



IEEE Standard for Local and metropolitan area networks

Virtual Bridged Local Area Networks

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

802.1QTM

IEEE
3 Park Avenue
New York, NY 10016-5997, USA
19 May 2006

IEEE Std 802.1QTM-2005
(Incorporates IEEE Std 802.1Q-1998, IEEE Std 802.1uTM-2001,
IEEE Std 802.1vTM-2001, and IEEE Std 802.1sTM-2002)

*Recognized as an
American National Standard (ANSI)*

IEEE Std 802.1Q™-2005
(Incorporates IEEE Std 802.1Q-1998, IEEE Std 802.1u™-2001,
IEEE Std 802.1v™-2001, and IEEE Std 802.1s™-2002)

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

Virtual Bridged Local Area Networks

Sponsor

**LAN/MAN Standards Committee
of the
IEEE Computer Society**

Approved 28 March 2006

American National Standards Institute

Approved 7 December 2005

IEEE-SA Standards Board

Abstract: This standard specifies how the MAC Service is supported by Virtual Bridged Local Area Networks, the principles of operation of those networks, and the operation of VLAN-aware Bridges, including management, protocols, and algorithms.

Keywords: Bridged Local Area Networks, local area networks (LANs), MAC Bridges, metropolitan area networks, Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), Virtual Bridged Local Area Networks (virtual LANs)

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

Copyright © 2006 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 19 May 2006. Printed in the United States of America.

IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

Print: ISBN 0-7381-4876-6 SH95508
PDF: ISBN 0-7381-4877-6 SS95508

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

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

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

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

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

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

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

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
Piscataway, NJ 08854
USA

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

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

Introduction

This introduction is not part of IEEE Std 802.1Q-2005, IEEE Standards for Local and metropolitan area networks—Virtual Bridged Local Area Networks.

The MAC Bridge standardization activities that resulted in the development of IEEE Std 802.1D™-1993 introduced the concept of Filtering Services in Bridged Local Area Networks, and mechanisms whereby filtering information in such LANs may be acquired and held in a Filtering Database.

IEEE Std 802.1D™, 1998 Edition, a revision of IEEE Std 802.1D-1993, extended this concept of Filtering Services to define additional capabilities aimed at

- a) The provision of expedited traffic capabilities, to support the transmission of time-critical information in a LAN environment.
- b) The use of signaled priority information as the basis for identifying expedited classes of traffic.
- c) The provision of filtering services that support the dynamic definition and establishment of Groups in a LAN environment, and the filtering of frames by Bridges such that frames addressed to a particular Group are forwarded only on those LAN segments that are required to reach members of that Group.
- d) The provision of a Generic Attribute Registration Protocol (GARP) that is used to support the mechanism for providing Group filtering capability and is made available for use in other attribute registration applications.

This standard, first published as IEEE Std 802.1Q-1998, makes use of the concepts and mechanisms of LAN Bridging that were introduced by IEEE Std 802.1D, and it defines additional mechanisms that allow the implementation of Virtual Bridged Local Area Networks. The following mechanisms are described:

- e) Virtual LAN Services.
- f) The operation of the Forwarding Process that is required.
- g) The structure of the Filtering Database that is required.
- h) The nature of the protocols and procedures that are required to provide Virtual LAN services, including the definition of the frame formats used to represent VLAN identification information, and the procedures used to insert and remove VLAN identifiers and the headers in which they are carried.
- i) The ability to support end-to-end signaling of priority information regardless of the intrinsic ability of the underlying MAC protocols to signal priority information.
- j) The GARP VLAN Registration Protocol (GVRP) that allows distribution and registration of VLAN membership information (the protocol described makes use of the GARP protocol defined in ISO/IEC 15802-3).
- k) The management services and operations that are required to configure and administer networks.

The 2003 Edition of the standard incorporated three amendments, IEEE Std 802.1u™-2001, IEEE Std 802.1v™-2001, and IEEE Std 802.1s™-2002, into the text of IEEE Std 802.1Q-1998. These amendments describe enhancements to the standard to allow

- l) Dynamic Group and VLAN registration to be restricted, based on the contents of static filtering entries.
- m) VLAN classification according to link layer protocol type.

- n) Support for VLANs carried over multiple Spanning Tree instances.

This revision of the standard is the result of balloting the 2003 Edition, along with maintenance changes to align the text with improvements made to IEEE Std 802.1D.

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

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

Notice to users

Errata

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

Interpretations

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

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents or patent applications for which a license may be required to implement an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention. A patent holder or patent applicant has filed a statement of assurance that it will grant licenses under these rights without compensation or under reasonable rates and nondiscriminatory, reasonable terms and conditions to applicants desiring to obtain such licenses. The IEEE makes no representation as to the reasonableness of rates, terms, and conditions of the license agreements offered by patent holders or patent applicants. Further information may be obtained from the IEEE Standards Department.

Participants

The following is a list of participants in the Interworking activities of the IEEE 802.1 Working Group.

Tony Jeffree, *Chair and Editor*
Mick Seaman, *Chair, Interworking Task Group*

Mike Borza	Romain Insler	Dan Romascanu
Paul Bottorff	Ran Ish-Shalom	Jessy V. Rouyer
Jim Burns	Michael Johas Teener	Ali Sajassi
Dirceu Cavendish	Hal Keen	Panagiotis Saltsidis
Arjan de Heer	Yongbum Kim	Sam Sambasivan
Russell Dietz	Loren Larsen	John Sauert
Linda Dunbar	Yannick Le Goff	Koichiro Seto
Anush Elangovan	David Martin	Curtis Simonson
Hesham Elbakoury	John Messenger	Bob Sultan
David Elie-Dit-Cosaque	Dinesh Mohan	Muneyoshi Suzuki
Don Fedyk	Bob Moskowitz	Yoshihiro Suzuki
Norm Finn	Don O'Connor	Francois Tallet
David Frattura	Karen O'Donoghue	John Viega
Anoop Ghanwani	Glenn Parsons	Dennis Volpano
Ken Grewal	Ken Patton	Manoj Wadekar
Steve Haddock	Ray Qiu	Ludwig Winkel
Takashi Hasegawa	Karen Randall	Michael D. Wright
	Allyn Romanow	

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

Brandon Barry	Neil Jarvis	Jessy V. Rouyer
Les Bell	Tony Jeffree	Ali Sajassi
Mike Borza	Hal Keen	Dolors Sala
Paul Bottorff	Yongbum Kim	Sam Sambasivan
Jim Burns	Shobhan Lakkapragada	John Sauer
Dirceu Cavendish	Bill Lane	Mick Seaman
Paul Congdom	Loren Larson	Koichiro Seto
Sharam Davari	Yannick Le Goff	Muneyoshi Suzuki
Arjan de Heer	Marcus Leech	Jonathan Thatcher
Craig Easley	John Messenger	Geoff Thompson
Anush Elangovan	Dinesh Mohan	Michel Thorsen
Helsham Elbakoury	Bob Moskowitz	Jonathan R. Thatcher
David Elie-Dit-Cosaque	Don O'Connor	John Viega
Norm Finn	Don Pannell	Preeti Vinayakray-Jani
David Fattura	Glenn Parsons	John Vollbrecht
Gerard Goubert	Karen Randall	Dennis Valpano
Stephen Haddock	Allyn Romanow	Karl Weber
Ran Ish-Shalom	Dan Romascanu	Ludwig Winkel
Atsushi Iwata		Michael D. Wright

When the IEEE-SA Standards Board approved this standard on 7 December 2005, it had the following membership:

Steve M. Mills, *Chair*
Richard H. Hulett, *Vice Chair*
Don Wright, *Past Chair*
Judith Gorman, *Secretary*

Mark D. Bowman
Dennis B. Brophy
Joseph Bruder
Richard Cox
Bob Davis
Julian Forster*
Joanna N. Guenin
Mark S. Halpin
Raymond Hapeman

William B. Hopf
Lowell G. Johnson
Herman Koch
Joseph L. Koepfinger*
David J. Law
Daleep C. Mohla
Paul Nikolic

T. W. Olsen
Glenn Parsons
Ronald C. Petersen
Gary S. Robinson
Frank Stone
Malcolm V. Thaden
Richard L. Townsend
Joe D. Watson
Howard L. Wolfman

*Member Emeritus

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

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

Jennie M. Steinhagen
IEEE Standards Project Editor

Historical participants

Since the initial publication, many IEEE standards have added functionality or provided updates to material included in this standard. The following is a historical list of participants who have dedicated their valuable time, energy, and knowledge to the creation of this material:

IEEE 802.1Q Standard	Date approved by IEEE	Officers at the time of Working Group Letter Ballot
IEEE Std 802.1Q-1998	8 December 1998	William P. Lidinsky , <i>Chair</i> Mick Seaman , <i>Chair, Interworking Task Group</i> Tony Jeffree , <i>Coordinating Editor</i> Anil Rijasinghani, Richard Hausmann, Michele Wright, Paul Langille, P. J. Singh , <i>Editorial Team</i>
IEEE Std 802.1u-2001	17 March 2001	Tony Jeffree , <i>Chair</i> Neil Jarvis , <i>Vice Chair</i> Mick Seaman , <i>Chair, Interworking Task Group</i>
IEEE Std 802.1v-2001	17 March 2001	Tony Jeffree , <i>Chair</i> Neil Jarvis , <i>Vice Chair</i> Mick Seaman , <i>Chair, Interworking Task Group</i> David Delany , <i>Editor</i> Andrew Smith , <i>Editor</i>
IEEE Std 802.1s-2002	11 December 2002	Tony Jeffree , <i>Chair</i> Neil Jarvis , <i>Vice Chair</i> Mick Seaman , <i>Chair, Interworking Task Group</i> Norm W. Finn , <i>Editor</i>

Steve Adams	Ariel Hendel	Kirk Preiss
Stephen Ades	John Hickey	Steve Ramberg
Ken Alonge	David Hollender	Shlomo Reches
Floyd Backes	Steve Horowitz	Frank Reichstein
John Bartlett	Bob Hott	Dick Reohr
Les Bell	Michelle Hsiung	James Richmond
Avner Ben-Dor	Rita Hunt	John J. Roese
Michael Berger	David Husak	Doug Ruby
James S. Binder	Altaf Hussain	Ray Samora
David Brady	Ran Ish-Shalom	Ayman Sayed
Martin Brewer	Vipin K. Jain	Ted Schroeder
Bill Bunch	Shyam Kaluve	Benjamin Schultz
Bob Cardinal	Allen Kasey	Rich Seifert
Paul Carroll	Toyayuki Kato	Lee Sendelbach
Jeffrey Catlin	Hal Keen	Himanshu Shah
Dennis Cave	Daniel Kelley	K. Karl Shimada
Alan Chambers	Kevin Ketchum	Fred Shu
Steve Chan	Keith Klamm	Phil Simmons
David W. Chang	Bruce Kling	Curtis Simonson
Ken Chapman	Walter Knitl	Rosemary V. Slager
Hon Wah Chin	Dan Krent	Alexander Smith
Chi Chong	Paul Kummer	Michel Soerensen
Chris Christ	Paul Lachapelle	Larry Stefani
Marc Cochran	Bill Lane	Stuart Soloway
Paul Congdon	Loren Larsen	Sundar Subramaniam
Glenn Connery	Johann Lindmeyr	Richard Sweatt
David Cullerot	Gary Littleton	Robin Tasker
Ted Davies	Robert D. Love	Michel Thorsen
Andy Davis	Andy Luque	Fouad Tobagi
Prakash Desai	Peter Martini	Naoki Tsukutari
Jeffrey Dietz	Keith McCloghrie	Dhadesugoor Vaman
Kurt Dobbins	Martin McNealis	Steve Van Seters
Peter Ecclesine	Milan Merhar	Dono van-Mierop
J. J. Ekstrom	John Messenger	Manoj Wadekar
Hesham El Bakoury	Colin Mick	John Wakerly
Yishai Fraenkel	Amol Mitra	Peter Wang
Paul Frantz	Yaron Nachman	Philip Wang
Lars Henrik Frederiksen	Krishna Narayanaswamy	Y. C. Wang
Anoop Ghanwani	Paul Nikolich	Trevor Warwick
John Grinham	Lawrence Ng	Bob Watson
Steve Haddock	Henry Ngai	Alan Weissberger
Sharam Hakimi	Satoshi Obara	Glenn Wenig
John Hart	Eugene O'Neil	Keith Willette
Scott Harvell	Toshio Ooka	Robert Williams
Wayne Hathaway	Jörg Ottensmeyer	Michael Witkowski
Vic Hayes	Luc Pariseau	Edward Wong
David Head	Yonadav Perry	Michael D. Wright
Gaby Hecht	John Pickens	Allen Yu
Deepak Hegde	Gideon Prat	Wayne Zakowski

