IEEE Standards

IEEE Std 802-2001®
(Revision of IEEE Std 802-1990™)

802®

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

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

7 February 2002

Print: SH94947
PDF: SS94947

IEEE Std 802-2001®
(Revision of IEEE Std 802-1990™)

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

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 6 December 2001

IEEE-SA Standards Board

Abstract: IEEE Std 802-2001®, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, provides an overview to the family of IEEE 802® Standards. It defines compliance with the family of IEEE 802® Standards; it describes the relationship of the IEEE 802® Standards to the Open Systems Interconnection Basic Reference Model [ISO/IEC 7498-1:1994] and explains the relationship of these standards to the higher layer protocols; it provides a standard for the structure of LAN MAC addresses; and it provides a standard for identification of public, private, and standard protocols.
Keywords: IEEE 802® standards compliance, Local Area Networks (LANs), LAN/MAN architecture, LAN/MAN reference model, Metropolitan Area Networks (MANs).

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

Print: ISBN 0-7381-2940-2 SH94947
PDF: ISBN 0-7381-2941-0 SS94947

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

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

The IEEE and its designees are the sole entities that may authorize the use of the IEEE-owned certification marks and/or trademarks to indicate compliance with the materials set forth herein.

IEEE-SA Trademark Usage/Compliance Statement

Proper usage of the trademark **IEEE Std 802-2001**® is mandatory and is to be followed in all references of the Standard. The mark **IEEE**® is the registered trademark of the Institute of Electrical and Electronics Engineers, Inc., and must be used in bold type. It is to appear with the registered trademark symbol "®" the first time "**IEEE**" appears in the text. The use of "IEEE Std xxxx-200x" should include the trademark symbol "TM" (e.g., **IEEE Std xxxx-200x**™) at least the first time it is used in text, unless the number of the standard is also trademark registered (e.g., **802**®), then the symbol "®" must be used.

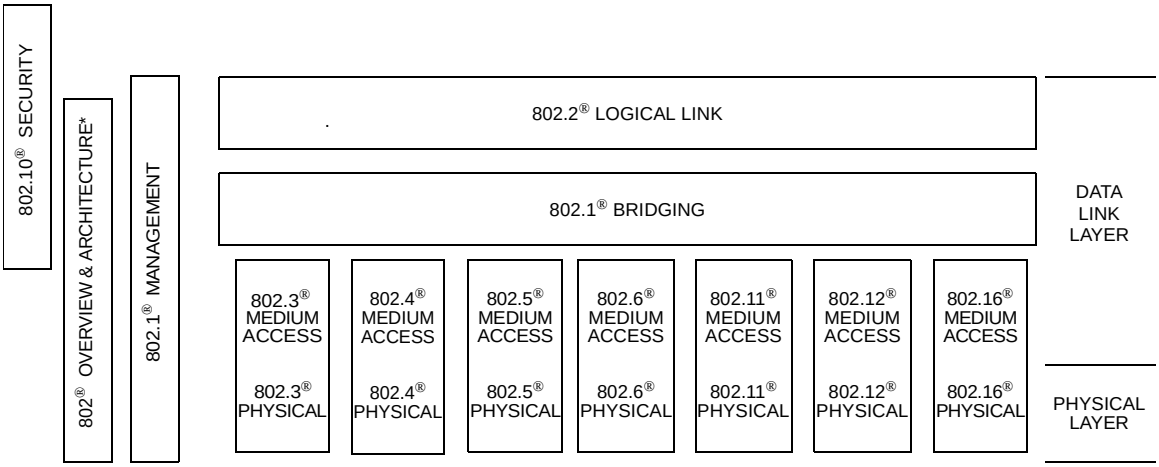
It is not permissible to use the standard number alone or with "**IEEE**" to indicate conformance or compliance with the associated standard. The user of the Standard should contact the Manager, Standards Licensing and Contracts for information concerning issues regarding indicating product compliance with an **IEEE** standard. To represent that a product has been designed to meet an **IEEE** standard, it is permissible to state that "the product has been engineered, designed or manufactured with the intent to meet the requirements of **IEEE Std xxxx-200x**™". However, it is ***not*** permissible to state or refer to a product as "xxxx compliant," "xxxx certified," "**IEEE xxxx** conformant," "**IEEE xxxx** certified," or the like, unless the user has obtained a Certification License from the Manager, Standards Licensing and Contracts.

Introduction

(This introduction is not part of IEEE Std 802-2001®, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.)

IEEE Std 802-2001® provides an overview to the family of IEEE 802® Standards. It defines compliance with the family of IEEE 802® Standards; it describes the relationship of the IEEE 802® Standards to the Open Systems Interconnection Basic Reference Model [ISO/IEC 7498-1: 1994] and explains the relationship of these standards to higher layer protocols; it provides a standard for the structure of LAN MAC addresses; and it provides a standard for the identification of public, private, and standard protocols.

This standard is part of a family of standards for local and metropolitan area networks. The relationship between the standard and other members of the family is shown below. (The numbers in the figure refer to IEEE standard numbers.)



* Formerly IEEE Std 802.1A®.

This family of standards deals with the Physical and Data Link Layers as defined by the International Organization for Standardization (ISO) Open Systems Interconnection Basic Reference Model (ISO/IEC 7498-1:1994). The access standards define several types of medium access technologies and associated physical media, each appropriate for particular applications or system objectives. Other types are under investigation.

The standards defining the technologies noted above are as follows:

• IEEE Std 802®:[1]	*Overview and Architecture*. This standard provides an overview to the family of IEEE 802® Standards. This document forms part of the IEEE Std 802.1® scope of work.
• IEEE Std 802.1B® and 802.1K® [ISO/IEC 15802-2]:	*LAN/MAN Management*. Defines an Open Systems Interconnection (OSI) management-compatible architecture, and services and protocol elements for use in a LAN/MAN environment for performing remote management.

[1]The IEEE 802® Architecture and Overview Specification, originally known as IEEE Std 802.1A®, has been renumbered as IEEE Std 802®. This has been done to accommodate recognition of the base standard in a family of standards. References to IEEE Std 802.1A® should be considered as references to IEEE Std 802®.

• IEEE Std 802.1D®	*Media Access Control* (*MAC) Bridges*. Specifies an architecture and protocol for the [ISO/IEC 15802-3]: interconnection of IEEE 802® LANs below the MAC service boundary.
• IEEE Std 802.1E® [ISO/IEC 15802-4]:	*System Load Protocol*. Specifies a set of services and protocol for those aspects of management concerned with the loading of systems on IEEE 802® LANs.
• IEEE Std 802.1F®	*Common Definitions and Procedures for IEEE 802® Management Information*.
• IEEE Std 802.1G® [ISO/IEC 15802-5]:	*Remote Media Access Control (MAC) Bridging*. Specifies extensions for the interconnection, using non-LAN systems communication technologies, of geographically separated IEEE 802® LANs below the level of the logical link control protocol.
• IEEE Std 802.1H® [ISO/IEC TR 11802-5]	*Recommended Practice for Media Access Control (MAC) Bridging of Ethernet V2.0 in IEEE 802® Local Area Networks.*
• IEEE Std 802.1Q®	*Virtual Bridged Local Area Networks*. Defines an architecture for Virtual Bridged LANs, the services provided in Virtual Bridged LANs, and the protocols and algorithms involved in the provision of those services.
• IEEE Std 802.2® [ISO/IEC 8802-2]:	*Logical Link Control.*
• IEEE Std 802.3® [ISO/IEC 8802-3]:	*CSMA/CD Access Method and Physical Layer Specifications*.
• IEEE Std 802.4® [ISO/IEC 8802-4]:	*Token Bus Access Method and Physical Layer Specifications.*
• IEEE Std 802.5® [ISO/IEC 8802-5]:	*Token Ring Access Method and Physical Layer Specifications*.
• IEEE Std 802.6® [ISO/IEC 8802-6]:	*Distributed Queue Dual Bus Access Method and Physical Layer Specifications.*
• IEEE Std 802.10®:	*Interoperable LAN/MAN Security.* Currently approved: Secure Data Exchange (SDE).
• IEEE Std 802.11®: [ISO/IEC 8802-11]	*Wireless LAN Medium Access Control (MAC) Sublayer and Physical Layer Specifications.*
• IEEE Std 802.12®: [ISO/IEC 8802-12]	*Demand Priority Access Method, Physical Layer and Repeater Specification*.
• IEEE Std 802.15®:	*Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for: Wireless Personal Area Networks.*
• IEEE Std 802.16®:	*Standard Air Interface for Fixed Broadband Wireless Access Systems*.
• IEEE Std 802.17®:	*Resilient Packet Ring Access Method and Physical Layer Specifications.*

