

**IEEE Standard for  
Local and metropolitan area networks—  
Media Access Control (MAC) Bridges and  
Virtual Bridged Local Area Networks—  
Amendment 20: Shortest Path Bridging**

IEEE Computer Society

Sponsored by the  
LAN/MAN Standards Committee

---

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

29 June 2012

**IEEE Std 802.1aq™-2012**  
(Amendment to IEEE Std 802.1Q™-2011  
as amended by IEEE Std 802.1Qbe™-2011,  
IEEE Std 802.1Qbc™-2011, IEEE Std 802.1Qbb™-2011,  
IEEE Std 802.1Qaz™-2011, and  
IEEE Std 802.1Qbf™-2011)



**IEEE Std 802.1aq™-2012**  
(Amendment to IEEE Std 802.1Q™-2011  
as amended by IEEE Std 802.1Qbe™-2011,  
IEEE Std 802.1Qbc™-2011, IEEE Std 802.1Qbb™-2011,  
IEEE Std 802.1Qaz™-2011, and  
IEEE Std 802.1Qbf™-2011)

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

**Media Access Control (MAC) Bridges and  
Virtual Bridged Local Area Networks—**

**Amendment 20: Shortest Path Bridging**

Sponsor

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

Approved 29 March 2012

**IEEE-SA Standards Board**

**Abstract:** This amendment to IEEE Std 802.1Q-2011 specifies shortest path bridging of unicast and multicast frames, including protocols to calculate multiple active topologies that can share learned station information, and support of a virtual local area network (VLAN) by multiple, per topology VLAN identifiers (VIDs).

**Keywords:** Bridged Local Area Networks, IEEE 802.1aq, LANs, local area networks, MAC Bridges, metropolitan area networks, MSTP, Multiple Spanning Tree Protocol, Provider Bridged Local Area Networks, Shortest Path Bridging Protocol, SPB, 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 © 2012 by The Institute of Electrical and Electronics Engineers, Inc.  
All rights reserved. Published 29 June 2012. 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.

**PDF:** ISBN 978-0-7381-7262-0 STD97237  
**Print:** ISBN 978-0-7381-7368-9 STDPD97237

IEEE prohibits discrimination, harassment and bullying. For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.  
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.

**Notice and Disclaimer of Liability Concerning the Use of IEEE Documents:** IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. 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 IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. 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 any IEEE Standard document.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, 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 in its standards 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 ten years. When a document is more than ten years old and has not undergone a revision process, 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 its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

**Translations:** The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

**Official Statements:** A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. 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 of IEEE.

**Comments on Standards:** Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important to ensure that any responses to comments and questions also receive 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 comments or questions except in those cases where the matter has previously been addressed. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant [IEEE working group](#).

Comments on standards should be submitted to the following address:

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

**Photocopies:** 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 802.1aq-2012, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks—Amendment 20: Shortest Path Bridging.

This amendment to IEEE Std 802.1Q-2011 specifies shortest path bridging of unicast and multicast frames, including protocols to calculate multiple active topologies that can share learned station information, and support of a virtual local area network (VLAN) by multiple, per topology VLAN identifiers (VIDs).

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

## Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

## Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

## Updating of IEEE documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the [IEEE-SA website](#) or contact the IEEE at the address listed previously. For more information about the IEEE Standards Association or the IEEE standards development process, visit the [IEEE-SA website](#).

## Errata

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

## 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 by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA website <http://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or nondiscriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

## Participants

At the time this amendment was submitted to the IEEE-SA Standards Board for approval, the IEEE 802.1 Working Group had the following membership:

**Tony Jeffree, *Chair***  
**Glenn Parsons, *Vice Chair***  
**Donald Fedyk and Michael Seaman, *Editors***  
**Stephen Haddock, *Chair, Interworking Task Group***

Zehavit Alon  
Yafan An  
Ting Ao  
Peter Ashwood-Smith  
Christian Boiger  
Paul Bottorff  
Rudolf Brandner  
Craig Carlson  
Paul Congdon  
Rodney Cummings  
Claudio DeSanti  
Zhemin Ding  
Donald Eastlake  
Janos Farkas  
Norman Finn  
Ilango Ganga  
Geoffrey Garner  
Anoop Ghanwani

Mark Gravel  
Eric Gray  
Yingjie Gu  
Craig Gunther  
Hitoshi Hayakawa  
Hal Keen  
Srikanth Keesara  
Yongbum Kim  
Philippe Klein  
Oliver Kleineberg  
Michael Krause  
Lin Li  
Jeff Lynch  
Thomas Mack-Crane  
David Martin  
John Messenger  
John Morris  
Eric Multanen

David Olsen  
Donald Pannell  
Mark Pearson  
Joseph Pelissier  
Rene Raeber  
Karen T. Randall  
Josef Roese  
Dan Romascanu  
Jessy Rouyer  
Ali Sajassi  
Panagiotis Saltsidis  
Rakesh Sharma  
Kevin Stanton  
Robert Sultan  
Michael Johas Teener  
Patricia Thaler  
Chait Tumuluri  
Maarten Vissers

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

|                     |                   |                      |
|---------------------|-------------------|----------------------|
| Thomas Alexander    | Tetsushi Ikegami  | Satoshi Obara        |
| Butch Anton         | Noriyuki Ikeuchi  | Maximilian Riegel    |
| Danilo Antonelli    | Paul Isaacs       | Benjamin Rolfe       |
| Michael Bahr        | Atsushi Ito       | Jessy Rouyer         |
| Nancy Bravin        | Raj Jain          | Randall Safier       |
| William Byrd        | Tony Jeffree      | Panagiotis Saltsidis |
| Keith Chow          | Vincent Jones     | Peter Saunderson     |
| Charles Cook        | Shinkyō Kaku      | Bartien Sayogo       |
| Patrick Diamond     | Piotr Karocki     | Benson Schliesser    |
| Thomas Dineen       | Michael Kelsen    | Rich Seifert         |
| Donald Eastlake     | Stuart J. Kerry   | Gil Shultz           |
| Richard Eckard      | Yongbum Kim       | Kapil Sood           |
| Richard Edgar       | Bruce Kraemer     | Matthew Squire       |
| John Egan           | Paul Lambert      | Thomas Starai        |
| Jose Dominic Espejo | Juan L. Lazaro    | Walter Struppler     |
| Donald Fedyk        | Michael Lerer     | Robert Sultan        |
| Yukihiro Fujimoto   | William Lumpkins  | Joseph Tardo         |
| Devon Gayle         | Greg Luri         | William Taylor       |
| Gregory Gillooly    | Thomas Mack-Crane | Michael Johas Teener |
| Joel Goergen        | Elvis Maculuba    | Mark-Rene Uchida     |
| Randall Groves      | Wayne W. Manges   | Dmitri Varsanofiev   |
| Michael Gundlach    | David Martin      | Prabodh Varshney     |
| C. Guy              | Gary Michel       | John Vergis          |
| Stephen Haddock     | Jose Morales      | Ludwig Winkel        |
| David Hunter        | Michael S. Newman | Oren Yuen            |

When the IEEE-SA Standards Board approved this amendment on 29 March 2012, it had the following membership:

**Richard H. Hulett**, *Chair*  
**John Kulick**, *Vice Chair*  
**Robert M. Grow**, *Past Chair*  
**Judith Gorman**, *Secretary*

|                     |                       |                    |
|---------------------|-----------------------|--------------------|
| Satish Aggarwal     | Alexander Gelman      | Oleg Logvinov      |
| Masayuki Ariyoshi   | Paul Houzé            | Ted Olsen          |
| Peter Balma         | Jim Hughes            | Gary Robinson      |
| William Bartley     | Young Kuyn Kim        | Jon Walter Rosdahl |
| Ted Burse           | Joseph L. Koepfinger* | Mike Seavey        |
| Clint Chaplin       | David J. Law          | Yatin Trivedi      |
| Wael Diab           | Thomas Lee            | Phil Winston       |
| Jean-Philippe Faure | Hung Ling             | Yu Yuan            |

\*Member Emeritus

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

Richard DeBlasio, *DOE Representative*  
Michael Janezic, *NIST Representative*

Catherine Berger  
*IEEE Standards Program Manager, Document Development*

Kathryn Bennett  
*IEEE Standards Program Manager, Technical Program Development*

## Contents

|      |                                                            |    |
|------|------------------------------------------------------------|----|
| 1.   | Overview .....                                             | 2  |
| 1.3  | Introduction .....                                         | 2  |
| 2.   | Normative references .....                                 | 3  |
| 3.   | Definitions .....                                          | 4  |
| 4.   | Abbreviations .....                                        | 6  |
| 5.   | Conformance .....                                          | 7  |
| 5.4  | VLAN-aware Bridge component requirements.....              | 7  |
| 5.5  | C-VLAN component conformance .....                         | 8  |
| 5.6  | S-VLAN component conformance.....                          | 9  |
| 6.   | Support of the MAC Service .....                           | 10 |
| 6.5  | Quality of service maintenance .....                       | 10 |
| 6.9  | Support of the EISS .....                                  | 12 |
| 7.   | Principles of network operation .....                      | 15 |
| 7.1  | Network overview .....                                     | 15 |
| 7.2  | Use of VLANs .....                                         | 15 |
| 7.3  | Active topology .....                                      | 16 |
| 7.4  | <del>7.3</del> VLAN topology .....                         | 16 |
| 7.5  | <del>7.4</del> Locating end stations .....                 | 17 |
| 7.6  | <del>7.5</del> Ingress, forwarding, and egress rules ..... | 19 |
| 8.   | Principles of bridge operation .....                       | 21 |
| 8.1  | Bridge operation .....                                     | 21 |
| 8.2  | Bridge architecture .....                                  | 22 |
| 8.3  | Model of operation .....                                   | 22 |
| 8.4  | Active topologies, learning, and forwarding .....          | 23 |
| 8.6  | The Forwarding Process .....                               | 25 |
| 8.7  | The Learning Process .....                                 | 26 |
| 8.8  | The Filtering Database.....                                | 27 |
| 8.9  | MST, SPB, and ESP configuration information.....           | 33 |
| 8.10 | Spanning Tree Protocol Entity .....                        | 35 |
| 8.13 | Addressing .....                                           | 36 |
| 9.   | Tagged frame format .....                                  | 39 |
| 9.7  | Backbone Service Instance Tag Control Information .....    | 39 |
| 12.  | Bridge management .....                                    | 40 |
| 12.1 | Management functions .....                                 | 40 |
| 12.2 | VLAN-aware bridge objects.....                             | 40 |
| 12.3 | Data Types .....                                           | 40 |

|       |                                                                                                      |     |
|-------|------------------------------------------------------------------------------------------------------|-----|
| 12.7  | Filtering Database .....                                                                             | 40  |
| 12.10 | Bridge VLAN managed objects .....                                                                    | 40  |
| 12.12 | MST configuration entities .....                                                                     | 43  |
| 12.13 | Provider Bridge management .....                                                                     | 44  |
| 12.25 | Shortest Path Bridging managed objects .....                                                         | 44  |
| 13.   | Spanning Tree Protocols .....                                                                        | 58  |
| 13.1  | Protocol design requirements .....                                                                   | 59  |
| 13.2  | Protocol support requirements .....                                                                  | 60  |
| 13.3  | Protocol design goals .....                                                                          | 61  |
| 13.4  | RSTP overview .....                                                                                  | 61  |
| 13.5  | MSTP overview .....                                                                                  | 67  |
| 13.6  | <a href="#">SPB overview</a> .....                                                                   | 72  |
| 13.7  | <del>13.6</del> Compatibility and interoperability .....                                             | 73  |
| 13.8  | <del>13.7</del> MST Configuration Identifier .....                                                   | 74  |
| 13.9  | <del>13.8</del> Spanning Tree Priority Vectors .....                                                 | 75  |
| 13.10 | <del>13.9</del> CIST Priority Vector calculations .....                                              | 77  |
| 13.11 | <del>13.10</del> MST Priority Vector calculations .....                                              | 79  |
| 13.12 | <del>13.11</del> Port Role assignments .....                                                         | 81  |
| 13.13 | <del>13.12</del> Stable connectivity .....                                                           | 82  |
| 13.14 | <del>13.13</del> Communicating Spanning Tree information .....                                       | 83  |
| 13.15 | <del>13.14</del> Changing Spanning Tree information .....                                            | 84  |
| 13.16 | <del>13.15</del> Changing Port States with RSTP or MSTP .....                                        | 85  |
| 13.17 | <a href="#">Changing Port States with SPB</a> .....                                                  | 90  |
| 13.18 | <del>13.16</del> Managing spanning tree topologies .....                                             | 93  |
| 13.19 | <del>13.17</del> Updating learned station location information .....                                 | 94  |
| 13.20 | <del>13.18</del> Managing reconfiguration .....                                                      | 96  |
| 13.21 | <del>13.19</del> Partial and disputed connectivity .....                                             | 97  |
| 13.22 | <del>13.20</del> In-service upgrades .....                                                           | 97  |
| 13.23 | <del>13.21</del> Fragile bridges .....                                                               | 98  |
| 13.24 | <del>13.22</del> Spanning tree protocol state machines .....                                         | 99  |
| 13.25 | <del>13.23</del> State machine timers .....                                                          | 101 |
| 13.26 | <del>13.24</del> Per bridge variables .....                                                          | 103 |
| 13.27 | <del>13.25</del> Per port variables .....                                                            | 105 |
| 13.28 | <del>13.26</del> State machine conditions and parameters .....                                       | 117 |
| 13.29 | <del>13.27</del> State machine procedures .....                                                      | 119 |
| 13.30 | <del>13.28</del> The Port Timers state machine .....                                                 | 131 |
| 13.31 | <del>13.29</del> Port Receive state machine .....                                                    | 131 |
| 13.32 | <del>13.30</del> Port Protocol Migration state machine .....                                         | 132 |
| 13.33 | <del>13.31</del> Bridge Detection state machine .....                                                | 132 |
| 13.34 | <del>13.32</del> Port Transmit state machine .....                                                   | 133 |
| 13.35 | <del>13.33</del> Port Information state machine .....                                                | 134 |
| 13.36 | <del>13.34</del> Port Role Selection state machine .....                                             | 135 |
| 13.37 | <del>13.35</del> Port Role Transitions state machine .....                                           | 135 |
| 13.38 | <del>13.36</del> Port State Transition state machine .....                                           | 139 |
| 13.39 | <del>13.37</del> Topology Change state machine .....                                                 | 141 |
| 13.40 | <del>13.38</del> Layer 2 Gateway Port Receive state machine .....                                    | 142 |
| 13.41 | <del>13.39</del> Customer Edge Port Spanning Tree operation .....                                    | 142 |
| 13.42 | <del>13.40</del> Virtual Instance Port Spanning Tree operation .....                                 | 144 |
| 14.   | <a href="#">Encoding of Bridge Protocol Data Units (BPDUs)</a> <del>Use of BPDUs by MSTP</del> ..... | 145 |
| 14.1  | BPDU Structure .....                                                                                 | 145 |

