



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

**Virtual Bridged Local Area Networks
Amendment 10: Provider Backbone
Bridge Traffic Engineering**

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997, USA
5 August 2009

IEEE Std 802.1Qay™-2009
(Amendment to
IEEE Std 802.1Q™-2005)

IEEE Std 802.1Qay™-2009

(Amendment to
IEEE Std 802.1Q™-2005)

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

Virtual Bridged Local Area Networks

**Amendment 10: Provider Backbone
Bridge Traffic Engineering**

Sponsor

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

Approved 17 June 2009

IEEE-SA Standards Board

Abstract: This amendment supports provisioning systems that explicitly select traffic engineered paths within Provider Backbone Bridged Networks.

Keywords: Bridged Local Area Networks, Connectivity Fault Management, LANs, local area networks, metropolitan area networks, MAC Bridges, MANs, Multiple Registration Protocol (MRP), Multiple Spanning Tree Protocol (MSTP), Multiple VLAN Registration Protocol (MVRP), Provider Backbone Bridge, Provider Bridged Local Area Networks, Traffic Engineering, virtual LANs, Virtual Bridged Local Area Networks

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

Copyright © 2009 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 5 August 2009. Printed in the United States of America.

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

PDF: ISBN 978-0-7381-5992-8 STD95941
Print: ISBN 978-0-7381-5993-5 STDPD95941

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

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

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

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

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

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

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE. Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required.

Comments and recommendations on standards, and requests for interpretations should be addressed to:

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

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

Introduction

This introduction is not part of IEEE Std 802.1Qay-2009, IEEE Standards for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 10: Provider Backbone Bridge Traffic Engineering.

Notice to users

Laws and regulations

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

Copyrights

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

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association website at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA website at <http://standards.ieee.org>.

Errata

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

Interpretations

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

Patents

Attention is called to the possibility that implementation of this amendment may require use of subject matter covered by patent rights. By publication of this amendment, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this amendment are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

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

Tony Jeffree, *Chair*
Paul Congdon, *Vice Chair*
Stephen Haddock, *Chair, Interworking Task Group*
Panagiotis Saltisidis, *Editor*

Osama Aboul-Magd
Zehavit Alon
Caitlin Bestler
Jan Bialkowski
Rob Boatright
Jean-Michel Bonnamy
Paul Bottorff
Rudolf Brandner
Craig W. Carlson
Weiyang Cheng
Rao Cherukuri
Diego Crupnicoff
Claudio Desanti
Zheming Ding
Linda Dunbar
Hesham M. Elbakoury
David Elie-Dit-Cosaque
Janos Farkas
Donald Fedyk
Norman Finn
Robert Frazier
John Fuller
Geoffrey Garner
Anoop Ghanwani
Franz Goetz
Yannick Le Goff
Eric Gray
Karanvir Grewal
Craig Gunther
Mitch Gusat
Asif Hazarika
Charles Hudson

Romain Insler
Michael Johas Teener
Abhay Karandikar
Prakash Kashyap
Hal Keen
Keti Kilcrease
Yongbum Kim
Philippe Klein
Mike Ko
Vinod Kumar
Bruce Kwan
Kari Laihonon
Michael Lerer
Gael Mace
Ben Mack-Cran
David Martin
Riccardo Martinotti
Alan McGuire
James McIntosh
Menucher Menuchery
John Messenger
Matthew Mora
Eric Multanen
Kevin Nolish
Hiroshi Ohta
David Olsen
Donald Pannell
Joseph Pelissier
David Peterson
Hayim Porat
Max Pritikin
Ananda Rajagopal

Karen Randall
Gunter Roeck
Josef Roesse
Derek J. Rohde
Dan Romascanu
Moran Roth
Jessy V. Rouyer
Hyunsurk Ryu
Jonathan Sadler
Ali Sajassi
Joseph Salowey
Satish Sathe
John Sauer
Michael Seaman
Koichiro Seto
Himanshu Shah
Nurit Sprecher
Kevin B. Stanton
Robert A. Sultan
Muneyoshi Suzuki
George Swallow
Attila Takacs
Patricia Thaler
Oliver Thorp
Manoj Wadekar
Yuehua Wei
Brian Weis
Bert Wijnen
Michael D. Wright
Chien-Hsien Wu
Ken Young
Glen Zorn

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

Butch Anton	Tony Jeffree	Maximilian Riegel
Khin Mi Mi Aung	Shinkyu Kaku	Robert Robinson
Gennaro Boggia	Piotr Karocki	Benjamin Rolfe
Paul Bottorff	Stuart J. Kerry	Jessy V. Rouyer
Juan Carreon	Chad Kiger	Randall Safier
Keith Chow	Yongbum Kim	John Sauer
Thomas Dineen	Michael Lerer	Bartien Sayogo
Linda Dunbar	Li Li	Michael Seaman
Sourav Dutta	William Lumpkins	Kapil Sood
Donald Fedyk	Arthur Marris	Nurit Sprecher
C. Fitzgerald	David Martin	Thomas Starai
Robert Frazier	Alan McGuire	Walter Struppler
Yukihiro Fujimoto	Jonathon McLendon	Robert A. Sultan
Randall Groves	Gary Michel	Joseph Tardo
C. Guy	Jose Morales	William Taylor
Stephen Haddock	Michael S. Newman	Patricia Thaler
John Hawkins	Kevin Nolish	Prabodh Varshney
Atsushi Ito	Satoshi Obara	Maarten Vissers
Raj Jain	Glenn Parsons	Ken Young
		Oren Yuen

When the IEEE-SA Standards Board approved this standard on 17 June 2009, it had the following membership:

Robert M. Grow, *Chair*
Thomas Prevost, *Vice Chair*
Steve M. Mills, *Past Chair*
Judith Gorman, *Secretary*

John Barr	Alexander Gelman	David J. Law
Karen Bartleson	Jim Hughes	Ted Olsen
Victor Berman	Richard H. Hulett	Glenn Parsons
Ted Burse	Young Kyun Kim	Ronald C. Petersen
Richard DeBlasio	Joseph L. Koepfinger*	Narayanan Ramachandran
Andy Drozd	John Kulick	Jon Walter Rosdahl
Mark Epstein		Sam Sciacca

*Member Emeritus

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

Howard L. Wolfman, TAB Representative
Michael Janezic, NIST Representative
Satish Aggarwal, NRC Representative

Don Messina
IEEE Standards Program Manager, Document Development

Kathryn Cush
IEEE Standards Program Manager, Technical Program Development

Contents

1. Overview.....	2
1.1 Scope.....	2
3. Definitions	3
4. Abbreviations.....	5
5. Conformance.....	7
5.6 S-VLAN component conformance	7
5.8 B-component conformance.....	7
5.11 Backbone Edge Bridge conformance	8
6. Support of the MAC Service	9
6.10 Support of the EISS by Provider Instance Ports	9
6.11 Support of the EISS by Customer Backbone Ports.....	9
6.19 TE Service Instance Multiplex Entity.....	9
8. Principles of bridge operation.....	11
8.4 ~~Port states and the active topology~~ Active topologies, learning, and forwarding	11
8.6 The Forwarding Process	12
8.7 The Learning Process.....	13
8.8 The Filtering Database.....	13
8.9 MST and ESP configuration information	17
12. Bridge management	19
12.6 Forwarding process.....	19
12.14 CFM entities	19
12.16 Backbone Edge Bridge management.....	23
12.19 PBB-TE Protection Switching managed objects	24
17. Management protocol	29
17.2 Structure of the MIB	29
17.3 Relationships to other MIBs	33
17.4 Security Considerations	34
17.7 MIB modules	35
18. Principles of Connectivity Fault Management operation	69
19. CFM Entity operation	71
19.2 Maintenance association End Point.....	71
19.3 MIP Half Function	73
19.4 Maintenance Point addressing	74
20. Connectivity Fault Management protocols.....	75
20.1 Continuity Check protocol.....	75
20.2 Loopback protocol	76
20.3 Linktrace protocol.....	78
20.4 Connectivity Fault Management state machines	80

