

IEEE Std 802.1Q™, 2003 Edition

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

802.1Q™

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

Virtual Bridged Local Area Networks

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee



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

7 May 2003

Print: SH95124
PDF: SS95124

IEEE Std 802.1Q™, 2003 Edition
(Incorporates IEEE Std 802.1Q-1998, IEEE Std 802.1u™-2001,
IEEE Std 802.1v™-2001, and IEEE Std 802.1s™-2002)

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

Virtual Bridged Local Area Networks

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Abstract: This standard defines an architecture for Virtual Bridged LANs, the services provided in Virtual Bridged LANs, and the protocols and algorithms involved in the provision of those services.

Keywords: local area networks, MAC Bridge management, media access control bridges, virtual LANs

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

Copyright © 2003 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 7 May 2003. Printed in the United States of America.

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

Print: ISBN 0-7381-3662-X SH95124
PDF: ISBN 0-7381-3663-8 SS95124

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

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

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

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

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

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

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

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

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

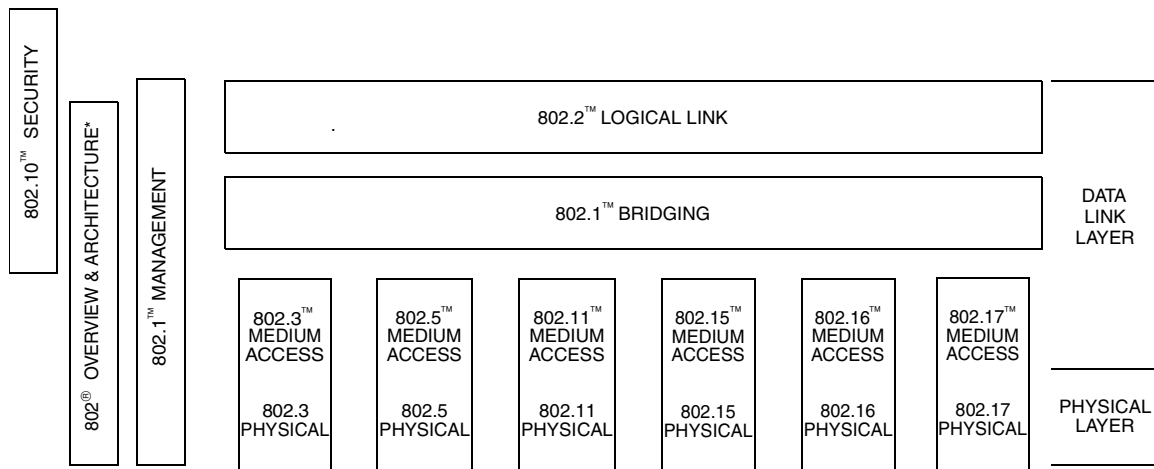
Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not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

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 to IEEE Std 802.1Q™, 2003 Edition

(This introduction is not part of IEEE Std 802.1Q, 2003 Edition, IEEE Standards for Local and metropolitan area networks— Virtual Bridged Local Area Networks.)

This standard is part of a family of standards for local and metropolitan area networks. The relationship between the standard and other members of the family is shown below. (The numbers in the figure refer to IEEE standard designations.¹)



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

The standards defining the technologies noted above are as follows:

- IEEE Std 802™:²
 - Overview and Architecture.* This standard provides an overview to the family of IEEE 802 Standards. This document forms part of the IEEE Std 802.1 scope of work.
- IEEE Std 802.1B™ and 802.1K™ [ISO/IEC 15802-2]:
 - LAN/MAN Management.* Defines an Open Systems Interconnection (OSI) management-compatible architecture, and services and protocol elements for use in a LAN/MAN environment for performing remote management.

¹The IEEE Standards referred to in the above figure and list are trademarks owned by the Institute of Electrical and Electronics Engineers, Incorporated.

²The IEEE 802 Overview and Architecture Specification, originally known as IEEE Std 802.1A, has been renumbered as IEEE Std 802. This has been done to accommodate recognition of the base standard in a family of standards. References to IEEE Std 802.1A should be considered as references to IEEE Std 802.

- IEEE Std 802.1D™ *Media Access Control (MAC) Bridges.* Specifies an architecture and protocol for the [ISO/IEC 15802-3]: interconnection of IEEE 802 LANs below the MAC service boundary.

- IEEE Std 802.1E™ *System Load Protocol.* Specifies a set of services and protocol [ISO/IEC 15802-4]: for those aspects of management concerned with the loading of systems on IEEE 802 LANs.

- IEEE Std 802.1F™ *Common Definitions and Procedures for IEEE 802 Management Information.*

- IEEE Std 802.1G™ *Remote Media Access Control (MAC) Bridging.* Specifies [ISO/IEC 15802-5]: extensions for the interconnection, using non-LAN systems communication technologies, of geographically separated IEEE 802 LANs below the level of the logical link control protocol.

- IEEE Std 802.1H™ *Recommended Practice for Media Access Control (MAC) Bridging of Ethernet V2.0 in IEEE 802 Local Area Networks.* [ISO/IEC TR 11802-5]

- IEEE Std 802.1Q™ *Virtual Bridged Local Area Networks.* Defines an architecture for Virtual Bridged LANs, the services provided in Virtual Bridged LANs, and the protocols and algorithms involved in the provision of those services.

- IEEE Std 802.2™ [ISO/IEC 8802-2]: *Logical Link Control.*

- IEEE Std 802.3™ [ISO/IEC 8802-3]: *CSMA/CD Access Method and Physical Layer Specifications.*

- IEEE Std 802.5™ [ISO/IEC 8802-5]: *Token Ring Access Method and Physical Layer Specifications.*

- IEEE Std 802.10™: *Standard for Interoperable LAN Security (SILS).* Currently approved: Secure Data Exchange (SDE).

- IEEE Std 802.11™: *Wireless LAN Medium Access Control (MAC) Sublayer and Physical Layer Specifications.* [ISO/IEC 8802-11]

- IEEE Std 802.15™: *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for: Wireless Personal Area Networks.*

- IEEE Std 802.16™: *Standard Air Interface for Fixed Broadband Wireless Access Systems.*

- IEEE P802.17™: *Resilient Packet Ring Access Method and Physical Layer Specifications.* Currently under development as a draft IEEE Standard.

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

Conformance test methodology

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

IEEE Std 802.1Q, 2003 Edition

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

IEEE Std 802.1D, 1998 Edition, an amended version of IEEE Std 802.1D-1993, extends this concept of Filtering Services in order to define additional capabilities in Bridged LANs aimed at

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

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

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

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

- l) Dynamic Group and VLAN registration to be restricted, based on the contents of static filtering entries;
- m) VLAN classification according to link layer protocol type;
- n) Support for VLANs carried over multiple Spanning Tree instances.

This 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
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Participants

The following is a list of participants in the Interworking activities of the IEEE 802.1 Working Group during the development of IEEE Std 802.1Q-1998 . Voting members at the time of publication are marked with an asterisk (*).

William P. Lidinsky, Chair*

Mick Seaman, Chair, Interworking Task Group*

Editing Team:

Tony Jeffree*, Coordinating Editor

Anil Rijisinhani*, Richard Hausman*, Michele Wright*, Paul Langille*, P. J. Singh*

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

The following persons were on the balloting committee of IEEE Std 802.1Q. Balloters may have voted for approval, disapproval, or abstention.

Corey Anderson	Stephen R. Haddock	Shimon Muller
Kit Athul	Allen W. Hathaway	Paul Nikolich
Thomas W. Bailey	Donald N. Heirman	Charles Oestereicher
Peter K. Campbell	Raj Jain	Roger Pandanda
James T. Carlo	Neil A. Jarvis	John R. Pickens
David E. Carlson	Anthony A. Jeffree	Vikram Punj
Alan M. Chambers	Robert W. Klessig	Edouard Y. Rocher
R. Allan Cobb	Stephen Barton Kruger	James W. Romlein
Robert S. Crowder	William G. Lane	Floyd E. Ross
Thomas J. Dineen	David J. Law	Michael Salzman
Peter Ecclesine	Lanse M. Leach	Norman Schneidewind
Philip H. Enslow	Randolph S. Little	Mick Seaman
Changxin Fan	Peter Martini	Rich Seifert
John W. Fendrich	Milan Merhar	Leo Sintonen
Michael A. Fischer	John L. Messenger	Michael A. Smith
Harvey A. Freeman	Bennett Meyer	Patricia Thaler
Gautam Garai	David S. Millman	Geoffrey O. Thompson
Harry Gold	John E. Montague	Mark-Rene Uchida
Julio Gonzalez-Sanz	Wayne D. Moyers	Oren Yuen

When the IEEE 802.1 Working Group approved Amendment 802.1u, it had the following membership:

Tony Jeffree, Chair and Editor

Neil Jarvis, Vice Chair

Mick Seaman, Chair, Interworking Task Group

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

The following members of the balloting committee voted on Amendment 802.1u. Balloters may have voted for approval, disapproval, or abstention.

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

When the IEEE 802.1 Working Group approved Amendment 802.1v, it had the following membership:

Tony Jeffree, *Chair and Editor*
Neil Jarvis, *Vice Chair*
Mick Seaman, *Chair, Interworking Task Group*
David Delaney, *Editor*
Andrew Smith, *Editor*

Floyd Backes
Les Bell
Alan Chambers
Marc Cochran
Paul Congdon
Hesham El Bakoury
Norman W. Finn
Sharam Hakimi
Bob Hott

Toyayuki Kato
Hal Keen
Daniel Kelley
Keith Klamm
Bill Lidinsky
Yaron Nachman
Satoshi Obara
Luc Pariseau
Anil Rijsinghani

John J. Roeser
Ted Schroeder
Benjamin Schultz
Rosemary V. Slager
Andrew Smith
Michel Soerensen
Robin Tasker
Manoj Wadekar
Robert Williams

The following members of the balloting committee voted on Amendment 802.1v. Balloters may have voted for approval, disapproval, or abstention.