Figures

Figure 6-1—Internal organization of the MAC sublayer	15
Figure 6-2—Example of operation of port-and-protocol based classification	30
Figure 7-1—VLAN Bridging overview	34
Figure 8-1—A Bridged Local Area Network	39
Figure 8-2—VLAN-aware Bridge architecture	41
Figure 8-3—Relaying MAC frames	43
Figure 8-4—Observation of network traffic	43
Figure 8-5—Operation of Spanning Tree protocol.....	43
Figure 8-6—Operation of GARP.....	44
Figure 8-7—Management Port transmission and reception	44
Figure 8-8—Bridge Port Transmit and Receive	46
Figure 8-9—Forwarding Process functions	47
Figure 8-10—Logical points of attachment of the Higher Layer and Relay Entities	69
Figure 8-11—Effect of control information on the forwarding path.....	70
Figure 8-12—Per-Port points of attachment.....	70
Figure 8-13—Single point of attachment—relay permitted	71
Figure 8-14—Single point of attachment—relay not permitted.....	71
Figure 8-15—Effect of Port State	72
Figure 8-16—Effect of authorization	72
Figure 8-17—Ingress/egress control information in the forwarding path	73
Figure 9-1—VLAN TAG TCI format.....	76
Figure 9-2—E-RIF Route Control (RC) field.....	78
Figure 10-1—Example of GMRP propagation in a VLAN context	81
Figure 11-1—Operation of GVRP.....	84
Figure 13-1—Diagrammatic conventions	134
Figure 13-2—An example network	136
Figure 13-3—Example network with CIST Priority Vectors, Port Roles, and MST Regions	137
Figure 13-4—MSTI Active Topology in Region 2 of the example network	138
Figure 13-5—CIST and MSTI active topologies in Region 1 of the example network.....	150
Figure 13-6—Agreements and Proposals	154
Figure 13-7—CIST and MSTI Active Topologies in a Region.....	155
Figure 13-8—Enhanced Agreements.....	156
Figure 13-9—MSTP state machines—overview and relationships.....	160
Figure 13-10—MSTP overview notation	161
Figure 13-11—Port Receive state machine	180
Figure 13-12—Port Transmit state machine.....	181
Figure 13-13—Port Information state machine	182
Figure 13-14—Port Role Selection state machine.....	183
Figure 13-15—Disabled Port role transitions	184
Figure 13-16—Port Role Transitions state machine—MasterPort.....	184
Figure 13-17—Port Role Transitions state machine—RootPort	185
Figure 13-18—Port Role Transitions state machine—DesignatedPort	186
Figure 13-19—Port Role Transitions state machine—AlternatePort and BackupPort	186
Figure 13-20—Port State Transition state machine.....	187
Figure 13-21—Topology Change state machine	187
Figure 14-1—MST BPDU parameters and format.....	192
Figure 14-2—MSTI Configuration Message parameters and format.....	196
Figure B-1—Connecting independent VLANs—1	226
Figure B-2—Connecting independent VLANs—2	227
Figure B-3—Duplicate MAC Addresses	227
Figure B-4—Asymmetric VLAN use: “multi-netted server”	228

Figure C-1—Services and environments	234
Figure C-2—Heterogeneous Bridging functions	235
Figure C-3—Tagged IEEE 802.3 MAC frame format	239
Figure C-4—Tagged frames on 8802-5 Token Ring LANs.....	239
Figure C-5—Tagged frames on FDDI LANs	241
Figure C-6—Tagged frames on 802.3/Ethernet LANs	242
Figure C-7—Translation between E-C-T/C,U and E-C-T/C,T.....	250
Figure C-8—Translation between E-C-T/C,U and E-C-T/R,T.....	251
Figure C-9—Translation between L-C-T/C,U and L-C-T/C,T.....	252
Figure C-10—Translation between L-C-T/C,U and L-C-T/R,T.....	253
Figure C-11—Translation between E-X-X/R,U and E-X-X/C,T	254
Figure C-12—Translation between E-X-X/R,U and E-X-X/R,T (8802-5 & SR FDDI).....	255
Figure C-13—Translation between E-X-X/R,U and E-X-X/R,T (transparent FDDI)	256
Figure C-14—Translation between L-X-X/R,U and L-X-X/C,T	257
Figure C-15—Translation between L-X-X/R,U and L-X-X/R,T (8802-5 and SR FDDI)	258
Figure C-16—Translation between L-X-X/R,U and L-X-X/R,T (transparent FDDI)	259
Figure C-17—Relaying Ethernet Type-encoded tagged frames.....	260
Figure C-18—Relaying LLC-encoded tagged frames.....	261
Figure C-19—Relaying tagged frames between transparent and SR forms	263
Figure C-20—SNAP-encoded Protocol Type format	263
Figure E-1—Static filtering inconsistency	268
Figure E-2—Interoperability with IEEE 802.1D Bridges: example 1.....	269
Figure E-3—Interoperability with IEEE 802.1D Bridges: example 2.....	270
Figure E-4—Interoperability between Port-based and Port-and-Protocol-based classification	277

Tables

Table 6-2—FDDI and Token Ring priority regeneration	24
Table 6-1—FDDI and Token Ring access priorities	24
Table 6-3—Priority regeneration	29
Table 8-1—VLAN-aware Bridge reserved addresses	49
Table 8-2—Recommended priority to traffic class mappings.....	50
Table 8-3—Ageing time parameter value	56
Table 8-4—Combining Static and Dynamic Filtering Entries for an individual MAC Address	62
Table 8-5—Combining Static Filtering Entry and Group Registration Entry for “All Group Addresses” and “All Unregistered Group Addresses”	63
Table 8-6—Forwarding or Filtering for specific group MAC Addresses	64
Table 8-7—Determination of whether a Port is in a VLAN’s member set	64
Table 8-8—Standard LLC address assignment	68
Table 9-2—Reserved VID values.....	76
Table 9-1—IEEE 802.1Q Ethernet Type allocations	76
Table 11-1—GVRP Application address	86
Table 13-1—Configuration Digest Signature Key	142
Table 13-2—Sample Configuration Digest Signature Keys.....	142
Table 13-3—Internal Port Path Costs	189
Table G-1—Traffic type to traffic class mapping.....	281
Table G-2—Traffic type acronyms.....	282
Table G-3—Defining traffic types.....	283

Contents

1. Overview	1
1.1 Scope	1
1.2 VLAN aims and benefits	2
2. Normative references	3
3. Definitions	5
4. Abbreviations	9
5. Conformance	11
5.1 Requirements terminology	11
5.2 Protocol Implementation Conformance Statement (PICS)	11
5.3 VLAN-aware Bridge requirements	11
5.4 MAC-specific bridging methods	13
6. Support of the MAC Service in VLANs	15
6.1 Support of the MAC service	15
6.2 Preservation of the MAC service	16
6.3 Quality of service maintenance	16
6.4 Internal Sublayer Service	21
6.5 Support of the Internal Sublayer Service by specific MAC procedures	23
6.6 Enhanced Internal Sublayer Service	25
6.7 Support of the EISS	26
6.8 Protocol VLAN classification	29
7. Principles of network operation	33
7.1 Network overview	33
7.2 Use of VLANs	34
7.3 VLAN topology	35
7.4 Locating end stations	35
7.5 Ingress, forwarding, and egress rules	37
8. Principles of bridge operation	38
8.1 Bridge operation	38
8.2 Bridge architecture	41
8.3 Model of operation	42
8.4 Port states and the active topology	44
8.5 Bridge Port Transmit and Receive	45
8.6 The Forwarding Process	47
8.7 The Learning Process	51
8.8 The Filtering Database	52
8.9 MST configuration information	65
8.10 Spanning Tree Protocol Entity	66
8.11 GARP Entities	66
8.12 Bridge Management Entity	66
8.13 Addressing	67

9. Tagged frame format	74
9.1 Purpose of tagging	74
9.2 Representation and encoding of tag fields	74
9.3 Tag format.....	75
9.4 Tag Protocol Identifier (TPID) formats	75
9.5 Tag Protocol Identification	75
9.6 VLAN Tag Control Information	76
9.7 Embedded Routing Information Field (E-RIF)	77
10. Use of GMRP in VLANs.....	79
10.1 Definition of a VLAN Context	79
10.2 GMRP Participants and GIP Contexts.....	79
10.3 Context identification in GMRP PDUs	80
10.4 Default Group filtering behavior and GMRP propagation	80
11. VLAN topology management.....	82
11.1 Static and dynamic VLAN configuration	82
11.2 GARP VLAN Registration Protocol.....	83
11.3 Conformance to GVRP	88
11.4 Procedural model	89
12. Bridge management	90
12.1 Management functions.....	90
12.2 Managed objects	91
12.3 Data types	91
12.4 Bridge Management Entity.....	92
12.5 MAC entities.....	95
12.6 Forwarding process.....	95
12.7 Filtering Database	99
12.8 Bridge Protocol Entity	104
12.9 GARP Entities.....	111
12.10 Bridge VLAN managed objects.....	114
12.11 GMRP entities.....	124
12.12 MST configuration entities	126
13. The Multiple Spanning Tree Protocol (MSTP)	131
13.1 Protocol design requirements.....	131
13.2 Protocol support requirements	132
13.3 MSTP overview	132
13.4 Relationship of MSTP to RSTP.....	138
13.5 Modeling an MST Region as a single RSTP Bridge	139
13.6 STP and RSTP compatibility	140
13.7 MST Configuration Identification	141
13.8 MST Regions	142
13.9 Spanning Tree Priority Vectors	143
13.10 CIST Priority Vector calculations.....	144
13.11 MST Priority Vector calculations	146
13.12 Port Role assignments.....	148
13.13 Stable connectivity.....	148

13.14 Communicating Spanning Tree information	150
13.15 Changing Spanning Tree information.....	151
13.16 Changing Port States.....	152
13.17 Updating learned station location information	157
13.18 MSTP and point-to-point links	158
13.19 Multiple Spanning Tree state machines.....	158
13.20 Notational conventions used in state diagrams	160
13.21 State machine timers	160
13.22 MSTP performance parameters	161
13.23 Per-Bridge variables	162
13.24 Per-Port variables.....	164
13.25 State machine conditions and parameters.....	169
13.26 State machine procedures	172
13.27 The Port Timers state machine	179
13.28 Port Receive state machine.....	179
13.29 Port Protocol Migration state machine	180
13.30 Bridge Detection state machine	180
13.31 Port Transmit state machine	180
13.32 Port Information state machine.....	182
13.33 Port Role Selection state machine	183
13.34 Port Role Transitions state machine	183
13.35 Port State Transition state machine	187
13.36 Topology Change state machine.....	187
13.37 Performance	188
 14. Use of BPDUs by MSTP	 190
14.1 BPDUs Structure	190
14.2 Encoding of parameter types	190
14.3 BPDUs formats and parameters	192
14.4 Validation of received BPDUs	193
14.5 Transmission of BPDUs	193
14.6 Encoding and decoding of STP Configuration, RST, and MST BPDUs	194
 Annex A (normative) PICS proforma.....	 197
 Annex B (informative) Shared and Independent VLAN Learning.....	 225
 Annex C (informative) MAC method dependent aspects of VLAN support	 233
 Annex D (informative) Background to VLANs	 265
 Annex E (informative) Interoperability considerations	 266
 Annex F (informative) Frame translation considerations	 278
 Annex G (informative) Priority	 279
 Annex H (informative) Bibliography	 284

IEEE Standard for Local and metropolitan area networks—

Virtual Bridged Local Area Networks

1. Overview

IEEE 802® Local Area Networks (LANs)¹ of all types can be connected together with Media Access Control (MAC) Bridges, as specified in IEEE Std 802.1D™.^{2,3} This standard defines the operation of Bridges that permit the definition, operation, and administration of Virtual LANs (VLANs) within Virtual Bridged Local Area Networks.

