IEEE Std 802.1t-2001
(Amendment to IEEE Std 802.1D, 1998 Edition)

IEEE Standard for Local and metropolitan area networks— Common specifications

Part 3: Media Access Control (MAC) Bridges— Amendment 1

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 17 March 2001

IEEE-SA Standards Board

Abstract: This amendment to IEEE Std 802.1D, 1998 Edition is intended to document maintenance items identified in the text of IEEE Std 802.1D, 1998 Edition (ISO/IEC 15802-3:1998). The document identifies any proposed changes to the text that have arisen as a consequence of maintenance activity. These are documented in the usual form for Amendments to IEEE 802® standards; i.e., as an explicit set of editing instructions that, if correctly applied to the text of ISO/IEC 15802-3:1998, will create a corrected document.
Keywords: local area networks, MAC Bridge management, MAC bridges, media access control (MAC) bridges, multicast address filtering, traffic class expediting

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

Print: ISBN 0-7381-2814-7 SH94915
PDF: ISBN 0-7381-2815-5 SS94915

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

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

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

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

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

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

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

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

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

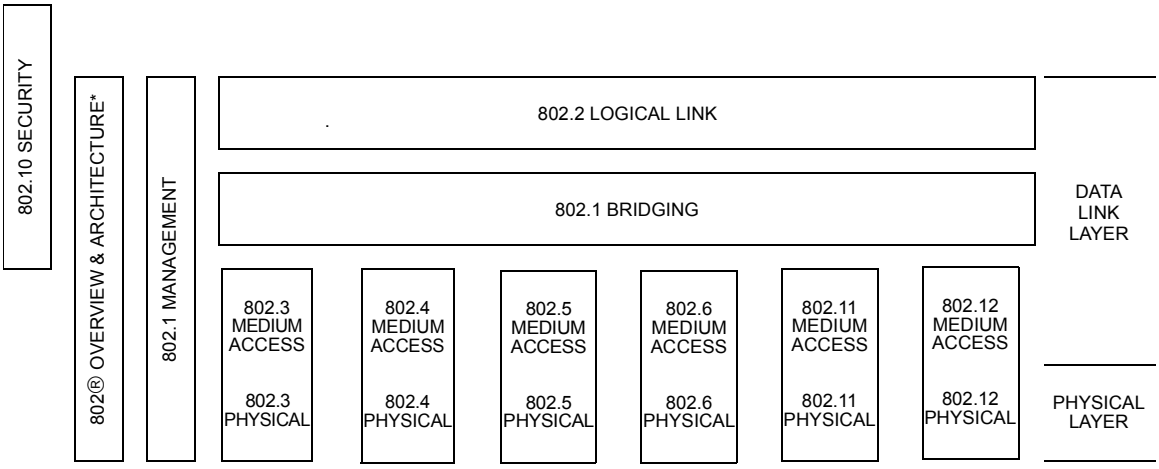
IEEE is the sole entity that may authorize the use of certification marks, trademarks, or other designations to indicate compliance with the materials set forth herein.

Introduction

[This introduction is not a part of IEEE Std 802.1t-2001, IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 3: Media Access Control (MAC) Bridges: Amendment 1.]

This amendment to IEEE 802.1D, 1998 Edition is intended to document maintenance items identified in the text of IEEE Std 802.1D, 1998 Edition (ISO/IEC 15802-3:1998). The document identifies any proposed changes to the text that have arisen as a consequence of maintenance activity. These are documented in the usual form for Amendments to IEEE 802® standards; i.e., as an explicit set of editing instructions that, if correctly applied to the text of ISO/IEC 15802-3:1998, will create a corrected document.

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



* Formerly IEEE Std 802.1A.

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

The standards defining the technologies noted above are as follows:

• IEEE Std 802[1]: *Overview and Architecture*. This standard provides an overview to the family of IEEE 802 Standards. This document forms part of the 802.1 scope of work.

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

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

• IEEE Std 802.16:	*Standard Air Interface for Fixed Broadband Wireless Access Systems*.
• IEEE Std 802.17:	*Resilient Packet Ring Access Method and Physical Layer Specifications.*

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

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

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

Conformance test methodology

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

Participants

When the IEEE 802.1 Working Group approved this standard, it had the following membership:

Tony Jeffree, *Chair and Editor*
Neil Jarvis, *Vice-Chair*
Mick Seaman, *Chair, Interworking Task Group*

Floyd Backes
Les Bell
Alan Chambers
Marc Cochran
Paul Congdon
Hesham El Bakoury
Norman W. Finn
Sharam Hakimi
Bob Hott
Toyayuki Kato
Hal Keen
Daniel Kelley
Keith Klamm
Bill Lidinsky
Yaron Nachman
Satoshi Obara
Luc Pariseau
Anil Rijsinghani
John J. Roese
Ted Schroeder
Benjamin Schultz
Rosemary V. Slager
Andrew Smith
Michel Soerensen
Robin Tasker
Manoj Wadekar
Robert Williams

The following members of the balloting committee voted on this standard:

Jacob Ben Ary
James T. Carlo
Keith Chow
Guru Dutt Dhingra
Thomas J. Dineen
Christos Douligeris
Sourav K. Dutta
Philip H. Enslow
Changxin Fan
John W. Fendrich
Richard A. Froke
Robert J. Gagliano
Gautam Garai
Alireza Ghazizahedi
Tim Godfrey
Robert M. Grow
Chris G. Guy
Simon Harrison
Raj Jain
Kamran Jamal
Neil A. Jarvis
Anthony A. Jeffree
Stuart J. Kerry
Daniel R. Krent
Stephen Barton Kruger
David J. Law
William Lidinsky
Randolph S. Little
Peter Martini
Bennett Meyer
David S. Millman
John E. Montague
Robert Mortonson
Robert O'Hara
Satoshi Obara
Roger Pandanda
Vikram Punj
Gary S. Robinson
Edouard Y. Rocher
James W. Romlein
Floyd E. Ross
Jaideep Roy
Rich Seifert
Leo Sintonen
Joseph S. Skorupa
Fred J. Strauss
Jonathan R. Thatcher
Mark-Rene Uchida
Scott A. Valcourt
John Viaplana
Paul A. Willis
Oren Yuen

When the IEEE-SA Standards Board approved this standard on 17 March 2001, it had the following membership:

Donald N. Heirman, *Chair*

James T. Carlo, *Vice Chair*

Judith Gorman, *Secretary*

Chuck Adams
Mark D. Bowman
Clyde R. Camp
Richard DeBlasio
Harold E. Epstein
H. Landis Floyd
Jay Forster*
Howard M. Frazier
James H. Gurney
Raymond Hapeman
Richard J. Holleman
Richard H. Hulett
Lowell G. Johnson
Joseph L. Koepfinger*
Peter H. Lips
Paul J. Menchini
Daleep C. Mohla
Robert F. Munzner
Ronald C. Petersen
Malcolm V. Thaden
Geoffrey O. Thompson
Akio Tojo
Howard L. Wolfman

*Member Emeritus

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

Satish K. Aggarwal, *NRC Representative*

Alan H. Cookson, *NIST Representative*

Donald R. Volzka, *TAB Representative*

Jennifer McClain Longman

IEEE Standards Project Editor

Contents

IEEE Standard for
Local and metropolitan area networks—
Common specifications

Part 3: Media Access Control (MAC) Bridges—Amendment 1

EDITORIAL NOTE—This amendment to IEEE Std 802.1D, 1998 Edition (ISO/IEC 15802-3:1998) defines the changes necessary in order to address maintenance items that have been brought to the attention of the 802.1 Working Group. These changes are defined as a series of additions to, and modifications of, the existing text of ISO/IEC 15802-3:1998; this supplement therefore assumes all material, including references, abbreviations, definitions, procedures, services and protocols defined in the base text. Text shown in ***bold italics*** in this amendment defines the editing instructions necessary in order to incorporate the modifications and additions into the base text. Three editing instructions are used: ***change, delete,*** and ***insert***. ***Change*** is used to make a change to existing material. The editing instruction specifies the location of the change and describes what is being changed either by using ~~strikethrough~~ to remove old material or underscore to add new material. ***Delete*** removes existing material. ***Insert*** adds new material without changing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. Editorial notes will not be carried over into future editions of IEEE Std 802.1D.

1. Overview

1.1 Introduction

Insert item d), and change the NOTE, as follows:

d) Validation of access to the LAN.

NOTE 1—Scope, definitions, references, and conformance requirements relating to the operation of Source Routing Transparent Bridge operation can be found in Annex C.1.

NOTE 2—Validation of access to the LAN is supported when this standard is used in conjunction with the Port-based access control mechanisms specified in P802.1X.

1.2 Scope

Remove existing item h). Insert additional items g) and h) as shown below, in sequence following item f), and renumber the remaining items:

g) Establishes the requirements for a protocol between Bridges in a Bridged LAN 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).

h) Specifies the encoding of GMRP protocol data units.

2. References

Change all ISO [IEEE] and ISO/IEC [IEEE] references in Clause 2 so that the primary reference for these standards is the IEEE standard number and name, with the ISO standard number retained in parentheses. Change all references to these standards throughout the remaining clauses and subclauses accordingly, so that the IEEE standard number is cited.

Delete the reference to ISO/IEC 15802-2.

Insert a reference to RFC 2233 as follows:

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

Insert a reference to RFC 2674 as follows:

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.

Change the reference to IGMP, delete footnote 5, renumbering subsequent footnotes, update existing footnote 6 (new footnote 5) to give the current RFC website address and apply new footnote 5 to this IGMP reference, as follows:

~~IETF INTERNET-DRAFT, Fenner, Internet Group Management Protocol (IGMP), Version 2, January 20th 1975~~

IETF RFC 2236, Fenner, Internet Group Management Protocol (IGMP), Version 2, November 1975

[5]IETF RFCs are available from the Internet Engineering Task Force website at http://www.ietf.org/rfc.html.

Change the wording of footnote 3 as follows:

[3]IEEE 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.

Change the wording of existing footnote 8 as follows:

[8]ISO [IEEE] and ISO/IEC [IEEE] documents are available from ISO Central Secretariat, 1 rue de Varembé, 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.

Insert a reference to 802.1Q, as follows:

IEEE Std 802.1Q-1998, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.

Insert a reference to P802.1X as follows:

IEEE P802.1X (Draft 11, March 2001) Local and Metropolitan Area Networks—Port Based Network Access Control.

Insert a reference to IEEE Std 802.3, 2000 Edition, as follows:

IEEE Std 802.3, 2000 Edition, IEEE Standards 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.

