

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

**Part 3: Media Access Control (MAC) Bridges—
Amendment 2: Rapid Reconfiguration**

Sponsor

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

Approved 14 June 2001
IEEE-SA Standards Board

Approved 25 October 2001
American National Standards Institute

Abstract: This amendment to IEEE Std 802.1D, 1998 Edition (ISO/IEC 15802-3: 1998) and IEEE Std 802.1t-2001 defines the changes necessary to the operation of a MAC Bridge in order to provide rapid Spanning Tree reconfiguration capability.

Keywords: local area networks, MAC Bridge management, MAC Bridges, media access control (MAC) bridges, Rapid Spanning Tree Algorithm and Protocol (RSTP)

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

Copyright © 2001 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 9 July 2001. Printed in the United States of America.

Print: ISBN 0-7381-2924-0 SH94939
PDF: ISBN 0-7381-2925-9 SS94939

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

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

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

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

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

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

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

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

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

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

IEEE is the sole entity that may authorize the use of certification marks, trademarks, or other designations to indicate compliance with the materials set forth herein.

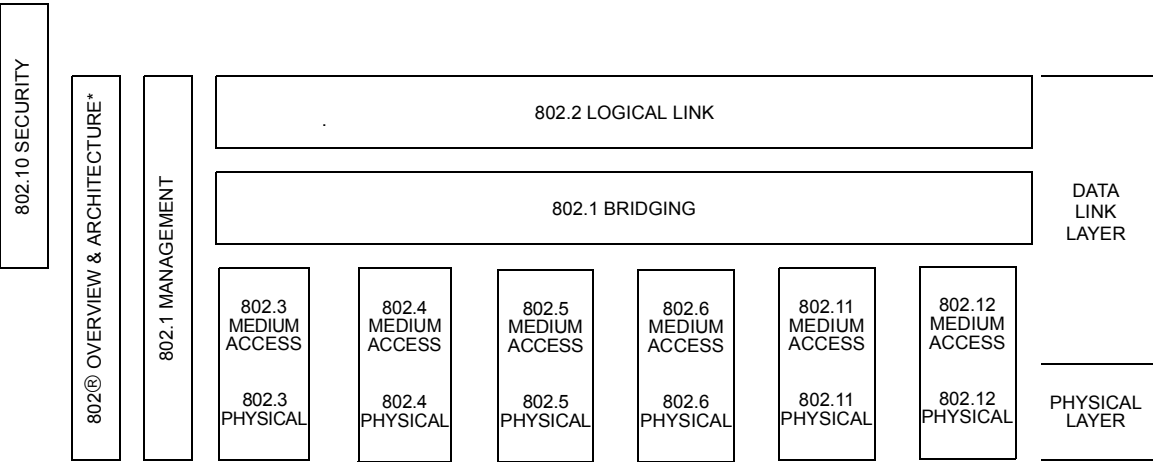
Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; (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 a part of IEEE Std 802.1w-2001, IEEE Standard for Local and metropolitan area networks—Common specifications—Part 3: Media Access Control (MAC) Bridges: Amendment 2—Rapid Reconfiguration.]

This amendment to IEEE Std 802.1D, 1998 Edition (ISO/IEC 15802-3:1998) defines the changes necessary to the operation of a MAC Bridge in order to provide rapid Spanning Tree reconfiguration capability. These changes are documented in the usual form for Amendments to IEEE 802® standards; i.e., as an explicit set of editing instructions that, if correctly applied to the text of IEEE Std 802.1D, 1998 Edition (ISO/IEC 15802-3:1998), will create an amended document.

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



* Formerly IEEE Std 802.1A.

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

The standards defining the technologies noted above are as follows:

- IEEE Std 802¹: *Overview and Architecture.* This standard provides an overview to the family of IEEE 802 Standards. This document forms part of the 802.1 scope of work.

¹The 802 Architecture and Overview Specification, originally known as IEEE Std 802.1A, has been renumbered as IEEE Std 802. This has been done to accommodate recognition of the base standard in a family of standards. References to IEEE Std 802.1A should be considered as references to IEEE Std 802.

- ANSI/IEEE Std 802.1B and 802.1K [ISO/IEC 15802-2]: *LAN/MAN Management*. Defines an Open Systems Interconnection (OSI) management-compatible architecture, and services and protocol elements for use in a LAN/MAN environment for performing remote management.
- ANSI/IEEE Std 802.1D *Media Access Control (MAC) Bridges*. Specifies an architecture and protocol for the [ISO/IEC 15802-3]: interconnection of IEEE 802 LANs below the MAC service boundary.
- ANSI/IEEE Std 802.1E [ISO/IEC 15802-4]: *System Load Protocol*. Specifies a set of services and protocol for those aspects of management concerned with the loading of systems on IEEE 802 LANs.
- ANSI/IEEE Std 802.1F *Common Definitions and Procedures for IEEE 802 Management Information*.
- ANSI/IEEE Std 802.1G [ISO/IEC 15802-5]: *Remote Media Access Control (MAC) Bridging*. Specifies extensions for the interconnection, using non-LAN systems communication technologies, of geographically separated IEEE 802 LANs below the level of the logical link control protocol.
- ANSI/IEEE Std 802.1H [ISO/IEC TR 11802-5] *Recommended Practice for Media Access Control (MAC) Bridging of Ethernet V2.0 in IEEE 802 Local Area Networks*.
- ANSI/IEEE Std 802.1Q *Virtual Bridged Local Area Networks*. Defines an architecture for Virtual Bridged LANs, the services provided in Virtual Bridged LANs, and the protocols and algorithms involved in the provision of those services.
- ANSI/IEEE Std 802.2 [ISO/IEC 8802-2]: *Logical Link Control*.
- ANSI/IEEE Std 802.3 [ISO/IEC 8802-3]: *CSMA/CD Access Method and Physical Layer Specifications*.
- ANSI/IEEE Std 802.4 [ISO/IEC 8802-4]: *Token Bus Access Method and Physical Layer Specifications*.
- ANSI/IEEE Std 802.5 [ISO/IEC 8802-5]: *Token Ring Access Method and Physical Layer Specifications*.
- ANSI/IEEE Std 802.6 [ISO/IEC 8802-6]: *Distributed Queue Dual Bus Access Method and Physical Layer Specifications*.
- ANSI/IEEE Std 802.10: *Interoperable LAN/MAN Security*. Currently approved: Secure Data Exchange (SDE).
- ANSI/IEEE Std 802.11: [ISO/IEC 8802-11] *Wireless LAN Medium Access Control (MAC) Sublayer and Physical Layer Specifications*.
- ANSI/IEEE Std 802.12: [ISO/IEC 8802-12] *Demand Priority Access Method, Physical Layer and Repeater Specification*.
- IEEE Std 802.15: *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for: Wireless Personal Area Networks*.

- IEEE Std 802.16: *Standard Air Interface for Fixed Broadband Wireless Access Systems.*
- IEEE Std 802.17: *Resilient Packet Ring Access Method and Physical Layer Specifications.*

In addition to the family of standards, the following is a recommended practice for a common physical layer technology:

- IEEE Std 802.7: *IEEE Recommended Practice for Broadband Local Area Networks.*

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

Conformance test methodology

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

Participants

When the IEEE 802.1 Working Group approved this standard, it had the following membership:

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

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

Hal Keen
 Daniel Kelley
 Keith Klamm
 Joe Laurence
 Bill Lidinsky
 Yaron Nachman
 LeRoy Nash
 Satoshi Obara
 Luc Pariseau
 Anil Rijasinghani

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

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

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

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

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

When the IEEE-SA Standards Board approved this standard on 14 June 2001, it had the following membership:

Donald N. Heirman, *Chair*
James T. Carlo, *Vice Chair*
Judith Gorman, *Secretary*

Chuck Adams
Mark D. Bowman
Clyde R. Camp
Richard DeBlasio
Harold E. Epstein
H. Landis Floyd
Jay Forster*
Howard M. Frazier

James H. Gurney
Raymond Hapeman
Richard J. Holleman
Richard H. Hulett
Lowell G. Johnson
Joseph L. Koepfinger*
Peter H. Lips

Paul J. Menchini
Daleep C. Mohla
Robert F. Munzner
Ronald C. Petersen
Malcolm V. Thaden
Geoffrey O. Thompson
Akio Tojo
Howard L. Wolfman

*Member Emeritus

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

Satish K. Aggarwal, *NRC Representative*
Alan H. Cookson, *NIST Representative*
Donald R. Volzka, *TAB Representative*

Jennifer McClain Longman
IEEE Standards Project Editor

The marks “**IEEE**” and “**802**” are registered trademarks belonging to the IEEE. When using these marks to refer to The Institute of Electrical and Electronics Engineers, **802** standards or other standards, the marks should be in bold typeface and, at least once in text, use the registered trademark symbol “®”.