In addition to the family of standards, the following is a recommended practice for a common physical layer technology:

• IEEE Std 802.7®:	*IEEE Recommended Practice for Broadband Local Area Networks*.

The reader of this standard is urged to become familiar with the complete family of standards.

Conformance test methodology

An additional standards series, identified by the number 1802™, has been established to identify the conformance test methodology documents for the IEEE 802® family of standards. Thus the conformance test documents for IEEE 802.3® are numbered 1802.3™, the conformance test documents for IEEE 802.5® will be 1802.5™, and so on. Similarly, ISO will use 18802 to number conformance test standards for 8802 standards.

Participants

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

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

Steve Adams
Floyd Backes
John Bartlett
Les Bell
Michael Berger
James S. Binder
Bill Bunch
Paul Carroll
Jeffrey Catlin
David W. Chang
Hon Wah Chin
Chris Christ
Paul Congdon
Glenn Connery
David Cullerot
Ted Davies
David Delaney
Jeffrey Dietz
Peter Ecclesine
J. J. Ekstrom
Norman W. Finn
Lars Henrik Frederiksen
Anoop Ghanwani
Sharam Hakimi
John Hart
Richard Hausman
David Head
Deepak Hegde
Ariel Hendel
Steve Horowitz
Altaf Hussain
Vipin K. Jain
Toyoyuki Kato
Hal Keen
Kevin Ketchum
Keith Klamm
Bruce Kling
Dan Krent
Paul Lachapelle
Paul Langille
Johann Lindmeyr
Milan Merhar
John Messenger
Colin Mick
Yaron Nachman
Krishna Narayanaswamy
Lawrence Ng
Henry Ngai
Satoshi Obara
Toshio Ooka
Jorg Ottensmeyer
Luc Pariseau
John Pickens
Steve Ramberg
Shlomo Reches
James Richmond
Anil Rijsinghani
Ayman Sayed
Mick Seaman
Lee Sendelbach
Himanshu Shah
Phil Simmons
Paramjeet Singh
Rosemary V. Slager
Alexander Smith
Andrew Smith
Larry Stefani
Stuart Soloway
Sundar Subramaniam
Robin Tasker
Pat Thaler
Steve Van Seters
Dono van-Mierop
John Wakerly
Peter Wang
Y. C. Wang
Trevor Warwick
Keith Willette
Michael Witkowski
Edward Wong
Michael D. Wright
Michele Wright
Allen Yu
Wayne Zakowski

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

Don Aelmore
Jack S. Andresen
Lek Ariyavisitakul
Thomas W. Bailey
Kevin Barry
Brad J. Booth
Chris Byham
James T. Carlo
David E. Carlson
Alan M. Chambers
Thomas J. Dineen
Christos Douligeris
Sourav K. Dutta
Paul S. Eastman
Richard Eckard
Philip H. Enslow
Changxin Fan
John W. Fendrich
Michael A. Fischer
Howard M. Frazier
Ken J. Friedenbach
Robert J. Gagliano
Gautam Garai
Alireza Ghazizahedi
Patrick S. Gonia
Julio Gonzalez-Sanz
Robert M. Grow
David B. Gustavson
Chris G. Guy
Vic Hayes
Donald N. Heirman
Raj Jain
David V. James
Tony A. Jeffree
Henry D. Keen
Peter M. Kelly
Stuart J. Kerry
Daniel R. Krent
Stephen Barton Kruger
David J. Law
Walter Levy
William P. Lidinsky
Randolph S. Little
Joseph G. Maley
Roger B. Marks
Peter Martini
Richard McBride
Bennett Meyer
Tremont Miao
David S. Millman
Mart Molle
John E. Montague
Masahiro Morikura
Wayne D. Moyers
Shimon Muller
Paul Nikolich
Erwin Noble
Ellis S. Nolley
Robert O'Hara
Satoshi Obara
Charles Oestereicher
Roger Pandanda
Vikram Punj
Sailesh Rao
Stanley A. Reible
James A. Renfro
Gary S. Robinson
Edouard Y. Rocher
James W. Romlein
Floyd E. Ross
Christoph Ruland
Robert Russell
Norman Schneidewind
James E. Schuessler
Gregory D. Schumacher
Michael Seaman
Rich Seifert
Leo Sintonen
Michael A. Smith
Fred J. Strauss
Walter T. Thirion
Geoffrey O. Thompson
Mark-Rene Uchida
Scott A. Valcourt
Paul A. Willis
Wayne Zakowski
Johathan M. Zweig

When the IEEE-SA Standards Board approved this standard on 6 December 2001, it had the following membership:

Donald N. Heirman, *Chair*
James T. Carlo, *Vice Chair*
Judith Gorman, *Secretary*

Satish K. Aggarwal
Mark D. Bowman
Gary R. Engmann
Harold E. Epstein
H. Landis Floyd
Jay Forster*
Howard M. Frazier
Ruben D. Garzon
James H. Gurney
Richard J. Holleman
Lowell G. Johnson
Robert J. Kennelly
Joseph L. Koepfinger*
Peter H. Lips
L. Bruce McClung
Daleep C. Mohla
James W. Moore
Robert F. Munzner
Ronald C. Petersen
Gerald H. Peterson
John B. Posey
Gary S. Robinson
Akio Tojo
Donald W. Zipse

*Member Emeritus

Also included is the following nonvoting IEEE-SA Standards Board liaison:

Alan Cookson, *NIST Representative*
Donald R. Volzka, *TAB Representative*

Jennifer McClain Longman
IEEE Standards Project Editor

Contents

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

1. Scope

1.1 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 contains descriptions of the networks considered as well as a reference model (RM) for protocol standards. Compliance with the family of IEEE 802® Standards is defined, and a standard for the identification of public, private, and standard protocols is included.

1.2 Key concepts

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 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.

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.

The basic communications capabilities provided by all 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 shorter, fixed-length units; isochronous communication transmits data as a steady stream of octets, or groups of octets, at equal time intervals.)

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.

