



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

Virtual Bridged Local Area Networks

**Amendment 5:
Connectivity Fault Management**

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

17 December 2007

IEEE Std 802.1ag™-2007
(Amendment to
IEEE Std 802.1Q™-2005
as amended by
IEEE Std 802.1ad™-2005
and IEEE Std 802.1ak™-2007)

IEEE Std 802.1ag™-2007

(Amendment to
IEEE Std 802.1Q™-2005
as amended by
IEEE Std 802.1ad™-2005
and IEEE Std 802.1ak™-2007)

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

Virtual Bridged Local Area Networks

Amendment 5: Connectivity Fault Management

Sponsor

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

Approved 27 September 2007

IEEE SA-Standards Board

Abstract: This amendment specifies protocols, procedures, and managed objects to support connectivity fault management. These allow discovery and verification of the path, through bridges and LANs, taken for frames addressed to and from specified network users. Connectivity faults can be detected and isolated to an individual bridge or LAN.

Keywords: error detection, fault management, LANs, local area networks, MAC Bridges, MANs, metropolitan area networks, OAM, transparent bridging, VLANs

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

Copyright © 2007 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 17 December 2007. Printed in the United States of America.

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

PDF: ISBN 978-0-7381-5689-7 STD95724
Print: ISBN 978-0-7381-5690-3 STDPD95724

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

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

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

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

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

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

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

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

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

Introduction

This introduction is not part of IEEE Std 802.1ag-2007, IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 5: Connectivity Fault Management.

The MAC Bridge standardization activities that resulted in the development of IEEE Std 802.1D™ introduced the concept of Filtering Services in Bridged Local Area Networks, mechanisms whereby filtering information in such LANs can be acquired and held in a Filtering Database, as well as support for expedited data, dynamic filtering of Group MAC addresses through the GMRP protocol, and the GARP protocol that supports GMRP and can support other applications.

IEEE Std 802.1Q-2005, a revision of IEEE Std 802.1Q-1998, defines mechanisms that allow the implementation of Virtual Bridged Local Area Networks, including:

- a) Virtual LAN Services;
- b) The operation of the Forwarding Process that is required;
- c) The structure of the Filtering Database that is required;
- d) The nature of the protocols and procedures that are required in order to provide Virtual LAN services, including the definition of the frame formats used to represent VLAN identification information, and the procedures used in order to insert and remove VLAN identifiers and the headers in which they are carried;
- e) The ability to support end-to-end signaling of priority information regardless of the intrinsic ability of the underlying MAC protocols to signal priority information;
- f) The GARP VLAN Registration Protocol (GVRP) that allows distribution and registration of VLAN membership information (the protocol described makes use of the GARP protocol defined in IEEE Std 802.1D);
- g) The management services and operations that are required in order to configure and administer networks;
- h) The ability to restrict Dynamic Group and VLAN registration based on the contents of static filtering entries;
- i) VLAN classification according to link layer protocol type;
- j) Support for VLANs carried over multiple Spanning Tree instances.

IEEE Std 802.1ad-2005, an amendment to IEEE Std 802.1Q-2005, defines mechanisms that allow the implementation of Provider Bridged Networks, including:

- k) The differentiation between Service VLANs (S-VLANs), identified by a new S-VLAN tag, and customer VLANs (C-VLANs), identified by the IEEE 802.1Q tag;
- l) The encapsulation of C-VLAN tags within S-VLAN tags, in order to allow a service provider to carry some or all of a customer's C-VLANs within a single S-VLAN;
- m) The provision of two levels of drop precedence separate from the priority levels of IEEE Std 802.1D, and the replacement of the Canonical Format Indicator of the C-VLAN tag by a Drop Eligible Indicator in the S-VLAN tag to carry the drop precedence;
- n) The passing of certain of the customers' control PDUs, including IEEE 802.1AB LLDP PDUs and IEEE 802.1Q Bridge PDUs, transparently through the Provider Bridged Network as ordinary data;
- o) The reassignment of MAC addresses used for control PDUs, including BPDUs, for use by Provider Bridges;
- p) The definition of C-VLAN components, added to Provider Bridge Ports to provide the functions necessary to support the allocation of C-VLANs to S-VLANs, to map priorities between networks, and to interact with the customers' control protocols; and
- q) The managed objects necessary to control these functions.

This standard provides Connectivity Fault Management (CFM) capabilities useful to Virtual Bridged Local Area Networks for detecting, isolating, and reporting connectivity faults. It is aimed primarily at Provider

Bridged Networks, but is useful also for C-VLAN networks. The mechanisms defined in this standard include:

- r) The ability to configure multiple nested Maintenance Domains over a Bridged Network or a network of Bridged Networks, each potentially managed by a different administrative organization;
- s) The ability to configure Maintenance Associations (MAs), each identified with a single Maintenance Domain, and on any given Bridge, a set of VLANs;
- t) The protocols, procedures, and CFM Protocol Data Unit (CFM PDU) formats required to detect, isolate, and report connectivity faults;
- u) The ability, within an MA, to configure and manage Maintenance Points (MPs) that generate and respond to CFM PDUs; and
- v) The ability to command MPs to perform certain fault isolation operations, and to inspect the results.

CFM is not to be confused with the Ethernet OAM capabilities described in IEEE Std 802.3™, Clause 57. IEEE 802.3 OAM is concerned with detecting and reporting faults on a single point-to-point IEEE 802.3 LAN. IEEE Std 802.1ag-2007 is concerned with detecting, isolating, and reporting connectivity faults spanning networks comprising multiple LANs, including LANs other than IEEE 802.3 media.

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 can be obtained from

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

Notice to users

Errata

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

Interpretations

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

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. A patent holder or patent applicant has filed a statement of assurance that it will grant licenses under these rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses. Other Essential Patent Claims may exist for which a statement 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 are reasonable or non-discriminatory. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the following were participants in the IEEE 802.1 Working Group:

Anthony A. Jeffree, *Chair*

Paul Congdon, *Vice Chair*

Stephen R. Haddock, *Interworking Task Group Chair*

Norman W. Finn, *Editor-in-Chief*

David V. Elie-Dit-Cosaque, **Dinesh Mohan**,
Oscar Rodriguez, **Ali Sajassi**, *Assistant Editors*

Alexei Beliaev
Jean-Michel Bonnamy
Mike Borza
Paul Bottorff
Rudolf Brandner
Jim Burns
Dirceu Cavendish
Frank Chao
Uri Cummings
Russell Dietz
Linda Dunbar
Hesham Elbakoury
Donald W. Fedyk
Felix Feifei Feng
David Frattura
John Fuller
Geoffrey Garner
Anoop Ghanwani
Ken Grewal
Romain Insler
Ran Ish-Shalom

Vipin Jain
Hal Keen
Yongbum Kim
Mike Ko
Bruce Kwan
Kari Laihonon
Yannick Le Goff
David Martin
John Messenger
Hiroshi Ohta
Don Pannell
Glenn Parsons
Ken Patton
Haim Porat
Ray Qiu
Karen Randall
Robert Roden
Josef Roese
Allyn Romanow
Dan Romascanu

Jessy V. Rouyer
Eric Ryu
Panagiotis Saltsidis
Sam Sambasivan
John M. Sauer
Michael J. Seaman
Koichiro Seto
Curtis Simonson
Nurit Sprecher
Kevin B. Stanton
Robert Sultan
Muneyoshi Suzuki
Francois Tallet
Michael Johas Teener
John Terry
Patricia A. Thaler
Dennis Volpano
Manoj Wadekar
Bert Wijnen
Ludwig Winkel
Michael D. Wright

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

Toru Aihara
Thomas Alexander
Butch Anton
Hugh Barrass
Tomo Bogataj
Matthew Burnburg
Edward J. Carley
James T. Carlo
Juan C. Carreon
Keith Chow
Bryan P. Cook
Tommy P. Cooper
Wael W. Diab
Russell S. Dietz

Thomas J. Dineen
Sourav K. Dutta
David V. Elie-Dit-Cosaque
Donald W. Fedyk
Norman W. Finn
C. J. Fitzgerald
Yukihiro Fujimoto
Devon L. Gayle
Michael D. Geipel
Randall C. Groves
C. G. Guy
Stephen R. Haddock
John F. Hawkins
David Hunter

Atsushi Ito
Raj Jain
Anthony A. Jeffree
Michael D. Johas Teener
Peter G. Jones
Bobby Jose
Shinkyō Kaku
Junghong Kao
Piotr Karocki
Stuart J. Kerry
Lior Khernmash
Yongbum Kim
Cees Klik
Thomas M. Kurihara

Jeremy Landt
 Juan L. Lazaro
 John Lemon
 G. Luri
 Arthur Marris
 Marco Mascitto
 Jonathon C. McIendon
 Richard I. Mellitz
 Gary L. Michel
 Dinesh Mohan
 Jose Morales
 Michael S. Newman
 Paul Nikolich
 Satoshi Obara

Robert O'Hara
 Stephen R. Palm
 Vikram Punj
 Jose Puthenkulam
 Maximilian Riegel
 Robert A. Robinson
 Fernando Lucas
 Rodriguez
 Jessy V. Rouyer
 John M. Sauer
 Bartien Sayogo
 Thomas Schossig
 Michael J. Seaman

Amjad A. Soomro
 Matthew B. Squire
 Manikantan Srinivasan
 Thomas E. Starai
 Walter Struppler
 Alourdes T. Sully
 Robert Sultan
 Joseph J. Tardo
 Patricia A. Thaler
 Mark-Rene Uchida
 Stanley S. Wang
 Stephen C. Webb
 Oren Yuen
 Janusz Zalewski

When the IEEE-SA Standards Board approved this standard on 27 September 2007, it had the following membership:

Steve M. Mills, *Chair*

Robert M. Grow, *Vice Chair*

Don Wright, *Past Chair*

Judith Gorman, *Secretary*

Richard DeBlasio
 Alex Gelman
 William R. Goldbach
 Arnold M. Greenspan
 Joanna N. Guenin
 Julian Forster*
 Kenneth S. Hanus
 William B. Hopf

Richard H. Hulett
 Hermann Koch
 Joseph L. Koepfinger*
 John Kulick
 David J. Law
 Glenn Parsons
 Ronald C. Petersen
 Tom A. Prevost

Narayanan Ramachandran
 Greg Ratta
 Robby Robson
 Anne-Marie Sahazizia
 Virginia C. Sulzberger
 Malcolm V. Thaden
 Richard L. Townsend
 Howard L. Wolfman