|       |                                                                                                        |     |
|-------|--------------------------------------------------------------------------------------------------------|-----|
| 14.2  | Encoding of parameter types .....                                                                      | 147 |
| 14.3  | <del>14.5</del> Transmission of BPDUs .....                                                            | 151 |
| 14.4  | <del>14.6</del> Encoding and decoding of STP Configuration, RST, <del>and</del> MST, and SPT BPDUs.... | 151 |
| 14.5  | <del>14.4</del> Validation of received BPDUs .....                                                     | 154 |
| 14.6  | <a href="#">Validation and interoperability</a> .....                                                  | 155 |
| 17.   | Management Information Base (MIB) .....                                                                | 157 |
| 17.2  | Structure of the MIB .....                                                                             | 157 |
| 17.3  | Relationship to other MIBs .....                                                                       | 162 |
| 17.4  | Security considerations .....                                                                          | 162 |
| 17.7  | MIB modules .....                                                                                      | 163 |
| 20.   | Connectivity Fault Management protocols .....                                                          | 273 |
| 27.   | Shortest Path Bridging (SPB) .....                                                                     | 275 |
| 27.1  | Protocol design requirements .....                                                                     | 277 |
| 27.2  | Protocol support .....                                                                                 | 278 |
| 27.3  | Protocol design goals .....                                                                            | 278 |
| 27.4  | ISIS-SPB VLAN configuration .....                                                                      | 279 |
| 27.5  | ISIS-SPB information .....                                                                             | 282 |
| 27.6  | Calculating CIST connectivity .....                                                                    | 282 |
| 27.7  | Connectivity between regions in the same domain .....                                                  | 283 |
| 27.8  | Calculating SPT connectivity .....                                                                     | 284 |
| 27.9  | Loop prevention .....                                                                                  | 285 |
| 27.10 | SPVID and SPSourceID allocation .....                                                                  | 285 |
| 27.11 | Allocation of VIDs to FIDs .....                                                                       | 287 |
| 27.12 | SPBV SPVID translation .....                                                                           | 287 |
| 27.13 | VLAN topology management .....                                                                         | 288 |
| 27.14 | Individual addresses and SPBM .....                                                                    | 289 |
| 27.15 | SPBM group addressing .....                                                                            | 290 |
| 27.16 | Backbone service instance topology management .....                                                    | 291 |
| 27.17 | Equal cost shortest paths, ECTs, and load spreading .....                                              | 292 |
| 27.18 | Using SPBV and SPBM .....                                                                              | 292 |
| 27.19 | Security considerations .....                                                                          | 296 |
| 28.   | ISIS-SPB Link State Protocol .....                                                                     | 297 |
| 28.1  | ISIS-SPB control plane MAC .....                                                                       | 297 |
| 28.2  | Formation and maintenance of ISIS-SPB adjacencies .....                                                | 298 |
| 28.3  | Loop prevention .....                                                                                  | 299 |
| 28.4  | The Agreement Digest .....                                                                             | 299 |
| 28.5  | Symmetric shortest path tie breaking .....                                                             | 302 |
| 28.6  | Symmetric ECT framework .....                                                                          | 303 |
| 28.7  | Symmetric ECT .....                                                                                    | 304 |
| 28.8  | Predefined ECT Algorithm details .....                                                                 | 305 |
| 28.9  | ECT Migration .....                                                                                    | 306 |
| 28.10 | MAC Address registration .....                                                                         | 307 |
| 28.11 | Circuit IDs and Port Identifiers .....                                                                 | 308 |
| 28.12 | ISIS-SPB TLVs .....                                                                                    | 308 |
|       | Annex A (normative) PICS proforma—Bridge implementations.....                                          | 319 |

|                                                                  |     |
|------------------------------------------------------------------|-----|
| Annex F (informative) Shared and Independent VLAN Learning ..... | 321 |
| Annex M (informative) Bibliography .....                         | 324 |

## Figures

|                                                                                                                        |     |
|------------------------------------------------------------------------------------------------------------------------|-----|
| Figure 7-1—VLAN Bridging overview .....                                                                                | 15  |
| Figure 8-11—Forwarding Process functions .....                                                                         | 25  |
| Figure 12-3—SPB Management objects .....                                                                               | 45  |
| Figure 13-1—Diagrammatic conventions for spanning tree topologies.....                                                 | 64  |
| Figure 13-2—Physical topology and active topology .....                                                                | 65  |
| Figure 13-3—Port Roles and Port States .....                                                                           | 65  |
| Figure 13-4—A Backup Port.....                                                                                         | 66  |
| Figure 13-5—“Ring Backbone” example.....                                                                               | 66  |
| Figure 13-6—An MST Bridge network.....                                                                                 | 68  |
| Figure 13-7—CIST Priority Vectors, Port Roles, and MST Regions .....                                                   | 69  |
| Figure 13-8—MSTI Active Topology in Region 2 .....                                                                     | 70  |
| Figure 13-9—CIST and MSTI active topologies in Region 1 of the example network .....                                   | 83  |
| Figure 13-10—Agreements and Proposals .....                                                                            | 87  |
| Figure 13-11—CIST and MSTI Active Topologies in Region 2 of Figure 13-6 .....                                          | 88  |
| Figure 13-12—Enhanced Agreements.....                                                                                  | 89  |
| Figure 13-13—Spanning tree protocol state machines—overview and relationships.....                                     | 100 |
| Figure 13-14—MSTP overview notation .....                                                                              | 101 |
| Figure 13-15—Port Timers state machine.....                                                                            | 131 |
| Figure 13-16—Port Receive state machine .....                                                                          | 131 |
| Figure 13-17—Port Protocol Migration state machine.....                                                                | 132 |
| Figure 13-18—Bridge Detection state machine .....                                                                      | 132 |
| Figure 13-19—Port Transmit state machine.....                                                                          | 133 |
| Figure 13-20—Port Information state machine .....                                                                      | 134 |
| Figure 13-21—Port Role Selection state machine.....                                                                    | 135 |
| Figure 13-22—Disabled Port role transitions .....                                                                      | 136 |
| Figure 13-23—Port Role Transitions state machine—MasterPort.....                                                       | 136 |
| Figure 13-24—Port Role Transitions state machine—RootPort .....                                                        | 137 |
| Figure 13-25—Port Role Transitions state machine—DesignatedPort.....                                                   | 138 |
| Figure 13-26—Port Role Transitions state machine—AlternatePort and BackupPort .....                                    | 138 |
| Figure 13-27—Port State Transition state machine.....                                                                  | 139 |
| Figure 13-28—Topology Change state machine .....                                                                       | 141 |
| Figure 13-29—L2 Gateway Port Receive state machine.....                                                                | 142 |
| Figure 14-1— <a href="#">RST</a> , <a href="#">MST</a> , <a href="#">SPT</a> , and STP Configuration BPDU format ..... | 146 |
| Figure 14-2— <a href="#">STP TCN BPDU format</a> .....                                                                 | 146 |
| Figure 14-3— <del>Figure 14.2</del> —MSTI Configuration Message parameters and format .....                            | 153 |
| Figure 27-1—Configuring VLAN support in an SPT Region (example) .....                                                  | 280 |
| Figure 27-2—SPBM Group MAC Address—general format .....                                                                | 291 |
| Figure 27-3—SPBM Group MAC Addresses used by this standard.....                                                        | 291 |
| Figure 27-4—SPBV campus network example.....                                                                           | 293 |
| Figure 27-5—SPT Bridge Network using SPBM example .....                                                                | 295 |
| Figure 28-1—Agreement Digest field format .....                                                                        | 299 |
| Figure 28-2—MT-Capability TLV .....                                                                                    | 309 |
| Figure 28-3—SPB MCID sub-TLV .....                                                                                     | 309 |
| Figure 28-4—SPB Digest sub-TLV .....                                                                                   | 310 |
| Figure 28-5—SPB Base VLAN-Identifiers sub-TLV .....                                                                    | 311 |
| Figure 28-6—SPB Instance sub-TLV.....                                                                                  | 312 |
| Figure 28-7—SPB Instance Opaque ECT-ALGORITHM sub-TLV .....                                                            | 314 |
| Figure 28-8—SPB Link Metric sub-TLV.....                                                                               | 314 |
| Figure 28-9—SPB Adjacency Opaque ECT-ALGORITHM sub-TLV.....                                                            | 315 |
| Figure 28-10—SPBV MAC Address sub-TLV.....                                                                             | 315 |
| Figure 28-11—SPBM Service Identifier and Unicast Address sub-TLV .....                                                 | 317 |
| Figure F-6—Rooted-Multipoint with tagged interfaces .....                                                              | 322 |

|                                                               |     |
|---------------------------------------------------------------|-----|
| Figure F-7—SPBV VLAN Shared Learning and VID Translation..... | 323 |
|---------------------------------------------------------------|-----|

## Tables

|                                                                                                       |     |
|-------------------------------------------------------------------------------------------------------|-----|
| Table 8-6—Ageing time parameter value .....                                                           | 27  |
| Table 8-13— <del>Table 8-12</del> Standard LLC address assignment .....                               | 36  |
| Table 8-14—ISIS-SPB reserved addresses.....                                                           | 38  |
| Table 8-15—ISIS-SPB Recommended Address Usage .....                                                   | 38  |
| Table 9-3—Reserved I-SID values.....                                                                  | 39  |
| Table 13-1—Configuration Digest Signature Key .....                                                   | 74  |
| Table 13-2—Sample Configuration Digest Signature Keys.....                                            | 75  |
| Table 13-3—Bridge and Port Priority values .....                                                      | 93  |
| Table 13-4—Port Path Cost values.....                                                                 | 94  |
| Table 13-5—Timer and related parameter values .....                                                   | 102 |
| Table 17-1—Structure of the MIB modules .....                                                         | 157 |
| Table 17-7—IEEE8021-QBRIDGE MIB structure and relationship to IETF RFC 4363 and this<br>standard..... | 157 |
| Table 17-9—IEEE8021-PB MIB structure and relationship to this standard .....                          | 158 |
| Table 17-10—IEEE8021-MSTP MIB structure and relationship to this standard .....                       | 158 |
| Table 17-25—IEEE8021-SPB MIB structure and relationship to this standard .....                        | 159 |
| Table 27-1—Allocation of VIDs to FIDs and FIDs to MSTIDs in an SPT Region (example).....              | 279 |
| Table 28-1—Bridge Priority Masking.....                                                               | 305 |



# IEEE Standard for Local and metropolitan area networks—

## Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks—

### Amendment 20: Shortest Path Bridging

This amendment to IEEE Std 802.1Q™-2011 specifies changes to allow bridged frames to travel on the shortest path between their source and destination(s). Changes are applied to the base text of IEEE Std 802.1Q-2011 as amended by IEEE Std 802.1Qbe™-2011, IEEE Std 802.1Qbc™-2011, IEEE Std 802.1Qbb™-2011, IEEE Std 802.1Qaz™-2011, and IEEE Std 802.1Qbf™-2011.

***IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.***

***This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.***

NOTE—The editing instructions contained in this amendment define how to merge the material contained therein into the existing base standard and its amendments to form the comprehensive standard. Text shown in bold italics in this amendment defines the editing instructions necessary to changes to this base text. Three editing instructions are used: ***change***, ***delete***, and ***insert***. ***Change*** is used to make a change to existing material. The editing instruction specifies the location of the change and describes what is being changed. Changes to existing text may be clarified using ~~strikeout~~ markings to indicate removal of old material and underscore markings to indicate addition of new material. ***Delete*** removes existing material. ***Insert*** adds new material without changing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. Editorial notes will not be carried over into future editions of IEEE Std 802.1Q.<sup>1</sup>

<sup>1</sup>Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

## 1. Overview

### 1.3 Introduction

*Insert the following text after item bh) in 1.3:*

This standard specifies shortest path bridging of unicast and multicast frames, specifying protocols to calculate multiple active topologies that can share learnt station information, and support of a VLAN by multiple, per topology shortest path VLAN identifiers (SPVIDs). To this end it:

- bi) Describes the use of shortest paths to increase throughput and minimize transit delay, while introducing a negligible rate of frame misordering.
- bj) Requires that active topologies calculated by spanning tree protocols and Shortest Path Tree (SPT) protocols be stable, predictable, reproducible, reverse path congruent and unicast-multicast congruent to: permit learning of station location from the source addresses of all frames, simplify the detection and management of faults, and maintain the characteristics of the MAC Service provided.
- bk) Specifies the calculation of symmetric sets of shortest path trees (SPTs), each rooted at a bridge within an SPT Region comprising bridges operating compatible protocols and configurations.
- bl) Specifies the use of Bridge Protocol Data Units (BPDUs) to identify and bound SPT Regions, and to ensure loop-free interoperability with regions using the Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP).
- bm) Specifies both Shortest Path Bridging VID (SPBV) and Shortest Path Bridging MAC (SPBM):
  - 1) for SPBV, identifying each SPT by SPVID and locating end stations by source MAC address learning;
  - 2) for SPBM, identifying each SPT by VID and source MAC address and distributing end station location information explicitly.
- bn) Supports management selection of the Common Spanning Tree (CST), a Multiple Spanning Tree Instance (MSTI) or SPB for support of any given VLAN within an SPT Region.
- bo) Specifies a protocol that automatically assigns SPVIDs for each VLAN supported by SPBV.
- bp) Supports load sharing by equal cost trees (ECT) through the calculation of multiple SPT Sets, with each shortest path VLAN being assigned to one SPT Set.
- bq) Specifies ISIS-SPB: the use of and extensions to the Intermediate System to Intermediate System protocol (IS-IS) to calculate SPTs for both SPBV and SPBM.
- br) Describes the addressing of ISIS-SPB entities and specifies the group MAC Addresses they use.
- bs) Specifies the use of loop prevention (for SPBV and for multicast frames for SPBM) and loop mitigation (for unicast frames for SPBM).
- bt) Specifies an Agreement Protocol that prevents loops, specifying the necessary state information and computation as part of ISIS-SPB, and communicating agreement information for the CIST and (as a compact Digest) for SPTs in each BPDU.

## 2. Normative references

*Insert the following references into Clause 2 in alphanumeric order:*

IETF RFC 5120 (Feb. 2008) M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs).<sup>2</sup>

IETF RFC 5303 (Oct. 2008), Three-Way Handshake for IS-IS Point-to-Point Adjacencies.

IETF RFC 5305 (Oct. 2008), IS-IS Extensions for Traffic Engineering.

IETF RFC 6165 (Apr. 2011), Extensions to IS-IS for Layer-2 Systems.

ISO/IEC 9577:1999, Information technology — Protocol identification in the network layer.<sup>3</sup>

ISO/IEC 10589:2002, Information technology — Telecommunications and information exchange between systems — Intermediate System to Intermediate System intra-domain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service.

---

<sup>2</sup>Internet RFCs are retrievable by FTP at [ds.internic.net/rfc/rfcnnnn.txt](http://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.

<sup>3</sup>ISO/IEC publications are available from the ISO Central Secretariat (<http://www.iso.ch/>). ISO/IEC publications are also available in the United States from the American National Standards Institute (<http://www.ansi.org/>)

### 3. Definitions

*Insert the following definitions into Clause 3 in alphabetic order, number them appropriately, and renumber the subsequent definitions accordingly:*

**3.x Adjacency:** A neighbor in IS-IS. From Clause 3.6 of ISO 10589.

**3.x Agreement Protocol:** A protocol that uses control plane synchronisation between adjacent bridges to guarantee loop prevention, so enabling rapid transition to forwarding after network topology changes (13.16, 13.17).

**3.x Base VID:** The VID used to identify a VLAN in management operations in both SPBV and SPBM.

**3.x ECT Algorithm:** A Shortest Path Tree algorithm yielding a consistent result for a given root bridge when run by all bridges within an SPT Region.

**3.x Equal Cost Tree (ECT):** A unique instantiation of a Shortest Path Tree that uses a specific method to pick from equal cost alternatives. In networks that have more than one diverse path between nodes, different Shortest Path Trees from the same root node that have equal cost paths from the root node to leaf nodes are considered ECTs.

**3.x Multi-Topology (MT):** One of a set of independent topologies that IS-IS supports within an IS-IS domain. This MT extension can be used for a variety of purposes, such as an in-band management network “on top” of the original IS-IS topology, maintaining separate IS-IS routing domains for isolated topology islands within the network, or forcing a subset of an address space to follow a different topology.

**3.x Multi-Topology Identifier (MTID):** The identifier of an IS-IS MT.

**3.x Port State:** One of a number of possible combinations of per tree *forwarding* and *learning* variables, used by a spanning tree protocol or shortest path tree protocols for each Bridge Port, to enforce the active topology of that tree. There is port state for every tree and there could be many trees per port.

**3.x Rapid Spanning Tree (RST) Bridge:** A Bridge capable of supporting only a single spanning tree, the CST, by the Rapid Spanning Tree Algorithm and Protocol (RSTP), defined in Clause 13.

**3.x Shortest Path Bridging (SPB):** The method of bridging using shortest path trees for forwarding from each bridge. SPB is used for references that are applicable to all modes of Shortest Path Bridging, SPBM and SPBV.

**3.x Shortest Path Bridging MAC Mode (SPBM):** The Shortest Path Bridging method where all SPTs are rooted at a Backbone Edge Bridge (BEB). In frames with a group destination address the SPT is identified by a destination MAC address derived from the SPSourceID; in frames with an individual address the SPT is identified by a MAC address of the source BEB. This method does not use learning.

**3.x Shortest Path Bridging VID Mode (SPBV):** The Shortest Path Bridging method where VIDs (SPVIDs) are used to identify the SPTs for individual and group addresses. This method is learning capable.

**3.x Shortest Path First (SPF):** Abbreviation for the Dijkstra Shortest Path First Algorithm that is used in Link state protocols such as IS-IS.

**3.x Shortest Path Source Identifier (SPSourceID):** A 20-bit identifier of a bridge that is unique within a SPT Domain. SPSourceID is used to auto-create SPT Domain significant Group MAC Addresses utilizing the local address bit in SPBM (27.10).

**3.x Shortest Path Tree (SPT) Bridge:** A VLAN-aware Bridge capable of operating Shortest Path Bridging (SPB) protocols.

**3.x Shortest Path Tree (SPT) Domain:** A set of SPT Bridges that are interconnected by LANs and have the same configured IS-IS area address. An SPT Domain contains one or more SPT Regions each comprising some or all of the bridges in the Domain.

**3.x Shortest Path Tree (SPT) Region:** A set of LANs and SPT Bridges interconnected via Ports on those SPT Bridges, where each LAN's CIST Designated Bridge is an SPT Bridge, and each Port is either the Designated Port on one of the LANs, or else a non-Designated Port of an SPT Bridge that is connected to one of the LANs, whose MCID matches exactly the MST Configuration Identifier (MCID) or the Auxiliary MCID (27.4.1) of the Designated Bridge of that LAN.

**3.x Shortest Path Tree (SPT) Set:** A set of shortest path trees determined by one ECT Algorithm and capable of supporting one or more VLANs within an SPT Region (8.9.4, 13.6). The set is the union of all the shortest path trees from all sources to all other bridges using that single ECT Algorithm. A single SPT set is created for each ECT Algorithm. Active SPT Sets are identified by their {ECT Algorithm, FID} tuples.

**3.x Shortest Path VID (SPVID):** The identifier of both the VLAN and the SPT that is used for the transmission of a tagged frame in SPBV.

**3.x Spanning Tree Algorithm and Protocol (STP) Bridge:** A Bridge capable of supporting only a single spanning tree, the CST, by the Spanning Tree Algorithm and Protocol (STP) defined in Clause 8 of IEEE Std 802.1D, 1998 Edition.

**3.x SPB System Identifier:** A unique 6-byte value for each ISIS-SPB capable bridge and is equivalent to the IS-IS System ID. The System Identifier is used to identify unique bridges in the topology. For the purpose of this document this ID is the 6-byte Bridge Address (8.13.8).

## 4. Abbreviations

*Insert the following abbreviations into Clause 4 in alphabetic order:*

|          |                                 |
|----------|---------------------------------|
| ECT      | Equal Cost Tree                 |
| ISIS-SPB | IS-IS for SPBV and SPBM         |
| LSP      | Link State PDU                  |
| MT       | Multiple Topology               |
| PATHID   | Path Identifier                 |
| SPB      | Shortest Path Bridging          |
| SPT      | Shortest Path Tree              |
| SPVID    | Shortest Path VLAN Identifier   |
| SPBM     | Shortest Path Bridging MAC Mode |
| SPBV     | Shortest Path Bridging VID Mode |

## 5. Conformance

### 5.4 VLAN-aware Bridge component requirements

#### 5.4.1 VLAN-aware Bridge component options

*Change 5.4.1 as follows:*

An implementation of a VLAN-aware Bridge component may

- a) Support MST operation (5.4.1.1);
- b) Support Port-and-Protocol-based VLAN classification (5.4.1.2), including multiple VID values per port, administrative control of the values of the multiple VIDs, and a Protocol Group Database.
- c) Support CFM operation (5.4.1.4);
- d) [Support Shortest Path Bridging operation \(5.4.5\);](#)
- e) ~~+~~Support congestion notification (5.4.3);
- f) ~~+~~Support Priority-based Flow Control (5.11);
- g) ~~+~~Support Extended Filtering Services (6.16.5) and the operation of Multiple MAC Registration Protocol (MMRP, see 10.9) to support automatic configuration and management of MAC address information on all Ports (5.4.1.3);
- h) ~~+~~Allow the Filtering Database to contain Static and Dynamic VLAN Registration Entries (8.8) for more than one VID, up to a maximum of 4094 VIDs;
- i) [Allow translation of VIDs through support of the VID Translation Table or through support of both the VID Translation Table and Egress VID translation table on one or more Bridge Ports \(6.9\);](#)

NOTE 1—The maximum number of VIDs 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 VIDs that can be supported does not imply any such limitation with regard to the internal architecture of a Bridge.

- j) ~~+~~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;
- k) ~~+~~Support enabling and disabling of Ingress Filtering (6.9);
- l) ~~+~~Allow configuration of more than one VID whose untagged set includes that Port (8.8.2);
- m) ~~+~~Support the management functionality defined in Clause 12;
- n) ~~+~~Support more than one FID (8.8);
- o) ~~+~~Allow allocation of more than one VID to each supported FID (8.8, 8.8.8);
- p) ~~+~~Allow configuration of VLAN Learning Constraints (8.8.8, 12.10.3);
- q) ~~+~~Allow configuration of fixed VID to FID allocations (8.8.8, 12.10.3);
- r) ~~+~~Allow configuration of the Restricted\_MAC\_Address\_Registration parameter (10.12.2.3) for each port of the Bridge;
- s) ~~+~~Support the ability to configure the value of the Restricted\_VLAN\_Registration parameter (11.2.3.2.3) for each Port of the Bridge;
- t) ~~+~~Support forwarding and queuing for time-sensitive streams (5.4.1.5);
- u) ~~+~~Support SMIv2 MIB modules for the management of VLAN-aware Bridge capabilities (Clause 17);
- v) ~~+~~Support Multiple Stream Reservation Protocol (MSRP; Clause 35);
- w) ~~+~~Support the operation of MVRP (5.4.2, 11.2) as a New-only Participant;
- x) ~~+~~Support the MVRP Extension Management Information Base (MIB) module defined in 17.7.15;
- y) ~~+~~Support enhanced transmission selection (ETS) (see 5.4.1.6);
- z) ~~+~~Support DCBX (see 5.4.1.7).

NOTE 2—In previous versions of IEEE Std 802.1Q, the MIB modules were maintained by IETF (e.g., IETF RFC 4363 for the Q-BRIDGE MIB). For this standard, the relevant set of MIB modules required to manage a Bridge is contained in Clause 17.

*Insert the following subclause, 5.4.5, after 5.4.4:*

#### **5.4.5 Shortest Path Bridging operation (optional)**

A VLAN-aware Bridge implementation that conforms to the provisions of this standard for SPB in Clause 27 shall:

- a) Support SPB, in either VID mode (SPBV) or MAC mode (SPBM), as specified in Clause 27;
- b) Support the IS-IS Link State Protocol with procedures to ensure Loop Prevention as specified in Clause 28 to provide SPT computation for shortest path bridging;
- c) Encode, decode, and validate SPT BPDUs for the Agreement Protocol (13.17) and support Agreement Protocol logic in IS-IS as specified in Clause 28;
- d) Support at least three FIDs;
- e) Support the management functionality specified in Clause 12.

A VLAN-aware Bridge implementation in conformance to the provisions of this standard for SPB in Clause 27 may:

- f) Support both SPB VID mode (SPBV) and SPB MAC mode (SPBM);
- g) Support the SPB Management Information Base (MIB) module defined in 17.7.19;
- h) Support both the VID Translation Table and Egress VID translation table (6.9) on SPBV Boundary Ports.

### **5.5 C-VLAN component conformance**

*Change 5.5 as follows:*

A C-VLAN component comprises a VLAN-aware Bridge component with the EISS on all Ports supported by the use of a Customer VLAN tag (C-TAG) (6.8, 9.5).

A conformant implementation of a C-VLAN component shall

- a) Comprise a single conformant VLAN-aware bridge component;
- b) Recognize and use C-TAGs;
- c) Filter the Reserved MAC Addresses specified in Table 8-1;
- d) Use the Customer Bridge MVRP Address specified in Table 10-1; and

shall not

- ~~e) Use a VID Translation Table (6.5.6) on any Port;~~
- ~~f) Use Service VLAN tags (S-TAG) except in support of the functionality specified in 6.13.~~

## 5.6 S-VLAN component conformance

### 5.6.1 S-VLAN component options

*Change 5.6.1 as follows:*

A conformant S-VLAN component may implement any of the options specified for a VLAN-aware Bridge component (5.4.1). ~~and may~~

~~Allow translation of VIDs through support of a VID Translation Table (6.9) on each Port.~~

## 6. Support of the MAC Service

### 6.5 Quality of service maintenance

#### 6.5.1 Service availability

*In 6.5.1, insert the following note after list item c), and number the existing notes at the end of the subclause as “NOTE 2” and “NOTE 3”:*

NOTE 1—Each reference to spanning tree algorithms and protocols throughout Clause 6 includes any whose purpose is to verify that each transmitted frame gives rise to at most one service indication at any of the MSAPs for which frames for that LAN or VLAN are to be received. Such protocols include RSTP (13.4), MSTP (13.5), and SPB (Clause 27).