1.3 Application and support

The networks are intended to have wide applicability in many environments. The primary aim is to provide for moderate-cost devices and networks, suitable for 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:

— File transfer
— Graphics
— Text processing
— Desktop publishing
— Electronic mail
— Database access
— Transaction processing
— Multimedia
— Office automation

— Process control
— Robotics
— Integrated Services (voice, video and data) applications
— Client/server applications

The networks are intended to support various data devices, such as the following:

— Computers
— Terminals
— Mass storage devices
— Printers and plotters
— Photocopiers and facsimile machines
— Image and video monitors
— Wireless terminals
— Monitoring and control equipment
— Bridges, routers, and gateways
— Integrated Services devices, including ISDN terminals and end systems supporting combined voice, video, and data applications

1.4 An international family of standards

The terms LAN and MAN 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 defined in the family of IEEE 802® Standards. In turn, these medium access control (MAC) standards are defined for a variety of physical media. A logical link control (LLC) standard, a 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 are also defined.

The IEEE 802® Standards have been developed and applied in the context of an increasingly global data communications industry. This global context is recognized in that most IEEE 802® Standards are progressed to become also international 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.

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.

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, the following definitions apply. *The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition [B2],[2] should be referenced for terms not defined in this clause.

3.1.1 access domain: A set of LAN or MAN stations together with interconnecting data transmission media and related equipment (e.g., connectors, repeaters), in which the LAN or MAN stations use the same MAC protocol to establish the sequence of stations that are in temporary control of the shared transmission media.

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®) or FDDI environment. See Figure 8 for a comparative example of bit-reversed and hexadecimal representation.

[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/).

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

3.1.3 bridge, MAC bridge: A functional unit that interconnects two or more LANs or MANs that use the same Data Link layer protocols above the MAC sublayer, but can use different MAC protocols.

3.1.4 canonical format: The format of a MAC data frame in which the octets of any MAC addresses conveyed in the MAC user data field have the same bit ordering as in the Hexadecimal Representation.

3.1.5 end station: A device attached to a LAN or MAN, which acts as a source of, and/or destination for, data traffic carried on the LAN or MAN.

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.

3.1.13 IEEE 802® MAN, 802® MAN: A MAN consisting of one or more interconnected subnetworks each using a 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.

3.1.14 interconnection: The provision of data communication paths between LAN or MAN stations.

3.1.15 interworking: The use of interconnected LAN or MAN stations 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.

3.1.18 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; one of the fields contains a sequence of octets of user data.

3.1.19 MAC protocol: The protocol that governs access to the transmission medium in a LAN or MAN, to enable the exchange of data between LAN or MAN stations.

3.1.20 MAN: A computer network, extending over a large geographical area such as an urban area and providing integrated communication services such as data, voice, and video.

3.1.21 noncanonical format: The format of a MAC data frame in which the octets of MAC addresses conveyed in the MAC user data field have the same bit ordering as in the Bit-reversed representation.

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.

3.1.23 station: An end station or bridge.

4. Abbreviations and acronyms

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
FDDI	fibre distributed data interface (ISO/IEC 9314)
IM	implementation model
I/G	individual/group
ISDN	integrated services digital network
ISLAN	integrated services LAN (ISO/IEC 8802-9)
LAN	local area network
LLC	logical link control (ISO/IEC 8802-2)
LSAP	link service access point (ISO/IEC 8802-2)
LSB	least significant bit
MAC	medium access control, media access control[3]
MAN	metropolitan area network

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

MIB	management information base
MOCS	managed object conformance statement
MSAP	MAC service access point
MSB	most significant bit
PDU	protocol data unit
PhSAP	physical service access point
PICS	protocol implementation conformance statement
RM	reference model
OSI	open systems interconnection (ISO/IEC 7498-1)
OUI	organizationally unique identifier
SNAP	subnetwork access protocol
SNMP	simple network management protocol (RFC 1157[4])
U/L	universally or locally administered
WAN	wide area network

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.

6. Reference and implementation models

6.1 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 the Open Systems Interconnection (OSI) Basic Reference Model (OSI/RM), ISO/IEC 7498-1. It is assumed that the reader has some familiarity with the OSI/RM and its terminology. The IEEE 802® Standards encompass the functionality of the lowest two layers of the OSI/RM (i.e., Physical layer and Data Link layer) and the higher layers as they relate to LAN management. The LAN&MAN/RM is similar to the OSI/RM in terms of its layers and the placement of its service boundaries.

For the mandatory packet services supported by all LANs and MANs, the Data Link layer is structured as two sublayers, with the LLC sublayer 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

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

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.

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.

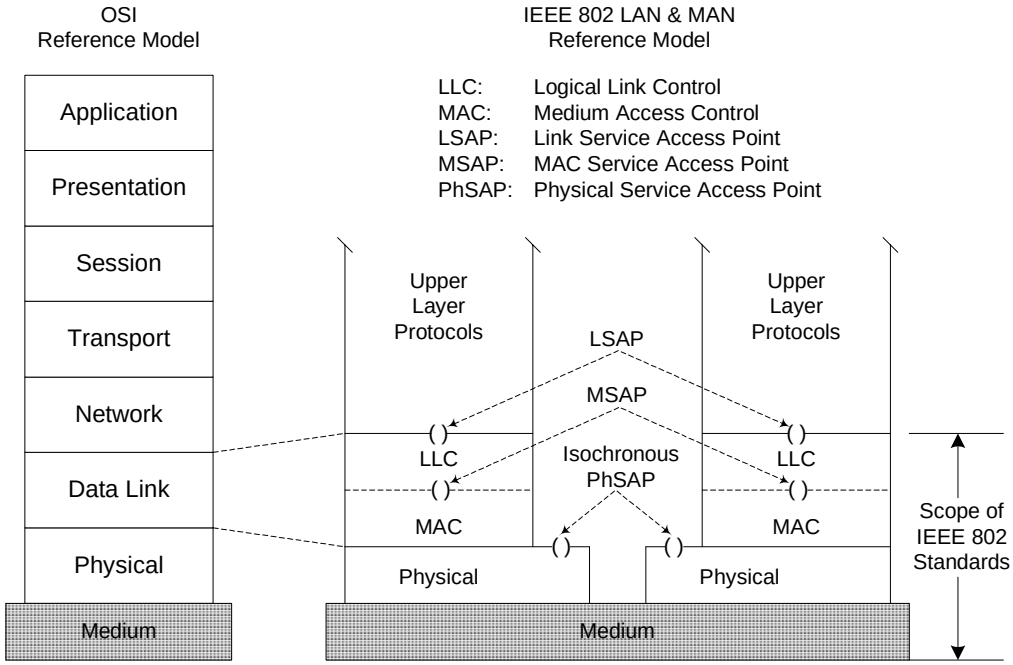


Figure 1—IEEE 802® RM for end stations (LAN&MAN/RM)

The LAN&MAN/IM is more specific than the LAN&MAN/RM, 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 relation to the LAN&MAN/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.