Contents

1.	Overview.....	1
1.1	Introduction.....	1
1.2	Scope.....	2
2.	References.....	3
4.	Abbreviations.....	3
5.	Conformance.....	4
5.1	Static conformance requirements.....	4
5.2	Options.....	5
6.	Support of the MAC Service	6
6.3	Quality of service maintenance.....	6
6.4	Internal Sublayer Service provided within the MAC Bridge	8
6.5	Support of the Internal Sublayer Service by specific MAC procedures.....	9
8.	The Spanning Tree algorithm and protocol.....	10
9.	Encoding of Bridge Protocol Data Units (BPDUs).....	10
9.1	Structure.....	10
9.2	Encoding of parameter types	11
9.3	BPDU formats and parameters	13
12.	Generic Attribute Registration Protocol (GARP).....	18
12.7	Overview of GARP protocol operation	18
14.	Bridge management	19
14.2	Managed objects	19
14.8	Bridge Protocol Entity	19
17.	Rapid Spanning Tree Algorithm and Protocol (RSTP).....	24
17.1	Requirements	24
17.2	Requirements of the MAC bridges	25
17.3	Overview.....	26
17.4	Computation of the active topology.....	26
17.5	Port States	29
17.6	Topology examples.....	31
17.7	Communicating Spanning Tree Information	35
17.8	Changing Spanning Tree Information	35
17.9	Changing Port States.....	36
17.10	Updating Learned Station Location Information.....	38
17.11	RSTP and point-to-point links	42
17.12	STP compatibility	42

17.13 Rapid Spanning Tree state machines	42
17.14 Notational conventions used in State Diagrams	45
17.15 State machine timers	46
17.16 State machine performance parameters	47
17.17 Per-Bridge Variables.....	48
17.18 Per-Port variables.....	49
17.19 State machine procedures	54
17.20 The Port Timers state machine	59
17.21 The Port Information state machine.....	59
17.22 The Port Role Selection state machine	61
17.23 The Port Role Transitions state machine	62
17.24 Port State Transition state machine	67
17.25 Topology Change state machine.....	68
17.26 Port Protocol Migration state machine	70
17.27 Port Transmit state machine	71
17.28 Performance	73
Annex A (normative) PICS Proforma	77
Annex B (informative) Calculating Spanning Tree parameters.....	93
Annex F (informative) Target topology, migration, and interoperability	101
Annex G (informative) Bibliography	108

IEEE Standard for Local and metropolitan area networks— Common specifications

Part 3: Media Access Control (MAC) Bridges— Amendment 2: Rapid Reconfiguration

Editorial notes

This amendment to IEEE Std 802.1D, 1998 Edition (ISO/IEC 15802-3:1998) and IEEE Std 802.1t-2001 defines the changes necessary to the operation of a MAC Bridge in order to provide rapid reconfiguration capability. These changes are defined as a series of additions to, and modifications of, the combined text that is generated by applying the editing instructions contained in IEEE Std 802.1t-2001 to the text of IEEE Std 802.1D, 1998 Edition; this amendment, therefore, assumes all material, including references, abbreviations, definitions, procedures, services, and protocols defined in IEEE Std 802.1D, 1998 Edition and IEEE Std 802.1t-2001. Text shown in ***bold italics*** in this amendment defines the editing instructions necessary in order to incorporate the modifications and additions into the base text. Three editing instructions are used: ***change***, ***delete***, and ***insert***. ***Change*** is used to make a change to existing material. The editing instruction specifies the location of the change and describes what is being changed either by using ~~striketrough~~ (to remove old material) or underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without changing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. Editorial notes will not be carried over into future editions of IEEE Std 802.1D, 1998 Edition.

1. Overview

Change the Introduction and Scope as indicated below:

1.1 Introduction

IEEE 802® Local Area Networks (or LANs; see 3.4) of all types can be connected together using MAC Bridges. Each individual LAN has its own independent MAC. The Bridged LAN created allows the interconnection of stations attached to separate LANs as if they were attached to a single LAN, although they are in fact attached to separate LANs each with its own MAC. A MAC Bridge operates below the MAC Service Boundary, and is transparent to protocols operating above this boundary, in the Logical Link Control (LLC) sublayer or Network Layer (ISO/IEC 7498-1: 1994¹). The presence of one or more MAC Bridges can lead to differences in the Quality of Service provided by the MAC sublayer; it is only because of such differences that MAC Bridge operation is not fully transparent.

¹Information about references can be found in Clause 2.

A Bridged LAN can provide for

- a) The interconnection of stations attached to LANs of different MAC types;
- b) An effective increase in the physical extent, the number of permissible attachments, or the total performance of a LAN;
- c) Partitioning of the physical LAN for administrative or maintenance reasons;
- d) Validation of access to the LAN;
- e) Increased availability of the MAC Service in the face of reconfiguration or failure of components of the Bridged LAN.

NOTE 1—Scope, definitions, references, and conformance requirements relating to the operation of Source Routing Transparent Bridge operation can be found in Annex C.1.

NOTE 2—Validation of access to the LAN is supported when this standard is used in conjunction with the Port-based access control mechanisms specified in IEEE Std 802.1X-2001.

1.2 Scope

For the purpose of compatible interconnection of data processing equipment using the IEEE 802 MAC Service supported by interconnected IEEE 802 LANs (see 3.4) using different or identical Media Access Control methods, this standard specifies a general method for the operation of MAC Bridges. To this end it

- a) Positions the bridging function within an architectural description of the MAC Sublayer.
- b) Defines the principles of operation of the MAC Bridge in terms of the support and preservation of the MAC Service, and the maintenance of Quality of Service.
- c) Specifies the MAC Internal Sublayer Service provided by individual LANs to the Media Access Method Independent Functions that provide frame relay in the Bridge.
- d) Identifies the functions to be performed by Bridges, and provides an architectural model of the internal operation of a Bridge in terms of Processes and Entities that provide those functions.
- e) Establishes the requirements for a protocol between the Bridges in a Bridged LAN to configure the network, and specifies the distributed computation of a Spanning Tree active topology.
- f) Specifies the encoding of the Bridge Protocol Data Units (BPDUs).
- g) Establishes the requirements for Bridge Management in the Bridged LAN, identifying the managed objects and defining the management operations.
- h) Establishes the requirements for a protocol between Bridges in a Bridged LAN to configure multicast filtering information, and specifies the means of registering and distributing multicast filtering information by means of the GARP Multicast Registration Protocol (GMRP).
- i) Specifies the encoding of GMRP protocol data units.
- j) Specifies performance requirements and recommends default values and applicable ranges for the operational parameters of a Bridge.
- k) Specifies the requirements to be satisfied by equipment claiming conformance to this standard.
- l) Specifies criteria for the use of MAC-specific bridging methods.
- m) Specifies enhancements to the operation of Spanning Tree protocol, and to the other mechanisms that support reconfiguration of the physical and filtering connectivity, in order to allow support for rapid reconfiguration of Bridged LAN connectivity.

This standard specifies the operation of MAC Bridges that attach directly to IEEE 802 LANs, as specified in the relevant MAC standards for the MAC technology or technologies implemented.

The configuration protocol and associated algorithm required for the distributed computation of a Spanning Tree active topology referred to in item e) appears in two forms in this standard. Clause 8 specifies a version of the Spanning Tree algorithm and protocol that is consistent with the specification contained in IEEE Std 802.1D, 1998 Edition; Clause 17 specifies the Rapid Spanning Tree Algorithm and Protocol; this version offers a significant reduction in the time taken to reconfigure the active topology of the Bridged LAN in the face of changes to the physical topology or its configuration parameters. The two versions of the algorithm and protocol are capable of interoperating within the same Bridged LAN; hence, it is not necessary for implementations to support both versions of the Spanning Tree algorithm and protocol.

In view of the improved performance offered, it is recommended that the Rapid Spanning Tree algorithm and Protocol is supported in preference to the original version in new MAC Bridge implementations.

NOTE 1—The original version of the Spanning Tree algorithm and protocol has been retained in this standard to allow implementations that pre-date the availability of the Rapid Spanning Tree Algorithm and Protocol to continue to claim conformance to IEEE Std 802.1D.

The specification of Remote Bridges, which interconnect LANs using Wide Area Network (WAN) media for the transmission of frames between Bridges, is outside the scope of this standard.

NOTE 2—Remote MAC Bridging is specified in ISO/IEC 15802-5: 1997 [ANSI/IEEE Std 802.1G, 1997 Edition] ANSI/IEEE Std 802.1G, 1998 Edition (ISO/IEC 15802-5:1998) [B1]².

2. References

Add the following references, in alphabetical sequence with the existing references:

IEEE Std 802.1t-2001, Supplement to ISO/IEC 15802-3 (IEEE Std 802.1D) Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 3: Media Access Control (MAC) Bridges: Technical and editorial Corrections.

IEEE Std 802.1X-2001, IEEE Standard for Local and Metropolitan Area Networks: Port based Network Access Control.

