



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

**Part 15.4: Wireless Medium Access Control
(MAC) and Physical Layer (PHY)
Specifications for Low-Rate Wireless
Personal Area Networks (WPANs)**

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997, USA
8 September 2006

IEEE Std 802.15.4™-2006
(Revision of
IEEE Std 802.15.4-2003)

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

**Part 15.4: Wireless Medium Access Control
(MAC) and Physical Layer (PHY)
Specifications for Low-Rate Wireless
Personal Area Networks (WPANs)**

Sponsor

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

Approved 7 June 2006

IEEE-SA Standards Board

Abstract: IEEE Std 802.15.4-2003 defined the protocol and compatible interconnection for data communication devices using low-data-rate, low-power, and low-complexity short-range radio frequency (RF) transmissions in a wireless personal area network (WPAN). This revision extends the market applicability of IEEE Std 802.15.4, removes ambiguities in the standard, and makes improvements revealed by implementations of IEEE Std 802.15.4-2003.

Keywords: ad hoc network, low data rate, low power, LR-WPAN, mobility, PAN, personal area network, radio frequency, RF, short range, wireless, wireless personal area network, WPAN

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

Copyright © 2006 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 8 September 2006. Printed in the United States of America.

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

Print: ISBN 0-7381-4996-9 SH95552
PDF: ISBN 0-7381-4997-7 SS95552

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

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

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

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

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

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

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

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

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

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

Introduction

This introduction is not part of IEEE Std 802.15.4-2006, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).

This standard defines the protocol and interconnection of devices via radio communication in a personal area network (PAN). The standard uses carrier sense multiple access with collision avoidance (CSMA-CA) medium access mechanism and supports star as well as peer-to-peer topologies. The media access is contention based; however, using the optional superframe structure, time slots can be allocated by the PAN coordinator to devices with time critical data. Connectivity to higher performance networks is provided through a PAN coordinator.

This revision was initiated to incorporate additional features and enhancements as well as some simplifications to the 2003 edition of this standard. The standard now includes two optional physical layers (PHYs) yielding higher data rates in the lower frequency bands and, therefore, specifies the following four PHYs:

- An 868/915 MHz direct sequence spread spectrum (DSSS) PHY employing binary phase-shift keying (BPSK) modulation
- An 868/915 MHz DSSS PHY employing offset quadrature phase-shift keying (O-QPSK) modulation
- An 868/915 MHz parallel sequence spread spectrum (PSSS) PHY employing BPSK and amplitude shift keying (ASK) modulation
- A 2450 MHz DSSS PHY employing O-QPSK modulation

The 868/915 MHz PHYs support over-the-air data rates of 20 kb/s, 40 kb/s, and optionally 100kb/s and 250kb/s. The 2450 MHz PHY supports an over-the-air data rate of 250 kb/s. The PHY chosen depends on local regulations and user preference.

This revision also incorporates the following additions and enhancements to the 2003 edition:

- Adds support for a shared time base through the addition of a data time stamping mechanism
- Adds extensions of the 2.4GHz derivative modulation yielding higher data rates at the lower frequency bands
- Incorporates a mechanism for communicating the revision level on a frame-by-frame basis
- Adds support for beacon scheduling
- Allows synchronization of broadcast messages in beacon-enabled PANs
- Improves usage of security suite

Also, this revision incorporates the following changes and simplifications:

- Makes GTS support optional
- Removes restrictions for manually enabling the receiver
- Simplifies passive and active scan procedures
- Allows for more flexibility in the CSMA-CA algorithm
- Reduces association time in nonbeacon networks

This revision is backward-compatible to the 2003 edition; in other words, devices conforming to this standard are capable of joining and functioning in a PAN composed of devices conforming to IEEE Std 802.15.4-2003.

Notice to users

Errata

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

Interpretations

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

Patents

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

Participants

At the time the draft of this standard was sent to sponsor ballot, the IEEE P802.15 Working Group had the following voting members:

Robert F. Heile, *Chair*
James D. Allen, *Vice Chair*
Patrick W. Kinney, *Assistant Vice Chair*
James P. K. Gilb, *Editor-in-Chief*
Patrick W. Kinney, *Secretary*
Michael D. McInnis, *Assistant Secretary and Editor*

John R. Barr, *Task Group 3b Chair*
Reed Fisher, *Task Group 3c Chair*
Patrick W. Kinney, *Task Group 4a Chair*
Myung Lee, *Task Group 5 Chair*

Robert D. Poor, *Task Group 4b Chair*
Marco Naeve, *Task Group 4b Vice Chair*
Monique B. Brown, *Task Group 4b Editor-in-Chief*
Eric T. Gnoske, *Task Group 4b Secretary*

Philip E. Beecher, *MAC Contributing Editor*
Monique B. Brown, *MAC Technical Editor*
Edgar H. Callaway, Jr., *MAC Contributing Editor*
Francois Chin, *PHY Contributing Editor*
Robert C. Cragie, *MAC/Security Contributing Editor*
Paul Gorday, *PHY Contributing Editor*
James P. K. Gilb, *Draft D3 Editor-in-Chief*
Øyvind Janbu, *MAC/PHY/Security Contributing Editor*
Marco Naeve, *General Description/PICS Editor, MAC Contributing Editor*
Clinton C. Powell, *PHY Technical Editor*
Joseph Reddy, *Security Contributing Editor*

Zachary Smith, *MAC Contributing Editor*
René Struik, *Security Contributing Editor*
Andreas C. Wolf, *PHY Contributing Editor*

Roberto Aiello	Tzyy Hong Jiang	Raad Raad
Richard Alfvén	David Julian	Pekka Ranta
Mikio Aoki	Jeyhan Karaoguz	Dani Raphaeli
Takashi Arita	Michael Kelly	Gregg Rasor
Larry Arnett	Stuart Kerry	Charles Razzell
Arthur Astrin	Jae-Hyon Kim	Ivan Reede
Yasaman Bahreini	Jaeyoung Kim	Yuko Rikuta
Jay Bain	Jinkyong Kim	Terry Robar
Alan Berkema	Yongsuk Kim	Glyn Roberts
Bruce Bosco	Kursat Kimyacioglu	Richard Roberts
Mark Bowles	Matthias Kindler	Benjamin Rolfe
Charles Brabenec	Guenter Kleindl	Philippe Rouzet
David Brenner	Ryuji Kohno	Chandos Rypinski
Vern Brethour	Mike Krell	Ali Sadri
Ronald Brown	Yasushi Kudo	Saeid Safavi
Bill Carney	Akiomi Kunisa	Zafer Sahinoglu
Kuor-Hsin Chang	Yuzo Kuramochi	Tomoki Saito
Jonathon Cheah	Jiun-You Lai	Syed Saleem
Kwan-Wu Chin	Ismail Lakkis	Kamran Sayrafian
Sarm-Goo Cho	John Lampe	Jean Schwoerer
Sungsoo Choi	Kyung Kuk Lee	Erik Schylander
Yun Choi	Wooyong Lee	Alireza Seyedi
Chun-Ting Chou	David Leeper	Sanjeev Sharma
Manoj Choudhary	Huan-Bang Li	Siddharth Shetty
Celestino Corral	Haixiang Liang	John Shi
Joe Decuir	Ian Macnamara	Shusaku Shimada
Javier Del Prado Pavon	Akira Maeki	Yuichi Shiraki
Kai Dombrowski	Patricia Martigne	Gadi Shor
Stefan Drude	Abbie Mathew	William Shvodian
Amal Ekbal	Taisuke Matsumoto	Thomas Siep
Jason Ellis	Gustaf Max	Michael Sim
Shahriar Emami	Michael McLaughlin	Kazimierz Siwiak
Paul Everest	Charlie Mellone	V. Somayazulu
Mark W. Fidler	Klaus Meyer	Amjad Soomro
Kris Fleming	Samuel Mo	Carl Stevenson
Amir Freund	Andreas Molisch	Kazuaki Takahashi
Camillo Gentile	Mark Moore	Kenichi Takizawa
Ian Gifford	Ken Naganuma	Teik-Kheong Tan
Sung-Wook Goh	Yves-Paul Nakache	Mike Tanahashi
Sorin Goldenberg	Hiroyuki Nakase	Yasushi Tanaka
Vivek Gupta	Saishankar Nandagopalan	James Taylor
Rainer Hach	Chiu Ngo	Arnaud Tonnerre
Robert Hall	Erwin Noble	Ichihiko Toyoda
Shinsuke Hara	John O'Connor	Jerry Upton
Jeff Harris	Knut Odman	Bart Van Poucke
Allen Heberling	Hiroyo Ogawa	Chris Weber
Eric Heinze	Yasuyuki Okuma	Matthew Welborn
Barry Herold	Philip Orlik	Magnus Wiklund
Keisuke Higuchi	Laurent Ouvry	Gerald Wineinger
Jin-Meng Ho	John Pardee	Patrick Worfolk
Patrick Houghton	Nirmalendu Patra	Tracy Wright
Robert Huang	Dave Patton	Hirohisa Yamaguchi
Tian-Wei Huang	Xiaoming Peng	Kamyä Yekeh Yazdandoost
Hideto Ikeda	Tony Pollock	Su-Khiong Yong
Tetsushi Ikegami	Vidyasagar Premkumar	Zhan Yu
Adrian Jennings	Yihong Qi	Serdar Yurdakul
Ho-In Jeon		Mahmoud Zadeh
		Bin Zhen

Major contributions were received from the following individuals:

Jon Adams	Colin Lanzl	Huai-Rong Shao
Helmut P. Adamski	Myung Lee	Mark Shea
Jonathan Avey	Zhongding Lei	Stephen J. Shellhammer
Jon Beniston	Liang Li	Mark A. Tillinghast
Bernd Grohmann	Yong Liu	Johannes Van Leeuwen
José A. Gutierrez	Frederick Martin	Richard Wilson
Jesper Holm	Frank Poegel	Ping Xiong
ZhiJian Hu	Matthias Scheide	Bing Xu
Phil A. Jamieson	D. C. Seward	ChenYang Yang
Yuen-Sam Kwok		Chunhui Zhu

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

Helmut P. Adamski	Patrick S. Gonia	Michael S. Newman
Toru Aihara	Ron K. Greenthaler	Paul Nikolich
Richard L. Alfvén	Bernd Grohmann	Erwin R. Noble
Butch Anton	Randall C. Groves	Richard H. Noens
Mikio Aoki	Pradeep Gupta	Satoshi Obara
Lee R. Armstrong	José A. Gutierrez	Knut T. Odman
John R. Barr	C. G. Guy	Chris L. Osterloh
Hugh Barrass	Siamack Haghighi	Satoshi Oyama
Philip E. Beecher	Karl F. Heubaum	Subburajan Ponnuswamy
Alexei Beliaev	Dennis Horwitz	Robert D. Poor
Gennaro Boggia	Arshad Hussain	Clinton C. Powell
Monique B. Brown	Atsushi Ito	Vikram Punj
Matthew K. Burnburg	Peeya Iwagoshi	Maurice M. Reintjes
William A. Byrd	Raj Jain	Maximilian Riegel
Sean S. Cai	David V. James	Robert A. Robinson
Edgar H. Callaway, Jr.	Phil A. Jamieson	Frank H. Rocchio
James T. Carlo	Øyvind Janbu	Jon W. Rosdahl
Juan C. Carreon	Bobby Jose	John C. Sargent III
Jon S. Chambers	Efthymios G. Karabetsos	Stephen J. Shellhammer
YiMing Chen	Stuart J. Kerry	Nicoll B. Shepherd
Danila Chernetsov	Brian G. Kiernan	Shusaku Shimada
Elizabeth Chesnutt	Yongbum Kim	William M. Shvodian
Aik Chindapol	Patrick W. Kinney	Matthew L. Smith
Keith Chow	Jeremy A. Landt	Amjad A. Soomro
Ryon K. Coleman	Solomon Lee	Thomas E. Starai
Tommy P. Cooper	Charles A. Lennon, Jr.	René Struik
Robert C. Cragie	Daniel G. Levesque	Mark A. Sturza
Javier Del-Prado-Pavon	JanRay Liao	Norman L. Swenson
Russell S. Dietz	Chiwoo Lim	David W. Thompson
Thomas J. Dineen	WeiTing Lin	Mark A. Tillinghast
Carlo Donati	Daniel M. Lubar	Svein A. Tunheim
Sourav K. Dutta	William Lumpkins	MarkRene Uchida
Paul S. Eastman	G. L. Luri	Scott A. Valcourt
Andre F. Fournier	Nathaniel J. Melby	Johannes Van Leeuwen
Avraham Freedman	Gary L. Michel	Amanda E. Walker
Ignacio Marin Garcia	William J. Mitchell	Stanley S. Wang
Devon L. Gayle	Apurva N. Mody	HungYu Wei
Theodore Georgantas	John S. Monson	Andreas C. Wolf
Ian C. Gifford	Said Moridi	Derek T. Woo
James P. K. Gilb	Ronald G. Murias	Eric V. Woods
Eric T. Gnoske	Marco Naeve	Forrest D. Wright
Nikhil Goel	Madihally J. Narasimha	Oren Yuen
Sergiu R. Goma	Nabil Nasser	Surong Zeng

