IEEE STANDARDS ASSOCIATION

IEEE Standard for

Local and metropolitan area networks—

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

Amendment 19: PBB-TE Infrastructure Segment Protection

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

23 December 2011

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

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

IEEE Standard for
Local and metropolitan area networks—

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

Amendment 19: PBB-TE Infrastructure Segment Protection

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 7 December 2011

IEEE-SA Standards Board

Abstract: This amendment to IEEE Std 802.1Q-2011 specifies localized protection of selected Traffic Engineered Service Instances traversing a common sequence of Provider Network Ports.
Keywords: Bridged Local Area Networks, IEEE 802.1Qbf, Infrastructure Segment Protection, LANs, local area networks, MAC Bridges, MANs, metropolitan area networks, Provider Backbone Bridge, Traffic Engineering

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

PDF: **ISBN 978-0-7381-7153-1** **STD97185**
Print: **ISBN 978-0-7381-7178-4** **STDPD97185**

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

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

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

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation, 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 his or her independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

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 on standards and requests for interpretations should be addressed to:

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

Introduction

This introduction is not part of IEEE Std 802.1Qbf-2011, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks—Amendment 19: PBB-TE Infrastructure Segment Protection.

This amendment to IEEE Std 802.1Q-2011 specifies localized protection of selected Traffic Engineered Service Instances traversing a common sequence of Provider Network Ports.

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

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

Notice to users

Laws and regulations

Users of 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

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

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

Participants

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

Tony Jeffree, *Chair*
Paul Congdon, *Vice Chair*
Robert Sultan, *Editor*
Stephen Haddock, *Chair, Interworking Task Group*

Zehavit Alon
Yafan An
Ting Ao
Peter Ashwood-Smith
Christian Boiger
Paul Bottorff
Rudolf Brandner
Craig Carlson
Rodney Cummings
Claudio DeSanti
Zhemin Ding
Donald Eastlake
Janos Farkas
Donald Fedyk
Norman Finn
Ilango Ganga
Geoffrey Garner
Anoop Ghanwani
Mark Gravel
Eric Gray
Yingjie Gu
Craig Gunther
Hitoshi Hayakawa
Hal Keen
Srikanth Keesara
Yongbum Kim
Philippe Klein
Oliver Kleineberg
Michael Krause
Lin Li
Jeff Lynch
Thomas Mack-Crane
David Martin
John Messenger
John Morris
Eric Multanen
David Olsen
Donald Pannell
Glenn Parsons
Mark Pearson
Joseph Pelissier
Rene Raeber
Karen T. Randall
Josef Roese
Dan Romascanu
Jessy Rouyer
Ali Sajassi
Panagiotis Saltsidis
Michael Seaman
Rakesh Sharma
Kevin Stanton
Michael Johas Teener
Patricia Thaler
Chait Tumuluri
Maarten Vissers

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

Thomas Alexander
Butch Anton
Hugh Barrass
Nancy Bravin
William Byrd
Radhakrishna Canchi
Keith Chow
Charles Cook
Wael Diab
Patrick Diamond
Thomas Dineen
Carlo Donati
Sourav Dutta
Yukihiro Fujimoto
Randall Groves
Stephen Haddock
John Hawkins
David Hunter
Paul Isaacs
Atsushi Ito
Raj Jain
Tony Jeffree
Vincent Jones
Shinkyo Kaku
Piotr Karocki
Stuart J. Kerry
Yongbum Kim
Geoff Ladwig
Shen Loh
William Lumpkins
Greg Luri
Thomas Mack-Crane
Elvis Maculuba
Arthur Marris
Jeffery Masters
Gary Michel
Jose Morales
Michael S. Newman
Satoshi Obara
Karen T. Randall
Maximilian Riegel
Robert Robinson
Benjamin Rolfe
Jessy Rouyer
Randall Safier
Peter Saunderson
Bartien Sayogo
Kapil Sood
Thomas Starai
Walter Struppler
Robert Sultan
Joseph Tardo
Michael Johas Teener
Patricia Thaler
Mark-Rene Uchida
Prabodh Varshney
John Vergis
Hung-Yu Wei
Oren Yuen

When the IEEE-SA Standards Board approved this amendment on 7 December 2011, it had the following membership:

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

Masayuki Ariyoshi
William Bartley
Ted Burse
Clint Chaplin
Wael Diab
Jean-Philippe Faure
Alexander Gelman
Paul Houzé
Jim Hughes
Joseph L. Koepfinger*
David J. Law
Thomas Lee
Hung Ling
Oleg Logvinov
Ted Olsen
Gary Robinson
Jon Walter Rosdahl
Sam Sciacca
Mike Seavey
Curtis Siller
Phil Winston
Howard Wolfman
Don Wright

*Member Emeritus

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

Satish K. Aggarwal, *NRC Representative*
Richard DeBlasio, *DOE Representative*
Michael Janezic, *NIST Representative*

Michelle Turner
IEEE Standards Program Manager, Document Development

Kathryn Bennett
IEEE Standards Program Manager, Technical Program Development

Contents

Figures

Tables

IEEE Standard for
Local and metropolitan area networks—

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

Amendment 19: PBB-TE Infrastructure Segment Protection

This amendment to IEEE Std 802.1Q™-2011 specifies localized protection of selected Traffic Engineered Service Instances traversing a common sequence of Provider Network Ports. Changes are applied to the base text of IEEE Std 802.1Q-2011 as amended by IEEE Std 802.1Qbe™-2011, IEEE Std 802.1Qbc™-2011, IEEE Std 802.1Qbb™-2011, and IEEE Std 802.1Qaz™-2011.

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

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

1. Overview

1.3 Introduction

Insert the following list item after item ag) in 1.3, and reletter the subsequent list items in 1.3 accordingly:

ah) Supports protection of a group of Traffic Engineered service instances that traverses a sequence of LANs and intervening Bridges using a method that does not require the modification of data or control frames.

3. Definitions

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

3.x Active Segment: The Infrastructure Segment, either the Working Segment or the Protection Segment, that is currently carrying traffic of TESIs associated with the IPG.

3.x candidate Protection Segment: In the case of M:1 IPS, an Infrastructure Segment that can assume the role of Protection Segment.

3.x current Protection Segment: In the case of M:1 IPS, the candidate Protection Segment that is currently assuming the role of Protection Segment;

3.x Infrastructure Protection Group (IPG): In the case of 1:1 IPS, a set comprising a Working Segment and a Protection Segment or, in the case of M:1 IPS, a set comprising a Working Segment and one or more Protection Segments.

3.x Infrastructure Protection Switching (IPS): The switching of a selected group of TESIs from a Working Segment to a Protection Segment or from a Protection Segment to a Working Segment due to failure of connectivity, restoration of connectivity, or administrative command.

3.x Infrastructure Segment: A sequence of PNPs and the intervening LANs and Bridge relay entities.

3.x Protection Segment: An Infrastructure Segment associated with an IPG that can carry TESI traffic when the Working Segment associated with that IPG has failed or when directed by administrative command.

3.x Segment Endpoint Bridge (SEB): A PBB at the endpoint of an Infrastructure Segment.

3.x Segment Endpoint Port (SEP): A PNP at the endpoint of an Infrastructure Segment.

3.x Segment Identifier (SEG-ID): A pair of SMP-IDs specifying the identity of an Infrastructure Segment.

3.x Segment Intermediate Bridge (SIB): A PBB having an intermediate position within an Infrastructure Segment.

3.x Segment Intermediate Port (SIP): A PNP having an intermediate position within an Infrastructure Segment.

3.x Segment Monitoring Path (SMP): A unidirectional path carrying CFM traffic associated with the monitoring of an Infrastructure Segment.

3.x Segment Monitoring Path Identifier (SMP-ID): A 3-tuple <SMP-DA, SMP-SA, SMP-VID> where the SMP-DA is the MAC address of the destination PNP of the SMP, the SMP-SA is the MAC address of the origin PNP of the SMP, and SMP-VID is a VID allocated to the TE-MSTID (8.9) and associated with the SMP.

3.x Working Segment: The Infrastructure Segment, among the Infrastructure Segments associated with an IPG, on which TESI traffic is carried when no connectivity failure of that segment has been detected and no administrative command is active.

4. Abbreviations

Insert the following abbreviations into Clause 4 in alphabetical order:

IPG	Infrastructure Protection Group
IPS	Infrastructure Protection Switching
SEB	Segment Endpoint Bridge
SEG-ID	Segment Identifier
SEP	Segment Endpoint Port
SIB	Segment Intermediate Bridge
SIP	Segment Intermediate Port
SMP	Segment Monitoring Path
SMP-ID	Segment Monitoring Path Identifier

5. Conformance

5.6 S-VLAN component conformance

5.6.2 S-VLAN component requirements for PBB-TE

Change the following list items in 5.6.2 as shown:

c) Allow ...; ~~and/or~~
d) Support ... ~~.~~ ; and/or
e) Support Infrastructure Protection Switching as specified in 26.11.

Insert the following subclause, 5.6.3, after 5.6.2:

5.6.3 S-VLAN component requirements for PBB-TE IPS

An S-VLAN component implementation that conforms to the provisions of this standard for PBB-TE IPS (26.11) shall

a) Support 1:1 IPS as specified in 26.11.2

An S-VLAN component implementation that conforms to the provisions of this standard for PBB-TE IPS (26.11) may

b) Support M:1 IPS as specified in 26.11.5

5.8 B-component conformance

5.8.2 B-component requirements for PBB-TE

Insert the following list item at the end of 5.8.2:

n) Support Infrastructure Protection Switching as specified in 26.11

Insert the following subclause, 5.8.3, after 5.8.2:

5.8.3 B-component requirements for PBB-TE IPS

A B-component implementation that conforms to the provisions of this standard for PBB-TE IPS (26.11) shall

a) Support 1:1 IPS as specified in 26.11.2

A B-component implementation that conforms to the provisions of this standard for PBB-TE IPS (26.11) may

b) Support M:1 IPS as specified in 26.11.5

6. Support of the MAC Service

6.20 Support of the ISS with signaled priority

Insert the following subclause, 6.21 (including Figure 6-13), after 6.20.2:

6.21 Infrastructure Segment Multiplex Entity

The Infrastructure Segment Multiplex Entity allows shims defined for SEPs and SIPs to be instantiated per Infrastructure Segment at a Service Access Point that supports multiple Infrastructure Segments. Figure 6-13 illustrates two Infrastructure Segment Multiplex Entities, placed back-to-back. A set of back-to-back Infrastructure Segment Multiplex Entities may be used at the multiplexed (E)ISS SAPs that are associated with SMP-VIDs on a Provider Network Port to provide per Infrastructure Segment SAPs that support Connectivity Fault Management (CFM) shims for Infrastructure Segment MAs as shown in Figure 26-10.

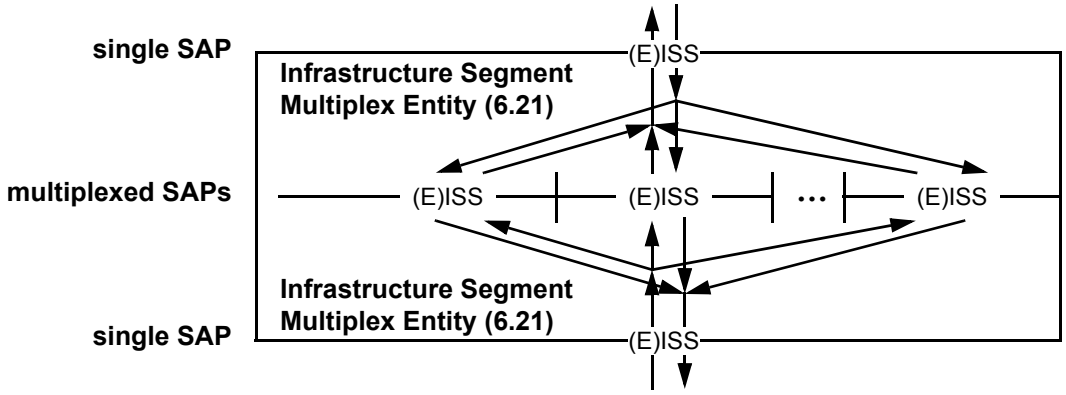

Figure 6-13—Two back-to-back Up and Down Infrastructure Segment Multiplex Entities

An Infrastructure Segment Multiplex Entity has one (E)ISS SAP that supports multiple Infrastructure Segment instances, and a number of multiplexed (E)ISS SAPs each supporting a single Infrastructure Segment instance. Each multiplexed SAP has destination_address, source_address, and vlan_identifier combinations assigned by the Infrastructure Segment 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 Infrastructure Segment 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 (6.6.2) presented to the uppermost single (E)ISS SAP in Figure 6-13 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 6-13 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 an Infrastructure Segment MEP is set to FALSE when the Infrastructure Segment 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 Infrastructure Segment Multiplex Entity to FALSE. The MAC_Operational parameter of the passive SAP on an Infrastructure Segment 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

8.3 Model of operation

Insert the following text (including Figure 8-8) at the end of 8.3, and renumber the subsequent figures in Clause 8 accordingly:

Figure 8-8 illustrates the operation of the IPS Control entity. The IPS Control entity functions as an intermediary between the Bridge Management entity and the FDB for operations related to TESIs associated with an IPG. Infrastructure Segment MEPs associated with an IPG communicate the operational state of the associated Infrastructure Segment to the IPS control entity (26.11.3).

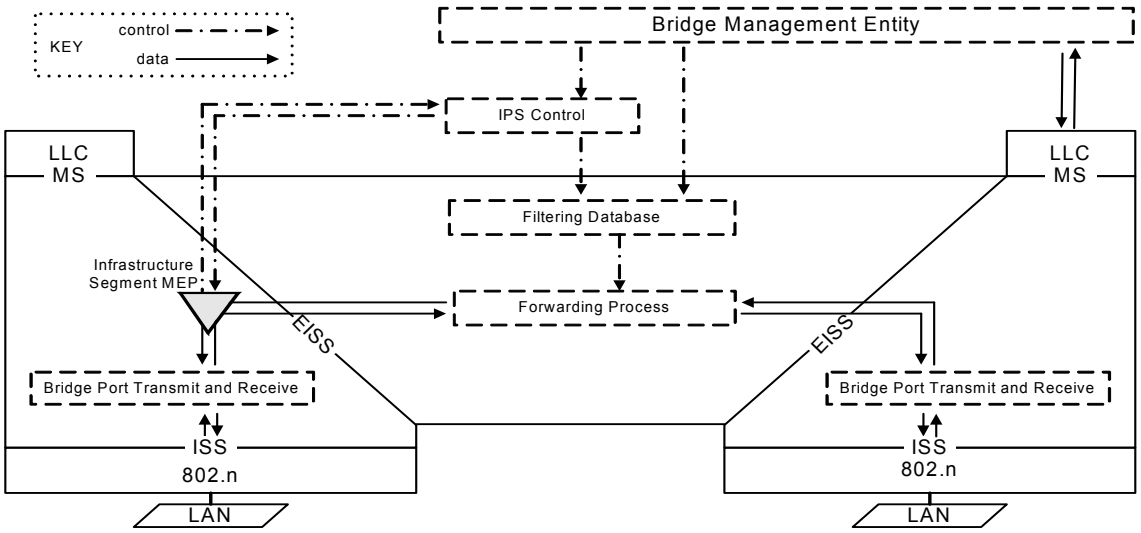

Figure 8-8—Infrastructure Segment MEP placement in a PNP

8.8 The Filtering Database

Change the sixth paragraph in 8.8 as follows:

Static filtering information is added to, modified, and removed from the Filtering Database only under explicit management control<u> except when PBB-TE IPS is deployed, in which case the static filtering information for traffic associated with IPGs configured on the Bridge is added to, modified, and removed from the Filtering Database only under the direction of IPS Control (26.11.3)</u>. It shall not be automatically removed by any ageing mechanism. Management of static filtering information may be carried out by use of the remote management capability provided by Bridge Management (8.12) using the operations specified in Clause 12.

12. Bridge management

12.7 Filtering Database

12.7.7 General Filtering Database operations

12.7.7.1 Create Filtering Entry

12.7.7.1.3 Outputs

Insert the following list item after item a) in 12.7.7.1.3, and reletter the remaining list item in 12.7.7.1.3 accordingly:

b) Operation rejected because the specified Static Filtering Entry is associated with an Infrastructure Protection Group and is administered by IPS Control;

12.14 CFM entities

12.14.2 CFM Stack managed object

12.14.2.1 Read CFM Stack managed object

12.14.2.1.2 Inputs

Change list item d) in 12.14.2.1.2 as indicated:

d) A specific VID, I-SID, TE-SID, or SEG-ID associated with an MP, or 0, in the case that the MP is associated with no VID, I-SID, TE-SID, or SEG-ID. ~~or I-SID for I-components 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.~~

Change 12.14.4 through 12.14.4.1.2 as indicated:

12.14.4 Configuration Error List managed object

The Configuration Error List managed object is a list of {~~service instance~~ identifier, port} pairs configured in error together with the identity of the configuration error. The ~~service instance~~ identifier is a VID, I-SID, ~~or~~ TE-SID, or SEG-ID, and the port is a simple bridge port or aggregated bridge port.

12.14.4.1 Read Configuration Error List managed object

12.14.4.1.1 Purpose

To list the entries in the Configuration Error List where each entry describes the ~~Service Instance I~~identifier and port pair that identifies the entry, together with a description of the particular configuration error.

12.14.4.1.2 Inputs

a) A VID~~vlan identifier or~~, I-SID, or TE-SID, specifying which service instance to check for ports in error or a SEG-ID specifying which Infrastructure Segment to check for 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

12.14.5.3 Create Maintenance Association managed object

12.14.5.3.2 Inputs

Change 12.14.5.3.2 as indicated:

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~~ VID-based ~~MA~~, or Infrastructure Segment 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, the I-SID, ~~or~~ the TE-SID, or the SEG-ID monitored by this MA, or 0, if the MA is not attached to any VID, ~~or~~ I-SID, ~~or~~ TE-SID, or SEG-ID. In the case ~~of~~ that a list of VIDs is specified, the first VID in the list is the MA's Primary VID (default none). The specification of I-SID 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. The SEG-ID is allowed only in the case that IPS is supported.

12.14.5.3.3 Outputs

Insert the following list item after item 7) in 12.14.5.3.3 a) ("Operation status..."), and renumber the remaining list item in 12.14.5.3.3 a) accordingly:

8) Operation rejected because the SEG-ID value specified does not correspond to a valid Infrastructure Segment;

12.14.6 Maintenance Association managed object

12.14.6.1 Read Maintenance Association managed object

12.14.6.1.3 Outputs

Change list item b) in 12.14.6.1.3 as indicated:

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

12.14.6.3 Create Maintenance association End Point managed object

12.14.6.3.3 Outputs

Change list item 4) in 12.14.6.3.3 a) ("Operation status...") as indicated:

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), I-SID, ~~or~~ TE-SID, or SEG-ID as this MEP (or for no VID, I-SID, ~~or~~ TE-SID, or SEG-ID, if this MEP's MA has no VID, I-SID, ~~or~~ TE-SID, or SEG-ID), on that Bridge Port or aggregated IEEE 802.3 port;

12.14.7 Maintenance association End Point managed object

12.14.7.1 Read Maintenance association End Point managed object

12.14.7.1.3 Outputs

Change list item d) in 12.14.7.1.3 as indicated:

d) (writable) An integer indicating the Primary VID of the MEP, always one of the VIDs assigned to the MEP's MA. The value 0 indicates that either the Primary VID 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). In the case of an Infrastructure Segment associated MEP, the Primary VID (MEPprimaryVID, 20.9.7) is not writable but is always associated with the value of the SMP-VID parameter identifying the MA's SMP that has the MEP's MAC address in its SMP-SA field;

Change list item h) in 12.14.7.1.3 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, or SEG-ID);

Change list item i) in 12.14.7.1.3 as indicated:

i) The MAC address of the MEP (19.4); In the case of a MEP that is associated with a TESI, the MAC address of the CBP upon which the MEP is operating. In the case of a MEP that is associated with an Infrastructure Segment, the MAC address of the PNP upon which the MEP is operating;

Insert the following subclauses, 12.24 through 12.24.2.3.3, after 12.23:

12.24 1:1 PBB-TE Infrastructure Protection Switching (IPS) managed objects

The IPS managed objects model operations that create, modify, delete, or inquire about the configuration and the operation of IPS (26.11). To this end, they describe objects related to an Infrastructure Protection Group (IPG) (26.11.2.1). The following are the IPS managed objects associated with a SEB:

a) IPG list managed object (12.24.1);
b) IPG managed object (12.24.2).