4. Abbreviations

Insert the following abbreviations:

kG/s	Kilobit per second
MG/s	Megabit per second
TG/s	Terabit per second

5. Conformance

5.2 Options

Insert the following as items n) and o):

n) Support the ability to configure the value of the Restricted_Group_Registration parameter (10.3.2.3) for each Port of the Bridge.

o) Support the use of the adminEdgePort and operEdgePort parameters (14.8.2), and the operation of the Bridge Detection State Machine (18.2), on one or more Ports.

6. Support of the MAC Service

6.1 Support of the MAC Service

Insert the following paragraph and Note at the end of 6.1:

The operation of MAC Bridges supports the provision of the MAC Service only to devices that are authenticated and authorized for such use. Unauthorized devices may be denied access to the Bridged LAN, other than as necessary to support the protocol exchanges that are required by any authentication process that is supported.

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 P802.1X.

Change the following subclauses of 6.3 as indicated:

6.3 Quality of service maintenance

6.3.1 Service availability

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

The service availability can be increased by automatic reconfiguration of the Bridged LAN in order to avoid the use of a failed component (e.g., repeater, cable, or connector) in the data path. The service availability can be lowered by failure of a Bridge itself, through denial of service by the Bridge, or through frame filtering by the Bridge.

A Bridge may deny service and discard frames (6.3.2) in order to preserve other aspects of the MAC Service (6.3.3 and 6.3.4) when automatic reconfiguration takes place. Service may be denied to end stations that do not benefit from the reconfiguration; hence, the service availability is lowered for those end stations. Bridges may filter frames in order to localize traffic in the Bridged LAN. Should an end station move, it may then be unable to receive frames from other end stations until the filtering information held by the Bridges is updated.

A Bridge may deny service and discard frames in order to prevent access to the network by devices that are not authorized for such access.

To maximize the service availability, no loss of service or delay in service provision should be caused by Bridges, except as a consequence of a failure, removal, or insertion of a Bridged LAN 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 LAN, and is independent of individual instances of service provision.

NOTE—This is true only in circumstances where admission control mechanisms are not present, i.e., where the Bridges provide a “best effort” service. The specification and applicability of admission control mechanisms 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

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, hence, must 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 connected topology of the Bridged LAN necessitate frame discard for a limited period of time to maintain other aspects of Quality of Service.

   5) The device attached to the Port is not authorized for access to the network.

6.3.9 Priority

In Note 2 and in the footnote at the bottom of the page, the footnote number is incorrect, as footnote number 8 has already been used on page 4. Change “8” to “9” in the reference and the footnote.

6.4 Internal Sublayer Service provided within the MAC Bridge

Change 6.4 as indicated, splitting the existing text into a new subclause 6.4.1 and adding subclause 6.4.2:

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 the attached end station, these additional elements can be 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. Three 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, MAC_action, 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,
mac_action,
destination_address,
source_address,
mac_service_data_unit,
user_ priority,
frame_check_sequence
)

Each ~~M_UNITDATA_indication~~M_UNITDATA.indication primitive corresponds to the receipt of an error-free MAC frame from an individual 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 **mac_action** parameter indicates the action requested of a MAC entity receiving the indication. If the value of the frame_type parameter is user_data_frame, then the mac_action parameter is one of request_with_response, request_with_no_response, or response. For mac_specific_frames and reserved_frames, this parameter does not apply.

The **destination_address** parameter is either 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 1—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 H.2 for further explanation of the use of user_priority values and how they map to traffic classes.

Bridges have the capability to regenerate user priority from the user priority information contained in the data indication and the User Priority Regeneration Table for the reception Port, as specified in 7.5.1. The user_priority parameter takes the value of the Regenerated user_priority. In the case of IEEE 802 LAN MAC types that are not able to signal priority, the user_priority parameter takes the value of the Default User Priority for the Port on which the indication was received. The default value of Default User Priority is 0 for all Ports of the Bridge; the value for a given Port may be modified by means of the management functionality described in Clause 14 if such management functionality is supported.

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,
                        mac_ action,
                        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 **mac_action** parameter indicates the action requested of the destination MAC entity.

The **destination_address** parameter is either 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 2—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 H.2 for further explanation of the use of user_priority values and how they map to traffic classes.

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 described, the Internal Sublayer Service provided by a MAC entity to the MAC Relay Entity within a Bridge 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. These parameters are defined as follows:

MAC_Enabled: The value of this parameter is TRUE if the MAC entity is permitted to be used; its value 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 is capable of being 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—The intent here is to allow a common approach across MACs for handling the fact that:

a) A MAC can inherently be working or not (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).

6.5 Support of the Internal Sublayer Service by specific MAC procedures

Change 6.5.1 as indicated.

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 explicitly encoded in MAC frames.

The **mac_action** parameter takes only the value request_with_no_response and is not explicitly encoded in MAC frames.

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

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

The number of octets of data in the **mac_service_data_unit** parameter is ~~encoded in the length field of the MAC frame (IEEE Std 802.3, 3.2.6), and the octets of data are encoded in the data field (IEEE Std 802.3, 3.2.7).~~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 takes the value of the Default User Priority parameter for the Port through which the MAC frame was received (see 6.4).

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 IEEE Std 802.3, 3.2.8.

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 G).

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 802.3 MAC. ISO/IEC 11802-5 defines the recommended practice for bridging Ethernet V2.0 frames.

~~NOTE 3—IEEE Std 802.3, 1998 Edition, describes the use of either a Length or an Ethernet protocol type in its frame format; however, the text of this subclause has yet to be revised to describe the use of Ethernet protocol types.~~

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, 2000 Edition), and the value of MAC_Operational is directly determined by the value of the aAggOperState attribute (30.7.1.13 in 802.3).

b) Otherwise, for 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.

Change 6.5.3 as indicated.

6.5.3 Support by ISO/IEC 8802-5 (token-passing ring)

The token-passing ring access method is specified in ISO/IEC 8802-5. 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 enqueuing 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 (ISO/IEC 8802-5, 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 below.

The **frame_type** parameter is encoded in the frame_type bits (FF bits) of the frame control field (ISO/IEC 8802-5, 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 **mac_action** parameter only takes the value request_with_no_response and is not explicitly encoded in MAC frames.

The **destination_address** parameter is encoded in the destination address field of the MAC frame (ISO/IEC 8802-5, 3.2.4.1).

The **source_address** parameter is encoded in the source address field of the MAC frame (ISO/IEC 8802-5, 3.2.4.2).

The **mac_service_data_unit** parameter is encoded in the information field (ISO/IEC 8802-5, 3.2.6).

The **user_priority** parameter associated with user_data_frames is encoded in the YYY bits of the frame control field (ISO/IEC 8802-5, 3.2.3).

The **frame_check_sequence** parameter is encoded in the FCS field of the MAC frame (ISO/IEC 8802-5, 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 ISO/IEC 8802-5, 3.2.7.

The Address Recognized (A) bits in the Frame Status field of a frame ISO/IEC 8802-5, 3.2.9) may be set to 1 if an ~~M_UNITDATA~~M_UNITDATA.indication primitive with frame_type and mac_action parameter values of user_data_frame and request_with_no_response respectively 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 ISO/IEC 8802-5.

If the A bits are set to 1, the Frame Copied (C) bits (ISO/IEC 8802-5, 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 ISO/IEC 8802-5:1998/Amd. 1).

   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 ISO/IEC 8802-5:1998/Amd. 1).

b) For all other 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 ISO/IEC 8802-5:1998).

   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 ISO/IEC 8802-5:1998).

7. Principles of operation

7.1 Bridge operation

7.1.1 Relay

Insert new items e), f), and m), renumbering old items e) through n), as shown:

A MAC Bridge relays individual MAC user data frames between the separate MACs of the Bridged LANs connected to its Ports. The order of frames shall be preserved as defined in 7.7.3.

The functions that support the relaying of frames and maintain the Quality of Service supported by the Bridge are

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, or if its mac_action parameter is not request_with_no_response (6.4).

d) Regeneration of user priority, if required (6.4).

e) Frame discard in order to suppress loops in the physical topology of the Bridged LAN.

f) Frame discard on reception at Ports that are in the Disabled Port State (8.4.5).

g) ~~e)~~ Frame discard following the application of filtering information.

h) ~~f)~~ Frame discard on transmittable service data unit size exceeded (6.3.8).

i) ~~g)~~ Forwarding of received frames to other Bridge Ports.

j) ~~h)~~ Selection of traffic class, following the application of filtering information.

k) ~~i)~~ Queuing of frames by traffic class.

l) ~~j)~~ Frame discard to ensure that a maximum bridge transit delay is not exceeded (6.3.6).

m) Frame discard to ensure that frames are not relayed to Ports that are in the Disabled Port State (8.4.5).

n) ~~k)~~ Selection of queued frames for transmission.

o) ~~l)~~ Selection of outbound access priority (6.3.9).

p) ~~m)~~ Mapping of service data units and recalculation of Frame Check Sequence, if required (6.3.7, 7.7.6).

q) ~~n)~~ Frame transmission.

7.1.2 Filtering and relaying information

Insert the following text after item a), renumbering items b) through g) accordingly:

A Bridge also filters frames in order to allow frames received on Ports that are in the Disabled Port State (8.4.5) to be discarded, and to prevent frames received on Ports that are in the Disabled Port State from being relayed to other Ports. The function that supports the use and maintenance of information for this purpose is:

b) Status and administrative control information associated with the Port and its associated MAC.

7.2 Bridge architecture

7.2.1 Architectural model of a Bridge

Insert the following text, adding it to the end of the first paragraph of 7.2.1:

The term "LLC Entities," used in Figures 7-3 and 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.

7.4 Port State, Active Ports and the Active Topology

Change the first paragraph as shown:

State information associated with each Bridge Port governs whether or not it participates in relaying MAC frames. A Port can be placed in the *Disabled* Port State (8.4.5) ~~by management~~, in which case it plays no part in the operation of the Bridged LAN; frames received on a Port that is in the Disabled Port State are not relayed to other Ports, and frames are not relayed to Ports that are in the Disabled Port State. ~~a~~. A Port that is not disabled can be dynamically excluded from participation in frame relaying by operation of the Spanning Tree algorithm. If neither of these applies to a Port, it is described as *forwarding*.