#### 6.5.3 Frame misordering

*Change Note 2 in 6.5.3 as follows:*

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 13),~~ When a protocol that is capable of rapid reconfiguration after network component failure, such as RSTP, MSTP, or SPB is used, 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 misordering and duplication; in order to allow Bridges that support RSTP to be used in environments where sensitive protocols are in use, the forceVersion parameter (13.7.2) 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 K.3 of IEEE Std 802.1D-2004.

#### 6.5.4 Frame duplication

*Change 6.5.4 as follows:*

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.~~

The potential for frame duplication in a bridged network arises through the possibility of the following:

- a) Repeated transmission, through a given Bridge Port, of a frame received on another Bridge Port;
- b) Multiple paths between source and destination end stations;
- c) A loop in a path between source and destination stations.

A bridge does not transmit any given received frame more than once through any Port (8.6.7).

~~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.~~

When bridges in a network connect individual LANs in such a way that physical topology is capable of providing multiple paths between any source and destination, a protocol is required to ensure that the active topology comprises a single path. SST bridges assign all frames to a single active topology, other bridges assign frames to an active topology using the VID or VID and destination address. For frames assigned to

ESPs by PBB-TE, the protocol comprises the operation of an external agent that configures static filtering entries in the Filtering Database (see 25.10); for all other frames RSTP, MSTP, or ISIS-SPB is used to configure the controls used for active topology enforcement (8.6.1). Reception of duplicate copies of a single transmitted frame can be avoided by loop prevention (6.5.4.1) or loop mitigation (6.5.4.2).

NOTE—Where RSTP, MSTP, or SPB is ~~in~~ used (see Clause 13), 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 K.2 of IEEE Std 802.1D-2004.

*Insert the following subclauses, 6.5.4.1 and 6.5.4.2, after 6.5.4:*

#### **6.5.4.1 Loop prevention**

Each bridge that participates in RSTP, MSTP, or ISIS-SPB calculates a spanning tree for each active topology, and prevents loops by exchanging information between neighboring bridges to ensure either that their topology calculations are consistent and each frame is consistently allocated to the same active topology, or that frames are not relayed.

#### **6.5.4.2 Loop mitigation**

Each bridge that participates in SPBM may mitigate loops. The properties of loop mitigation are listed below. Allowing temporary loops to form for unicast traffic and using loop mitigation provides for faster response to topology changes. Loop mitigation is accomplished if a unicast frame can only be forwarded by the bridges as follows:

- a) From at most one reception Port to at most one transmission Port; and
- b) To a different transmission Port from the reception Port;

and

- c) Each bridge does not relay, from any reception Port, a frame whose source address and VID are the same as that used by any entity within the bridge; and
- d) Each bridge does not transmit, through any Port, a frame whose destination address and VID are the same as that used by any entity within the bridge;

and

- e) All LANs in the network provide only point-to-point connectivity.

Loop mitigation limits the effect of loops since any loop in the active topology cannot include either the source or destination of the frame, nor can the loop cause multiple copies of the initial frame to be delivered to the destination, or to or from any LAN in the network that is not part of the loop.

Loop mitigation does not require that neighboring bridges assign a given frame to the same active topology; or even that the reception and transmission Ports for that frame have been derived from the same topology calculation within a given bridge. While this standard specifies the calculation of paths that are reverse path congruent (Clause 3) to support bi-directional communication, that property has no bearing on loop mitigation. As a consequence, the dynamic filtering entries that are used for active topology enforcement (8.6.1) and loop mitigation with SPBM (27.4.1) can be updated one at a time after ISIS-SPB has completed a link state calculation or during the course of that calculation.

## 6.9 Support of the EISS

### *Change 6.9 as follows:*

The EISS is supported by tagging and detagging functions that in turn use the ISS (6.6, 6.7). Any given instance of the EISS shall be supported by using one but not both of the following VLAN tag types:

- a) Customer VLAN tag (C-TAG); or
- b) Service VLAN tag (S-TAG);

selected as specified in 9.5.

Each Bridge Port shall support the following parameters for use by these functions:

- c) 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*.
- d) A PVID parameter for port-based VLAN classification;

and may support the following parameter:

- e) A VID Set for port-and-protocol-based classification (6.12);

~~An instance of the EISS supported by using the S-VLAN tag type may also support the following parameter:~~

- f) A VID translation table;
- ~~g) An Egress VID translation table.~~

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.

NOTE 1—The VID translation tables are for use only at the edge of administrative or control protocol domains, e.g., Network-Network Interfaces, Shortest Path Bridging domains, or Root and Leaf interfaces to a rooted multipoint service, as described in this standard. Control protocols that are designed for operation through ports where VID translation is permitted (e.g., MSTP, MVRP, CFM) explicitly compensate for the translation of VID values carried within their PDUs. Successful operation and maintenance of Bridged Local Area Networks depends on the fact that VID values are not translated at other ports or at ports within the operational span of control protocols that do not recognize translation.

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 2—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.

~~The VID translation table, when supported, shall contain a one-to-one bidirectional mapping of VID values included in the S-TAG of frames transmitted and received on the port (local VID) and VID values passed in the parameters of the EISS service primitives (relay VID). The table is configurable by management, and the default table configuration maps each value of the local VID to the same value for the relay VID.~~

The VID translation table and Egress VID translation table provide a mapping between “local VID” values and “relay VID” values. The local VID is the value encoded in a VLAN tag header in the initial octets of the `mac_service_data_unit` parameter of an ISS service primitive (`M_UNITDATA.indication` or `M_UNITDATA.request`). The relay VID is the value contained in the `vlan_identifier` parameter of an EISS service primitive (`EM_UNITDATA.indication` or `EM_UNITDATA.request`). The VID translation table may be supported by itself, or in combination with the Egress VID translation table. When only the VID translation table is supported it is used for bidirectional mapping between the local VID and the relay VID in both indication and request service primitives. This enforces a symmetric one-to-one translation (i.e., if local VID A maps to relay VID B then relay VID B will map to local VID A). When both tables are supported the VID translation table is used only for mapping the local VID to a relay VID in indication service primitives, and the Egress VID translation table is used for mapping the relay VID to a local VID in request service primitives. This allows asymmetric and many-to-one translations (e.g., for translating to and from SPVIDs at the edge of an SPT Region). Both tables are configurable by management, and the default configuration maps each value of the local VID to the same value for the relay VID, and vice versa. For Bridge Ports at the boundary of an SPBV SPT Region the tables are dynamically modified by the ISIS-SPB.

### 6.9.1 Data indications

*Change the first paragraph in 6.9.1 as follows:*

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` 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 translation table is supported and the translated VID value (relay VID) is FFF (indicating local discard); or
  - 3) ~~2)~~ The VID value is 000 (indicating priority-tagged), and the Acceptable Frame Types is *Admit Only VLAN-tagged frames*; or
  - 4) ~~3)~~ The VID value is in the range 001-FFE, and the Acceptable Frame Types is *Admit Only Untagged and Priority-tagged frames*.

*Change the fifth paragraph in 6.9.1 as follows:*

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

- e) The value contained in the VID field, optionally translated using the VID translation table, if the frame is VLAN-tagged;
- f) 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;~~ supported and the frame is untagged, Priority-tagged, or the VID translation table is supported and the translated VID value (relay VID) is zero;
- g) As determined by port-and-protocol-based VLAN classification (6.12) if that capability is implemented and the frame is untagged or Priority-tagged ~~or the VID translation table is supported and the translated VID value (relay VID) is zero.~~

### 6.9.2 Data requests

*Change the first and third paragraphs of 6.9.2 as follows:*

On invocation of an EM\_UNITDATA.request primitive by a user of the E-ISS, [the frame is discarded if the Egress VID translation table is supported and the translated VID value \(local VID\) is FFF \(reserved in Table 9-2\). Otherwise,](#) an M-UNITDATA.request primitive is invoked, with parameter values as follows:

The **destination\_address**, **source\_address**, **drop\_eligible**, 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 VID 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**, (optionally translated using the VID translation table [or Egress VID translation table](#)), **priority**, and **drop\_eligible** parameters are used to determine the contents of the tag header, in accordance with Clause 9.

## 7. Principles of network operation

*Change the introductory text of Clause 7 as follows:*

This clause establishes the principles and a model of Virtual Bridged Local Area Network operation. It defines the context necessary for:

- a) The operation of individual VLAN-aware Bridges (Clause 8);
- b) Their participation in the Spanning Tree (Clause 8 of IEEE Std 802.1D, 1998 Edition), Rapid Spanning Tree (Clause 13), or Multiple Spanning Tree Protocol (Clause 13), and Shortest Path Bridging protocols (SPB) (Clause 27);
- c) The management of individual Bridges (Clause 12); and
- d) The management of VLAN Topology (Clause 11)

to support, preserve, and maintain the quality of the MAC Service as discussed in Clause 6.

### 7.1 Network overview

*Replace Figure 7.1 with the following figure (which includes references to SPB):*

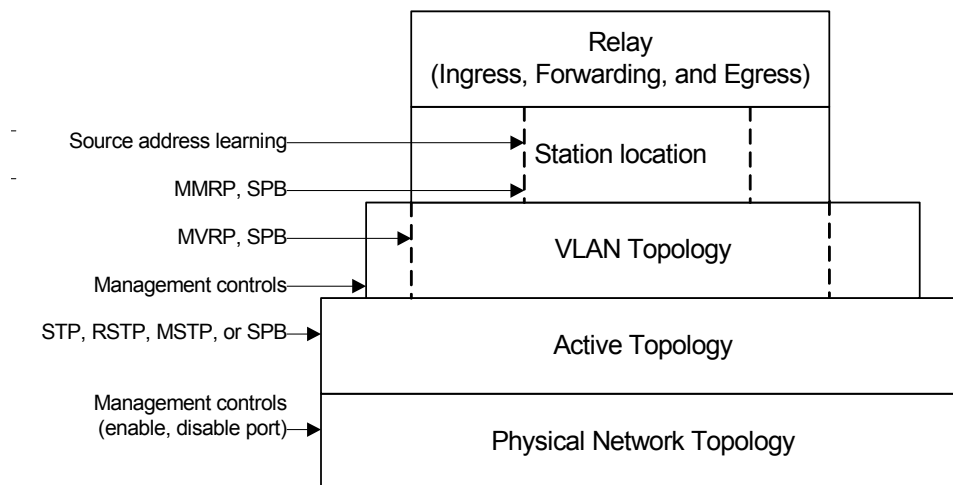


**Figure 7-1—VLAN Bridging overview**

### 7.2 Use of VLANs

*Change the following list item in 7.2 as follows:*

- d) Identify ~~the~~ configuration parameters that partition ~~or restrict access from one part of the~~ a physical network.

*Insert the following subclause, 7.3, after 7.2, and renumber the subsequent subclauses in Clause 7 accordingly:*

### 7.3 Active topology

Bridges cooperate to calculate one or more loop-free and fully connected active topologies, i.e., spanning trees. The algorithms and protocols—RSTP (13.4), MSTP (13.5), SPB (Clause 27)—that support that calculation provide rapid recovery from network component failure (6.5.1) by using alternate physical connectivity, without requiring management intervention.

The bridge's forwarding processes constrain the potential path for each user data frame to a single spanning tree. A bridge that uses RSTP or STP allocates all frames to a single Common Spanning Tree (CST). An MST or SPT Region (13.8, 27.4.1) comprises the transitive closure of bridges that use MSTP or SPB and that agree on the allocation of frames with a given VLAN Identifier (VID) to a given subtree within the region. That subtree can be a Multiple Spanning Tree Instance (MSTI), a Shortest Path Tree (SPT), or the Internal Spanning Tree (IST) that is the logical continuation of the CST through the region. Interoperability between MST and SPT Bridges and Single Spanning Tree (SST) Bridges, and between differently configured MST/SPT Bridges, is achieved by allocating all frames to the CST at region boundaries. Thus the spanning tree for a given frame can comprise subtrees of the CST together with an MSTI or SPT within each region. Frames with different VIDs can be assigned to the same or to different trees and subtrees within a region.

NOTE—In a stable network, the MSTP and SPB algorithms verify that each MST/SPT Region is fully connected internally. However, if the CST Root lies outside the region, the region can be partitioned temporarily as necessary to prevent external connectivity between Bridge Ports at the region boundary from creating a loop. A given region of the network can be an MST Region, an SPT Region, or both, but the protocol mechanisms that verify connectivity internal to the region require that regions do not overlap or subset other regions.