12.24.1 IPG list managed object

There is one IPG list managed object per SEB. The IPG list managed object contains a list of the IPGs that have been configured on the SEB.

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

a) Read IPG list (12.24.1.1);
b) Create IPG managed object (12.24.1.2); and
c) Delete IPG managed object (12.24.1.3).

12.24.1.1 Read IPG list

12.24.1.1.1 Purpose

To obtain information about the set of IPGs associated with a SEB.

12.24.1.1.2 Inputs

None.

12.24.1.1.3 Outputs

A list, perhaps empty, of the IPG managed objects configured on the SEB. For each item in the list, the Read IPG list command returns:

a) A value identifying the IPG;
b) A reference to the particular Maintenance Association managed object (12.14.6) identifying the Infrastructure Segment MA that corresponds to the working entity of the IPG;
c) A reference to the particular Maintenance Association managed object (12.14.6) identifying the Infrastructure Segment MA that corresponds to the protection entity of the IPG; and
d) In the case of M:1 IPS, a prioritized list of references to Maintenance Association managed object (12.14.6), each of which identifies a candidate Protection Segment associated with the IPG.

12.24.1.2 Create IPG managed object

12.24.1.2.1 Purpose

To create a new IPG managed object in a SEB and add it to the IPG list managed object associated with the SEB.

12.24.1.2.2 Inputs

a) A reference to a particular Maintenance Association managed object (12.14.6) identifying the Infrastructure Segment MA that corresponds to the working entity of the IPG; and
b) In the case of 1:1 IPS, a reference to a particular Maintenance Association managed object (12.14.6) identifying the Infrastructure Segment MA that corresponds to the protection entity of the IPG or, in the case of M:1 IPS, a prioritized list of references to Maintenance Association managed object (12.14.6), each of which identifies an Infrastructure Segment MA associated with an Infrastructure Segment that is a candidate Protection Segment for the IPG.

12.24.1.2.3 Outputs

a) Operation status. This takes one of the following values:
    1) Operation rejected due to nonexistent MD;
    2) Operation rejected due to a nonexistent MA;
    3) Operation rejected because a referenced MA is not associated with an Infrastructure Segment;
    4) Operation rejected because the referenced MAs do not belong to the same MD;
    5) Operation rejected because two or more managed objects referenced are associated with the same MA;
    6) Operation rejected because neither SMP-ID associated with a SEG-ID identifying one of the referenced Infrastructure MAs contains in its SMP-SA field the MAC address of a PNP associated with the SEB; or
    7) Operation accepted.

12.24.1.3 Delete IPG managed object

12.24.1.3.1 Purpose

To remove a specific IPG managed object from the IPG list managed object associated with the SEB and to delete that IPG managed object.

12.24.1.3.2 Inputs

a) A reference to a particular IPG managed object (12.24.2).

12.24.1.3.3 Outputs

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

12.24.2 IPG managed object

There can be any number of IPG managed objects per SEB.

The management operations that can be performed on the IPG managed object are as follows:

a) Read IPG managed object (12.24.2.1);
b) Write IPG managed object (12.24.2.2); and
c) Apply administrative command to IPG managed object (12.24.2.3).

12.24.2.1 Read IPG managed object

12.24.2.1.1 Purpose

To obtain information from a SEB regarding a specified IPG managed object.

12.24.2.1.2 Inputs

a) A reference to an IPG managed object (12.24.2).

12.24.2.1.3 Outputs

a) Operation status. This takes one of the following values:
   1) Operation rejected due to nonexistent IPG; or
   2) Operation accepted.
b) The MAID and Port Number associated with the Working Segment and an indication (TRUE or FALSE) as to whether the Working Segment is operational;
c) The MAID and Port Number associated with the Protection Segment and an indication (TRUE or FALSE) as to whether the Protection Segment is operational;
d) (optional) In the case of M:1 IPS, the list of MAIDs and Port Numbers associated with Candidate Protection Segments ordered from highest to lowest priority and an indication (TRUE or FALSE) as to whether each candidate Protection Segment is operational;
e) (writable) A list of TE-SIDs, possibly NULL, identifying TESIs protected by the IPG. If not NULL, the IPG is considered to be enabled;

f) An enumerated value indicating the operational state of the Service Mapping state machine (Figure 26-22) for each IPG:
   1) WORKING_SEGMENT;
   2) PROTECTION_SEGMENT;
   3) WTR; or
   4) PROT_ADMIN.

g) An enumerated value indicating the status of active requests within the IPG:
   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 Segment 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 Segment is in effect;
   4) **p.SFH:** Set if SFH (26.10.3.3.3) is TRUE on the Protection Segment;
   5) **w.SFH:** Set if SFH (26.10.3.3.3) is TRUE on the Working Segment;
   6) **MStoProtection:** Set if MStoProtection (26.10.3.3.6) is TRUE, indicating that an administrative command to perform manual switching to the Protection Segment 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 Segment is in effect;

h) (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 and 12 min; the default value is 5 min. The value 0 indicates nonrevertive operation. The value 0 is not permitted when the IPG is associated with M:1 IPS;

i) (writable) (optional) The hold-off period (26.10.3.3.9). The range of the hold-off period is 0 to 10 s in steps of 100 ms; the default value is 0.

j) (optional) An enumerated value indicating the operational state of the Protection Segment Selection state machine (Figure 26-26) for each IPG:
   1) PS_ASSIGNED;
   2) SEGMENT_OK;
   3) SEGMENT_FAILED;
   4) ASSIGN_NEW_PS; or
   5) REVERT_TO_BETTER_PS.

k) (writable) (optional) The M:1 wait-to-restore (MWTR) period (26.11.5.4.7.). In revertive operation it may be configured in steps of 1 min between 5 and 12 min; the default value is 5 min. The value 0 indicates nonrevertive operation.

12.24.2.2 Write IPG managed object

12.24.2.2.1 Purpose

To update a writable item associated with a specified IPG managed object.

12.24.2.2.2 Inputs

a) A reference to an IPG managed object (12.24.2);
b) The identity of a writable item in 12.24.2.1.3 that is to be updated; and
c) The updated value of the specified item.

12.24.2.2.3 Outputs

a) Operation status. This takes one of the following values:
   1) Operation rejected due to specification of nonexistent IPG;
   2) Operation rejected due to the selection of an item that is not writable;
   3) Operation rejected due to lack of authority to set the value of this item;

4) Operation rejected due to the specification of an invalid value for the selected item; or
5) Operation accepted.

12.24.2.3 Apply administrative command to IPG managed object

12.24.2.3.1 Purpose

To apply a specified administrative command to an IPG managed object.

12.24.2.3.2 Inputs

a) A reference to an IPG managed object (12.24.2); 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 Segment;
   3) **Forced Switch:** An administrative command to perform forced switching to the Protection Segment;
   4) **Manual Switch To Protection:** An administrative command to perform manual switching to the Protection Segment if that Infrastructure Segment is operational;
   5) **Manual Switch To Working:** An administrative command to perform manual switching to the Working Segment if that Infrastructure Segment is operational.

12.24.2.3.3 Outputs

a) Operation status. This takes one of the following values:
   1) Operation rejected due to specification of a nonexistent IPG;
   2) Operation rejected due to lack of authority to apply the specified command to the identified IPG managed object;
   3) Operation rejected due to an active higher priority request; or
   4) Operation accepted.

17. Management Protocol

17.2 Structure of the MIB

Insert the following row at the end of Table 17-1:

Table 17-1—Structure of the MIB modules

Module	Subclause	Defining IEEE standard	Reference	Notes
IEEE8021-TEIPS MIB	17.2.18	802.1Qbf	26.11	Initial version in 802.1Qbf

17.2.1 Structure of the IEEE8021-TC MIB

Insert the following rows at the end of Table 17-2:

Table 17-2—IEEE8021-TC MIB Structure

IEEE MIB object	Reference
IEEE8021TeIpsIpgid	12.24.2
IEEE8021TeIpsIpgConfigAdmin	26.10.3.3.4, 26.10.3.3.5, 26.10.3.3.6, 26.10.3.3.7, 12.14.2.1.2 f) and j)
IEEE8021TeIpsIpgActiveRequests	12.24.2.2.1 b)
IEEE8021TeipsSegid	26.11.1, 3.9
IEEE8021TeipsSmpid	26.11.1, 3.13

Insert the following subclauses, 17.2.18 through 17.2.18.3 (including Table 17-24), after 17.2.17:

17.2.18 Structure of the IEEE8021-TEIPS MIB

The IEEE8021-TEIPS MIB provides objects to configure and manage Infrastructure Protection Switching in a PBB-TE Region (26.11).

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 17-24 shows the mapping of the IPS Clause 12 managed objects to the tables and columns of the TEIPS MIB that model those managed objects.

An Infrastructure Protection Group (IPG) can be referenced externally. For this reason, a canonical external IPG identifier is provided via the textual convention `IEEE8021TeipsIpgid`. The convention defines a simple integer of local significance to a particular bridge component for the purpose of MIB management.

Table 17-24—IEEE8021-TE IPS MIB Structure and relationship to this standard

Variable	MIB Object	Reference
	ieee8021TeipsIpgTable	
	ieee8021TeipsIpgid	12.24.1.1.3 a)
	ieee8021TeipsIpgWorkingMA	12.24.1.1.3 b)
	ieee8021TeipsIpgProtectionMA	12.24.1.1.3 c)
	ieee8021TeipsIpgWorkingPortNumber	12.24.2.2.1 b)
	ieee8021TeipsIpgProtectionPortNumber	12.24.2.1.1 c)
	ieee8021TeipsTesiTable	
	ieee8021TeipsTesiId	12.24.2.1.3 f)
	ieee8021TeipsCandidatePsTable	
	ieee8021TeipsCandidatePsMA	12.24.2.1.3 e)
	ieee8021TeipsCandidatePsPortNumber	12.24.2.1.3 e)
	ieee8021TeipsCandidatePsOperational	12.24.2.1.3 e)
	ieee8021TeipsIpgConfigTable	
	ieee8021TeipsIpgConfigState	12.24.2.1.3 g)
	ieee8021TeipsIpgConfigCommandStatus	12.24.2.1.3 h)
	ieee8021TeipsIpgConfigCommandLast	12.24.2.3.2 b)
	ieee8021TeipsIpgConfigAdmin	12.24.2.2.1 b)
	ieee8021TeipsIpgConfigActiveRequests	12.24.2.1.3 h)
WTRwhile (26.10.3.2.1)	ieee8021TeipsIpgConfigWTR	12.24.2.1.3 i)
HoldOffWhile (26.10.3.2.2)	ieee8021TeipsIpgConfigHoldOff	12.24.2.1.3 j)
	ieee8021TeipsIpgM1ConfigState	12.24.2.1.3 k)
WTRwhile (26.10.3.2.1)	ieee8021TeipsIpgConfigMWTR	12.24.2.1.3 l)

An Infrastructure Segment can be referenced externally. For this reason, a canonical external Infrastructure Segment identifier is provided via the textual convention `IEEE8021TeipsSegid`. The convention defines a simple integer of local significance to a particular bridge component for the purpose of MIB management.

In the case of 1:1 IPS, an IPG specifies a Working Segment and a Protection Segment. In the case of M:1 IPS, the IPG specifies a Working Segment and a list of candidate Protection Segments from which the Protection Segment is selected. Each Infrastructure Segment is associated with a pair of Segment Monitoring Paths (SMPs). Each SMP is identified by a 3-tuple consisting of a <SMP-DA,SMP-SA,SMP-VID> tuple. Each such tuple is represented by the textual convention `IEEE8021TeipsSmpid`, which is a fixed-length octet string containing the two MAC addresses and the VID value.

17.2.18.1 Using the MIB to create MAs associated with Infrastructure Segments

IPS requires a mechanism to monitor the health of each Infrastructure Segment associated with an IPG. The CFM Maintenance Association provides this mechanism.

Configuring an MA requires adding a row to the CFM MIB's StackTable. Two columns are used in the StackTable to define the Infrastructure Segment upon which the MA operates. These are the `IEEE8021ServiceSelectorType` column and the `IEEE8021ServiceSelectorValue` column. The first column defines how the value in the second column is to be interpreted. If the value of the first column is set to `segid(4)`, then the second column is interpreted as the external representation of a SEG-ID.

Thus, Infrastructure Segments, and their corresponding identifiers, configured in the `ieee8021TeipsSegTable` provide the SEG-ID values that are used as parameters to rowcreate operations for the `CFMStackTable` to create MAs that monitor the health of Infrastructure Segments. Creating entries in the `CFMStackTable`, in turn, defines `MAID` values, represented as unsigned integers, that are used subsequently to configure the protected services.

17.2.18.2 Using the MIB to create IPGs

Infrastructure Protection Groups (IPGs) are created by adding rows to the `ieee8021TeipsIpgTable`. Each entry in the table contains columns representing the Working and Protection Segment MAs associated with the IPG, the Port Number associated with each Infrastructure Segment MA, and a RowStatus column used to manage the creation and deletion of the IPG. The MAs are referred to by MAID and can be found in the `StackTable` of the CFM MIB managed objects. The value of the Port Number column is derived from the corresponding Infrastructure Segment MA.

17.2.18.3 Using the MIB to query and configure IPGs

Each IPG has status and configuration information that can be managed. This information is located in the `ieee8021TeipsIpgConfigTable`. This table allows management stations to determine whether the Working Segment or Protection Segment is active, and it allows traffic to be switched by management command. It provides optional parameters for configuration of the waiting time before triggering a switchover and the time to restore after a failure condition has cleared.

17.3 Relationships to other MIBs

17.3.17 Relationship of the Priority-based Flow Control MIB to other MIB modules

Insert the following subclause, 17.3.18, after 17.3.17:

17.3.18 Relationship of the IEEE8021-TEIPS MIB to other MIB modules

The IEEE8021-TEIPS MIB is used to manage IB type Backbone Edge Bridges and Backbone Core Bridges that support IPS functionality. The IEEE8021-TEIPS-MIB uses textual conventions and objects from the following MIB modules:

IEEE8021-TC-MIB
IEEE8021-BRIDGE-MIB

The IEEE8021-TEIPS-MIB has the purpose of managing Infrastructure Protection Switching in a PBB-TE Region (26.11). Thus, use of the IEEE8021-TEIPS MIB requires that the system support the same set of MIB modules specified within 17.3.10 and requires the compliances described by Table 17-21.

17.4 Security considerations

17.4.17 Security considerations for the Priority-based Flow Control MIB

Insert the following subclause, 17.4.18, after 17.4.17:

17.4.18 Security considerations of the IEEE8021-TEIPS MIB

There are a number of management objects defined in this MIB module with a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a nonsecure environment without proper protection can have a negative effect on network operations. These tables and objects and their sensitivity/vulnerability are described below.

The following tables and objects in the TEIPS-MIB could be manipulated to interfere with the operation of PBBs. This could, for example, be used to force a reinitialization of state machines to cause network instability or to change the forwarding and filtering policies. The following are all the writable objects from the IEEE8021-TEIPS-MIB:

ieee8021TeipsIpgid
ieee8021TeipsIpgWorkingMA
ieee8021TeipsIpgProtectionMA
ieee8021TeipsTesiId
ieee8021TeipsCandidatePsMA
ieee8021TeipsIpgConfigWTR
ieee8021TeipsIpgConfigHoldOff
ieee8021TeipsIpgConfigMWTR