When the IEEE-SA Standards Board approved this standard on 8 June 2006, it had the following membership:

Steve M. Mills, *Chair*
Richard H. Hulett, *Vice Chair*
Don Wright, *Past Chair*
Judith Gorman, *Secretary*

Mark D. Bowman
Dennis B. Brophy
Joseph Bruder
Richard Cox
Bob Davis
Julian Forster*
Joanna N. Guenin
Mark S. Halpin
Raymond Hapeman

William B. Hopf
Lowell G. Johnson
Herman Koch
Joseph L. Koepfinger*
David J. Law
Daleep C. Mohla
Paul Nikolich

T. W. Olsen
Glenn Parsons
Ronald C. Petersen
Gary S. Robinson
Frank Stone
Malcolm V. Thaden
Richard L. Townsend
Joe D. Watson
Howard L. Wolfman

*Member Emeritus

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

Satish K. Aggarwal, *NRC Representative*
Richard DeBlasio, *DOE Representative*
Alan H. Cookson, *NIST Representative*

Don Messina
IEEE Standards Program Manager, Document Development

Michael Kipness
IEEE Standards Program Manager, Technical Program Development

Contents

1.	Overview.....	1
1.1	General.....	1
1.2	Scope.....	1
1.3	Purpose.....	2
2.	Normative references.....	3
3.	Definitions	5
4.	Acronyms and abbreviations	9
5.	General description	13
5.1	Introduction.....	13
5.2	Components of the IEEE 802.15.4 WPAN.....	13
5.3	Network topologies.....	14
5.3.1	Star network formation	14
5.3.2	Peer-to-peer network formation.....	15
5.4	Architecture	15
5.4.1	Physical layer (PHY)	17
5.4.2	MAC sublayer.....	17
5.5	Functional overview	17
5.5.1	Superframe structure.....	17
5.5.2	Data transfer model.....	18
5.5.2.1	Data transfer to a coordinator	19
5.5.2.2	Data transfer from a coordinator.....	20
5.5.2.3	Peer-to-peer data transfers	21
5.5.3	Frame structure	21
5.5.3.1	Beacon frame	21
5.5.3.2	Data frame.....	22
5.5.3.3	Acknowledgment frame.....	22
5.5.3.4	MAC command frame	23
5.5.4	Improving probability of successful delivery	23
5.5.4.1	CSMA-CA mechanism	23
5.5.4.2	Frame acknowledgment.....	24
5.5.4.3	Data verification	24
5.5.5	Power consumption considerations	24
5.5.6	Security	24
5.6	Concept of primitives.....	25
6.	PHY specification	27
6.1	General requirements and definitions	27
6.1.1	Operating frequency range.....	27
6.1.2	Channel assignments.....	28
6.1.2.1	Channel numbering.....	29
6.1.2.2	Channel pages	29
6.1.3	Minimum long interframe spacing (LIFS) and short interframe spacing (SIFS) periods	30

6.1.4	RF power measurement	31
6.1.5	Transmit power	31
6.1.6	Out-of-band spurious emission	31
6.1.7	Receiver sensitivity definitions	31
6.2	PHY service specifications	31
6.2.1	PHY data service	32
6.2.1.1	PD-DATA.request	32
6.2.1.2	PD-DATA.confirm	33
6.2.1.3	PD-DATA.indication	34
6.2.2	PHY management service	34
6.2.2.1	PLME-CCA.request	35
6.2.2.2	PLME-CCA.confirm	35
6.2.2.3	PLME-ED.request	36
6.2.2.4	PLME-ED.confirm	36
6.2.2.5	PLME-GET.request	37
6.2.2.6	PLME-GET.confirm	38
6.2.2.7	PLME-SET-TRX-STATE.request	39
6.2.2.8	PLME-SET-TRX-STATE.confirm	40
6.2.2.9	PLME-SET.request	40
6.2.2.10	PLME-SET.confirm	41
6.2.3	PHY enumerations description	42
6.3	PPDU format	43
6.3.1	Preamble field	43
6.3.2	SFD field	44
6.3.3	Frame Length field	45
6.3.4	PSDU field	45
6.4	PHY constants and PIB attributes	45
6.4.1	PHY constants	45
6.4.2	PHY PIB attributes	45
6.5	2450 MHz PHY specifications	47
6.5.1	Data rate	47
6.5.2	Modulation and spreading	47
6.5.2.1	Reference modulator diagram	47
6.5.2.2	Bit-to-symbol mapping	47
6.5.2.3	Symbol-to-chip mapping	47
6.5.2.4	O-QPSK modulation	48
6.5.2.5	Pulse shape	49
6.5.2.6	Chip transmission order	49
6.5.3	2450 MHz band radio specification	49
6.5.3.1	Transmit power spectral density (PSD) mask	49
6.5.3.2	Symbol rate	49
6.5.3.3	Receiver sensitivity	49
6.5.3.4	Receiver jamming resistance	50
6.6	868/915 MHz band binary phase-shift keying (BPSK) PHY specifications	50
6.6.1	868/915 MHz band data rates	50
6.6.2	Modulation and spreading	50
6.6.2.1	Reference modulator diagram	50
6.6.2.2	Differential encoding	51
6.6.2.3	Bit-to-chip mapping	51
6.6.2.4	BPSK modulation	51
6.6.3	868/915 MHz band radio specification	52
6.6.3.1	Operating frequency range	52
6.6.3.2	915 MHz band transmit PSD mask	52
6.6.3.3	Symbol rate	52

6.6.3.4	Receiver sensitivity	52
6.6.3.5	Receiver jamming resistance	52
6.7	868/915 MHz band (optional) amplitude shift keying (ASK) PHY specifications	53
6.7.1	868/915 MHz band data rates	53
6.7.2	Modulation and spreading	53
6.7.2.1	Reference modulator diagram	53
6.7.2.2	Bit-to-symbol mapping	54
6.7.2.3	Symbol-to-chip mapping	54
6.7.2.4	ASK modulation	55
6.7.3	868/915 MHz band radio specification for the ASK PHY	57
6.7.3.1	Operating frequency range	57
6.7.3.2	915 MHz band transmit PSD mask	57
6.7.3.3	Symbol rate	57
6.7.3.4	Receiver sensitivity	57
6.7.3.5	Receiver jamming resistance	57
6.7.4	SHR for ASK PHY	58
6.7.4.1	Preamble for ASK PHY	58
6.7.4.2	SFD for ASK PHY	58
6.7.4.3	Example of PSSS encoding	58
6.8	868/915 MHz band (optional) O-QPSK PHY specifications	60
6.8.1	868/915 MHz band data rates	60
6.8.2	Modulation and spreading	60
6.8.2.1	Reference modulator diagram	60
6.8.2.2	Bit-to-symbol mapping	60
6.8.2.3	Symbol-to-chip mapping	60
6.8.2.4	O-QPSK modulation	61
6.8.2.5	Pulse shape	62
6.8.2.6	Chip transmission order	62
6.8.3	868/915 MHz band radio specification	62
6.8.3.1	Operating frequency range	62
6.8.3.2	Transmit PSD mask	62
6.8.3.3	Symbol rate	63
6.8.3.4	Receiver sensitivity	63
6.8.3.5	Receiver jamming resistance	63
6.9	General radio specifications	63
6.9.1	TX-to-RX turnaround time	63
6.9.2	RX-to-TX turnaround time	64
6.9.3	Error-vector magnitude (EVM) definition	64
6.9.4	Transmit center frequency tolerance	65
6.9.5	Transmit power	65
6.9.6	Receiver maximum input level of desired signal	65
6.9.7	Receiver ED	65
6.9.8	Link quality indicator (LQI)	65
6.9.9	Clear channel assessment (CCA)	66
7.	MAC sublayer specification	67
7.1	MAC sublayer service specification	67
7.1.1	MAC data service	68
7.1.1.1	MCPS-DATA.request	68
7.1.1.2	MCPS-DATA.confirm	71
7.1.1.3	MCPS-DATA.indication	72
7.1.1.4	MCPS-PURGE.request	75
7.1.1.5	MCPS-PURGE.confirm	75

7.1.1.6	Data service message sequence chart	76
7.1.2	MAC management service.....	76
7.1.3	Association primitives	77
7.1.3.1	MLME-ASSOCIATE.request.....	78
7.1.3.2	MLME-ASSOCIATE.indication	80
7.1.3.3	MLME-ASSOCIATE.response	81
7.1.3.4	MLME-ASSOCIATE.confirm	83
7.1.3.5	Association message sequence charts	85
7.1.4	Disassociation primitives	86
7.1.4.1	MLME-DISASSOCIATE.request	86
7.1.4.2	MLME-DISASSOCIATE.indication.....	89
7.1.4.3	MLME-DISASSOCIATE.confirm	90
7.1.4.4	Disassociation message sequence charts	91
7.1.5	Beacon notification primitive	92
7.1.5.1	MLME-BEACON-NOTIFY.indication.....	92
7.1.6	Primitives for reading PIB attributes	94
7.1.6.1	MLME-GET.request.....	95
7.1.6.2	MLME-GET.confirm.....	96
7.1.7	GTS management primitives	97
7.1.7.1	MLME-GTS.request	97
7.1.7.2	MLME-GTS.confirm	99
7.1.7.3	MLME-GTS.indication.....	100
7.1.7.4	GTS management message sequence charts.....	102
7.1.8	Primitives for orphan notification.....	103
7.1.8.1	MLME-ORPHAN.indication.....	103
7.1.8.2	MLME-ORPHAN.response.....	104
7.1.8.3	Orphan notification message sequence chart.....	106
7.1.9	Primitives for resetting the MAC sublayer	106
7.1.9.1	MLME-RESET.request	106
7.1.9.2	MLME-RESET.confirm	107
7.1.10	Primitives for specifying the receiver enable time	108
7.1.10.1	MLME-RX-ENABLE.request	108
7.1.10.2	MLME-RX-ENABLE.confirm.....	110
7.1.10.3	Message sequence chart for changing the state of the receiver	110
7.1.11	Primitives for channel scanning.....	111
7.1.11.1	MLME-SCAN.request.....	111
7.1.11.2	MLME-SCAN.confirm.....	114
7.1.11.3	Channel scan message sequence charts	116
7.1.12	Communication status primitive	116
7.1.12.1	MLME-COMM-STATUS.indication	116
7.1.13	Primitives for writing PIB attributes.....	119
7.1.13.1	MLME-SET.request	119
7.1.13.2	MLME-SET.confirm	121
7.1.14	Primitives for updating the superframe configuration.....	122
7.1.14.1	MLME-START.request.....	122
7.1.14.2	MLME-START.confirm.....	126
7.1.14.3	Message sequence chart for updating the superframe configuration.....	126
7.1.15	Primitives for synchronizing with a coordinator	127
7.1.15.1	MLME-SYNC.request.....	127
7.1.15.2	MLME-SYNC-LOSS.indication	128
7.1.15.3	Message sequence chart for synchronizing with a coordinator	131
7.1.16	Primitives for requesting data from a coordinator	131
7.1.16.1	MLME-POLL.request.....	132
7.1.16.2	MLME-POLL.confirm	133

7.1.16.3	Message sequence chart for requesting data from a coordinator	134
7.1.17	MAC enumeration description.....	135
7.2	MAC frame formats.....	137
7.2.1	General MAC frame format.....	138
7.2.1.1	Frame Control field.....	138
7.2.1.2	Sequence Number field.....	140
7.2.1.3	Destination PAN Identifier field.....	140
7.2.1.4	Destination Address field.....	140
7.2.1.5	Source PAN Identifier field	141
7.2.1.6	Source Address field.....	141
7.2.1.7	Auxiliary Security Header field.....	141
7.2.1.8	Frame Payload field.....	141
7.2.1.9	FCS field.....	141
7.2.2	Format of individual frame types.....	142
7.2.2.1	Beacon frame format	142
7.2.2.2	Data frame format.....	146
7.2.2.3	Acknowledgment frame format.....	147
7.2.2.4	MAC command frame format.....	147
7.2.3	Frame compatibility	148
7.3	MAC command frames.....	149
7.3.1	Association request command	150
7.3.1.1	MHR fields	150
7.3.1.2	Capability Information field	150
7.3.2	Association response command.....	151
7.3.2.1	MHR fields	151
7.3.2.2	Short Address field	152
7.3.2.3	Association Status field	152
7.3.3	Disassociation notification command.....	152
7.3.3.1	MHR fields	153
7.3.3.2	Disassociation Reason field.....	153
7.3.4	Data request command.....	153
7.3.5	PAN ID conflict notification command.....	154
7.3.6	Orphan notification command	155
7.3.7	Beacon request command	156
7.3.8	Coordinator realignment command	156
7.3.8.1	MHR fields	157
7.3.8.2	PAN Identifier field	157
7.3.8.3	Coordinator Short Address field.....	157
7.3.8.4	Logical Channel field.....	157
7.3.8.5	Short Address field	157
7.3.8.6	Channel Page field.....	157
7.3.9	GTS request command.....	158
7.3.9.1	MHR fields	158
7.3.9.2	GTS Characteristics field.....	158
7.4	MAC constants and PIB attributes.....	159
7.4.1	MAC constants	159
7.4.2	MAC PIB attributes	160
7.5	MAC functional description	166
7.5.1	Channel access.....	167
7.5.1.1	Superframe structure.....	167
7.5.1.2	Incoming and outgoing superframe timing.....	169
7.5.1.3	Interframe spacing (IFS).....	169
7.5.1.4	CSMA-CA algorithm.....	170
7.5.2	Starting and maintaining PANs	172

7.5.2.1	Scanning through channels	172
7.5.2.2	PAN identifier conflict resolution.....	176
7.5.2.3	Starting and realigning a PAN	177
7.5.2.4	Beacon generation.....	178
7.5.2.5	Device discovery.....	179
7.5.3	Association and disassociation	179
7.5.3.1	Association.....	179
7.5.3.2	Disassociation	181
7.5.4	Synchronization	182
7.5.4.1	Synchronization with beacons	182
7.5.4.2	Synchronization without beacons	183
7.5.4.3	Orphaned device realignment	183
7.5.5	Transaction handling.....	183
7.5.6	Transmission, reception, and acknowledgment.....	185
7.5.6.1	Transmission	185
7.5.6.2	Reception and rejection	186
7.5.6.3	Extracting pending data from a coordinator	187
7.5.6.4	Use of acknowledgments and retransmissions	189
7.5.6.5	Promiscuous mode	190
7.5.6.6	Transmission scenarios	191
7.5.7	GTS allocation and management.....	192
7.5.7.1	CAP maintenance	193
7.5.7.2	GTS allocation	193
7.5.7.3	GTS usage.....	194
7.5.7.4	GTS deallocation	195
7.5.7.5	GTS reallocation.....	196
7.5.7.6	GTS expiration.....	197
7.5.8	Frame security.....	197
7.5.8.1	Security-related MAC PIB attributes.....	197
7.5.8.2	Functional description.....	199
7.6	Security suite specifications.....	206
7.6.1	PIB security material	206
7.6.2	Auxiliary security header.....	210
7.6.2.1	Integer and octet representation.....	210
7.6.2.2	Security Control field.....	210
7.6.2.3	Frame Counter field.....	212
7.6.2.4	Key Identifier field.....	212
7.6.3	Security operations	213
7.6.3.1	Integer and octet representation.....	213
7.6.3.2	CCM* Nonce	213
7.6.3.3	CCM* prerequisites	213
7.6.3.4	CCM* transformation data representation.....	214
7.6.3.5	CCM* inverse transformation data representation	215
7.7	Message sequence charts illustrating MAC-PHY interaction	216
Annex A (normative)	Service-specific convergence sublayer (SSCS).....	227
A.1	IEEE 802.2 convergence sublayer.....	227
A.1.1	MA-UNITDATA.request	227
A.1.1.1	Semantics of the service primitive.....	227
A.1.1.2	Appropriate usage	228
A.1.1.3	Effect on receipt.....	228
A.1.2	MA-UNITDATA.indication	228
A.1.2.1	Semantics of the service primitive.....	228

A.1.2.2	When generated	228
A.1.2.3	Appropriate usage	228
A.1.3	MA-UNITDATA-STATUS.indication.....	229
A.1.3.1	Semantics of the service primitive.....	229
A.1.3.2	When generated	229
A.1.3.3	Appropriate usage	229
Annex B (normative)	CCM* mode of operation	231
B.1	Introduction.....	231
B.2	Notation and representation	231
B.2.1	Strings and string operations.....	231
B.2.2	Integers, octets, and their representation	231
B.3	Symmetric-key cryptographic building blocks.....	231
B.3.1	Block cipher	231
B.3.2	Mode of operation.....	232
B.4	Specification of generic CCM* mode of operation	232
B.4.1	CCM* mode encryption and authentication transformation.....	232
B.4.1.1	Input transformation	233
B.4.1.2	Authentication transformation	233
B.4.1.3	Encryption transformation	234
B.4.2	CCM* mode decryption and authentication checking transformation	234
B.4.2.1	Decryption transformation	235
B.4.2.2	Authentication checking transformation.....	235
B.4.3	Restrictions	235
Annex C (informative)	Test vectors for cryptographic building blocks.....	237
C.1	AES block cipher	237
C.2	Mode of operation.....	237
C.2.1	MAC beacon frame.....	237
C.2.1.1	Description.....	237
C.2.1.2	CCM* mode encryption and authentication transformation.....	238
C.2.1.3	CCM* mode decryption and authentication checking transformation	240
C.2.2	MAC data frame	241
C.2.2.1	Description.....	241
C.2.2.2	CCM* mode encryption and authentication transformation.....	241
C.2.2.3	CCM* mode decryption and authentication checking transformation	243
C.2.3	MAC command frame	245
C.2.3.1	Description.....	245
C.2.3.2	CCM* mode encryption and authentication transformation.....	245
C.2.3.3	CCM* mode decryption and authentication checking transformation	247
Annex D (normative)	Protocol implementation conformance statement (PICS) proforma	251
D.1	Introduction.....	251
D.1.1	Scope.....	251
D.1.2	Purpose.....	251
D.2	Abbreviations and special symbols.....	251
D.3	Instructions for completing the PICS proforma.....	252
D.4	Identification of the implementation.....	252
D.5	Identification of the protocol	253
D.6	Global statement of conformance	253
D.7	PICS proforma tables.....	254

D.7.1	Major roles for devices compliant with IEEE Std 802.15.4-2006	254
D.7.2	Major capabilities for the PHY	255
D.7.2.1	PHY functions	255
D.7.2.2	PHY packet	255
D.7.2.3	Radio frequency (RF)	256
D.7.3	Major capabilities for the MAC sublayer	256
D.7.3.1	MAC sublayer functions	256
D.7.3.2	MAC frames	258
Annex E (informative)	Coexistence with other IEEE standards and proposed standards	261
E.1	Introduction	261
E.2	Standards and proposed standards characterized for coexistence	261
E.3	General coexistence issues	261
E.3.1	Clear channel assessment (CCA)	262
E.3.2	Modulation	262
E.3.2.1	2400 MHz band PHY	262
E.3.2.2	800/900 MHz band PHYs	262
E.3.3	ED and LQI	263
E.3.4	Low duty cycle	263
E.3.5	Low transmit power	263
E.3.5.1	2400 MHz band PHY	263
E.3.5.2	800 MHz band PHYs	263
E.3.5.3	900 MHz band PHYs	264
E.3.6	Channel alignment	264
E.3.7	Dynamic channel selection	264
E.3.8	Neighbor piconet capability	264
E.4	2400 MHz band coexistence performance	265
E.4.1	Assumptions for coexistence quantification	265
E.4.1.1	Channel model	265
E.4.1.2	Receiver sensitivity	266
E.4.1.3	Transmit power	266
E.4.1.4	Receiver bandwidth	266
E.4.1.5	Transmit spectral masks	266
E.4.1.6	IEEE 802.11b transmit PSD	267
E.4.1.7	Interference characteristics	267
E.4.1.8	Bit error rate (BER) calculations	267
E.4.1.9	Packet error rate (PER)	268
E.4.2	BER model	268
E.4.3	Coexistence simulation results	268
E.5	800/900 MHz bands coexistence performance	273
E.5.1	Victims and assailants	273
E.5.2	Bandwidth	273
E.5.3	Path loss model	273
E.5.4	Temporal model	274
E.5.5	Coexistence assurance results	275
E.5.5.1	868 MHz BPSK PHY	275
E.5.5.2	868 MHz O-QPSK PHY	276
E.5.5.3	868 MHz PSSS PHY	278
E.5.5.4	915 MHz BPSK PHY	279
E.5.5.5	915 MHz O-QPSK PHY	280
E.5.5.6	915 MHz PSSS PHY	281
E.6	Notes on the calculations	282

Annex F (informative) IEEE 802.15.4 regulatory requirements	283
F.1 Introduction.....	283
F.2 Applicable U.S. (FCC) rules.....	285
F.2.1 Section 15.35 of FCC CFR47	285
F.2.2 Section 15.209 of FCC CFR47	287
F.2.3 Section 15.205 of FCC CFR47	287
F.2.4 Section 15.247 of FCC CFR47	288
F.2.5 Section 15.249 of FCC CFR47	289
F.3 Applicable European rules.....	290
F.3.1 European 2400 MHz band rules	291
F.3.2 European 868–870 MHz band rules	292
F.4 Applicable Japanese rules.....	294
F.5 Emissions specification analysis with respect to known worldwide regulations	295
F.5.1 General analysis and impact of detector bandwidth and averaging rules.....	295
F.5.2 Frequency spreading and averaging effects specific to IEEE Std 802.15.4	297
F.6 Summary of out-of-band spurious emissions limits	299
F.7 Phase noise requirements inferred from regulatory limits.....	300
F.8 Summary of transmission power levels	301
Annex G (informative) Bibliography	303
G.1 General.....	303
G.2 Regulatory documents	304

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

**Part 15.4: Wireless Medium Access Control
(MAC) and Physical Layer (PHY)
Specifications for Low-Rate Wireless
Personal Area Networks (WPANs)**

1. Overview

1.1 General

Wireless personal area networks (WPANs) are used to convey information over relatively short distances. Unlike wireless local area networks (WLANs), connections effected via WPANs involve little or no infrastructure. This feature allows small, power-efficient, inexpensive solutions to be implemented for a wide range of devices.

This document defines a standard for a low-rate WPAN (LR-WPAN).

1.2 Scope

The scope of this revision is to produce specific enhancements and corrections to IEEE Std 802.15.4, all of which will be backwards compatible with IEEE Std 802.15.4-2003. These enhancements and corrections include resolving ambiguities, reducing unnecessary complexity, increasing flexibility in security key usage, considerations for newly available frequency allocations, and others.

IEEE Std 802.15.4 defines the physical layer (PHY) and medium access control (MAC) sublayer specifications for low-data-rate wireless connectivity with fixed, portable, and moving devices with no battery or very limited battery consumption requirements typically operating in the personal operating space (POS) of 10 m. It is foreseen that, depending on the application, a longer range at a lower data rate may be an acceptable tradeoff.

It is the intent of this revision to work toward a level of coexistence with other wireless devices in conjunction with Coexistence Task Groups, such as IEEE 802.15.2 and IEEE 802.11/ETSI-BRAN/MMAC 5GSG.

1.3 Purpose

The purpose of this revision is to extend the market applicability of IEEE Std 802.15.4 and to remove ambiguities in the standard. Implementations of the 2003 edition of this standard have revealed potential areas of improvements. Additional frequency bands are being made available in various countries that are attractive for this application space.

2. Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

FIPS Pub 197, Advanced Encryption Standard (AES).¹

IEEE Std 802[®], IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture.²

ISO/IEC 8802-2 (IEEE Std 802.2[™]), Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 2: Logical link control.³

ISO/IEC 9646-7 (ITU-T Rec. X.296), Information technology — Open systems interconnection — Conformance testing methodology and framework — Part 7: Implementation conformance statements.

¹FIPS publications are available from the National Technical Information Service (NTIS), U. S. Dept. of Commerce, 5285 Port Royal Rd., Springfield, VA 22161 (<http://www.ntis.org/>).

²IEEE Publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (<http://standards.ieee.org>).

³ISO/IEC publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembe, CH-1211, Genève 20, Switzerland/Suisse (<http://www.iso.ch/>). ISO/IEC publications are also available in the United States from Global Engineering Documents, 15 Inverness Way East, Englewood, Colorado 80112, USA (<http://global.ihs.com/>). Electronic copies are available in the United States from the American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (<http://www.ansi.org/>).

3. Definitions

For the purposes of this standard, the following terms and definitions apply. Terms not defined in this clause can be found in the *The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition [B3].⁴

3.1 alternate personal area network (PAN) coordinator: A coordinator that is capable of replacing the PAN coordinator, if the PAN coordinator leaves the network for any reason. A PAN can have zero or more alternate PAN coordinators.

3.2 association: The service used to establish membership for a device in a wireless personal area network (WPAN).

3.3 authentication tag: Information that allows the verification of authenticity of a message.

3.4 beacon-enabled personal area network (PAN): A PAN in which all coordinators emit regular beacons, i.e., have beacon order $< 0x0F$.

3.5 block cipher: A cryptographic function that operates on strings of fixed size.

3.6 block size: The size, in bits, of the strings on which a block cipher operates.

3.7 contention access period (CAP): The period of time immediately following a beacon frame during which devices wishing to transmit will compete for channel access using a slotted carrier sense multiple access with collision avoidance (CSMA-CA) mechanism.

3.8 contention access period (CAP) symbol: A symbol period occurring during the CAP.

3.9 coordinator: A full-function device (FFD) capable of relaying messages. If a coordinator is the principal controller of a personal area network (PAN), it is called the PAN coordinator.

3.10 data authentication: The process whereby an entity receiving a message corroborates evidence about the true source of the information in the message and, thereby, evidence that the message has not been modified in transit.

3.11 data authenticity: Assurance about the source of information.

3.12 device: Any entity containing an implementation of the IEEE 802.15.4 medium access control (MAC) and physical interface to the wireless medium. A device may be a reduced-function device (RFD) or a full-function device (FFD).

3.13 encryption: The transformation of a message into a new representation so that privileged information is required to recover the original representation.

3.14 frame: The format of aggregated bits from a medium access control (MAC) sublayer entity that are transmitted together in time.

3.15 full-function device (FFD): A device capable of operating as a coordinator.

3.16 group key: A key that is known only to a set of devices.

3.17 idle period: A duration of time where no transceiver activity is scheduled to take place.

⁴The numbers in brackets correspond to the numbers of the bibliography in Annex G.

3.18 key: Privileged information that may be used, for example, to protect information from disclosure to, and/or undetectable modification by, parties that do not have access to this privileged information.

3.19 key establishment: A process whereby two or more parties establish a key.

3.20 keying material: The combination of a key and associated security information (e.g., a nonce value).

3.21 key management: The collection of processes for the establishment and maintenance of keying relationships over a system's lifetime.

3.22 key sharing group: A set of devices that share a key.

3.23 local clock: The symbol clock internal to a device.

3.24 link key: A secret key that is shared between precisely two devices.

3.25 minimum security level: Indication of minimum protection required on information in transit.

3.26 mobile device: A device whose logical location in the network may change during use.

3.27 m-sequence: Maximal length linear feedback shift register sequence.

3.28 nonbeacon-enabled personal area network (PAN): A PAN in which coordinators do not emit regular beacons, i.e., have beacon order = 0x0F.

3.29 nonce: A nonrepeating value, such as an increasing counter, a sufficiently long random string, or a timestamp.

3.30 orphaned device: A device that has lost contact with its associated coordinator.

3.31 packet: The formatted, aggregated bits that are transmitted together in time across the physical medium.

3.32 payload data: The contents of a data message that is being transmitted.

3.33 personal area network (PAN) coordinator: A coordinator that is the principal controller of a PAN. An IEEE 802.15.4 network has exactly one PAN coordinator.

3.34 personal operating space (POS): The space about a person or object that is typically about 10 m in all directions and envelops the person or object whether stationary or in motion.

3.35 plain text: A string of unscrambled information.

3.36 protection: The combination of security services provided for information in transit, such as confidentiality, data authenticity, and/or replay protection.

3.37 radio sphere of influence: The region of space throughout which a radio may successfully communicate with other like radios.

3.38 reduced-function device (RFD): A device that is not capable of operating as a coordinator.

3.39 security level: Indication of purported protection applied to information in transit.

3.40 self-healing: The ability of the network to detect, and recover from, faults appearing in either network nodes or communication links, without human intervention.

3.41 self-organizing: The ability of network nodes to detect the presence of other nodes and to organize into a structured, functioning network without human intervention.

3.42 symmetric key: A secret key that is shared between two or more parties that may be used for encryption/decryption or integrity protection/integrity verification, depending on its intended use.

3.43 transaction: The exchange of related, consecutive frames between two peer medium access control (MAC) entities, required for a successful transmission of a MAC command or data frame.

3.44 transaction queue: A list of the pending transactions, which are to be sent using indirect transmission, that are initiated by the medium access control (MAC) sublayer of a given coordinator. The transaction queue is maintained by that coordinator while the transactions are in progress, and its length is implementation-dependent but must be at least one.

4. Acronyms and abbreviations

AES	advanced encryption standard
ASK	amplitude shift keying
AWGN	additive white Gaussian noise
AWN	affected wireless network
BE	backoff exponent
BER	bit error rate
BI	beacon interval
BLE	battery life extension
BO	beacon order
BPSK	binary phase-shift keying
BSN	beacon sequence number
CAP	contention access period
CBC-MAC	cipher block chaining message authentication code
CCA	clear channel assessment
CCM	counter with CBC-MAC (mode of operation)
CCM*	extension of CCM
CFP	contention-free period
CRC	cyclic redundancy check
CSMA-CA	carrier sense multiple access with collision avoidance
CTR	counter mode
CW	contention window (length)
DSN	data sequence number
DSSS	direct sequence spread spectrum
ED	energy detection
EIRP	effective isotropic radiated power
EMC	electromagnetic compatibility
ERP	effective radiated power
EVM	error-vector magnitude
FCS	frame check sequence
FFD	full-function device
FH	frequency hopping
FHSS	frequency hopping spread spectrum
GTS	guaranteed time slot
IFS	interframe space or spacing
ISM	industrial, scientific, and medical
IUT	implementation under test
IWN	interfering wireless network
LIFS	long interframe spacing
LLC	logical link control
LQI	link quality indication
LPDU	LLC protocol data unit
LR-WPAN	low-rate wireless personal area network
LSB	least significant bit
MAC	medium access control

MCPS	MAC common part sublayer
MCPS-SAP	MAC common part sublayer service access point
MFR	MAC footer
MHR	MAC header
MIC	message integrity code
MLME	MAC sublayer management entity
MLME-SAP	MAC sublayer management entity service access point
MSB	most significant bit
MPDU	MAC protocol data unit
MSDU	MAC service data unit
NB	number of backoff (periods)
OCDM	orthogonal code division multiplexing
O-QPSK	offset quadrature phase-shift keying
OSI	open systems interconnection
PAN	personal area network
PC	personal computer
PD	PHY data
PD-SAP	PHY data service access point
PER	packet error rate
PHR	PHY header
PHY	physical layer
PIB	PAN information base
PICS	protocol implementation conformance statement
PLME	physical layer management entity
PLME-SAP	physical layer management entity service access point
PN	pseudo-random noise
POS	personal operating space
PPDU	PHY protocol data unit
PSD	power spectral density
PSDU	PHY service data unit
PSSS	parallel sequence spread spectrum
RF	radio frequency
RFD	reduced-function device
RX	receive or receiver
SD	superframe duration
SER	symbol error rate
SFD	start-of-frame delimiter
SHR	synchronization header
SIFS	short interframe spacing
SIR	signal-to-interference ratio
SNR	signal-to-noise ratio
SO	superframe order
SPDU	SSCS protocol data units
SRD	short-range device
SSCS	service-specific convergence sublayer
SUT	system under test

TRX	transceiver
TX	transmit or transmitter
WLAN	wireless local area network
WPAN	wireless personal area network

5. General description

5.1 Introduction

An LR-WPAN is a simple, low-cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements. The main objectives of an LR-WPAN are ease of installation, reliable data transfer, short-range operation, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol.

Some of the characteristics of an LR-WPAN are as follows:

- Over-the-air data rates of 250 kb/s, 100kb/s, 40 kb/s, and 20 kb/s
- Star or peer-to-peer operation
- Allocated 16-bit short or 64-bit extended addresses
- Optional allocation of guaranteed time slots (GTSS)
- Carrier sense multiple access with collision avoidance (CSMA-CA) channel access
- Fully acknowledged protocol for transfer reliability
- Low power consumption
- Energy detection (ED)
- Link quality indication (LQI)
- 16 channels in the 2450 MHz band, 30 channels in the 915 MHz band, and 3 channels in the 868 MHz band

Two different device types can participate in an IEEE 802.15.4 network; a full-function device (FFD) and a reduced-function device (RFD). The FFD can operate in three modes serving as a personal area network (PAN) coordinator, a coordinator, or a device. An FFD can talk to RFDs or other FFDs, while an RFD can talk only to an FFD. An RFD is intended for applications that are extremely simple, such as a light switch or a passive infrared sensor; they do not have the need to send large amounts of data and may only associate with a single FFD at a time. Consequently, the RFD can be implemented using minimal resources and memory capacity.

This standard is backward-compatible to the 2003 edition; in other words, devices conforming to this standard are capable of joining and functioning in a PAN composed of devices conforming to IEEE Std 802.15.4-2003.

5.2 Components of the IEEE 802.15.4 WPAN

A system conforming to this standard consists of several components. The most basic is the device. A device may be an RFD or an FFD. Two or more devices within a POS communicating on the same physical channel constitute a WPAN. However, this WPAN shall include at least one FFD, operating as the PAN coordinator.

An IEEE 802.15.4 network is part of the WPAN family of standards although the coverage of the network may extend beyond the POS, which typically defines the WPAN.

A well-defined coverage area does not exist for wireless media because propagation characteristics are dynamic and uncertain. Small changes in position or direction may result in drastic differences in the signal strength or quality of the communication link. These effects occur whether a device is stationary or mobile, as moving objects may impact station-to-station propagation.

5.3 Network topologies

Depending on the application requirements, an IEEE 802.15.4 LR-WPAN may operate in either of two topologies: the star topology or the peer-to-peer topology. Both are shown in Figure 1. In the star topology the communication is established between devices and a single central controller, called the PAN coordinator. A device typically has some associated application and is either the initiation point or the termination point for network communications. A PAN coordinator may also have a specific application, but it can be used to initiate, terminate, or route communication around the network. The PAN coordinator is the primary controller of the PAN. All devices operating on a network of either topology shall have unique 64-bit addresses. This address may be used for direct communication within the PAN, or a short address may be allocated by the PAN coordinator when the device associates and used instead. The PAN coordinator might often be mains powered, while the devices will most likely be battery powered. Applications that benefit from a star topology include home automation, personal computer (PC) peripherals, toys and games, and personal health care.

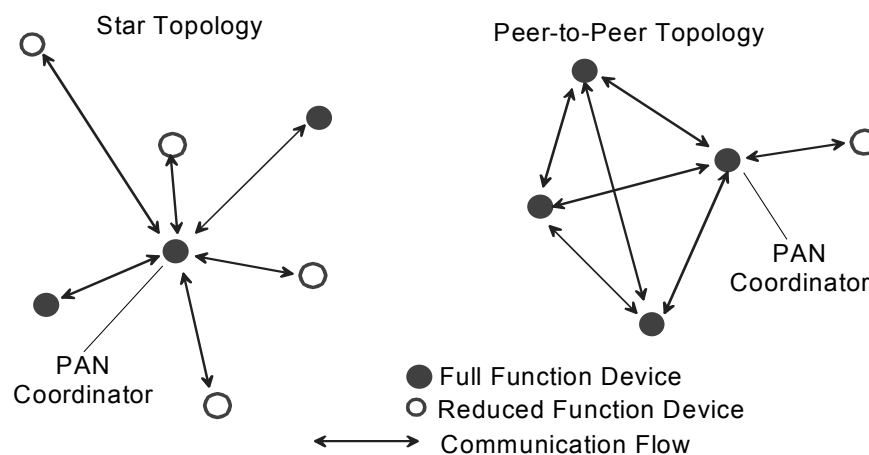


Figure 1—Star and peer-to-peer topology examples

The peer-to-peer topology also has a PAN coordinator; however, it differs from the star topology in that any device may communicate with any other device as long as they are in range of one another. Peer-to-peer topology allows more complex network formations to be implemented, such as mesh networking topology. Applications such as industrial control and monitoring, wireless sensor networks, asset and inventory tracking, intelligent agriculture, and security would benefit from such a network topology. A peer-to-peer network can be ad hoc, self-organizing, and self-healing. It may also allow multiple hops to route messages from any device to any other device on the network. Such functions can be added at the higher layer, but are not part of this standard.

Each independent PAN selects a unique identifier. This PAN identifier allows communication between devices within a network using short addresses and enables transmissions between devices across independent networks. The mechanism by which identifiers are chosen is outside the scope of this standard.

The network formation is performed by the higher layer, which is not part of this standard. However, 5.3.1 and 5.3.2 provide a brief overview on how each supported topology can be formed.

5.3.1 Star network formation

The basic structure of a star network is illustrated in Figure 1. After an FFD is activated, it can establish its own network and become the PAN coordinator. All star networks operate independently from all other star networks currently in operation. This is achieved by choosing a PAN identifier that is not currently used by any other network within the radio sphere of influence. Once the PAN identifier is chosen, the PAN

coordinator allows other devices, potentially both FFDs and RFDs, to join its network. The higher layer can use the procedures described in 7.5.2 and 7.5.3 to form a star network.

5.3.2 Peer-to-peer network formation

In a peer-to-peer topology, each device is capable of communicating with any other device within its radio sphere of influence. One device is nominated as the PAN coordinator, for instance, by virtue of being the first device to communicate on the channel. Further network structures are constructed out of the peer-to-peer topology and it is possible to impose topological restrictions on the formation of the network.

An example of the use of the peer-to-peer communications topology is the cluster tree. The cluster tree network is a special case of a peer-to-peer network in which most devices are FFDs. An RFD connects to a cluster tree network as a leaf device at the end of a branch because RFDs do not allow other devices to associate. Any of the FFDs may act as a coordinator and provide synchronization services to other devices or other coordinators. Only one of these coordinators can be the overall PAN coordinator, which may have greater computational resources than any other device(s) in the PAN. The PAN coordinator forms the first cluster by choosing an unused PAN identifier and broadcasting beacon frames to neighboring devices. A contention resolution mechanism is required if two or more FFDs simultaneously attempt to establish themselves as PAN coordinators; however, such a mechanism is outside the scope of this standard. A candidate device receiving a beacon frame may request to join the network at the PAN coordinator. If the PAN coordinator permits the device to join, it adds the new device as a child device in its neighbor list. Then the newly joined device adds the PAN coordinator as its parent in its neighbor list and begins transmitting periodic beacons; other candidate devices may then join the network at that device. If the original candidate device is not able to join the network at the PAN coordinator, it will search for another parent device. The detailed procedures describing how a PAN is started and how devices join a PAN are found in 7.5.2 and 7.5.3.

The simplest form of a cluster tree network is a single cluster network, but larger networks are possible by forming a mesh of multiple neighboring clusters. Once predetermined application or network requirements are met, the first PAN coordinator may instruct a device to become the PAN coordinator of a new cluster adjacent to the first one. Other devices gradually connect and form a multicluster network structure, such as the one seen in Figure 2. The lines in Figure 2 represent the parent-child relationships of the devices and not the communication flow. The advantage of a multicluster structure is increased coverage area, while the disadvantage is an increase in message latency.

5.4 Architecture

The IEEE 802.15.4 architecture is defined in terms of a number of blocks in order to simplify the standard. These blocks are called layers. Each layer is responsible for one part of the standard and offers services to the higher layers. The layout of the blocks is based on the open systems interconnection (OSI) seven-layer model (see ISO/IEC 7498-1:1994 [B12]).

The interfaces between the layers serve to define the logical links that are described in this standard.

An LR-WPAN device comprises a PHY, which contains the radio frequency (RF) transceiver along with its low-level control mechanism, and a MAC sublayer that provides access to the physical channel for all types of transfer. Figure 3 shows these blocks in a graphical representation, which are described in more detail in 5.4.1 and 5.4.2.

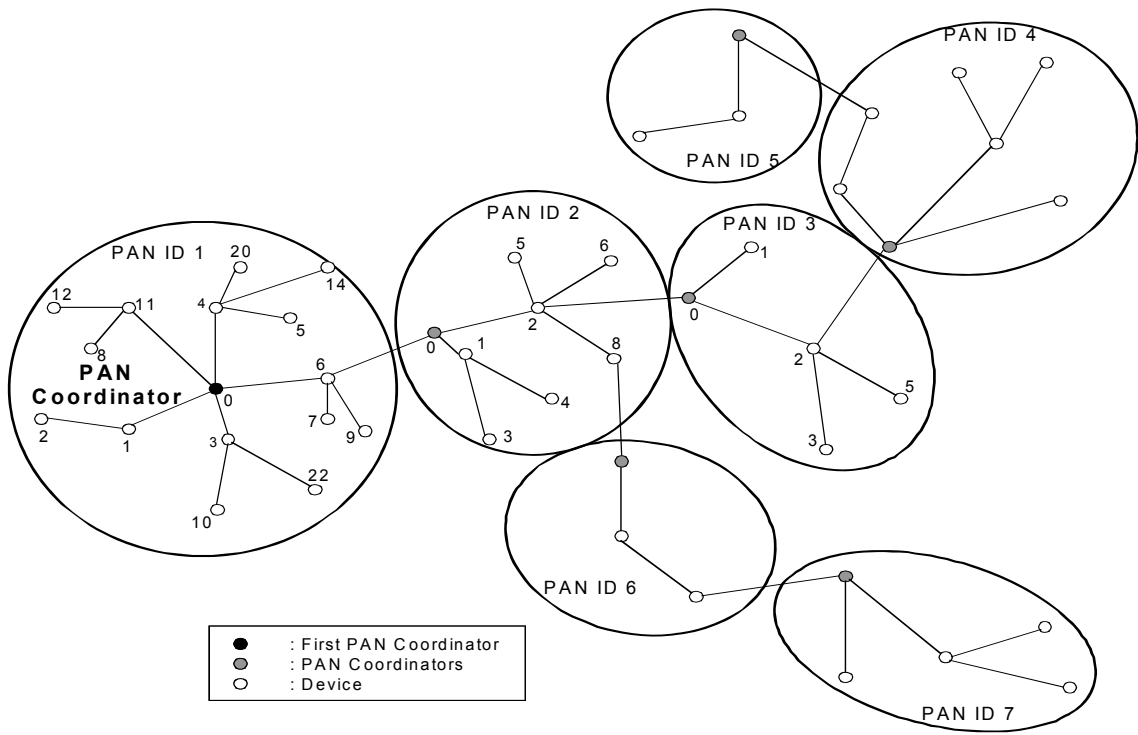
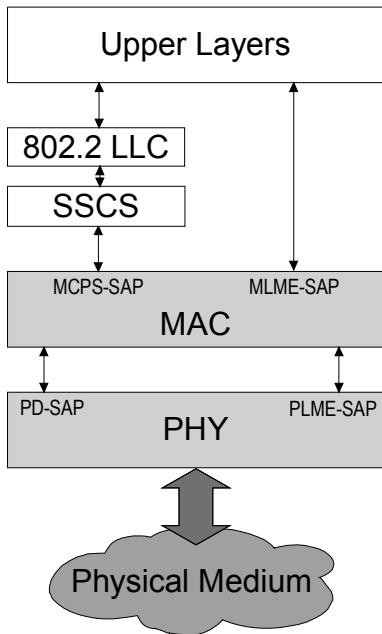


Figure 2—Cluster tree network



NOTE—For MCPS-SAP, see 7.1; for MLME-SAP, see 5.4.2; for PD-SAP, see 6.2; and for PLME-SAP, see 5.4.1.

Figure 3—LR-WPAN device architecture

The upper layers, shown in Figure 3, consist of a network layer, which provides network configuration, manipulation, and message routing, and an application layer, which provides the intended function of the device. The definition of these upper layers is outside the scope of this standard. An IEEE 802.2 Type 1 logical link control (LLC) can access the MAC sublayer through the service-specific convergence sublayer (SSCS), defined in Annex A. The LR-WPAN architecture can be implemented either as embedded devices or as devices requiring the support of an external device such as a PC.

5.4.1 Physical layer (PHY)

The PHY provides two services: the PHY data service and the PHY management service interfacing to the physical layer management entity (PLME) service access point (SAP) (known as the PLME-SAP). The PHY data service enables the transmission and reception of PHY protocol data units (PPDUs) across the physical radio channel.

Clause 6 contains the specifications for the PHY.

The features of the PHY are activation and deactivation of the radio transceiver, ED, LQI, channel selection, clear channel assessment (CCA), and transmitting as well as receiving packets across the physical medium. The radio operates at one or more of the following unlicensed bands:

- 868–868.6 MHz (e.g., Europe)
- 902–928 MHz (e.g., North America)
- 2400–2483.5 MHz (worldwide)

Refer to Annex F for an informative summary of regulatory requirements.

5.4.2 MAC sublayer

The MAC sublayer provides two services: the MAC data service and the MAC management service interfacing to the MAC sublayer management entity (MLME) service access point (SAP) (known as MLME-SAP). The MAC data service enables the transmission and reception of MAC protocol data units (MPDUs) across the PHY data service.

The features of the MAC sublayer are beacon management, channel access, GTS management, frame validation, acknowledged frame delivery, association, and disassociation. In addition, the MAC sublayer provides hooks for implementing application-appropriate security mechanisms.

Clause 7 contains the specifications for the MAC sublayer.

5.5 Functional overview

A brief overview of the general functions of a LR-WPAN is given in 5.5.1 through 5.5.6 and includes information on the superframe structure, the data transfer model, the frame structure, improving probability of successful delivery, power consumption considerations, and security.

5.5.1 Superframe structure

This standard allows the optional use of a superframe structure. The format of the superframe is defined by the coordinator. The superframe is bounded by network beacons sent by the coordinator (see Figure 4a) and is divided into 16 equally sized slots. Optionally, the superframe can have an active and an inactive portion (see Figure 4b). During the inactive portion, the coordinator may enter a low-power mode. The beacon frame is transmitted in the first slot of each superframe. If a coordinator does not wish to use a superframe structure, it will turn off the beacon transmissions. The beacons are used to synchronize the attached

devices, to identify the PAN, and to describe the structure of the superframes. Any device wishing to communicate during the contention access period (CAP) between two beacons competes with other devices using a slotted CSMA-CA mechanism. All transactions are completed by the time of the next network beacon.

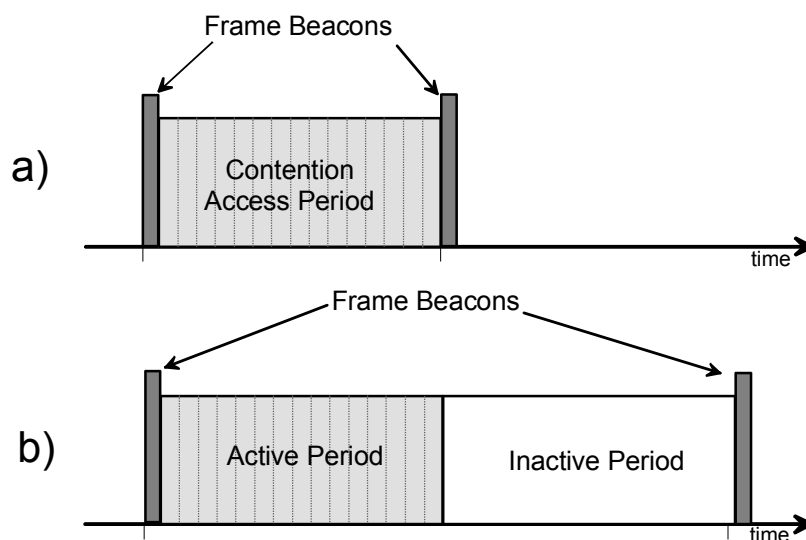


Figure 4—Superframe structure without GTTs

For low-latency applications or applications requiring specific data bandwidth, the PAN coordinator may dedicate portions of the active superframe to that application. These portions are called guaranteed time slots (GTSs). The GTSs form the contention-free period (CFP), which always appears at the end of the active superframe starting at a slot boundary immediately following the CAP, as shown in Figure 5. The PAN coordinator may allocate up to seven of these GTSs, and a GTS may occupy more than one slot period. However, a sufficient portion of the CAP remains for contention-based access of other networked devices or new devices wishing to join the network. All contention-based transactions are completed before the CFP begins. Also each device transmitting in a GTS ensures that its transaction is complete before the time of the next GTS or the end of the CFP. More information on the superframe structure can be found in 7.5.1.1.

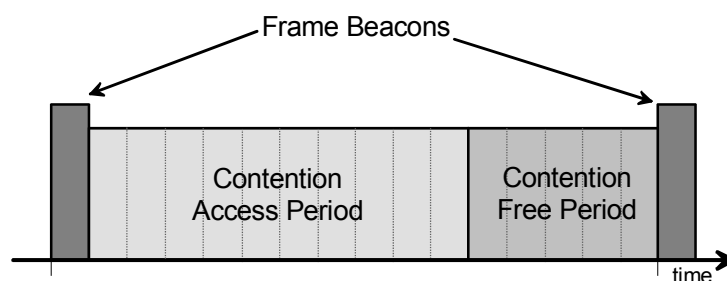


Figure 5—Superframe structure with GTTs

5.5.2 Data transfer model

Three types of data transfer transactions exist. The first one is the data transfer to a coordinator in which a device transmits the data. The second transaction is the data transfer from a coordinator in which the device receives the data. The third transaction is the data transfer between two peer devices. In star topology, only two of these transactions are used because data may be exchanged only between the coordinator and a device. In a peer-to-peer topology, data may be exchanged between any two devices on the network; consequently all three transactions may be used in this topology.

The mechanisms for each transfer type depend on whether the network supports the transmission of beacons. A beacon-enabled PAN is used in networks that either require synchronization or support for low-latency devices, such as PC peripherals. If the network does not need synchronization or support for low-latency devices, it can elect not to use the beacon for normal transfers. However, the beacon is still required for network discovery. The structure of the frames used for the data transfer is specified in 7.2.

5.5.2.1 Data transfer to a coordinator

When a device wishes to transfer data to a coordinator in a beacon-enabled PAN, it first listens for the network beacon. When the beacon is found, the device synchronizes to the superframe structure. At the appropriate time, the device transmits its data frame, using slotted CSMA-CA, to the coordinator. The coordinator may acknowledge the successful reception of the data by transmitting an optional acknowledgment frame. This sequence is summarized in Figure 6.

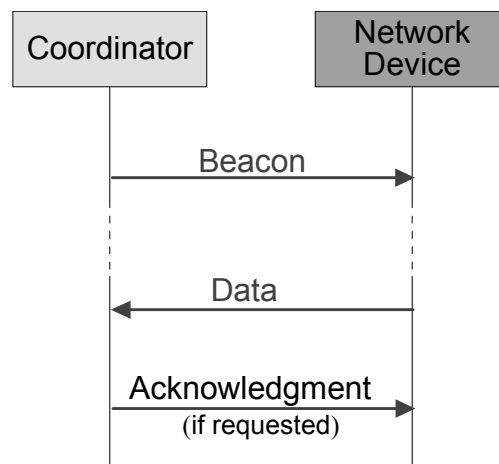


Figure 6—Communication to a coordinator in a beacon-enabled PAN

When a device wishes to transfer data in a nonbeacon-enabled PAN, it simply transmits its data frame, using unslotted CSMA-CA, to the coordinator. The coordinator acknowledges the successful reception of the data by transmitting an optional acknowledgment frame. The transaction is now complete. This sequence is summarized in Figure 7.

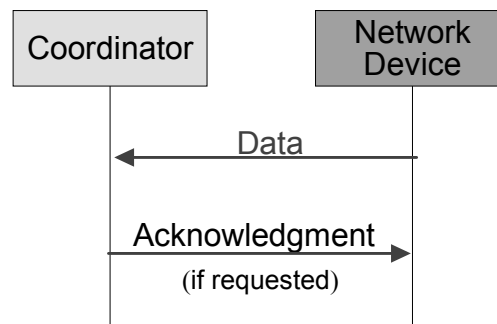


Figure 7—Communication to a coordinator in a nonbeacon-enabled PAN

5.5.2.2 Data transfer from a coordinator

When the coordinator wishes to transfer data to a device in a beacon-enabled PAN, it indicates in the network beacon that the data message is pending. The device periodically listens to the network beacon and, if a message is pending, transmits a MAC command requesting the data, using slotted CSMA-CA. The coordinator acknowledges the successful reception of the data request by transmitting an acknowledgment frame. The pending data frame is then sent using slotted CSMA-CA or, if possible, immediately after the acknowledgment (see 7.5.6.3). The device may acknowledge the successful reception of the data by transmitting an optional acknowledgment frame. The transaction is now complete. Upon successful completion of the data transaction, the message is removed from the list of pending messages in the beacon. This sequence is summarized in Figure 8.

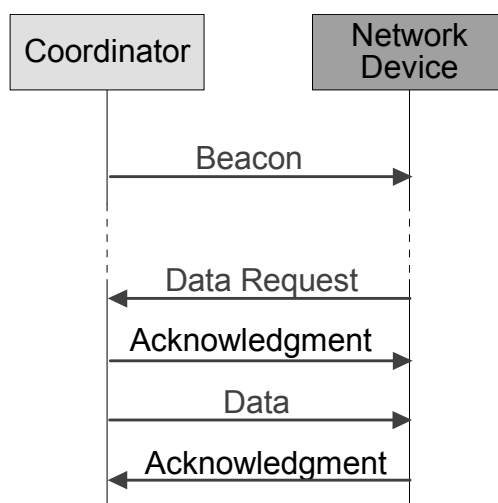


Figure 8—Communication from a coordinator in a beacon-enabled PAN

When a coordinator wishes to transfer data to a device in a nonbeacon-enabled PAN, it stores the data for the appropriate device to make contact and request the data. A device may make contact by transmitting a MAC command requesting the data, using unslotted CSMA-CA, to its coordinator at an application-defined rate. The coordinator acknowledges the successful reception of the data request by transmitting an acknowledgment frame. If a data frame is pending, the coordinator transmits the data frame, using unslotted CSMA-CA, to the device. If a data frame is not pending, the coordinator indicates this fact either in the acknowledgment frame following the data request or in a data frame with a zero-length payload (see 7.5.6.3). If requested, the device acknowledges the successful reception of the data frame by transmitting an acknowledgment frame. This sequence is summarized in Figure 9.

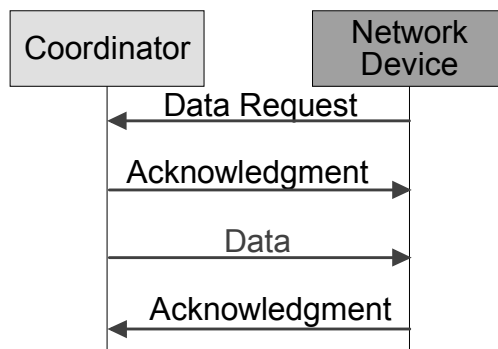


Figure 9—Communication from a coordinator in a nonbeacon-enabled PAN

5.5.2.3 Peer-to-peer data transfers

In a peer-to-peer PAN, every device may communicate with every other device in its radio sphere of influence. In order to do this effectively, the devices wishing to communicate will need to either receive constantly or synchronize with each other. In the former case, the device can simply transmit its data using unslotted CSMA-CA. In the latter case, other measures need to be taken in order to achieve synchronization. Such measures are beyond the scope of this standard.

5.5.3 Frame structure

The frame structures have been designed to keep the complexity to a minimum while at the same time making them sufficiently robust for transmission on a noisy channel. Each successive protocol layer adds to the structure with layer-specific headers and footers. This standard defines four frame structures:

- A beacon frame, used by a coordinator to transmit beacons
- A data frame, used for all transfers of data
- An acknowledgment frame, used for confirming successful frame reception
- A MAC command frame, used for handling all MAC peer entity control transfers

The structure of each of the four frame types is described in 5.5.3.1 through 5.5.3.4. The diagrams in these subclauses illustrate the fields that are added by each layer of the protocol.

5.5.3.1 Beacon frame

Figure 10 shows the structure of the beacon frame, which originates from within the MAC sublayer. A coordinator can transmit network beacons in a beacon-enabled PAN. The MAC payload contains the superframe specification, GTS fields, pending address fields, and beacon payload (see 7.2.2.1). The MAC payload is prefixed with a MAC header (MHR) and appended with a MAC footer (MFR). The MHR contains the MAC Frame Control field, beacon sequence number (BSN), addressing fields, and optionally the auxiliary security header. The MFR contains a 16-bit frame check sequence (FCS). The MHR, MAC payload, and MFR together form the MAC beacon frame (i.e., MPDU).

