 17 illustrates how a SNAP PDU appears in a complete MAC frame (the IEEE 802.3® MAC format is used for the example). The LLC 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 LLC PDU types may also be used with SNAP.~~

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



~~(Deleted)~~

~~**Figure 17—SNAP PDU in IEEE 802.3® MAC frame**~~

9.2 EtherTypes

9.2.1 Format, function, and administration

~~The~~ Protocol discrimination performed by the EPD method is based on EtherTypes. For example, the value of the Type/Length field in the IEEE 802.3® MAC frame format ~~is compatible with~~directs the ~~alternative Ethernet MAC frame format, in~~protocol parser into the ~~sense that~~LPD HLPDE if the value is less than 1536. This allows frames of both formats ~~can~~to be freely intermixed on a given ~~LAN~~IEEE 802 network and at a given ~~LAN~~ station. ~~The service provided~~

EtherType protocol identification values are assigned by ~~use of~~ the ~~Ethernet frame format differs from~~IEEE RA[19] and are used to identify the ~~ISO/IEC 15802-1 MAC service in~~ protocol that ~~there~~ is ~~a 16-bit type value associated with each frame transferred, and that~~to be invoked to process the ~~minimum amount of MAC sublayer~~ user data ~~transferred is 64 octets~~ in the frame.

An ~~value~~ EtherType is a sequence of 2 octets, interpreted as a 16-bit numeric value with the first octet containing the most significant 8 bits and the second octet containing the least significant 8 bits. Values in the 0–1535 range are not available for use in order to retain legacy compatibility with Length field based protocols, e.g., IEEE Std 802.3.

[19] More information on EtherTypes can be found on the IEEE RA web site, http://standards.ieee.org/develop/regauth/ethertype/.

~~The function~~Examples of ~~the Ethernet type value is~~ EtherTypes are 0x0800 and 0x8DD, which are used to identify ~~the protocol that is~~ IPv4 and IPv6, respectively.

It is strongly recommended when designing new protocols to be ~~invoked to process the user data in the frame~~identified by an EtherType, that fields are defined to provide for subtyping. The format used for subtyping in a protocol described in 9.2.3 is recommended.

9.2.2 EtherTypes for prototype and vendor-specific protocol development

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

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

a) Two EtherType values, known as the Local Experimental EtherTypes, as specified in 9.2.3, assigned, as the name implies, for experimental use within a local area

b) A single EtherType value, known as the OUI Extended EtherType, as specified in 9.2.4, assigned for the identification of vendor-specific protocols

The values of the Local Experimental EtherTypes and the OUI Extended EtherType are listed in Table 2.

Table 2—Assigned EtherType values

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

(New)

9.2.3 Local Experimental EtherTypes

The Local Experimental EtherTypes are intended for use in conjunction with experimental protocol development within a privately administered development network, for example, within an experimental network that has no wide area connectivity. Within that network, a local administrator is free to use a Local Experimental EtherType and to assign subtypes for protocol development purposes. However, by virtue of the way these EtherTypes are intended to be used, the following practical and administrative constraints apply to their use:

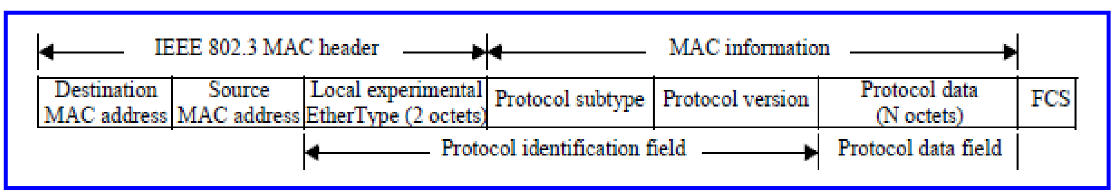
a) Since the format for protocols using the Local Experimental EtherTypes does not contain a means to identify the administrative domain, it might not be possible to identify the protocol of a frame if protocols developed within different administrative domains using Local Experimental EtherTypes are 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 12 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.



(New)

Figure 12—Example of an IEEE 802.3 frame carrying the Local Experimental EtherType

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

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

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

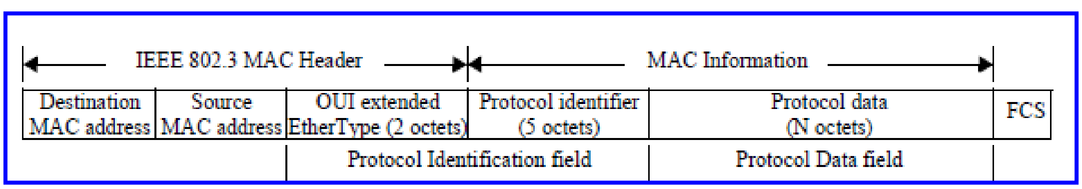
9.2.4 OUI Extended EtherType

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

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

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

NOTE—The 2 octets of the protocol identifier that are administered by the OUI assignee can be used in any way that the assignee chooses; however, as OUIs are a finite resource, it is advisable not to choose an allocation approach that is wasteful, as would be the case, for example, if the assignee chose to use these 2 octets to encode a length value.



(New)

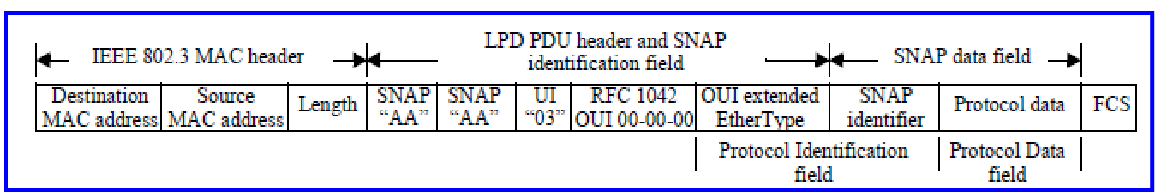
Figure 13—IEEE 802.3 frame with the OUI Extended EtherType encoded in the Length/Type field

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

As discussed in 9.2.3, it is good protocol development practice to use a protocol subtype, along with a protocol version identifier in order to avoid having to allocate a new protocol identifier when a protocol is revised or enhanced. Users of the OUI Extended EtherType are, therefore, encouraged to include protocol subtype and version information in the specification of the protocol data for their protocols.

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

As the OUI Extended EtherType is a normal EtherType value, it is possible to use the encoding described in 9.4 to carry its value within an LPD PDU, using a SNAP identifier with the IETF RFC 1042 [B1] OUI. Figure 14 shows the format of an IEEE 802.3 frame carrying the OUI Extended EtherType encoded in this way. In this case, it would be more appropriate to use the SNAP identifier directly (i.e., omit the IETF RFC1042 OUI and OUI Extended EtherType fields shown in Figure 14); however, this is a valid encoding of theOUI Extended EtherType that can result from the application of the encapsulation described in 9.4.



(New)

Figure 14—IEEE 802.3 frame with the OUI Extended EtherType encoded in an LPD PDU

9.3 OUI and OUI-36 as protocol identifiers

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

The LSB of the first octet of an OUI, as shown in Figure 15, or OUI-36, as shown in Figure 16, used as a protocol identifier is referred to as the M bit. All OUI and OUI-36 identifiers assigned by the IEEE have the M bit set to zero. Values with the M bit set to one are reserved.

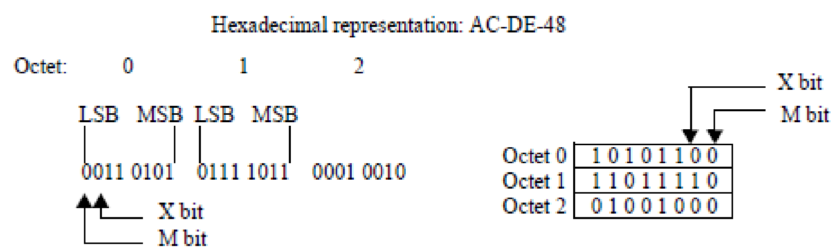
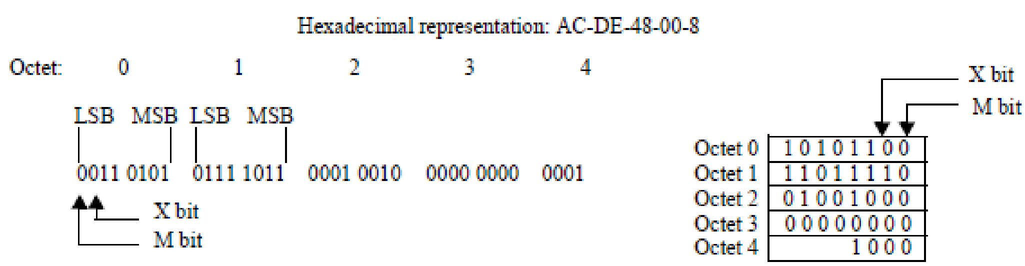


Figure 15—Format of an OUI used as protocol identifier



(New)

Figure 16—Format of an OUI-36 used as a protocol identifier

~~As with OUIs, administration of Ethernet types was originally undertaken by the Xerox Corporation, and it is now the responsibility of the IEEE using procedures defined by the IEEE RAC (see Clause 9). All assignments of Ethernet types made by the predecessor administration remain in effect under the IEEE's administration.~~

The X bit of a protocol identifier is the bit of the first octet adjacent to the M bit. All OUI and OUI-36 identifiers assigned by the IEEE with the X bit set to zero may also be used to create EUI-48 and EUI-64 addresses. An OUI or OUI-36 identifier assigned by the IEEE with the X bit set to one shall only be used as an OUI or OUI-36 protocol identifier, respectively. Any MAC address created with an OUI or OUI-36 with the X bit set to one are, by definition, locally administered addresses; they may be used but there is no assurance of uniqueness.

9.4 Encapsulation of Ethernet frames ~~over LLC~~with LPD

This subclause specifies the standard method for conveying Ethernet frames across IEEE 802® ~~LANs~~ networks that offer only the LPD function and not the EPD function in the LLC sublayer~~, and not the Ethernet sublayer, directly above the MAC sublayer.~~.