Terry S. Arnold
James T. Carlo
Keith Chow
Robert S. Crowder
Guru Dutt Dhingra
Thomas J. Dineen
Christos Douligeris
Sourav K. Dutta
Philip H. Enslow
Changxin Fan
John W. Fendrich
Michael A. Fischer
Richard A. Froke
Robert J. Gagliano
Gautam Garai
Alireza Ghazizahedi
Tim Godfrey
Robert M. Grow
Chris G. Guy
Simon Harrison

Osamu Ishida
Raj Jain
Kamran Jamal
Neil A. Jarvis
Anthony A. Jeffree
Jack R. Johnson
Stuart J. Kerry
Daniel R. Krent
Stephen Barton Kruger
Joseph Kubler
David J. Law
William Lidinsky
Randolph S. Little
Ronald Mahany
Peter Martini
Bennett Meyer
David S. Millman
James F. Mollenauer
John E. Montague

Robert Mortonson
Robert O'Hara
Satoshi Obara
Roger Pandanda
Vikram Punj
Gary S. Robinson
Edouard Y. Rocher
James W. Romlein
Floyd E. Ross
Jaideep Roy
Rich Seifert
Leo Sintonen
Joseph S. Skorupa
Fred J. Strauss
Jonathan R. Thatcher
Mark-Rene Uchida
Scott A. Valcourt
John Viaplana
Paul A. Willis
Oren Yuen

When the IEEE 802.1 Working Group approved Amendment 802.1s, it had the following membership:

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

Les Bell
Paul Congdon
Hesham Elbakoury
Robert W. Hott

Ran Ish-Shalom
Shyam Kaluve
Hal Keen
Loren Larsen

Frank Reichstein
Curtis Simonson
Michel Thorsen
Michael D. Wright

The following members of the balloting committee voted on Amendment 802.1s. Balloters may have voted for approval, disapproval, or abstention.

Vishal Anand
Linda Cheng
Keith Chow
Dr. Guru Dutt Dhingra
Thomas Dineen
Michael Eckhoff
Mike Geipel
Stuart Holoman
Raj Jain

Tony Jeffree
Pranav Koushik
Jeffrey Lynch
Kyle Maus
George Miao
Paul Nikolich
Ellis Nolley
Satoshi Obara
Subbu Ponnuswamy

Vikram Punj
Maximilian Riegel
Thomas Ruf
Mick Seaman
Rich Seifert
Pat Thaler
Dmitri Varsanofiev
Cassio Vinhal
Oren Yuen

When the IEEE-SA Standards Board approved this standard on 8 December 1998, it had the following membership:

Richard J. Holleman, *Chair*

Donald N. Heirman, *Vice Chair*

Judith Gorman, *Secretary*

Satish K. Aggarwal
Clyde R. Camp
James T. Carlo
Gary R. Engmann
Harold E. Epstein
Jay Forster*
Thomas F. Garrity
Ruben D. Garzon

James H. Gurney
Jim D. Isaak
Lowell G. Johnson
Robert Kennelly
E. G. "Al" Kiener
Joseph L. Koepfinger*
Stephen R. Lambert
Jim Logothetis
Donald C. Loughry

L. Bruce McClung
Louis-François Pau
Ronald C. Petersen
Gerald H. Peterson
John B. Posey
Gary S. Robinson
Hans E. Weinrich
Donald W. Zipse

*Member Emeritus

Kristin M. Dittmann
*IEEE Standards Project Editor,
IEEE Std 802.1Q-1998*

Jennifer McClain Longman
*IEEE Standards Project Editor,
IEEE Std 802.1u-2001
IEEE Std 802.1v-2001*

Andrew Ickowicz
*IEEE Standards Project Editor,
IEEE Std 802.1s-2002
IEEE Std 802.1Q, 2003 Edition*

Contents

1.	Overview	1
1.1	Scope.....	1
1.2	VLAN aims and benefits	2
1.3	Relationship with IEEE Std 802.1D	2
2.	References.....	4
3.	Definitions	7
4.	Abbreviations.....	11
5.	Conformance.....	12
5.1	Static conformance requirements.....	12
5.2	Options.....	13
5.3	Protocol Implementation Conformance Statement (PICS).....	14
5.4	MAC-specific bridging methods.....	14
6.	Support of the MAC Service in VLANs.....	15
6.1	Support of the MAC service	15
6.2	Preservation of the MAC service.....	15
6.3	Quality of service maintenance.....	15
6.4	Enhanced Internal Sublayer Service provided within VLAN Bridges	20
6.5	Support of the Internal Sublayer Service by IEEE Std 802.3 (CSMA/CD)	24
7.	Principles of network operation	25
7.1	Network Overview.....	25
7.2	Use of VLANs	26
7.3	VLAN Topology	26
7.4	Locating end stations	27
7.5	Ingress, Forwarding, and Egress Rules.....	29
8.	Principles of bridge operation.....	31
8.1	Bridge operation	31
8.2	Bridge architecture.....	33
8.3	Model of operation.....	36
8.4	Port states and parameters.....	41
8.5	Frame reception	43
8.6	The Forwarding Process	44
8.7	Frame transmission.....	50
8.8	The Learning Process.....	51
8.9	VLAN classification	51
8.10	The Filtering Database.....	55
8.11	MST configuration information.....	68
8.12	Spanning Tree Protocol Entity and GARP Protocol Entities	69
8.13	Bridge Management.....	70
8.14	Addressing	70

9.	Tagged frame format.....	79
9.1	Overview.....	79
9.2	Transmission and representation of octets.....	82
9.3	Structure of the tag header.....	82
10.	Use of GMRP in VLANs.....	90
10.1	Definition of a VLAN Context.....	90
10.2	GMRP Participants and GIP Contexts.....	90
10.3	Context identification in GMRP PDUs.....	91
10.4	Default Group filtering behavior and GMRP propagation.....	91
11.	VLAN topology management.....	93
11.1	Static and dynamic VLAN configuration.....	93
11.2	GARP VLAN Registration Protocol.....	94
11.3	Conformance to GVRP.....	99
11.4	Procedural model.....	100
12.	VLAN Bridge Management.....	110
12.1	Management functions.....	110
12.2	Managed objects.....	111
12.3	Data types.....	111
12.4	Bridge Management Entity.....	112
12.5	MAC entities.....	115
12.6	Forwarding process.....	115
12.7	Filtering Database.....	119
12.8	Bridge Protocol Entity.....	124
12.9	GARP Entities.....	132
12.10	Bridge VLAN managed objects.....	134
12.11	GMRP entities.....	145
12.12	MST configuration entities.....	146
13.	The Multiple Spanning Tree Protocol (MSTP).....	152
13.1	Protocol Design Requirements.....	152
13.2	Protocol Support Requirements.....	153
13.3	MSTP Overview.....	153
13.4	Relationship of MSTP to RSTP.....	158
13.5	Modelling an MST Region as a single RSTP Bridge.....	159
13.6	STP and RSTP compatibility.....	160
13.7	MST Configuration Identification.....	161
13.8	MST Regions.....	162
13.9	Spanning Tree Priority Vectors.....	163
13.10	CIST Priority Vector Calculations.....	164
13.11	MST Priority Vector Calculations.....	166
13.12	Port Role Assignments.....	168
13.13	Stable Connectivity.....	168
13.14	Communicating Spanning Tree Information.....	170
13.15	Changing Spanning Tree Information.....	171
13.16	Changing Port States.....	172
13.17	Updating Learned Station Location Information.....	177

13.18 MSTP and point-to-point links	178
13.19 Multiple Spanning Tree State Machines.....	178
13.20 Notational Conventions used in State Diagrams	180
13.21 State Machine Timers	180
13.22 State Machine Performance Parameters	181
13.23 Per-Bridge Variables.....	182
13.24 Per-Port Variables.....	184
13.25 State Machine Conditions.....	189
13.26 State Machine Procedures.....	191
13.27 The Port Timers state machine	198
13.28 Port Receive state machine	199
13.29 Port Protocol Migration state machine	199
13.30 Port Transmit state machine	200
13.31 Port Information state machine.....	201
13.32 Port Role Selection state machine	201
13.33 Port Role Transitions state machine	202
13.34 Port State Transition state machine	205
13.35 Topology Change state machine.....	205
13.36 Performance	206
14. Use of BPDUs by MSTP	208
14.1 BPDU Structure	208
14.2 Encoding of parameter types	208
14.3 BPDU formats and parameters	210
14.4 Validation of received BPDUs	210
14.5 Transmission of BPDUs	211
14.6 Encoding and decoding of STP Configuration, RST, and MST BPDUs	211
Annex A (normative) PICS proforma.....	215
Annex B (informative) Shared and Independent VLAN Learning	245
Annex C (informative) MAC method dependent aspects of VLAN support	253
Annex D (informative) Background to VLANs	284
Annex E (informative) Interoperability considerations.....	290
Annex F (informative) Frame translation considerations.....	302
Annex G (informative) Differences between 802.1s and 802.1w state machines.....	304

IEEE Standards for Local and metropolitan area networks—

Virtual Bridged Local Area Networks

1. Overview

IEEE 802™ Local Area Networks (LANs) of all types can be connected together with Media Access Control (MAC) Bridges, as specified in IEEE Std 802.1D™, 1998 Edition¹. This standard defines the operation of Virtual LAN (VLAN; see 3.38) Bridges that permit the definition, operation, and administration of VLAN topologies within a Bridged LAN (see 3.35) infrastructure.

1.1 Scope

For the purpose of compatible interconnection of information technology equipment using the IEEE 802 MAC Service supported by interconnected IEEE 802 standard LANs using different or identical MAC methods, this standard specifies a general method for the operation of MAC Bridges that support the construction of VLANs (see 3.38). To this end it

- a) Positions the function of VLANs within an architectural description of the MAC Sublayer;
- b) Defines enhancements to the Support of the MAC Service, as described and defined in IEEE Std 802.1D, 1998 Edition, for the purposes of VLAN Bridging;
- c) Specifies an Enhanced Internal Sublayer Service provided to the Media Access Independent functions that provide frame relay (3.7) in the VLAN Bridge;
- d) Specifies the operation of the functions that provide frame relay in the VLAN Bridge;
- e) Defines the structure, encoding, and interpretation of the VLAN control information carried in tagged frames (3.33) in a VLAN;
- f) Specifies the rules that govern the insertion and removal of VLAN control information in frames;
- g) Specifies the rules that govern the ability to carry data in Canonical format and Non-canonical format using different LAN MAC methods;

NOTE—The meanings of the terms *Canonical format* and *Non-canonical format* are discussed in Annex F.

- h) Establishes the requirements for, and specifies the means of, automatic configuration of VLAN topology information;
- i) Defines the management functionality that may be provided in a VLAN Bridge in order to facilitate administrative control over VLAN operation;
- j) Defines the operation of the Multiple Spanning Tree algorithm and protocol (MSTP);
- k) Defines the enhancements made to the Rapid Spanning Tree Algorithm and Protocol in order to create MSTP;
- l) Describes the protocols and procedures necessary to support interoperation between MST and SST Bridges in the same Bridged LAN;
- m) Specifies the requirements to be satisfied by equipment claiming conformance to this standard.