7.9 The Filtering Database

Change the third paragraph after item d), as shown:

Two entry types are used to represent dynamic filtering information. Dynamic Filtering Entries are used to specify the Ports on which individual MAC Addresses have been learned. They are created and updated by the Learning Process (7.8), and are subject to ageing and removal by the Filtering Database. Group Registration Entries support the registration of group MAC Addresses. They are created, updated, and removed by the GMRP protocol in support of Extended Filtering Services (6.6.5, 7.9.3, and Clause 10), subject to the state of the *Restricted_Group_Registration* management control (10.3.2.3). If the value of this control is TRUE, then the creation of a Group Registration Entry is not permitted unless a Static Filtering Entry exists that permits dynamic registration for the Group concerned. Dynamic filtering information may be read by use of the remote management capability provided by Bridge Management (7.11) using the operations specified in Clause 14.

7.9.3 Group Registration Entries

Insert the following text at the end of 7.9.3:

The creation of Group Registration Entries is subject to the Restricted_Group_Registration management control (10.3.2.3). If the value of this control is TRUE, a dynamic entry for a given Group may only be created if a Static Filtering Entry already exists for that Group, in which the Registrar Administrative Control value is Normal Registration.

7.9.6 Permanent Database

Insert a second Note at the end of this subclause, and renumber the existing Note, as follows:

NOTE 1—This aspect of the Permanent Database can be viewed as providing a “boot image” for the Filtering Database, defining the contents of all initial entries, before any dynamic filtering information is added.

NOTE 2—10.3.2.3 defines an initial state for the contents of the Permanent Database, required for the purposes of GMRP operation.

7.11 Bridge management

Remove the second paragraph, as follows:

~~Clause 15 specifies the protocol operations, identifiers, and values to be used in realizing these management operations through the use of ISO/IEC 15802-2.~~

7.12 Addressing

Change Table 7-9 as follows:

Table 7-9—Reserved addresses

Assignment	Value
Bridge Group Address	01-80-C2-00-00-00
IEEE Std. 802.3x Full Duplex PAUSE operation	01-80-C2-00-00-01
~~Reserved for future standardization~~ IEEE Std 802.3ad Slow_Protocols_Multicast address	01-80-C2-00-00-02
~~Reserved for future standardization~~ IEEE P802.1X PAE address	01-80-C2-00-00-03
Reserved for future standardization	01-80-C2-00-00-04
Reserved for future standardization	01-80-C2-00-00-05
Reserved for future standardization	01-80-C2-00-00-06
Reserved for future standardization	01-80-C2-00-00-07
Reserved for future standardization	01-80-C2-00-00-08
Reserved for future standardization	01-80-C2-00-00-09
Reserved for future standardization	01-80-C2-00-00-0A
Reserved for future standardization	01-80-C2-00-00-0B
Reserved for future standardization	01-80-C2-00-00-0C
Reserved for future standardization	01-80-C2-00-00-0D
Reserved for future standardization	01-80-C2-00-00-0E
Reserved for future standardization	01-80-C2-00-00-0F

7.12.7 Points of attachment and connectivity for Higher Layer Entities

Change the initial paragraphs, up to and including the paragraph preceding the NOTE, as follows:

Higher Layer Entities, such as the Bridge Protocol Entity and GARP Protocol Entity (7.10), and Bridge Management (7.11), are modeled as being connected directly to the Bridged LAN via one or more points of attachment. From the point of view of their attachment to the Bridged LAN, Higher Layer Entities associated with a Bridge can be regarded as if they are distinct end stations, directly connected to one or more of the LAN segments served by the Bridge Ports, in the same way as any other end station is connected to the Bridged LAN. In practice, the Higher Layer Entities will, in many cases, share the same physical points of attachment used by the relay function of the Bridge, as stated in 7.12; however, from the point of view of the transmission and reception of frames by these functions, the behavior is the same as if they were contained in logically separate end stations with points of attachment "outside" the Port(s) with which they are associated. Figure 7-9 is functionally equivalent to Figure 7-3, but illustrates this logical separation between the points of attachment used by the Higher Layer Entities and points of attachment used by the MAC Relay Entity. Although this logical separation exists, some types of Higher Layer Entity may take notice of the operational status of a Bridge Port with respect to its enabled/disabled states (7.4). For example, BPDUs are never transmitted or received on Ports that are Disabled. The manner in which a given type of Higher Layer Entity makes use of this Port state information is part of the definition of the operation of that entity type.

Higher Layer Entities fall into ~~two~~the following distinct categories:

a) Those entities, such as the Bridge Management Entity, that require only a single point of attachment to the Bridged LAN;

b) Those entities, such as Bridge Protocol Entities and GARP Participants, that require a point of attachment per Port of the Bridge;

c) Those entities that require a point of attachment per Port of the Bridge for some purposes, and only a single point of attachment for other purposes.

The fundamental distinction between ~~these~~ the first two categories is that for ~~the latter~~ type b) entities, it is essential for the operation of the entity concerned that it is able to associate received frames with the LAN segment on which those frames were originally seen by the Bridge, and that it is able to transmit frames to peer entities that are connected directly to that LAN segment. It is therefore essential that

d) It does not receive frames via a point of attachment associated with one Port that have been relayed by the Bridge from other Ports; and

e) Frames that it transmits via ~~one point of attachment~~ a point of attachment associated with one Port are not relayed by the Bridge to any other Ports.

For this reason, the MAC Addresses used to reach entities of this type are permanently configured in the Filtering Database in order to prevent the Bridge from relaying such frames received via any Port to any other Port of the Bridge, as defined in 7.12.3 and 7.12.6. Similarly, for entities of type c), the MAC Addresses used in protocol exchanges that require a point of attachment per Port are configured in the Permanent Database.

Change the paragraph following the NOTE as follows:

The MAC Relay Entity ~~Bridge~~ forwards a frame received on one Port through the other Port(s) of the Bridge, subject to the following control information permitting such forwarding to take place:

Insert the following text, Figure 7-15, Figure 7-16, and NOTE, at the end of 7.12.7:

Figure 7-15 illustrates the effect of setting the Port State to enabled or disabled, with respect to the ability of Higher Layer Entities to make use of that Port for the transmission and reception of frames. The example shows that Port A's Bridge Port State has been administratively disabled (see 14.8.2.2, Force Port state); the MAC entity is physically capable of transmitting and receiving frames (i.e., MAC_Operational = TRUE, see 6.4.2), but the administrative action has forced the Bridge Port's operational state to disabled. Higher Layer Entities A and B are both able to transmit and receive frames using the MAC entity associated with the Port. However, if Higher Layer Entity B is defined such that it takes notice of the Port State (for example, a Bridge Protocol Entity), it would not use Port A's MAC entity for transmission or reception of frames while the Bridge Port is disabled. Higher Layer Entities A and B are not reachable from Port B via the relay function of the Bridge, as Bridge Port A is not in a forwarding state. Should MAC_Operational become FALSE, the Port's operational state will be Disabled, even if the Port is administratively enabled.

The functions of the Port Access Entity (PAE, see P802.1X) that are concerned with the exchange of EAPOL PDUs provide an example of Higher Layer Entity A; the Bridge Protocol Entity provides an example of Higher Layer Entity B.

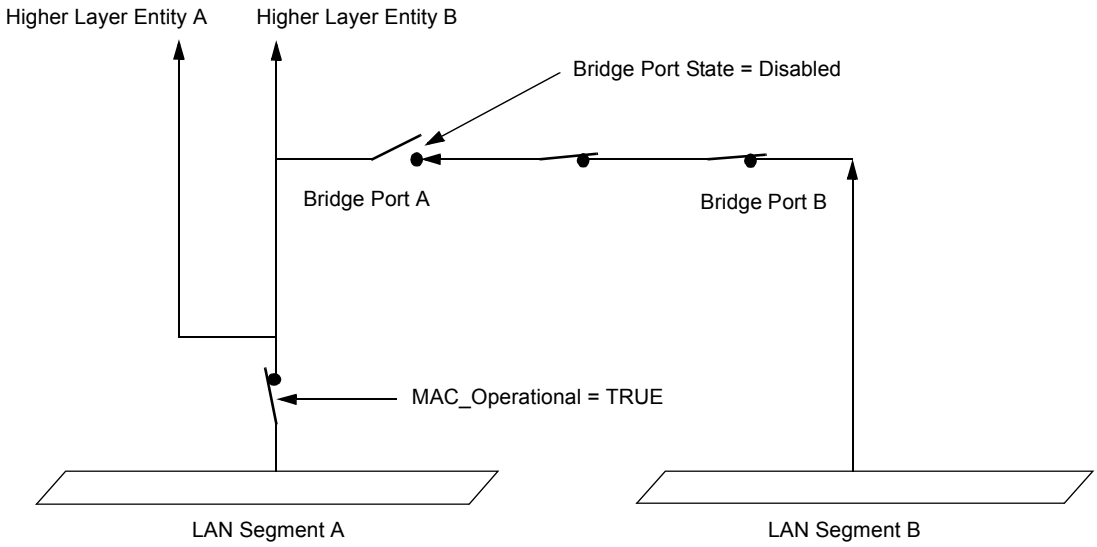


Figure 7-15—Effect of Port State

Figure 7-16 illustrates the effect of authorization, with respect to the ability of Higher Layer Entities to make use of that Port for the transmission and reception of frames. The example shows that Port A has not been authorized; the MAC entity is physically capable of transmitting and receiving frames (i.e., MAC_Operational = TRUE, see 6.4.2), but the fact that the Port has not been authorized (either as a result of administrative action, or as a result of an authentication failure) has forced the Port's operational state to be disabled. Higher Layer Entity A, because it is defined not to take notice of either the Port State or the authorization state, is still able to transmit and receive frames using the MAC entity associated with the Port. However, Higher Layer Entity B is defined such that it takes notice of the authorization state, and is therefore not able to use Port A's MAC entity for transmission or reception of frames. Higher Layer Entities A and B are not reachable from Bridge Port B via the relay function of the Bridge, as Bridge Port A is not in a forwarding state.