An Ethernet frame conveyed on an ~~LLC~~LPD-only ~~LAN~~IEEE 802 network shall be encapsulated in a SNAP ~~PDU~~data unit contained in an ~~LLC~~ LPD PDU of type UI, as follows ~~(see Figure 18):~~:

a) The Protocol Identification field of the SNAP ~~PDU~~data unit shall contain a ~~protocol~~ SNAP identifier in which

1) The three OUI octets each take the value zero.

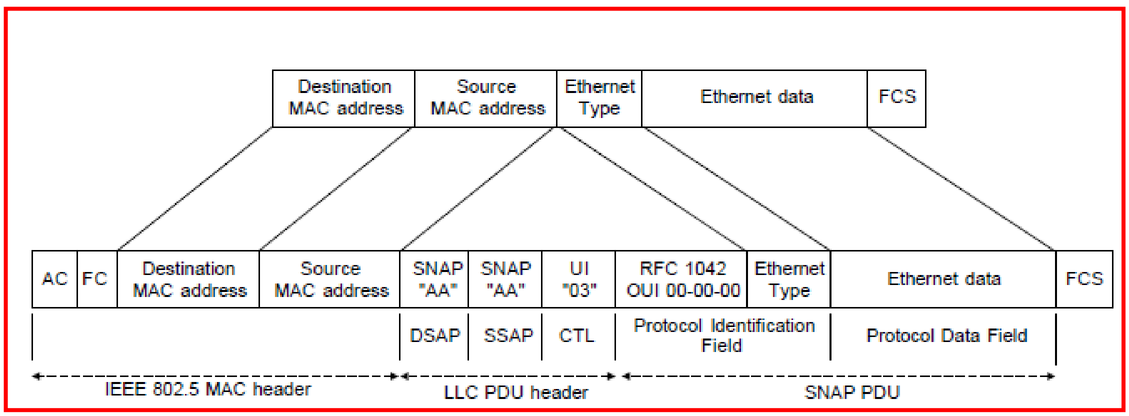
2) The two remaining octets take the values, in the same order, of the 2 octets of the Ethernet frame's EtherType.

b) The Protocol Data field of the SNAP ~~PDU~~data unit shall contain the user data octets, in order, of the Ethernet frame.

c) The values of the Destination MAC Address field and Source MAC Address field of the Ethernet frame shall be used in the Destination MAC Address field and Source MAC Address field, respectively, of the MAC frame in which the SNAP ~~PDU~~ data unit is conveyed.

NOTE—This encapsulation was originally specified in IETF RFC 1042 [B1], which contains recommendations relating to its use. Further recommendations are contained in IETF RFC 1390 [B2].

~~2—ISO/IEC TR 11802-5 (IEEE Std 802.1H-1997™) contains recommendations for bridges, addressing the conse- quences of certain problems that arose from differing interpretations of RFC 1042.~~



~~(Deleted)~~

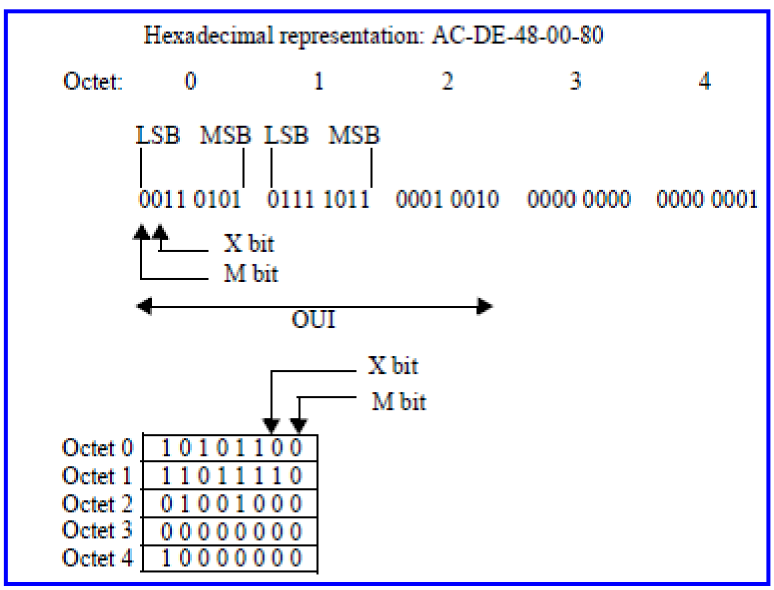
~~**Figure 18—Ethernet frame SNAP-encapsulated in IEEE 802.5® frame**~~

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 assigned to it may use its OUI to assign universally unique 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 in exactly the same fashion as in EUI-48. The remaining 2 octets are administered by the assignee. In the SNAP identifier, an example of which is shown in Figure 17, the OUI is contained in octets 0, 1, 2 with octets 3, 4 being assigned by the assignee of the OUI.



(New)

Figure 17—SNAP identifier

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

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

SNAP identifiers may be assigned universally or locally. The X bit of a SNAP identifier is the bit of the first octet adjacent to the M bit. All universally assigned SNAP identifiers derived from OUIs have the X bit set to zero. SNAP identifiers with the X bit set to one are locally assigned and have no relationship to the protocol identifiers assigned by the IEEE RA. They may be used, but there is no assurance of uniqueness.

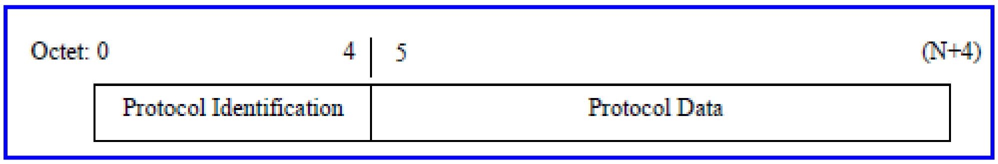
9.5.2 SNAP address

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

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

9.5.3 SNAP data unit format

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

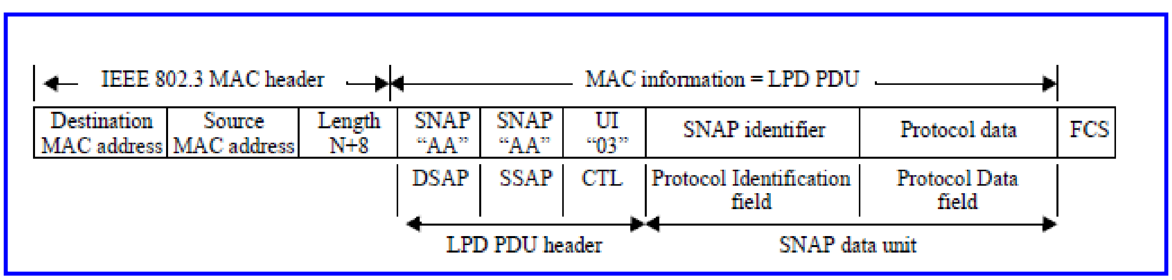


(New)

Figure 18—SNAP data unit format

In Figure 18, the Protocol Identification field contains a SNAP identifier whose format and administration are as described in 9.5.1. The Protocol Data field is a field whose length, format, and content are specified by a public or private protocol specification.

Figure 19 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.



(New)

Figure 19—SNAP data unit in IEEE 802. 3 MAC frame

10. Allocation of OID values in IEEE 802 standards

10.1 General

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

10.2 OIDs and ISO standards

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

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

iso (1)

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

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

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

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

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

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

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

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

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

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

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

10.3 The OID hierarchy for IEEE 802 standards

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

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

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

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

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

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

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

and the value used for IEEE 802.11™ standards is:

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

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

It is the responsibility of each working group to ensure that any values that are allocated to the fifth and subsequent arcs are documented, in a manner that ensures that the same OID value cannot be assigned to two different objects. In the IEEE 802.1 Working Group, this has been achieved in the past by placing tables of OID allocations in an annex within the standard concerned[20]; in the IEEE 802.3 Working Group, a master spreadsheet of allocated OID values is maintained by the chair and posted on the working group's website. For future allocations, adopting a master spreadsheet approach is appropriate.

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

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.

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

10.5 Migration from previous OID allocations

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

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

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

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

— If migration is desired, there is no requirement to remove the old OID values[21]. Indeed, this is not permitted for objects in SNMP MIB modules that are not obsolete, as specified in IETF RFC 2578, nor is it permitted to associate such objects with more than one OID value. Instead, new definitions are required to be created and registered under the desired OID tree[22].

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

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

~~11. ISLAN and MAN support for isochronous bearer services~~

~~In addition to the mandatory LAN and MAN services described so far, some IEEE 802® LANs and MANs, notably, ISO/IEC 8802-9 and ISO/IEC 8802-6, also make provision for supporting isochronous bearer services. Isochronous bearer services are distinctive relative to packet services such as the MAC service and LLC, in that they maintain a flow of service data units at constant time intervals from a transmitter to a receiver for the duration of a service. In almost all circumstances, such isochronous bearer services are carried over duplex bidirectional connections thereby providing effective and efficient means of supporting the ubiquitous WAN voice telephony services. IEEE 802® ISLANs and MANs provide isochronous bearer services designed to interwork readily with these WAN services as standardized by ITU-T, in particular, as defined in the I series of ITU-T Recommendations.~~

~~NOTE—Use of an end-to-end physical layer isochronous bearer service, which intrinsically delivers data with timing preserved, needs to be distinguished from use of a packet-based service for conveyance of time-sensitive data such as voice or video. The latter approach can be successful, given adequate bandwidth in the LANs and bridges, and provided that bridges do not introduce the possibility of excessive delay for packets carrying the time-sensitive data.~~

~~11.1 Key concepts~~

~~Applications requiring sustained periodic use of end-to-end network bandwidth are common. Two of the IEEE 802® standards address this requirement; both the ISO/IEC 8802-9 ISLAN standard and the optional isochronous service on an ISO/IEC 8802-6 Distributed Queue Dual Bus (DQDB) MAN use synchronously cyclic methods to ensure precise timing of the acceptance, transfer, and delivery of continuous streams of information. This applies whether or not asynchronous packet services are also provided concurrently.~~

~~The ISLAN employs a time-division multiplex (TDM) bearer mechanism within the Physical layer. The isochronous service on a DQDB MAN uses a Pre-Arbitrated function to ensure precisely timed access to the media, as distinct from the packet service Queued Arbitrated function. In each case, this permits the support and delivery of a plurality of transparent isochronous service channels, the provision of an octet alignment signal for these channels, and a facility to provide and accept these precise timing signals. It is the provision of the timing signal that principally distinguishes the isochronous services from the asynchronous packet services that are provided from the ISLAN Physical layer.~~

