

IEEE Standard for High Data Rate Wireless Multi-Media Networks

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

IEEE Std 802.15.3™-2016
(Revision of
IEEE Std 802.15.3-2003)

IEEE Std 802.15.3™-2016
(Revision of
IEEE Std 802.15.3-2003)

IEEE Standard for High Data Rate Wireless Multi-Media Networks

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 15 May 2016
IEEE-SA Standards Board

Abstract: The protocol and compatible interconnection of data and multimedia communication equipment via 2.4 GHz and 60 GHz radio transmissions in a Wireless Personal Area Network (WPAN) using low power and multiple modulation formats to support scalable data rates is defined in this standard. The Medium Access Control (MAC) sublayer protocol supports both isochronous and asynchronous data types.

Keywords: ad hoc network, IEEE 802.15.3™, mobility, mm-wave, radio frequency, wireless

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

Copyright © 2016 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 25 July 2016. Printed in the United States of America.

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

PDF: ISBN 978-1-5044-2023-5 STD20940
Print: ISBN 978-1-5044-2024-2 STDPD20940

IEEE prohibits discrimination, harassment, and bullying. For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

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

Important Notices and Disclaimers Concerning IEEE Standards Documents

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

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

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

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

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

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

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

Translations

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

Official statements

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

Comments on standards

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

Comments on standards should be submitted to the following address:

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

Laws and regulations

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

Copyrights

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

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

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

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at <http://ieeexplore.ieee.org/browse/standards/collection/ieee> or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE-SA Website at <http://standards.ieee.org>.

Errata

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

Patents

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

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

Participants

At the time this standard was completed, the IEEE 802.15 working group had the following membership:

IEEE 802.15 Working group

Robert F. Heile, *Working Group Chair*

Rick Alfvén, *Working Group Vice-Chair*

Patrick Kinney, *Working Group Vice-Chair, Working Group Secretary*

James P. K. Gilb, *Working Group Technical Editor*

Benjamin A. Rolfe, *Working Group Treasurer*

James P. K. Gilb, *802.15.3m Chair, 802.15.3RevA Technical Editor*

Mohamed Abdallah
Keiji Akiyama
Hideki Aoyama
Arthur Astrin
Tuncer Baykas
Philip Beecher
Monique Brown
Kiran Bynam
Edgar Callaway
Chris Calvert
Radhakrishna Canchi
Jaesang Cha
Soo-Young Chang
Clint Chaplin
Stephen Chasko
Sangsung Choi
Hee-Sang Chung
Hendricus De Ruijter
Guido Dolmans
Igor Dotlic
Andrew Estrada
David Evans
Kiyoshi Fukui
Tim Godfrey
Yoshiho Goto
Jussi Haapola
Shinsuke Hara
Marco Hernandez
Ken Hiraga
Jay Holcomb
Koji Horisaki
Iwao Hosako
Bing Hui

Yeong Min Jang
Seong-Soon Joo
Volker Jungnickel
Jeritt Kent
Jaehwan Kim
Junhyeong Kim
Young-Hoon Kim
Youngsoo Kim
Shoichi Kitazawa
Tero Kivinen
Ryuji Kohno
Fumihide Kojima
Keitarou Kondou
Thomas Kuerner
Amarjeet Kumar
Byung-Jae Kwak
Namtuan Le
Hoosung Lee
Jae Seung Lee
Moon-Sik Lee
Myung Lee
Huan-Bang Li
Liang Li
Michael Lynch
Itaru Maekawa
Hiroyuki Matsumura
Kenichi Mori
Robert Moskowitz
Mohammad Nekoui
Chiu Ngo
Trang Nguyen
Paul Nikolich
Makoto Noda

John Notor
Hiroyo Ogawa
Mitsuaki Oshima
Chandrashekha P. S. Bhat
Glenn Parsons
Charles Perkins
Albert Petrick
Clinton Powell
Verotiana Rabarijaona
Demir Rakanovic
Ivan Reede
Richard Roberts
Noriyuki Sato
Norihiko Sekine
Nikola Serafimovski
Kunal Shah
Stephen Shellhammer
Shusaku Shimada
Gyung Chul Sihn
Gary Stuebing
Don Sturek
Mineo Takai
Kou Togashi
Kiyoshi Toshimitsu
Murat Uysal
Billy Verso
Brian Weis
Makoto Yaita
Peter Yee
Hidetoshi Yokota
Yu Zeng
Junwen Zhang
Chunhui Zhu

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

Tomoko Adachi	Noriyuki Ikeuchi	Satoshi Oyama
Thomas Alexander	Yasuhiko Inoue	Tomas Pajda
Richard Alfvén	Sergiu Iordanescu	Arumugam Paventhan
James D. Allen	Paul Isaacs	Dalibor Pokrajac
Nobumitsu Amachi	Akio Iso	Clinton Powell
Carol Ansley	Atsushi Ito	Venkatesha Prasad
Yusuke Asai	Adri Jovin	Demir Rakanovic
Alfred Asterjadhi	Shinkyō Kaku	R. K. Rannow
Gennaro Boggia	Piotr Karocki	James Reilly
Nancy Bravin	Jeritt Kent	Maximilian Riegel
William Byrd	Stuart Kerry	Robert Robinson
Radhakrishna Canchi	Yongbum Kim	Benjamin Rolfe
William Carney	Patrick Kinney	Naotaka Sato
Juan Carreon	Tero Kivinen	Frank Schewe
Yesenia Cevallos	Adrian Kliks	Reinhard Schrage
Minho Cheong	Yasushi Kudoh	Andy Scott
Peter Cibula	Thomas Kuerner	Michael Seaman
Charles Cook	Thomas Kurihara	Daniel Smolinski
Richard Doyle	Paul Lambert	Manikantan Srinivasan
Constantin Dumitrescu	Jeremy Landt	Dorothy Stanley
Sourav Dutta	Joseph Levy	Thomas Starai
Richard Edgar	Arthur H. Light	Eugene Stoudenmire
David Evans	William Lumpkins	Rene Struik
Liu Fangfang	Michael Lynch	Walter Struppler
Avraham Freedman	Elvis Maculuba	Mark Sturza
Yukihiro Fujimoto	Jeffery Maki	David Thompson
Yue Gao	Roger Marks	Pedro Tonhozi de Oliveira
Alexander Gelman	Jeffery Masters	Lorenzo Vangelista
James P. K. Gilb	Michael McInnis	Dmitri Varsanofiev
Eric W. Gray	Richard Mellitz	Prabodh Varshney
Randall Groves	Juichi Nakada	George Vlantis
Michael Gundlach	Nabil Nasser	Hung-Yu Wei
Robert F. Heile	Michael Newman	Andreas Wolf
Jerome Henry	Chiu Ngo	Chun Yu Charles Wong
Marco Hernandez	Nick S.A. Nikjoo	Oren Yuen
Werner Hoelzl	Makoto Noda	Zhen Zhou
Rita Horner	John Notor	

When the IEEE-SA Standards Board approved this standard on 15 May 2016, it had the following membership:

Jean-Philippe Faure, *Chair*
Ted Burse, *Vice-Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Chuck Adams	Ronald W. Hotchkiss	Mehmet Ulema
Masayuki Ariyoshi	Michael Janezic	Yingli Wen
Stephen Dukes	Joseph L. Koepfinger*	Howard Wolfman
Jianbin Fan	Hung Ling	Don Wright
J. Travis Griffith	Kevin Lu	Yu Yuan
Gary Hoffman	Annette D. Reilly	Daidi Zhong
	Gary Robinson	

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802.15.3-2016, IEEE Standard for High Data Rate Wireless Multi-Media Networks.

IEEE Std 802.15.3-2016 was originally developed to provide superior quality of service (QoS) over relatively medium range wireless links.

The idea of a high-rate addition to the IEEE 802.15 family of standards was first proposed in November 1999 at the IEEE Plenary meeting in Kaua'i, HI. The 802.15.3 task group began its official work at the March 2000 IEEE Plenary meeting in Albuquerque, NM, creating a criteria document and evaluation method. The down-selection of MAC and PHY proposals was completed at the November 2000 IEEE 802 Plenary meeting in Tampa, FL, and the writing of the draft began in December 2000. After working on the draft for one year, the document was ready for the task group ballot process in December 2001. The draft received final working group approval at the November 2002 IEEE Plenary meeting in Kaua'i, HI, and began the sponsor ballot process following the meeting. The draft went through one sponsor ballot and two recirculations before it was submitted to the IEEE Standards Association Standards Board (IEEE-SASB) for approval. The IEEE-SASB approved 802.15.3 as an IEEE standard in June 2003.

IEEE Std 802.15.3-2003 defined an ad-hoc MAC that enabled simple and fast network formation, excellent QoS, strong security with 128-bit AES encryption in CCM mode and methods to coexist with other wireless networks in the band. The PHY operated in the license exempt 2.4 GHz band with data rates of 11 Mb/s to 55 Mb/s at distances of greater than 70 m.

Interest in working on an amendment to fix and enhance IEEE Std 802.15.3 began in the September 2003 meeting in Singapore. A study group was formed at the November 2003 meeting in Albuquerque, which completed a project authorization request that was approved in March 2004. Work progressed quickly, and the first task group letter ballot was successfully completed in March 2005. After one recirculation, the draft began sponsor ballot in August 2005. The ballot was successful, and after a recirculation ballot to validate some minor changes, IEEE Std 802.15.3b was approved by the IEEE Standards Board on 6 December 2005, just over two years after the study group started.