LLC: Logical Link Control
MAC: Medium Access Control
PHY: Physical Layer
PLS: Physical Layer Signaling
PMA: Physical Medium Attachment
1: Attachment Unit Cable
2: Attachment Unit Connectors
AUI: Attachment Unit Interface
MAU: Medium Attachment Unit
MDI: Medium Dependent Interface

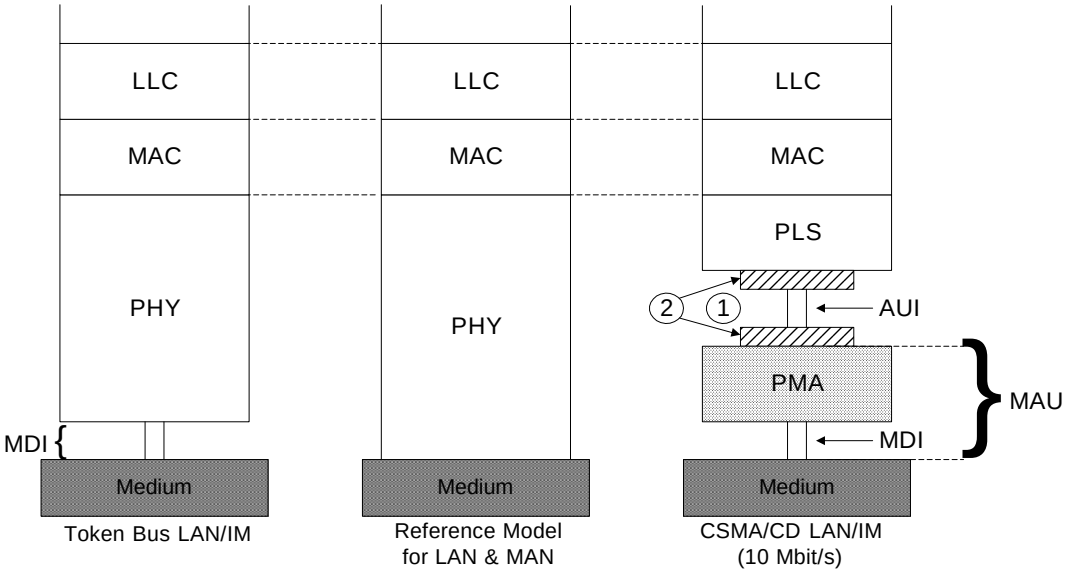


Figure 2—IEEE 802® RM and two examples of end-station implementation model

Considerations of management and security in LANs and MANs are also covered by IEEE 802® standards; these optional features lead to an elaboration of the RM (Figure 3). LAN/MAN management provides a Data Link layer management protocol for exchange of management information between LAN stations; managed objects are defined for all LAN/MAN protocol standards. The Secure Data Exchange (SDE) entity forms part of the LLC sublayer and provides a secure connectionless service immediately above the MAC sublayer.

LMM: LAN/MAN Management
SDE Secure Data Exchange

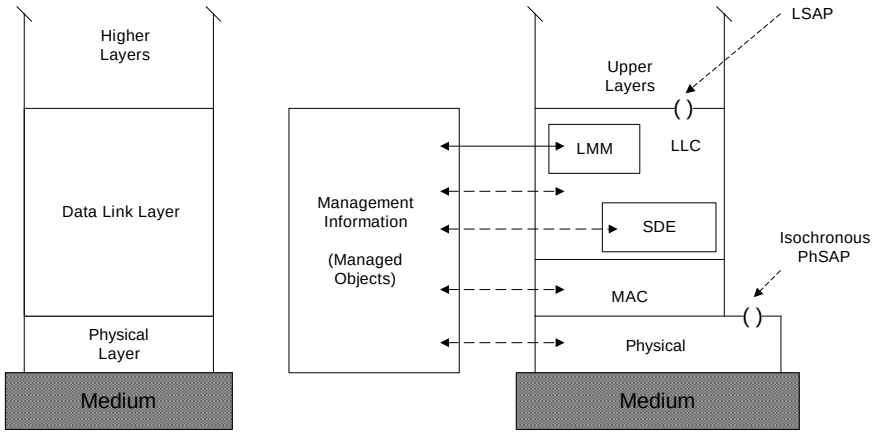


Figure 3—IEEE 802® RM with end-station management and security

6.2 RM description for end stations

The LAN&MAN/RM maps to the OSI/RM as shown in Figure 1. The applicable part of the OSI/RM consists of the lowest two layers: the Data Link layer and the Physical layer. These map onto the same two layers in the IEEE LAN&MAN/RM. The MAC sublayer of the LAN&MAN/RM exists between the Physical layer 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, in addition to the common core features). Service access points (SAPs) for addressing endpoints are shown.

6.2.1 Service access points (SAPs)

Multiple-link service access points (LSAPs) provide interface ports to support multiple higher layer users above the LLC sublayer.

The MAC sublayer provides a single MAC service access point (MSAP) as an interface port to the LLC sublayer in an end station. In general, the MSAP is identified (for transmission and reception) by a single individual MAC address and (for reception) by the LAN-wide broadcast MAC address; it can 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.

6.2.2 LLC sublayer

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®.

6.2.3 MAC sublayer

The MAC sublayer performs the functions necessary to provide packet-based, connectionless-mode (datagram style) data transfer between stations in support of the LLC sublayer or of the Ethernet sublayer (see 6.1) for LANs that support it. The term *MAC frame*, or simply *frame*, is used to describe the packets transferred within the MAC sublayer. 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.

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 the Ethernet 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 (see 6.3), and filtering of frames according to their destination addresses to reduce the extent of propagation of frames in parts of a LAN or MAN 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, 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. 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 9, and particularly 9.5, 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.

6.2.4 Physical layer

The Physical layer provides the capability of transmitting and receiving bits between Physical layer entities. A pair of Physical layer 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-to-end timing preserved between isochronous-service PhSAPs.

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

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/s and above, or for wireless transmission, the Physical layer can map blocks of several bits (e.g., 4, 5, or 8 bits) to different multi-element symbols. In some Physical-layer 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).

6.2.5 Layer and sublayer management

The LLC sublayer, MAC sublayer, and Physical layer 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 8 for further information.

6.3 Interconnection and interworking

In some cases, the end systems on a LAN or MAN have no need to communicate with end systems 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 need to communicate with end systems on other networks and so devices that interconnect the LAN or MAN 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 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 interconnection, using devices usually termed *repeaters* or *hubs* (6.3.1)

— MAC-sublayer interconnection, using devices termed *bridges* (6.3.2)

— Network-layer interconnection, using devices usually termed *routers* (6.3.3)

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.

6.3.1 Physical-layer interconnection: repeaters and hubs

The original IEEE 802® LAN specifications 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 one can be transmitting at a given time, with all other stations acting as (potential) receivers.

A repeater is a device used to interconnect segments of the physical communications media, for example, to extend the range of a LAN 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.

6.3.2 MAC-sublayer interconnection: bridges

6.3.2.1 Bridges and bridged LANs

Bridges (see 3.1.3) are devices that interconnect multiple access domains. ISO/IEC 15802-3 provides the basic specification for bridge interworking among IEEE 802® networks. A *bridged* LAN (see 3.1 of ISO/IEC 15802-3) consists of one or more bridges together with the complete set of access domains that they interconnect. A bridged LAN provides end stations belonging to any of its access domains with the appearance of a LAN that contains the whole set of attached end stations.

A bridged LAN can provide for the following:

— Communication between stations attached to LANs of different MAC types

— An increase in the total throughput of a LAN

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

— Partitioning of the physical LAN for administrative or maintenance reasons

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 does not make any such distinction. Hence, this standard only uses the term bridge.

6.3.2.2 Relaying and filtering by bridges

A bridge processes protocols in the MAC sublayer and is functionally transparent to LLC 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 information. Figure 4 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.