¹Information about references can be found in Clause 2.

1.2 VLAN aims and benefits

VLANs aim to offer the following benefits:

- a) VLANs are supported over all IEEE 802 LAN MAC protocols, and over shared media LANs as well as point-to-point LANs.
- b) VLANs facilitate easy administration of logical groups of stations that can communicate as if they were on the same LAN. They also facilitate easier administration of moves, adds, and changes in members of these groups.
- c) Traffic between VLANs is restricted. Bridges forward unicast, multicast, and broadcast traffic only on LAN segments that serve the VLAN to which the traffic belongs.
- d) As far as possible, VLANs maintain compatibility with existing bridges and end stations.
- e) If all Bridge Ports are configured to transmit and receive untagged frames (3.36), bridges will work in plug-and-play IEEE Std 802.1D mode. End stations will be able to communicate throughout the Bridged LAN.

NOTE—Whether a VLAN Bridge will operate in IEEE Std 802.1D mode depends upon the configuration of the various Port parameters (8.4) and the Filtering Database (8.11). A VLAN Bridge in its default configuration is transparent to untagged frames (3.36) but is not transparent to tagged frames (3.33), so the operation of such Bridges in the presence of tagged traffic differs from that of an IEEE Std 802.1D Bridge. If the configuration settings of VLAN Bridges are changed from the default values defined in this standard, then transparency with respect to untagged frames may also be affected.

1.3 Relationship with IEEE Std 802.1D

This standard makes use of specific aspects of the MAC Bridge specification contained in IEEE Std 802.1D; those aspects therefore become provisions of this standard. Table 1-1 shows how the relevant clauses of IEEE Std 802.1D, 1998 Edition are incorporated into this standard.

Table 1-1—Relationship between this standard and IEEE Std 802.1D

IEEE Std 802.1D clause	Use in this standard
5. Conformance	Provision of this standard, as extended by Clause 5
6. Support of the MAC Service	Provision of this standard, as modified by Clause 6
7. Principles of operation	Replaced by Clause 8
8. The spanning tree algorithm and protocol	Provision of this standard
9. Encoding of bridge protocol data units	Provision of this standard
10. GARP Multicast Registration Protocol (GMRP)	Provision of this standard, as modified by Clause 11
11. Example “C” code implementation of GMRP	Provision of this standard, as modified by Clause 11
12. Generic Attribute Registration Protocol (GARP)	Provision of this standard
13. Example “C” code implementation of GARP	Provision of this standard
14. Bridge management	Replaced by Clause 12
15. Management protocol	Not applicable
16. Bridge performance	Provision of this standard
17. Rapid Spanning Tree Algorithm and Protocol	Provision of this standard, as modified by Clauses 13 and 14
Annex A (normative) PICS proforma	Replaced by Annex A
Annex B (informative) Calculating Spanning Tree parameters	Provision of this standard
Annex C (normative) Source-routing transparent bridge operation	Provision of this standard
Annex D (normative) PICS proforma for source routing transparent bridge operation	Provision of this standard
Annex E (normative) Allocation of Object Identifier values	Not applicable
Annex F (informative) Target topology, migration, and interoperability	Provision of this standard
Annex G (informative) Preserving the integrity of FCS fields in MAC Bridges	Provision of this standard
Annex H (informative) Design considerations for Traffic Class Expediting and Dynamic Multicast Filtering	Provision of this standard

2. References

The following standards contain provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

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

IEEE Std 802™-1990, IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture.³

IEEE Std 802.1B™, 1995 [ISO/IEC 15802-2: 1995], IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 2: LAN/MAN Management.

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

IEEE Std 802.1D, 1998 Edition [ISO/IEC 15802-3: 1998], IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 3: Media Access Control (MAC) Bridges.

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

IEEE Std 802.1H™-1997 [ISO/IEC 11802-5: 1997], IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and Metropolitan Area Networks—Technical Reports and Guidelines—Part 5: Media Access Control Bridging of Ethernet V2.0 in IEEE 802 Local Area Networks.

IEEE Std 802.1t™-2001, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 3: Media Access Control (MAC) Bridges—Amendment 1.

IEEE Std 802.1w™-2001, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 3: Media Access Control (MAC) Bridges—Amendment 2: Rapid Reconfiguration. [Amendment to IEEE Std 802.1D, 1998 Edition (ISO/IEC 15802-3:1998) and IEEE Std 802.1t-2001]

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

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

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

³IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (<http://standards.ieee.org/>).

IEEE Std 802.3TM, 1998 Edition, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

IEEE Std 802.3acTM-1998, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Supplement to Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications: Frame Extensions for Virtual Bridged Local Area Network (VLAN) tagging on 802.3 Networks.

IEEE Std 802.4TM-1990 [ISO/IEC 8802-4: 1990], IEEE Standard for Information processing systems—Local area networks—Part 4: Token-passing bus access method and physical layer specifications.⁴

IEEE Std 802.5TM, 1998 Edition [ISO/IEC 8802-5: 1998], IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 5: Token ring access method and physical layer specifications.

IEEE Std 802.6TM, 1994 Edition [ISO/IEC 8802-6: 1994], IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 6: Distributed Queue Dual Bus (DQDB) access method and physical layer specifications.⁴

IEEE Std 802.9TM, 1996 Edition [ISO/IEC 8802-9: 1996], IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 9: Integrated Services (IS) LAN Interface at the Medium Access Control (MAC) and Physical (PHY) Layers.⁴

IEEE Std 802.9aTM-1995, IEEE Standards for Local and Metropolitan Area Networks: Supplement to Integrated Services (IS) LAN Interface at the Medium Access Control (MAC) and Physical (PHY) Layers: Specification of ISLAN 16-T.

IEEE Std 802.12TM, 1998 Edition [ISO/IEC 8802-12: 1998], IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 12: Demand-Priority access method, physical layer and repeater specifications.⁴

IETF RFC 1042, Postel & Reynolds, A Standard for the Transmission of IP Datagrams over IEEE 802 Networks, February 1988.⁵

IETF RFC 1390, D. Katz, Transmission of IP and ARP over FDDI Networks, January 1993.

IETF RFC 2104, HMAC: Keyed-Hashing for Message Authentication, Krawczyk, H., Bellare, M., and R. Canetti, February 1997.⁶

ISO 6937-2: 1994, Information technology—Coded graphic character set for text communication—Latin alphabet.⁷

⁴This IEEE Standard has been withdrawn; future revisions of IEEE Std 802.1Q will address its presence in the text of IEEE Std 802.1Q, 2003 Edition.

⁵Internet RFCs are retrievable by FTP at [ds.internic.net/rfc/rfcnnnn.txt](ftp://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.

⁶IETF documents are available at <http://www.ietf.org>.

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

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

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

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

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

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

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

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

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

ISO/IEC 15802-1: 1995, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 1: Medium Access Control (MAC) service definition.

3. Definitions

The following terms are specific to this standard:

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

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

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

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

NOTE—The procedure for untagging a frame is discussed in 9.1.

3.5 Ethernet Type-encoding: The use of the Type interpretation of an IEEE 802.3 Length/Type field value in a frame as a protocol identifier associated with the MAC Service user data carried in the frame.⁸

NOTES

1—The term *frame* is defined in 3.6.

2—Ethernet Type-encoding can be used with MAC Service user data carried on non-IEEE 802.3 MACs by means of the SNAP-based encapsulation techniques specified in IEEE Std 802.1H, IETF RFC 1042, and IETF RFC 1390.

3.6 Frame: A unit of data transmission on an IEEE 802 LAN MAC that conveys a protocol data unit (PDU) between MAC Service users. There are three types of frame; *untagged*, *VLAN-tagged*, and *priority-tagged*.

NOTE—The term *IEEE 802 LAN* is defined in IEEE Std 802.1D, 1998 Edition. *Untagged frame* is defined in 3.36, *VLAN-tagged frame* is defined in 3.40, and *priority-tagged frame* is defined in 3.20.

3.7 Frame relay: The function of the Forwarding Process that forwards frames between the Ports of a Bridge.

NOTE—The operation of the Forwarding Process is defined in 8.7.

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

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

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

3.10 Internal Spanning Tree (IST): The connectivity provided by the CIST within a given MST Region.

⁸The use of Ethernet Type values as a means of protocol identification was defined in the specification of Ethernet V2.0 (The Ethernet, AA-K759B-TK, Digital Equipment, Intel, and Xerox Corps., Nov. 1982).

3.11 Legacy region: A set of LAN segments interconnected such that there is physical connectivity between any pair of segments using only IEEE Std 802.1D, 1998 Edition-conformant, VLAN-unaware MAC Bridges.

NOTE—In other words, if, in a Bridged LAN containing both IEEE Std 802.1D, 1998 Edition and IEEE 802.1Q Bridges, all the IEEE 802.1Q Bridges were to be removed, the result would be a set of one or more Bridged LANs, each with its own distinct Spanning Tree. Each of those Bridged LANs is a legacy region. The term *VLAN-unaware* is defined in 3.41.

3.12 Logical Link Control (LLC) encoding: The use of LLC addressing information in a frame as a protocol identifier associated with the MAC Service user data carried in the frame.

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

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

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

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

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

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

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

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

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

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

NOTE—The term *tagged frame* is defined in 3.33; *tag header* is defined in 3.34. See also *VLAN-tagged frame* (3.40) and *untagged frame* (3.36).

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

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

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

3.24 Rapid Spanning Tree Algorithm and Protocol (RSTP): The Rapid Spanning Tree Algorithm and Protocol described in Clause 17 of IEEE Std 802.1w-2001.

3.25 Rapid Spanning Tree Bridge Protocol Data Unit (RST BPDU): The RST BPDU specified in Clause 9 of IEEE Std 802.1w-2001.

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

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

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

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

3.29 Single Spanning Tree (SST) Bridge: A Bridge capable of supporting only a single spanning tree, the CST. The single spanning tree may be supported by the Spanning Tree Algorithm and Protocol (STP) defined in IEEE Std 802.1D, 1998 Edition, or by the Rapid Spanning Tree Algorithm and Protocol (RSTP), defined in IEEE Std 802.1w-2001.

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

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

3.32 Spanning Tree Bridge Protocol Data Unit (ST BPDU): A Bridge Protocol Data Unit specified for use by the Spanning Tree Algorithm and Protocol, i.e. a Configuration or Topology Change Notification BPDU as described in Clause 9 of IEEE Std 802.1D, 1998 Edition.

3.33 Tagged frame: A *tagged frame* is a frame that contains a tag header immediately following the Source MAC Address field of the frame or, if the frame contained a Routing Information field, immediately following the Routing Information field. There are two types of tagged frames: VLAN-tagged frames and priority-tagged frames.

NOTE—The term *tag header* is defined in 3.34, *priority-tagged frame* is defined in 3.20, and *VLAN-tagged frame* is defined in 3.40. See also *untagged frame* (3.36).

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

NOTE—The structure of the tag header is defined in 9.3.

3.35 Terms used in IEEE Std 802.1D, 1998 Edition: The following terms used in this standard are used in IEEE Std 802.1D, 1998 Edition:

Active topology
Bridge Port
Bridged Local Area Network (also Bridged LAN)
GARP Participant
GARP Application
GIP Context
Group
IEEE 802 Local Area Network (also IEEE 802 LAN, or LAN)
Port

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

NOTE—The term *tag header* is defined in 3.34. See also *tagged frame* (3.33).

3.37 Virtual Bridged Local Area Network (LAN): A Bridged LAN in which the existence of one or more VLAN-aware Bridges allows the definition, creation, and maintenance of VLANs.

NOTE—The term *VLAN-aware* is defined in 3.39.

3.38 Virtual Local Area Network (VLAN): A subset of the active topology of a Bridged Local Area Network. Associated with each VLAN is a VLAN Identifier (VID).

3.39 VLAN-aware: A property of Bridges or end stations that recognize and support VLAN-tagged frames.

3.40 VLAN-tagged frame: A tagged frame whose tag header carries both VLAN identification and priority information.

3.41 VLAN-unaware: A property of Bridges or end stations that do not recognize VLAN-tagged frames.

4. Abbreviations

The following abbreviations are used in this standard:

BPDU	Bridge Protocol Data Unit (IEEE Std 802.1D, 1998 Edition)
CFI	Canonical Format Indicator (Annex F)
CIST	Common and Internal Spanning Tree
CST	Common Spanning Tree
E-ISS	Enhanced Internal Sublayer Service (7.1)
FCS	Frame Check Sequence (7.1)
FID	Filtering Identifier (8.11.3, 8.11.7)
GARP	Generic Attribute Registration Protocol (IEEE Std 802.1D, 1998 Edition)
GID	GARP Information Declaration (IEEE Std 802.1D, 1998 Edition)
GIP	GARP Information Propagation (IEEE Std 802.1D, 1998 Edition)
GMRP	GARP Multicast Registration Protocol (Clause 10, IEEE Std 802.1D, 1998 Ed.)
GVRP	GARP VLAN Registration Protocol (Clause 11)
ISS	Internal Sublayer Service (Clause 7, IEEE Std 802.1D, 1998 Edition)
IST	Internal Spanning Tree
IVL	Independent VLAN Learning (3.8)
LAN	Local Area Network (IEEE Std 802)
LS	Least-significant
LLC	Logical Link Control (IEEE Std 802.2)
MAC	Medium Access Control (IEEE Std 802)
MCID	MST Configuration Identifier
MIB	Management Information Base (ISO/IEC 7498-4)
MS	Most-significant
MSDU	MAC Service Data Unit (ISO/IEC 15802-1)
MST	Multiple Spanning Tree
MST BPDU	Multiple Spanning Tree Bridge Protocol Data Unit
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
NCFI	Non-Canonical Format Indicator (Annex F)
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement (Annex A)
PID	Protocol Identifier
PVID	Port VID (8.4.4)
RIF	Routing Information Field (IEEE Std 802.5)
RST BPDU	Rapid Spanning Tree Bridge Protocol Data Unit
RSTP	Rapid Spanning Tree Protocol
SST	Single Spanning Tree
ST BPDU	Spanning Tree Bridge Protocol Data Unit
STP	Spanning Tree Protocol
STPID	SNAP-encoded Tag Protocol Identifier (9.3)
SVL	Shared VLAN Learning (3.26)
TCI	Tag Control Information (9.3)
TPID	Tag Protocol Identifier (9.3)
VID	VLAN Identifier (7.1, 8.4.4, 9.3)
VLAN	Virtual LAN (3.38)

5. Conformance

5.1 Static conformance requirements

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

- a) Conform to the requirements of IEEE Std 802.1D, 1998 Edition, and IEEE Std 802.1w-2001, as modified by the provisions of this standard;
- b) Relay and filter frames as described in 8.1 and specified in 8.5, 8.6, 8.7, 8.8, and 8.9;
- c) On each Port, support at least one of the permissible values for the Acceptable Frame Types parameter, as defined in 8.4.3;
- d) Support the following on each Port that supports untagged and priority-tagged frames:
 - 1) A Port VLAN Identifier (PVID) value (8.4.4);
 - 2) The ability to configure at least one VLAN whose untagged set includes that Port (8.8 and 8.11.9);
 - 3) Configuration of the PVID value via management operations (12.10);
 - 4) Configuration of Static Filtering Entries via management operations (12.7).
- e) Support the ability to insert tag headers into, modify tag headers in, and remove tag headers from relayed frames, as described and specified in 7.1 and Clause 9, as required by the value(s) of the Acceptable Frame Types parameter that are supported on each Port, and by the ability of each Port to be configured to transmit VLAN-tagged frames and/or untagged frames. These requirements are summarized in Table 5-1 for frames relayed between any pair of Ports;

Table 5-1—Support requirements for insertion, removal, and modification of tag headers

		Reception Port receives as (and does not discard):		
		VLAN-tagged	Priority-tagged	Untagged
Transmission Port transmits as:	Untagged	Shall support removal of tag headers.	Shall support removal of tag headers.	N/A.
	VLAN-tagged	Shall support conversion of the tagged frame format if the format required for the destination MAC differs from the received format.	Shall support the insertion of a non-null Virtual LAN Identifier (VID) in tag headers, plus conversion of the tagged frame format if the format required for the destination MAC differs from the received format.	Shall support the insertion of tag headers of a format appropriate to the destination MAC, carrying a non-null VID.

- f) Support the ability to perform automatic configuration and management of VLAN topology information by means of Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) (Clause 11) on all Ports;
- g) Support the ability for the Filtering Database to contain static and dynamic configuration information for at least one VLAN, by means of Static and Dynamic VLAN Registration Entries (8.11);
- h) Support at least one Filtering Identifier (FID) (6.4, 8.11.3, 8.11.7, and 8.11.8);
- i) Support the ability to allocate at least one VID to each FID that is supported (6.4, 8.11.3, 8.11.7, and 8.11.8).

NOTE 1—Under some circumstances, the ability for VLAN Bridges to successfully interoperate depends upon the number of FIDs supported, and the number of VIDs that can be allocated to each FID. These circumstances are discussed in Annex B, along with the implications with respect to interoperability.

- j) A MAC bridge for which conformance to the provisions of this standard for an MST Bridge is claimed (5.2, 13) shall:
 - 1) Support the Multiple Spanning Tree Algorithm and Protocol, (MSTP) as specified in Clause 13 and the attendant conformance requirements stated in Clause 5 of IEEE Std 802.1w-2001;
 - 2) Support the CIST plus a stated maximum number of MSTIs, where that number is at least 2 (8.10.7) and at most 64 (13.14);

NOTE 2—In other words, a conformant MST Bridge must support a minimum of three spanning tree instances—the CIST and at least two additional MSTIs.

- 3) Support a stated maximum number of FIDs that is at least as large as the number of MSTIs supported (8.10.7);
- 4) Support the ability to associate each FID to a spanning tree (8.11.3);
- 5) Support the transmission and reception of MST Configuration Identifier information (8.11.2).
- 6) For each Port, be capable of supporting a set of port-state information for each spanning tree instance supported (8.4.1, 8.4.2, 13.34);
- 7) For each Port, be capable of supporting an instance of the Spanning Tree Protocol and its associated parameters for each spanning tree instance supported (8.12, 13);
- 8) Use the Bridge Group Address as specified in 8.14.3;
- 9) Support the default values for Bridge Forward Delay and Bridge Priority parameters specified in 13.23;
- 10) Support the operation of GVRP in each supported spanning tree context (11.2.3.3, 11.2.3.4);
- 11) Support the VLAN bridge management functions for the bridge protocol entity for each supported spanning tree, independently (12.8)
- 12) Support, in particular, management of the bridge priority parameters, and of the port priority and path cost parameters for every port, independently for each supported spanning tree (12.8.1.1, 12.8.1.3, 13.24);
- 13) Support the VLAN management functions for each supported spanning tree (12.10.1 and 12.11.1);
- 14) Support management of the MSTI configuration (12.12).

5.2 Options

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

- a) Support operation in Extended Filtering Mode (IEEE Std 802.1D, 1998 Edition, 6.6.5) and the operation of GARP Multicast Registration Protocol (GMRP) (IEEE Std 802.1D, 1998 Edition, Clause 10) as modified by Clause 10;
- b) Support the ability for the Filtering Database to contain static and dynamic configuration information for more than one VLAN, by means of Static and Dynamic VLAN Registration Entries (8.11), up to a maximum of 4094 VLANs;

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

- c) On each Port, support both of the permissible values for the Acceptable Frame Types parameter, as defined in 8.4.3. If both values are supported, then the implementation shall support configuration of the parameter value via management;
- d) Support the ability to enable and disable Ingress Filtering (8.4.5);

- e) Support the ability to configure more than one VLAN whose untagged set includes that Port (8.8 and 8.11.9);
- f) Support the management functionality defined in Clause 12;
- g) Support more than one FID (6.4, 8.11.3, 8.11.7, and 8.11.8);
- h) Support the ability to allocate more than one VID to each FID that is supported (6.4, 8.11.3, 8.11.7, and 8.11.8);
- i) Support the ability to configure VLAN Learning Constraints via management (8.11.7 and 12.10.3);
- j) Support the ability to configure fixed VID to FID allocations via management (8.11.7.1 and 12.10.3);
- k) Support any other optional capabilities defined in IEEE Std 802.1D, 1998 Edition, as modified by the provisions of this standard.
- l) Support Port-and-Protocol-based VLAN classification, including multiple VID values per port, administrative control of the values of the multiple VIDs, and a Protocol Group Database. If this option is supported:
 - 1) One or more of the following Protocol Classifications and Protocol Template formats must be supported: Ethernet, RFC_1042, SNAP_8021H, SNAP_Other, or LLC_Other (8.6.1 and 8.6.2).
 - 2) The configuration of the contents of the Protocol Group Database may be supported.
- m) Support the ability to configure the value of the Restricted_Group_Registration parameter (10.3.2 in IEEE Std 802.1t-2001) for each Port of the Bridge;
- n) Support the ability to configure the value of the Restricted_VLAN_Registration parameter (11.2.3.2.3) for each Port of the Bridge.
- o) Support MST operation (7, 8.4.1, 8.4.2, 8.6.2, 8.10.7, 8.11, 8.12, 8.14.3, 11.2.3.4, 11.3.1, 13, 14.);
- p) A MAC bridge for which support of MSTP is claimed (13) may support a greater number of FIDs than spanning trees (8.10.7).

5.3 Protocol Implementation Conformance Statement (PICS)

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

5.4 MAC-specific bridging methods

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

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

IEEE Std 802.1D, 1998 Edition, Annex C, defines one such MAC-specific bridging method, source routing, and that method is also a provision of this standard. While this standard defines how source-routed frames can be transported in a VLAN environment, it does not attempt to specify VLAN aspects of the source routing bridging method itself.

6. Support of the MAC Service in VLANs

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

6.1 Support of the MAC service

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

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

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

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

NOTE—Authentication and authorization to access a LAN may be achieved by administrative or management mechanisms, or by means of an active authorization mechanism, such as is defined in IEEE Std 802.1X-2001.

6.2 Preservation of the MAC service

The MAC Service offered by a Virtual Bridged LAN consisting of LANs interconnected by VLAN Bridges is similar to that offered by a single LAN (see 6.3). In consequence,

- a) A VLAN Bridge is not directly addressed by communicating end stations, except as an end station for management purposes: frames transmitted between end stations carry the MAC Address of the peer-end station in their Destination Address field, not the MAC Address, if any, of the VLAN Bridge.
- b) All MAC Addresses must be unique within any set of VLANs supported by the Virtual Bridged LAN that share the same Filtering Identifier (FID).
- c) The MAC Addresses of end stations are not restricted by the topology and configuration of the Virtual Bridged LAN.

6.3 Quality of service maintenance

6.3.1 Service availability

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

The service availability can be increased by automatic reconfiguration of the Virtual Bridged LAN in order to avoid the use of a failed component (e.g., repeater, cable, or connector) in the data path. The service availability can be lowered by failure of a VLAN Bridge itself, through denial of service by the VLAN Bridge, or through frame filtering by the VLAN Bridge. Changes in topology, caused by component failures, the addition or removal of components, or by administrative changes, are detected and signalled by the following means:

- a) Physical detection of component failure and signalling of that failure by the Enhanced Internal Sub-layer Service (6.4 and 6.5);
- b) Detection of component failure through the operation of a spanning tree algorithm and protocol;
- c) Explicit signalling of reconfiguration events through the operation of a spanning tree algorithm and protocol.

Automatic reconfiguration can be achieved rapidly on the detection of a physical topology change (see Clause 17 of IEEE Std 802.1w-2001), thus minimizing any service denial that is caused by the reconfiguration.

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

To minimize the effects of service denial caused by reconfiguration events, filtering information that has been dynamically learnt can be modified when automatic reconfiguration takes place, or in preparation for future reconfiguration events (Clause 17 and 17.10 of IEEE Std 802.1w-2001). However, filtering information that is statically configured cannot be modified in this way.

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

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

NOTE 1—This is true only in circumstances where admission control mechanisms are not present, i.e., where the VLAN Bridges provide a “best effort” service. The specification and applicability of admission control mechanisms in VLAN Bridges is outside the scope of this standard.

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

6.3.2 Frame loss

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

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

- a) Frame corruption during physical layer transmission or reception.
- b) Frame discard by a VLAN Bridge because
 - 1) It is unable to transmit the frame within some maximum period of time and, hence, must discard the frame to prevent the maximum frame lifetime (6.3.6) from being exceeded.
 - 2) It is unable to continue to store the frame due to exhaustion of internal buffering capacity as frames continue to arrive at a rate in excess of that at which they can be transmitted.
 - 3) The size of the service data unit carried by the frame exceeds the maximum supported by the MAC procedures employed on the LAN to which the frame is to be relayed.
 - 4) Changes in the connected topology of the Virtual Bridged LAN necessitate frame discard for a limited period of time to maintain other aspects of Quality of Service (see 8.3.3 of IEEE Std 802.1D, 1998 Edition, and 17.9 of IEEE Std 802.1w-2001).
 - 5) The device attached to the Port is not authorized for access to the network.
 - 6) The configuration of Static Filtering Entries or Static VLAN Registration Entries in the Filtering Database (8.11.1, 8.11.2) disallows the forwarding of frames with particular destination addresses or VLAN classifications on specific Ports.

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

6.3.3 Frame misordering

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

NOTE 1—The operation of the Forwarding Process in VLAN Bridges (8.7) is such that the frame-ordering characteristics of the MAC Service are preserved.

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

NOTE 2—Where STP is in use (see Clause 8 of IEEE Std 802.1D, 1998 Edition), frame misordering cannot occur during normal operation. Where RSTP is in use (see Clause 17 of IEEE Std 802.1w-2001), there is an increased probability that frames that are in transit through the Virtual Bridged LAN will be misordered, due to the fact that a VLAN Bridge can buffer frames awaiting transmission through its Ports. The probability of misordering occurring as a result of such an event is dependent upon implementation choices, and is associated with Spanning Tree reconfiguration events. Some known LAN protocols, for example, LLC Type 2, are sensitive to frame duplication; in order to allow VLAN Bridges that support RSTP to be used in environments where sensitive protocols are in use, the forceVersion parameter (17.16.1 of IEEE Std 802.1w-2001) can be used to force a VLAN Bridge that supports RSTP to operate in an STP-compatible manner. A more detailed discussion of misordering in RSTP can be found in F.2.4 of IEEE Std 802.1w-2001.

6.3.4 Frame duplication

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

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

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

NOTE—Where RSTP is in use (see Clause 17 of IEEE Std 802.1w-2001), there is an increased probability that a Spanning Tree reconfiguration event can cause frames that are in transit through the Virtual Bridged LAN to be duplicated, due to the fact that a VLAN Bridge can buffer frames awaiting transmission through its Ports. As the probability of duplication occurring as a result of such an event is small, and the frequency of Spanning Tree reconfiguration events is also small, the degradation of the properties of the MAC service caused by this source of frame duplication is considered to be negligible. A more detailed discussion of frame duplication in RSTP can be found in F.2.4 of IEEE Std 802.1w-2001.

6.3.5 Transit delay

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

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

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

6.3.6 Frame lifetime

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

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

The value of the maximum bridge transit delay is based on both the maximum delays imposed by all the VLAN Bridges in the Virtual Bridged LAN and the desired maximum frame lifetime. A recommended and an absolute maximum value are specified in Table 8-2 of IEEE Std 802.1D, 1998 Edition.

6.3.7 Undetected frame error rate

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

The FCS calculated for a given service data unit is dependent on the MAC method employed. It is therefore necessary to recalculate the FCS within a VLAN Bridge providing a relay function between IEEE 802 MACs of dissimilar types if differences in the method of calculation and/or the coverage of the FCS, or changes to the data that is within the coverage of the FCS, would lead to a different FCS being calculated for the service data unit by the two MAC methods. This introduces the possibility of additional undetected

errors arising from the operation of a VLAN Bridge. For frames relayed between LANs of the same MAC type, the VLAN Bridge shall not introduce an undetected frame error rate greater than that which would have been achieved by preserving the FCS.

NOTE—Application of the techniques described in Annex G of IEEE Std 802.1D, 1998 Edition, allow an implementation to achieve an arbitrarily small increase in undetected frame error rate, even in cases where the data that is within the coverage of the FCS is changed. As a maintenance activity on this standard, revision of the wording of this requirement will be initiated, with a view to placing a quantitative limit on the increase in undetected frame error rate that is acceptable in a conformant implementation.

6.3.8 Maximum Service Data Unit Size

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

6.3.9 Priority

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

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

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

The transmission delay comprises

- a) A queuing delay until the frame becomes first in line for transmission on the Port, in accordance with the procedure for selecting frames for transmission described in 8.7.4;
- b) The access delay for transmission of the frame.

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

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

The VLAN Bridge maps the user priority onto one or more traffic classes; VLAN Bridges that support more than one traffic class are able to support expedited classes of traffic. The Forwarding Process, 7.7 8.7, describes the use of user priority and traffic classes in VLAN Bridges. Given the constraints placed upon frame misordering in a VLAN Bridge, as expressed in 6.3.3, the mappings of priority and traffic class are static.

NOTE 1—The term Traffic Class, as used in this standard, is used only in the context of the operation of the priority handling and queueing functions of the Forwarding Process, as described in 8.7. Any other meanings attached to this term in other contexts do not apply to the use of the term in this standard.

The ability to signal user_priority in IEEE 802 LANs allows user_priority to be carried with end-to-end significance across a Virtual Bridged LAN. This, coupled with a consistent approach to the mapping of user_priority to traffic classes, and of user_priority to access_priority, allows consistent use of user_priority information to be made, according to the capabilities of the VLAN Bridges and MAC methods that are involved in the transmission path.

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

Under normal circumstances, user_priority is not modified in transit through the relay function of a VLAN Bridge; however, there may be some circumstances where it is desirable for management purposes to control how user_priority is propagated. The User Priority Regeneration Table (Table 7-48-1) provides the ability to map incoming user_priority values on a per-Port basis, under management control. In its default state, this table provides an identity mapping from user_priority values to Regenerated user_priority values; i.e., by default, the Regenerated user_priority is identical to the incoming user_priority.

6.3.10 Throughput

The total throughput provided by a Virtual Bridged LAN can be significantly greater than that provided by an equivalent single LAN. VLAN Bridges may localize traffic within the Virtual Bridged LAN by filtering frames. Filtering services available in Virtual Bridged LANs are described in 6.6 of IEEE Std 802.1D, 1998 Edition.

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

6.4 Enhanced Internal Sublayer Service provided within VLAN Bridges

The Enhanced Internal Sublayer Service (E-ISS) is derived from the Internal Sublayer Service (ISS, defined in 6.4 of IEEE Std 802.1D, 1998 Edition) by augmenting that specification with elements necessary to the operation of the tagging and untagging functions of the VLAN Bridge. Within the attached end station, these elements can be considered to be either below the MAC Service boundary, and pertinent only to the operation of the service provider; or local matters not forming part of the peer-to-peer nature of the MAC Service.

Bridges that support these functions are known as *VLAN-aware Bridges* (3.17). The E-ISS defines the MAC Service provided to the relay function in VLAN-aware Bridges.

The relationships between the MAC Entity, the ISS, the E-ISS, and the MAC Relay Entity in a VLAN-aware Bridge are illustrated in Figure 6-1 and Figure 8-3.

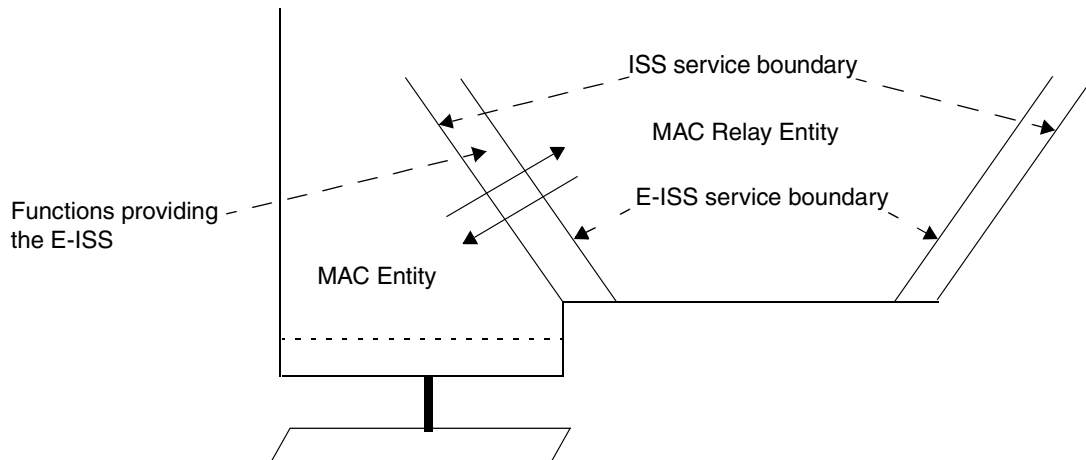


Figure 6-1—Relationships between MAC Entity, ISS, E-ISS, and MAC Relay Entity

6.4.1 E-ISS service definition

The unit-data primitives that define this service are

```
EM_UNITDATA.indication
(
    frame_type,
    mac_action,
    destination_address,
    source_address,
    mac_service_data_unit,
    user_priority,
    frame_check_sequence,
    canonical_format_indicator,
    vlan_identifier,
    rif_information (optional)
)
```

Each data indication primitive corresponds to the receipt of a M_UNITDATA.indication primitive from the Internal Sublayer Service, as defined in 6.4 of IEEE Std 802.1D, 1998 Edition.

The **frame_type**, **mac_action**, **destination_address**, **source_address**, **mac_service_data_unit**, **user_priority**, and **frame_check_sequence** parameters are as defined for the M_UNITDATA.indication primitive of the Internal Sublayer service.

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

NOTE—The meanings of the terms Canonical format and Non-canonical format are discussed in Annex F.

The **vlan_identifier** parameter carries the VLAN identifier associated with the indication.

The **rif_information** parameter is present if a tag header was present in the indication, and if that tag header contained a Routing Information Field (RIF). Its value is equal to the value of the RIF.

```
EM_UNITDATA.request      (  
    frame_type,  
    mac_action,  
    destination_address,  
    source_address,  
    mac_service_data_unit,  
    user_priority,  
    access_priority,  
    frame_check_sequence,  
    canonical_format_indicator,  
    vlan_classification,  
    rif_information (optional),  
    include_tag  
)
```

A data request primitive is invoked in order to generate a M_UNITDATA.request primitive, as defined in the Internal Sublayer Service, 6.4 of IEEE Std 802.1D, 1998 Edition.

The **frame_type**, **mac_action**, **destination_address**, **source_address**, **mac_service_data_unit**, **user_priority**, **access_priority**, and **frame_check_sequence** parameters are as defined for the M_UNITDATA.request primitive of the Internal Sublayer service.

The definition of the **canonical_format_indicator** parameter is as defined for the EM_UNITDATA.indication.

The **vlan_classification** parameter carries the VLAN classification assigned to the frame by the forwarding process (8.6.1).

The **rif_information** parameter, if present, carries the value of any RIF information to be associated with the request.

The **include_tag** parameter carries a Boolean value. True indicates to the service provider that the **mac_service_data_unit** parameter of the data request shall include a tag header (9.3). False indicates that a tag header shall not be included.

6.4.2 Support of the E-ISS in VLAN-aware Bridges

6.4.2.1 Data indication primitives

On receipt of a data indication from the Internal Sublayer Service, an EM_UNITDATA.indication primitive is invoked, with parameter values as follows:

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

NOTE 1—The **mac_action** parameter only ever takes the value **request_with_no_response** for frames relayed by the Bridge. The **frame_check_sequence** parameter of the data indication carries the FCS value contained in the received frame. The original FCS associated with a frame is invalidated if there are changes to any fields of the frame, if fields are added or removed, or if bit ordering or other aspects of the frame encoding have changed. An invalid FCS is signalled in the E-ISS by an unspecified value in the **frame_check_sequence** parameter of the data request primitive. This signals the need for the FCS to be regenerated according to the normal procedures for the transmitting MAC. The options for regenerating the FCS under these circumstances are discussed in Annex G of IEEE Std 802.1D, 1998 Edition.

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

- a) If the received **mac_service_data_unit** parameter contained a tag header (9.3), then the value used is equal to the value of the received **mac_service_data_unit** following removal of the tag header. Otherwise;
- b) The value used is equal to the value of the received **mac_service_data_unit**.

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

- c) If the received **mac_service_data_unit** parameter contained a tag header (9.3), then the value contained in the **user_priority** field of the tag header is used. Otherwise;
- d) The value of the received **user_priority** parameter, regenerated as defined in 8.5.1 and 6.4 of IEEE Std 802.1D, 1998 Edition, is used.

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

- e) If the received **mac_service_data_unit** parameter contained a tag header (9.3), then the value(s) contained in the Canonical Format Indicator (CFI) (and Non-Canonical Format Indicator [NCFI], if present) field(s) of the tag header are used to determine this parameter value, in accordance with the definition of the CFI and NCFI field(s) in Clause 9. Otherwise;
- f) If the MAC entity that received the data indication was an ISO/IEC 8802-5 Token Ring MAC, then the parameter carries the value False. Otherwise;
- g) The parameter carries the value True.

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

- h) If the initial octets of the received **mac_service_data_unit** parameter contained a tag header (9.3), then the value contained in the VID field of the tag header is used. Otherwise;
- i) A value equal to the null VLAN ID (as defined in Table 9-2) is used.

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

- j) If the initial octets of the received **mac_service_data_unit** parameter contained a tag header (9.3), and that tag header contained a RIF field in which one or more route descriptors were present, then the value contained in the RIF field is used. Otherwise;
- k) The parameter is not present.

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

6.4.2.2 Data request primitives

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

The **frame_type**, **mac_action**, **destination_address**, **source_address**, **user_priority**, and **access_priority** parameters carry values equal to the corresponding parameters in the received data request.

If the value of the **include_tag** parameter is False, the value of the **mac_service_data_unit** parameter is determined as follows:

- a) If the destination MAC method is the same as the MAC method on which the corresponding data indication was received, then the value used is equal to the value of the `mac_service_data_unit` parameter received in the data request. Otherwise;
- b) The value used is equal to the value of the `mac_service_data_unit` parameter received in the data request, modified, if necessary, in accordance with the procedures described in ISO/IEC 11802-5, IETF RFC 1042, and IETF RFC 1390.
- c) If the `canonical_format_indicator` parameter indicates that the `mac_service_data_unit` may contain embedded MAC Addresses in a format inappropriate to the destination MAC method, then the Bridge shall either
 - 1) Convert any embedded MAC Addresses in the `mac_service_data_unit` to the format appropriate to the destination MAC method; or
 - 2) Discard the EISS data request without issuing a corresponding ISS data request.

If the value of the **include_tag parameter** is True, then a tag header, formatted as necessary for the destination MAC method, is inserted as the first N octets of the `mac_service_data_unit` parameter. The values of the `user_priority`, `canonical_format_indicator`, `vlan_classification`, and `rif_information` (if present) parameters are used to determine the contents of the tag header, in accordance with the structure defined in 9.2 and 9.3. The value inserted after the tag header is determined as follows:

- d) If the destination MAC method is the same as the MAC method on which the corresponding data indication was received, then the value used is equal to the value of the `mac_service_data_unit` parameter received in the data request. Otherwise;
- e) The value used is equal to the value of the `mac_service_data_unit` parameter received in the data request, modified, if necessary, in accordance with the procedures described in ISO/IEC 11802-5, IETF RFC 1042, and IETF RFC 1390.

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

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

NOTE—The original FCS associated with a frame is invalidated if there are changes to any fields of the frame, if fields are added or removed, or if bit ordering or other aspects of the frame encoding have changed. An invalid FCS is signalled in the E-ISS by an unspecified value in the `frame_check_sequence` parameter of the data request primitive. This signals the need for the FCS to be regenerated according to the normal procedures for the transmitting MAC. The options for regenerating the FCS under these circumstances are discussed in Annex G of IEEE Std 802.1D, 1998 Edition.

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

In addition to the provisions of 6.5.1 of IEEE Std 802.1D, 1998 Edition, on receipt of an `M_UNITDATA.request` primitive that represents a tagged frame, the implementation is permitted to adopt either of the following approaches with regard to the operation of Transmit Data Encapsulation for frames whose length would, using the procedure as described, be less than 68 octets:

- a) Use the procedure as described in 6.5.1 of IEEE Std 802.1D, 1998 Edition. This can result in tagged frames of less than 68 octets (but at least 64 octets) being transmitted; or
- b) Include additional octets before the FCS field in order for the transmitted frame length for such frames to be 68 octets. This results in a minimum tagged frame length of 68 octets.

When a tagged frame of less than 68 octets in length is received on a CSMA/CD LAN segment, and is forwarded as an untagged frame, the provisions of 6.5.1 of IEEE Std 802.1D, 1998 Edition, result in additional octets being included before the FCS field on transmission in order that the transmitted frame length meets the minimum frame size requirements of 3.2.7 in IEEE Std 802.3, 1998 Edition.

7. Principles of network operation

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 Bridges (Clause 8);
- b) their participation in the Spanning Tree (Clause 8 of IEEE Std 802.1D, 1998 Edition), Rapid Spanning Tree (Clause 17 of IEEE Std 802.1w-2001), or Multiple Spanning Tree Protocol (Clause 13);
- 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

The operation of a Virtual Bridged Local Area Network, the Bridges, and the LANs, that compose that network comprises:

- a) A physical topology comprising LANs, Bridges, and Bridge Ports. Each Bridge Port attaches a LAN to a Bridge and is capable of providing bidirectional connectivity for MAC user data frames. Each LAN is connected to every other LAN by a Bridge and zero or more other LANs and Bridges.
- b) Calculation of one or more active topologies, each a loop-free subset of the physical topology.
- c) Rules for the classification of MAC user data frames that allow each Bridge to allocate, directly or indirectly, each frame to one and only one active topology.
- d) Management control of the connectivity provided for differently classified data frames by the selected active topology.
- e) Implicit or explicit configuration of end station location information, identifying LANs with attached end stations that need to receive user data frames with a given destination address.
- f) Communication of end station location information to allow Bridges to restrict user data frames to LANs in the path provided to their destination(s) by the chosen active topology.

These elements and their interrelationships are illustrated in Figure 7-1.

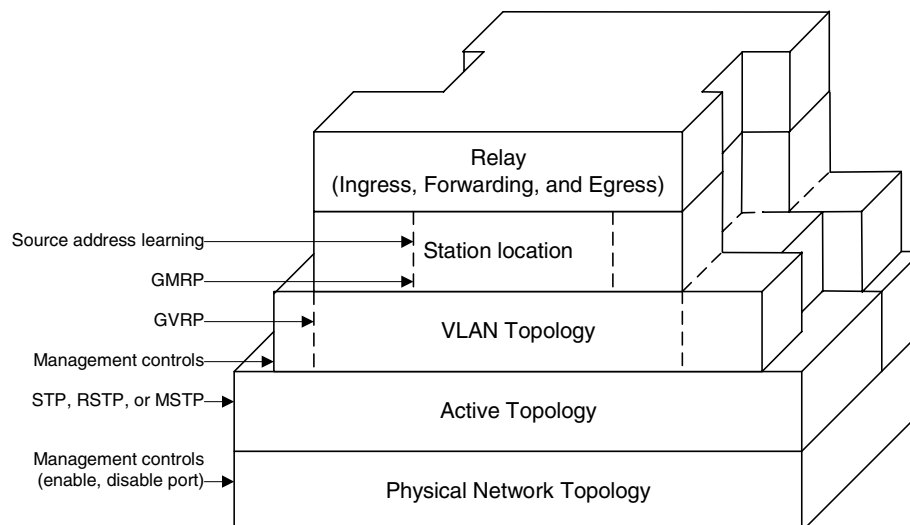


Figure 7-1—VLAN Bridging overview

NOTE 1—The physical and active topologies can be represented as bi-partite graphs. Bridges and LANs are nodes in these graphs (including LANs that are point-to-point links) and the Bridge Ports are edges.

NOTE 2—This standard applies the notion of a physical topology to media access control methods, like wireless, where there is no tangible physical connection between a Bridge and an attached LAN. A Bridge Port models this association just as for wired connectivity.

NOTE 3—Each of the active topologies [(b) above] does not necessarily span the entire network, but does span all those Bridges and LANS between which data frame connectivity is desired for frames allocated to that active topology.

NOTE 4—The destination addressing information associated with a MAC user data frame includes the VLAN classification of the frame [see (d) above].

NOTE 5—Implicit configuration [(d) above], or recognition, of end station location includes observation of the source address of the user data frame transmitted by that station. The user data frame itself communicates that location information [(e) above] along the portion of the chosen active topology leading to the frame's destination(s).

7.2 Use of VLANs

Virtual Local Area Networks (VLANs) and their VLAN Identifiers (VIDs) provide a convenient and consistent network wide reference for Bridges to:

- a) identify rules for the classification of user data frames into VLANs;
- b) effectively extend the source and destination MAC addresses, by treating frames and addressing information for different VLANs independently.
- c) identify and select from different active topologies;
- d) identify the configuration parameters that partition or restrict access from one part of the network to another.

Taken together these capabilities allow VLAN aware Bridges to emulate a number of separately manageable, or virtual, Bridged Local Area Networks. A LAN segment that has been selected by network management to receive frames assigned to a given VLAN is said to form part of, belong to, or be a member of the VLAN. Similarly, end stations that are attached to those LAN segments and that can receive frames assigned to the VLAN are said to be attached to that VLAN.

NOTE—Separate control over the transmission and over the reception of frames to and from LAN segments and end stations is possible. To avoid ambiguity VLAN membership is defined by reception.

Inclusion of the VID in VLAN-tagged frames guards against connectivity loops arising from differing classifications by different Bridges, and permits enhanced classification rules to be used by some Bridges while others simply forward the previously classified frames.

The VLAN tag allows frames to carry priority information, even if the frame has not been classified as belonging to a particular VLAN.

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.

At any time the current extent of a VLAN can be further reduced from the maximum to include only those LAN segments 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 1—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 2—To accommodate end stations that do not participate in the GVRP protocol specified in Clause 11, management controls associated with each Bridge Port allow the Port to identify the attached LAN segment as connecting end stations that require services using specified VLANs.

7.4 Locating end stations

Functioning as a distributed system, Bridges within the current extent of a VLAN can, through explicit and or implicit cooperation, locate those LAN segments 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 LAN segments where their transmission is necessary.

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

The multicast registration protocol (GMRP), specified in Clause 10 of IEEE Std 802.1D, 1998 Edition, allows end stations to advertise their presence and their desire to join (or leave) a multicast group in the context of a VLAN. The protocol communicates this information to other Bridges, using the VLAN and its active topology.

NOTE 2—To accommodate end stations that do not participate in GMRP, management controls associated with each Bridge Port allow the Port to identify the attached LAN segment as connecting end stations that are intended to receive specified group addresses. The continuous operation of GMRP and the propagation of location information through 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 a LAN segment 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 VLAN if the location of the destination or destinations is unknown. The learnt information is stored in the Filtering Database used to filter frames on the basis of their destination addresses.

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 VLAN's. This is known as *Shared VLAN Learning* (3.26);
- 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* (3.8);
- c) For some configurations, it is immaterial as to whether learned information is shared between VLANs or not.

NOTE 1—Annex B discusses the need for Shared and Independent VLAN Learning, and also some of the 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 VLAN-Bridged LAN, there may be a combination of configuration requirements, so that individual VLAN Bridges may be called upon 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 VLAN 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 VLAN Bridges by means of a set of *VLAN Learning Constraints* (8.10.7.2) and fixed allocations of VLANs to filtering databases (8.10.7.1), which may be configured into the Bridges by means of management operations. By analyzing the set of learning constraints and fixed allocations for the VLANs 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 VLAN, which Filtering Database it will feed any learned information into (and use learned information from).

The manner in which this mapping of VLANs onto Filtering Databases is achieved is defined in 8.10.7; the result is that each VLAN 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 VLANs onto each Filtering Database. Such a Bridge is known as an SVL/IVL Bridge (3.28).

The conformance requirements in this standard (5.1, 5.2) recognize that VLAN 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 upon the number of Filtering Databases that can be supported, and/or the number of VLANs 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 VLANs onto each one;
- g) Support for a single Filtering Database only. MAC Address information that is learned in one VLAN can be used in filtering decisions taken relative to all other VLANs 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 VLAN can be mapped onto each Filtering Database. MAC Address information that is learned in one VLAN cannot be used in filtering decisions taken relative to any other VLAN. Bridges that support this mode of operation are referred to as IVL Bridges.

7.5 Ingress, Forwarding, and Egress Rules

The relay function provided by the Forwarding Process (8.6) of each individual 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 belonging to a particular VLAN;
 - 2) Priority-tagged, i.e., including a tag header conveying explicit user priority information but not identifying the frames as belonging to a specific VLAN;
 - 3) VLAN-tagged, i.e., explicitly identifying the frames as belonging to a particular VLAN.

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 (7.3), station location information (7.4), and the additional management controls specified in Clause 8. This aspect of relay implements the *forwarding* rules.
- c) Determination of the appropriate frame format type, VLAN-tagged or untagged, for transmission through the selected Bridge Ports. 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 part of the relay functionality of a VLAN-aware Bridge and is only performed on frames that can be forwarded through other Bridge Ports. To facilitate coexistence with Bridges conforming to IEEE Std 802.1D, 1998 Edition, frames that carry control information to determine the active topology and current extent of each VLAN, i.e., spanning tree and GVRP BPDUs, are not forwarded. Permanently configured static entries in the filtering database (8.2, 8.3, and 8.13) ensure that such frames are discarded by the Forwarding Process (8.6).

NOTE 1—GARP PDUs destined for any GARP application are forwarded or filtered depending upon whether the application concerned is supported by the bridge, as specified in 8.13.

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.

NOTE 1—Additional ingress classification methods may be the subject of future standardization.

NOTE 2—This classification of untagged and priority-tagged frames is part of the functionality of the MAC relay entity (Figure 8-3, Figure 8-4), and is therefore only of significance for received frames that are potentially to be forwarded through other Ports of the Bridge (see Spanning Tree).

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

- d) All untagged; or
- e) All VLAN tagged with the same VID.

NOTE 4—In other words, a Bridge can transmit untagged frames for some VLANs and VLAN-tagged frames for other VLANs on a given link, but cannot transmit using both formats for the same VLAN. The single format rule only applies to the frame transmission behavior of individual VLAN-aware stations; i.e., it does not express a requirement for a Bridge to police the behavior of the other stations attached to a segment and enforce a single format.

8. Principles of bridge operation

This clause establishes the principles of operation of a VLAN-aware Bridge, by reference to a model of that operation, as follows:

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

The provisions of this clause replace the provisions of Clause 7 of IEEE Std 802.1D, 1998 Edition in a VLAN-aware Bridge.

8.1 Bridge operation

The principal elements of Bridge operation are

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

8.1.1 Relay

A MAC Bridge relays individual MAC user data frames between the separate MACs of the Bridged LANs connected to its Ports. The order of frames shall be preserved as defined in 8.6.5.

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

- a) Frame reception.
- b) Discard on received frame in error (6.3.2).
- c) Frame discard if the `frame_type` is not `user_data_frame`, or if its `mac_action` parameter is not `request_with_no_response` (8.5, 6.4).
- d) Regeneration of user priority, if required (6.4).
- e) Application of VLAN ingress rules to classify each received frame to a particular VLAN (8.6.1).
- f) Frame discard if the frame is not classified or the receiving port does not accept frame from that VLAN.
- g) Frame discard following the application of filtering information.
- h) Frame discard on transmittable service data unit size exceeded (6.3.8).
- i) Forwarding of received frames to other Bridge Ports.
- j) Frame discard following the application of VLAN egress rules if the service data unit cannot be mapped correctly or the receiving port does not transmit frames to the particular VLAN to which the frame belongs.
- k) Selection of traffic class, following the application of filtering information.
- l) Queuing of frames by traffic class.
- m) Frame discard to ensure that a maximum bridge transit delay is not exceeded (6.3.6).
- n) Selection of queued frames for transmission.
- o) Selection of outbound access priority (6.3.9).
- p) Mapping of service data units and recalculation of Frame Check Sequence, if required (8.6.9, 6.3.7).
- q) Frame transmission.