IEEE Std 802.15.3b-2005 fixed mistakes and added enhancements that improve the efficiency of the base standard. Some of the key changes/additions in this amendment are as follows:

- An improved definition of the medium access control (MAC) layer management entity (MLME) service access point (SAP).
- A new acknowledgment (ACK) policy, implied-ACK, which allows polling and a more efficient use of channel time.
- A method for relinquishing time in a channel time allocation (CTA) to allow another device (DEV) time to transmit data.
- The ability to assign device identifiers (DEVIDs) to group addresses to allow multicast connections.
- Faster recovery of network operations when the piconet coordinator (PNC) abruptly disconnects with the conditional handover and the next PNC processes.
- Multiple contention periods during a superframe.

In the July 2003 meeting in San Francisco, an interest group was formed to consider a mmWave PHY for the existing standard. A study group was formally created in the March 2004 IEEE 802 plenary meeting in Orlando and developed a project authorization request that was approved in March 2005. The first meeting as a task group was in May 2005 in Cairns, Australia and the group worked steadily developing channel models and evaluation documents. The PHY modes were selected in November 2007 at the Atlanta meeting

and draft progressed rapidly, entering working group letter ballot in June 2008. After three working group recirculation ballots, sponsor ballot started in March 2009. A total of three sponsor recirculation ballots were held, leading to approval of IEEE Std 802.15.3c-2009 by the IEEE-SA Standards Board on 11 September 2009.

Some of the key features of IEEE Std 802.15.3c-2009 and additions are as follows:

- Operation in the 60 GHz band.
- New data rates, with the highest greater than 5 Gb/s.
- Beamforming negotiation for the transmitter to increase the communication range.
- MAC packet aggregation and the acknowledgment of individual subpackets to reduce retransmission overhead.

The PHY specifies three modes and one common mode. The three PHY modes are as follows:

- Single carrier (SC) mode optimized for low power and low complexity.
- High-speed interface (HSI) mode optimized for low-latency bidirectional data transfer.
- Audio/video (AV) mode optimized for the delivery of uncompressed, high-definition video and audio.

In 2015, there were two new projects that wanted to add additional optional PHYs. To support the development of these new amendments, the base standard needed to be revised to create a single document that incorporated the prior two amendments. A PAR was generated in July 2015 at the IEEE Plenary meeting in Waikoloa Village, HI. The PAR was approved by the IEEE SASB in September 2015 and the initial draft was completed soon thereafter (by the same Technical Editor who worked on the previous three documents). After two working group ballots, the sponsor ballot began in December 2015 and completed in February 2016 after two Sponsor ballot recirculations. IEEE Std 802.15.3-2016 was approved by the IEEE-SA Standards Board in May 2016.

Contents

1.	Overview.....	26
1.1	Scope.....	26
1.2	Purpose.....	26
2.	Normative references.....	27
3.	Definitions, acronyms, and abbreviations.....	28
3.1	Definitions	28
3.2	Acronyms and abbreviations	29
4.	General description	33
4.1	What is a piconet?.....	33
4.2	Components of an IEEE 802.15.3 piconet.....	33
4.3	Overview of medium access control (MAC) functionality	33
4.3.1	Coordination	34
4.3.1.1	Starting a piconet	34
4.3.1.2	Handing over control of the piconet	34
4.3.1.3	Creating a child piconet	34
4.3.1.4	Creating a neighbor piconet.....	35
4.3.2	Ending a piconet	35
4.3.3	Ending a piconet with a dependent piconet involved	35
4.3.4	Association and disassociation	36
4.3.5	Security overview	36
4.3.6	The IEEE 802.15.3 superframe	36
4.3.7	Channel time management	37
4.3.8	Data communications between DEVs	38
4.3.9	Information discovery in the piconet	38
4.3.10	Dynamic channel selection	39
4.3.11	Power management	39
4.3.12	Controlling transmit power in the piconet	40
4.3.13	Superframe structure using quasi-omni mode	40
4.3.14	Frame aggregation	41
4.3.15	Beam forming	41
4.3.16	Channel probing	41
4.3.17	Unequal error protection (UEP)	41
4.4	Characteristics of the 2.4 GHz PHY	41
4.4.1	General characteristics	41
4.4.2	Coexistence and interoperability	42
4.5	Characteristics of the mmWave PHY	42
4.5.1	mmWave PHY characteristics	42
4.5.2	Piconets using mmWave PHY modes	43
4.6	Conventions	44
4.7	Concept of primitives.....	44
5.	Layer management.....	46
5.1	Overview of management model.....	46
5.2	Generic management primitives	47
5.2.1	MLME-GET.request	48

5.2.2	MLME-GET.confirm	48
5.2.3	MLME-SET.request	48
5.2.4	MLME-SET.confirm	48
5.3	MLME SAP interface	49
5.3.1	Resetting the MAC/MLME	50
5.3.1.1	MLME-RESET.request	50
5.3.1.2	MLME-RESET.confirm	50
5.3.2	Scanning for piconets	51
5.3.2.1	MLME-SCAN.request	53
5.3.2.2	MLME-SCAN.confirm	53
5.3.2.3	MLME-SCAN.indication	54
5.3.3	Starting a piconet	54
5.3.3.1	MLME-START.request	55
5.3.3.2	MLME-START.confirm	55
5.3.4	Stopping a piconet	55
5.3.4.1	MLME-STOP.request	56
5.3.4.2	MLME-STOP.confirm	56
5.3.5	Associating with a piconet	57
5.3.5.1	MLME-ASSOCIATE.request	58
5.3.5.2	MLME-ASSOCIATE.confirm	58
5.3.5.3	MLME-ASSOCIATE.indication	58
5.3.6	Disassociation from a piconet	58
5.3.6.1	MLME-DISASSOCIATE.request	59
5.3.6.2	MLME-DISASSOCIATE.confirm	59
5.3.6.3	MLME-DISASSOCIATE.indication	60
5.3.7	Security management	60
5.3.7.1	MLME-MEMBERSHIP-UPDATE.request	62
5.3.7.2	MLME-MEMBERSHIP-UPDATE.confirm	62
5.3.7.3	MLME-SECURITY-ERROR.indication	62
5.3.7.4	MLME-SECURITY-MESSAGE.request	62
5.3.7.5	MLME-SECURITY-MESSAGE.confirm	63
5.3.7.6	MLME-SECURITY-MESSAGE.indication	63
5.3.8	PNC handover	63
5.3.8.1	MLME-PNC-HANDOVER.indication	63
5.3.8.2	MLME-PNC-HANDOVER.response	64
5.3.8.3	MLME-NEW-PNC.indication	64
5.3.9	Requesting DEV information from the PNC	64
5.3.9.1	MLME-DEV-INFO.request	65
5.3.9.2	MLME-DEV-INFO.confirm	65
5.3.9.3	MLME-DEV-INFO.indication	65
5.3.10	Security information retrieval	65
5.3.10.1	MLME-SECURITY-INFO.request	65
5.3.10.2	MLME-SECURITY-INFO.confirm	66
5.3.10.3	MLME-SECURITY-INFO.indication	67
5.3.10.4	MLME-SECURITY-INFO.response	67
5.3.11	Application specific data management	67
5.3.11.1	MLME-APPLICATION-SPECIFIC.request	68
5.3.11.2	MLME-APPLICATION-SPECIFIC.confirm	69
5.3.11.3	MLME-APPLICATION-SPECIFIC.indication	69
5.3.12	Piconet services management	69
5.3.12.1	MLME-ANNOUNCE-SERVICE.request	70
5.3.12.2	MLME-ANNOUNCE-SERVICE.confirm	70
5.3.12.3	MLME-PICONET-SERVICES.request	71
5.3.12.4	MLME-PICONET-SERVICES.confirm	71

5.3.12.5	MLME-PICONET-SERVICES.indication	71
5.3.13	Stream management	71
5.3.13.1	MLME-CREATE-STREAM.request	73
5.3.13.2	MLME-CREATE-STREAM.confirm	74
5.3.13.3	MLME-CREATE-STREAM.indication	74
5.3.13.4	MLME-MODIFY-STREAM.request	74
5.3.13.5	MLME-MODIFY-STREAM.confirm	75
5.3.13.6	MLME-TERMINATE-STREAM.request	75
5.3.13.7	MLME-TERMINATE-STREAM.confirm	75
5.3.13.8	MLME-TERMINATE-STREAM.indication	75
5.3.14	Piconet parameter management	76
5.3.14.1	MLME-BSID-CHANGE.request	76
5.3.14.2	MLME-BSID-CHANGE.confirm	76
5.3.14.3	MLME-PICONET-PARM-CHANGE.indication	77
5.3.15	Power management	77
5.3.15.1	MLME-PS-SET-INFORMATION.request	79
5.3.15.2	MLME-PS-SET-INFORMATION.confirm	79
5.3.15.3	MLME-SPS-CONFIGURE.request	79
5.3.15.4	MLME-SPS-CONFIGURE.confirm	80
5.3.15.5	MLME-PM-MODE-CHANGE.request	80
5.3.15.6	MLME-PM-MODE-CHANGE.confirm	80
5.3.15.7	MLME-PM-MODE-CHANGE.indication	80
5.3.15.8	MLME-MONITOR-PM-MODE.request	81
5.3.15.9	MLME-MONITOR-PM-MODE.confirm	81
5.3.15.10	MLME-MONITOR-PM-MODE.indication	81
5.3.16	Multicast operations	82
5.3.16.1	MLME-MULTICAST-CONFIGURATION.request	83
5.3.16.2	MLME-MULTICAST-CONFIGURATION.confirm	83
5.3.16.3	MLME-MULTICAST-RX-SETUP.request	83
5.3.16.4	MLME-MULTICAST-RX-SETUP.confirm	84
5.3.17	Timing synchronization	84
5.3.17.1	MLME-BEACON-EVENT.request	84
5.3.17.2	MLME-BEACON-EVENT.confirm	84
5.3.17.3	MLME-BEACON-EVENT.indication	85
5.3.18	Transmit switched diversity (TSD)	85
5.3.18.1	MLME-TXDIV.request	85
5.3.18.2	MLME-TXDIV.confirm	86
5.4	MAC management	86
5.4.1	MAC PIB PNC group	86
5.4.2	MAC PIB characteristic group	87
5.5	MAC SAP	88
5.5.1	MAC-ASYNC-DATA.request	91
5.5.2	MAC-ASYNC-DATA.confirm	91
5.5.3	MAC-ASYNC-DATA.indication	91
5.5.4	MAC-ISOCH-DATA.request	92
5.5.5	MAC-ISOCH-DATA.confirm	92
5.5.6	MAC-ISOCH-DATA.indication	93
6.	MAC frame formats	94
6.1	Frame format conventions	94
6.2	General frame format	95
6.2.1	Frame Control field	96
6.2.1.1	Protocol Version field	96