20.5	CFM state machine timers	81
20.9	MEP variables	81
20.11	MEP Continuity Check Initiator procedures	82
20.16	MEP Continuity Check Receiver variables	82
20.17	MEP Continuity Check Receiver procedures	82
20.25	MEP Mismatch variables	83
20.26	MEP Mismatch state machines	84
20.28	MP Loopback Responder procedures	85
20.31	MEP Loopback Initiator transmit procedures	86
20.38	MEP Mismatch Fault Notification Generator variables	87
20.39	MEP Mismatch Fault Notification Generator procedures	87
20.40	MEP Mismatch Fault Notification Generator state machine	87
20.42	MEP Linktrace Initiator procedures	89
20.47	LTM Receiver procedures	89
21.	Encoding of CFM Protocol Data Units	93
21.3	CFM request and indication parameters	93
21.5	TLV Format	93
21.6	Continuity Check Message format	94
21.7	Loopback Message and Loopback Reply formats	94
21.8	Linktrace Message Format	96
22.	CFM in systems	97
22.1	CFM shims in Bridges	97
22.2	Maintenance Entity creation	99
25.	Support of the MAC Service by Provider Backbone Bridged Networks	105
25.10	Support of the MAC Service by a PBB-TE Region	105
26.	Principles of Provider Backbone Bridged Network Operation	109
26.4	Backbone addressing	109
26.9	Connectivity Fault Management in a PBB-TE Region	109
26.10	Protection switching for point-to-point TE service instances	113
26.11	Mismatch defect	122
Annex A (normative)	PICS proforma	125
A.5	Major capabilities	125
A.8	Basic Filtering Services	126
A.9	Addressing	126
A.14	Bridge Management	127
A.21	VLAN support	128
A.23	Connectivity Fault Management	128
A.24	Management Information Base (MIB)	129
A.25	Protection Switching	130
Annex H (informative)	Bibliography	131

List of figures

Figure 6-7	Two back-to-back Up and Down TE Service Instance Multiplex Entities	10
Figure 19-3	MIP Half Function	74
Figure 20-1	MEP state machines—overview and relationships	80
Figure 20-8	MEP Traffic Field Mismatch state machine	84
Figure 20-9	MEP Local Mismatch state machine	85
Figure 20-13	MEP Mismatch Fault Notification Generator state machine	88
Figure 22-9	Creating MEPs and MIPs	100
Figure 25-13	Internal organization of the MAC sublayer in a PBB-TE Region	105
Figure 25-14	PBB-TE Region	107
Figure 26-7	Independent ESPs using the same ESP-DAs and ESP-VIDs	110
Figure 26-8	PBB-TE MEP placement in a CBP	111
Figure 26-9	Protection Switching Architecture	113
Figure 26-10	PBB-TE point-to-point protection switching	115
Figure 26-11	Mapping data traffic to the protection entity	117
Figure 26-12	Relationships of the Protection switching state machines—overview	117
Figure 26-13	Hold-off state machine	121
Figure 26-14	Clear Manual Switch state machine	121
Figure 26-15	Service Mapping state machine	122

List of tables

Table 8-7	Forwarding or Filtering for specific group MAC Addresses.....	17
Table 17-1	Structure of the MIB modules	29
Table 17-2	IEEE8021-TC MIB structure.....	29
Table 17-11	IEEE8021-CFM MIB correspondence between variables, managed objects, and MIB objects.....	30
Table 17-11	IEEE8021-CFM MIB correspondence between variables, managed objects, and MIB objects.....	30
Table 17-16	IEEE8021-PBBTE MIB Structure and relationship to this standard.....	31
Table 17-17	Example of ieee8021PbbTeTeSidTable	32
Table 17-18	PBB-TE required MIB compliances.....	34
Table 19-1	Actions taken by MP OpCode Demultiplexers.....	72
Table 21-6	Type Field values.....	93
Table 21-21	Loopback Message and Loopback Reply formats.....	94
Table 21-22	PBB-TE MIP TLV format	95
Table 22-1	MEP creation	100
Table 22-2	MIP creation	102
Table 26-8	Protection Requests Hierarchy.....	119

IEEE Standard for Local and metropolitan area networks—

Virtual Bridged Local Area Networks

Amendment 10: Provider Backbone Bridge Traffic Engineering

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

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

Editorial Note

This amendment specifies changes to IEEE Std 802.1Q-2005, as amended by IEEE Std 802.1ad-2005, IEEE Std 802.1ag-2007, IEEE Std 802.1ak-2007, IEEE Std 802.1ah-2008, and IEEE Std 802.1ap-2008, that support provisioning systems that explicitly select traffic engineered paths within Provider Backbone Bridged Networks. Changes are applied to the base text of IEEE Std 802.1Q-2005 as amended by IEEE Std 802.1ad-2005, IEEE Std 802.1ak-2007, IEEE Std 802.1ag-2007, IEEE Std 802.1ah-2008, and IEEE Std 802.1ap-2008. Text shown in bold italics in this amendment defines the editing instructions for changes to this base text. Three editing instructions are used: **change**, **delete**, and **insert**. **Change** is used to make a change to existing material. The editing instruction specifies the location of the change and describes what is being changed. Changes to existing text may be clarified using **strikeout** markings to indicate removal of old material, and **underline** markings to indicate addition of new material. **Delete** removes existing material. **Insert** adds new material without changing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. Editorial notes will not be carried over into future editions of IEEE Std 802.1Q.

1. Overview

1.1 Scope

Insert the following text and bullets immediately after bullet z re-lettering as needed:

This standard specifies protocols, procedures, and managed objects to allow support of provisioning systems that explicitly select traffic engineered paths within Provider Backbone Bridged Networks by allowing a network operator to disable unknown destination address forwarding, source address learning and spanning tree protocols for administratively selected VLAN Identifiers, while allowing other network control protocols to dynamically determine active topologies for other services. These interoperable capabilities are supported by management of individual bridges by SNMP using an SMIPv2 MIB, by extensions to the other control protocols specified in this standard, by the use of CFM with the addresses and VLAN Identifiers that specify traffic engineered connections, and by 1:1 path protection switching capable of load sharing. To this end, it:

- a) Enables construction of active topologies by an external agent that is responsible for setting up Ethernet Switched Paths (ESPs) by splitting the B-VID space between distributed spanning tree protocols and provisioned control.
- b) Supports discard of frames with unknown destination addresses for B-VIDs under provisioned control.
- c) Supports the operation of Continuity Check, Loopback, and Linktrace protocols on provisioned traffic engineered paths.
- d) Supports 1:1 protection switching capable of load sharing for Traffic Engineered service instances.
- e) Provides required extension to SNMP management by SMIPv2 MIB modules.

This standard does not specify operation of Ethernet Switched Paths (ESPs) through multiple Provider Backbone Bridge Traffic Engineered (PBB-TE) Regions. All the Backbone Edge Bridges specified for use in a PBB-TE Region are IB-BEBs.

3. Definitions

Insert the following definitions, renumbering to place them in the appropriate collating order:

3.1 bidirectional protection switching: A protection switching architecture in which, for a failure, including a unidirectional failure (i.e., a failure affecting only one direction of transmission), both directions including the affected direction and the unaffected direction, are switched.

3.2 co-routed paths: Two unidirectional connectivity paths (one in each direction) supporting a bidirectional connectivity are co-routed if they traverse exactly the same bridge ports in the graph that describes the active topology, but in the reverse order, within known bounded time after the last change in active topology.

3.3 ESP-VID: A VID associated with a special value of the Multiple Spanning Tree Instance Identifier (MSTID) in the MST Configuration Table, the TE-MSTID, indicating that the VID is under the control of an external agent responsible for setting up Ethernet Switched Paths. Learning is disabled and forwarding is enabled for all frames allocated to ESP-VIDs.

3.4 Ethernet Switched Path (ESP): A provisioned traffic engineered unidirectional connectivity path among two or more Customer Backbone Ports (CBPs) that extends over a PBBN. The path is identified by a 3-tuple <ESP-DA, ESP-SA, ESP-VID>, where ESP-DA and ESP-SA are MAC addresses and ESP-VID is a VID allocated to TE-MSTID. An Ethernet Switched Path is point-to-point or point-to-multipoint.

3.5 forced switch: An administrative command to force the backbone service instances assigned to a Traffic Engineering (TE) protection group to be carried by this group's protection entity.

3.6 manual switch: An administrative command to move the backbone service instances assigned to a Traffic Engineering (TE) protection group to a specific TESI associated with this TE protection group in absence of signal failures on both of the entities in the group.

3.7 PBB-TE Region: A PBB-TE Region comprises a contiguous set of IB-BEBs and BCBs, capable of providing TE service instances, that have allocated a common subset of ESP-VIDs to an external agent that provides the active topology construction mechanism within this ESP-VID space and manages the Filtering Database of Bridges within the region to control the forwarding of frames with particular values of ESP-VID and destination MAC address.

3.8 point-to-point ESP: An ESP between two Customer Backbone Ports (CBPs). The ESP-DA and the ESP-SA in the ESP's 3-tuple identifier are the individual MAC addresses of the two CBPs.