*Change the former 7.3 as follows:*

### 7.4 ~~7.3~~ VLAN topology

~~Each Bridge cooperates with others to operate a spanning tree protocol to calculate one or more loop free, fully connected, active topologies. This calculation supports the quality of the MAC Service (Clause 6) and provides rapid recovery from network component failure, by using alternate physical connectivity, without requiring management intervention.~~

~~All user data frames classified as belonging to a given VLAN are constrained by the forwarding process of each Bridge to a single active topology. Each and every VLAN is thus associated with a spanning tree, although more than one VLAN can be associated with any given tree. Each VLAN may occupy the full extent of the active topology of its associated spanning tree or a connected subset of that active topology. The maximum extent of the connected subset may be bounded by management by explicitly excluding certain Bridge Ports from a VLAN's connectivity.~~

Typically each of the VIDs for frames assigned to the CST, and to the IST or an MSTI within an MST Region, supports a different VLAN, and each VLAN is supported by only one VID and only one subtree within the region. However, frames for VLANs supported by shortest path bridging are assigned to the SPT rooted at the bridge where they enter an SPT Region, and SPBV requires that each source bridge for a given VLAN uses a unique SPVID. To provide interoperability with other regions and end systems that support a VLAN with a single VID, the VIDs for SPBV VLANs are translated at the SPT Region boundary (6.9, 27.12). SPBM uses a single VID for all the shortest path trees for a given VLAN.

NOTE 1—Support of a network comprising a single SPT Region with directly attached VLAN-unaware or priority tagging end stations does not require VID translation. This includes, for example, a PBN or PBBN where the edge of the network corresponds with the boundary of the SPT Region.

Within a given region, the SPTs that support any given shortest path VLAN provide full and symmetric connectivity (6.3). To allow frames in different VLANs to make use of equal cost shortest paths, multiple SPT sets can be used, each providing full symmetric connectivity between all bridges in the region.

Each VLAN may occupy the full extent of the active topology of its associated spanning tree(s) or a continuously connected subset of that active topology. The connected subset must be continuously connected otherwise the VLAN is split. The maximum extent of the connected subset may be bounded by management by explicitly excluding certain Bridge Ports from a VLAN's connectivity.

At any time the current extent of a VLAN can be further reduced from the maximum to include only those LANs that provide communication between attached devices, by the use of protocol that allows end stations to request and release services that use the VLAN. Such a protocol is specified in Clause 11. The dynamic determination of VLAN extent provides flexibility and bandwidth conservation, at the cost of network management complexity.

NOTE 2—Dynamic determination of VLAN extent is generally preferable to static configuration for bandwidth conservation, as the latter is error prone and can defeat potential alternate connectivity-requiring active management intervention to recover from network component failure.

NOTE 3—To accommodate end stations that do not participate in the MVRP protocol specified in Clause 11, management controls associated with each Bridge Port allow the Port to identify the attached LAN as connecting end stations that require services using specified VLANs.

NOTE 4—Where a given VLAN is supported by multiple VIDs, as for shortest path bridging, management controls identify the VLAN by a Base VID (that used when frames are allocated to the CST). Use of this single VID reduces the configuration burden, particularly when bridges are added to the SPT Region and further SPVIDs are allocated.

*Change the former 7.4 as shown:*

## **7.5 ~~7.4~~ Locating end stations**

Functioning as a distributed system, ~~Bridges~~ bridges within the current extent of a VLAN can, through explicit and or implicit cooperation, locate those LANs where an attached end station or end stations are intended to receive frames addressed to a specified individual address or group address. Bridges can thus reduce traffic by confining frames to the LANs where their transmission is necessary.

NOTE 1—Individually ~~Bridges~~ bridges do not determine the precise location of end stations but merely determine which of their Bridge Ports need to forward frames toward the destination(s). For the system of Bridges this is sufficient to restrict frames to the paths necessary to reach the destination LANs.

The multiple MAC registration protocol (MMRP), specified in Clause 10, allows end stations to advertise their presence and their desire to join (or leave) a multicast group, or to register an individual MAC address, in the context of a VLAN. The protocol communicates this information to other ~~Bridges~~ bridges using the VLAN and its active topology.

NOTE 2—To accommodate end stations that do not participate in MMRP, management controls associated with each Bridge Port allow the Port to identify the attached ~~LAN LANs~~ as connecting end stations that are intended to receive specified group addresses. The continuous operation of MMRP and the propagation of location information through ~~Bridges~~ bridges using the current active topology for the VLAN support multicast traffic reduction, while ensuring rapid restoration of multicast connectivity without management intervention if alternate connectivity is selected following network component failure.

Each end station implicitly advertises its attachment to an [individual](#) LAN and its individual MAC address whenever it transmits a frame. Bridges learn from the source address as they forward the frame along the active topology to its destination or destinations – or throughout the [Bridged Local Area Network or](#) VLAN if the location of the destination or destinations is unknown. The learned information is stored in the Filtering Database [\(8.8\) and](#) used to filter frames on the basis of their destination addresses.

[Address information learned from a frame with a given VID can be used to filter frames with other VIDs. For example, information learned from a frame with any of the VIDs that support shortest path bridging for a given VLAN \(i.e., VIDs associated with the same Base VID\) is used to filter frames with any of the VIDs for that VLAN. In some network configurations, it is also necessary to use address information learned in any one of a set of VLANs to filter frames with VIDs that identify any VLAN in the set \(Shared VLAN Learning, Clause 3\). In other configurations it is necessary or desirable not to share learned information between certain VLANs \(Independent VLAN Learning, Clause 3\) while in some cases it is immaterial whether address information is shared between VLANs or not. Annex F discusses the network configuration requirements, and some of the related interoperability issues.](#)

~~The Filtering Database architecture defined in this standard recognizes that~~

- ~~a) For some configurations, it is necessary to allow address information learned in one VLAN to be shared among a number of VLANs. This is known as Shared VLAN Learning (3.159);~~
- ~~b) For some configurations, it is desirable to ensure that address information learned in one VLAN is not shared with other VLANs. This is known as Independent VLAN Learning (3.73);~~
- ~~c) For some configurations, it is immaterial as to whether learned information is shared between VLANs.~~

~~NOTE 1—Annex B discusses the need for Shared and Independent VLAN Learning and some related interoperability issues.~~

~~Shared VLAN Learning is achieved by including learned information from a number of VLANs in the same Filtering Database; Independent VLAN Learning is achieved by including information from each VLAN in distinct Filtering Databases.~~

~~NOTE 2—The actual Filtering Database specification specifies a single Filtering Database that, through the inclusion of VLAN identification information in each database entry, can model the existence of one or more distinct Filtering Databases.~~

~~Within a given network, there may be a combination of configuration requirements, so that individual Bridges may be called on to share learned information, or not share it, according to the requirements of particular VLANs or groups of VLANs. The Filtering Database structure that is defined in this standard allows both Shared and Independent VLAN Learning to be implemented within the same Bridge; i.e., allows learned information to be shared between those VLANs for which Shared VLAN Learning is necessary, while also allowing learned information not to be shared between those VLANs for which Independent VLAN Learning is necessary. The precise requirements for each VLAN with respect to sharing or independence of learned information (if any) are made known to Bridges by means of a set of VLAN Learning Constraints (8.8.8.2) and fixed allocations of VIDs to filtering databases (8.8.8.1), which may be configured into the Bridges by means of management operations. By analyzing the set of learning constraints and fixed allocations for the VIDs that are currently active, the Bridge can determine~~

- ~~d) How many independent Filtering Databases are required in order to meet the constraints;~~
- ~~e) For each VID, which Filtering Database it will feed any learned information into (and use learned information from).~~

~~The manner in which this mapping of VIDs onto Filtering Databases is achieved is defined in 8.8.8; the result is that each VID is associated with exactly one Filtering Database.~~

~~The most general application of the Filtering Database specification in this standard is a Bridge that can support M independent Filtering Databases and can map N VID's onto each Filtering Database. Such a Bridge is known as an SVL/IVL Bridge (3.161).~~

~~The conformance requirements in this standard (5.4) recognize that Bridges will be implemented with differing capabilities in order to meet a wide range of application needs, and that the full generality of the SVL/IVL approach is not always either necessary or desirable, as observed in the discussion in Annex B. In a given conformant implementation, there may be restrictions placed on the number of Filtering Databases that can be supported and/or the number of VID's that can be mapped onto each Filtering Database. The full spectrum of conformant Filtering Database implementations is therefore as follows:~~

- ~~f) The SVL/IVL Bridge, as described above. Such Bridges provide support for M Filtering Databases, with the ability to map N VID's onto each one;~~
- ~~g) Support for a single Filtering Database only. MAC Address information that is learned in association with one VID can be used in filtering decisions taken relative to all other VID's supported by the Bridge. Bridges that support a single Filtering Database are referred to as SVL Bridges;~~
- ~~h) Support for multiple Filtering Databases, but only a single VID can be mapped onto each Filtering Database. MAC Address information that is learned in association with one VID cannot be used in filtering decisions taken relative to any other VID. Bridges that support this mode of operation are referred to as IVL Bridges;~~

Clause 15 and Clause 16 describe how the mapping of Customer VLANs (C-VLANs) into Service VLANs (S-VLANs) is accomplished within Provider Bridged Networks and Provider Backbone Bridged Networks. These networks provide additional mapping facilities to support hierarchies of VLANs allowing a provider a separate filtering database from customers. The conformance definitions of 5.3 have been extended to support S-VLANs. Clause 25 and Clause 26 describe how the mapping of S-VLANs into backbone service instances is accomplished within Provider Backbone Bridged Networks.

*Change the former 7.5 as shown:*

## **7.6 ~~7.5~~ Ingress, forwarding, and egress rules**

The relay function provided by each Bridge controls:

- a) Classification of each received frame as belonging to one and only one VLAN, and discard or acceptance of the frame for further processing on the basis of that classification and the received frame format, which can be one of three possible types:
  - 1) Untagged, and not explicitly identifying the frame as being associated with a particular VID;
  - 2) Priority-tagged, i.e., including a tag header conveying explicit priority information but not identifying the frames as being associated with a specific VID;
  - 3) VLAN-tagged, i.e., explicitly associating the frames with a particular VID.
 This aspect of relay implements the *ingress* rules.
- b) Implementation of the decisions governing where each frame is to be forwarded as determined by the current extent of the VLAN topology (7.4), station location information (7.5), and the additional management controls specified in Clause 8. This aspect of relay implements the *forwarding* rules.
- c) Queueing of frames for transmission through the selected Bridge Ports, management of the queued frames, selection of frames for transmission, and determination of the appropriate frame format type, VLAN-tagged or untagged. This aspect of relay implements the *egress* rules.

The structuring of the relay functionality into the implementation of ingress, forwarding, and egress rules constitutes a generic approach to the provision of VLAN functionality. All VLAN-aware Bridges can correctly forward received frames that are already VLAN-tagged. These are classified as belonging to the

VLAN identified by the VID in the tag header. All VLAN-aware Bridges can also classify untagged and priority-tagged frames received on any given port as belonging to a specified VLAN. In addition to this default Port-based ingress classification, this standard specifies an optional Port-and-Protocol-based classification.

The classification of untagged and priority-tagged frames, and the addition or removal of tag headers, is performed in support of the EISS (6.9).

Frames that carry control information to determine the active topology and current extent of each VLAN, i.e., spanning tree [or SPB](#) and MVRP PDUs, and frames from other link constrained protocols, such as EAPOL and LLDP, are not forwarded. Permanently configured static entries in the filtering database (8.2, 8.3, and 8.12) ensure that such frames are discarded by the Forwarding Process (8.6).

NOTE—MRPDUs destined for any MRP application are forwarded or filtered depending on whether the application concerned is supported by the bridge, as specified in 8.12.

The forwarding rules specified for VLAN-tagged frames facilitate the interoperation of bridges conformant to this standard with end stations that directly support attachment of MAC service users to VLANs by transmitting VLAN-tagged frames, and with Bridges that are capable of additional proprietary ingress classification methods.

Frames transmitted on a given LAN by a VLAN-aware Bridge for a given VLAN shall be either:

- d) All untagged; or
- e) All VLAN tagged with the same VID; [or](#)
- f) [All VLAN tagged, each with an SPVID allocated to the Base VID for that VLAN.](#)

## 8. Principles of bridge operation

*Change the introductory text of Clause 8 as indicated:*

This clause

- a) Explains the principal elements of the operation of VLAN-aware ~~Bridge~~bridges, and the operation of VLAN-aware bridge components within systems, and lists the supporting functions.
- b) Establishes a ~~Bridge-bridge~~ architecture that governs the provision of these functions.
- c) Provides a model of ~~Bridge-bridge~~ operation in terms of processes and entities that support the functions.
- d) Details the addressing requirements in a ~~Bridged Local Area Network~~bridged network.
- e) Specifies the addressing of ~~Entities~~entities in a ~~Bridge~~bridge.

NOTE—The provisions of this clause subsume the provisions of Clause 7 of IEEE Std 802.1D-2004.

### 8.1 Bridge operation

#### 8.1.1 Relay

*Change the first paragraph in 8.1.1 as follows:*

A MAC Bridge or VLAN-aware Bridge relays individual MAC user data frames between the separate MACs of the ~~bridged individual~~ LANs connected to its Ports. The functions that support relaying of frames and maintain the Quality of Service are

- a) Frame reception (8.5).
- b) Discard on received frame in error (6.5.2).
- c) Discard of frames that do not carry user data (6.7).
- d) Priority and drop eligibility decoding from a VLAN TAG, if present, and regeneration of priority, if required (6.9).
- e) ~~Classification of each received frame to a particular VLAN~~ Assignment of a VLAN Identifier to each received frame (6.9).
- f) Assure that each frame is confined to an active topology (8.6.1). ~~g) Frame discard to suppress loops in the physical topology of the network (8.6.1).~~
- g) ~~f) Frame discard to support management control over the active topology of each VLAN (6.9, 8.6.2).~~
- h) Frame discard following the application of filtering information (8.6.3).
- i) Metering of frames, potentially marking as drop eligible or discarding frames exceeding bandwidth limits (8.6.5).
- j) Forwarding of received frames to other Bridge Ports (8.6.4).
- k) Selection of traffic class and queuing of frames by traffic class (8.6.6).
- l) Frame discard to ensure that a maximum bridge transit delay is not exceeded (6.5.6, 8.6.7).
- m) Preferential discard of drop eligible frames to preserve QoS for other frames (8.6.7).
- n) Selection of queued frames for transmission (8.6.8).
- o) Mapping of service data units and Frame Check Sequence recalculation, if required (6.5.7).
- p) Frame discard on transmittable service data unit size exceeded (6.5.8).
- q) Selection of outbound access priority (6.5.9).
- r) Frame transmission (8.5).