6.2.1.2	Frame Type field.....	97
6.2.1.3	SEC field.....	97
6.2.1.4	ACK Policy field, Imp-ACK Request field, and Blk-ACK field	97
6.2.1.5	Retry field	97
6.2.1.6	More Data field.....	98
6.2.1.7	Imp-ACK Negative Acknowledgment (NAK) field.....	98
6.2.1.8	CTA Relinquish field.....	98
6.2.2	Piconet ID (PNID) field	99
6.2.3	SrcID and DestID fields	99
6.2.4	Fragmentation Control field	99
6.2.4.1	MSDU Number field	99
6.2.4.2	Fragment Number field.....	100
6.2.4.3	Last Fragment Number field.....	100
6.2.5	Stream Index field	100
6.2.6	MAC header validation	100
6.2.7	MAC Frame Body field	101
6.2.7.1	Frame Payload field.....	101
6.2.7.2	Secure session ID (SECID) field	101
6.2.7.3	Secure Frame Counter (SFC) field	101
6.2.7.4	Secure Payload field	101
6.2.7.5	Integrity Code field.....	101
6.2.7.6	Frame Check Sequence (FCS) field.....	101
6.2.8	SC and HSI aggregated frame format	102
6.2.8.1	Standard aggregation format.....	102
6.2.8.1.1	Non-secure standard aggregation format.....	102
6.2.8.1.2	Secure standard aggregation format	105
6.2.8.2	Low-latency aggregation formats	105
6.2.8.2.1	Non-secure low-latency aggregation format.....	105
6.2.8.2.2	Secure low-latency aggregation format	108
6.2.9	AV aggregated frame format	109
6.2.9.1	Extended MAC header format.....	109
6.2.9.1.1	Extended Control Header field	110
6.2.9.1.2	MAC Extension Header field	111
6.2.9.1.3	Security Header field	112
6.2.9.1.4	Video Header field.....	112
6.2.9.2	Subframe format	113
6.2.9.3	AV aggregated	115
6.2.9.4	Regular.....	115
6.2.9.5	Directional ACK.....	116
6.3	Format of individual frame types.....	116
6.3.1	Beacon frame	116
6.3.1.1	Non-secure Beacon frame.....	116
6.3.1.2	Secure Beacon frame	118
6.3.2	Acknowledgment frames	119
6.3.2.1	Imm-ACK frame.....	119
6.3.2.2	Delayed ACK (Dly-ACK) frame	120
6.3.3	Command frame	121
6.3.3.1	Non-secure Command frame.....	121
6.3.3.2	Secure Command frame.....	122
6.3.4	Data frame	123
6.3.4.1	Non-secure Data frame	123
6.3.4.2	Secure Data frame.....	123
6.3.5	Multi-protocol Data frame	124
6.3.5.1	Non-secure Multi-protocol Data frame.....	124

6.3.5.2	Secure Multi-protocol Data frame	125
6.3.6	Sync frame	125
6.4	Information elements (IEs)	126
6.4.1	CTA IE	128
6.4.2	BSID IE	129
6.4.3	Parent Piconet IE	129
6.4.4	DEV Association IE	129
6.4.5	PNC shutdown IE	130
6.4.6	Piconet Parameter Change IE	131
6.4.7	AS IE	132
6.4.8	Pending channel time map (PCTM) IE	132
6.4.9	PNC Handover IE	133
6.4.10	CTA Status IE	133
6.4.11	Capability IE	134
6.4.12	Transmit Power Parameters IE	140
6.4.13	PS Status IE	141
6.4.14	CWB IE	141
6.4.15	Overlapping PNID IE	142
6.4.16	Piconet Services IE	142
6.4.17	Vendor Defined IE	143
6.4.18	Group ID IE	143
6.4.19	Stream Renew IE	144
6.4.20	Next PNC IE	144
6.4.21	Piconet Channel Status IE	144
6.4.22	Synchronization IE	145
6.4.23	TSD IE	147
6.4.24	UEP Specific IE	148
6.4.25	IFS IE	148
6.4.26	CTA Relinquish Duration IE	149
6.4.27	Feedback IE	149
6.4.28	Mapping IE	151
6.4.29	BST Clustering IE	152
6.4.30	PET Clustering IE	152
6.4.31	Beam PET IE	153
6.4.32	HRS Beam PET IE	154
6.4.33	PET Amplitude IE	155
6.4.34	PET Phase IE	155
6.4.35	Sync Frame Frequency IE	156
6.4.36	Directional Peer IE	156
6.5	MAC commands	157
6.5.1	Association and disassociation commands	159
6.5.1.1	Association Request command	159
6.5.1.2	Association Response command	160
6.5.1.3	Disassociation Request command	161
6.5.2	Security commands	161
6.5.2.1	Request Key command	161
6.5.2.2	Request Key Response command	161
6.5.2.3	Distribute Key Request command	162
6.5.2.4	Distribute Key Response command	162
6.5.3	PNC handover commands	162
6.5.3.1	PNC Handover Request command	163
6.5.3.2	PNC Handover Response command	163
6.5.3.3	PNC Handover Information command	164
6.5.4	Information request commands	164

6.5.4.1	PNC Information Request command	164
6.5.4.2	PNC Information command	164
6.5.4.3	Security Information Request command	166
6.5.4.4	Security Information command	166
6.5.4.5	Probe Request command	167
6.5.4.6	Probe Response command	169
6.5.5	Information announcement commands	171
6.5.5.1	Piconet Services command	171
6.5.5.2	Announce command	171
6.5.5.3	Announce Response command	173
6.5.6	Channel time allocation request, modification, and termination commands	173
6.5.6.1	Channel Time Request command	173
6.5.6.2	Channel Time Response command	176
6.5.7	Channel status commands	177
6.5.7.1	Channel Status Request command	177
6.5.7.2	Channel status response	177
6.5.7.3	Remote Scan Request command	178
6.5.7.4	Remote Scan Response command	178
6.5.7.5	Transmit Power Change command	180
6.5.8	Power management commands	180
6.5.8.1	PS Set Information Request command	180
6.5.8.2	PS Set Information Response command	180
6.5.8.3	SPS Configuration Request command	181
6.5.8.4	SPS Configuration Response command	182
6.5.8.5	PM Mode Change command	183
6.5.8.6	PM Mode Change Response command	183
6.5.9	Special commands	184
6.5.9.1	Security Message command	184
6.5.9.2	Vendor Defined command	184
6.5.9.3	AS IE Request command	185
6.5.9.4	AS IE Response command	185
6.5.10	Multicast configuration commands	186
6.5.10.1	Multicast Configuration Request command	186
6.5.10.2	Multicast Configuration Response command	186
7.	MAC functional description	187
7.1	Introduction	187
7.2	Starting, maintaining, and stopping piconets	188
7.2.1	Scanning through channels	188
7.2.2	Starting a piconet	189
7.2.3	PNC handover	190
7.2.4	Preliminary handover	193
7.2.5	Next PNC	194
7.2.6	Dependent PNC handover	195
7.2.7	Child piconet	198
7.2.8	Neighbor piconet	200
7.2.9	Stopping piconet operations	202
7.2.9.1	Stopping an independent or parent piconet	203
7.2.9.2	Parent PNC stopping a dependent piconet	203
7.2.9.3	Dependent PNC termination of a dependent piconet	204
7.2.10	Non-PNC-capable DEVs	204
7.3	Association and disassociation with a piconet	204
7.3.1	Association	204