3.9 point-to-multipoint ESP: An ESP among one root Customer Backbone Port (CBP) and n leaf CBPs. The ESP-DA in the ESP's 3-tuple identifier is a group MAC address identifying the n leaf CBPs, and the ESP-SA is the individual MAC address of the root.

3.10 point-to-point TE service instance: A TE service instance supported by two point-to-point ESPs where the ESPs' endpoints have the same Customer Backbone Port (CBP) MAC addresses.

NOTE—For reasons relating to TESI monitoring diagnostics, operational simplicity, etc. this standard assumes that the point-to-point ESPs associated with a point-to-point TESI are co-routed. Support for a point-to-point TESI that comprises non co-routed ESPs is problematic and is not defined in this standard.

3.11 point-to-multipoint TE service instance: A TE service instance supported by a set of ESPs that comprises one point-to-multipoint ESP from a root to n leaves plus a point-to-point ESP from each of the leaves to the root.

NOTE—For reasons relating to TESI monitoring diagnostics, operational simplicity, etc. this standard assumes that the point-to-point ESPs associated with a point-to-multipoint TESI are routed from each of the n leaves to the root along the branches of the point-to-multipoint ESP. Support for a point-to-multipoint TESI that comprises ESPs not routed in this way is problematic and is not defined in this standard.

3.12 Traffic Engineering (TE): The process that controls the placement of traffic demands in a network, in order to optimize the resource utilization and to ensure that the quality of service objectives for each defined class of service are met.

3.13 Traffic Engineering (TE) protection group: A group of two point-to-point TE service instances between a pair of Customer Backbone Ports (CBPs), which carries an assigned set of backbone service instances, and continues to carry these backbone service instances if any one of the TE service instances in the group is failed or disabled.

3.14 Traffic Engineering service instance (TESI): An instance of the MAC service supported by a set of ESPs and identified by TE-SID, forming a bidirectional service. A TE service instance is point-to-point or point-to-multipoint.

3.15 Traffic Engineering service instance identifier (TE-SID): An identifier of the TE service instance which corresponds to a series of 3-tuples <ESP-DA, ESP-SA, ESP-VID>, each one identifying one of the TE service instance's ESPs.

NOTE—The TE-SID is not used as a tag parameter.

4. Abbreviations

Add the following abbreviations, in the appropriate collating sequence.

BSI	backbone service instance
CIST-MSTID	Common and Internal Spanning Tree Multiple Spanning Tree Instance Identifier
ESP	Ethernet Switched Path
FS	Forced Switch
LoP	Lockout of Protection
PBB-TE	Provider Backbone Bridge-Traffic Engineering
SF	Signal Fail
TE-MSTID	Traffic Engineering Multiple Spanning Tree Instance Identifier
TE-SID	Traffic Engineering service instance identifier
TESI	Traffic Engineering service instance

5. Conformance

5.6 S-VLAN component conformance

Insert the following subclause after 5.6.1:

5.6.2 S-VLAN component requirements for PBB-TE

An S-VLAN component implementation that conforms to the provisions of this standard for PBB-TE (25.10) shall

- a) Disable learning for a set of B-VIDs allocated to TE-MSTID as specified in 8.4 and in 8.9; and
- b) Discard frames with unregistered destination addresses for B-VIDs allocated to TE-MSTID (8.8.1).

An S-VLAN component implementation that conforms to the provisions of this standard for PBB-TE (25.10) may

- c) Allow control of all B-VIDs by an external agent, conforming to the Reserved VID values of Table 9-2; and/or
- d) Support MIP creation and the corresponding CFM extensions for TE service instances as specified in 26.9.

5.8 B-component conformance

Insert the following subclause after 5.8.1:

5.8.2 B-component requirements for PBB-TE

A B-component implementation that conforms to the provisions of this standard for PBB-TE (25.10) shall

- a) Disable learning for a set of B-VIDs allocated to TE-MSTID as specified in 8.4 and in 8.9
- b) Discard frames with unregistered destination addresses for B-VIDs allocated to TE-MSTID (8.8.1)
- c) Support the Default Backbone Destination field in the backbone service instance tables on the CBPs providing TE service instances as specified in 6.11
- d) Support the Backbone VLAN identifier field in the backbone service instance tables on the CBPs providing TE service instances as specified in 6.11
- e) Support the creation of MEPs for the TE service instances on CBPs as specified in 26.9
- f) Support 1:1 protection switching as specified in 26.10.3
- g) Provide control via all of the PBB-TE required managed objects specified in Clause 12

A B-component implementation that conforms to the provisions of this standard for PBB-TE (25.10) may

- h) Allow control of all B-VIDs by an external agent, conforming to the Reserved VID values of Table 9-2
- i) Support MIP creation and the corresponding CFM extensions for TE service instances as specified in 26.9
- j) Support the Hold-Off timer used by the protection switching protocol as specified in 26.10.3
- k) Support sharing of TESIs among TE protection groups in order to provide 1:1 protection switching that is capable load sharing as specified in 12.19.1.2 and 26.10.2
- l) Support the Mismatch defect identification as specified in 26.11
- m) Support the PBB-TE Management Information Base (MIB) module defined in Clause 17

5.11 Backbone Edge Bridge conformance

Insert the following subclause after the last paragraph:

5.11.1 Backbone Edge Bridge requirements for PBB-TE

A Backbone Edge Bridge that conforms to the provisions of this standard for PBB-TE (25.10) shall comprise one B-component capable of providing TE service instances (5.8.2) and one or more I-components (5.7) or T-components (5.16).

6. Support of the MAC Service

6.10 Support of the EISS by Provider Instance Ports

Insert a new item d) after item c) as follows:

- d) An enableConnectionIdentifier.

Insert a new paragraph at the end of the subclause as follows:

The enableConnectionIdentifier parameter allows the VIP to use the connection_identifier parameter to learn associations between a backbone MAC address and a customer MAC address. The default value is TRUE. This parameter should be configured to FALSE at the root node of a point-to-multipoint TE service instance.

6.10.1 Data indications

Change the paragraph before NOTE 3 as follows:

If enableConnectionIdentifier is TRUE then the connection_identifier parameter references the value of the source_address parameter (B-SA) of the M_UNITDATA.indication primitive received from the PIP-ISS; otherwise the connection_identifier parameter is null. The connection_identifier parameter in the M_UNITDATA.indication primitive received from the PIP-ISS is ignored.

6.10.2 Data requests

Change the first sentence of the second paragraph as follows:

If enableConnectionIdentifier is TRUE and the connection_identifier is not null and the connection_identifier references an address retained by the Provider Instance Port, then the value for the destination_address is the address referenced by the connection_identifier.

6.11 Support of the EISS by Customer Backbone Ports

Insert the following sentence before the last sentence in the paragraph before item c):

Entries in the Backbone Service Instance table may be set automatically by the protection switching procedures described in 26.10.3.4.

Insert the following NOTE at the end of the subclause:

NOTE—If a CBP is associated with a TE service instance the Default Backbone Destination field and the Backbone VLAN identifier field shall be supported.

Insert the following subclause after 6.18:

6.19 TE Service Instance Multiplex Entity

The TE Service Instance Multiplex Entity allows shims defined for PBB-TE to be instantiated per TE service instance at a Service Access Point that supports multiple TE service instances. Figure 6-7 illustrates two TE Service Instance Multiplex Entities, placed back-to-back. A set of back-to-back TE Service Instance Multiplex Entities may be used at the multiplexed (E)ISS SAPs that are associated with ESP-VIDs on a

Customer Backbone Port to provide per TE service instance SAPs that support Connectivity Fault Management (CFM) shims for PBB-TE MAs as shown in Figure 26-8.

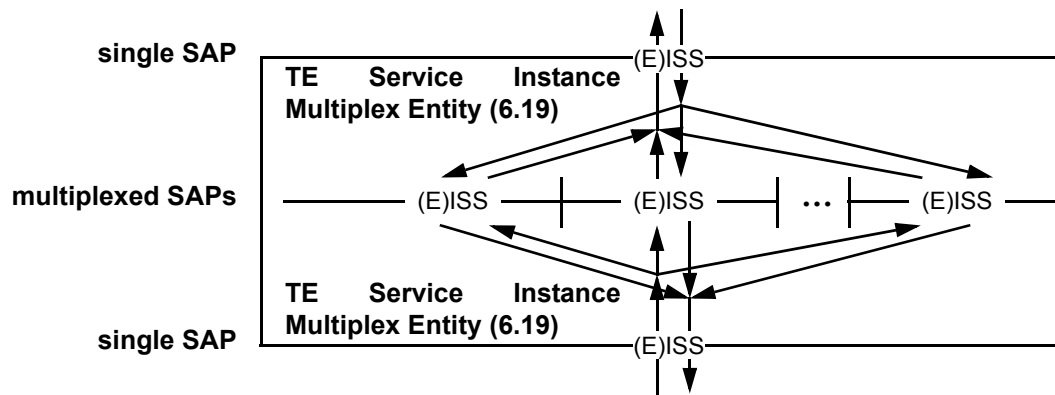


Figure 6-7—Two back-to-back Up and Down TE Service Instance Multiplex Entities

A TE Service Instance Multiplex Entity has one (E)ISS SAP that supports multiple TE service instances, and a number of multiplexed (E)ISS SAPs each supporting a single TE service instance. Each multiplexed SAP has destination_address, source_address, and vlan_identifier combinations assigned by the TE Service Instance Multiplex Entity. Every destination_address, source_address, and vlan_identifier combination can be assigned to a multiplexed SAP, and no destination_address, source_address, and vlan_identifier combination is assigned to more than one multiplexed SAP.