ISO/IEC 14882: 1998, Information Tecnology—Programming languages—C++.

4. Abbreviations

Insert the following abbreviations, in the correct collating sequence:

<u>RSTP</u>	<u>Rapid Spanning Tree Algorithm and Protocol</u>
<u>STP</u>	<u>Spanning Tree Algorithm and Protocol</u>
<u>RST BPDU</u>	<u>Rapid Spanning Tree Bridge Protocol Data Unit</u>
<u>TCN</u>	<u>Topology Change Notification</u>

²The numbers in brackets preceded by the letter B correspond to those of the bibliography in Annex G.

5. Conformance

5.1 Static conformance requirements

Replace items h) through j) as follows:

- h) ~~Implement the Spanning Tree Algorithm and Protocol, described in Clause 8, as specified in 8.7.~~
- i) ~~Not exceed the values given in 8.10.2 for the following parameters:~~
 - 1) ~~Maximum bridge transit delay~~
 - 2) ~~Maximum Message Age increment overestimate~~
 - 3) ~~Maximum BPDU transmission delay~~
- j) ~~Use the value given in Table 8-3 for the following parameter:~~
 - 1) ~~Hold Time~~
- h) Implement one of:
 - 1) The Spanning Tree Algorithm and Protocol, described in Clause 8, as specified in 8.7, or
 - 2) The Rapid Spanning Tree Algorithm and Protocol, described in Clause 17, as specified in 17.13.
- i) If the Spanning Tree Algorithm and Protocol is implemented:
 - 1) Not exceed the values given in 8.10.2 for the following parameters:
 - i) Maximum bridge transit delay
 - ii) Maximum Message Age increment overestimate
 - iii) Maximum BPDU transmission delay
 - 2) Use the value given in Table 8-3 for the following parameter:
 - i) Hold Time
- j) If the Rapid Spanning Tree Algorithm and Protocol is implemented:
 - 1) Not exceed the values given in 17.28.2 for the following parameters:
 - i) Maximum bridge transit delay
 - ii) Maximum Message Age increment overestimate
 - iii) Maximum BPDU transmission delay
 - 2) Use the value given in Table 17-5 for the following parameter:
 - i) Hold Time
 - 3) Implement the adminEdgePort and operEdgePort parameters and the operation of the Bridge Detection state machine on all Ports of the Bridge, as defined in Clause 18 of IEEE Std 802.1t-2001.
 - 4) Implement the adminPointToPointMAC and operPointToPointMAC parameters on all Ports of the Bridge, in accordance with the definition of those parameters in 6.4 and any relevant specific MAC procedures defined in 6.5.

5.2 Options

Change items e) through i) as follows:

- e) Provide the capability to assign values to the following parameters to allow configuration of the Spanning Tree active topology:

- 1) Bridge Priority
- 2) Port Priority
- 3) Path Cost for each Port

A Bridge that provides this capability shall implement the range of values specified in 8.10.2 and Table 8-4 and Table 8-5 if the Spanning Tree Algorithm and Protocol is implemented, or shall implement the range of values specified in 17.28.2 and Table 17-6 and Table 17-7 if the Rapid Spanning Tree Algorithm and Protocol is implemented.

- f) Provide the capability to set the values of the following parameters of the Spanning Tree Algorithm and Protocol:

- 1) Bridge Max Age
- 2) Bridge Hello Time
- 3) Bridge Forward Delay

A Bridge that provides this capability shall implement the range of values specified in 8.10.2 and Table 8-3 if the Spanning Tree Algorithm and Protocol is implemented, or shall implement the range of values specified in 17.28.2 and Table 17-5 if the Rapid Spanning Tree Algorithm and Protocol is implemented.

- g) Support management of the Bridge. Bridges claiming to support management shall support all the management objects and operations defined in Clause 14.
- h) Support the use of a remote management protocol. Bridges claiming to support remote management shall
- 1) State which remote management protocol standard(s) or specification(s) are supported.
 - 2) State which standard(s) or specification(s) for managed object definitions and encodings are supported for use by the remote management protocol.
- i) Support the ability to disable topology change detection, as described in 8.5.5.10, only if the Spanning Tree Algorithm and Protocol is implemented.

NOTE—The Rapid Spanning Tree Algorithm and Protocol does not support the ability to disable topology change detection; in RSTP, this function has been superseded by the Admin and Oper Edge Port parameters.

Add the following as items p and q):

- p) Implement both the Spanning Tree Algorithm and Protocol, described in Clause 8, as specified in 8.7, and the Rapid Spanning Tree Algorithm and Protocol, described in Clause 17, as specified in 17.13. The implementation shall support only one of the two algorithms on all Bridge Ports at any given time.
- q) Support the ability to transfer learned MAC Address information from a retiring Root Port to a new Root Port, as described in 17.10.

6. Support of the MAC Service

Change the following subclauses of Clause 6 as indicated:

6.3 Quality of service maintenance

6.3.1 Service availability

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

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

- a) Physical detection of component failure and signalling of that failure by the Internal Sublayer Service (6.4 and 6.5);
- b) Detection of component failure through the operation of the Spanning Tree algorithm and protocol;
- c) Explicit signalling of reconfiguration events through the operation of the Spanning Tree algorithm and protocol.

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

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

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

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

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

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

6.3.2 Frame loss

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

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

- a) Frame corruption during physical layer transmission or reception.
- b) Frame discard by a Bridge because
 - 1) It is unable to transmit the frame within some maximum period of time and, hence, must discard the frame to prevent the maximum frame lifetime (6.3.6) from being exceeded.
 - 2) It is unable to continue to store the frame due to exhaustion of internal buffering capacity as frames continue to arrive at a rate in excess of that at which they can be transmitted.
 - 3) The size of the service data unit carried by the frame exceeds the maximum supported by the MAC procedures employed on the LAN to which the frame is to be relayed.
 - 4) Changes in the connected topology of the Bridged LAN necessitate frame discard for a limited period of time to maintain other aspects of Quality of Service (see 8.3.3 and 17.9).
 - 5) The device attached to the Port is not authorized for access to the network.
 - 6) The configuration of Static Filtering Entries in the Filtering Database (7.9.1) disallows the forwarding of frames with particular destination addresses on specific Ports.
 - 7) As Static Filtering Entries are associated with particular Ports or combinations of Ports, there is a possibility that mis-configuration of Static Filtering Entries will lead to unintended frame discard during or following automatic reconfiguration of the Bridged LAN.

6.3.3 Frame misordering

The MAC Service ~~(9.2 of ISO/IEC 15802-1) does not permit the~~ permits a negligible rate of reordering of frames with a given user priority for a given combination of destination address and source address. MA_UNITDATA.indication service primitives corresponding to MA_UNITDATA.request primitives, with the same requested priority and for the same combination of destination and source addresses, are received in the same order as the request primitives were processed.

NOTE 1—The operation of the Forwarding Process in Bridges (7.7) is such that the frame-ordering characteristics of the MAC Service are preserved.

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

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

6.3.4 Frame duplication

The MAC Service (9.2 of ISO/IEC 15802-1) ~~does not permit the~~ permits a negligible rate of duplication of frames. The operation of Bridges ~~does not introduce~~ introduces a negligible rate of duplication of user data frames.

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

~~A Bridge shall not duplicate user data frames.~~ Where Bridges in a Bridged LAN are capable of connecting the individual MACs in such a way that multiple paths between any source station–destination station pairs exist, the operation of a protocol is required to ensure that a single path is used.

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

6.4 Internal Sublayer Service provided within the MAC Bridge

Add a new subclause 6.4.3 as follows:

6.4.3 Point to Point MAC parameters

In addition to the unit-data service primitives described, the Internal Sublayer Service provided by a MAC entity to the MAC Relay Entity within a Bridge makes available a pair of parameters that permit inspection of, and control over, the administrative and operational state of the point-to-point status of the MAC entity by the MAC Relay Entity. These parameters are defined as follows:

operPointToPointMAC: This parameter can take two values, as follows:

- a) **True.** This value indicates that the MAC is connected to a point-to-point LAN segment; i.e., there is at most one other system attached to the LAN segment.
- b) **False.** This value indicates that the MAC is connected to a non-point-to-point LAN segment; i.e., there can be more than one other system attached to the LAN segment.

adminPointToPointMAC: This parameter can take three values, as follows:

- a) **ForceTrue.** This value indicates that the administrator requires the MAC to be treated as if it is connected to a point-to-point LAN segment, regardless of any indications to the contrary that are generated by the MAC entity.
- b) **ForceFalse.** This value indicates that the administrator requires the MAC to be treated as if it is connected to a non-point-to-point LAN segment, regardless of any indications to the contrary that are generated by the MAC entity.
- c) **Auto.** This value indicates that the administrator requires the point-to-point status of the MAC to be determined in accordance with the specific MAC procedures defined in 6.5.

If adminPointToPointMAC is set to ForceTrue, then operPointToPointMAC shall be set True. If adminPointToPointMAC is set to ForceFalse, then operPointToPointMAC shall be set False.