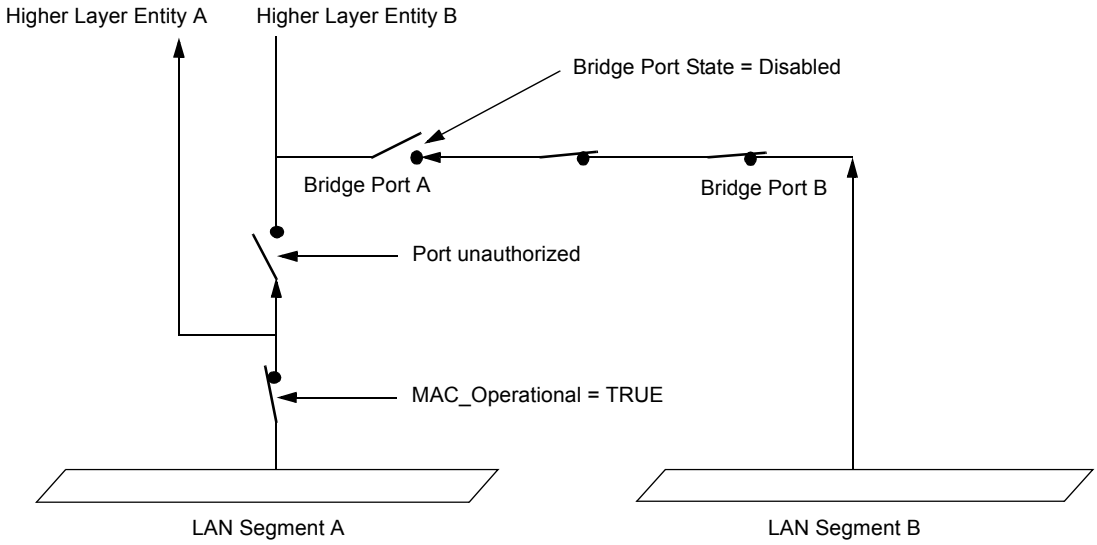


Figure 7-16—Effect of authorization

NOTE—The administrative and operational state values associated with the MAC, the Port's authorization state, and the Port State, equate to the ifAdminStatus and ifOperStatus parameters associated with the corresponding interface definitions; see IETF RFC 2233.

8. The spanning tree algorithm and protocol

8.1 Requirements to be met by the algorithm

Change items c) and f) as shown:

c) The ~~entire~~ active topology ~~will stabilize in any sized Bridged LAN. It~~ will, with a high probability, stabilize within a short, known bounded interval in order to minimize the time for which the service is unavailable for communication between any pair of end stations (6.1).

f) The communications bandwidth consumed by the Bridges in establishing and maintaining ~~the~~ a spanning tree on any particular LAN will be a small percentage of the total available bandwidth and independent of the total traffic supported by the Bridged LAN regardless of the total number of Bridges or LANs (6.3.10).

8.3 Overview

8.3.1 The active topology and its computation

Replace Figure 8-1 with the corrected version shown:

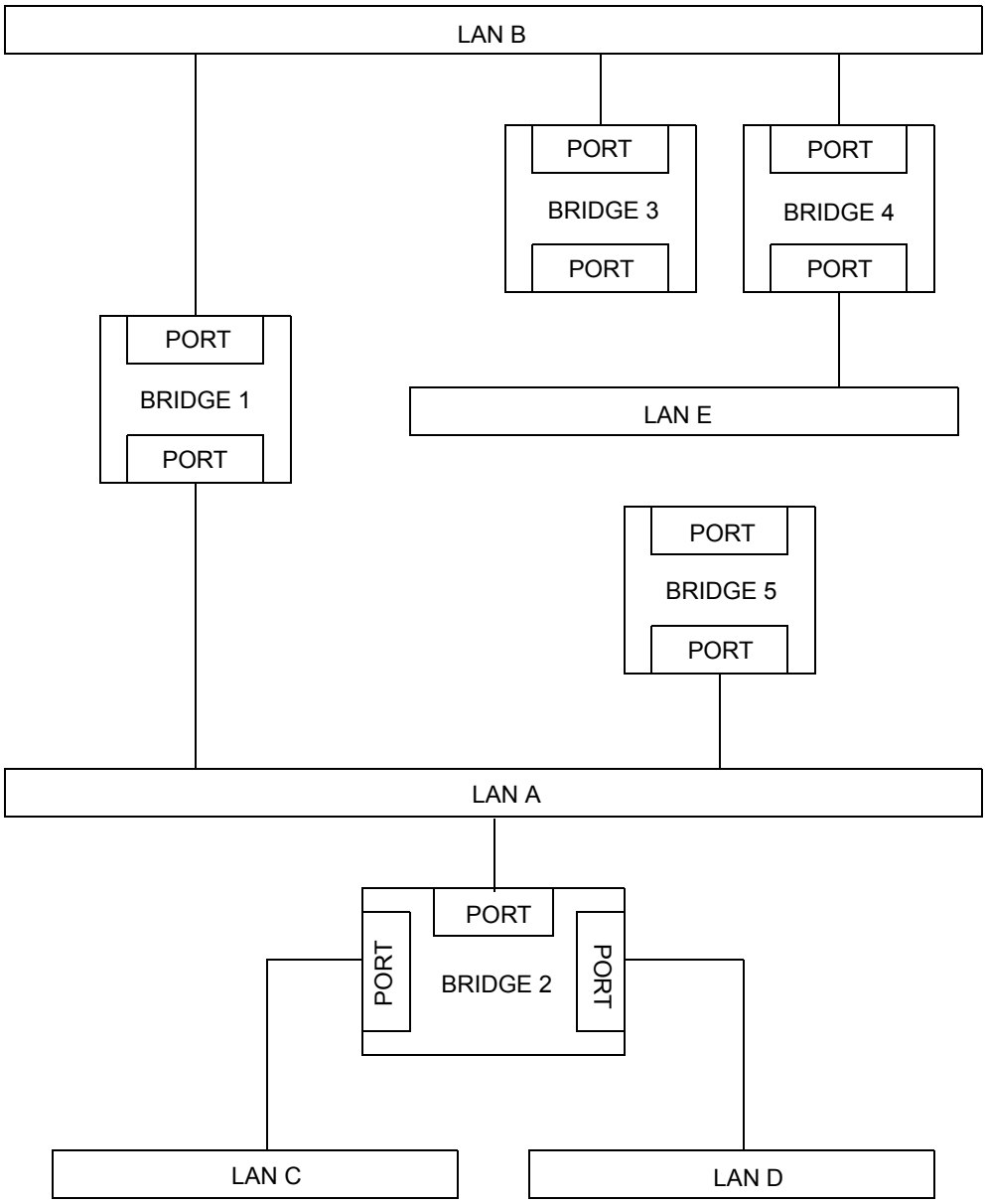


Figure 8-1—Active topology

8.4 Port States

8.4.5 Disabled

Change the last two sentences of 8.4.5 as follows:

This State is entered from any other State ~~by the operation of management~~ as a result of the Port becoming inoperable. A Port is inoperable if any of the following conditions are true:

a) The value of the MAC_Enabled parameter associated with the Port's MAC is False; or

b) The value of the MAC_Operational parameter associated with the Port's MAC is False; or

c) The Port has been disabled as a result of administrative or management action.

NOTE—For a Port on which Port-based access control (as specified in P802.1X) is in operation, case c) includes the possibility of the Port being disabled due to authorization failure. It is possible for the MAC_Operational and MAC_Enabled parameters both to be TRUE (i.e., the MAC is working and usable) but for the Port State to be nonetheless Disabled, as a result of management action or authorization failure.

This State is left, and the Blocking State is entered, when the Port ~~is enabled by management action, and the Blocking State is entered~~ becomes operable.

8.10 Performance

8.10.2 Parameter values

Change the third paragraph, as follows:

If the values of Bridge Hello Time, Bridge Max Age, and Bridge Forward Delay can be set by management, the Bridge shall have the capability to use the full range of values in the parameter ranges specified in Table 8-3, with a ~~granularity~~resolution of ~~1 s~~ *r* seconds, where $0 < r <= 1$.

Change the list of relationships that a Bridge shall enforce, as follows:

A Bridge shall enforce the following relationships:

$2 \times (Bridge\_Forward\_Delay - 1.0\ seconds) >= Bridge\_Max\_Age$

$Bridge\_Max\_Age >= 2 \times (Bridge\_Hello\_Time + 1.0\ seconds)$

$Bridge\_Hello\_Time > Hold\_Time$

Change the paragraph that discusses Path Cost, as follows:

It is recommended that default values of the **Path Cost** parameter for each Bridge Port be based on the values shown in Table 8-5, the values being chosen according to the speed of the LAN segment to which each Port is attached.

Where intermediate link speeds are created as a result of the aggregation of two or more links of the same speed (see Clause 43 in IEEE Std 802.3, 2000 Edition), it may be appropriate to modify the recommended values shown in Table 8-5 to reflect the change in link speed. However, as the primary purpose of the Path Cost is to establish the active topology of the network, it may be inappropriate for the Path Cost to track the effective speed of such links too closely, as the resultant active topology may differ from that intended by the network administrator. For example, if the network administrator had chosen an active topology that makes use of aggregated links for resilience (rather than for increased data rate), it would be inappropriate to cause a Spanning Tree topology change as a result of one of the physical links in an aggregation failing. Similarly, with links that can autonegotiate their data rate, reflecting such changes of data rate in changes to Path Cost may not be appropriate, depending upon the intent of the network administrator. Hence, as a default behavior, such dynamic changes of data rate shall not automatically cause changes in Path Cost for the Port concerned.

Change the definition of Hold Time in Table 8-3, as follows:

Table 8-3—Spanning tree algorithm timer values

Parameter	Recommended or default value	Fixed value	Range
Bridge Hello Time	2.0	—	1.0–10.0
Bridge Max Age	20.0	—	6.0–40.0
Bridge Forward Delay	15.0	—	4.0–30.0
Hold Time	—	~~1.0~~Not more than 3 BPDUs transmitted in any 2 second interval	—

All times are in seconds.
— Not applicable.
Subclause 8.10.2 constrains the relationship between Bridge Max Age and Bridge Forward Delay.

Change the contents of Table 8-4, and the paragraph that precedes it, as follows:

Table 8-4—Bridge and port priority parameter values

Parameter	Recommended or default value	Range
Bridge Priority	32 768	0–61 440 in steps of 4096
Port Priority	128	0–240 in steps of 16

If the values of the **Bridge Priority** and the **Port Priority** for each of the Ports can be set by management, the Bridge shall have the capability to use the full range of values in the parameter ranges specified in Table 8-4, with a granularity of ~~1~~ 4096 for Bridge Priority and a granularity of 16 for Port Priority.