7.3.2	Piconet services	206
7.3.3	Broadcasting piconet information	208
7.3.4	Disassociation	209
7.4	Channel access.....	210
7.4.1	Interframe space (IFS)	211
7.4.2	Carrier sense multiple access with collision avoidance (CSMA/CA)	211
7.4.3	Channel time allocation period channel access	213
7.4.3.1	Channel time allocations (CTAs)	213
7.4.3.2	Channel time allocation (CTA) and channel time usage	215
7.4.3.3	Management CTAs	216
7.4.3.4	Slotted aloha access	216
7.4.3.5	Allocation of MCTAs	217
7.4.3.6	Guard time	217
7.4.3.7	Calculating channel time requests	219
7.4.3.8	Relinquishing CTA time to another DEV.....	220
7.5	Channel time management.....	222
7.5.1	Isochronous stream management	222
7.5.1.1	Isochronous stream creation	223
7.5.1.2	Isochronous stream modification	226
7.5.1.3	Isochronous stream termination.....	229
7.5.2	Asynchronous channel time reservation and termination	231
7.5.2.1	Asynchronous channel time reservation	231
7.5.2.2	Asynchronous channel time termination	233
7.5.3	Multicast group configuration	234
7.6	Synchronization	235
7.6.1	Time accuracy	236
7.6.2	Beacon generation	236
7.6.3	Beacon reception	237
7.6.4	Beacon information announcement	237
7.6.5	Superframe support for directional PHYs	238
7.6.5.1	Quasi-omni beacon	239
7.6.5.2	Directional CAP.....	240
7.6.5.3	Directional association.....	241
7.6.5.4	DEV quasi-omni transmit direction training and tracking.....	242
7.7	Fragmentation and defragmentation	243
7.8	Aggregation	244
7.8.1	Standard aggregation	244
7.8.2	Low-latency aggregation	245
7.9	Acknowledgment and retransmission.....	246
7.9.1	No acknowledgment (no-ACK)	246
7.9.2	Immediate acknowledgment (Imm-ACK)	246
7.9.3	Delayed acknowledgment (Dly-ACK)	247
7.9.4	Implied acknowledgment (Imp-ACK)	248
7.9.5	Block acknowledgment (Blk-ACK)	250
7.9.5.1	Blk-ACK for standard aggregation.....	250
7.9.5.2	Blk-ACK for low-latency aggregation	251
7.9.6	Retransmissions	252
7.9.7	Duplicate detection	252
7.10	Peer discovery.....	252
7.10.1	PNC information request	252
7.10.2	Probe request and response	253
7.10.3	Announce	254
7.10.4	Channel status request	254
7.10.5	Remote scan	254

7.10.6	PNC channel scanning	255
7.10.7	Channel probing	255
7.11	Changing piconet parameters.....	256
7.11.1	Moving beacon	256
7.11.2	Changing superframe duration	256
7.11.3	Setting the PNID or BSID	257
7.11.4	Maintaining synchronization in dependent piconets	258
7.12	Interference mitigation.....	258
7.12.1	Dynamic channel selection	259
7.12.2	Transmit power control	260
7.12.2.1	Maximum transmitter power for the CAP, beacon, and directed MCTAs ..	260
7.12.2.2	Adjustable transmitter power in a CTA	261
7.13	Multi-rate support	261
7.14	Power management.....	262
7.14.1	Piconet synchronized power save (PSPS) mode	263
7.14.2	Device synchronized power save (DSPS) mode	264
7.14.2.1	Creation, use, and management of DSPS sets	264
7.14.2.2	Changing DSPS mode and operation.....	265
7.14.2.3	CTA timing in DSPS mode	266
7.14.3	Asynchronous power save (APS) mode	268
7.14.4	MSCs for power save modes	269
7.15	AS IE operation	272
7.16	MAC sublayer parameters	275
7.17	Unequal error protection (UEP).....	278
7.18	Sync frame transmission and virtually dependent piconet	278
8.	Security	280
8.1	Security mechanisms	280
8.1.1	Security membership and key establishment	280
8.1.2	Key transport	280
8.1.3	Data encryption	280
8.1.4	Data integrity	280
8.1.5	Beacon integrity protection	280
8.1.6	Command integrity protection	281
8.1.7	Freshness protection	281
8.2	Security modes.....	281
8.2.1	Security mode 0	281
8.2.2	Security mode 1	281
8.3	Security support	281
8.3.1	PNC handover	281
8.3.2	Changes in the piconet group data key	282
8.3.3	Joining a secure piconet	282
8.3.4	Membership update	282
8.3.5	Secure frame generation	283
8.3.6	Updating CurrentTimeToken	284
8.3.7	Secure frame reception	284
8.3.8	Selecting the SECID for a new key	285
8.3.9	Key selection	285
8.4	Protocol details	289
8.4.1	Security information request and distribution	289
8.4.2	Key distribution protocol	291
8.4.3	Key request protocol	291

9.	Security specifications	292
9.1	Modes for security	292
9.2	Symmetric cryptography building blocks	292
9.2.1	Notational conventions	292
9.2.2	CCM combined encryption and data authentication	292
9.2.3	CCM parameters	292
9.2.4	Nonce value	292
9.2.5	AES encryption	293
9.3	Symmetric cryptography implementation	293
9.3.1	Symmetric cryptography data formats	293
9.3.2	Symmetric cryptographic operations	293
9.4	CCM mode.....	295
9.4.1	Inputs	295
9.4.2	Data authentication	296
9.4.3	Encryption	298
9.4.4	Output	298
9.4.5	Decryption	299
9.4.6	Restrictions	299
9.4.7	List of symbols	299
10.	PHY specification for the 2.4 GHz band	301
10.1	Overview of the 2.4 GHz PHY	301
10.2	General requirements	302
10.2.1	Operating frequency range	302
10.2.2	Radio frequency (RF) power measurements	302
10.2.3	Channel assignments	302
10.2.4	Scanning channels	302
10.2.5	Unwanted emissions	303
10.2.6	Operating temperature range	303
10.2.7	PHY layer timing	303
10.2.7.1	Interframe space.....	303
10.2.7.2	Receive-to-transmit turnaround time	303
10.2.7.3	Transmit-to-receive turnaround time	304
10.2.7.4	Time between successive transmissions	304
10.2.7.5	Channel switch time.....	304
10.2.8	Data size restrictions	304
10.2.8.1	Maximum frame length	304
10.2.8.2	Maximum transfer unit size	304
10.2.8.3	Minimum fragment size.....	304
10.2.9	Header check sequence	304
10.2.10	Channel access methods	306
10.3	Modulation and coding	306
10.3.1	Base data rate	307
10.3.2	Signal constellations	307
10.3.3	DQPSK modulation	308
10.3.4	QPSK and 16/32/64-QAM with trellis coding	309
10.4	PHY frame format	316
10.4.1	Frame format	316
10.4.2	PHY preamble	317
10.4.3	Header modulation	319
10.4.4	Scrambling	319
10.4.5	PHY header	321

10.4.6	Stuff bits	322
10.4.7	Tail symbols	322
10.5	Transmitter specifications	325
10.5.1	Error vector magnitude definition	325
10.5.2	EVM calculated values	326
10.5.3	Transmit power spectral density (PSD) mask	326
10.5.4	Transmit center frequency tolerance	326
10.5.5	Symbol rate	326
10.5.6	Clock synchronization	327
10.5.7	Transmit power-on and power-down ramp	327
10.5.8	RF carrier suppression	327
10.5.9	Transmit power	327
10.6	Receiver specifications	328
10.6.1	Error rate criterion	328
10.6.2	Receiver sensitivity	328
10.6.3	Receiver maximum input level	329
10.6.4	Receiver jamming resistance	329
10.6.5	Receiver CCA performance	330
10.6.6	Receiver RSSI	330
10.6.7	Link quality indication	330
10.7	PHY management	330
11.	PHY specification for millimeter wave	333
11.1	General requirements	333
11.1.1	Regulatory information	333
11.1.2	RF power measurements	334
11.1.3	Unwanted emissions	334
11.1.4	Operating temperature range	334
11.1.5	RF channelization	334
11.1.6	Transmit PSD mask	334
11.1.7	Error vector magnitude calculation	334
11.1.7.1	SC PHY	334
11.1.7.2	AV and HSI PHYs	335
11.1.8	Common PHY management for mmWave PHY modes	336
11.1.8.1	Supported MCSs	336
11.1.8.2	Preferred fragment size	336
11.1.8.3	Receive Status field	337
11.1.9	Requirements for mmWave PNCs	338
11.1.10	CP operation	338
11.1.11	mmWave PHY mode usage in CTA	339
11.1.12	Common mode signaling (CMS)	339
11.1.12.1	Forward error correction for CMS	340
11.1.12.2	Code spreading for CMS	340
11.1.12.3	Scrambling for CMS	340
11.1.12.4	PHY preamble for CMS	341
11.1.12.5	Frame header for CMS	341
11.1.12.6	PHY header for CMS	342
11.1.12.7	PHY Payload field for CMS	343
11.1.12.8	Receiver clear channel assessment performance for CMS	343
11.1.13	mmWave PHY PIB	343
11.2	Single Carrier Mode of mmWave PHY	344
11.2.1	PHY operating specifications of SC PHY	345
11.2.1.1	Channelization	345