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

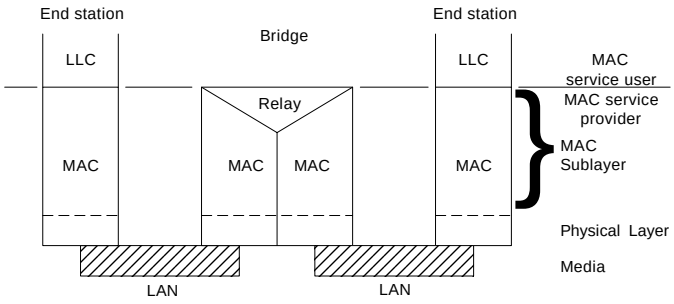


Figure 4—Internal organization of the MAC sublayer with bridging

6.3.2.3 The Spanning Tree Protocol

A key aspect of ISO/IEC 15802-3 is its specification of the Spanning Tree Protocol, which is used by bridges to configure their interconnections in order to prevent looping data paths in the bridged LAN. In the event that the basic interconnection topology of bridges and LANs contains multiple possible paths between certain points, use of the Spanning Tree Protocol 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, the Spanning Tree Protocol 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 adapts to changes in the configuration of the bridged LAN, maintaining connectivity while avoiding data loops. Some configuration changes can cause temporary interruptions of connectivity between parts of the bridged LAN, typically lasting for a few tens of seconds at most.

6.3.2.4 Transparent bridging and source routing

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

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.

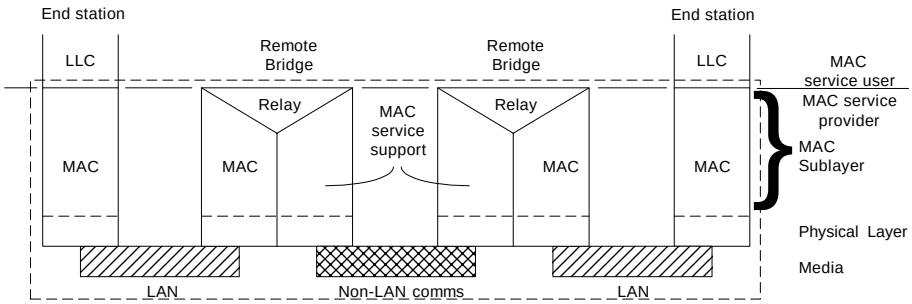


Figure 5—Internal organization of MAC sublayer with remote bridges

6.3.2.6 Bridging example

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

Figure 6 illustrates the kind of bridged LAN that can be configured with bridge-style interconnection. The bridges A and B, and the CSMA/CD LAN configurations to which they attach, are typical of the older style of bridged LAN in which a bridge interconnects a small number of access domains each containing many

end stations, as is similar with K, L, and M and their Token Ring LANs. 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 802.3® LANs. S is a backbone bridge, handling a number of high-speed LAN attachments. T and U are bridges that support multiple end stations, with connection to the backbone. B and K also provide access to the backbone. 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.

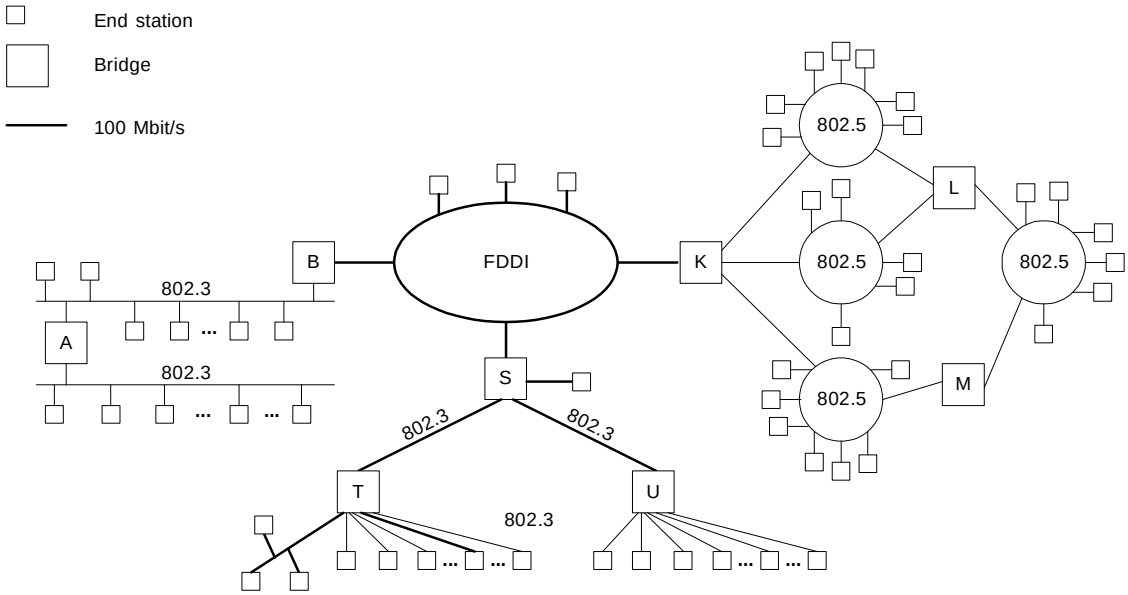


Figure 6—A bridged LAN

6.3.3 Network-layer interconnection: routers

The third category of interconnection uses Network-layer interconnection devices, generally known as routers, that operate as LAN/MAN 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 are often interconnected by routers for the Internet Protocol (IP) and its related routing and management protocols, either directly to other LANs or by means of WAN links.

7. General requirements for an 802® LAN or MAN

7.1 Services supported

With the descriptions in Clause 6 as a basis, an IEEE 802® LAN or MAN can be characterized as a communication resource that provides sufficient capabilities to support the MAC service defined in ISO/IEC 15802-1, between two or more MSAPs. In particular, this requires the ability to convey LLC data from one MSAP to *n* other MSAPs, where *n* can be any number from 1 to all of the other MSAPs on the network. An IEEE 802® LAN is required, at a minimum, to support both LLC Type 1 and the MAC Internal Sublayer Service defined in ISO/IEC 15802-3. In addition, an ISLAN or MAN may optionally support isochronous bearer services compatible with ISDN services as defined in the ITU-T I-series Recommendations.

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.

7.3 Error rates

Error performance of IEEE 802® LANs and MANs is required to be such 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 of an intended receiving peer MAC entity, due only to operation of the Physical layer, shall be less than 8×10^{-8} per octet of MAC frame length.

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.

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.

c) The probability that an 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—For example, (a) the worst-case probability of losing a maximum-length IEEE 802.3® frame (1518 octets) through physical-layer damage 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 7.5×10^{-11}, or approximately 1 in 13 300 000 000.

7.4 Service availability

Insertion of a device into, or removal of a device from, a LAN or MAN shall cause at most a transient loss of availability of the access domain(s) to which the device attaches, lasting not more than 1 s. Failure of a device, including loss of power, shall not cause more than a transient fault for the access domain(s) to which it attaches, with duration of order 1 s.

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 of IEEE 802® LAN and MAN standards.

7.6 Regulatory requirements

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 IEEE 802® wireless LAN standards may be subject to local regulations that pertain to the use of radio-frequency transmission. 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.

8. LAN/MAN management

The provision of an adequate means of remote management is an important factor in the design of today's LAN 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 8.1 and 8.2, respectively.

8.1 General-purpose LAN/MAN management

This subclause introduces the functions of management to assist in the identification of the requirements placed on IEEE 802® LAN/MAN 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.

8.1.1 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-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 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.

8.1.2 Management architecture

The management facilities defined in IEEE 802® LAN and MAN standards are based on the concept of managed objects, which model the semantics of management operations. Operations on a managed object supply information concerning, or facilitate control over, 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 to which the equipment being managed is connected.

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

— The Simple Network Management Protocol (SNMP), as described in RFC 1157

— The OSI 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.