~~Both methods for providing isochronous bearer services require the prior establishment of a connection for each isochronous information flow. For the DQDB MAN isochronous services, the mechanisms used for establishing and clearing connections are left outside of the scope of the IEEE 802® Standard. For ISLAN, see 11.4 below for an overview of the mechanisms used.~~

~~11.2 Applications~~

~~Applications for isochronous bearer services include the following:~~

— ~~PBX interconnections at DS1 (1.544 Mbit/s) or E1 (2.048 Mbit/s) rates~~

— ~~Low (384 kbit/s) to medium (44.2097 Mbit/s) bandwidth constant bit-rate compressed video~~

— ~~Channels with bandwidth in multiples of 56 or 64 kbit/s for conveyance of voice and audio~~

— ~~Multimedia combinations of these along with data services~~

~~Multimedia applications can require simultaneous, integrated use of two or more of these audio/voice, video, text, and graphics information streams. This can require the conveyance over common bearer channels of multiple isochronous and bursty information streams, in distinct channels with specific timing relationships. This provides the main rationale for incorporating isochronous services in LANs and MANs.~~

~~The provision of isochronous (TDM bearer) services enables direct interworking with a WAN network such that the access unit or hub (LAN/WAN interworking unit) can forward information in its native form, so that ISLAN terminals and access units do not have to provide gateway functions to transform the user information streams. In addition, the provision of isochronous bearer services greatly reduces the latency as information is queued/dequeued at the Physical service interface. This is of value in meeting established norms of loop delay on end-to-end connections for many human interactive services.~~

~~Typical isochronous services include the following:~~

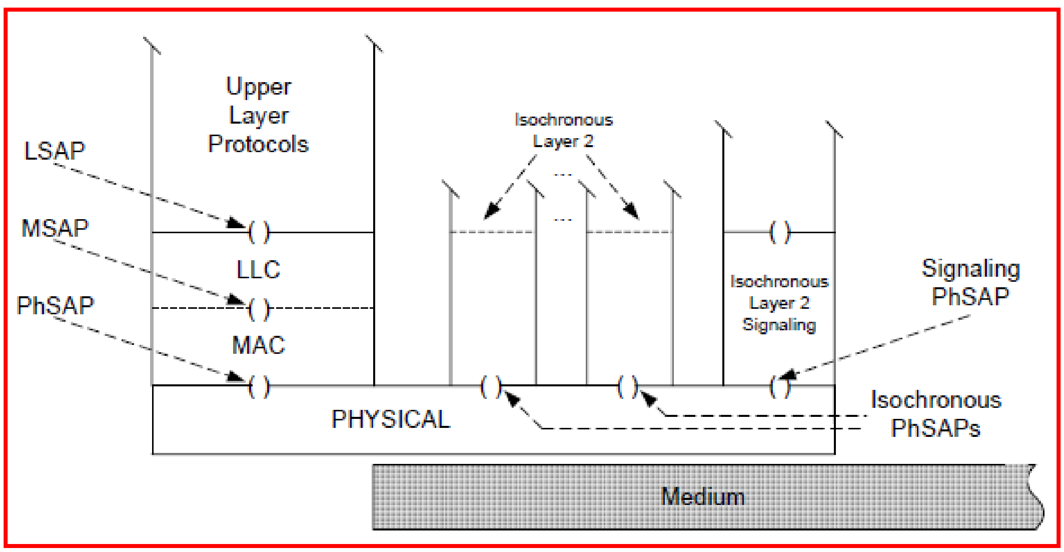
- ~~Unrestricted 64 kbit/s information transfer~~
- ~~Restricted 56 kbit/s information transfer~~
- ~~Synchronous data~~
- ~~Facsimile data~~
- ~~Wideband video and image transfer~~

~~The ISO/IEC 8802-9 ISLAN is specifically designed to provide concurrent support for LLC conformant packet services and narrowband ITU-T conformant ISDN services, both packet and isochronous, as defined in ITU-T I-series Recommendations.~~

~~11.3 Isochronous service access points and PhSAPs~~

~~The ISLAN and DQDB MAN standards both support concurrent packet and isochronous services within the Physical layer by means of convergence functions. In both cases, there is therefore a need for explicit identification of the distinct packet and isochronous channels provided over the common media supporting the ISLAN or MAN. In addition, both offer support for multiple isochronous bearer channels, and thus, there is a need to distinguish among multiple Physical service connections.~~

~~In the ISLAN standard, multiple PhSAPs are used to provide for the plurality of connections at the Physical service boundary, and for access by the user to the Physical-layer services for packet transfer and for D channel signaling (see Figure 19). For the DQDB MAN isochronous services, Connection Endpoint (CEs) identifiers are used for a similar purpose.~~



~~(Deleted)~~

~~Figure 19—ISLAN RM (end station)~~

~~PhSAPs and CEs are the architectural mechanism by which symbol streams are passed to the Physical service provider by the Physical service user, and to the Physical service user by the Physical service provider. The distinction of different PhSAPs at a single ISLAN Physical service boundary is required because that service boundary is used simultaneously to provide both packet-mode and (multiple) circuit-mode Physical services.~~

~~It is a function of the layer management of the PHY multiplexing sublayer to provide each Physical service user with both the information stream and a channel identifier that is mapped onto the PhSAP relevant to the service provided to that user.~~

~~11.4 ISLAN signaling~~

~~The ISLAN standard provides for direct interworking with ITU-T conformant ISDN I.series Recommendations. These require means of establishing, maintaining, and disestablishing end-to-end connections across (in the ISLAN case) both the ISLAN and intervening WAN. To this end, ISO/IEC 8802-9 includes specifications for extensions to the ITU-T I- and Q-series signaling protocols carried in a signaling-specific D channel. This is a packet-based protocol, but to achieve interworking with the ITU-T Recommendations, it is distinct from the LLC packet service provided over ISLAN.~~

~~The signaling service provided by the protocols carried in the D channel permits negotiation of end-to-end network resources such that a guaranteed service can be provided to the users of an end-to-end isochronous channel. Thus, the ISLAN management signalling entity is responsible, as a management agent, for performing the following tasks:~~

— ~~Negotiation of bandwidth (configuration) management, fault management, performance management, and security management of the access link between device and hub~~

— ~~Negotiation of service provisioning over the local ISLAN interface in order to access the WAN based ISDN services~~

~~The ISLAN signaling message elements are provided in compliance with international (ITU-T) network signaling methods with appropriate protocol extensions.~~

Annex A

(informative)

Bibliography~~(Additional references for LAN/MAN-related standards)~~

~~A.1 General LAN/MAN standards and specifications~~

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] IETF RFC 1042, A Standard for the Transmission of IP Datagrams over IEEE 802 ~~®~~Networks. Postel, J., and J. Reynolds, Feb. 1988.[23] ~~.~~ ~~[7]~~

[B2] IETF RFC 1390, Transmission of IP and ARP over FDDI Networks. Katz, D., Jan. 1993.

[B3] IETF RFC 2579, STD 58, Textual Conventions for SMIv2. McCloghrie, K., D. Perkins, J. Schoenwaelder, J. Case, M. Rose, and S. Waldbusser, Apr. 1999.

[B4] IETF RFC 2580, STD 58, Conformance Statements for SMIv2. McCloghrie, K., D. Perkins, J. Schoenwaelder, J. Case, M. Rose, and S. Waldbusser, Apr. 1999.

[B5] IETF RFC 3411, STD 62, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.

~~[7]Internet RFCs are available from the Internet Engineering Task Force on the World Wide Web browser at http://www.ietf.org/rfc/rfcnnnn.txt (where nnnn is the four-digit RFC number, padded with leading zeros if necessary). For more infor- mation, call the IETF secretariat at +1-703-620-8990.~~

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

[B6] IETF RFC 5677, IEEE 802.21 Mobility Services Framework Design (MSFD). Melia, T., G. Bajko, S. Das, N. Golmie, and J. C. Zuniga, Dec. 2009.

[B7] ISO/IEC 7498-1:1994, Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model.~~[1]~~

~~[1] ISO/IEC publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse (http://www.iso.ch/). ISO/IEC publications are also available in the United States from Global Engineering Documents, 15 Inverness Way East, Englewood, Colorado 80112, USA (http://global.ihs.com/). Electronic copies are available in the United States from the American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (http://www.ansi.org/).~~

Annex B

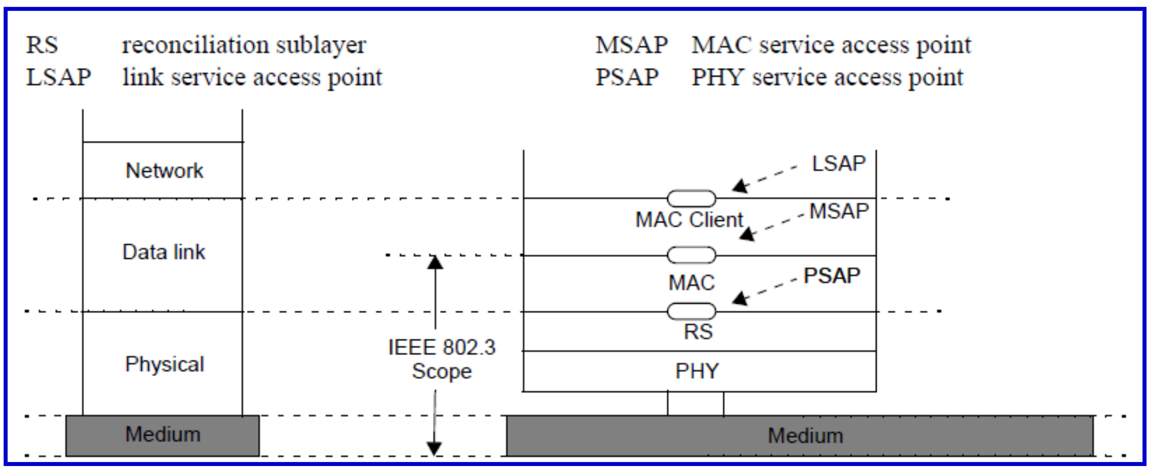
(informative)