If adminPointToPointMAC is set to Auto, then the value of operPointToPointMAC is determined in accordance with the specific procedures defined for the MAC entity concerned, as defined in 6.5. If these procedures determine that the MAC entity is connected to a point-to-point LAN segment, then operPointToPointMAC is set TRUE; otherwise it is set FALSE. In the absence of a specific definition of how to determine whether the MAC is connected to a point-to-point LAN segment or not, the value of operPointToPointMAC shall be FALSE.

The value of operPointToPointMAC is determined dynamically; i.e., it is re-evaluated whenever the value of adminPointToPointMAC changes, and whenever the specific procedures defined for the MAC entity evaluate a change in its point-to-point status.

6.5 Support of the Internal Sublayer Service by specific MAC procedures

6.5.1 Support by IEEE Std 802.3 (CSMA/CD)

Add the following text at the end of this subclause:

From the point of view of determining the value of operPointToPointMAC (6.4.3), the MAC is considered to be connected to a point-to-point LAN segment if any of the following conditions are true:

- a) The MAC entity concerned contains a Link Aggregation sublayer, and the set of physical MACs associated with the Aggregator are all aggregatable; or
- b) The MAC entity concerned supports autonegotiation (Clause 28 of IEEE Std 802.3), and the autonegotiation function has determined that the LAN segment is to be operated in full duplex mode; or
- c) The MAC entity has been configured by management means for full duplex operation.

Otherwise, the MAC is considered to be connected to a LAN segment that is not point-to-point.

8. The Spanning Tree algorithm and protocol

Change the definition of Hold Time in Table 8-3, as follows:

Table 8-3—Spanning Tree algorithm timer values

Parameter	Recommended or default value	Fixed value	Range
Bridge Hello Time	2.0	—	1.0–10.0
Bridge Max Age	20.0	—	6.0–40.0
Bridge Forward Delay	15.0	—	4.0–30.0
Hold Time	—	~~Not more than 3 BPDUs transmitted in any 2 second interval~~ <u>Not more than TxHoldCount (17.16.6) BPDUs transmitted in any HelloTime (17.16.3) interval</u>	—

All times are in seconds.

— Not applicable.

Subclause 8.10.2 constrains the relationship between Bridge Max Age and Bridge Forward Delay.

NOTE—Implementations that are conformant to the definition of Hold Time in IEEE Std 802.1D, 1998 Edition are also conformant to the revised definition of Hold Time stated in this table.

9. Encoding of Bridge Protocol Data Units (BPDUs)

Change the text of Clause 9 as shown:

This clause specifies the structure and encoding of the BPDUs for the Spanning Tree Protocol (Clause 8) and Rapid Spanning Tree Protocol (Clause 17), exchanged between Bridge Protocol Entities.

9.1 Structure

9.1.1 Transmission and representation of octets

All BPDUs shall contain an integral number of octets. The octets in a BPDU are numbered starting from 1 and increasing in the order they are put into a Data Link Service Data Unit (DLSDU). The bits in an octet are numbered from 1 to 8, where 1 is the low-order bit.

When consecutive bits within an octet are used to represent a binary number, the higher bit number has the most significant value.

When consecutive octets are used to represent a binary number, the lower octet number has the most significant value.

All Bridge Protocol Entities respect these bit and octet ordering conventions, thus allowing communications to take place.

9.1.2 Components

A Protocol Identifier is encoded in the initial octets of all BPDUs. This standard ~~reserves~~ specifies a single Protocol Identifier value for use in BPDUs. All other Protocol Identifier values are reserved for future

standards use. This standard places no further restriction on the structure, encoding, or use of BPDUs with different values of the Protocol Identifier field, should these exist, by other standard protocols.

BPDUs used by Bridge Protocol Entities operating the Spanning Tree Algorithm and Protocol specified in Clause 8 and the Rapid Spanning Tree Algorithm and Protocol specified in Clause 17 use the ~~reserved~~specified Protocol Identifier value and have the following structure.

9.2 Encoding of parameter types

9.2.1 Encoding of protocol identifiers

A Protocol Identifier shall be encoded in two octets.

9.2.2 Encoding of protocol version identifiers

A Protocol Version Identifier shall be encoded in one octet. If two Protocol Version Identifiers are interpreted as unsigned binary numbers, then the greater number will be associated with the more recently defined Protocol Version.

9.2.3 Encoding of BPDUs types

The type of the BPDU shall be encoded as a single octet. The bit pattern contained in the octet merely serves to distinguish the type; no ordering relationship between BPDUs of different types is implied.

9.2.4 Encoding of flags

A flag shall be encoded as a bit in a single octet. A number of flags may be thus encoded in a single octet. A flag is set if the corresponding bit in the octet takes the value 1. Bit positions in the octet that do not correspond to flags defined for a given type of BPDU are reset, i.e., shall take the value 0. No additional flags will be defined for a BPDU of given protocol version and type.

9.2.5 Encoding of Bridge Identifiers

A Bridge Identifier shall be encoded as eight octets, taken to represent an unsigned binary number. Two Bridge Identifiers may be numerically compared and the lesser number shall denote the Bridge with ~~higher~~better priority.

NOTE 1—Use of the terms “higher” and “lower” to describe both the relative numerical values and the relative priority of Spanning Tree priority information can cause confusion, as lesser numbers convey better priorities. In this clause and in Clause 17 (Rapid Spanning Tree), relative numeric values are described as “least,” “lesser,” “equal,” and “greater” and their comparisons as “less than,” “equal to,” or “greater than,” while relative Spanning Tree priorities are described as “best,” “better,” “the same,” “different,” and “worse” and their comparisons as “better than,” “the same as,” “different from,” and “worse than.” The terms “higher” and “lower” have been retained in Clause 8. Further, in Clause 17, the terms “superior” and “inferior” have been introduced for comparisons not simply based on strict ordered comparison of priority components. This distinction is not necessary in Clause 8.

The four most significant bits of the most significant octet of a Bridge Identifier comprises a settable priority component that permits the relative priority of Bridges to be managed (8.5.3.7 and Clause 14). The next most significant twelve bits of a Bridge Identifier (the four least significant bits of the most significant octet, plus the second most significant octet) comprise a locally assigned system ID extension. The six least significant octets ensure the uniqueness of the Bridge Identifier; they shall be derived from the globally unique Bridge Address (7.12.5) according to the following procedure.

NOTE 2—The number of bits that are considered to be part of the system ID (60 bits) differs in this version of the standard from the 1998 and prior versions (formerly, the priority component was 16 bits and the system ID component 48 bits). This change was made in order to allow implementations of Multiple Spanning Trees (P802.1s, a supplement to IEEE Std 802.1Q) to make use of the 12-bit system ID extension as a means of generating a distinct Bridge Identifier per

VLAN, rather than forcing such implementations to allocate up to 4094 MAC addresses for use as Bridge Identifiers. To maintain management compatibility with older implementations, the priority component is still considered, for management purposes, to be a 16-bit value, but the values that it can be set to are restricted to only those values where the least significant 12 bits are zero (i.e., only the most significant 4 bits are settable).

The third most significant octet is derived from the initial octet of the MAC Address; the least significant bit of the octet (Bit 1) is assigned the value of the first bit of the Bridge Address, the next most significant bit is assigned the value of the second bit of the Bridge Address, and so on. In a Bridged LAN utilizing 48-bit MAC Addresses, the fourth through eighth octets are similarly assigned the values of the second to the sixth octets of the Bridge Address.

9.2.6 Encoding of Root Path Cost

Root Path Cost shall be encoded as four octets, taken to represent an unsigned binary number, a multiple of arbitrary cost units. Subclause 8.10.2 contains recommendations as to the increment to the Root Path Cost, in order that some common value can be placed on this parameter without requiring a management installation practice for Bridges in a Bridged LAN.

9.2.7 Encoding of Port Identifiers

A Port Identifier shall be encoded as two octets, taken to represent an unsigned binary number. If two Port Identifiers are numerically compared, the lesser number shall denote the Port with ~~higher~~ better priority. The more significant four bits of a Port Identifier is a settable priority component that permits the relative priority of Ports on the same Bridge to be managed (8.5.5 and Clause 14). The less significant twelve bits is the Port Number expressed as an unsigned binary number. The value 0 is not used as a Port Number.

NOTE—The number of bits that are considered to be part of the Port Number (12 bits) differs in this version of the standard from the 1998 and prior versions (formerly, the priority component was 8 bits and the Port Number component also 8 bits). This change was made in recognition of the fact that modern switched LAN infrastructures call for increasingly large numbers of Ports to be supported in a single Bridge. To maintain management compatibility with older implementations, the priority component is still considered, for management purposes, to be an 8-bit value, but the values that it can be set to are restricted to those values where the least significant 4 bits are zero (i.e., only the most significant 4 bits are settable).