17.7 MIB modules

17.7.1 Definitions for the IEEEE8021-TC MIB Module

Delete the entire text of 17.7.1, and insert the following text:

```
IEEE8021-TC-MIB DEFINITIONS ::= BEGIN

-- ============================================================
-- TEXTUAL-CONVENTIONs MIB for IEEE 802.1
-- ============================================================

IMPORTS
    MODULE-IDENTITY, Unsigned32, org
        FROM SNMPv2-SMI -- RFC 2578
    TEXTUAL-CONVENTION
        FROM SNMPv2-TC; -- RFC 2579

ieee8021TcMib MODULE-IDENTITY
    LAST-UPDATED "201108230000Z" -- August 23, 2011
    ORGANIZATION "IEEE 802.1 Working Group"
    CONTACT-INFO
        "  WG-URL: http://grouper.ieee.org/groups/802/1/index.html
         WG-EMail: stds-802-1@ieee.org
```

```
           Contact: David Levi
            Postal: C/O IEEE 802.1 Working Group
                    IEEE Standards Association
                    445 Hoes Lane
                    P.O. Box 1331
                    Piscataway
                    NJ 08855-1331
                    USA
            E-mail: STDS-802-1-L@LISTSERV.IEEE.ORG

           Contact: Kevin Nolish
            Postal: C/O IEEE 802.1 Working Group
                    IEEE Standards Association
                    445 Hoes Lane
                    P.O. Box 1331
                    Piscataway
                    NJ 08855-1331
                    USA
            E-mail: STDS-802-1-L@LISTSERV.IEEE.ORG"
    DESCRIPTION
        "Textual conventions used throughout the various IEEE 802.1 MIB
         modules.

         Unless otherwise indicated, the references in this MIB
         module are to IEEE 802.1Q-2011.

         Copyright (C) IEEE.
         This version of this MIB module is part of IEEE802.1Q;
         see the draft itself for full legal notices."
    REVISION     "201108230000Z" -- August 23, 2011
    DESCRIPTION
         "Modified textual conventions  to support the IEEE 802.1
          MIBs for PBB-TE Infrastructure Protection Switching."
    REVISION     "201104060000Z" -- April 6, 2011
    DESCRIPTION
         "Modified textual conventions  to support Remote Customer
          Service Interfaces."
    REVISION     "201102270000Z" -- February 27, 2011
    DESCRIPTION
         "Minor edits to contact information etc. as part of
          2011 revision of IEEE Std 802.1Q."

    REVISION     "200811180000Z" -- November 18, 2008
    DESCRIPTION
         "Added textual conventions needed to support the IEEE 802.1
          MIBs for PBB-TE.  Additionally, some textual conventions were
          modified for the same reason."

    REVISION     "200810150000Z" -- October 15, 2008
    DESCRIPTION
         "Initial version."
    ::= { org ieee(111) standards-association-numbers-series-
standards(2)
```



```
          lan-man-stds(802) ieee802dot1(1) 1 1 }

ieee802dot1mibs OBJECT IDENTIFIER
    ::= { org ieee(111) standards-association-numbers-series-
standards(2)
          lan-man-stds(802) ieee802dot1(1) 1 }

-- ================================================================
-- Textual Conventions
-- ================================================================

IEEE8021PbbComponentIdentifier ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS       current
    DESCRIPTION
        "The component identifier is used to distinguish between the
        multiple virtual bridge instances within a PB or PBB.  Each
        virtual bridge instance is called a component.  In simple
        situations where there is only a single component the default
        value is 1.  The component is identified by a component
        identifier unique within the BEB and by a MAC address unique
        within the PBBN.  Each component is associated with a Backbone
        Edge Bridge (BEB) Configuration managed object."
    REFERENCE "12.3 l)"
    SYNTAX       Unsigned32 (1..4294967295)

IEEE8021PbbComponentIdentifierOrZero ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS       current
    DESCRIPTION
        "The component identifier is used to distinguish between the
        multiple virtual bridge instances within a PB or PBB.  In simple
        situations where there is only a single component the default
        value is 1.  The component is identified by a component
        identifier unique within the BEB and by a MAC address unique
        within the PBBN.  Each component is associated with a Backbone
        Edge Bridge (BEB) Configuration managed object.

        The special value '0' means 'no component identifier'.  When
        this TC is used as the SYNTAX of an object, that object must
        specify the exact meaning for this value."
    REFERENCE "12.3 l)"
    SYNTAX       Unsigned32 (0 | 1..4294967295)

IEEE8021PbbServiceIdentifier ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS       current
    DESCRIPTION
        "The service instance identifier is used at the Customer
        Backbone Port of a PBB to distinguish a service instance
        (Local-SID). If the Local-SID field is supported, it is
        used to perform a bidirectional 1:1 mapping between the
        Backbone I-SID and the Local-SID. If the Local-SID field
        is not supported, the Local-SID value is the same as the
```

```
        Backbone I-SID value."
    REFERENCE "12.16.3, 12.16.5"
    SYNTAX       Unsigned32 (256..16777214)

IEEE8021PbbServiceIdentifierOrUnassigned ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS       current
    DESCRIPTION
        "The service instance identifier is used at the Customer
        Backbone Port of a PBB to distinguish a service instance
        (Local-SID). If the Local-SID field is supported, it is
        used to perform a bidirectional 1:1 mapping between the
        Backbone I-SID and the Local-SID. If the Local-SID field
        is not supported, the Local-SID value is the same as the
        Backbone I-SID value.

        The special value of 1 indicates an unassigned I-SID."
    REFERENCE "12.16.3, 12.16.5"
    SYNTAX       Unsigned32 (1|256..16777214)

IEEE8021PbbIngressEgress ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "A 2 bit selector which determines if frames on this VIP may
        ingress to the PBBN but not egress the PBBN, egress to the
        PBBN but not ingress the PBBN, or both ingress and egress
        the PBBN."
    REFERENCE "12.16.3, 12.16.5, 12.16.6"
    SYNTAX       BITS {
                     ingress(0),
                     egress(1)
                 }

IEEE8021PriorityCodePoint ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "Bridge ports may encode or decode the PCP value of the
        frames that traverse the port. This textual convention
        names the possible encoding and decoding schemes that
        the port may use.  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."
    REFERENCE "12.6.2.6"
    SYNTAX       INTEGER {
                     codePoint8p0d(1),
                     codePoint7p1d(2),
                     codePoint6p2d(3),
                     codePoint5p3d(4)
                 }

IEEE8021BridgePortNumber ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
```

```
    STATUS       current
    DESCRIPTION
        "An integer that uniquely identifies a bridge port, as
        specified in 17.3.2.2 of IEEE 802.1ap.
        This value is used within the spanning tree
        protocol to identify this port to neighbor bridges."
    REFERENCE "17.3.2.2"
    SYNTAX       Unsigned32 (1..65535)

IEEE8021BridgePortNumberOrZero ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS       current
    DESCRIPTION
        "An integer that uniquely identifies a bridge port, as
        specified in 17.3.2.2 of IEEE 802.1ap.  The value 0
        means no port number, and this must be clarified in the
        DESCRIPTION clause of any object defined using this
        TEXTUAL-CONVENTION."
    REFERENCE "17.3.2.2"
    SYNTAX       Unsigned32 (0..65535)

IEEE8021BridgePortType ::= TEXTUAL-CONVENTION
    STATUS       current
    DESCRIPTION
        "A port type.  The possible port types are:

             customerVlanPort(2) - Indicates a port is a C-tag
                 aware port of an enterprise VLAN aware bridge.

             providerNetworkPort(3) - Indicates a port is an S-tag
                 aware port of a Provider Bridge or Backbone Edge
                 Bridge used for connections within a PBN or PBBN.

             customerNetworkPort(4) - Indicates a port is an S-tag
                 aware port of a Provider Bridge or Backbone Edge
                 Bridge used for connections to the exterior of a
                 PBN or PBBN.

             customerEdgePort(5) - Indicates a port is a C-tag
                 aware port of a Provider Bridge used for connections
                 to the exterior of a PBN or PBBN.

             customerBackbonePort(6) - Indicates a port is a I-tag
                 aware port of a Backbone Edge Bridge's B-component.

             virtualInstancePort(7) - Indicates a port is a virtual
                 S-tag aware port within a Backbone Edge Bridge's
                 I-component which is responsible for handling
                 S-tagged traffic for a specific backbone service
                 instance.

             dBridgePort(8) - Indicates a port is a VLAN-unaware
                 member of an 802.1D bridge.
```

```
            remoteCustomerAccessPort (9) - Indicates a port is an
                S-tag aware port of a Provider Bridge used for
                connections to remote customer interface LANs
                through another PBN."
    REFERENCE   "12.16.1.1.3 h4), 12.16.2.1/2,
                12.13.1.1, 12.13.1.2, 12.15.2.1, 12.15.2.2"
    SYNTAX      INTEGER {
                    none(1),
                    customerVlanPort(2),
                    providerNetworkPort(3),
                    customerNetworkPort(4),
                    customerEdgePort(5),
                    customerBackbonePort(6),
                    virtualInstancePort(7),
                    dBridgePort(8),
                    remoteCustomerAccessPort(9)
                }

IEEE8021VlanIndex ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS      current
    DESCRIPTION
        "A value used to index per-VLAN tables: values of 0 and
        4095 are not permitted.  If the value is between 1 and
        4094 inclusive, it represents an IEEE 802.1Q VLAN-ID with
        global scope within a given bridged domain (see VlanId
        textual convention).  If the value is greater than 4095,
        then it represents a VLAN with scope local to the
        particular agent, i.e., one without a global VLAN-ID
        assigned to it.  Such VLANs are outside the scope of
        IEEE 802.1Q, but it is convenient to be able to manage them
        in the same way using this MIB."
    REFERENCE   "9.6"
    SYNTAX      Unsigned32 (1..4094|4096..4294967295)

IEEE8021VlanIndexOrWildcard ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS      current
    DESCRIPTION
        "A value used to index per-VLAN tables.  The value 0 is not
        permitted, while the value 4095 represents a 'wildcard'
        value.  An object whose SYNTAX is IEEE8021VlanIndexOrWildcard
        must specify in its DESCRIPTION the specific meaning of the
        wildcard value.  If the value is between 1 and
        4094 inclusive, it represents an IEEE 802.1Q VLAN-ID with
        global scope within a given bridged domain (see VlanId
        textual convention).  If the value is greater than 4095,
        then it represents a VLAN with scope local to the
        particular agent, i.e., one without a global VLAN-ID
        assigned to it.  Such VLANs are outside the scope of
        IEEE 802.1Q, but it is convenient to be able to manage them
        in the same way using this MIB."
    REFERENCE   "9.6"
    SYNTAX      Unsigned32 (1..4294967295)
```



```
IEEE8021MstIdentifier ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS      current
    DESCRIPTION
        "In an MSTP Bridge, an MSTID, i.e., a value used to identify
        a spanning tree (or MST) instance.  In the PBB-TE environment
        the value 4094 is used to identify VIDs managed by the PBB-TE
        procedures."
    SYNTAX      Unsigned32 (1..4094)

IEEE8021ServiceSelectorType ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
       "A value that represents a type (and thereby the format)
        of a IEEE8021ServiceSelectorValue.  The value can be one of
        the following:

        ieeeReserved(0)   Reserved for definition by IEEE 802.1
                          recommend to not use zero unless
                          absolutely needed.
        vlanId(1)         12-Bit identifier as described in IEEE802.1Q.
        isid(2)           24-Bit identifier as described in IEEE802.1ah.
        tesid(3)          32 Bit identifier as described below.
        segid(4)          32 Bit identifier as described below.
        ieeeReserved(xx)  Reserved for definition by IEEE 802.1
                          xx values can be [5..7].

        To support future extensions, the IEEE8021ServiceSelectorType
        textual convention SHOULD NOT be sub-typed in object type
        definitions.  It MAY be sub-typed in compliance statements in
        order to require only a subset of these address types for a
        compliant implementation.

        The tesid is used as a service selector for MAs that are present
        in bridges that implement PBB-TE functionality.  A selector of
        this type is interpreted as a 32 bit unsigned value of type
        IEEE8021PbbTeTSidId.  This type is used to index the
        Ieee8021PbbTeTeSidTable to find the ESPs which comprise the TE
        Service Instance named by this TE-SID value.

        The segid is used as a service selector for MAs that are present
        in bridges that implement IPS functionality.  A selector of
        this type is interpreted as a 32 bit unsigned value of type
        IEEE8021TeipsSegid.  This type is used to index the
        Ieee8021TeipsSegTable to find the SMPs which comprise the
        Infrastructure Segment named by this segid value.

        Implementations MUST ensure that IEEE8021ServiceSelectorType
        objects and any dependent objects (e.g.,
        IEEE8021ServiceSelectorValue objects) are consistent.  An
        inconsistentValue error MUST be generated if an attempt to
        change an IEEE8021ServiceSelectorType object would, for
```

```
        example, lead to an undefined IEEE8021ServiceSelectorValue
value."
    SYNTAX      INTEGER {
                    vlanId(1),
                    isid(2),
                    tesid(3),
                    segid(4)
                }

IEEE8021ServiceSelectorValueOrNone ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS       current
    DESCRIPTION
        "An integer that uniquely identifies a generic MAC service,
         or none.  Examples of service selectors are a VLAN-ID
         (IEEE 802.1Q) and an I-SID (IEEE 802.1ah).

         An IEEE8021ServiceSelectorValueOrNone value is always
         interpreted within the context of an
         IEEE8021ServiceSelectorType value.  Every usage of the
         IEEE8021ServiceSelectorValueOrNone textual convention is
         required to specify the IEEE8021ServiceSelectorType object
         that provides the context.  It is suggested that the
         IEEE8021ServiceSelectorType object be logically registered
         before the object(s) that use the
         IEEE8021ServiceSelectorValueOrNone textual convention, if
         they appear in the same logical row.

         The value of an IEEE8021ServiceSelectorValueOrNone object
         must always be consistent with the value of the associated
         IEEE8021ServiceSelectorType object.  Attempts to set an
         IEEE8021ServiceSelectorValueOrNone object to a value
         inconsistent with the associated
         IEEE8021ServiceSelectorType must fail with an
         inconsistentValue error.

         The special value of zero is used to indicate that no
         service selector is present or used.  This can be used in
         any situation where an object or a table entry MUST either
         refer to a specific service, or not make a selection.

         Note that a MIB object that is defined using this
         TEXTUAL-CONVENTION SHOULD clarify the meaning of
         'no service' (i.e., the special value 0), as well as the
         maximum value (i.e., 4094, for a VLAN ID)."
    SYNTAX       Unsigned32 (0 | 1..4294967295)

IEEE8021ServiceSelectorValue ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS       current
    DESCRIPTION
        "An integer that uniquely identifies a generic MAC service.
         Examples of service selectors are a VLAN-ID (IEEE 802.1Q)
         and an I-SID (IEEE 802.1ah).
```



```
        An IEEE8021ServiceSelectorValue value is always interpreted
        within the context of an IEEE8021ServiceSelectorType value.
        Every usage of the IEEE8021ServiceSelectorValue textual
        convention is required to specify the
        IEEE8021ServiceSelectorType object that provides the context.
        It is suggested that the IEEE8021ServiceSelectorType object
        be logically registered before the object(s) that use the
        IEEE8021ServiceSelectorValue textual convention, if they
        appear in the same logical row.

        The value of an IEEE8021ServiceSelectorValue object must
        always be consistent with the value of the associated
        IEEE8021ServiceSelectorType object.  Attempts to set an
        IEEE8021ServiceSelectorValue object to a value inconsistent
        with the associated IEEE8021ServiceSelectorType must fail
        with an inconsistentValue error.

        Note that a MIB object that is defined using this
        TEXTUAL-CONVENTION SHOULD clarify the
        maximum value (i.e., 4094, for a VLAN ID).”
    SYNTAX       Unsigned32 (1..4294967295)

IEEE8021PortAcceptableFrameTypes ::= TEXTUAL-CONVENTION
    STATUS      current
    DESCRIPTION
        “Acceptable frame types on a port.”
    REFERENCE   “12.10.1.3, 12.13.3.3, 12.13.3.4”
    SYNTAX      INTEGER {
                    admitAll(1),
                    admitUntaggedAndPriority(2),
                    admitTagged(3)
                }

IEEE8021PriorityValue ::= TEXTUAL-CONVENTION
    DISPLAY-HINT “d”
    STATUS      current
    DESCRIPTION
        “An 802.1Q user priority value.”
   REFERENCE   “12.13.3.3”
    SYNTAX      Unsigned32 (0..7)

IEEE8021PbbTeProtectionGroupId ::= TEXTUAL-CONVENTION
    DISPLAY-HINT “d”
    STATUS       current
    DESCRIPTION
        “The PbbTeProtectionGroupId identifier is used to distinguish
         protection group instances present in the B Component of
         an IB-BEB.”
    REFERENCE “12.19.2”
    SYNTAX       Unsigned32 (1..429467295)

IEEE8021PbbTeEsp ::= TEXTUAL-CONVENTION
    STATUS current
```

```
    DESCRIPTION
       "This textual convention is used to represent the logical
        components that comprise the 3-tuple that identifies an
        Ethernet Switched Path.  The 3-tuple consists of a
        destination MAC address, a source MAC address and a VID.
        Bytes (1..6) of this textual convention contain the
        ESP-MAC-DA, bytes (7..12) contain the ESP-MAC-SA, and bytes
        (13..14) contain the ESP-VID."
    REFERENCE "802.1Qay 3.2"
    SYNTAX OCTET STRING ( SIZE(14))

IEEE8021PbbTeTSidId ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS current
    DESCRIPTION
       "This textual convention is used to represent an identifier
        that refers to a TE Service Instance.  Note that, internally
        a TE-SID is implementation dependent.  This textual convention
        defines the external representation of TE-SID values."
    REFERENCE
        "802.1Qay 3.11"
    SYNTAX  Unsigned32 (1..42947295)

IEEE8021PbbTeProtectionGroupConfigAdmin ::= TEXTUAL-CONVENTION
    STATUS current
    DESCRIPTION
        "This textual convention is used to represent administrative
        commands that can be issued to a protection group.  The value
        noAdmin(1) is used to indicate that no administrative action
        is to be performed."
    REFERENCE "26.10.3.3.5
               26.10.3.3.6
               26.10.3.3.7
               12.19.2.3.2"
    SYNTAX    INTEGER {
                 clear(1),
                 lockOutProtection(2),
                 forceSwitch(3),
                 manualSwitchToProtection(4),
                 manualSwitchToWorking(5)
              }

IEEE8021PbbTeProtectionGroupActiveRequests ::= TEXTUAL-CONVENTION
   STATUS current
   DESCRIPTION
       "This textual convention is used to represent the status of
        active requests within a protection group."
    REFERENCE
       "12.19.2.1.3 d)"
   SYNTAX   INTEGER {
                noRequest(1),
                loP(2),
                fs(3),
                pSFH(4),
```



```
                wSFH(5),
                manualSwitchToProtection(6),
                manualSwitchToWorking(7)
            }

IEEE8021TeipsIpgid ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS       current
    DESCRIPTION
        "The TEIPS IPG identifier is used to distinguish
         IPG instances present in a PBB."
    REFERENCE "12.24.1.1.3 a)"
    SYNTAX       Unsigned32 (1..429467295)

IEEE8021TeipsSegid ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "d"
    STATUS current
    DESCRIPTION
       "This textual convention is used to represent an
        identifier that refers to an Infrastructure Segment.
        Note that, internally a SEG-ID implementation
        dependent.  This textual convention defines the
        external representation of SEG-ID values."
    REFERENCE
        "26.11.1"
    SYNTAX  Unsigned32 (1..42947295)

IEEE8021TeipsSmpid ::= TEXTUAL-CONVENTION
    STATUS current
    DESCRIPTION
       "This textual convention is used to represent the logical
        components that comprise the 3-tuple that identifies a
        Segment Monitoring Path (SMP).  The 3-tuple consists of a
        destination MAC address, a source MAC address and a VID.
        Bytes (1..6) of this textual convention contain the
        SMP-MAC-DA, bytes (7..12) contain the SMP-MAC-SA, and bytes
        (13..14) contain the SMP-VID."
    REFERENCE "26.11.1"
    SYNTAX OCTET STRING ( SIZE(14))

IEEE8021TeipsIpgConfigAdmin ::= TEXTUAL-CONVENTION
    STATUS current
    DESCRIPTION
        "This textual convention is used to represent administrative
        commands that can be issued to an IPG.  The value
        clear(1) is used to indicate that no administrative action
        is to be performed."
    REFERENCE "12.24.2.1.3 h)"
    SYNTAX    INTEGER {
                clear(1),
                lockOutProtection(2),
                forceSwitch(3),
                manualSwitchToProtection(4),
                manualSwitchToWorking(5)
```

```
            }

IEEE8021TeipsIpgConfigActiveRequests ::= TEXTUAL-CONVENTION
   STATUS current
   DESCRIPTION
       "This textual convention is used to represent the status of
        active requests within an IPG."
    REFERENCE
       "12.24.2.1.3 d)"
   SYNTAX   INTEGER {
               noRequest(1),
               loP(2),
               fs(3),
               pSFH(4),
               wSFH(5),
               manualSwitchToProtection(6),
               manualSwitchToWorking(7)
           }

END
```

Insert the following subclause, 17.7.18, after 17.7.17:

17.7.18 Definitions for the IEEE8021-TEIPS MIB module

```
IEEE8021-TEIPS-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    NOTIFICATION-TYPE,
    OBJECT-TYPE,
    Unsigned32
        FROM SNMPv2-SMI
    RowStatus,
    StorageType,
    TruthValue
        FROM SNMPv2-TC
    ieee802dot1mibs,
    IEEE8021BridgePortNumber,
    IEEE8021TeipsIpgConfigActiveRequests,
    IEEE8021TeipsIpgid,
    IEEE8021TeipsIpgConfigAdmin,
    IEEE8021PbbTeTSidId
        FROM IEEE8021-TC-MIB
    ieee8021BridgeBaseComponentId
        FROM IEEE8021-BRIDGE-MIB
    MODULE-COMPLIANCE,
    NOTIFICATION-GROUP,
    OBJECT-GROUP
        FROM SNMPv2-CONF;

ieee8021TeipsMib MODULE-IDENTITY
    LAST-UPDATED "201108170000Z" -- (YYYYMMDDHHMM Zulu=GMT)
    ORGANIZATION "IEEE 802.1 Working Group"
    CONTACT-INFO
```



```
        "WG-URL:   http://grouper.ieee.org/groups/802/1/index.html
         WG-EMail: stds-802-1@ieee.org
         Contact:  Bob Sultan
                   c/o Tony Jeffree, IEEE 802.1 Working Group Chair
         Postal:   IEEE Standards Board
                   445 Hoes Lane
                   P.O. Box 1331
                   Piscataway, NJ 08855-1331
                   USA
         E-mail:   tony@jeffree.co.uk
        "

    DESCRIPTION
       "Copyright (C) IEEE.  All Rights Reserved
        This MIB module is part of IEEE 802.1Q;
        See the IEEE 802.1Q standard for full legal notices.

        Unless otherwise indicated, the references in this
        MIB module are to IEEE 802.1Q-2011 as amended by
        the following standards:
              IEEE 802.1az
              IEEE 802.1bb
              IEEE 802.1bc
              IEEE 802.1be"

    REVISION "201108170000Z" -- (YYYYMMDDHHMM Zulu=GMT)

    DESCRIPTION
      "Version 1 of the TEIPS MIB module based upon IEEE 802.1Qbf"
    ::= { iso(1) org(3) ieee(111)
         standards-association-numbers-series-standards (2)
         lan-man-stds (802) ieee802dot1 (1) ieee802dot1mibs (1) 24 }

ieee8021TeipsNotifications OBJECT IDENTIFIER ::= { ieee8021TeipsMib 0 }
ieee8021TeipsObjects       OBJECT IDENTIFIER ::= { ieee8021TeipsMib 1 }
ieee8021TeipsConformance   OBJECT IDENTIFIER ::= { ieee8021TeipsMib 2 }

--
-- 802.1Qbf MIB Objects
--

-- ============================================================
-- the ieee8021TeipsIpgTable
-- ============================================================
ieee8021TeipsIpgTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF Ieee8021TeipsIpgEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The IPG table.  Each entry in this table corresponds to an
        Infrastructure Protection Group (IPG) associated with a PBB
        supporting Infrastructure Protection Switching (IPS)."
    REFERENCE
        "12.20.1"
```

```
    ::= { ieee8021TeipsObjects 1 }

ieee8021TeipsIpgEntry OBJECT-TYPE
    SYNTAX Ieee8021TeipsIpgEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "The IPG table entry."
    INDEX {ieee8021BridgeBaseComponentId,
           ieee8021TeipsIpgid }
    ::= { ieee8021TeipsIpgTable 1 }

Ieee8021TeipsIpgEntry ::=
    SEQUENCE {
        ieee8021TeipsIpgid                    IEEE8021TeipsIpgid,
        ieee8021TeipsIpgWorkingMA             Unsigned32,
        ieee8021TeipsIpgProtectionMA          Unsigned32,
        ieee8021TeipsIpgWorkingPortNumber     IEEE8021BridgePortNumber,
        ieee8021TeipsIpgProtectionPortNumber  IEEE8021BridgePortNumber,
        ieee8021TeipsIpgStorageType           StorageType,
        ieee8021TeipsIpgRowStatus             RowStatus
    }

ieee8021TeipsIpgid OBJECT-TYPE
    SYNTAX      IEEE8021TeipsIpgid
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
         "Uniquely identifies an IPG within the PBB."
    REFERENCE
        "12.20.1.1.3 a"
    ::= { ieee8021TeipsIpgEntry 1 }


ieee8021TeipsIpgWorkingMA OBJECT-TYPE
    SYNTAX     Unsigned32
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
       "Identifies the Segment MA that corresponds to
        the IPG's working entity.  The MA index in
        this column must hold a value that is the
        value of dot1agCfmStackMaIndex column for
        some entry in the dot1agCfmStackTable before
        the RowStatus for this row can be set to
        Active.  Furthermore, this column may not be
        modified when the RowStatus for this row is
        Active."
    REFERENCE
        "12.20.1.1.3 b)"
::= { ieee8021TeipsIpgEntry 2 }

ieee8021TeipsIpgProtectionMA OBJECT-TYPE
    SYNTAX     Unsigned32
```



```
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
       "Identifies the Segment MA that corresponds to the
        IPG's protection entity.  The MA index in this
        column must hold a value that is the value of
        dot1agCfmStackMaIndex column for some entry in
        the dot1agCfmStackTable before the RowStatus
        for this row can be set to Active.  Furthermore,
        this column may not be modified when the
        RowStatus for this row is Active."
    REFERENCE
        "12.20.1.1.3 c)"
::= { ieee8021TeipsIpgEntry 3 }

ieee8021TeipsIpgWorkingPortNumber OBJECT-TYPE
    SYNTAX     IEEE8021BridgePortNumber
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
       "Identifies the local Port associated with the
        IPG Working Segment."
    REFERENCE
        "12.20.2.1.3 b)"
::= { ieee8021TeipsIpgEntry 4 }

ieee8021TeipsIpgProtectionPortNumber OBJECT-TYPE
    SYNTAX     IEEE8021BridgePortNumber
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
       "Identifies the local Port associated with the
        IPG Protection Segment."
    REFERENCE
        "12.20.2.1.3 c)"
::= { ieee8021TeipsIpgEntry 5 }

ieee8021TeipsIpgStorageType OBJECT-TYPE
    SYNTAX     StorageType
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
       "This object indicates the persistence of this
        entry. All read-create columns must be
        writable if this column is set to permanent."
    DEFVAL { nonVolatile }
    ::= { ieee8021TeipsIpgEntry 6 }

ieee8021TeipsIpgRowStatus OBJECT-TYPE
    SYNTAX     RowStatus
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
       "The status of this row.
```

```
        The writable columns in a row cannot be
        changed if the row is active.  The
        TeipsIpgWorkingMA and TeipsIpgProtectionMA
        columns must be specified before the row
        can be activated."
    REFERENCE
        "12.20.1.2"
    ::= { ieee8021TeipsIpgEntry 7 }

-- ============================================================
-- the ieee8021TeipsTesiTable
-- ============================================================
ieee8021TeipsTesiTable OBJECT-TYPE
    SYNTAX     SEQUENCE OF Ieee8021TeipsTesiEntry
    MAX-ACCESS not-accessible
    STATUS     current
    DESCRIPTION
        "The IPG TE-SID table contains identifies
         the TE service instances associated with
         an IPG."
    REFERENCE
        "12.20.2.1.3 e)"
    ::= { ieee8021TeipsObjects 2 }

ieee8021TeipsTesiEntry  OBJECT-TYPE
    SYNTAX     Ieee8021TeipsTesiEntry
    MAX-ACCESS not-accessible
    STATUS     current
    DESCRIPTION
        "The TE-IPS TESI entry.  Each entry identifies
         a TESI associated with an IPG."
    INDEX { ieee8021TeipsIpgid,
      ieee8021TeipsTesiIndex }
    ::= { ieee8021TeipsTesiTable 1 }

Ieee8021TeipsTesiEntry ::=
    SEQUENCE {
        ieee8021TeipsTesiIndex       Unsigned32,
        ieee8021TeipsTesiId          IEEE8021PbbTeTSidId,
        ieee8021TeipsTesiStorageType StorageType,
        ieee8021TeipsTesiRowStatus   RowStatus
    }

ieee8021TeipsTesiIndex OBJECT-TYPE
    SYNTAX     Unsigned32 (1..4294967295)
    MAX-ACCESS not-accessible
    STATUS     current
    DESCRIPTION
        "This is an identifier, of local signifigance to a
         particular PBB-TE TE-SID associated with an IPG."
    REFERENCE
        "12.20.2.1.3 e"
    ::= { ieee8021TeipsTesiEntry 1 }
```



```
ieee8021TeipsTesiId OBJECT-TYPE
    SYNTAX     IEEE8021PbbTeTSidId
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
        "This column holds the TESI identifier corresponding
         to a TE service instance associated with an IPG."
    REFERENCE
        "12.20.2.1.3 e"
    ::= { ieee8021TeipsTesiEntry 2 }

ieee8021TeipsTesiStorageType OBJECT-TYPE
    SYNTAX     StorageType
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
       "This object indicates the persistence of this
        entry. All read-create columns must be
        writable for permanent rows."
    DEFVAL { nonVolatile }
    ::= { ieee8021TeipsTesiEntry 3 }

ieee8021TeipsTesiRowStatus OBJECT-TYPE
    SYNTAX     RowStatus
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
        "This column holds the status for this row.
         When the status is active, no columns of
         this table may be modified.  All columns
         must have a valid value before the row
         can be activated."
    ::= { ieee8021TeipsTesiEntry 4 }

-- ============================================================
-- the ieee8021TeipsCandidatePsTable
-- ============================================================
ieee8021TeipsCandidatePsTable OBJECT-TYPE
    SYNTAX     SEQUENCE OF Ieee8021TeipsCandidatePsEntry
    MAX-ACCESS not-accessible
    STATUS     current
    DESCRIPTION
        "The Candidate PS table lists, in priority order,
         from highest priority to lowest priority, the
         Maintenance Associations corresponding to
         candidate Protection Segments associated with
         an IPG."
    REFERENCE
        "12.20.2.1.3 d)"
    ::= { ieee8021TeipsObjects 3 }

ieee8021TeipsCandidatePsEntry  OBJECT-TYPE
    SYNTAX     Ieee8021TeipsCandidatePsEntry
    MAX-ACCESS not-accessible
```

```
    STATUS     current
    DESCRIPTION
        "A Candidate PS entry.  Each entry identifies a
         candidate Protection Segment associated with an IPG."
    INDEX { ieee8021TeipsIpgid,
      ieee8021TeipsCandidatePsIndex }
    ::= { ieee8021TeipsCandidatePsTable 1 }

Ieee8021TeipsCandidatePsEntry ::=
    SEQUENCE {
        ieee8021TeipsCandidatePsIndex Unsigned32,
        ieee8021TeipsCandidatePsMA    Unsigned32,
        ieee8021TeipsCandidatePsPort  IEEE8021BridgePortNumber,
        ieee8021TeipsCandidatePsOper        TruthValue,
        ieee8021TeipsCandidatePsStorageType StorageType,
        ieee8021TeipsCandidatePsRowStatus   RowStatus
    }

ieee8021TeipsCandidatePsIndex OBJECT-TYPE
    SYNTAX     Unsigned32 (1..4294967295)
    MAX-ACCESS not-accessible
    STATUS     current
    DESCRIPTION
        "This is an identifier, of local signifigance
         to a particular candidate Protection Segment
         associated with an IPG."
    REFERENCE
        "12.20.2.1.3 d)"
    ::= { ieee8021TeipsCandidatePsEntry 1 }

ieee8021TeipsCandidatePsMA OBJECT-TYPE
    SYNTAX     Unsigned32
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
        "This column holds the candidate Protection
         Segment MA corresponding to a candidate
         Protection Segment associated with an IPG."
    REFERENCE
        "12.20.2.1.3 d)"
    ::= { ieee8021TeipsCandidatePsEntry 2 }

ieee8021TeipsCandidatePsPort OBJECT-TYPE
    SYNTAX     IEEE8021BridgePortNumber
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "This column holds the Port Number
         corresponding to the candidate Protection
         Segment associated with an IPG."
    REFERENCE
        "12.20.2.1.3 d)"
    ::= { ieee8021TeipsCandidatePsEntry 3 }
```



```
ieee8021TeipsCandidatePsOper OBJECT-TYPE
    SYNTAX     TruthValue
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "This column indicates whether or not
         the candidate Protection Segment is
         operational."
    REFERENCE
        "12.20.2.1.3 d)"
    ::= { ieee8021TeipsCandidatePsEntry 4 }

ieee8021TeipsCandidatePsStorageType OBJECT-TYPE
    SYNTAX     StorageType
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
       "This object indicates the persistence
        of this entry. All read-create
        columns must be writable for permanent rows."
    DEFVAL { nonVolatile }
    ::= { ieee8021TeipsCandidatePsEntry 5 }

ieee8021TeipsCandidatePsRowStatus OBJECT-TYPE
    SYNTAX     RowStatus
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
        "This column holds the status for this row.
         When the status is active, no columns
         of this table may be modified.  All
         columns must have a valid value before the row
         can be activated."
    ::= { ieee8021TeipsCandidatePsEntry 6 }

-- ============================================================
-- the ieee8021TeipsIpgConfigTable
-- ============================================================
ieee8021TeipsIpgConfigTable OBJECT-TYPE
    SYNTAX     SEQUENCE OF Ieee8021TeipsIpgConfigEntry
    MAX-ACCESS not-accessible
    STATUS     current
    DESCRIPTION
        "The PBB-TE IPS IPG config table contains
         configuration and status information for
         each IPG configured in the system.
         Entries in this table are created implicitly
         by the creation of entries in the
         ieee8021TeipsIpgTable."
     REFERENCE
         "12.20.2.1.3 f,g,h,i,j,k)"
     ::= { ieee8021TeipsObjects 4 }

ieee8021TeipsIpgConfigEntry OBJECT-TYPE
```

```
    SYNTAX     Ieee8021TeipsIpgConfigEntry
    MAX-ACCESS not-accessible
    STATUS     current
    DESCRIPTION
        "The IPG confguration table entry.  Rows are
         created in this table implicitly when a row
         is added to the ieee8021TeipsIpgTable."
    INDEX { ieee8021BridgeBaseComponentId,
            ieee8021TeipsIpgid }
    ::= { ieee8021TeipsIpgConfigTable 1 }

Ieee8021TeipsIpgConfigEntry ::=
    SEQUENCE {
        ieee8021TeipsIpgConfigState INTEGER,
        ieee8021TeipsIpgConfigCommandStatus
            IEEE8021TeipsIpgConfigAdmin,
        ieee8021TeipsIpgConfigCommandLast
            IEEE8021TeipsIpgConfigAdmin,
        ieee8021TeipsIpgConfigCommandAdmin
            IEEE8021TeipsIpgConfigAdmin,
        ieee8021TeipsIpgConfigActiveRequests
            IEEE8021TeipsIpgConfigActiveRequests,
        ieee8021TeipsIpgConfigWTR          Unsigned32,
        ieee8021TeipsIpgConfigHoldOff      Unsigned32,
        ieee8021TeipsIpgM1ConfigState      INTEGER,
        ieee8021TeipsIpgConfigMWTR         Unsigned32,
        ieee8021TeipsIpgConfigNotifyEnable TruthValue,
        ieee8021TeipsIpgConfigStorageType  StorageType
    }
ieee8021TeipsIpgConfigState OBJECT-TYPE
    SYNTAX   INTEGER {
               workingSegment(1),
               protectionSegment(2),
               waitToRestore(3),
               protAdmin(4)
             }
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "This column indicates the current state of the
         protection switching state machine for an IPG.
         The value can be one of the following:

        workingSegment(1)    The protection switching state machine
                             is in the WORKING_PATH state.
        protectionSegment(2) The protection switching state machine
                             is in the PROTECTION_PATH state.
        waitToRestore(3)     The protection switching state machine
                             is in the WTR state.
        protAdmin(4)         The protection switching state machine
                             is in the PROT_ADMIN state."

    REFERENCE "12.20.2.1.3 f)"
    ::= { ieee8021TeipsIpgConfigEntry 1 }
```



```
ieee8021TeipsIpgConfigCommandStatus OBJECT-TYPE
    SYNTAX     IEEE8021TeipsIpgConfigAdmin
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "This column indicates the status of
         administrative commands within the
         protection group.  It reflects the current
         operational administrative command being
         acted upon by the IPG."
     REFERENCE "12.20.2.1.3 f)"
    ::= { ieee8021TeipsIpgConfigEntry 2 }

ieee8021TeipsIpgConfigCommandLast OBJECT-TYPE
    SYNTAX     IEEE8021TeipsIpgConfigAdmin
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "This column indicates the last attempted administrative
         command applied to the IPG.  It is changed
         whenever a write is made to the CommandAdmin column of
         this table and is essentially record of the last attempted
         administrative operation."
     REFERENCE "12.20.2.1.3 f)"
    ::= { ieee8021TeipsIpgConfigEntry 3 }

ieee8021TeipsIpgConfigCommandAdmin OBJECT-TYPE
    SYNTAX     IEEE8021TeipsIpgConfigAdmin
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
       "This column is used by the operator to request
        that the IPG state machine perform some
        administrative operation.  The operator requests
        a command by writing the command value to this
        column.  The state machine indicates the command
        that it is performing by setting the value of the
        CommandStatus column of this table.  This column
        always reads back as clear(1)."
     REFERENCE "12.20.2.1.3 f"
     DEFVAL { clear }
    ::= { ieee8021TeipsIpgConfigEntry 4 }

ieee8021TeipsIpgConfigActiveRequests OBJECT-TYPE
    SYNTAX     IEEE8021TeipsIpgConfigActiveRequests
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "This column shows the status of active requests
         associated with the IPG."
    REFERENCE "12.20.2.1.3 f)"
    ::= { ieee8021TeipsIpgConfigEntry 5 }
```

```
ieee8021TeipsIpgConfigWTR OBJECT-TYPE
    SYNTAX     Unsigned32 ( 0 | 5..12 )
    UNITS      "minutes"
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
        "This column is used to configure the
         wait-to-restore timer for the IPG operation.
         The timer may be configured in steps of 1 minute
         between 5 and 12 minutes, the default being 5.
         Additionally, the value 0 is used to indicate
         that the IPG is to operate non-revertively.  The
         value 0 is not permitted if the IPG is configured
         for M:1 IPS operation."
    REFERENCE "12.20.2.1.3 h)"
    DEFVAL { 5 }
    ::= { ieee8021TeipsIpgConfigEntry 6 }

ieee8021TeipsIpgConfigHoldOff OBJECT-TYPE
    SYNTAX     Unsigned32( 0..100 )
    UNITS      "deciseconds"
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
       "This column is used to configure the hold off
        timer.  The purpose is to allow IPS to fix the problem
        before a higher-layer mechanism, such as PBB-TE TESI
        protection, is invoked or to allow an inner IPG to fix
        the problem before IPS is invoked by the outer IPG when
        IPGs are nested.  The hold off timer has a period of
        from 0 to 10 seconds, the default being 0, with a 100ms
        granularity."
    REFERENCE "12.20.2.1.3 i)"
    DEFVAL { 0 }
    ::= { ieee8021TeipsIpgConfigEntry 7 }

ieee8021TeipsIpgM1ConfigState OBJECT-TYPE
    SYNTAX   INTEGER {
               psAssigned(1),
               segmentOk(2),
               segmentFailed(3),
               assignNewPs(4),
               revertToBetterPs(5)
             }
    MAX-ACCESS read-only
    STATUS     current
    DESCRIPTION
        "This column indicates the current state of the M:1 protection
         switching state machine for an IPG if M:1 IPS is supported.
         The value can be one of the following:

        psAssigned(1)        The protection switching state machine
                             is in the PS_ASSIGNED state.
        segmentOk(2)         The protection switching state machine
```



```
                              is in the SEGMENT_OK state.
        segmentFailed(3)      The protection switching state machine
                              is in the SEGMENT_FAILED state.
        assignNewPs(4)        The protection switching state machine
                              is in the ASSIGN_NEW_PS state.
        revertToBetterPs(5)   The protection switching state machine
                              is in the REVERT_T0_BETTER_PS state."

    REFERENCE "12.20.2.1.3 j)"
    ::= { ieee8021TeipsIpgConfigEntry 8 }

ieee8021TeipsIpgConfigMWTR OBJECT-TYPE
    SYNTAX     Unsigned32 ( 0 | 5..12 )
    UNITS      "minutes"
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
        "This column is used to configure the M:1 wait-to-restore
         timer for the IPG operation if M:1 protection is
         supported.  The timer may be configured in steps of
         1 minute between 5 and 12 minutes, the default being 5.
         Additionally, the value 0 is used to indicate that the
         IPG is to operate non-revertively."
    REFERENCE "12.20.2.1.3 k)"
    DEFVAL { 5 }
    ::= { ieee8021TeipsIpgConfigEntry 9 }


ieee8021TeipsIpgConfigNotifyEnable OBJECT-TYPE
    SYNTAX     TruthValue
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
        "This column is used to enable or disable transmission
         of ieee8021TeipsIpgAdminFailure notifications.
         These notifications are generated whenever an
         administrative command cannot be performed by the IPG."
    DEFVAL { false }
    ::= { ieee8021TeipsIpgConfigEntry 10 }

ieee8021TeipsIpgConfigStorageType OBJECT-TYPE
    SYNTAX     StorageType
    MAX-ACCESS read-create
    STATUS     current
    DESCRIPTION
       "This object indicates the persistence of this entry. For
        permanent objects the ieee8021TeipsIpgConfigCommandAdmin
        column must be writable."

    DEFVAL { nonVolatile }
    ::= { ieee8021TeipsIpgConfigEntry 11 }


-- ****************************************************************
```

```
-- NOTIFICATIONS (TRAPS)
-- These notifications will be sent to the management entity
-- whenever an IPG admin command cannot be performed
-- ****************************************************************

ieee8021TeipsIpgAdminFailure NOTIFICATION-TYPE
    OBJECTS {
        ieee8021TeipsIpgConfigState,
        ieee8021TeipsIpgConfigCommandStatus,
        ieee8021TeipsIpgConfigCommandLast
    }
    STATUS  current
    DESCRIPTION
        "An IPG generates this notification whenever
         an adminisistrative command cannot be
         executed by the IPS state machine.  For
         example, when a requested  manual switch
         cannot be performed because of a signal
         failure condition.

         The management entity receiving the
         notification can identify
         the system from the network source
         address of the notification and can
         identify the IPG by the indices of
         the OID of the ieee8021TeipsIpgConfigState
         variable in the notification:

         ieee8021BridgeBaseComponentId - Identifies
         the  component on the bridge where the
         protection group is configured.

         ieee8021TeipsIpgid - The ID of the protection group.
        "
    ::= { ieee8021TeipsNotifications 1 }

--
-- MIB Module Compliance Statements
--

ieee8021TeipsCompliances OBJECT IDENTIFIER ::= {
ieee8021TeipsConformance 1 }
ieee8021TeipsGroups     OBJECT IDENTIFIER ::= { ieee8021TeipsConformance
2 }

--
-- Units of Conformance

ieee8021TeipsIpgGroup OBJECT-GROUP
    OBJECTS {
        ieee8021TeipsIpgWorkingMA,
        ieee8021TeipsIpgProtectionMA,
        ieee8021TeipsIpgWorkingPortNumber,
        ieee8021TeipsIpgProtectionPortNumber,
```

```
        ieee8021TeipsIpgStorageType,
        ieee8021TeipsIpgRowStatus
    }
    STATUS  current
    DESCRIPTION
        "Objects for the IPG group."
    ::= { ieee8021TeipsGroups 1 }

ieee8021TeipsCandidatePsGroup OBJECT-GROUP
    OBJECTS {
        ieee8021TeipsCandidatePsMA,
        ieee8021TeipsCandidatePsPort,
        ieee8021TeipsCandidatePsOper,
        ieee8021TeipsCandidatePsStorageType,
        ieee8021TeipsCandidatePsRowStatus
    }
    STATUS  current
    DESCRIPTION
        "Objects for the Candidate PS group."
    ::= { ieee8021TeipsGroups 2 }

ieee8021TeipsIpgTesiGroup OBJECT-GROUP
    OBJECTS {
        ieee8021TeipsTesiId,
        ieee8021TeipsTesiStorageType,
        ieee8021TeipsTesiRowStatus
    }
    STATUS  current
    DESCRIPTION
        "Objects for the IPG Tuple group."
    ::= { ieee8021TeipsGroups 3 }

ieee8021TeipsIpgConfigManGroup OBJECT-GROUP
    OBJECTS {
        ieee8021TeipsIpgConfigState,
        ieee8021TeipsIpgConfigCommandStatus,
        ieee8021TeipsIpgConfigCommandLast,
        ieee8021TeipsIpgConfigCommandAdmin,
        ieee8021TeipsIpgConfigActiveRequests,
        ieee8021TeipsIpgConfigNotifyEnable,
        ieee8021TeipsIpgConfigStorageType
    }
    STATUS current
    DESCRIPTION
        "Mandatory objects for the TeipsConfiguration group."
    ::= { ieee8021TeipsGroups 4 }

ieee8021TeipsIpgConfigOptGroup OBJECT-GROUP
    OBJECTS {
        ieee8021TeipsIpgConfigWTR,
        ieee8021TeipsIpgConfigMWTR,
        ieee8021TeipsIpgM1ConfigState,
        ieee8021TeipsIpgConfigHoldOff
    }
```

```
    STATUS current
    DESCRIPTION
        "Optional 0bjects for the TeipsConfiguration group."
    ::= { ieee8021TeipsGroups 5 }

ieee8021TeipsNotificationsGroup NOTIFICATION-GROUP
    NOTIFICATIONS {
       ieee8021TeipsIpgAdminFailure
    }
    STATUS    current
    DESCRIPTION
        "Objects for the notifications group."
    ::= { ieee8021TeipsGroups 6 }

ieee8021TeipsCompliance MODULE-COMPLIANCE
    STATUS    current
    DESCRIPTION
        "The compliance statement for support
         of the TEIPS MIB module."
    MODULE
        MANDATORY-GROUPS {
            ieee8021TeipsIpgGroup,
            ieee8021TeipsIpgTesiGroup,
            ieee8021TeipsIpgConfigManGroup,
            ieee8021TeipsNotificationsGroup
        }
        GROUP ieee8021TeipsIpgConfigOptGroup
        DESCRIPTION
           "This group allows implmementation to
            optionally change the WaitToRestore,
            M:1 WaitToRestore, and HoldOff timers
            for IPGs."

        GROUP ieee8021TeipsCandidatePsGroup
        DESCRIPTION
           "This group allows implmementation to
            optionally list candidate Protection
            Segments when M:1 IPS is deployed."


    OBJECT ieee8021TeipsIpgConfigWTR
    MIN-ACCESS not-accessible
    DESCRIPTION "This object is optional."

    OBJECT ieee8021TeipsIpgConfigHoldOff
    MIN-ACCESS not-accessible
    DESCRIPTION"This object is optional."

    OBJECT ieee8021TeipsIpgConfigMWTR
    MIN-ACCESS not-accessible
    DESCRIPTION "This object is optional."

    OBJECT ieee8021TeipsIpgRowStatus
      SYNTAX       RowStatus { active(1), notInService(2) }
```

```
      WRITE-SYNTAX RowStatus { notInService(2), createAndGo(4),
                               destroy(6) }
      DESCRIPTION "Support for createAndWait is not required."

    OBJECT ieee8021TeipsTesiRowStatus
      SYNTAX       RowStatus { active(1), notInService(2) }
      WRITE-SYNTAX RowStatus { notInService(2), createAndGo(4),
                               destroy(6) }
      DESCRIPTION "Support for createAndWait is not required."

    ::= { ieee8021TeipsCompliances 1 }

END
```

19. Connectivity Fault Management Entity operation

19.2 Maintenance association End Point

19.2.1 MEP identification

Change the second through fourth paragraphs of 19.2.1 as shown:

The MEP is identified for data forwarding purposes by:

c) A set of VIDs, including a Primary VID, inherited from the MA.; or
d) An I-SID in the case of a backbone service instance MA; or
e) A set of 3-tuples <~~MAC-~~ESP-DA, ~~MAC-~~ESP-SA, ESP-VID> inherited from the MA- when the MA is associated with a TESI; or
f) A SEG-ID inherited from the MA when the MA is associated with an Infrastructure Segment.

From the MA, the MEP inherits a Maintenance Domain, and from this it inherits:

g) ~~f)~~ A Maintenance Domain Level (MD Level), inherited from its Maintenance Domain; and
h) ~~g) A Primary VID, or an I-SID in the case of a Backbone Service Instance, or a set of CBP MACaddresses and a set of ESP-VIDs in the case of a TESI, inherited from its MA.~~ One of the following inherited from its MA:
    1) A Primary VID; or
    2) an I-SID in the case of a Backbone Service Instance; or
    3) a TE-SID in the case of a TESI; or
    4) a SEG-ID in the case of an Infrastructure Segment.

A MEP is associated with two Bridge Ports. For a Down MEP, both associations are with the same Bridge Port. For an Up MEP, the two associations can be with either the same, or with different Bridge Ports (see 19.4, J.6). The two Bridge Ports are:

i) ~~h)~~ The Bridge Port on which the MEP is configured; and
j) ~~i)~~ The Bridge Port on which the MEP is implemented, and from which it inherits its Individual MAC address.

The set of MEPs configured with identical values for MAID defines an MA. Thus, one can say that the MA, and not the MEPs, possesses this parameter. However, an MA is a diffuse entity that can be spread among a number of geographically separated Bridges. Each Bridge has its own Maintenance Association managed object for an MA, from which its MEPs MAID, MD Level, and Primary VID, ~~or~~ I-SID, ~~or~~ series of <ESP-DA, ESP-SA, ESP-VID> 3-tuples, or SEG-ID are derived. In the case of a VLAN-associated MA, t~~T~~he selection of which of the MA's VIDs is the Primary VID can be overridden for a specific MEP. Although this information can be incorrectly configured (i.e., configured differently than some other Bridge), the Maintenance Association managed object ensures the uniform configuration of MEPs in a single Bridge.

20. Connectivity Fault Management protocols

20.9 MEP variables

Insert the following text at the end of 20.9:

The following variables are present only in Infrastructure Segment MAs, are local to a single Infrastructure Segment MEP, and are accessible by more than one state machine:

j) ISpresentTraffic (20.9.10);
k) ISpresentmmLoc (20.9.11).

20.9.9 presentmmLoc

Insert the following subclauses, 20.9.10 and 20.9.11, after 20.9.9:

20.9.10 ISpresentTraffic

A Boolean value indicating if at least one TESI protected by the IPG is configured to use the segment monitored by the Infrastructure Segment MEP. ISpresentTraffic is TRUE if and only if the port upon which this MEP is configured is the outbound port of the entry in the FDB corresponding to the TESI protected by the IPG.

20.9.11 ISpresentmmLoc

ISpresentmmLoc is the logical AND of presentRDI (20.9.6) and ISpresentTraffic (20.9.10).

20.11 MEP Continuity Check Initiator procedures

20.11.1 xmitCCM()

Insert the following list item at the end of 20.11.1:

p) Only in the case of an Infrastructure Segment MEP, optionally fills the Traffic field (21.6.1.4) with the value ISpresentTraffic (20.9.10)

20.16 MEP Continuity Check Receiver variables

Change the second paragraph of 20.16 as indicated:

The following variable is present only in PBB-TE MEP or Infrastructure Segment MEP that supports the Traffic field (21.6.1.4), is local to a single PBB-TE MEP or Infrastructure Segment MEP, and is accessible by the MEP Mismatch state machines (20.26):

m) rcvdTrafficBit (20.16.13)

20.16.13 rcvdTrafficBit

Change 20.16.13 as indicated:

Boolean flag which is applicable only for PBB-TE MEPs and Infrastructure Segment MEPs supporting the Traffic field (21.6.1.4). Set by MEPprocessEqualCCM() according to the Traffic field of the last-received valid CCM.

20.17 MEP Continuity Check Receiver procedures

20.17.1 MEPprocessEqualCCM()

Change list item b) in 20.17.1 as indicated:

b) Otherwise, if the MAID of the received CCM does not exactly match the MAID configured in the receiving MEP [(item a) in 12.14.1.2.2, item b) in 12.14.5.3.2] then MEPprocessEqualCCM() sets xconCCMreceived (20.23.1) true (this procedural step being optional in the case of a PBB-TE MEP or Infrastructure Segment MEP), reconstructs the frame containing the CCM into recvdFrame, and places a timer counter value into recvdInterval corresponding to the value of the CCM Interval field in the received CCM.

Change list item 8) in 20.17.1 d) ("Otherwise, MEPprocessEqualCCM():") as indicated:

8) Only in the case of a PBB-TE MEP or Infrastructure Segment MEP, optionally copies the Traffic field (21.6.1.4) to rcvdTrafficBit (20.16.13).

20.25 MEP Mismatch variables

Change 20.25 as follows:

The following variables are local to the MEP Mismatch state machines for a PBB-TE MEP or Infrastructure Segment MEP implementing the Traffic field (21.6.1.4):

20.25.1 mmCCMreceived

Change 20.25.1 as follows:

Boolean flag set to TRUE when rcvdTrafficBit (20.16.13) does not match the presentTraffic (20.9.8) in the case of a PBB-TE MEP or rcvdTrafficBit (20.16.13) does not match the ISpresentTraffic (20.9.10) in the case of an Infrastructure segment MEP.

20.25.2 mmCCMdefect

Change 20.25.2 as follows:

A Boolean flag set and cleared by the MEP Mismatch state machines to indicate that one or more CCMs with Traffic fields not matching the presentTraffic (20.9.8) has been received in the case of a state machine associated with a PBB-TE MEP or that one or more CCMs with ISpresentTraffic (20.9.10) has been received in the case of a state machine associated with an Infrastructure Segment MEP, over a period that is greater than 3.5 times the configured CCM transmission rate and given by the mmCCMTime (20.25.3). This variable is readable as a managed object (12.14.7.1.3 ah)).

20.25.5 mmLocdefect

Change 20.25.5 as follows:

A Boolean flag set and cleared by the MEP Local Mismatch state machine to indicate that presentmmLoc (20.9.9) or ISpresentmmLoc (20.9.11) is set to TRUE, over a period of 50 ms (12.14.7.1.3 ai)).

20.26 MEP Mismatch state machines

Change 20.26 as follows:

The MEP Mismatch state machines implement the functions specified by the state diagrams in Figure 20-8, Figure 20-9, and the variable declarations in ~~20.23~~20.25. There is one MEP Traffic Field Mismatch state machine and one MEP Local Mismatch state machine per PBB-TE MEP or Infrastructure Segment MEP implementing the Traffic field (21.6.1.4).

20.38 MEP Mismatch Fault Notification Generator variables

Change 20.38 as follows:

The following variables are local to the MEP Mismatch Fault Notification Generator state machine for a PBB-TE MEP or Infrastructure Segment MEP implementing the Traffic field (21.6.1.4):

20.39 MEP Mismatch Fault Notification Generator procedures

Change 20.39 as follows:

The following procedure is local to the MEP Mismatch Fault Notification Generator state machine for a PBB-TE MEP or Infrastructure Segment MEP implementing the Traffic field (21.6.1.4):

20.40 MEP Mismatch Fault Notification Generator state machine

Change 20.40 as follows:

A PBB-TE MEP or Infrastructure Segment MEP implementing the Traffic field (21.6.1.4) creates a single instance of the MEP Mismatch Fault Notification Generator state machine. The MEP Mismatch Fault Notification Generator state machine implements the function specified by the state diagram in Figure 20-14, the variables in 20.38, and the procedure in 20.39. The current state of the MEP Mismatch Fault Notification Generator state machine is available in a managed object (12.14.7.1.3 ak)).

21. Encoding of CFM Protocol Data Units

21.6 Continuity Check Message format

21.6.1 Flags

21.6.1.4 Traffic field

Change 21.6.1.4 as indicated:

In the case of a PBB-TE MA or Infrastructure Segment MA, the second most significant bit of the Flags field is the Traffic bit. This bit if supported, is used to indicate the presence of backbone service instances in the monitored TESI or the assignment of TESIs in the monitored Infrastructure Segments. This bit is set to 1 if the transmitting MEP's presentTraffic variable (20.9.8) is set in the case of a PBB-TE MEP or the transmitting MEP's ISpresentTraffic variable (20.9.10) is set in the case of a Infrastructure Segment MEP, and 0 if not. This field is not examined if the receiving MPs are not PBB-TE or Infrastructure Segment MEPs supporting the traffic field.

26. Principles of Provider Backbone Bridged Network operation

26.9 Connectivity Fault Management in a PBB-TE Region

Change 26.9 as follows:

Connectivity Fault Management (CFM) as specified in Clause 18 through Clause 22, provides capabilities useful in detecting, isolating, and reporting connectivity faults in VID-based service instances, backbone service instances, ~~and~~ TESIs, and Infrastructure Segments. As the original CFM protocol in IEEE Std 802.1ag-2007 was primarily focused on VID-based services, the list of additions that are specifically related to TESIs and Infrastructure Segments is summarized here.

NOTE—MIP function is not supported for an Infrastructure Segment MA. Loopback is supported on Infrastructure Segment MEPs. It is not useful to apply the Linktrace operation to an Infrastructure Segment MA. No extension is made to the Loopback or Linktrace operations supporting their use for an Infrastructure Segment MA. This does not preclude the use of MIPs associated with a PBB-TE MA.

In particular this subclause summarizes PBB-TE considerations related to the following:

a) Addressing PBB-TE MEPs (26.9.1)
b) TESI identification (26.9.2)
c) PBB-TE MEP placement in a Bridge Port (26.9.3)
d) PBB-TE MIP placement in a Bridge Port (26.9.4)
e) TESI Maintenance Domains (26.9.5)
f) PBB-TE enhancements of the CFM protocols (26.9.6)
g) Addressing Infrastructure Segment MEPs (26.9.7)
h) Infrastructure Segment identification (26.9.8)
i) Infrastructure Segment MEP placement in a Bridge Port (26.9.9)
j) Infrastructure Segment Maintenance Domains (26.9.10)
k) IPS extensions to Continuity Check operation (26.9.11)

26.9.6 PBB-TE enhancements of the CFM protocols

Insert the following subclauses, 26.9.7 through 26.9.11 (including Figure 26-9 and Figure 26-10) after 26.9.6.3, and renumber the subsequent figures in Clause 26 accordingly:

26.9.7 Addressing Infrastructure Segment MEPs

The configuration of an Infrastructure Segment MA requires a parameter identifying the associated Infrastructure Segment. An Infrastructure Segment is composed of a pair of counterdirectional and co-routed Segment Monitoring Paths (SMPs) (26.11.1). Each SMP is identified by an SMP Identifier (SMP-ID). Thus, an Infrastructure Segment is identified by a pair of SMP-IDs that is known as an Infrastructure Segment Identifier (SEG-ID). The SEG-ID is specified on configuration of the associated Infrastructure Segment MA (12.14.5.3.2).

A MEP associated with an Infrastructure Segment requires the same set of parameters required by a VID-based MEP, with the following changes:

a) The Primary VID is not writable but is always set to the value of the SMP-VID parameter that corresponds to the MA's SMP that has the MEP's MAC address in its SMP-SA field (12.14.7.1.3 d));
b) The MAC address of the MEP is the MAC address of the PNP upon which the MEP is operating (12.14.2.1.2 i)).

26.9.8 Infrastructure Segment identification

Two SMPs are distinct if their corresponding SMP-ID values (3-tuples) differ in at least one parameter. Thus, independent Infrastructure Segments can be associated with SMPs having identical values of SMP-DA and SMP-VID. Figure 26-9 depicts a case in which two SMPs, having identical values of SMP-DA and SMP-VID, are distinguished by their SMP-SA values. The Infrastructure Segment Multiplex Entity (6.21) allows shims defined for PBB-TE IPS to be instantiated per Infrastructure Segment at a Service Access Point that supports multiple Infrastructure Segments.

