802.1ad™

IEEE Standard for
Local and metropolitan area networks

Virtual Bridged Local Area Networks

Amendment 4: Provider Bridges

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

26 May 2006

IEEE Std 802.1ad™-2005
(Amendment to
IEEE Std 802.1Q™-2005)

Recognized as an
American National Standard (ANSI)

IEEE Std 802.1ad™-2005
(Amendment to
IEEE Std 802.1Q™-2005)

IEEE Standard for
Local and metropolitan area networks—

Virtual Bridged Local Area Networks

Amendment 4: Provider Bridges

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 28 March 2006

American National Standards Institute

Approved 7 December 2005

IEEE-SA Standards Board

Abstract: This amendment enables a service provider to use the architecture and protocols of IEEE Std 802.1Q to offer the equivalent of separate LANs, Bridged Local Area Networks, or Virtual Bridged Local Area Networks to a number of customers, while requiring no cooperation between the customers, and minimal cooperation between each customer and the service provider.
Keywords: Bridged Local Area Networks, local area networks (LANs), MAC Bridges, metropolitan area networks, Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), Virtual Bridged Local Area Networks (virtual LANs)

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

Print: ISBN 0-7381-4874-1 SH95507
PDF: ISBN 0-7381-4875-X SS95507

Introduction

This introduction is not part of IEEE Std 802.1ad, IEEE Standards for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 4: Provider Bridges.

Notice to users

Errata

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

Interpretations

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

Patents

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

Participants

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

Tony Jeffree, *Chair*
Mick Seaman, *Chair, Interworking Task Group*
Stephen Haddock, *Editor*

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

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

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

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

Historical participants

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

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

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

Figures

Figure 6-3—Service access priority selection 14
Figure 9-1— ~~V~~C-TAG TCI format 22
Figure 9-2— S-TAG TCI format 23
Figure 15-1—Internal organization of the MAC sublayer in a Provider Bridged Network 40
Figure 15-2—Port-based service interface to a Provider Bridged Network 41
Figure 15-3—Port-based service interface to a Provider Bridged Network 42
Figure 15-4—C-tagged service interface to a Provider Bridged Network 42
Figure 15-5—C-tagged service interface to a Provider Bridged Network 42
Figure 15-6—Customer Edge Ports 43
Figure 15-7—S-tagged service interface to a Provider Bridged Network 43
Figure 15-8—S-tagged interface to a Provider Bridged Network 44
Figure 16-1—Provider Bridged Network with interface examples 47

Tables

Table 6-3—Priority Code Point encoding 12
Table 6-4—Priority Code Point decoding 12
Table 6-5—Service Access Priority 15
Table 8-1—C-VLAN component Reserved addresses 18
Table 8-2—S-VLAN component Reserved addresses 19
Table 9-1—802.1Q Ethernet Type allocations 22
Table G-4—Priority Code Point encoding 58
Table G-5—Priority Code Point decoding 59

Contents

1. Overview 1

1.1 Scope 1

3. Definitions 3

4. Abbreviations 5

5. Conformance 6

5.2 Conformant components and equipment 6
5.3 Protocol Implementation Conformance Statement (PICS) 6
5.4 VLAN-aware Bridge ~~component~~ requirements 6
5.5 C-VLAN component conformance 7
5.6 S-VLAN component conformance 7
5.7 VLAN Bridge conformance 8
5.8 Provider Bridge conformance 8

6. Support of the MAC Service in VLANs 10

6.6 Enhanced Internal Sublayer Service 10
6.7 Support of the EISS 10
6.9 Support of the ISS for attachment to a Provider Bridged Network 13
6.10 Support of the ISS within a system 16
6.11 Support of the ISS by additional technologies 16

8. Principles of bridge operation 17

8.1 Bridge operation 17
8.6 The Forwarding Process 17
8.12 Bridge Management Entity 20
8.13 Addressing 20

9. Tagged frame format 22

9.5 Tag Protocol Identification 22
9.6 ~~Customer~~ VLAN Tag Control Information 22
9.7 Service VLAN Tag Control Information 23
9.8 Embedded Routing Information Field (E-RIF) 23

11. VLAN topology management 24

12. Bridge management 25

12.13 Provider Bridge management 31

13. The Multiple Spanning Tree Protocol (MSTP) 38

13.38 Customer Edge Port Spanning Tree operation 38

15. Support of the MAC Service by Provider Bridged Networks 40

15.1 Service transparency 40
15.2 Customer service interfaces 41
15.3 Port-based service interface 41
15.4 C-tagged service interface 42
15.5 S-tagged service interface 43
15.6 Service instance segregation 44
15.7 Service instance selection and identification 44
15.8 Service priority selection 45
15.9 Service access protection 45

16. Principles of Provider Bridged Network operation 46

16.1 Provider Bridged Network overview 46
16.2 Provider Bridged Network 47
16.3 Service instance connectivity 48
16.4 Service provider learning of customer end station addresses 49
16.5 Detection of connectivity loops through attached networks 49
16.6 Network management 50

Annex A (normative) PICS proforma 51

Annex G (informative) Priority and drop precedence 56

Annex H (informative) Bibliography 60

IEEE Standard for
Local and metropolitan area networks—

Virtual Bridged Local Area Networks

Amendment 4: Provider Bridges

[This amendment is based on IEEE Std 802.1Q™-2006.]

NOTE—The editing instructions contained in this amendment define how to merge the material contained therein into the existing base standard and its amendments to form the comprehensive standard.

The editing instructions are shown in ***bold italic.*** Four editing instructions are used: change, delete, insert, and replace. ***Change*** is used to make corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using ~~strikethrough~~ (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editorial notes will not be carried over into future editions because the changes will be incorporated into the base standard.

1. Overview

Insert the following paragraph after the initial paragraph of Clause 1:

This standard further extends the specification of VLAN-aware MAC Bridges to enable a service provider organization to use a common infrastructure of Bridges and LANs to offer the equivalent of separate LANs, Bridged, or Virtual Bridged Local Area Networks to independent customer organizations.

1.1 Scope

Insert the following text and bullets immediately after bullet m):

To enable a service provider to use a Virtual Bridged Local Area Network to provide separate instances of the IEEE 802® MAC Service, MAC Internal, and Enhanced Internal Sublayer Services[1] to multiple

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

independent customers, in a manner that does not require cooperation among the customers and that requires a minimum of cooperation between the customers and the provider of the MAC Service, this standard further specifies the operation of Provider Bridges. To this end it

n) Differentiates Customer VLANs (C-VLANs) that are under the administrative control of a single customer of a service provider, from the Service VLANs (S-VLANs) that are used by a service provider to support different customers.
o) Specifies VLAN TAG formats for both C-VLANs and S-VLANs, allowing each to be distinguished and separately applied and administered by customers and by a service provider.
p) Specifies the functionality of a generic VLAN-aware bridge component within a system and the specific requirements of derived C-VLAN and S-VLAN components.
q) Specifies a VLAN Bridge as comprising a single C-VLAN component, and a Provider Bridge as encompassing bridges that comprise a single S-VLAN component and no C-VLAN components (S-VLAN Bridge) or a single S-VLAN component and one or more C-VLAN components (Provider Edge Bridge).
r) Specifies parameters and mappings that allow the Enhanced Internal Sublayer Service to support traffic classes that comprise distinct aggregate flows supporting different QoS characteristics and provide independent guarantees to different customers, through support of priority and drop precedence marking.
s) Specifies the incorporation of flow metering, transmission queue management, and transmission selection algorithms within the forwarding process of a Bridge.
t) Positions the support of S-VLANs within the architectural description of the MAC Sublayer and specifies their relationship to media access method dependent functions and to the media independent functions used by customers to administer their networks, including the support of C-VLANs.
u) Allocates the reserved multicast addresses to media access method dependent, provider network, and customer network functions, specifying the filtering to be applied in each type of VLAN-aware bridge component.
v) Defines the principles of network operation in terms of the support and preservation of the MAC Service, and the maintenance of Quality of Service for each service instance, including the segregation of data belonging to different organizations.
w) Specifies customer interfaces to a Provider Bridged Network in terms of the operation and configuration of the VLAN-aware bridge components of Provider Bridges, including interfaces that
    1) Provide access to a single service instance through a Bridge Port
    2) Allow a customer to select amongst and identify service instances by Customer VLAN Identifier (C-VID)
    3) Allow a customer to select amongst and identify service intstances by Service VLAN Identifier (S-VID)
    4) Support customer signaling of priority information on a frame by frame basis
    5) Multiplex service instances over LANs that provide access to a provider network
    6) Support fault tolerance through redundant provision of access LANs and equipment.
x) Describes the functions to be performed within the Provider Bridged Network in order to support and maintain the connectivity provided to customer service instances.
y) Establishes the requirements for Bridge Management in the Provider Bridged Network, identifying the managed objects and defining the management operations.
z) Specifies performance requirements, and recommends default values and applicable ranges for the operational parameters of a Provider Bridge.

3. Definitions

Insert the following definitions into Clause 3, in appropriate collating sequence, renumbering existing/new definitions as appropriate:

3.1 C-VLAN component: A VLAN-aware bridge component with each Port supported by an instance of the EISS that can recognize, insert, and remove Customer VLAN tags.

3.2 C-VLAN Bridge: A VLAN Bridge.

3.3 customer: The purchaser of a service instance from a service provider. Often a business.

NOTE—Certain terms in this standard, including customer and service provider, reflect common business relationships that exist among the users of equipment implemented in conformance with IEEE Std 802.1Q. The use of these terms does not imply or impose any requirement on such business relationships.[2]

3.4 Customer Bridge: A MAC Bridge as specified by IEEE Std 802.1D™ or a VLAN Bridge as specified by IEEE Std 802.1Q.

3.5 Customer Bridged Local Area Network: A network of Customer Bridges.

3.6 Customer Edge Port: A C-VLAN component Port on a Provider Edge Bridge that is connected to customer owned equipment and receives and transmits frames for a single customer.

3.7 customer equipment: The physical embodiment of one or more customer systems.

3.8 Customer Network Port: An S-VLAN component Port on a Provider Bridge or within a Provider Edge Bridge that receives and transmits frame for a single customer.

3.9 customer system: A system attached to Provider Bridged Network but not intended by the service provider to be under the control of the service provider.

3.10 customer tagged frames: Frames that include a C-TAG.

3.11 C-tagged service interface: The interface provided by a Provider Edge Bridge to allow the attached customer to select between and identify service instances using the C-VID associated with transmitted and received frames.

3.12 Customer VLAN: A VLAN identified by an C-VID.

3.13 Customer VLAN ID: A VLAN Identifier conveyed in a C-TAG.

3.14 Customer VLAN tag: A VLAN tag with a Tag Protocol Identification value allocated for "802.1Q Tag Protocol Type".

3.15 Port-based service interface: The interface provided by a Provider Bridge that associates all customer frames with a single service instance.

3.16 Provider Bridge: An S-VLAN Bridge or a Provider Edge Bridge.

3.17 Provider Bridged Network: A network using Provider Bridges to offer customer protocol transparent connectivity.

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

3.18 Provider Edge Bridge: A system comprising a single S-VLAN component and one or more C-VLAN components implemented in accordance with Clause 5 of IEEE Std 802.1Q.

3.19 Provider Edge Port: A C-VLAN component Port within a Provider Edge Bridge that connects to a Customer Network Port and receives and transmits frames for a single customer.

3.20 Provider Network Port: An S-VLAN component Port on a Provider Bridge that can transmit and receive frames for multiple customers.

3.21 service instance: An instance of the MAC Service, providing the service at a number of service access points. The term "service instance" is often used to refer to the service and connectivity provided by a service provider to a customer.

NOTE—In general, a service provider can use a number of technologies to support a service instance; within IEEE Std 802.1Q, a service instance is supported by a single S-VLAN.

3.22 service provider: An organization that contracts to provide one or more service instances to a customer.

3.23 service tagged frames: Frames that include an S-TAG.

3.24 S-tagged service interface: The interface provided by a Provider Bridge to allow the attached customer to select between and identify service instances using the S-VID associated with transmitted and received frames.

3.25 Service VLAN: A VLAN identified by an S-VID.

3.26 Service VLAN ID: A VLAN Identifier conveyed in an S-TAG.

3.27 Service VLAN tag: A VLAN tag with a Tag Protocol Identification value allocated for "802.1Q Service Tag Type."

3.28 S-VLAN component: A VLAN-aware bridge component with each Port supported by an instance of the EISS that can recognize, insert, and remove Service VLAN tags.

3.29 S-VLAN Bridge: A system comprising a single S-VLAN component implemented in accordance with Clause 5 of IEEE Std 802.1Q.

3.30 VLAN-aware bridge component: The media access method independent functionality supporting an instance of the EISS at each Port that can recognize, insert, and remove VLAN tags, and the functionality that relays frames between Ports.

3.31 VLAN Bridge: A system comprising a single C-VLAN component implemented in accordance with Clause 5 of IEEE Std 802.1Q.

4. Abbreviations

Insert the following abbreviations, in the appropriate collating sequence:

C-TAG	Customer VLAN tag
C-VID	Customer VLAN Identifier
C-VLAN	Customer VLAN
DEI	Drop Eligible Indicator
S-TAG	Service VLAN tag
S-VID	Service VLAN Identifier
S-VLAN	Service VLAN

5. Conformance

Delete 5.2, and replace with the following two new subclauses:

5.2 Conformant components and equipment

This subclause specifies requirements and options for the following core component:

a) VLAN-aware bridge component (5.4);

for the following two components that use that core functionality:

b) C-VLAN component (5.5);
c) S-VLAN component (5.6);

and for the following systems that include instances of either or both of the above two components:

d) VLAN Bridge (5.7);
e) S-VLAN Bridge (5.8.1);
f) Provider Edge Bridge (5.8.2).

NOTE—A VLAN Bridge can also be referred to as a Customer Bridge or a C-VLAN Bridge. Both S-VLAN Bridges and Provider Edge Bridges are types of Provider Bridges.

5.3 Protocol Implementation Conformance Statement (PICS)

A claim of conformance specifies implementation of a C-VLAN component, an S-VLAN component, or a specific system. A component or system can support multiple claims for a range of possible behaviors.

The supplier of an implementation that is claimed to conform to this standard shall provide the information necessary to identify both the supplier and the implementation and shall complete a copy of the PICS proforma provided in Annex A for that specific component or system, together with the further information and completed PICS(s) required to identify subcomponents.

NOTE 1—C-VLAN component and S-VLAN component PICS' both require completion of a PICS for a VLAN-aware bridge component; the VLAN Bridge PICS requires a claim of conformance for a single C-VLAN component; the Provider Edge Bridge requires a claim of conformance for a single S-VLAN component and one or more claims for C-VLAN components.

NOTE 2—The claim of conformance that could be made to IEEE Std 802.1Q for an implementation of a VLAN-aware Bridge is replaced by a claim of conformance to a VLAN Bridge. Although the current and subsequent amendment(s) or revision(s) of this standard has changed the presentation of the information, the technical requirements of conformance remain unchanged.

Renumber the existing 5.3 to 5.4, and change the headings and introductory sentences as follows:

5.4 VLAN-aware Bridge component requirements

An implementation of a VLAN-aware Bridge component shall

5.4.1 VLAN-aware Bridge component options

An implementation of a VLAN-aware Bridge component may

Insert the following subclauses 5.5 through 5.8, and renumber the existing subclauses:

5.5 C-VLAN component conformance

A C-VLAN component comprises a VLAN-aware Bridge component with the EISS on all Ports supported by the use of a Customer VLAN tag (C-TAG) (6.6, 9.5).

A conformant implementation of a C-VLAN component shall

a) Comprise a single conformant VLAN-aware bridge component;
b) Recognize and use Customer VLAN tags;
c) Filter the Reserved MAC Addresses specified in Table 8-1;
d) Use the GVRP Application Address specified in Table 11-1; and

shall not

e) Use a VID Translation Table (6.7) on any Port;
f) Use Service VLAN tags except in support of the functionality specified in 6.9.

5.5.1 C-VLAN component options

A conformant C-VLAN component may implement the options specified for a VLAN-aware bridge component whose use is not specifically prohibited by 5.4.1 and may

a) Support encoding the drop_eligible parameter in the PCP field of the tag header (6.7.3); and
b) Allow support of the ISS as specified in subclause 6.9 to facilitate priority selection on a Provider Bridged Network; and
c) Implement RSTP, with the enhancements to support Customer Edge Ports, as specified in 13.38.