Upon receiving a Request or Indication from its single (E)ISS SAP, the TE Service Instance Multiplex Entity uses the destination_address, source_address, and vlan_identifier to select the corresponding one of its multiplexed SAPs to present the Request or Indication. The Request or Indication presented at the multiplexed SAPs has the same parameters as the original Request or Indication at the Single SAP. Similarly, any Request or Indication received from a multiplexed SAP is transparently presented to the single (E)ISS SAP.

The MAC_Operational status parameter (6.8.2) presented to the uppermost single (E)ISS SAP in Figure 6-7 is TRUE if and only if

- a) The uppermost single (E) ISS SAP's MAC_Enabled parameter is TRUE; and
- b) At least one of its multiplexed SAPs' MAC_Operational status parameters is TRUE.

The MAC_Operational status parameter of each of the multiplexed SAPs in Figure 6-7 is computed separately, and is TRUE if and only if

- c) The lowermost single (E)ISS SAP's MAC_Operational parameter is TRUE; and
- d) That multiplexed SAP's MAC_Enabled parameter is TRUE.

The MAC_Operational parameter of the passive SAP on a PBB-TE MEP is set to FALSE when the PBB-TE MEP declares an errorCCMdefect (20.21.3) or an xconCCMdefect (20.23.3), setting the MAC_Operational parameter of the associated multiplexed SAP on the TE Service Instance Multiplex Entity to FALSE. The MAC_Operational parameter of the passive SAP on a PBB-TE MEP is set back to TRUE when both defects are cleared, setting back to TRUE the MAC_Operational parameter of the associated multiplexed SAP.

8. Principles of bridge operation

Change 8.4 as follows:

8.4 ~~Port states and the active topology~~Active topologies, learning, and forwarding

~~Each Bridge Port has an operational Port State that governs whether or not it forwards frames classified as belonging to a given VLAN, and whether or not it learns from their source addresses.~~

~~The An active topology of a Bridged Local Area Network at any time is the set of communication paths formed is the connectivity provided, for frames with a specified set of VID, destination address, and source address values, a set of communication paths formed by interconnecting the LANs and Bridges in a bridged network by the with forwarding Bridge Ports.~~

~~The function of the distributed Spanning Tree algorithm and the Rapid Spanning Tree Protocol (RSTP, IEEE Std 802.1D Clause 17) used by SST Bridges to execute that algorithm, is to construct an active topology that is simply connected relative to communication between any pair of end stations, irrespective of the VLAN classification of frames used. The Multiple Spanning Tree Protocol (MSTP, Clause 13) used by MST Bridges constructs multiple active topologies. The distributed spanning tree algorithms and protocols, i.e. the Rapid Spanning Tree Protocol (RSTP, IEEE Std 802.1D Clause 17), and the Multiple Spanning Tree Protocol (MSTP, Clause 13), construct one or more active topologies, each simply and fully connected for frames belonging to any given VLAN. The *forwarding* and *learning* performed by each Bridge Port for each spanning tree is dynamically managed by RSTP, or MSTP to prevent temporary loops and reduce excessive traffic in the network while minimizing denial of service following any change in the *physical topology* of the network.~~

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

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

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

The term Port State summarizes per tree combinations of forwarding and learning, and any additional per tree variables used by a given spanning tree protocol to enforce the active topologies it has calculated, and is used by RSTP and MSTP as follows. Any port that has learning and forwarding disabled is assigned the Port State Discarding. Any, a Port that has learning enabled but forwarding disabled for frames allocated to a given spanning tree has the Port State *Learning* for that tree, and a Port that both learns and forwards frames has the Port State *Forwarding*. However the RSTP and MSTP state machines (IEEE Std 802.1D-2004, Clause 17 and Clause 13 of this standard) do not control the Port State directly but use independent forwarding and learning variables for each tree.

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

MSTP constructs multiple spanning trees, the Common and Internal Spanning Tree (CIST) and additional Multiple Spanning Tree Instances (MSTIs), and maintains a Port State for each spanning tree for each Port.

An MST Bridge allocates all frames classified as belonging to a given VLAN to the CIST or to one of the MSTIs using the MST Configuration Table. An MSTID of 0 identifies the CIST. A reserved MSTID value (TE-MSTID) is used to identify VIDs for use by PBB-TE with ESPs. A single VID is used to identify frames assigned to any given VLAN that is supported by the CIST or an MSTI. That VID is used by the Forwarding Process (8.6) to identify the spanning tree for the relayed frame, and thus identifies the applicable Port State.

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

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

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

8.6 The Forwarding Process

Change 8.6.1 as follows:

8.6.1 Active topology enforcement

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

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

~~Bridges with MST or PBB-TE capabilities, use the VID of the received frame to determine forwarding and learning for each Bridge Port for that frame as follows:~~

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

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

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

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

all VIDs allocated to the TE-MSTID (0xFFFE) are ESP-VIDs, and all VIDs allocated to other values of MSTID are assigned to the MSTI identified by that MSTID.

~~An MST Bridge allocates all frames with a given VID to the CIST or to a Multiple Spanning Tree Instance (MSTI). The allocation can be controlled by configuration of the MST Configuration Table (8.9.1) maintained by the Forwarding Process, subject to constraints (if any) imposed by the allocation of VIDs to FIDs (8.8.7). VIDs allocated to different spanning trees shall also be allocated to different FIDs. VIDs allocated to a given spanning tree may share the same FID.~~

Change subclause title of 8.6.2 as follows:

8.6.2 Ingress filtering

8.6.5 Flow classification and metering

Change the sentence before item a) as indicated:

Flow classification rules ~~may~~ can be based on:

Insert the following new item b) after item a) and reletter subsequent items accordingly:

- b) Source MAC Address

8.6.7 Queue management

Change bullet c) of 8.6.7 as follows:

- c) If the ~~associated~~ transmission Port is no longer forwarding for that frame (8.4, 8.6.1) ~~leaves the Forwarding state.~~

8.7 The Learning Process

Change the initial paragraph of 8.7, creating two paragraphs as follows:

The Learning Process receives the source MAC Addresses and VIDs of received frames from the Forwarding Process, subject to active topology enforcement (8.6.1) and following the application of the ingress ~~rules~~ filtering (8.6.2). The Learning Process is not invoked (see 8.6.1) for frames whose VID is an ESP-VID.

When invoked, the Learning Process ~~It~~ shall create or update a Dynamic Filtering Entry (8.8.3) that specifies the reception Port for the frame's source address and VID, if and only if the source address is an Individual Address, i.e., is not a Group Address, the resulting number of entries would not exceed the capacity of the Filtering Database, and the filtering utility criteria for the receiving Bridge Port are met, as specified below.

8.8 The Filtering Database

Change the initial text of 8.8 as follows:

The Filtering Database supports frame filtering (8.6.3) queries by the Forwarding Process ~~as to~~ determine whether received frames ~~received by the Forwarding Process~~, with given values of destination MAC Address ~~parameter~~ and VID, are to be forwarded through a given potential transmission Port (8.6.2, 8.6.3, 8.6.3).

8.8.1 Static Filtering Entries

Change the first two paragraphs as indicated.

A Static Filtering Entry specifies

- a) A MAC Address specification, comprising
 - 1) An Individual MAC Address; or
 - 2) A group MAC Address; or
 - 3) All Individual Addresses, for which no more specific Static Filtering Entry exists; or
 - 4) All Group Addresses, for which no more specific Static Filtering Entry exists; or
 - 5) All Unregistered Group Addresses, for which no more specific Static Filtering Entry exists.
- b) A VLAN identifier specification, comprising:
 - 1) The VID of a specific VLAN to which the static filtering information applies; or
 - 2) The wildcard VID (see Table 9-2), indicating that the static filtering information applies to all VLANs for which no specific Static Filtering Entry exists.
- c) A Port Map, containing a control element for each outbound Port, specifying that a frame with a destination MAC Address and VID that meets this specification is to be
 - 1) Forwarded, independently of any dynamic filtering information held by the Filtering Database; or
 - 2) Filtered, independently of any dynamic filtering information; or
 - 3) Forwarded or filtered on the basis of dynamic filtering information, or on the basis of the default Group filtering behavior for the outbound Port (8.8.6) if no dynamic filtering information is present specifically for the MAC Address.