8.1.2 Filtering and relaying information

A Bridge maintains filtering and relaying information for the following purposes:

- a) Prevention of frame duplication: to ensure that frame duplication does not occur, by maintaining a loop-free logical topology;
- b) Traffic segregation: to separate communication by different sets of users or groups of users of the Bridged LAN;
- c) Traffic reduction: to confine frames to those parts of the Bridged LAN that lie on the path(s) between their source and destination(s);
- d) Traffic expediting: to classify frames in order to expedite time critical traffic;
- e) Conversion of frame formats: to present frames in a format (tagged or untagged) that is appropriate for the destination LAN and its attached stations.

8.1.2.1 Prevention of frame duplication

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 (6.3.4). The functions that support the use and maintenance of information for this purpose are

- a) Configuration and calculation of Bridged LAN topology.
- b) In MST Bridges, explicit configuration of the relationship between VLANs and spanning trees (8.11).

8.1.2.2 Traffic segregation

A Bridge can filter frames to confine them to the LAN segments that belong to the VLAN to which they are assigned, and thus define the VLAN's maximum extent (7.3). The functions that support the use and maintenance of information for this purpose are

- a) Explicit configuration of the Ingress Rules associated with each Port (8.4, 8.6.1 8.9):
 - 1) Configuration of <commentRef>PVID for each Port, to associate a VID with untagged and priority-tagged frames;
 - 2) In Bridges implementing Port-and-Protocol based classification, the configuration of a VID for untagged and priority-tagged frames for each protocol;
 - 3) Enabling or disabling the application of Static VLAN Registration Entries to received frames through configuration of the Enable Ingress Filtering parameter;
- b) Explicit configuration of the Egress Rules associated with each Port (8.6.4):
 - 1) Configuration of Static VLAN Registration Entries.

A Bridge can filter frames to partially partition a Virtual Bridged Local Area Network. Frames assigned to any given VLAN and addressed to specific end stations or groups of end stations can be excluded from relay to certain Bridge Ports. The functions that support the use and maintenance of information for this purpose are:

- c) Permanent configuration of Reserved Addresses (Table 8-10);
- d) Configuration of Static Filtering Entries (8.10.1) and Group Registration Entries (8.10.4).

NOTE—The use of VLANs is generally less error prone and is preferred to filtering using destination addresses if a Bridged Local Area Network is to be partitioned for reasons of scale, efficiency, management, or security. Destination address filtering is the only mechanism available to Bridges that are not VLAN aware.

8.1.2.3 Traffic reduction

A Bridge can filter frames to confine them to LAN segments that either have end stations attached to their assigned VLAN or that connect those LAN segments, and thus define the current practical extent of the

VLAN (7.4). LANs not attaching to or forming part of the path between the source and destination(s) of any given communication do not have to support the transmission of related frames, potentially improving the quality of the MAC service for other communications. The functions that support the use and maintenance of information for this purpose are:

- a) Automatic learning of dynamic filtering information for unicast destination addresses through observation of source addresses of frames, together with the ageing out or flushing of that information to support the movement of end stations and changes in active topology;
- b) Ageing out or flushing of dynamic filtering information that has been learned;
- c) Automatic inclusion and removal of Bridge Ports in the VLAN, through configuration of Dynamic VLAN Registration Entries by means of GVRP (8.10.5 and 11.2);
- d) Explicit configuration of management controls associated with the operation of GVRP by means of Static VLAN Registration Entries (8.10.2 and 11.2);
- e) Automatic configuration of Group Registration Entries by means of GMRP exchanges;
- f) Explicit configuration of the management controls associated with the operation of GMRP by means of Group Registration Entries.

8.1.2.4 Traffic expediting

A Bridge classifies frames into traffic classes in order to expedite transmission of frames generated by critical or time-sensitive services. The function that supports the use and maintenance of information for this purpose is

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

8.1.2.5 Conversion of frame formats

A Bridge adds and removes tag headers (9.3) from frames, and performs the associated frame translations that may be required, in accordance with the egress rules (8.6.4). The function that supports the use and maintenance of information for this purpose is

- a) Explicit configuration of tagging requirements on egress for each Port (8.10.2 and 8.10.9).

8.1.3 Bridge management

The functions that support Bridge Management control and monitor the provision of the above functions. They are specified in Clause 12.

8.2 Bridge architecture

8.2.1 Architectural model of a Bridge

Figure 8-1 gives an example of the physical topology of a Bridged LAN. The component LANs are interconnected by means of MAC Bridges; each Port of a MAC Bridge connects to a single LAN. Figure 7-1 illustrates a Bridge with two Ports, and Figure 6-1 illustrates the architecture of such a Bridge.

A Bridge is modeled as consisting of

- a) A MAC Relay Entity that interconnects the Bridge's Ports;
- b) At least two Ports;
- c) Higher layer entities, including at least a Spanning Tree Protocol Entity⁹.

⁹The Spanning Tree Protocol Entity was formerly known as the Bridge Protocol Entity.

8.2.2 MAC Relay Entity

The MAC Relay Entity handles the MAC independent functions of relaying frames between Bridge Ports, filtering frames, and learning filtering information. It uses the Enhanced Internal Sublayer Service provided by the separate MAC Entities for each Port. (The Enhanced Internal Sublayer Service and its support are described in 6.4 and 6.5.) Frames are relayed between Ports attached to different LANs.

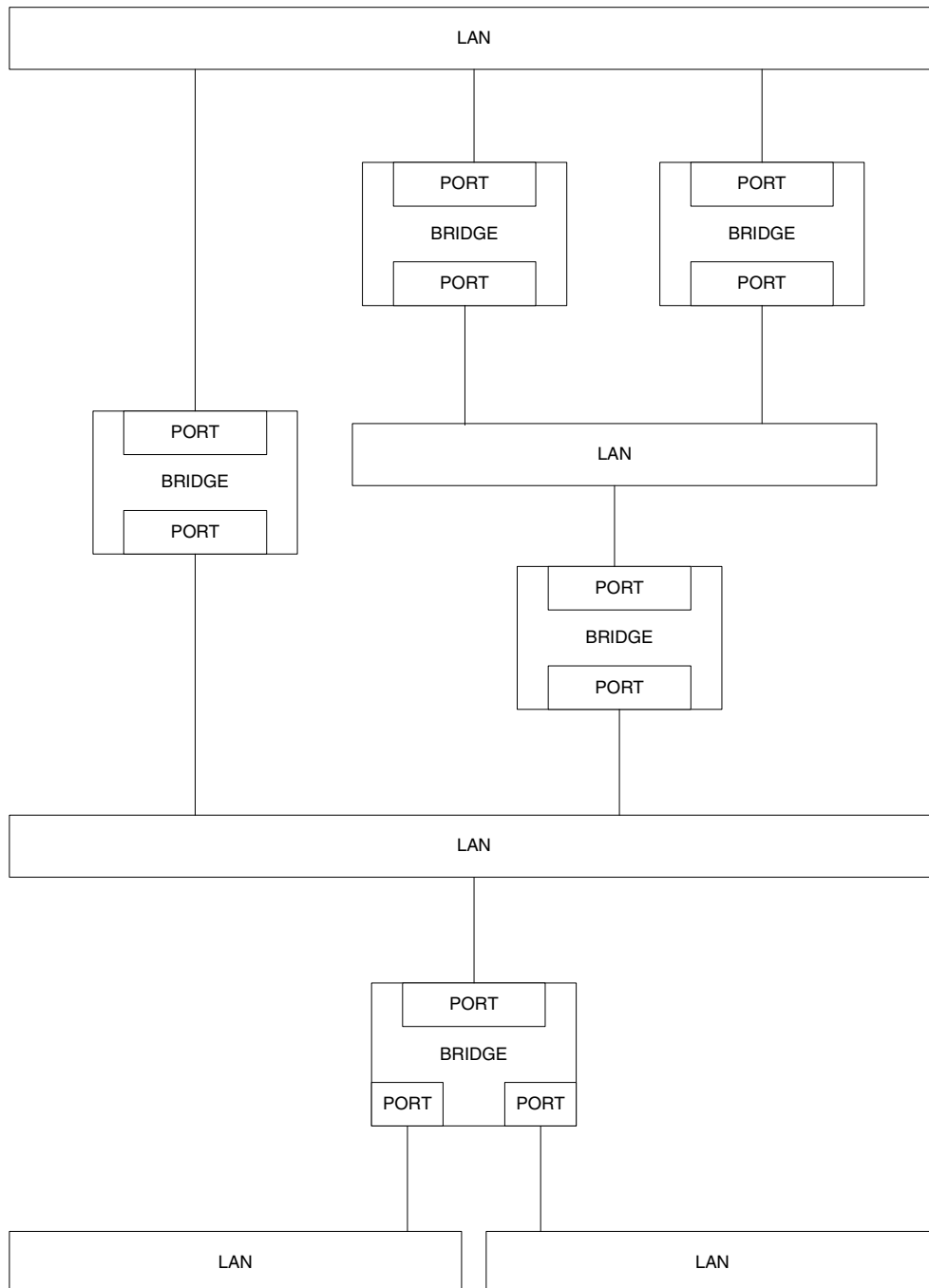
8.2.3 Ports

Each Bridge Port transmits and receives frames to and from the LAN to which it is attached. An individual MAC Entity permanently associated with the Port provides the Enhanced Internal Sublayer Service used for frame transmission and reception. The MAC Entity handles all the MAC method dependent functions (MAC protocol and procedures) as specified in the relevant standard for that IEEE 802 LAN MAC technology.

8.2.4 Higher Layer Entities

The Spanning Tree Protocol Entity handles calculation and configuration of Bridged LAN topology.

The Spanning Tree Protocol Entity and other higher layer protocol users, such as Bridge Management (8.1.3) and GARP application entities including GARP Participants (Clause 12 of IEEE Std 802.1D, 1998 Edition), make use of Logical Link Control procedures. These procedures are provided separately for each Port, and use the MAC Service provided by the individual MAC Entities.

**Figure 8-1—Example of a Bridged LAN**