1.1 Scope

For the purpose of compatible interconnection of information technology equipment using the IEEE 802 MAC Service supported by interconnected IEEE 802 standard LANs using different or identical media access control methods, this standard specifies the operation of MAC Bridges that support Virtual LANs (VLANs). To this end it

- a) Positions the support of VLANs within an architectural description of the MAC Sublayer;
- b) Defines the principles of operation of the VLAN-aware Bridge in terms of the support and preservation of the MAC Service, and the maintenance of Quality of Service;
- c) Specifies an Enhanced Internal Sublayer Service provided to the Media Access Independent functions that provide frame relay in a VLAN-aware Bridge;
- d) Establishes the principles and a model of Virtual Bridged Local Area Network operation;
- e) Identifies the functions to be performed by VLAN-aware Bridges, and provides an architectural model of the operation of a Bridge in terms of Processes and Entities that provide those functions;
- f) Specifies a frame format that allows a VLAN Identifier (VID) and priority information to be carried by VLAN tagged user data frames;
- g) Specifies the rules that govern the addition or removal of VLAN tags to and from user data frames;
- h) Specifies the rules that govern the ability to carry user data in either Canonical format or Non-canonical format in VLAN-tagged frames;

NOTE—The meanings of the terms *Canonical format* and *Non-canonical format* are discussed in IEEE Std 802.⁴

¹IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

²Information on references can be found in Clause 2.

³Throughout this standard, references to IEEE Std 802.1D, without qualification as to the date of publication, refer to the most recent revision or edition of the standard that is identified in the references section (Clause 2). In those cases where the reference is intended to be to an earlier published version of the standard, the reference is qualified by the publication date of that revision or edition.

⁴Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

- i) Establishes the requirements for automatic configuration of VLAN topology;
- j) Establishes the requirements for VLAN-aware Bridge Management in a Virtual Bridged Local Area Network, identifying managed objects and defining management operations;
- k) Defines the operation of the Multiple Spanning Tree algorithm and protocol (MSTP);
- l) Describes the protocols and procedures necessary to support interoperation between MST and SST Bridges in the same Virtual Bridged Local Area Networks;
- m) Specifies the requirements to be satisfied by equipment claiming conformance to this standard.

1.2 VLAN aims and benefits

VLANs aim to offer the following benefits:

- a) VLANs facilitate easy administration of logical groups of stations that can communicate as if they were on the same LAN. They also facilitate easier administration of moves, adds, and changes in members of these groups.
- b) Traffic between VLANs is restricted. Bridges forward unicast, multicast, and broadcast traffic only on individual LANs that serve the VLAN to which the traffic belongs.
- c) As far as possible, VLANs maintain compatibility with existing bridges and end stations.
- d) If all Bridge Ports are configured to transmit and receive untagged frames (3.39), bridges will work in plug-and-play IEEE Std 802.1D mode. End stations will be able to communicate throughout the network.

NOTE—Whether a Bridge will operate in IEEE Std 802.1D mode depends on the configuration of the various Port parameters (8.4) and the Filtering Database (8.8). A Bridge in its default configuration is transparent to untagged frames (3.39) but is not transparent to tagged frames (3.36), so the operation of such Bridges in the presence of tagged traffic differs from that of an IEEE Std 802.1D Bridge. If the configuration settings of Bridges are changed from the default values defined in this standard, then transparency with respect to untagged frames may also be affected.

2. Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

ANSI X3.159, American National Standards for Information Systems—Programming Language—C.⁵

IEEE Std 802®, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture.^{6, 7}

IEEE Std 802.1D™-1993 [ISO/IEC 10038:1993], IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local area networks—Media Access Control (MAC) bridges.

IEEE Std 802.1D™, 1998 Edition [ISO/IEC 15802-3:1998], 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.

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

IEEE Std 802.1F™, IEEE Standards for Local and Metropolitan Area Networks: Common Definitions and Procedures for IEEE 802 Management Information.

IEEE Std 802.1H™ [ISO/IEC 11802-5], IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and Metropolitan Area Networks—Technical Reports and Guidelines—Part 5: Media Access Control Bridging of Ethernet V2.0 in IEEE 802 Local Area Networks.

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

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

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

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

IETF RFC 1042 (Feb. 1988), *A Standard for the Transmission of IP Datagrams over IEEE 802 Networks*, Postel, J., and Reynolds, J.⁸

⁵ANSI publications are available from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

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

⁷The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

⁸Internet RFCs are retrievable by FTP at ds.internic.net/rfc/rfcnnnn.txt (where nnnn is a standard's publication number such as 1042), or call InterNIC at 1-800-444-4345 for information about receiving copies through the mail.

IETF RFC 1390 (Jan. 1993), *Transmission of IP and ARP over FDDI Networks*, Katz, D.

IETF RFC 1493 (July 1993), *Definitions of Managed Objects for Bridges*, Decker, E., Langille, P., Rijhsinghani, A., and McCloghrie, K.

IETF RFC 2104 (Feb. 1997), *HMAC: Keyed-Hashing for Message Authentication*, Krawczyk, H., Bellare, M., and Canetti, R.⁹

IETF RFC 2674 (Aug. 1999), *Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions*, Bell, E., Smith, A., Langille, P., Rijhsinghani, A., and McCloghrie, K.

ISO 6937-2, Information technology—Coded graphic character set for text communication—Latin alphabet.¹⁰

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

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

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

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

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

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

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

Metro Ethernet Forum (MEF) Technical Specification MEF 10, Ethernet Service Attributes Phase I, November 2004.¹¹

⁹IETF documents are available at <http://www.ietf.org>.

¹⁰ISO and ISO/IEC documents are available from the ISO Central Secretariat, 1 rue de Varembe, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

¹¹MEF publications are available at <http://www.metroethernetforum.org/TechSpec.htm>.

3. Definitions

For the purposes of this standard, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standards Terms* [B1]¹² should be referenced for terms not defined in this clause.

This standard makes use of the following terms defined in IEEE Std 802.1D:

- Active topology
- Bridge Port
- GARP Participant
- GARP Application
- GIP Context
- Group
- Port

The following terms are specific to this standard or to this standard and IEEE Std 802.1D:

3.1 Boundary Port: A Bridge Port attaching an MST Bridge to a LAN that is not in the same region.

3.2 Bridge: A VLAN-aware Bridge implemented in accordance with Clause 5 of this standard.

NOTE—This term defines a Bridge as specified in this standard. Where there is a need to refer generically to a bridge, being either a MAC Bridge as specified in IEEE Std 802.1D or a bridge as specified in this standard, the term is used without capitalization to indicate that the term is being used in the generic sense.

3.3 Bridged Local Area Network: A concatenation of individual IEEE 802 LANs interconnected by MAC Bridges.

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

3.4 Common and Internal Spanning Tree (CIST): The single Spanning Tree calculated by STP and RSTP and the logical continuation of that connectivity through MST Bridges and Regions, calculated by MSTP to ensure that all LANs in the Bridged Local Area Network are simply and fully connected.

3.5 Common Spanning Tree (CST): The single Spanning Tree calculated by STP, RSTP, and MSTP to connect MST Regions.

3.6 detagged frame: The detagged frame of an untagged frame is the frame itself. The detagged frame of a tagged frame or a priority-tagged frame is the frame that results from untagging the frame by the appropriate procedure.

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

¹²The numbers in brackets correspond to those of the bibliography in Annex H.

3.8 Frame: A unit of data transmission on an IEEE 802 LAN that conveys a MAC Protocol Data Unit (MPDU) and can cause a service indication with, at a minimum, destination and source MAC addresses and an MAC Service Data Unit (MSDU) or an MPDU that is the result of a service request with those parameters.

3.9 Frame relay: Forwarding of frames between the Ports of a Bridge.

3.10 Group: A Group associates all of the following:

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

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

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

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

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

3.12 Independent Virtual Local Area Network (VLAN) Learning (IVL): Configuration and operation of the Learning Process and the Filtering Database such that, for a given set of VLANs, if a given individual MAC Address is learned in one VLAN, that learned information is not used in forwarding decisions taken for that address relative to any other VLAN in the given set.

NOTE—In a Bridge that supports only IVL operation, the “given set of VLANs” is the set of all VLANs.

3.13 Independent Virtual Local Area Network (VLAN) Learning (IVL) Bridge: A Bridge that supports only Independent VLAN Learning.

3.14 Internal Spanning Tree (IST): The connectivity provided by the CIST within an MST Region.

3.15 Legacy region: A set of LANs connected such that there is physical connectivity between any pair of segments using only IEEE Std 802.1D conformant, VLAN-unaware MAC Bridges.

NOTE—If, in a Bridged Local Area Network containing both IEEE 802.1D and IEEE 802.1Q Bridges, all IEEE 802.1Q Bridges were to be removed, the result would be one or more Bridged Local Area Networks, each with its own distinct Spanning Tree. Each of those networks is a legacy region.

3.16 MST Bridge: A Bridge capable of supporting the CST, and one or more MSTIs, and of selectively mapping frames classified in any given VLAN to the CST or a given MSTI.

3.17 MST Configuration Table: A configurable table that allocates each and every possible VLAN to the Common Spanning Tree or a specific Multiple Spanning Tree Instance.

3.18 MST Region: A set of LANs and MST Bridges physically connected via Ports on those MST Bridges, where each LAN's CIST Designated Bridge is an MST Bridge, and each Port is either the Designated Port on one of the LANs or else a non-Designated Port of an MST Bridge that is connected to one of the LANs, whose MCID matches exactly the MCID of the Designated Bridge of that LAN.

NOTE—It follows from this definition that the MCID is the same for all LANs and Ports in the Region, and that the set of MST Bridges in the region are interconnected by the LANs.

3.19 Multiple Spanning Tree Algorithm and Protocol (MSTP): The Multiple Spanning Tree Algorithm and Protocol described in Clause 13 of this standard.

3.20 Multiple Spanning Tree Bridge Protocol Data Unit (MST BPDU): The MST BPDU specified in Clause 14 of this standard.

3.21 Multiple Spanning Tree (MST) Configuration Identifier: A name for, revision level, and a summary of a given allocation of VLANs to Spanning Trees.

NOTE—Each MST Bridge uses a single MST Configuration Table and Configuration Identifier.

3.22 Multiple Spanning Tree Instance (MSTI): One of a number of Spanning Trees calculated by MSTP within an MST Region, to provide a simply and fully connected active topology for frames classified as belonging to a VLAN that is mapped to the MSTI by the MST Configuration Table used by the MST Bridges of that MST Region.

3.23 Priority-tagged frame: A tagged frame whose tag header carries priority information but carries no VLAN identification information.

3.24 protocol group database: Specifies a group of protocols by assigning a unique protocol group identifier to all protocols of the same group.