*Member Emeritus

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

Satish K. Aggarwal, *NRC Representative*

Alan H. Cookson, *NIST Representative*

Michelle D. Turner

IEEE Standards Program Manager, Document Development

Michael D. Kipness

IEEE Standards Program Manager, Technical Program Development

Figures

Figure 6-1—MAC entities, the MAC Service, and MAC Service users (clients).....	14
Figure 6-2—An interface stack.....	15
Figure 6-3—Two back-to-back EISS Multiplex Entities	18
Figure 12-1—Relationships among CFM managed objects.....	24
Figure 18-1—One Maintenance Domain: operator’s view	119
Figure 18-2—One service instance: operator’s view.....	120
Figure 18-3—One service instance: customer’s view	120
Figure 18-4—MEP and MIP Symbols.....	121
Figure 18-5—Maintenance Associations: one service instance in a provider network.....	122
Figure 18-6—Maintenance Associations: Expansion of Figure 18-5.....	123
Figure 18-7—MEPs, MIPs, and MD Levels	124
Figure 19-1—CFM Protocol shims	125
Figure 19-2—Maintenance association End Point (MEP).....	128
Figure 19-3—MIP Half Function	133
Figure 19-4—Linktrace Output Multiplexer shim.....	135
Figure 19-5—Linktrace Output Multiplexer architecture.....	135
Figure 20-1—MEP state machines—overview and relationships	146
Figure 20-2—MEP Continuity Check Initiator state machine	152
Figure 20-3—MHF Continuity Check Receiver state machine.....	153
Figure 20-4—MEP Continuity Check Receiver state machine	156
Figure 20-5—Remote MEP state machine	158
Figure 20-6—Remote MEP Error state machine.....	159
Figure 20-7—MEP Cross Connect state machine	160
Figure 20-8—MP Loopback Responder state machine	162
Figure 20-9—MEP Loopback Initiator transmit state machine.....	164
Figure 20-10—MEP Loopback Initiator receive state machine	165
Figure 20-11—MEP Fault Notification Generator state machine	167
Figure 20-12—MEP Linktrace Initiator receive state machine.....	171
Figure 20-13—Linktrace Responder, MEPs, MHFs, and LOMs	173
Figure 20-14—LTM Receiver state machine	178
Figure 20-15—LTR Transmitter state machine.....	179
Figure 22-1—MEPs and MIPs distinguished by VID (incomplete picture).....	208
Figure 22-2—Alternate view of Forwarding process	209
Figure 22-3—Combining per-VLAN Maintenance Points into two shims	210
Figure 22-4—More complete picture of Maintenance Point placement in a Bridge Port	211
Figure 22-5—Service instance spanning two Bridges protected by Up MPs.....	213
Figure 22-6—Service instance spanning two Bridges protected by Down MPs.....	213
Figure 22-7—Maintenance Point placement in a non-VLAN aware Bridge Port.....	215
Figure 22-8—Maintenance Point placement relative to other standards.....	216
Figure 22-9—Creating MEPs and MIPs.....	219
Figure 22-10—CFM in a Provider Edge Bridge C-tagged service interface.....	225
Figure 22-11—Up MEPs in a Management Port.....	226
Figure 22-12—CFM in the enterprise environment	227
Figure 22-13—CFM on a Bridge conformant to IEEE Std 802.1Q-2005	228
Figure J.1—Up MPs in a CFM Port	244

Tables

Table 8-9—Continuity Check Message Group Destination MAC Addresses.....	22
Table 8-10—Linktrace Message Group Destination MAC Addresses.....	22
Table 17-1—Correspondence between variables, managed objects, and MIB objects.....	43
Table 17-2—Sensitive managed objects: tables and notifications	50
Table 17-3—Sensitive managed objects: variables in dot1agCfmMdTable	50
Table 19-1—Actions taken by MP OpCode Demultiplexers	129
Table 19-2—Received destination_address filtering by CFM entities.....	134
Table 19-3—SAP use for Linktrace Messages and Linktrace Replies.....	136
Table 20-1—Fault Alarm defects and priorities	140
Table 20-2—Deriving enableRmepDefect and Port Status TLV in a Bridge	149
Table 21-1—CFM PDU Encapsulation: Type/Length Media	186
Table 21-2—CFM PDU Encapsulation: LLC Media	186
Table 21-4—OpCode Field range assignments	187
Table 21-3—Common CFM Header format.....	187
Table 21-5—TLV format.....	188
Table 21-6—Type Field values	189
Table 21-7—Organization-Specific TLV format	189
Table 21-8—Sender ID TLV format	190
Table 21-9—Port Status TLV format	191
Table 21-10—Port Status TLV values.....	191
Table 21-11—Interface Status TLV format.....	192
Table 21-12—Interface Status TLV values	192
Table 21-15—Continuity Check Message format	193
Table 21-13—Data TLV format.....	193
Table 21-14—End TLV format	193
Table 21-16—CCM Interval field encoding.....	194
Table 21-17—CCM MAID field format: Maintenance Domain present	195
Table 21-19—Maintenance Domain Name Format	196
Table 21-18—CCM MAID field format: Maintenance Domain not present	196
Table 21-20—Short MA Name Format.....	197
Table 21-21—Loopback Message and Loopback Reply formats.....	198
Table 21-22—Linktrace Message format	199
Table 21-23—Linktrace Message Flags field.....	199
Table 21-25—Linktrace Reply format.....	201
Table 21-24—LTM Egress Identifier TLV format.....	201
Table 21-27—Relay Action field values	202
Table 21-26—Linktrace Reply Flags field	202
Table 21-28—LTR Egress Identifier TLV format.....	203
Table 21-29—Reply Ingress TLV format.....	203
Table 21-30—Ingress Action field values	204
Table 21-31—Reply Egress TLV format	205
Table 21-32—Egress Action field values	205
Table 22-1—MEP creation	218
Table 22-2—MIP creation	220
Table 22-3—Bandwidth required for CCMs for 1 MA	223
Table 22-4—Bandwidth required for CCMs for 1000 MAs	223
Table J.1—Provider MD Level allocation.....	240
Table J.2—IEEE / ITU-T terminology differences	241

Contents

1.	Overview.....	1
1.1	Scope.....	1
2.	Normative references	3
3.	Definitions.....	5
4.	Abbreviations.....	9
5.	Conformance.....	11
5.10	VLAN-aware end station requirements for Connectivity Fault Management.....	11
6.	Support of the MAC Service.....	13
6.1	Basic architectural concepts and terms	13
6.2	Provision of the MAC service.....	16
6.3	Support of the MAC service	17
6.15	EISS Multiplex Entity	18
8.	Principles of bridge operation.....	21
8.3	Model of operation.....	21
8.12	Bridge management entity	21
8.13	Addressing	21
12.	Bridge management	23
12.1	Management functions.....	23
12.2	Managed objects	23
12.14	CFM entities	23
15.	Support of the MAC Service by Provider Bridged Networks	41
15.10	Connectivity Fault Management.....	41
17.	Management protocol	43
17.1	Internet Standard Management Framework.....	43
17.2	Relationship with the managed objects definitions	43
17.3	Relationship to other MIB modules.....	48
17.4	Security	48
17.5	Definitions for the Connectivity Fault Management MIB.....	50
18.	Principles of Connectivity Fault Management operation	117
18.1	Maintenance Domains and Domain Service Access Points	118
18.2	Service instances and Maintenance Associations	119
18.3	Maintenance Domain Levels	121
19.	Connectivity Fault Management Entity operation.....	125
19.1	Maintenance Points.....	125
19.2	Maintenance association End Point	126
19.3	MIP Half Function	131
19.4	Maintenance Point addressing	134

19.5 Linktrace Output Multiplexer	135
19.6 Linktrace Responder	136
20. Connectivity Fault Management protocols	137
20.1 Continuity Check protocol	138
20.2 Loopback protocol	141
20.3 Linktrace protocol	142
20.4 Connectivity Fault Management state machines	146
20.5 CFM state machine timers	146
20.6 CFM procedures	148
20.7 Maintenance Domain variable	148
20.8 Maintenance Association variables	148
20.9 MEP variables	148
20.10 MEP Continuity Check Initiator variables	150
20.11 MEP Continuity Check Initiator procedures	151
20.12 MEP Continuity Check Initiator state machine	151
20.13 MHF Continuity Check Receiver variables	151
20.14 MHF Continuity Check Receiver procedures	152
20.15 MHF Continuity Check Receiver state machine	152
20.16 MEP Continuity Check Receiver variables	153
20.17 MEP Continuity Check Receiver procedures	155
20.18 MEP Continuity Check Receiver state machine	156
20.19 Remote MEP variables	156
20.20 Remote MEP state machine	158
20.21 Remote MEP Error variables	158
20.22 Remote MEP Error state machine	159
20.23 MEP Cross Connect variables	159
20.24 MEP Cross Connect state machine	160
20.25 MP Loopback Responder variables	160
20.26 MP Loopback Responder procedures	161
20.27 MP Loopback Responder state machine	161
20.28 MEP Loopback Initiator variables	162
20.29 MEP Loopback Initiator transmit procedures	163
20.30 MEP Loopback Initiator transmit state machine	163
20.31 MEP Loopback Initiator receive procedures	164
20.32 MEP Loopback Initiator receive state machine	165
20.33 MEP Fault Notification Generator variables	165
20.34 MEP Fault Notification Generator procedures	167
20.35 MEP Fault Notification Generator state machine	167
20.36 MEP Linktrace Initiator variables	168
20.37 MEP Linktrace Initiator procedures	170
20.38 MEP Linktrace Initiator receive variables	170
20.39 MEP Linktrace Initiator receive procedures	171
20.40 MEP Linktrace Initiator receive state machine	171
20.41 Linktrace Responder variables	171
20.42 LTM Receiver procedures	172
20.43 LTM Receiver state machine	178
20.44 LTR Transmitter procedure	178
20.45 LTR Transmitter state machine	179
20.46 CFM PDU validation and versioning	179
20.47 PDU identification	182
20.48 Use of transaction IDs and sequence numbers	183

21.	Encoding of CFM Protocol Data Units.....	185
21.1	Structure, representation, and encoding.....	185
21.2	CFM encapsulation	185
21.3	CFM request and indication parameters	186
21.4	Common CFM Header.....	186
21.5	TLV Format	188
21.6	Continuity Check Message format.....	193
21.7	Loopback Message and Loopback Reply formats	198
21.8	Linktrace Message Format.....	199
21.9	Linktrace Reply Format	201
22.	Connectivity Fault Management in systems	207
22.1	CFM shims in Bridges	207
22.2	Maintenance Entity creation	217
22.3	MPs, Ports, and MD Level assignment.....	221
22.4	Stations and Connectivity Fault Management	222
22.5	Scalability of Connectivity Fault Management	222
22.6	CFM in Provider Bridges.....	224
22.7	Management Port MEPs and CFM in the enterprise environment.....	226
22.8	Implementing CFM on existing Bridges.....	228
Annex A	(normative) PICS proforma.....	229
Annex H	(informative) Bibliography.....	237
Annex J	(informative) Connectivity Fault Management protocol design and use	239

Virtual Bridged Local Area Networks

Amendment 5: Connectivity Fault Management

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

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

1. Overview

Insert the following paragraph after the initial paragraphs in Clause 1:

This standard specifies protocols and protocol entities within the architecture of VLAN-aware Bridges that provide capabilities for detecting, verifying, and isolating connectivity failures in Virtual Bridged Local Area Networks. These capabilities can be used in networks operated by multiple independent organizations, each with restricted management access to each other's equipment.

1.1 Scope

Insert the following at end of 1.1, renumbering the list items so that they follow in order from those in the existing text.

This standard specifies protocols, procedures, and managed objects to support connectivity fault management. These allow discovery and verification of the path, through bridges and LANs, taken for frames addressed to and from specified network users, and support detection and isolation of a connectivity fault to a specific bridge or LAN. To this end it:

- a) Defines Maintenance Domains, Maintenance Associations, their constituent Maintenance Points, and the managed objects required to create and administer them;
- b) Describes the protocols and procedures used by Maintenance Points to detect and diagnose connectivity faults within a Maintenance Domain.