NOTE—The stated ranges and granularities for Bridge Priority and Port Priority differ from the equivalent text and table in IEEE Std 802.1D, 1998 Edition and earlier versions of this standard. The rationale for these changes can be found in 9.2.5 and 9.2.7. Expressing these value ranges in steps of 4096 and 16, respectively, (rather than as 4-bit values with a range of 0 to 15) allows these parameters to be managed consistently across old and new implementations of this standard; the step values chosen ensure that the low-order bits that have been re-assigned cannot be modified, but that the magnitude of the priority values can be directly compared with those based on previous versions of the standard.

Delete the penultimate paragraph as follows:

~~A Bridge shall not use a lower value for the Path Cost parameter associated with any Port than the absolute minimum value specified in 8-5.~~

Replace the existing Table 8-5 as shown below:

Table 8-5—Path Cost Parameter Values

Parameter	Link Speed	Recommended value	Recommended range	Range
Path Cost	<=100 kb/s	200 000 000*	20 000 000–200 000 000	1–200 000 000
Path Cost	1 Mb/s	20 000 000*	2 000 000–200 000 000	1–200 000 000
Path Cost	10 Mb/s	2 000 000*	200 000–20 000 000	1–200 000 000
Path Cost	100 Mb/s	200 000*	20 000–2 000 000	1–200 000 000
Path Cost	1 Gb/s	20 000	2 000–200 000	1–200 000 000
Path Cost	10 Gb/s	2 000	200–20 000	1–200 000 000
Path Cost	100 Gb/s	200	20–2 000	1–200 000 000
Path Cost	1 Tb/s	20	2–200	1–200 000 000
Path Cost	10 Tb/s	2	1–20	1–200 000 000

*Bridges conformant to IEEE Std 802.1D, 1998 Edition, i.e., that support only 16-bit values for Path Cost, should use 65 535 as the Path Cost for these link speeds when used in conjunction with Bridges that support 32 bit Path Cost values.

Insert a NOTE 2 after Table 8-5 (and renumber the existing NOTE as NOTE 1), as follows:

NOTE 2—BPDUs are capable of carrying 32 bits of Path Cost information; however, IEEE Std. 802.1D, 1998 Edition and earlier revisions of this standard limited the range of the Path Cost parameter to a 16-bit unsigned integer value. The recommended values shown in Table 8-5 make use of the full 32-bit range available in BPDUs in order to extend the range of link speeds supported by the protocol. The recommended values for any intermediate link speed can be calculated as 20 000 000 000/(Link Speed in Kb/s). Limiting the range of the Path Cost parameter to 1–200 000 000 ensures that the accumulated Path Cost cannot exceed 32 bits over a concatenation of 20 hops. In LANs where Bridges that use the recommended values defined in the IEEE Std. 802.1D, 1998 Edition and Bridges that use the recommended values shown in this table are required to interwork, either the older Bridges will need to be re-configured in order to make use of the Path Cost values shown, or the new Bridges will need to be re-configured to make use of Path Cost values compatible with the values used by the older Bridges. The range of Path Costs that can be configured in an older Bridge is insufficient to accommodate the range of data rates available.

9. Encoding of Bridge Protocol Data Units

9.2 Encoding of parameter types

9.2.5 Encoding of Bridge Identifiers

Change the second paragraph as shown:

The ~~two~~ four most significant ~~octets~~ bits of the most significant octet of a Bridge Identifier comprises a settable priority component that permits the relative priority of Bridges to be managed (8.5.3.7 and Clause 14). The next most significant twelve bits of a Bridge Identifier (the four least significant bits of the most significant octet, plus the second most significant octet) comprise a locally assigned system ID extension. The six least significant octets ensure the uniqueness of the Bridge Identifier; they shall be derived from the globally unique Bridge Address (7.12.5) according to the following procedure.

NOTE—The number of bits that are considered to be part of the system ID (60 bits) differs in this version of the standard from the 1998 and prior versions (formerly, the priority component was 16 bits and the system ID component 48 bits).

This change was made in order to allow implementations of Multiple Spanning Trees (P802.1s, a supplement to IEEE Std 802.1Q) to make use of the 12-bit system ID extension as a means of generating a distinct Bridge Identifier per VLAN, rather than forcing such implementations to allocate up to 4094 MAC addresses for use as Bridge Identifiers. To maintain management compatibility with older implementations, the priority component is still considered, for management purposes, to be a 16-bit value, but the values that it can be set to are restricted to only those values where the least significant 12 bits are zero (i.e., only the most significant 4 bits are settable).

9.2.7 Encoding of Port Identifiers

Change the paragraph as shown:

A Port Identifier shall be encoded as two octets, taken to represent an unsigned binary number. If two Port Identifiers are numerically compared, the lesser number shall denote the Port of higher priority. The more significant ~~octet~~ four bits of a Port Identifier is a settable priority component that permits the relative priority of Ports on the same Bridge to be managed (8.5.5 and Clause 14). The less significant ~~octet~~ twelve bits is the Port Number expressed as an unsigned binary number. The value 0 is not used as a Port Number.

NOTE—The number of bits that are considered to be part of the Port Number (12 bits) differs in this version of the standard from the 1998 and prior versions (formerly, the priority component was 8 bits and the Port Number component also 8 bits). This change was made in recognition of the fact that modern switched LAN infrastructures call for increasingly large numbers of Ports to be supported in a single Bridge. To maintain management compatibility with older implementations, the priority component is still considered, for management purposes, to be an 8-bit value, but the values that it can be set to are restricted to those values where the least significant 4 bits are zero (i.e., only the most significant 4 bits are settable).

9.3.3 Validation of received BPDUs

Change item a) as follows:

a) The BPDU Type denotes a Configuration BPDU and the BPDU contains at least 35 octets, and the value of the BPDUs Message Age parameter is less than that of its Max Age parameter, and the Bridge Identifier and Port Identifier parameters from the received BPDU do not match the values that would be transmitted in a BPDU from this port; or

Insert the following NOTE immediately after item a), renumbering the existing NOTE as NOTE 2:

NOTE 1—If the Bridge Identifier and Port Identifier both match the values that would be transmitted in a BPDU from this Port, then the BPDU is discarded, in order to prevent processing of the Port's own BPDUs; for example, if they are received by the Port as a result of a loopback condition. If a loopback condition exists, then there may be other undesirable side effects with respect to Bridge operation caused by the looping back of data frames relayed through the Port .

10. GARP Multicast Registration Protocol (GMRP)

10.3 Definition of the GMRP Application

10.3.2 Provision and support of Extended Filtering Services

10.3.2.2 Registration and de-registration events

Insert the following paragraph between the second and third paragraphs of 10.3.2.2:

The creation of new Group Registration Entries may be restricted by use of the Restricted_Group_Registration control (10.3.2.3). If the value of this control is TRUE, then creation of a new dynamic entry is permitted only if there is a Static Filtering Entry for the VLAN concerned, in which the Registrar Administrative Control value is Normal Registration.

10.3.2.3 Administrative controls

Insert the following paragraph at the end of 10.3.2.3:

Further administrative control over dynamic Group registration may be achieved, if supported, by means of a per-Port Restricted_Group_Registration control parameter. If the value of this control is TRUE for a given Port, the creation or modification of Dynamic Group Registration Entries as a result of GMRP exchanges on that Port shall be restricted only to those MAC addresses for which Static Filtering Entries exist in which the Registrar Administrative Control value is Normal Registration. If the value of the Restricted_Group_Registration control is FALSE, dynamic Group registration is not so restricted. Where management capability is implemented, the value of the Restricted_Group_Registration control can be manipulated by means of the management functionality defined in 14.10.1. If management of this parameter is not supported, the value of this parameter shall be FALSE for all Ports.

12. Generic Attribute Registration Protocol (GARP)

12.2 Overview of GARP operation

Insert the following paragraph at the end of 12.2:

GARP operates only on Ports that are authorized (see 7.12.7) and are supported by a MAC that is operational (see 6.4.2). On any Port that is unauthorized, or for which the MAC_Operational parameter is FALSE, any GARP entity shall not transmit GARP PDUs, and shall discard, without processing, any received GARP PDUs.

12.3 GARP architecture

12.3.3 GIP

Change items a) through d) as follows [leaving the text between items b) and c) as is]:

a) Any GID_Join.indication received by GIP from a given Port in the set is propagated as a GID_Join.request to the instance(s) of GID associated with ~~any~~each other Port in the set;

b) Any GID_Leave.indication received by GIP from a given Port in the set is propagated as a GID_Leave.request to the instance(s) of GID associated with ~~any~~each other Port in the set (Port P, say) if and only if no registration now exists for that Attribute on any other Port in the set excluding Port P.

c) If a Port is added to the set of Ports that are in a Forwarding state, and that Port has previously registered an attribute (a GID_Join.indication has occurred more recently than any GID_Leave.indication for that attribute), then GID_Join.requests for that attribute are propagated to the instance(s) of GID associated with ~~any~~each other Port in the set;

d) If a Port is removed from the set of Ports that are in a Forwarding state, and that Port has previously registered an attribute (a GID_Join.indication has occurred more recently than any GID_Leave.indication for that attribute), and no other Port in the set has registered that attribute, then GID_Leave.requests for that attribute are propagated to the instance(s) of GID associated with ~~any~~each other Port in the set.

12.5 Requirements for interoperability between GARP Participants

Change the contents of the GARP Application addresses table (Table 12-1) as shown below.

Table 12-1—GARP Application addresses

Assignment	Value
GMRP address (See Clause 10)	01-80-C2-00-00-20
~~Reserved~~GVRP address (See IEEE Std 802.1Q)	01-80-C2-00-00-21
Reserved	01-80-C2-00-00-22
Reserved	01-80-C2-00-00-23
Reserved	01-80-C2-00-00-24
Reserved	01-80-C2-00-00-25
Reserved	01-80-C2-00-00-26
Reserved	01-80-C2-00-00-27
Reserved	01-80-C2-00-00-28
Reserved	01-80-C2-00-00-29
Reserved	01-80-C2-00-00-2A
Reserved	01-80-C2-00-00-2B
Reserved	01-80-C2-00-00-2C
Reserved	01-80-C2-00-00-2D
Reserved	01-80-C2-00-00-2E
Reserved	01-80-C2-00-00-2F

12.8 State machine descriptions

Insert the following line to the start of the list of state machine abbreviations; i.e., immediately before rJoinIn:

Initialize state machine (re)initialization event.

12.8.1 Applicant state machine

Change the Applicant state table (Table 12-3) as shown below.