3.25 protocol group identifier: Designates a group of protocols that are associated together when assigning a VID to a frame.

3.26 protocol template: A tuple of values that specify a data-link encapsulation format and an identification of the protocol layer above the data-link layer.

3.27 Rapid Spanning Tree Algorithm and Protocol (RSTP): The Rapid Spanning Tree Algorithm and Protocol described in Clause 17 of IEEE Std 802.1D.

3.28 Rapid Spanning Tree Bridge Protocol Data Unit (RST BPDU): The RST BPDU specified in Clause 9 of IEEE Std 802.1D.

3.29 Shared Virtual Local Area Network (VLAN) Learning (SVL): Configuration and operation of the Learning Process and the Filtering Database such that, for a given set of VLANs, if an individual MAC Address is learned in one VLAN, that learned information is used in forwarding decisions taken for that address relative to all other VLANs in the given set.

NOTE—In a Bridge that supports only SVL operation, the “given set of VLANs” is the set of all VLANs.

3.30 Shared Virtual Local Area Network (VLAN) Learning (SVL) Bridge: A type of Bridge that supports only Shared VLAN Learning.

3.31 Shared Virtual Local Area Network (VLAN) Learning (SVL)/Independent Virtual Local Area Network (VLAN) Learning (IVL) Bridge: An SVL/IVL Bridge is a type of Bridge that simultaneously supports both Shared VLAN Learning and Independent VLAN Learning.

3.32 Single Spanning Tree (SST) Bridge: A Bridge capable of supporting only a single spanning tree, the CST. The single spanning tree may be supported by the Spanning Tree Algorithm and Protocol (STP) defined in Clause 8 of IEEE Std 802.1D, 1998 Edition, or by the Rapid Spanning Tree Algorithm and Protocol (RSTP), defined in Clause 17 of IEEE Std 802.1D.

3.33 Spanning Tree: A simply and fully connected active topology formed from the arbitrary physical topology of connected Bridged Local Area Network components by relaying frames through selected bridge ports and not through others. The protocol parameters and states used and exchanged to facilitate the calculation of that active topology and to control the bridge relay function.

3.34 Spanning Tree Algorithm and Protocol (STP): The Spanning Tree Algorithm and Protocol described in Clause 8 of IEEE Std 802.1D, 1998 Edition.

3.35 Spanning Tree Bridge Protocol Data Unit (ST BPDU): A Bridge Protocol Data Unit specified for use by the Spanning Tree Algorithm and Protocol, i.e., a Configuration or Topology Change Notification BPDU as described in Clause 9 of IEEE Std 802.1D.

3.36 Tagged frame: A *tagged frame* is a frame that contains a tag header immediately following the Source MAC Address field of the frame or, if the frame contained a Routing Information field, immediately following the Routing Information field.

3.37 Tag header: A *tag header* allows priority information, and optionally, VLAN identification information, to be associated with a frame.

3.38 Traffic Class: Traffic Classes are numbered from zero through N-1, where N is the number of outbound queues associated with a given Bridge Port, and $1 \leq N \leq 8$, and each Traffic Class has a one-to-one correspondence with a specific outbound queue for that Port. Traffic Class 0 corresponds to nonexpedited traffic; non-zero Traffic Classes correspond to expedited classes of traffic. A fixed mapping determines, for a given priority associated with a frame and a given number of Traffic Classes, what Traffic Class will be assigned to the frame.

3.39 Untagged frame: An *untagged frame* is a frame that does not contain a tag header immediately following the Source MAC Address field of the frame or, if the frame contained a Routing Information field, immediately following the Routing Information field.

3.40 Virtual Bridged Local Area Network: A concatenation of individual IEEE 802 LANs interconnected by Bridges, including VLAN-aware Bridges.

3.41 VLAN-aware Bridge: A Bridge that recognizes frames with a VLAN tag and can insert or remove tag headers.

3.42 VLAN-tagged frame: A *VLAN-tagged frame* is a tagged frame whose tag header carries both VLAN identification and priority information.

3.43 VLAN-unaware Bridge: A Bridge that does not recognize VLAN-tagged frames.

4. Abbreviations

The following abbreviations are used in this standard:

BPDU	Bridge Protocol Data Unit (IEEE Std 802.1D)
CFI	Canonical Format Indicator (IEEE Std 802)
CIST	Common and Internal Spanning Tree
CST	Common Spanning Tree
EISS	Enhanced Internal Sublayer Service (6.6)
FCS	Frame Check Sequence
FID	Filtering Identifier (8.8.7, 8.9.3)
GARP	Generic Attribute Registration Protocol (IEEE Std 802.1D)
GID	GARP Information Declaration (IEEE Std 802.1D)
GIP	GARP Information Propagation (IEEE Std 802.1D)
GMRP	GARP Multicast Registration Protocol (Clause 10 of IEEE Std 802.1D)
GVRP	GARP VLAN Registration Protocol (Clause 11)
ISS	Internal Sublayer Service (6.4 of IEEE Std 802.1D)
IST	Internal Spanning Tree
IVL	Independent VLAN Learning (3.12)
LAN	Local Area Network (IEEE Std 802)
LLC	Logical Link Control (IEEE Std 802.2)
MAC	Medium Access Control (IEEE Std 802)
MCID	MST Configuration Identifier
MIB	Management Information Base (ISO/IEC 7498-4)
MS	MAC Service
MSDU	MAC Service Data Unit (ISO/IEC 15802-1)
MST	Multiple Spanning Tree
MST BPDU	Multiple Spanning Tree Bridge Protocol Data Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
NCFI	Non-Canonical Format Indicator
PCP	Priority Code Point
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement (Annex A)
PID	Protocol Identifier
PVID	Port VID
RED	Random Early Detection
RIF	Routing Information Field (IEEE Std 802.5)
RST BPDU	Rapid Spanning Tree Bridge Protocol Data Unit
RSTP	Rapid Spanning Tree Protocol
SST	Single Spanning Tree
ST BPDU	Spanning Tree Bridge Protocol Data Unit
STP	Spanning Tree Protocol
STPID	SNAP-encoded Tag Protocol Identifier (9.3)

SVL	Shared VLAN Learning (3.29)
TCI	Tag Control Information (9.3)
TPID	Tag Protocol Identifier (9.3)
VID	VLAN Identifier (7.2, 9.3)
VLAN	Virtual LAN
WRED	Weighted Random Early Detection

5. Conformance

This clause specifies the mandatory and optional capabilities provided by conformant implementations of this standard. An implementation can

- a) Compose all or part of the functionality of a system;
- b) Provide, as specified by this standard, one or more instances of the MAC Service to other functional entities whose specification is outside the scope of this standard;
- c) Provide, as specified by this standard, one or more instances of the MAC Internal Sublayer Service (ISS) to other implementations or instances of the same implementation that conform to this standard.

Accordingly, and as detailed in 5.3, this clause specifies conformance requirements for common systems and for functional components within systems, possibly connected to other system components with interfaces that are not otherwise accessible.

5.1 Requirements terminology

For consistency with existing IEEE and IEEE 802.1 standards, requirements placed upon conformant implementations of this standard are expressed using the following terminology:

- a) **Shall** is used for mandatory requirements;
- b) **May** is used to describe implementation or administrative choices (“may” means “is permitted to”, and hence, “may” and “may not” mean precisely the same thing);
- c) **Should** is used for recommended choices (the behaviors described by “should” and “should not” are both permissible but not equally desirable choices).

The PICS proforma (see Annex A) reflects the occurrences of the words “shall,” “may,” and “should” within the standard.

The standard avoids needless repetition and apparent duplication of its formal requirements by using **is**, **is not**, **are**, and **are not** for definitions and the logical consequences of conformant behavior. Behavior that is permitted but is neither always required nor directly controlled by an implementer or administrator, or whose conformance requirement is detailed elsewhere, is described by **can**. Behavior that never occurs in a conformant implementation or system of conformant implementations is described by **cannot**. The word **allow** is used as a replacement for the cliché “Support the ability for”, and the word **capability** means “can be configured to”.

5.2 Protocol Implementation Conformance Statement (PICS)

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

5.3 VLAN-aware Bridge requirements

An implementation of a VLAN-aware Bridge shall

- a) Conform to the requirements of IEEE Std 802.1D, as modified by the provisions of this standard;
- b) Conform to the relevant standard for the Media Access Control technology implemented at each Port in support of the MAC ISS, as specified in 6.4 and 6.5;
- c) Support the MAC Enhanced Internal Sublayer Service at each Port, as specified in 6.6 and 6.7;

- d) Implement an IEEE 802.2 conformant LLC class with Type 1 operation as required by 8.2;
- e) Relay and filter frames as described in 8.1 and specified in 8.5, 8.6, 8.7, and 8.8;
- f) On each Port, support at least one of the permissible values for the Acceptable Frame Types parameter, as defined in 6.7;
- g) Support the following on each Port that supports untagged and priority-tagged frames:
 - 1) A Port VLAN Identifier (PVID) value (6.7);
 - 2) Configuration of at least one VLAN whose untagged set includes that Port (8.8.2);
 - 3) Configuration of the PVID value via management operations (12.10);
 - 4) Configuration of Static Filtering Entries via management operations (12.7).
- h) Allow tag headers to be inserted, modified, and removed from relayed frames, as specified in 8.1 and Clause 9, as required by the value(s) of the Acceptable Frame Types parameter supported on each Port, and by the ability of each Port to transmit VLAN-tagged and/or untagged frames;
- i) Allow automatic configuration and management of VLAN topology using the Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) (Clause 11) on all Ports;
- j) Allow static and dynamic configuration information for at least one VLAN, by means of Static and Dynamic VLAN Registration Entries in the Filtering Database (8.11);
- k) Support at least one Filtering Identifier (FID) (6.4, 8.11.3, 8.11.7, and 8.11.8);
- l) Allow allocation of at least one VID to each FID that is supported (6.4, 8.11.3, 8.11.7, and 8.11.8).

NOTE—Under some circumstances, the ability for VLAN-aware Bridges to successfully interoperate depends on the number of FIDs supported and on the number of VIDs that can be allocated to each FID. These circumstances are discussed in Annex B, along with interoperability implications.

5.3.1 VLAN-aware Bridge options

An implementation of a VLAN-aware Bridge may

- a) Support MST operation (5.3.1.1);
- b) Support Port-and-Protocol-based VLAN classification (5.3.1.2), including multiple VID values per port, administrative control of the values of the multiple VIDs, and a Protocol Group Database.
- c) Support Extended Filtering Services (6.6.5 of IEEE Std 802.1D) and the operation of GARP Multicast Registration Protocol (GMRP) (Clause 10 of IEEE Std 802.1D) as modified by Clause 10 of this standard;
- d) Allow the Filtering Database to contain Static and Dynamic VLAN Registration Entries (8.8) for more than one VLAN, up to a maximum of 4094 VLANs;

NOTE—The maximum number of VLANs that can be supported is 4094 rather than 4096, as the VID values 0 and FFF are reserved, as indicated in Table 9-2. As conformance to this standard is only with regard to externally visible protocol behavior, this limit on the number of VLANs that can be supported does not imply any such limitation with regard to the internal architecture of a Bridge.

- e) On each Port, support all of the permissible values for the Acceptable Frame Types parameter, as defined in 8.3, and support configuration of the parameter value via management;
- f) Support enabling and disabling of Ingress Filtering (6.7);
- g) Allow configuration of more than one VLAN whose untagged set includes that Port (8.8.2);
- h) Support the management functionality defined in Clause 12;
- i) Support more than one FID (8.8);
- j) Allow allocation of more than one VID to each supported FID (8.8, 8.8.7);
- k) Allow configuration of VLAN Learning Constraints (8.8.7, 12.10.3);
- l) Allow configuration of fixed VID to FID allocations (8.8.7, 12.10.3);
- m) Allow configuration of the Restricted_Group_Registration parameter (IEEE Std 802.1D) for each Port of the Bridge;
- n) Support the ability to configure the value of the Restricted_VLAN_Registration parameter (11.2.3.2.3) for each Port of the Bridge.