9.2.8 Encoding of Timer Values

Timer Values shall be encoded in two octets, taken to represent an unsigned binary number multiplied by a unit of time of 1/256 of a second. This permits times in the range 0 to, but not including, 256 s to be represented.

9.2.9 Encoding of Port Role values

Port Role values shall be encoded in two consecutive flag bits, taken to represent an unsigned integer, as follows:

- a) A value of 0 indicates Unknown.
- b) A value of 1 indicates Alternate or Backup.
- c) A value of 2 indicates Root.
- d) A value of 3 indicates Designated.

The Unknown value of Port Role cannot be generated by a valid implementation; however, this value is accepted on receipt.

NOTE—Should the Unknown value of the Port Role parameter be received, the state machines will effectively treat the RST BPDU as if it were a Configuration BPDU.

9.2.10 Encoding of Length Values

Length Values shall be encoded in two octets, taken to represent an unsigned binary number.

9.3 BPDU formats and parameters

9.3.1 Configuration BPDUs

The format of the Configuration BPDUs is shown in Figure 9-1. Each transmitted Configuration BPDU shall contain the following parameters (8.5.1) and no others. Where a specific parameter value is indicated in this subclause, that parameter value shall be encoded in all transmitted Configuration BPDUs:

- a) The Protocol Identifier is encoded in Octets 1 and 2 of the BPDU. It takes the value 0000 0000 0000 0000, which identifies the Spanning Tree Algorithm and Protocol as specified in Clause 8 and the Rapid Spanning Tree Algorithm and Protocol as specified in Clause 17.
- b) The Protocol Version Identifier is encoded in Octet 3 of the BPDU. It takes the value 0000 0000.
- c) The BPDU Type is encoded in Octet 4 of the BPDU. This field ~~shall take~~ takes the value 0000 0000. This denotes a Configuration BPDU.
- d) The Topology Change Acknowledgment flag is encoded in Bit 8 of Octet 5 of the BPDU.
- e) The Topology Change flag is encoded in Bit 1 of Octet 5 of the BPDU.
- f) The remaining flags, Bits 2 through 7 of Octet 5, are unused and take the value 0.
- g) The Root Identifier is encoded in Octets 6 through 13 of the BPDU.
- h) The Root Path Cost is encoded in Octets 14 through 17 of the BPDU.
- i) The Bridge Identifier is encoded in Octets 18 through 25 of the BPDU.
- j) The Port Identifier is encoded in Octets 26 and 27 of the BPDU.
- k) The Message Age timer value is encoded in Octets 28 and 29 of the BPDU.
- l) The Max Age timer value is encoded in Octets 30 and 31 of the BPDU.
- m) The Hello Time timer value is encoded in Octets 32 and 33 of the BPDU.
- n) The Forward Delay timer value is encoded in Octets 34 and 35 of the BPDU.

The Message Age (Octets 28 and 29) shall be less than Max Age (Octets 30 and 31).

	Octet
Protocol Identifier	1
	2
Protocol Version Identifier	3
BPDU Type	4
Flags	5
	6
	7
Root Identifier	8
	9
	10
	11
	12
	13
Root Path Cost	14
	15
	16
	17
	18
Bridge Identifier	19
	20
	21
	22
	23
	24
	25
Port Identifier	26
	27
Message Age	28
	29
Max Age	30
	31
Hello Time	32
	33
Forward Delay	34
	35

Figure 9-1—Configuration BPDU parameters and format

9.3.2 Topology change notification BPDUs

The format of the Topology Change Notification BPDUs is shown in Figure 9-2. Each transmitted Topology Change Notification BPDU shall contain the following parameters (8.5.2) and no others. Where a specific parameter value is indicated in this subclause, that parameter value shall be encoded in all transmitted Topology Change Notification BPDUs:

- a) The Protocol Identifier is encoded in Octets 1 and 2 of the BPDU. It takes the value 0000 0000 0000 0000, which identifies the Spanning Tree Algorithm and Protocol as specified in Clause 8 and the Rapid Spanning Tree Algorithm and Protocol as specified in Clause 17 of this standard.
- b) The Protocol Version Identifier is encoded in Octet 3 of the BPDU. It takes the value 0000 0000.

- c) The BPDU Type is encoded in Octet 4 of the BPDU. This field ~~shall take~~ takes the value 1000 0000 (where bit 8 is shown at the left of the sequence). This denotes a Topology Change Notification BPDU.

Protocol Identifier	Octet 1
	2
Protocol Version Identifier	3
BPDU Type	4

Figure 9-2—Topology change notification BPDU parameters and format

9.3.3 Rapid Spanning Tree BPDUs (RST BPDUs)

The format of the RST BPDUs is shown in Figure 9-3. Each transmitted RST BPDU shall contain the following parameters and no others. Where a specific parameter value is indicated in this subclause, that parameter value shall be encoded in all transmitted RST BPDUs:

- a) The Protocol Identifier is encoded in Octets 1 and 2 of the BPDU. It takes the value 0000 0000 0000 0000, which identifies the Spanning Tree Algorithm and Protocol as specified in Clause 8 and the Rapid Spanning Tree Algorithm and Protocol as specified in Clause 17.
- b) The Protocol Version Identifier is encoded in Octet 3 of the BPDU. It takes the value 0000 0010.
- c) The BPDU Type is encoded in Octet 4 of the BPDU. This field takes the value 0000 0010. This denotes a Rapid Spanning Tree BPDU.
- d) The Topology Change flag is encoded in Bit 1 of Octet 5 of the BPDU (see 17.19.16).
- e) The Proposal flag is encoded in Bit 2 of Octet 5 of the BPDU (see 17.19.16).
- f) The Port Role is encoded in Bits 3 and 4 of Octet 5 of the BPDU (see 17.19.16).
- g) The Learning flag is encoded in Bit 5 of Octet 5 of the BPDU (see 17.19.16).
- h) The Forwarding flag is encoded in Bit 6 of Octet 5 of the BPDU (see 17.19.16).
- i) The Agreement flag is encoded in Bit 7 of Octet 5 of the BPDU (see 17.19.16).
- j) The Topology Change Acknowledgment flag is encoded in Bit 8 of Octet 5 of the BPDU as zero (see 17.19.16).
- k) The Root Identifier is encoded in Octets 6 through 13 of the BPDU (see 17.18.17, 17.19.16).
- l) The Root Path Cost is encoded in Octets 14 through 17 of the BPDU (see 17.18.17, 17.19.16).
- m) The Bridge Identifier is encoded in Octets 18 through 25 of the BPDU. (see 17.18.17, 17.19.16)
- n) The Port Identifier is encoded in Octets 26 and 27 of the BPDU (see 17.18.17, 17.19.16).
- o) The Message Age timer value is encoded in Octets 28 and 29 of the BPDU (see 17.18.18, 17.19.16).
- p) The Max Age timer value is encoded in Octets 30 and 31 of the BPDU (see 17.18.18, 17.19.16).
- q) The Hello Time timer value is encoded in Octets 32 and 33 of the BPDU (see 17.18.18, 17.19.16).
- r) The Forward Delay timer value is encoded in Octets 34 and 35 of the BPDU (see 17.18.18, 17.19.16).
- s) The Version 1 Length value is encoded in Octet 36 of the BPDU. It takes the value 0000 0000, which indicates that there is no Version 1 protocol information present.

NOTE—The presence of a Version 1 Length value of 0, indicating that no version 1 information is present, is required in Version 2 BPDUs in order to make it possible to define subsequent versions of the protocol that can carry additional parameters other than those defined for Version 1 of the protocol (defined in IEEE Std 802.1G).

The Message Age (Octets 28 and 29) shall be less than Max Age (Octets 30 and 31).

Protocol Identifier	Octet
	1
Protocol Version Identifier	2
	3
BPDU Type	4
Flags	5
Root Identifier	6
	7
	8
	9
	10
	11
	12
	13
Root Path Cost	14
	15
	16
	17
Bridge Identifier	18
	19
	20
	21
	22
	23
	24
	25
Port Identifier	26
Message Age	27
	28
Max Age	29
	30
Hello Time	31
	32
Forward Delay	33
	34
Version 1 Length	35
	36

Figure 9-3—RST BPDU parameters and format

9.3.4 Validation of received BPDUs

A Bridge Protocol Entity shall process a received BPDU as specified in 8.7 and 17.13 if and only if the BPDU contains at least four octets and the Protocol Identifier has the value specified for BPDUs (9.3.2), and

- a) The BPDU Type denotes a Configuration BPDU and the BPDU contains at least 35 octets, and the Bridge Identifier and Port Identifier parameters from the received BPDU do not match the values that would be transmitted in a BPDU from this Port; or

NOTE 1—If the Bridge Identifier and Port Identifier both match the values that would be transmitted in a BPDU from this Port, then the BPDU is discarded, in order to prevent processing of the Port's own BPDUs; for example, if they are received by the Port as a result of a loopback condition. If a loopback condition exists, then there may be other undesirable side effects with respect to Bridge operation caused by the looping back of data frames relayed through the Port.