Table 12-3—Applicant state table

		STATE										
		VA	**AA**	**QA**	**LA**	**VP**	**AP**	**QP**	**VO**	**AO**	**QO**	**LO**
EVENT	**transmitPDU!**	sJ[E,I] AA	sJ[E,I] QA	-x-	sLE VO	sJ[E,I] AA	sJ[E,I] QA	-x-	-x-	-x-	-x-	sE VO
	rJoinIn	AA	QA	QA	LA	AP	QP	QP	AO	QO	QO	AO
	rJoinEmpty	VA	VA	VA	VO	VP	VP	VP	VO	VO	VO	VO
	rEmpty	VA	VA	VA	LA	VP	VP	VP	VO	VO	VO	VO
	rLeaveIn	VA	VA	~~VA~~ VP	LA	VP	VP	VP	LO	LO	LO	VO
	rLeaveEmpty	VP	VP	VP	VO	VP	VP	VP	LO	LO	LO	VO
	LeaveAll	VP	VP	VP	VO	VP	VP	VP	LO	LO	LO	VO
	ReqJoin	-x-	-x-	-x-	VA	-x-	-x-	-x-	VP	AP	QP	VP
	ReqLeave	LA	LA	LA	-x-	VO	AO	QO	-x-	-x-	-x-	-x-
	Initialize	VO	VO	VO	VO	VO	VO	VO	VO	VO	VO	VO

Insert the following paragraph at the end of 12.8.1:

The initial state for the Applicant state machine on (re)initialization is VO.

12.8.2 Registrar state machine

Change the Registrar state table (Table 12-4) as shown below.

Table 12-4—Registrar state table

		STATE		
		IN	**LV**	**MT**
EVENT	**rJoinIn**	IN	Stop leavetimer IndJoin IN	IndJoin IN
	rJoinEmpty	IN	Stop leavetimer IndJoin IN	IndJoin IN
	rEmpty	IN	LV	MT
	rLeaveIn	Start leavetimer LV	LV	MT
	rLeaveEmpty	Start leavetimer LV	LV	MT
	LeaveAll	Start leavetimer LV	LV	MT
	leavetimer!	-x-	IndLeave MT	-x-
	Initialize	MT	MT	MT

Insert the following paragraph at the end of 12.8.2:

The initial state for the Registrar state machine on (re)initialization is MT.

12.8.4 Combined Applicant/Registrar state machine

Change the Combined Applicant/Registrar state table (Table 12-7) as shown below.

Table 12-7—Combined Applicant/Registrar state table

		EVENT									
		leavetimer!	**transmitPDU!**	**rJoinIn**	**rJoinEmpty**	**rEmpty**	**rLeaveIn**	**rLeaveEmpty, LeaveAll**	**ReqJoin**	**ReqLeave**	**Initialize**
STATE	**VA.MT**	-x-	AA.MT	AA.IN	VA.IN	VA.MT	~~VP~~VA.MT	VP.MT	-x-	LA.MT	VO.MT
	VA.LV	VA.MT	AA.LV	AA.IN	VA.IN	VA.LV	~~VP~~VA.LV	VP.LV	-x-	LA.LV	VO.MT
	VA.IN	-x-	AA.IN	AA.IN	VA.IN	VA.IN	~~VP~~VA.LV	VP.LV	-x-	LA.IN	VO.MT
	AA.MT	-x-	QA.MT	QA.IN	VA.IN	VA.MT	~~VP~~VA.MT	VP.MT	-x-	LA.MT	VO.MT
	AA.LV	AA.MT	QA.LV	QA.IN	VA.IN	VA.LV	~~VP~~VA.LV	VP.LV	-x-	LA.LV	VO.MT
	AA.IN	-x-	QA.IN	QA.IN	VA.IN	VA.IN	~~VP~~VA.LV	VP.LV	-x-	LA.IN	VO.MT
	QA.MT	-x-	—	QA.IN	VA.IN	VA.MT	VP.MT	VP.MT	-x-	LA.MT	VO.MT
	QA.LV	QA.MT	—	QA.IN	VA.IN	VA.LV	VP.LV	VP.LV	-x-	LA.LV	VO.MT
	QA.IN	-x-	—	QA.IN	VA.IN	VA.IN	VP.LV	VP.LV	-x-	LA.IN	VO.MT
	LA.MT	-x-	VO.MT	LA.IN	VO.IN	LA.MT	LA.MT	VO.MT	VA.MT	-x-	VO.MT
	LA.LV	LA.MT	VO.LV	LA.IN	VO.IN	LA.LV	LA.LV	VO.LV	VA.LV	-x-	VO.MT
	LA.IN	-x-	VO.LV	LA.IN	VO.IN	LA.IN	LA.LV	VO.LV	VA.IN	-x-	VO.MT
	VP.MT	-x-	AA.MT	AP.IN	VP.IN	VP.MT	VP.MT	VP.MT	-x-	VO.MT	VO.MT
	VP.LV	VP.MT	AA.LV	AP.IN	VP.IN	VP.LV	VP.LV	VP.LV	-x-	VO.LV	VO.MT
	VP.IN	-x-	AA.IN	AP.IN	VP.IN	VP.IN	VP.LV	VP.LV	-x-	VO.IN	VO.MT
	AP.IN	-x-	QA.IN	QP.IN	VP.IN	VP.IN	VP.LV	VP.LV	-x-	AO.IN	VO.MT
	QP.IN	-x-	—	QP.IN	VP.IN	VP.IN	VP.LV	VP.LV	-x-	QO.IN	VO.MT
	VO.MT	-x-	—	AO.IN	VO.IN	VO.MT	LO.MT	LO.MT	VP.MT	-x-	VO.MT
	VO.LV	VO.MT	—	AO.IN	VO.IN	VO.LV	LO.LV	LO.LV	VP.LV	-x-	VO.MT
	VO.IN	-x-	—	AO.IN	VO.IN	VO.IN	LO.LV	LO.LV	VP.IN	-x-	VO.MT
	AO.IN	-x-	—	QO.IN	VO.IN	VO.IN	LO.LV	LO.LV	AP.IN	-x-	VO.MT
	QO.IN	-x-	—	QO.IN	VO.IN	VO.IN	LO.LV	LO.LV	QP.IN	-x-	VO.MT
	LO.MT	-x-	VO.MT	AO.IN	VO.IN	VO.MT	~~LO~~VO.MT	~~LO~~VO.MT	VP.MT	-x-	VO.MT
	LO.LV	LO.MT	VO.LV	AO.IN	VO.IN	VO.LV	~~LO~~VO.LV	~~LO~~VO.LV	VP.LV	-x-	VO.MT

12.8.5 Applicant Only State Machine

Change the Applicant Only State Machine table (Table 12-8) as shown below.

Table 12-8—Applicant Only State Machine

		STATE									
		VA	**AA**	**QA**	**LA**	**VP**	**AP**	**QP**	**VO**	**AO**	**QO**
EVENT	**transmit-PDU!**	sJ[I] AA	sJ[I] QA	-x-	sLE VO	sJ[I] AA	sJ[I] QA	-x-	-x-	-x-	-x-
	rJoinIn	AA	QA	QA	LA	AP	QP	QP	AO	QO	QO
	rJoinEmpty	VA	VA	VA	VO	VP	VP	VP	VO	VO	VO
	rEmpty	VA	VA	VA	LA	VP	VP	VP	VO	VO	VO
	rLeaveIn	VA	VA	~~VA~~ VP	LA	VP	VP	VP	VO	VO	VO
	rLeave-Empty	VP	VP	VP	VO	VP	VP	VP	VO	VO	VO
	LeaveAll	VP	VP	VP	VO	VP	VP	VP	VO	VO	VO
	ReqJoin	-x-	-x-	-x-	VA	-x-	-x-	-x-	VP	AP	QP
	ReqLeave	LA	LA	LA	-x-	VO	AO	QO	-x-	-x-	-x-
	Initialize	VO	VO	VO	VO	VO	VO	VO	VO	VO	VO

Insert the following paragraph at the end of 12.8.5:

The initial state for the Applicant Only state machine on (re)initialization is MT.

12.10 Procedures

12.10.3 Protocol event definitions

Insert the following as new subclause 12.10.3.1, renumbering subsequent subclauses:

12.10.3.1 Initialize

The state machine is initialized or reinitialized.

14. Bridge management

14.2 Managed objects

Insert the following as item g):

g) GMRP participants (14.10 and Clause 10).

14.3 Data types

Insert the following as items i) through k):

i) Port Number, an Unsigned value assigned to a Port as part of a Port Identifier. Valid Port Numbers are in the range 1 through 4095;

j) Port Priority, an Unsigned value used to represent the priority component of a Port Identifier. Valid Port Priorities are in the range 0 through 240, in steps of 16;

k) Bridge Priority, an Unsigned value used to represent the priority component of a Bridge Identifier. Valid Bridge Priorities are in the range 0 through 61440, in steps of 4096.

14.8 Bridge Protocol Entity

14.8.1 The Protocol Entity

14.8.1.2 Set Bridge Protocol parameters

14.8.1.2.3 Outputs

Replace the existing text as follows:

~~None.~~

a) Operation status. This takes one of the following values:

1) Operation rejected due to invalid Bridge Priority value (14.3); or

2) Operation accepted.

Change 14.8.2, Bridge Port, and its subclauses as follows:

14.8.2 Bridge Port

A Bridge Port object models the operations related to an individual Bridge Port in relation to the operation of the Spanning Tree Algorithm and Protocol. There are a fixed set of Bridge Ports per Bridge; each can, therefore, be identified by a permanently allocated Port Number, as a fixed component of the Protocol Entity resource. The management operations that can be performed on a Bridge Port are Read Port Parameters, Force Port State, and Set Port Parameters.

14.8.2.1 Read Port Parameters

14.8.2.1.1 Purpose

To obtain information regarding a specific Port within the Bridge's Bridge Protocol Entity.

14.8.2.1.2 Inputs

a) Port Number—the number of the Bridge Port.

14.8.2.1.3 Outputs

a) Uptime—count in seconds of the time elapsed since the Port was last reset or initialized.

b) State—the current state of the Port (i.e., Disabled, Listening, Learning, Forwarding, or Blocking) (8.4 and 8.5.5.2).

c) Port Identifier—the unique Port identifier comprising two parts, the Port Number and the Port Priority field (8.5.5.1).

d) Path Cost (8.5.5.3).

e) Designated Root (8.5.5.4).

f) Designated Cost (8.5.5.5).

g) Designated Bridge (8.5.5.6).

h) Designated Port (8.5.5.7).

i) Topology Change Acknowledge (8.5.5.8).

j) adminEdgePort (18.3.3). Present in implementations that support the identification of edge ports.

k) operEdgePort (18.3.4). Present in implementations that support the identification of edge ports.