### 8.1.2 Filtering and relaying information

*Change the following list item in 8.1.2 as follows:*

- a) Duplicate frame prevention: to maintain a loop-free active topology for ~~each VLAN~~every frame;

### 8.1.3 Duplicate frame prevention

*Change 8.1.3 as follows:*

A Bridge filters frames, i.e., does not relay frames received by a Bridge Port to other Ports on that Bridge, in order to prevent the duplication of frames (6.5.4). The functions that support the use and maintenance of information for this purpose are

- a) Configuration and calculation of one or more spanning tree active topologies.
- b) In MST Bridges, explicit configuration ~~to assign of the relationship between~~VIDs ~~and spanning trees to MSTIs~~ (8.9).
- c) In SPT Bridges: explicit or default selection of shortest path, CIST, or MSTI support for specified VLANs; and automatic assignment of VIDs to SPTs for shortest path VLANs.

## 8.2 Bridge architecture

*Change the third and fourth paragraphs and their accompanying notes in 8.2 as shown:*

Each Bridge Port also functions as an end station ~~and shall provide providing one or more instances of the~~ MAC Service to an LLC Entity that operates LLC Type 1 procedures to support protocol identification, multiplexing, and demultiplexing, for PDU transmission and reception by the Spanning Tree Protocol Entity and other higher layer entities. Other types of LLC procedures can also be supported for use by other protocols. The Bridge Port provides additional MAC service access points if those are explicitly required by the specifications of the attached higher layer entities. Each instance of the MAC Service is provided to a distinct LLC Entity that supports protocol identification, multiplexing, and demultiplexing, for PDU transmission and reception by one or more higher layer entities.

~~NOTE 1—In most cases, each Port provides a single instance of the MAC Service, to an LLC Entity that supports all Higher Layer Entities that require a point of attachment to the Port. Further instances are only provided when the specifications of the Higher Layer Entities require the use of different instances of the MAC service or of different source addresses.~~

~~An LLC Entity for each Bridge Port shall use an instance of the MAC Service provided for that Port to support the operation of LLC Type 1 procedures in order to support the operation of the Spanning Tree Protocol Entity. Bridge Ports may support other types of LLC procedures for use by other protocols, such as protocols providing Bridge Management (8.12).~~

~~NOTE 2—For simplicity of specification, this standard refers to a single LLC Entity that can provide both the procedures specified by ISO/IEC 8802.2 and Ethernet Type protocol discrimination in the cases where the media access method for the attached LAN supports the latter.~~

## 8.3 Model of operation

*Change the following list item in 8.3 as follows:*

- d) The Forwarding Process (8.6), that:
  - 1) Enforces ~~a~~loop-free active topologyies for all frames ~~for all VLANs~~ (8.1.3, 8.4, 8.6.1);

***Change paragraphs 7 to 9 and the accompanying note in 8.3 as follows (note that Figure 8-6 and Figure 8-7 remain unchanged):***

Figure 8-6 illustrates the operation of the Multiple Registration Protocol (MRP) Entity (8.11).

Higher Layer Entities that require only one point of attachment for the ~~Bridge~~ bridge as a whole may attach to an LLC Entity that uses an instance of the MAC Service provided by a Management Port. A Management Port does not use an instance of the ISS to attach to a network but uses the Bridge Port Transmit and Receive Process and the MAC Relay Entity to provide connectivity to other Bridge Ports and the attached LANs.

NOTE—Management port functionality may also be provided by an end station connected to an IEEE 802 LAN that is wholly contained within the system that incorporates the ~~Bridge~~ bridge. The absence of external connectivity to the LAN ~~ensures means~~ that the management port is always forwarding access to the management port through the bridge's relay functionality can be assured at all times.

Figure 8-7 illustrates the reception and transmission by an ~~Entity~~ entity attached to a Management Port.

## 8.4 Active topologies, learning, and forwarding

***Change 8.4 as follows:***

An *active topology* is the connectivity provided, for frames with a specified set of VID, destination address, and source address values, by interconnecting the LANs and bridges in a bridged network with *forwarding* Bridge Ports.

The distributed spanning tree algorithms and protocols, i.e., the Rapid Spanning Tree Protocol (RSTP, Clause 13), ~~and~~ the Multiple Spanning Tree Protocol (MSTP, Clause 13), and ISIS-SPB (Clause 27) construct one or more active topologies, each simply and fully connected for frames being associated with any given ~~VID~~ VLAN and transmitted from any end station to any other. The *forwarding* and *learning* performed by each Bridge Port for each spanning tree is dynamically managed by RSTP, ~~or~~ MSTP, or ISIS-SPB to prevent temporary loops and reduce excessive traffic in the network while minimizing denial of service following any change in the *physical topology* of the network.

Provider Backbone Bridge Traffic Engineering enables construction of active topologies by the external agent that is responsible for setting up Ethernet Switched Paths (ESPs).

Any port that is not enabled, i.e., has MAC\_Operational (6.6.2) False or has been excluded from the active topology by management setting of the Administrative Bridge Port State to Disabled, has both forwarding and learning disabled for all spanning trees and ESPs.

If the Bridge Port is enabled, PBB-TE disables learning and enables forwarding for all frames allocated to each ESP-VID. An external agent manages the Filtering Database to control the forwarding of frames with particular values of ESP-VID and destination MAC address.

The term Port State summarizes per tree combinations of forwarding and learning, and any additional per tree variables used by a given spanning tree protocol to enforce the active topologies it has calculated, and is used by RSTP and MSTP as follows. Any port that has learning and forwarding disabled is assigned the Port State Discarding. A Port that has learning enabled but forwarding disabled has the Port State *Learning*, and a Port that both learns and forwards frames has the Port State *Forwarding*. However the RSTP and MSTP state machines (Clause 13) do not control the Port State directly but use independent forwarding and learning variables for each tree.

ISIS-SPB controls both forwarding and learning variables for each SPT and Bridge Port directly when used to support Shortest Path Bridging VID (SPBV, Clause 27) just like RSTP and MSTP. ISIS-SPB disables

[learning and sets forwarding to true when supporting Shortest Path Bridging MAC \(SPBM, Clause 27\).](#)

RSTP constructs a single spanning tree, the Common Spanning Tree (CST), and maintains a single Port State for each Bridge Port. SST Bridges allocate all frames to that single spanning tree irrespective of their VLAN classification or source and destination MAC addresses.

MSTP constructs multiple spanning trees, the Common and Internal Spanning Tree (CIST) and additional Multiple Spanning Tree Instances (MSTIs), and maintains a Port State for each spanning tree for each Bridge Port. An MST Bridge allocates all frames classified as belonging to a given VLAN to the CIST or to one of the MSTIs using the MST Configuration Table. An MSTID of 0 identifies the CIST. A reserved MSTID value (TE-MSTID) is used to identify VIDs for use by PBB-TE with ESPs. [Further MSTID values are used to identify the use of SPBV or SPBM.](#) A single VID is used to identify frames assigned to any given VLAN that is supported by the CIST or an MSTI. That VID is used by the Forwarding Process (8.6) to identify the spanning tree for the relayed frame, and thus identifies the applicable Port State.

[ISIS-SPB constructs symmetric \(Clause 3\) shortest path trees \(SPTs\) rooted at each bridge within an SPT Region, and maintains independent forwarding and learning variables for each SPT for each Bridge Port.](#)

[Each frame classified as belonging to a VLAN supported by SPBV, is allocated to an SPT rooted at the bridge that first relays the frame into the Region. If a C-VLAN, S-VLAN or B-VLAN is supported by SPBV \(Clause 27\) the frame is assigned a Shortest Path VLAN Identifier \(SPVID\) that is used by the Forwarding Process \(8.6\) to identify both the VLAN and the SPT, and thus identifies the applicable learning and forwarding values.](#)

[If a B-VLAN is supported by SPBM, \(Clause 27\) the frame is assigned a B-VID value that identifies the frame as subject to SPBM and identifies the B-VLAN and the SPT Set \(Clause 3\). The SPT is identified \(from amongst those in that set\) by the source address of the frame \(B-SA\) which identifies the SPT root. When ISIS-SPB sets forwarding True for that SPT, a Dynamic Filtering Entry for that B-VID, source address tuple is included in the Filtering Database so that it passes the active topology enforcement check \(8.6.1\). If a B-VLAN is supported by SPBM, learning is disabled for all frames for that B-VID.](#)

Figure 8-5 illustrates the operation of the Spanning Tree Protocol Entity, which operates the Spanning Tree algorithm and its related protocols, and its modification of Port state information as part of determining the active topology of the network.

Figure 8-3 illustrates the Forwarding Process's use of the Port State: first, for a Port receiving a frame, to determine whether the received frame is to be relayed through any other Ports; and second, for another Port in order to determine whether the relayed frame is to be forwarded through that particular Port.

Figure 8-4 illustrates the use of the Port state information for a Port receiving a frame, in order to determine whether the station location information is to be incorporated in the Filtering Database.

## 8.6 The Forwarding Process

Replace Figure 8-11 with the following figure (which connects Active topology enforcement to the Filtering Database):

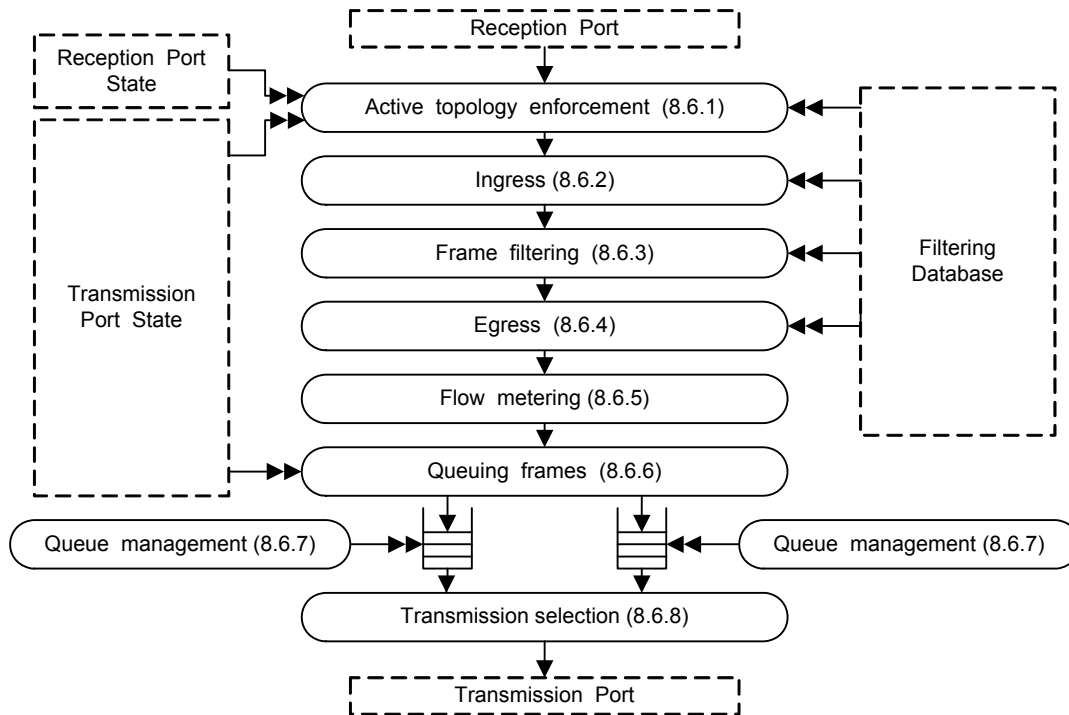


Figure 8-11—Forwarding Process functions

### 8.6.1 Active topology enforcement

Change 8.6.1 as follows:

To prevent data loops and unwanted learning of source MAC addresses, the Forwarding Process determines the values (TRUE, or FALSE) of the learning and forwarding controls (8.4) appropriate to each received frame and Bridge Port. If learning is true for the reception Port and ingress filtering (8.6.2) would not cause the received frame to be discarded, the source address and VID are submitted to the Learning Process. If forwarding is true for the reception Port, each Bridge Port, other than the reception Port, with forwarding true is identified as a potential transmission Port.

An SST Bridge supports a single active topology, the Common Spanning Tree (CST). For each Bridge Port, RSTP determines a single value for forwarding and a single value for learning (8.4) for all frames.

Bridges with MST, ~~or~~ PBB-TE, or SPB capabilities use the VID of the received frame to determine forwarding and learning for that frame for each Bridge Port that is enabled, i.e., has MAC\_Operational True and an Administrative Bridge Port State of Enabled, as follows:

If the bridge supports PBB-TE, and the VID is an ESP-VID, forwarding is true and learning is false. Control over the active topology of each ESP is provided by configuration of static filtering entries in the Filtering Database (8.8.1, 25.10.1).

If the bridge uses MSTP to configure the CIST, and the VID identifies a VLAN assigned to the CIST, forwarding and learning are as determined by MSTP (Clause 13) for the CIST.

If the bridge uses MSTP to configure MSTIs, and the VID identifies a VLAN assigned to an MSTI calculated by MSTP, forwarding and learning are as determined by MSTP for that MSTI.

If the bridge uses ISIS-SPB to configure the CIST, and the VID identifies a VLAN assigned to the CIST, forwarding and learning take the value of forwarding determined by ISIS-SPB (Clause 28) for the CIST.