8.1.3 Managed object definitions

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

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

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

The functionality of a managed object can be described in a manner that is independent of the protocol that will be 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:

a) SNMP has standards for the structure of management information known as SMIv1 (RFC 1155, RFC 1212 and RFC 1215) and SMIv2 (RFC 1902, RFC 1903 and RFC 1904), which provides ASN.1-based macros 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 depend on which of the available management protocols the standard will support.

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.

8.2 Special-purpose LAN/MAN management standards

Special-purpose protocols relating to the management functionality of IEEE 802® stations can be developed where the use of a general-purpose management protocol is inappropriate. An example of a special-purpose management protocol is ISO/IEC 15802-4, which defines the services and protocols for remote station loading in a LAN/MAN environment. This protocol permits the simultaneous loading of multiple stations by use of the group-addressing capability in IEEE 802® technologies.

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.

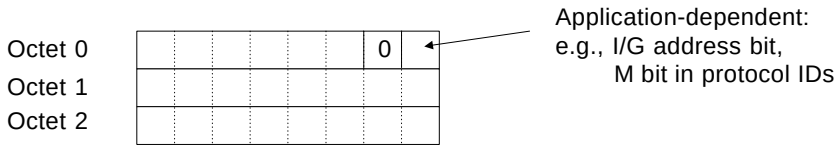


Figure 7—OUI

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.

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

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).

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

9.2 48-bit universal LAN MAC addresses

9.2.1 Concept

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 address can be attached to any LAN in the world with an assurance that the address is unique.

A 48-bit universal address consists of two parts. The first 24 bits correspond to the OUI as assigned by the IEEE, except 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 example of which is shown in Figure 8, the OUI is contained in octets 0, 1, 2, and the value assigned by the assignee is contained in octets 3, 4, 5. This address, including its OUI, is used throughout this document as the basis for examples of LAN MAC addresses and protocol identifiers.

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.

NOTE—The upper, bit-stream representation of the universal address in Figure 8 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 fields (see 6.2.3). See also 9.5 for further discussion of bit-ordering issues. The lower, octet-sequence representation shows the bits within each octet in the usual order for binary numerals; the order of octet transmission is from the top downward.

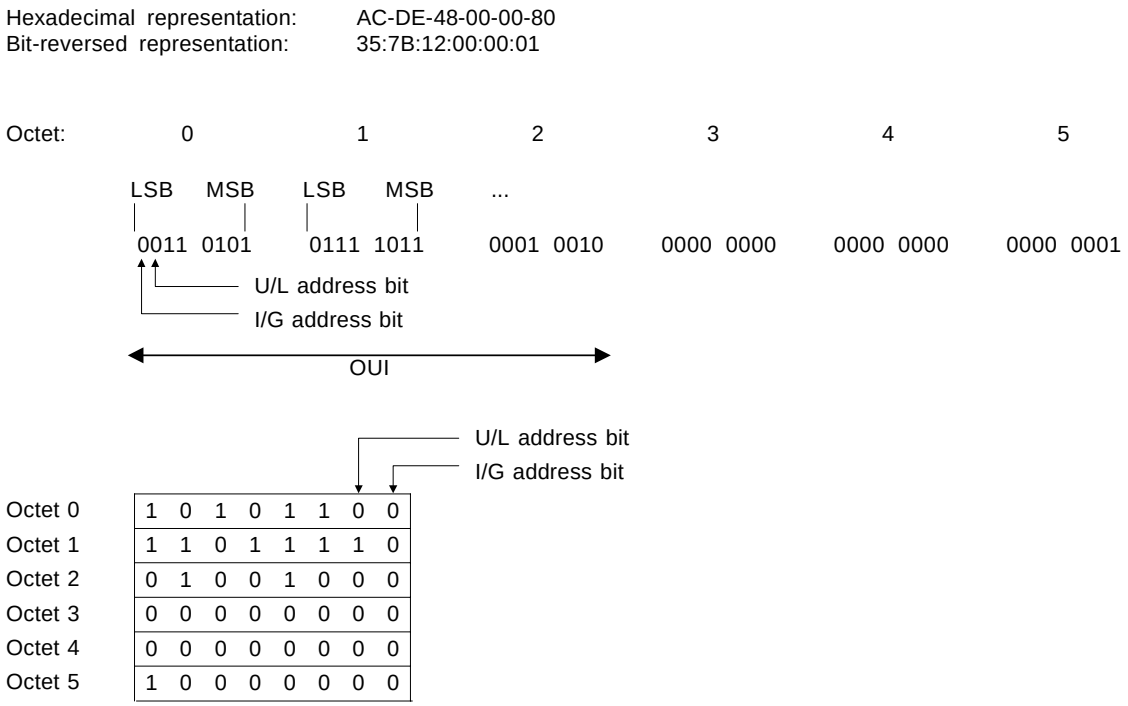


Figure 8—Universal address

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.

9.2.2 Assignment by organizations

Varying the last 24 bits in the block of MAC addresses for a given OUI allows the OUI assignee approximately 16 million unique individual addresses and 16 million unique group addresses that no other organization may assign (i.e., universally unique). The IEEE intends not to assign additional OUIs 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. It is important to note that in no way should these addresses 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 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 carry the same address will, of course, depend on the assignment or manufacturing process, the nature of the organization, and the organization's philosophy. 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.

9.2.3 Uniqueness of address assignment

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

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

NOTE—It is recognized that an alternative approach has gained currency in 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 single LAN MAC address is used to identify all of the system's points of attachment to the LANs in question. This approach, unlike the recommended one, does not automatically meet the requirements of IEEE Std 802.1D-1998™ MAC bridging.

9.3 Protocol identifiers

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 48-bit LAN MAC addresses. 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.

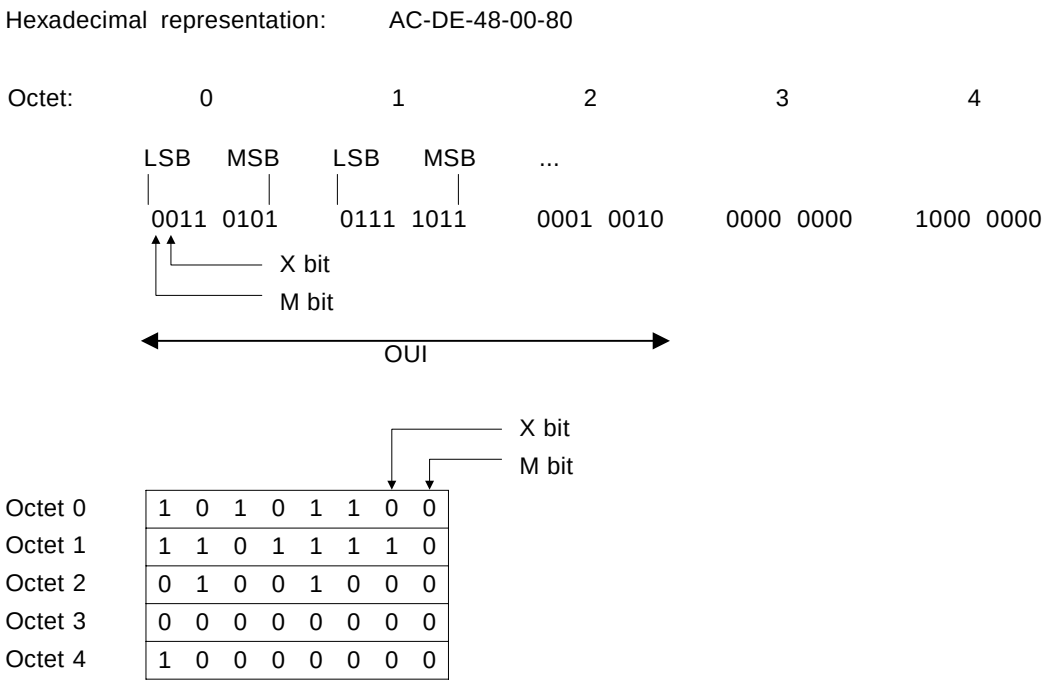


Figure 9—Protocol identifier

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.