5.3.1.1 Multiple Spanning Tree (MST) operation (optional)

A VLAN-aware Bridge implementation in conformance to the provisions of this standard for an MST Bridge (5.3.1, 8.3, 8.4, 8.6.1, 8.9, 8.10, 11.2, 11.3.1, Clause 13, and Clause 14) shall:

- 1) Support the Multiple Spanning Tree Protocol (MSTP) as specified in Clause 13;
- 2) Support the Common and Internal Spanning Tree (CIST) plus a stated maximum number of Multiple Spanning Tree Instances (MSTIs), where that number is at least 2 (8.9) and at most 64 (13.14);

NOTE—In other words, a conformant MST Bridge supports a minimum of three spanning tree instances—the CIST and at least two additional MSTIs.

- 3) Support a stated maximum number of FIDs not less than the number of MSTIs (8.9);
- 4) Support the ability to associate each FID to a spanning tree (8.9.3);
- 5) Support the transmission and reception of MST Configuration Identifier information (8.9.2).
- 6) Support a Port State for each Port for each spanning tree instance supported (8.4, 13.35);
- 7) Support operation of spanning tree protocol for each spanning tree instance and Port (8.10, 13);
- 8) Use the Bridge Group Address as specified in 8.13.3;
- 9) Support the default values for Bridge Forward Delay and Bridge Priority parameters specified in 13.23;
- 10) Support the operation of GVRP in each supported spanning tree context (11.2.3.3, 11.2.3.4);
- 11) Support the Bridge management functions for the bridge protocol entity for each supported spanning tree, independently (12.8)
- 12) Support, in particular, management of the bridge priority parameters, and of the port priority and path cost parameters for every port, independently for each supported spanning tree (12.8.1.1, 12.8.1.3, 13.24);
- 13) Support VLAN management functions for each supported spanning tree (12.10.1 and 12.11.1);
- 14) Support management of the MSTI configuration (12.12).

A VLAN-aware Bridge implementation in conformance to the provisions of this standard for an MST Bridge (5.3.1, 13) may

- 15) Support a greater number of FIDs than spanning trees (8.8.7).

5.3.1.2 Port-and-protocol-based VLAN classification (optional)

A VLAN-aware bridge component implementation in conformance to the provisions of this standard for port-and-protocol-based VLAN classification (5.3.1) shall

- 1) Support one or more of the following Protocol Classifications and Protocol Template formats: Ethernet, RFC_1042, SNAP_8021H, SNAP_Other, or LLC_Other (6.8);

and may

- 2) Support configuration of the contents of the Protocol Group Database.

5.4 MAC-specific bridging methods

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

- a) Not prevent communication between stations in a network.

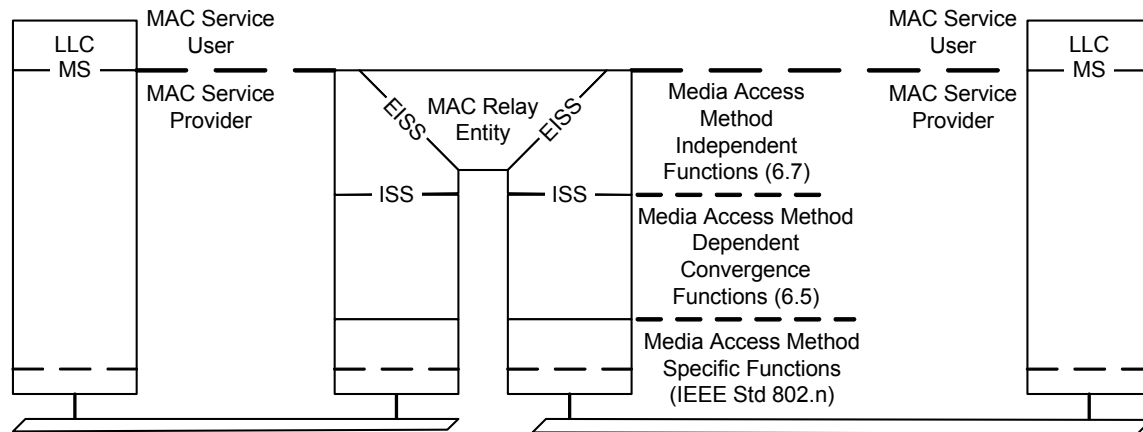
- b) Preserve the MAC Service.
- c) Preserve the characteristics of each bridging method within its own domain.
- d) Provide for the ability of both bridging techniques to coexist simultaneously on a LAN without adverse interaction.

Annex C of IEEE Std 802.1D defines one such MAC-specific bridging method, source routing, and that method is also a provision of this standard. Although this standard defines how source-routed frames can be transported in a VLAN environment, it does not attempt to specify VLAN aspects of the source routing bridging method.

6. Support of the MAC Service in VLANs

VLAN-aware MAC Bridges interconnect the separate IEEE 802 LANs that compose a Virtual Bridged Local Area Network by relaying and filtering frames between the separate MACs of the bridged LANs.

The position of a VLAN-aware Bridge's MAC Relay Entity (8.2) within the MAC Sublayer is shown in Figure 6-1.



NOTE—The notation “IEEE Std 802.n” in this figure indicates that the specifications for these functions can be found in the relevant standard for the media access method concerned; for example, n would be 3 (IEEE Std 802.3) in the case of Ethernet.

Figure 6-1—Internal organization of the MAC sublayer

The MAC Sublayer comprises:

- a) Media access method specific functions¹³ that realize transmission and reception of MAC Protocol Data Units (MPDUs);
- b) Media access method dependent convergence functions that use item a) to provide a media access method independent service;
- c) Media access method independent functions that use a media independent service to provide the same or another media independent service.

A VLAN-aware Bridge's MAC Relay Entity forwards frames between the instances of the media independent Enhanced Internal Sublayer Service (EISS, 6.4). The EISS is provided by the functions specified in 6.7 using the media independent Internal Sublayer Service (6.4). The convergence functions that provide the ISS using the media specific functions for each IEEE 802 LAN MAC type are specified in 6.5.

The provisions of Clause 6 of IEEE Std 802.1D apply to this standard, with the additions and modification defined in this clause.

6.1 Support of the MAC service

The MAC Service (MS) provided to end stations attached to a Virtual Bridged Local Area Network is the (unconfirmed) connectionless mode MAC Service defined in ISO/IEC 15802-1. The MAC Service is defined as an abstraction of the features common to a number of specific MAC Services; it describes the

¹³The media access method specific functions together with media access method dependent convergence functions that realize a MAC Service for use in end stations are specified for each IEEE 802 LAN media access control method or “MAC type” (e.g., IEEE 802.3, IEEE 802.11) by the relevant standard for that media access control method and are commonly referred to as “the MAC.”

transfer of user data between source and destination end stations, via MA-UNITDATA request primitives and corresponding MA-UNITDATA indication primitives issued at MAC Service access points. Each MA-UNITDATA request and indication primitive has four parameters: Destination Address, Source Address, MAC Service data unit (MSDU), and Priority.

The style of Bridge operation maximizes the availability of the MAC Service to end stations and assists in the maintenance of the network. It is therefore desirable that Bridges be capable of being configured in the network:

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

The operation of 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 network, 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 IEEE Std 802.1X.

6.2 Preservation of the MAC service

The MAC Service offered by a network consisting of LANs interconnected by Bridges is similar to that offered by a single LAN (see 6.3).

- a) Frames transmitted between end stations carry the MAC Addresses of the peer-end stations in their destination and source address fields, not an address of a Bridge. The Bridge relay is not directly addressed by communicating end stations.
- b) The MAC Addresses of end stations are not restricted by the network's topology or configuration.
- c) All MAC Addresses need to be unique within a VLAN, and within any set of VLANs for which filtering information is shared by a Bridge.

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 network 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, through denial of service by the Bridge, or through frame filtering by the Bridge. Changes in topology, caused by component failures, the addition or removal of components, or by administrative changes, are detected and signaled by the following means:

- a) Physical detection of component failure and signaling of that failure by the Enhanced Internal Sublayer Service (6.6 and 6.7);
- b) Detection of component failure through the operation of a spanning tree algorithm and protocol;
- c) Explicit signaling of reconfiguration events through the operation of a spanning tree algorithm and protocol.

Automatic reconfiguration can be achieved rapidly on the detection of a physical topology change (see Clause 17 of IEEE Std 802.1D), thus minimizing any service denial that is caused by the reconfiguration.

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 network. 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.

To minimize the effects of service denial caused by reconfiguration events, filtering information that has been dynamically learned can be modified when automatic reconfiguration takes place, or in preparation for future reconfiguration events (Clause 17 and 17.10 of IEEE Std 802.1D). However, filtering information that is statically configured cannot be modified in this way.

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 network component; or as a consequence of the movement of an end station; or as a consequence of an attempt to perform unauthorized access. These events are regarded as extraordinary. The operation of any additional protocol necessary to maintain the quality of the MAC Service is thus limited to the configuration of the network and is independent of individual instances of service provision.

NOTE 1—This is true only in circumstances where admission control mechanisms are not present, i.e., where the Bridges provide a “best effort” service.

NOTE 2—The operation of management on the Bridge can result in the Bridge being reset, either as a result of a specific Bridge reset operation or as a consequence of manipulating the Bridge’s configuration. From the point of view of service availability, resetting the Bridge is an extraordinary event that has a similar effect to physical removal of the Bridge from the network, followed by reinsertion of the Bridge into the network.

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 network necessitate frame discard for a limited period of time to maintain other aspects of Quality of Service (see 17.10 of IEEE Std 802.1D).
 - 5) The device attached to the Port is not authorized for access to the network.
 - 6) The configuration of Static Filtering Entries or Static VLAN Registration Entries in the Filtering Database (8.8.1, 8.8.2) disallows the forwarding of frames with particular destination addresses or VLAN classifications on specific Ports.

- 7) A flow metering algorithm (8.6.5) determines that discard is necessary.

NOTE—As Static Filtering Entries and Static VLAN Registration Entries are associated with particular Ports or combinations of Ports, there is a possibility that misconfiguration of such entries will lead to unintended frame discard during or following automatic reconfiguration of the network.

6.3.3 Frame misordering

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

NOTE 1—The operation of the Forwarding Process in Bridges (8.6) is such that the frame-ordering characteristics of the MAC Service are preserved.

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

NOTE 2—Where STP is in use (see Clause 8 of IEEE Std 802.1D, 1998 Edition), frame misordering cannot occur during normal operation. Where RSTP is in use (see Clause 17 of IEEE Std 802.1D), there is an increased probability that frames that are in transit through the network will be misordered, because a Bridge can buffer frames awaiting transmission through its Ports. The probability of misordering occurring as a result of such an event is dependent on implementation choices and is associated with Spanning Tree reconfiguration events. Some known LAN protocols, for example, LLC Type 2, are sensitive to frame duplication; in order to allow Bridges that support RSTP to be used in environments where sensitive protocols are in use, the forceVersion parameter (17.16.1 of IEEE Std 802.1D) can be used to force a Bridge that supports RSTP to operate in an STP-compatible manner. A more detailed discussion of misordering in RSTP can be found in F.2.4 of IEEE Std 802.1D.

6.3.4 Frame duplication

The MAC Service (9.2 of ISO/IEC 15802-1) permits a negligible rate of duplication of frames. The operation of Bridges introduces a negligible rate of duplication of user data frames.

The potential for frame duplication in a network arises through the possibility of duplication of received frames on subsequent transmission within a Bridge, or through the possibility of multiple paths between source and destination end stations.

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

NOTE—Where RSTP is in use (see Clause 17 of IEEE Std 802.1D), there is an increased probability that a Spanning Tree reconfiguration event can cause frames that are in transit through the network to be duplicated, because a Bridge can buffer frames awaiting transmission through its Ports. As the probability of duplication occurring as a result of such an event is small, and the frequency of Spanning Tree reconfiguration events is also small, the degradation of the properties of the MAC service caused by this source of frame duplication is considered to be negligible. A more detailed discussion of frame duplication in RSTP can be found in F.2.4 of IEEE Std 802.1D.

6.3.5 Transit delay

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

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

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

6.3.6 Frame lifetime

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

To enforce the maximum frame lifetime, a Bridge may be required to discard frames. Since the information provided by the MAC Sublayer to a Bridge does not include the transit delay already experienced by any particular frame, Bridges discard frames to enforce a maximum delay in each Bridge.

The value of the maximum bridge transit delay is based on both the maximum delays imposed by all Bridges in the network and the desired maximum frame lifetime. A recommended and an absolute maximum value are specified in Table 7-3 of IEEE Std 802.1D.

6.3.7 Undetected frame error rate

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

The FCS calculated for a given service data unit is dependent on the MAC method employed. It is therefore necessary to recalculate the FCS within a Bridge providing a relay function between IEEE 802 LAN MACs of dissimilar types if differences in the method of calculation and/or the coverage of the FCS, or changes to the data that is within the coverage of the FCS, would lead to a different FCS being calculated for the service data unit by the two MAC methods. This introduces the possibility of additional undetected errors arising from the operation of a Bridge. For frames relayed between LANs of the same MAC type, the Bridge shall not introduce an undetected frame error rate greater than that which would have been achieved by preserving the FCS.

NOTE—Application of the techniques described in Annex F of IEEE Std 802.1D allows an implementation to achieve an arbitrarily small increase in undetected frame error rate, even in cases where the data that is within the coverage of the FCS is changed. As a maintenance activity on this standard, revision of the wording of this requirement will be initiated, with a view to placing a quantitative limit on the increase in undetected frame error rate that is acceptable in a conformant implementation.

6.3.8 Maximum Service Data Unit Size

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

6.3.9 Priority

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

The MAC Sublayer maps the requested priority onto the priorities supported by the individual MAC method. The requested priority may be conveyed to the destination station.

The transmission delay experienced by a frame in a Bridge can be managed by associating a priority with the frame.

The transmission delay comprises

- a) A queuing delay until the frame becomes first in line for transmission on the Port, in accordance with the procedure for selecting frames for transmission described in 8.6.8;
- b) The access delay for transmission of the frame.

Queuing delays can be managed using priority. Access delays can be managed using priority in MAC methods that support more than one priority.

The priority associated with a frame can be signaled by means of the priority signaling mechanisms inherent in some IEEE 802 LAN MAC types. Since not all IEEE 802 LAN MAC types are able to signal the priority associated with a frame, VLAN-aware Bridges regenerate priority based on a combination of signaled information and configuration information held in the Bridge.

The Bridge maps the priority onto one or more traffic classes; Bridges that support more than one traffic class are able to support expedited classes of traffic. The Forwarding Process, 8.6, describes the use of priority and traffic classes in Bridges. Given the constraints placed on frame misordering in a Bridge, as expressed in 6.3.3, the mappings of priority and traffic class are static.

NOTE 1—The term “Traffic Class,” as used in this standard, is used only in the context of the operation of the priority handling and queueing functions of the Forwarding Process, as described in 8.6. Any other meanings attached to this term in other contexts do not apply to the use of the term in this standard.

The ability to signal priority in IEEE 802 LANs, coupled with a consistent approach to the mapping of priority to traffic classes, and of priority to the priority requested from the individual LAN or supporting service, allows consistent use of priority information to be made, according to the capabilities of the Bridges and MAC methods that are involved in the transmission path.

NOTE 2—This standard defines a frame format and associated procedures that can be used to carry priority information across LAN MAC types that are not able to signal priority.

Under normal circumstances, priority is not modified in transit through the relay function of a Bridge; however, there may be some circumstances where it is desirable for management purposes to control how priority is propagated. The Priority Regeneration Table (Table 6-3) provides the ability to map incoming priority values on a per-Port basis, under management control. In its default state, this table provides an identity mapping from priority values to Regenerated priority values; i.e., by default, the Regenerated priority is identical to the incoming priority.

6.3.10 Throughput

The total throughput provided by a network can be significantly greater than that provided by an equivalent single LAN. Bridges may localize traffic within the network by filtering frames. Filtering services available in bridged networks are described in 6.6 of IEEE Std 802.1D.

The throughput between end stations on individual LANs, communicating through a Bridge, can be lowered by frame discard in the Bridge due to the inability to transmit at the required rate on the LAN forming the path to the destination for an extended period.

6.4 Internal Sublayer Service

The Internal Sublayer Service (ISS) augments the specification of the MAC Service (ISO/IEC 15802-1) with elements necessary to the performance of the relay function. Within an end station, these additional elements are considered to be either below the MAC Service boundary, and pertinent only to the operation of the service provider; or local matters not forming part of the peer-to-peer nature of the MAC Service. The ISS excludes MAC-specific features and procedures whose operation is confined to an individual LAN.

NOTE—No new service primitives are defined. The `frame_check_sequence` is added to list of parameters associated with the `MA_UNITDATA.request` and `MA_UNITDATA.indication` primitives.

6.4.1 Service primitives and parameters

The ISS is specified by two unit-data primitives, an `M_UNITDATA.indication` and an `M_UNITDATA.request`, together with the parameters of those primitives. Each `M_UNITDATA` indication corresponds to the receipt of an error-free MAC frame from a LAN. A data request primitive is invoked to transmit a frame to an individual LAN.

NOTE 1—Detailed specifications of error conditions in received frames are contained in the relevant MAC standards; for example, FCS errors, length errors, and non-integral number of octets.

```
M_UNITDATA.indication    (
                           destination_address,
                           source_address,
                           mac_service_data_unit,
                           priority,
                           frame_check_sequence
                           )
```

```
M_UNITDATA.request      (
                           destination_address,
                           source_address,
                           mac_service_data_unit,
                           priority,
                           frame_check_sequence
                           )
```

The **`destination_address`** parameter is the address of an individual MAC entity or a group of MAC entities. The **`source_address`** parameter is the individual address of the source MAC entity. The **`mac_service_data_unit`** parameter is the service user data. The default **`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.

The **frame_check_sequence** parameter is explicitly provided with the M_UNITDATA.indication so that it can be used in a related M_UNITDATA.request. The parameter comprises the FCS value and sufficient information to determine whether the FCS value can be used. If the frame_check_sequence parameter is provided with an M_UNITDATA.request and the receiving and the transmitting service providers

- a) Use the same algorithm to determine the FCS; and
- b) Apply that algorithm to the same fields of the frame, i.e., the FCS coverage is the same; and
- c) The data that is within the coverage of the FCS remains the same;

the transmitting service provider should use the supplied FCS value (6.3.7, 6.6).

NOTE 2—There are two possibilities for recreating a valid FCS. The first is to generate a new FCS by algorithmically modifying the received FCS, based on knowledge of the FCS algorithm and the transformations that the frame has undergone between reception and transmission. The second is to rely on the normal MAC procedures to recalculate the FCS for the outgoing frame. The former approach can be preferable in terms of its ability to protect against increased levels of undetected frame errors. Annex F of IEEE Std 802.1D discusses these possibilities in more detail. The frame_check_sequence parameter of the Enhanced Internal Sublayer Service (6.6) is able to signal the validity, or otherwise, of the FCS; an unspecified value in this parameter in a data request indicates to the transmitting MAC that the received FCS is no longer valid, and the FCS must therefore be recalculated.

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.

NOTE 3—The ISS specification in this standard differs from that in IEEE Std 802.1D as it omits the frame_type and access_priority parameters. The frame_type is not required as the receipt of a frame other than a user data frame does not cause a data indication, nor are such frames transmitted by the media independent bridge functions. The mapping of the ISS to particular access methods specified by this standard includes derivation of the access_priority parameter (for those media that require it) from the ISS priority parameter.

6.4.2 Status parameters

The Internal Sublayer Service also makes available status parameters that reflect the operational state and administrative controls over each instance of the service provided.

The **MAC_Enabled** parameter is TRUE if use of the service is permitted; and is otherwise FALSE. The value of this parameter is determined by administrative controls specific to the entity providing the service, as specified in 6.5.

The **MAC_Operational** parameter is TRUE if the entity providing the service is capable of transmitting and receiving frames and its use is permitted by management, i.e., MAC_Enabled is also TRUE. Its value is otherwise FALSE. The value of this parameter is determined by the specific MAC procedures, as specified in 6.5.

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

- a) A MAC can inherently be working or not;
- b) If the MAC is working, its operational state can be administratively overridden.

6.4.3 Point-to-point parameters

The Internal Sublayer Service also makes available status parameters that reflect the point-to-point status of each instance of the service provided and provide administrative control over the use of that information.

If the **operPointToPointMAC** parameter is TRUE, the service is used as if it provides connectivity to at most one other system; if FALSE, the service is used as if it can provide connectivity to a number of systems.

The **adminPointToPointMAC** parameter can take one of three values. If it is

- a) **ForceTrue**, operPointToPointMAC shall be TRUE, regardless of any indications to the contrary generated by the service providing entity.
- b) **ForceFalse**, operPointToPointMAC shall be FALSE.
- c) **Auto**, operPointToPointMAC is determined by the service providing entity, as specified in 6.5.

The value of operPointToPointMAC is determined dynamically; i.e., it is re-evaluated whenever adminPointToPointMAC or the status of the service providing entity changes.

6.5 Support of the Internal Sublayer Service by specific MAC procedures

This subclause specifies support of the Internal Sublayer Service by MAC Entities that use specific IEEE 802 media access methods, including the mapping to the MAC protocol and procedures for each access method, and the encoding of the parameters of the service in MAC frames. The mapping is specified by reference to the IEEE 802 standards that specify each access method. The mapping draws attention to any special responsibilities of Bridges attached to LANs of that type. MAC control frames, typically frames that control some aspect of the operation of the MAC, i.e., frames that do not convey MAC user data, do not give rise to ISS data indications and are therefore not forwarded by a Bridge to any LAN other than that on which they originated.

Each MAC Entity examines all frames received on the LAN to which it is attached. All error-free received user data frames give rise to M_UNITDATA indication primitives. A frame that is in error, as defined by the relevant MAC specification, is discarded by the MAC Entity without giving rise to any M_UNITDATA indication.

Support of the ISS by the CSMA/CD access method is specified in 6.5 of IEEE Std 802.1D as amended by 6.5.1 of this standard.

Support of the ISS by the Wireless LAN (IEEE Std 802.11) access method is specified in 6.5 of IEEE Std 802.1D.

Support of the ISS by the Token Ring (IEEE Std 802.5) access method is specified in 4.1.13.2 of IEEE Std 802.5, with the following additions:

- a) Following an M_UNITDATA.request, the priority parameter referenced by that clause shall be set equal to the value of the priority parameter of the ISS as specified in this standard. The column marked “8802-5 (default)” in Table 6-1 should be used to derive the access priority from the priority, but the column marked “8802-5 (alternate)” may be used for backwards compatibility with equipment manufactured in accordance with IEEE Std 802.1D, 1993 Edition. The use of this alternate mapping reduces the number of available access priority values to three. The frame type of each frame resulting from an M_UNITDATA.request shall be LLC, and the receipt of frames of other types shall not result in an M_UNITDATA.indication.
- b) Following receipt of a frame, the priority parameter signaled in the corresponding M_UNITDATA.indication shall be regenerated from the priority specified in 4.1.13.2 of IEEE Std 802.5 using a Priority Regeneration Table for the MAC instance. This specifies the regenerated priority for each of the eight possible received values (0 through 7). Table 6-2 defines default values. If these are modified by management, the value of the table entries may be independently set for each MAC instance and value of received priority, and may use the full range of values in the parameter ranges specified.