RMs for IEEE 802 standards

B.1 IEEE 802.3 RMs

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

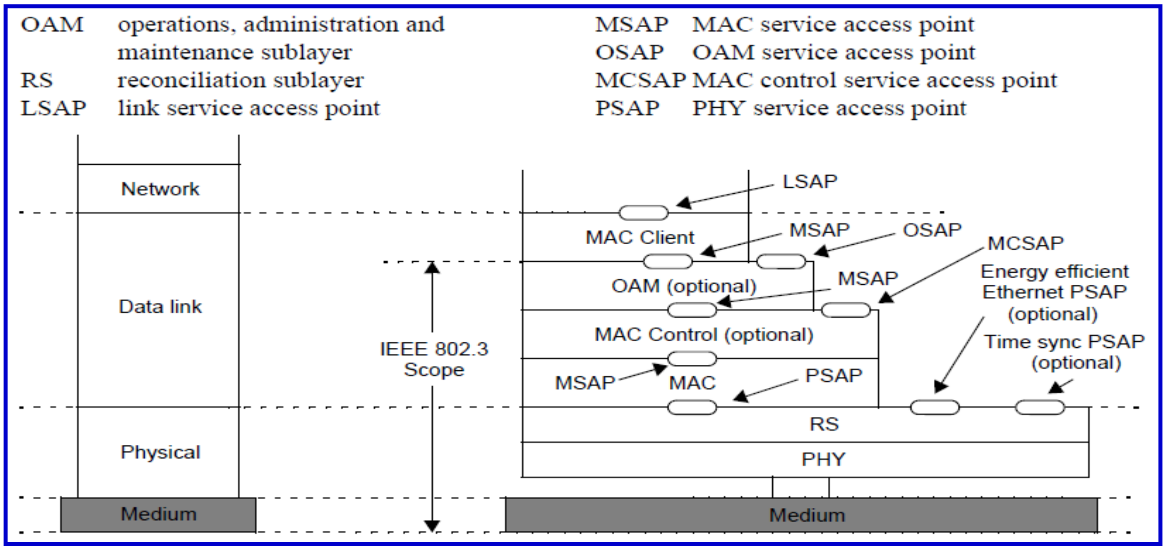
The basic RM for IEEE 802.3 stations without optional sublayers is illustrated in Figure B.1.



(New)

Figure B.1—Basic RM for IEEE 802.3 stations

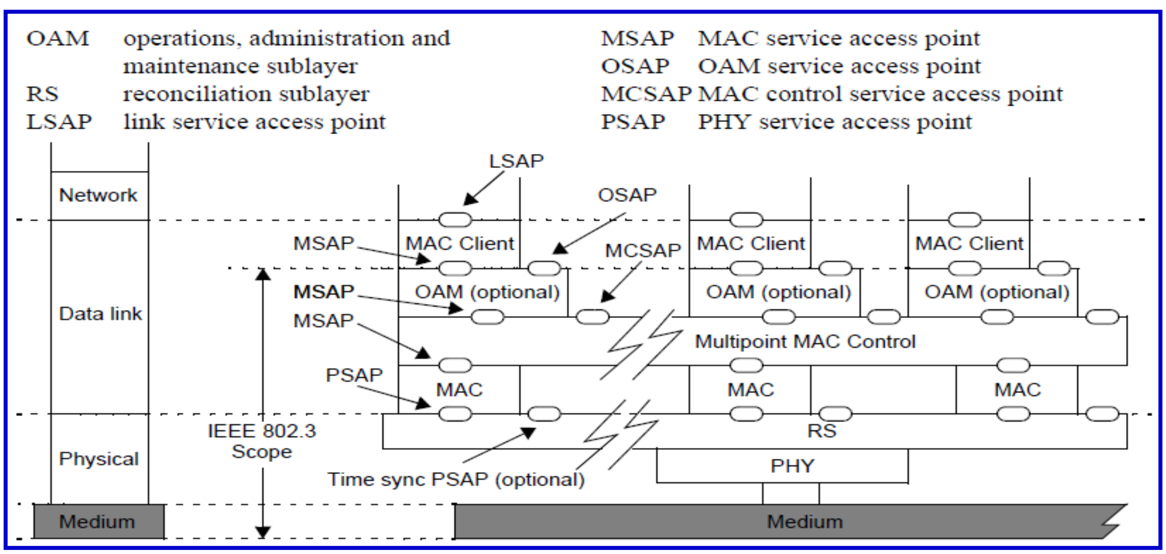
The RM for IEEE Std 802.3 is illustrated in Figure B.2.



(New)

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

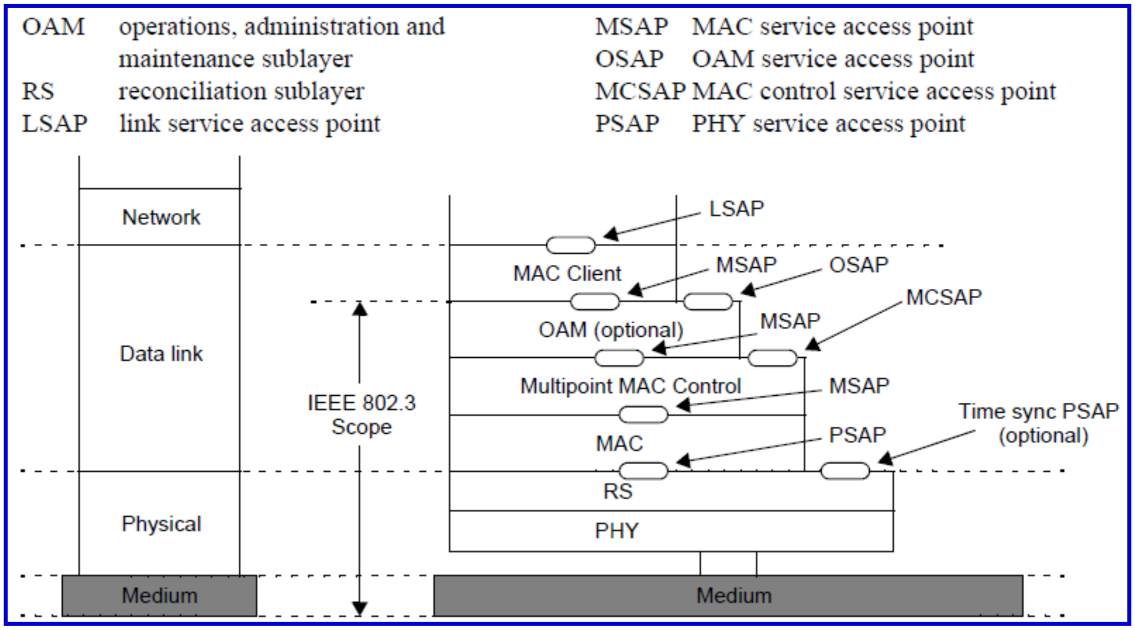
The RM for IEEE 802.3 Ethernet passive optical networks (EPON) optical line terminal (OLT) is illustrated in Figure B.3.



(New)

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

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



(New)

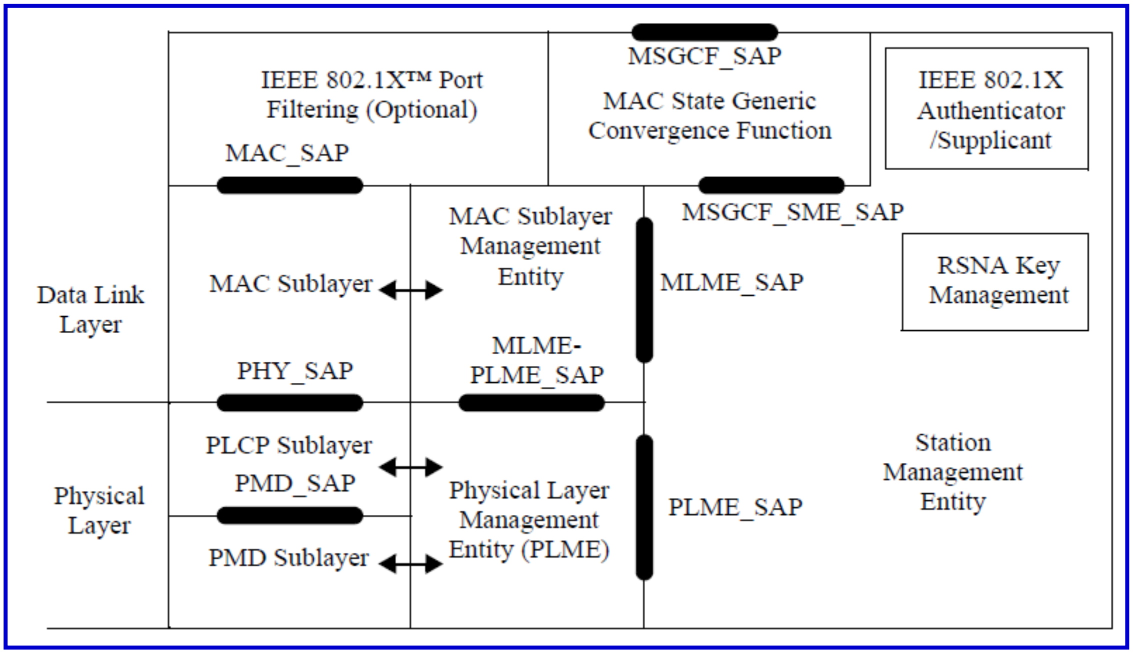
Figure B.4—The RM for IEEE 802.3 point-to-multipoint ONUOAM

IEEE Std 802.3 was amended in 2004 to introduce the concept of subscriber access network.[24] The purpose of Ethernet in the first mile (EFM), as well as its distinction from traditional Ethernet networks, is that it specifies functionality required for the subscriber access network, i.e., public network access. Network design considerations for public access that may differ from traditional Ethernet LANs include the OAM function and the regulatory requirements.

B.2 IEEE 802.11 RM

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

[24] IEEE Std 802.3ah™-2004, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications—Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks.