9.4 Standard group MAC addresses

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 standard group MAC addresses to be used with standard protocols. The administration of these addresses, including the procedure for application and a list of currently assigned values, is defined in ISO/IEC TR 11802-2. These standard group MAC addresses come from a block of universally administered LAN MAC addresses derived from an OUI 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.

9.5 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.

9.5.1 General considerations

The transmission of data on IEEE 802.3® and 802.4® LAN types is represented (6.2.3) as occurring LSB first within each octet. This is true for the entire frame: LAN MAC address fields (source and destination), MAC-specific fields (e.g., length 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, each octet of the MAC Information field is represented as being transmitted MSB first. The LAN MAC address fields (source and destination), 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 IEEE 802.3® and IEEE 802.4® LANs. For frames that originate within the MAC (e.g., MAC-embedded management frames), the ordering of bits within the MAC Information field is defined by the MAC specification—ISO/IEC 8802-5, etc.

For most purposes, the difference in the bit-orderings 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.

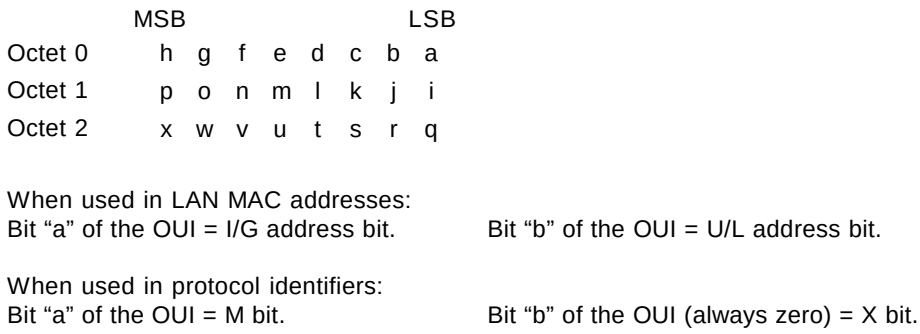


Figure 10—Bit significance of an OUI

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

.

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

(B) OUI within a MAC Address field:

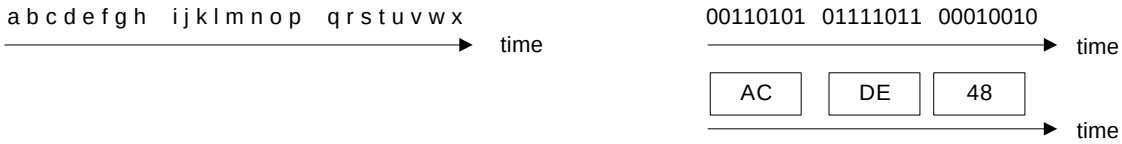
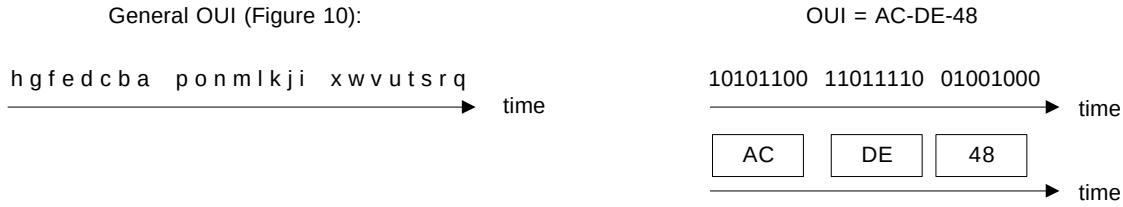


Figure 11—IEEE 802.3®, etc., frame: Order of bit and octet transmission for an OUI

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



(B) OUI within a MAC Address field:

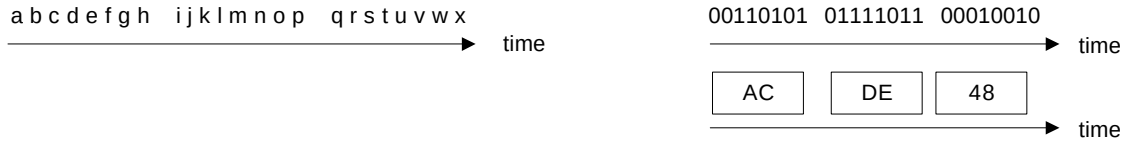


Figure 12—IEEE 802.5®, etc., frame: Order of bit and octet transmission for an OUI

OUI within a MAC address contained in the MAC Information field:

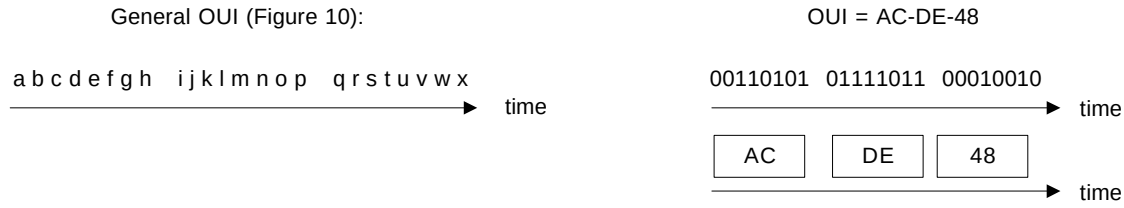


Figure 13—IEEE 802.3®, etc., frame: Order of bit and octet transmission for an OUI in a MAC address contained in a MAC Information field

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.

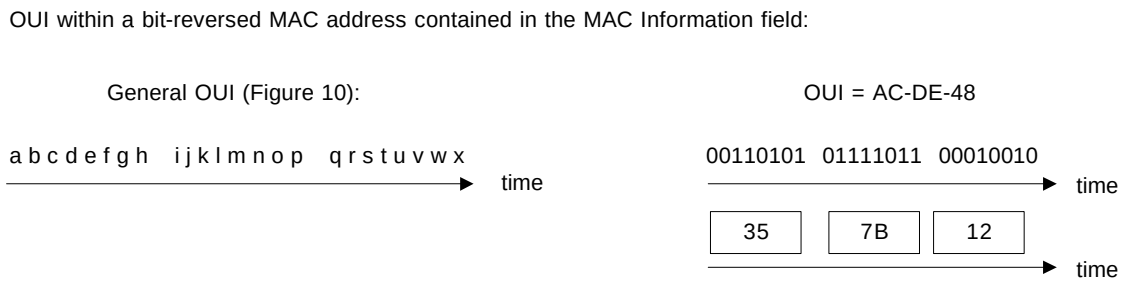


Figure 14—IEEE 802.5®, etc., frame: Order of bit and octet transmission for an OUI in a MAC address contained in a MAC Information field (noncanonical format)

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.

