

IEEE Std 802.1D™- 2004
(Revision of IEEE Std 802.1D-1998)

IEEE Standards

802.1D™

**IEEE Standard for
Local and metropolitan area networks**

Media Access Control (MAC) Bridges

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee



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

9 June 2004

Print: SH95213

PDF: SS95213

AVA **Documents**
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 26, 2026 at 03:20:55 UTC from IEEE Xplore. Restrictions apply.

Full document details: [IEEE 802.1D-2004](#)

Recognized as an
American National Standard (ANSI)

IEEE Std 802.1D™-2004
(Revision of IEEE Std 802.1D-1998)

IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges

Sponsor
LAN MAN Standards Committee
of the
IEEE Computer Society

Approved 4 June 2004
American National Standard Institute

Approved 9 February 2004
IEEE-SA Standards Board

Abstract: An architecture for the interconnection of IEEE 802® Local Area Networks (LANs) below the MAC Service boundary is defined. MAC Bridges, as specified by this standard, allow communications between end stations attached to separate LANs, each with its own separate MAC, to be transparent to logical link control (LLC) and network layer protocols, just as if the stations were attached to the same LAN.

Keywords: active topology, filtering, GARP, GMRP, LANs, local area networks, MAC Bridges, MAC Service, MANs, metropolitan area networks, multicast registration, transparent bridging, quality of service, RSTP, spanning tree

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

Copyright © 2004 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 9 June 2004. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

Print: ISBN 0-7381-3881-5 SH95213
PDF: ISBN 0-7381-3982-3 SS95213

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.

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. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE. Current interpretations can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/interp/index.html>.

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL for errata periodically.

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.

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

[This introduction is not part of IEEE Std 802.1D-2004, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges.]

The MAC Bridge standardization activities that resulted in the development of IEEE Std 802.1D-1990 (subsequently republished as IEEE Std 802.1D, 1993 Edition [ISO/IEC 10038:1993] and IEEE Std 802.1D, 1998 Edition [ISO/IEC 15802-3: 1998]) specified an architecture and protocol for the interconnection of IEEE 802 LANs below the MAC Service boundary.

The 2004 revision of this standard incorporates two amendments into the 1998 Edition:

- a) IEEE Std 802.1t-2001, technical and editorial corrections to the 1998 Edition; and
- b) IEEE Std 802.1w-2001, Rapid Reconfiguration, which specified the Rapid Spanning Tree Algorithm and Protocol (RSTP).

In addition, this revision includes further technical and editorial corrections, and removes the original Spanning Tree Protocol (STP) as a conformance option.

Relationship between IEEE Std 802.1D and IEEE Std 802.1Q

Another IEEE standard, IEEE Std 802.1Q™-2003, extends the concepts of MAC Bridging and filtering services to support the definition and management of Virtual LANs (VLANs).

The capabilities defined in IEEE Std 802.1Q-2003 include the definition of a VLAN frame format that is able to carry VLAN identification and user priority information over LAN technologies, such as CSMA/CD, that have no inherent capability to signal priority information. This information is carried in an additional header field, known as the *Tag Header*, which is inserted immediately following the Destination MAC Address, and Source MAC Address (and Routing Information field, if present) of the original frame. IEEE Std 802.1Q-2003 extends the priority handling aspects of this standard to make use of the ability of the VLAN frame format to carry user priority information end to end across any set of concatenated underlying MACs.

The VLAN Bridging specification contained in IEEE Std 802.1Q-2003 is independent of this standard, in the sense that IEEE Std 802.1Q-2003 contains its own statement of the conformance requirements for VLAN Bridges. However, IEEE Std 802.1Q-2003 makes use of many of the elements of the specification contained in this standard, in particular

- a) The Bridge architecture
- b) The Internal Sublayer Service, and the specification of its provision by IEEE 802 LAN MACs
- c) The major features of the operation of the forwarding process
- d) The Rapid Spanning Tree Protocol
- e) The Generic Attribute Registration Protocol (GARP)
- f) The GARP Multicast Registration Protocol (GMRP)

Since the original Spanning Tree Protocol (STP) has been removed from the 2004 revision of IEEE Std 802.1D, an implementation of RSTP is required for any claim of conformance for an implementation of IEEE Std 802.1Q-2003 that refers to the current revision of IEEE Std 802.1D unless that implementation includes the Multiple Spanning Tree Protocol (MSTP) specified in IEEE Std 802.1Q-2003. MSTP is based on RSTP, extended to provide support for multiple spanning trees.

Notice to users

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/interp/index.html>.

Patents

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

Participants

At the time this standard was completed, the 802.1D working group had the following membership:

Tony Jeffree, *Chair and Editor*

Paul Congdon, *Vice-Chair*

Mick Seaman, *Interworking Task Group Chair and Editor*

Les Bell
Paul Bottorff
Jim Burns
Marco Carugi
Dirceu Cavendish
Arjan de Heer
Anush Elangovan
Hesham Elbakoury
David Elie-Dit-Cosaque
Norm Finn
David Frattura
Gerard Goubert
Stephen Haddock
Atsushi Iwata

Neil Jarvis
Manu Kaycee
Hal Keen
Bill Lane
Roger Lapuh
Loren Larsen
Yannick Le Goff
Marcus Leech
Mahalingam Mani
Dinesh Mohan
Bob Moskowitz
Don O Connor
Don Pannell
Glenn Parsons

Ken Patton
Allyn Romanow
Dan Romascanu
Jessy V. Rouyer
Ali Sajassi
Dolors Sala
Muneyoshi Suzuki
Jonathan Thatcher
Michel Thorsen
Dennis Volpano
Karl Weber
Ludwig Winkel
Michael D. Wright

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

Butch Anton	Julian Ho	Rajesh Moorkath
Edward Carley	Atsushi Ito	Charles Ngethe
Clint Chaplin	Peeya Iwagoshi	Satoshi Obara
Sunghyun Choi	Tony Jeffree	Stephen Palm
Keith Chow	Stanley Johnson	Ashley Peacock
Christopher Cooke	Stuart Kerry	Subbu Ponnuswamy
Wael Diab	Shyam Kaluve	Vikram Punj
Thomas Dineen	Cees Klik	Maximilian Riegel
Sourav Dutta	Kshitij Kumar	Floyd Ross
Clint Early	Pi-Cheng Law	Mick Seaman
Will Foulds	Randolph Little	Gil Shultz
David Frattura	Ryan Madron	Adrian Stephens
Anoop Ghanwani	Nikolai Malykh	Scott Valcourt
Robert M. Grow	Kyle Maus	Dmitri Varsanofiev
Stephen Haddock	George Miao	Michael D. Wright
		Oren Yuen

When the IEEE-SA Standards Board approved this standard on 9 February 2004, it had the following membership:

Don Wright, *Chair*

Chuck Adams,	Mark S. Halpin	Daleep Mohla
Stephen Berger	Raymond Hapeman	Paul Nikolich
Mark D. Bowman	Richard J. Holleman	T. W. Olsen
Joseph Bruder	Richard Hulett	Ronald C. Petersen
Bob Davis	Lowell Johnson	Gary S. Robinson
Roberto de Boisson	Hermann Koch	Frank Stone
Julian Forster*	Joseph Koepfinger*	Malcolm V. Thaden
Judith Gorman	Thomas J. McGean	Doug Topping
Arnold M. Greenspan	Steve M. Mills	Joe D. Watson

*Member Emeritus

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

Satish K. Aggarwal, *NRC Representative*
Richard DeBlasio, *DOE Representative*
Alan Cookson, *NIST Representative*

Michelle D. Turner
IEEE Standards Project Editor

Contents

1. Overview	1
1.1 Introduction	1
1.2 Scope	1
2. References	3
3. Definitions	5
3.1 Bridged Local Area Network	5
3.2 Expedited traffic	5
3.3 Group	5
3.4 IEEE 802 Local Area Network (LAN)	5
4. Abbreviations	7
5. Conformance	9
5.1 Required capabilities	9
5.2 Optional capabilities	9
5.3 Protocol Implementation Conformance Statement	10
5.4 Recommendations	10
5.5 MAC-specific bridging methods	10
6. Support of the MAC Service	11
6.1 Support of the MAC Service	11
6.2 Preservation of the MAC Service	12
6.3 Quality of Service maintenance	12
6.4 Internal Sublayer Service provided within the MAC Bridge	16
6.5 Support of the Internal Sublayer Service by specific MAC procedures	19
6.6 Filtering services in Bridged Local Area Networks	24
7. Principles of Bridge operation	29
7.1 Bridge operation	29
7.2 Bridge architecture	31
7.3 Model of operation	32
7.4 Port States and the active topology	35
7.5 Frame reception	35
7.6 Frame transmission	37
7.7 The Forwarding Process	37
7.8 The Learning Process	41
7.9 The Filtering Database	42
7.10 Spanning Tree Protocol Entity and GARP Entities	49
7.11 Bridge management	49
7.12 Addressing	49
8. Spanning tree algorithm and protocol	57
9. Encoding of bridge protocol data units	59
9.1 Structure	59
9.2 Encoding of parameter types	59

9.3	BPDU formats and parameters	61
10.	GARP Multicast Registration Protocol (GMRP)	67
10.1	Purpose	67
10.2	Model of operation	67
10.3	Definition of the GMRP Application	70
10.4	Conformance to GMRP	72
11.	Example “C” code implementation of GMRP	75
12.	Generic Attribute Registration Protocol (GARP)	77
12.1	GARP overview	77
12.2	GARP architecture	79
12.3	Requirements to be met by GARP	82
12.4	Requirements for interoperability between GARP Participants	83
12.5	Conformance to GARP Applications	83
12.6	Protocol Operation	84
12.7	State machine descriptions	90
12.8	Administrative controls	95
12.9	Procedures	96
12.10	Structure and encoding of GARP Protocol Data Units	101
12.11	Timer values, granularity and relationships	106
12.12	Interoperability considerations	106
13.	Example “C” code implementation of GARP	109
14.	Bridge management	111
14.1	Management functions	111
14.2	Managed objects	112
14.3	Data types	112
14.4	Bridge Management Entity	113
14.5	MAC Entities	116
14.6	Forwarding Process	116
14.7	Filtering Database	119
14.8	Spanning Tree Protocol Entity	123
14.9	GARP Entities	127
14.10	GMRP entities	129
15.	Management protocol	133
16.	Bridge performance	135
16.1	Guaranteed Port Filtering Rate	135
16.2	Guaranteed Bridge Relaying Rate	135
17.	Rapid Spanning Tree Protocol (RSTP)	137
17.1	Protocol design requirements	137
17.2	Protocol support requirements	138
17.3	RSTP overview	138
17.4	STP compatibility	143
17.5	Spanning tree priority vectors	143
17.6	Priority vector calculations	143

17.7	Port Role assignments	145
17.8	Communicating spanning tree information	145
17.9	Changing spanning tree information.....	145
17.10	Changing Port States	146
17.11	Updating learned station location information	148
17.12	RSTP and point-to-point links	151
17.13	RSTP performance parameters	151
17.14	Performance parameter management.....	153
17.15	Rapid Spanning Tree state machines	155
17.16	Notational conventions used in state diagrams	155
17.17	State machine timers	157
17.18	Per-Bridge variables.....	158
17.19	Per-Port variables	159
17.20	State machine conditions and parameters	164
17.21	State machine procedures	165
17.22	Port Timers state machine.....	170
17.23	Port Receive state machine	170
17.24	Port Protocol Migration state machine	171
17.25	Bridge Detection state machine	171
17.26	Port Transmit state machine.....	172
17.27	Port Information state machine	173
17.28	Port Role Selection state machine.....	174
17.29	Port Role Transitions state machine	174
17.30	Port State Transition state machine.....	177
17.31	Topology Change state machine	178
17.32	RSTP performance requirements	179
18.	Bridge Detection state machine	181
Annex A	(normative) PICS Proforma.....	183
A.1	Introduction	183
A.2	Abbreviations and special symbols.....	183
A.3	Instructions for completing the PICS proforma.....	184
A.4	PICS proforma for IEEE Std 802.1D.....	186
A.5	Major Capabilities.....	187
A.6	Media Access Control Methods	188
A.7	Relay and filtering of frames	189
A.8	Basic Filtering Services	190
A.9	Addressing	191
A.10	Rapid Spanning Tree Protocol	192
A.11	BPDU Encoding.....	193
A.12	Implementation Parameters.....	193
A.13	Performance	194
A.14	Bridge management	195
A.15	Remote Management.....	196
A.16	Expedited Traffic Classes.....	196
A.17	Extended Filtering Services.....	196
A.18	GMRP	197
A.19	GARP	198