11.2.1.2	Scanning channels.....	345
11.2.2	Modulation, forward error correction, and spreading	345
11.2.2.1	MCS-dependent parameters.....	345
11.2.2.2	Header rate-dependent parameters.....	347
11.2.2.3	Timing-related parameters.....	348
11.2.2.4	Frame-related parameters	348
11.2.2.5	Modulation.....	349
11.2.2.5.1	p/2 BPSK	349
11.2.2.5.2	p/2 QPSK	349
11.2.2.5.3	p/2 8-PSK.....	350
11.2.2.5.4	p/2 16-QAM.....	351
11.2.2.6	FEC	351
11.2.2.6.1	Reed-Solomon block codes in GF(28).....	351
11.2.2.6.2	Irregular LDPC codes	352
11.2.2.6.3	Rate 14/15 LDPC code	353
11.2.2.7	Stuff bits.....	353
11.2.2.8	Code spreading	356
11.2.2.8.1	Golay sequences	356
11.2.2.8.2	PRBS generation with LFSR	356
11.2.2.9	Unequal error protection.....	357
11.2.2.10	Scrambling	358
11.2.3	SC PHY frame format	359
11.2.3.1	PHY preamble.....	360
11.2.3.1.1	Sync field	360
11.2.3.1.2	SFD field.....	360
11.2.3.1.3	Channel estimation sequence (CES).....	360
11.2.3.2	Frame header.....	360
11.2.3.2.1	SC PHY header.....	362
11.2.3.2.2	Base header HCS	363
11.2.3.2.3	Base header FEC.....	363
11.2.3.2.4	MAC subheader HCS	363
11.2.3.2.5	MAC subheader FEC.....	364
11.2.3.3	SC PHY Payload field	364
11.2.3.3.1	SC PHY Payload scrambling.....	364
11.2.3.3.2	Modulation.....	364
11.2.3.3.3	FEC	364
11.2.3.3.4	Code spreading	364
11.2.3.4	Pilot word and PCES	365
11.2.3.4.1	Subblocks and pilot word	365
11.2.3.4.2	Pilot channel estimation sequence (PCES).....	365
11.2.4	Transmitter specifications	366
11.2.4.1	Error vector magnitude	366
11.2.4.2	Transmit center frequency tolerance.....	366
11.2.4.3	Symbol rate	366
11.2.4.4	Transmit power-on and power-down ramp	366
11.2.5	Receiver specifications	366
11.2.5.1	Error rate criterion	366
11.2.5.2	Receiver sensitivity.....	367
11.2.5.3	Receiver maximum input level.....	367
11.2.5.4	Receiver clear channel assessment performance	367
11.2.6	PHY layer timing	368
11.2.6.1	Interframe space.....	368
11.2.6.2	Receive-to-transmit turnaround time.....	368
11.2.6.3	Transmit-to-receive turnaround-time.....	368

11.2.6.4	Time between successive transmissions	368
11.2.6.5	Channel switch.....	369
11.2.7	PHY management for SC PHY	369
11.2.7.1	Maximum frame size	369
11.2.7.2	Maximum transfer unit size	369
11.2.7.3	Minimum fragment size.....	369
11.2.8	Optional OOK/DAMI modes	369
11.2.8.1	OOK.....	369
11.2.8.2	DAMI.....	370
11.2.8.3	FEC	370
11.2.8.4	OOK/DAMI spreading	370
11.3	High Speed Interface mode of mmWave PHY	370
11.3.1	General operating specifications	370
11.3.1.1	Operating frequency bands	370
11.3.2	HSI PHY modulation, forward error correction, and spreading	370
11.3.2.1	MCS-dependent parameters.....	370
11.3.2.2	HSI PHY timing-related parameters.....	372
11.3.2.3	HSI PHY frame-related parameters.....	373
11.3.2.4	HSI PHY FEC.....	373
11.3.2.4.1	LDPC block code.....	374
11.3.2.4.2	EEP data multiplexer	374
11.3.2.4.3	UEP data multiplexer.....	374
11.3.2.4.4	Bit interleaver	375
11.3.2.5	Stuff bits.....	376
11.3.2.6	Constellation mapping	376
11.3.2.7	HSI spreader	378
11.3.2.7.1	Spreader for spreading factor of 1	379
11.3.2.7.2	Spreader for spreading factor of 48	379
11.3.2.8	Tone interleaver	379
11.3.2.9	HSI PHY OFDM modulator	380
11.3.2.9.1	Pilot subcarriers	381
11.3.2.9.2	Guard subcarriers.....	382
11.3.2.10	PCES insertion.....	382
11.3.2.11	HSI PHY scrambling	382
11.3.3	HSI PHY frame format	383
11.3.3.1	PHY preamble.....	383
11.3.3.2	Frame header.....	384
11.3.3.3	HSI PHY header	386
11.3.3.4	Header check sequences	387
11.3.3.4.1	Main Header HCS.....	387
11.3.3.4.2	MAC Subheader HCS.....	387
11.3.3.5	PHY Payload field	388
11.3.4	Transmitter specifications	388
11.3.4.1	EVM requirement	388
11.3.4.2	Chip rate and clock alignment	389
11.3.5	Receiver specifications	389
11.3.5.1	Receiver sensitivity.....	389
11.3.5.2	Receiver CCA performance.....	389
11.3.5.3	Receiver maximum input level.....	389
11.3.5.4	PHY layer timing	389
11.3.5.5	Interframe spacing	389
11.3.5.6	Receive-to-transmit turnaround time.....	390
11.3.5.7	Transmit-to-receive turnaround time.....	390
11.3.5.8	Time between successive transmissions.....	390

11.3.5.9	Channel switch time.....	390
11.3.6	HSI PHY management	390
11.3.6.1	PHY supported data rate encoding	390
11.3.6.2	HSI PHY fragment size encoding.....	390
11.3.6.3	Maximum frame length	391
11.3.6.4	Maximum transfer unit size	391
11.3.6.5	Minimum fragment size.....	391
11.4	Audio/Visual mode of mmWave PHY	391
11.4.1	General requirements	392
11.4.1.1	AV PHY channelization	392
11.4.1.2	PHY layer timing	393
11.4.1.2.1	Interframe space.....	393
11.4.1.2.2	Receive-to-transmit turnaround time	394
11.4.1.2.3	Transmit-to-receive turnaround time	394
11.4.1.2.4	Time between successive transmissions	394
11.4.1.2.5	Channel switch time.....	394
11.4.1.2.6	CCA detect time.....	394
11.4.1.3	Data size restrictions	394
11.4.1.3.1	Maximum frame length	394
11.4.1.3.2	Maximum transfer unit size	395
11.4.1.3.3	Minimum fragment size.....	395
11.4.1.4	Header check sequence	395
11.4.2	AV PHY modulation and forward error correction	395
11.4.2.1	AV PHY base rate.....	396
11.4.2.2	Repetition coding and spatial diversity	397
11.4.2.3	Stuff bits.....	397
11.4.2.4	HRP splitter and scrambler	398
11.4.2.5	LRP scrambler	398
11.4.2.6	HRP outer code	399
11.4.2.7	HRP outer interleaver	399
11.4.2.8	Convolutional encoder	400
11.4.2.9	Puncturing.....	400
11.4.2.10	HRP data multiplexer and bit interleaver	400
11.4.2.10.1	EEP data multiplexer	401
11.4.2.10.2	UEP coding data multiplexer.....	402
11.4.2.10.3	UEP mapping data multiplexer.....	404
11.4.2.10.4	HRP header data multiplexer.....	405
11.4.2.11	Bit reversal tone interleaver	406
11.4.2.12	Signal constellations	406
11.4.2.13	AV PHY non-data subcarriers	407
11.4.2.14	AV PHY OFDM modulation	408
11.4.3	AV PHY frame formats	409
11.4.3.1	HRP preamble.....	410
11.4.3.2	HRP header	411
11.4.3.3	LRP preamble sequences	411
11.4.3.4	Long omni LRP preamble.....	412
11.4.3.5	Short omni LRP preamble	413
11.4.3.6	Omni LRP header	414
11.4.3.7	Directional LRP preamble	414
11.4.3.8	Directional LRP header and payload	415
11.4.4	AV PHY transmitter requirements	416
11.4.4.1	TX mask.....	416
11.4.4.2	EVM requirement	417
11.4.4.3	Symbol timing.....	417

11.4.4.4	TX frequency accuracy	418
11.4.4.5	TX power ramp on and off	418
11.4.5	AV PHY Receiver characteristics	418
11.4.5.1	Error rate criterion	418
11.4.5.2	Sensitivity	418
11.4.5.3	Maximum input level.....	418
11.4.6	Preambles and training symbols	418
12.	Beam forming	423
12.1	Introduction.....	423
12.2	Beam forming terminology.....	423
12.2.1	Quasi-omni patterns	424
12.2.2	Sectors	424
12.2.3	Beams	425
12.2.4	Clusters	426
12.3	Beam forming codebooks	427
12.3.1	Beam forming codebooks	428
12.4	Beam forming reference model	429
12.5	Beam forming protocol.....	431
12.5.1	Two-level training mechanism	431
12.5.1.1	Sector-level training.....	431
12.5.1.1.1	AAS sector-level training	431
12.5.1.1.2	SAS sector-level training.....	434
12.5.1.1.3	Sector-level training failure remedy	437
12.5.1.2	Beam-level training.....	437
12.5.1.2.1	AAS beam-level training	437
12.5.1.2.2	SAS beam-level training.....	440
12.5.2	Beam tracking	443
12.6	On-demand beam forming	445
12.7	Proactive beam forming.....	445
12.8	TSD.....	445
Annex A (informative)	Bibliography	447
Annex B (normative)	Frame convergence sublayer	448
B.1	Generic convergence sublayer	448
B.2	EPD FCSL PDU classification	449
B.3	EPD FCSL	449
B.3.1	EPD FCSL QoS support	450
B.3.2	Data entity inter-relationships.....	450
B.4	EPD FCSL SAP.....	451
B.4.1	MA-UNITDATA.request	452
B.4.2	MA-UNITDATA.indication	452
B.4.3	MA-UNITDATA-STATUS.indication.....	453
B.5	Stream SAP.....	454
B.5.1	Stream creation, modification, and deletion	454
B.5.1.1	STREAM_INITIATE.request.....	456
B.5.1.2	STREAM_INITIATE.confirm.....	456
B.5.1.3	STREAM_INITIATE.indication	456
B.5.1.4	STREAM_MODIFY.request	457
B.5.1.5	STREAM_MODIFY.confirm.....	457
B.5.1.6	STREAM_END.request.....	457