- b) The BPDU Type denotes a Topology Change Notification BPDU; or
- c) The BPDU Type denotes a Rapid Spanning Tree BPDU and the BPDU contains at least 36 octets, and the Bridge Identifier and Port Identifier parameters from the received BPDU do not match the values that would be transmitted in a BPDU from this Port.

NOTE 2—The operation of the RSTP Port Information state machine (see 17.21) checks that the value of the BPDU's Message Age parameter is less than that of its Max Age parameter, and if not, will immediately age out the received information.

~~In case a), any octets that are present beyond Octet 35 are ignored, as far as processing according to this standard is concerned. Similarly, in case b), any octets beyond Octet 4 are ignored.~~

~~NOTE—The Protocol Version Identifier is not checked on receipt, in order to allow the possibility of future specification of extensions to the Spanning Tree Protocol, identified as new versions by different values of the Protocol Version Identifier.~~

The following rules apply to the validation and interpretation of BPDUs, in order to ensure that backwards compatibility is maintained between versions of this protocol.

For an implementation that supports version A of the protocol, a received BPDU of a given type that carries a protocol version number B is interpreted as follows:

- d) Where B is greater than or equal to A, the BPDU shall be interpreted as if it carried the supported version number, A. Specifically:
 - 1) All BPDU types, parameters, and flags that are defined in version A shall be interpreted in the manner specified for version A of the protocol for the given BPDU type.
 - 2) All BPDU types, parameters, and flags that are undefined in version A for the given BPDU type shall be ignored.
 - 3) All octets that appear in the BPDU beyond the largest numbered octet defined for version A for the given BPDU type shall be ignored.
- e) Where B is less than A, the BPDU shall be interpreted as specified for the version number, B, carried in the BPDU. Specifically:
 - 1) All BPDU parameters and flags shall be interpreted in the manner specified for version B of the protocol for the given BPDU type.
 - 2) All BPDU parameters and flags that are undefined in version B for the given BPDU type shall be ignored.
 - 3) All octets that appear in the BPDU beyond the largest numbered octet defined for version B for the given BPDU type shall be ignored.

NOTE 3—In other words, if the protocol version implemented differs from the protocol version number carried in the BPDU, then only those BPDU types, parameters, and flags that are specified within the lesser numbered protocol version are interpreted by the implementation (in accordance with the lesser numbered protocol version's specification), and no attempt is made to interpret any additional BPDU types, parameters, and flags that may be specified within the greater numbered protocol version. In the specific case of STP (version 0) and RSTP (version 2), as there is only a single RST BPDU type defined in version 2, and as the RST BPDU type is undefined in version 0, a version 0 implementation will ignore all RST BPDUs. Version 2 implementations, however, recognize and process both version 0 and version 2 BPDUs. As version 2 makes no changes to the BPDU types defined for version 0 (and always transmits such BPDU types with 0 as the version identifier), version 0 BPDUs are always interpreted by version 2 implementations according to their version 0 definition.

12. Generic Attribute Registration Protocol (GARP)

12.7 Overview of GARP protocol operation

Add new subclause 12.7.10:

12.7.10 Use of GARP in point-to-point LANs

The full GARP participant state machine was designed to operate correctly in shared media environments. The fact that in such environments there might be three or more active GARP participants was the motivation behind the Passive Member and Observer states; the result is reduced traffic on a shared media LAN where more than one participant is interested in registering a particular attribute value.

In LANs that are based on point-to-point connectivity between systems, i.e., where it is certain that there can at most be only two GARP participants on any given LAN, the added complexity of the full Applicant state machine is redundant. Therefore, it is recommended in such environments to implement the Simple Applicant state machine in preference to the full Applicant state machine. The Point to Point MAC parameters (see 6.4.3) provide a means of determining whether a given MAC supports a shared media LAN segment or a point to point LAN segment.

The method of determining the timing of transmission opportunities in the state machines (the use of a timer value randomized between 0 and JoinTime seconds) was also chosen to accommodate the use of GARP in shared media environments, to avoid the risk of multicast storms occurring during periods of configuration change. In point-to-point LANs, these considerations do not apply. More particularly, in LANs that support RSTP, it is desirable to allow transmission opportunities to occur without delay under circumstances where a Rapid Spanning Tree configuration change is occurring, in order to minimize the period during which denial of service might occur due to the delay in propagating registration changes. Therefore, in point-to-point LANs, it is recommended that the definition of when a transmission opportunity (transmit-PDU!—see 12.8) can occur is redefined as follows:

transmitPDU! An opportunity to transmit a GARP PDU has occurred. A maximum transmission rate is imposed of no more than three such transmission opportunities in any period of 1.5*JoinTime seconds.

14. Bridge management

Change 14.2, Managed Objects, as follows:

14.2 Managed objects

Managed objects model the semantics of management operations. Operations upon an object supply information concerning, or facilitate control over, the Process or Entity associated with that object.

The managed resources of a MAC Bridge are those of the Processes and Entities established in 7.3 and 12.2. Specifically

- a) The Bridge Management Entity (14.4 and 7.11).
- b) The individual MAC Entities associated with each Bridge Port (14.5, 7.2, 7.5, and 7.6).
- c) The Forwarding Process of the MAC Relay Entity (14.6, 7.2, and 7.7).
- d) The Filtering Database of the MAC Relay Entity (14.7 and 7.9).
- e) The Bridge Protocol Entity (14.8, 7.10, ~~and~~ Clause 8, and Clause 17).
- f) GARP Participants (Clause 12).
- g) GMRP participants (14.10, IEEE Std 802.1D Clause 10).

The management of each of these resources is described in terms of managed objects and operations below.

NOTE—The values specified in this clause, as inputs and outputs of management operations, are abstract information elements. Questions of formats or encodings are a matter for particular protocols that convey or otherwise represent this information. This standard specifies one such protocol encoding in Clause 15 (for optional remote management).

Change 14.8, Bridge Protocol Entity, and its subclauses, as follows:

14.8 Bridge Protocol Entity

The Bridge Protocol Entity is described in 7.10, ~~and~~ Clause 8, and Clause 17. The objects that comprise this managed resource are

- a) The Protocol Entity itself and
- b) The Ports under its control.

14.8.1 The Protocol Entity

The Protocol Entity object models the operations that can be performed upon, or inquire about, the operation of the Spanning Tree Algorithm and Protocol. There is a single Protocol Entity per Bridge; it can, therefore, be identified as a single fixed component of the Protocol Entity resource.

The management operations that can be performed on the Protocol Entity are Read Bridge Protocol Parameters and Set Bridge Protocol Parameters.

14.8.1.1 Read Bridge Protocol parameters

14.8.1.1.1 Purpose

To obtain information regarding the Bridge's Bridge Protocol Entity.

14.8.1.1.2 Inputs

None.

14.8.1.1.3 Outputs

- a) Bridge Identifier—as defined in 8.5.3.7 and 17.17.3.
- b) Time Since Topology Change—in an STP Bridge, the count in seconds of the time elapsed since the Topology Change flag parameter for the Bridge (8.5.3.12) was last True, or in an RSTP Bridge, the count in seconds of the time since the tcWhile timer (17.15.7) for any Port was non-zero.
- c) Topology Change Count—in an STP Bridge, the count of the times the Topology Change flag parameter for the Bridge has been set (i.e., transitioned from False to True) since the Bridge was powered on or initialized, or in an RSTP Bridge, the count of times that there has been at least one non-zero tcWhile timer (17.15.7).
- d) Topology Change—in an STP Bridge, the value of the Topology Change parameter (8.5.3.12), or in an RSTP Bridge, asserted if the tcWhile timer (17.15.7) for any Port is non-zero.
- e) Designated Root (8.5.3.1 and 17.18.17).
- f) Root Path Cost (8.5.3.2 and 17.18.17).
- g) Root Port (8.5.3.3 and 17.17.5).
- h) Max Age (8.5.3.4 and 17.18.18).
- i) Hello Time (8.5.3.5 and 17.16.3).
- j) Forward Delay (8.5.3.6 and 17.16.2).
- k) Bridge Max Age (8.5.3.8 and 17.17.4).
- l) Bridge Hello Time (8.5.3.9 and 17.17.4).
- m) Bridge Forward Delay (8.5.3.10 and 17.17.4).
- n) Hold Time (8.5.3.14) or Transmission Limit (TxHoldCount in 17.16.6).
- o) forceVersion—the value of the Force Protocol Version parameter for the Bridge (provided only by RSTP Bridges; see 17.16.1).

14.8.1.2 Set Bridge Protocol parameters

14.8.1.2.1 Purpose

To modify parameters in the Bridge's Bridge Protocol Entity in order to force a configuration of the Spanning Tree and/or tune the reconfiguration time to suit a specific topology. In RSTP implementations, this operation causes these values to be set for all Ports of the Bridge.