Annex B (informative) Calculating spanning tree parameters	199
Annex C (normative) Source-routing transparent bridge operation	201
C.1 Overview	201
C.2 Support of the MAC Service	204
C.3 Principles of operation	208
C.4 Bridge management	223
C.5 Management protocol	227
Annex D (normative) PICS Proforma for source-routing transparent bridge operation	229
D.1 Introduction	229
D.2 Relay and filtering of frames	229
D.3 Bridge numbers and LAN IDs	230
D.4 Bridge management	230
Annex E (informative) Allocation of Object Identifier values	231
Annex F (informative) Preserving the integrity of FCS fields in MAC Bridges	233
F.1 Background	233
F.2 Basic mathematical ideas behind CRC and FCS	233
F.3 Detection Lossless Circuit approach	235
F.4 Algorithmic modification of an FCS	236
F.5 Conclusions	239
Annex G (informative) User priorities and traffic classes	241
G.1 Traffic types	241
G.2 What are we managing?	241
G.3 Traffic type to traffic class mapping	242
Annex H (informative) Generic Attribute Registration Protocol Design	245
H.1 Use of an unconfirmed protocol	245
H.2 Design of the Applicant state machine	245
H.3 Design of the Registrar state machine	246
H.4 Analysis of GARP State Machine Operation	246
Annex I (informative) Introduction of GARP, GMRP, and Extended Filtering Services	261
I.1 Migration considerations	261
I.2 Interoperability with higher-layer multicast protocols and related issues	263
Annex J (informative) RSTP Migration	265
J.1 Overview of protocol changes	265
J.2 BPDU formats	265
Annex K (informative) Frame duplication and misordering	267
K.1 Background	267
K.2 Frame duplication	267
K.3 Frame misordering	268
K.4 Other considerations	269

IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges

1. Overview

1.1 Introduction

IEEE 802 Local Area Networks (or LANs; see 3.4) of all types can be connected together using MAC Bridges. The Bridged Local Area Network created allows the interconnection of stations as if they were attached to a single LAN, even if they are attached to separate LANs each with its own independent MAC. A MAC Bridge operates below the MAC Service Boundary, and is transparent to protocols operating above this boundary, in the Logical Link Control (LLC) sublayer or Network Layer (ISO/IEC 7498-1: 1994¹). The presence of one or more MAC Bridges can lead to differences in the Quality of Service (QoS) provided by the MAC sublayer; it is only because of such differences that MAC Bridge operation is not fully transparent.

A Bridged Local Area Network can provide for

- a) The interconnection of stations attached to LANs of different MAC types.
- b) An effective increase in the physical extent, the number of permissible attachments, or the total performance of a LAN.
- c) Partitioning of the physical LAN for administrative or maintenance reasons.
- d) Validation of access to the LAN.
- e) Increased availability of the MAC Service in the face of reconfiguration or failure of network components.

1.2 Scope

For the purpose of compatible interconnection of data-processing equipment using the IEEE 802 MAC Service supported by interconnected IEEE 802 LANs (see 3.4) using different or identical Media Access Control methods, this standard specifies a general method for the operation of MAC Bridges. To this end this standard

- a) Positions the bridging function within an architectural description of the MAC Sublayer.
- b) Defines the principles of operation of the MAC Bridge in terms of the support and preservation of the MAC Service, and the maintenance of QoS.
- c) Specifies the MAC Internal Sublayer Service provided by individual LANs to the Media Access Method Independent Functions that provide frame relay in the Bridge.

¹Information about references can be found in Clause 2.

- d) Identifies the functions to be performed by Bridges, and provides an architectural model of the internal operation of a Bridge in terms of Processes and Entities that provide those functions.
- e) Establishes the requirements for a protocol between the Bridges in a Bridged Local Area Network to configure the network, and specifies the distributed computation of a Spanning Tree active topology.
- f) Establishes the requirements for a protocol between Bridges in a Bridged Local Area Network to configure multicast filtering information, and specifies the means of registering and distributing multicast filtering information by means of the GARP Multicast Registration Protocol (GMRP).
- g) Establishes the requirements for Bridge Management in the Bridged Local Area Network, identifying the managed objects and defining the management operations.
- h) Specifies performance requirements and recommends default values and applicable ranges for the operational parameters of a Bridge.
- i) Specifies the requirements to be satisfied by equipment claiming conformance to this standard.
- j) Specifies criteria for the use of MAC-specific bridging methods.

This standard specifies the operation of MAC Bridges that attach directly to IEEE 802 LANs, as specified in the relevant MAC standards for the MAC technology or technologies implemented.

2. References

The following standards contain provisions that, 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 indicated below. Members of ISO and IEC maintain registers of currently valid International Standards.

ANSI X3.159-1989, American National Standards for Information Systems—Programming Language—C.²

IEEE Std 802[®]-2001, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.³

IEEE Std 802.1H[™], 1997 Edition [ISO/IEC 11802-5: 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.⁴

IEEE Std 802.1Q[™]-2003, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.

IEEE Std 802.1X[™]-2001, IEEE Standards for Local and Metropolitan Area Networks—Port Based Network Access Control.

IEEE Std 802.2[™], 1998 Edition [ISO/IEC 8802-2: 1998], Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.⁵

IEEE Std 802.3[™]-2002, IEEE Standard for Local and Metropolitan Area Networks, Supplement to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications: Aggregation of Multiple Link Segments.

IEEE Std 802.5, 1998 Edition [ISO/IEC 8802-5: 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.

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

IETF RFC 2236, Fenner, Internet Group Management Protocol (IGMP), Version 2, November 1975.⁶

IETF RFC 1493, Decker, Langille, Rijsinghani and McCloughrie, Definitions of Managed Objects for Bridges, July 1993.

²ANSI publications are available from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

³IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA. IEEE publications can be ordered on-line from the IEEE Standards Website: <http://www.standards.ieee.org>.

⁴The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

⁵ISO [IEEE] and ISO/IEC [IEEE] documents are available from ISO Central Secretariat, 1 rue de Varembe, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA. ISO [IEEE] and ISO/IEC [IEEE] documents can be ordered on-line from the IEEE Standards Website: <http://www.standards.ieee.org>.

⁶Internet RFCs are available from the Internet Engineering Task Force website at <http://www.ietf.org/rfc.html>.

IETF RFC 2233, The Interfaces Group MIB using SMIv2, McCloghrie, K., Kastenholz, F., November 1997.

IETF RFC 2674, Bell, Smith, Langille, Rijsinghani, McCloghrie, Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions, August 1999.

ISO/IEC 7498-1: 1994, Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 1: The Basic Model.⁷

ISO/IEC 8824-1: 2002, Information technology—Abstract Syntax Notation One (ASN.1): Specification of basic notation.

ISO/IEC 8825-1: 2002, Information technology—ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

ISO/IEC 9595: 1998, Information technology—Open Systems Interconnection—Common management information service.

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

ISO/IEC 9596-1: 1998, Information technology—Open Systems Interconnection—Common management information protocol—Part 1: Specification.

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: 2002, 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 14882: 2003, Information Technology—Programming languages—C++.

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.

⁷ISO and ISO/IEC documents are available from the ISO Central Secretariat, 1 rue de Varembe, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

3. Definitions

For the purposes of this standard, the following terms and definitions apply.

3.1 Bridged Local Area Network

A concatenation of individual IEEE 802 LANs interconnected by MAC Bridges.

NOTE—Unless explicitly specified, the use of the word *network* in this standard refers to a Bridged Local Area Network. The term Bridged Local Area Network is not otherwise abbreviated. The term *Local Area Network* and the abbreviation LAN are used exclusively to refer to an individual LAN specified by a MAC technology without the inclusion of Bridges. This precise use of terminology within this specification allows a Bridged Local Area Network to be distinguished from an individual LAN that has been bridged to other LANs in the network. In more general usage such precise terminology is not required, as it is an explicit goal of this standard that Bridges are transparent to the users of the MAC Service.

3.2 Expedited traffic

Traffic that requires preferential treatment as a consequence of jitter, latency, or throughput constraints, or as a consequence of management policy.

3.3 Group

A Group associates

- a) A group MAC address,
- b) A set of properties that define membership characteristics, and
- c) A set of properties that define the forwarding/filtering behavior of a Bridge with respect to frames destined for members of that group MAC address.

with a set of end stations that all wish to receive information destined for that group MAC address. Members of such a set of end stations are said to be *Group members*.

A Group is said to *exist* if the properties associated with that Group are visible in an entry in the Filtering Database of a Bridge, or in the GARP state machines that characterize the state of the Group; a Group is said to *have members* if the properties of the Group indicate that members of the Group can be reached through specific Ports of the Bridge.

NOTE—An example of the information that Group members might wish to receive is a multicast video data stream.

3.4 IEEE 802 Local Area Network (LAN)

IEEE 802 LANs (also referred to in the text simply as LANs) are LAN technologies that provide a MAC Service equivalent to the MAC Service defined in ISO/IEC 15802-1. IEEE 802 LANs include IEEE Std 802.3 (CSMA/CD), IEEE Std 802.5 (Token Ring), IEEE Std 802.11 (Wireless), and ISO 9314-2 (FDDI) LANs.

4. Abbreviations

The following abbreviations are used in this standard.

BPDU	Bridge Protocol Data Unit
CRC	Cyclic Redundancy Check
FCS	Frame Check Sequence
GARP	Generic Attribute Registration Protocol
GARP PDU	GARP Protocol Data Unit
Gb/s	Gigabit per second (1 Gb/s is equivalent to 1 000 000 000 bits per second)
GID	GARP Information Declaration
GIP	GARP Information Propagation
GMRP	GARP Multicast Registration Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
kb/s	Kilobit per second (1 kb/s is equivalent to 1000 bits per second)
MAC	Media Access Control
Mb/s	Megabit per second (1 Mb/s is equivalent to 1 000 000 bits per second)
RSTP	Rapid Spanning Tree Algorithm and Protocol
RST BPDU	Rapid Spanning Tree Bridge Protocol Data Unit
STP	Spanning Tree Algorithm and Protocol
Tb/s	Terabit per second (1 Tb/s is equivalent to 1 000 000 Mb/s)
TCN	Topology Change Notification

5. Conformance

5.1 Required capabilities

A MAC Bridge for which conformance to this standard is claimed shall

- a) Conform to the relevant MAC standards technologies implemented at its Ports, as specified in 6.4 and 6.5.
 - b) Conform to IEEE Std 802.2 for the implementation of a class of LLC supporting Type 1 operation as required by 7.3 and 7.1.2.
 - c) Relay and filter frames as described in 7.1 and specified in 7.5, 7.6, 7.7, and 7.9.
 - d) Maintain the information required to support Basic Filtering Services, as described in 6.6 and 7.1 and specified in 7.5, 7.8, and 7.9.
 - e) Conform to the provisions for addressing specified in 7.12.
 - f) Implement the Rapid Spanning Tree Protocol, as specified in Clause 17.
 - g) Encode transmitted BPDUs and validate received BPDUs as specified in Clause 9.
 - h) Specify the following parameters of the implementation
 - 1) Filtering Database Size, the maximum number of entries.
 - 2) Permanent Database Size, the maximum number of entries.
 - i) Specify the following performance characteristics of the implementation
 - 1) A Guaranteed Port Filtering Rate for each Bridge Port
 - 2) A Guaranteed Bridge Relaying Rate for the Bridge
 - 3) The related time intervals T_F and T_R for these parameters as specified in Clause 16.
- Operation of the Bridge within the specified parameters shall not violate any of the other conformance provisions of this standard.

5.2 Optional capabilities

A MAC Bridge for which conformance to this standard is claimed may

- a) Support management of the Bridge. Bridges claiming to support management shall support all the management objects and operations for all implemented capabilities as defined in Clause 14.
- b) Support the use of a remote management protocol. Bridges claiming to support remote management shall
 - 1) State which remote management protocol standard(s) or specification(s) are supported.
 - 2) State which standard(s) or specification(s) for managed object definitions and encodings are supported for use by the remote management protocol.
- c) Support multiple Traffic Classes for relaying and filtering frames through one or more outbound Ports, controlling the mapping of the priority of forwarded frames as specified in 6.4, 7.5.1, and 7.7.
- d) Support Extended Filtering Services for relaying and filtering frames as described in 7.1 and specified in 7.5, 7.6, 7.7, and 7.9. Bridges claiming to support of Extended Filtering Services shall
 - 1) Implement the GARP Multicast Registration Protocol (GMRP), as specified in Clause 10.
 - 2) Implement the Generic Attribute Registration Protocol (GARP), in support of the GMRP Application as specified in Clause 12.