B.5.1.7	STREAM_END.confirm	458
B.5.1.8	STREAM_END.indication	458
B.5.2	Stream data interface	458
B.5.2.1	STREAM_DATA.request	459
B.5.2.2	STREAM_DATA.confirm	460
B.5.2.3	STREAM_DATA.indication	460
Annex C (informative)	Security considerations	461
C.1	Background assumptions	461
C.1.1	Physical assumptions	461
C.1.2	Network assumptions	461
C.1.3	Attack model assumptions	462
C.1.4	Security key lifecycle issues	462
C.1.4.1	Key lifecycle	462
C.1.4.2	Membership lifecycle	462
C.1.4.3	Group membership change rekey	462
C.2	Claimed security services	462
C.2.1	Beacon protection protocol	462
C.2.2	Distribute key protocol	463
C.2.3	Key request protocol	463
C.2.4	Data protection protocol	464
C.3	Properties of the IEEE 802.15.3 security suite	464
C.3.1	Key usage	464
C.3.2	Replay prevention	464
Annex D (informative)	Coexistence, interoperability, and interference	466
D.1	Interoperability	466
D.1.1	Interoperability with IEEE 802.11 DSSS and IEEE 802.11b	466
D.1.2	IEEE 802.11 FHSS and IEEE 802.15.1	467
D.2	Coexistence	467
D.2.1	Coexistence with IEEE Std 802.11b	467
D.2.1.1	Passive scanning	468
D.2.1.2	Dynamic channel selection	468
D.2.1.3	The ability to request channel quality information	468
D.2.1.4	Link quality and RSSI	468
D.2.1.5	Channel plan that minimizes channel overlap	468
D.2.1.6	Lower transmit power	469
D.2.1.7	Transmit power control	469
D.2.1.8	Neighbor piconet capability	469
D.2.2	Coexistence with IEEE 802.15.1 and IEEE 802.11 FHSS	470
D.2.2.1	PHY collaborative coexistence enhancements	470
D.2.2.2	MAC coexistence via collaboration	470
D.2.2.3	Other techniques	471
D.3	Coexistence performance	471
D.3.1	Allowed operation	471
D.3.2	Assumptions for coexistence calculations	471
D.3.3	Performance impact on IEEE 802.15.3 piconets	473
D.3.3.1	IEEE 802.11b overlapping with IEEE 802.15.3	473
D.3.3.2	IEEE 802.15.1 and IEEE 802.11 FHSS overlapping with IEEE 802.15.3	476
D.4	Notes on the calculations	477

Annex E (normative) Protocol implementation conformance statement (PICS) proforma.....	478
E.1 Introduction.....	478
E.1.1 Scope.....	478
E.1.2 Purpose.....	478
E.2 Abbreviations and special symbols.....	478
E.3 Instructions for completing the PICS proforma.....	479
E.4 Identification of the implementation.....	479
E.5 Identification of the protocol	480
E.6 Global statement of conformance	481
E.7 PICS proforma—IEEE Std 802.15.3-2016.....	481
E.7.1 Major roles for IEEE 802.15.3 DEVs.....	481
E.7.2 PHY functions.....	482
E.7.3 Major capabilities for the MAC sublayer	483
E.7.3.1 MAC frames	483
E.7.3.2 MAC sublayer functions	486
E.7.4 Security support	490
Annex F (informative) Implementation considerations.....	491
F.1 Channel time requests.....	491
F.1.1 Types of CTAs.....	491
F.1.2 Interpretation of channel time requests.....	492
F.1.3 Determining CTA Rate Factor from stream requirements	493
F.1.3.1 Example 1.....	494
F.1.3.2 Example 2.....	495
F.1.4 PNC interpretation of CTA rate factor	495
F.1.5 Creating channel time requests from MLME requests	496
F.1.6 Interpreting channel time requests	498
F.2 Sample frames.....	500
F.3 Use of multiple mmWave PHYs in a single piconet	502
Annex G (normative) Optional OOK/DAMI modes	504
G.1 Introduction.....	504
G.2 Child piconet operation.....	504
G.3 DAMI.....	504
G.4 PHY preamble.....	506
G.5 PHY frame format	507
G.6 Interframe space.....	507
G.7 Eye opening for OOK.....	508
G.8 EVM for DAMI	508

IEEE Standard for High Data Rate Wireless Multi-Media Networks

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

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

1. Overview

1.1 Scope

This standard defines PHY and MAC specifications for high data rate wireless connectivity (typically over 200 Mbps) with fixed, portable, and moving devices. Data rates are high enough to satisfy a set of consumer multimedia industry needs, as well as to support emerging wireless switched point-to-point and high rate close proximity point-to-point applications.

1.2 Purpose

The purpose of this standard is to provide for low complexity, low cost, low power consumption, and high data rate wireless connectivity among devices that support a variety of applications such as a set of consumer multimedia industry needs, wireless switched point-to-point applications in data centers, wireless backhaul/fronthaul intra-device communications, and a wide variety of additional use cases such as rapid large multimedia data downloads and file exchanges between two devices in close proximity, including between mobile devices and stationary devices (kiosks, ticket gates, etc.), and/or wireless data storage devices.

2. Normative references

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

ANSI X3.66-1979: Advanced data communication control procedures (ADCCP).¹

IEEE Std 802[®]-2014, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.^{2, 3}

ISO/IEC 646:1991, Information Technology—ISO 7-bit coded character set for information interchange.⁴

NIST FIPS Pub 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/N.I.S.T., November 26, 2001.⁵

¹ ANSI publications are available from the American National Standards Institute (<http://www.ansi.org>).

² IEEE publications are available from the Institute of Electrical and Electronics Engineers (<http://standards.ieee.org/>).

³ The IEEE standards referred to in Clause 2 are trademarks belonging to the Institute of Electrical and Electronics Engineers, Inc.

⁴ ISO/IEC publications are available from the International Organization for Standardization (<http://www.iso.ch/>) and the International Electrotechnical Commission (<http://www.iec.ch/>). ISO/IEC publications are also available in the United States from the American National Standards Institute (<http://www.ansi.org>).

⁵ NIST FIPS publications are available from the National Institute for Standards and Technology (<http://www.nist.gov>).

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For this standard, the following terms and definitions apply. *The IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.⁶

ad hoc network: A network typically created in a spontaneous manner. The principal characteristic of an ad hoc network is its limited temporal and spatial extent.

association: The service used to assign a device identifier to a device to enable communications in a piconet.

channel time allocation: A contiguous period of time in the superframe allocated by the piconet coordinator for communication between specified source and destination.

coexistence: The ability of one system to perform a task in a given shared environment where other systems have an ability to perform their tasks and may or may not be using the same set of rules.

data authentication: Authentication of the sender of the data and provision of data integrity.

data integrity: The assurance that the data has not been modified from its original form.

dBm: Decibels relative to a milliwatt.

device: An entity that implements an IEEE 802.15.3 conformant media access control and physical layer interface to the wireless medium.

device address: The EUI-48 associated with device in an IEEE 802.15.3 piconet.

disassociation: The service that removes an existing association.

frame: Format of aggregated bits that are transmitted together in time.

guard interval: A time period placed at the front of a symbol for inter-symbol interference avoidance.

integrity code: A data string generated using a symmetric key that is typically appended to data in order to provide data integrity and source authentication similar to a digital signature.

interoperable: The ability of two systems to perform a given task using a single set of rules.

medium access control command data unit: The unit of data exchanged between two peer medium access control entities using the services of the physical layer to implement the medium access control management protocol.

medium access control protocol data unit: The unit of data exchanged between two peer medium access control entities using the services of the physical layer.

medium access control service data unit: Information that is delivered as a unit between medium access control service access points.

⁶ *The IEEE Standards Dictionary Online* is available at
http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html.

payload protection: The generic term for providing security services on the contents of a data message, including confidentiality, integrity, and authentication.

piconet: A collection of one or more logically associated devices that share a single identifier with a common coordinator.

piconet coordinator: An entity that has device functionality and also provides coordination and other services, e.g., quality of service, synchronization, association, via the wireless medium for associated devices.

quality of service: A collective measure of the level of service (e.g., availability, latency, throughput, error rate) delivered between devices.

secure frame: A command or data frame in which cryptographic techniques are applied to provide encryption or integrity.

secure piconet: A piconet in which cryptographic techniques are implemented to provide security services.

stream: A unidirectional, logical data connection between two devices that may or may not have quality of service requirements associated with it.

superframe: The basic time division of an IEEE 802.15.3 piconet containing a beacon, the channel time allocation period and optionally the contention access period.

symmetric key: A secret key shared between two or more parties that may be used for encryption/decryption or integrity protection/integrity verification.

wireless medium: The medium used to implement the transfer of protocol data units between peer physical layer entities of a wireless personal area network.

3.2 Acronyms and abbreviations

AAS	asymmetric antenna system
ACK	acknowledgment
AES	advanced encryption standard
AS	application specific
ATP	association timeout period
AV	audio/visual
AWGN	additive white Gaussian noise
BBIFS	beam-forming beam-level interframe spacing
BCRD	bidirectional channel time allocation relinquish duration
BcstID	broadcast identifier
BER	bit error rate
BIFS	backoff interframe space
Blk-ACK	block acknowledgment
BPSK	binary phase-shift keying
BSID	beacon source identifier
BSIFS	beam-forming sector-level interframe spacing
BST	beam switching/steering and tracking
CAP	contention access period

CBC	cipher block chaining
CBC-MAC	cipher block chaining-message authentication code
CCA	clear channel assessment
CCM	counter mode encryption and cipher block chaining message authentication code
CES	channel estimation sequence
CID	Company ID
CMS	common mode signaling
CP	contention period
CRC	cyclic redundancy check
CSMA/CA	carrier sense multiple access with collision avoidance
CTA	channel time allocation
CTAP	channel time allocation period
CWB	continued wake beacon
DAMI	dual alternate mark inversion
DestID	destination identifier
DEV	device
DEVID	device identifier
Dly-ACK	delayed acknowledgment
DME	device management entity
DQPSK	differential quadrature phase-shift keying
DSPS	device synchronized power save
EEP	equal error protection
EIRP	equivalent isotropic radiated power
EPD	Ethertype protocol discrimination
FCS	frame check sequence
FCSL	frame convergence sublayer
FEC	forward error correction
FER	frame error rate
HCS	header check sequence
HR	high rate
HRP	high-rate physical layer
HRPDU	high-rate protocol data unit
HRS	high resolution
HSI	high speed interface
ID	identifier
IE	information element
IFS	interframe space
Imm-ACK	immediate acknowledgment
Imp-ACK	implied acknowledgment
KO	key originator
LAN	local area network
LDPC	low-density parity check
LFSR	linear feedback shift register
LLC	logical link control
LQI	link quality indication
LRP	low-rate physical layer

LRPDU	low-rate protocol data unit
LSB	least significant bit
MAC	medium access control
MAN	metropolitan area network
MCDU	MAC command data unit
MCS	modulation and coding scheme
McstID	multicast identifier
MCTA	management channel time allocation
MIFS	minimum interframe space
MLME	MAC layer management entity
mmWave	millimeter wave
MPDU	MAC protocol data unit
MPR	mandatory PHY rate
MR	medium rate
MSB	most significant bit
MSC	message sequence chart
MSDU	MAC service data unit
NAK	negative acknowledgment
NbrID	neighbor identifier
NLOS	non-line-of-sight
OFDM	orthogonal frequency-division multiplexing
OOK	on-off keying
OUI	organizationally unique identifier
PAL	protocol adaptation layer
PAN	personal area network
PCES	pilot channel estimation sequence
PCTM	pending channel time map
PDU	protocol data unit
PET	pattern estimation and tracking
PHY	physical layer
PIB	PAN information base
PLME	PHY layer management entity
PN	pseudo noise
PNC	piconet coordinator
PNCID	piconet coordinator identifier
PNID	piconet identifier
PPDU	PHY protocol data unit
PRBS	pseudo-random bit sequence
PRNG	pseudo-random number generator
PS	power save
PSD	power spectral density
PSPS	piconet synchronized power save
PSRC	power source
QAM	quadrature amplitude modulation
QoS	quality of service
QPSK	quadrature phase-shift keying

QT	quasi-omni training
RF	radio frequency
RIFS	retransmission interframe space
RS	Reed Solomon
RSSI	received signal strength indication
RSSIR	received signal strength indication relative to sensitivity
RX	receive or receiver
SAP	service access point
SAS	symmetric antenna system
SC	single carrier
S-CAP	sub-contention access period
SDU	service data unit
SEC	security
SECID	security identifier
SFC	secure frame counter
SIFS	short interframe space
SINR	signal-to-interference-plus-noise ratio
SNR	signal-to-noise ratio
SPS	synchronous power save
SrcID	source identifier
SSB	single side band
ST	sector training
STP	stream timeout period
TCM	trellis coded modulation
TPC	transmit power control
TSD	transmit switched diversity
TU	time unit
TX	transmit or transmitter
UEP	unequal error protection
WAN	wide area network
WLAN	wireless local area network
WPAN	wireless personal area network

4. General description

4.1 What is a piconet?

A piconet is a wireless ad hoc data communications system that allows a number of independent data devices (DEVs) to communicate with each other. A piconet is distinguished from other types of data networks in that communications are normally confined to a small area around person or object that typically covers 10 m in all directions and envelops the person or a thing whether stationary or in motion.

This is in contrast to local area network (LAN), metropolitan area network (MAN), and wide area network (WAN), each of which covers a successively larger geographic area, such as a single building or a campus or that would interconnect facilities in different parts of a country or of the world.

4.2 Components of an IEEE 802.15.3 piconet

An IEEE 802.15.3 piconet consists of several components, as shown in Figure 4-1. The basic component is the DEV. One DEV is required to assume the role of the piconet coordinator (PNC) of the piconet. The PNC provides the basic timing for the piconet with the beacon. Additionally, the PNC manages the quality of service (QoS) requirements, power save modes, and access control to the piconet.

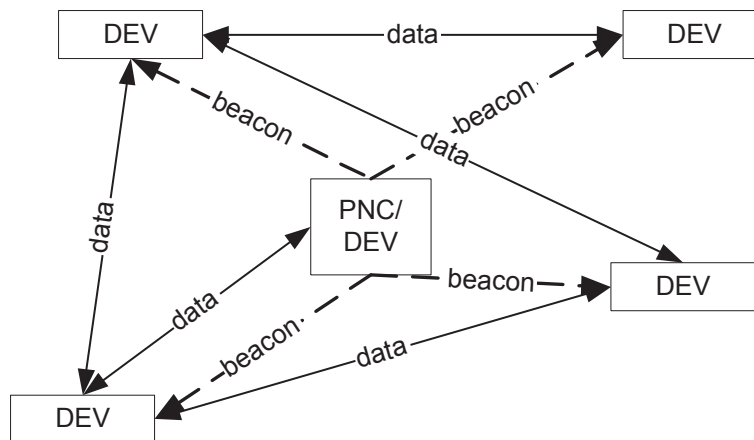


Figure 4-1—IEEE 802.15.3 piconet elements

Because IEEE 802.15.3 piconets form without pre-planning and for only as long as the piconet is needed, this type of operation is referred to as an ad hoc network.

This standard allows a DEV to request the formation of a subordinate piconet. The original piconet is referred to as the parent piconet. The subordinate piconet is referred to as either a child or neighbor piconet, depending on the method the DEV used to associate with the parent PNC. Child and neighbor piconets are also referred to as dependent piconets since they rely on the parent PNC to allocate channel time for the operation of the dependent piconet. An independent piconet is a piconet that does not have any dependent piconets.

4.3 Overview of medium access control (MAC) functionality

IEEE 803.15.3 MAC is designed to support the following goals:

- Fast connection time
- Ad hoc networks
- Data transport with quality of service (QoS)
- Security
- Dynamic membership
- Efficient data transfer

4.3.1 Coordination

A piconet is formed when an IEEE 802.15.3 DEV that is capable of acting as the PNC begins transmitting beacons. Thus, even if there are no associated DEVs, the PNC sending the beacon is considered to be a piconet.

4.3.1.1 Starting a piconet

To start a piconet, a DEV that is capable of acting as the PNC scans the available channels to find one that is not being used, as described in 7.2.1. If it finds one that is clear, it starts the piconet by simply sending the beacon after making sure that the channel has remained empty for a specified period of time, as described in 7.2.2. If no channels are available, the DEV has the option of attempting to start a dependent piconet, as described in 7.2.7 and 7.2.8 and summarized in 4.3.1.3 and 4.3.1.4. While the process of starting a piconet does not ensure that the “most capable” PNC is initially selected based on the criteria in 7.2.3, the association and handover process does allow the “most capable” DEV to eventually become the PNC of the piconet.

While the PNC is allowed to handover to a dependent PNC, this does not imply that the dependent PNC will merge the two piconets. IEEE Std 802.15.3 does not provide a process for merging two piconets into a single piconet.

4.3.1.2 Handing over control of the piconet

When a DEV associates with an existing piconet, as described in 7.3.1 and 4.3.4, the PNC checks the capabilities of the new DEV to see if it is more capable to be the PNC of the piconet based on the criteria defined in 7.2.3. If the new DEV is more capable and the current security policies allow it, then the PNC has the option of handing over control of the piconet to the DEV that has just joined. This handover process, as described in 7.2.3, maintains all existing time allocations so that there is no interruption in the delivery of data in the piconet. If the PNC is shutting down or wants to leave the piconet, it also uses the handover process to give control to another DEV in the piconet. The handover process also supports the handing over of a dependent PNC, as described in 7.2.6.

4.3.1.3 Creating a child piconet

A child piconet is one that is formed under an established piconet. The established piconet then becomes the parent piconet. The child piconet functionality is useful for either extending the area of coverage of the piconet or shifting some computational or memory requirements to another PNC-capable DEV. It is possible for the parent piconet to have more than one child piconet. In addition, it is also possible for a child PNC to allow a child piconet as a part of its own piconet.

The child piconet uses a distinct piconet identifier (PNID) and acts as an autonomous piconet except that it is dependent on a private channel time allocation (CTA) from the parent piconet. Association and security membership for the child piconet are handled within the child piconet and do not involve the parent PNC.