14.8.1.2.2 Inputs

- a) Bridge Max Age—the new value (8.5.3.8 and 17.17.4).
- b) Bridge Hello Time—the new value (8.5.3.9 and 17.17.4).
- c) Bridge Forward Delay—the new value (8.5.3.14 and 17.17.4).
- d) Bridge Priority—the new value of the priority part of the Bridge Identifier (8.5.3.7 and 17.17.3).
- e) forceVersion (optional)—the new value of the Force Protocol Version parameter (provided only by RSTP Bridges; see 17.16.1).

14.8.1.2.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to invalid Bridge Priority value (14.3); or
 - 2) Operation accepted.

14.8.1.2.4 Procedure

The input parameter values are checked for compliance with 8.10.2 (STP Bridges) or 17.28.2 (RSTP Bridges). If they do not comply, or the value of Bridge Max Age or Bridge Forward Delay is less than the lower limit of the range specified in Table 8-3 (STP Bridges) or Table 17-5 (RSTP Bridges), then no action shall be taken for any of the supplied parameters. If the value of any of Bridge Max Age, Bridge Forward Delay, or Bridge Hello Time is outside the range specified in Table 8-3 (STP Bridges) or Table 17-5 (RSTP Bridges), then the Bridge need not take action.

~~Otherwise, the Bridge's Bridge Max Age, Bridge Hello Time, and Bridge Forward Delay parameters are set to the supplied values. The Set Bridge Priority procedure (8.8.4) is used to set the priority part of the Bridge Identifier to the supplied value.~~

Otherwise:

- a) The Bridge's Bridge Max Age, Bridge Hello Time, and Bridge Forward Delay parameters are set to the supplied values.
- b) In STP Bridges, the Set Bridge Priority procedure (8.8.4) is used to set the priority part of the Bridge Identifier to the supplied value.
- c) In RSTP Bridges, the priority component of the Bridge Identifier (17.17.3) is updated using the supplied value. For all Ports of the Bridge, the reselect parameter (17.18.29) is set TRUE, and the selected parameter (17.18.31) is set FALSE.

14.8.2 Bridge Port

A Bridge Port object models the operations related to an individual Bridge Port in relation to the operation of the Spanning Tree Algorithm and Protocol. There are a fixed set of Bridge Ports per Bridge; each can, therefore, be identified by a permanently allocated Port Number, as a fixed component of the Protocol Entity resource. The management operations that can be performed on a Bridge Port are Read Port Parameters, Force Port State, ~~and Set Port Parameters, and Force BPDU Migration Check.~~

14.8.2.1 Read Port Parameters

14.8.2.1.1 Purpose

To obtain information regarding a specific Port within the Bridge's Bridge Protocol Entity.

14.8.2.1.2 Inputs

- a) Port Number—the number of the Bridge Port.

14.8.2.1.3 Outputs

- a) Uptime—count in seconds of the time elapsed since the Port was last reset or initialized.
- b) State—the current state of the Port (i.e., Disabled, Listening, Learning, Forwarding, or Blocking) (8.4. ~~and~~ 8.5.5.2, ~~and~~ 17.5).
- c) Port Identifier—the unique Port identifier comprising two parts, the Port Number and the Port Priority field (8.5.5.1 ~~and~~ 17.18.16).
- d) Path Cost (8.5.5.3 ~~and~~ 17.16.5).
- e) Designated Root (8.5.5.4 ~~and~~ 17.18.17).
- f) Designated Cost (8.5.5.5 ~~and~~ 17.18.17).
- g) Designated Bridge (8.5.5.6 ~~and~~ 17.18.17).
- h) Designated Port (8.5.5.7 ~~and~~ 17.18.17).
- i) Topology Change Acknowledge (8.5.5.8 ~~and~~ 17.18.37).
- j) adminEdgePort (18.3.3). Present in implementations that support the identification of edge ports.
- k) operEdgePort (18.3.4). Present in implementations that support the identification of edge ports.
- l) MAC Enabled—the current state of the MAC Enabled parameter (6.4.2 of IEEE Std 802.1t-2001). Present if the implementation supports the MAC Enabled parameter.
- m) MAC Operational—the current state of the MAC Operational parameter (6.4.2 of IEEE Std 802.1t-2001). Present if the implementation supports the MAC Operational parameter.
- n) adminPointToPointMAC—the current state of the adminPointToPointMAC parameter (6.4.3). Present if the implementation supports the adminPointToPointMAC parameter.
- o) operPointToPointMAC - the current state of the operPointToPointMAC parameter (6.4.3). Present if the implementation supports the operPointToPointMAC parameter.

14.8.2.2 Force port state

14.8.2.2.1 Purpose

To ~~force set~~ the Administrative Bridge Port state (see 17.5) for the specified Port into Disabled or Blocking Enabled.

14.8.2.2.2 Inputs

- a) Port Number—the number of the Bridge Port.
- b) State—either Disabled or ~~Blocking~~ (8.4 ~~and~~ 8.5.5.2) Enabled.

14.8.2.2.3 Outputs

None.

14.8.2.2.4 Procedure

In Bridges that support STP, if the selected state is Disabled, the Disable Port procedure (8.8.3) is used for the specified Port. If the selected state is Blocking/Enabled, the Enable Port procedure (8.8.2) is used.

In Bridges that support RSTP, the effect of changing this parameter is defined in 17.5.

14.8.2.3 Set Port Parameters

14.8.2.3.1 Purpose

To modify parameters for a Port in the Bridge's Bridge Protocol Entity in order to force a configuration of the Spanning Tree.

14.8.2.3.2 Inputs

- a) Port Number—the number of the Bridge Port.
- b) Path Cost—the new value (8.5.5.3 and 17.16.5).
- c) Port Priority—the new value of the priority field for the Port Identifier (8.5.5.1 and 17.18.17).
- d) adminEdgePort—the new value of the adminEdgePort parameter (18.3.3). Present in implementations that support the identification of edge ports.
- e) MAC Enabled—the new value of the MAC Enabled parameter (6.4.2 of IEEE Std 802.1t-2001). May be present if the implementation supports the MAC Enabled parameter.
- f) adminPointToPointMAC—the new value of the adminPointToPointMAC parameter (6.4.3). May be present if the implementation supports the adminPointToPointMAC parameter.

14.8.2.3.3 Outputs

- a) Operation status. This takes one of the following values:
 - 1) Operation rejected due to invalid Port Priority value (14.3); or
 - 2) Operation accepted.

14.8.2.3.4 Procedure

~~The~~ In STP Bridges, the Set Path Cost procedure (8.8.6) is used to set the Path Cost parameter for the specified Port. The Set Port Priority procedure (8.8.5) is used to set the priority part of the Port Identifier (8.5.5.1) to the supplied value.

In RSTP Bridges, the Path Cost (17.16.5) and Port Priority (17.18.17) parameters for the Port are updated using the supplied values. The reselect parameter for the Port (17.18.29) is set TRUE, and the selected parameter for the Port (17.18.31) is set FALSE.

Insert new subclause 14.8.2.4, Force BPDU Migration Check

14.8.2.4 Force BPDU Migration Check

This operation is available only in Bridges that support RSTP, as specified in Clause 17.

14.8.2.4.1 Purpose

To force the specified Port to transmit RST BPDUs (see 17.26).

14.8.2.4.2 Inputs

- a) Port Number—the number of the Bridge Port.

14.8.2.4.3 Outputs

None.

14.8.2.4.4 Procedure

The mcheck variable (17.18.10) for the specified Port is set to the value TRUE if the value of the forceVersion variable (17.16.1) is greater than or equal to 2.

Insert new Clause 17 as follows:

17. Rapid Spanning Tree Algorithm and Protocol (RSTP)

The configuration algorithm and protocol described in this clause reduce the Bridged LAN topology to a single Spanning Tree. The configuration algorithm and protocol described here supersede the Spanning Tree Algorithm and Protocol described in Clause 8, and provide significantly faster reconfiguration. Clause 8 is retained in this standard in order to allow existing implementations of the Spanning Tree Algorithm and Protocol to remain conformant, and Bridges based on either specification can interoperate successfully. However, it is recommended that the Rapid Spanning Tree Algorithm and Protocol (RSTP) be adopted in future MAC Bridge implementations.

17.1 Requirements

The Rapid Spanning Tree Algorithm and Protocol operates to support, preserve, and maintain the quality of the MAC Service (6.1, 6.2, and 6.3), meeting the following requirements:

- a) It selects a simply and fully connected active topology from a Bridged LAN of arbitrary physical topology, eliminating data loops (6.3.3 and 6.3.4).
- b) It provides for fault tolerance by automatic reconfiguration of the Spanning Tree topology as a result of the failure of LAN components, and for the automatic accommodation of any Bridge or Bridge Port added to the Bridged LAN without the formation of transient data loops (6.1).
- c) The active topology will, with a high probability, stabilize within a short, known bounded interval in order to minimize the time for which the service is unavailable for communication between any pair of end stations (6.1).