2. Normative references

Change the introductory paragraph as shown, add the references in alphanumeric order, and update the footnote numbering:

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in the text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 802a™-2003, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture—Amendment 1: Ethertypes for Prototype and Vendor-Specific Protocol Development.

IETF RFC 1035 (STD 13), Domain Names: Implementation and Specification.¹

IETF RFC 2119 (BCP 14), Key Words for Use in RFCs to Indicate Requirement Levels.

IETF RFC 2578 (STD 58), Structure of Management Information Version 2 (SMIv2).

IETF RFC 2579 (STD 58), Textual Conventions for SMIv2.

IETF RFC 2580 (STD 58), Conformance Statements for SMIv2.

IETF RFC 2685 (Proposed standard), Virtual Private Networks Identifier.

IETF RFC 2863 (Draft standard), The Interfaces Group MIB.

IETF RFC 3413 (STD 62), Simple Network Management Protocol (SNMP) Applications.

IETF RFC 3414 (STD 62), User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3).

IETF RFC 3415 (STD 62), View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).

IETF RFC 3417 (STD 62), Transport Mappings for the Simple Network Management Protocol (SNMP).

IETF RFC 3418 (STD 62), Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).

IETF RFC 3419 (Proposed standard), Textual Conventions for Transport Addresses.

IETF RFC 4188 (Proposed standard), Definitions of Managed Objects for Bridges.

IETF RFC 4318 (Proposed standard), Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol.

IETF RFC 4363 (Proposed standard), Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions.

IETF RFC 4789 (Proposed standard), Simple Network Management Protocol (SNMP) over IEEE 802 Networks.

¹IETF documents are available at <http://www.ietf.org/>.

ITU-T G.806 (2006), Characteristics of Transport Equipment—Description Methodology and Generic Functionality.²

ITU-T X.690 (2002), Information Technology—ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER), and Distinguished Encoding Rules (DER).

ITU-T Y.1731 (2006), OAM Functions and Mechanisms for Ethernet-based Networks.

²ITU-T publications are available from the International Telecommunications Union, Place des Nations, CH-1211, Geneva 20, Switzerland/Suisse (<http://www.itu.int/>).

3. Definitions

Change the following definition, but do not change the NOTE following this definition.

~~**3.65 service instance:** An instance of the MAC Service, providing the service at a number of service access points. The term “service instance” is often used to refer to the service and connectivity provided by a service provider to a customer.~~

3.65 service instance: A service instance is a set of Service Access Points (SAPs) such that a Data.Request primitive presented to one SAP can result in a Data.Indication primitive occurring at one or more of the other SAPs in that set. In the context of operators and customers, a particular customer is given access to all of the SAPs of such a set by the operator. In customer Bridges the service instance is identified by a C-VID, and in Provider Bridges by an S-VID.

Insert the following definitions, and renumber the definitions in alphabetical order.

3.1 Active SAP: The SAP, bounding an MP, that is on the side of the MP towards the monitored MA.

3.2 Connectivity Fault Management (CFM): Connectivity Fault Management comprises capabilities for detecting, verifying, and isolating connectivity failures in Virtual Bridged Local Area Networks.

3.3 Continuity Check Message (CCM): A multicast CFM PDU transmitted periodically by a MEP in order to ensure continuity over the MA to which the transmitting MEP belongs. No reply is sent by any MP in response to receiving a CCM.

3.4 Domain Service Access Point (DoSAP): A member of a set of SAPs at which a Maintenance Domain is capable of offering connectivity to systems outside the Maintenance Domain. Each DoSAP provides access to an instance either of the EISS or of the ISS.

3.5 Down MEP: A MEP residing in a Bridge that receives CFM PDUs from, and transmits them towards, the direction of the LAN.

3.6 Down MP: A MEP or an MHF residing in a Bridge that receives CFM PDUs from, and transmits them towards, the direction of the LAN.

3.7 EISS Service Access Point (EISS-SAP): An instance of the EISS.

NOTE—See 6.8.

3.8 Fault Alarm: An out-of-band signal, which can be an SNMP Notification, that notifies a system administrator of a connectivity failure.

3.9 Intermediate Service Access Points (ISAP): A SAP, interior to a Maintenance Domain, through which frames can pass in transit from DoSAP to DoSAP.

3.10 ISS Service Access Point (ISS-SAP): An instance of the ISS.

NOTE—See 6.6.

3.11 Layer Management Interface: An interface used for carrying management controls, counters, status parameters, or event indications that are not communicated to an entity's peers.

NOTE—This is not one of the SAPs defined in this standard.

3.12 Linktrace Message (LTM): A CFM PDU initiated by a MEP to trace a path to a target MAC address, forwarded from MIP to MIP, up to the point at which the LTM reaches its target, a MEP, or can no longer be forwarded. Each MP along the path to the target generates an LTR.

3.13 Linktrace Output Multiplexer (LOM): A CFM shim that enables the Linktrace Responder to forward LTMs out a specific Bridge Port without passing the LTMs through the Frame filtering entity.

3.14 Linktrace Reply (LTR): A unicast CFM PDU sent by an MP to a MEP, in response to receiving an LTM from that MEP.

3.15 Loopback Message (LBM): A unicast CFM PDU transmitted by a MEP, addressed to a specific MP, in the expectation of receiving an LBR.

3.16 Loopback Reply (LBR): A unicast CFM PDU transmitted by an MP to a MEP, in response to an LBM received from that MEP.

3.17 Maintenance Association (MA): A set of MEPs, each configured with the same MAID and MD Level, established to verify the integrity of a single service instance. An MA can also be thought of as a full mesh of Maintenance Entities among a set of MEPs so configured.

3.18 Maintenance association End Point (MEP): An actively managed CFM entity, associated with a specific DoSAP of a service instance, which can generate and receive CFM PDUs and track any responses. It is an end point of a single MA and is an end point of a separate Maintenance Entity for each of the other MEPs in the same MA.

3.19 Maintenance association End Point Identifier (MEPID): A small integer, unique over a given MA, identifying a specific MEP.

3.20 Maintenance Association Identifier (MAID): An identifier for a Maintenance Association, unique over the domain that CFM is to protect against the accidental concatenation of service instances. The MAID has two parts: the Maintenance Domain Name and the Short MA Name.

3.21 Maintenance C-VLAN: One C-VLAN, among a number of C-VLANs carried over a single service instance, that is used for CFM PDUs.

3.22 Maintenance Domain: The network or the part of the network for which faults in connectivity can be managed. The boundary of a Maintenance Domain is defined by a set of DoSAPs, each of which can become a point of connectivity to a service instance.

3.23 Maintenance domain Intermediate Point (MIP): A CFM entity consisting of two MHFs.

3.24 Maintenance Domain Name: The identifier, unique over the domain for which CFM is to protect against accidental concatenation of service instances, of a particular Maintenance Domain.

3.25 Maintenance Entity (ME): A point-to-point relationship between two MEPs within a single MA.

3.26 Maintenance Point (MP): One of either a MEP or a MIP.

3.27 MD Level: A small integer in a field in a CFM PDU that is used, along with the VID in the VLAN tag, to identify to which Maintenance Domain among those associated with the CFM frame's VID, and thus to which MA, a CFM PDU belongs. The MD Level determines the MPs that are a) interested in the contents of a CFM PDU, and b) through which the frame carrying that CFM PDU is allowed to pass.

3.28 MEP CCM Database: A database, maintained by every MEP, that maintains received information about other MEPs in the Maintenance Association.

3.29 MIP CCM Database: A database, maintained optionally by a MIP or MEP, that maintains received information about the MEPs in the Maintenance Domain.

3.30 MIP Half Function (MHF): A CFM entity, associated with a single Maintenance Domain, and thus with a single MD Level and a set of VIDs, that can generate CFM PDUs, but only in response to received CFM PDUs.

3.31 MP Level Demultiplexer: The component of an MP that separates CFM PDUs at different MD Levels.

3.32 MP Multiplexer: A component of an MP that merges frames from more than one input SAP, sending them to a single output SAP.

3.33 MP Type Demultiplexer: A component of an MP that identifies and separates CFM PDUs based on the Type/Length field.

3.34 MP OpCode Demultiplexer: A component of an MP that identifies and separates CFM PDUs with different values of the OpCode field.

3.35 Operations, Administration, and Maintenance (OAM): A group of network management functions that provide network fault indication, performance information, and data and diagnosis functions. (adapted from ATM Forum Glossary)

NOTE 1—Examples are ATM OAM {ITU-T I.610 (1999) [B13]}³ and IEEE 802.3 Clause 57 OAM.

3.36 operator: An operator provides a single network of Provider Bridges or a single Layer 2 or Layer 3 backbone network to the service provider.

NOTE 1—An operator can, in fact, be identical to, or a part of the same organization as, the service provider, but for the purposes of this standard, the operator and service provider are presumed to be separate organizations.

NOTE 2—Certain terms in this standard, including “customer,” “service provider,” and “operator” reflect common business relationships that often exist among organizations and individuals that use equipment implemented in accordance with this standard. Terms such as “customer VID” or “operator MD Level” are no more than convenient labels for entities defined here; their use does not imply any requirement upon the business relationships among vendors or users of devices compliant with this standard.

3.37 Owner: An Owner of a system (and in particular, a Bridge) is a user who has full access to the System Group of the SNMPv2-MIB (IETF RFC 3418).

3.38 Passive SAP: The SAP, bounding an MP, that is on the side of the MP away from the monitored MA.

3.39 Primary VID: The VID, among a list of VIDs associated with a service instance, on which all CFM PDUs generated by MPs except for forwarded LTMs are to be transmitted.

3.40 Service Access Point (SAP): The point at which a service is offered.

NOTE—In this standard, an instance of either the ISS (6.6) or the EISS (6.8). This term is used in place of the awkward “ISS Service Access Point” or “EISS Service Access Point,” where no loss of clarity is introduced.

3.41 shim: A protocol entity that uses the same service as it provides.

NOTE—Within this standard, shims make use of the ISS or the EISS.

³The numbers in brackets correspond to those of the bibliography in Annex H.

3.42 Short MA Name: The part of the MAID that is unique within the Maintenance Domain and is appended to the Maintenance Domain Name to form the MAID.

3.43 Up MEP: A MEP residing in a Bridge that transmits CFM PDUs towards, and receives them from, the direction of the Bridge Relay Entity.

3.44 Up MP: A MEP or an MHF residing in a Bridge that transmits CFM PDUs towards, and receives them from, the direction of the Bridge Relay Entity.