5.6 S-VLAN component conformance

An S-VLAN component comprises a VLAN-aware Bridge component with the EISS on all Ports supported by the use of a Service VLAN tag (S-TAG) (6.6, 9.5).

A conformant implementation of an S-VLAN component shall

a) Comprise a single conformant VLAN-aware bridge component; and
b) Recognize and use Service VLAN tags;
c) Support encoding the drop_eligible parameter in the PCP field of the tag header (6.7.3);
d) Filter the Reserved MAC Addresses specified in Table 8-2;
e) Use the GVRP Application Address specified in Table 8-1;
f) Allow the Acceptable Frame Types parameter (6.7) to be set to *Admit All Frames* for each Port;
g) Allow the Enable Ingress Filtering parameter (8.6.2) to be set for each Port; and

shall not

h) Recognize or use Customer VLAN tags;
i) Allow support of the ISS as specified in subclause 6.9 for any of its Ports;

i) Allow support of the ISS as specified in subclause 6.9 for any of its Ports;
j) Configure any of the GARP Application Addresses specified in Table 12-1 of IEEE Std 802.1D in the Filtering Database (8.10) or Permanent Database (8.10.10);
k) Use the GVRP Application Address specified in Table 11-1.

5.6.1 S-VLAN component options

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

a) Allow translation of VIDs through support of a VID Translation Table (6.6) on each Port.

5.7 VLAN Bridge conformance

A VLAN Bridge shall comprise a single conformant C-VLAN component (5.5).

Each VLAN Bridge Port shall be capable of attaching directly to an IEEE 802 LAN.

5.7.1 VLAN Bridge options

A VLAN Bridge may implement any C-VLAN component option (5.5).

5.8 Provider Bridge conformance

A Provider Bridge shall comprise a single conformant S-VLAN (5.6) component and zero or more C-VLAN components (5.5).

Each Port shall be capable of being configured as one of, and may be capable of being configured as any of

a) A Provider Network Port;
b) A Customer Network Port;
c) A Customer Edge Port;

as specified in Clause 15. Each Port configured as a Provider Network Port or Customer Network Port shall be capable of attaching the S-VLAN component of the Provider Bridge directly to an IEEE 802 LAN. Each Port configured as a Customer Edge Port shall be capable of attaching a C-VLAN component within the Provider Bridge directly to an IEEE 802 LAN.

5.8.1 S-VLAN Bridge conformance

An S-VLAN Bridge shall comprise a single conformant S-VLAN component (5.6). An S-VLAN Bridge does not have any physical interfaces configured as a Customer Edge Port, nor does it include any C-VLAN components.

5.8.2 Provider Edge Bridge conformance

A Provider Edge Bridge is a conformant Provider Bridge with the capability to include one or more C-VLAN components as specified in 15.4.

Each C-VLAN component shall comprise a single Customer Edge Port and a single distinct Provider Edge Port for each service instance that can be provided through that Customer Edge Port. Each Provider Edge Port shall be connected within the Provider Edge Bridge, as specified in 6.10, to a distinct Customer

Network Port on the S-VLAN component. Each C-VLAN component shall implement RSTP, with the enhancements to support Customer Edge Ports, as specified in 13.38.

NOTE—The single Customer Edge Port supported by a C-VLAN component can be supported by two or more independent instances of a MAC, aggregated as specified by Link Aggregation (Clause 43 of IEEE Std 802.3™).

Renumber the existing subclause 5.4 as 5.9.

6. Support of the MAC Service in VLANs

6.6 Enhanced Internal Sublayer Service

6.6.1 Service primitives

Change the service primitives to include a "drop_eligible" parameter, as follows:

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

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

Insert the following definition of the "drop_eligible" parameter before the definition of the vlan_identifier:

The **drop_eligible** parameter provides guidance to the recipient of the service indication or of an indication corresponding to the service request, and takes the values True or False. If drop_eligible is True, the parameters of the indication should be discarded in preference to others with drop_eligible False that result in frames queued with the same traffic class.

6.7 Support of the EISS

Replace the first two sentences of 6.7 as follows:

The EISS is supported by tagging and detagging functions that in turn use the ISS (6.4, 6.5). Any given instance of the EISS shall be supported by using one but not both of the following VLAN tag types:

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

selected as specified in Clause 9.5.

Insert the following sentence after item c):

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

d) A VID translation table.

Insert a new paragraph at the end of 6.7 (following the NOTE):

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

6.7.1 Data indications

Insert the following sentence to the paragraph before NOTE 1:

The values of the remaining parameters are affected by the contents of the tag header if the frame contains a VLAN tag of the type supported by this instance of the EISS.

Change item c) as follows:

c) The value contained in the VID field, optionally translated using the VID translation table, if the frame is VLAN-tagged;

Replace the sentence beginning with "The value of the priority parameter ..." through item f), renumbering subsequent items in the list, with the following:

The value of the **drop_eligible** and **priority** parameters are determined as follows:

f) If the frame is tagged, the value of the drop_eligible parameter and the received priority value are decoded from the tag header as described in 6.7.3. Otherwise;

g) The received priority is the value in the M_UNITDATA.indication and the value of the drop_eligible parameter is False.

h) The value of the priority parameter is then regenerated from the received priority, as specified in 6.7.4.

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

i) If the frame ~~is tagged~~ contains a Customer VLAN tag, then the value is as specified in Clause 9. Otherwise;

6.7.2 Data requests

Change the second sentence of the third paragraph of 6.7.2 as follows:

The values of the **vlan_identifier** (optionally translated using the VID translation table), **priority**, **drop_eligible**, **canonical_format_indicator**, and **rif_information** (if present) parameters are used to determine the contents of the tag header, in accordance with Clause 9.

Change the second sentence of the fifth paragraph of 6.7.2 as follows:

If the **canonical_format_indicator** parameter indicates that the mac_service_data_unit may contain embedded MAC Addresses in a format inappropriate to the destination MAC type, and no Customer VLAN tag header is to be inserted, then

Insert the following as new subclause 6.7.3, re-numbering the existing 6.7.3 as 6.7.4:

6.7.3 Priority Code Point encoding

The priority and drop_eligible parameters are encoded in the Priority Code Point (PCP) field of the VLAN tag using the Priority Code Point Encoding Table for the Port, and they are decoded from the PCP using the Priority Code Point Decoding Table. For each Port, the Priority Code Point Encoding Table has 16 entries, corresponding to each of the possible combinations of the eight possible values of priority (0 through 7) with the two possible values of drop_eligible (True or False). For each Port, the Priority Code Point Decoding Table has 8 entries, corresponding to each of the possible PCP values.

Alternative values for each table are specified as rows in Table 6-3 and Table 6-4, with each alternative labeled by the number of distinct priorities that can be communicated, and the number of these for which drop precedence can be communicated. For example, the table entries 6P2D allow six distinct priorities with drop precedence for two. The default values (8P0D) specify a PCP value equal to the priority value and do not support communication of drop precedence in the PCP field. The combination of the priority and drop_eligible parameters is shown by the priority alone if drop_eligible is False, and by the priority followed by the letters “DE” if drop_eligible is True.

Table 6-3—Priority Code Point encoding

priority drop_eligible		7	7DE	6	6DE	5	5DE	4	4DE	3	3DE	2	2DE	1	1DE	0	0DE
PCP	8P0D (default)	7	7	6	6	5	5	4	4	3	3	2	2	1	1	0	0
	7P1D	7	7	6	6	5	4	5	4	3	3	2	2	1	1	0	0
	6P2D	7	7	6	6	5	4	5	4	3	2	3	2	1	1	0	0
	5P3D	7	7	6	6	5	4	5	4	3	2	3	2	1	0	1	0

Table 6-4—Priority Code Point decoding

PCP		7	6	5	4	3	2	1	0
priority drop_eligible	8P0D (default)	7	6	5	4	3	2	1	0
	7P1D	7	6	4	4DE	3	2	1	0
	6P2D	7	6	4	4DE	2	2DE	1	0
	5P3D	7	6	4	4DE	2	2DE	0	0DE

If the VLAN tag is a Service VLAN tag, then Table 6-3 and Table 6-4 shall be supported. If the VLAN tag is a Customer VLAN tag, then the 8P0D row of each table shall be supported, and the remaining rows may be supported.

NOTE—To avoid potential misordering of packets, all Ports on a LAN should select the same row of Table 6-3 and Table 6-4. Interoperability considerations with Bridges supporting only the 8P0D row are discussed in G.7.

The values in the Priority Code Point Encoding Table and Priority Code Point Decoding Table may be modified by management, as described in Clause 12. If this capability is provided, the value of the table entries shall be independently settable for each Port. The values shall be constrained as follows:

a) For any two priority values with the same drop_eligible value, the lower priority shall not map to a higher PCP than the higher priority.
b) The lower of any two PCP values shall not map to a higher priority than the higher PCP.
c) With the exception of values 0 and 1, any priority value combined with drop_eligible True shall not map to a higher PCP than the same priority value combined with drop_eligible False.
d) With the exception of values 0 and 1, any PCP value shall not map to a priority value combined with drop_eligible True if a lower PCP maps to the same priority value combined with drop_eligible False.

The values may be further constrained, but if the tables can be modified, the default values shown in Table 6-3 and Table 6-4, and the alternative sets of values in Table 6-3 and Table 6-4 shall be settable.

If the VLAN tag is a Service VLAN tag (S-TAG), the drop_eligible parameter may also be encoded in and decoded from the Drop Eligible Indicator (DEI) in the S-TAG. Use of the DEI allows the S-TAG to convey eight distinct priorities, each with a drop eligible indication. If this capability is provided, it shall be independently manageable for each Port by means of a Use_DEI parameter. If the Use_DEI is True for the Port, the drop_eligible parameter is encoded in the DEI of transmitted frames, and the drop_eligible parameter shall be True for a received frame if the DEI is set in the S-TAG or the Priority Code Point Decoding Table indicates drop_eligible True for the received PCP value. If the Use_DEI parameter is False, the DEI shall be transmitted as zero and ignored on receipt. The default value of the Use_DEI parameter is False.

6.7.4 Regenerating priority

Renumber Table 6-3 as Table 6-5. There are no changes to the remainder of 6.7.4 (renumbered from 6.7.3).

Insert new subclauses 6.9, 6.10, and 6.11 after 6.8 as follows:

6.9 Support of the ISS for attachment to a Provider Bridged Network

This standard specifies both Customer Bridges (3.5) and Provider Bridges (3.17). The operation of Provider Bridges and Provider Bridged Networks is, by design, largely transparent to Customer Bridges and Customer Bridged Local Area Networks. Figure 15-1 illustrates the relationship of the service provided by the MAC Sublayer functionality of Provider Bridges to that used by a Customer Bridge. This subclause enables a mechanism for a Customer Bridge attached to a Provider Bridged Network to request priority handling of frames.

The functions specified in this subclause provide the ISS to the MAC Relay Entity of a Customer Bridge by making use of the underlying ISS provided by the Media Access Method Convergence function as shown in Figure 6-3. These functions shall be one of:

a) When Service Access Priority Selection is disabled, the functions shall be null; i.e., each M_UNITDATA.request received from the provided ISS results in a M_UNITDATA.request with indentical parameters presented to the underlying ISS, and each M_UNITDATA.indication received from the underlying ISS results in a M_UNITDATA.indication with identical parameters presented to the provided ISS.
b) When Service Access Priority Selection is enabled, the mac_service_data_unit in each M_UNIDATA.request is priority-tagged with an S-VLAN tag header when presented to the underlying ISS, and if an S-VLAN tag header is present in the mac_service_data_unit parameter in a M_UNITDATA.indication received from the underlying ISS.

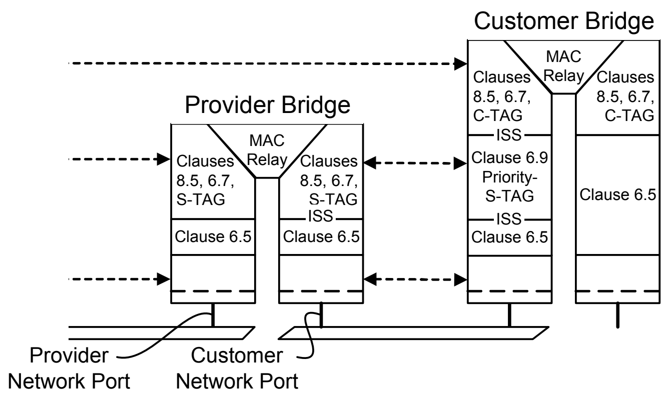

Figure 6-3—Service access priority selection

Specification of a null function allows a Customer Bridge without additional functionality to connect to a Provider Bridged Network.

Specification of the Service Access Priority Selection function allows the Customer Bridge Port to request priority handling of the frame from a Port-based service interface (15.3) to a Provider Bridged Network on the basis of the priority assigned within the Customer Bridged Local Area Network, while allowing for differences in cost and service level ascribed to individual values of priority within the service provider and customer networks.

6.9.1 Data requests

For each M_UNITDATA.request received from the provided ISS, a M_UNITDATA.request is presented to the underlying ISS with the following parameters:

The destination_address, source_address, and priority parameters are unchanged.

A tag header, formatted as necessary for the destination MAC type, is inserted as the initial octets of the mac_service_data_unit parameter. The Tag Protocol Identification is the Service VLAN Tag Ethertype (9.5). The Tag Control Information contains a null VLAN Identifier field, and PCP and DEI fields constructed as specified in 6.7.3 using a drop_eligible value of false and a service_access_priority value derived from the priority parameter using the Service Access Priority Table 6-5.

Table 6-5—Service Access Priority

Received priority	Default service access priority	Range
0	0	0–7
1	1	0–7
2	2	0–7
3	3	0–7
4	4	0–7
5	5	0-7
6	6	0–7
7	7	0–7

Table 6-5 specifies default service_access_priority values for each of the eight possible values of the priority parameter in the M_UNITDATA.request received from the provided ISS. These default values shall be used as the initial values of the corresponding entries of the Service Access Priority Table for each Port supporting Service Access Priority Selection. The values in the table may be modified by management. If this capability is provided, the value of the table entries shall be independently settable for each Port and for each value of priority, and the Bridge shall have the capability to use the full range of the values in the parameter ranges specified in the table.

The frame_check_sequence parameter is either unspecified or contains a value modified from the received frame_check_sequence value taking into account the changes in the mac_service_data_unit parameter.

NOTE—The priority of the original service request made of the customer network can be carried transparently and unchanged across the Provider Bridged Network in the Customer VLAN tag.

6.9.2 Data indications

For each M_UNITDATA.indication received from the underlying ISS, a M_UNITDATA.request is presented to the supported ISS with the following parameters:

The destination_address and source_address parameters are unchanged.

If the initial octets of the mac_service_data_unit do not contain a tag header with the Service VLAN tag Ethertype value (9.5), then the mac_service_data_unit and frame_check_sequence parameters are unchanged; otherwise,

a) the mac_service_data_unit is detagged by removing the octets of the Service VLAN tag header, and
b) the priority parameter is decoded from the Priority Code Point field (6.7.3), and
c) the frame_check_sequence parameter is either unspecified or contains a value modified from the received frame_check_sequence value taking into account the changes in the mac_service_data_unit parameter.

6.10 Support of the ISS within a system

A single system can comprise two or more instances of VLAN-aware Bridge components connected by one or more of their Ports. If those Ports are not otherwise accessible, the ISS may be provided by means outside the scope of this specification. Figure 15-4 provides an example. Each instance of such an implementation of the ISS shall support the MAC status and Point-to-point parameters. An M_UNITDATA.request at one of the Ports connected to such an instance of the ISS shall result in M_UNITDATA.indications with identical parameters at all other Ports connected to that instance.

For convenience of management, such instances of ISS provision are assigned the LAN MAC Type 802.1. Management parameters common to MACs of this type are specified in Clause 12.

NOTE—The ISS can also be supported at Bridge Ports wholly contained within a system by any IEEE 802 LAN technology, subject to the system requirements of the particular media access method.

6.11 Support of the ISS by additional technologies

The ISS may be supported by other technologies that provide either an IEEE 802 MAC Service or an emulated IEEE 802 MAC Service. The technology is responsible for invoking a M_UNIDATA.indication with appropriate parameters (6.4) for each received frame, and transmitting a frame in response to each M_UNITDATA.request. The mac_service_data_unit parameter in a M_UNITDATA.indication may include a tag header of a type recognized by the functions using the ISS (6.6). If multiplexing of multiple virtual instances of the MAC Service is provided, each virtual service must be

a) identified by the VID field in a tag header of a type recognized by the functions using the ISS, or
b) attached to separate instance of the ISS with no tag header in the mac_service_data_unit

(i.e., the only multiplexing recognized by the functions of the bridge relay are those identified by a VID).

8. Principles of bridge operation

8.1 Bridge operation

8.1.1 Relay

Change item d) and item i) of 8.1.1 as shown.

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

d) Priority and drop eligibility decoding from a VLAN tag, if present, and regeneration of priority, if required (6.6).

i) Metering of frames, potentially marking as drop eligible or discarding frames exceeding bandwidth limits (8.6.5).

Insert a new item m) in 8.1.1 and reletter subsequent items appropriately.

m) Preferential discard of drop eligible frames to preserve QoS for other frames (8.6.7).

8.6 The Forwarding Process

8.6.3 Frame filtering

Change the last paragraph of 8.6.3 as follows:

Each of the Reserved MAC Addresses specified in Table 8-1 shall be permanently configured in the Filtering Database in C-VLAN components~~aware Bridges~~. Each of the Reserved MAC Addresses specified in Table 8-2 shall be permanently configured in the Filtering Database in S-VLAN components. The Filtering Database Entries for Reserved MAC Addresses shall specify filtering for all Bridge Ports and all VLANs. Management shall not provide the capability to modify or remove entries for Reserved MAC Addresses.

Insert the following NOTE to the end of 8.6.3:

NOTE—The Reserved MAC Addresses specified in Table 8-1 determine the span of connectivity for the protocol frames using the address; they do not identify the protocol. The protocols are identified by the type field following the address fields. Specifically, the address allocated of IEEE 802.1X™ PAE determines that frames will only be conveyed to directly connected bridges, whether they are Customer or Provider Bridges, whereas the address allocated for IEEE 802.1AB™ LLDP determines that frames will be conveyed between peer Customer Bridges, regardless of whether they are connected through one or more Provider Bridges. It is anticipated that other protocols may use these same addresses to achieve the same span of connectivity. For example, an instance of LLDP intending to discover a directly attached bridge, regardless of whether it is a Customer or Provider Bridge, may use the IEEE 802.1X PAE address. Likewise an instance of IEEE 802.1X PAE intending to operate between peer Customer Bridges, even through a Provider Bridged Network, may use the IEEE 802.1AB LLDP address.

Replace Table 8-1 with the following table:

Table 8-1—C-VLAN component Reserved addresses

Assignment	Value
Bridge Group Address	01-80-C2-00-00-00
IEEE 802.3 Full Duplex PAUSE operation	01-80-C2-00-00-01
IEEE 802.3 Slow_Protocols_Multicast address	01-80-C2-00-00-02
IEEE 802.1X PAE address	01-80-C2-00-00-03
Reserved for future standardization—media access method specific	01-80-C2-00-00-04
Reserved for future standardization—media access method specific	01-80-C2-00-00-05
Reserved for future standardization	01-80-C2-00-00-06
Reserved for future standardization	01-80-C2-00-00-07
Provider Bridge Group Address	01-80-C2-00-00-08
Reserved for future standardization	01-80-C2-00-00-09
Reserved for future standardization	01-80-C2-00-00-0A
Reserved for future standardization	01-80-C2-00-00-0B
Reserved for future standardization	01-80-C2-00-00-0C
Provider Bridge GVRP Address	01-80-C2-00-00-0D
IEEE 802.1AB Link Layer Discovery Protocol multicast address	01-80-C2-00-00-0E
Reserved for future standardization	01-80-C2-00-00-0F

Insert new Table 8-2, renumbering subsequent tables:

Table 8-2—S-VLAN component Reserved addresses

Assignment	Value
IEEE 802.3 Full Duplex PAUSE operation	01-80-C2-00-00-01
IEEE 802.3 Slow_Protocols_Multicast address	01-80-C2-00-00-02
IEEE 802.1X PAE address	01-80-C2-00-00-03
Reserved for future standardization—media access method specific	01-80-C2-00-00-04
Reserved for future standardization—media access method specific	01-80-C2-00-00-05
Reserved for future standardization	01-80-C2-00-00-06
Reserved for future standardization	01-80-C2-00-00-07
Provider Bridge Group Address	01-80-C2-00-00-08
Reserved for future standardization	01-80-C2-00-00-09
Reserved for future standardization	01-80-C2-00-00-0A

8.6.5 Flow metering

Change the third paragraph of subclause 8.6.5 as follows:

Frames classified using the same set of classification rules are subject to the same flow meter. The flow meter can change the drop_eligible parameter associated with each frame and can ~~may~~ discard frames on the basis of the following parameters for each received frame and previously received frames, and the time elapsed since those frames were received:

Insert an new item before the existing item d) of 8.6.5, relettering existing item d) to item e):

d) The received value of the drop_eligible parameter

Insert the following NOTE 1 before the existing NOTE at the end of 8.6.5, and then renumber the existing NOTE as NOTE 2.

NOTE 1—Changing the value of the drop_eligible parameter may change the contents of the frame, depending on how the frame is tagged when transmitted, which may then require updating the frame_check_sequence. Mechanisms for conveying information from ingress to egress that the frame_check_sequence may require updating are implementation dependent.

8.6.7 Queue management

Change the NOTE at the end of 8.6.7 as follows:

NOTE—Applicable queue management algorithms include RED (random early detection) and WRED (weighted random early detection) (IETF RFC 2309 [B10]). If the Bridge supports drop precedence, i.e., is capable of decoding or encoding the drop_eligible parameter from or to the PCP field of VLAN tags (6.7.3), the algorithm should exhibit a higher probability of dropping frames with drop_eligible True.

Insert the following paragraph at the end of 8.6.7:

The probability of removing a frame with drop_eligible set shall not be less than that of removing a frame with drop_eligible False, all other conditions being equal. If a queue management algorithm is implemented, it should preferentially discard frames with drop_eligible True. If a Bridge supports encoding or decoding of drop_eligible from the PCP field of a VLAN tag (6.7.3) on any of its Ports, then it shall implement a boolean parameter Require Drop Encoding on each of its Ports with default value FALSE. If Require Drop Encoding is True and the Bridge Port cannot encode particular priorities with drop_eligible, then frames queued with those priorities and drop_eligible True shall be discarded and not transmitted.

8.12 Bridge Management Entity

Add the following item after item d):

e) Provider Bridges MIB.

In the NOTE and footnote 13, change "MSTP" to "MSTP and Provider Bridges".

8.13 Addressing

8.13.4 Reserved MAC Addresses

Change 8.13.4 as follows:

Any frame with a destination address that is a Reserved MAC Address shall not be forwarded by a Bridge. Reserved MAC Addresses for C-VLAN ~~aware Bridges~~ components and for S-VLAN components are specified in Table 8-1 and Table 8-2, respectively. These Group MAC Addresses are reserved for assignment to standard protocols, according to the criteria for such assignments (Clause 5.5 of ISO/IEC TR 11802-2).

8.13.5 Group MAC Addresses for spanning tree protocols

Change 8.13.5 as follows:

A Spanning Tree Protocol Entity uses an instance of the MAC Service provided by each of the Bridge's Ports to transmits frames addressed to the Spanning Tree Protocol Entities of all the other Bridges attached to the same LAN as that Port. A 48-bit universally administered Group Address, known as the Bridge Group Address, has been assigned (Table 8-1) for use by C-VLAN ~~aware Bridges~~ components for this purpose.

It is essential to the operation of the Spanning Tree Protocols that frames with this destination address both reach all peer protocol entities attached to the same LAN and do not reach protocol entities attached to other LANs. The Bridge Group Address is therefore included in the block of C-VLAN ~~aware Bridge~~ components Reserved MAC Addresses and is always filtered by Customer Bridges and C-VLAN components of Provider Edge Bridges (8.6.3).

As a network of Provider Bridges needs to appear to attached Customer Bridges as if it was a single LAN, frames addressed to the Bridge Group Address are forwarded by S-VLAN components. Provider Bridges also use a Spanning Tree Protocol to provide one or more loop-free active topologies, so a distinct 48-bit universally administered Group Address, the Provider Bridge Group Address, that can be confined to the LANs that their Bridge Ports attach has been assigned (Table 8-2). The Provider Bridge Group Address is included in both the C-VLAN component and the S-VLAN component Reserved MAC Addresses and is always filtered by all Bridges (8.6.3).

The source MAC address field of frames transmitted by Spanning Tree Protocol Entities contains the individual MAC Address for the Bridge Port used to transmit the frame.

8.13.6 Group MAC Addresses for GARP Applications

Change 8.13.6 as follows:

A GARP Entity that supports a given GARP Application transmits frames addressed to all other GARP Entities that implement the same GARP Application. The peers of each such entity bound a region of the network that contains no peers, commonly a single LAN in the case where all Bridges attached to the LAN implement the application. A distinct universally administered 48-bit Group Address is assigned to each GARP application. Filtering Database Entries for each GARP Application address assigned to an application that is supported by a C-VLAN ~~aware Bridge~~ component should be configured in the Filtering Database so as to confine frames for that application to the peer region, whereas addresses for applications that are not supported should not be included.

A set of 48-bit Universal Addresses, known as GARP Application addresses, have been assigned for use by C-VLAN ~~aware Bridges~~ components. The values of the GARP Application addresses are defined in Table 12-1 of IEEE Std 802.1D. These group MAC Addresses are reserved for assignment to standard protocols, according to the criteria for such assignments (Clause 5.5 of ISO/IEC TR 11802-2).

NOTE—Table 11-1 allocates a group MAC Address for use by the GVRP application; however, the value allocated in that table is one of the GARP Application addresses reserved by Table 12-1 of IEEE Std 802.1D.

As a network of Provider Bridges needs to appear to attached Customer Bridges as if it was a single LAN, Customer Bridge GARP Application Addresses are always forwarded by S-VLAN components. Certain GARP Applications may also be used by Provider Bridges, so distinct 48-bit universally administered Group Addresses that are C-VLAN component Reserved MAC Addresses but not S-VLAN component Reserved MAC Addresses are assigned for such use. One such address, the Provider Bridge GVRP Address, is assigned by this standard (Table 8-1).

The source address field of MAC frames conveying BPDUs or GARP PDUs contains the individual MAC Address for the Bridge Port through which the PDU is transmitted (8.13.2).

9. Tagged frame format

Change 9.5 as follows:

9.5 Tag Protocol Identification

~~A single type of tag is~~Two types of tags are specified:

a) a Customer VLAN tag (~~V~~C-TAG), for general use by C-VLAN Bridges (5.7) and C-VLAN components of Provider Edge Bridges (5.8.1);

b) a Service VLAN tag (S-TAG), reserved for use by S-VLAN Bridges (5.8), the S-VLAN component of Provider Edge Bridges (5.8.1), and C-VLAN Bridges desiring to signal priority to a Provider Bridged Network (6.9).

A distinct Ethertype has been allocated (Table 9-1) for use in the TPID field (9.4) of each tag type so they can be distinguished from each other, and from other protocols.

Table 9-1—802.1Q Ethernet Type allocations

Tag Type	Name	Value
Customer VLAN tag	IEEE 802.1Q Tag Protocol Type (802.1QTagType)	81-00
Service VLAN tag	IEEE 802.1Q Service Tag Type (802.1QSTagType)	88-a8

9.6 Customer VLAN Tag Control Information

Change the first paragraph and the paragraph after NOTE 1 of 9.6 as follows:.

The ~~V~~C-TAG TCI field (Figure 9-1) is two octets in length and encodes the vlan_identifier, drop_eligible, and priority parameters of the corresponding EISS M_UNITDATA.request as unsigned binary numbers and a Canonical Format Indicator (CFI) as a single bit.

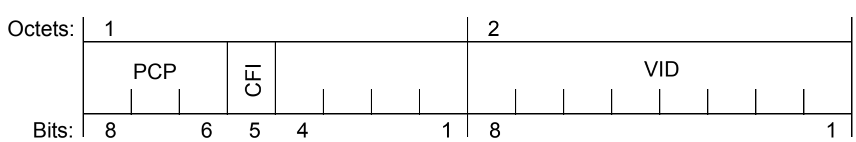

Figure 9-1— ~~V~~C-TAG TCI format

The VLAN Identifier (VID) is encoded in a 12-bit field. A VLAN-aware Bridge may not support the full range of VID values but shall support the use of all VID values in the range 0 through a maximum N, less than or equal to 4094 and specified for that implementation. Table 9-2 identifies VID values that have specific meanings or uses.

NOTE 1—There is a distinction between the range of VIDs that an implementation can support and the maximum number of active VLANs supported at any one time. An implementation supports only 16 active VLANs, for example, may use VIDs chosen from anywhere in the identifier space, or from a limited range. The latter can result in difficulties where different Bridges in the same network support different maximums. It is recommended that new implementations of this standard support the full range of VIDs, even if the number of active VLANs is limited.

The priority and drop_eligible parameters are ~~is~~ conveyed in the 3-bit Priority Code Point (PCP) field as specified in 6.7.3.

Insert new subclause 9.7, and Figure 9-2, as follows, renumbering subsequent subclauses appropriately:

9.7 Service VLAN Tag Control Information

The S-TAG TCI field (Figure 9-2) is two octets in length, and it encodes the priority, drop_eligible, and vlan_identifier parameters of the corresponding EISS M_UNITDATA.request as unsigned binary numbers.

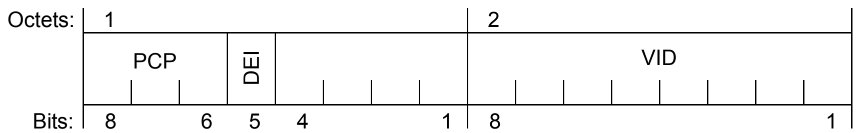

Figure 9-2— S-TAG TCI format

The semantics and structure of the S-TAG is identical to that of the C-TAG, with the exception that bit 5 in octet 1, the Drop Eligible Indicator (DEI) bit, does not convey a CFI (9.6). The priority and drop_eligible parameters are conveyed in the 3-bit PCP field and the DEI bit as specified in 6.7.3.

NOTE—Although a Service VLAN tag never includes a routing information field or an indication of canonical or non-canonical address formats, the MSDU of the associated frame can contain a Customer VLAN tag with these elements.

Change 9.8 (renumbered from 9.7) as follows:

9.8 Embedded Routing Information Field (E-RIF)

Replace "VLAN tag" with "C-VLAN tag" wherever the former occurs in this subclause.

11. VLAN topology management

Insert a new subclause 11.2.4 as follows:

11.2.4 VID Translation Table

If a VID Translation Table (6.7) is in use for a Bridge Port, the VID values received in GVRP Attributes are translated on reception of GVRP PDUs prior to GVRP processing as specified in this subclause (11.2) and translated after processing for encoding GVRP Attributes in transmitted GVRP PDUs.

Insert a new item f) in 11.3.1 as follows:

f) If a VID Translation Table (6.7) is in use for a Bridge Port, translate the VID values received in GVRP Attributes on that port prior to GVRP processing as specified in this subclause (11.2), and translate the VID values after processing for encoding in GVRP Attributes to be transmitted on that port.

12. Bridge management

12.6.2 Priority handling

Change the initial paragraph as follows:

The Priority Handling object models the operations that can be performed on, or inquire about, the Default Priority parameter, the Priority Regeneration Table parameter, ~~and~~ the Outbound Access Priority Table parameter, the Priority Code Point parameters, and the Service Access Priority parameters for each Port. The operations that can be performed on this object are as follows:

Insert the following items after item e):

f) Read Port Priority Code Point Selection (12.6.2.6);
g) Set Port Priority Code Point Selection (12.6.2.7);
h) Read Port Priority Code Point Decoding Table (12.6.2.8);
i) Optionally, Set Port Priority Code Point Decoding Table (12.6.2.9);
j) Read Port Priority Code Point Encoding Table (12.6.2.10);
k) Optionally, Set Port Priority Code Point Encoding Table (12.6.2.11);
l) Read Use_DEI parameter (12.6.2.12);
m) Optionally, Set Use_DEI parameter (12.6.2.13);
n) Read Require Drop Encoding parameter (12.6.2.14);
o) Optionally, Set Require Drop Encoding parameter (12.6.2.15);
p) Read Service Access Priority Selection (12.6.2.16);
q) Optionally, Set Service Access Priority Selection (12.6.2.17);
r) Read Service Access Priority Table (12.6.2.18);
s) Optionally, Set Service Access Priority Table (12.6.2.19).

Insert the following subclause to the end of 12.6.2:

12.6.2.6 Read Port Priority Code Point Selection

12.6.2.6.1 Purpose

To read which row of the Priority Code Point Encoding Table and Priority Code Point Decoding Table (6.7.3) is currently selected for use on this Port.

12.6.2.6.2 Inputs

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

12.6.2.6.3 Outputs

a) Priority Code Point Selection: this takes one of the following values:
   1) 8P0D;
   2) 7P1D;
   3) 6P2D;
   4) 5P3D.

12.6.2.7 Set Port Priority Code Point Selection

12.6.2.7.1 Purpose

To set which row of the Priority Code Point Encoding Table and Priority Code Point Decoding Table (6.7.3) will be selected for use on this Port.

12.6.2.7.2 Inputs

a) Port Number: the number of the Bridge Port.
b) Priority Code Point Selection: this takes one of the following values:
   1) 8P0D;
   2) 7P1D;
   3) 6P2D;
   4) 5P3D.

12.6.2.7.3 Outputs

None.

12.6.2.8 Read Priority Code Point Decoding Table

12.6.2.8.1 Purpose

To read the current contents of a row in the Priority Code Point Decoding Table (6.7.3) for a Port.

12.6.2.8.2 Inputs

a) Port Number: the number of the Bridge Port.
b) Priority Code Point Row: this takes one of the following values:
   1) 8P0D;
   2) 7P1D;
   3) 6P2D;
   4) 5P3D.

12.6.2.8.3 Outputs

a) Priority value for Priority Code Point 0: Integer in range 0–7;
b) Drop_eligible value for Priority Code Point 0: Boolean;
c) Priority value for Priority Code Point 1: Integer in range 0–7;
d) Drop_eligible value for Priority Code Point 1: Boolean;
e) Priority value for Priority Code Point 2: Integer in range 0–7;
f) Drop_eligible value for Priority Code Point 2: Boolean;
g) Priority value for Priority Code Point 3: Integer in range 0–7;
h) Drop_eligible value for Priority Code Point 3: Boolean;
i) Priority value for Priority Code Point 4: Integer in range 0–7;
j) Drop_eligible value for Priority Code Point 4: Boolean;
k) Priority value for Priority Code Point 5: Integer in range 0–7;
l) Drop_eligible value for Priority Code Point 5: Boolean;
m) Priority value for Priority Code Point 6: Integer in range 0–7;
n) Drop_eligible value for Priority Code Point 6: Boolean;
o) Priority value for Priority Code Point 7: Integer in range 0–7;
p) Drop_eligible value for Priority Code Point 7: Boolean.

12.6.2.9 Set Priority Code Point Decoding Table

12.6.2.9.1 Purpose

To modify the contents of a row in the Priority Code Point Decoding Table (6.7.3) for a Port.

12.6.2.9.2 Inputs

a) Port Number: the number of the Bridge Port;
b) Priority Code Point Row: this takes one of the following values:
   1) 8P0D;
   2) 7P1D;
   3) 6P2D;
   4) 5P3D;
c) Priority value for Priority Code Point 0: Integer in range 0–7;
d) Drop_eligible value for Priority Code Point 0: Boolean;
e) Priority value for Priority Code Point 1: Integer in range 0–7;
f) Drop_eligible value for Priority Code Point 1: Boolean;
g) Priority value for Priority Code Point 2: Integer in range 0–7;
h) Drop_eligible value for Priority Code Point 2: Boolean;
i) Priority value for Priority Code Point 3: Integer in range 0–7;
j) Drop_eligible value for Priority Code Point 3: Boolean;
k) Priority value for Priority Code Point 4: Integer in range 0–7;
l) Drop_eligible value for Priority Code Point 4: Boolean;
m) Priority value for Priority Code Point 5: Integer in range 0–7;
n) Drop_eligible value for Priority Code Point 5: Boolean;
o) Priority value for Priority Code Point 6: Integer in range 0–7;
p) Drop_eligible value for Priority Code Point 6: Boolean;
q) Priority value for Priority Code Point 7: Integer in range 0–7;
r) Drop_eligible value for Priority Code Point 7: Boolean.

12.6.2.9.3 Outputs

None.

12.6.2.10 Read Priority Code Point Encoding Table

12.6.2.10.1 Purpose

To read the current contents of a row in the Priority Code Point Encoding Table (6.7.3) for a Port.

12.6.2.10.2 Inputs

a) Port Number: the number of the Bridge Port;
b) Priority Code Point Row: this takes one of the following values:
   1) 8P0D;
   2) 7P1D;
   3) 6P2D;
   4) 5P3D.

12.6.2.10.3 Outputs

a) Priority Code Point value for priority 0 with drop_eligible False: Integer in range 0–7;
b) Priority Code Point value for priority 0 with drop_eligible True: Integer in range 0–7;
c) Priority Code Point value for priority 1 with drop_eligible False: Integer in range 0–7;
d) Priority Code Point value for priority 1 with drop_eligible True: Integer in range 0–7;
e) Priority Code Point value for priority 2 with drop_eligible False: Integer in range 0–7;
f) Priority Code Point value for priority 2 with drop_eligible True: Integer in range 0–7;
g) Priority Code Point value for priority 3 with drop_eligible False: Integer in range 0–7;
h) Priority Code Point value for priority 3 with drop_eligible True: Integer in range 0–7;

i) Priority Code Point value for priority 4 with drop_eligible False: Integer in range 0–7;
j) Priority Code Point value for priority 4 with drop_eligible True: Integer in range 0–7;
k) Priority Code Point value for priority 5 with drop_eligible False: Integer in range 0–7;
l) Priority Code Point value for priority 5 with drop_eligible True: Integer in range 0–7;
m) Priority Code Point value for priority 6 with drop_eligible False: Integer in range 0–7;
n) Priority Code Point value for priority 6 with drop_eligible True: Integer in range 0–7;
o) Priority Code Point value for priority 7 with drop_eligible False: Integer in range 0–7;
p) Priority Code Point value for priority 7 with drop_eligible True: Integer in range 0–7.

12.6.2.11 Set Priority Code Point Encoding Table

12.6.2.11.1 Purpose

To modify the contents of a row in the Priority Code Point Encoding Table (6.7.3) for a Port.

12.6.2.11.2 Inputs

a) Port Number: the number of the Bridge Port;
b) Priority Code Point Row: this takes one of the following values:
    1) 8P0D;
    2) 7P1D;
    3) 6P2D;
    4) 5P3D;
c) Priority Code Point value for priority 0 with drop_eligible False: Integer in range 0–7;
d) Priority Code Point value for priority 0 with drop_eligible True: Integer in range 0–7;
e) Priority Code Point value for priority 1 with drop_eligible False: Integer in range 0–7;
f) Priority Code Point value for priority 1 with drop_eligible True: Integer in range 0–7;
g) Priority Code Point value for priority 2 with drop_eligible False: Integer in range 0–7;
h) Priority Code Point value for priority 2 with drop_eligible True: Integer in range 0–7;
i) Priority Code Point value for priority 3 with drop_eligible False: Integer in range 0–7;
j) Priority Code Point value for priority 3 with drop_eligible True: Integer in range 0–7;
k) Priority Code Point value for priority 4 with drop_eligible False: Integer in range 0–7;
l) Priority Code Point value for priority 4 with drop_eligible True: Integer in range 0–7;
m) Priority Code Point value for priority 5 with drop_eligible False: Integer in range 0–7;
n) Priority Code Point value for priority 5 with drop_eligible True: Integer in range 0–7;
o) Priority Code Point value for priority 6 with drop_eligible False: Integer in range 0–7;
p) Priority Code Point value for priority 6 with drop_eligible True: Integer in range 0–7;
q) Priority Code Point value for priority 7 with drop_eligible False: Integer in range 0–7;
r) Priority Code Point value for priority 7 with drop_eligible True: Integer in range 0–7.

12.6.2.11.3 Outputs

None.

12.6.2.12 Read Use_DEI Parameter

12.6.2.12.1 Purpose

To read the current state of the Use_DEI parameter (6.7.3) for the Port.

12.6.2.12.2 Inputs

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

12.6.2.12.3 Outputs

a) Use_DEI parameter: Boolean.

12.6.2.13 Set Use_DEI Parameter

12.6.2.13.1 Purpose

To set the current state of the Use_DEI parameter (6.7.3) for the Port.

12.6.2.13.2 Inputs

a) Port Number: the number of the Bridge Port.
a) Use_DEI parameter: Boolean.

12.6.2.13.3 Outputs

None.

12.6.2.14 Read Require Drop Encoding Parameter

12.6.2.14.1 Purpose

To read the current state of the Require Drop Encoding parameter (8.6.6) for the Port.

12.6.2.14.2 Inputs

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

12.6.2.14.3 Outputs

a) Require Drop Encoding parameter: Boolean.

12.6.2.15 Set Require Drop Encoding Parameter

12.6.2.15.1 Purpose

To set the current state of the Require Drop Encoding parameter (8.6.6) for the Port.

12.6.2.15.2 Inputs

a) Port Number: the number of the Bridge Port.
b) Require Drop Encoding parameter: Boolean.

12.6.2.15.3 Outputs

None.

12.6.2.16 Read Service Access Priority Selection

12.6.2.16.1 Purpose

To read the current state of whether Service Access Priority Selection is enabled (6.9) for the Port.

12.6.2.16.2 Inputs

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

12.6.2.16.3 Outputs

a) Enable Service Access Priority Selection: the permissible values are as follows:
    1) Enabled;
    2) Disabled.

12.6.2.17 Set Service Access Priority Selection

12.6.2.17.1 Purpose

To enable or disable Service Access Priority Selection (6.9) for the Port.

12.6.2.17.2 Inputs

a) Port Number: the number of the Bridge Port.
b) Service Access Priority Selection: the permissible values are as follows:
    1) Enabled;
    2) Disabled.

12.6.2.17.3 Outputs

None.

12.6.2.18 Read Service Access Priority Table

12.6.2.18.1 Purpose

To read the current contents of the Service Access Priority Table (6.9.1) for the Port.

12.6.2.18.2 Inputs

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

12.6.2.18.3 Outputs

a) Service Access Priority value for Received Priority 0: Integer in range 0–7;
b) Service Access Priority value for Received Priority 1: Integer in range 0–7;
c) Service Access Priority value for Received Priority 2: Integer in range 0–7;
d) Service Access Priority value for Received Priority 3: Integer in range 0–7;
e) Service Access Priority value for Received Priority 4: Integer in range 0–7;
f) Service Access Priority value for Received Priority 5: Integer in range 0–7;
g) Service Access Priority value for Received Priority 6: Integer in range 0–7;
h) Service Access Priority value for Received Priority 7: Integer in range 0–7.

12.6.2.19 Set Service Access Priority Table

12.6.2.19.1 Purpose

To modify the contents of the Service Access Priority Table (6.9.1) for the Port.

12.6.2.19.2 Inputs

a) Port Number: the number of the Bridge Port;
b) Service Access Priority value for Received Priority 0: Integer in range 0–7;
c) Service Access Priority value for Received Priority 1: Integer in range 0–7;
d) Service Access Priority value for Received Priority 2: Integer in range 0–7;
e) Service Access Priority value for Received Priority 3: Integer in range 0–7;
f) Service Access Priority value for Received Priority 4: Integer in range 0–7;
g) Service Access Priority value for Received Priority 5: Integer in range 0–7;
h) Service Access Priority value for Received Priority 6: Integer in range 0–7;
i) Service Access Priority value for Received Priority 7: Integer in range 0–7.

12.6.2.19.3 Outputs

None.

Insert the following subclause to the end of Clause 12:

12.13 Provider Bridge management

The conformance requirements of Provider Bridges are specified in 5.8. The S-VLAN component and the externally accessible ports of all Provider Bridges, including Provider Edge Bridges, are managed using the managed objects defined in 12.4 through 12.12. This subclause defines additional managed objects specific to the operation of Provider Bridges.

The internal ports, LANs, and C-VLAN components of a Provider Edge Bridge are not managed directly using the managed objects defined in 12.4 through 12.12. Their operation is controlled and monitored through managed objects defined in this subclause.

Each externally accessible Bridge Port on a Provider Bridge is designated as a Provider Network Port, Customer Network Port, or Customer Edge Port. Designating a port as a Customer Edge Port implies Provider Edge Bridge functionality and, specifically, the existence of a C-VLAN component associated with that port. This C-VLAN component is uniquely identified within the Bridge by the port number of the associated Customer Edge Port.

Adding a Customer Edge Port to the member set of an S-VLAN implies the existence of an internal LAN connecting the S-VLAN component to the C-VLAN component, and the corresponding internal Customer Network Port and Provider Edge Port. This internal connection is uniquely identified by Customer Edge Port number and the S-VID.

The management of the forwarding process, filtering data base, and C-VLANs of the C-VLAN component and the internal connections are achieved through the Customer Edge Port Configuration managed object defined here (12.13.3).

A C-VLAN component associated with a Customer Edge Port that is in the member set of more than one S-VLAN (implying more than one internal connection in the S-VLAN component) runs an instance of the Rapid Spanning Tree Protocol that participates with the customer Spanning Tree Protocol (13.38). This protocol instance is managed using the managed objects defined in 12.8 and 12.12. All BPDUs generated by this protocol instance use the MAC address of the Customer Edge port as a source address. For each internal Provider Edge Port, the protocol uses the S-VID associated with that internal connection as a port number. For the Customer Edge Port, the protocol uses the value 0xFFF as the port number.

The following managed objects define the semantics of the management operations specific to Provider Bridges:

a) The Provider Bridge Port Type managed object (12.13.1);
b) The Network Port Configuration managed object (12.13.2);
c) The Customer Edge Port Configuration managed object (12.13.3).

12.13.1 Provider Bridge Port Type managed object

The management operations that can be performed on the Provider Bridge Port Type managed object are as follows:

a) Read Provider Bridge Port Type (12.13.1.1);
b) Optionally, Configure Provider Bridge Port Type (12.13.1.2).

12.13.1.1 Read Provider Bridge Port Type

12.13.1.1.1 Purpose

To obtain information regarding the designated type of an externally accessible port on a Provider Bridge.

12.13.1.1.2 Inputs

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

12.13.1.1.3 Outputs

a) Port Type: this takes one of the following values:
    1) Provider Network Port;
    2) Customer Network Port;
    3) Customer Edge Port.

12.13.1.2 Configure Provider Bridge Port Type

12.13.1.2.1 Purpose

To designate the type of an externally accessible port on a Provider Bridge.

12.13.1.2.2 Inputs

a) Port Number: the number of the Bridge Port.
b) Port Type: this takes one of the following values:
    1) Provider Network Port;
    2) Customer Network Port;
    3) Customer Edge Port.

12.13.1.2.3 Outputs

None.

12.13.2 Network Port Configuration managed object

The Network Port Configuration managed object applies to each externally accessible Customer Network Port or Provider Network Port on a Provider Bridge. It includes

a) The VID Translation Table, which provides a bidirectional mapping between a local S-VID (used in data and protocol frames transmitted and received through this Customer Network Port or Provider Network Port) and a relay S-VID (used by the filtering and forwarding processes of the S-VLAN component in a Provider Bridge).

The management operations that can be performed are as follows:

b) Read VID Translation Table Entry (12.13.2.1);
c) Configure VID Translation Table Entry (12.13.2.6).

12.13.2.1 Read VID Translation Table Entry

12.13.2.1.1 Purpose

To read the relay S-VID associated with the local S-VID.

12.13.2.1.2 Inputs

a) Port Number: the number of the Customer or Provider Network Port.
b) Local VLAN Identifier: a 12-bit VID.

12.13.2.1.3 Outputs

a) Relay VLAN Identifier: a 12-bit VID.

12.13.2.6 Configure VID Translation Table Entry

12.13.2.6.1 Purpose

To modify an entry in the VID Translation Table.

12.13.2.6.2 Inputs

a) Port Number: the number of the Customer or Provider Network Port.
b) Local VLAN Identifier: a 12-bit VID.
c) Relay VLAN Identifier: a 12-bit VID.

12.13.2.6.3 Outputs

None.

12.13.3 Customer Edge Port Configuration managed object

The Customer Edge Port Configuration managed object applies to each externally accessible Customer Edge Port on a Provider Edge Bridge. It includes

a) The C-VID Registration Table, which provides a mapping between a Customer VLAN Identifier (C-VID) and the service instance represented by a Service VLAN Identifier (S-VID) selected for that C-VLAN. This table provides the equivalent functionality of

1) configuring the PVID of the internal Customer Network Port on the S-VLAN component;
2) adding the corresponding Provider Edge Port on the C-VLAN component to the member set of the C-VLAN;
3) adding the Provider Edge Port and/or Customer Edge Port to the untagged set of the C-VLAN (if it is desired that frames forwarded to that port are transmitted untagged for this C-VLAN).

b) The Provider Edge Port configuration parameters, which provide the subset of the Bridge VLAN Configuration managed object (12.10.1) that is relevant for the internal ports of the C-VLAN component associated with the Customer Edge Port.
c) The Service Priority Regeneration Table, which provides the Priority Regeneration Table (12.6.2) for each internal Customer Network Port connected to the C-VLAN component associated with the Customer Edge Port.

The management operations that can be performed are as follows:

a) Read C-VID Registration Table Entry (12.13.3.1);
b) Configure C-VID Registration Table Entry (12.13.3.2);
c) Read Provider Edge Port Configuration (12.13.3.3);
d) Set Provider Edge Port Configuration (12.13.3.4);
e) Read Service Priority Regeneration Table (12.13.3.5);
f) Set Service Priority Regeneration Table (12.13.3.6).

12.13.3.1 Read C-VID Registration Table Entry

12.13.3.1.1 Purpose

To read the VLAN Identifier of the service associated with a specific Customer VLAN in the C-VLAN component of a Provider Edge Bridge.

12.13.3.1.2 Inputs

a) Port Number: the number of the Customer Edge Port;
b) Customer VLAN Identifier: a 12-bit C-VID.

12.13.3.1.3 Outputs

a) Service VLAN Identifier: a 12-bit S-VID;
b) Untagged PEP: a boolean indicating frames for this C-VLAN should be forwarded untagged through the Provider Edge Port;
c) Untagged CEP: a boolean indicating frames for this C-VLAN should be forwarded untagged through the Customer Edge Port.

12.13.3.2 Configure C-VID Registration Table Entry

12.13.3.2.1 Purpose

To modify an entry in the C-VID Registration Table.

12.13.3.2.2 Inputs

a) Port Number: the number of the Customer Edge Port;
b) Customer VLAN Identifier: a 12-bit C-VID;
c) Service VLAN Identifier: a 12-bit S-VID;
d) Untagged PEP: a boolean indicating frames for this C-VLAN should be forwarded untagged through the Provider Edge Port;

e) Untagged CEP: a boolean indicating frames for this C-VLAN should be forwarded untagged through the Customer Edge Port.

12.13.3.2.3 Outputs

None.

12.13.3.3 Read Provider Edge Port Configuration

12.13.3.3.1 Purpose

To read the current configuration of an internal Provider Edge Port in the C-VLAN component of a Provider Edge Bridge.

12.13.3.3.2 Inputs

a) Port Number: the number of the Customer Edge Port;
b) Service VLAN Identifier: a 12-bit S-VID.

12.13.3.3.3 Outputs

a) PVID: a 12-bit C-VID to be used for untagged frames received at the Provider Edge Port;
b) Default User Priority: an integer range 0-7 to be used for untagged frames received at the Provider Edge Port;
c) Acceptable Frame Types: the Acceptable Frame Types (8.6.2) for frames received at the Provider Edge Port. The permissible values for the parameter are as follows:
    1) *Admit only VLAN-Tagged frames*;
    2) *Admit only Untagged and Priority-Tagged frames*;
    3) *Admit all frames*;
d) Enable Ingress Filtering: the Enable Ingress Filtering parameter for frames received at the Provider Edge Port. The permissible values for the parameter are as follows:
    1) Enabled;
    2) Disabled.

12.13.3.4 Set Provider Edge Port Configuration

12.13.3.4.1 Purpose

To modify the configuration of a Provider Edge Port in the C-VLAN component of a Provider Edge Bridge.

12.13.3.4.2 Inputs

a) Port Number: the number of the Customer Edge Port;
b) Service VLAN Identifier: a 12-bit S-VID;
c) PVID: a 12-bit C-VID to be used for untagged frames received at the Provider Edge Port;
d) Default User Priority: an integer range 0-7 to be used for untagged frames received at the Provider Edge Port;
e) Acceptable Frame Types: the Acceptable Frame Types (8.6.2) for frames received at the Provider Edge Port. The permissible values for the parameter are as follows:
    1) *Admit only VLAN-Tagged frames*;
    2) *Admit only Untagged and Priority-Tagged frames*;
    3) *Admit all frames*;

f) Enable Ingress Filtering: the Enable Ingress Filtering parameter for frames received at the Provider Edge Port. The permissible values for the parameter are as follows:
   1) Enabled;
   2) Disabled.

12.13.3.4.3 Outputs

None.

12.13.3.5 Read Service Priority Regeneration Table

12.13.3.5.1 Purpose

To read the current contents of the Priority Regeneration Table (6.7.3) for an internal Customer Network Port connected to the C-VLAN component associated with a Customer Edge Port.

12.13.3.5.2 Inputs

a) Port Number: the number of the Customer Edge Port;
b) Service VLAN Identifier: a 12-bit S-VID.

12.13.3.5.3 Outputs

a) Regenerated Priority value for Received Priority 0: Integer in range 0–7;
b) Regenerated Priority value for Received Priority 1: Integer in range 0–7;
c) Regenerated Priority value for Received Priority 2: Integer in range 0–7;
d) Regenerated Priority value for Received Priority 3: Integer in range 0–7;
e) Regenerated Priority value for Received Priority 4: Integer in range 0–7;
f) Regenerated Priority value for Received Priority 5: Integer in range 0–7;
g) Regenerated Priority value for Received Priority 6: Integer in range 0–7;
h) Regenerated Priority value for Received Priority 7: Integer in range 0–7.

12.13.3.6 Set Service Priority Regeneration Table

12.13.3.6.1 Purpose

To modify the contents of the Priority Regeneration Table (6.7.3) for an internal Customer Network Port connected to the C-VLAN component associated with a Customer Edge Port.

12.13.3.6.2 Inputs

a) Port Number: the number of the Customer Edge Port;
b) Service VLAN Identifier: a 12-bit S-VID;
c) Regenerated Priority value for Received Priority 0: Integer in range 0–7;
d) Regenerated Priority value for Received Priority 1: Integer in range 0–7;
e) Regenerated Priority value for Received Priority 2: Integer in range 0–7;
f) Regenerated Priority value for Received Priority 3: Integer in range 0–7;
g) Regenerated Priority value for Received Priority 4: Integer in range 0–7;
h) Regenerated Priority value for Received Priority 5: Integer in range 0–7;
i) Regenerated Priority value for Received Priority 6: Integer in range 0–7;
j) Regenerated Priority value for Received Priority 7: Integer in range 0–7.

12.13.3.6.3 Outputs

None.

13. The Multiple Spanning Tree Protocol (MSTP)

Insert the following subclause after 13.37:

13.38 Customer Edge Port Spanning Tree operation

This subclause specifies the operation of the Spanning Tree Protocol Entity within a C-VLAN component that supports a Customer Edge Port (Figure 15-4) of a Provider Edge Bridge. The Customer Edge Port and each Provider Edge Port are treated as separate Bridge Ports by the spanning tree protocol.

If the C-VLAN component connects to the S-VLAN component with a single Provider Edge Port, and the associated service instance supports no more than two customer interfaces, then all frames (including Spanning Tree BPDUs) addressed to the Bridge Group Address may be relayed between the two Ports of the C-VLAN component without modification. Otherwise, the Spanning Tree Protocol Entity shall execute the Rapid Spanning Tree Protocol (RSTP, Clause 17 of IEEE Std 802.1D), as modified by the provisions of this subclause.

The RSTP enhancements specified do not reduce Provider Bridged Network connectivity between Customer Edge Ports to a single spanning tree of service instances but ensure that connectivity for frames assigned to any given C-VLAN is loop free. In this respect, the C-VLAN component's spanning tree protocol operation is equivalent to, but simpler to manage than, the operation of MSTP.

13.38.1 Provider Edge Port operPointToPointMAC and operEdge

The value of the adminPointToPointMAC parameter for a Provider Edge Port is always Auto, and no management control over its setting is provided. The value of the operPointToPointMAC parameter, used by the RSTP state machines, shall be true if the service instance corresponding to the Provider Edge Port connects at most two customer interfaces, and false otherwise.

The value of the adminEdge, autoEdge, and operEdge parameters for a Provider Edge Port are always false, true, and false, respectively. No management control over their setting is provided.

13.38.2 updtRolesTree()

The spanning tree priority vectors and timer values are calculated as specified for the updtRolesTree() procedure in IEEE Std 802.1D. The port role for each Port, its port priority vector, and timer information are also updated as specified by IEEE Std 802.1D, with one exception. If selectedRole was to be set to AlternatePort, the Port is an Provider Edge Port, and the root priority vector was derived from another Provider Edge Port, then the selectedRole shall be set to Root Port.

NOTE—The effect of this enhancement is to allow the C-VLAN component to have multiple Root Ports (just as if separate per S-VLAN trees were being provided), if they are all Provider Edge Ports. As the C-VLAN component assigns each frame to a single C-VLAN and maps any given C-VLAN to and from at most one Provider Edge Port, no loop is created.

13.38.3 setReRootTree(), setSyncTree(), setTcPropTree()

IEEE Std 802.1D specifies that the setReRootTree() and setSyncTree() procedures set the reRoot and sync variables for all Ports of the bridge, and the setTcPropTree() sets the tcProp variable for all Ports other than the Port that invoked the procedure. If the Port invoking the procedure is a Customer Edge Port, then this behavior is unchanged; if it is a Provider Edge Port, then the behavior of each procedure shall be as follows.

The setReRootTree() procedure sets reRoot for the Port invoking the procedure and for the Customer Edge Port.

The setSyncTree() procedure sets sync for the Port invoking the procedure and for the Customer Edge Port.

The setTcPropTree() procedure sets tcProp for the Customer Edge Port.

13.38.4 allSynced, reRooted

IEEE Std 802.1D specifies a single value of the allSynced and reRooted state machine conditions for all Bridge Ports. This specification requires an independent value of each of these conditions for each Port of the C-VLAN component. If that Port is the Customer Edge Port, then allSynced shall be true if and only if synced is true for all Provider Edge Ports, and reRooted shall be true if and only if rrWhile is zero for all Provider Edge Ports. If the Port for which the condition is being evaluated is a Provider Edge Port, then allSynced shall take the value of synced for the Customer Edge Port, and reRooted shall be true if and only if rrWhile is zero for the Customer Edge Port.

13.38.5 Configuration parameters

All performance and configuration parameters for RSTP should be set to their recommended defaults, with the exception of the following, which are chosen to minimize the chance of interfering with the customer’s spanning tree configuration (e.g., by the C-VLAN component becoming the root of the customer spanning tree), as follows:

a) The Bridge Identifier Priority/Bridge Priority (17.14 and Table 17-2 of IEEE Std 802.1D) should be set to 61 440. This sets the priority part of the Bridge Identifier (the most significant 4 bits; see 9.2.5 of IEEE Std 802.1D) to hex F.
b) The following 12 bits (the Bridge Identifier system ID extension) should be set to hex FFF.
c) The Port Priority (17.14 and Table 17-2 of IEEE Std 802.1D) should be set to 32. This sets the priority part of the Port Identifier (the most significant 4 bits) to hex 2, a higher priority than the default (128, or hex 8).
d) The Port Path Cost values for Provider Edge Ports should be set are to 128.

All BPDUs generated by the Spanning Tree Protocol Entity within a C-VLAN component use the MAC address of the Customer Edge Port as a source address. For each internal Provider Edge Port, the protocol uses the S-VID associated with the corresponding internal Customer Network Port on the S-VLAN component as a port number. For the Customer Edge Port, the protocol uses the value 0xFFF as the port number.

Insert the following new clause after Clause 14.

15. Support of the MAC Service by Provider Bridged Networks

Provider Bridges interconnect the separate MACs of the IEEE 802 LANs that compose a Provider Bridged Network, relaying frames to provide connectivity between all LANs that provide customer interfaces for each service instance. The position of the Provider Bridge S-VLAN component bridging function within the MAC Sublayer is shown in Figure 15-1.

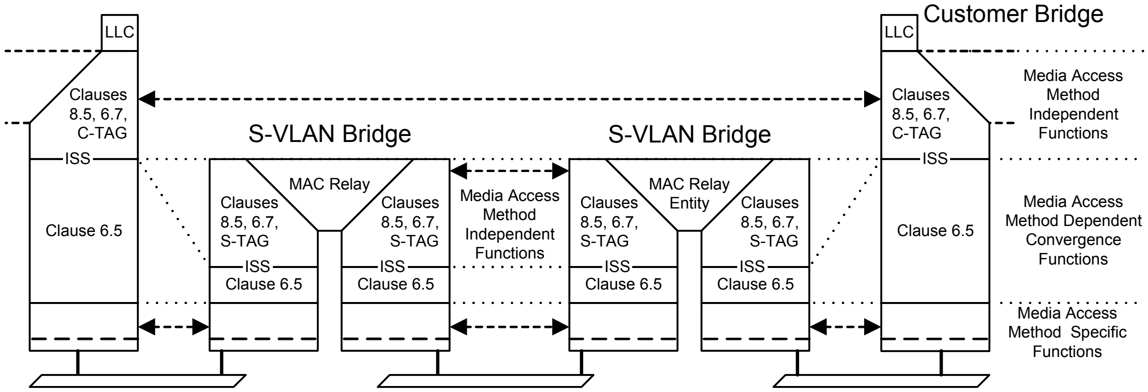

Figure 15-1—Internal organization of the MAC sublayer in a Provider Bridged Network

This clause discusses the following aspects of provisioning service instances on a Provider Bridged Network

a) Service transparency
b) Customer service interfaces
c) Service instance segregation
d) Service instance selection and identification
e) Service priority selection
f) Service access protection

NOTE—In describing the MAC Service, this standard makes use of term "service" as defined by the OSI Reference Model (ISO 7498). In this sense, a service comprises a set of primitives and associated parameters, provided by one protocol layer in the architectural model to the protocol layer above, and the causal relationships between the primitives invoked by an upper layer protocol entity in one system with those resulting indications to a peer entity in another system. The term "service" used by service providers, while including layering concepts, goes far beyond this formal definition, and commonly specifies some or all of the following: interfacing considerations across multiple protocol layers (including physical connectors, for example); selection of interface points; interfacing equipment; quality of service guarantees and measurement methods; charging methods and responsibilities; connectivity verification and other management tools; and regulatory issues. Many of these aspects lie outside the scope of this standard; the reader is referred to the Bibliography in Annex H, which includes references to completed and ongoing work in the MEF (Metro Ethernet Forum) and the ITU.

15.1 Service transparency

The operation of Provider Bridges and the networks they compose is, by design, largely transparent to Customer Bridges and Customer Bridged Local Area Networks as illustrated by Figure 15-1.

The service provided by Provider Bridges is transparent to the use of the MAC Service by end stations attached to the Customer Bridged LANs and transparent to the operation of media access method independent functions by Customer Bridges.

The service is not transparent to the operation of media access method dependent convergence functions, specified in 6.5 of this standard, or to the operation of the media access method specific functions specified by standards for each media access method. Media access method dependent and specific functions operate between bridges, whether Customer Bridges or Provider Bridges, attached to the same LAN. Where these functions make use of standard Group MAC Addresses, those addresses are included in the Reserved Addresses that are always filtered by Customer Bridges (Table 8-1) and by Provider Bridges (Table 8-2).

Frames transmitted and received by media access method independent functions particular to Provider Bridged Network operation are not forwarded by Customer Bridges between provider networks. Where these frames are addressed using standard Group MAC Addresses, those addresses are included in the Reserved Addresses that are always filtered by Customer Bridges (Table 8-1). In addition, such frames may be filtered from Provider Edge Ports.

15.2 Customer service interfaces

A service provider can offer a customer one or more types of service interfaces, each providing different capabilities for service selection, priority selection, and service access protection (15.7, 15.8, and 15.9). Some service interfaces are provided by the service provider operating systems that include C-VLAN components, or by customer operating systems that include S-VLAN components. In all cases, segregation of different service instances is achieved at an interface wholly under the control of the service provider by authentication and authorization of the attached customer systems, and by verification of customer provided parameters that provide service instance selection.

NOTE—The term "service access protection" describes provision of service access over multiple access LANs with redundancy and rapid failover in case of failure of an access LAN or attached equipment.

Access to a given service instance can be provided through different types of customer interface.

15.3 Port-based service interface

The customer service interfaces that can be provided by a provider network are specified by reference to a Customer Network Port provided by the S-VLAN component of a Provider Bridge. The Customer Network Port provides a single service instance, as illustrated in Figure 15-2 and Figure 15-3. The attached customer system can be a bridge, a router, or an end station.

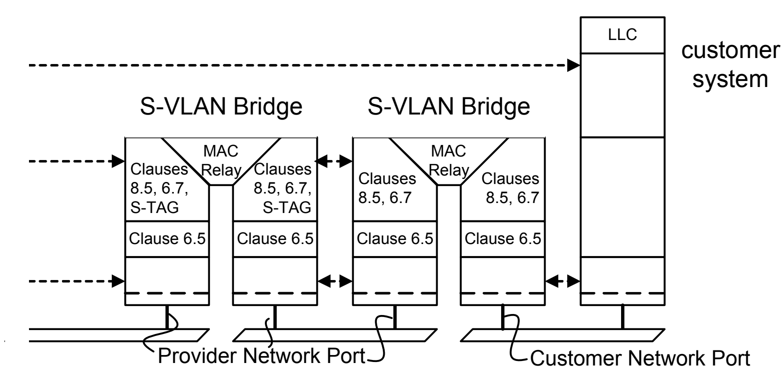

Figure 15-2—Port-based service interface to a Provider Bridged Network

This interface is Port-based; i.e., customers select and identify different service instances by associating each with a different Customer Network Port. Frames transmitted to a Customer Network Port by a C-VLAN aware customer system do not include an S-VID but can be priority-tagged with an S-TAG (6.9).

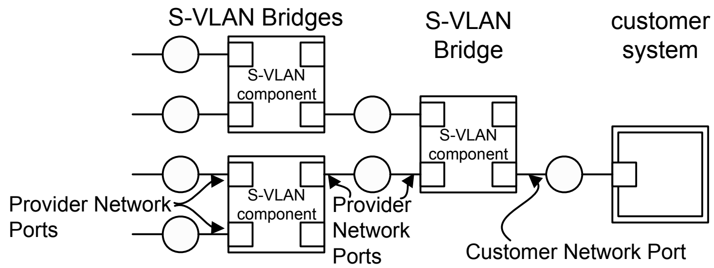

Figure 15-3—Port-based service interface to a Provider Bridged Network

NOTE—The terms "Customer Network Port," "Customer Edge Port, Provider Network Port," and "Provider Edge Port," do not refer to the ownership of equipment, or necessarily to differently implemented Ports, but to Ports that are configured to fulfil the requirements of precise roles within a structured provider network design. These requirements are described in 15.6 through 15.9 and in Clause 16. All "Network" Ports are part of S-VLAN components, and all "Edge" Ports are part of C-VLAN components, whereas all "Customer" Ports receive data from a single customer inbound to the network and transmit data outbound from the network to a single customer. See Clause 3 for definitions.

15.4 C-tagged service interface

A C-tagged service interface can be provided by a Provider Edge Bridge comprising one or more C-VLAN components attached to Port-based service interfaces provided by a single S-VLAN aware component, as illustrated by Figure 15-4 and Figure 15-5.

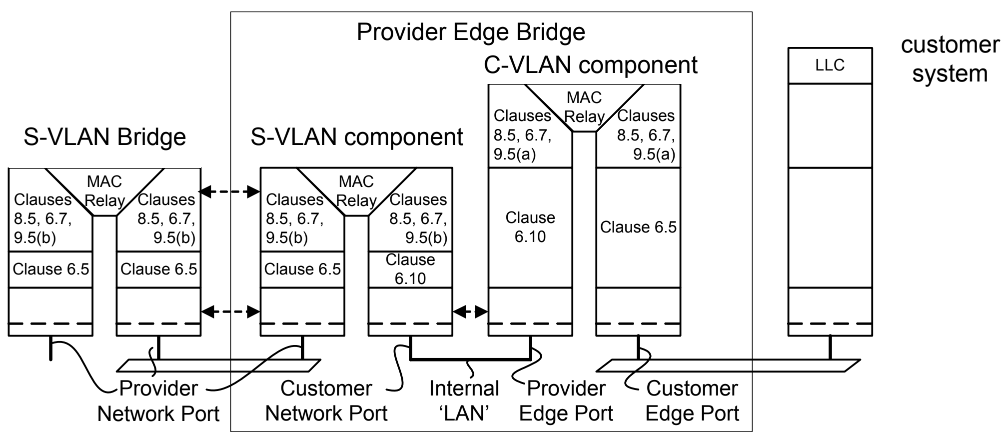

Figure 15-4—C-tagged service interface to a Provider Bridged Network

The C-tagged service interface allows service instance selection and identification by C-VID. Each frame from the customer system is assigned to a C-VLAN and presented at zero or one internal Port-based service interfaces, each supporting a single service instance that the customer desires to carry that C-VLAN.

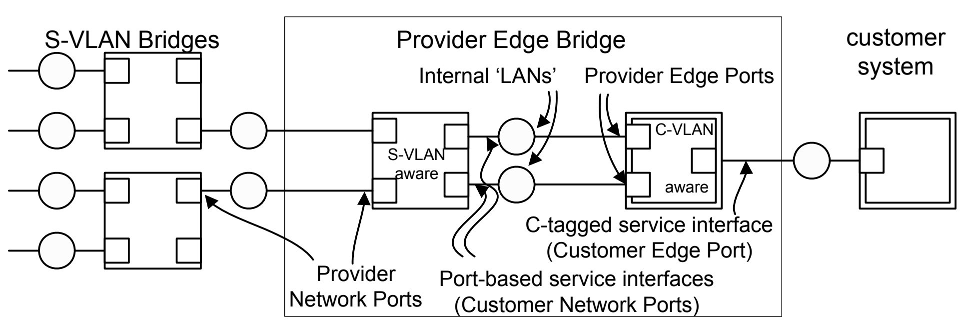

Figure 15-5—C-tagged service interface to a Provider Bridged Network

NOTE—The restriction that each C-VLAN map to a single service instance allows the customer equipment receiving frames to correctly identify the service instance used, supports mechanisms that guard against accidental creation of data loops, and prevents configuration of the C-VLAN component to create a multi-point service from point-to-point service instances. The service provider can offer a multi-point service through appropriate configuration of the S-VLAN component.

Similarly frames from the provider network are assigned to an internal interface or "LAN" on the basis of the S-VID. As each internal interface supports a single service instance, the S-TAG can be, and is, removed at this interface. If multiple C-VLANs are supported by this service instance, the frames will have C-TAGs with the possible exception of frames for a single C-VID. The C-VLAN component applies a PVID to untagged frames received on each internal "LAN," allowing full control over the delivery of frames for each C-VLAN through the Customer Edge Port.

Each Provider Edge Bridge can support multiple Customer Edge Ports for the same customer or for multiple customers. Each Customer Edge Port is supported by a dedicated C-VLAN component as illustrated in Figure 15-6.

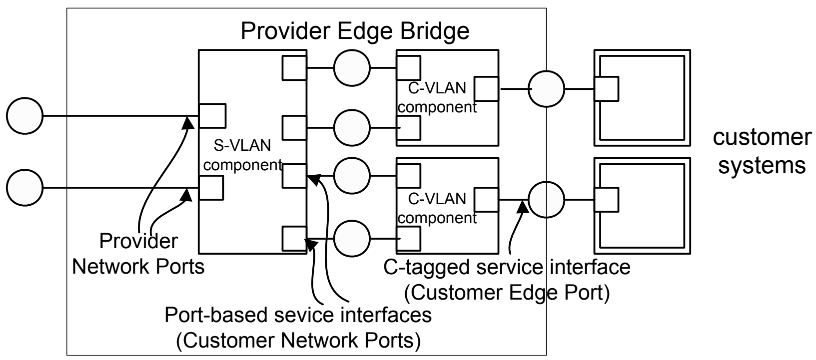

Figure 15-6—Customer Edge Ports

15.5 S-tagged service interface

An S-tagged service interface can be provided to an S-VLAN Bridge operated by a customer as illustrated by Figure 15-7 and Figure 15-8, or to a customer-operated Provider Edge Bridge that in turn provides C-tagged service interfaces within the customer's own network as described in 15.4.

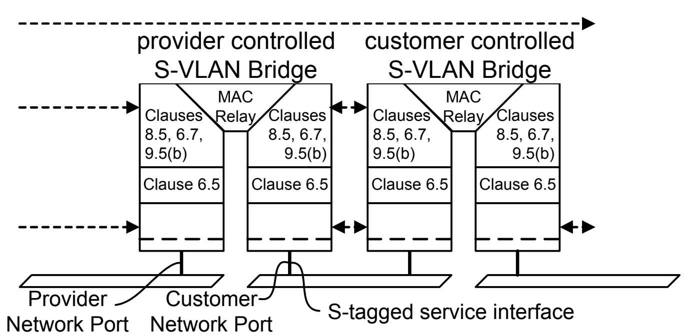

Figure 15-7—S-tagged service interface to a Provider Bridged Network

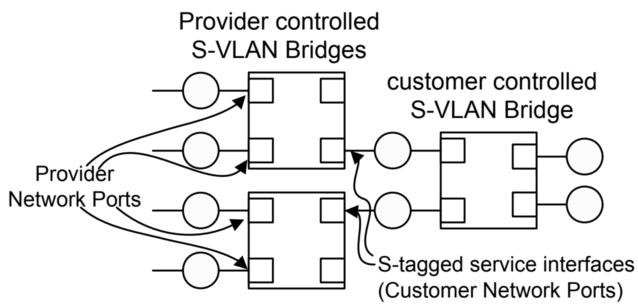

Figure 15-8—S-tagged interface to a Provider Bridged Network

15.6 Service instance segregation

Segregation of data frames associated with different MAC Service instances is achieved by supporting each service instance with a separate Service VLAN (S-VLAN) and ensuring that:

a) Provider Bridges are configured such that no customer data frames are transmitted through a Provider Network Port untagged, i.e., without a Service VLAN Tag (S-TAG).
b) No frames are accepted, i.e., received and relayed, from any customer system without first being subject to service instance selection.
c) No frames are delivered to any customer system without explicit service instance identification.
d) Prior to transmission through a Provider Network Port, customer data frames are received through a Customer Network Port within the provider network that is exclusively accessed by a single customer. The S-VIDs of all frames received through that Customer Network Port correspond to service instances that the customer is permitted to access.
e) Provider Bridges and the S-VLAN component of each Provider Edge Bridge within the provider network can only be directly controlled by the service provider. Customer equipment, including customer-owned Provider Bridges, are not within the provider network and are controlled by the customer.
f) Only frames that have been transmitted through a Provider Network Port can be received through other Provider Network Ports within the provider network.

15.7 Service instance selection and identification

Service instance selection is provided for Port-based service interfaces by configuring a Customer Network Port with a PVID value corresponding to the S-VID used to identify the service instance and an Acceptable Frame Types value of *Admit Only Untagged and Priority-tagged frames*.

Service instance selection is provided for C-tagged service interfaces by a C-VLAN component internal to a Provider Edge Bridge. The C-VLAN component uses the C-VID to direct frames to an internal Provider Edge Port supporting a specific service instance. Frames for at most one C-VLAN can be conveyed untagged over a single service instance. Management control of associating C-VIDs with Provider Edge Ports is accomplished using the C-VID Registration Table (12.13.3), which provides equivalent functionality to configuring the PVID of the internal Customer Network Port with the S-VID of the service instance, and adding the Provider Edge Port to the Member Set, and possibly Untagged Set, of the C-VLAN. No management control is provided for Protocol-based VID assignment on internal Customer Network Ports.

NOTE 1—A Provider Edge Bridge can configure the C-VLAN component associated with a Customer Edge Port to select the same service instance for all frames. This creates a service interface similar, but not identical, to a Port-based service interface. The C-VLAN component allows modification of the C-TAG (insertion of a C-TAG with the PVID value in untagged frames, assigning the PVID value to priority-tagged frames, or stripping the C-TAG from frames forwarded through the Provider Edge Port) but never forwards a frame with a null C-VID. A Port-based service interface does not modify the C-TAG of received frames in any way. A Provider Edge Bridge may offer a Port-based service interface by configuring the Port to be a Customer Network Port rather than a Customer Edge Port; in which case, there is no associated C-VLAN component.

Service instance selection is provided by the attached customer system for S-tagged service interfaces. The Customer Network Port is configured with Enable Ingress Filtering (8.6.2), and the Port is only included in the Member Set for S-VLANs corresponding to service instances that the customer is permitted to use.

For all service interfaces described, the Customer Network Port determines the S-VID for each customer data frame as specified in 6.7.1 for an EISS instance using a Service VLAN Tag type.

The VID Translation Table for the Port (6.7.1) allows a service provider to assign S-VIDs independently from those used by a customer (or other service provider) to identify service instances on an S-tagged service interface (15.5). The table also allows customers to identify the same service instance by different VIDs at different interfaces.

NOTE 2—The means used by a service provider and a customer to determine the VIDs used by the customer to select and identify a given service instance are outside the scope of this standard.

The service instance for each frame received by the attached customer system is identified in the same way as frames transmitted using the same interface, but not necessarily in the same way that the service instance is selected or identified at other interfaces. A single service instance can support Port-based, C-tagged, and S-tagged service interfaces.

15.8 Service priority selection

For all service interface types, the service priority is selected using the received priority for each frame, possible regenerated using the Priority Regeneration Table (6.7.4). The mechanism for determining the received priority varies with the type of service interface.

Service priority selection is provided for Port-based service interfaces using the received priority signaled from the media access method of the port. If the media access method used to attach to the interface does not directly support priority, this will result in the selection of a single value for all frames. A customer system may also signal priority to a Port-based service interface on a per-frame basis by priority-tagging each frame with an S-TAG with a null VID. Subclause 6.9 specifies a function to support priority-tagging with an S-TAG on Customer Bridges.

Service priority selection is provided by C-tagged service interfaces using the priority conveyed in the C-TAG of each frame. A C-tagged service interface can provide a single service instance for all C-VIDs received and in this way function much as a Port-based service interface with the addition of the capability of the customer to independently signal priority with each frame.

Service priority selection is provided by S-tagged interfaces using the received priority decoded from the PCP field in the S-TAG.

15.9 Service access protection

A customer system or systems at a single location can attach to two or more service interfaces using separate LANs for attachment, thus providing fault tolerance through redundancy of the interface components.

Insert the following new clause after Clause 15.

16. Principles of Provider Bridged Network operation

This clause establishes the principles and a model of Provider Bridged Network operation. It provides the context necessary to understand how the

a) Operation of individual Provider Bridges (Clause 8),
b) Configuration and management of individual Provider Bridges (Clause 12), and
c) Management of Spanning Tree and VLAN Topologies within a provider network (Clause 7, Clause 11, Clause 13)

support, preserve, and maintain the quality of each instance of the MAC Service offered to the customers of the provider network (Clause 6, Clause 15), including

d) Independence of each service instance supported by a service provider from other service instances (Clause 15);
e) Identification of service instances within the provider network (Clause 15, 8.8);
f) Maintenance of service availability in the event of the failure, restoration, removal, or insertion of LAN components connecting a customer network to a provider network (Clause 6, Clause 11, Clause 13, 16.2).

A Provider Bridged Network is a Virtual Bridged Local Area Network that comprises Provider Bridges (S-VLAN Bridges and Provider Edge Bridges) and attached LANs, under the administrative control of a single service provider. The principal elements of provider network operation are those specified in Clause 7 for Virtual Bridged Local Area Networks in general, as amended by this clause.

NOTE 1—Unless explicitly stated, the term “provider network” in this standard refers to a Provider Bridged Network. The term “Provider Bridged Network” is used exclusively to refer to networks configured and managed as specified by this clause and comprising only (a) Provider Bridges and Provider Edge Bridges and (b) communications media and equipment providing the Internal Sublayer Service (6.4). Although the requirements of Clause 15 are generally applicable to similar services, a generalized framework for all network designs that could support these requirements, while useful in the context of other equipment and services, is outside the scope of this standard. This clause describes specific best practice for Provider Bridged Networks to ensure that the requirements for bridge functionality are clear. Conformance of a Provider Bridge implementation to this standard does not require that the implementation be used as specified in this clause, merely that it is capable of being so used.

NOTE 2—Within a provider network, an instance or instances of the MAC Service are reserved for the service provider’s own use to configure and manage the network. All frames associated with such service instances, and that are not confined to an individual LAN, are subject to service instance selection, segregation, and identification as specified in 16.1.

16.1 Provider Bridged Network overview

The principal elements of Provider Bridge Network operation comprise

a) Service instance segregation within the provider network for customer frames (15.6).
b) Service instance selection on ingress, and service instance identification for on egress, for each customer frame (15.7).
c) Resource allocation and configuration to provide service instance connectivity (16.3).

and may also include

d) Management of customer end station address learning (16.4).

e) Prevention of connectivity loops formed through attached networks (16.5).

16.2 Provider Bridged Network

An example Provider Bridged Network is illustrated by Figure 16-1.

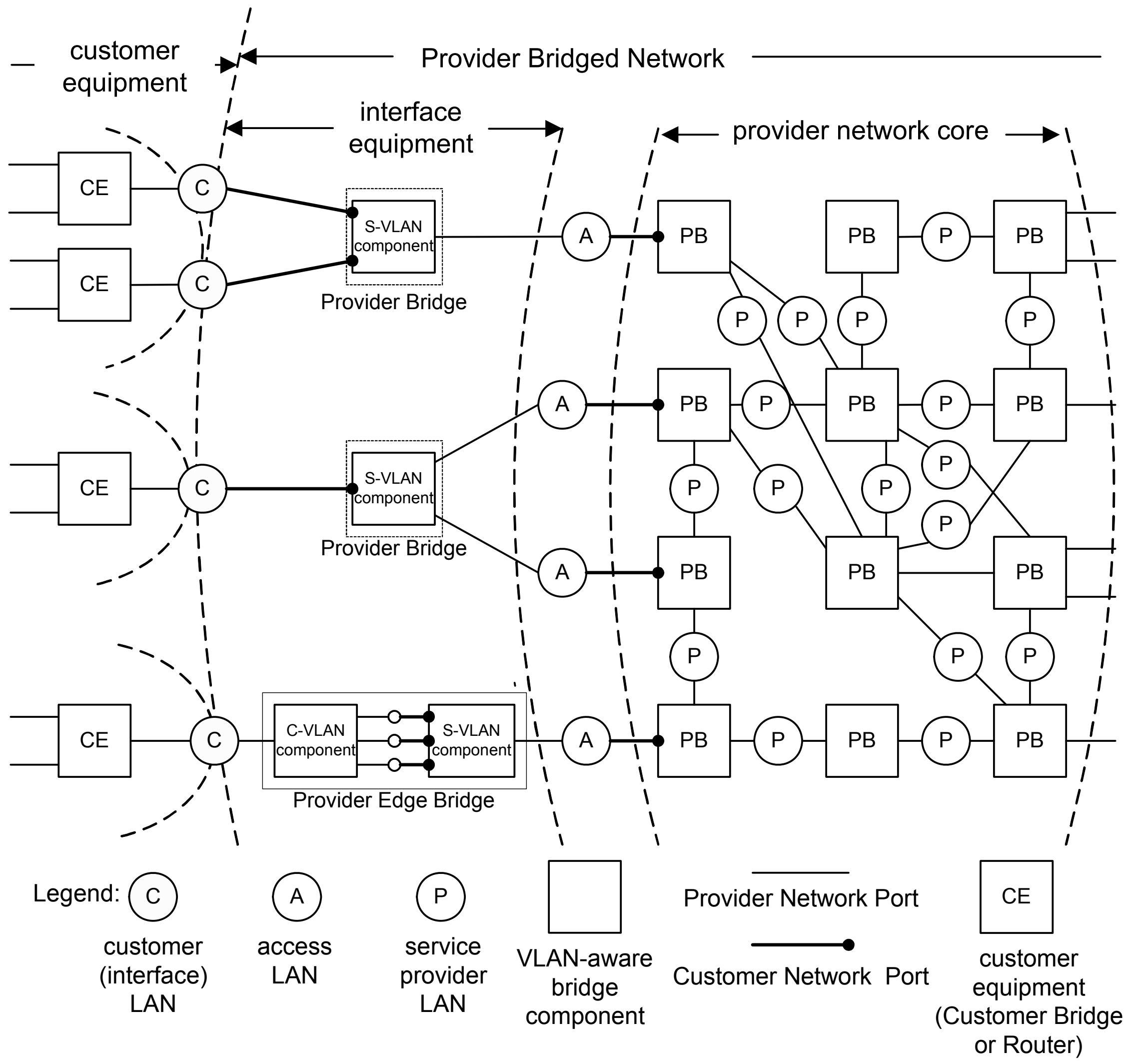

Figure 16-1—Provider Bridged Network with interface examples

Customer equipment attaches, via one or more customer interface LANs, to equipment that provides the service interfaces specified in Clause 15. That interface equipment can be located in the core of the provider network, such that both the equipment and the attached LANs are secure against direct addition of frames either by the customer or by others. More commonly the interface equipment connects to the network core using one or more access LANs, which can be subject to external interference. Figure 16-1 provides examples. Within the network core, Provider Bridges and LANs are secured so that only the service provider can manage the reception, transmission, and relay of frames between Provider Bridges.

The arbitrary physical network topology of the network core and the connectivity that it provides to support segregated instances (15.6) of the MAC Service is designed and managed (16.3) by the service provider to meet bandwidth and service availability requirements at the Provider Network Ports. Application of the Service VLAN ingress and egress rules at these Ports in support of service instance selection and identification (15.7) ensures that frames cannot be transmitted or received on any service instance by any customer's equipment without prior agreement with the service provider.

Although the application of the ingress and egress rules, together with the use of the MSTP restrictedRole and restrictedTcn (13.25.15, 13.25.16) parameters and GVRP registration controls (16.3), permit service providers to allow direct attachment of customer-operated equipment to access LANs, there are commonly other reasons, such as OAM&P support of access LANs, why interface equipment is mandated. The interface equipment, as illustrated by, but not limited to, the examples in Figure 16-1 can be used to partition and enhance network access functionality to provide

a) Service instance multiplexing on a single access LAN;
b) Provision of resilient, and optionally physically route diverse, access;
c) Reduced management of customer use of multiple service instances;
d) Selective multiplexing of customer VLANs onto service instances;
e) Reliable identification of the customer point of attachment;

without requiring customer systems to understand the internal details of the provider network.

Provider Bridge A in Figure 16-1 uses physically separate customer interface LANs to provide separate Port-based service interfaces to the customer equipment and uses Service VLAN tags to multiplex the corresponding service instances over a single access LAN. The interface equipment can be managed by the service provider to use S-VIDs that do not require use of a VID Translation Table at the edge of the core network. Alternatively, the latter can translate S-VIDs to remove the need for such management, with all interface equipment using the same S-VIDs in the same way.

Provider Bridge B in Figure 16-1 uses a single customer interface LAN to provide a Port-based service interface to the customer equipment and uses two access LANs to provide resilient connectivity to distinct Provider Bridges in the core network. Receipt of Provider Bridge BPDUs by Bridge B protects against the failure of an access LAN, of one of the core bridges, or of some internal physical connectivity within the provider network. Use of the MSTP restrictedRole and restrictedTcn parameters by Provider Network Ports ensures that receipt of frames from the access LANs cannot disrupt the active topology or address learning within the core network. Where multiple service instances are provided at a single customer point of attachment, both access links can be used.

Provider Edge Bridge C in Figure 16-1 provides a C-tagged service interface to the customer equipment and uses Customer VLAN tags on the customer interface LAN to select between multiple Service VLAN tagged service instances on the access LAN. Individual Customer VLANs can be conveyed on any service instance, and this distribution of Customer VLANs can be changed in response to changes in the connectivity offered by the service instances through customer systems at other points of customer attachment. The traffic for a particular Customer VLAN can be the majority of that carried on a specific service instance; specifying that frames for that Customer VLAN are untagged on the internal LAN that corresponds to that service instance within the Provider Edge Bridge allows those frames to be carried through the provider network without a C-VID following the S-VID if the overhead of conveying the additional octets is a concern.

16.3 Service instance connectivity

The VLAN Topology of each S-VLAN is established by the mechanisms introduced in 7.1 and Figure 7-1. The service provider can use and configure MSTP to provide a number of independent spanning tree active topologies and can assign each S-VLAN independently to one of these to best use the resources in the network. GVRP running in the context of each spanning tree active topology configures the extent of each S-VLAN to the subset of that active topology necessary to support connectivity between the customer points of attachment to the MAC Service instance provided, and it can reconfigure that connectivity as required if the spanning tree active topology changes.

NOTE 1—Autoconfiguration of the extent of each S-VLAN is accomplished by the service provider configuring the GARP Administrative Control “Registration Fixed” for the S-VLAN on each Customer Network Port where the corresponding MAC Service Instance can be selected. The Enable Ingress Filtering parameter is not typically used within an individual provider network, as it limits the ability of the network to carry service instances following changes in the active topology. However, it can be used to limit the reachability of service instances used by the service provider for network management and to restrict service instances carried from one provider network domain to another

The operation of MSTP within a provider network is independent of the operation of any spanning tree protocol within attached customer networks. This independence is achieved by using the Provider Bridge Group Address (Table 8-1) as the destination address of all MSTP BPDUs transmitted on all Provider Bridge Ports and by setting the restrictedRole and restrictedTcn parameters (13.25.15, 13.25.16) for Customer Network Ports. Frames received by Customer Network Ports and addressed to the Bridge Group Address are subject to service instance selection and relay in the same way as customer data frames.

NOTE 2—Customer BPDUs addressed to the Bridge Group Address are conveyed transparently, allowing the customer to use an instance of MSTP or RSTP that is completely independent of the provider network to establish and maintain full and loop-free connectivity of the customer connected networks and services. A customer can also use GVRP to limit the transmission of frames assigned to C-VLANs to the service instances required for C-VLAN connectivity.

The operation of GVRP within a provider network is independent of the operation of any configuration protocol within attached customer networks. The S-VLAN GVRP Address (Table 8-1) is used as the destination address of all GARP PDUs transmitted in support of the GVRP Application. Frames received by Customer Network Ports and addressed to the GARP Address (Table 12-1 of IEEE Std. 802.1D) are subject to service instance selection and relay in the same way as customer data frames. The GARP Administrative Control for each S-VLAN is either “Registration Fixed” or “Registration Forbidden” on all Customer Network Ports, so no information is received from any Provider Bridge GVRP PDU that has been erroneously transmitted by a customer system.

16.4 Service provider learning of customer end station addresses

Customer data frames for any given MAC Service instance are restricted to that part of the provider network that supports the VLAN topology of the associated S-VLAN as described in 16.3 and are further restricted by learning the source addresses of frames as described in Clause 7 and Clause 8.

In a Provider Bridged Network that commonly provides interfaces to each customer at a small fraction of the total number of customer interfaces provided, the requirement for learning customer end station addresses can be much reduced by applying enhanced filtering utility criteria (8.7). In particular, learning can be restricted to the ingress and egress Provider Bridge Ports of each S-VLAN that connects only two customer points of attachment, or to the customer systems attached to those Ports.

16.5 Detection of connectivity loops through attached networks

The transmission and reception of MSTP BPDUs through Customer Network Ports will detect accidental direct connection of those ports, or their interconnection by a network that is transparent to frames with the Provider Bridge Group Address as the destination MAC address. However, a service provider cannot rely on any customer network relaying such frames and should develop a policy and mechanisms to deal with potential data loops that can arise if the attached customer systems do not correctly operate their own instance or instances of a spanning tree protocol.

NOTE 1—Use of the restrictedRole parameter at ingress ports ensures that receipt of BPDUs addressed to the Provider Bridge Group Address cannot disrupt internal connectivity within the provider network.

NOTE 2—Specification of service provider policies, mechanisms, and heuristics used to detect or minimize the impact of data loops created by customer systems is not addressed by this standard. They can include, but are not limited to, bandwidth limitation, charging policies, detection of the repetitive movement of the apparent location of customer stations, and customer agreement to allow the use of service provider loop detection protocols by not filtering the associated frames.

NOTE 3—A data loop is not the only possible cause of excess bandwidth consumption by a given customer of a provider network, and the service provider is usually required to meet service guarantees to other customers irrespective of the cause of the excess bandwidth demand. Data loops are not a unique threat to satisfactory overall network performance. Their distinct characteristic is consumption of discretionary bandwidth without benefitting any customer. The customer that creates the loop can suffer particularly serious network degradation or excess cost as the service provider limits the total bandwidth consumed by that customer. It is, therefore, in the interests of each customer and the service provider to raise service satisfaction by preventing and detecting loops.

Each C-VLAN component within a Provider Edge Bridge implements RSTP, with the enhancements to support loop-free connectivity between Customer Edge Ports, as specified in 13.38, thus interoperating with customer equipment and spanning tree configurations to support reliable and deterministic prevention of loops, and supporting provision of redundant connectivity.

16.6 Network management

Management of a Provider Bridge is directly under the control of the service provider. Provider network customers shall not have access to managed objects related to elements of Provider Bridges within the provider network.

Annex A

(normative)

PICS proforma

A.5 Major capabilities

Insert the following items at the end of A.5:

Item	Feature	Status	References	Support
CB	Can the Bridge be configured to operate as a C-VLAN Bridge, recognizing and using C-TAGs?	O.2	5.7	Yes [ ]
PB	Can the Bridge be configured to operate as a Provider Bridge, recognizing and using S-TAGs?	O.2	5.8	Yes [ ]
PEB	Can the Bridge be configured to operate as a Provider Edge Bridge with one or more Ports operating as a Customer Edge Ports?	PB:O	5.8.2	Yes [ ]
PB-2	State which Ports support the following values for the Provider Bridge Port Type: — Provider Network Port; — Customer Network Port; — Customer Edge Port.	PB:M	5.8	 Ports: _____ Ports: _____ Ports: _____

A.9 Addressing

Change items in A.9 as follows:

Item	Feature	Status	References	Support
ADDR-1	Does each Port have a separate MAC Address?	M	8.13.2	Yes [ ]
ADDR-2	Are frames addressed to a MAC Address for a Port and received from or relayed to the attached LAN submitted to LLC Service User for the destination LLC Address?	M	8.5, 8.13.1	Yes [ ]
ADDR-3	Are all BPDUs and GARP PDUs transmitted using the Bridge Spanning Tree Protocol LLC Address?	M	8.13.3, Table 8-8	Yes [ ]
ADDR-4	Are PDUs addressed to the Bridge Spanning Tree Protocol Address with an unknown Protocol Identifier discarded on receipt?	M	{D}9.3.4	Yes [ ]
ADDR-5	Are all BPDUs generated by a Spanning Tree Protocol Entity associated with a C-VLAN component transmitted to the Bridge Group Address?	CB OR PEB:M	8.13.3, Table 8-1, Table 8-2	Yes [ ] N/A [ ]
ADDR-6	Are all BPDUs generated by a Spanning Tree Protocol Entity associated with an S-VLAN component transmitted to the Provider Bridge Group Address?	PB:M	Table 8-1	Yes [ ] N/A [ ]
ADDR-~~6~~7	Are all GARP PDUs transmitted to the Group Address assigned for the GARP Application?	M	8.13.3, {D}Table 12-1, Table 8-1	Yes [ ]
ADDR-~~7~~8	Is it possible to create entries in the Permanent or Filtering Databases for unsupported GARP application addresses or delete or modify entries for supported application addresses?	X	8.13.3	No [ ]
ADDR-~~8~~9	Is the source MAC address of BPDUs and GARP PDUs for GARP Applications supported by the Bridge the address of the transmitting Port?	M	8.13.3	Yes [ ]
ADDR-10	Is the source MAC address of BPDUs generated by a Spanning Tree Entity associated with a C-VLAN component of a Provider Edge Bridge the address of the associated Customer Edge Port?	PEB:M	12.13	Yes [ ] N/A [ ]
ADDR-~~9~~11	Is Bridge Management accessible through a Port using the MAC Address of the Port?	MGT:O	8.13.7	Yes [ ] No [ ]

A.9 Addressing *(continued)*

Change items in A.9 as follows:

Item	Feature	Status	References	Support
ADDR-~~10~~12	Is a 48-bit Universally Administered MAC Address assigned to each Bridge as its Bridge Address?	M	8.13.8	Yes [ ]
ADDR-~~11~~13	Is the Bridge Address the Address of a Port?	O	8.13.8	Yes [ ] No [ ]
ADDR-~~12~~14	Is the Bridge Address the Address of Port 1?	ADDR-~~11~~13: O	8.13.3	Yes [ ] No [ ]
ADDR-~~13~~15	Are frames addressed to any of the C-VLAN component Reserved Addresses relayed by the Bridge a C-VLAN component?	CB OR PEB:X	8.13.4 Table 8-1	No [ ] N/A [ ]
ADDR-16	Are frames addressed to any of the S-VLAN component Reserved Addresses relayed by an S-VLAN component?	PB:X	Table 8-2	No [ ] N/A [ ]
ADDR-~~14~~17	Is it possible to delete or modify entries in the Permanent and Filtering Databases for the Reserved Addresses?	X	8.13.4, {D}7.12.6	No [ ]

A.10 Rapid Spanning Tree Protocol

Insert the following item at the end of A.10:

Item	Feature	Status	References	Support
RSTP-21	Does each C-VLAN component of a Provider Edge Bridge operate an instance of Rapid Spanning Tree as modified for Customer Edge Ports?	RSTP AND PEB:M	13.38	Yes [ ]

A.14 Bridge management

Insert the following items to A.14, renumbering the items currently labled MGT-15 through MGT-71 as appropriate:

Item	Feature	Status	References	Support
MGT-15	Read Port Priority Code Point Selection	MGT and VLAN-29:M	12.6.2.6	Yes [ ] N/A [ ]
MGT-16	Set Port Priority Code Point Selection	MGT AND VLAN-29:M	12.6.2.7	Yes [ ] N/A [ ]
MGT-17	Read Priority Code Point Decoding Table	MGT AND VLAN-29:M	12.6.2.8	Yes [ ] N/A [ ]
MGT-18	Set Priority Code Point Decoding Table	MGT AND VLAN-29:O	12.6.2.9	Yes [ ] No [ ] N/A [ ]
MGT-19	Read Priority Code Point Encoding Table	MGT AND VLAN-29:M	12.6.2.10	Yes [ ] N/A [ ]
MGT-20	Set Priority Code Point Encoding Table	MGT AND VLAN-29:O	12.6.2.11	Yes [ ] No [ ] N/A [ ]
MGT-21	Read Use_DEI parameter	MGT AND PB:M	12.6.2.12	Yes [ ] N/A [ ]
MGT-22	Set Use_DEI parameter	MGT AND PB:O	12.6.2.13	Yes [ ] No [ ] N/A [ ]
MGT-23	Read Require Drop Encoding parameter	MGT AND VLAN-29:M	12.6.2.14	Yes [ ] N/A [ ]
MGT-24	Set Require Drop Encoding parameter	MGT AND VLAN-29:M	12.6.2.15	Yes [ ] N/A [ ]
MGT-25	Read Service Access Priority Selection	MGT AND VLAN-30:M	12.6.2.16	Yes [ ] N/A [ ]
MGT-26	Set Service Access Priority Selection	MGT AND VLAN-30:M	12.6.2.17	Yes [ ] No [ ] N/A [ ]
MGT-27	Read Service Access Priority Table	MGT AND VLAN-30:M	12.6.2.18	Yes [ ] N/A [ ]
MGT-28	Set Service Access Priority Table	MGT AND VLAN-30:O	12.6.2.19	Yes [ ] No [ ] N/A [ ]
MGT-86	Read Provider Bridge Port Type	MGT AND PB:M	12.13.1.1	Yes [ ] N/A [ ]
MGT-87	Configure Provider Bridge Port Type	MGT AND PB:O	12.13.1.2	Yes [ ] No [ ] N/A [ ]
MGT-88	Read VID Translation Table Entry	MGT AND VLAN-31:M	12.13.2.1	Yes [ ] N/A [ ]
MGT-89	Configure VID Translation Table Entry	MGT AND VLAN-31:M	12.13.2.2	Yes [ ] N/A [ ]
MGT-90	Read C-VID Registration Table Entry	MGT AND PEB:M	12.13.3.1	Yes [ ] N/A [ ]

A.14 Bridge management *(continued)*

Insert the following items to A.14, renumbering the items currently labled MGT-15 through MGT-71 as appropriate:

Item	Feature	Status	References	Support
MGT-91	Configure C-VID Registration Table Entry	MGT AND PEB:M	12.13.3.2	Yes [ ] N/A [ ]
MGT-92	Read Provider Edge Port Configuration	MGT AND PEB:M	12.13.3.3	Yes [ ] N/A [ ]
MGT-93	Set Provider Edge Port Configuration	MGT AND PEB:M	12.13.3.4	Yes [ ] N/A [ ]
MGT-94	Read Service Priority Regeneration Table	MGT AND PEB:M	12.13.3.5	Yes [ ] N/A [ ]
MGT-95	Set Service Priority Regeneration Table	MGT AND PEB:O	12.13.3.6	Yes [ ] No [ ] N/A [ ]

A.21 VLAN support

Insert/change the following items in A.21, renumbering the items currently labled VLAN-2 through VLAN-27 as appropriate:

Item	Feature	Status	References	Support
VLAN-1	Does the implementation support, on each Port, one or more of the permissible combinations of values for the Acceptable Frame Types parameter?	M	5.3	Yes [ ]
VLAN-2	Does the implementation support, on each Provider Bridge Port, the *Admit All Frames* value for the Acceptable Frame Types Parameter?	PB:M	5.6	Yes [ ] N/A [ ]
VLAN-~~9~~10	Does the implementation support the ability to enable and disable Ingress Filtering?	CB:O PB:M	5.4.1, 5.6, 8.4	Yes [ ] No [ ] N/A [ ]
VLAN-29	Is encoding of the drop_eligible parameter in the Priority Code Point field of the VLAN tag supported?	CB:O PB:M	5.5.1, 5.6, 6.7.3, 9.6, 9.7	Yes [ ] No [ ] N/A [ ]
VLAN-30	Is Service Access Priority Selection supported?	CB:O PB:X	5.5.1, 5.6, 6.9	Yes [ ] No [ ] N/A [ ]
VLAN-31	Is the VID translation table supported?	CB:X PB:M	5.5, 5.6.1, 6.7	Yes [ ] No [ ] N/A [ ]

Annex G

(informative)

Priority and drop precedence

Change the first two paragraphs as follows:

This standard allows management of priorities, flow metering, queue assignment, and queue servicing ~~service disciplines to be managed to best support the goals of network administrators~~. This annex documents the rationale for the recommended and default priority to traffic class mappings in Table 8-3 and the encoding of priority and drop eligibility in Table 6-3 and Table 6-4.

Classification of user data frames into a small number of behavior aggregates, together with aggregate dependent forwarding behavior in each Bridge, allows signaling of application requirements to the network. Frame classification, aggregate bandwidth metering, ~~and~~ policing, and drop precedence marking also facilitate network scaling and provision of services to independent customers through allocation of those functions to appropriate bridges in the network.

G.4 Traffic types and priority values

Modify the last paragraph of G.4 as follows:

The priority to traffic class mappings in Table 8-3 differs in one minor respect from those specified in prior revisions of this standard and in IEEE Std 802.1D-2004 and its prior revisions. Priority value 2 was described as “Spare” and positioned lower than 0 (Best Effort) in priority order. This change may result in networks, including bridges conformant to prior revisions of this standard, and implementing four or more traffic classes, providing less-than-expected priority to traffic described in this annex as Excellent Effort, and misordering drop eligible traffic for Critical Applications. The change allows better use of the available traffic classes given the low demand for two distinct priorities of lesser importance than Best Effort and the best use of the PCP when encoding drop eligibility.

Insert the following subclauses after G.4

G.5 Supporting drop precedence

It is often desirable to meter traffic from different users to ensure fairness or to meet bandwidth guarantees; however, dropping all traffic in excess of a committed rate is likely to result in severe under-utilization of the networks, because most traffic sources are bursty in nature. At the same time, it is burdensome to meter traffic at all points in the network where bandwidth contention occurs. One solution is to mark those frames in excess of the committed rate as drop eligible on admission to the network.

This standard allows drop eligibility to be conveyed separately from priority in Service VLAN tags (S-TAGs) so that all previously introduced traffic types can be marked as drop eligible. To provide compatibility with previous revisions of this standard while allowing drop eligibility to be conveyed in Customer VLAN tags (C-TAGs), this standard also allows a subset of the priorities to be conveyed along with drop eligibility marking for some of those priorities within the Priority Code Point (PCP) field of both S-TAGs and C-TAGs.

G.6 Priority code point allocation

The Priority Code Point of VLAN tags allows encoding of five, six, seven, or eight distinct priorities, with a single level of drop eligibility on three, two, one, or zero of those priorities, respectively. Table 6-3 and Table 6-4 specify encoding and decoding for five through eight priorities. The tables are consistent with the following step-by-step reduction in the number of distinct priorities to provide drop eligibility for certain traffic types:

a) If eight distinct priorities are required, drop eligibility cannot be encoded in the PCP (but may be encoded in S-TAGs using the DEI).
b) Drop eligibility in support of QoS maintenance for traffic conforming to a committed rate is most effective when used to support time-critical traffic. If seven priorities, one of which can be marked as drop eligible, are required, then the traffic class queuing distinction between Voice and Video is sacrificed to providing drop eligibility for the combined traffic types. This does not preclude marking all Video traffic as drop eligible upon ingress to a network, so as to provide the same guarantee to Voice as a distinct priority.
c) The distinctions between Critical Applications and Excellent Effort, and between Best Effort and Background traffic types, is removed to provide drop eligibility for Critical Applications and for Best Effort.
d) Although the use of four priorities, each with drop eligibility, is possible, it is not recommended. Combining Network Control with Internetwork Control could only serve to increase the guarantees provided to the latter at the expense of the former, which if not delivered threatens the stability of the overall network in any case. Moreover, both traffic types should be supportable with guaranteed bandwidth if the network is to be operated successfully.

Choosing first to combine Video and Voice, and then Critical Applications with Excellent Effort (for six queues), provides consistency with the allocation of priorities to traffic classes in the absence of drop eligibility. Bridges that do not implement drop eligibility, but are configured to use the same number or fewer traffic classes, will not misorder frames. If such a bridge is configured to use only five traffic classes, and in accordance with Table 8-3, it will not misorder frames with a priority code point encoded using any of the alternatives provided by Table 6-3.

G.7 Interoperability

Encoding of drop eligibility within the PCP, as opposed to explicitly with the DEI in the S-TAG, provides interoperability with bridges are not capable of supporting the DEI in the S-TAG. It also provides compatibility with the use of the MPLS EXP bits to convey priority and drop eligibility.

However, the requirement to provide different combinations of priorities with drop eligibility within the confines of the PCP means that priority and drop eligibility information can be lost for frames traversing a network if the combinations used on individual LANs differ. Use of the DEI does not suffer from this problem. In some cases, loss of drop eligibility information at the boundary between administrative domains risks impacting profile conformant traffic from some users with out-of-profile drop eligible traffic from others; in other cases, the drop eligible marking has already done its job (the next LAN, for example, might deliver traffic to a single customer). Without explicit management, a Bridge Port cannot decide, so the Require Drop Encoding parameter (8.6.7) has been provided.

If bridges attached to the same LAN encode and decode the PCP differently, then incorrect priority values can be attributed and subsequent misordering of frames can occur. Misordering will not occur, with the recommended priority to traffic class mappings of Table 8-3 and the recommended PCP encoding and decoding in Table 6-3 and Table 6-4, if the Bridge performing the incorrect decoding assumes fewer priorities than are actually encoded or if all bridges subsequently transited by the frame use the same number or fewer traffic classes than those used for the encoding. However, incorrect decoding will in all probability affect other service guarantees that the network is intended to support. If a Bridge can be used in a network that encodes drop eligibility in the PCP, and there is any likelihood of the Bridge being brought into service prior to the network dependent service level configuration, then five priorities, three with drop eligibility (5P3D encoding and decoding), should be used. Bridges that do not support drop precedence should be configured to support five or fewer traffic classes in the same circumstances.

The use of separate Priority Code Point Encoding and Priority Code Point Decoding Tables for each Bridge Port allows adaptation between the encoding scheme in one domain of the network and the encoding scheme used in another to be accomplished in only one of any pair of bridges, each serving as a boundary of its domain, connected by a point-to-point LAN. However, if more than two bridges are attached to a LAN, all need to use the same encoding so that each of its recipients can assign the correct priority to the frame.

The default PCP encoding and decoding, as documented in Table 6-3 and Table 6-4, are reproduced in Table G-4 and Table G-5, with the addition of the default allocation of priorities to traffic classes to the latter.

NOTE—The sequence of the columns for the priority values of 0 and 1 in Table G-4 and Table G-5 are reversed from the sequence in Table 6-3 and Table 6-4 in order to show the alignment with the traffic classes in Table G-3.

Table G-4—Priority Code Point encoding

priority drop_eligible		7	7DE	6	6DE	5	5DE	4	4DE	3	3DE	2	2DE	0	0DE	1	1DE
PCP	8P0D	7	7	6	6	5	5	4	4	3	3	2	2	0	0	1	1
	7P1D	7	7	6	6	5	4	5	4	3	3	2	2	0	0	1	1
	6P2D	7	7	6	6	5	4	5	4	3	2	3	2	0	0	1	1
	5P3D	7	7	6	6	5	4	5	4	3	2	3	2	1	0	1	0

Table G-5—Priority Code Point decoding

<table>
<tr><th colspan="2">PCP</th><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>0</td><td>1</td></tr>
<tr><th rowspan="4">priority drop eligible</th><td>8P0D</td><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>0</td><td>1</td></tr>
<tr><td>7P1D</td><td>7</td><td>6</td><td>4</td><td>4DE</td><td>3</td><td>2</td><td>0</td><td>1</td></tr>
<tr><td>6P2D</td><td>7</td><td>6</td><td>4</td><td>4DE</td><td>2</td><td>2DE</td><td>0</td><td>1</td></tr>
<tr><td>5P3D</td><td>7</td><td>6</td><td>4</td><td>4DE</td><td>2</td><td>2DE</td><td>0DE</td><td>0</td></tr>
<tr><th rowspan="8">number of traffic classes</th><td>1</td><td colspan="8">BE</td></tr>
<tr><td>2</td><td colspan="4">VO</td><td colspan="4">BE</td></tr>
<tr><td>3</td><td colspan="2">NC</td><td colspan="2">VO</td><td colspan="4">BE</td></tr>
<tr><td>4</td><td colspan="2">NC</td><td colspan="2">VO</td><td colspan="2">CA</td><td colspan="2">BE</td></tr>
<tr><td>5</td><td>NC</td><td>IC</td><td colspan="2">VO</td><td colspan="2">CA</td><td colspan="2">BE</td></tr>
<tr><td>6</td><td>NC</td><td>IC</td><td colspan="2">VO</td><td colspan="2">CA</td><td>BE</td><td>BK</td></tr>
<tr><td>7</td><td>NC</td><td>IC</td><td colspan="2">VO</td><td>CA</td><td>EE</td><td>BE</td><td>BK</td></tr>
<tr><td>8</td><td>NC</td><td>IC</td><td>VO</td><td>VI</td><td>CA</td><td>EE</td><td>BE</td><td>BK</td></tr>
</table>

Annex H

(informative)

Bibliography

Insert the following bibliographic citations in numerical order:

[B19] ITU-T G.8010-2004, Series G: Transmission systems and media, digital systems and networks digital networks—General aspects.[3]

[B20] ITU-T G.8011-2004, Ethernet over Transport—Ethernet services framework digital network—General aspects.

[B21] ITU-T G.8011.1-2004, Ethernet private line service digital networks—General aspects.

[B22] ITU-T G.8012-2004, Ethernet UNI and Ethernet NNI Series G: Transmission systems and media, digital systems and network digital networks—General aspects.

[B23] ITU-T G.8021-2004, Characteristics of Ethernet transport network equipment functional blocks Series G: Transmission systems and media, digital systems and network digital networks—General aspects.

[3]ITU-T publications are available from the International Telecommunications Union, Place des Nations, CH-1211, Geneva 20, Switzerland/Suisse (http://www.itu.int/).