- d) The active topology will be predictable and reproducible, and may be selected by management of the parameters of the algorithm, thus allowing the application of Configuration Management, following traffic analysis, to meet the goals of Performance Management (6.1 and 6.3.10).
- e) It operates transparently to the end stations, such that they are unaware of their attachment to a single LAN or a Bridged LAN when using the MAC Service (6.2).
- f) The communications bandwidth consumed by the Bridges in establishing and maintaining a Spanning Tree on any particular LAN is always a very small fraction of the total available bandwidth and is independent of the total traffic supported by the Bridged LAN regardless of the total number of Bridges or LANs (6.3.10).

Additionally, the algorithm and protocol meet the following goals, which limit the complexity of Bridges and their configuration:

- g) The memory requirements associated with each Bridge Port are independent of the number of Bridges and LANs in the Bridged LAN.
- h) Bridges do not have to be individually configured before being added to the Bridged LAN, other than having their MAC Addresses assigned through normal procedures.
- i) In normal operation, the time taken to configure the active topology of a Bridge LAN is independent of the timer values of the protocol.

NOTE—The values of the timers used can therefore be considerably relaxed. This contrasts with the operation of the Spanning Tree Algorithm and Protocol specified in Clause 8, where the time taken to configure is sensitive to the values of timers.

17.2 Requirements of the MAC bridges

In order for the Bridge Protocol to operate, the following are required:

- a) A unique MAC group address, recognized by all the Bridges within the Bridged LAN, that identifies the Bridge Protocol Entities of all Bridges attached to an individual LAN.
- b) An identifier for each Bridge, unique within the Bridged LAN.
- c) A distinct Port identifier for each Bridge Port, that can be assigned independently of the values used in other Bridges.

Values for each of these parameters, or a mechanism for assigning values to them, shall be provided by each Bridge. In the case of MAC Bridges that use 48-bit Universally Administered Addresses, the unique MAC Address that identifies the Bridge Protocol Entities is the Bridge Group Address (7.12.3).

In addition, to allow the configuration of the Spanning Tree active topology to be managed, the following are required:

- d) A means of assigning the relative priority of each Bridge within the set of Bridges in the Bridged LAN.
- e) A means of assigning the relative priority of each Port within the set of Ports of an individual Bridge.
- f) A means of assigning a path cost component to each Port.

These parameters may be set by management when Bridge Management is supported.

17.3 Overview

The Rapid Spanning Tree Algorithm is a distributed algorithm that selects one Bridge to be the “root” of a fully (“spanning”) and simply (“tree”) connected active topology, and assigns Port Roles (17.4.1) to individual ports on each Bridge in the Bridged LAN. Port Roles are assigned according to whether the port is to be part of the active topology connecting the Bridge to the Root Bridge (a Root Port) or connecting a LAN through the Bridge to the Root Bridge (a Designated Port), or is an Alternate or Backup Port that may provide connectivity if other Bridges, Bridge Ports, or LANs fail or are removed.

State machines associated with the Port Roles maintain and change the Port States (7.4, 17.5) that control the processing and forwarding of frames by a MAC Relay Entity (7.3). A Port State (17.5) of Discarding, Learning, or Forwarding is assigned to support (6.1) and maintain the quality (6.3) of the MAC Service. In particular, to reduce the probability of data loops and the duplication and misordering of frames to a negligible level, a transition to the Forwarding Port State may be delayed until the assignment of Port Roles is known to be consistent between Bridges.

NOTE—The Rapid Spanning Tree Algorithm and Protocol cannot protect against temporary loops caused by the interconnection of two LAN segments by devices other than Bridges (e.g., LAN repeaters) that operate invisibly with respect to support of the Bridges’ MAC Internal Sublayer Service.

The operation of RSTP provides for rapid recovery of connectivity following the failure of a Bridge, Bridge Port, or a LAN. A new Root Port can transition rapidly to the Forwarding Port State, and the use of explicit acknowledgements between Bridges allow Designated Ports to transition rapidly to the Forwarding Port State. The timers used by RSTP define worst case delays, and are used only as a backup to the normal operation of the protocol.

RSTP allows Bridge Ports to be configured such that they can transition directly to the Forwarding Port State on re-initialization of the Bridge. This may be appropriate where a specific Bridge Port is known to be connected to a LAN segment that is at the edge of the Bridged LAN, i.e., where no further Bridges are reachable via that LAN segment.

17.4 Computation of the active topology

17.4.1 Port Role Assignment

The Rapid Spanning Tree Algorithm assigns one of the following Port Roles to each Bridge Port: Root Port, Designated Port, Alternate Port, or Backup Port. A fifth role, Disabled Port, identifies a Port as having no role within the operation of Spanning Tree. Port Role assignments for ports throughout the Bridged Local Area Network are determined as follows by:

- a) A unique Bridge Identifier associated with each Bridge
- b) A Path Cost associated with each Bridge Port
- c) A Port Identifier associated with each Bridge Port

The Bridge with the best Bridge Identifier is selected as the Root Bridge. The unique Bridge Identifier for each Bridge is derived, in part, from the Bridge Address (7.12.5) and, in part, from a manageable priority component (9.2.5). The relative priority of Bridges is determined by the numerical comparison of the unique identifiers, with the lower numerical value indicating the better identifier.

Every Bridge has a Root Path Cost associated with it. For the Root Bridge this is zero. For all other Bridges it is the sum of the Path Costs for each Bridge Port receiving frames on the least cost path from the Root Bridge to that Bridge. The Path Cost associated with each Port may be manageable. Additionally, 17.28.2

recommends default values for the Path Costs associated with Ports attached to LANs of specific MAC types and speeds.

The Bridge Port on each Bridge receiving the frames on the least cost path from the Root Bridge is assigned the role of Root Port for that Bridge (the Root Bridge does not have a Root Port). If a Bridge has two or more ports with the same least Path Cost sum from the Root, then the port with the best Port Identifier is selected as the Root Port. Part of the Port Identifier is fixed and is different for each Port on a Bridge, and part is a manageable priority component (9.2.7). The relative priority of Ports is determined by the numerical comparison of the unique identifiers, with the lower numerical value indicating the better identifier.

Each LAN in the Bridged Local Area Network also has an associated Root Path Cost. This is the Root Path Cost of the lowest cost Bridge with a Bridge Port connected to that LAN. This Bridge is selected as the Designated Bridge for that LAN. If there are two or more Bridges with the same Root Path Cost, then the Bridge with the best priority (least numerical value) is selected as the Designated Bridge. The Bridge Port on the Designated Bridge that is connected to the LAN is assigned the role of Designated Port for that LAN. If the Designated Bridge has two or more ports connected to the LAN, then the Bridge Port with the best priority Port Identifier (least numerical value) is selected as the Designated Port.

In a Bridged Local Area Network whose physical topology is stable, i.e., the Rapid Spanning Tree Algorithm has communicated consistent information throughout the network, every LAN has one and only one assigned Designated Port, and every Bridge with the exception of the Root Bridge has a Root Port connected to a LAN.

Any operational Bridge Port that is not assigned a Port Role of Root Port or Designated Port is a Backup Port if that Bridge is the Designated Bridge for the attached LAN, and an Alternate Port otherwise.

An Alternate Port offers an alternate path in the direction of the Root Bridge to that provided by the Bridge's own Root Port, whereas a Backup Port acts as a backup for the path provided by a Designated Port in the direction of the leaves of the Spanning Tree. Backup Ports exist only where there are two or more connections from a given Bridge to a given LAN; hence, they (and the Designated Ports that they back up) can only exist where two ports are connected together in loopback by a point to point link, or where the Bridge has two or more connections to a shared media LAN segment.

NOTE—The distinction between the Alternate and Backup Port Roles does not appear in the Spanning Tree Algorithm and Protocol described in Clause 8. This distinction is introduced in RSTP in order to make it possible to describe the possibility of rapidly transitioning an Alternate Port to Forwarding on failure of the Root Port.

If the Port's MAC_Operational parameter (see 6.4.2 in IEEE Std 802.1t-2001) is FALSE, either as a consequence of management action or because the Port is not operable, the Bridge Port is assigned a Port Role of Disabled Port. If the Port's MAC_Operational parameter becomes TRUE, the Bridge Port is initially assigned a Port Role of Designated Port, as it is not aware of any other Bridge attached to the same LAN.

17.4.2 Spanning tree priority vectors

17.4.2.1 Definition

RSTP Bridges send information to each other, in Configuration Messages (see 17.7), to assign Port roles. The information sent for this purpose is known as a *spanning tree priority vector*. Spanning tree priority vectors provide the basis for a concise specification of RSTP's computation of the active topology, both in distributed terms across an entire Bridged LAN and in terms of the operation of each individual Bridge in support of the overall distributed algorithm. Each spanning tree priority vector comprises the following components: