

Abstract: Services and protocol elements that permit the exchange of management information between stations attached to ISO/IEC standard local and metropolitan area networks are defined. The standard includes the specification of managed objects that permit the operation of the protocol elements to be remotely managed. In addition, an architecture for station discovery and the dynamic control of event forwarding is defined. Services and protocols that support station discovery and the dynamic control of event forwarding are defined.

Keywords: event forwarding; local area networks, management; metropolitan area networks, management

The Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street, New York, NY 10017-2394, USA

Copyright © 1995 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 1995. Printed in the United States of America.

ISBN 1-55937-501-9

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

DATE TBD

SH94259

International Standard ISO/IEC 15802-2 : 1995
ANSI/IEEE Std 802.1B, 1995 edition
(Incorporating ANSI/IEEE Std 802.1B-1992 and 802.1k-1993)

**Information technology—
Telecommunications and information
exchange between systems—
Local and metropolitan area networks—
Common specifications—**

Part 2: LAN/MAN management

Sponsor

**Technical Committee on Computer Communications
of the
IEEE Computer Society**

International Standard ISO/IEC 15802-2 : 1995

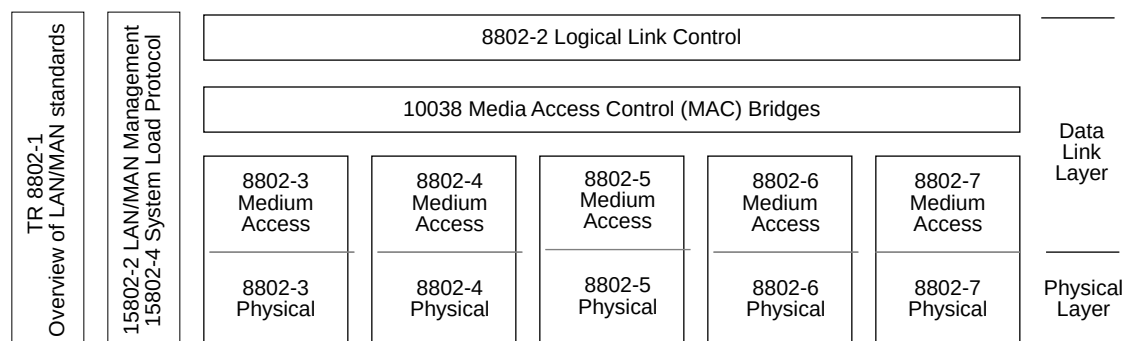
ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75% of the national bodies casting a vote.

In 1993, ANSI/IEEE Std 802.1B-1992 and 802.1k-1993 were adopted by ISO/IEC JTC 1, as Draft International Standard ISO/IEC DIS 15802-2. A further revision was subsequently approved by ISO/IEC JTC 1 in the form of this new edition, which is published as International Standard ISO/IEC 15802-2 : 1995.

Foreword to International Standard ISO/IEC 15802-2 : 1995

This International Standard is part of a family of International Standards for Local and Metropolitan Area Networks. The relationship between this International Standard and the other members of the family is shown below. (The numbers in the figure refer to ISO Standard numbers.)



This family of International Standards deals with the Physical and Data Link layers as defined by the ISO Open Systems Interconnection Basic Reference Model (ISO 7498 : 1984). The access standards define five types of medium access technologies and associated physical media, each appropriate for particular applications or system objectives. Other types are under investigation.

The International Standards defining the access technologies are as follows:

- ISO/IEC 8802-3 [ANSI/IEEE Std 802.3, 1993 Edition], a bus utilizing CSMA/CD as the access method.
- ISO/IEC 8802-4 [ANSI/IEEE Std 802.4-1990], a bus utilizing token passing as the access method.
- ISO/IEC 8802-5 [ANSI/IEEE Std 802.5-1992], a ring utilizing token passing as the access method.
- ISO/IEC 8802-6 [ANSI/IEEE Std 802.6, 1994 Edition], a dual bus utilizing distributed queuing as the access method.
- ISO 8802-7, a ring utilizing slotted ring as the access method.

ISO/IEC TR 8802-1 provides an overview of the LAN/MAN standards, along with details of their document numbering.

ISO/IEC 8802-2 [ANSI/IEEE Std 802.2, 1994 Edition], *Logical Link Control*, is used in conjunction with the medium access standards to provide the data link layer service to network layer protocols.

ISO/IEC 10038 [ANSI/IEEE Std 802.1D, 1993 Edition], *Media Access Control (MAC) bridges*, specifies an architecture and protocol for the interconnection of IEEE 802 LANs below the level of the logical link control protocol.

ISO/IEC 15802-2 [ANSI/IEEE Std 802.1B, 1995 Edition], *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.

ISO/IEC 15802-4 [ANSI/IEEE Std 802.1E, 1994 Edition], *System Load Protocol*, specifies a set of services and protocol for those aspects of management concerned with the loading of systems in ISO/IEC LAN/MAN environments.

The main body of the International Standard serves for both the ISO/IEC 15802-2 : 1994 and IEEE Std 802.1B, 1995 Edition standards. ISO and IEEE each have a unique foreword.

ANSI/IEEE Std 802.1B, 1995 Edition

IEEE Standards documents are developed within the Technical Committees of the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE that have expressed an interest in participating in the development of the standard.

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

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.

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 all 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 technical 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 on standards and requests for interpretations should be addressed to:

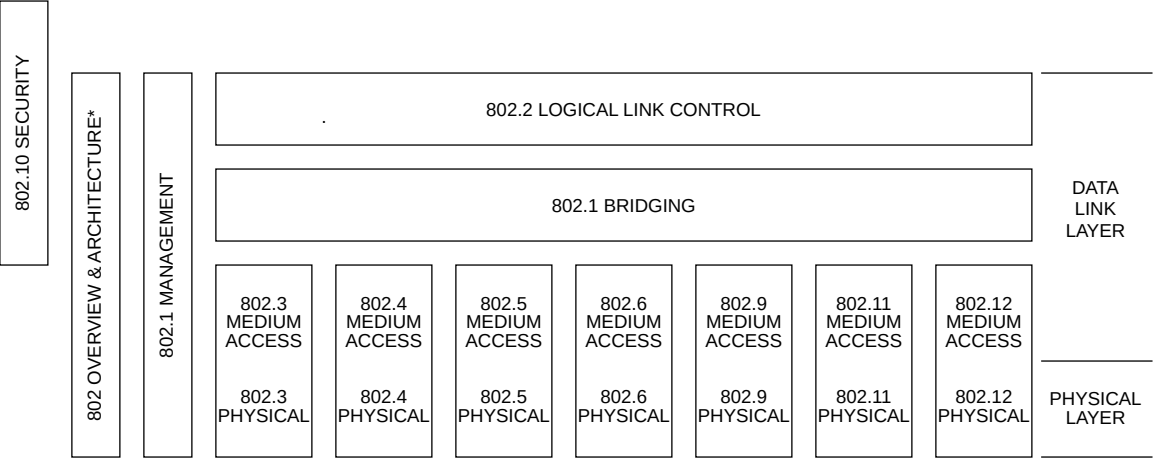
Secretary, IEEE Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

IEEE Standards documents may involve the use of patented technology. Their approval by the Institute of Electrical and Electronics Engineers does not mean that using such technology for the purpose of conforming to such standards is authorized by the patent owner. It is the obligation of the user of such technology to obtain all necessary permissions.

Foreword to ANSI/IEEE Std 802.1B, 1995 Edition

(This foreword is not a part of ANSI/IEEE Std 802.1B, 1995 Edition.)

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 7498 : 1984). 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 802¹: Overview and Architecture. This standard provides an overview to the family of IEEE 802 Standards. This document forms part of the 802.1 scope of work.
- ANSI/IEEE Std 802.1B [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.
- ANSI/IEEE Std 802.1D [ISO/IEC 10038]: MAC Bridging. Specifies an architecture and protocol for the interconnection of IEEE 802 LANs below the MAC service boundary.
- ANSI/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.

¹The 802 Architecture and Overview standard, 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.

- ANSI/IEEE Std 802.2 [ISO/IEC 8802-2]: Logical Link Control
- ANSI/IEEE Std 802.3 [ISO/IEC 8802-3]: CSMA/CD Access Method and Physical Layer Specifications
- ANSI/IEEE Std 802.4 [ISO/IEC 8802-4]: Token Bus Access Method and Physical Layer Specifications
- ANSI/IEEE Std 802.5 [ISO/IEC 8802-5]: Token Ring Access Method and Physical Layer Specifications
- ANSI/IEEE Std 802.6 [ISO/IEC 8802-6]: Distributed Queue Dual Bus Access Method and Physical Layer Specifications
- IEEE Std 802.9: Integrated Services (IS) LAN Interface at the Medium Access Control (MAC) and Physical (PHY) Layers
- IEEE Std 802.10: Interoperable LAN/MAN Security, *Currently approved:* Secure Data Exchange (SDE)

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 following additional working groups have authorized standards projects under development:

- IEEE 802.11: Wireless LAN Medium Access Control (MAC) Sublayer and Physical Layer Specifications
- IEEE 802.12: Demand Priority Access Method/Physical Layer Specifications

Conformance test methodology

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

ANSI/IEEE Std 15802-2 : 1995 Edition

This document defines services and protocol elements that permit the exchange of management information between stations attached to IEEE 802 local and metropolitan area networks. The standard includes the specification of managed objects that permit the operation of the protocol elements to be remotely managed.

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

This standard contains state-of-the-art material. The area covered by this standard is undergoing evolution. Revisions are anticipated within the next few years to clarify existing material, to correct possible errors, and to incorporate new related material. Information on the current revision state of this and other IEEE 802 standards may be obtained from

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

IEEE 802 committee working documents are available from

IEEE Document Distribution Service
AlphaGraphics #35 Attn: P. Thrush
10201 N. 35th Avenue
Phoenix, AZ 85051
USA

Participants

The following is a list of participants in the Network Management effort of the IEEE Project 802 Working Group at the time of 802.1B's approval. Voting members at the time of publication are marked with an asterisk (*). Those who were participants at the time of 802.1k's approval are marked with a dagger (†).

William P. Lidinsky, Chair*†

Tony Jeffree, Chair, Network Management Task Group*†

Fumio Akashi	Kathy de Graaf	Ronald Presti†
Paul D. Amer	Rich Graham	Ron L. G. Prince
Charles Arnold	Michael A. Gravel	Maurice Qureshi†
Naharaj Arunkumar	Andrew Green†	Nigel Ramsden
Floyd Backes*†	Sharam Hakimi*†	Rich Rehberg
Ann Ballard	Jeanne Haney†	Jim Reinstedler
Richard Bantel	Mogens Hansen	Trudy Reusser
Robert Barrett*†	Harold Harrington	Eduard Rocher
David Bartolini	John Hart*†	Paul Rosenblum*†
Sy Bederman	Mike Harvey†	Paul Ruocchio*†
Amatzia Ben-Artzi†	Bob Herbst	Tom Rutt*†
Anthony Berent†	Long Huang†	John Salter
Orna Berry*†	Jack R. Hung	Alan Sarsby
Robert Bledsoe	Thomas Hytry	Susan Schanning
Kwame Boakye	Jay Israel	Mick Seaman*†
Laura Bridge*†	Jan-Olof Jemnemo*†	Gerry Segal*†
Brian Brown†	Albert Juandy†	Rich Seifert*†
Juan Bulnes	George Kajos†	Steve Senum*†
Fred Burg	Ram Kedlaya	Himanshu Shah*†
Peter Carbone	Hal Keen*†	Howard Sherry
Alan Chambers*†	Alan Kirby	Wu-Shi Shung
Ken Chapman	Kimberly Kirkpatrick	W. Earl Smith*†
Alice Chen	Steve Kleiman	Mike Soha
Michael Chernick	Yoav Kluger†	Dan Stokesberry
Jade Chien	James Kristof†	Lennart Swartz
Steve Cooper*†	Hans Lackner*†	Kenta Takumi
Jim Corrigan	H. Eugene Latham	Elysia Chiaw-Meng Tan
Paul Cowell*†	Choon Lee†	Robin Tasker*†
Mike Coy†	Chao-yu Liang	Angus Telfer
Andy Davis*†	Bing Liao	Dave Thompson
Peter Dawe	George Lin*†	Geoff Thompson†
Stan Degen	Mike Lumpkin	Nathan Tobol
Frank Deignan	Andy Luque	Wendell Turner
Desh Deshpande	Phil Magnuson	Peter Videcrantz*†
Ron Dhondy	Joseph E. Massery†	Donald G. Vincent†
Mike Dickerson	Bruce McClure	Paul Wainright
Kurt Dobbins	Tom McGowan	Trevor Warwick†
Eiji Doi	Margaret A. Merrick	Scott Wasson
Barbara J. Don Carlos	Jim Montrose	Bob Watson
David Dyer-Bennet	Jerry O'Keefe	Richard Watson*
Walter Eldon	Alan Oppenheimer*†	Daniel Watts
Eldon D. Feist	Richard Patti*†	Alan Weissberger
Len Fishler*†	Dave T. Perkins†	Deborah Wilbert
Kevin Flanagan	Roger Pfister	Bert Williams†
Bill Futral*†	Thomas L. Phinney	Jerry A. Wyatt†
Lionel Geretz*†	Clive Philbrick	Amnon Yacoby*†
Richard Gilbert*†	John Pickens*	Igor Zhovnirovsky
Harry Gold†	David Piscitello	Carolyn Zimmer*†
Pat Gonia	Daniel Pitt	Nick Zuccherio
	Vencat Prasad*†	

Additional participants in the development of 802.1k included the following:

Sai Boeker

Mike Dickerson
Bonnie B. Hromis

Brian J. Phillips

The following persons were on the balloting committee of 802.1B. Those who also balloted 802.1k are marked with an asterisk.

W. B. Adams*	R. Juvonen	D. Rosich*
D. Aelmore*	K. H. Kellermayr*	V. Rozentouler
H. Alkhatib	G. C. Kessler*	D. J. Rypka
K. Athul*	R. W. Klessig	D. Sanford
J. D. Brock	J. Y. Lee*	R. Sankar
P. Campbell*	F. C. Lim	J. G. Sanz
B. J. Casey*	R. S. Little*	B. P. Schanning*
A. Castaldo	J. Loo	C. Scheel
K. Chon*	D. C. Loughry*	N. Schneidewind
R. Ciciliani	N. C. Low*	G. D. Schumacher
M. H. Coden*	W. Lu*	J. R. Schwab*
R. Crowder*	G. Luderer	A. S. Sethi*
L. F. M. De Moraes	J. F. P. Luhukay*	D. A. Sheppard*
A. M. Dunn	A. J. Luque*	L. Sintonen
P. Eastman*	K. G. McDonald	H. P. Solomon*
L. G. Egan	W. McDonald*	C. M. Stillebroer*
J. E. Emrich*	R. H. Miller*	F. J. Strauss*
P. H. Enslow*	D. S. Millman*	E. Sykas*
C. Fan*	C. B. M. Mishra*	A. N. Tantawy
J. W. Fendrich*	K. Mori*	P. Thaler
H. C. Folts*	G. Moseley	G. O. Thompson*
H. A. Freeman*	A. C. Nigam	B. A. Trent*
I. Fromm*	E. S. Nolley*	R. Tripi*
G. Fullerton*	D. O'Mahony*	M. Uchida*
P. Fung	C. Oestereicher*	L. D. Umbaugh*
R. Gagliano*	Y. Oh*	C. M. Weaver, Jr.
W. W. Garman	A. J. Pina*	D. F. Weir*
I. Ghansah	U. W. Pooch*	A. J. Weissberger
P. Gonja*	V. Punj*	R. Wenig*
A. W. Hathaway	A. Putnins*	E. J. Whitaker*
P. L. Hutton	T. L. D. Regulinski*	P. A. Willis*
R. J. Iliff	G. S. Robinson*	J. A. Wyatt
A. A. Jeffree*	P. T. Robinson*	O. Yuen*
J. R. Johnson		W. Zhao

In addition to those indicated above, the following persons were on the balloting committee of 802.1k:

R. M. Amy	G. Lau	E. J. Reilly
W. E. Ayen	D. B. McIndoe	R. Rosenthal
M. Diaz	W. H. L. Moh	F. Ross
J. Gonzalez Sanz	J. E. Montague	C. Spurgeon
C. Guarnieri	D. T. Perkins	J. T. Vorhies
L. M. Lam	J. Pickens	A. D. Waren
	P. K. Piele	

When the IEEE Standards Board approved 802.1B on September 17, 1992, it had the following membership:

Marco W. Migliaro, Chair

Donald C. Loughry, Vice Chair

Andrew G. Salem, Secretary

Dennis Bodson
Paul L. Borrill
Clyde R. Camp
Donald C. Fleckenstein
Jay Forster*
David F. Franklin
Ramiro Garcia
Thomas L. Hannan

Donald N. Heirman
Ben C. Johnson
Walter J. Karplus
Ivor N. Knight
Joseph L. Koepfinger*
Irving Kolodny
D. N. "Jim" Logothetis
Lawrence V. McCall

Don T. Michael*
L. John Rankine
Wallace S. Read
Ronald H. Reimer
Gary S. Robinson
Martin V. Schneider
Terrance R. Whittemore
Donald W. Zipse

*Member Emeritus

Also included are the following nonvoting IEEE Standards Board liaisons:

Satish K. Aggarwal
James Beall
Richard B. Engelman
David E. Soffrin
Stanley I. Warshaw

Kristin M. Dittmann
IEEE Standards Project Editor

When the IEEE Standards Board approved 802.1k on June 17, 1993, it had the following membership:

Wallace S. Read, Chair

Donald C. Loughry, Vice Chair

Andrew G. Salem, Secretary

Gilles A. Baril
Clyde R. Camp
Donald C. Fleckenstein
Jay Forster*
David F. Franklin
Ramiro Garcia
Donald N. Heirman
Jim Isaak

Ben C. Johnson
Walter J. Karplus
Lorraine C. Kevra
E. G. "Al" Kiener
Ivor N. Knight
Joseph L. Koepfinger*
D. N. "Jim" Logothetis

Don T. Michael*
Marco W. Migliaro
L. John Rankine
Arthur K. Reilly
Ronald H. Reimer
Gary S. Robinson
Leonard L. Tripp
Donald W. Zipse

*Member Emeritus

Also included are the following nonvoting IEEE Standards Board liaisons:

Satish K. Aggarwal
James Beall
Richard B. Engelman
David E. Soffrin
Stanley I. Warshaw

Kristin M. Dittmann
IEEE Standards Project Editor

IEEE Std 802.1B-1992 was approved by the American National Standards Institute on February 23, 1993.

IEEE Std 802.1k-1993 was approved by the American National Standards Institute on January 4, 1994.

Contents

CLAUSE	PAGE
1. Scope.....	1
2. References.....	2
3. Definitions.....	4
3.1 Definitions related to local and metropolitan area networks	4
3.2 Logical Link Control definitions	4
3.3 Basic Reference Model definitions.....	4
3.4 Management Framework definitions	4
3.5 Systems Management Overview definitions	4
3.6 Structure of Management Information (SMI) Information Model definitions	4
3.7 Common Management Information Service (CMIS) definitions	5
3.8 Abstract Syntax Notation One (ASN.1) definitions	5
3.9 Guidelines for the Definition of Managed Objects (GDMO) definitions.....	5
3.10 Conformance testing definitions	5
3.11 Terms defined in this International Standard.....	5
3.12 Acronyms and abbreviations.....	6
4. LAN/MAN Management and Systems Management	7
5. Architecture.....	8
5.1 Management communication.....	8
5.2 Management information and management operations.....	10
5.3 Relationship with CMIS/CMIP.....	12
5.4 Relationship with other management protocols.....	13
6. Services	13
6.1 LAN/MAN Management service.....	13
6.2 Convergence function and convergence service.....	13
6.3 Relationship between LMMS services and the managed object boundary	16
7. Protocol.....	18
7.1 LMMP definition	18
7.2 Use of underlying services by the LMMP	18
7.3 Convergence protocol definition.....	19
7.4 Use of underlying services by the CPE.....	30
8. LAN/MAN Management managed object definitions.....	32
8.1 Overview of managed object structure	32
8.2 LAN/MAN Management managed object class definition	33
8.3 Specific CPE Info managed object class	34
8.4 Resource Type ID managed object class	34
8.5 Access class table entry managed object class definition	35
8.6 Notification type table entry managed object class definition.....	37

CLAUSE	PAGE
8.7 Event report destination table entry managed object class definition.....	38
8.8 Data definitions for the LMM managed objects	39
9. Event forwarding and access control	41
9.1 Event forwarding	41
9.2 Access control.....	42
10. Conformance.....	44
10.1 Static conformance.....	44
10.2 Protocol implementation conformance statement.....	45
10.3 Dynamic conformance	45
11. Discovery and dynamic control of event forwarding	46
11.1 Scope.....	46
11.2 Architecture.....	46
11.3 Service definition	50
11.4 Protocol specification.....	60
11.5 Management information definitions for DEFED	65
11.6 Management information definitions for Extended Notification Type table.....	71
11.7 ASN.1 definitions	72
12. Use of group addresses for LAN/MAN Management	73
ANNEX	
A. PICS proforma	74
A.1 Introduction.....	74
A.2 Abbreviations and special symbols.....	74
A.3 Instructions for completing the PICS proforma.....	74
A.4 Identification	76
A.5 Major capabilities.....	77
A.6 Convergence protocol details.....	78
A.7 Convergence protocol parameters	78
A.8 Managed object support.....	79
B. Allocation of object identifier values.....	80
B.1 Introduction.....	80
B.2 Allocation tables	80

Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Common specifications— Part 2: LAN/MAN management

1. Scope

This International Standard defines an Open Systems Interconnection (OSI) management-compatible architecture, and service and protocol elements for use in a LAN/MAN environment for the purpose of performing remote management of LAN-based or MAN-based devices. The protocol described is a connectionless-mode management protocol that makes use of Logical Link Control (LLC) Type 1 procedures as a means of conveying management information between stations in a LAN/MAN environment, thus providing for interworking of ISO/IEC standard LAN/MAN devices for management purposes. The management information is conveyed using the protocol data unit (PDU) formats defined in ISO/IEC 9596-1 : 1991.¹ To this end, this International Standard

- a) Describes the services required for the transfer of management information between management processes in LAN/MAN stations.
- b) Defines the protocol and PDUs for conducting management information exchanges that support the provision of those services. This protocol is defined as an (N)-layer management protocol specific to the management of layers 1 and 2 in a LAN/MAN environment.
- c) Defines a convergence protocol and PDUs used for the exchange of management PDUs.
- d) Describes the underlying services required for transfer of management PDUs between peer-management entities by means of the convergence protocol.
- e) Defines an access control mechanism and an event report forwarding mechanism that operate in conjunction with the management protocol.
- f) Defines managed object classes that relate to the operation of the management protocol and the convergence protocol.

This International Standard provides the PICS proforma for the System Load Protocol in compliance with the relevant requirements, and in accordance with the relevant guidance, given in ISO/IEC 9646-2 : 1991.

NOTES

1—This International Standard provides only a set of management tools. The management operations that are specified by this International Standard are only meaningful in conjunction with the managed object definitions contained in the appropriate layer standards.

2—This International Standard defines an (N)-layer management protocol for the management of stations attached to ISO/IEC standard LAN or MAN subnetworks, in accordance with the terminology contained in the OSI Management Framework, ISO/IEC 7498-4 : 1989 and the OSI Systems Management Overview, ISO/IEC 10040 : 1992. The service and protocol described in this International Standard are based upon the OSI Common Management Information Service and Protocol standards (ISO/IEC 9595 : 1991 and ISO/IEC 9596-1 : 1991), and are therefore designed to be used in conjunction with managed objects defined in accordance with the Guidelines for the definition of managed objects (ISO/IEC 10165-4 : 1992). As such, this International Standard is intended to be complementary to the functionality of the OSI Management standards being developed in ISO/IEC JTC1 SC21/WG4.

¹Information on references can be found in clause 2.

3—To evaluate conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented for a given protocol. Such a statement is called a Protocol Implementation Conformance Statement (PICS). Annex A to this International Standard contains the PICS proforma for the LAN/MAN Management Protocol.

2. References

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

IEEE Std 802-1990, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture (ANSI).²

IEEE Std 802.1F-1993, IEEE Standards for Local and Metropolitan Area Networks: Common Definitions and Procedures for IEEE 802 Management Information (ANSI).

IEEE Std 802.10-1992, IEEE Standards for Local and Metropolitan Area Networks: Standard for Interoperable LAN/MAN Security (SILS), *Currently Contains Secure Data Exchange (SDE) (Clause 2)* (ANSI).

ISO 6093 : 1985, Information processing systems—Representation of numerical values in character strings for information interchange.³

ISO 7498 : 1984, Information processing systems—Open Systems Interconnection—Basic Reference Model.

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

ISO/IEC 8802-2 : 1994 [ANSI/IEEE Std 802.2, 1994 Edition], Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.

ISO/IEC 8824 : 1990, Information technology—Open Systems Interconnection—Specification of Abstract Syntax Notation One (ASN.1).

ISO/IEC 8825 : 1990, Information technology—Open Systems Interconnection—Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).

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

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

ISO/IEC 9596-2 : 1993, Information technology—Open Systems Interconnection—Common management information protocol—Part 2: Protocol Implementation Conformance Statement (PICS) proforma.

ISO/IEC 9646-1 : 1991, Information technology—Open Systems Interconnection—Conformance testing methodology and framework—Part 1: General concepts.

²IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA.

³ISO and ISO/IEC publications are available from the ISO Central Secretariat, 1 rue de Varembé, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse. In the US, they are available from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

ISO/IEC 9646-2 : 1991, Information technology—Open Systems Interconnection—Conformance testing methodology and framework—Part 2: Abstract test suite specification.

ISO/IEC 10038 : 1993 [ANSI/IEEE Std 802.1D, 1993 Edition], Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Media access control (MAC) bridges.

ISO/IEC 10040 : 1992, Information technology—Open Systems Interconnection—Systems management overview.

ISO/IEC 10164-1 : 1993, Information technology—Open Systems Interconnection—Systems management—Part 1: Object Management Function.

ISO/IEC 10164-1 : 1993, Information technology—Open Systems Interconnection—Systems management—Part 2: State Management Function.

ISO/IEC 10164-3 : 1993, Information technology—Open Systems Interconnection—Systems management—Part 3: Attributes for Representing Relationships.

ISO/IEC 10164-4 : 1992, Information technology—Open Systems Interconnection—Systems management—Part 4: Alarm Reporting Function.

ISO/IEC 10164-5 : 1993, Information technology—Open Systems Interconnection—Systems management—Part 5: Event Report Management Function.

ISO/IEC 10164-6 : 1993, Information technology—Open Systems Interconnection—Systems management—Part 6: Log Control Function.

ISO/IEC 10164-7 : 1992, Information technology—Open Systems Interconnection—Systems management—Part 7: Security Alarm Reporting Function.

ISO/IEC 10165-1 : 1993, Information technology—Open Systems Interconnection—Management information services—Structure of management information—Part 1: Management Information Model.

ISO/IEC 10165-2 : 1992, Information technology—Open Systems Interconnection—Management information services—Structure of management information—Part 2: Definition of management information.

ISO/IEC 10165-4 : 1992, Information technology—Open Systems Interconnection—Management information services—Structure of management information—Part 4: Guidelines for the definition of managed objects.

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

ISO/IEC 15802-4 : 1994 [ANSI/IEEE Std 802.1E, 1994 Edition], Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 4: System load protocol.

ISO/IEC TR 10178 : 1992, Information technology—Telecommunications and information exchange between systems—The structure and coding of Logical Link Control addresses in Local Area Networks.

ISO/TR 8509 : 1987, Information processing systems—Open Systems Interconnection—Service conventions.

ITU-T Recommendation X.219 (1988), Remote Operations: Model, Notation and Service Definition, *Blue Book*, Vol. VIII.4.⁴

⁴ITU-T publications are available from the International Telecommunications Union, Sales Section, Place des Nations, CH-1211, Genève 20, Switzerland/Suisse. They are also available in the United States from the U.S. Department of Commerce, Technology Administration, National Technical Information Service (NTIS), Springfield, VA 22161, USA.

3. Definitions

3.1 Definitions related to local and metropolitan area networks

Many of the specialized terms used in this International Standard are defined in IEEE Std 802-1990.

3.2 Logical Link Control definitions

This International Standard makes use of the following terms defined in ISO/IEC 8802-2 : 1994:

- a) LLC address
- b) LSAP address

3.3 Basic Reference Model definitions

This International Standard makes use of the following terms defined in ISO 7498 : 1984:

- a) open system
- b) systems management

3.4 Management Framework definitions

This International Standard makes use of the following terms defined in ISO/IEC 7498-4 : 1989:

- a) managed object
- b) management information base

3.5 Systems Management Overview definitions

This International Standard makes use of the following terms defined in ISO/IEC 10040 : 1992:

- a) agent
- b) (N)-layer management protocol
- c) managed object class
- d) management information
- e) manager
- f) notification
- g) notification type
- h) (systems management) operation
- i) systems managed object
- j) systems management protocol

3.6 Structure of Management Information (SMI) Information Model definitions

This International Standard makes use of the following terms defined in ISO/IEC 10165-1 : 1993:

- a) behaviour
- b) containment
- c) managed object boundary
- d) name binding

- e) package
- f) subordinate object
- g) superior object

3.7 Common Management Information Service (CMIS) definitions

This International Standard makes use of the following terms defined in ISO/IEC 9595 : 1991:

- a) attribute
- b) Common Management Information Services

3.8 Abstract Syntax Notation One (ASN.1) definitions

This International Standard makes use of the following terms defined in ISO/IEC 8824 : 1990:

- a) object identifier
- b) type

3.9 Guidelines for the Definition of Managed Objects (GDMO) definitions

This International Standard makes use of the following terms defined in ISO/IEC 10165-4 : 1992:

- a) managed object class definition
- b) template

3.10 Conformance testing definitions

This International Standard uses the following terms defined in ISO/IEC 9646-1 : 1991:

- a) PICS proforma
- b) protocol implementation conformance statement (PICS)
- c) static conformance review

3.11 Terms defined in this International Standard

The following terms are used throughout this document in a specialized manner:

3.11.1 affiliate: A remote convergence protocol entity (CPE) whose CPE address is known to the local CPE.

3.11.2 affiliation: A state that exists if both remote and local CPEs know each other's CPE addresses.

3.11.3 asynchronous: Protocol operation in which more than one exchange between a given pair of entities can be handled simultaneously.

3.11.4 convergence protocol: A protocol that provides the convergence service.

3.11.5 convergence service: A service that provides enhancements to an underlying service in order to provide for the specific requirements of the convergence service user.

3.11.6 CPE address: The LSAP address at which the CPE may be reached.

3.11.7 CPE instance identifier: The tuple of CPE address and CPE instance number that uniquely identifies a CPE instance within the LAN/MAN environment, within the limits of uniqueness of the CPE address and instance values used.

3.11.8 CPE instance number: A number, allocated to the CPE at instantiation time, that distinguishes a CPE instance from all other CPE instances, past and present, associated with a particular CPE address.

3.11.9 LAN/MAN Management: The management functionality specific to the management of IEEE 802 Local or Metropolitan Area subnetworks.

3.11.10 resource: That part of a LAN/MAN environment for which a managed object provides the management view. The management view of a resource may be limited to a subset of the functionality of the resource; some aspects of the resource may therefore be inaccessible for management purposes.

3.11.11 synchronous: Protocol operation in which only one exchange between a given pair of entities can be handled at any moment in time. The current exchange must complete before the next can be initiated.

3.12 Acronyms and abbreviations

The following acronyms and abbreviations are used in this International Standard:

ACF	Access Control Function
ACSE	Association Control Service Element
APDU	Application PDU
ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
Conf	Confirm
CP	Convergence Protocol
CPDU	Convergence Protocol Data Unit
CPE	Convergence Protocol Entity
DLSDU	Data Link Service Data Unit
DSAP	Destination SAP
GDMO	Guidelines for the Definition of Managed Objects
ID	Identifier
Ind	Indication
LAN	Local Area Network
LCI	Local CPE Instance
LLC	Logical Link Control
LMMP	LAN/MAN Management Protocol
LMM_PDU	LAN/MAN Management Protocol Data Unit
LMMPE	LAN/MAN Management Protocol Entity
LMMS	LAN/MAN Management Service
LMMU	LAN/MAN Management User
LRG	Local Request Group
LRI	Local Request Instance
LSAP	Link SAP
MAC	Media Access Control
MAN	Metropolitan Area Network
MIB	Management Information Base
OSI	Open Systems Interconnection
PDU	Protocol Data Unit

PE	Protocol Entity
PICS	Protocol Implementation Conformance Statement
QOS	Quality of Service
RCI	Remote CPE Instance
Req	Request
RO-APDU	Remote Operations APDU
ROSE	Remote Operations Service Element
RRG	Remote Request Group
RRI	Remote Request Instance
Rsp	Response
SAP	Service Access Point
SDU	Service Data Unit
SMI	Structure of Management Information
SNAP	Subnetwork Access Protocol
SSAP	Source SAP
TR	Technical Report

4. LAN/MAN Management and Systems Management

OSI systems management functions are defined as those functions that support management applications, and that allow such applications to manipulate resources in the OSI environment. The management functional areas that give rise to these functions are described in the OSI Management Framework (ISO/IEC 7498-4 : 1989) and Systems Management Overview (ISO/IEC 10040 : 1992). The current set of functions defined by ISO/IEC are to be found in the Systems Management Function standards (ISO/IEC 10164, Parts 1–7).

The OSI Management Framework (ISO/IEC 7498-4 : 1989) defines Systems Management as an Application layer activity, related to the management of the use of OSI resources and their status across all seven layers of the OSI architecture. As a consequence, Systems Management requires the use of Application layer protocols supported by a full seven-layer protocol stack. The OSI Systems Management functions therefore require the support of CMIS, CMIP, and ROSE [ISO/IEC 9595 : 1991, ISO/IEC 9596-1 : 1991, and ITU-T Recommendation X.219 (1988)], which in turn require the support of a full connection-oriented OSI stack.

Typical systems management activities include

- a) Management of the activation and deactivation of OSI resources
- b) Software loading
- c) Reporting status, status changes, and statistics
- d) Error detection, diagnosis, and recovery

The requirements for Systems Management protocol support can, however, be in conflict with the general requirements for management of the communications environment in that

- Management of the communication capability of a station is often required when part of the communication capability is unavailable, inoperable, or approaching inoperability. This may require the management protocol to be carried directly by simple, lower-layer services. Examples of such requirements are initialization and loading of a station's system software during "boot-strapping" of the system.
- Many of the devices that make up a communications network are constrained by memory or other resource limitations in ways that prohibit support of a full seven-layer connection-oriented OSI protocol stack for management purposes (e.g., modems, link layer bridges, repeaters, and hubs), and more economical methods of operation are a practical necessity.

The OSI Management Framework (ISO/IEC 7498-4 : 1989) allows for the provision of management functionality by means of (N)-layer management protocols in circumstances where the services of all seven layers are not available and where management is performed entirely within the context of specific layers. The IEEE 802.1 LAN/MAN Management protocol is therefore defined as an (N)-layer management protocol specific to the management of layers 1 and 2 in a LAN/MAN environment. It provides a means for resource-constrained, simple, or broken systems to be managed in a manner that is better suited to the capabilities of such systems while allowing them to interoperate in the OSI environment. This is achieved by defining the LAN/MAN Management protocol in such a way that it requires only the services of the lower two layers, specifically the simple connectionless services available at the link layer in LAN/MAN technologies, to support the exchange of management information between stations.

The use of the LAN/MAN Management protocol does not preclude the use of OSI systems management protocols; in particular, the concepts of managed objects and management information used in this International Standard are based on those described in the OSI Structure of Management Information standards (ISO/IEC 10165, Parts 1, 2, and 4), and the protocol defined in this International Standard makes use of the protocol data units defined in CMIP (ISO/IEC 9596-1 : 1991) to carry management information between systems. The management information exchanged between stations may therefore be defined in a manner that makes it available both to the LAN/MAN Management protocol and to CMIP (ISO/IEC 9596-1 : 1991); hence this information may also be used to support Systems Management. The manner in which this specification is accomplished is described in IEEE Std 802.1F-1993.

NOTES

1—It is recommended that, where practicable, management is performed through the use of OSI Systems Management, which operates over a full seven-layer protocol stack.

2—The management services and supporting protocols described in this International Standard were developed with the specific aim of providing remote management for layers 1 and 2 of the OSI reference model as they apply to a LAN/MAN environment. The use of these mechanisms in other contexts is outside the scope of this International Standard, but such use is in no way precluded.

5. Architecture

This clause contains a description of the major components of the LAN/MAN Management architecture and defines the terms used in relation to the architecture.

Within a LAN/MAN station, there are components that are concerned with the normal communication activities of the station, and components that are concerned with its management activities. The description in this clause relates only to

- a) The management aspects of a LAN/MAN station and
- b) The communication services and protocols that are required for management purposes.

NOTE—The description of the architecture makes use of the OSI concepts of a *service definition*, which defines, in an abstract manner, the mechanisms that permit the exchange of information between peer entities in the OSI environment; and of a *peer protocol*, which is used, in a defined way, to provide a given service. It should be borne in mind that service definitions do not describe exposed interfaces, and are therefore not the subject of conformance requirements.

5.1 Management communication

Figure 5-1 is an adaptation of figure A.2 in Annex A of the OSI Management Framework, ISO/IEC 7498-4 : 1989, showing how the concept of the (N)-layer management protocol is utilized in this International Standard in order to define an (N)-layer management protocol for use in the management of layers 1 and 2 in a LAN/MAN environment. The LAN/MAN Management Protocol defined by this International Standard corresponds to the (N)-layer management protocol shown in the figure; it in turn makes use of the services provided by the normal communication protocols available at layers 1 and 2 in a LAN/MAN environment.

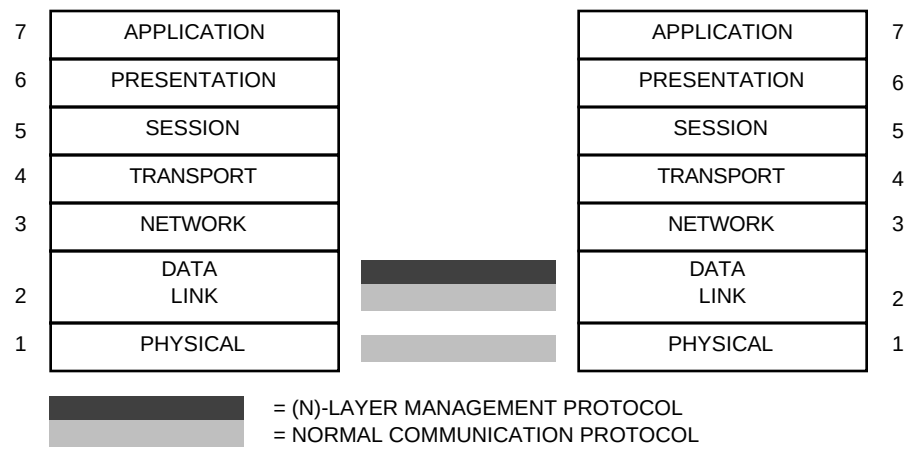


Figure 5-1—(N)-layer management protocol exchange at the Data Link layer

Figure 5-2 depicts the service and protocol elements that are involved in management communication between LAN/MAN stations by means of the LAN/MAN Management protocol. There are three major elements involved in LAN/MAN Management communication: the *LAN/MAN Management Service (LMMS)*, the *LAN/MAN Management Protocol Entity (LMMPE)*, and the *Convergence Protocol Entity (CPE)*.

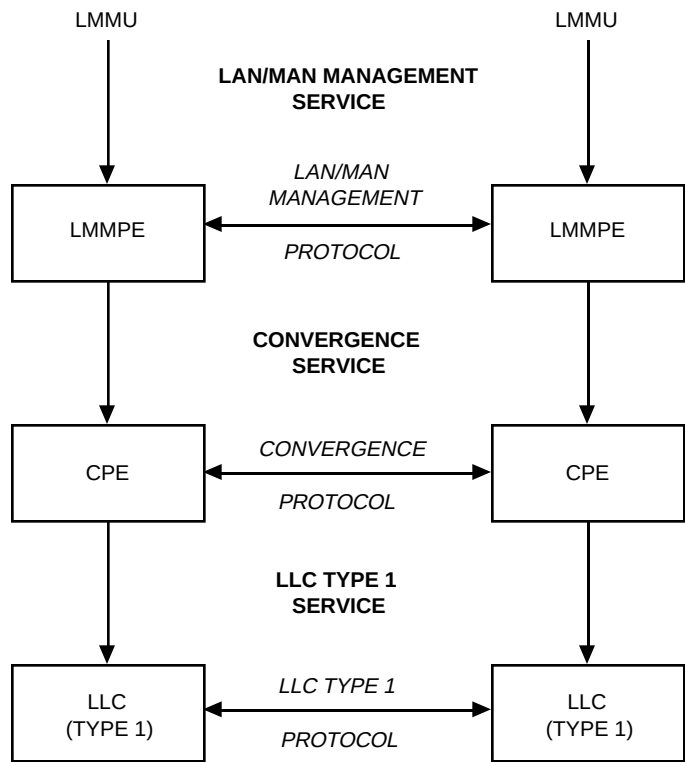


Figure 5-2—LAN/MAN Management communication architecture

The LMMS defines the service that is available to the management process known as the *LAN/MAN Management User (LMMU)* for the purposes of exchanging management information with another LMMU. The LMMS makes use of service primitives defined in the Common Management Information Service (CMIS) (ISO/IEC 9595 : 1991), in the manner defined in clause 6.

The LMMPE is the protocol entity that is responsible for providing the LMMS, by means of LAN/MAN Management protocol exchanges. The LMMS makes use of procedures and protocol data units defined in the Common Management Information Protocol (CMIP) (ISO/IEC 9596-1 : 1991), in the manner defined in clause 7.

The CPE is a protocol entity that is responsible for providing convergence functions that enable the LMMS to be provided in a LAN/MAN environment. These functions are concerned with the provision of reliability and the maintenance of logical associations between LMMUs. The convergence service and the protocol that support these functions are described in clause 7.

The CPE assumes the availability of the Data Link service as an underlying service for the exchange of LAN/MAN Management protocol data units (LMM_PDUs). Only the LLC Type 1 (unacknowledged connectionless) procedures are used to support the operation of the convergence protocol.

5.2 Management information and management operations

The component of a station that exists within a given OSI layer is known as a layer subsystem. Within a layer subsystem, resources such as protocol machines provide the normal communication functions of the layer. The definition of the functions of these entities is not within the scope of this International Standard.

For management purposes, it may be necessary to provide a means of monitoring and controlling aspects of the operation of layer subsystems and their components. This is achieved by the provision of management functionality that is concerned with providing the *management view* of the layer subsystem. This functionality provides *management information* about the layer subsystem, effects control over it in defined ways, and indicates the occurrence of certain events within it. This functionality is defined in terms of one or more *managed objects* that provide the management view of the resources of the layer subsystem.

NOTE—The OSI Management Framework (ISO 7498 : 1984) describes the concept of the *Management Information Base (MIB)*, which is a conceptual repository of management information that corresponds to the set of managed objects instantiated in a system and the information associated with them; however, the MIB is not explicitly defined as part of the 802.1 architecture, as the concept does not add value to the concepts of managed objects and management information. The concepts described here are directly compatible with the OSI concept of the MIB and the managed objects that it contains; in particular, the use of CMIP (ISO/IEC 9596-1 : 1991) PDUs as the basis for the LMMP permits managed objects defined in accordance with the GDMO (ISO/IEC 10165-4 : 1992) templates to be compatible with both the LMMP and the CMIP.

Layer subsystems are also responsible for participating in other distributed functions (e.g., dynamic routing at the network layer). In order to achieve this, specific protocols may exist for communication of management information related to those functions. This aspect of management is not within the scope of this International Standard.

The functionality of a managed object is made available via the *managed object boundary*, as expressed in the OSI Management Information Model (ISO/IEC 10165-1 : 1993). The Management Information Model defines the set of generic operation and notification types that a managed object may support; a given managed object may support a subset of these types.

NOTE—The terms *managed object* and *managed object boundary* replace the terms *layer management entity (LME)* and *layer management interface (LMI)* that were used in early drafts of this International Standard, as follows:

- a) An LME corresponds to the set of managed objects that provide the management view of a layer subsystem.
- b) An LMI corresponds to the functionality available at the managed object boundaries of the set of managed objects represented by an LME.

The use of the terms LME and LMI is deprecated.

The functionality of a managed object may be utilized for management purposes by a managing process. Where the managing process is local to the managed object, the mechanisms used to effect this interaction are outside the scope of this International Standard. Where the managing process is remote from the managed object with which it is required to interact, the managing process may make use of the LMMS in order to communicate with a peer-managing process in the remote station. This communication is described in terms of the roles that each managing process plays in a particular exchange of management information—either the role of a *Manager* or the role of an *Agent*. The Manager and Agent managing processes involved in such exchanges are users of the LMMS and are therefore known as *LAN/MAN Management users (LMMUs)*. The terms Manager and Agent are used for descriptive purposes only, and refer to the roles adopted in individual exchanges of management information. A managing process may be capable of adopting either role, and may therefore participate in successive management information exchanges as a Manager or as an Agent, as appropriate to the type of exchange taking place.

A Manager *requests* management operations to be performed by a remote LMMU, the Agent. An Agent *performs* the requested operations on managed objects accessible to it as though they had been requested locally, and *responds* by returning any results to the originating Manager. However, an Agent maintains complete jurisdiction over whether the requested operations are performed. The Agent may, on the basis of access control information held locally, determine that particular operations on particular managed objects may not be performed by particular Managers. The basis upon which this determination is made is described in clauses 8 and 9.

A managed object may from time to time emit notifications that contain information related to events that have occurred within the managed object. The Agent may, on the basis of event forwarding information held locally, determine whether such notification-related information should be *forwarded* to one or more Managers in the form of event reports. The basis upon which this determination is made is described in clause 8.

Figures 5-3 and 5-4 show the relationship between the Manager, the Agent, the LMMS, the LMMP, and managed objects during management information exchanges.

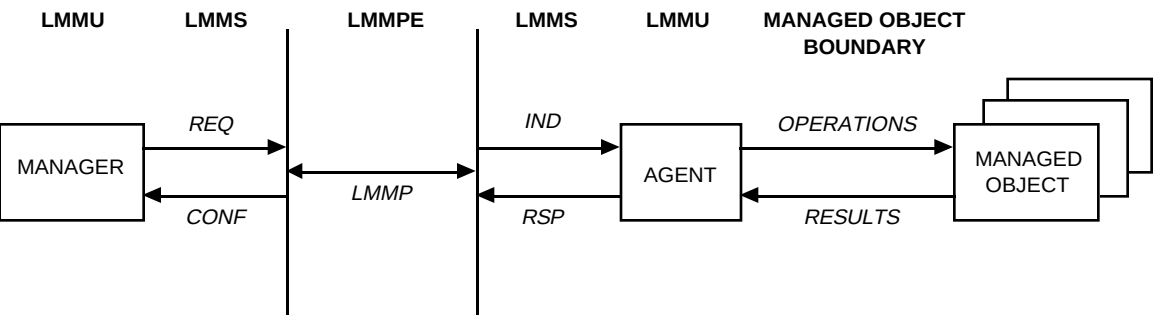


Figure 5-3—LAN/MAN Management information exchanges: operations

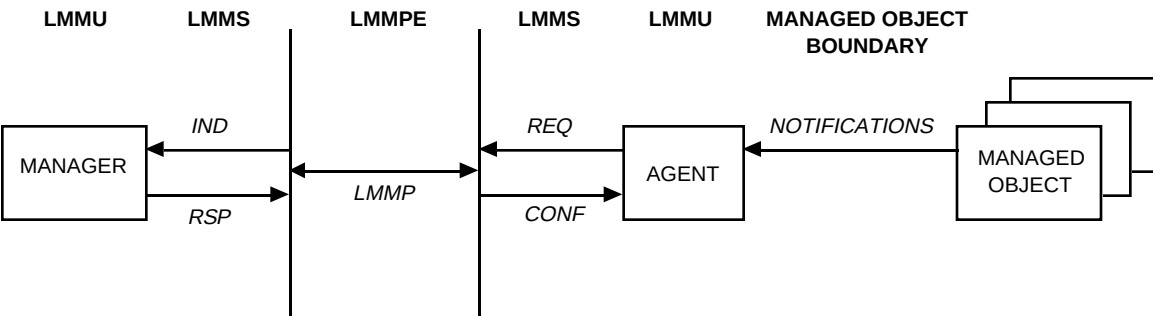


Figure 5-4—LAN/MAN Management information exchanges: notifications

In an environment where more than one Manager may exist, Managers and Agents may be grouped logically into management domains in order to determine which Manager(s) may request operations of which Agent(s), and to determine which Manager(s) an Agent should send event reports. Managed objects are defined in clause 8 for this purpose. The exact nature of management domains (whether hierarchical, exclusive, overlapping, etc.) is outside the scope of this International Standard.

The managed objects defined in clause 8 provide management functionality specific to the management of the security, event forwarding, and other management protocol-related functionality described in this International Standard, and allow these resources to be managed in a fashion analogous to the management of the resources of a layer subsystem.

5.3 Relationship with CMIS/CMIP

As indicated in 5.1, the LMMS and LMMP are realized by making use of the services, protocol data units, and procedures defined in CMIS and CMIP (ISO/IEC 9595 : 1991 and ISO/IEC 9596-1 : 1991) in the manner described in 6.1 and 7.1. This means that the functionality available from the LMMS and CMIS are the same, and that the PDUs used to express that functionality are also the same. This leads directly to the following two scenarios where CMIS/CMIP and LMMS/LMMP may be used in combination:

- a) Use of CMIP and LMMP in the same Manager and/or Agent system, in order to permit management of, or management by, systems that implement only one of the two protocols.
- b) “Proxy” Managers, which implement both protocols, and are capable of relaying requests between CMIP-based systems and LMMP-based systems.

In both scenarios, the compatibility between the services and protocols means that the managed object definitions are the same, regardless of the choice of protocol. Managed objects instantiated in accordance with those definitions may be accessed by either or both protocols.

NOTE—These scenarios are included for illustrative purposes only, and do not imply any conformance requirement upon the use of either CMIP or LMMP.

Figure 5-5 shows the correspondence between the protocol stacks for CMIP and the LMMP. The CPE is responsible for the control of errors, such as those arising due to lost CPDUs or misordering of CPDUs; and it relies upon the error-detection capabilities of the underlying MAC service, in particular CRC checking, for other aspects of data integrity.

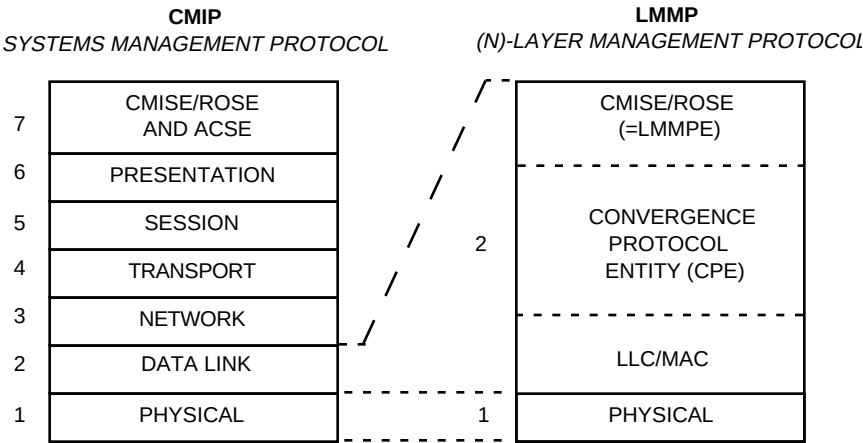


Figure 5-5—Comparison between CMIP and LMMP protocol stacks

5.4 Relationship with other management protocols

Management information defined for use with other management protocols can be accessed by use of the LMMP, provided that suitable definitions of that management information are available, expressed as managed object definitions using the notation defined in ISO/IEC 10165-4 : 1992.

6. Services

This clause defines the LAN/MAN Management service provided by the LMMPE, the Convergence service provided by the CPE, and the relationship between LMMS services and the managed object boundary.

6.1 LAN/MAN Management service

The LMMS consists of the services defined in CMIS (ISO/IEC 9595 : 1991), with the exception that the LMMS does not require the provision of association establishment or release services and places some additional constraints upon the existing service definitions in order to meet the requirements for operation in a connectionless LAN/MAN environment. As such, it relies on error reporting to indicate functionality that is not supported, as stated in the definition of the systems management application context contained in ISO/IEC 10040 : 1992. The access control parameters of the LMMS service primitives may be used to exchange access control information between Manager and Agent, for the purposes of the access control mechanisms described in 9.2. The LMMS services are summarized in table 6-1.

Table 6-1—LMMS services

Service	Type
M-ACTION	confirmed/non-confirmed
M-CANCEL-GET	confirmed
M-CREATE	confirmed
M-DELETE	confirmed
M-EVENT-REPORT	confirmed/non-confirmed
M-GET	confirmed
M-SET	confirmed/non-confirmed

6.1.1 Additional constraints on CMIS

Given that the LMMS does not require an explicit association establishment or release phase, the references to A-ABORT in clause 9 of CMIS do not apply to this International Standard.

6.2 Convergence function and convergence service

The convergence function of the CPE provides

- a) The information necessary for stations participating in management information exchanges to detect station reboot or reset.
- b) The information necessary for stations participating in management information exchanges to detect or determine
 - 1) Duplication of information

- 2) Out-of-sequence information
- 3) Temporal ordering of information
- 4) Information loss
- c) The information necessary to identify the abstract syntax of the management information being exchanged and the LMMP protocol version.
- d) Mechanisms that improve the reliability of communication for confirmed information exchanges in circumstances where the rate of packet loss in connectionless LAN/MAN data transfers is considered to be unacceptably high for management information exchanges.

Items a), b), and c) are provided by means of information that is carried in CPDUs exchanged between peer CPEs. Item d) is provided by means of a simple protocol state machine that performs timeouts and retries in conjunction with the reliable quality of service (QOS) provided by the LMMS. The details of the CPDU structure and the state machines that support these aspects of the CPE are described in clause 7.

The convergence function operates on the basis of an *affiliation* between the CPEs involved in an exchange of information; the minimum requirement for an affiliation is that the CPEs are aware of each other's *CPE instance identifiers* (see 7.3.1).

NOTES

1—The convergence protocol provides a means whereby a change in the status of an affiliation may be detected, caused by a system reboot or reset by either party. The action taken upon such events is a local matter.

The convergence function places a limit on the number of outstanding requests between affiliates.

2—CPE-Abort indications (see 6.2.3) will result if the convergence service user operates using ROSE Operation Class 2 (asynchronous), or any other analogous procedure that may result in multiple outstanding requests at the convergence service level, and the number of outstanding requests exceeds the capabilities of the affiliates concerned.

The operation of the convergence function may result in a non-negligible rate of user information loss, depending upon whether the reliable QOS is chosen, the number of retries that are configured, and the behaviour of the LAN/MAN environment in which the protocol is operated. Where the reliable QOS option is not used, reliability is directly dependent upon the reliability of the unacknowledged connectionless-mode services available in the LAN/MAN environment.

The convergence function does not provide any capability for segmentation and reassembly of user data; the maximum size of any user data is therefore constrained by the maximum frame size available in the LAN/MAN environment.

The convergence function may be viewed as a PDU delivery service for the user of the convergence service, the LMMPE. The CPE accepts PDUs from the convergence service user for delivery to a particular destination, and delivers them to the peer CPE at that destination. The receiving CPE then passes the received PDU to its service user. In addition to this delivery service, the CPE provides an abort indication service that alerts the convergence service user to service provider aborts. The service primitives associated with the convergence service are described below.

6.2.1 Conventions

This International Standard defines the services provided by the CPE following the descriptive conventions defined in ISO/TR 8509 : 1987. The definition of each CPE service includes a table that lists the parameters of its primitives. For a given primitive, the presence of each parameter is described by one of the following values:

M	The parameter is mandatory.
(=)	The value of the parameter is equal to the value of the parameter in the column to the left.
U	The use of the parameter is a service-user option.
—	The parameter is not present in the interaction described by the primitive concerned.
C	The parameter is conditional. The condition(s) are defined by the text that describes the parameter.

6.2.2 CPE-Data service

The CPE-Data service is invoked by the convergence service user issuing a CPE-Data request service primitive to the CPE, with parameters set according to the parameter definitions contained in this clause. The CPE User Information contained in the CPE-Data request primitive is delivered to the appropriate peer CPE, using the requested QOS, by means of the convergence protocol described in 7.3. The information is then passed to the peer convergence service user by the peer CPE issuing a CPE-Data request primitive, with parameters set to reflect the CPE User Information received and the actual QOS used.

The parameters associated with the CPE-Data request and indication primitives are listed in table 6-2.

Table 6-2—Parameters associated with the CPE-Data service

Parameter Name	Req	Ind
Destination Address	M	—
Source Address	—	M
QOS	M	M
Status	—	M
CPE User Information	M	M

- a) **Destination Address:** Indicates to the CPE the address of the peer convergence service user to which the CPE User Information is to be delivered.
- b) **Source Address:** Indicates the CPE address of the requesting convergence service user.
- c) **QOS:** In request primitives, indicates to the CPE the quality of service with which the CPE User Information is to be delivered to the peer convergence service user. This parameter permits the requesting convergence service user to specify the following:
 - 1) **Priority.** This value corresponds to the priority with which the CPE is requested to deliver the CPE User Information.
 - 2) **Reliability.** The CPE service user may request either *basic* or *enhanced* reliability. This value determines whether the CPE will deliver the CPE User Information by making direct use of the underlying LLC service, or whether the CPE will provide enhancements that improve the reliability of the underlying service.

In indication primitives, the QOS parameter indicates the actual quality of service used for delivery of the CPE User Information.

NOTE—Requesting basic reliability will result in the use of the underlying LLC Type 1 procedures without the application of timeouts and retries. Requesting enhanced reliability will result in the use of timeouts and retries in order to recover from data loss. The Priority value is mapped directly onto the priority parameter in the DL-UNITDATA primitives.

- d) **Status:** Indicates the status of the CPE from which the CPE User Information was received. The permitted values are
 - 1) New affiliate
 - 2) Old affiliate
 - 3) Changed affiliate
 The three affiliate types are described in 7.3.1.2.
- e) **CPE User Information:** Contains the information that the requesting convergence service user requests the CPE to deliver to the peer convergence service user.

6.2.3 CPE-Abort service

If the CPE is unable to deliver CPE User Information associated with a CPE-Data service primitive to its destination, the CPE issues a CPE-Abort indication primitive to the requesting convergence service user, giving the reason for the failure and the CPE User Information that it has failed to deliver.

The parameters associated with the CPE-Abort indication primitive are listed in table 6-3.

Table 6-3—Parameters associated with the CPE-Abort service

Parameter Name	Ind
Reason	M
CPE User Information	M

- a) **Reason:** Indicates the reason for the convergence service provider abort. This parameter takes one of the following values:
 - 1) Timeout
 - 2) Resource limitation
 - 3) Failure of underlying services
- b) **CPE User Information:** Contains the information that the requesting convergence service user requests the CPE to deliver to the peer convergence service user.

6.2.4 CPE-Status service

If information held about an old affiliate changes, the CPE issues a CPE-Status indication primitive to the convergence service user.

The parameters associated with the CPE-Status indication primitive are listed in table 6-4.

Table 6-4—Parameters associated with the CPE-Status service

Parameter Name	Ind
CPE identifier	M
Status	M

- a) **CPE identifier:** The instance identifier of the CPE whose status information is being reported.
- b) **Status:** Indicates the status of the CPE from which the new status information was received. The permitted values are changed affiliate. The meaning of changed affiliate is defined in 7.3.1.2.

6.3 Relationship between LMMS services and the managed object boundary

6.3.1 Managed objects and the managed object boundary

The OSI Management Information Model (ISO/IEC 10165-1 : 1993) defines the architectural basis for the definition of the managed objects and the set of operations and notifications that a managed object may support. The managed object boundary is the boundary at which the management operations and notifications supported by a managed object are made visible. Each managed object supports a defined set of operations and notifications, as identified in the managed object class definition for the managed object class of which it is an instance. The operations are of two types: those that apply to attribute manipulation, and those that apply to a managed object as a whole. Notifications may be emitted as a result of changes in attribute states