4. Abbreviations

Insert the following abbreviations in alphabetical order:

CCM	Continuity Check Message
CFM	Connectivity Fault Management
DoSAP	Domain Service Access Point
ISAP	Intermediate Service Access Point
ITU-T	International Telecommunications Union—Telecommunication Standardization Sector
LBM	Loopback Message
LBR	Loopback Reply
LMI	Layer Management Interface
LOM	Linktrace Output Multiplexer
LTM	Linktrace Message
LTR	Linktrace Reply
ME	Maintenance Entity
MA	Maintenance Association
MAID	Maintenance Association Identifier
MEP	Maintenance association End Point
MEPID	Maintenance association End Point Identifier
MHF	MIP Half Function
MIP	Maintenance domain Intermediate Point
MP	Maintenance Point
MSAP	MAC Service Access Point

5. Conformance

5.4.1 VLAN-aware Bridge component options

Insert the following item after item b) in 5.4.1 and renumber the list items:

- c) Support CFM operation (5.4.1.3);

Insert the following subclause after 5.3.1.2:

5.4.1.3 Connectivity Fault Management (optional)

A VLAN-aware Bridge component implementation that conforms to the provisions of this standard for Connectivity Fault Management (Clause 18, Clause 19, Clause 20, Clause 21, Clause 22) shall:

- a) Support the creation of Maintenance Domains at eight MD Levels, with multiple non-overlapping Maintenance Domains at each MD Level, using the managed objects specified in 12.14;
- b) Support the creation of a Maintenance Association (MA) on each VLAN supported by the Bridge for each MD Level;
- c) Support the creation of a single MIP for each Maintenance Domain on each Port, all MIPs being at the same MD Level;
- d) Support the creation of eight Up MEPs on each VLAN on each Port, each MEP at a different MD Level;
- e) Support the creation of eight Down MEPs on each VLAN on each Port, each MEP at a different MD Level;
- f) Support the creation of eight Down MEPs attached to no VLAN on each Port, each MEP at a different MD Level;
- g) Support the maintenance of a MEP CCM Database;
- h) Provide control via all of the required managed objects specified in 12.14;
- i) Conform to the state machines and procedures in Clause 20; and
- j) Transmit and receive required CFM PDUs in the formats specified in Clause 21.

A VLAN-aware Bridge component implementation that conforms to the provisions of this standard for Connectivity Fault Management may:

- k) Support the creation of MIPs at different MD Levels on a single Port;
- l) Support the creation of MIPs at lower or equal MD Levels than MEPs on the same Port;
- m) Support the maintenance of a MIP CCM Database in a MIP or MEP;
- n) Support the CFM Management Information Base (MIB) module defined in 17.5; and/or
- o) Support the creation of MAs that are associated with more than one VLAN (see 22.1.5).

Insert the following subclause after 5.9:

5.10 VLAN-aware end station requirements for Connectivity Fault Management

A VLAN-aware Station implementation that conforms to the provisions of this standard for Connectivity Fault Management (Clause 18, Clause 19, Clause 20, Clause 21, Clause 22) shall:

- a) Support the creation of Maintenance Domains at eight MD Levels, with multiple non-overlapping Maintenance Domains at each MD Level, using the managed objects specified in 12.14;
- b) Support the creation of a Maintenance Association (MA) on each VLAN supported by the Station for each MD Level;
- c) Support the creation of eight Down MEPs on each VLAN on each Port, each MEP at a different MD Level;

- d) Support the creation of eight Down MEPs attached to no VLAN on each Port, each MEP at a different MD Level;
- e) Support the maintenance of a MEP CCM Database;
- f) Provide control via all of the required managed objects specified in 12.14;
- g) Conform to the state machines and procedures in Clause 20; and
- h) Transmit and receive required CFM PDUs in the formats specified in Clause 21.

A VLAN-aware Station implementation that conforms to the provisions of this standard for Connectivity Fault Management may:

- i) Support the CFM Management Information Base (MIB) module defined in 17.5; and/or
- j) Support the creation of MAs that are associated with more than one VLAN (see 22.1.5).

6. Support of the MAC Service in VLANs

Change the title of Clause 6, and delete the last paragraph of the introductory text as shown:

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

Insert the following text after the introductory text to Clause 6, before 6.1:

This clause:

- a) Summarizes basic architectural concepts and terms used throughout this standard, introduces the primitives and parameters of the MAC Service, and defines VLANs in terms of the connectivity provided to service users (6.1, 6.2, 6.3);
- b) Describes how Bridges preserve and maintain the quality of the MAC Service (6.4, 6.5);
- c) Specifies the MAC Internal Sublayer Service (ISS) and MAC status parameters, and their support by specific media access methods (6.6, 6.7, 6.11);
- d) Specifies the Enhanced Internal Sublayer Service (EISS) used by VLAN-aware stations, the encoding of VLAN identifier and priority parameters in transmitted frames, and the classification of received frames that do not explicitly convey those parameters (6.8, 6.9, 6.10); and
- e) Specifies how entities defined in terms of the ISS can support the EISS (6.15).

Insert the following new subclauses before 6.1, and renumber the subsequent subclauses.

6.1 Basic architectural concepts and terms

The architectural concepts used in this and other IEEE 802.1 standards are based on the layered protocol model introduced by the OSI Reference Model (ISO/IEC 7498-1) and used in the MAC Service Definition (ISO/IEC 15802-1), in IEEE Std 802[®], in other IEEE 802 standards, and elsewhere in networking. IEEE 802.1 standards in particular have developed terms and distinctions useful in describing the MAC Service and its support by protocol entities within the MAC Sublayer.⁴

6.1.1 Protocol entities, peers, layers, services, and clients

The fundamental notion of the model is that each protocol entity within a system is instantiated at one of a number of strictly ordered layers, and communicates with peer entities (operating the same or an interoperable protocol within the same layer) in other systems by using the service provided by interoperable protocol entities within the layer immediately below, and thus provides service to protocol entities in the layer above. The implied repetitive stacking of protocol entities is essentially unbounded at the lowest level and is bounded at the highest level by an application supported by peer systems. In descriptions of the model, the relative layer positions of protocol entities and services is conventionally referred to by N , designating a numeric level. The N -service is provided by an N -entity that uses the $(N - 1)$ service provided by the $(N - 1)$ entity, while the N -service user is an $(N + 1)$ entity. Figure 6-1 illustrates these concepts with reference to the MAC Sublayer, which contains MAC entities that provide the MAC Service, to MAC Service users.

6.1.2 Service interface primitives, parameters, and frames

Each N -service is described in terms of service primitives and their parameters, each primitive corresponding to an atomic interaction between the N -service user and the N -service provider, with each invocation of a primitive by a service user resulting in the service issuing corresponding primitives to peer

⁴Drawing on prior network layer standards, including ISO/IEC 7498-1, wherever possible.

service users. The purpose of the model is to provide a framework and requirements for the design of protocols while not unnecessarily constraining the internal design of systems: primitives and their parameters are limited to, but include all of the information elements conveyed to corresponding peer protocol entities or required by other systems (and not supplied by protocols in lower layers) to identify (address) those entities and deliver the information. The parameters of service primitives do not include information that is used only locally, i.e., within the same system, to identify entities or organize resources for example.⁵

The primitives of the MAC Service comprise a data request and a corresponding data indication, each with MAC destination address, MAC source address, a MAC service data unit comprising one or more octets of data, and priority parameters. Taken together these parameters are conveniently referred to as a frame, although this does not imply that they are physically encoded by a continuous signal on a communication medium, that no other fields are added or inserted by other protocol entities prior to transmission, or that the priority is always encoded with the other parameters transmitted.

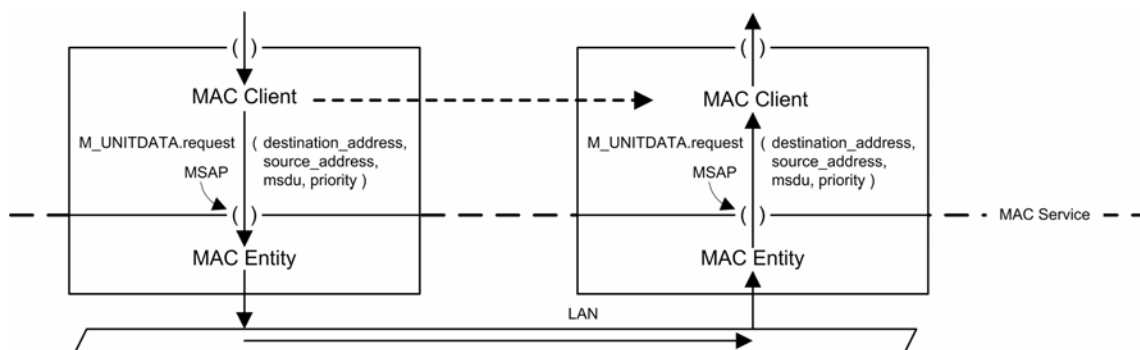


Figure 6-1—MAC entities, the MAC Service, and MAC Service users (clients)

6.1.3 Layer management interfaces

A given N-entity can have many associated management controls, counters, and status parameters that are not communicated to its user's peers and whose values are either not determined by its user or not required to change synchronously with the occurrence of individual N-service primitives to ensure successful (N + 1)-protocol operation. Communication of the values of these parameters to and from local entities, i.e., within the same system, is modeled as occurring not through service primitives⁶ but through a layer management interface (LMI). One protocol entity, for example an SNMP entity, can be used to establish the operational parameters of another. Communication of the results of Fault Alarms to entities responsible for managing the network is one of the uses of LMIs in this standard.

⁵These points are frequently misunderstood by those unfamiliar with the reference model, who take it as simply restating common sense principles of modular engineering. Early variants of the MAC Service, for example, omitted the source MAC address parameter on the grounds that it was a fixed property of the transmitting station and should be supplied by the MAC entity itself, despite the fact that communicating peer service users (and the protocols they operate) required that information. The introduction of MAC Bridges necessitated the development of a MAC Internal Sublayer Service with the required parameter, and has led to a restatement of the service definition included in a number of standards. However the source address parameter would still have been required even if MAC Bridges did not exist. Similarly versions of the MAC Service have included local acknowledgment primitives or status return codes for primitives issued. These play no part in defining the peer-to-peer communication and do not conform to the reference model. The scope of some IEEE 802 standards does include the definition of interfaces, particularly electrical interfaces, within systems. These play a valuable role in defining components used to build those systems, but should not be confused with OSI service interfaces.

⁶This would require considerable enlargement and continuous modification of service interfaces, obscuring their original purpose, not to mention the creation of many additional interfaces and the addition of "pass-through" functions to others.

6.1.4 Service access points, interface stacks, and ports

Each service is provided to a single protocol entity at a service access point (SAP) within a system. A given N-entity can support a number of N-SAPs and use one or more $(N - 1)$ -SAPs. The SAP serves to delineate the boundary between protocol specifications and to specify the externally observable relationship between entities operating those protocols. An SAP is an abstraction and does not necessarily correspond to any concrete realization within a system, but an N-entity often associates management counters with the SAP and provides status parameters that can be used by the $(N + 1)$ -entity using the SAP. Examples include the MAC_Operational and operPointToPoint MAC status parameters (6.6.2, 6.6.3).

The network and link layers⁷ of the reference model accommodate many different real networks, subnetworks, and links with the requirements for bandwidth, multiplexing, security, and other aspects of communication differing from network to network. A given service, e.g., the MAC Service, is often provided by a number of protocols, layered to achieve the desired result. Together the entities that support a particular SAP compose an interface stack. Figure 6-2 provides an example, showing the use of Link Aggregation (IEEE Std 802.3, Clause 43).