(New)

Figure B.5—IEEE 802.11 STA RM

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

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

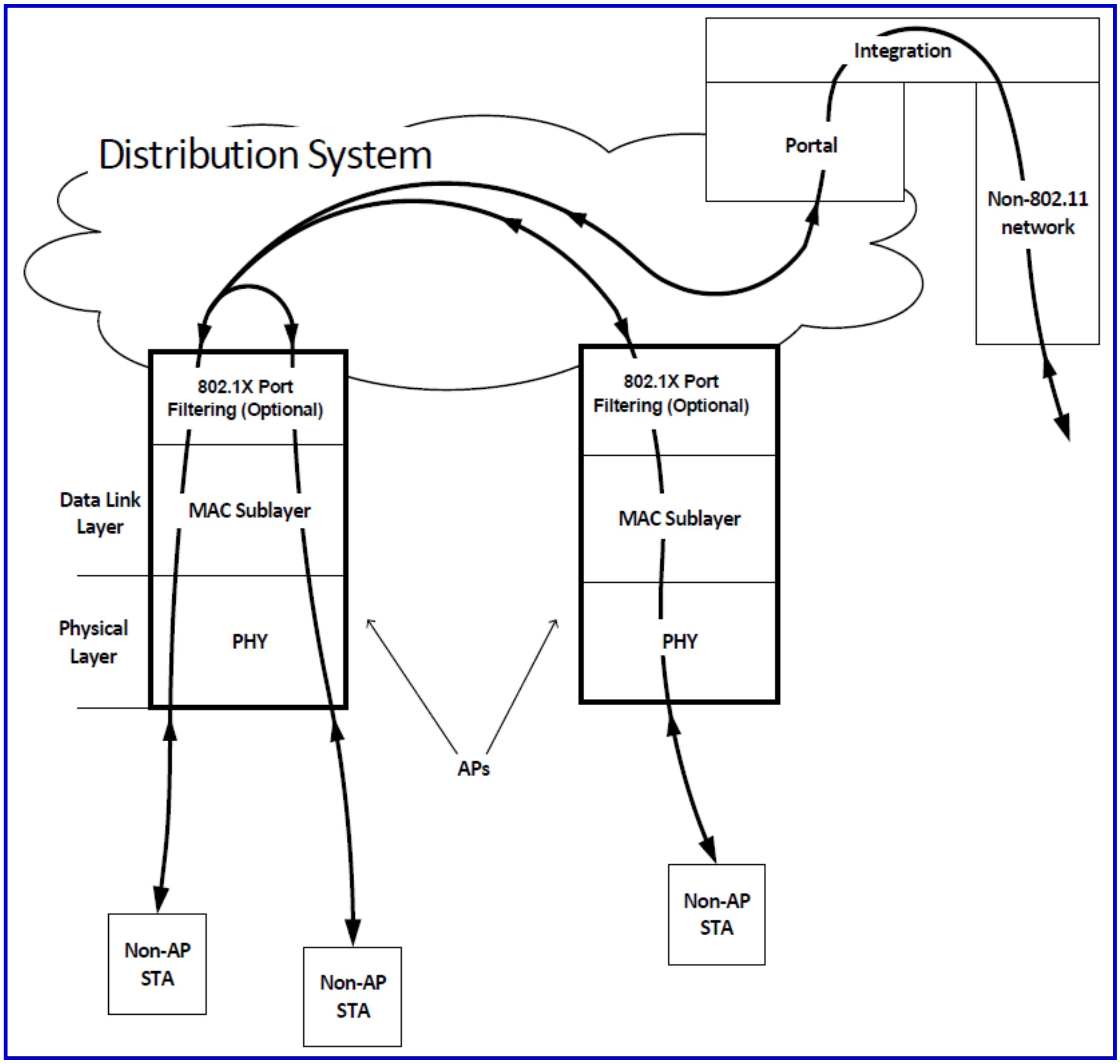
The second interconnection model, the infrastructure model, supports multiple STAs, collected into one or more wireless access domains. These access domains might be interconnected via the distribution system and can interwork with other IEEE 802 networks via one or more portals.

Each access domain in the infrastructure model is established by an access point (AP), which extends the basic STA model to include repeating and forwarding functions that allow communications between non-AP STAs that do not directly interconnect. The AP acts as a forwarding entity to enable communications between non-AP STAs within the access domain (intra-BSS relay). The AP performs a forwarding function, via the distribution system, to enable communications between non-AP STAs in different IEEE 802.11

wireless access domains (inter-BSS relay). Finally, via the distribution system, and portals, APs support communications between IEEE 802.11 STAs and stations attached to other, non-IEEE 802.11 networks.

The third interconnection model, is a mesh model consisting of autonomous STAs. Inside the mesh, STAs establish peer-to-peer wireless links with neighbor STAs to mutually exchange messages. Further, using the mesh's multi-hop capability, messages can be transferred between STAs that are not in direct communication with each other over a single instance of the wireless medium. From the data delivery point of view, it appears as if all STAs in a mesh are directly connected at the MAC layer even if the STAs are not within range of each other. A mesh might have interfaces to external networks and can be a distribution system medium for the infrastructure model.

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



(New)

Figure B.6—IEEE 802.11 infrastructure model

B.3 IEEE 802.15™ RMs

B.3.1 IEEE 802.15.3™ RM

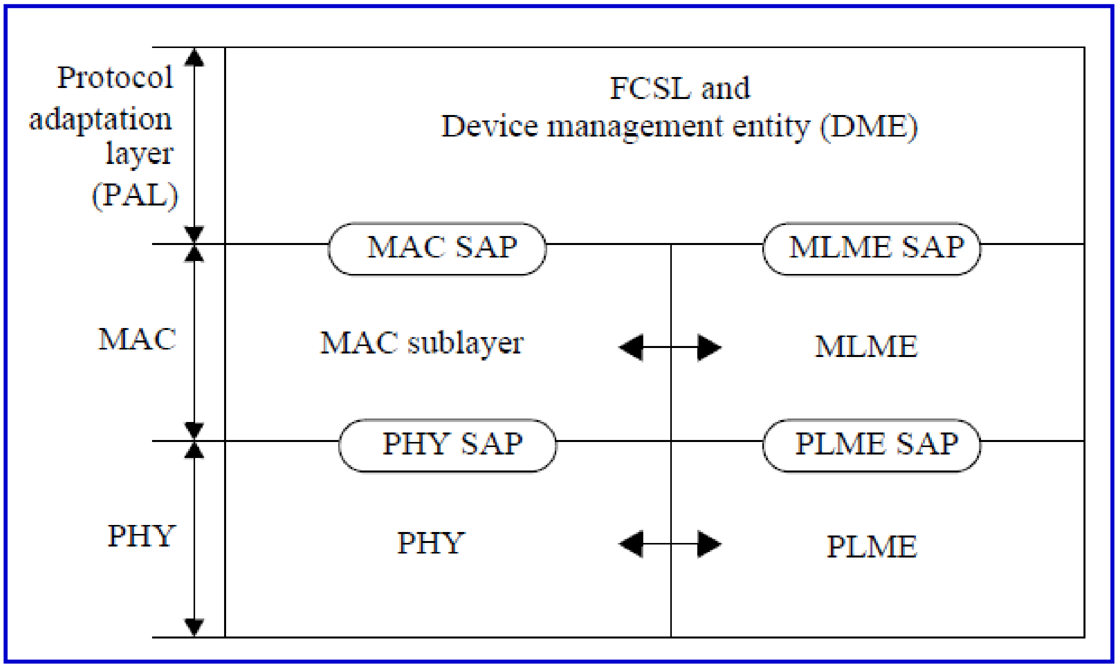
The RM for IEEE Std 802.15.3 is illustrated in Figure B.7.

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

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

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

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



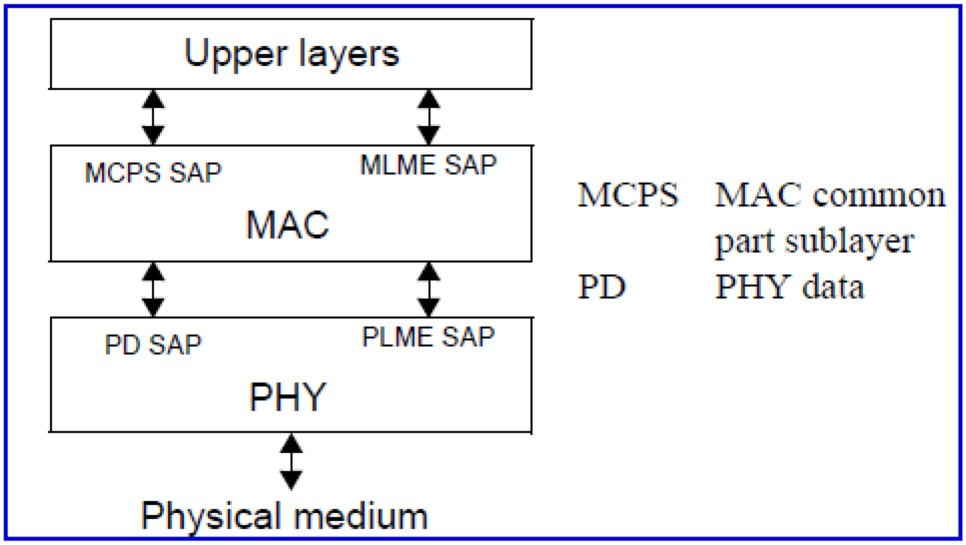
(New)

Figure B.7—IEEE 802.15.3 RM

B.3.2 IEEE 802.15.4™ RM

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

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

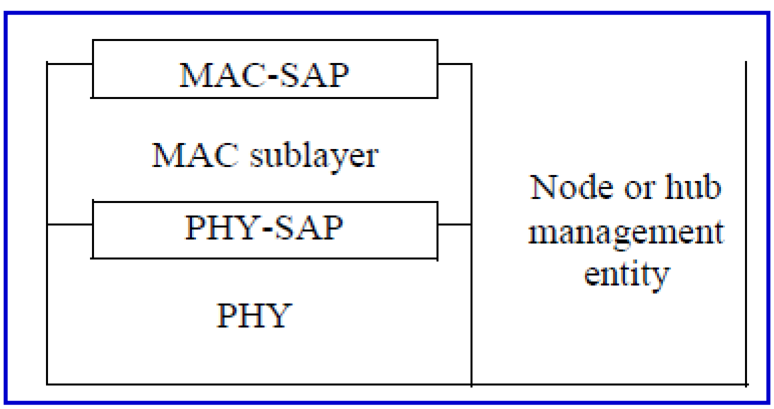


(New)