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

8.8.8 Querying the Filtering Database

Retain the existing Table 8-5 and Table 8-6 referenced by 8.8.8 unchanged, but change the text of the subclause as follows:

~~If a frame is classified into a VLAN containing a given outbound Port in its member set (8.8.9), forwarding or filtering through that Port is determined by the control elements of filtering entries for the frame's destination MAC Address and for VLANs with the same VID or Filtering Identifier (FID, 8.8.7) as the frame's VLAN.~~

If the VID assigned to a relayed frame identifies a VLAN or an ESP with a given outbound Bridge Port in its member set (8.8.9), the Filtering Database entries that are applicable to the frame's destination MAC Address and VID determine whether the frame is filtered or forwarded through that Bridge Port. More than one entry can apply to a given frame. This subclause (8.8.8) specifies the effect of combining applicable entries, and of the absence of certain types of entries (not all possible entries are necessarily present). For an overview of the different types of entries, see the introductory text of 8.8.

Each entry in the Filtering Database for a MAC Address comprises

- a) ~~A MAC Address specification;~~
- b) ~~A VID or, in the case of Dynamic Filtering Entries, an FID;~~

- e) A Port Map, with a control element and optionally a connection_identifier (8.8.11, 6.8.1), for each outbound Port.

For Dynamic Filtering Entries, the FID that corresponds to a given VID is determined as specified in 8.8.7.

For a given VID, a given individual MAC Address specification can be included in the Filtering Database in a Static Filtering Entry, a Dynamic Filtering Entry, both or neither. Table 8-5 combines Static Filtering Entry and Dynamic Filtering Entry information for an individual MAC Address to specify forwarding, or filtering, of a frame with that destination MAC Address and VID through an outbound Port.

NOTE 1—The use of FID in this table for Static Filtering Entries, and the text in parentheses in the headings, reflects the fact that, where more than one VID maps to a given FID, there may be more than one Static Filtering Entry that affects the forwarding decision for a given individual MAC Address. The effect of all Static Filtering Entries for that address, and for VIDs that correspond to that FID, is combined, such that, for a given outbound Port:

- IF <any static entry for any VIDs that map to that FID specifies Forwarding> THEN <result = Forwarding>
- ELSE IF <any static entry for any VIDs that map to that FID specifies Filtering> THEN <result = Filtering>
- ELSE <result = Use Dynamic Filtering Information>

The Filtering Database entries applicable to a frame whose destination MAC Address is a specific Individual MAC Address are: the Dynamic Filtering Entry (if present) with that MAC Address and the FID to which the frame's VID is allocated (8.8.7), and all Static Filtering Entries (if any) with that MAC Address, or with "All Individual MAC Address," as their MAC Address specification and a VID that is also allocated to that FID, as their VLAN identifier specification. An entry with a wildcard VID applies only if there is no applicable Static Filtering Entry for a specific VID. Table 8-5 specifies the result of combining this information for an individual MAC address and a given outbound Bridge Port, and can be summarized as follows:

- IF any static entry for a VID allocated to the FID specifies Forward THEN Forward
- ELSE IF any static entry for a VID allocated to the FID specifies Filter THEN Filter
- ELSE IF a static entry for the wildcard VID specifies Forward THEN Forward
- ELSE IF a static entry for the wildcard VID specifies Filter THEN Filter
- ELSE IF dynamic (learnt filtering information) entry for the FID specifies Filter THEN Filter
- ELSE Forward

Table 8-6 specifies the result, Registered or Not Registered, of combining a Static Filtering Entry and a Group Registration Entry for the "All Group Addresses" address specification, and for the "All Unregistered Group Addresses" address specification for an outbound Port. Table 8-7 combines Static Filtering Entry and Group Registration Entry information for a specific group MAC Address with the Table 8-6 results for All Group Addresses and All Unregistered Group Addresses to specify forwarding, or filtering, of a frame with that destination group MAC Address through an outbound Port.

The Filtering Database entries applicable (if present) to a frame whose destination MAC Address is a specific group MAC Address are the Static Filtering Entries and MAC Address Registration Entries (for the frame's VID and for the wildcard VID) whose address specification is that group MAC address or "All Group Addresses" or "All Unregistered Group Addresses". A Static Filtering Entry for a wildcard VID applies only if there is no applicable Static Filtering Entry for a specific VID. MAC Address Registration Entries do not use wildcard VIDs. Table 8-6 specifies the results, Registered or Not Registered for a given outbound Bridge Port, of combining the entries for the "All Group Addresses" and for combining the entries for "All Unregistered Group Addresses." Table 8-7 combines these results with the entries for the specific group MAC Address. The result of Table 8-6 for "All Group Addresses" can be summarized as follows:

- IF a static entry for "All Group Addresses" and the frame's VID specifies Forward (Registration Fixed) THEN "All Group Addresses" is Registered
- ELSE IF a static entry for "All Group Addresses" and the frame's VID specifies Filter (Registration Forbidden) THEN "All Group Addresses" is Not Registered

- ELSE IF a dynamic (MAC Address Registration) entry for “All Group Addresses” and the frame’s VID specifies Forward (Registered) THEN “All Group Addresses” is Registered
- ELSE “All Group Addresses” is NOT Registered

NOTE—The result for “All Unregistered Group Addresses” is given by substituting that address specification for “All Group Address” throughout the summary.

The result of Table 8-7 can be summarized as follows:

- IF a static entry for the specific group address and the frame’s VID specifies Forward THEN Forward
- ELSE IF a static entry for the specific group address and the frame’s VID specifies Filter THEN Filter
- ELSE IF a static entry for the specific group address and the wildcard VID specifies Forward THEN Forward
- ELSE IF a static entry for the specific group address and the wildcard VID specifies Filter THEN Filter
- ELSE IF the Table 8-6 result for “All Group Addresses” is Registered THEN Forward
- ELSE IF the Table 8-6 result for “All Unregistered Group Addresses” is Registered THEN Forward
- ELSE IF a dynamic (MAC Address Registration) entry for the specific group address and the frame’s VID specifies Forward THEN Forward
- ELSE Filter

Where a given VID is allocated to the same FID as one or more other VIDs, it is an implementation option as to whether

- a) The results shown in Table 8-7 directly determine the forwarding/filtering decision for a given VID and group MAC Address (i.e., the operation of the Bridge with respect to group MAC Addresses ignores the allocation of VIDs to FIDs); or
- b) The results for a given MAC Address and VID are combined with the corresponding results for that MAC Address for each other VID that is allocated to the same FID, so that if the Table 8-7 result is Forward in any one VLAN that shares that FID, then frames for that group MAC Address will be forwarded for all VLANs that share that FID (i.e., the operation of the Bridge with respect to group MAC Addresses takes account of the allocation of VIDs to FIDs).

NOTE 2—In case d), the implementation effectively operates a single FDB per VLAN for group MAC Addresses. In case e), the implementation combines static and registered information for group MAC Addresses in accordance with the VID to FID allocations currently in force, in much the same manner as for individual MAC Addresses.

When forwarding or filtering a frame with a destination group MAC Address, a VLAN-aware Bridge may:

- a) Ignore the allocation of VIDs to FID, and use Table 8-7 directly for the frame’s VID; or
- b) Take the same decision for all VIDs allocated to any given FID, forwarding if Table 8-7 specifies Forward for any VID allocated to the same FID as the frame’s VID, and filtering otherwise.