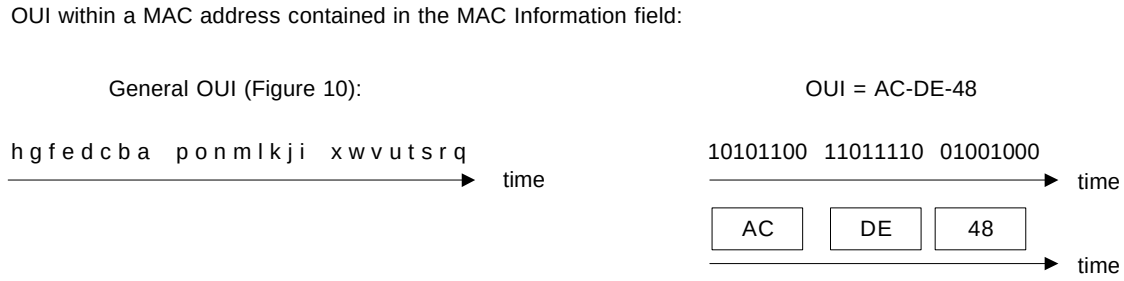


Figure 15—FDDI frame: Order of bit and octet transmission for an OUI in a MAC address contained in a MAC Information field (canonical format)

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.

9.5.3 Recommendation

Designers of protocols that operate above the Data Link layer 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.

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

10.1 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.

By providing for the coexistence of multiple Network layer protocols, the migration of existing LANs to future standard protocols is facilitated, and multiple higher layer protocols are more easily accommodated.

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 layer protocols have been assigned reserved LLC addresses, as recorded in ISO/IEC TR 11802-1. 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.

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 a protocol identifier that enables SNAP to discriminate among these protocols.

10.3.2 SNAP PDU format

Each SNAP PDU shall conform to 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 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.

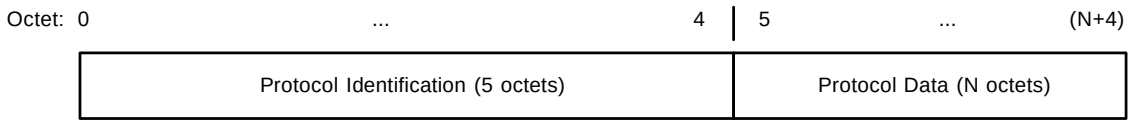


Figure 16—SNAP PDU format

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.

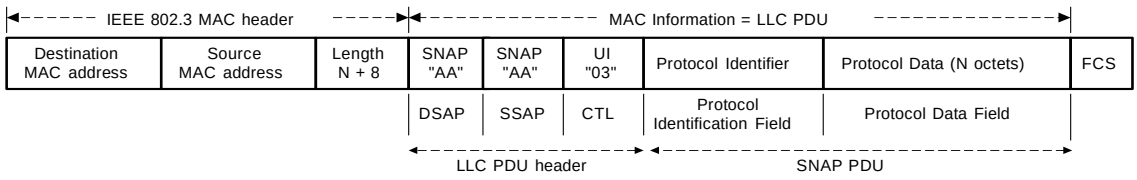


Figure 17—SNAP PDU in IEEE 802.3® MAC frame

10.4 Ethernet types: Format, function, and administration

The IEEE 802.3® MAC frame format is compatible with the alternative Ethernet MAC frame format, in the sense that frames of both formats can be freely intermixed on a given LAN and at a given LAN station. The service provided by use of the Ethernet frame format differs from the ISO/IEC 15802-1 MAC service in that there is a 16-bit type value associated with each frame transferred, and that the minimum amount of MAC-sublayer user data transferred is 64 octets.

An Ethernet type value is a sequence of two 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 range 0–1535 are not available for use.

The function of the Ethernet type value is to identify the protocol that is to be invoked to process the user data in the frame.

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.

10.5 Encapsulation of Ethernet frames over LLC

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

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

a) The Protocol Identification field of the SNAP PDU shall contain a protocol 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 two octets of the Ethernet frame's Ethernet type.

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

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

NOTES

1—This encapsulation was originally specified in RFC 1042, which contains recommendations relating to its use. Further recommendations are contained in RFC 1390.

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

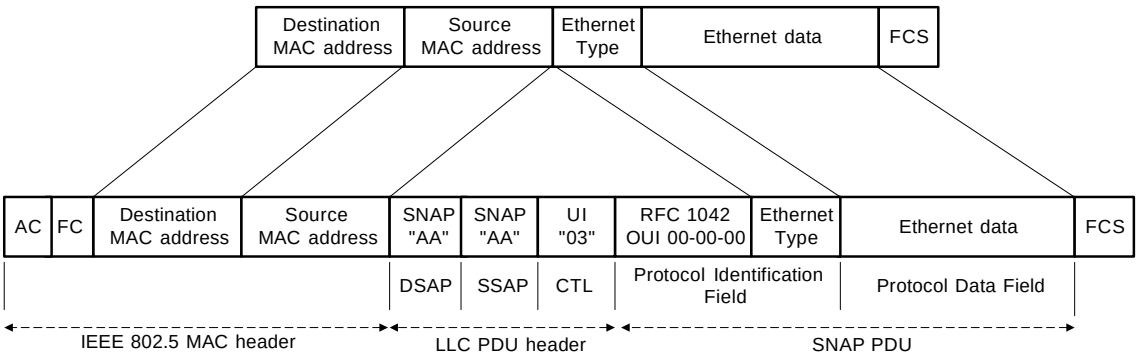


Figure 18—Ethernet frame SNAP-encapsulated in IEEE 802.5® frame

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.

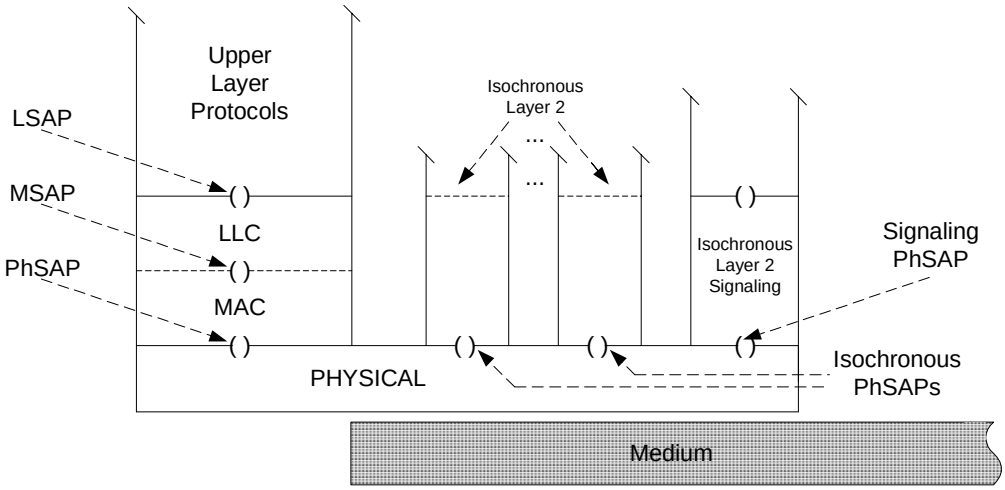


Figure 19—ISLAN RM (end station)

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

[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.

[B9] ISO/IEC 8802-9:1996 (IEEE Std 802.9-1996™), Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 9: Integrated Services (IS) LAN Interface at the Medium Access Control (MAC) and Physical (PHY) Layers.

[B10] ISO/IEC 8802-11:1999 (IEEE Std 802.11-1999™), Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) 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/).

[B11] ISO/IEC 8802-12:1998 (IEEE Std 802.12-1998™), 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.

[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.

[B18] RFC 1042, A Standard for the Transmission of IP Datagrams over IEEE 802® Networks. Postel, J., and Reynolds, J., February 1988.[7]

[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.

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.

[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 information, call the IETF secretariat at +1-703-620-8990.

[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 Systems Interconnection—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™), Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common 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.

[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., July 1994.

[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.