Figure B.8—IEEE 802.15.4 RM

B.3.3 IEEE 802.15.6™ RM

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



(New)

Figure B.9—IEEE 802.15.6 RM

B.3.4 IEEE 802.15.7™ RM

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

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

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

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

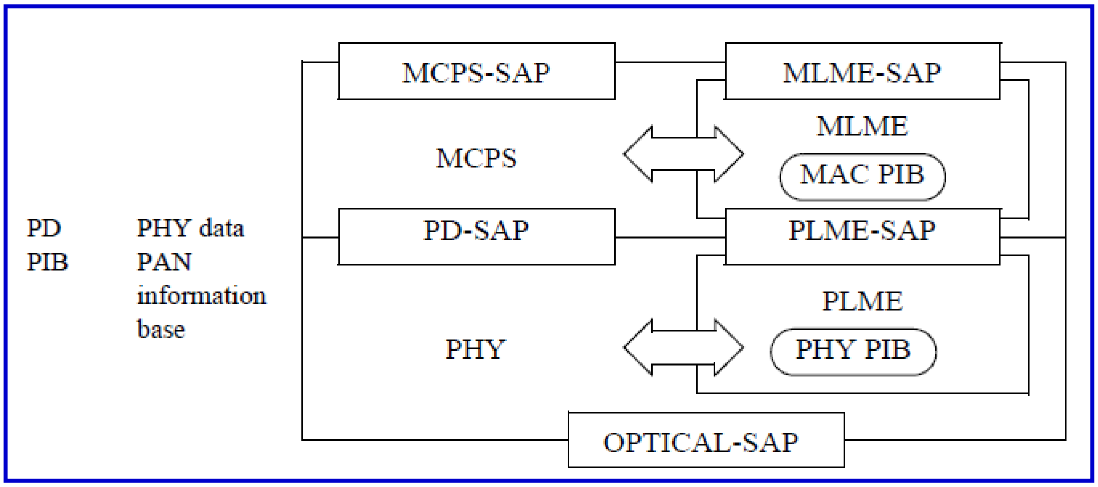
In addition to these external interfaces, an implicit interface also exists between the MLME and the MCPS that allows the MLME to use the MAC data service.

The PHY provides two services, accessed through two SAPs:

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

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

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



(New)

Figure B.10—IEEE 802.15.7 RM

B.4 IEEE 802.16™ RM

B.4.1 Protocol RM

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

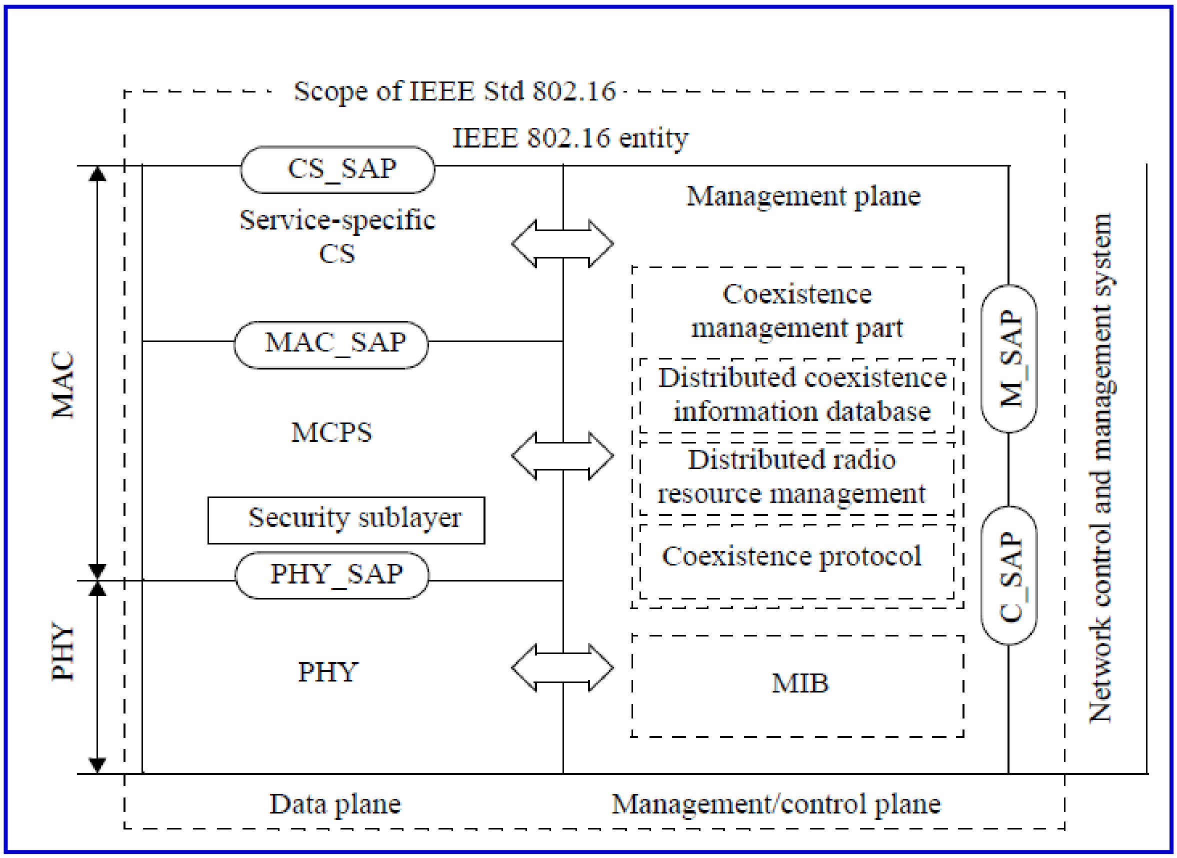
The service-specific convergence sublayer (CS) provides any transformation or mapping of external network data, received through the CS SAP, into MSDUs received by the MCPS through the MAC SAP. This includes classifying external network service data units and associating them to the proper MAC service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

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

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

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

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



(New)

Figure B.11—IEEE 802.16 protocol RM

B.4.2 Network RM

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

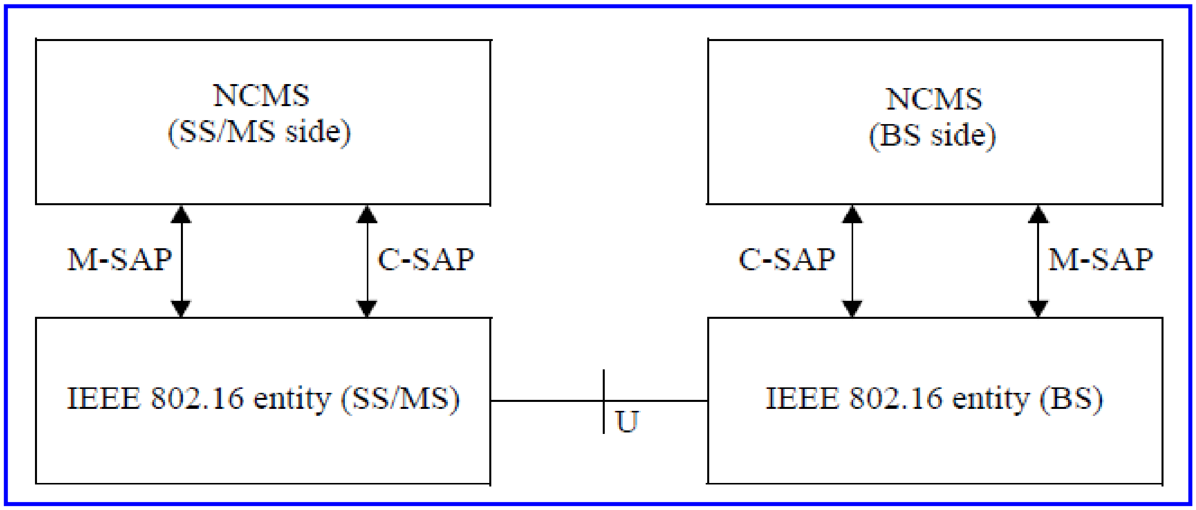
The network control and management system (NCMS) abstraction allows the PHY/MAC layers specified in IEEE Std 802.16 to be independent of the network architecture, the transport network, and the protocols used at the backend and, therefore, allows greater flexibility.

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

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

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

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

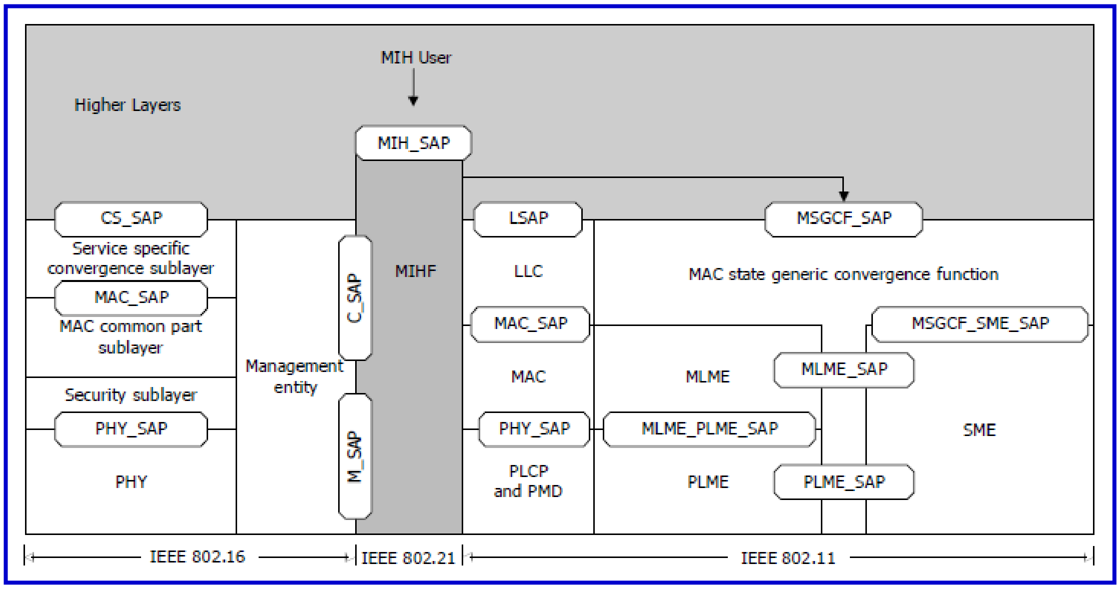


(New)

Figure B.12—IEEE 802.16 network RM

B.5 IEEE 802.21™ RM

Figure B.13 shows an implementation view of a dual-mode IEEE 802.11/IEEE 802.16 station with IEEE 802.21 MIH functionality. The MIHF provides the required services to perform handovers between IEEE 802.11 and IEEE 802.16 access technologies. Also, the MIHF becomes a higher layer when it requires data transport services to communicate with an IEEE 802.21 MIH peer. For layer 2 transport of MIH data, services are provided by the IEEE 802.16 CS SAP or the IEEE 802.11 LSAP. For layer 3 transport, services are provided as described in IETF RFC 5677 [B6].