Change Table 8-7 as follows:

Table 8-7—Forwarding or Filtering for specific group MAC Addresses

				Static Filtering Entry Control Element for this group MAC Address, VID and outbound Port specifies:				
				Registration Fixed (Forward)	Registration Forbidden (Filter)	Use MAC Address Registration Information, or no Static Filtering Entry present. MAC Address Registration Entry Control Element for this group MAC Address, VID and outbound Port specifies:		
						Registered (Forward)	Not Registered (Filter)	No MAC Address Registration Entry present
All Group Addresses control elements for this VID and Port specify (Table 8-6):	Not Registered	All Unregistered Group Addresses control elements for this VID and Port specify (Table 8-6):	Not Registered	Forward	Filter	Forward	Filter (Filter Unregistered Groups)	Filter (Filter Unregistered Groups)
			Registered	Forward	Filter	Forward	Filter Forward (Forward Unregistered Groups)	Forward (Forward Unregistered Groups)
	Registered			Forward	Filter	Forward (Forward All Groups)	Forward (Forward All Groups)	Forward (Forward All Groups)

Change the title of 8.9 as follows:

8.9 MST and ESP configuration information

Insert a new paragraph at the end of the subclause as follows:

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

8.9.1 MST Configuration Table

Insert a new paragraph before the last paragraph stating

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

8.13.11 Connectivity Fault Management entities

Change the second paragraph and the NOTE following as indicated:

Any given CFM entity is configured to recognize one or more Individual MAC address, and one or more Group MAC addresses, in received frames, and to use one or more Individual MAC address or one or two of the more Group MAC addresses for transmitted frames. The Individual MAC addresses ~~is~~ are unique, within a bridged network, to a specific Bridge, though not necessarily to a single Bridge Port (J.6). For VLAN based and backbone service instances, the ~~The~~ Group MAC addresses are selected from Table 8-9 and Table 8-10 according to the MD Level and OpCode fields in the CFM PDU header. For these service instances, Loopback Messages (LBMs, 20.2), Loopback Replies (LBRs, 20.2), and Linktrace Replies (LTRs, 20.3) are carried in unicast frames—while Continuity Check Messages (CCMs, 20.1) use addresses from Table 8-9, and Linktrace Messages (LTMs, 20.3) use addresses from Table 8-10. In the case of TE service instance, all CFM messages use the Individual MAC Addresses or the Group MAC addresses that are associated with the monitored service (20.1, 20.2, 20.3).

NOTE—The Group destination MAC addresses in Table 8-9 are there primarily to make it possible for Bridges built prior to IEEE Std 802.1ag-2007 to process CFM. ~~In future revisions of this standard, it is possible that this~~ This restriction on the choice of Group destination MAC addresses to be used on a CFM PDU ~~will be~~ is relaxed for ESP-VIDs. See 22.8.

12. Bridge management

12.6 Forwarding process

12.6.1 Port counters

12.6.1.1.2 Inputs

Change the first sentence of the paragraph as follows:

If the VLAN Identifier parameter is supported, then the forwarding Port counters are maintained per VLAN VID per Port.

12.14 CFM entities

12.14.2 CFM Stack managed object

Change 12.14.2.1.2 as follows:

12.14.2.1.2 Inputs

- a) An interface, either a Bridge Port, or an aggregated IEEE 802.3 port within a Bridge Port, on which MPs might be configured;
- b) An MD Level;
- c) A value indicating the direction in which any reported MP faces, either:
 - 1) Down (Active SAP is further away from the Frame filtering entity); or
 - 2) Up (Active SAP is closer to the Frame filtering entity); and
- d) A specific VID or I-SID for I- or B-components or the TE-SID to which the MEPs and MHFs are attached, or 0, for those attached to no VID or I-SID or TE-SID.

12.14.3 Default MD Level managed object

12.14.3.1 Read Default MD Level managed object

Change 12.14.3.1.1 as follows:

12.14.3.1.1 Purpose

To read the table of default parameters for controlling MHFs ~~on VIDs or I-SIDs of I- or B-components~~ not associated with any MA configured on the Bridge component.

12.14.3.2 Write Default MD Level managed object

Change 12.14.3.2.1 as indicated:

12.14.3.2.1 Purpose

To write entries in the table of default parameters for controlling MHFs ~~on VIDs or on I-SIDs used in an I- or B-component~~ not associated with any MA configured on the Bridge component.

12.14.4 Configuration Error List managed object

12.14.4.1 Read Configuration Error List managed object

Change 12.14.4.1.1 as follows:

12.14.4.1.1 Purpose

To read entries in the list of ~~Bridge Ports or aggregated~~ ports and VLANs or I-SID used in I- or B-components or TE-SID currently configured in error. The Configuration Error List managed object lists only those Bridge Ports or aggregated ports and vlan_identifiers that have configuration errors.

Change 12.14.4.1.2 as follows:

12.14.4.1.2 Inputs

- a) A vlan_identifier or I-SID or TE-SID, specifying which VLAN service instance to check for ~~Bridge Ports or aggregated~~ ports in error; and
- b) An interface, either a Bridge Port, or an aggregated IEEE 802.3 port within a Bridge Port.

12.14.5 Maintenance Domain managed object

Change 12.14.5.3.2 and 12.14.15.3.3 as indicated:

12.14.5.3.2 Inputs

- a) A reference to a particular Maintenance Domain managed object (12.14.5);
- b) The Short MA Name of an MA within that Maintenance Domain, including the format specifier from Table 21-20 (21.6.5.4). In the case of a PBB-TE or a VIDLAN based MA, the default value is a 2-octet integer (format 3) containing the primary VID, or 0, if the MA is not attached to a VID; and
- c) The list of ~~VIDs or the I-SID, or the TE-SID~~ monitored by this MA, or 0, if the MA is not attached to a VID or I-SID, or TE-SID. In the case of a list of VIDs, the first VID in the list is the MA's Primary VID (default none). The specification of I-SID based MAs are only possible is allowed only in the case of I- or B- components. The TE-SID is allowed only in the case that PBB-TE is supported.

12.14.5.3.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to nonexistent Maintenance Domain;
 - 2) Operation rejected due to invalid Short MA Name (21.6.5.4);
 - 3) Operation rejected due to the existence of another MA in the same Maintenance Domain with the same Short MA Name;
 - 4) Operation rejected because creation of this MA would exceed the number of MD Levels supported by some Bridge Port [item c) in 22.2.4];
 - 5) Operation rejected because the VID list provided [item c) in 12.14.5.3.2] specifies a different Primary VID, or contains one or more, but not all, of the VIDs, in the definition of another MA or an entry in the Default MD Level managed object; or
 - 6) Operation rejected because the I-SID value specified does not correspond to a valid Backbone Service Instance;
 - 7) Operation rejected because the TE-SID value specified does not correspond to a valid TE Service Instance;
 - 8) Operation accepted.

12.14.6 Maintenance Association managed object**12.14.6.1.3 Outputs***Change list item b) as indicated:*

- b) The VID(s) ~~or the I-SID used in I- and B-components, or TE-SID~~ monitored by this MA, or 0, if the MA is not attached to any VID, ~~or I-SID, or TE-SID~~. In the case of a list of VIDs, the first VID returned is the MA's Primary VID.

12.14.6.3.3 Outputs*Change the list items as indicated:*

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to nonexistent MA;
 - 2) Operation rejected because the specified MEPID already exists in this MA in this Bridge;
 - 3) Operation rejected because MEPID is not in the MA's list of MEPIDs [item g) in 12.14.6.1.3];
 - 4) Operation rejected due to the existence of a MEP in the same direction (Up or Down) at that same MD Level, for the same VID(s), ~~or I-SID or TE-SID~~ as this MEP (or for no VID, ~~or I-SID or TE-SID~~, if this MEP's MA has no VID, ~~or I-SID or TE-SID~~), on that Bridge Port or aggregated IEEE 802.3 port;
 - 5) Operation failed because one or more of the listed VIDs, ~~or I-SID or TE-SID~~ in this MA are assigned to some other MA on which Up MEPs are configured on any Bridge Port;
 - 6) Operation rejected because the Bridge is incapable of instantiating a MEP on that Bridge Port or aggregated IEEE 802.3 port;
 - 7) Operation rejected because an Up MEP cannot be configured for an MA that has no VID, ~~or I-SID or TE-SID~~;
 - 8) Operation rejected because a MEP exists on this MA that has a different value for its Up/Down parameter [item c) in 12.14.6.3.2]; or
 - 9) Operation accepted.

