



BSI Standards Publication

Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements

Part 1AB: Station and media access control connectivity discovery

National foreword

This British Standard is the UK implementation of ISO/IEC/IEEE 8802-1AB:2017. It supersedes BS ISO/IEC/IEEE 8802-1AB:2014, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/6, Data communications.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2017
Published by BSI Standards Limited 2017

ISBN 978 0 580 95311 8

ICS 35.110

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2017.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

INTERNATIONAL
STANDARD

ISO/IEC/
IEEE
8802-1AB

Second edition
2017-07

**Information technology —
Telecommunications and information
exchange between systems — Local
and metropolitan area networks —
Specific requirements —**

**Part 1AB:
Station and media access control
connectivity discovery**

*Technologies de l'information — Télécommunications et échange
d'information entre systèmes — Réseaux locaux et métropolitains —
Exigences spécifiques —*

*Partie 1AB: Découverte de connectivité des stations et du contrôle
d'accès aux supports*



Reference number
ISO/IEC/IEEE 8802-1AB:2017(E)
Documents
© IEEE 2016
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© IEEE 2016

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO or IEEE at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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

stds.ipr@ieee.org
www.ieee.org

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and nongovernmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of ISO/IEC JTC 1 is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is called to the possibility that implementation of this standard may require the 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. ISO/IEEE is not responsible for identifying essential patents or patent claims for which a license may be required, for conducting inquiries into the legal validity or scope of patents or patent claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance or a Patent Statement and Licensing Declaration Form, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from ISO or the IEEE Standards Association.

ISO/IEC/IEEE 8802-1AB was prepared by the LAN/MAN of the IEEE Computer Society (as IEEE Std 802.1AB-2016). It was adopted by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 6, Telecommunications and information exchange between systems, in parallel with its approval by the ISO/IEC national bodies, under the “fast-track procedure” defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE. IEEE is responsible for the maintenance of this document with participation and input from ISO/IEC national bodies.

This second edition of ISO/IEC/IEEE 8802-1AB cancels and replaces the first edition (ISO/IEC/IEEE 8802-1AB:2014, which has been technically revised).

IEEE Std 802.1AB™-2016

(Revision of
IEEE Std 802.1AB-2009)

**IEEE Standard for
Local and metropolitan area networks—
Station and Media Access Control
Connectivity Discovery**

Sponsor

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

Approved 29 January 2016

IEEE-SA Standards Board

Abstract: A protocol and a set of managed objects that can be used for discovering the physical topology from adjacent stations in IEEE 802[®] LANs are defined in this document.

Keywords: IEEE 802.1AB[™], link layer discovery protocol, management information base, topology discovery, topology information

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

Copyright © 2016 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 11 March 2016. Printed in the United States of America.

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

PDF: ISBN 978-1-5044-0632-1 STD20761
Print: ISBN 978-0-5044-0633-8 STDPD20761

IEEE prohibits discrimination, harassment and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

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.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

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

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. 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.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied on as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive 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 comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board

445 Hoes Lane

Piscataway, NJ 08854 USA

Laws and regulations

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

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, 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.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, 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 order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at <http://ieeexplore.ieee.org/xpl/standards.jsp> or contact IEEE at the address listed previously. For more information about the IEEE-SA or IEEE's standards development process, visit the IEEE-SA Website at <http://standards.ieee.org>.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: <http://standards.ieee.org/findstds/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at <http://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

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

Participants

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

Glenn Parsons, *Chair*
John Messenger, *Vice Chair and Maintenance Task Group Chair*
Tony Jeffree, *Editor*

Christian Boiger	Hal Keen	Jessy Rouyer
Paul Bottorff	Stephan Kehrer	Panagiotis Saltsidis
David Chen	Marcel Kiessling	Michael Seaman
Feng Chen	Philippe Klein	Daniel Sexton
Weiyang Cheng	Jouni Korhonen	Johannes Specht
Rodney Cummings	Yizhou Li	Wilfried Steiner
János Farkas	Christophe Mangin	Patricia Thaler
Norman Finn	Tom McBeath	David Thornburg
Geoffrey Garner	James McIntosh	Jeremy Touve
Eric Gray	Hiroki Nakano	Paul Unbehagen
Craig Gunther	Bob Noseworthy	Karl Weber
Stephen Haddock	Donald R. Pannell	Brian Weis
Mark Hantel	Walter Pienciak	Jordon Woods
Marc Holness	Karen Randall	Helge Zinner
Michael Johas Teener	Maximilian Riegel	Juan Carlos Zuniga
	Dan Romascanu	

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

Thomas Alexander	Raj Jain	Robert Robinson
Butch Anton	Tony Jeffree	Benjamin Rolfe
Lee Armstrong	Michael Johas Teener	Dan Romascanu
Stefan Aust	Adri Jovin	Jessy Rouyer
Christian Boiger	Shinkyō Kaku	John Santhoff
Nancy Bravin	Piotr Karocki	Bartien Sayogo
William Byrd	Stuart Kerry	Michael Seaman
Juan Carreon	Yongbum Kim	Thomas Starai
Rodney Cummings	Paul Lambert	Eugene Stoudenmire
Douglas Dorr	Robert Landman	Rene Struik
János Farkas	David Lewis	Walter Struppler
Yukihiro Fujimoto	Arthur H. Light	Michael Swearingen
David Gregson	William Lumpkins	Patricia Thaler
Randall Groves	Michael Lynch	Mark-Rene Uchida
Craig Gunther	Elvis Maculuba	Lorenzo Vangelista
Stephen Haddock	Jonathon McLendon	Dmitri Varsanofiev
Marek Hajduczenia	Richard Mellitz	George Vlantis
Jerome Henry	John Messenger	Khurram Waheed
Marco Hernandez	Charles Moorwood	Karl Weber
Guido Hiertz	Michael Newman	Hung-Yu Wei
Werner Hoelzl	Nick S. A. Nikjoo	Natalie Wienckowski
Noriyuki Ikeuchi	Satoshi Obara	Andreas Wolf
Sergiu Iordanescu	Alon Regev	Oren Yuen
Atsushi Ito	Maximilian Riegel	Zhen Zhou

When the IEEE-SA Standards Board approved this standard on 29 January 2016, it had the following membership:

John Kulick, *Chair*
Jon Walter Rosdahl, *Vice Chair*
Richard H. Hulett, *Past Chair*
Konstantinos Karachalios, *Secretary*

Masayuki Ariyoshi
 Ted Burse
 Stephen Dukes
 Jean-Phillippe Faure
 J. Travis Griffith
 Gary Hoffman
 Michael Janezic

Joseph L. Koepfinger*
 David J. Law
 Hung Ling
 Andrew Myles
 T. W. Olsen
 Glenn Parsons
 Ronald C. Peterson
 Annette D. Reilly

Stephen J. Shellhammer
 Adrian P. Stephens
 Yatin Trivedi
 Phillip Winston
 Don Wright
 Yu Yuan
 Daidi Zhong

*Member Emeritus

Historical participants

Included is a historical list of participants in the IEEE 802.1 Working Group who have dedicated their valuable time, energy, and knowledge to the creation of this material.

The following individuals participated in the 2005 publication of this standard.

Tony Jeffree, *Chair*
Paul Congdon, *Vice Chair*
Bill Lane, *Technical Editor*
Mick Seaman, *Interworking Task Group Chair*

Les Bell
 Paul Bottorff
 Jim Burns
 Marco Carugi
 Dirceu Cavendish
 Arjan de Heer
 Anush Elangovan
 Hesham Elbakoury
 David Elie-Dit-Cosaque
 Norm Finn
 David Frattura
 Gerard Goubert
 Steve Haddock
 Ran Ish-Shalom
 Atsushi Iwata

Neil Jarvis
 Manu Kaycee
 Hal Keen
 Roger Lapuh
 Loren Larsen
 Joe Lawrence
 Yannick Le Goff
 Marcus Leech
 Mahalingam Mani
 Dinesh Mohan
 Bob Moskowitz
 Don O'Connor
 Don Pannell
 Glenn Parsons

Ken Patton
 Frank Reichstein
 John Roesse
 Allyn Romanow
 Dan Romascanu
 Jessy V. Rouyer
 Ali Sajassi
 Dolores Sala
 Muneyoshi Suzuki
 Jonathan Thatcher
 Michel Thorsen
 Dennis Volpano
 Karl Weber
 Ludwig Winkel
 Michael D. Wright

The following individuals participated in the 2009 publication of this standard.

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

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

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

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

The following individuals participated in the development of Corrigendum 1 to the 2009 publication of this standard.

Tony Jeffree, Chair and Editor
Glenn Parsons, Vice-Chair and Maintenance Task Group Chair

Ting Ao	Robert Grow	Karen Randall
Kenneth Boehlke	Yingjie Gu	Josef Roese
Christian Boiger	Craig Gunther	Dan Romascanu
Brad Booth	Stephen Haddock	Jessy Rouyer
Paul Bottorff	Hitoshi Hayakawa	Ali Sajassi
Jeffrey Catlin	Mirko Jakovljevic	Panagiotis Saltsidis
Xin Chang	Markus Jochim	Rick Schell
Weiyang Cheng	Michael Johas Teener	Michael Seaman
Diego Crupnicoff	Girault Jones	Koichiro Seto
Rodney Cummings	Daya Kamath	Daniel Sexton
Donald Eastlake, III	Hal Keen	Rakesh Sharma
János Farkas	Yongbum Kim	Johannes Specht
Donald Fedyk	Philippe Klein	Kevin Stanton
Norman Finn	Oliver Kleineberg	Wilfried Steiner
Andre Fredette	Jeff Lynch	Patricia Thaler
Geoffrey Garner	Ben Mack-Crane	Jeremy Touve
Anoop Ghanwani	John Messenger	Albert Tretter
Franz Goetz	Eric Multanen	Maarten Vissers
Mark Gravel	Henry Muysshondt	Yuehua Wei
Eric Gray	David Olsen	Min Xiao
	Donald Pannell	

The following individuals participated in the development of Corrigendum 2 to the 2009 publication of this standard.

Glenn Parsons, Working Group Chair
John Messenger, Vice-Chair and Maintenance Task Group Chair
Tony Jeffree, Editor

Ting Ao	Hitoshi Hayakawa	Dan Romascanu
Christian Boiger	Jeremy Hitt	Jessy V. Rouyer
Paul Bottorff	Rahil Hussain	Panagiotis Saltsidis
David Chen	Michael Johas Teener	Behcet Sarikaya
Feng Chen	Peter Jones	Michael Seaman
Weiyang Cheng	Hal Keen	Daniel Sexton
Diego Crupnicoff	Marcel Kiessling	Johannes Specht
Rodney Cummings	Yongbum Kim	Kevin B. Stanton
Patrick Diamond	Philippe Klein	Wilfried Steiner
Aboubacar Kader Diarra	Jouni Korhonen	Vahid Tabatabaee
János Farkas	Jeff Lynch	Patricia Thaler
Norman Finn	Ben Mack-Crane	Jeremy Touve
Geoffrey Garner	Christophe Mangin	Karl Weber
Anoop Ghanwani	James McIntosh	Yuehua Wei
Mark Gravel	Eric Multanen	Brian Weis
Eric W. Gray	Donald Pannell	Jordon Woods
Craig Gunther	Karen Randall	Juan-Carlos Zuniga
Stephen Haddock	Maximilian Riegel	

Introduction

This introduction is not part of IEEE Std 802.1AB™-2016, IEEE Standard for Local and metropolitan area networks—Station and Media Access Control Connectivity Discovery.

This revision of IEEE Std 802.1AB does not include any new functionality. It simply incorporates the following into the base text of the 2009 revision:

- IEEE Std 802.1AB-2009/Cor 1-2013
- IEEE Std 802.1AB-2009/Cor 2-2015

Three annexes from the 2009 revision have been deleted:

- Annex D (Using LLDP to detect potential communication problems) was deleted because it was considered to be no longer useful.
- Annex E and Annex F were deleted because the material in them can be found in Annex D of IEEE Std 802.1Q-2014 and Clause 79 of IEEE Std 802.3-2012, respectively.

The bibliography (found in Annex G of the 2009 revision) is Annex D in this revision.

Contents

1.	Overview	1
1.1	Scope	2
1.2	Purpose	2
2.	Normative references	3
3.	Definitions and numerical representation	5
3.1	Definitions	5
3.2	Numerical representation	6
4.	Acronyms and abbreviations	7
5.	Conformance	9
5.1	Terminology	9
5.2	Protocol Implementation Conformance Statement (PICS)	9
5.3	Required capabilities	9
5.4	Optional capabilities	10
6.	Principles of operation	11
6.1	Transmission and reception	12
6.2	LLDP operational modes	12
6.3	LLDP information categories	13
6.4	TLV selection	13
6.5	Transmission principles	13
6.6	Reception principles	14
6.7	Systems with multiple LLDP Agents	14
6.8	LLDP and Link Aggregation	18
7.	LLDPDU transmission, reception, and addressing	19
7.1	Destination address	19
7.2	Source address	21
7.3	EtherType use and encoding	21
7.4	LLDPDU reception	22
8.	LLDPDU and TLV formats	23
8.1	LLDPDU bit and octet ordering conventions	23
8.2	LLDPDU format	23
8.3	TLV categories	24
8.4	Basic TLV format	24
8.5	Basic management TLV set formats and definitions	26
8.6	Organizationally Specific TLVs	34
9.	LLDP agent operation	37
9.1	Overview	37
9.2	State machines	40
10.	LLDP management	57
10.1	Data storage and retrieval	57

10.2	The LLDP management entity's responsibilities.....	57
10.3	Managed objects	59
10.4	Data types.....	59
10.5	LLDP variables	59
11.	LLDP MIB definitions.....	62
11.1	Internet Standard Management Framework.....	62
11.2	Structure of the LLDP MIB	62
11.3	Relationship to other MIBs.....	67
11.4	Security considerations for LLDP base MIB module.....	68
11.5	LLDP MIB modules	70
Annex A	(normative) PICS proforma.....	121
Annex B	(normative) PTOPO MIB update	127
Annex C	(informative) Example LLDP transmission frame formats.....	128
Annex D	(informative) Bibliography.....	129

List of figures

Figure 6-1, LLDP agent and its relationship to its LLC entity	11
Figure 6-2, Relationship between LLDP agents, LLC Entities, MSAPs, and the LLDP management entity	15
Figure 6-3, LLDP in a MAC Bridge	16
Figure 6-4, LLDP in an end system with port-based network access control	16
Figure 6-5, LLDP in a MAC Bridge that uses port-based network access control on both ports	17
Figure 6-6, Scope of group MAC addresses	17
Figure 6-7, Multiplexing and demultiplexing using shims	18
Figure 7-1, MSDU format	19
Figure 8-1, LLDPDU format	23
Figure 8-2, Basic TLV format	24
Figure 8-3, End Of LLDPDU TLV format	26
Figure 8-4, Chassis ID TLV format	26
Figure 8-5, Port ID TLV format	28
Figure 8-6, Time To Live TLV format	29
Figure 8-7, Port Description TLV format	29
Figure 8-8, System Name TLV format	30
Figure 8-9, System Description TLV format	31
Figure 8-10, System Capabilities TLV format	31
Figure 8-11, Management Address TLV format	33
Figure 8-12, Basic format for Organizationally Specific TLVs	35
Figure 9-1, Transmit state machine	54
Figure 9-2, Receive state machine	55
Figure 9-3, Transmit timer state machine	56
Figure 11-1, LLDP MIB block diagram	62
Figure C.1, IEEE 802.3 LLDP frame format	128
Figure C.2, IEEE 802.11 LLDP frame format	128

List of tables

Table 7-1, Group MAC addresses used by LLDP	20
Table 7-2, Support for MAC addresses in different systems	21
Table 7-3, LLDP EtherType	22
Table 8-1, TLV type values	25
Table 8-2, chassis ID subtype enumeration	27
Table 8-3, port ID subtype enumeration	28
Table 8-4, System capabilities	32
Table 9-1, Subclause/operating mode applicability	37
Table 9-2, State machine symbols	41
Table 11-1, MIB object groups and operating mode applicability	63
Table 11-2, LLDP MIB structure and object cross reference	63

IEEE Standard for Local and metropolitan area networks— Station and Media Access Control Connectivity Discovery

IMPORTANT NOTICE: IEEE Standards documents are not intended to ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

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

1. Overview

The Link Layer Discovery Protocol (LLDP) specified in this standard allows stations attached to an IEEE 802[®] LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by those management entity or entities.

The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

1.1 Scope

The scope of this standard is to define a protocol and management elements, suitable for advertising information to stations attached to the same IEEE 802 LAN, for the purpose of populating physical topology and device discovery management information databases. The protocol facilitates the identification of stations connected by IEEE 802 LANs/MANs, their points of interconnection, and access points for management protocols.

This standard defines a protocol that

- a) Advertises connectivity and management information about the local station to adjacent stations on the same IEEE 802 LAN.
- b) Receives network management information from adjacent stations on the same IEEE 802 LAN.
- c) Operates with all IEEE 802 access protocols and network media.
- d) Establishes a network management information schema and object definitions that are suitable for storing connection information about adjacent stations.
- e) Provides compatibility with the IETF PTOPO MIB (IETF RFC 2922 [B9]).¹

1.2 Purpose

An IETF MIB (IETF RFC 2922 [B9]) and a number of vendor specific MIBs have been created to describe a network's physical topology and associated systems within that topology.

This standard specifies the necessary protocol and management elements to

- a) Facilitate multi-vendor inter-operability and the use of standard management tools to discover and make available physical topology information for network management.
- b) Make it possible for network management to discover certain configuration inconsistencies or malfunctions that can result in impaired communication at higher layers.
- c) Provide information to assist network management in making resource changes and/or re-configurations that correct configuration inconsistencies or malfunctions identified in b) above.

¹The numbers in brackets correspond to those in the bibliography in Annex D.

2. Normative references

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 802[®], IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.^{2, 3}

IEEE Std 802.1AC[™], IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Service Definition.

IEEE Std 802.1AE[™], IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security.

IEEE Std 802.1AX[™], IEEE Standard for Local and Metropolitan Area Networks—Link Aggregation.

IEEE Std 802.1Q[™], IEEE Standards for Local and Metropolitan Area Networks: Bridges and Bridged Networks.

IEEE Std 802.1X[™], IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control.

IEEE Std 802.3[™], IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.

IETF RFC 2863, The Interfaces Group MIB, June 2000.⁴

IETF RFC 3046, DHCP Relay Agent Information Option, January 2001.

IETF RFC 3232, Assigned Numbers: RFC 1700 is Replaced by an On-line Database, January 2002.⁵

IETF RFC 3410, Introduction and Applicability Statements for Internet Standard Management Framework, December 2002.

IETF RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP), December 2002.

IETF RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), December 2002.

IETF RFC 3629, UTF-8, a transformation format of ISO 10646, November 2003.

IETF RFC 4502, Remote Network Monitoring Management Information Base Version 2, May 2006.

²IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

³IEEE publications are available from The Institute of Electrical and Electronics Engineers (<http://standards.ieee.org>).

⁴IETF documents (i.e., RFCs) are available for download at <http://www.rfc-archive.org/>.

⁵The IETF RFC 3232 ianaAddressFamilyNumbers on-line database module is accessible at <http://www.iana.org>.

IETF RFC 4639, Cable Device Management Information Base for Data-Over-Cable Service Interface Specification (DOCSIS) Compliant Cable Modems and Cable Modem Termination Systems, December 2006.

IETF RFC 4789, Simple Network Management Protocol (SNMP) over IEEE 802 Networks, November 2006.

IETF RFC 6933, Entity MIB (Version 4), May 2013.

ISO/IEC 8824-1 [ITU-T Rec. X.680 (2002)], Abstract Syntax Notation One (ASN.1): Specification of Basic Notation.⁶

⁶ASN.1 standards are available at <http://asn1.elibel.tm.fr/en/standards/index.htm#asn1>.

3. Definitions and numerical representation

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.⁷

alpha-numeric information: Information that is encoded using the 8-bit Universal Character Set (UCS)/Unicode Transformation Format (UTF-8) octet sequence [IETF RFC 3629].

chassis: A physical component incorporating one or more IEEE 802[®] LAN stations and their associated application functionality.

chassis identifier: An administratively assigned name that identifies the particular chassis within the context of an administrative domain that comprises one or more networks.

IEEE 802[®] LAN: Local area network (LAN) technologies that provide a media access control (MAC) Service equivalent to the MAC Service defined in IEEE Std 802.1AC.

IEEE 802[®] LAN station: An IEEE 802-compatible entity that incorporates all the necessary mechanisms to participate in media access control of an IEEE 802 LAN, and that is at least capable of providing the MAC service plus the mandatory capabilities of the LLC.

NOTE 1—For example, routers and host computers are stations in a bridged network. Bridges, in addition to their relay function, also include station capabilities.⁸

Link Layer Discovery Protocol (LLDP): A media-independent protocol capable of running on all IEEE 802[®] LAN stations and to allow an LLDP agent to learn the connectivity and management information from adjacent stations.

LLDP agent: The protocol entity that implements LLDP for a particular MSAP associated with a Port.

MAC service access point (MSAP): The access point for MAC services provided to the LLC sublayer.

MSAP identifier: The identifier of a MAC service access point.

NOTE 2—In this standard, the concatenation of the chassis identifier and the port identifier is used by LLDP as an MSAP identifier, to identify the port associated with an IEEE 802[®] LAN station.

management entity: The protocol entity that implements a particular network management protocol and that provides access support to a MIB associated with the protocol and implemented on a host chassis.

Management Information Base (MIB): The instantiation of all MIB modules in a managed entity (e.g., system or device).

Management Information Base module (MIB module): The specification or schema for a data base that can be populated with the information required to support a network management information system.

network: An interconnected group of systems, each comprising one or more IEEE 802[®] LAN stations.

⁷IEEE Standards Dictionary Online subscription is available at:
http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html.

⁸Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

Network Management System (NMS): A management system that is capable of utilizing the information in a MIB.

object identifier (OID): An identifier used to name an object. Structurally, an OID consists of a node in a hierarchically-assigned namespace, formally defined in ISO/IEC 8824-1, Abstract Syntax Notation 1 (ASN.1). OIDs are used in this standard to identify MIB modules and the objects they contain.

physical network topology: The identification of systems, of IEEE 802[®] LAN stations that compose each system, and of the IEEE 802 LAN stations that attach to the same IEEE 802 LAN.

port: The entity in a chassis/system to support an MSAP. A port incorporates one and only one MSAP and identifies the collection of manageable entities that provide the MAC Service at the MSAP.

port identifier: An administratively assigned name that identifies the particular port within the context of a system, where the identification is convenient, local to the system, and persistent for the system's use and management (whereas the MAC address that globally identifies the MSAP can not be).

system: A managed collection of hardware and software components incorporating one or more chassis, stations and ports.

station only: A non-forwarding IEEE 802[®] LAN station such as a user workstation, network file server, or print server.

type, length, value (TLV): A short, variable length encoding of an information element consisting of sequential type, length, and value fields where the type field identifies the type of information, the length field indicates the length of the information field in octets, and the value field contains the information, itself.

3.2 Numerical representation

Decimal, hexadecimal, and binary numbers are used within this document. For clarity, decimal numbers are generally used to represent counts, hexadecimal numbers are used to represent addresses, and binary numbers are used to describe bit patterns within binary fields.

Decimal numbers are represented in their usual 0, 1, 2, ... format. Hexadecimal numbers are represented by a string of one or more hexadecimal (0–9, A–F) digits followed by the subscript 16, except in C-code contexts, where they are written as $0\times123EF2$, etc. Binary numbers are represented by a string of one or more binary (0,1) digits, followed by the subscript 2. Thus the decimal number “26” may also be represented as “ $1A_{16}$ ” or “ 11010_2 ”.

MAC addresses, EtherType values, and OUI/EUI values are represented as strings of 8-bit hexadecimal numbers separated by hyphens and without a subscript, as, for example, “01-80-C2-00-00-15” or “AA-55-11”, using the hexadecimal representation defined in IEEE Std 802.

4. Acronyms and abbreviations

AP	Access Point
BSSID	basic service set identification
DA	Destination Address
DS	Distribution System
EPD	Ethertype Protocol Discrimination
EUI	Extended Unique Identifier
FCS	Frame Check Sequence
IANA	Internet Assigned Numbers Authority
ID	Identifier
IETF	Internet Engineering Task Force
KaY	Media access control Security Key Agreement Entity
LLC	logical link control (sublayer)
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol data unit
LSAP	link service access point
MAC	media access control (sublayer)
MAU	medium attachment unit
MDI	media dependent interface
MIB	Management Information Base (module)
MSAP	Media access control service access point
MSDU	Media access control service data unit
NMS	Network Management System
OID	object identifier
OUI	organizationally unique identifier
PD	Powered Device
PHY	physical (sublayer)

PMD	physical media dependent (sublayer)
PSE	Power Sourcing Equipment
PVID	port virtual local area network identifier
PPVID	port and protocol virtual local area network identifier
PTOPO	the name of the Internet Engineering Task Force physical topology Management Information Base
RFC	Request for comments
SA	Source Address
SecY	Media access control Security Entity
SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
TPMR	Two-port Media access control relay
TLV	type, length, value
TTL	time to live (value)
UCS	Universal Character Set
UTF-8	8-bit Universal Character Set/Unicode Transformation Format
VID	virtual local area network identifier

5. Conformance

This clause specifies the mandatory and optional capabilities provided by conformant implementations of this standard.

5.1 Terminology

For consistency with IEEE and existing IEEE 802.1™ standards terminology, requirements placed upon conformant implementations of this standard are expressed using the following terminology:

- a) *Shall* is used for mandatory requirements.
- b) *May* is used to describe implementation or administrative choices (“may” means “is permitted to,” and hence, “may” and “may not” mean precisely the same thing).
- c) *Should* is used for recommended choices (the behaviors described by “should” and “should not” are both permissible but not equally desirable choices).

The PICS proforma (see Annex A) reflects the occurrences of the words *shall*, *may*, and *should* within the standard.

The standard avoids needless repetition and apparent duplication of its formal requirements by using *is*, *is not*, *are*, and *are not* for definitions and the logical consequences of conformant behavior. Behavior that is permitted but is neither always required nor directly controlled by an implementor or administrator, or whose conformance requirement is detailed elsewhere, is described by *can*. Behavior that never occurs in a conformant implementation or system of conformant implementations is described by *can not*. The word *allow* is used as a replacement for the phrase “support the ability for,” and the word *capability* means “is able to, or can be configured to.”

5.2 Protocol Implementation Conformance Statement (PICS)

The supplier of an implementation that is claimed to conform to this standard shall complete a copy of the PICS proforma provided in Annex A and shall provide the information necessary to identify both the supplier and the implementation.

5.3 Required capabilities

A system for which conformance to this standard is claimed shall, for all ports for which support is claimed, include the following capabilities:

- a) If port access is controlled by IEEE Std 802.1X,⁹ LLDP exchanges shall be supported through the controlled port, as specified in Clause 6.
- b) The destination and source addressing shall conform to 7.1 and 7.2.
- c) EtherType encapsulation shall conform to 7.3.
- d) LLDPDU recognition and reception shall conform to the operation of the receive state machine as defined in 9.2.9.
- e) LLDPDU encapsulation shall conform to the specifications in 8.2.
- f) The basic TLV format capability shall be implemented as defined in 8.4.
- g) The basic management set of TLVs shall be implemented as defined in 8.5.
- h) The Organizationally Specific TLV format capability shall be implemented as defined in 8.6.

⁹Information on references can be found in Clause 2.

- i) The protocol shall conform to the specifications for all Clause 9 subclauses indicated in Table 9-1 for the particular operating mode (transmit only, receive only, or transmit and receive) being implemented.
- j) If receipt of LLDPDUs is supported, for every set of TLVs (the basic management set and any organizationally specific sets) supported, support shall be implemented for receipt of every TLV defined in the set.
- k) If transmission of LLDPDUs is supported, for every set of TLVs (the basic management set and any organizationally specific sets) supported, support shall be implemented for transmission of every TLV defined in the set.
- l) If transmission of LLDPDUs is supported, for every set of TLVs (the basic management set and any organizationally specific sets) supported, a capability shall be implemented for users to determine which optional TLVs are transmitted in any particular LLDPDU.
- m) If SNMP is supported, then
 - 1) The system shall conform to the LLDP management specifications in Clause 11 and shall implement the sections of version 2 of the basic LLDP MIB indicated in Table 11-1 for the operating mode being implemented.
 - 2) The system shall support at least one of the transport mappings defined by IETF RFC 3417 or IETF RFC 4789.
- n) If SNMP is not supported, the system shall provide storage and retrieval capability equivalent to the functionality specified in 10.1 for the operating mode being implemented.

5.4 Optional capabilities

A system for which conformance to this standard is claimed may, for each port for which support is claimed, support the following capabilities:

- a) If port access is controlled by IEEE Std 802.1X, LLDP exchanges may be supported through the uncontrolled port, as specified in Clause 6.

LLDP is a link layer protocol that allows an IEEE 802 LAN station to advertise the capabilities and current status of the system associated with an MSAP. The MSAP provides the MAC service to an LLC Entity, and that LLC Entity provides an LSAP to an LLDP agent that transmits and receives information to and from the LLDP agents of other stations attached to the same LAN. The information distributed and received in each LLDPDU is stored in one or more Management Information Bases (MIBs). Figure 6-1 illustrates the LLDP agent and its relationship to its LLC Entity and MSAP, and to additional MIBs designed by the IETF, IEEE 802, and others.



NOTE 1—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 Length/Type field as specified in IEEE Std 802.3, or the use of the SNAP encapsulation of EtherTypes as described in IEEE Std 802. Hence, “LSAP” in the above description can refer to the use of IEEE Std 802.2 LLC addresses, or an EtherType, as a means of higher layer protocol identification.

AVA Documents
Document Sharing Hub

6.1 Transmission and reception

The information fields in each LLDP frame are contained in a Link Layer Discovery Protocol Data Unit (LLDPDU) as a sequence of variable length information elements, that each include type, length, and value fields (known as TLVs), where

- a) Type identifies what kind of information is being sent.
- b) Length indicates the length of the information string in octets.
- c) Value is the actual information that needs to be sent (for example, a binary bit map or an alphanumeric string that can contain one or more fields).

Each LLDPDU contains the following three mandatory TLVs (see Table 8-1), and can contain optional TLVs as selected by network management:

- d) A Chassis ID TLV.
- e) A Port ID TLV.
- f) A Time To Live TLV.
- g) Zero or more optional TLVs, as allowed by the maximum size of the LLDPDU.
- h) An optional End Of LLDPDU TLV.

The chassis ID and the port ID values are concatenated to form a logical MSAP identifier that is used by the recipient to identify the sending LLDP agent/port. Both the chassis ID and port ID values can be defined in a number of convenient forms. Once selected, however, the chassis ID/port ID value combination remains the same as long as the particular port remains operable.

NOTE 1—The statement above is true for any LLDP agent; however, there can be multiple LLDP agents sending and receiving LLDPDUs using different MAC addresses.

A non-zero value in the time to live (TTL) field of the Time To Live TLV tells the receiving LLDP agent how long all information pertaining to this LLDPDU's MSAP identifier is valid so that all the associated information can later be automatically discarded by the receiving LLDP agent if the sender fails to update it in a timely manner. A zero value indicates that any information pertaining to this LLDPDU's MSAP identifier is to be discarded immediately.

NOTE 2—A TTL value of zero can be used, for example, to signal that the sending port has initiated a port shutdown procedure.

The End Of LLDPDU TLV marks the end of the LLDPDU.

The format for the LLDPDU is defined in 8.2. The TLV categories and the basic TLV format are defined in 8.3 and 8.4. The specific format and field contents for the Chassis ID TLV are defined in 8.5.2; for the Port ID TLV, in 8.5.3; for the Time To Live TLV in 8.5.4; and for the End Of LLDPDU TLV, in 8.5.1.

6.2 LLDP operational modes

LLDP is a one way protocol. An LLDP agent can transmit information about the capabilities and current status of the system associated with its MSAP identifier. The LLDP agent can also receive information about the capabilities and current status of the system associated with a remote MSAP identifier. LLDP does not itself contain a mechanism for soliciting specific information from other LLDP agents, nor does it provide a specific means of confirming the receipt of information.

NOTE—The LLDP protocol is designed to advertise information useful for discovering pertinent information about a remote port and to populate topology MIBs. It is not intended to act as a configuration protocol for remote systems, nor as a mechanism to signal control information between ports. During the operation of LLDP, it may be possible to

discover configuration inconsistencies between systems on the same IEEE 802 LAN. LLDP does not provide a mechanism to resolve those inconsistencies. Rather, it provides a means to report discovered information to higher layer management entities.

LLDP allows the transmitter and the receiver to be separately enabled, making it possible to configure an implementation so the local LLDP agent can either transmit only or receive only, or so the local LLDP agent can transmit and receive LLDP information.

6.3 LLDP information categories

The following basic management TLV set (this set is required in all LLDP implementations) is defined by this standard and can be used to describe the system and/or to assist in the detection of configuration inconsistencies associated with the MSAP identifier:

- a) Port Description TLV.
- b) System Name TLV.
- c) System Description TLV.
- d) System Capabilities TLV (indicates both the system's capabilities and its current primary network function, such as end station, bridge, router).
- e) Management Address TLV.

Table 8-1 includes a list of the optional TLVs in the basic management set and provides subclause references for their specific definitions.

Organizationally Specific TLVs can be defined by either the professional organizations or the individual vendors that are involved with the particular functionality being implemented within a system. The basic format and procedures for defining Organizationally Specific TLVs are provided in 8.6.

6.4 TLV selection

Information for constructing the various TLVs to be sent is stored in the LLDP local system MIB. The selection of which particular TLVs to send is under control of network management. Information received from remote LLDP agents is stored in the LLDP remote systems MIB.

6.5 Transmission principles

Transmission can be initiated either by the expiration of a transmit countdown timing counter or by a change in the value of one or more of the information elements (managed objects) associated with the local system. When a transmit cycle is initiated, the LLDP management entity extracts the managed objects from the LLDP local system MIB and formats this information into TLVs. The TLVs are inserted into an LLDPDU that is passed to the LLDP transmit module. The LLDP transmit module prepends addressing parameters to the LLDPDU as defined in 8.2, 8.3, and 8.4. The LLDPDU and TLV formats are defined in Clause 8. The LLDP transmit state machine is described in 9.2.1 and 9.2.8.

NOTE 1—Because a transmission cycle can be initiated whenever a change occurs within the LLDP local system MIB, it is possible that a series of successive changes over a short period of time could trigger a number of LLDP frames to be sent, each reporting only a single change. LLDP utilizes a transmission delay timer that can be set by network management to ensure that there is a defined maximum number of LLDPDU transmissions in a given time period.

NOTE 2—Under normal circumstances, the information in the receiving LLDP agent's remote systems MIB is refreshed periodically to avoid being discarded due to ageing. To prevent the receiving LLDP agent's remote systems MIB information being aged out because a refresh frame has been lost in transmission, the sending LLDP agent typically sets the TTL value so that several refresh cycles can occur before the received MIB information ages out.

LLDP can disclose information about a device and network that could be considered sensitive in certain environments. Implementers are encouraged to provide controls that take into account the link protection characteristics when including information in an LLDP message. Different information can be included if an LLDP message is being sent on the uncontrolled port, the controlled port, or a MACsec protected connectivity association.

6.6 Reception principles

The LLDP receive module uses the services of the LLC entity to recognize that the incoming MA_UNITDATA.indication contains the correct combination of destination address and MSDU header values to identify it as resulting from a received LLDPDU. The LLDPDU recognition procedures are defined in 7.4 and 9.2.7.7.

6.6.1 LLDPDU and TLV error handling

The LLDPDU is checked to ensure that it contains the correct sequence of three mandatory TLVs at the beginning of the frame (Chassis ID TLV, Port ID TLV, and Time To Live TLV) and then each optional TLV is validated in succession. LLDPDUs that contain detectable errors in the first three mandatory TLVs are discarded. Optional TLVs that contain detectable errors are discarded [see 9.2.7.7.2 c)]. TLVs that are not recognized, but that also contain no basic format errors, are assumed to be valid and are stored for possible later retrieval by network management (see 9.2.7.7.1 and 9.2.7.4). If the End Of LLDPDU TLV is present, any octets that follow it are discarded.

TLVs in which the information string length field contains a value that is greater than the sum of the lengths of the fields within the information string are not discarded.

NOTE—This approach allows later versions of a TLV to define additional fields at the end of the information string; implementations based on an earlier version of the TLV can therefore continue to process the fields that were defined in that version and ignore any new fields added at the end of the information string in later versions. Any information contained in such new fields is not made available to network management protocols via the standard MIB.

6.6.2 LLDP remote systems MIB update

The LLDP remote systems MIB is updated after all TLVs have been validated. LLDP remote system MIB update procedures are defined in 9.2.7.7.4, 9.2.7.7.5, and 9.2.7.4. The LLDP receive state machine is described in 9.2.1 and 9.2.9.

6.7 Systems with multiple LLDP Agents

Each LLDP agent advertises a single set of information in the various TLVs it encodes in each transmitted LLDPDU, and is associated with the MSAP that supports the LLC entity that the agent uses to transmit and receive. Each LLDP agent uses its LSAP directly, without the use of any additional multiplexing or addressing above the LSAP to support the use of that LSAP by multiple agents; and each LLC entity provides service to one and only one protocol entity at each of its LSAPs that it supports, using the service provided by a single MSAP. It follows that each LLDP agent makes use of a unique MSAP, and that the agent can be uniquely identified by the receiving agent using the MSAP's identifier as specified in 6.2. A single LLDP management entity can support the operation of multiple LLDP agents within the same system.

Figure 6-2 illustrates the relationship between the LLDP agents, LLC Entities, MSAPs, and the LLDP management entity.

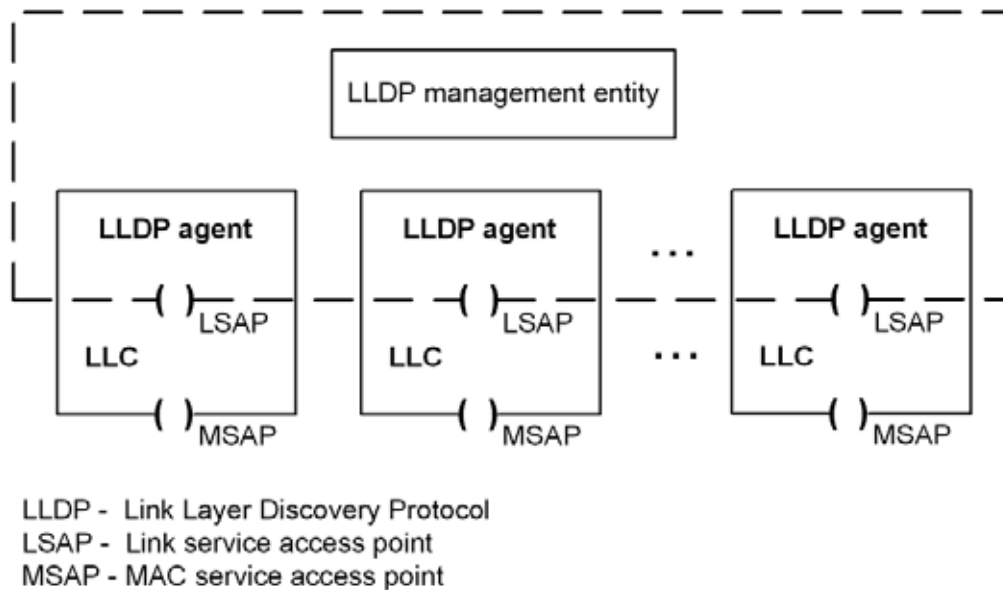


Figure 6-2—Relationship between LLDP agents, LLC Entities, MSAPs, and the LLDP management entity

A given system can require the use of multiple LLDP agents because it naturally comprises multiple MSAPs, or because it needs to be able to transmit different information (different sets of TLVs) to different sets of peers. These sets of peers can be determined by the way that the MAC service is supported within the system (see IEEE Std 802.1AC-2015 for a description of the connectionless connectivity that characterizes an IEEE 802 LAN). A MAC Bridge (see IEEE Std 802.1Q), for example, attaches to multiple LANs, each providing the MAC service at a distinct MSAP. A different example is a station that uses port-based network access control (IEEE Std 802.1X) to provide both a Controlled Port and an Uncontrolled Port, i.e., two distinct MSAPs with potentially different connectivity, for transmission and reception to and from a single LAN. Similarly, different destination addresses can be associated with different sets of potential recipients. Table 7-1 identifies group MAC addresses that can be used for LLDPDU transmission, and 7.1 describes the different transmission scopes associated with each address. LLDP can also be used in conjunction with individual MAC addresses, and with other group MAC addresses. Distinct LLDP agents, and hence separate and distinct protocol state machines, local and remote MIB tables, and MSAPs are maintained for each LLDPDU destination address, even if the use of two or more MSAPs can result in transmission and reception on the same LAN.

NOTE—For a given MAC address that is used as a destination address in received LLDPDUs, there is the possibility for a station to receive LLDPDUs from multiple senders. All LLDPDUs that carry that destination MAC address are received by a single LLDP agent, via a single MSAP; however, as the LLDPDU carries information that identifies the source of the LLDPDU, information carried in LLDPDUs from different senders is able to be recorded independently in the remote systems MIB.

Figure 6-3 illustrates the use of LLDP in a MAC Bridge, with an LLDP agent for each of the two ports shown. Figure 6-4 shows the use of LLDP in an end system with port-based network access control (IEEE Std 802.1X) supported by MACsec (IEEE Std 802.1AE); an LLDP agent is supported by the Controlled Port and an additional LLDP agent may be supported by the Uncontrolled Port. Figure 6-5 shows LLDP in a MAC Bridge that uses port-based network access control on both ports.

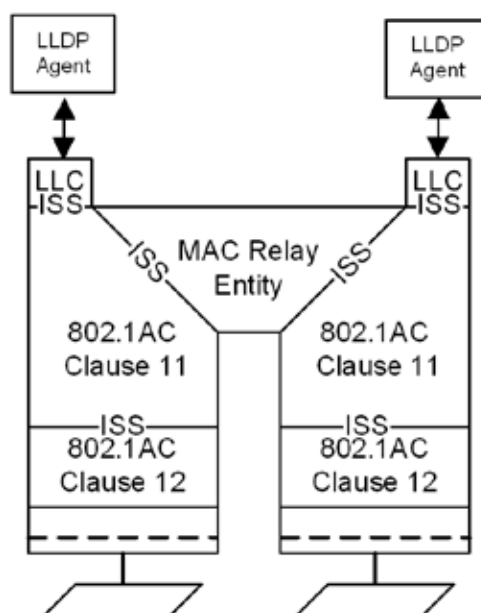


Figure 6-3—LLDP in a MAC Bridge

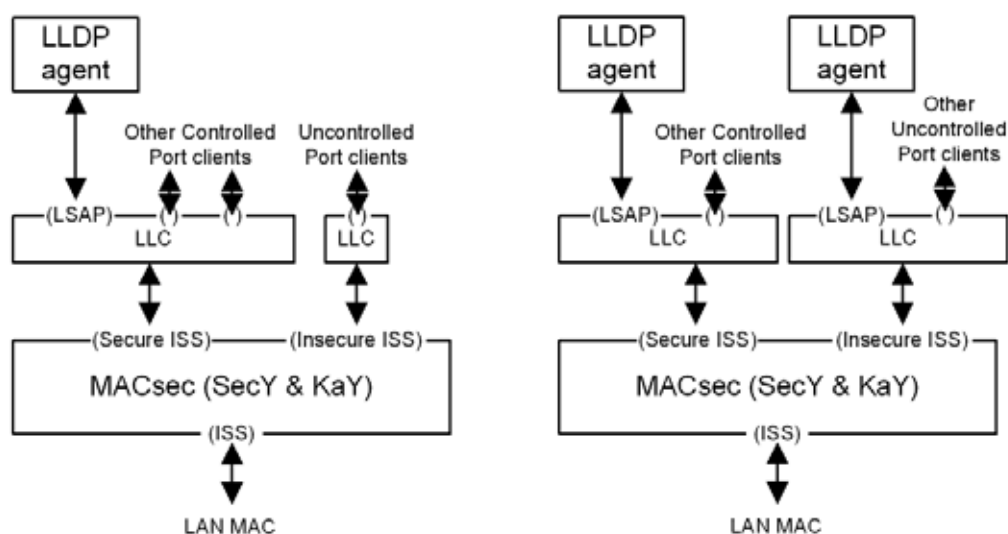


Figure 6-4—LLDP in an end system with port-based network access control

LLDP frames sent on an unprotected link may be modified by an attacker. If an implementation is going to take action based upon a received LLDP attribute, it is advisable to take into account whether the message was received on a protected link, and allow for the system to be configured such that only information received in protected messages is acted upon.



The diagram illustrates a network topology for a customer bridge. It shows a sequence of bridges connected in a line. From left to right, the components are: a Customer Bridge, a Nearest non-TPMR Bridge, an S-VLAN Bridge, a Nearest non-TPMR Bridge, another S-VLAN Bridge, a Nearest non-TPMR Bridge, a TPMR bridge, and a final Customer Bridge. A dashed line at the top is labeled 'Nearest Customer Bridge'. Arrows indicate the 'Nearest Bridge' for each bridge in the sequence.

More than one LLDP agent, each using a different address scope, can be instantiated for a given system port by adding a simple shim that provides the necessary distinct MSAPs by multiplexing and demultiplexing between those MSAPs and a common MSAP for the port, as illustrated in Figure 6-7.

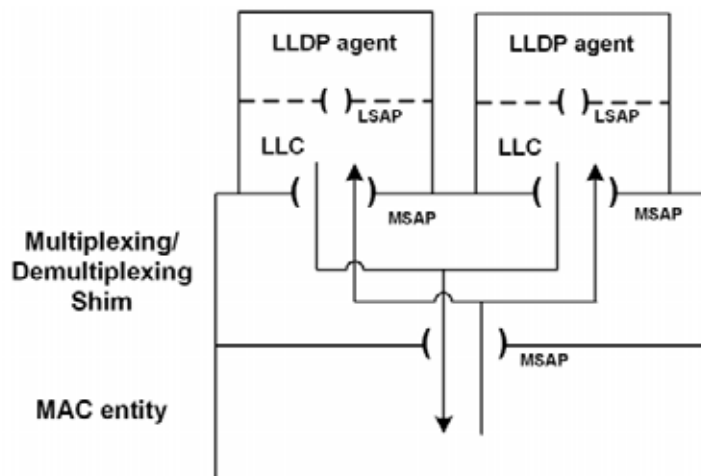


Figure 6-7—Multiplexing and demultiplexing using shims

6.8 LLDP and Link Aggregation

An LLDP agent can be configured on an IEEE 802.1AX™ Aggregated Port and/or on any number of the physical ports belonging to the Aggregation. Some TLVs (e.g., the Power Via MDA TLV defined in 79.3.2 of IEEE Std 802.3-2012) only make sense when transmitted from an LLDP agent configured on a physical port, and can cause incorrect operation if configured on an Aggregation. Other TLVs (e.g., the DCBX TLVs defined in 38.4 of IEEE Std 802.1Q-2014) make sense only when transmitted from an Aggregated Port, because they carry information applicable to the simulated single interface represented by the Aggregation. Not all standards that define LLDP TLVs are careful to state whether each TLV is applicable to an Aggregation, to a physical port, or to both. Only LLDP TLVs that are appropriate for transmission on a given Port should be transmitted on that Port.

An LLDP agent configured on an Aggregated Port, or on one of the physical ports of an Aggregation, transmits the Link Aggregation TLV, and processes received LLDPDUs, as specified in F.1 of IEEE Std 802.1AX-2014. An LLDP agent configured on a physical port of an Aggregation uses the LLDP Parser/Multiplexer as specified in 6.1.3 of IEEE Std 802.1AX-2014 for the transmission and reception of LLDPDUs containing TLVs that are specific to that physical port. Since a port not running Link Aggregation is equivalent to an Aggregation with a single physical port, any LLDP agent can transmit the Link Aggregation TLV and process received LLDPDUs as specified in 802.1AX.

NOTE—The consideration of aggregated vs. Physical ports is similar to the distinction among destination MAC addresses discussed in 7.1. In both cases, LLDP TLVs that carry information specific to a physical link should be used only in the LLDP agent with the shortest reach.

7. LLDPDU transmission, reception, and addressing

This standard is intended to be compatible with all IEEE 802 MACs.

LLDP uses the service provided by the LLDP/LSAP and LLC to transmit and receive LLDPDUs. Each LLDPDU is transmitted as a single MAC service request by an LLC entity that uses a single instance of the MAC Service provided at an MSAP. Each incoming LLDP frame is received at the MSAP by the LLC entity as a MAC service indication.

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., EtherType Protocol Discrimination (EPD) as specified in IEEE Std 802.

The parameters of each service request and service indication comprise

- a) Destination address
- b) Source address
- c) EtherType
- d) LLDPDU

The LLDP EtherType, used to identify the LLDP protocol, is prepended to the LLDPDU as shown in Figure 7-1 to form the MSDU of the corresponding MAC service request.



Figure 7-1—MSDU format

The values of the parameters used by LLDP, and their encoding by the LLC entity that supports the LLDP LSAP, are specified in the following subclauses.

7.1 Destination address

A set of standard group MAC addresses that can be used by LLDP is specified in Table 7-1. These addresses are in the range of IEEE Std 802.1Q C-VLAN and MAC Bridge component Reserved addresses (see Table 8-1 in IEEE Std 802.1Q-2014), the S-VLAN component Reserved addresses (see Table 8-2 in IEEE Std 802.1Q-2014), and the TPMR component Reserved addresses (see Table 8-3 in IEEE Std 802.1Q-2014). The choice of address used determines the scope of propagation of LLDPDUs within a bridged LAN, as follows:

- a) The **nearest bridge** group MAC address is an address that no conformant Two-Port MAC Relay (TPMR) component, S-VLAN component, C-VLAN component, or MAC Bridge component can forward. LLDPDUs transmitted using this destination address can therefore travel no further than those stations that can be reached via a single individual LAN from the originating station. LLDPDUs received on this address therefore represent information about stations that are attached to the same individual LAN segment as the recipient station.

NOTE 1—This address was selected in order to make it possible to transmit an LLDP frame containing information specific to a single individual LAN, and for that information not to be propagated further than the extent of that individual LAN, to avoid the meaning of that information being misinterpreted. For example, a TLV containing the auto-negotiation status of an IEEE 802.3™ LAN would be open to misinterpretation if it were to be propagated via a Bridge

onto a second IEEE 802.3 LAN, and would be meaningless if propagated onto a LAN based on a different MAC technology. This is the “LLDP_Multicast address” that was used in IEEE Std 802.1AB-2005. This address was erroneously omitted from the table of S-VLAN component Reserved addresses added to IEEE Std 802.1Q by IEEE Std 802.1ad-2005, but has been added to that table by IEEE Std 802.1aj™-2009 [B1] and is included in subsequent revisions of IEEE Std 802.1Q.

- b) The ***nearest non-TPMR bridge*** group MAC address is an address that no conformant C-VLAN component, S-VLAN component, or MAC Bridge can forward. However, this address is relayed by TPMR components. Therefore, LLDPDUs received on this address represent information about stations that are not separated from the recipient station by any intervening C-VLAN component, S-VLAN component, or MAC Bridge. There may, however, be one or more TPMR components in the path between the originating and receiving stations.

NOTE 2—This address was selected in order to make it possible to communicate information between adjacent bridges and for that communication to be transparent to the presence or absence of TPMRs in the transmission path. This address is primarily intended for use within provider bridged networks.

- c) The ***nearest Customer Bridge*** group MAC address is an address that no conformant C-VLAN component or MAC Bridge forwards. However, this address is relayed by TPMR components and S-VLAN components. Therefore, LLDPDUs received on this address represent information about stations that are not separated from the recipient station by any intervening C-VLAN components (e.g., a C-VLAN Bridge or Provider Edge Bridge). There may, however, be TPMR components and/or S-VLAN components in the path between the originating and receiving stations.

NOTE 3—This address was selected in order to make it possible to communicate information between adjacent Customer Bridges and for that communication to be transparent to the presence or absence of TPMRs or S-VLAN components in the communication path. The scope of this address is the same as that of a customer-to-customer MACSec connection.

Table 7-1—Group MAC addresses used by LLDP

Name	Value	Purpose
<i>Nearest bridge</i>	01-80-C2-00-00-0E	Propagation constrained to a single physical link; stopped by all types of bridge
<i>Nearest non-TPMR bridge</i>	01-80-C2-00-00-03	Propagation constrained by all bridges other than TPMRs; intended for use within provider bridged networks
<i>Nearest Customer Bridge</i>	01-80-C2-00-00-00	Propagation constrained by customer bridges; this gives the same coverage as a customer-customer MACSec connection

NOTE 4—The LSAP or EtherType field is necessary to distinguish between different protocols conveyed in frames with the same group or individual destination address. Prior to revision of this standard to allow multiple address scopes, the destination address 01-80-C2-00-00-00 was only explicitly specified for Spanning Tree Protocol BPDUs. It is therefore possible that some implementations recognize only a frame's destination address before applying priority handling resources intended to guard against BPDUs loss. Since LLDP rate limits LLDPDU transmission, the additional consumption of these resources by LLDPDUs is unlikely to pose a problem for robust implementations.

It is assumed in the foregoing definitions of the scope of these group MAC addresses that an end station attached to an individual LAN is a potential recipient of any of these addresses, and therefore such end stations fall within the scope of these addresses as well as the identified bridge components.

In addition to determining the scope of transmission, the support of more than one destination MAC address allows different sets of TLVs to be supported over the different transmission scopes.

In addition to the prescribed support for standard group MAC addresses shown in Table 7-1, implementations of LLDP may support the following destination addresses for LLDPDUs:

- d) Any group MAC address.
- e) Any individual MAC address.

Support for the use of each of these destination addresses, for both transmission and reception of LLDPDUs, is either mandatory, recommended, permitted, or not permitted, according to the type of system in which LLDP is implemented, as shown in Table 7-2.

Table 7-2—Support for MAC addresses in different systems

Address	C-VLAN Bridge	S-VLAN Bridge	TPMR Bridge	End station
<i>Nearest bridge</i>	Mandatory	Mandatory	Mandatory	Mandatory
<i>Nearest non-TPMR bridge</i>	Mandatory	Mandatory	Not permitted	Recommended
<i>Nearest Customer Bridge</i>	Mandatory	Not permitted	Not permitted	Recommended
<i>Any other group MAC address</i>	Permitted	Permitted	Permitted	Permitted
<i>Any individual MAC address</i>	Permitted	Permitted	Permitted	Permitted

NOTE 5 —Where the implementation supports the use of individual MAC addresses, there is a need for some means whereby the sender can ascertain what address to use, and what scope is associated with that address; how this is achieved is outside the scope of this standard.

NOTE 6—The option of using an individual MAC addresses supports the use of LLDP in IEEE Std 802.11™ [B2] and other wireless LANs, where it is desirable to target specific TLV content at specific logical Ports. In particular, the use of an individual MAC address allows an access point to direct LLDP frames at an individual station with which it is associated.

NOTE 7—If an individual MAC address is used as the destination address by a given LLDP Agent, then that agent would not also receive LLDPDUs on that address; it makes no sense for an LLDP Agent to send LLDP frames to an individual MAC address that it also receives LLDP frames on. Similarly, if an Agent is able to receive LLDPDUs sent to a given individual MAC address, it would not also transmit LLDPDUs to that address. Therefore, Agents associated with individual MAC addresses are either transmitters or receivers of LLDPDUs for a given address, but not both.

NOTE 8—The destination MAC address used by a given LLDP agent defines only the scope of transmission and the intended recipient(s) of the LLDPDUs; it plays no part in protocol identification. In particular, the group MAC addresses identified in Table 7-1 are not used exclusively by LLDP; other protocols that require to use a similar transmission scope are free to use the same addresses.

7.2 Source address

The source address shall be the individual MAC address of the sending station or port.

7.3 EtherType use and encoding

The EtherType used to identify the LLDP protocol shall be the LLDP EtherType specified in Table 7-3.

Table 7-3—LLDP EtherType

Name	Value
LLDP EtherType	88-CC

Where the LLC entity uses an MSAP that is supported by a specific media access control method (for example, IEEE Std 802.3) or a media access control independent entity (for example, IEEE Std 802.1AE) that directly supports encoding of EtherTypes, the LLC entity shall encode the LLDP EtherType as the two octet LLDPDU header in the MSDU of the corresponding MAC service request.

Where the LLC entity uses an MSAP that is supported by a specific media access control method that does not directly support EtherType encoding (for example, IEEE Std 802.11 [B2]), the encoding shall be as specified in IEEE Std 802.1AC.

NOTE—Annex C provides example LLDP transmission frame formats for both direct-encoded and SNAP-encoded LLDP EtherType encoding methods.

7.4 LLDPDU reception

The LLDPDU shall be delivered to the LLDP receive module if, and only if

- a) The destination MAC address is equal to the MAC address associated with the corresponding LLDP Agent; and

NOTE—The destination MAC address can be one of the addresses in Table 7-1, or any other valid MAC address—see 7.1.

- b) The EtherType is equal to the value shown in Table 7-3.

8. LLDPDU and TLV formats

8.1 LLDPDU bit and octet ordering conventions

All LLDPDUs shall contain an integral number of octets. The octets in an LLDPDU are numbered starting from 1 and increasing in the order they are put into the LLDPDU. The bits in an octet are numbered from 1 to 8, where bit 1 is the low-order bit.

When consecutive bits within an octet are used to represent a binary number, the highest 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 TLVs respect these bit and octet ordering conventions.

When the encoding of a field or a number of fields is represented using a diagram

- a) Octets are shown with the lowest numbered octet nearest the left of the page, the octet numbering increasing from left to right.
- b) Within an octet, bits are shown with bit 8 to the left and bit 1 to the right.

8.2 LLDPDU format

The LLDPDU shall contain the following ordered sequence of three mandatory TLVs followed by zero or more optional TLVs as shown in Figure 8-1. An End of LLDPDU TLV may be present as the last TLV in the LLDPDU.

- a) Three mandatory TLVs shall be included at the beginning of each LLDPDU and shall be in the order shown.
 - 1) Chassis ID TLV
 - 2) Port ID TLV
 - 3) Time To Live TLV
- b) Optional TLVs as selected by network management (may be inserted in any order).

NOTE 1—"Optional" in the sense that they are not required for LLDP operation; however, their presence could be required by other system elements that use LLDP.

- c) If the End Of LLDPDU TLV is present, it shall be the last TLV in the LLDPDU.

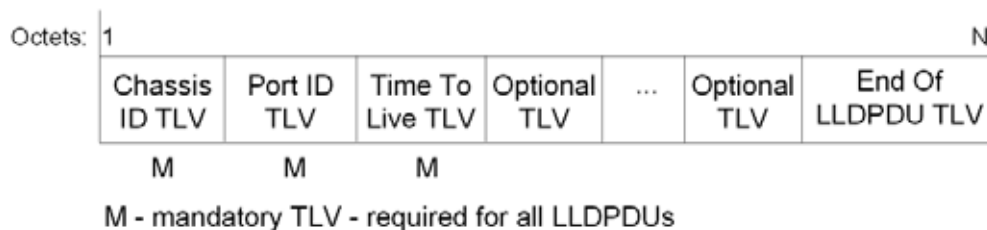


Figure 8-1—LLDPDU format

The maximum length of the LLDPDU shall be the maximum information field length allowed by the particular transmission rate and protocol. In IEEE 802.3 MACs, for example, the maximum LLDPDU length is the maximum data field length for the basic, untagged MAC frame (1500 octets).

NOTE 2—There is no defined minimum length of an LLDPDU, other than that implied by the requirement that conformant implementations support the mandatory TLVs specified in Table 8-1.

8.3 TLV categories

The TLVs are grouped into two general categories as follows:

- a) A set of TLVs that are considered to be basic to the management of network stations and that are a required capability of all LLDP implementations. Each TLV in this category is identified by a unique TLV type value that indicates the particular kind of information contained in the TLV.
- b) Organizationally specific extension sets of TLVs that are defined by standards groups such as IEEE 802.1 and IEEE 802.3 and others to enhance management of network stations that are operating with particular media and/or protocols.
 - 1) TLVs in this category are identified by a common TLV type value that indicates the TLV as belonging to the set of Organizationally Specific TLVs.
 - 2) Each organization is identified by its organizationally unique identifier (OUI).
 - 3) Organizationally Specific TLV subtype values indicate the kind of information contained in the TLV.

The basic TLV format and general field definition rules are defined in 8.4. Specific definitions and usage requirements for all basic management set TLVs are defined in 8.5. Usage rules/requirements that pertain to each individual basic TLV are contained in the definition for that particular TLV.

The basic format and the field definition/general usage rules/restrictions for Organizationally Specific TLVs are defined in 8.6. Usage rules/requirements that pertain to each individual basic TLV are contained in the definition for that particular TLV.

8.4 Basic TLV format

Figure 8-2 shows the basic TLV format.

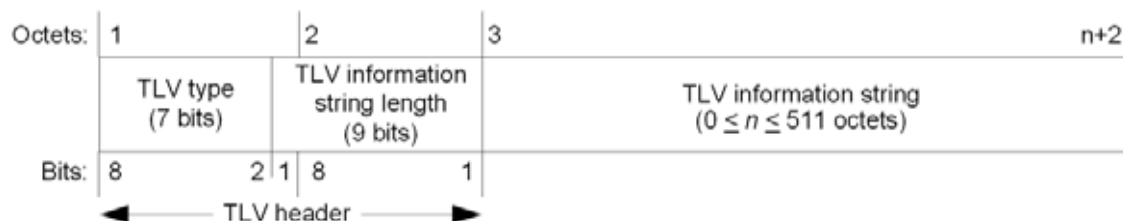


Figure 8-2—Basic TLV format

The TLV type field occupies the seven most significant bits of the first octet of the TLV format. The least significant bit in the first octet of the TLV format is the most significant bit of the TLV information string length field.

8.4.1 TLV type

The TLV type field is seven bits long and identifies the specific TLV. Two classes of TLVs are defined:

- a) Mandatory TLVs that shall be included in all LLDPDUs.
- b) Optional TLVs that may be included in LLDPDUs.

Table 8-1 lists the currently defined TLVs, their identifying TLV type values, and whether they are mandatory or optional for inclusion in any particular LLDPDU.

Table 8-1—TLV type values

TLV type ^a	TLV name	Usage in LLDPDU	Reference
0	End Of LLDPDU	Optional	8.5.1
1	Chassis ID	Mandatory	8.5.2
2	Port ID	Mandatory	8.5.3
3	Time To Live	Mandatory	8.5.4
4	Port Description	Optional	8.5.5
5	System Name	Optional	8.5.6
6	System Description	Optional	8.5.7
7	System Capabilities	Optional	8.5.8
8	Management Address	Optional	8.5.9
9–126	Reserved for future standardization	—	—
127	Organizationally Specific TLVs	Optional	—

^aTLVs with type values 0–8 are members of the basic management set.

8.4.2 TLV information string length

The TLV information string length field shall contain the length of the information string, in octets.

8.4.3 TLV information string

The information string

- a) May be fixed or variable length.
- b) May include one or more information fields with associated subtype identifiers and field length designators as in, for example, the Management Address TLV (see 8.5.9).
- c) May contain either binary or alpha-numeric information that is instance specific for the particular TLV type and/or subtype.
 - 1) Bit 1 in binary bit maps shall be the least significant bit in the field.
 - 2) The first octet of an alpha-numeric field shall be the most significant octet.
 - 3) Alpha-numeric information shall be encoded in UTF-8 [IETF RFC 3629].

8.5 Basic management TLV set formats and definitions

8.5.1 End Of LLDPDU TLV

The End Of LLDPDU TLV is a 2-octet, all-zero TLV that is used to mark the end of the TLV sequence in LLDPDUs. The format for this TLV is shown in Figure 8-3.

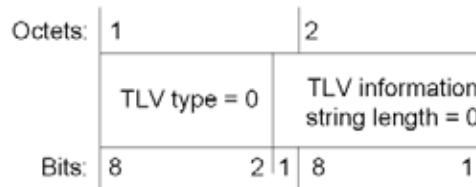


Figure 8-3—End Of LLDPDU TLV format

NOTE—Some IEEE 802 MACs require the data field in a frame to contain a minimum number of octets. For example, the IEEE 802.3 MAC adds pad octets to complete a minimum length data field if the user's data is less than the minimum required length. Since pad octets are unspecified, an End Of LLDPDU TLV can be used to prevent non-zero pad octets from being interpreted by the receiving LLDP agent as another TLV.

8.5.2 Chassis ID TLV

The Chassis ID TLV is a mandatory TLV that identifies the chassis containing the IEEE 802 LAN station associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field. Each LLDPDU shall contain one, and only one, Chassis ID TLV and the chassis ID field value shall remain constant for all LLDPDUs while the MAC status parameter for the Port remains operational.

The Chassis ID TLV shall be the first TLV in the LLDPDU. Its format is shown in Figure 8-4.

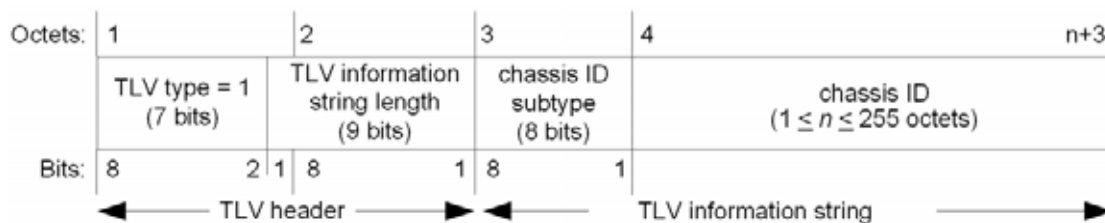


Figure 8-4—Chassis ID TLV format

8.5.2.1 TLV information string length

The TLV information string length field shall indicate the exact length, in octets, of the (chassis ID subtype + chassis ID) fields.

8.5.2.2 chassis ID subtype

The chassis ID subtype field shall contain an integer value indicating the basis for the chassis ID entity that is listed in the chassis ID field. The defined chassis ID subtypes and their preferred use order are listed in Table 8-2.