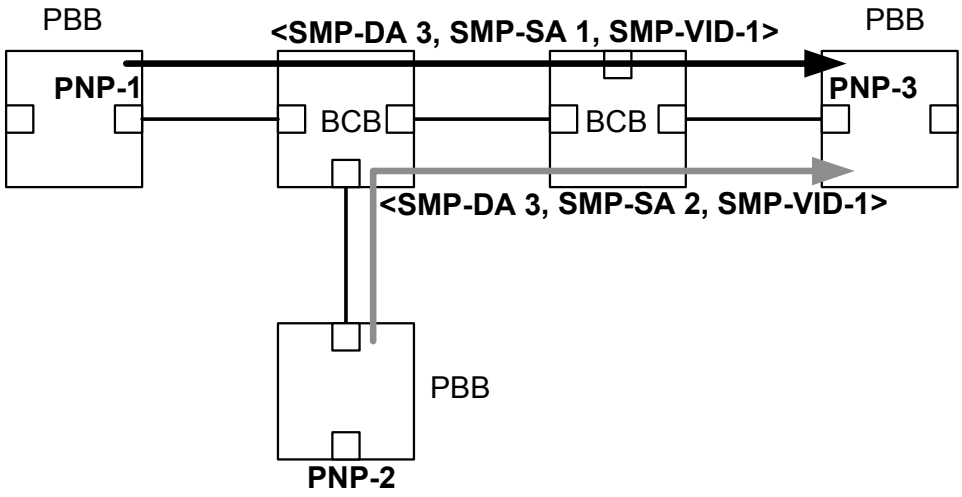

Figure 26-9—Independent Infrastructure Segments distinguished by SMP-SA

26.9.9 Infrastructure Segment MEP placement in a Bridge Port

Infrastructure Segment MEPs are always Down MEPs and are placed only on PNPs as these correspond to the demarcation points of the Infrastructure Segment. The Infrastructure Segment MEPs are placed between the Port filtering entities (8.6.1, 8.6.2, and 8.6.4) and the Queuing entities (8.6.5, 8.6.6, 8.6.7, and 8.6.8) in the SMP-VID space identified by the EISS Multiplex Entity (6.17). Since the Infrastructure Segment MAC addresses can be reused by different Infrastructure Segments, the Infrastructure Segment MEPs need to be further differentiated by the Infrastructure Segment Multiplex Entity (6.21). In principle, separately for each Infrastructure Segment, there can be from zero to eight Down MEPs, ordered by increasing MD Level, from Frame filtering towards Port filtering, even though not more than one MD Level is expected for Infrastructure Segment MAs. Figure 26-10 depicts an example of Infrastructure Segment MEPs on a PNP.

26.9.10 Infrastructure Segment Maintenance Domains

A Provider Backbone Bridge deploying IPS specifies a set of Infrastructure Segment MDs independent of those described in 26.8 and 26.9.5. In particular the CFM stacks in Figure 26-2 have Infrastructure Segment MD levels in parallel to the depicted Backbone MD levels for Ports instantiating Infrastructure Segments while Infrastructure Segment MDs will be present in parallel to the Backbone MD levels depicted in Figure 26-3.

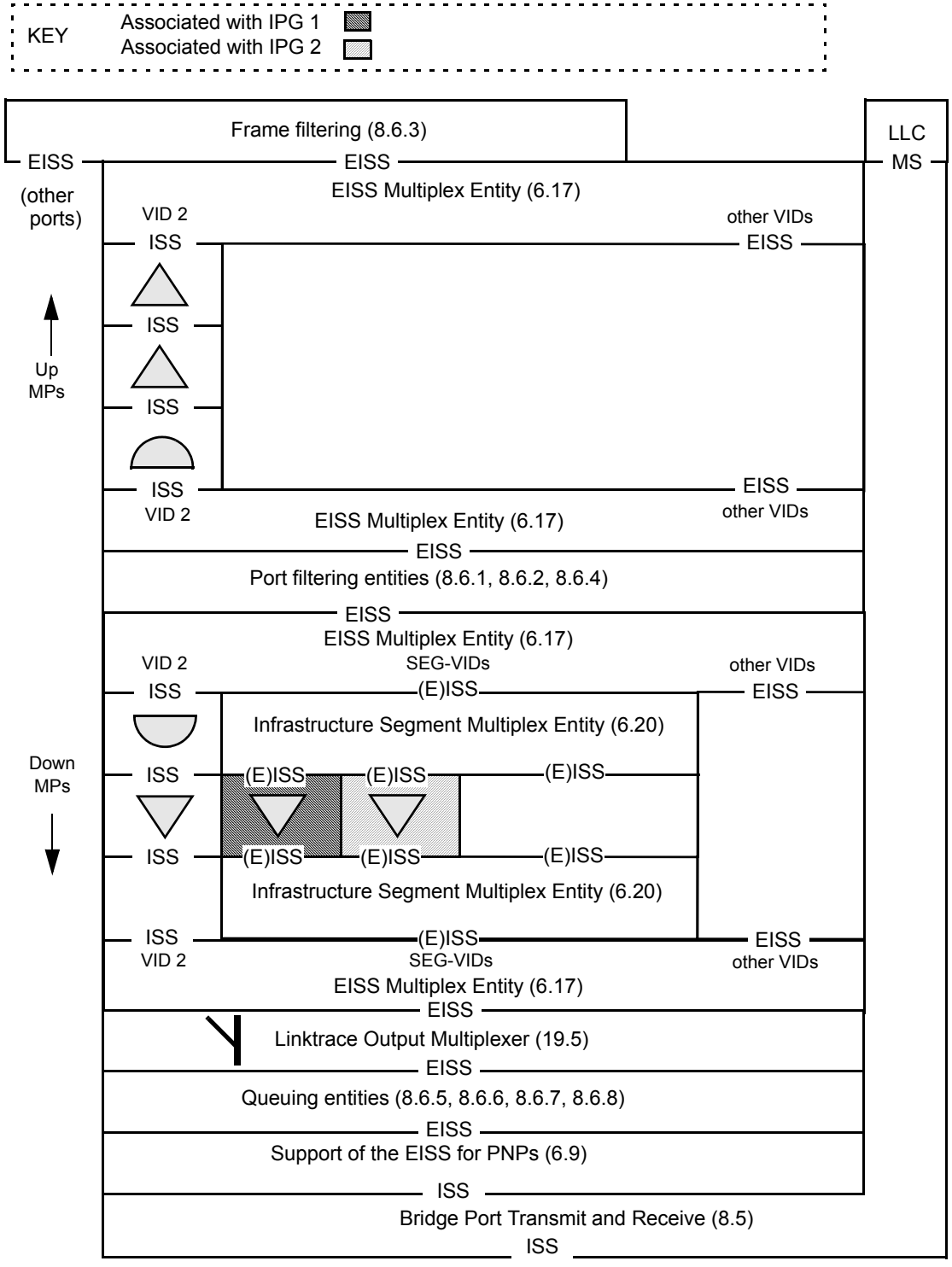

Figure 26-10—Infrastructure Segment MEP placement in a PNP

26.9.11 IPS extensions to Continuity Check operation

The Continuity Check protocol is described in 20.1 and the corresponding state machines in Clause 20. The only enhancement required by the Infrastructure Segment MA is in the procedure that is responsible for constructing and transmitting a CCM (20.11.1):

a) The destination_address parameter is set to the MAC address indicated by the value of the SMP-DA field of the SMP-ID having as SMP-SA the MAC address of the MEP emitting the CCM.

All other Continuity Check processes are the same as those for a VID-based MA.

26.10 Protection switching for point-to-point TESIs

26.10.3 Protection Switching state machines

Change Figure 26-14 (formerly Figure 26-12) as follows:

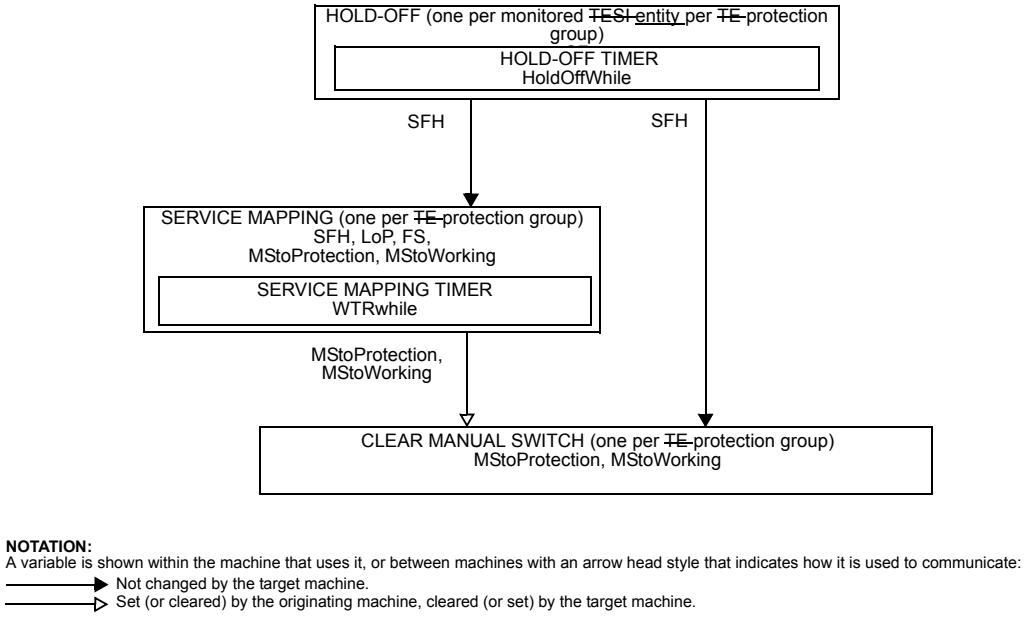

Figure 26-14—Relationships of the Protection switching state machines—overview

Change the second paragraph of 26.10.3 as follows:

There is one set of Protection Switching state machines per ~~TE~~ protection group ~~per CBP~~on each Bridge that terminates the protection group. The ~~TE~~ protection group consists of the working and the protection ~~TESI~~entities. The Protection Switching state machine reuses the defect variables that are presented in Table 20-1. Variables and procedures that are preceded with "w." refer to the working entity while those that are preceded with "p." refer to the protection entity. These internal prefix/entity associations remain the same following a protection switch to the protection entity.

26.10.3.2 State machine timers

26.10.3.2.1 WTRwhile

Change 26.10.3.2.1 as follows:

A timer to be used to prevent frequent operation of the protection switch due to an intermittent defect. This timer allows for a fixed period of time to elapse before data traffic is mapped from the protection ~~TESI~~entity to the working ~~TESI~~entity when in revertive mode.

26.10.3.2.2 HoldOffWhile

Change 26.10.3.2.2 as follows:

In order to coordinate timing of protection switches at multiple layers or across cascaded or nested protected domains, a hold-off timer may be required. The purpose is to allow either a server layer protection switch to have a chance to fix the problem before switching at a client layer, ~~or~~ to allow an upstream protected domain to switch before a downstream domain, or to allow the inner protected domain to switch before the outer protected domain in the case of IPS nested protection domains.

26.10.3.3 Protection Switching variables

26.10.3.3.1 BEGIN

Change 26.10.3.3.1 as follows:

This is a Boolean variable controlled by the system initialization process. A value of TRUE causes all Protection Switching state machines per ~~TE~~ protection group to continuously execute their initial state. A value of FALSE allows these state machines to perform transitions out of their initial state, in accordance with the relevant state machine definitions.

26.10.3.3.5 FS

Change 26.10.3.3.5 as follows:

A Boolean flag indicating the presence of an administrative command to force switch the data traffic to the protection ~~TESI~~entity. Its value is set to 1 by an administrator action [item b3) in 12.18.2.3.2 or 12.24.2.3.2]. It can be reset by an administrator action that corresponds to a request of the same or higher priority according to Table 26-8.

26.10.3.3.6 MStoProtection

Change 26.10.3.3.6 as follows:

A Boolean flag indicating the presence of an administrative command to manually switch the data traffic to the protection ~~TESI~~entity, in the absence of a failure of the working or the protection ~~TESI~~entity. Its value is set to 1 by an administrator action [item b4) in 12.18.2.3.2 or 12.24.2.3.2]. It can be reset by an administrator action that corresponds to a request of the same or higher priority according to Table 26-8 and by the operation of the Clear Manual Switch state machine.

26.10.3.3.7 MStoWorking

Change 26.10.3.3.7 as follows:

A Boolean flag indicating the presence of an administrative command to manually switch the data traffic to the working ~~TESI~~entity in the absence of a failure of the working or the protection ~~TESI~~entity. Its value is set to 1 by an administrator action [item b5) in 12.18.2.3.2 or 12.24.2.3.2]. It can be reset by an administrator action that corresponds to a request of the same or higher priority according to Table 26-8 and by the operation of the Clear Manual Switch state machine.

26.10.3.3.8 WTRTime

Change 26.10.3.3.8 as follows:

The wait-to-restore (WTR) period, as provided by the corresponding managed object [~~item e) in 12.14.6.1.3~~ item e) in 12.18.2.1.3 or item h) in 12.24.2.1.3]. May be configured by the operator in 1 min steps between 5 and 12 min; the default value is 5 min. A value of 0 indicates nonrevertive mode. The overall accuracy of the WTR timer (e.g., <±25 ms) should be sufficient to allow both ~~CBPs~~ ports at the protection domain termination to revert ~~back~~ to the working entity in less than 50 ms.

26.10.3.3.9 HoldOffTime

Change 26.10.3.3.9 as follows:

The hold-off period as provided by the corresponding managed object [item f) in 12.18.2.1.3 or item i) in 12.24.2.1.3]. The suggested range of the hold-off timer is 0 to 10 s in steps of 100 ms (accuracy of ±5 ms); the default value is 0.

Change the heading for 26.10.3.4 as shown:

26.10.3.4 Protection Switching procedures for PBB-TE TESI Protection

Insert the following note in 26.10.3.4 after the existing note, and renumber the existing note as NOTE 1:

NOTE 2—The procedure descriptions in this subclause are specific to PBB-TE TESI Protection. A description of the corresponding procedures for IPS can be found in 26.11.4.1.1 and 26.11.4.1.2, respectively.

Insert the following subclauses, 26.11 through 26.11.5.7 (including Figure 26-18 through Figure 26-26), after 26.10.3.5, and renumber the subsequent subclause in Clause 26 accordingly:

26.11 Infrastructure Protection Switching in a PBB-TE Region

In addition to supporting end-to-end linear protection for TESIs (26.10), PBB-TE supports localized protection of selected TESIs traversing a common sequence of PNPs. Such a sequence of PNPs, together with the intervening MAC relay entities and LANs, is called an Infrastructure Segment. The group of TESIs associated with the Infrastructure Segment is protected from the failure of one or more components (i.e., port, LAN, or MAC Relay Entity) of the Infrastructure Segment. The method of providing such protection is called Infrastructure Protection Switching (IPS). 1:1 IPS and M:1 IPS are described by this standard. Support for IPS is optional. If IPS is supported, 1:1 IPS is required, and M:1 IPS is optional. IPS may be triggered automatically by a change in the operational state of an Infrastructure Segment or manually by administrative command.

NOTE—A complete discussion on the various protection switching mechanisms and terminology is provided by ITU-T G.8031 (2009) [B39]. The ITU-T uses the term "bridge" for the logical entity that selects either or both of the transmit paths at the sending end of a protected domain. This is not to be confused with the term "Bridge" used in this standard.

As illustrated in Figure 26-18, a Bridge supporting IPS is a PBB. Definitions of entities associated with an Infrastructure Segment and properties of such entities are as follows:

a) A PBB terminating the Infrastructure Segment is a Segment Endpoint Bridge (SEB);
b) A PBB in the interior of the Infrastructure Segment is a Segment Intermediate Bridge (SIB);
c) A PNP terminating the Infrastructure Segment is called a Segment Endpoint Port (SEP);
d) A PNP in the interior of the Infrastructure Segment is called a Segment Intermediate Port (SIP);
e) A SEB contains one SEP and does not contain a SIP;
f) A SIB contains exactly two SIPs and, by definition, cannot contain a SEP;
g) A SEP is connected to a single SIP or SEP in a neighboring PBB via a LAN;
h) A SIP is connected to one other SIP within the SIB via the MAC Relay Entity and is connected to a single SEP or SIP in a neighboring PBB via a LAN.

The role of SEB or SIB is assigned to a PBB only with respect to a particular Infrastructure Segment. Similarly, the role of SEP or SIP is assigned to a Port only with respect to a particular Infrastructure Segment.

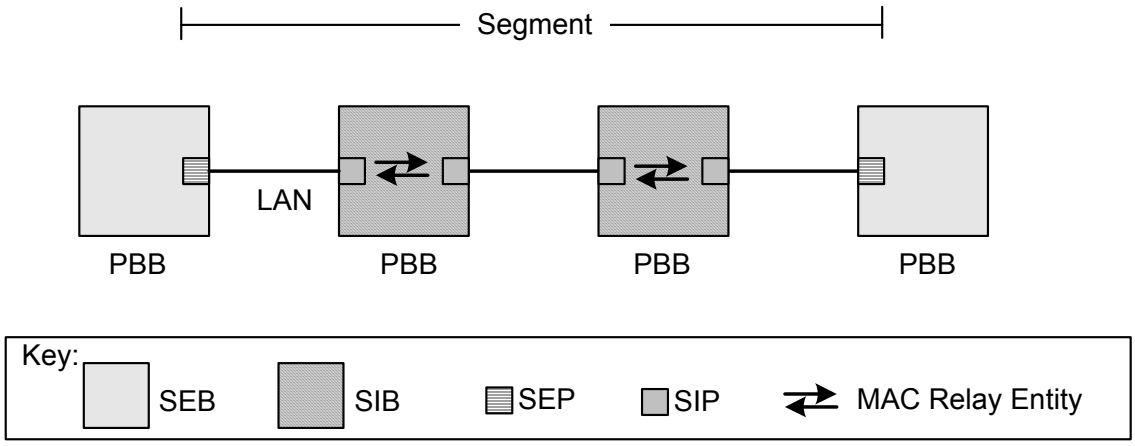

Figure 26-18—Segment terminology and properties

26.11.1 Infrastructure Segment monitoring

As illustrated in Figure 26-19, each Infrastructure Segment is associated with an MA for purposes of determining the connectivity state of that Infrastructure Segment. The Infrastructure Segment MA is associated with a pair of co-routed counterdirectional Infrastructure Segment Monitoring Paths (SMPs). Each SMP is identified by an <SMP-DA, SMP-SA, SMP-VID> 3-tuple that is known as an SMP Identifier (SMP-ID). The SMP-SA takes the value of the MAC address of the SEP from which the SMP originates. The SMP-DA takes the value of the MAC address of the SEP in which the SMP terminates. It follows from the co-routed and counterdirectional properties of the pair of SMPs that the SMP-DA value of one SMP in the pair of SMPs is equal to the SMP-SA value of the other SMP of the pair. The SMP-VID is 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 (8.9). The pair of SMP-IDs associated with an Infrastructure Segment is known as an Infrastructure Segment Identifier (SEG-ID). The MA managed object (12.14.6) associated with an Infrastructure Segment specifies the SEG-ID identifying that Infrastructure Segment. The value of the SEG-ID is inherited by the MEP associated with the Infrastructure Segment MA..

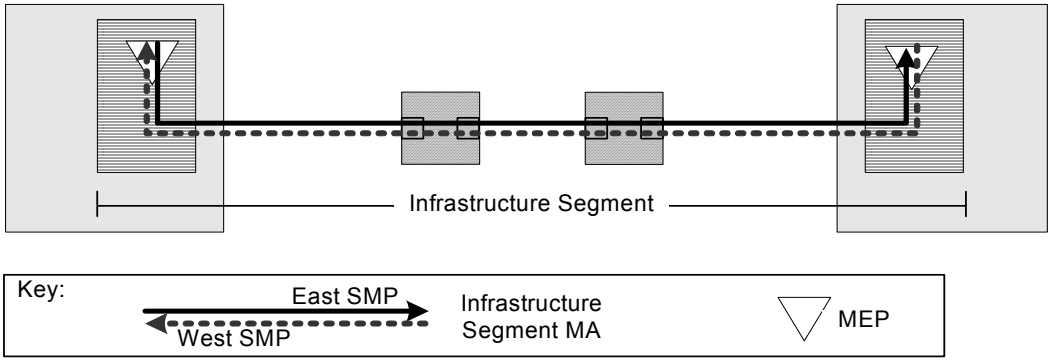

Figure 26-19—Infrastructure Segment monitoring

The operational state of the Infrastructure Segment is indicated by the Signal Fail (SF) variable (26.10.3.3.2) of the Protection Switching state machines (26.10.3). A value of TRUE indicates that the associated Infrastructure Segment is not operational. A value of FALSE indicates that the associated Infrastructure Segment is operational.

NOTE—For proper network operation, each SMP, of the pair of SMPs identifying an Infrastructure Segment MA, is represented by a Static Filtering Entry configured via the Create Filtering Entry operation (12.7.7.1) in each SIB along the path of the Infrastructure Segment. The SMP-ID <SMP-DA, SMP-SA, SMP-VID> would be represented by the Static Filtering Entry <SMP-DA, SMP-VID, outbound port value>. The outbound port value is the port number of the port by which the SMP exits the SIB. Proper operation further includes the creation, at each SEP, of a Maintenance Domain managed object (12.14.5), a Maintenance Association managed object (12.14.6), and a Maintenance association End Point managed object (12.14.7) associated with the Infrastructure Segment MA.

26.11.2 1:1 IPS

Figure 26-20 depicts two Infrastructure Segments with a TESI that has been provisioned to fully traverse the upper Infrastructure Segment. The Infrastructure Segment traversed by the provisioned TESI is known as the Working Segment with respect to that TESI. The lower Infrastructure Segment terminates in the same pair of SEBs that terminates the Working Segment but is otherwise diverse from the Working Segment. The lower Infrastructure Segment is known as the Protection Segment with respect to the TESI that traverses the Working Segment.

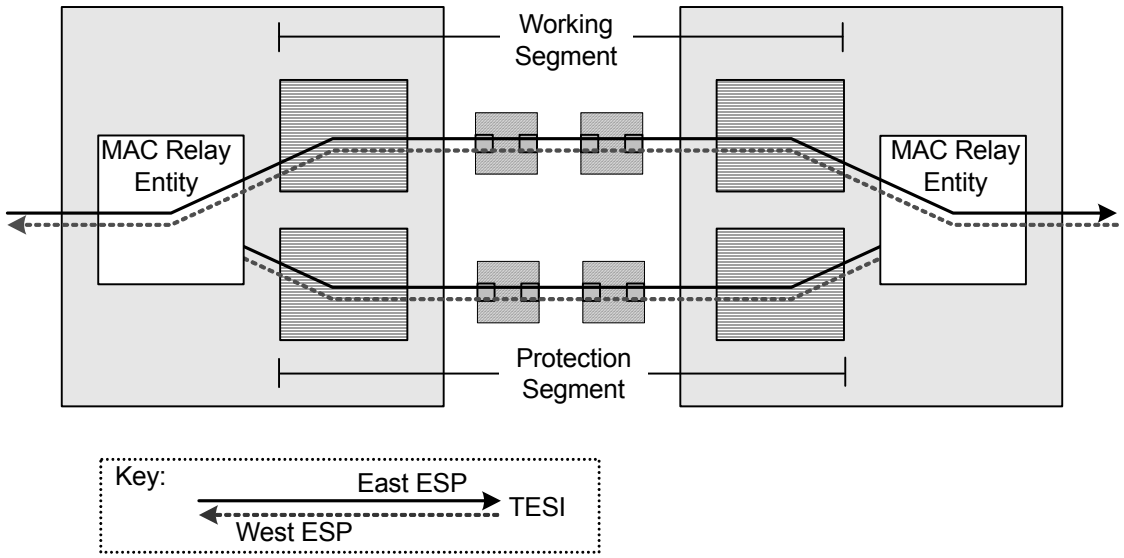

Figure 26-20—Working Segment and Protection Segment

26.11.2.1 Infrastructure Protection Group

The associated Working and Protection Segments depicted in Figure 26-20 are said to form an Infrastructure Protection Group (IPG). The Working and Protection Segments are fully disjoint except for the common SEBs in which they terminate; that is, they share no common SEP, SIB, SIP, LAN, or MAC Relay Entity. One or more TESIs, each identified by a TE-SID are associated with an IPG at the SEB by which the TESI enters that IPG. A TESI is associated with the IPG via the Write IPG managed object (12.24.2.2). Multiple TESIs may be associated with an IPG. TESIs associated with an IPG may have diverse end-to-end paths, but they follow a common path traversing the IPG. Two or more TESIs may be associated with ESPs having the same <ESP-DA, ESP-VID> 2-tuple. In particular this can occur if the TESIs are distinguished only by different values of ESP-SA. In such cases where TESIs share a common value of <ESP-DA, ESP-VID>, the association of one such TESI with an IPG at a SEB implies that all such TESIs are associated with that IPG. In other words, all such TESIs are protected by the IPG, or no such TESIs are protected by the IPG.

NOTE—An Infrastructure Segment can be associated with more than one IPG. For example, the operator can designate Infrastructure Segment 1 as the Working Segment of IPG1 and Infrastructure Segment 2 as the Protection Segment of IPG1. The operator can concurrently designate Infrastructure Segment 2 as the Working Segment of IPG2 and Infrastructure Segment 1 as an Protection Segment of IPG2. This property can be utilized as a method of load sharing across multiple Infrastructure Segments during normal operation.

26.11.2.1.1 Nested IPGs

IPGs are said to be nested with respect to a TESI if

a) The TESI is associated with both IPGs and
b) The set of SEPs and SIPs comprising the Working Segment of one IPG, the inner IPG, is identical to a contiguous sequence of SIPs contained within the Working Segment of the other IPG, the outer IPG.

In Figure 26-21, IPG2 (dashed) is nested within IPG1 (solid). IPG1 is the outer IPG, and IPG2 is the inner IPG. The Working Segment of the inner IPG is fully contained within the Working Segment of the outer IPG. The SEBs associated with the outer IPG are different from those associated with the inner IPG. Each nested IPG deploys an independent set of MAs for the purpose of monitoring the operational state of Infrastructure Segments associated with that IPG.

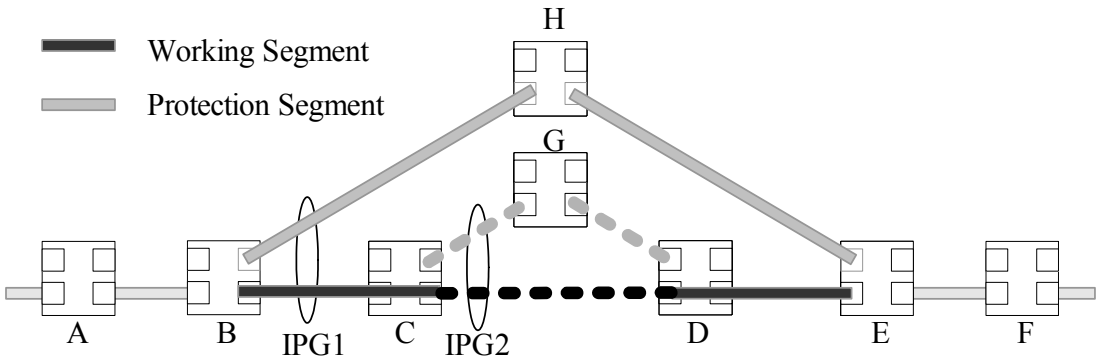

Figure 26-21—Nested IPGs

NOTE—Two IPGs are said to overlap with respect to a TESI if (a) the TESI is associated with both IPGs and (b) the IPGs share a sequence of PNPs. Designing networks having IPGs that overlap, but are not nested, requires careful study of issues not specifically identified in this standard.

26.11.2.2 Protection Switching method

When a TESI is assigned to an IPG by provisioning, traffic associated with that TESI transits the IPG via the Working Segment or the Protection Segment as directed by the Protection Switching state machines (26.10.3). In the absence of faults or outstanding administrative commands, TESI traffic transits the IPG via the Working Segment. The Protection Switching state machines can cause the TESI traffic to transit the IPG via the Protection Segment by invoking the Protection Switching procedure mapDataToProtection() (26.11.4.1.2). This procedure causes the value of the outbound Port field of the FDB entry corresponding to the <ESP_{in}-DA, ESP_{in}-VID> 2-tuple of each TESI associated with the IPG to be assigned the Port Number associated with the Protection Segment. The notation "ESP_{in}" denotes the ESP, of the pair of ESPs associated with the TESI, that *enters* the IPG via the SEB. The Protection Switching state machines can cause the traffic to transit the IPG via the Working Segment by invoking the Protection Switching procedure mapDataToWorking() (26.11.4.1.1). This procedure causes the value of the outbound Port field of the FDB entry corresponding to each <ESP_{in}-DA, ESP_{in}-VID> 2-tuple of each TESI associated with the IPG to be assigned the Port Number associated with Working Segment. The two SEBs associated with the IPG perform protection activities independently. At any point in time, traffic associated with an IPG is carried on either the Working Segment or the Protection Segment. The Infrastructure Segment carrying the TESI traffic is known as the active Infrastructure Segment.

NOTE—Proper operation of the network requires that the FDB entry provisioned in a SIB to forward traffic along an Infrastructure Segment associated with the IPG identify only a single outbound Port. In other words, the portion of a TESI transiting an IPG is provisioned as point-to-point, without regard to whether the TESI is point-to-point or point-to-multipoint from an end-to-end perspective.

26.11.2.3 Hold-off timer

An IPG is provisioned with a "hold-off timer" value. The hold-off timer delays protection action associated with the failure of an Infrastructure Segment. The delay provides a lower layer with the opportunity to take corrective action before IPS is performed. Use of the hold-off timer can increase the total time required to recover from a failure.

In the case of nested IPGs, proper operation of the network requires that the outer IPG be provisioned with a "hold-off timer" value greater than that of the inner IPG. The outer IPG Working Segment is provisioned to coincide with the path of the inner IPG Working Segment. CCM traffic monitoring the outer IPG Working Segment traverses the Active Segment of the Inner IPG. The TESI list associated with the Inner IPG Endpoint Bridge is provisioned to include the SEG-ID associated with the CCM on the outer IPG Working Segment MA that ingresses the Inner IPG SEB. Thus, on a failure of the inner IPG Working Segment, traffic associated with the outer IPG Working Segment, including the CCM traffic associated with the outer IPG Working Segment MA, is protected. The outer IPG will not be aware of the protection switch of the inner IPG and will not perform protection switching activities.

26.11.2.4 Reversion

An IPG is provisioned to operate in revertive mode or nonrevertive mode. In revertive mode, traffic is switched from the Protection Segment to the Working Segment when the Working Segment becomes operational. In nonrevertive mode, traffic remains associated with the Protection Segment when the Working Segment becomes operational unless

a) The Protection Segment fails or
b) Traffic is switched to the Working Segment by administrative command.

An IPG operates in revertive mode if that IPG is provisioned to support M:1 IPS.

26.11.2.4.1 Wait-to-restore timer

An IPG operating in revertive mode is provisioned with a "wait-to-restore (WTR) timer" value. The WTR timer delays reversion from the Protection Segment to the Working Segment on recovery of the Working Segment. Use of the WTR timer reduces the severity of "flapping," or rapid oscillation, that may occur if the Working Segment is experiencing intermittent connectivity failure. Setting the WTR time to zero indicates that the IPG is operating in nonrevertive mode.

26.11.2.5 Administrative commands

IPS supports the following administrative commands:

— Lockout of Protection (LoP): allows the operator to suppress automatic switching from Working Segment to Protection Segment;
— Forced Switch (FS): allows the operator to force traffic to the Protection Segment as if a connectivity failure exists on the Working Segment. The behavior persists until the command is withdrawn;
— Manual Switch to Protection (MStoProtection): switches traffic to the Protection Segment, but does not force traffic to remain associated with the Protection Segment;
— Manual Switch to Working (MStoWorking): switches traffic to the Working Segment, but does not force traffic to remain associated with the Working Segment.

26.11.3 IPS Control entity

The IPS Control entity contains the 1:1 IPS state machines (26.11.4) and, if M:1 IPS (26.11.5) is supported, the M:1 IPS state machines (26.11.5.1). There is an instance of the IPS Control entity for each SEB.

As shown in Figure 26-22, the operation of the IPS state machines depends upon input from Bridge Management and from each Infrastructure Segment MA associated with the IPG. The input from Bridge Management includes the list of TESIs [12.14.2.1.2 e)] associated with the IPG and Administrative commands (26.11.2.5) associated with the IPG. The outbound Port field of a Static Filtering Entry associated with an IPG can be modified by IPS Control. When a Static Filtering Entry is no longer associated with an IPG, the Outbound Port value of that Static Filtering Entry is restored by IPS control to the Port associated with the Working Segment of the IPG and IPS Control cannot subsequently modify the Outbound Port value. While the Outbound Port value can be modified by IPS Control, addition and deletion of FDB entries remains under the control of Bridge Management.

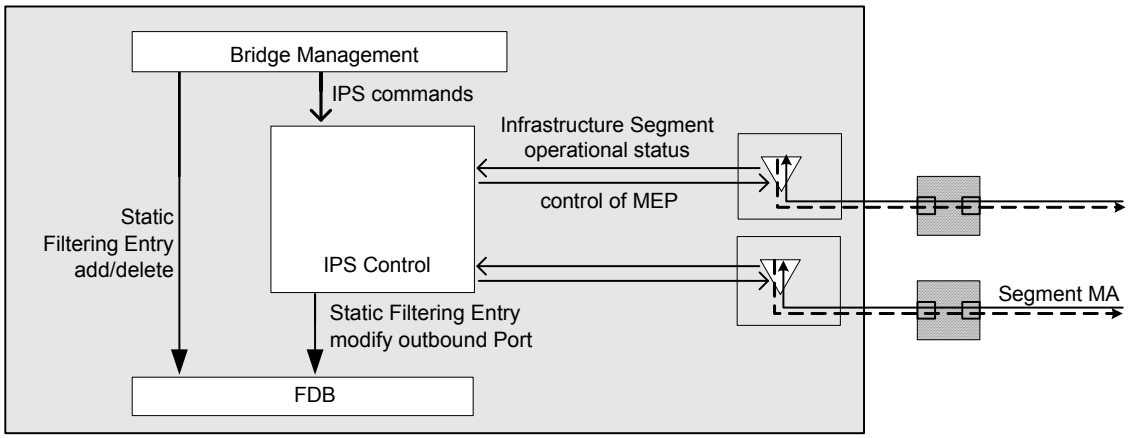

Figure 26-22—IPS Control entity

IPS Control maintains the following entities associated with the IPG:

a) The SEG-ID identifying the Working Segment MA;
b) The SEG-ID identifying the Protection Segment MA;
c) The 1:1 IPS state machines;
d) The list of the TESIs describing traffic protected by the IPG;

When an IPG is associated with optional M:1 IPS, the following additional entities are maintained:

e) The list of SEG-IDs identifying the MAs of candidate Protection Segments;
f) The M:1 IPS state machines.

26.11.4 1:1 IPS state machines

Protection switching for point-to-point TESIs (26.10) and 1:1 IPS (26.11.2) both utilize Protection Switching state machines (26.10.3). In the case of 1:1 IPS, the "Protection Group" is an "IPG," the "working entity" is the "Working Segment," and the "protection entity" is the "Protection Segment." One set of Protection Switching state machines is instantiated per IPG per SEB.

26.11.4.1 Procedures referenced by the 1:1 IPS state machines

The procedures mapDataToWorking() and mapDataToProtection() referenced by the 1:1 IPS state machines and described in the subclauses that follow, differ from the procedures of the same name (26.10.3.4) referenced by the TESI Protection state machines.

26.11.4.1.1 mapDataToWorking()

This procedure changes the value of the outbound Port field of each Static Filtering Entry identified by the <ESP_{in}-DA, ESP_{in}-VID> 2-tuple associated with each TESI on the list of TESIs associated with an IPG to the port Number associated with the Working Segment of the IPG.

26.11.4.1.2 mapDataToProtection()

This procedure changes the value of the outbound Port field of each Static Filtering Entry identified by the <ESP_{in}-DA, ESP_{in}-VID> 2-tuple associated with each TESI on the list of TESIs associated with an IPG to the port Number associated with the Protection Segment of the IPG.

26.11.5 M:1 IPS

This subclause describes extensions to 1:1 IPS (26.11.2) supporting M:1 IPS when this optional feature is implemented. An IPG is constrained to operate in 1:1 revertive mode when that IPG supports M:1 IPS.

As illustrated in Figure 26-23, a list of candidate Protection Segments, ordered by priority value, is provisioned for each IPG. deploying M:1 IPS. The list contains at least one candidate Protection Segment. Candidate Protection Segments are mutually disjoint and disjoint from the Working Segment. The candidate Protection Segment having the highest (lowest numeric) priority among the operational candidate Protection Segments is the Protection Segment referenced by the 1:1 IPS state machine. This selected candidate Protection Segment is called the "current" Protection Segment. In the absence of any operational candidate Protection Segments, the current Protection Segment retains the value it had prior to the failure of the last candidate Protection Segment. In this case, the 1:1 IPS Protection Segment is declared to have failed. If the 1:1 IPS Protection Segment is not operational and a candidate Protection Segment becomes operational, that candidate Protection Segment assumes the role of 1:1 IPS Protection Segment, and the 1:1 IPS Protection Segment becomes operational. If a candidate Protection Segment of higher priority than the current Protection Segment becomes operational, then that candidate Protection Segment assumes the role of the 1:1

IPS Protection Segment following expiration of the M:1 wait-to-restore timer. If the current Protection Segment has changed and the 1:1 IPS Protection Segment is the active Infrastructure Segment, then Static Filtering Entries associated with TESIs protected by the IPG are updated with the Port number of the current Protection Segment as described in 26.11.2.2. Thus, M:1 IPS is deployed using an extension of 1:1 IPS that allows the current Protection Segment to be replaced by a candidate Protection Segment of higher priority, provided that such a candidate exists and is operational.

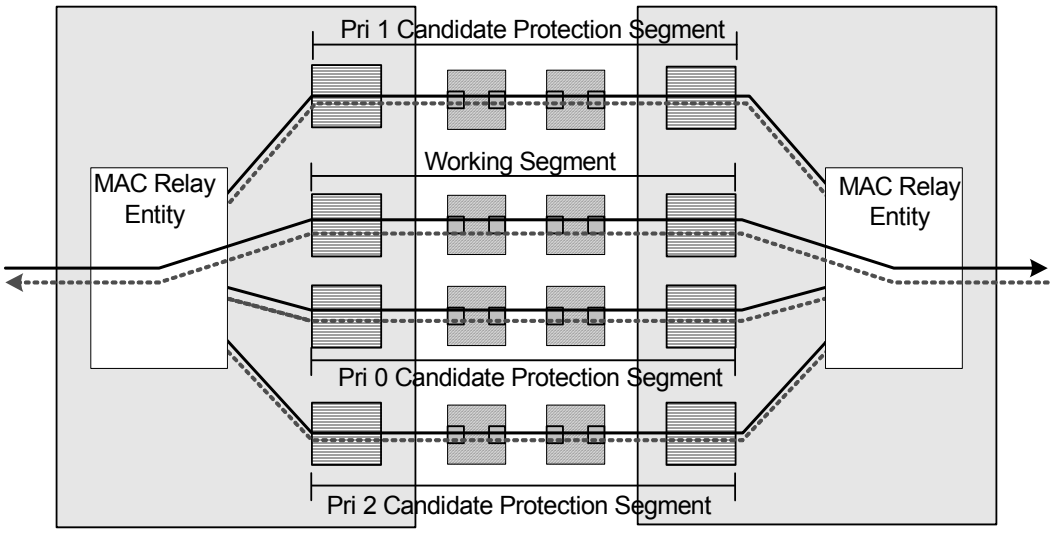

Figure 26-23—M:1 IPS

26.11.5.1 M:1 IPS state machines

There is one set of M:1 IPS state machines per IPG.

The M:1 IPS state machines comprise one M:1 Hold-off state machine (26.11.5.6) per candidate Protection Segment and one Protection Segment Selection state machine (26.11.5.7) per IPG, in addition to the 1:1 IPS state machines (26.11.4). The relationship between the M:1 IPS state machines and the 1:1 IPS state machines is illustrated in Figure 26-24.

26.11.5.2 Notational conventions used in state diagrams

The Protection Switching state machines are specified using the notational conventions defined in Annex E. Additionally, in cases of multiple instances of a state variable, each instance is represented by adding the suffix "[n]" to indicate the n^{th} instance. If instances of a state variable may be associated with either the Working Segment or the Protection Segment, the references can be distinguished by prefixing "w." or "p." to distinguish the two cases.

26.11.5.3 State machine timers

The timer variables declared in this subclause are part of the specification of the operation of Protection Switching. The accompanying descriptions of their meaning and use are provided to aid in the comprehension of the protocol only and are not part of the specification. Timer variables deployed by the M:1 IPS state machines are:

a) HoldOffWhile (26.10.3.2.2): one instance per M:1 Hold-off state machine;
b) MWTRwhile (26.11.5.3.1): one instance per M:1 Hold-off state machine.

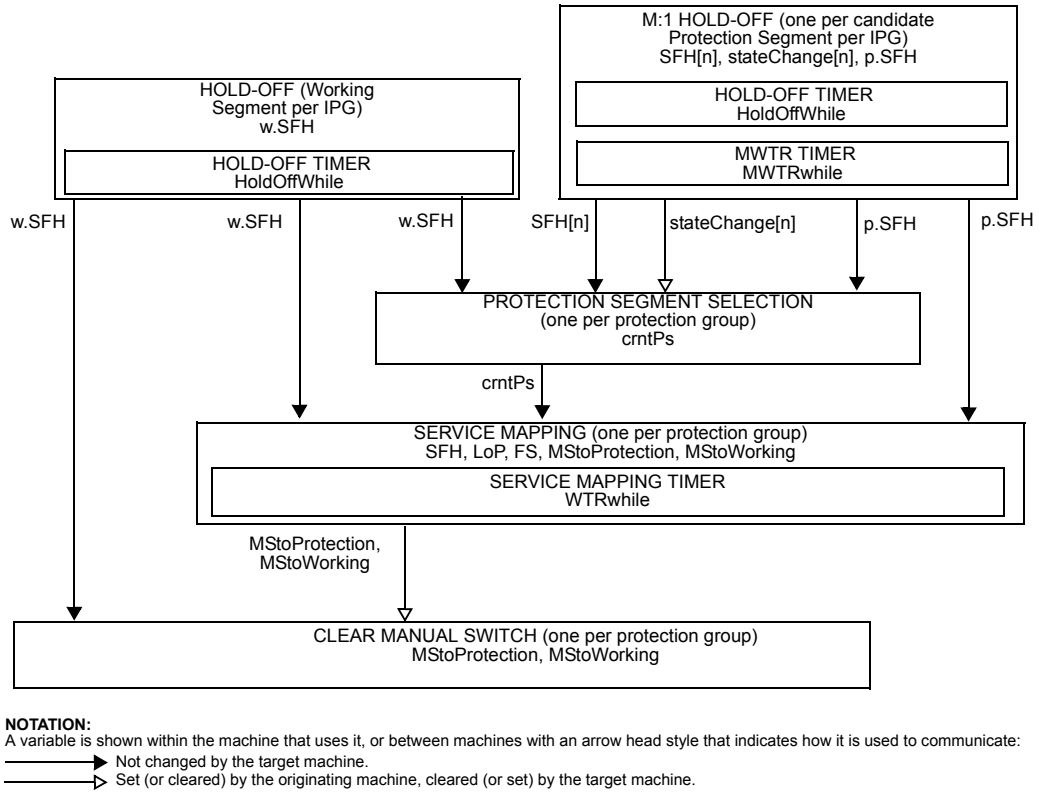

Figure 26-24—M:1 IPS state machines

26.11.5.3.1 MWTRwhile

A timer to be used to prevent frequent operation of the protection switch among candidate Protection Segments due to an intermittent defect. This timer allows for a fixed period of time to elapse before data traffic is mapped from a lower priority Protection Segment to a higher priority Protection Segment when in M:1 revertive mode.

26.11.5.4 Variables referenced by M:1 IPS state machines

The following variables are referenced by the M:1 IPS state machines:

a) BEGIN (26.11.5.4.1);
b) SF (26.11.5.4.2);
c) SFH (26.11.5.4.3);
d) stateChange (26.11.5.4.4);
e) pri (26.11.5.4.5);
f) allPsSFH (26.11.5.4.8);
g) crntPs (26.11.5.4.6);
h) WTRTime (26.10.3.3.8);
i) MWTRTime (26.11.5.4.7); and
j) HoldOffTime (26.10.3.3.9).

26.11.5.4.1 BEGIN

This is a Boolean variable controlled by the system initialization process. A value of TRUE causes all M:1 IPS state machines per IPG to continuously execute their initial state. A value of FALSE allows these state machines to perform transitions out of their initial state, in accordance with the relevant state machine definitions.

26.11.5.4.2 SF

SF is the logical OR of someRMEPCCMdefect (20.33.5), someRDIdefect (20.33.7), xConCCMdefect (20.23.3), and errorCCMdefect (20.21.3). An instance of this variable, identified by the notation SF[n], is specified per candidate Protection Segment.

26.11.5.4.3 SFH

A Boolean flag set and cleared by the M:1 Hold-off state machine to indicate that SF is set for a period that is equal to, or larger than, the HoldOffTime. The variable is set equal to SF if the hold-off timer is not supported. An instance of this variable, identified by the notation SFH[n], is specified per candidate Protection Segment.

26.11.5.4.4 stateChange

A Boolean flag set by the M:1 Hold-off state machine and cleared by the Protection Segment Selection state machine indicating the value of SFH associated with a candidate Protection Segment has changed. An instance of the variable, identified by the notation stateChange[n], is specified per candidate Protection Segment.

26.11.5.4.5 pri

An integer value associated with each candidate Protection Segment and unique within the IPG indicating the selection priority of a candidate Protection Segment. Lower numeric values are associated with higher priority. An instance of the variable, identified by the notation pri[n], is specified per candidate Protection Segment.

26.11.5.4.6 crntPs

An integer value identifying the operational candidate Protection Segment having the highest (lowest numeric) selection priority. In the event that no candidate Protection Segment is available, the value is that of the last candidate Protection Segment to be available.

26.11.5.4.7 MWTRTime

The M:1 wait-to-restore (MWTR) period associated with reverting from a lower priority to a higher priority candidate Protection Segment, as provided by the corresponding managed object [item l) in 12.20.2.1.3]. May be configured by the operator in 1 min steps between 5 and 12 min; the default value is 5 min. A value of 0 indicates M:1 nonrevertive mode. The overall accuracy of the MWTR timer (e.g., <±25 ms) should be sufficient to allow both SEBs at the termination of the IPG to revert to the same value of the Protection Segment in less than 50 ms.

26.11.5.4.8 allPsSFH

The logical AND of the value of SFH[n] over the M candidate Protection Segments.

26.11.5.5 Procedures referenced by M:1 IPS state machines

The following procedures are referenced by the M:1 IPS state machines:

a) highestPriOperPs() (26.11.5.5.1);
b) setPs(n) (26.11.5.5.2); and
c) mapDataToProtection() (26.10.3.4.2).

26.11.5.5.1 highestPriOperPs()

Returns the identity of the highest priority candidate Protection Segment for which SFH[n] == FALSE or, in the event that SFH[n] == TRUE for all candidate Protection Segments, the value NULL.

26.11.5.5.2 setPs(n)

Establishes the n^{th} candidate Protection Segment as the Protection Segment referenced by the Service Mapping state machine.

26.11.5.6 M:1 Hold-off state machine

The M:1 Hold-off state machine is specified by the state diagram in Figure 26-25 and the variables in 26.11.5.4.

NOTE—The state NO_SFH_WTR is entered only in the case that M:1 reversion has been provisioned (i.e., MWTRTime != 0) and the candidate Protection Segment “n” is operational (i.e., !SF[n]). The state allows the machine to wait a period of time (i.e., MWTRTime) before permitting the candidate Protection Segment “n” to become available for selection as the Protection Segment, thus increasing stability. If, during this time, it is determined that *no* candidate Protection Segments are available for selection (i.e., allPsSFH), but candidate Protection Segment “n” *is* operational, then it is prudent not to wait MWTRTime but instead to proceed directly to the selection of candidate Protection Segment “n” as the current Protection Segment. In other words, when no candidate Protection Segment has met the criterion for availability (i.e., allPsSFH), but there is a candidate Protection Segment that is operational (i.e., !SF[n]), then it is not necessary to wait MWTRTime before proceeding with selection.

26.11.5.7 Protection Segment Selection state machine

The Protection Segment Selection state machine is specified by the state diagram in Figure 26-26 and the variables in 26.11.5.4.

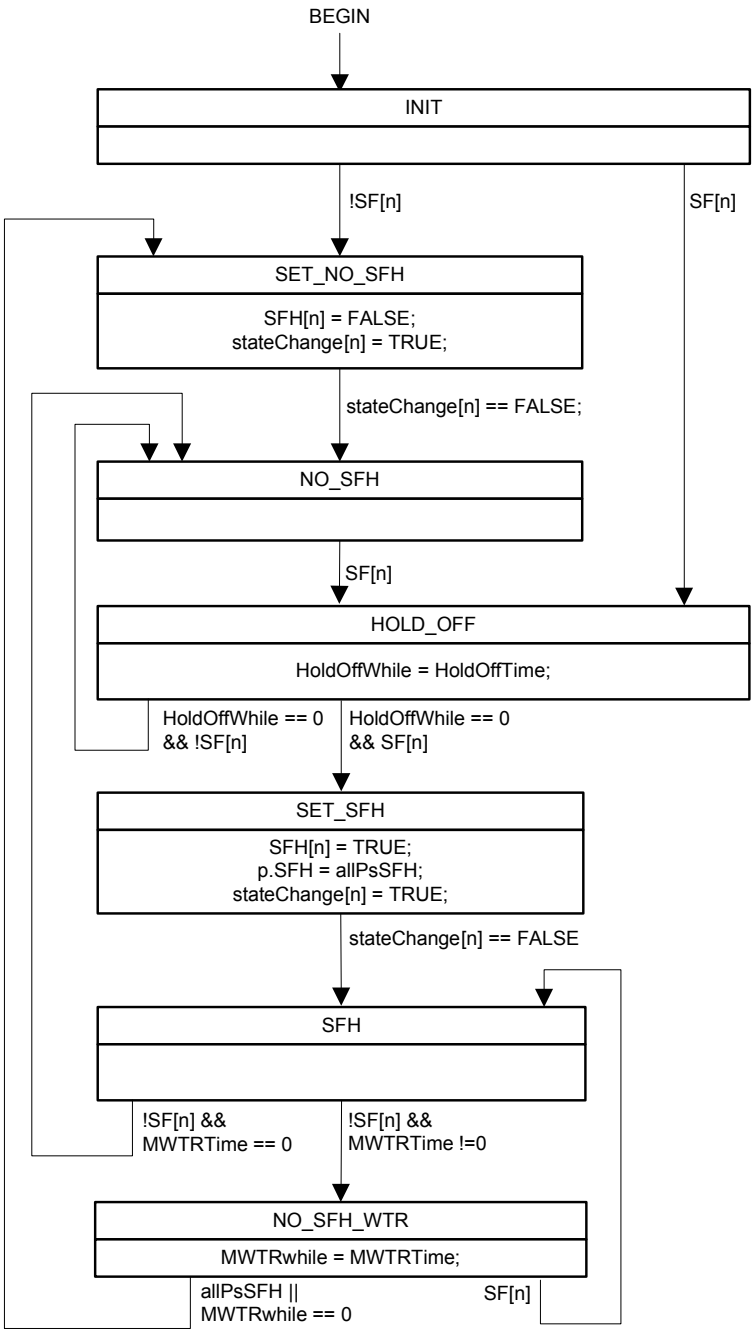

Figure 26-25—M:1 Hold-off state machine

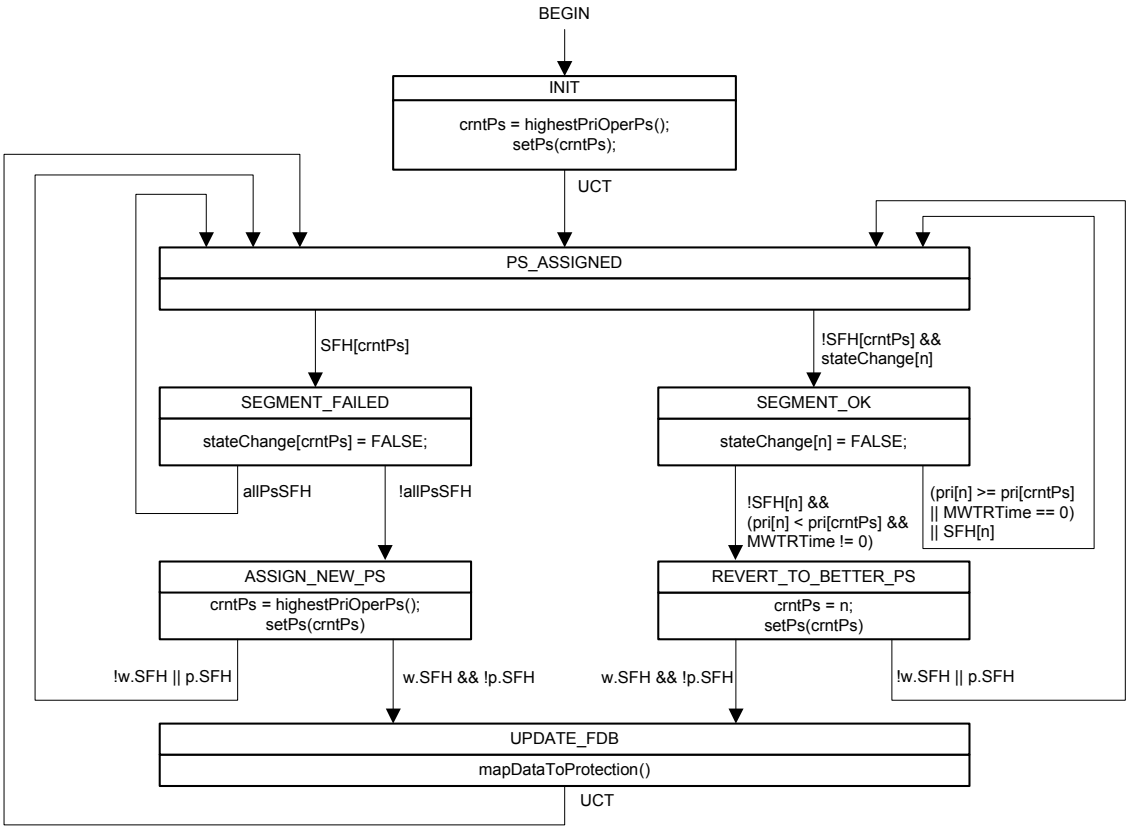

Figure 26-26—Protection Segment Selection state machine

Change 26.12 (formerly 26.11) as follows:

26.12 Mismatch defect

Under ~~certain~~ equipment malfunction conditions and/or ~~wrong~~ incorrect configuration, a mismatch between the mappings of the backbone service instances to the appropriate TESI at the terminating CBPs can happen. Similarly, a mismatch can occur in the mapping of a TESI to the appropriate Infrastructure Segment at the terminating PNP. To maintain the proper operation of the network, ~~this~~ such a mismatch should be detected and reported. There can be two types of mismatch:

a) Protection switching incomplete
b) Working/protection configuration mismatch

An example of protection switching incomplete mismatch is when, due to ~~certain~~ equipment malfunction, the near end (East B-Component in Figure 26-13) fails to switch over but it sends a CCM with the RDI field set to the far end (West B-Component in Figure 26-13).[2] The far end transmits to the protection TESI while the near end is still transmitting in the working TESI. Similarly a mismatch can also happen when the near end transmits to the protection TESI but the far end fails to start transmitting to the protection TESI when it receives a CCM with the RDI field set.

[2]Figure 26-13 was numbered Figure 26-11 before this amendment introduced changes that required the renumbering of several figures in this clause.

The mismatch can also happen because of ~~wrong~~ incorrect configuration. For example, one end is configured to send traffic on working TESI while the other end is configured to send traffic on protection TESI. Or one end is configured as revertive mode while the other end is configured as nonrevertive mode. The mismatch occurs when a failure is cleared.

NOTE—Since a merging selector is used, in the case of TESI protection, there is not necessarily a traffic loss in all mismatch cases.

PBB-TE MEPs and Infrastructure Segment MEPs that support the Traffic field (21.6.1.4) can detect ~~this defect~~ such a mismatch. The Mismatch state machine in ~~20.24~~ 20.26 ~~is providing~~ provides this capability.

Annex A

(normative)

PICS proforma—Bridge implementations[3]

A.5 Major capabilities

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

Item	Feature	Status	References	Support
IPS	Is Infrastructure Protection Switching supported?	PBBTE: O	5.6.2, 5.8.2, 26.11	Yes [ ] No [ ] N/A [ ]

A.14 Bridge Management

Insert the following rows at the end of A.14:

Item	Feature	Status	References	Support
MGT-217	Read IPG list	IPS: M	12.24.1.1	Yes [ ] N/A [ ]
MGT-218	Create IPG managed object	IPS: M	12.24.1.2	Yes [ ] N/A [ ]
MGT-219	Delete IPG managed object	IPS: M	12.24.1.3	Yes [ ] N/A [ ]
MGT-222	Read IPG managed object	IPS: M	12.24.2.1	Yes [ ] N/A [ ]
MGT-221	Write IPG managed object	IPS: M	12.24.2.2	Yes [ ] N/A [ ]
MGT-222	Apply administrative command to IPG managed object	IPS: M	12.24.2.3	Yes [ ] N/A [ ]

A.24 Management Information Base (MIB)

Insert the following row at the end of A.24:

Item	Feature	Status	References	Support
MIB-37	Is the IEEE8021-TE-IPS-MIB module fully supported (per its MODULE-COMPLIANCE)?	MIB: O	17.7.18	Yes [ ] No [ ] N/A [ ]

[3]*Copyright release for PICS proformas:* Users of this standard may freely reproduce the PICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed PICS.

Insert the following subclause, A.36, after A.35:

A.36 Infrastructure Protection Switching (IPS)

Item	Feature	Status	References	Support	
	If item IPS is not supported, mark N/A and continue at the subsequent subclause.			N/A [ ]	
IPS-1	Is 1:1 IPS supported?	IPS: M	26.11.2	Yes [ ]	N/A [ ]
IPS-2	Is M:1 IPS supported?	IPS: O	26.11.5	Yes [ ] N/A [ ]	No [ ]
IPS-3	Are the operator commands Forced Switch, Lockout of Protection, MStoWorking, and MStoProtection implemented?	IPS: M	26.11.2.5	Yes [ ]	N/A [ ]
IPS-4	Is the hold-off timer implemented?	IPS: O	26.11.2.3	Yes [ ] N/A [ ]	No [ ]
IPS-5	Is the M:1 wait-to-restore (MWTR) timer implemented?	IPS-2: O	26.11.5.4.7	Yes [ ] N/A [ ]	No [ ]