If the bridge uses ISIS-SPB, and the VID is used by SPBV as an SPVID, both forwarding and learning take the value of forwarding determined by ISIS-SPB for the SPT identified by that SPVID.

If the bridge uses ISIS-SPB and the VID identifies a VLAN supported by SPBM, then for that VID:

- learning is False for all Bridge Ports;
- forwarding is True for the reception Port if and only if a Dynamic Filtering Entry for the frame's source address exists and specifies Forward for that Port; and
- forwarding is True for all other Bridge Ports.

NOTE 1—Effective control over the egress component of an SPT for VLANs supported by SPBM is provided by ISIS-SPB configuration of (a) a Dynamic Filtering Entry for the VLAN's VID and Root MAC Address (for unicast frames); and (b) MAC Address Registration Entries for the VID and SPT specific Group MAC Addresses (for multicast frames); and (c) a MAC Address Registration Entry for the VID to filter "All Unregistered Group Addresses" at all Ports.

All bridges other than SST Bridges implement the MST Configuration Table (8.9.1). The use of VIDs to determine learning and forwarding, as required by this clause shall be consistent with that table as follows. ~~VIDs allocated by the MST Configuration Table (8.9.1) of value: All VIDs allocated by the MST Configuration Table to the CIST-MSTID (0x000) are assigned to the CIST, all VIDs allocated to the TE-MSTID (0xFFE) are ESP-VIDs, and all VIDs allocated to other values of MSTID are assigned to the MSTI identified by that MSTID.~~

- CIST-MSTID (0x000) are CIST VIDs.
- SPBM-MSTID (0xFFC) are Base VIDs supported by SPBM.
- SPBV-MSTID (0xFFD) are Base VIDs supported by SPBV.
- TE-MSTID (0xFFE) are ESP-VIDs supported by PBB-TE.
- SPVID-MSTID (0xFFF) are VIDs reserved for use by ISIS-SPB as SPVIDs.
- All VIDs allocated to other values of MSTID are assigned to the MSTI identified by that MSTID.

NOTE 2—While MST Configuration Table is capable of detailing the configuration of each SPVID it captures the allocation of Base VIDs only. Individual allocation of SPVIDs are captured in the ISIS-SPB database, the SPB ECT Static Entry (12.25.4) and in the port VID translation tables. By specifying only the type of VID and its allocation to SPB, backwards compatibility with STP, RSTP and MSTP is maintained.

## 8.7 The Learning Process

*Change the first paragraph of 8.7 as follows:*

The Learning Process receives the source MAC Addresses and VIDs of received frames from the Forwarding Process, subject to active topology enforcement (8.6.1) and the application of ingress filtering (8.6.2). The Learning Process is not invoked (see 8.6.1) for frames whose VID is an ESP-VID or identifies a VLAN supported by SPBM.

*Insert the following subclause, 8.7.3 (including Table 8-6), after 8.7.2, and renumber the subsequent tables in Clause 8 accordingly:*

### 8.7.3 Ageing of Dynamic Filtering Entries

Dynamic Filtering Entries shall be automatically removed after a specified time, the Ageing Time, has elapsed since the entry was created or last updated by the Learning Process.

The ageing out of Dynamic Filtering Entries ensures that end stations that have been moved to a different part of the network will not be permanently prevented from receiving frames. It also takes account of changes in the active topology of the network that can cause end stations to appear to move from the point of view of the bridge; i.e., the path to those end stations subsequently lies through a different Bridge Port.

The Ageing Time may be set by management (Clause 12). A range of applicable values and a recommended default is specified in Table 8-6; this is suggested to remove the need for explicit configuration in most cases. If the value of Ageing Time can be set by management, the Bridge shall have the capability to use values in the range specified, with a granularity of 1 s.

**Table 8-6—Ageing time parameter value**

| Parameter   | Recommended default value | Range              |
|-------------|---------------------------|--------------------|
| Ageing time | 300.0 s                   | 10.0–1 000 000.0 s |

NOTE—The granularity is specified in order to establish a common basis for the granularity expressed in the management operations defined in Clause 12, not to constrain the granularity of the actual timer supported by a conformant implementation. If the implementation supports a granularity other than 1 s, then it is possible that the value read back by management following a Set operation will not match the actual value expressed in the Set.

The Spanning Tree Algorithm and Protocol specified in Clause 8 of IEEE Std 802.1D, 1998 Edition, includes a procedure for notifying all Bridges in the network of topology change. It specifies a short value for the Ageing Timer, to be enforced for a period after any topology change (8.3.5 of IEEE Std 802.1D, 1998 Edition). While the topology is not changing, this procedure allows normal ageing to accommodate extended periods during which addressed end stations do not generate frames themselves, perhaps through being powered down, without sacrificing the ability of the network to continue to provide service after automatic configuration.

## 8.8 The Filtering Database

*Change the first paragraph of 8.8 as follows:*

The Filtering Database supports queries by the Forwarding Process to determine whether received frames, with given values of destination MAC Address and VID, are to be forwarded through a given potential transmission Port (8.6.1, 8.6.3, 8.6.4). It can also be used, by SPBM (8.6.1), to determine whether received frames with given values of source B-MAC Address and B-VID, are to be forwarded from a given reception Port. The Filtering Database contains filtering information in the form of filtering entries that are either

- Static, and explicitly configured by management action; or
- Dynamic, and automatically entered into the Filtering Database by the normal operation of the bridge and the protocols it supports.

***In 8.8, change the following list items (including the insertion of Note 1) as shown, and renumber the subsequent notes in 8.8 accordingly:***

- h) Each Dynamic Filtering Entry specifies the Port through which a frame with a given individual MAC Address and VID has been or can be received. Dynamic Filtering Entries can be created and updated by the Learning Process (8.7) and by ISIS-SPB. Entries that are updated by the Learning Process are subject to ageing and removal by the Filtering Database.

NOTE 1—ISIS-SPB has to create the Dynamic Filtering Entries for VLANs supported by SPBM, since learning is not used. Initial creation of these entries does no harm for VLANs supported by SPBV (when learning is used) as it can reduce flooding of frames to unknown destinations.

- i) MAC Address Registration Entries support the registration of MAC Addresses. They are created, updated, and removed by MMRP in support of Extended Filtering Services (8.8.4, and Clause 10) and by ISIS-SPB. If the Restricted\_MAC\_Address\_Registration management control (10.12.2.3) is TRUE, then the creation of a MAC Address Registration Entry by MMRP is not permitted unless a Static Filtering Entry exists that permits dynamic registration for the Group concerned.
- j) Dynamic VLAN Registration Entries are used to specify the Ports on which VLAN membership has been dynamically registered. They are created, updated, and removed by MVRP, ~~and MRP~~, and ISIS-SPB, in support of automatic VLAN membership configuration (Clause 11 and Clause 39). The MVRP controlled Dynamic VLAN Registration Entries are subject to the state of the Restricted\_VLAN\_Registration management control (11.2.3.2.3). If the value of this control is TRUE, then the creation of a Dynamic VLAN Registration Entry by MVRP is not permitted unless a Static VLAN Registration Entry exists that permits dynamic registration for the VID concerned.

***In 8.8, change paragraph 15, and insert a new paragraph after paragraph 15 as follows:***

The Filtering Database shall support the creation, updating, and removal of Dynamic Filtering Entries by the Learning Process (8.7). In Bridges that support Extended Filtering Services, the Filtering Database shall support the creation, updating, and removal of MAC Address Registration Entries by MMRP (Clause 10). In bridges that support SPBM, Dynamic Filtering Entries are populated by ISIS-SPB (Clause 28). In bridges that support SPBV the Dynamic Filtering Entries are created and updated by the Learning Process (8.7) and the use of ISIS-SPB for this operation is optional (28.12.9).

Shortest Path Bridging (SPB), (27.10) allocates SPVIDs dynamically to support shortest path bridging of frames assigned to one or more VLANs, each identified by a Base VID (Clause 3). A Static Filtering Entry should not be created for an SPVID, irrespective of whether that SPVID is currently used or not, and SPVIDs should not be used in registration protocols that create MAC Address Registration Entries or Dynamic VLAN Registration Entries. In an SPT Bridge, configuration or registration of a filtering database entry with the Base VID of a VLAN supported by SPBV shall cause the bridge to filter frames as if that entry was also present for every one of the SPVIDs for that Base VID.

***Change the following note in 8.8 as shown:***

NOTE ~~23~~—The ability to create VLAN-dependent Filtering Database entries allows a Bridge to support ~~multiple~~ end stations with the same individual MAC Address residing on different VLANs. It also supports ~~End~~ stations with multiple interfaces, each using the same individual MAC Address, as long as not more than one end station or interface that uses a given MAC Address resides in a given VLAN.

### 8.8.1 Static Filtering Entries

***Change the following list item in 8.8.1 as follows:***

- a) A MAC Address specification, comprising
  - 3) All Individual Addresses, for which no more specific ~~Static~~ Filtering Entry exists; or

*Change the second paragraph of 8.8.1 as follows:*

All Bridges shall have the capability to support the first two values for the MAC Address specification, both values of the VLAN identifier specification, and all three values for each control element for all Static Filtering Entries [i.e., shall have the capability to support item a1), item a2), item b1), item b2), item c1), item c2), and item c3)]. All Bridges supporting PBB-TE [or SPT Bridges](#) shall, in addition, support items a3) and a4) for ESP-VIDs (8.9) [or VIDs identifying VLANs supported by SPBM respectively](#) and shall always have in their filtering databases Static Filtering Entries specifying items a3) and a4), and a Port Map specifying filtering for each outbound port, for every ESP-VID [or SPBM VID respectively](#).

## 8.8.2 Static VLAN Registration Entries

*Insert the following note at the end of 8.8.2:*

NOTE 3—For VLANs supported by SPBV the Filtering specified by a static VLAN registration entry for the Base VID is applied for all SPVIDs associated with that Base VID.

## 8.8.3 Dynamic Filtering Entries

*Change 8.8.3 as follows:*

A Dynamic Filtering Entry specifies

- a) An individual MAC Address;
- b) The FID, an identifier assigned by the MAC Bridge (8.8.8) to identify a set of VIDs for which no more than one Dynamic Filtering Entry can exist for any individual MAC Address;

NOTE 1—An FID identifies a set of VIDs among which *Shared VLAN Learning* (Clause 3) takes place. Any pair of FIDs identifies two sets of VIDs between which *Independent VLAN Learning* (Clause 3) takes place. The allocation of FIDs by a Bridge is described in 8.8.8.

- c) A Port Map specifying forwarding for the destination MAC Address and FID to a single Port.

NOTE 2—This is equivalent to specifying a single port number; hence, this specification is directly equivalent to the specification of dynamic entries in IEEE Std 802.1D, 1993 Edition [B9].

The Port Map may contain a **connection\_identifier** (8.8.12) for each outbound Port.

Dynamic Filtering Entries ~~are can be created, and updated, and removed~~ by the Learning Process (8.7). They shall be automatically removed after a specified time, the Ageing Time [\(8.7.3\)](#), has elapsed since the entry was created or last updated. ~~No more than one Dynamic Filtering Entry shall be created in the Filtering Database for a given combination of MAC Address and FID.~~

~~Dynamic Filtering Entries cannot be created or updated by management.~~

[Dynamic Filtering Entries can also be created and updated by SPB \(Clause 27\). ISIS-SPB \(Clause 28\) refreshes these entries, so they are not aged out by the normal operation of the Learning Process. These entries are used by SPBM \(Clause 27\) to support both unicast loop mitigation \(6.5.4.2\) and multicast loop prevention \(6.5.4.1\) for active topology enforcement \(8.6.1\), as well as to locate end stations. These entries are updated by the normal Learning Process for SPBV, but could also be controlled by ISIS-SPB. This allows entries for the higher layer entities in a bridge \(see Figure 8-11\) to be populated rapidly after any topology change.](#)

No more than one Dynamic Filtering Entry shall be created in the Filtering Database for a given combination of MAC Address and FID. Dynamic Filtering Entries cannot be created or updated by management.

NOTE 3—Dynamic Filtering Entries may be read by management (Clause 12). The FID is represented in the management Read operation by any one of the VIDs that it represents. For a given VID, the set of VIDs that share the same FID may also be determined by management.

~~The ageing-out of Dynamic Filtering Entries ensures that end stations that have been moved to a different part of the network will not be permanently prevented from receiving frames. It also takes account of changes in the active topology of the network that can cause end stations to appear to move from the point of view of the bridge; i.e., the path to those end stations subsequently lies through a different Bridge Port.~~

~~The Ageing Time may be set by management (Clause 12). A range of applicable values and a recommended default is specified in Table 8-6; this is suggested to remove the need for explicit configuration in most cases. If the value of Ageing Time can be set by management, the Bridge shall have the capability to use values in the range specified, with a granularity of 1 s.~~

**Table 8-6—Ageing time parameter value**

| Parameter   | Recommended default value | Range              |
|-------------|---------------------------|--------------------|
| Ageing time | 300.0 s                   | 10.0–1 000 000.0 s |

~~NOTE 4—The granularity is specified in order to establish a common basis for the granularity expressed in the management operations defined in Clause 12, not to constrain the granularity of the actual timer supported by a conformant implementation. If the implementation supports a granularity other than 1 s, then it is possible that the value read back by management following a Set operation will not match the actual value expressed in the Set.~~

~~The Spanning Tree Algorithm and Protocol specified in Clause 8 of IEEE Std 802.1D, 1998 Edition includes a procedure for notifying all Bridges in the network of topology change. It specifies a short value for the Ageing Timer, to be enforced for a period after any topology change (8.3.5 of IEEE Std 802.1D, 1998 Edition). While the topology is not changing, this procedure allows normal ageing to accommodate extended periods during which addressed end stations do not generate frames themselves, perhaps through being powered down, without sacrificing the ability of the network to continue to provide service after automatic configuration.~~

## 8.8.4 MAC Address Registration Entries

*Change the second and third paragraphs in 8.8.4 as follows:*

MAC Address Registration Entries are created, modified, and deleted by the operation of MMRP (Clause 10) or by ISIS-SPB. No more than one MAC Address Registration Entry shall be created in the Filtering Database for a given combination of MAC Address specification and VID.