Table 6-1—FDDI and Token Ring access priorities

priority	access priority		
	8802-5 (default)	8802-5 (alternate)	FDDI
0	0	4	0
1	1	4	1
2	2	4	2
3	3	4	3
4	4	4	4
5	5	5	5
6	6	6	6
7	6	6	6

NOTE—It is important that the regeneration and mapping of priority be consistent with the end-to-end significance of that priority in the network. Within a given Bridge, the values chosen for the Priority Regeneration Table for a given Port should be consistent with the priority to be associated with traffic received through that Port across the rest of the network, and should generate appropriate access priority values for each media access method on transmission.

Table 6-2—FDDI and Token Ring priority regeneration

Received priority	Default regenerated priority	Range
0	0	0–7
1	1	0–7
2	2	0–7
3	3	0–7
4	4	0–7
5	5	0–7
6	6	0–7
7	7	0–7

Support of the ISS by the FDDI access methods is specified in 6.5 of IEEE Std 802.1D. The priority parameter referenced by that clause shall be set equal to the value of the priority parameter of the ISS as specified in this standard. The column marked “FDDI” in Table 6-1 should be used to derive the access priority from the priority. A Priority Regeneration Table for the MAC instance shall be used to determine the priority parameter of each M_UNITDATA.indication as specified above for Token Ring.

6.5.1 Support of the Internal Sublayer Service by IEEE Std 802.3 (CSMA/CD)

On receipt of an M_UNITDATA.request primitive that represents a tagged frame, the implementation is permitted to adopt either of the following approaches with regard to the operation of Transmit Data Encapsulation for frames whose length would, using the procedure as described, be less than 68 octets:

- a) Use the procedure as described in 6.5.1 of IEEE Std 802.1D. This procedure can result in tagged frames of less than 68 octets (but at least 64 octets) being transmitted; or
- b) Include additional octets before the FCS field in order for the transmitted frame length for such frames to be 68 octets. This procedure results in a minimum tagged frame length of 68 octets.

When a tagged frame of less than 68 octets in length is received on a CSMA/CD LAN segment, and is forwarded as an untagged frame, the provisions of 6.5.1 of IEEE Std 802.1D, result in additional octets being included before the FCS field on transmission in order that the transmitted frame length meets the minimum frame size requirements of 3.2.7 in IEEE Std 802.3.

6.6 Enhanced Internal Sublayer Service

The EISS is derived from the ISS (see 6.4) by augmenting that specification with elements necessary to the operation of the tagging and untagging functions of a VLAN-aware Bridge (3.41). Within the attached end station, these 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.

The EISS provides the same service status and point-to-point parameters as the ISS (6.4.2, 6.4.3).

6.6.1 Service primitives

The unit-data primitives that define this service are

EM_UNITDATA.indication	(destination_address, source_address, mac_service_data_unit, priority, vlan_identifier, frame_check_sequence, canonical_format_indicator, rif_information (optional))
EM_UNITDATA.request	(destination_address, source_address, mac_service_data_unit, priority, vlan_identifier, frame_check_sequence, canonical_format_indicator, rif_information (optional))

The **destination_address**, **source_address**, **mac_service_data_unit**, **priority**, and **frame_check_sequence** parameters are as defined for the ISS.

The **vlan_identifier** parameter carries the VLAN identifier (VID).

The **canonical_format_indicator** parameter indicates whether embedded MAC Addresses carried in the **mac_service_data_unit** parameter are in Canonical format or Non-canonical format. The value False indicates Non-canonical format. The value True indicates Canonical format.

NOTE—The meanings of the terms “Canonical format” and “Non-canonical format” are discussed in IEEE Std 802.

The **rif_information** parameter is present if a tag header containing a Routing Information Field (RIF) is present (indication primitive) or requested (request primitive). Its value is equal to the value of the RIF.

6.6.2 Status parameters

The EISS also makes available the **MAC_Enabled** and **MAC_Operational** status parameters that reflect the operational state and administrative controls over each instance of the service provided. The values of these parameters are mapped directly from the values made available by the ISS (6.4.2).

6.6.3 Point-to-point parameters

The EISS also makes available the **operPointToPointMAC** and **adminPointToPointMAC** status parameters that reflect the point-to-point status of each instance of the service provided and provide administrative control over the use of that information. The values of these parameters are mapped directly from the values made available by the ISS (6.4.3).

6.7 Support of the EISS

The EISS is supported by tagging and detagging functions that in turn use the ISS (6.4, 6.5). Any given instance of the EISS shall be supported by using the VLAN tag type specified in 9.5. Each Bridge Port shall support the following parameters for use by these functions:

- a) an Acceptable Frame Types parameter with at least one of the following values:
 - 1) *Admit Only VLAN-tagged frames*;
 - 2) *Admit Only Untagged and Priority-tagged frames*;
 - 3) *Admit All frames*.
- b) a PVID parameter for port-based VLAN classification;

and may support the following parameter:

- c) a VID Set for port-and-protocol-based classification (6.8).

All three values for Acceptable Frame Types may be supported; if so, they shall be configurable using the management operations defined in Clause 12, and the default shall be *Admit All Frames*. A frame is treated as Untagged if the initial octets of the **mac_service_data_unit** parameter do not contain a VLAN tag of the type used to support the EISS (9.5), as Priority-tagged if the value contained in the VID field of the VLAN tag is zero, and as VLAN-tagged if the value is non-zero.

The PVID and VID Set shall contain valid VID values (Table 9-2) and may be configured by management. If they have not been explicitly configured, the PVID shall assume the value of the default PVID defined in Table 9-2 and the VID Set shall be empty.

NOTE—The default behavior of a Bridge that supports port-and-protocol-based classification is the same as that of a Bridge that supports only port-based classification, since all the Protocol Group Identifiers in the VID Set for each Port assign the same VID as the PVID.

6.7.1 Data indications

On receipt of an M_UNITDATA.indication primitive from the Internal Sublayer Service, the received frame is discarded if:

- a) The initial octets of the mac_service_data_unit do not contain a valid VLAN tag header (9.3) of the type used to support the EISS (9.5), and the Acceptable Frame Types is *Admit Only VLAN-tagged frames*; or,
- b) The initial octets of the mac_service_data_unit do not contain a valid VLAN tag header (9.3) of the type used to support the EISS (9.5), and
 - 1) The VID value is FFF, reserved in Table 9-2 for future implementation use; or
 - 2) The VID value is 000 (indicating priority-tagged), and the Acceptable Frame Types is *Admit Only VLAN-tagged frames*; or
 - 3) The VID value is in the range 001-FFE, and the Acceptable Frame Types is *Admit Only Untagged and Priority-tagged frames*.

Otherwise an EM_UNITDATA.indication primitive is invoked, with parameter values determined as follows:

The **destination_address**, **source_address**, and **frame_check_sequence** parameters carry values equal to the corresponding parameters in the received data indication.

NOTE 1—The frame_check_sequence parameter of the data indication carries the FCS value contained in the received frame. The original FCS associated with a frame is invalidated if there are changes to any fields of the frame, if fields are added or removed, or if bit ordering or other aspects of the frame encoding have changed. An invalid FCS is signaled in the E-ISS by an unspecified value in the frame_check_sequence parameter of the data request primitive. This signals the need for the FCS to be regenerated according to the normal procedures for the transmitting MAC. The options for regenerating the FCS under these circumstances are discussed in Annex F of IEEE Std 802.1D.

The value of the **mac_service_data_unit** parameter is as follows:

- a) If the frame is tagged, then the value used is equal to the value of the received mac_service_data_unit following removal of the tag header.
- b) Otherwise, the value used is equal to the value of the received mac_service_data_unit.

The value of the **vlan_identifier** parameter is as follows:

- c) The value contained in the VID field, if the frame is VLAN-tagged;
- d) The value of the PVID for the Port, if the frame is untagged or Priority-tagged and port-and-protocol VLAN classification is not implemented;
- e) As determined by port-and-protocol-based VLAN classification (6.8) if that capability is implemented and the frame is untagged or Priority-tagged.

The value of the **priority** parameter is determined as follows:

- f) The value of the priority parameter is regenerated from the received priority, as specified in 6.7.3.

The value of the **canonical_format_indicator** parameter is determined as follows:

- g) If the frame is tagged, then the value is as specified in Clause 9.

- h) Otherwise, if the MAC entity that received the data indication was an ISO/IEC 8802-5 Token Ring MAC, then the parameter carries the value False.
- i) Otherwise, the parameter carries the value True.

The value of the **rif_information** parameter is determined as follows:

- j) If the frame is tagged, then the value is as specified in Clause 9.
- k) Otherwise, the parameter is not present.

NOTE 2—This field can be present only in tag headers received using IEEE Std 802.3/Ethernet or transparent FDDI MACs. The presence of one or more route descriptors indicates that there is source-routing information present in the received frame.

6.7.2 Data requests

On invocation of an EM_UNITDATA.request primitive by a user of the E-ISS, an M-UNITDATA.request primitive is invoked, with parameter values as follows:

The **destination_address**, **source_address**, and **priority** parameters carry values equal to the corresponding parameters in the received data request.

Unless the Bridge Port is a member of the untagged set (8.8.2) for the VLAN identified by the **vlan_identifier** parameter, then a tag header, formatted as necessary for the destination MAC type, is inserted as the initial octets of the **mac_service_data_unit** parameter. The values of the **vlan_identifier**, **priority**, **canonical_format_indicator**, and **rif_information** (if present) parameters are used to determine the contents of the tag header, in accordance with Clause 9.

If the Bridge Port is a member of the untagged set (8.8.2) for the VLAN identified by the **vlan_identifier** parameter, no tag header is inserted.

The remaining octets of the **mac_service_data_unit** parameter are those accompanying the EISS-request. If the data request is a consequence of relaying a frame and the MAC type of the Port differs from that used to receive the frame, they are modified, if necessary, in accordance with the procedures described in ISO/IEC 11802-5, IETF RFC 1042, and IETF RFC 1390. If the **canonical_format_indicator** parameter indicates that the **mac_service_data_unit** may contain embedded MAC Addresses in a format inappropriate to the destination MAC type, and no tag header is to be inserted, then the Bridge shall either

- a) Convert any embedded MAC Addresses in the **mac_service_data_unit** to the format appropriate to the destination MAC type; or
- b) Discard the EISS data request without issuing a corresponding ISS data request.

The value of the **frame_check_sequence** parameter is determined as follows:

- c) If the **frame_check_sequence** parameter received in the data request is either unspecified or still carries a valid value, then that value is used.
- d) Otherwise, the value used is either derived from the received FCS information by modification to take account of the conditions that have caused it to become invalid, or the unspecified value is used.

6.7.3 Regenerating priority

The priority of received frames is regenerated using priority information contained in the frame and the Priority Regeneration Table for the reception Port. For each reception Port, the Priority Regeneration Table has eight entries, corresponding to the eight possible values of priority (0 through 7). Each entry specifies, for the given value of received priority, the corresponding regenerated value.

For untagged frames, the priority parameter signaled in the corresponding M_UNITDATA.indication is taken to be the received priority. For tagged frames, the priority signaled in the PCP field of the tag header is taken to be the received priority.

NOTE 1—IEEE 802 LAN technologies signal a maximum of eight priority values. Annex G further explains the use of priority values and how they map to traffic classes.

Table 6-3 specifies default regenerated priority values for each of the eight possible values of the received priority. These default values shall be used as the initial values of the corresponding entries of the Priority Regeneration Table for each Port.