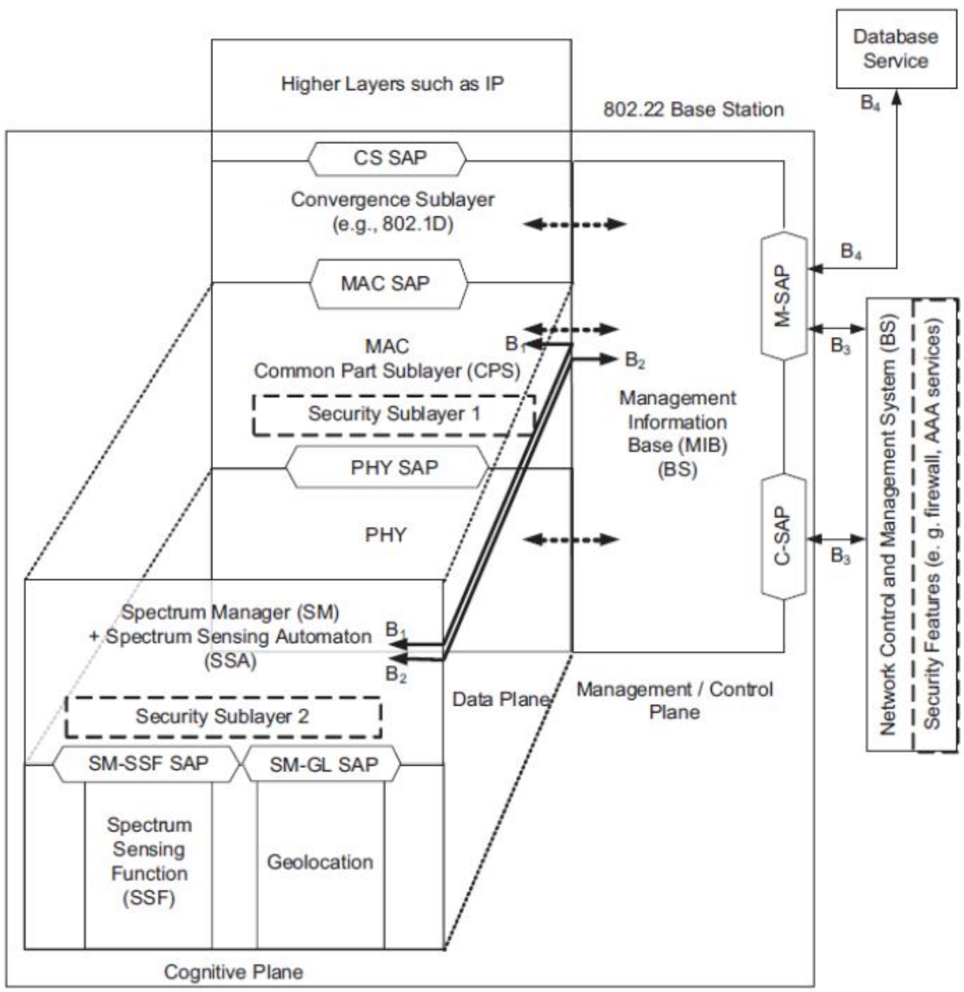
(New)

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

B.6 IEEE 802.22™ RM

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

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



(New)

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

B.6.1 Data plane

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

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

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

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

B.6.2 Management/control plane

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

B.6.3 Cognitive plane

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

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

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

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

Annex C

(informative)

Examples of bit ordering for addresses

C.1 General

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

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

C.2 Illustrative examples

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

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

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

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

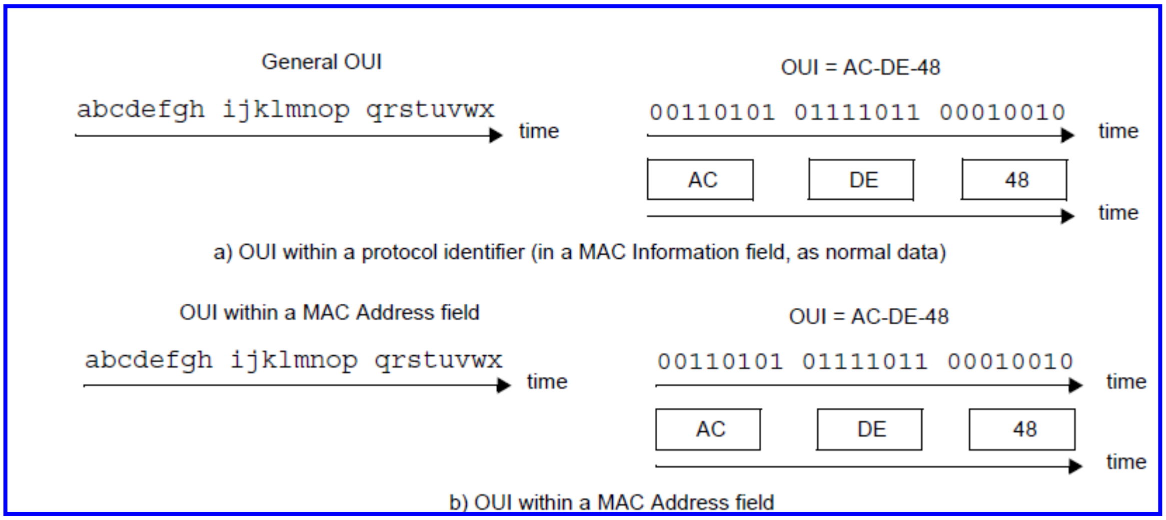
(New)

Figure C.1—Bit significance of an OUI

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

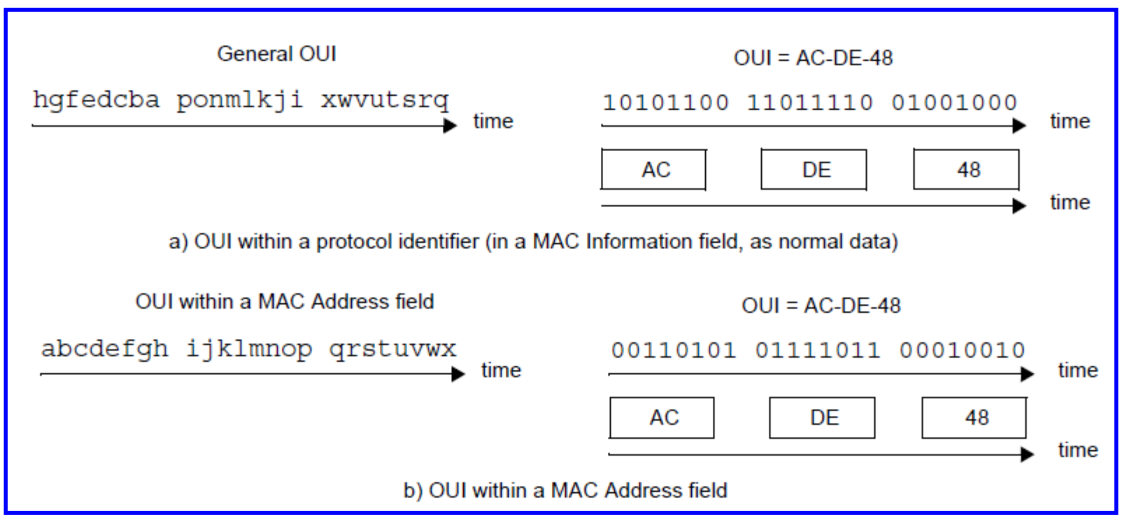
In some circumstances, it is necessary to convey EUI-48s as data within MAC Information fields, e.g., as part of a management protocol or a network layer routing protocol.

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



(New)

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

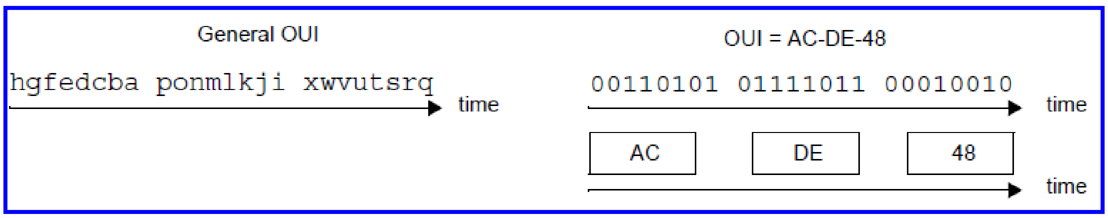


(New)

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

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

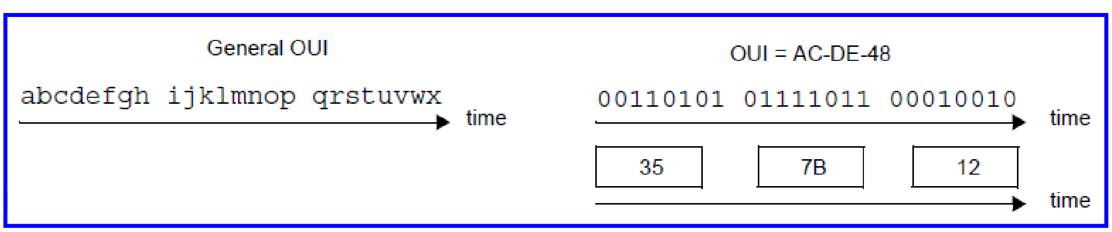
— Canonical format: The octets of the EUI-48 can be treated like any other data octets and transmitted with the bit-ordering of Figure C.3(a). The canonical format is illustrated in Figure C.4.