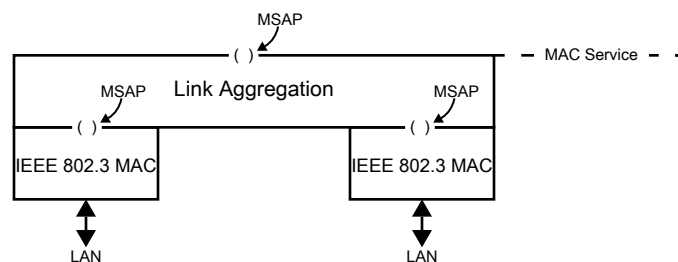


Figure 6-2—An interface stack

The term “port” is used to refer to the interface stack for a given SAP. Often the interface stack comprises a single protocol entity attached to a single LAN, and port can be conveniently used to refer to several aspects of the interface stack, including the physical interface connector for example. In more complex situations—such as that in Figure 6-2, where the parts of the interface stack provided by the IEEE 802.3 MAC entities effectively compose two ports that are then used by link aggregation to provide a single port to its user—the port has to be clearly specified in terms of the particular SAP supported.

6.1.5 MAC method independent protocols and shims

Protocols specified in IEEE Std 802.3, IEEE Std 802.11™-2007 [B5], and other IEEE 802 standards, can be specific to their LAN media or to the way access to that media is controlled. Other protocols and functions within the MAC sublayer, such as link aggregation and bridging, are MAC method independent—thus providing consistent management and interoperability across a range of media.

Definition of a service facilitates the specification of shims, i.e., protocol entities that use the same service as they provide. Protocol shims can be inserted into an interface stack to provide aggregation (e.g., IEEE Std 802.3, Clause 43), security (e.g., IEEE Std 802.1AE™-2006 [B4]), or multiplexing.

⁷The data link layer, as originally envisaged by the OSI reference model, contained no addressing and caused some involved in its development to reject the idea of LANs at the link layer. There is a sound argument for regarding LANs as simply subnetworks within the network layer, and in practice this is how they are treated. However this would have been unpalatable to many more people at a time when correspondence between LLC (IEEE Std 802.2) and HDLC was sought, together with the adoption of a unique network layer protocol (X.25). Continuing to regard the MAC Sublayer as part of the OSI Data Link Layer does relatively little harm, except when duplication of network layer functionality is proposed, and is convenient given the mass of historic documentation.

6.1.6 MAC Service clients

The protocol entity that uses the service provided at an MSAP is commonly referred to as client of the MAC Service or of the entity providing the service. Clients of the MAC Service (or ISS) include the MAC Relay Entity and the LLC Entity specified in IEEE Std 802.2. The latter provides protocol identification, multiplexing and demultiplexing to and from a number of clients that use a common MSAP. The clients of LLC are also often referred to as clients of the MAC.

NOTE—For the purposes of this standard, the terms “LLC” and “LLC Entity” include the service provided by the operation of entities that support protocol discrimination using an Ethertype, i.e., protocol discrimination based on the Type interpretation of the Ethertype field as specified in IEEE Std 802a™-2003 [B2].

6.1.7 Stations and systems

A LAN station comprises a single media access method specific entity, operating the MAC procedures specified in the applicable IEEE 802 standard, together with other protocol entities mandated by those standards (e.g., an LLC Entity) or commonly used in conjunction with that entity.

A system is a collection of hardware and software components whose intercommunication is not directly externally observable and outside the scope of the IEEE 802 standards that specify the system behavior as a whole. Management of a system, when supported, is typically provided through a single management entity. A system (such as a bridge) can contain many media access method specific entities, of the same or a variety of types, attached to different LANs. A system can therefore be said to comprise one or more LAN stations.

6.1.8 Connectionless connectivity

The MAC Service supported by an IEEE 802 LAN provides connectionless connectivity, i.e., communication between attached stations occurs without explicit a priori agreement between service users. The potential connectivity offered by a connectionless service composes a connectivity association that is established prior to the exchange of service primitives between service users. The way in which such a connectivity association is established depends on the particular protocols and resources that support it, and can be as simple as making a physical attachment to a wire. However simple or complex, the establishment of a connectivity association for connectionless data transfer involves only a two-party interaction between the service user and the service provider (though it can result in exchanges between service providing entities in several systems) and not a three-party user-service-user interaction as is the case for connection-oriented communication. With the continual increase in the number of ways that IEEE 802 LAN connectivity can be supported it is no longer useful to regard a LAN as a definite set of physical equipment, instead the connectivity association that exists between a set of MAC Service access points defines a LAN.⁸

6.2 Provision of the MAC service

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

NOTE 1—The primitives of the MAC Service are closely aligned with those of the ISS (6.6).

⁸A LAN is thus defined in terms of its external observable behavior, not by an abstraction of its internal operation.

In a Bridged Local Area Network, MAC Bridges (IEEE Std 802.1D) provide a single instance of the MAC Service for the network as a whole—a single LAN, as previously defined (6.1.8)—by forwarding between the individual LANs that compose the network, though frames with specified group destination addresses are confined to individual LANs.

NOTE 2—MAC Bridges can be configured to completely partition a bridged network, though that is rarely intended.

In a Virtual Bridged Local Area Network, Virtual LANs are defined in terms of the connectivity associations (6.1.8) supported by the network: if service requests made at two different MSAPs both result in service indications at any third MSAP, then the two MSAPs are transmitting on the same VLAN; and if the service requests made at any given MSAP can result in service indications at either (or both) of two MSAPs, then those two MSAPs are receiving on the same VLAN. When only two MSAPs are in bidirectional communication, they are using the same VLAN for both transmit and receive if a third station could be added in such a way that it would receive transmissions from both.

NOTE 3—This definition of a VLAN accommodates an unavoidable and sometimes useful consequence of configuration possibilities: use of a single MSAP can result in transmission on one VLAN and reception on another.

NOTE 4—Protocol VLAN classification can be used to classify frames transmitted from a single MSAP into separate VLANs. Where protocol classification is used, the preceding rules apply to frames of a single classification.

6.3 Support of the MAC service

Delete the first paragraph in 6.3 as follows.

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

Delete the last paragraph of 6.3 and the accompanying NOTE as follows:

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

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

Insert the following text at the beginning of 6.3:

In a Bridged Local Area Network at most one LAN can be supported on each of the individual LANs that, bridged together, compose the network. On the individual LANs of a Virtual Bridged Local Area Network, frames for different VLANs can be distinguished by the addition of a VLAN tag as the initial octets of a frame's MSDU.

When a VLAN-unaware end station is attached to an individual LAN, it will transmit and receive only untagged frames, and thus uses the VLAN(s) assigned by the Bridge Ports that classify those frames.

NOTE 1—Where there are only two stations attached to an individual LAN, each can assign received untagged frames to a different VLAN. However such assignments can defeat the operation of network configuration protocols and can only be recommended at the edge of a network to facilitate initial classification of untagged frames transmitted by VLAN-unaware end stations. Otherwise a change in a frame's VLAN can severely impact network operation by introducing frame forwarding loops. The same considerations apply to the use of protocol VLAN classification. The use of different VLAN assignments by Bridge Ports attached to the same LAN is usually a network configuration error.

NOTE 2—The LLC Entity in a VLAN-unaware end station can receive MAC Service indications that correspond to the receipt of VLAN-tagged frames but, being unable to recognize the tag's Ethertype value, will discard the frame and not deliver it to any LLC User.

A VLAN-aware end station uses the EISS Multiplex Entity (6.15) to provide multiple MSAPs, one per VLAN of interest, to separate MAC Clients.

Insert a new subclause at the end of Clause 6:

6.15 EISS Multiplex Entity

The EISS Multiplex Entity enables shims defined for the ISS to use the EISS. Figure 6-3 illustrates two EISS Multiplex Entities placed back-to-back.

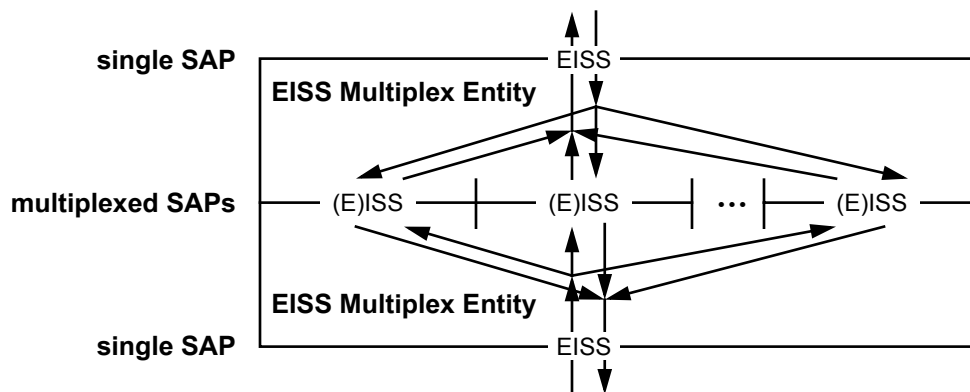


Figure 6-3—Two back-to-back EISS Multiplex Entities

An EISS Multiplex Entity has one EISS SAP, and a number of multiplexed SAPs, each either an ISS SAP or an EISS SAP. Each multiplexed ISS SAP is assigned to a single `vlan_identifier` value. Each multiplexed EISS SAP is assigned to one or more `vlan_identifier` values. Every `vlan_identifier` is assigned to some multiplexed SAP. Upon receiving a Request or Indication from its single EISS SAP, the EISS Multiplex Entity uses the `vlan_identifier` and `canonical_format_indicator` to select the corresponding one of its multiplexed SAPs to present the Request or Indication. Similarly, any Request or Indication received from a multiplexed SAP is presented to the single EISS SAP; the `vlan_identifier` and `canonical_format_indicator` parameters presented on the single EISS SAP are the ones associated with the multiplexed ISS SAP, or the ones obtained from the multiplexed EISS SAP.

Shims can be multiplied in this fashion to separately serve multiple `vlan_identifiers`. Figure 22-1 illustrates CFM shims deployed in this manner.

The `rif_information` parameter is not a parameter of the single EISS of an EISS Multiplex Entity if it uses the ISS on any of its multiplexed SAPs. The ISS does not support media that require the `rif_information` parameter.

The `MAC_Operational` status parameter (6.6.2) presented to the uppermost EISS-SAP in Figure 6-3 is true if and only if:

- a) The uppermost EISS-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 lower EISS Multiplex Entity's multiplexed SAPs in Figure 6-3 is computed separately and is true if and only if:

- c) The lowermost EISS-SAP's MAC_Operational parameter is true; and
- d) That multiplexed SAP's MAC_Enabled parameter is true.

8. Principles of bridge operation

8.3 Model of operation

Insert item 4) at the end of list b):

- 4) Linktrace response

Insert the following list immediately following list b):

- c) Zero or more Connectivity Fault Management (CFM) Entities, each of which can be either:
 - 1) A Maintenance association End Point (MEP);
 - 2) A Maintenance association Intermediate Point (MIP); or
 - 3) A Linktrace Output Multiplexer.

8.6.7 Queue management

Change item c) and insert a NOTE immediately following item c) as follows:

- c) If the associated Port leaves the Forwarding state. Frames entering the queue subsequent to the transition out of the Forwarding state (e.g., CFM frames from Down MPs, as described in 22.1, Figure 22-4, and Figure 22-7) are not discarded.

NOTE—CFM frames may be excepted, and not removed from the queue, on a transition out of the Forwarding state (see 22.1.3).

8.12 Bridge management entity

Change the following list items, delete footnotes 16–18, and renumber the remaining footnotes:

- b) ~~IETF RFC 1493~~ IETF RFC 4188;
- c) ~~RSTP MIB~~ IETF RFC 4318;
- d) ~~MSTP MIB~~ IETF RFC 4363;

Insert item e) immediately following item d):

- e) CFM MIB (17.5).

8.13 Addressing

Insert the following subclause after 8.13.10.

8.13.11 Connectivity Fault Management entities

CFM entities reside in shims. The entities in a CFM shim inspect every frame that passes through either of the shim's two SAPs, and decides whether to pass that frame through to the other SAP, process it, or both. The decision whether pass it through is not dependent on the destination_address, but the decision whether to process the frame is dependent on the destination_address (see Clause 19). A CFM entity shall discard any frame, directed to it by reason of its VID and MD Level, whose destination_address parameter does not correspond to a MAC address recognized by that CFM entity.

Any given CFM entity is configured to recognize one Individual MAC address, and one or more Group MAC addresses, in received frames, and to use one or two of the Group MAC addresses for transmitted frames. The Individual MAC address is unique, within a bridged network, to a specific Bridge, though not

necessarily to a single Bridge Port (J.6). The Group MAC addresses are selected from Table 8-9 and Table 8-10 according to the MD Level and OpCode fields in the CFM PDU header. Loopback Messages (LBMs, 20.2), Loopback Replies (LBRs, 20.2), and Linktrace Replies (LTRs, 20.3) are carried in unicast frames. Continuity Check Messages (CCMs, 20.1) use addresses from Table 8-9, and Linktrace Messages (LTMs, 20.3) use addresses from Table 8-10.

Table 8-9—Continuity Check Message Group Destination MAC Addresses

01-80-C2-00-00-3y	
MD Level of CCM	Four address bits “y”
7	7
6	6
5	5
4	4
3	3
2	2
1	1
0	0

Table 8-10—Linktrace Message Group Destination MAC Addresses

01-80-C2-00-00-3y	
MD Level of LTM	Four address bits “y”
7	F
6	E
5	D
4	C
3	B
2	A
1	9
0	8

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

12. Bridge management

12.1 Management functions

Insert the following paragraph at the end of 12.1.

It can be necessary, particularly in Provider Bridged Networks, for multiple organizations to manage a single Bridge, with each organization having different abilities to manage, or even detect the existence of, Bridge Ports, Bridges, or entire networks. Access to all of the managed objects in Clause 12 for reading, writing, or detection can be restricted. Access by certain organizations can be limited to only a small number of managed objects, particularly to those specified in 12.14.

12.1.1 Configuration management

Insert the following item g) after the last list item.

- g) The ability to create and delete the functional elements of Connectivity Fault Management and to control their operation.

12.1.2 Fault management

Insert the following item h) after the last list item.

- h) Within the context of multiple management organizations, the ability to:
 - 1) Actively monitor the connectivity of a set of managed end points on individual VLANs, simultaneously over multiple physical extents;
 - 2) Actively monitor and ensure the segregation of data among different VLANs;
 - 3) Issue trains of point-to-point query-response messages to selected network components in a VLAN; and
 - 4) Issue multicast query-relay-response messages to determine the path taken by frames addressed to specific individual MAC addresses through a VLAN.

12.2 Managed objects

Insert the following item i) after the last list item.

- i) The CFM Entities (12.14).

Insert the following subclause at the end of Clause 12.

12.14 CFM entities

The CFM managed objects model operations that modify, or enquire about, the configuration and the operation of CFM. Figure 12-1 illustrates the simple hierarchical relationships among the various CFM managed objects, including the control of access to those objects. See 17.5 for an explanation of methods available to distinguish between an Owner and a Maintenance Domain administrator. See Clause 18 for an explanation of the use of Maintenance Domains and Maintenance Associations (MAs). The following are the CFM managed objects in a Bridge:

- a) Maintenance Domain list managed object (12.14.1);
- b) CFM Stack managed object (12.14.2);
- c) Default MD Level managed object (12.14.3);
- d) Configuration Error List managed object (12.14.4);
- e) Maintenance Domain managed objects (12.14.5);

- f) Maintenance Association managed objects (12.14.6); and
- g) Maintenance association End Point managed objects (12.14.7).

12.14.1 Maintenance Domain list managed object

There is one Maintenance Domain list managed object per Bridge. It contains a list of the Maintenance Domains that have been configured on the Bridge.

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

- a) Read Maintenance Domain list (12.14.1.1);
- b) Create Maintenance Domain managed object (12.14.1.2); and
- c) Delete Maintenance Domain managed object (12.14.1.3).

NOTE—In Provider Bridge applications, each Maintenance Domain, and thus each Maintenance Domain managed object, can be controlled by a different administrative organization. Some or all of these administrative organizations can be different from that which controls the Maintenance Domain list managed object or the managed objects in Clause 12 other than those in 12.14. See 17.4 for a discussion of the means by which control of and access to different instances of the Maintenance Domain managed object are allocated to these different administrative organizations.

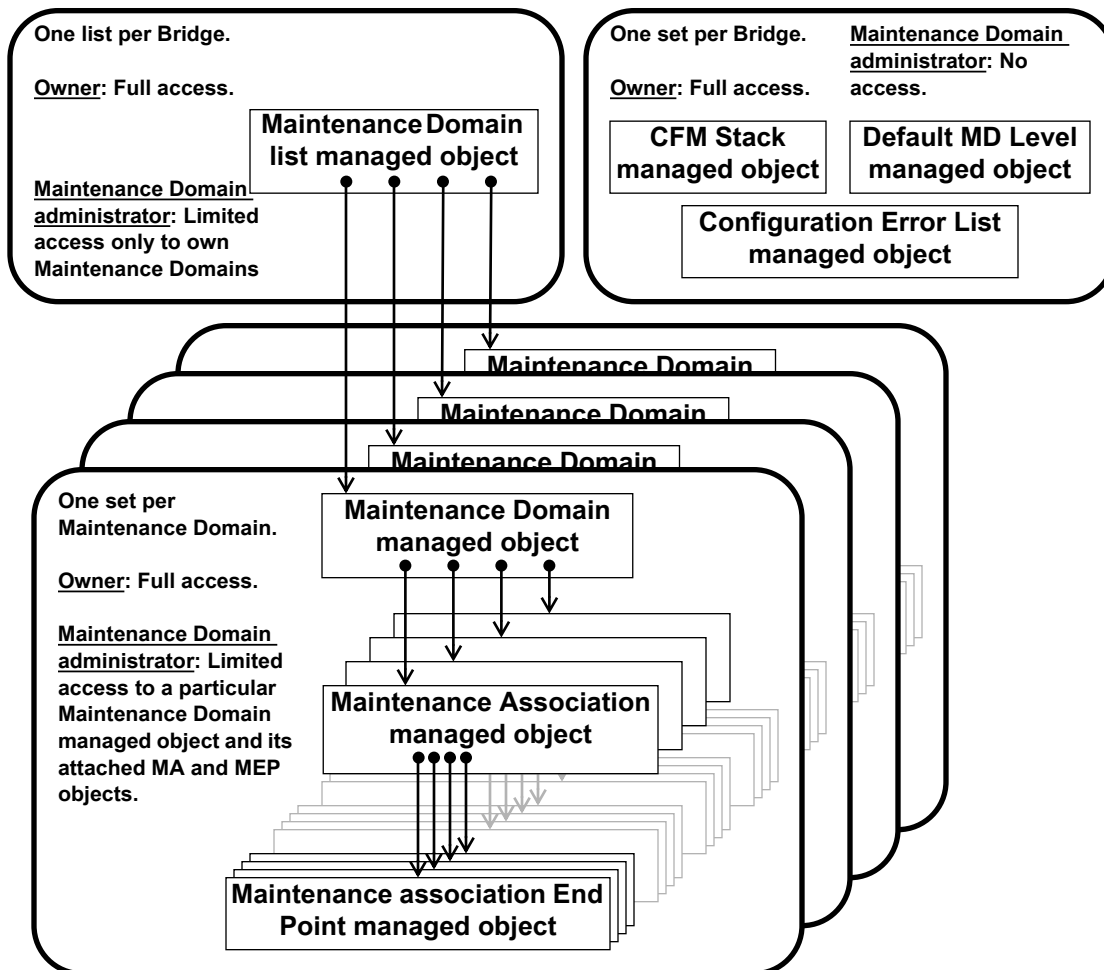


Figure 12-1—Relationships among CFM managed objects

12.14.1.1 Read Maintenance Domain list**12.14.1.1.1 Purpose**

To obtain information about all of the Maintenance Domains in a Bridge.

12.14.1.1.2 Inputs

None.

12.14.1.1.3 Outputs

- a) A list, perhaps empty, of the Maintenance Domain managed objects configured on the Bridge. For each item in the list, the Read Maintenance Domain list command returns:
 - 1) A Maintenance Domain Name, including the format specifier from Table 21-19 (21.6.5.1); and
 - 2) A reference to that Maintenance Domain's Maintenance Domain managed object (12.14.5).

12.14.1.2 Create Maintenance Domain managed object**12.14.1.2.1 Purpose**

To create a new Maintenance Domain managed object in a Bridge, and add it to the Bridge's Maintenance Domain list managed object.

12.14.1.2.2 Inputs

- a) A Maintenance Domain Name, including the format specifier from Table 21-19 (21.6.5.1); default value is the character string (format 4) "DEFAULT"; and
- b) The MD Level at which the Maintenance Domain is to be created; default value is 0.

12.14.1.2.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to invalid Maintenance Domain Name (21.6.5.1);
 - 2) Operation rejected because Maintenance Domain Name already exists;
 - 3) Operation rejected due to invalid MD Level; or
 - 4) Operation accepted.

12.14.1.3 Delete Maintenance Domain managed object**12.14.1.3.1 Purpose**

To delete a specific Maintenance Domain managed object from a Bridge and from the Bridge's Maintenance Domain list managed object.

12.14.1.3.2 Inputs

- a) A reference to a particular Maintenance Domain managed object (12.14.5).

12.14.1.3.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to invalid or nonexistent Maintenance Domain; or
 - 2) Operation accepted.

12.14.2 CFM Stack managed object

There is one CFM Stack managed object per Bridge. It permits retrieval of information about the Maintenance Points configured on a particular Bridge Port or aggregated port. The management operation that can be performed is:

- a) Read CFM Stack managed object (12.14.2.1).

12.14.2.1 Read CFM Stack managed object

12.14.2.1.1 Purpose

To obtain the contents of the CFM Stack managed object, which allows a network administrator to discover the relationships among MEPs and MHFs configured on a particular Bridge Port or aggregated port.

12.14.2.1.2 Inputs

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

12.14.2.1.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to illegal inputs;
 - 2) No MP is configured on the indicated Bridge Port or aggregated port at the indicated MD Level and direction;
 - 3) A MEP is configured; or
 - 4) An MHF is configured;
- b) Either the Maintenance Domain managed object (12.14.5) to which the MP's MA is associated, or an indication that there is no Maintenance Domain associated with the MP;
- c) Either the Maintenance Association managed object (12.14.6) to which the MP is associated, or an indication that there is no MA associated with the MP;
- d) If a MEP is configured, its MEPID, else 0; and
- e) The MAC address of the MP.

12.14.3 Default MD Level managed object

There is a single Default MD Level managed object per Bridge. It controls MIP Half Function (MHF) creation for VIDs that are not contained in the list of VIDs attached to any specific Maintenance Association managed object [item c) in 12.14.5.3.2], and the transmission of the Sender ID TLV (21.5.3) by those MHFs.

The management commands that can be performed on the Default MD Level managed object are as follows:

- a) Read Default MD Level managed object (12.14.3.1); and
- b) Write Default MD Level managed object (12.14.3.2).

12.14.3.1 Read Default MD Level managed object

12.14.3.1.1 Purpose

To read the table of default parameters for controlling MHFs on VIDs not associated with any MA.

12.14.3.1.2 Input

- a) A VID.

12.14.3.1.3 Output

- a) A list of VIDs associated with any MHF on the VID named in item a) in 12.14.3.1.2, always including that VID. The first VID is the MAs' Primary VID. List is empty if no VID specified in 12.14.3.1.2;
- b) A Boolean value indicating whether this entry is in effect or has been overridden by the existence of a Maintenance Association managed object associated with the same VID and MD Level, and on which is configured an Up MEP. True if this Maintenance Domain managed object is in effect;
- c) (writable) The MD Level at which MHFs are to be created;
- d) (writable) An enumerated value indicating whether the management entity can create MHFs for this VID(s), either defMHFnone (1, the default), defMHFdefault (2), or defMHFexplicit (3) (22.2.3); and
- e) (writable) An enumerated value indicating what, if anything, is to be included in the Sender ID TLV (21.5.3) transmitted by MPs configured in the Default Maintenance Domain, either sendIdNone (1, the default value), sendIdChassis (2), sendIdManage (3), or sendIdChassisManage (4).

12.14.3.2 Write Default MD Level managed object

12.14.3.2.1 Purpose

To write entries in the table of default parameters for controlling MHFs on VIDs not associated with any MA.

12.14.3.2.2 Inputs

- a) A list of VIDs, or 0, indicating no VID. The first VID in the list is the Primary VID;
- b) One of the writable managed object in 12.14.3.1.3.

12.14.3.2.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected because creating or assigning these VIDs to this MD Level would exceed the number of MD Levels supported by some Bridge Port (item c) in 22.2.4);
 - 2) Operation rejected because the VID list provided [item a) in 12.14.3.2.2] specifies a different Primary VID, or contains one or more but not all of the VIDs, in the definition of an MA or some other entry in the Default MD Level managed object; or
 - 3) Operation accepted.

12.14.4 Configuration Error List managed object

The Configuration Error List managed object provides a list of Bridge Ports, aggregated ports, and VIDs that are incorrectly configured.

12.14.4.1 Read Configuration Error List managed object

12.14.4.1.1 Purpose

To read entries in the list of Bridge Ports or aggregated ports and VLANs currently configured in error. The Configuration Error List managed object lists only those Bridge Ports or aggregated ports and `vlan_identifiers` that have configuration errors.

12.14.4.1.2 Inputs

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

12.14.4.1.3 Outputs

- a) An indication of the result of the operation, either:
 - 1) Operation rejected due to illegal `vlan_identifier`;
 - 2) Operation rejected due to illegal or non-existent Bridge Port or aggregated port; or
 - 3) Operation accepted; and
- b) If the operation was accepted, a vector of Boolean error conditions from 22.2.4, any of which may be true:
 - 1) CFMleak;
 - 2) ConflictingVLANs;
 - 3) ExcessiveLevels; and/or
 - 4) OverlappedLevels.

12.14.5 Maintenance Domain managed object

There can be any number of Maintenance Domain managed objects per Bridge. A Maintenance Domain managed object is required in order to create an MA with a MAID that includes that Maintenance Domain's Name. From this Maintenance Domain managed object, all Maintenance Association managed objects associated with that Maintenance Domain managed object can be accessed, and thus controlled.

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

- a) Read Maintenance Domain managed object (12.14.5.1);
- b) Write Maintenance Domain managed object (12.14.5.2);
- c) Create Maintenance Association managed object (12.14.5.3); and
- d) Delete Maintenance Association managed object (12.14.5.4).

NOTE 1—The Maintenance Domain managed object is defined in such a manner that it can be configured identically in all of the Bridges in that Bridged Network. All of the information local to a particular Maintenance Association or a particular Bridge is contained in other managed objects, e.g., the Maintenance Association managed object (12.14.6) or the Maintenance association End Point managed object (12.14.7).

NOTE 2—A single Maintenance Domain managed object can be used to manage any number of separate Maintenance Domains, as Maintenance Domains are defined in 18.1. For example, the Maintenance Association managed object for all of the physical links in a Bridged Network that are protected by MAs can be grouped together under a single Maintenance Domain managed object for the convenience of the network administrator.

NOTE 3—Multiple Maintenance Domain managed objects can be used to manage a single Maintenance Domain, as Maintenance Domains are defined in 18.1. For example, a Provider Bridged Network's DoSAPs could be split among two Maintenance Domain managed objects, one for point-to-point services and one for multipoint services.

12.14.5.1 Read Maintenance Domain managed object

12.14.5.1.1 Purpose

To obtain information from a Bridge about a specific Maintenance Domain managed object.

12.14.5.1.2 Inputs

- a) A reference to a particular Maintenance Domain managed object (12.14.5).

12.14.5.1.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to nonexistent Maintenance Domain; or
 - 2) Operation accepted;
- b) The MD Level of the specific Maintenance Domain identified by the Input;
- c) (writable) An enumerated value indicating whether the management entity can create MHFs for this Maintenance Domain, either defMHFnone (1, the default value), defMHFdefault (2), or defMHFexplicit (3) (22.2.3);
- d) (writable) An enumerated value indicating what, if anything, is to be included in the Sender ID TLV (21.5.3) transmitted by MPs configured in this Maintenance Domain, either sendIdNone (1, the default value), sendIdChassis (2), sendIdManage (3), or sendIdChassisManage (4) [item d) in 12.14.6.1.3];
- e) (writable) The network address to which Fault Alarms (12.14.7.7) are to be transmitted, or a value indicating “Fault Alarms are not to be transmitted.” Default value is “not transmitted”; and

NOTE—The variables c) through e) could be writable by the organization operating the Maintenance Domain.

- f) A list of references to the Maintenance Association managed objects (12.14.6) attached to the indicated Maintenance Domain managed object.

12.14.5.2 Write Maintenance Domain managed object

12.14.5.2.1 Purpose

To alter a value of a specific Maintenance Domain managed object.

12.14.5.2.2 Inputs

- a) A reference to a particular Maintenance Domain managed object (12.14.5);
- b) A reference to a writable managed object in 12.14.5.1.3 to be altered; and
- c) A new value for the managed object.

12.14.5.2.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to nonexistent Maintenance Domain;
 - 2) Operation rejected due to the selected managed object being Read-Only;
 - 3) Operation rejected due to invalid value for the selected managed object; or
 - 4) Operation accepted.

12.14.5.3 Create Maintenance Association managed object

12.14.5.3.1 Purpose

To create a new Maintenance Association managed object within a Maintenance Domain managed object.

12.14.5.3.2 Inputs

- a) A reference to a particular Maintenance Domain managed object (12.14.5);
- b) The Short MA Name of an MA within that Maintenance Domain, including the format specifier from Table 21-20 (21.6.5.4), 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 monitored by this MA, or 0, if the MA is not attached to a VID. The first VID in the list is the MA's Primary VID (default none).

12.14.5.3.3 Outputs

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

12.14.5.4 Delete Maintenance Association managed object

12.14.5.4.1 Purpose

To delete a specific Maintenance Association managed object from a Maintenance Domain managed object.

12.14.5.4.2 Inputs

- a) A reference to a particular Maintenance Association managed object (12.14.6).

12.14.5.4.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to nonexistent MA; or
 - 2) Operation accepted.

12.14.6 Maintenance Association managed object

There can be any number of Maintenance Association managed objects per Bridge, one for each service instance for which an MP is defined on that Bridge. From this Maintenance Association managed object, all Maintenance association End Point managed objects associated with that Maintenance Association managed object can be accessed, and thus controlled.

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

- a) Read Maintenance Association managed object (12.14.6.1);
- b) Write Maintenance Association managed object (12.14.6.2);
- c) Create Maintenance association End Point managed object (12.14.6.3); and
- d) Delete Maintenance association End Point managed object (12.14.6.4).

NOTE 1—The Maintenance Association managed object is defined in such a manner that it can be configured identically in all of the Bridges in its Maintenance Domain. All information local to a particular Bridge is contained in other managed objects, e.g., the Maintenance association End Point managed object (12.14.7).

NOTE 2—Although MIP Half Functions (MHFs) are created via the Maintenance Domain managed object, the Default MD Level managed object, and the Maintenance Association managed object, and although there is a Maintenance association End Point managed object, there is no “MIP Half Function managed object.” One reason for this omission is that no controls over the behavior of the MHF beyond its existence is required. Another is that the burden of implementing, providing access to, and providing the maintenance capabilities to access the counters and similar managed objects appropriate to an MHF Managed Object seemed to the developers of this standard to outweigh the benefits of having that information available.

12.14.6.1 Read Maintenance Association managed object

12.14.6.1.1 Purpose

To obtain information from a Bridge about a specific Maintenance Association managed object.

12.14.6.1.2 Inputs

- a) A reference to a particular Maintenance Association managed object (12.14.6).

12.14.6.1.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to nonexistent MA; or
 - 2) Operation accepted;
- b) The VID(s) monitored by this MA, or 0, if the MA is not attached to any VID. The first VID returned is the MA's Primary VID;
- c) (writable) An enumerated value indicating whether the management entity can create MHFs for this MA, either defMHFnone (1), defMHFdefault (2), defMHFexplicit (3), or defMHFdefer (4), (22.2.3), default value is defMHFdefer;
- d) (writable) An enumerated value indicating what, if anything, is to be included in the Sender ID TLV (21.5.3) transmitted by MPs configured in this MA, either:
 - 1) **sendIdNone:** The Sender ID TLV is not to be sent;
 - 2) **sendIdChassis:** The Chassis ID Length, Chassis ID Subtype, and Chassis ID fields of the Sender ID TLV are to be sent, but not the Management Address Length or Management Address fields;
 - 3) **sendIdManage:** The Management Address Length and Management Address of the Sender ID TLV are to be sent, but the Chassis ID Length is to be transmitted with a 0 value, and the Chassis ID Subtype and Chassis ID fields not sent;
 - 4) **sendIdChassisManage:** The Chassis ID Length, Chassis ID Subtype, Chassis ID, Management Address Length, and Management Address fields are all to be sent; or
 - 5) **sendIdDefer:** (the default value) The contents of the Sender ID TLV are determined by the Maintenance Domain managed object, item d) in 12.14.5.1.3;
- e) (writable) An enumerated value, other than 0, indicating the interval between CCM transmissions to be used by all MEPs in the MA (20.8.1, 21.6.1.3) (default 1 s);
- f) (writable) The network address to which Fault Alarms (12.14.7.7) are to be transmitted, a value indicating “not specified,” or a value indicating “Fault Alarms are not to be transmitted.” If “not specified,” the address used is that from the Maintenance Domain managed object [item e) in 12.14.5.1.3]; and

- g) (writable) A list of the MEPIDs of the MEPs in the MA.

12.14.6.2 Write Maintenance Association managed object

12.14.6.2.1 Purpose

To alter a value of a specific Maintenance Association managed object.

12.14.6.2.2 Inputs

- a) A reference to a particular Maintenance Association managed object (12.14.6);
- b) A reference to one of the writable managed objects in 12.14.6.1.3 is to be altered; and
- c) A new value for the managed object.

12.14.6.2.3 Outputs

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

12.14.6.3 Create Maintenance association End Point managed object

12.14.6.3.1 Purpose

To create a new Maintenance association End Point managed object within a Maintenance Association managed object on a specific Bridge Port or aggregated port.

12.14.6.3.2 Inputs

- a) A reference to a particular Maintenance Association managed object (12.14.6);
- b) A MEPID for the created MEP (default 1);
- c) A value indicating the direction in which the MEP faces on the Bridge Port or aggregated port, either:
 - 1) Down (Active SAP is further away from the Frame filtering entity) (the default); or
 - 2) Up (Active SAP is closer to the Frame filtering entity); and
- d) An interface, either a Bridge Port or an aggregated IEEE 802.3 port within a Bridge Port.

12.14.6.3.3 Outputs

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

- 8) Operation rejected because a MEP exists on this MA that has a different value for its Up/Down parameter [item c) in 12.14.6.3.2]; or
- 9) Operation accepted.

12.14.6.4 Delete Maintenance association End Point managed object

12.14.6.4.1 Purpose

To delete an existing Maintenance association End Point managed object from a Maintenance Association managed object.

12.14.6.4.2 Inputs

- a) A reference to a particular Maintenance association End Point managed object (12.14.7).

12.14.6.4.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to nonexistent MEP; or
 - 2) Operation accepted.

12.14.7 Maintenance association End Point managed object

There can be any number of Maintenance association End Point managed objects per Bridge, one for each MEP defined within that Bridge. From this Maintenance association End Point managed object, all management objects related to that MEP can be controlled.

The management operations that can be performed on the Maintenance association End Point managed object are as follows:

- a) Read Maintenance association End Point managed object (12.14.7.1);
- b) Write Maintenance association End Point managed object (12.14.7.2);
- c) Transmit Loopback Messages (12.14.7.3);
- d) Transmit Linktrace Message (12.14.7.4);
- e) Read Linktrace Reply (12.14.7.5);
- f) Read MEP Database (12.14.7.6); and
- g) Transmit MEP Fault Alarm (12.14.7.7).

12.14.7.1 Read Maintenance association End Point managed object

12.14.7.1.1 Purpose

To obtain information from a Bridge about a specific Maintenance association End Point managed object.

12.14.7.1.2 Inputs

- a) A reference to a particular Maintenance association End Point managed object (12.14.7).

12.14.7.1.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to nonexistent MEP; or
 - 2) Operation accepted;

- b) An interface, either a Bridge Port or an aggregated IEEE 802.3 port within a Bridge Port, to which the MEP is attached;
- c) A value indicating the direction in which the MEP faces on the interface, either:
 - 1) Down (Active SAP is further away from Frame filtering entity); or
 - 2) Up (Active SAP is closer to the Frame filtering entity);
- d) (writable) An integer indicating the Primary VID of the MEP, always one of the VID's 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 (20.9.7);
- e) (writable) A Boolean flag indicating the administrative state of the MEP (20.9.1) (default false);
- f) A value indicating the current state of the MEP Fault Notification Generator state machine (20.35);
- g) (writable) A Boolean flag indicating whether the MEP is or is not to generate CCMs (CClenabled, 20.10.1) (default false, no CCMs);
- 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 VID's);

NOTE—The management entity can obtain the default value for this variable from the Priority regeneration table in 6.9.3 by extracting the highest priority value in the table on this MEP's Bridge Port (1 is lowest, then 2, then 0, then 3–7), appropriate to the direction in which frames are emitted from the MEP's Active SAP.

- i) The MAC address of the MEP (19.4);
- j) (writable) The network address to which Fault Alarms (12.14.7.7) are to be transmitted, a value indicating “not specified,” or a value indicating “Fault Alarms are not to be transmitted.” If “not specified,” the address used is that from the Maintenance Association managed object [item f) in 12.14.6.1.3];
- k) (writable) An integer value specifying the lowest priority defect that is allowed to generate a Fault Alarm (20.9.5), either:
 - 1) All defects: DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM;
 - 2) Only DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM (the default);
 - 3) Only DefRemoteCCM, DefErrorCCM, and DefXconCCM;
 - 4) Only DefErrorCCM and DefXconCCM;
 - 5) Only DefXconCCM; or
 - 6) No defects are to be reported;
- l) (writable) The time that defects must be present before a Fault Alarm is issued (20.33.3) (default 2.5 s);
- m) (writable) The time that defects must be absent before resetting a Fault Alarm (20.33.4) (default 10 s);
- n) An enumerated value indicating the highest-priority defect that has been present since the MEP Fault Notification Generator state machine was last in the FNG_RESET state (20.33.9), either:
 - 1) **DefNone**: No defect has been present since the last FNG_RESET state;
 - 2) **DefRDICCM**: The last CCM received by this MEP from some remote MEP contained the RDI bit, so variable item o) in 12.14.7.1.3 is set;
 - 3) **DefMACstatus**: The last CCM received by this MEP from some remote MEP indicated that the transmitting MEP's associated MAC is reporting an error status via the Port Status TLV (21.5.4) or Interface Status TLV (21.5.5), so variable item p) in 12.14.7.1.3 is set;
 - 4) **DefRemoteCCM**: This MEP is not receiving CCMs from some other MEP in its configured list [item g) in 12.14.6.1.3], so variable item q) in 12.14.7.1.3 is set;
 - 5) **DefErrorCCM**: This MEP is receiving invalid CCMs, so variable item r) in 12.14.7.1.3, is set; or
 - 6) **DefXconCCM**: This MEP is receiving CCMs that could be from some other MA, so variable item s) in 12.14.7.1.3 is set;
- o) A Boolean flag (20.33.7) indicating that some other MEP in this MEP's MA is transmitting the RDI bit (can trigger DefRDICCM);

- p) A Boolean flag (20.33.6) indicating that a Port Status TLV (21.5.4) or Interface Status TLV (21.5.5) is indicating an error condition (can trigger DefMACstatus);
- q) A Boolean flag (20.33.5) indicating that CCMs are not being received from at least one of the configured remote MEPs (can trigger DefRemoteCCM);
- r) A Boolean flag (20.21.3) indicating that erroneous CCMs are being received from some MEP in this MEP's MA (can trigger DefErrorCCM);
- s) A Boolean flag (20.23.3) indicating that CCMs are being received from a MEP that could be in some other MA (can trigger DefXconCCM);
- t) The last-received CCM (20.21.2) that triggered a DefErrorCCM fault (20.21.3);
- u) The last-received CCM (20.23.2) that triggered a DefXconCCM fault (20.23.3);
- v) (optional) The total number of out-of-sequence CCMs received (20.16.12);
- w) The total number of CCMs transmitted (20.10.2);
- x) The next Loopback Transaction Identifier to be sent in an LBM (20.28.2);
- y) The total number of valid, in-order LBRs received (20.31.1);
- z) The total number of valid, out-of-order LBRs received (20.31.1);
- aa) (optional) The total number of LBRs received whose mac_service_data_unit did not match (except for the OpCode) that of the corresponding LBM (20.2.3);
- ab) The next LTM Transaction Identifier to be sent in an LTM (20.36.1);
- ac) The total number of unexpected LTRs received (20.39.1); and
- ad) The total number of LBRs transmitted (20.26.2).

12.14.7.2 Write Maintenance association End Point managed object

12.14.7.2.1 Purpose

To alter a value in a specific managed object within a specific Maintenance association End Point managed object.

12.14.7.2.2 Inputs

- a) A reference to a particular Maintenance association End Point managed object (12.14.7);
- b) A reference to one of the writable managed objects in 12.14.7.1.3 is to be altered; and
- c) A new value for the managed object.

12.14.7.2.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to nonexistent MEP;
 - 2) Operation rejected due to the selected managed object being Read-Only;
 - 3) Operation rejected due to invalid value for the selected managed object; or
 - 4) Operation accepted.

12.14.7.3 Transmit Loopback Messages

12.14.7.3.1 Purpose

To signal to the MEP to transmit some number of LBMs.

NOTE—The Maintenance association End Point managed object (12.14.7) can be examined to determine whether or not the corresponding LBRs have been received by the MEP.

12.14.7.3.2 Inputs

- a) A reference to a particular Maintenance association End Point managed object (12.14.7);

- b) An indication of the destination MAC address for LBMs transmitted by the MEP (20.29.1), either:
 - 1) The MEPID of a MEP in that MA; or
 - 2) An Individual destination MAC address;
- c) The number of LBMs to be transmitted (default 1);
- d) An arbitrary amount of data to be included in a Data TLV, along with an indication whether the Data TLV is to be included (20.29.1) (default no Data TLV); and
- e) The priority and drop_eligible parameters to be used in the transmitted LBMs [default is CCM priority item h) in 12.14.7.1.3, drop_eligible false].

12.14.7.3.3 Outputs

- a) An indication of whether the command was accepted by the MEP, either:
 - 1) Operation rejected due to nonexistent MEP;
 - 2) Operation rejected due to invalid number of LBMs to be transmitted;
 - 3) Operation rejected due to too much data to be transmitted;
 - 4) Operation rejected due to invalid priority or drop_eligible parameters to be transmitted;
 - 5) The LBM(s) will be (or have been) sent; or
 - 6) The LBM(s) will not be sent (e.g., because the Bridge is busy with another LBM transmit operation); and
- b) The Loopback Transaction Identifier (20.28.2) of the first LBM (to be) sent. The value returned is undefined if the Transmit Loopback Messages command was not accepted.

12.14.7.4 Transmit Linktrace Message

12.14.7.4.1 Purpose

To signal to the MEP to transmit an LTM and to create an LTM entry in the MEP's Linktrace Database.

NOTE—The Maintenance association End Point managed object (12.14.7) can be examined to determine whether or not the corresponding LTRs have been received by the MEP.

12.14.7.4.2 Inputs

- a) A reference to a particular Maintenance association End Point managed object (12.14.7);
- b) The Flags field for LTMs transmitted by the MEP (20.37.1);
- c) An indication of the Target MAC Address field to be transmitted, either:
 - 1) The MEPID of another MEP in the same MA; or
 - 2) An Individual destination MAC address; and
- d) An initial value for the LTM TTL field (21.8.4). Default value, if not specified, is 64.

12.14.7.4.3 Outputs

- a) An indication of whether the command was accepted by the MEP, either:
 - 1) Operation rejected due to nonexistent MEP;
 - 2) Operation rejected due to invalid Flags field to be transmitted;
 - 3) Operation rejected due to invalid Target MAC Address to be transmitted;
 - 4) Operation rejected due to invalid LTM TTL field to be transmitted;
 - 5) The command was accepted and the LTM has (or will be) transmitted; or
 - 6) The command was rejected and no LTM will be sent (e.g., because the Bridge is busy with another LTM transmit operation);
- b) The LTM Transaction Identifier (20.36.1) of the LTM sent. The value returned is undefined if the Transmit Linktrace Message command was not accepted; and
- c) The LTM Egress Identifier TLV value transmitted in the LTM. The value returned is undefined if the Transmit Linktrace Message command was not accepted.