The values in the Priority Regeneration Table may be modified by management, as described in Clause 12. If this capability is provided, the value of the table entries shall be independently settable for each reception Port and for each value of received priority, and the Bridge shall have the capability to use the full range of values in the parameter ranges specified in Table 6-3.

NOTE 2—The regeneration and mapping of priority within the Bridge should be consistent with the end-to-end significance of that priority across the rest of the Bridged Local Area Network. The regenerated priority value is used:

- Via the traffic class table (8.6.6) to determine the traffic class for a given outbound Port, and
- Via fixed, MAC type-specific mappings (6.5) to determine the access priority that will be used for certain media access methods.

Table 6-3—Priority regeneration

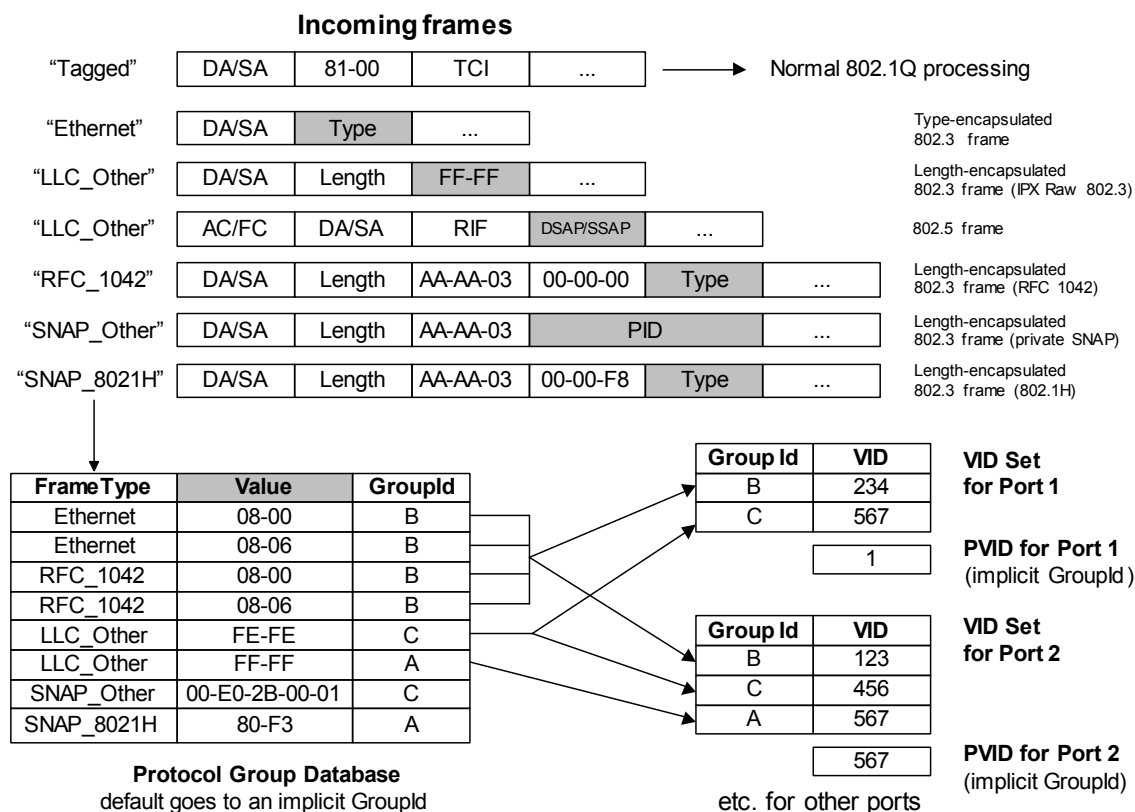
Received priority	Default regenerated priority	Range
0	0	0–7
1	1	0–7
2	2	0–7
3	3	0–7
4	4	0–7
5	5	0–7
6	6	0–7
7	7	0–7

6.8 Protocol VLAN classification

Each instance of the tagging and detagging functions that supports the EISS (6.7), and implements the optional port-and-protocol-based VLAN classification, shall implement a VID Set, each member of which associates values of a Protocol Group Identifier (6.8.2) with a VID. Each Untagged and Priority-tagged frame received is assigned a **vlan_identifier** equal to the VID Set value for the receiving Port and the Protocol Group Identifier selected by matching the received frame with a Protocol Template.

The **detagged_frame_type** parameter indicates the frame format. Its value is determined as follows:

- a) If the frame is Untagged or Priority Tagged, this parameter is present and indicates the link-layer encapsulation format of the *Detagged Frame*. The Detagged Frame of an Untagged Frame is the frame itself. The Detagged Frame of a Tagged Frame or Priority Tagged Frame is the frame that results from untagging the frame in accordance with the frame format described in Clause 9. The value of **detagged_frame_type** is as follows:
 - 1) Ethernet, if the Detagged Frame uses Type-encapsulated IEEE 802.3 format
 - 2) RFC_1042, if the Detagged Frame is of the format specified by 10.5 in IEEE Std 802-2001 for the encoding of an IEEE 802.3 Type Field in an IEEE 802.2/SNAP header (this supersedes the original definition, which appeared in RFC 1042)
 - 3) SNAP_8021H, if the Detagged Frame is of the format specified by IEEE Std 802.1H, 1997 Edition, for the encoding of an IEEE 802.3 Type Field in an IEEE 802.2/SNAP header
 - 4) SNAP_Other, if the Detagged Frame contains an LLC UI PDU with DSAP and SSAP fields equal to the LLC address reserved for SNAP and the 5-octet SNAP Protocol Identifier (PID) value is not in either of the ranges used for RFC_1042 or SNAP_8021H above
 - 5) LLC_Other, if the Detagged Frame contains both a DSAP and an SSAP address field in the positions specified by IEEE 802.2 Logical Link Control, but is not any of the formats described for LLC frames above
- b) Else the parameter is not present.



NOTE—The PID shown in this figure is a Protocol Identifier, as defined in 5.3 of IEEE Std 802. It is a 5-octet value consisting of a 3-octet OUI value followed by a 2-octet locally administered identifier.

Figure 6-2—Example of operation of port-and-protocol based classification

The **EtherType** value is present if the `detagged_frame_type` parameter is present and has the value Ethernet, RFC_1042, or SNAP_8021H. Its value is the value of the IEEE 802.3 Length/Type Field present in the Detagged Frame.¹⁴ The value is determined as follows:

- c) If the `detagged_frame_type` parameter is present and has the value Ethernet, RFC_1042, or SNAP_8021H, then this parameter is present and has the value of the IEEE 802.3 Type Field present in the Detagged Frame.
- d) Else the parameter is not present.

The **llc_saps** parameter is present if the `detagged_frame_type` parameter is present and has the value LLC_Other. Its value is determined as follows:

- e) If the `detagged_frame_type` parameter is present and has the value LLC_Other, then this parameter is present and its value is the pair of LLC IEEE 802.2 DSAP and SSAP address field values.
- f) Else the parameter is not present.

NOTE 1—A frame that is encapsulated using values of hex FF/FF in the position where an LLC header is to be expected (as defined by IEEE Std 802.2, 1998 Edition) is known as a “Novell IPX Raw” encapsulation. Such frames do not conform to IEEE Std 802.2, 1998 Edition, in that they do not include some of the other required LLC fields. For the purposes of this standard, they are treated as LLC_Other, regardless of whether they are legal LLC frames.

NOTE 2—Bridges are not required, for the purposes of this standard, to completely verify the format of frames as meeting IEEE Std 802.2 or not. They are only required to recognize the DSAP and SSAP fields of such frames.

The **snap_pid** parameter is present if the `detagged_frame_type` parameter is present and has the value SNAP_Other. Its value is determined as follows:

- g) If the `detagged_frame_type` parameter is present and has the value SNAP_Other, then the parameter is present and its value is the contents of the 5 octets following the LLC header, i.e., the PID field.
- h) Else the parameter is not present.

6.8.1 Protocol Templates

In a Bridge that supports Port-and-Protocol-based VLAN classification, a Protocol Template is a tuple that specifies a protocol to be identified in received frames. A Protocol Template has one of the following formats:

- a) A value “Ethernet” and a 16-bit IEEE 802.3 Type Field value
- b) A value “RFC_1042” and a 16-bit IEEE 802.3 Type Field value
- c) A value “SNAP_8021H” and a 16-bit IEEE 802.3 Type Field value
- d) A value “SNAP_Other” and a 40-bit PID value
- e) A value “LLC_Other” and a pair of IEEE 802.2 LSAP values: DSAP and SSAP

A Protocol Template *matches* a frame if

- f) The frame’s `detagged_frame_type` is Ethernet, the Protocol Template is of type Ethernet, and the frame’s IEEE 802.3 Type Field is equal to the value of the IEEE 802.3 Type Field of the Protocol Template, or
- g) The frame’s `detagged_frame_type` is RFC_1042, the Protocol Template is of type RFC_1042 and the frame’s IEEE 802.3 Type Field is equal to the IEEE 802.3 Type Field of the Protocol Template, or

¹⁴The use of Ethernet Type values as a means of protocol identification was defined in the specification of Ethernet V2.0 (The Ethernet, AA-K759B-TK, Digital Equipment, Intel, and Xerox Corps., Nov. 1982).

- h) The frame's `detagged_frame_type` is `SNAP_8021H`, the Protocol Template is of type `SNAP_8021H`, and the frame's IEEE 802.3 Type Field is equal to the IEEE 802.3 Type Field of the Protocol Template, or
- i) The frame's `detagged_frame_type` is `SNAP_Other`, the Protocol Template is of type `SNAP_Other`, and the frame's `snap_pid` is equal to the PID of the Protocol Template, or
- j) The frame's `detagged_frame_type` is `LLC_Other`, the Protocol Template is of type `LLC_Other`, and the frame's `llc_saps` matches the value of the DSAP and SSAP of the Protocol Template.

NOTE—If a port does not support Protocol Templates of the frame's `detagged_frame_type`, then no match will occur.

6.8.2 Protocol Group Identifiers

A Bridge that supports Port-and-Protocol-based VLAN classification shall support Protocol Group Identifiers.

A Protocol Group Identifier, shown as “Group Id” in Figure 6-2, designates a group of protocols that will be associated with one member of the VID Set of a Port. The association of protocols into groups is established by the contents of the Protocol Group Database, as described in 6.8.3. The identifier has scope only within a single bridge.

An implicit Protocol Group Identifier is assigned to frames that match none of the entries in the Protocol Group Database. Therefore, every incoming frame can be assigned to a Protocol Group Identifier.

6.8.3 Protocol Group Database

A Bridge that supports Port-and-Protocol-based VLAN classification shall support a single Protocol Group Database. The Protocol Group Database groups together a set of one or more Protocols by assigning them the same Protocol Group Identifier (6.8.2). Each entry of the Protocol Group Database comprises the following:

- a) A Protocol Template
- b) A Protocol Group Identifier

The Protocol Group Database specifies a mapping from Protocol Templates to Protocol Group Identifiers. If two entries of the Protocol Group Database contain different Protocol Group Identifiers, then their Protocol Templates must also be different.

The entries of the Protocol Group Database may be configured by management. A Bridge that supports Port-and-Protocol-based VLAN classification shall support at least one of the Protocol Template formats.

An implicit Protocol Group Database entry exists that matches all frames. This entry is invoked for frames that do not match the template of any of the other entries. It references an implicit Protocol Group Identifier that selects the PVID on each port. In this way, it is ensured that all incoming frames are matched by a Protocol Group Identifier and, hence, are assigned to a VID.

NOTE—If there are no entries in the Protocol Group Database, then the frame relay behavior of this Bridge is identical to the frame relay behavior of a Bridge having the same number of Ports that supports only Port-based VLAN classification.