(New)

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

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



(New)

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

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

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

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

Annex D

(informative)

List of IEEE 802 standards

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

IEEE Std 802.1AB™, IEEE Standard for Local and metropolitan area networks—Station and Medium Access Control Connectivity Discovery.[25, 26]

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

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

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

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

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

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

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

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

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

IEEE Std 802.1Q™, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks.

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

IEEE Std 802.3™, IEEE Standard for Ethernet.

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

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

IEEE Std 802.15.1™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part ~~6: Distributed Queue Dual Bus (DQDB)~~15.1: Wireless medium access ~~method~~control (MAC) and physical layer (PHY) specifications. for wireless personal area networks (WPANs).

~~[B1] Ethernet Version 2.0, A Local Area Network—Data Link Layer and Physical Layer~~

~~Specifications. Digital Equipment Corp., Intel Corp., and Xerox Corp., November 1982.~~

~~[B2] IEEE 100™, The Authoritative Dictionary of IEEE Standards Terms, Seventh Edition.~~

~~[B3] IEEE Std 802.10-1992™, IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS) (includes IEEE Std 802.10b-1992™).[6]~~

~~[B4] ISO/IEC TR 8802-1:1997, Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks Technical reports and guidelines—Part 1:Overview of Local Area Network Standards.~~

~~[B5] ISO/IEC 8802-3:1999 (IEEE Std 802.3-1998™), Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.~~

~~[B6] ISO/IEC 8802-4:1990 (IEEE Std 802.4-1990™), Information processing systems—Local area networks—Part 4: Token-passing bus access method and physical layer specifications.~~

~~[B7] ISO/IEC 8802-5:1998 (IEEE Std 802.5-1998™), Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements—Part 5: Token ring access method and physical layer specifications.~~

~~[B8] ISO/IEC 8802-6:1994 (IEEE Std 802.6-1994™), Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 6: Distributed Queue Dual Bus (DQDB) access method and physical layer specifications~~

~~[6] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (http://standards.ieee.org/).~~

~~[B9] ISO/IEC 8802-9:1996 (~~IEEE Std 802.~~9-1996™),~~15.2™, IEEE Recommended Practice for

Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements— Part ~~9: Integrated Services (IS) LAN Interface at the~~ 15.2: Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands~~Medium Access Control (MAC) and Physical (PHY) Layers~~.

~~[B10] ISO/IEC 8802-11:1999 (~~IEEE Std 802.~~11-1999™),~~15.3™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.3: Wireless ~~LAN~~ Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs).

~~[B11] ISO/IEC 8802-12:1998 (~~IEEE Std 802.~~12-1998™),~~ 15.4™, IEEE Standard for Local and metropolitan area networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs).

IEEE Std 802.15.5™, IEEE Recommended Practice for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—~~Part 12: Demand-Priority access method, physical layer and repeater specifications.~~ Part 15.5: Mesh Topology Capability in Wireless Personal Area Networks (WPANs).

~~[B12] ISO 9314-1:1989, Information processing systems—Fibre Distributed Data Interface (FDDI)—Part 1: Token Ring Physical Layer Protocol (PHY).~~

~~[B13] ISO 9314-2:1989, Information processing systems—Fibre Distributed Data Interface (FDDI)—Part 2: Token Ring Media Access Control (MAC).~~

~~[B14] ISO 9314-3:1990, Information processing systems—Fibre Distributed Data Interface (FDDI)—Part 3: Token Ring Physical Layer Medium Dependent (PMD).~~

~~[B15] ISO 9314-6:1989, Information processing systems—Fibre Distributed Data Interface (FDDI)—~~

~~Part 6: Token Ring Station Management (SMT).~~

~~[B16] ISO/IEC TR 11802-5:1997 (IEEE Std 802.1H-1997™), Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks— Technical reports and guidelines—Part 5: Media Access Control (MAC) Bridging of Ethernet V2.0 in Local Area Networks.~~

~~[B17] ISO/IEC 15802-5:1998 (IEEE Std 802.1G-1998™), Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 5: Remote Media Access Control (MAC) Bridging.~~

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

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

~~[B19] RFC 1390, Transmission of IP and ARP over FDDI Networks. Katz, D., January 1993.~~

~~A.2 Management~~

~~NOTE—Many of the standards listed in Clause 2 and A.1 contain specifications of their managed objects.~~

~~[B20] IEEE Std 802.1F-1993™, IEEE Standards for Local and Metropolitan Area Networks: Common Definitions and Procedures for IEEE 802® Management Information.~~

IEEE Std 802.16.1™, IEEE Standard for Wireless MAN-Advanced Air Interface for Broadband

Wireless Access Systems.

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

~~NOTE—Some of the content of IEEE Std 802.1F-1993™ is also included in ISO/IEC 10742.~~

~~[B21] ISO/IEC 7498-4:1989, Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 4: Management framework.~~

~~[B22] ISO/IEC 8824-1:1995, Information technology—Abstract Syntax Notation One (ASN.1)—Specification of basic notation.~~

~~[B23] ISO/IEC 8824-2:1995, Information technology—Abstract Syntax Notation One (ASN.1)—Information object specification.~~

~~[B24] ISO/IEC 8824-3:1995, Information technology—Abstract Syntax Notation One (ASN.1)—Constraint specification.~~

~~[B25] ISO/IEC 8824-4:1995, Information technology—Abstract Syntax Notation One (ASN.1)—Parameterization of ASN.1 specifications.~~

~~[B26] ISO/IEC 8825-1:1995, Information technology—ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).~~

~~[B27] ISO/IEC 9595:1991, Information technology—Open Systems Interconnection—Common management information service definition.~~

~~[B28] ISO/IEC 9596-1:1991, Information technology—Open Systems Interconnection—Common management information protocol—Part 1: Specification~~

~~[B29] ISO/IEC 10040:1992, Information technology—Open SystemsInterconnection—Systems management overview.~~

~~[B30] ISO/IEC 10164-1/8:1993, Information technology—Open Systems Interconnection—Systems management: [various functions].~~

~~[B31] ISO/IEC 10165-1:1993, Information technology—Open Systems Interconnection—Structure of management information: Management information model.~~

~~[B32] ISO/IEC 10165-2:1992, Information technology—Open Systems Interconnection—Structure of management information: Definition of management information.~~

~~[B33] ISO/IEC 10165-4:1992, Information technology—Open Systems Interconnection—Structure of management information: Guidelines for the definition of managed objects.~~

~~[B34] ISO/IEC 10742:1994, Information technology—Telecommunications and information exchange between systems—Elements of management information related to OSI Data Link Layer standards.~~

~~[B35] ISO/IEC 15802-2:1995 (IEEE Std 802.1B-1995™), Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 2: LAN/MAN management, service and protocol.~~

~~[B36] ISO/IEC 15802-4:1994 (IEEE Std 802.1E-1994™),~~IEEE Std 802.17™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—~~Common~~Specific requirements—Part 17: Resilient packet ring (RPR) access method and physical layer specifications~~—Part 4: System load protocol~~.

~~[B37] RFC 1095, The Common Management Services and Protocol over TCP/IP (CMOT). Warrior, U., and Besaw, L., April 1989.~~

~~[B38] RFC 1155, Structure and Identification of Management Information for TCP/IP-based Internets.~~

~~Rose, M., and McCloghrie, K., May 1990.~~

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

IEEE Std 802.20.2™, IEEE Standard for to IEEE 802.20 Systems—Protocol Implementation Conformance Statement (PICS) Proforma.

~~[B39] RFC 1157, A Simple Network Management Protocol (SNMP). Case, J., Fedor, M., Schoffstall, M., and Davin, J., May 1990.~~

~~[B40] RFC 1212, Concise MIB Definitions. Rose, M., and McCloghrie, K. (Editors), March 1991. [B41] RFC 1215, A Convention for Defining Traps for use with the SNMP. Rose, M., March 1991.~~ \

~~[B42] RFC 1493, Definitions of Managed Objects for Bridges. Decker, E., Langille, P., Rijsinghani, A., and McCloghrie, K., July 1993.~~

~~[B43] RFC 1643, Definitions of Managed Objects for the Ethernet-like Interface Types. Kastenholtz, F., July1994.~~

~~[B44] RFC 1902, Structure of Management information for Version 2 of the Simple Network Management Protocol (SNMPv2). Case, J., McCloghrie, K., Rose, M., and Waldbusser, S., January 1996.~~

~~[B45] RFC 1903, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2). Case, J., McCloghrie, K., Rose, M., and Waldbusser, S., January 1996.~~

~~[B46] RFC 1904, Conformance Statements for Version 2 of the Simple Network Management~~

~~Protocol (SNMPv2). Case, J., McCloghrie, K., Rose, M., and Waldbusser, S., January 1996.~~

~~[B47] RFC 1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2). Case, J., McCloghrie, K., Rose, M., and Waldbusser, S., January 1996.~~

IEEE Std 802.20.3™, IEEE Standard for Minimum Performance Characteristics of IEEE 802.20 Terminals and Base Stations/Access Nodes.

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

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

IEEE Std 802.22.1™, IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 22.1: Standard to Enhance Harmful Interference Protection for Low-Power Licensed Devices Operating in TV Broadcast Bands.

Annex E

(informative)

History

E.1 Universal addresses

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

The IEEE RA, because of the work in ~~Project~~ IEEE 802® on standardizing networking ~~LAN~~ technologies, ~~has~~ assumed the responsibility of defining and carrying out procedures for the universal administration of these addresses ~~IEEE and ISO/IEC LANs (e.g., CSMA/CD, Token Bus, Token Ring, and FDDI). In carrying out the procedures, the IEEE acts as the Registration Authority for OUIs.~~[5]. The IEEE RA has also been designated by ISO/IEC to act as a registration authority for the ISO/IEC 8802 series of standards. The responsibility for defining the procedures is discharged by the IEEE Registration Authority Committee, which is chartered by the IEEE Standards Association Board of Governors.

E.2 IEEE RA address block products

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

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

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

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

Consensus

WE BUILD IT.

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