NOTE—It is possible to have a Static Filtering Entry that has values of Forward or Filter on some or all Ports that mask the dynamic values held in a corresponding MAC Address Registration Entry. The values in the MAC Address Registration Entry will continue to be updated by MMRP; hence, subsequent modification of that entry to allow the use of dynamic filtering information on one or more Ports immediately activates the true MMRP registration state that was hitherto masked by the static information.

The creation of MAC Address Registration Entries by MMRP is subject to the Restricted\_MAC\_Address\_Registration management control (10.12.2.3). If the value of this control is TRUE, a dynamic entry for a given MAC address may only be created if a Static Filtering Entry already exists for that MAC address, in which the Registrar Administrative Control value is Normal Registration.

### 8.8.8 Allocation of VIDs to FIDs

*Change 8.8.8 and 8.8.8.1 as follows:*

~~The allocation of VIDs to FIDs within a Bridge determines how learned individual MAC Address information is used in forwarding/filtering decisions within a Bridge; whether such learned information is confined to individual VIDs, shared among all VIDs, or confined to specific sets of VIDs.~~

~~The allocation of VIDs to FIDs is determined on the basis of~~

- ~~a) The set of VLAN Learning Constraints that have been configured into the Bridge (by means of the management operations defined in Clause 12);~~
- ~~b) Any fixed mappings of VIDs to FIDs that may have been configured into the Bridge (by means of the management operations defined in Clause 12);~~
- ~~c) The set of active VIDs (i.e., those VIDs on whose behalf the Bridge may be called on to forward frames). A VID is active if either of the following is true:
  - ~~1) The VID's member set (8.8.10) contains one Port that is in a forwarding state, and at least one other Port of the Bridge is both in a forwarding state and has Ingress Filtering (8.6.2) disabled;~~
  - ~~2) The VID's member set contains two or more Ports that are in a forwarding state.~~~~
- ~~d) The capabilities of the Bridge with respect to the number of FIDs that it can support, and the number of VIDs that can be allocated to each FID.~~

~~A Bridge shall support a minimum of one FID and may support up to 4094 FIDs. For the purposes of the management operations, FIDs are numbered from 1 through N, where N is the maximum number of FIDs supported by the implementation.~~

~~A Bridge shall support the ability to allocate at least one VID to each FID and may support the ability to allocate more than one VID to each FID.~~

~~The number of VLAN Learning Constraints supported by a Bridge is an implementation option.~~

~~NOTE—In an SVL/IVL Bridge (3.167), a number of FIDs are supported, and one or more VIDs can be mapped to each FID. In an SVL Bridge (3.166), a single FID is supported, and all VIDs are mapped to that FID. In an IVL Bridge (3.76), a number of FIDs are supported, and only one VID can be mapped to each FID.~~

~~An MST Bridge shall support the ability to allocate at least one FID to each spanning tree and may support the ability to allocate more than one FID to each spanning tree.~~

~~NOTE—In other words, the number of FIDs supported by the Bridge must be greater than or equal to the number of spanning trees supported by the Bridge.~~

~~An MST Bridge shall ensure that the maximum supported numbers of FIDs and VIDs can be associated unambiguously. This requires either 1) a number of fixed VID to FID allocations at least equal to the maximum number of VIDs supported; or 2) one I-Constraint entry per FID supported and one S-Constraint entry per MSTI supported, or both (8.8.8.2).~~

The allocation of VIDs to FIDs within a VLAN-aware Bridge determines how learned individual MAC Address information is used in forwarding and filtering decisions. If two VIDs are allocated to the same FID learned information is shared, i.e., an individual MAC address learned following receipt of a frame affects the forwarding or filtering of a subsequent frame with the same address as its destination address if either of the two VIDs have been assigned to each of the two frames. If two VIDs are allocated to different FIDs learned information is independent, i.e., an individual MAC address for frames that have one of the VIDs assigned does not affect forwarding or filtering of frames with the other VID. Independent VLAN Learning can allow two separate stations to use the same MAC address, provided they use different VLANs, and also allows frames transmitted by a single station to be assigned to independent active topologies. Shared VLAN Learning allows support of a single VLAN by multiple VIDs, enabling further control over the filtering of frames for that VLAN, and allowing shortest path bridging to support the VLAN with a set of symmetric trees while still using learning. Further considerations for the use of Independent and or Shared VLAN Learning are described in Annex F (informative).

A VLAN-aware Bridge shall support either Shared or Independent VLAN Learning, and may support both. If Independent VLAN Learning is not supported the bridge shall support a single FID. If Independent VLAN Learning is supported, the number of FIDs shall be the same as the maximum number of VLANs supported by the implementation. For the purposes of the management operations, FIDs are numbered from 1 through N, where N is the maximum number of FIDs supported by the implementation. A bridge that supports both Shared and Independent VLAN Learning shall be capable of allocating any VID to any FID, through configuration of the VID to FID allocation table. Following any set of management operations designed to change the allocation of VIDs to FIDs, whether initiated by an administrative request or as a consequence of other aspects of the bridge's operation, the value of any FID that is in use should be the same as that of one of the VIDs allocated to that FID. One exception to this rule is the allocation of SPVIDs to FIDs for SPBV (Clause 27). SPVIDs that are allocated are associated with a Base VID's FID. The learning behavior of SPVIDs assigned to a FID is determined by the learning behavior of the associated Base VID's FID (27.11)

#### **8.8.8.1 Fixed and dynamic VID to FID allocations**

~~A Bridge may support the ability to define fixed allocations of specific VIDs to specific FIDs, via an~~ The VID to FID allocation table ~~that~~ may be read and modified by means of the management operations defined in Clause 12. For each VID supported by the implementation, the allocation table indicates one of the following:

- a) The VID is currently not allocated to any FID; or
- b) A fixed allocation has been defined (via management), allocating this VID to a specific FID; or
- c) A dynamic allocation has been defined ~~(as a result of applying the VLAN Learning Constraints),~~ allocating this VID to a specific FID.

~~For any VID that has no fixed allocation defined, the Bridge can dynamically allocate that VID to an appropriate FID, in accordance with the current set of VLAN Learning Constraints.~~

An SPT Bridge can dynamically allocate VIDs, that have been reserved for use as SPVIDs, to FIDs.

An MST Bridge shall support Independent VLAN Learning and may support Shared VLAN Learning. An MST Bridge shall be capable of allocating any FID to any MSTID through configuration of the FID to MSTID Allocation Table (12.12.2). An SPT Bridge supports both Independent and Shared VLAN Learning.

***Delete 8.8.8.2 (VLAN Learning Constraints) and 8.8.8.3 (VLAN Learning Constraint inconsistencies and violations) in their entirety.***

*Change 8.9 through 8.9.3 as follows:*

## 8.9 MST, SPB, and ESP configuration information

In order to support multiple spanning trees, and shortest path bridging, all the bridges in an MST or SPT Region have an MST Bridge ~~has~~ to be configured with an unambiguous ~~assignments~~ of VID to spanning trees. ~~This is achieved by:~~

- a) ~~Ensuring that the allocation of VID to FID (8.8.8) is unambiguous; and~~
- b) ~~Ensuring that each FID supported by the Bridge is allocated to exactly one Spanning Tree.~~

~~The first of these requirements is met by configuring a set of VLAN learning constraints and/or fixed VID to FID mappings that are self-consistent, and which define an I Constraint, an S Constraint, or a fixed VID to FID allocation for all VID supported by the Bridge.~~

~~The second requirement is met by means of the FID to MSTI Allocation Table (8.9.3).~~

The combination of the VID to FID allocations (8.8.8) and the FID to MSTI allocations (8.9.3) defines a mapping of VID to spanning trees, MSTIDs, represented by the MST Configuration Table (8.9.1). If an MSTID is included in the MSTI List (12.12.1), frames with VID allocated to that MSTID will be supported by an MSTI calculated by MSTP (Clause 13). If the MSTID is not included in the MSTI List, and is not a reserved MSTID, those frames will be supported by the IST.

A ~~Bridge~~ bridge supporting PBB-TE can assign specific VID values to ESPs but can also support any of the spanning tree protocols. This is achieved by allocating the VID associated with the PBB-TE ESPs to a special MSTID, the TE-MSTID.

An SPT Bridge can allocate any given VLAN to the CIST, or to the reserved MSTIs, as well as supporting shortest path bridging for other VLANs within an SPT Region. The assignment of VLANs and VID to MSTIs is subject to similar considerations and constraints as for MST Bridges. In addition to the Base VID used to identify frames for the VLAN when transmitted on the CST outside the region, each VLAN supported by SPBV uses a number of dynamically allocated shortest path VID (SPVIDs), one for each SPT Bridge participating in the VLAN within the region.

The network administrator allocates enough SPVIDs for SPBV to avoid unintentionally excluding bridges from the topology. The details of SPVID allocation, including mitigation of the consequences of not allocating enough SPVIDs, are specified in 27.10.

Administratively, by not translating from Base VID to SPVID, an SPBV VLAN can be forced to the IST. When there is no shortage of SPVIDs and the MCIDs match but the Base VID algorithms disagree the algorithm defaults to the Spanning tree. This behavior allows SPBV to change the ECT Algorithms.

Dynamic SPVID allocation is supported by ISIS-SPB and allows the addition of bridges to existing SPT Regions without disruptive configuration changes, as well as allowing supporting auto configuration of shortest path bridging in simple networks where all user data is assigned to a VLAN identified by the default PVID of 1 (Table 9-2). However, prior to SPVID allocation, all bridges in an SPT Region have to agree which VLANs are to be shortest path bridged, and which SPT Set (ECT -Algorithm) is to be used for each of those VLANs. By default, all VLANs whose Base VID is allocated to MSTID 0xFFD will be supported by SPBV using the SPB default ECT Algorithm. The SPT configuration information can also specify that frames for SPBV and SPBM be supported by another specified SPB ECT Algorithm as specified by configuration (12.25.4, Table 28-1).

NOTE—The use of MSTIDs to support allocation of Base VIDs to SPB allows the per VLAN components of the necessary information to be conveyed in the MST Configuration Digest, thus avoiding any need for a separate digest. However the digest is not specific about how the VIDs are mapped to specific SPTs, just that they are allocated to SPBV, SPBM, or SPVIDs.

### 8.9.1 MST Configuration Table

The MST Configuration Table specifies an MSTID for each possible VID.

~~In an MST Bridge, defines, for each VID, the each~~ MSTID identifies ~~of the MSTI spanning tree instance to~~ which the VID is allocated and an MSTID of zero identifies the CIST.

~~In a Bridge that supports PBB-TE an MSTID of 0xFFE, the TE-MSTID, identifies VIDs that can be used by ESPs. Each of these VIDs, the ESP VIDs, shall be allocated to an individual FID.~~

The combination of the VID to FID allocations (8.8.8) and the FID to MSTID allocations (8.9.3) define a mapping of VIDs to MSTIDs summarized in the MST Configuration Table (8.9.1).~~The MST Configuration Table cannot be configured directly; configuration of the table occurs as a consequence of configuring the relationships between VIDs and FIDs (8.8.8) and between FIDs and spanning trees (8.9.3).~~

### 8.9.2 MST configuration identification

For two or more MST Bridges to be members of the same MST Region (Clause 3), it is necessary for those Bridges to ~~be directly connected together (i.e., support the same MST Region configuration and to be interconnected only by means of LANs, without intervening Bridges that are not members of the region), and for them to support the same MST Region configuration with all intervening Bridges being members of the region or being transparent to the BPDUs of the members of the region.~~ Two MST Region configurations are considered to be the same if the correspondence between VIDs and ~~spanning trees~~ MSTIDs is identical in both configurations and they use the same information to identify the configuration, including the same Configuration Name.

NOTE 1—If two adjacent MST Bridges consider themselves to be in the same MST Region despite having different mappings of VIDs to ~~spanning trees~~ MSTIDs, then the possibility exists of undetectable loops arising within the MST Region.

In order to ensure that adjacent MST Bridges are able to determine whether they are part of the same MST Region, the MST BPDU supports the communication of an MST Configuration Identifier (13.8).

NOTE 2—As the MST Configuration Identifier is smaller than the mapping information that it summarizes, there is a small but finite possibility that two MST Bridges will assume that they have the same MST Region Configuration when this is not actually the case. However, given the size of the identifier, this standard assumes that this possibility is sufficiently small that it can safely be ignored. Appropriate use of the Configuration Name and Revision Level portions of the identifier can remove the possibility of an accidental match between MST Configuration Identifiers that are derived from different configurations within a single administrative domain (see 13.8).

### 8.9.3 FID to MSTID Allocation Table

The FID to MSTID Allocation Table defines, for all FIDs that the Bridge supports, the MSTID ~~of the spanning tree instance~~ to which the FID is allocated. ~~An MSTID of zero is used to identify the CIST.~~

- a) The IST is identified by the reserved MSTID value 0.
- b) The use of PBB-TE is identified by the reserved MSTID value TE-MSTID (0xFFE).
- c) Each MSTID in the MSTI List identifies an MSTI.  
The reserved MSTID values 0 and TE-MSTID, SPBV-MSTID, SPBM-MSTID and 0xFFFF are never used in the MSTI List.