NOTE—The term capability is used to describe a set of related detailed provisions of this standard. Each capability can comprise both mandatory provisions, required if implementation of the capability is to be claimed, and optional provisions. Each detailed provision is specified in one or more of the other clauses of this standard. The Protocol Implementation Conformance Statement (PICS), described in 5.3, provides a useful checklist of these provisions.

5.3 Protocol Implementation Conformance Statement

The supplier of an implementation that is claimed to conform to this standard shall complete a copy of the PICS proforma provided in Annex A and shall provide the information necessary to identify both the supplier and the implementation.

5.4 Recommendations

Support of the relevant managed objects and management operations specified in Clause 14, and support of the use of SNMP to access them, is highly recommended.

5.5 MAC-specific bridging methods

MAC-specific bridging methods may exist. Use of a MAC-specific bridging method and the method specified in this standard on the same LAN shall

- a) Not prevent communication between stations in a Bridged Local Area Network.
- b) Preserve the MAC Service.
- c) Preserve the characteristics of each bridging method within its own domain.
- d) Allow both bridging techniques to coexist simultaneously on a LAN without adverse interaction.

6. Support of the MAC Service

MAC Bridges interconnect the separate IEEE 802 LANs that compose a Bridged Local Area Network by relaying and filtering frames between the separate MACs of the bridged LANs. The position of the bridging function within the MAC Sublayer is shown in Figure 6-1.

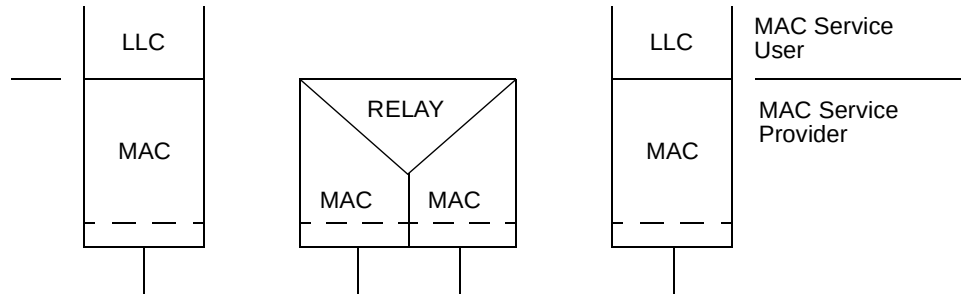


Figure 6-1—Internal organization of the MAC sublayer

This clause discusses the following aspects of service provision:

- a) Provision of the MAC Service to end stations.
- b) Preservation of the MAC Service.
- c) Maintenance of QoS.
- d) Provision of the Internal Sublayer Service within the MAC Bridge.
- e) Support of the Internal Sublayer Service by specific MAC procedures.
- f) Filtering services.

6.1 Support of the MAC Service

The MAC Service provided to end stations attached to a Bridged Local Area Network is the (unconfirmed) connectionless-mode MAC Service defined in ISO/IEC 15802-1. The MAC Service is defined as an abstraction of the features common to a number of specific MAC Services; it describes the transfer of user data between source and destination end stations, via MA-UNITDATA request primitives and corresponding MA-UNITDATA indication primitives issued at MAC service access points. Each MA-UNITDATA request and indication primitive has four parameters: Destination Address, Source Address, MAC Service data unit (MSDU), and Priority.

To improve the availability of the MAC Service to end stations and support network management, MAC Bridges can be configured:

- a) To provide redundant paths between end stations to enable the network to continue to provide the MAC Service in the event of component failure (of Bridge or LAN).
- b) So that the paths supported between end stations are predictable and configurable given the availability of network components.

A MAC Bridge may restrict the provision of the MAC Service to authenticated and authorized devices. Unauthorized devices can be denied access to a bridged LAN, except as necessary for the purpose of conducting protocol exchanges required by an authentication process.

NOTE—Authentication and authorization to access a LAN may be achieved by administrative or management mechanisms, or by means of an active authorization mechanism, such as is defined in IEEE Std 802.1X.

6.2 Preservation of the MAC Service

The MAC Service provided by a Bridged Local Area Network is similar to that provided by a single LAN (6.3). In consequence,

- a) A Bridge is not directly addressed by communicating end stations, except as an end station for management purposes—frames transmitted between end stations carry the MAC Address of the peer-end station in their Destination Address field, not a MAC Address of the Bridge.
- b) All MAC Addresses need to be unique within the network.
- c) MAC Addresses of end stations are not restricted by the topology and configuration of the network.

6.3 Quality of Service maintenance

Quality of Service comprises the following:

- a) Service availability
- b) Frame loss
- c) Frame misordering
- d) Frame duplication
- e) Frame transit delay
- f) Frame lifetime
- g) Undetected frame error rate
- h) Maximum service data unit size supported
- i) Frame priority
- j) Throughput

6.3.1 Service availability

Service availability is measured as a fraction of some total time during which the MAC Service is provided. The operation of a Bridge can increase or lower the service availability.

Service availability can be increased by automatic reconfiguration of the network (see Clause 17) to avoid the use of a failed component (e.g., repeater, cable, or connector) in the data path. Service availability can be lowered by the failure of a Bridge or by a Bridge filtering frames.

A Bridge can discard frames (6.3.2) to preserve other aspects of the MAC Service (6.3.3 and 6.3.4) during reconfiguration, lowering service availability for end stations that do not benefit from the reconfiguration. If an end station moves, it can then be unable to receive frames from other end stations until the filtering information held by the Bridges and used to localize traffic is updated. To minimize service denial, filtering information that has been dynamically learned can be modified when reconfiguration takes place (17.11). However, filtering information that is statically configured cannot be modified in this way.

A Bridge may deny service and discard frames to prevent network access by unauthorized devices.

To maximize the service availability, no loss of service or delay in service provision is caused by Bridges, except as a consequence of a failure, removal, or insertion of a network component, or as a consequence of the movement of an end station, or as a consequence of an attempt to perform unauthorized access. These are regarded as extraordinary events. The operation of any additional protocol necessary to maintain the quality of the MAC Service is thus limited to the configuration of the Bridged Local Area Network, and is independent of individual instances of service provision.

NOTE—This is true only in the absence of admission control mechanisms, i.e., where the Bridges provide a “best effort” service. The specification and applicability of admission controls in Bridges is outside the scope of this standard.

6.3.2 Frame loss

The MAC Service does not guarantee the delivery of Service Data Units. Frames transmitted by a source station arrive, uncorrupted, at the destination station with high probability. The operation of a Bridge introduces minimal additional frame loss.

A frame transmitted by a source station can fail to reach its destination station as a result of the following:

- a) Frame corruption during physical layer transmission or reception.
- b) Frame discard by a Bridge because
 - 1) It is unable to transmit the frame within some maximum period of time, and is required to discard the frame to prevent the maximum frame lifetime (6.3.6) from being exceeded.
 - 2) It is unable to continue to store the frame due to exhaustion of internal buffering capacity as frames continue to arrive at a rate in excess of that at which they can be transmitted.
 - 3) The size of the service data unit carried by the frame exceeds the maximum supported by the MAC procedures employed on the LAN to which the frame is to be relayed.
 - 4) Changes in the physical topology of the network necessitate frame discard for a limited period of time to maintain other aspects of QoS (see 17.10).
 - 5) The device attached to the Port is not authorized for access to the network.
 - 6) The configuration of Static Filtering Entries in the Filtering Database (7.9.1) disallows the forwarding of frames with particular destination addresses on specific Ports.

NOTE—As Static Filtering Entries are associated with particular Ports or combinations of Ports, there is a possibility that mis-configuration of Static Filtering Entries will lead to unintended frame discard during or following automatic reconfiguration of the Bridged Local Area Network.

6.3.3 Frame misordering

The MAC Service (9.2 of ISO/IEC 15802-1) permits a negligible rate of reordering of frames with a given user priority for a given combination of destination address and source address. MA_UNITDATA.indication service primitives corresponding to MA_UNITDATA.request primitives, with the same requested priority and for the same combination of destination and source addresses, are received in the same order as the request primitives were processed.

NOTE 1—The Forwarding Process in Bridges (7.7) does not misorder or duplicate frames.

Where Bridges are capable of connecting the individual MACs in such a way that multiple paths between any source station–destination station pairs exist, the operation of a protocol is required to ensure that a single path is used.

NOTE 2—Frame misordering and duplication (6.3.4) does not occur during normal operation. When RSTP is configuring or reconfiguring the network (see Clause 17), there is an increased and implementation-dependent probability that frames that are in transit will be misordered or duplicated as network paths change, since a Bridge can buffer frames awaiting transmission through its Ports. Since the probability of duplication or misordering occurring as a result of reconfiguration is small, and the frequency of physical network failures leading to reconfiguration is also generally small, the degradation of the properties of the MAC service is considered to be negligible. Some LAN protocols, for example, LLC Type 2, are particularly sensitive to frame misordering and duplication; to support these the Force Protocol Version parameter (17.13.4) can be used to delay the transition of ports to a Forwarding state and further reduce the probability of such events. A more detailed discussion of misordering and duplication in RSTP can be found in Annex K (informative).

6.3.4 Frame duplication

The MAC Service (9.2 of ISO/IEC 15802-1) permits a negligible rate of duplication of frames. Bridges do not duplicate user data frames.

The potential for frame duplication in a Bridged Local Area Network arises through the possibility of multiple paths between source and destination end stations. Where Bridges can connect individual LANs to provide multiple paths, the operation of a protocol is required to ensure that a single path is used.

6.3.5 Frame transit delay

The MAC Service introduces a variable frame transit delay that is dependent on media types and media access control methods. Frame transit delay is the elapsed time between an MA_UNITDATA.request primitive and the corresponding MA_UNITDATA.indication primitive. Elapsed time values are calculated only on Service Data Units that are successfully transferred.

Since the MAC Service is provided at an abstract interface within an end station, it is not possible to specify the total frame transit delay precisely. It is, however, possible to measure the media access and frame transmission and reception, and the transit delay introduced by an intermediate system, in this case a Bridge.

The minimum additional transit delay introduced by a Bridge is the time taken to receive a frame plus that taken to access the media onto which the frame is to be relayed. The frame is completely received before it is relayed as the Frame Check Sequence (FCS) is to be calculated and the frame discarded if in error.

6.3.6 Frame lifetime

The MAC Service mandates an upper bound to the transit delay experienced for a particular instance of communication. This maximum frame lifetime is necessary to ensure the correct operation of higher layer protocols. The additional transit delay introduced by a Bridge is discussed in 6.3.5.

Since the information provided by the MAC Sublayer to a Bridge does not include the transit delay already experienced by any particular frame, Bridges discard frames to enforce a maximum delay in each Bridge. A recommended and an absolute maximum value are specified in Table 7-3.

6.3.7 Undetected frame error rate

The MAC Service introduces a very low undetected frame error rate in transmitted frames. Undetected errors are protected against by the use of an FCS that is appended to the frame by the MAC Sublayer of the source station prior to transmission, and checked by the destination station on reception.

The FCS calculated for a given service data unit is dependent on the media access control method. It is therefore necessary to recalculate the FCS within a Bridge providing a relay function between IEEE 802 MACs of dissimilar types where there are differences in the method of calculation and/or the coverage of the FCS, or changes to the data that is within the coverage of the FCS. This introduces the possibility of additional undetected errors arising from the operation of a Bridge.

NOTE—Application of the techniques described in Annex F (informative) allow an implementation to achieve an arbitrarily small increase in undetected frame error rate, even in cases where the data that is within the coverage of the FCS is changed.

6.3.8 Maximum Service Data Unit Size

The Maximum Service Data Unit Size that can be supported by an IEEE 802 LAN varies with the MAC method and its associated parameters (speed, electrical characteristics, etc.). It may be constrained by the owner of the LAN. The Maximum Service Data Unit Size supported by a Bridge between two LANs is the smaller of that supported by the LANs. No attempt is made by a Bridge to relay a frame to a LAN that does not support the size of Service Data Unit conveyed by that frame.