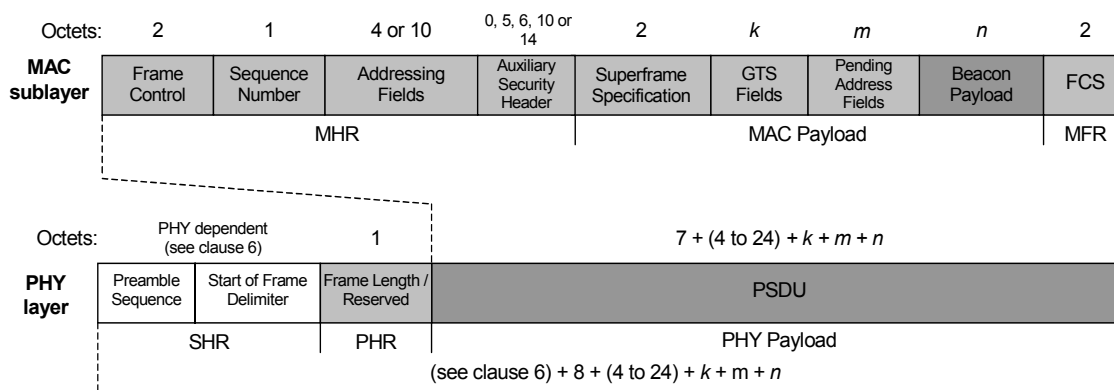


Figure 10—Schematic view of the beacon frame and the PHY packet

The MAC beacon frame is then passed to the PHY as the PHY service data unit (PSDU), which becomes the PHY payload. The PHY payload is prefixed with a synchronization header (SHR), containing the Preamble Sequence and Start-of-Frame Delimiter (SFD) fields, and a PHY header (PHR) containing the length of the PHY payload in octets. The SHR, PHR, and PHY payload together form the PHY packet (i.e., PPDU).

5.5.3.2 Data frame

Figure 11 shows the structure of the data frame, which originates from the upper layers.



Figure 11—Schematic view of the data frame and the PHY packet

The data payload is passed to the MAC sublayer and is referred to as the MAC service data unit (MSDU). The MAC payload is prefixed with an MHR and appended with an MFR. The MHR contains the Frame Control field, data sequence number (DSN), addressing fields, and optionally the auxiliary security header. The MFR is composed of a 16-bit FCS. The MHR, MAC payload, and MFR together form the MAC data frame, (i.e., MPDU).

The MPDU is passed to the PHY as the PSDU, which becomes the PHY payload. The PHY payload is prefixed with an SHR, containing the Preamble Sequence and SFD fields, and a PHR containing the length of the PHY payload in octets. The preamble sequence and the data SFD enable the receiver to achieve symbol synchronization. The SHR, PHR, and PHY payload together form the PHY packet, (i.e., PPDU).

5.5.3.3 Acknowledgment frame

Figure 12 shows the structure of the acknowledgment frame, which originates from within the MAC sublayer. The MAC acknowledgment frame is constructed from an MHR and an MFR; it has no MAC payload. The MHR contains the MAC Frame Control field and DSN. The MFR is composed of a 16-bit FCS. The MHR and MFR together form the MAC acknowledgment frame (i.e., MPDU).

The MPDU is passed to the PHY as the PSDU, which becomes the PHY payload. The PHY payload is prefixed with the SHR, containing the Preamble Sequence and SFD fields, and the PHR containing the length of the PHY payload in octets. The SHR, PHR, and PHY payload together form the PHY packet, (i.e., PPDU).

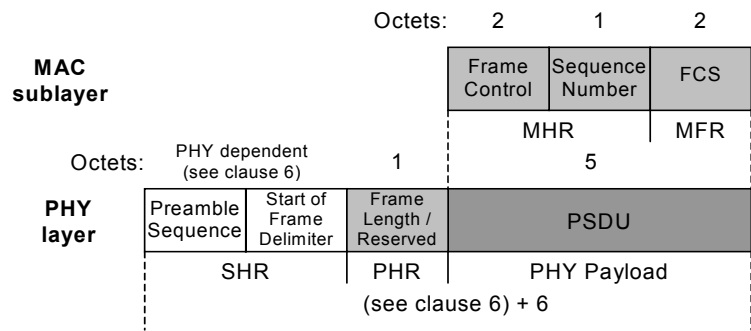


Figure 12—Schematic view of the acknowledgment frame and the PHY packet

5.5.3.4 MAC command frame

Figure 13 shows the structure of the MAC command frame, which originates from within the MAC sublayer. The MAC payload contains the Command Type field and the command payload (see 7.2.2.4). The MAC payload is prefixed with an MHR and appended with an MFR. The MHR contains the MAC Frame Control field, DSN, addressing fields, and optionally the auxiliary security header. The MFR contains a 16-bit FCS. The MHR, MAC payload, and MFR together form the MAC command frame, (i.e., MPDU).

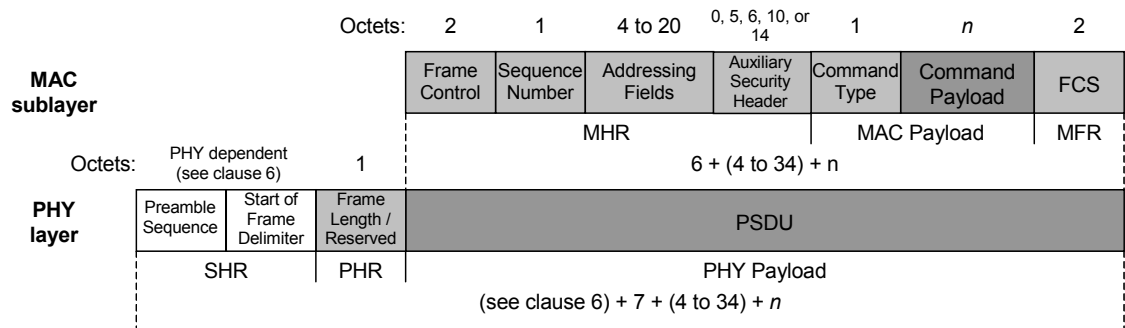


Figure 13—Schematic view of the MAC command frame and the PHY packet

The MPDU is then passed to the PHY as the PSDU, which becomes the PHY payload. The PHY payload is prefixed with an SHR, containing the Preamble Sequence and SFD fields, and a PHR containing the length of the PHY payload in octets. The preamble sequence enables the receiver to achieve symbol synchronization. The SHR, PHR, and PHY payload together form the PHY packet, (i.e., PPDU).

5.5.4 Improving probability of successful delivery

The IEEE 802.15.4 LR-WPAN employs various mechanisms to improve the probability of successful data transmission. These mechanisms are the CSMA-CA mechanism, frame acknowledgment, and data verification and are briefly discussed in 5.5.4.1 through 5.5.4.3.

5.5.4.1 CSMA-CA mechanism

The IEEE 802.15.4 LR-WPAN uses two types of channel access mechanism, depending on the network configuration. Nonbeacon-enabled PANs use an unslotted CSMA-CA channel access mechanism, as described in 7.5.1. Each time a device wishes to transmit data frames or MAC commands, it waits for a random period. If the channel is found to be idle, following the random backoff, the device transmits its data. If the channel is found to be busy following the random backoff, the device waits for another random period before trying to access the channel again. Acknowledgment frames are sent without using a CSMA-CA mechanism.

Beacon-enabled PANs use a slotted CSMA-CA channel access mechanism, where the backoff slots are aligned with the start of the beacon transmission. The backoff slots of all devices within one PAN are aligned to the PAN coordinator. Each time a device wishes to transmit data frames during the CAP, it locates the boundary of the next backoff slot and then waits for a random number of backoff slots. If the channel is busy, following this random backoff, the device waits for another random number of backoff slots before trying to access the channel again. If the channel is idle, the device begins transmitting on the next available backoff slot boundary. Acknowledgment and beacon frames are sent without using a CSMA-CA mechanism.

5.5.4.2 Frame acknowledgment

A successful reception and validation of a data or MAC command frame can be optionally confirmed with an acknowledgment, as described in 7.5.6.4. If the receiving device is unable to handle the received data frame for any reason, the message is not acknowledged.

If the originator does not receive an acknowledgment after some period, it assumes that the transmission was unsuccessful and retries the frame transmission. If an acknowledgment is still not received after several retries, the originator can choose either to terminate the transaction or to try again. When the acknowledgment is not required, the originator assumes the transmission was successful.

5.5.4.3 Data verification

In order to detect bit errors, an FCS mechanism employing a 16-bit International Telecommunication Union—Telecommunication Standardization Sector (ITU-T) cyclic redundancy check (CRC) is used to detect errors in every frame.

The FCS mechanism is discussed in 7.2.1.9.

5.5.5 Power consumption considerations

In many applications that use this standard, devices will be battery powered, and battery replacement or recharging in relatively short intervals is impractical. Therefore, the power consumption is of significant concern. This standard was developed with limited power supply availability in mind. However, the physical implementation of this standard will require additional power management considerations that are beyond the scope of this standard.

The protocol has been developed to favor battery-powered devices. However, in certain applications, some of these devices could potentially be mains powered. Battery-powered devices will require duty-cycling to reduce power consumption. These devices will spend most of their operational life in a sleep state; however, each device periodically listens to the RF channel in order to determine whether a message is pending. This mechanism allows the application designer to decide on the balance between battery consumption and message latency. Higher powered devices have the option of listening to the RF channel continuously.

5.5.6 Security

From a security perspective, wireless ad hoc networks are no different from any other wireless network. They are vulnerable to passive eavesdropping attacks and potentially even active tampering because physical access to the wire is not required to participate in communications. The very nature of ad hoc networks and their cost objectives impose additional security constraints, which perhaps make these networks the most difficult environments to secure. Devices are low-cost and have limited capabilities in terms of computing power, available storage, and power drain; and it cannot always be assumed they have a trusted computing base nor a high-quality random number generator aboard. Communications cannot rely on the online availability of a fixed infrastructure and might involve short-term relationships between devices that may never have communicated before. These constraints might severely limit the choice of cryptographic algorithms and protocols and would influence the design of the security architecture because the establishment and maintenance of trust relationships between devices need to be addressed with care. In addition, battery lifetime and cost constraints put severe limits on the security overhead these networks can tolerate, something that is of far less concern with higher bandwidth networks. Most of these security architectural elements can be implemented at higher layers and may, therefore, be considered to be outside the scope of this standard.

The cryptographic mechanism in this standard is based on symmetric-key cryptography and uses keys that are provided by higher layer processes. The establishment and maintenance of these keys are outside the

scope of this standard. The mechanism assumes a secure implementation of cryptographic operations and secure and authentic storage of keying material.

The cryptographic mechanism provides particular combinations of the following security services:

- *Data confidentiality*: Assurance that transmitted information is only disclosed to parties for which it is intended.
- *Data authenticity*: Assurance of the source of transmitted information (and, hereby, that information was not modified in transit).
- *Replay protection*: Assurance that duplicate information is detected.

The actual frame protection provided can be adapted on a frame-by-frame basis and allows for varying levels of data authenticity (to minimize security overhead in transmitted frames where required) and for optional data confidentiality. When nontrivial protection is required, replay protection is always provided.

Cryptographic frame protection may use a key shared between two peer devices (link key) or a key shared among a group of devices (group key), thus allowing some flexibility and application-specific tradeoffs between key storage and key maintenance costs versus the cryptographic protection provided. If a group key is used for peer-to-peer communication, protection is provided only against outsider devices and not against potential malicious devices in the key-sharing group.

For more detailed information on the cryptographic security mechanisms used for protected MAC frames following this standard, refer to Clause 7.

5.6 Concept of primitives

This subclause provides a brief overview of the concept of service primitives. Refer to ISO/IEC 8802.2⁵ for more detailed information.

The services of a layer are the capabilities it offers to the user in the next higher layer or sublayer by building its functions on the services of the next lower layer. This concept is illustrated in Figure 14, showing the service hierarchy and the relationship of the two correspondent N-users and their associated N-layer (or sublayer) peer protocol entities.

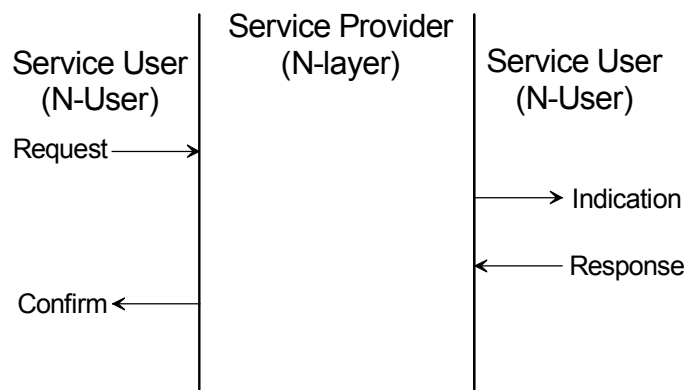


Figure 14—Service primitives

⁵For information on references, see Clause 2.