12.14.7 Maintenance association End Point managed object**12.14.7.1.3 Outputs***Change list item d) as indicated:*

- d) (writable) An integer indicating the Primary VID of the MEP, always one of the VIDs assigned to the MEP's MA ~~or the I-SID used in I- or B-components of the MEP~~. The value 0 indicates that either the Primary VID ~~or I-SID~~ is that of the MEP's MA, or that the MEP's MA is associated with no VID. In the case of a PBB-TE associated MEP, the Primary VID is not writable but is always associated with the value of the ESP-VID parameter identifying the MA's ESP that has the MEP's MAC address in its ESP-SA field (MEPprimaryVID, 20.9.7);

Change list item h) as indicated:

- h) (writable) The priority parameter for CCMs and LTMs transmitted by the MEP (default value: the highest priority, i.e., that with the highest numerical value, allowed to pass through the Bridge Port for any of this MEP's VIDs, ~~or I-SID or TE-SID~~);

Change list item i) as indicated:

- i) The MAC address of the MEP (19.4); In the case of a MEP that is associated with a TE service instance, the MAC address of the CBP upon which the MEP is operating;

Insert three new items at the end of the list as indicated:

- ae) (writable) A list indicating which of the remote MEPs in the same MA are active. The Remote MEP state machines (20.20) are instantiated only for the active remote MEPs. By default, all configured remote MEPs in the same MA are active.
- af) (writable) Only applicable for PBB-TE MEPs supporting the Traffic field (21.6.1.4), a Boolean flag indicating that the capability to report the presence of traffic is enabled. The default value is FALSE;
- ag) (writable) Only applicable for PBB-TE MEPs supporting the Traffic field (21.6.1.4), a Boolean flag indicating that the mismatch defect is allowed to generate a Fault Alarm. The default value is FALSE;
- ah) Only applicable for PBB-TE MEPs supporting the Traffic field (21.6.1.4), a Boolean flag indicating the presence of a traffic field mismatch defect (20.25.2) (can trigger DefMmCCM);
- ai) Only applicable for PBB-TE MEPs supporting the Traffic field (21.6.1.4), a Boolean flag indicating the presence of a local mismatch defect (20.25.5) (can trigger DefMmCCM);
- aj) Only applicable for PBB-TE MEPs supporting the Traffic field (21.6.1.4), an enumerated value indicating if the mismatch defect that has been present since the MEP Mismatch Fault Notification Generator state machine was last in the MFNG_RESET state, either:
 - 1) **DefNone:** No defect has been present since the last MFNG_RESET state; or
 - 2) **DefMmCCM:** This MEP is receiving CCMs that have different value in their Traffic field than the CCMs transmitted by this MEP or is transmitting CCMs with both the RDI and the Traffic field bit set to 1 and the disableLocdefect (20.25.4) variable is cleared, so variable item ah) in 12.14.7.1.3 is set;
- ak) Only applicable for PBB-TE MEPs supporting the Traffic field (21.6.1.4), a value indicating the current state of the MEP Mismatch Fault Notification Generator state machine (20.40).

12.14.7.3 Transmit Loopback Messages

12.14.7.3.2 Inputs

Insert a new item f) at the end of the list as follows:

- f) In the case of a PBB-TE MEP, the Reverse VID to be used in the associated PBB-TE MIP TLV (21.7.5). The parameter is not required in the case of PBB-TE MEPs associated with point-to-point TESIs or if the b2) entry is a MAC address corresponding to an entry in the ESP-DA field of any of the MA's ESPs.

12.14.7.3.3 Outputs

Insert a new item a5) in the list. Renumber subsequent items accordingly.

- a) An indication of whether the command was accepted by the MEP, either:
 - 5) Operation rejected due to invalid ESP-VID;

12.14.7.4 Transmit Linktrace Messages

12.14.7.4.2 Inputs

Insert a new item e) at the end of the list as follows:

- e) In the case of a PBB-TE MEP, the Reverse VID to be used in the associated PBB-TE MIP TLV (21.7.5). The parameter is not required in the case of PBB-TE MEPs associated with point-to-point TESIs.

12.14.7.4.3 Outputs

Insert a new item a5) in the list. Renumber subsequent items accordingly.

- a) An indication of whether the command was accepted by the MEP, either:
 - 5) Operation rejected due to invalid ESP-VID:

12.14.7.7 Transmit MEP Fault Alarm

Change 12.14.7.7.1 as indicated:

12.14.7.7.1 Purpose

To alert the Manager to the existence of a fault in a monitored MA, by issuing a Fault Alarm. Transmit MEP Fault Alarm is not a command; it is an unsolicited notification from the xmitFaultAlarm() procedure, issued upon detection of the Fault Alarm condition by the MEP Fault Notification Generator state machine, or by the MEP Mismatch Fault Notification Generator state machine. The Fault Alarm is sent to the address specified in item j) in 12.14.7.1.3.

12.14.7.7.2 Outputs

Change item c) as indicated:

- c) An enumerated value, equal to the contents of the variable highestDefect (20.33.9), and to the corresponding MEP managed object [item n) in 12.14.7.1.3] or indicating the presence of a mismatch defect [item aj) in 12.14.7.1.3].

12.16 Backbone Edge Bridge management

12.16.3 VIP configuration managed object

12.16.3.1.3 Outputs

Insert a new item g) at the end of the list as indicated:

- g) enableConnectionIdentifier—A Boolean to indicate if the connection_identifier parameter is allowed to learn associations between a backbone MAC address and a customer MAC address (6.10).

12.16.3.2.2 Outputs

Insert a new item e) at the end of the list as indicated:

- e) enableConnectionIdentifier—A Boolean that determines if the connection_identifier parameter is allowed to learn associations between a backbone MAC address and a customer MAC address (6.10). The default value is TRUE. This parameter should be configured to FALSE at the root node of a point-to-multipoint TE service instance.

12.16.5 CBP Configuration managed object

Insert a new item e) at the end of the list as indicated:

- e) TESI assignment managed object (12.16.5.3)

Insert a new subclause 12.16.5.3 after current 12.16.5.2 as indicated:

12.16.5.3 TESI assignment managed object

12.16.5.3.1 Purpose

All CBPs providing TE service instances shall implement the TESI assignment managed object to assign a particular TESI on this CBP.

12.16.5.3.2 Inputs

- a) ComponentID—the number identifying the bridge component associated with this port.
- b) Port Number—that component's Port Number for the Bridge Port.
- c) A series of ordered 3-tuples of the form <ESP-DA, ESP-SA, ESP-VID>.

12.16.5.3.3 Outputs

- a) Operation status—this takes one of the following values:
 - 1) Operation rejected because the ComponentID and Port Number do not identify a valid CBP;
 - 2) Operation rejected because a 3-tuple in the provided series has a VID value in its ESP-VID field that is not allocated to TE-MSTID;
 - 3) Operation rejected because no 3-tuple in the provided series has the CBP's MAC address in its ESP-SA field;
 - 4) Operation rejected because there are only two 3-tuples provided and the values in their ESP-DA and ESP-SA fields are not reversed;
 - 5) Operation rejected because there are more than two different values specified in the ESP-DA fields of the provided series of 3-tuples;
 - 6) Operation accepted.

Insert a new subclause 12.18 as follows:

12.18 PBB-TE Protection Switching managed objects

The PBB-TE Protection Switching managed objects model operations that create, modify, delete, or enquire about, the configuration and the operation of protection switching. The following are the PBB-TE Protection Switching managed objects in a B-component of an IB-BEB capable of supporting TE service instances:

- a) The TE protection group list managed object (12.18.1)
- b) The TE protection group managed object (12.18.2)

12.18.1 TE protection group list managed object

There is one TE protection group list managed object per IB-BEB. It contains a list of the TE protection groups that have been configured on the IB-BEB.

The management operations that can be performed on the TE protection group list managed object are as follows:

- a) Read TE protection group list (12.18.1.1)
- b) Create TE protection group managed object (12.18.1.2)
- c) Delete TE protection group managed object (12.18.1.3)

12.18.1.1 Read TE protection group list

12.18.1.1.1 Purpose

To obtain information about all of the TE protection groups in an IB-BEB.

12.18.1.1.2 Inputs

None.

12.18.1.1.3 Outputs

A list, perhaps empty, of the TE protection group managed objects configured on the IB-BEB. For each item in the list, the Read TE protection group list command returns:

- a) A reference to a particular Maintenance Association managed object (12.14.6) identifying a PBB-TE MA that corresponds to the group's working entity; and
- b) A reference to a particular Maintenance Association managed object (12.14.6) identifying a PBB-TE MA with the same end points as the one provided in item b) that corresponds to the group's protection entity.
- c) A reference to all TE protection group managed objects (12.18.2) that share a working or protection entity with the TE protection group in the list.

12.18.1.2 Create TE protection group managed object

12.18.1.2.1 Purpose

To create a new TE protection group managed object in an IB-BEB and add it to the IB-BEB's TE protection group list managed object.

12.18.1.2.2 Inputs

- a) A reference to a particular Maintenance Association managed object (12.14.6) identifying a PBB-TE MA that corresponds to the working entity; and
- b) A reference to a particular Maintenance Association managed object (12.14.6) identifying a PBB-TE MA with the same end points as the one provided in item a) that will monitor the protection entity.