14.8.2.2 Force port state

14.8.2.2.1 Purpose

To force the specified Port into Disabled or Blocking.

14.8.2.2.2 Inputs

a) Port Number—the number of the Bridge Port.

b) State—either Disabled or Blocking (8.4 and 8.5.5.2).

14.8.2.2.3 Outputs

None.

14.8.2.2.4 Procedure

If the selected state is Disabled, the Disable Port procedure (8.8.3) is used for the specified Port. If the selected state is Blocking, the Enable Port procedure (8.8.2) is used.

14.8.2.3 Set Port Parameters

14.8.2.3.1 Purpose

To modify parameters for a Port in the Bridge's Bridge Protocol Entity in order to force a configuration of the spanning tree.

14.8.2.3.2 Inputs

a) Port Number—the number of the Bridge Port.

b) Path Cost—the new value (8.5.5.3).

c) Port Priority—the new value of the priority field for the Port Identifier (8.5.5.1).

d) adminEdgePort—the new value of the adminEdgePort parameter (18.3.3). Present in implementations that support the identification of edge ports.

14.8.2.3.3 Outputs

~~None.~~

a) Operation status. This takes one of the following values:

1) Operation rejected due to invalid Port Priority value (14.3); or

2) Operation accepted.

14.8.2.3.4 Procedure

The Set Path Cost procedure (8.8.6) is used to set the Path Cost parameter for the specified Port. The Set Port Priority procedure (8.8.5) is used to set the priority part of the Port Identifier (8.5.5.1) to the supplied value.

Insert the following as new subclause 14.10:

14.10 GMRP entities

The following managed objects define the semantics of the management operations that can be performed upon the operation of GMRP in a Bridge:

a) The GMRP Configuration managed object (14.10.1).

14.10.1 GMRP Configuration managed object

The GMRP Configuration managed object models operations that modify, or enquire about, the overall configuration of the operation of GMRP. There is a single GMRP Configuration managed object per Bridge.

The management operations that can be performed on the GMRP Configuration managed object are as follows:

a) Read GMRP Configuration (14.10.1.1);

b) Notify Group registration failure (14.10.1.2);

c) Configure Restricted_Group_Registration parameters (14.10.1.3).

14.10.1.1 Read GMRP Configuration

14.10.1.1.1 Purpose

To obtain general GMRP configuration information from a Bridge.

14.10.1.1.2 Inputs

None.

14.10.1.1.3 Outputs

a) For each Port:

   1) Port number;

   2) State of the Restricted_Group_Registration parameter (10.3.2.3 in IEEE Std 802.1D), TRUE or FALSE.

14.10.1.2 Notify Group registration failure

14.10.1.2.1 Purpose

To notify a manager that GMRP has failed to register a given Group owing to lack of resources in the Filtering Database for the creation of a Group Registration Entry (7.9.3).

14.10.1.2.2 Inputs

None.

14.10.1.2.3 Outputs

a) The MAC address of the Group that GMRP failed to register;

b) The Port number of the Port on which the registration request was received.

c) The reason for the failure:

   1) Lack of Resources; or

   2) Registration Restricted.

14.10.1.3 Configure Restricted_Group_Registration parameters

14.10.1.3.1 Purpose

To configure the Restricted_Group_Registration parameter (10.3.2.3 in IEEE Std 802.1D) associated with one or more Ports.

14.10.1.3.2 Inputs

a) For each Port to be configured, a Port number and the value of the Restricted_Group_Registration parameter. The permissible values of this parameter are (as defined in 10.3.2.3 of IEEE Std 802.1D):
   1) TRUE;
   2) FALSE.

14.10.1.3.3 Outputs

None.

15. Management protocol

Delete the contents of this clause, replacing it with the following text:

In IEEE Std 802.1D, 1998 Edition, this clause contained managed object definitions for use with CMIP, defined using the GDMO object specification language. As the preponderance of LAN management implementations assume the use of SNMP rather than CMIP as the management protocol, the use of GDMO-based managed object definitions is no longer supported by this standard and is deprecated. The definition of the SNMP MIB for MAC Bridges can be found in IETF RFC 1493 and IETF RFC 2674.

17. Reserved for future use

Clause 17 has been reserved for future standardization of P802.1w, Rapid Spanning Tree.

Insert new Clause 18 as follows:

18. Bridge Detection state machine

The adminEdgePort parameter can be set by management (14.8.2) on a per-Port basis in order to indicate that a given Port is permitted to transit directly to the Forwarding Port State when a Port becomes Designated. This functionality is provided in order to permit Bridge Ports that are (administratively) known to be at the edge of the Bridged LAN to transition to Forwarding without delay. However, as the presence of a Bridge on a Port that has been marked as an edge Port could potentially cause a loop in the active topology, it is necessary to qualify the value of the administrative state variable according to the Port's knowledge of whether or not any BPDUs (i.e., any frames that shall be processed by the Bridge Protocol Entity, in accordance with the provisions of 9.3.3) have been received on the Port.

The Bridge Detection state machine controls the value of the corresponding operational state variable, operEdgePort, which may be used in order to determine whether a Port that becomes Designated is permitted to transit directly to Forwarding. A value of TRUE indicates that this state transition is permitted to occur. If a BPDU (i.e., a frame that shall be processed by the Bridge Protocol Entity, in accordance with the provisions of 9.3.3) is received on the Port, then the value of operEdgePort is set to FALSE. Following a Port initialization, or following a MAC_Operational (6.4.2) transition from FALSE to TRUE, operEdgePort is set to the value of adminEdgePort. Hence, if a Port that has been marked as an edge Port proves not to be one (by virtue of the presence of another Bridge), then it will cease to behave like an edge Port until such a time as it is reinitialized, or its MAC becomes operational.

18.1 Notational conventions used in State Diagrams

The state diagrams in this clause are used to represent the operation of a function as a group of connected, mutually exclusive states. Only one state of a function can be active at any given time.

Each state is represented in the state diagram as a rectangular box, divided into two parts by a horizontal line. The upper part contains the state identifier, written in upper case letters. The lower part contains any procedures that are executed on entry to the state.

All permissible transitions between states are represented by arrows, the arrowhead denoting the direction of the possible transition. Labels attached to arrows denote the condition(s) that must be met in order for the transition to take place. A transition that is global in nature (i.e., a transition that occurs from any of the possible states if the condition attached to the arrow is met) is denoted by an open arrow; i.e., no specific state is identified as the origin of the transition.

On entry to a state, the procedures defined for the state (if any) are executed exactly once, in the order that they appear on the page. Each action is deemed to be atomic; i.e., execution of a procedure completes before

the next sequential procedure starts to execute. No procedures execute outside of a state block. On completion of all of the procedures within a state, all exit conditions for the state (including all conditions associated with global transitions) are evaluated continuously until such a time as one of the conditions is met. All exit conditions are regarded as Boolean expressions that evaluate to True or False; if a condition evaluates to True, then the condition is met. When the condition associated with a global transition is met, it supersedes all other exit conditions including UCT. The label UCT denotes an unconditional transition (i.e., UCT always evaluates to True). The label ELSE denotes a transition that occurs if none of the other conditions for transitions from the state are met (i.e., ELSE evaluates to True if all other possible exit conditions from the state evaluate to False).

A variable that is set to a particular value in a state block retains this value until a subsequent state block executes a procedure that modifies the value.

Where it is necessary to segment a state machine description across more than one diagram, a transition between two states that appear on different diagrams is represented by an exit arrow drawn with dashed lines, plus a reference to the diagram that contains the destination state. Similarly, dashed arrows and a dashed state box are used on the destination diagram to show the transition to the destination state. In a state machine that has been segmented in this way, any global transitions that can cause entry to states defined in one of the diagrams are deemed to be potential exit conditions for all of the states of the state machine, regardless of which diagram the state boxes appear in.

Should a conflict exist between the interpretation of a state diagram and either the corresponding global transition tables or the textual description associated with the state machine, the state diagram takes precedence.

The interpretation of the special symbols and operators used in the state diagrams is as defined in Table 18-1; these symbols and operators are derived from the notation of the “C” programming language, ANSI X3.159.

Table 18-1—State machine symbols

Symbol	Interpretation
( )	Used to force the precedence of operators in Boolean expressions and to delimit the argument(s) of actions within state boxes.
;	Used as a terminating delimiter for actions within state boxes. Where a state box contains multiple actions, the order of execution follows the normal English language conventions for reading text.
=	Assignment action. The value of the expression to the right of the operator is assigned to the variable to the left of the operator. Where this operator is used to define multiple assignments, (e.g., a = b = X) the action causes the value of the expression following the right-most assignment operator to be assigned to all of the variables that appear to the left of the right-most assignment operator.
!	Logical NOT operator.
&&	Logical AND operator.
||	Logical OR operator.
if...then...	Conditional action. If the Boolean expression following the if evaluates to TRUE, then the action following the then is executed.
!=	Inequality. Evaluates to TRUE if the expression to the left of the operator is not equal in value to the expression to the right.
==	Equality. Evaluates to TRUE if the expression to the left of the operator is equal in value to the expression to the right.
*	Arithmetic multiplication operator.
–	Arithmetic subtraction operator.

18.2 Bridge Detection state machine definition

The Bridge Detection state machine, as defined by Figure 18-1 and the associated variable definitions in 18.3, shall be implemented on all Bridge Ports that support the use of the adminEdgePort and operEdgePort parameters.

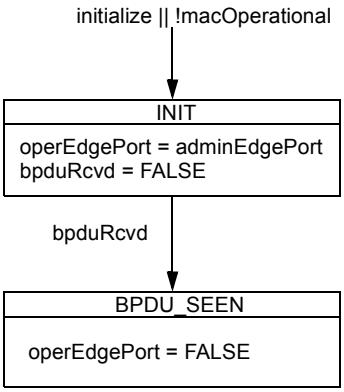


Figure 18-1—Bridge Detection State Machine

18.3 Variables used in the Bridge Detection state machine

18.3.1 initialize

This variable is externally controlled. When asserted it forces the state machine to its initial state.

18.3.2 macOperational

This variable directly reflects the value of the MAC_Operational parameter (6.4.2) for the Port.

18.3.3 adminEdgePort

The administrative value of the Edge Port parameter, as set by management (14.8.2). A value of TRUE indicates that this Port is considered to be an edge Port; a value of FALSE indicates that this Port is not considered to be an edge Port. The recommended default value of adminEdgePort is FALSE.

18.3.4 operEdgePort

The operational value of the Edge Port parameter. This is initialized to the value of adminEdgePort, and is set FALSE on reception of a BPDU (18.3.5).

18.3.5 bpduRcvd

This variable is set TRUE if a BPDU (i.e., a frame that shall be processed by the Bridge Protocol Entity, in accordance with the provisions of 9.3.3) is received on the Port.

Annex A

(normative)

PICS Proforma

Change the contents of A.5 by inserting new rows 1d, 1e as follows:

A.5 Major capabilities and options

Item	Feature	Status	References	Support
(1a)	Communications Support Which Media Access Control types are supported on Bridge Ports, implemented in conformance with the relevant MAC standards?		6.5	
(1a.1)*	CSMA/CD, IEEE Std 802.3	O.1		Yes [ ] No [ ]
(1a.2)*	Token Bus, ISO/IEC 8802-4	O.1		Yes [ ] No [ ]
(1a.3)*	Token Ring, ISO/IEC 8802-5	O.1		Yes [ ] No [ ]
(1a.4)*	FDDI, ISO 9314-2	O.1		Yes [ ] No [ ]
(1a.5)*	DQDB, ISO/IEC 8802-6	O.1		Yes [ ] No [ ]
(1a.6)*	ISLAN, ISO/IEC 8802-9	O.1		Yes [ ] No [ ]
(1a.7)*	ISLAN 16-T, IEEE Std 802.9a	O.1		Yes [ ] No [ ]
(1a.8)*	Demand Priority, ISO/IEC 8802-12 (IEEE Std 802.3 format)	O.1		Yes [ ] No [ ]
(1a.9)*	Demand Priority, ISO/IEC 8802-12 (ISO/IEC 8802-5 format)	O.1		Yes [ ] No [ ]
(1a.11)*	Wireless LAN, ISO/IEC DIS 8802-11	O.1		Yes [ ] No [ ]
(1b)	Is LLC Type 1 supported on all Bridge Ports in conformance with ISO/IEC 8802-2?	M	7.2, 7.3, 7.12, ISO/IEC 8802-2	Yes [ ]
(1c)	Is Source-Routing Transparent Bridge operation supported on any of the Bridge Ports? (If support is claimed, the PICS proforma detailed in Annex D shall also be completed).	O	Annex C	Yes [ ] No [ ]
(1d)*	Does the implementation support the use of the adminEdgePort and operEdgePort parameters on any Ports? State which Bridge Ports support the adminEdgePort and operEdgePort parameters	O	5.2, 14.8.2	Yes [ ] No [ ] Ports_____
(1e)	Does the implementation support the operation of the Bridge Detection State Machine on any Ports? State which Bridge Ports support the operation of the Bridge Detection State Machine	1d:M	5.2, 14.8.2, 18.2	Yes [ ] No [ ] Ports_____
(2)	Relay and filtering of frames (A.6)	M	7.5, 7.6, 7.7	Yes [ ]
(2a)	Does the Bridge support Basic Filtering Services?	M	6.6.5, 7.7.2	Yes [ ]
(2b)*	Does the Bridge support Extended Filtering Services?	O	6.6.5, 7.7.2	Yes [ ] No [ ]

A.5 Major capabilities and options *(continued)*

Item	Feature	Status	References	Support
	If item (2b) is not supported, mark "N/A" and continue at (2e)			N/A[ ]
(2c)*	Does the Bridge support dynamic Group forwarding and filtering behavior?	2b:M	6.6.5	Yes [ ] No [ ]
(2d)*	Does the Bridge support 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?	2b:O	6.6.5	Yes [ ] No [ ]
(2e)	Does the Bridge support expedited traffic classes on any of its Ports?	O	7.1.2, 7.7.3	Yes [ ] No [ ]
(4)*	Does the Bridge support management of the priority of relayed frames?	O	6.5, 7.5.1, 7.7.3, 7.7.5, Table 7-1, Table 7-2, Table 7-3	Yes [ ] No [ ]
(5)	Maintenance of filtering information (A.7)	M	7.8, 7.9	Yes [ ]
(7a)	Can the Filtering Database be read by management?	O	7.9	Yes [ ] No [ ]
(7c)*	Can Static Filtering Entries be created and deleted?	O	7.9.1	Yes [ ] No [ ]
(7g)	Can Static Filtering Entries be created and deleted in the Permanent Database?	O	7.9.6	Yes [ ] No [ ]
(7h)	Can Static Filtering Entries be created for a given MAC address specification with a distinct Port Map for each inbound Port?	O	7.9.1	Yes [ ] No [ ]
(7i)	Can Group Registration Entries be dynamically created, updated and deleted by GMRP?	2c:M	7.9.3, 10	Yes [ ] N/A [ ]
(10)	Addressing (A.8)	M	7.12	Yes [ ]
(9a)*	Can the Bridge be configured to use 48-bit Universal Addresses?	O.3	7.12	Yes [ ] No [ ]
(9b)*	Can the Bridge be configured to use 48-bit Local Addresses?	O.3	7.12	Yes [ ] No [ ]
(13)*	Spanning Tree algorithm and protocol (A.9)	M	8, 9	Yes [ ]
(16)*	Does the Bridge support management of the Spanning Tree topology?	O	8.2	Yes [ ] No [ ]
(17)*	Does the Bridge support management of the protocol timers?	O	8.10	Yes [ ] No [ ]
(19)*	Bridge Management Operations	O	14	Yes [ ] No [ ]
(20a)*	Are the Bridge Management Operations supported via a Remote Management Protocol?	19:O.4	5	Yes [ ] No [ ] N/A [ ]
(20b)*	Are the Bridge Management Operations supported via a local management interface?	19:O.4	5	Yes [ ] No [ ] N/A [ ]

Insert new row (15b) immediately following row (15a) of A.9, as follows:

(15b)	As a default behavior, is the Path Cost for a Port unaffected by any dynamic changes in the Port's data rate?	M	8.10.2	Yes [ ]

Change the contents of A.12 by inserting a new row 22i, renumbering subsequent rows, and inserting a new row 22o, as follows:

A.12 GARP and GMRP

Item	Feature	Status	References	Support
	If Item 2b is not supported, mark N/A and continue at item (~~22i~~22j).			N/A [ ]
(22a)	Is the GMRP Application address used as the destination MAC Address in all GMRP protocol exchanges?	2b:M	10.4.1, Table 12-1	Yes [ ]
(22b)	Are GMRP protocol exchanges achieved by means of LLC Type 1 procedures, using the LLC address for Spanning Tree protocol?	2b:M	12.4, 12.5, Table 7-8	Yes [ ]
(22c)	Are GMRP protocol exchanges achieved using the GARP PDU formats, and the definition of the attribute type and value encodings defined for GMRP?	2b:M	10.3.1, 12.4, 12.5, 12.11	Yes [ ]
(22d)	Does the implementation support the operation of the Applicant, Registrar, and Leave All state machines?	2b:M	12.8, 13	Yes [ ]
(22e)	Does the Bridge propagate GMRP registration information only on Ports that are part of the active topology for the Base Spanning Tree Context?	2b:M	12.3.3, 12.3.4, 13	Yes [ ]
(22f)	Are GARP PDUs received on Ports that are in the Forwarding State forwarded, filtered or discarded in accordance with the requirements for handling GARP Application addresses?	2b:M	7.12.3, 12.5	Yes [ ]
(22g)	Does the GMRP application operate as defined in Clause 10?	2b:M	10, 10.3	Yes [ ]
(22h)	Are received GARP PDUs that are not well formed for the GARP Applications supported, discarded?	2b:M	10.3.1, 12.4, 12.5, 12.10, 12.11	Yes [ ]
(22i)	Does the implementation support the use of the Restricted Group Registration parameter for each Port?	2b:O	5.2, 10.3.2	Yes [ ] No [ ]

A.12 GARP and GMRP *(continued)*

Item	Feature	Status	References	Support
(~~22i~~22j)	Are all GARP PDUs that are (a) received on Ports that are in the Forwarding State, and are (b) destined for GARP applications that the Bridge does not support, forwarded on all other Ports that are in Forwarding?	M	7.12.3, 12.5	Yes [ ]
(~~22j~~22k)	Are any GARP PDUs that are (a) received on any Port, and (b) destined for GARP applications that the Bridge does not support, submitted to any GARP Participants?	X	7.12.3, 12.5	No [ ]
(~~22k~~22l)	Are any GARP PDUs that are (a) received on any Ports that are not in the Forwarding State, and are (b) destined for GARP applications that the Bridge does not support, forwarded on any other Ports of the Bridge?	X	7.12.3, 12.5	No [ ]
(~~22l~~22m)	Are any GARP PDUs that are (a) received on any Ports that are in the Forwarding State, and are (b) destined for GARP applications that the Bridge supports, forwarded on any other Ports of the Bridge?	X	7.12.3, 12.5	No [ ]
(~~22m~~22n)	Are all GARP PDUs that are: (a) received on any Port, and (b) destined for GARP applications that the Bridge supports, submitted to the appropriate GARP Participants?	M	7.12.3, 12.5	Yes [ ]
22o	Are all GARP PDUs received on disabled Ports discarded?	M	12.2	Yes [ ]

Annex B

(informative)

Calculating Spanning Tree parameters

B.3 Calculation

Change the Hold time calculation description as follows:

B.3.6 Hold time

B.3.6.1 Step

Select a value for **Hold Time**.

B.3.6.2 Basis of choice

If **Hold Time** is greater than the **maximum BPDU transmission delay**, then the **Maximum Bridge Protocol Message propagation time** will be set, in the worst scenario, by a delay of **Hold Time** at each Bridge rather than by a delay of **maximum BPDU transmission delay**. This would invalidate the conclusion in B3.5, above. Therefore, the following has been chosen:

$$hold\_t \leq pdu\_d \quad (8)$$

B.3.6.3 Recommended values for IEEE 802 Bridged LANs

~~*hold_t = 1.0*~~ *Not more than 3 BPDUs transmitted in any Hello Time interval*

Annex C

(normative)

Source-Routing Transparent Bridge operation

C.1.1 Scope

Delete the first item after e), as follows:

~~— How the management operations are made available to a remote Manager using the protocol and architectural description provided by ISO/IEC 15802-2.~~

Annex E

(normative)

Allocation of Object Identifier values

E.2 Allocation tables

In the STATUS column of all of the allocation tables in E.2, change all instances of "C" (standing for Current) to "D" (standing for Deprecated).