The services are specified by describing the information flow between the N-user and the N-layer. This information flow is modeled by discrete, instantaneous events, which characterize the provision of a service. Each event consists of passing a service primitive from one layer to the other through a layer SAP associated with an N-user. Service primitives convey the required information by providing a particular service. These service primitives are an abstraction because they specify only the provided service rather than the means by which it is provided. This definition is independent of any other interface implementation.

A service is specified by describing the service primitives and parameters that characterize it. A service may have one or more related primitives that constitute the activity that is related to that particular service. Each service primitive may have zero or more parameters that convey the information required to provide the service.

A primitive can be one of four generic types:

- *Request*: The request primitive is passed from the N-user to the N-layer to request that a service is initiated.
- *Indication*: The indication primitive is passed from the N-layer to the N-user to indicate an internal N-layer event that is significant to the N-user. This event may be logically related to a remote service request, or it may be caused by an N-layer internal event.
- *Response*: The response primitive is passed from the N-user to the N-layer to complete a procedure previously invoked by an indication primitive.
- *Confirm*: The confirm primitive is passed from the N-layer to the N-user to convey the results of one or more associated previous service requests.

6. PHY specification

6.1 General requirements and definitions

The PHY is responsible for the following tasks:

- Activation and deactivation of the radio transceiver
- Energy detection (ED) within the current channel
- Link quality indicator (LQI) for received packets
- Clear channel assessment (CCA) for carrier sense multiple access with collision avoidance (CSMA-CA)
- Channel frequency selection
- Data transmission and reception

Constants and attributes that are specified and maintained by the PHY are written in the text of this clause in italics. Constants have a general prefix of “a”, e.g., *aMaxPHYPacketSize*, and are listed in Table 22 (in 6.4.1). Attributes have a general prefix of “phy”, e.g., *phyCurrentChannel*, and are listed in Table 23 (in 6.4.2).

This subclause specifies requirements that are common to all of the PHYs that conform to this standard.

The standard specifies the following four PHYs:

- An 868/915 MHz direct sequence spread spectrum (DSSS) PHY employing binary phase-shift keying (BPSK) modulation
- An 868/915 MHz DSSS PHY employing offset quadrature phase-shift keying (O-QPSK) modulation
- An 868/915 MHz parallel sequence spread spectrum (PSSS) PHY employing BPSK and amplitude shift keying (ASK) modulation
- A 2450 MHz DSSS PHY employing O-QPSK modulation

In addition to the 868/915 MHz BPSK PHY, which was originally specified in the 2003 edition of this standard, two optional high-data-rate PHYs are specified for the 868/915 MHz bands, offering a tradeoff between complexity and data rate. Both optional PHYs offer a data rate much higher than that of the 868/915 MHz BPSK PHY, which provides for 20 kb/s in the 868 MHz band and 40 kb/s in the 915 MHz band. The ASK⁶ PHY offers data rates of 250 kb/s in both the 868 MHz and 915 MHz bands, which is equal to that of the 2.4 GHz band PHY. The O-QPSK PHY, which offers a signaling scheme identical to that of the 2.4 GHz band PHY, offers a data rate in the 915 MHz band equal to that of the 2.4 GHz band PHY and a data rate of 100 kb/s in the 868 MHz band.

6.1.1 Operating frequency range

A compliant device shall operate in one or several frequency bands using the modulation and spreading formats summarized in Table 1.

Devices shall start in the mode (PHY) they are instructed to do so. If the device is capable of operating in the 868/915 MHz bands using one of the optional PHYs, it shall be able to switch dynamically between the optional 868/915 MHz band PHY and the mandatory 868/915 MHz BPSK PHYs when instructed to do so.

⁶The 868/915 MHz band ASK PHYs use BPSK modulation for the SHR and ASK modulation for the remainder of the PPDU.

Table 1—Frequency bands and data rates

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
868/915 (optional)	868–868.6	400	ASK	250	12.5	20-bit PSSS
	902–928	1600	ASK	250	50	5-bit PSSS
868/915 (optional)	868–868.6	400	O-QPSK	100	25	16-ary Orthogonal
	902–928	1000	O-QPSK	250	62.5	16-ary Orthogonal
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

This standard is intended to conform with established regulations in Europe, Japan, Canada, and the United States. The regulatory documents listed below are for information only and are subject to change and revisions at any time. Devices conforming to this standard shall also comply with specific regional legislation. Additional regulatory information is provided in Annex F.

Europe:

- Approval standards: European Telecommunications Standards Institute (ETSI)
- Documents: ETSI EN 300 328-1 [B26], ETSI EN 300 328-2 [B27], ETSI EN 300 220-1 [B25], ERC Recommendation 70-03 [B24]
- Approval authority: National type approval authorities

Japan:

- Approval standards: Association of Radio Industries and Businesses (ARIB)
- Document: ARIB STD-T66 [B22]
- Approval authority: Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT)

United States:

- Approval standards: Federal Communications Commission (FCC), United States
- Document: FCC CFR47, Section 15.247 [B29]

Canada:

- Approval standards: Industry Canada (IC), Canada
- Document: GL36 [B32]

6.1.2 Channel assignments

The introduction of the “868/915 MHz band (optional) amplitude shift keying (ASK) PHY specifications” and “868/915 MHz band (optional) O-QPSK PHY specifications” results in the total number of channel assignments exceeding the channel numbering capability of 32 channel numbers that was defined in the 2003 edition of this standard.

To support the growing number of channels, channel assignments shall be defined through a combination of channel numbers and channels pages.

The upper 5 most significant bits (MSBs) of the 32-bit channel bitmaps in *phyChannelsSupported* shall be used as an integer value to specify 32 possible channel pages. The lower 27 bits of the channel bit map shall be used as a bit mask to specify channel numbers within a channel page.

6.1.2.1 Channel numbering

A total of 27 channels numbered 0 to 26 are available per channel page.

For channel page 0, 27 channels numbered 0 to 26 are available across the three frequency bands. Sixteen channels are available in the 2450 MHz band, 10 in the 915 MHz band, and 1 in the 868 MHz band. This channel page supports the channels defined in the 2003 edition of this standard. The center frequency of these channels is defined as follows:

$$F_c = 868.3 \text{ in megahertz, for } k = 0$$

$$F_c = 906 + 2(k - 1) \text{ in megahertz, for } k = 1, 2, \dots, 10$$

$$\text{and } F_c = 2405 + 5(k - 11) \text{ in megahertz, for } k = 11, 12, \dots, 26$$

where

k is the channel number.

For channel pages 1 and 2, 11 channels numbered 0 to 10 are available across the two frequency bands to support the 868/915 MHz ASK and O-QPSK PHYs, respectively. Ten channels are available in the 915 MHz band and 1 in the 868 MHz band. The center frequency of these channels is defined as follows:

$$F_c = 868.3 \text{ in megahertz, for } k = 0$$

$$\text{and } F_c = 906 + 2(k - 1) \text{ in megahertz, for } k = 1, 2, \dots, 10$$

where

k is the channel number.

For each PHY supported, a compliant device shall support all channels allowed by regulations for the region in which the device operates.

6.1.2.2 Channel pages

A total of 32 channel pages are available with channel pages 3 to 31 being reserved for future use. The *phyPagesSupported* PHY PAN information base (PIB) attribute indicates which channel pages are supported by the current PHY, while the *phyCurrentPage* PHY PIB attribute identifies the channel page that is currently used. The PHY PIB attributes are described in 6.4.2.

If the requested PHY PIB attribute is the *phyCurrentPage*, the attribute was successfully set to a different value from the current value, and the channel is no longer valid, then the PHY shall also set the *phyCurrentChannel* to the lowest valid channel for the requested page.

The channel pages and associated channel numbers are shown in Table 2.

6.1.4 RF power measurement

Unless otherwise stated, all RF power measurements, either transmit or receive, shall be made at the appropriate transceiver to antenna connector. The measurements shall be made with equipment that is either matched to the impedance of the antenna connector or corrected for any mismatch. For devices without an antenna connector, the measurements shall be interpreted as effective isotropic radiated power (EIRP) (i.e., a 0 dBi gain antenna), and any radiated measurements shall be corrected to compensate for the antenna gain in the implementation.

6.1.5 Transmit power

The maximum transmit power shall conform with local regulations. Refer to Annex F for additional information on regulatory limits. A compliant device shall have its nominal transmit power level indicated by its PHY parameter, *phyTransmitPower* (see 6.4).

6.1.6 Out-of-band spurious emission

The out-of-band spurious emissions shall conform with local regulations. Refer to Annex F for additional information on regulatory limits on out-of-band emissions.

6.1.7 Receiver sensitivity definitions

The receiver sensitivity definitions used throughout this standard are defined in Table 4.

Table 4—Receiver sensitivity definitions

Term	Definition of term	Conditions
Packet error rate (PER)	Average fraction of transmitted packets that are not correctly received.	– Average measured over random PSDU data.
Receiver sensitivity	Threshold input signal power that yields a specified PER.	– PSDU length = 20 octets. – PER < 1%. – Power measured at antenna terminals. – Interference not present.

6.2 PHY service specifications

The PHY provides an interface between the MAC sublayer and the physical radio channel, via the RF firmware and RF hardware. The PHY conceptually includes a management entity called the PLME. This entity provides the layer management service interfaces through which layer management functions may be invoked. The PLME is also responsible for maintaining a database of managed objects pertaining to the PHY. This database is referred to as the PHY PAN information base (PIB).

Figure 15 depicts the components and interfaces of the PHY.

The PHY provides two services, accessed through two SAPs: the PHY data service, accessed through the PHY data SAP (PD-SAP), and the PHY management service, accessed through the PLME-SAP.

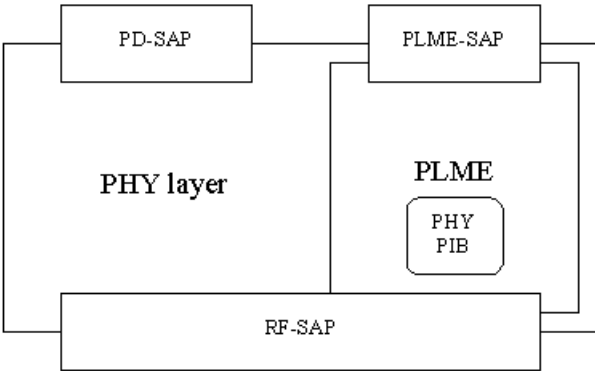


Figure 15—The PHY reference model

6.2.1 PHY data service

The PD-SAP supports the transport of MPDUs between peer MAC sublayer entities. Table 5 lists the primitives supported by the PD-SAP. These primitives are discussed in the subclauses referenced in the table.

Table 5—PD-SAP primitives

PD-SAP primitive	Request	Confirm	Indication
PD-DATA	6.2.1.1	6.2.1.2	6.2.1.3

6.2.1.1 PD-DATA.request

The PD-DATA.request primitive requests the transfer of an MPDU (i.e., PSDU) from the MAC sublayer to the local PHY entity.

6.2.1.1.1 Semantics of the service primitive

The semantics of the PD-DATA.request primitive is as follows:

PD-DATA.request (psduLength, psdu)

Table 6 specifies the parameters for the PD-DATA.request primitive.

Table 6—PD-DATA.request parameters

Name	Type	Valid range	Description
psduLength	Unsigned integer	$\leq aMaxPHYPacketSize$	The number of octets contained in the PSDU to be transmitted by the PHY entity.
psdu	Set of octets	—	The set of octets forming the PSDU to be transmitted by the PHY entity.