6.3.9 Frame priority

The MAC Service includes user priority as a QoS parameter. MA_UNITDATA.requests with a high priority may be given precedence over other request primitives made at the same station, or at other stations attached to the same LAN, and can give rise to earlier MA_UNITDATA.indications.

The MAC Sublayer maps the requested user priorities onto the access priorities supported by the individual media access method. The requested user priority can be conveyed to the destination station with the transmitted frame, using the priority signaling mechanisms inherent in some media access methods. Since not all IEEE 802 LAN MACs can signal the user priority associated with a frame, Bridges regenerate user priority based upon a combination of signaled information and configuration information held in the Bridge.

The transmission delay experienced by a frame in a Bridge comprises:

- a) A queuing delay until the frame becomes first in line for transmission on the Port, in accordance with the procedure for selecting frames for transmission described in 7.7.4.
- b) The access delay for transmission of the frame.

Queueing delays can be managed using user priority. Access delays can be managed using user priority in media access methods that support more than one access priority.

The Bridge maps user priority onto one or more traffic classes; Bridges that support more than one traffic class are able to support expedited classes of traffic. The Forwarding Process, 7.7, describes the use of user priority and traffic classes in MAC Bridges. Given the constraints placed upon frame misordering in a Bridge, as expressed in 6.3.3, the mappings of priority and traffic class are static.

NOTE 1—The term Traffic Class, as used in this standard, is used only in the context of the operation of the priority handling and queueing functions of the Forwarding Process, as described in 7.7. Any other meanings attached to this term in other contexts do not apply to the use of the term in this standard.

The ability to signal user priority in IEEE 802 LANs allows user priority to be carried with end-to-end significance across a Bridged Local Area Network. This, coupled with a consistent approach to the mapping of user priority to traffic classes and of user priority to access_priority, allows consistent use of priority information, according to the capabilities of the Bridges and MACs in the transmission path.

NOTE 2—IEEE Std 802.1Q™ defines a frame format and procedures that can be used to carry user priority across LAN MAC types that are not able to signal user priority. Use of the IEEE 802.1Q frame format allows the end-to-end significance of user priority to be maintained regardless of the ability of individual LAN MAC types to signal priority.

Under normal circumstances, user priority is not modified in transit through the relay function of a Bridge; however, network management can control how user priority is propagated. Table 7-1 provides the ability to map incoming user priority values on a per-Port basis. By default, the regenerated user priority is identical to the incoming user priority.

6.3.10 Throughput

The total throughput provided by a Bridged Local Area Network can be significantly greater than that provided by an equivalent single LAN. Bridges may localize traffic within the network by filtering frames. Filtering services are described in 6.6.

The throughput between end stations communicating through a Bridge can be lowered by frame discard due to the Bridge's inability to transmit on the LAN to the destination at the required rate for an extended period.

6.4 Internal Sublayer Service provided within the MAC Bridge

The Internal Sublayer Service provided by a MAC entity to the MAC Relay Entity within a Bridge is that provided by the individual MAC for the LAN Port. This observes the appropriate MAC procedures and protocol for the LAN to which it attaches. No control frames, i.e., frames that do not convey MAC user data, are forwarded on any LAN other than that on which they originated.

The Internal Sublayer Service is derived from the MAC Service defined by ISO/IEC 15802-1 by augmenting that specification with elements necessary to the performance of the relay function. Within an end station, these additional elements are considered to be either below the MAC Service boundary, and pertinent only to the operation of the service provider; or local matters not forming part of the peer-to-peer nature of the MAC Service. Two parameters are added to the list of parameters associated with the MA_UNITDATA.request and MA_UNITDATA.indication primitives defined by ISO/IEC 15802-1. These are `frame_type` and `frame_check_sequence`. The definition of the Internal Sublayer Service does not add any new service primitives to those defined by the LAN MAC Service Definition.

6.4.1 Service primitives

The Internal Sublayer Service excludes MAC-specific features and procedures whose operation is confined to that of the individual LANs. The unit-data primitives that describe this service are

```
M_UNITDATA.indication    (  
    frame_type,  
    destination_address,  
    source_address,  
    mac_service_data_unit,  
    user_priority,  
    frame_check_sequence  
)
```

Each M_UNITDATA indication corresponds to the receipt of an error-free MAC frame from a LAN.

NOTE—Detailed specifications of error conditions in received frames are contained in the relevant MAC standards; for example, FCS errors, length errors, non-integral number of octets.

The **frame_type** parameter indicates the class of frame. The value of this parameter is one of `user_data_frame`, `mac_specific_frame`, or `reserved_frame`.

The **destination_address** parameter is the address of an individual MAC entity or a group of MAC entities.

The **source_address** parameter is the individual address of the source MAC entity.

The **mac_service_data_unit** parameter is the service user data.

The **user_priority** parameter is the priority requested by the originating service user. The value of this parameter is in the range 0 through 7.

NOTE—The default `user_priority` value is 0. Values 1 through 7 form an ordered sequence of `user_priorities`, with 1 being the lowest value and 7 the highest. See 7.7.3 and Annex G (informative) for further explanation of the use of `user_priority` values.

The **frame_check_sequence** parameter is explicitly provided as a parameter of the primitive so that it can be used as a parameter to a related request primitive without recalculation.

The identification of the LAN from which particular frames are received is a local matter and is not expressed as a parameter of the service primitive.

```
M_UNITDATA.request      (  
    frame_type,  
    destination_address,  
    source_address,  
    mac_service_data_unit,  
    user_priority,  
    access_priority,  
    frame_check_sequence  
)
```

A data request primitive is invoked to transmit a frame to an individual LAN.

The **frame_type** parameter indicates the class of frame.

The **destination_address** parameter is the address of an individual MAC entity or a group of MAC entities.

The **source_address** parameter is the individual address of the source MAC entity.

The **mac_service_data_unit** parameter is the service user data.

The **user_priority** parameter is the priority requested by the originating service user. The value of this parameter is in the range 0 (lowest) through 7 (highest).

The **access_priority** parameter is the priority used by the local service provider to convey the request. It can be used to determine the priority attached to the transmission of frames queued by the local MAC Entity, both locally and among other stations attached to the same individual LAN, if the MAC method permits. The value of this parameter, if specified, is in the range 0 (lowest) through 7 (highest).

The **frame_check_sequence** parameter is explicitly provided as a parameter of the primitive so that it can be used without recalculation.

The identification of the LAN to which a frame is to be transmitted is a local matter and is not expressed as a parameter of the service primitive.

6.4.2 MAC status parameters

In addition to the unit-data service primitives, the Internal Sublayer Service makes available a pair of status parameters that permit inspection of, and control over, the administrative and operational state of the MAC entity by the MAC Relay Entity.

MAC_Enabled: The value of this parameter is TRUE if use of the MAC entity is permitted; and is otherwise FALSE. The value of this parameter is determined by the specific MAC procedures, as specified in 6.5.

MAC_Operational: The value of this parameter is TRUE if the MAC entity is in a functioning state and MAC_Enabled is also TRUE; i.e., the MAC entity can be used to transmit and/or receive frames, and its use is permitted by management. Its value is otherwise FALSE. The value of this parameter is determined by the specific MAC procedures, as specified in 6.5.

NOTE—These status parameters provide a common approach across MACs for handling the fact that:

- a) A MAC can inherently be working or not (as indicated by MAC_Operational).
- b) If the MAC is operational, there may be the need to override its operational state for administrative reasons, preventing any users from making use of its services (by means of MAC_Enabled).

6.4.3 Point-to-Point MAC parameters

In addition to the unit-data service primitives, the Internal Sublayer Service makes available a pair of parameters that permit inspection of, and control over, the administrative and operational state of the point-to-point status of the MAC entity by the MAC Relay Entity.

operPointToPointMAC: This parameter can take two values, as follows:

- a) **True.** The MAC is connected to a point-to-point LAN; i.e., there is at most one other system attached to the LAN.
- b) **False.** The MAC is connected to a non-point-to-point LAN; i.e., there can be more than one other system attached to the LAN.

adminPointToPointMAC: This parameter can take three values, as follows:

- a) **ForceTrue.** The administrator requires the MAC to be treated as if it is connected to a point-to-point LAN, regardless of any indications to the contrary that are generated by the MAC entity.
- b) **ForceFalse.** The administrator requires the MAC to be treated as connected to a non-point-to-point LAN, regardless of any indications to the contrary that are generated by the MAC entity.
- c) **Auto.** The administrator requires the point-to-point status of the MAC to be determined in accordance with the specific MAC procedures defined in 6.5.

If adminPointToPointMAC is set to ForceTrue, then operPointToPointMAC shall be set True. If adminPointToPointMAC is set to ForceFalse, then operPointToPointMAC shall be set False.

If adminPointToPointMAC is set to Auto, then the value of operPointToPointMAC is determined in accordance with the specific procedures defined for the MAC entity concerned, as defined in 6.5. If these procedures determine that the MAC entity is connected to a point-to-point LAN, then operPointToPointMAC is set TRUE; otherwise it is set FALSE. In the absence of a specific definition of how to determine whether the MAC is connected to a point-to-point LAN or not, the value of operPointToPointMAC shall be FALSE.

The value of `operPointToPointMAC` is determined dynamically; i.e., it is re-evaluated whenever the value of `adminPointToPointMAC` changes, and whenever the specific procedures defined for the MAC entity evaluate a change in its point-to-point status.

6.5 Support of the Internal Sublayer Service by specific MAC procedures

This subclause specifies the mapping of the Internal Sublayer Service to the MAC Protocol and Procedures of each individual IEEE 802 MAC type, and the encoding of the parameters of the service in MAC frames. The mapping is specified by reference to the IEEE 802 standards that specify the individual MAC methods. The mapping draws attention to any special responsibilities of Bridges attached to LANs of that MAC type.

6.5.1 Support by IEEE Std 802.3 (CSMA/CD)

The CSMA/CD access method is specified in IEEE Std 802.3. Clause 3 of that standard specifies the MAC frame structure, and Clause 4 specifies the MAC method.

On receipt of an `M_UNITDATA.request` primitive, the local MAC Entity performs Transmit Data Encapsulation, assembling a frame using the parameters supplied as specified below. It prepends a preamble and a Start Frame Delimiter before handing the frame to the Transmit Media Access Management Component in the MAC Sublayer for transmission (IEEE Std 802.3, 4.2.3).

On receipt of a MAC frame by Receive Media Access Management, the MAC frame is passed to Receive Data Decapsulation, which validates the FCS and disassembles the frame, as specified below, into the parameters that are supplied with an `M_UNITDATA.indication` primitive (IEEE Std 802.3, 4.2.4).

The **frame_type** parameter takes only the value `user_data_frame` and is not encoded in MAC frames.

The **destination_address** parameter is encoded in the destination address field (IEEE Std 802.3, 3.2.3).

The **source_address** parameter is encoded in the source address field (IEEE Std 802.3, 3.2.3).

The number of octets of data in the **mac_service_data_unit** parameter is either:

- a) Encoded in the Length/Type field of the MAC frame if the frame makes use of the Length interpretation of the Length/Type field (see 3.2.6 in IEEE Std 802.3), or
- b) Determined from the length of the received MAC frame, if the frame makes use of the Type interpretation of the Length/Type field (see 3.2.6 in IEEE Std 802.3).

The octets of data are encoded in the data field (see 3.2.7 in IEEE Std 802.3). The Length/Type field forms the initial octets of the `mac_service_data_unit` parameter.

The **user_priority** parameter provided in a data request primitive is not encoded in MAC frames. The `user_priority` parameter provided in a data indication primitive shall take the value of the Default User Priority parameter for the Port through which the MAC frame was received. The default value of this parameter is 0, it may be set by management in which case the capability to set it to any of the values 0 through 7 shall be provided.

The **frame_check_sequence** parameter is encoded in the FCS field of the MAC frame (IEEE Std 802.3, 3.2.8). The FCS is computed as a function of the destination address, source address, length, data, and PAD fields. If an `M_UNITDATA.request` primitive is not accompanied by this parameter, it is calculated in accordance with 3.2.8 in IEEE Std 802.3.

NOTE 1—Since the PAD field, if present, contributes to the FCS, this parameter needs to include at least the contribution of the PAD field to the FCS in order for the original FCS to be preserved. [See Annex F (informative).]

No special action, above that specified for the support of use of the MAC Service by LLC, is required for the support of the MAC Internal Sublayer Service by the CSMA/CD access method.

NOTE 2—The support by IEEE Std 802.3 is described only in terms of the operation of a Bridge when relaying frames that result from the use of LLC services over an IEEE 802.3 MAC. IEEE Std 802.1H defines the recommended practice for bridging Ethernet V2.0 frames.

The values of the MAC_Enabled and MAC_Operational parameters are determined as follows:

- a) For a MAC entity that contains a Link Aggregation sublayer, the value of MAC_Enabled is directly determined by the value of the aAggAdminState attribute (30.7.1.13 in IEEE Std 802.3-2002), and the value of MAC_Operational is directly determined by the value of the aAggOperState attribute (30.7.1.13 in IEEE Std 802.3).
- b) Otherwise, for IEEE 802.3 MAC entities that support the MAU managed Object Class (30.5.1 in IEEE Std 802.3):
 - 1) The value of MAC_Enabled is TRUE.
 - 2) The value of MAC_Operational is TRUE if the attribute aMediaAvailable carries the value *available*.
 - 3) The value of MAC_Operational is FALSE if the attribute aMediaAvailable carries any value other than *available*.
- c) Otherwise:
 - 1) The value of MAC_Enabled is TRUE.
 - 2) The value of MAC_Operational is TRUE.

From the point of view of determining the value of operPointToPointMAC (6.4.3), the MAC is considered to be connected to a point-to-point LAN if any of the following conditions are true:

- a) The MAC entity concerned contains a Link Aggregation sublayer, and the set of physical MACs associated with the Aggregator are all aggregatable; or
- b) The MAC entity concerned supports auto negotiation (Clause 28 of IEEE Std 802.3), and the auto negotiation function has determined that the LAN is to be operated in full duplex mode; or
- c) The MAC entity has been configured by management means for full duplex operation.

Otherwise, the MAC is considered to be connected to a LAN that is not point-to-point.

6.5.2 Support by IEEE Std 802.5 (token-passing ring)

The token-passing ring access method is specified in IEEE Std 802.5. Clause 3 of that standard specifies formats and facilities, and Clause 4 specifies token-passing ring protocols.

On receipt of an M_UNITDATA.request primitive the local MAC Entity composes a frame using the parameters supplied as specified below, appending the frame control, destination address, source address, and FCS fields to the user data, and enqueueing the frame for transmission. On transmission, the starting delimiter, access control field, ending delimiter, and frame status fields are added.

On receipt of a valid MAC frame (IEEE Std 802.5, 4.1.4) that was not transmitted by the Bridge Port's local MAC Entity, with the Routing Information Indicator bit (which occupies the same position in the source address field as does the Group Address bit in the destination address field) set to zero, an M_UNITDATA.indication primitive is generated, with parameters derived from the frame fields as specified in the paragraphs that follow.

The **frame_type** parameter is encoded in the frame_type bits (FF bits) of the frame control field (IEEE Std 802.5, 3.2.3.1). A bit pattern of 0 1 denotes a user_data_frame, a bit pattern of 0 0 denotes a mac_specific_frame, and a bit pattern of 1 0 or 1 1 denotes a reserved_frame.

The **destination_address** parameter is encoded in the destination address field (IEEE Std 802.5, 3.2.4.1).

The **source_address** parameter is encoded in the source address field (IEEE Std 802.5, 3.2.4.2).

The **mac_service_data_unit** parameter is encoded in the information field (IEEE Std 802.5, 3.2.6).

The **user_priority** parameter associated with user_data_frames is encoded in the YYY bits of the frame control field (IEEE Std 802.5, 3.2.3).

The **frame_check_sequence** parameter is encoded in the FCS field of the MAC frame (IEEE Std 802.5, 3.2.7). The FCS is computed as a function of the frame control, destination address, source address, and information fields. If an M_UNITDATA.request primitive is not accompanied by this parameter, it is calculated in accordance with IEEE Std 802.5, 3.2.7.

The Address Recognized (A) bits in the Frame Status field of a frame (IEEE Std 802.5, 3.2.9) may be set to 1 if an M_UNITDATA.indication primitive with a frame_type of user_data_frame is generated, or if such an indication would be generated if buffering had been available; otherwise, the A bits shall not be set except as required by IEEE Std 802.5.

If the A bits are set to 1, the Frame Copied (C) bits (IEEE Std 802.5, 3.2.9) may be set to 1 to reflect the availability of receive buffering; otherwise, the C bits shall not be set.

In order to support the MAC Internal Sublayer Service, a Token Ring Bridge must be capable of recognizing and removing frames transmitted by itself, even though they can carry a source address different from that of the Bridge Port that transmitted them.

The values of the MAC_Enabled and MAC_Operational parameters are determined as follows:

- a) For Dedicated Token Ring and High-Speed Token Ring MAC entities:
 - 1) The value of MAC_Enabled is TRUE.
 - 2) The value of MAC_Operational is set to TRUE upon invocation of a Mgt_Event_Report.request with an eventRequestType of CPortOperational (see 11.2.2.2 in IEEE Std 802.5).
 - 3) The value of MAC_Operational is set to FALSE upon invocation of a Mgt_Event_Report.request with an eventRequestType of CPortNonOperational, CPortFailure, or ProtocolError (see 11.2.2.2 in IEEE Std 802.5).
- b) For all other IEEE 802.5 MAC entities:
 - 1) The value of MAC_Enabled is TRUE.
 - 2) The value of MAC_Operational is set to TRUE upon invocation of a Mgt_Event.indication with an event parameter value of evRingOperational (see 6.1.2 in IEEE Std 802.5).
 - 3) The value of MAC_Operational is set to FALSE upon invocation of a Mgt_Event.indication with an event parameter value of evRingNonOperational, evRingBeaconing, evStationFailure, or evProtocolError (see 6.1.2 in IEEE Std 802.5).

6.5.3 Support by fibre distributed data interface (FDDI)

The FDDI access method is specified in ISO 9314-2:1989. Clause 6 of that standard specifies Services, and Clauses 7 and 8 specify Facilities and Operation, respectively.

On receipt of a valid frame (ISO 9314-2, 8.3.1) that was not transmitted by the Bridge Port's local MAC entity, with the first bit of the source address equal to zero, an M_UNITDATA.indication is generated. The associated parameters are derived from the frame fields as specified shortly below.

The Address Recognized (A) indicator in the Frame Status field of the frame (ISO 9314-2, 7.3.8) on the ring from which it was received shall not be set except as required by ISO 9314-2. The Frame Copied (C) indicator (ISO 9314-2, 7.3.8) may be set if an M_UNITDATA.indication primitive with a frame_type of user_data_frame is generated, if the frame is to be forwarded, and if receive buffering is available. Otherwise, the C indicator shall not be altered except as required by ISO 9314-2.

NOTE—This specification of the setting of the C indicator by ISO 9314-2 MAC Bridges enhances that given in ISO 9314-2. A Bridge can be required by ISO 9314-2 to alter the A and/or C indicators when receiving a frame addressed to the Bridge as an FDDI end station, or when receiving a frame associated with the operation of the FDDI MAC.

The parameters associated with the M_UNITDATA.indication generated on receipt of a frame follow:

The **frame_type** parameter is encoded in the frame format bits (CL, FF, and ZZZZ bits) of the Frame Control field (ISO 9314-2, 7.3.3). The bit pattern 0L01rXXX denotes a user_data_frame (asynchronous LLC frame, where L represents the address length and can be 0 or 1, r is reserved and can be received as 0 or 1, and XXX can range from 000 to 111). All other bit patterns yield a frame_type parameter value of not_user_data_frame.

The **destination_address** parameter is enclosed in the destination address field (ISO 9314-2, 7.3.4–7.3.4.1).

The **source_address** parameter is encoded in the source address field (ISO 9314-2, 7.3.4–7.3.4.2).

The **mac_service_data_unit** parameter is encoded in the information field (ISO 9314-2, 7.3.5).

The **user_priority** parameter associated with user_data_frames is encoded in the PPP bits of the frame control field (ISO 9314-2, 7.3.3.4) when the frame is an asynchronously transmitted LLC frame whose frame control field value is 0L010PPP, where L represents the address length (ISO 9314-2, 7.3.3.2).

The **frame_check_sequence** parameter is encoded in the Frame Check Sequence Field of the MAC frame (ISO 9314-2, 7.3.6). The frame_check_sequence is computed as a function of the frame control, destination address, source address, and information fields.

On receipt of an M_UNITDATA.request primitive, the local MAC entity composes a frame using the parameters supplied as specified above, appending the frame control, destination address, source address, and frame check sequence to the user data, and enqueueing the frame for transmission on reception of a suitable token (ISO 9314-2, 8.3.1). On transmission, the preamble, starting delimiter, ending delimiter, and frame status fields are added.

If an M_UNITDATA.request primitive is not accompanied by a frame check sequence, one is calculated in accordance with ISO 9314-2, 7.3.6.

The bit pattern of the frame control field shall be 0L01rPPP, indicating an asynchronous LLC frame with L representing the address length (ISO 9314-2, 7.3.3.2), r being reserved and set to zero, and PPP indicating the frame's priority (ISO 9314-2, 7.3.3.4).

If the **user_priority** parameter value is specified, it is encoded in the PPP bits and the access priority (ISO 9314-2, 8.1.4) is derived from the token-holding timer (THT) or otherwise by implementor option. If the user_priority parameter value is unspecified, the PPP bits shall be set to zero and the access priority derived from the THT.

In order to support the MAC Internal Layer Service, an FDDI bridge removes frames transmitted by itself as required by ISO 9314-2:1989, even though they can carry a source address different from that of the bridge port that transmitted them.

6.5.4 Support by IEEE Std 802.11 (Wireless LANs)

The wireless LAN access method is specified in IEEE Std 802.11, 1999 Edition. Clause 7 of that standard specifies frame formats, Clause 9 specifies the MAC sublayer function, and Clause 11 specifies the mandatory MAC sublayer management function.

A Bridge to an IEEE 802.11 LAN shall connect to an IEEE 802.11 Portal, which in turn connects to an IEEE 802.11 Distribution System. For the purposes of bridging, the service interface presented at the Portal is identical to the service interface presented at the IEEE 802.11 MAC SAP. An instance of an 802.11 Distribution System can be implemented from IEEE 802 LAN components. IEEE 802.11 STAs attach to the Distribution System via an IEEE 802.11 Access Point. A bridge shall not connect to an IEEE 802.11 Independent BSS. For a description of the IEEE 802.11 architecture, see Clause 5 of IEEE Std 802.11.

On receipt of an M_UNITDATA.request primitive, the portal constructs a MAC Service Data Unit and passes it to the MAC Data service for transmission (in accordance with the frame formats and procedures specified in IEEE Std 802.11 Clauses 6, 7, 9, and Annex C) using the parameters supplied as specified below.

On receipt of a valid MAC Service Data Unit (see IEEE Std 802.11 Clauses 6, 7, 9, and Annex C), the portal generates an M_UNITDATA.indication primitive with parameter values derived from the frame fields as specified below.

The frame_type parameter only takes the value user_data_frame. When processing MSDU_from_LLC, the frame_type of user_data_frame shall be translated according to parameters specified in 7.1.3.1 of IEEE Std 802.11 and is explicitly encoded in MAC frames.

The destination_address parameter is encoded in MAC frames as the DA described in Table 4 of 7.2.2 of IEEE Std 802.11.

The source_address parameter is encoded in MAC frames as the SA described in Table 4 of 7.2.2 of IEEE Std 802.11.

The mac_service_data_unit parameter is encoded in the Frame Body field (IEEE Std 802.11, 7.1.3.5) of MAC frames. The length of the MSDU shall be ≤ 2304 octets. The length is not encoded in MAC frames; rather, it is conveyed in the PHY headers.

The user_priority parameter is not encoded in MAC frames. The user_priority parameter provided in an M_UNITDATA.indication primitive shall take the value of the Default_User_Priority parameter for the port through which the MAC Service Data Unit was received. The default value of this parameter is 0, it may be set by management, in which case the capability to set it to any of the values 0 through 7 shall be provided.

The Frame Check Sequence (FCS) field of MAC frames is calculated and encoded in accordance with IEEE Std 802.11, 7.1.3.6.

The access_priority parameter is not encoded in MAC frames.

No special action, above that specified in IEEE Std 802.11, is required for the support of the MAC Internal Sublayer Service by the wireless LAN access method.

6.6 Filtering services in Bridged Local Area Networks

MAC Bridges provide filtering services that support aspects of the maintenance of QoS—in particular, transit delay, priority, and throughput. In addition, these services provide a degree of administrative control over the propagation of particular MAC Addresses in the network.

The services described are services in the most general sense; i.e., descriptions of functionality available to a MAC Service user or an administrator to control and access filtering capabilities. The descriptions make no assumptions as to how the service might be realized. There are at least the following possibilities:

- a) Use of existing protocols and mechanisms, defined in IEEE 802 standards and elsewhere.
- b) Use of management functionality, either locally defined or via remote management protocols.
- c) Other means, standardized or otherwise.

6.6.1 Purpose(s) of filtering service provision

Filtering services are provided for the purposes described in 6.6.1.1 and 6.6.1.2.

6.6.1.1 Administrative control

Filtering services provide administrative control over the use of particular source and destination addresses in designated parts of the network. Such control allows network managers and administrators to limit the extent of operation of network layer and other protocols that use individual and group MAC Addresses by establishing administrative boundaries across which specific MAC Addresses are not forwarded.

6.6.1.2 Throughput and end station load

Filtering services increase the overall throughput of the network, and reduce the load placed on end stations caused by the reception of frames that are destined for other end stations, by

- a) Limiting frames destined for specific MAC Addresses to parts of the network that, to a high probability, lie along a path between the source MAC Address and the destination MAC Address.
- b) Reducing the extent of group addressed frames to those parts of the network that contain end stations that are legitimate recipients of that traffic.

NOTE—Some aspects of the filtering services described in this standard are dependent upon the active participation of end stations. Where such participation is not possible, those aspects of the filtering services will be unavailable.

6.6.2 Goals of filtering service provision

The filtering services provided can be used to

- a) Allow the MAC Service provider to dynamically learn where the recipients of frames addressed to individual MAC Addresses are located.
- b) Allow end stations that are the potential recipients of MAC frames destined for group MAC Addresses to dynamically indicate to the MAC Service provider which destination MAC Address(es) they wish to receive.
- c) Exercise administrative control over the extent of propagation of specific MAC Addresses.

6.6.3 Users of filtering services

The filtering services provided are available to the following users:

- a) Network management and administration, for the purposes of applying administrative control. Interactions between administrators of the network and the filtering service provider may be achieved by local means or by means of explicit management mechanisms.
- b) End stations, for the purposes of controlling the destination addresses that they will receive. Interactions between end stations and the filtering service provider may be implicit, as is the case with the Learning Process (7.8), or by explicit use of filtering service primitives.

6.6.4 Basis of service

All filtering services in Bridged Local Area Networks rely on the establishment of filtering rules, and subsequent filtering decisions, that are based on the value(s) contained in the Source or Destination MAC Address fields in MAC frames.

NOTE—The filtering services defined by this standard use source address learning and destination address filtering.

6.6.5 Categories of service

Filtering services in Bridged Local Area Networks fall into the following categories:

- a) *Basic Filtering Services*. These services are supported by the Forwarding Process (7.7) and by Static Filtering Entries (7.9.1) and Dynamic Filtering Entries (7.9.2) in the Filtering Database. The information contained in the Dynamic Filtering Entries is maintained through the operation of the Learning Process (7.8).
- b) *Extended Filtering Services*. These services are supported by the Forwarding Process (7.7), and the Static Filtering Entries (7.9.1) and Group Registration Entries (7.9.3) in the Filtering Database. The information contained in the Group Registration Entries is maintained through the operation of GMRP (10). The categories of Extended Filtering Service are as follows:
 - 1) Support of dynamic Group forwarding and filtering behavior.
 - 2) The ability for static filtering information for individual MAC Addresses to specify a subset of Ports for which forwarding or filtering decisions are taken on the basis of dynamic filtering information.

NOTE—Basic Filtering Services as defined in this standard correspond exactly to the filtering capabilities provided by the MAC Bridges standard in IEEE Std 802.1D, 1993 Edition [ISO/IEC 10038: 1993].

All Bridges shall support Basic Filtering Services and may support either or both categories of Extended Filtering Services.

6.6.6 Service configuration

In the absence of explicit information in the Filtering Database, the behavior of the Forwarding Process with respect to the forwarding or filtering of frames destined for group MAC Addresses depends upon the categories of service supported by the Bridge.

Basic Filtering Services support the filtering behavior required for regions of a Bridged Local Area Network in which potential recipients of multicast frames exist, but where either the recipients or the Bridges are either unable to support the dynamic configuration of filtering information for those group MAC Addresses, or the recipients have a requirement to receive all traffic destined for group MAC Addresses.

Extended Filtering Services support the filtering behavior required for regions of a network in which potential recipients of multicast frames exist, and where both the potential recipients of frames and the Bridges are able to support dynamic configuration of filtering information for group MAC Addresses. In order to integrate this extended filtering behavior with the needs of regions of the network that support only Basic Filtering Services, Bridges that support Extended Filtering Services can be statically and dynamically

configured to modify their filtering behavior on a per-group MAC Address basis, and also on the basis of the overall filtering service provided by each outbound Port with regard to multicast frames. The latter capability permits configuration of the Port's default forwarding or filtering behavior with regard to group MAC Addresses for which no specific static or dynamic filtering information has been configured.

Service configuration provides the ability to configure the overall filtering for the following cases:

- a) Bridges that only implement Basic Filtering Services.
- b) Bridges that support Extended Filtering Services in a heterogeneous environment, where some equipment is unable to participate in Dynamic Multicast Filtering, or where some equipment (e.g., routers) have specific needs to see unfiltered traffic.
- c) Bridges that support Extended Filtering Services in a homogeneous environment, where all equipment is able to participate in Dynamic Multicast Filtering.

6.6.7 Service definition for Extended Filtering Services

The Filtering Services are described by means of service primitives that define particular types of interaction between MAC Service users and the MAC Service provider across the MAC Service boundary. As these interactions are not defined between peer entities, they are described simply in terms of service requests sent from the MAC Service user to the MAC Service provider.

6.6.7.1 Dynamic registration and de-registration services

These services allow MAC Service users dynamic control over the set of destination Group MAC Addresses that they will receive from the MAC Service provider, by:

- a) Registering/de-registering membership of specific Groups associated with those addresses.
- b) Registering/de-registering service requirements with regard to the overall forwarding/filtering behavior for Groups.

Provision of these services is achieved by means of GMRP and its associated procedures, as described in Clause 10.

NOTE—The intent of these services is to provide the MAC Service user with dynamic control over access to multicast data streams, for example, multiple video channels made available by a server using a different group MAC Address for each channel. The ability to both register and de-register Group membership, coupled with the filtering action associated with the Group membership, limits the impact of such services on the bandwidth available in the network. These services can be used to control the reception of other categories of multicast traffic, for similar reasons.

REGISTER_GROUP_MEMBER (MAC_ADDRESS)

Indicates to the MAC Service provider that the MAC Service user wishes to receive frames containing the group MAC Address indicated in the MAC_ADDRESS parameter as the destination address. The MAC Addresses that can be carried by this parameter do not include the following:

- a) Any individual address.
- b) Any of the Reserved Addresses identified in Table 7-10.
- c) Any of the GARP Application addresses, as defined in Table 12-1.

DEREGISTER_GROUP_MEMBER (MAC_ADDRESS)

Indicates to the MAC Service provider that the end station no longer wishes to receive frames containing the group MAC Address indicated in the MAC_ADDRESS parameter as the destination address.

REGISTER_SERVICE_REQUIREMENT (REQUIREMENT_SPECIFICATION)

Indicates to the MAC Service provider that the MAC Service user has a requirement for any devices that support Extended Filtering Services to forward frames in the direction of the MAC Service User in accordance with the definition of the service requirement defined by the REQUIREMENT_SPECIFICATION parameter. The values that can be carried by this parameter are as follows:

- a) Forward All Groups.
- b) Forward Unregistered Groups.

DEREGISTER_SERVICE_REQUIREMENT (REQUIREMENT_SPECIFICATION)

Indicates to the MAC Service provider that the MAC Service user no longer has a requirement for any devices that support Extended Filtering Services to forward frames in the direction of the MAC Service User in accordance with the definition of the service requirement defined by the REQUIREMENT_SPECIFICATION parameter. The values that can be carried by this parameter are as follows:

- a) Forward All Groups.
- b) Forward Unregistered Groups.

The use of these services can result in the propagation of group MAC Address and service requirement information across the Spanning Tree, affecting the contents of Group Registration Entries (7.9.3) in Bridges and end stations, and thereby affecting the frame forwarding behavior of the Bridges and end stations with regard to multicast frames.

7. Principles of Bridge operation

This clause:

- a) Explains the principal elements of Bridge operation and lists the functions that support these.
- b) Establishes an architectural model for a Bridge that governs the provision of these functions.
- c) Provides a model of Bridge operation in terms of Processes and Entities that support the functions.
- d) Details the addressing requirements in a Bridged Local Area Network and specifies the addressing of Entities in a Bridge.

7.1 Bridge operation

The principal elements of Bridge operation are as follows:

- a) Relay and filtering of frames.
- b) Maintenance of the information required to make frame filtering and relaying decisions.
- c) Management of the above.

7.1.1 Relay

A MAC Bridge relays individual MAC user data frames between the separate MACs of the bridged LANs connected to its Ports. The functions that support relaying frames and maintain QoS are as follows:

- a) Frame reception.
- b) Discard on received frame in error (6.3.2).
- c) Frame discard if the frame_type is not user_data_frame (6.4).
- d) Regeneration of user priority, if required (6.4).
- e) Frame discard to suppress loops in the physical topology of the network.
- f) Frame discard to support management control over the physical topology of the network.
- g) Frame discard following the application of filtering information.
- h) Frame discard on transmittable service data unit size exceeded (6.3.8).
- i) Forwarding of received frames to other Bridge Ports.
- j) Selection of traffic class, following the application of filtering information.
- k) Queuing of frames by traffic class.
- l) Frame discard to ensure that a maximum bridge transit delay is not exceeded (6.3.6).
- m) Selection of queued frames for transmission.
- n) Selection of outbound access priority (6.3.9).
- o) Mapping of service data units and recalculation of Frame Check Sequence, if required (6.3.7, 7.7.6).
- p) Frame transmission.

7.1.2 Filtering and relaying information

A Bridge filters frames, i.e., does not relay frames received by a Bridge Port to other Ports on that Bridge, in order to prevent frame duplication (6.3.4), and to allow administrative control over network resources. The functions that support the use and maintenance of information for this purpose are as follows:

- a) Distributed calculation and configuration of Port State (7.4) for each Bridge Port in the network, to provide a fully, simply, and symmetrically connected spanning tree active topology.
- b) Administrative setting of the MAC_Enabled (6.4.2) or Administrative Bridge Port State (14.8.2.2) to exclude a Bridge Port from the active topology.
- c) Default or administrative configuration of the Rapid Spanning Tree Protocol parameters (Clause 17) to influence inclusion in the active topology of specific Bridge Ports and the LANs they connect.

A Bridge also filters frames to reduce traffic in parts of the network that do not lie in the path between the source and destination of that traffic. The functions that support the use and maintenance of information for this purpose are as follows:

- d) Permanent configuration of reserved addresses.
- e) Explicit configuration of static filtering information.
- f) Automatic learning of dynamic filtering information for unicast destination addresses through observation of source addresses of network traffic.
- g) Ageing out of dynamic filtering information that has been learned.
- h) Automatic addition and removal of dynamic filtering information as a result of GMRP exchanges.

A Bridge expedites the transmission of frames generated by critical or time-sensitive services. The function that supports the use and maintenance of information for this purpose is as follows:

- i) Explicit configuration of traffic class information associated with the Ports of the Bridge.

7.1.3 Bridge management

The functions that support Bridge Management control and monitor the provision of the above functions are specified in Clause 14.

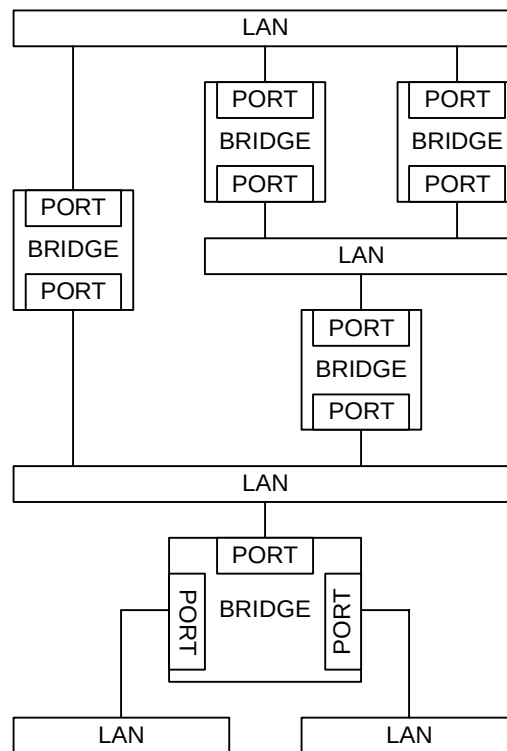


Figure 7-1—A Bridged Local Area Network

7.2 Bridge architecture

A Bridge is modeled as comprising:

- a) A MAC Relay Entity that interconnects the Bridge's Ports.
- b) At least two Port;.
- c) Higher-Layer Entities, including at least a Spanning Tree Protocol Entity.

The MAC Relay Entity handles the Media Access Method Independent Functions of relaying frames between Bridge Ports, filtering frames, and learning filtering information. It uses the Internal Sublayer Service (6.4, 6.5) provided by the separate MAC Entities of each Port.

Each Bridge Port transmits and receives frames to and from the LAN to which it is attached. An individual MAC Entity permanently associated with the Port provides the Internal Sublayer Service (6.4, 6.5) used for frame transmission and reception. The MAC Entity handles all the Media Access Method Dependent Functions (MAC protocol and procedures).

The Spanning Tree Protocol Entity calculates and configures the active topology of the network.

The Spanning Tree Protocol Entity and other higher-layer protocol users, such as Bridge Management (7.1.3) and GARP application entities including GARP Participants (Clause 12), make use of Logical Link Control procedures. These procedures are provided separately for each Port and use the MAC Service provided by the individual MAC Entities.

Figure 7-1 gives an example of the physical topology of a Bridged Local Area Network. LANs are interconnected by MAC Bridges; each Port of a Bridge connects to a single LAN. Figure 7-2 illustrates a Bridge with two Ports, and Figure 7-3 illustrates the architecture of such a Bridge. The term "LLC Entities," used in Figure 7-3 and Figure 7-9, refers to the union of the Link Layer capabilities (which include demultiplexing), provided by LLC (ISO/IEC 8802-2), and the Type interpretation of the Length/Type field specified in IEEE Std 802.3

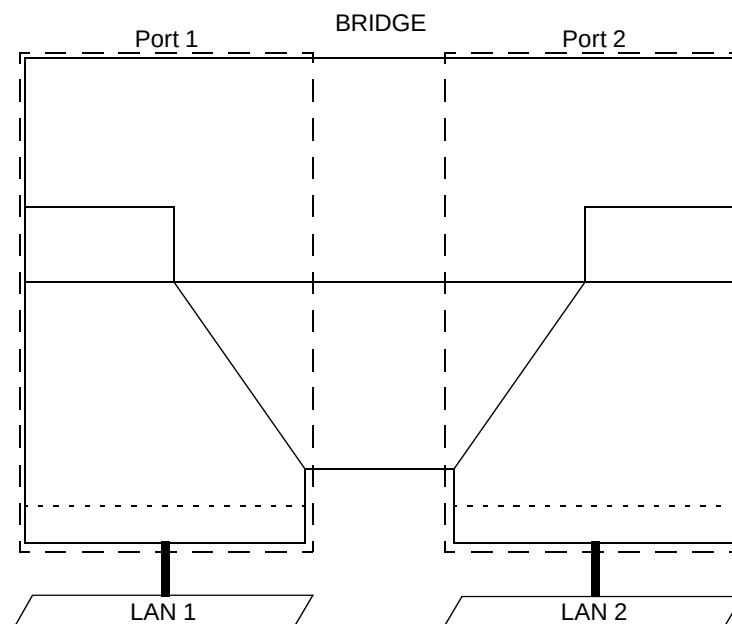


Figure 7-2—Bridge ports

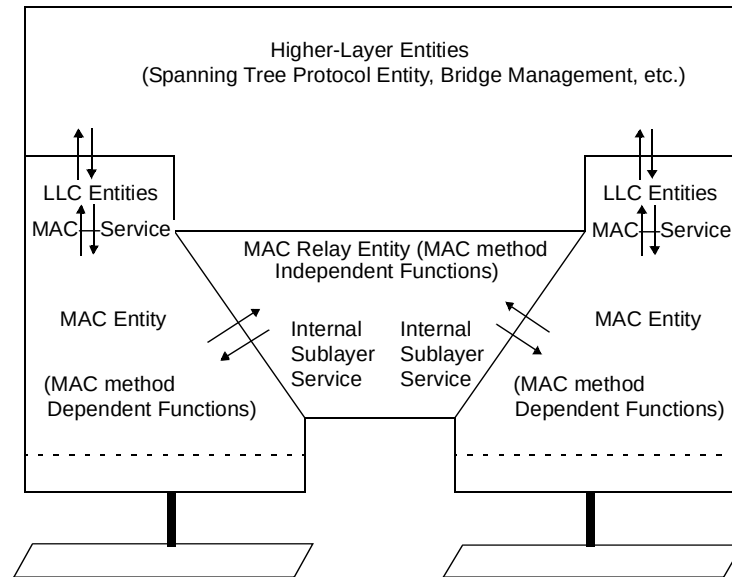


Figure 7-3—Bridge architecture

7.3 Model of operation

The model of operation is simply a basis for describing the functionality of the MAC Bridge. It is in no way intended to constrain real implementations of a MAC Bridge; these may adopt any internal model of operation compatible with the externally visible behavior that this standard specifies. Conformance of equipment to this standard is purely in respect of observable protocol.

Subclauses 7.5 and 7.6 specify the MAC Relay Entity's use of the Internal Sublayer Service. Port State information (7.4) governs each Port's participation in the Bridged Local Area Network.

Frames are accepted for transmission and delivered on reception to and from Processes and Entities that model the operation of the MAC Relay Entity in a Bridge. These are:

- a) The Forwarding Process (7.7), which forwards received frames that are to be relayed to other Bridge Ports, filtering frames on the basis of information contained in the Filtering Database (7.9) and on the state of the Bridge Ports (7.4).
- b) The Learning Process (7.8), which by observing the source addresses of frames received on each Port, updates the Filtering Database (7.9), conditionally on the Port state (7.4).
- c) The Filtering Database (7.9), which holds filtering information and supports queries by the Forwarding Process as to whether frames with given values of the destination MAC Address field can be forwarded to a given Port.

Each Bridge Port also functions as an end station providing the MAC Service to LLC, which, in turn, supports operation of the Spanning Tree Protocol Entity (7.10) and of other possible users of LLC, such as protocols providing Bridge Management (7.11).

Each Bridge Port shall support the operation of LLC Type 1 procedures in order to support the operation of the Spanning Tree Protocol Entity. Bridge Ports may support other types of LLC procedures, which may be used by other protocols.

Figure 7-4 illustrates a single instance of frame relay between the Ports of a Bridge with two Ports.

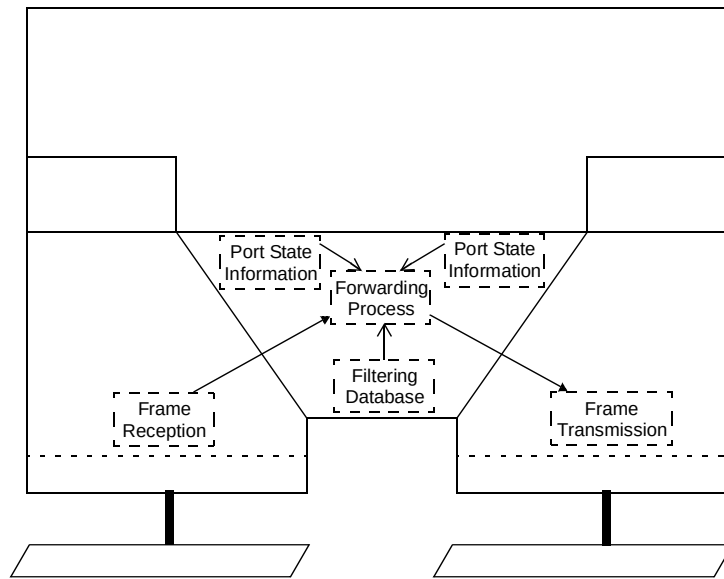


Figure 7-4—Relaying MAC frames

Figure 7-5 illustrates the inclusion of information carried by a single frame, received on one of the Ports of a Bridge with two Ports, in the Filtering Database.

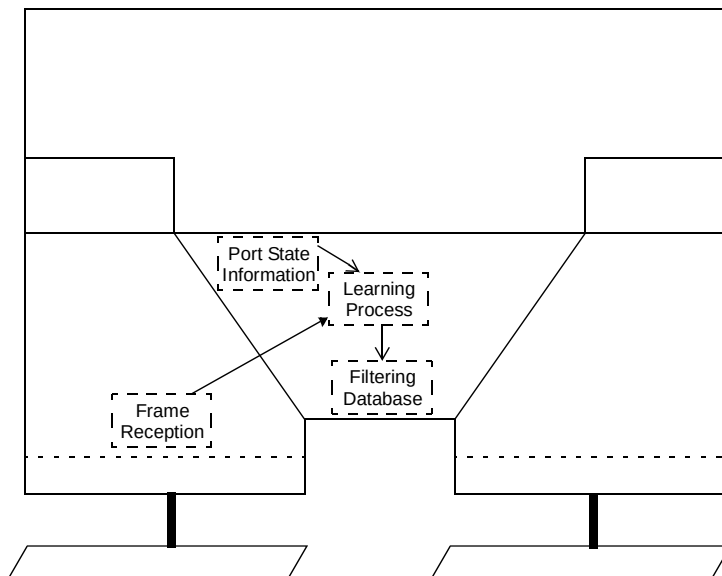


Figure 7-5—Observation of network traffic

Figure 7-6 illustrates the reception and transmission of Bridge Protocol Data Units by the Spanning Tree Protocol Entity.

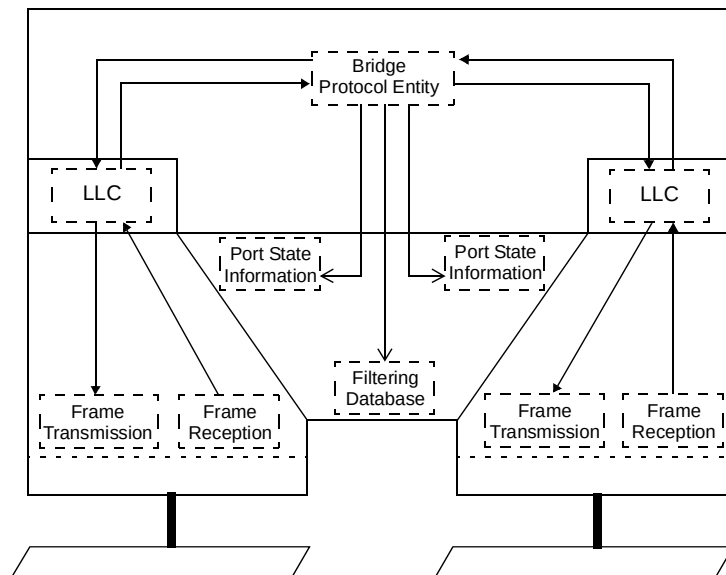


Figure 7-6—Operation of inter-bridge protocol

Figure 7-7 illustrates the reception and transmission of GARP Protocol Data Units by a GARP Entity (7.10).

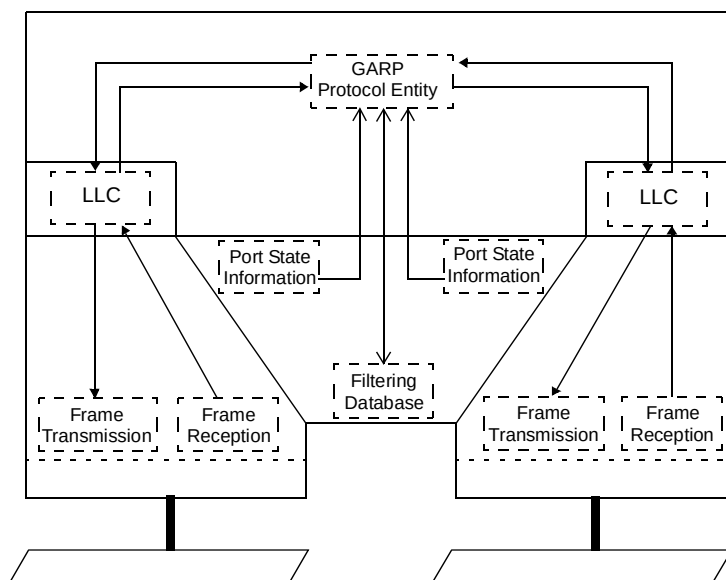


Figure 7-7—Operation of GARP

7.4 Port States and the active topology

Each Bridge Port has an operational Port State that governs whether or not it forwards MAC frames and whether or not it learns from their source addresses.

The *active topology* of a Bridged Local Area Network at any time is the set of communication paths formed by interconnecting the LANs and Bridges by the forwarding Ports. The function of the distributed Spanning Tree algorithm and the protocol (Clause 17) that operates that algorithm is to assign Port States to construct an active topology that is simply connected relative to the forwarding of frames between any given pair of MAC Addresses used to address end stations on the LANs. The *forwarding* and *learning* performed by each Bridge Port is dynamically managed to prevent temporary loops and reduce excessive traffic in the network while minimizing denial of service following any change in the *physical topology* of the network.

Any port that is not enabled, [i.e., has MAC_Operational (6.4.2) False or has been excluded from the active topology by management setting of the Administrative Bridge Port State to Disabled (14.8.2.2)] or has been dynamically excluded from forwarding and learning from MAC frames, is assigned the Port State *Discarding*. Any Port that has learning enabled but forwarding disabled has the Port State *Learning*, and a Port that both learns and forwards frames has the Port State *Forwarding*.

NOTE—The current IETF Bridge MIB (IETF RFC 1493) uses disabled, blocking, listening, learning, forwarding, and broken dot1dStpPortStates. The learning and forwarding states correspond exactly to the Learning and Forwarding Port States specified in this standard. Disabled, blocking, listening, and broken all correspond to the Discarding Port State — while those dot1dStpPortStates serve to distinguish reasons for discarding frames the operation of the Forwarding and Learning processes is the same for all of them. The dot1dStpPortState broken represents the failure or unavailability of the port's MAC as indicated by MAC_Operational FALSE; disabled represents exclusion of the port from the active topology by management setting of the Administrative Port State to Disabled; blocking represents exclusion of the port from the active topology by the spanning tree algorithm [computing an Alternate or Backup Port Role (17.7)]; listening represents a port that the spanning tree algorithm has selected to be part of the active topology (computing a Root Port or Designated Port role) but is temporarily discarding frames to guard against loops or incorrect learning.

Figure 7-6 illustrates the operation of the Spanning Tree Protocol Entity, which operates the Spanning Tree Algorithm and its related protocols, and its modification of Port state information as part of determining the active topology of the Bridged Local Area Network.

Figure 7-4 illustrates the Forwarding Process's use of Port state information: first, for a Port receiving a frame, in order to determine whether the received frame is to be relayed through any other Ports; and second, for another Port in order to determine whether the relayed frame is to be forwarded through that particular Port.

Figure 7-5 illustrates the use of the Port state information for a Port receiving a frame, by the Learning Process, in order to determine whether the station location information is to be incorporated in the Filtering Database.

7.5 Frame reception

The individual MAC Entity of each Bridge Port examines all frames transmitted on the attached LAN.

All error-free received frames give rise to M_UNITDATA indications that are handled as follows.

NOTE—A frame that is in error, as defined by the relevant MAC specification, is discarded by the MAC Entity without giving rise to any M_UNITDATA indication (see 6.4).

Frames with an M_UNITDATA.indication frame_type of user_data_frame (6.4), shall be submitted to the Learning and Forwarding Processes. Frames with other values of frame_type shall not be submitted to the Forwarding Process. They may be submitted to the Learning Process.

Frames with a frame_type of user_data_frame and addressed to the Bridge Port as an end station shall be submitted to LLC. Such frames carry either the individual MAC Address of the Port or a group address associated with the Port (7.12) in the destination address field. Frames submitted to LLC can also be submitted to the Learning and Forwarding Processes, as specified above.

Frames addressed to a Bridge Port as an end station, and relayed to that Bridge Port from other Bridge Ports in the same Bridge by the Forwarding Process, shall also be submitted to LLC. No other frames shall be submitted to LLC.

7.5.1 Regenerating user priority

The user_priority of each received frame is regenerated using the received user_priority and the User Priority Regeneration table for the reception Port. The table specifies the regenerated user_priority value for each of the eight possible values of user_priority (0 through 7) conveyed in received frames. Table 7-1 specifies defaults, these shall be used as the initial values of the entries of the table for each Port.

NOTE 1—IEEE 802 LAN technologies signal a maximum of 8 user_priority values. Annex G (informative) contains further explanation of the use of user_priority values and how they map to traffic classes.

The User Priority Regeneration Table may be modified by management, as described in Clause 14. If so management shall be able to set each of table entries for each reception Port and received user_priority independently, and to any of the values in the ranges specified in Table 7-1.

NOTE 2—The values chosen for the User Priority Regeneration table for a given Bridge Port should be consistent with the user priority to be associated with traffic received through that Port across the rest of the network, and should generate appropriate access priority values for each MAC. The user priority is used

- Via the traffic class table (7.7.3) to determine the traffic class for a given outbound Port, and
- Via fixed, MAC specific mappings (7.7.5) to determine the access priority.

Table 7-1 shows the default values for the regeneration of user priority. Table 7-2 shows the default values for the traffic class table, for all possible numbers of supported traffic classes. Table 7-4 shows the fixed mappings from user priority to access priority that are required for different outbound MAC methods.

Table 7-1—User Priority Regeneration

User Priority	Default Regenerated User Priority	Range
0	0	0–7
1	1	0–7
2	2	0–7
3	3	0–7
4	4	0–7
5	5	0–7
6	6	0–7
7	7	0–7

7.6 Frame transmission

The individual MAC Entity for each Bridge Port transmits frames submitted to it by the MAC Relay Entity.

Relayed frames are submitted for transmission by the Forwarding Process. The M_UNITDATA.request primitive associated with such frames conveys the values of the source and destination address fields received in the corresponding M_UNITDATA.indication primitive.

LLC Protocol Data Units are submitted by LLC as a user of the MAC Service provided by the Bridge Port. Frames transmitted to convey such Protocol Data Units carry the individual MAC Address of the Port in the source address field.

Each frame is transmitted subject to the MAC procedures to be observed for that specific IEEE 802 LAN technology. The frame_type of the corresponding M_UNITDATA.request shall be user_data_frame (6.5).

Frames transmitted following a request by the LLC user of the MAC Service provided by the Bridge Port shall also be submitted to the MAC Relay Entity.

7.7 The Forwarding Process

Frames submitted to the Forwarding Process after being received at any given Bridge Port (7.5) shall be forwarded through the other Bridge Ports subject to the constituent functions of the Forwarding Process. These functions enforce topology restrictions (7.7.1), use filtering database information to filter frames (7.7.2), queue frames (7.7.3), select queued frames for transmission (7.7.4), map priorities (7.7.5), and recalculate FCS, if required (7.7.6).

The Forwarding Process functions are described in 7.7.1–7.7.6 in terms of the action taken for a given frame received on a given Port (termed “the reception Port”). The frame can be forwarded for transmission on some Ports (termed “transmission Ports”), and is discarded without being transmitted at the other Ports.

NOTE—This description of the Forwarding Process is limited to the operation of the relay function of the MAC Bridge, and does not consider what can occur in real implementations once frames are passed to a MAC for transmission. In some MAC implementations, and under some traffic conditions, a degree of indeterminacy can be introduced between passing selected frames to the MAC for transmission and viewing the actual sequence of frames on the LAN medium. An example is the effect of different values for Token Holding Time in FDDI LANs. Such indeterminacy could result in apparent violation of the queuing/de-queueing and prioritization rules described. As a consequence, it is not possible to test conformance to the standard for some implementations simply by relating observed LAN traffic to the described model of the Forwarding Process; conformance tests have to allow for the (permissible) behavior of the MAC implementations as well.

Figure 7-4 illustrates the operation of the Forwarding Process in a single instance of frame relay between the Ports of a Bridge with two Ports. Figure 7-8 illustrates the detailed operation of the Forwarding Process.

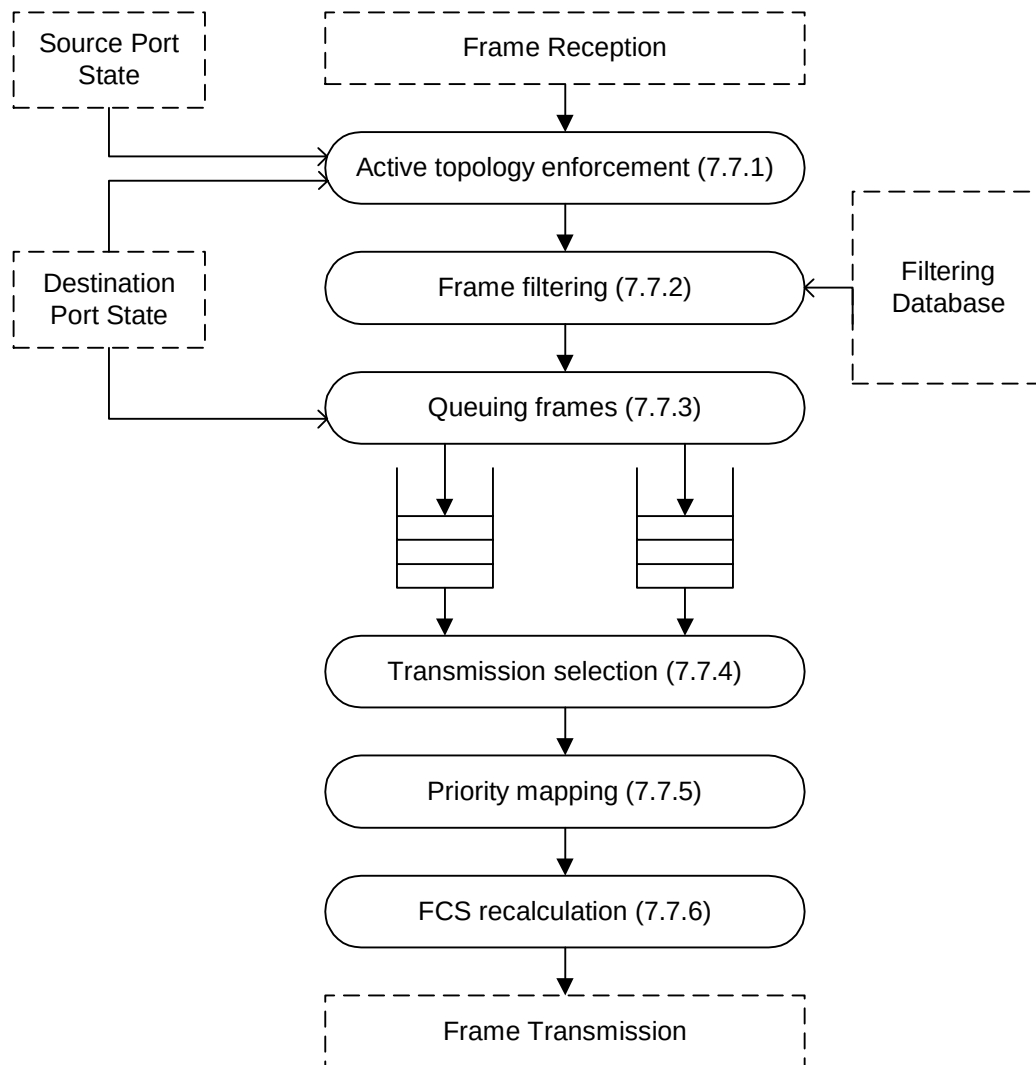


Figure 7-8—Operation of the Forwarding Process

7.7.1 Active topology enforcement

Each Port is selected as a potential transmission Port if, and only if

- The Port on which the frame was received was in the Forwarding State (7.4), and
- The Port considered for transmission is in the Forwarding State, and
- The Port considered for transmission is not the Port on which the frame was received, and
- The size of the `mac_service_data_unit` conveyed by the frame does not exceed the maximum size of `mac_service_data_unit` supported by the LAN attached to the Port considered for transmission.

For each Port not selected as a potential transmission Port, the frame shall be discarded.