12.18.1.2.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to nonexistent Maintenance Domain;
 - 2) Operation rejected due to non existent Maintenance Associations;
 - 3) Operation rejected because the referred MAs do not correspond to PBB-TE services;
 - 4) Operation rejected because the two referred MAs do not have the same end points;
 - 5) Operation rejected because the two referred MAs do not belong to the same MD;
 - 6) Operation rejected due to duplicate MAs; or
 - 7) Operation accepted. In addition, the list, perhaps empty, of the TE protection group managed objects (12.18.2) that share a working or protection entity with the created TE protection group is provided.

12.18.1.3 Delete TE protection group managed object

12.18.1.3.1 Purpose

To delete a specific TE protection group managed object from an IB-BEB and from the IB-BEB's TE protection group list managed object.

12.18.1.3.2 Inputs

- a) A reference to a particular TE protection group managed object (12.18.2).

12.18.1.3.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to nonexistent TE protection group;
 - 2) Operation rejected because the TE protection group is enabled; or
 - 3) Operation accepted.

12.18.2 TE protection group managed object

There can be any number of TE protection group managed objects per IB-BEB, one for each working and protection pair of TE service instances with common end points.

The management operations that can be performed on the TE protection group managed object are as follows:

- a) Read TE protection group managed object (12.18.2.1);
- b) Write TE protection group managed object (12.18.2.2); and
- c) TE protection group administrative commands managed object (12.18.2.3).

12.18.2.1 Read TE protection group managed object

12.18.2.1.1 Purpose

To obtain information from an IB-BEB about a specific TE protection group managed object.

12.18.2.1.2 Inputs

- a) A reference to a particular TE protection group managed object (12.18.2).

12.18.2.1.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to nonexistent TE protection group; or
 - 2) Operation accepted;
- b) (writable) A list of backbone-SIDs, identifying the protected backbone service instances, or NULL indicating that no backbone service instances are assigned to the TE protection group and that the TE protection group is disabled.
- c) An enumerated value indicating the operational state of the Service Mapping state machine (Figure 26-15) for each TE protection group:
 - 1) WORKING_PATH;
 - 2) PROTECTION_PATH;
 - 3) WTR; or
 - 4) PROT_ADMIN.

- d) An enumerated value indicating the status of active requests within the TE protection group:
 - 1) **NoRequest.** No administrative command is in effect;
 - 2) **LoP.** Set if LoP (26.10.3.3.4) is TRUE, indicating that an administrative command to prohibit the use of the protection entity is in effect;
 - 3) **FS.** Set if FS (26.10.3.3.5) is TRUE, indicating that an administrative command to perform forced switching to the protection path(s) is in effect;
 - 4) **p.SFH.** Set if SFH (26.10.3.3.3) is TRUE on the protection entity;
 - 5) **w.SFH.** Set if SFH (26.10.3.3.3) is TRUE on the working entity;
 - 6) **MStoProtection.** Set if MStoProtection (26.10.3.3.6) is TRUE, indicating that an administrative command to perform manual switching to the protection path(s) is in effect;
 - 7) **MStoWorking.** Set if MStoWorking (26.10.3.3.7) is TRUE, indicating that an administrative command to perform manual switching to the working path is in effect;
- e) (writable) (optional) The Wait-to-restore (WTR) period (26.10.3.3.8). In revertive operation it may be configured in steps of 1 min between 5 min and 12 min; the default value is 5 min. The value 0 indicates non-revertive operation; and
- f) (writable) (optional) The Hold-Off period (26.10.3.3.9). The range of the Hold-Off period is 0 s to 10 s in steps of 100 ms; the default value is 0.

12.18.2.2 Write TE protection group managed object

12.18.2.2.1 Purpose

To alter a value of a specific TE protection group managed object.

12.18.2.2.2 Inputs

- a) A reference to a particular TE protection group managed object (12.18.2);
- b) A reference to one of the writable managed objects in 12.18.2.1.3 that is to be altered; and
- c) A new value for the managed object.

12.18.2.2.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to nonexistent TE protection group;
 - 2) Operation rejected due to the selected managed object being Read-Only;
 - 3) Operation rejected due to lack of authority to set this variable;
 - 4) Operation rejected due to invalid value for the selected managed object;
 - 5) Operation accepted.

12.18.2.3 TE protection group administrative commands managed object

12.18.2.3.1 Purpose

To set an administrative command on a TE protection group managed object.

12.18.2.3.2 Inputs

- a) A reference to a particular TE protection group managed object (12.18.2); and
- b) An enumerated value indicating the exercised administrative command:
 - 1) **Clear.** An indication to clear all other administrative commands;
 - 2) **Lockout of Protection.** An administrative command to prohibit the use of the protection entity;
 - 3) **Forced Switch.** An administrative command to perform forced switching to the protection path(s);

- 4) **Manual Switch To Protection.** An administrative command to perform manual switching to the protection path(s) if it is operational;
- 5) **Manual Switch To Working.** An administrative command to perform manual switching to the working path if it is operational.

12.18.2.3.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to nonexistent TE protection group;
 - 2) Operation rejected due to lack of authority to set this variable;
 - 3) Operation rejected due to an active higher priority request; or
 - 4) Operation accepted.

17. Management information base (MIB)

17.2 Structure of the MIB

Insert a new row at the end of Table 17-1 as follows:

Table 17-1—Structure of the MIB modules

Module	Subclause	Defining IEEE standard	Reference	Notes
<u>IEEE8021-PBBTE MIB</u>	<u>17.7.10</u>	<u>802.1Qay</u>	=	<u>Initial version in IEEE Std 802.1Qay</u>

17.2.1 Structure of the IEEE8021-TC-MIB

Add the following entries to Table 17-2 to reflect new textual conventions defined for the use of the IEEE8021-PBBTE-MIB:

Table 17-2—IEEE8021-TC MIB structure

IEEE MIB object	Reference
<u>IEEE8021PbbTeProtectionGroupId</u>	<u>12.19.2</u>
<u>IEEE8021PbbTeEsp</u>	<u>3.4 in IEEE Std 802.1Qay</u>
<u>IEEE8021PbbTeTSidId</u>	<u>3.13 in IEEE Std 802.1Qay</u>
<u>IEEE8021PbbTeProtectionGroupConfigAdmin</u>	<u>26.10.3.3.4, 26.10.3.3.5, 26.10.3.3.6, 26.10.3.3.7, item d) in 12.18.2.1.3</u>
<u>IEEE8021PbbTeProtectionGroupActiveRequests</u>	<u>12.18.2.3.2</u>

17.2.2 Structure of the IEEE8021-CFM-MIB

Insert the following entries into Table 17-11 in front of the entry for Transmit Loopback Messages:

Table 17-11—IEEE8021-CFM MIB correspondence between variables, managed objects, and MIB objects

Variable	IEEE MIB table/object	Reference
	<u>dot1agCfmMepPbbTeCanReportPbbTePresence</u>	<u>12.14.17.1.3 af)</u>
	<u>dot1agCfmMepPbbTeTrafficMismatchDefect</u>	<u>12.14.17.1.3 ah)</u>
	<u>dot1agCfmMepPbbTeLbmReverseVid</u>	<u>12.14.7.3.2 f)</u>
	<u>dot1agCfmMepPbbTeLtmReverseVid</u>	<u>12.14.7.4.2 e)</u>
	<u>dot1agCfmMepPbbTeMismatchAlarm</u>	<u>12.14.17.1.3 ag)</u>
	<u>dot1agCfmMepPbbTeMismatchDefect</u>	<u>12.14.17.1.3 ai)</u>
	<u>dot1agCfmMepPbbTeMismatchSinceReset</u>	<u>12.14.17.1.3 aj)</u>
Transmit LoopbackMessages 12.14.7.3	dot1agCfmMepTable, dot1agCfmMepTransmitLbmStatus	

Insert the following entry into Table 17-11 before the entry for dot1agCfmFaultAlarm:

Table 17-11—IEEE8021-CFM MIB correspondence between variables, managed objects, and MIB objects

Variable	IEEE MIB table/object	Reference
	<u>dot1agCfmMepDbRMepIsActive</u>	<u>12.14.17.1.3 ae)</u>
Transmit MEP Fault Alarm (12.14.7.7)	dot1agCfmFaultAlarm	

Insert a new subclause 17.2.10 as follows:

17.2.10 Structure of the IEEE8021-PBBTE MIB

The IEEE8021-PBBTE MIB provides objects to configure and manage the IEEE 802.1Qay Provider Backbone Bridges—Traffic Engineering amendment.

Objects in this MIB module are arranged into subtrees. Each subtree is organized as a set of related objects. Where appropriate, the corresponding Clause 12 management reference is also included.

Table 17-15 shows the mapping of the PBB-TE Clause 12 managed objects to the tables and columns of the PBB-TE MIB that model those managed objects.