The child PNC is a member of the parent piconet and thus is able to exchange data with any DEV in the parent piconet. The child PNC is also a member of the child piconet and thus is able to exchange data with any DEV in the child piconet. Only DEVs in a child piconet that are also members of the parent piconet are

able to communicate directly with DEVs in the parent piconet who are not also members of that child piconet. The use of the child piconet is described in 7.2.7.

4.3.1.4 Creating a neighbor piconet

A neighbor piconet is formed under an established piconet. The established piconet then becomes the parent piconet. The neighbor piconet functionality is a mechanism for sharing the frequency spectrum between different piconets when there are no vacant PHY channels. It is possible for a single piconet to have more than one neighbor piconet or to have both child and neighbor piconets as a part of the parent piconet. In addition, it is possible for the neighbor PNC to allocate a child or neighbor piconets within its own piconet.

The neighbor piconet uses a distinct PNID and is an autonomous piconet except that it is dependent on a private CTA from the parent piconet. Association and security membership for the neighbor piconet are handled within the neighbor piconet and do not involve the parent PNC.

The neighbor PNC is not a member of the parent piconet and thus does not exchange information with any DEV in the parent piconet. The neighbor piconet mechanism is available to other wireless DEVs as a means of sharing the frequency spectrum. Any entity capable of initiating (i.e., requesting status as) an IEEE 802.15.3 neighbor piconet would also be capable of using this as a coexistence method. The use of the neighbor piconet is described in 7.2.8.

4.3.2 Ending a piconet

If the PNC is going to stop operation and there are no other PNC-capable DEVs in the piconet, the PNC places the PNC Shutdown information element (IE), as described in 6.4.5, into the beacon, as described in 7.2.9.1, to notify the members of the piconet.

In the case that the PNC abruptly leaves the piconet without handing over control to another PNC-capable DEV in the piconet, the piconet stops operation. After the association timeout period (ATP) expires, a PNC-capable DEV from the old piconet will be able to start a new piconet using the normal process, as described in 7.2.2.

In the case of dependent piconets, the parent PNC is able to end the dependent piconet via the Disassociation Request command, described in 6.5.1.3, for neighbor piconets, or by using the stream termination procedure, described in 7.5.1.3, for child piconets, as described in 7.2.9.2.

4.3.3 Ending a piconet with a dependent piconet involved

If the parent piconet ends operation, the parent PNC will indicate in the PNC Shutdown IE, as described in 6.4.5, a dependent piconet that will be able to continue to operate. All other dependent piconets will cease operation when the parent piconet ends operation. The dependent PNC that was selected to remain will remove the Parent Piconet IE, as described in 6.4.3, from its Beacon frame, signifying that it is no longer a dependent piconet. In the case where the parent piconet was temporarily disrupted, the parent PNC is able to attempt to join the dependent piconet and potentially receive a transfer of control via PNC handover.

A child piconet ends its piconet with the shutdown procedure and then uses the Channel Time Request command, as described in 6.5.6.1, to terminate the stream and release the resources in the parent piconet. When the child PNC shuts down its piconet, it is not required to leave the parent piconet.

The neighbor piconet uses the Disassociation Request command, as described in 6.5.1.3, to end its relationship with the parent PNC.

When a dependent piconet ends operation it has no effect on the parent piconet except to release resources.

4.3.4 Association and disassociation

In order to participate in a piconet, a DEV needs to join the piconet using the association process, as described in 7.3.1. Associating with the piconet provides the DEV with an identifier that is unique within that piconet, the DEVID, as described in 6.2.3. The DEVID is used instead of the DEV address to save overhead in the system. The association process optionally provides information about the services available in the piconet as well as the services provided by the DEV, as described in 7.3.2. The association process also provides the PNC with the capabilities of the new DEV to enable the PNC to decide if it wants to hand over control of the piconet to the new DEV, as described in 7.2.3 and 4.3.1.2.

When a new DEV joins the piconet, the PNC broadcasts the information about all of the DEVs in the piconet, as described in 7.3.3, and places information in the beacon about the new DEV. This allows other DEVs in the piconet to become aware of the new DEV as well as giving information to the new DEV about the members of the piconet.

When a DEV wants to leave the piconet or if the PNC wants to remove a DEV from the piconet, the disassociation process, as described in 7.3.4, is used. The DEVID of the disassociated DEV is no longer valid, until reissued by the PNC. However, the PNC is not allowed to reissue the DEVID until a waiting period has expired, as described in 7.3.1.

4.3.5 Security overview

Security is one of the following two modes, as described in 8.2:

- a) Mode 0—Open: Security membership is not required and payload protection (either data integrity or data encryption) is not used by the MAC. The PNC is allowed to use a list of DEV addresses to admit or deny entry to the piconet.
- b) Mode 1—Secure membership and payload protection: DEVs establish secure membership with the PNC before they have access to the piconet's resources. Data sent in Mode 1 is allowed to use payload protection (data integrity or data encryption with data integrity). Data integrity is required for most of the commands that are sent when in Mode 1.

When security is enabled, i.e., when Mode 1 is being used, DEVs that wish to join the piconet are required to establish secure membership with the PNC. The DEVs are also allowed to establish a secure relationship with other DEVs for secure communications. A DEV has established a secure membership or a secure relationship when it gets a management key for the security relationship. The process of establishing secure membership or a secure relationship is outside of the scope of this standard. The PNC or DEV that generates and distributes the key is called the key originator.

The payload protection protocol, as described in 9.2.2, uses a symmetric key that is generated by the key originator and is securely distributed to DEVs that have established secure membership or a secure relationship with the key originator, as described in 8.4.2. The symmetric key encryption algorithm used is the advanced encryption standard (AES) 128 in counter mode encryption and cipher block chaining-message authentication code (CCM).

4.3.6 The IEEE 802.15.3 superframe

Timing in the IEEE 802.15.3 piconet is based on the superframe, which is illustrated in Figure 4-2. The superframe is composed of the following three parts:

- The beacon, as described in 6.3.1, which is used to set the timing allocations and to communicate management information for the piconet. The beacon consists of the Beacon frame, as described in 6.3.1, as well as any Announce commands sent by the PNC as a beacon extension, as described in 7.6.3.

- The contention access period (CAP), as described in 7.4.2, which is used to communicate commands and/or asynchronous data if it is present in the superframe.
- The channel time allocation period (CTAP), 7.4.3, which is composed of channel time allocations (CTAs), including management CTAs (MCTAs). CTAs are used for commands, isochronous streams, and asynchronous data connections.

In Figure 4-2 the MCTAs are shown first, but the PNC is allowed to place any number of them at any position in the superframe.

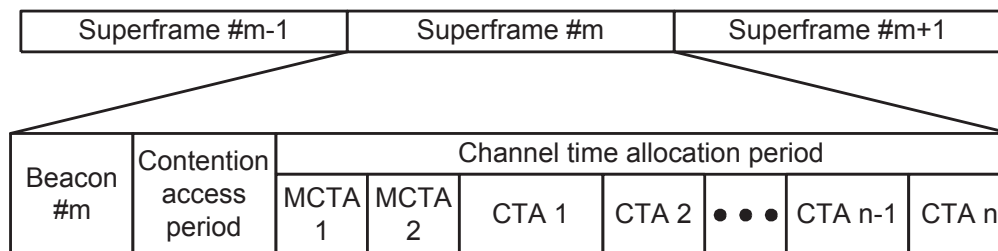


Figure 4-2—IEEE 802.15.3 piconet superframe

The length of the CAP is determined by the PNC and communicated to the DEVs in the piconet via the beacon. However, the PNC is able to replace the functionality provided in the CAP with management CTAs (MCTAs), except in the case of the 2.4 GHz PHY where the PNC is required to allow DEVs to use the CAP, as described in 10.2.10. MCTAs are a type of CTA that is used for communications between the DEVs and the PNC.

The CAP uses carrier sense multiple access/collision avoidance (CSMA/CA) for the medium access, as described in 7.4.2. The CTAP, on the other hand, uses a standard TDMA protocol where the DEVs have specified time windows, as described in 7.4.3.1. MCTAs, as described in 7.4.3.3, are either assigned to a specific source/destination pair and use TDMA for access or they are shared CTAs that are accessed using the slotted aloha protocol, as described in 7.4.3.4.

4.3.7 Channel time management

All data in the IEEE 802.15.3 piconet is exchanged in a peer-to-peer manner. There are three methods for communicating data between DEVs in the piconet, as follows:

- Sending asynchronous data in the CAP, if present, as described in 7.4.2.
- Allocating channel time for isochronous streams in the CTAP, as described in 7.5.1.
- Allocating asynchronous channel time in the CTAP, as described in 7.5.2.

If the CAP is present in the superframe and the PNC allows data in the CAP, DEVs in the piconet are able to use the CAP to send small amounts of data without having to allocate channel time.

If the DEV needs channel time on a regular basis, it makes a request from the PNC for isochronous channel time, as described in 7.5.1.1. If the resources are available, the PNC allocates time in a CTA for the DEV. If the requirements for the data change, then the DEV is able to request a change to the allocation, as described in 7.5.1.2. The source DEV, destination DEV, or the PNC are all allowed to terminate the stream, as described in 7.5.1.3.

For regular CTAs, the PNC is able to change their position within the superframe every superframe. If a DEV misses a beacon, it is unable to use the allocation for a regular CTA. To avoid lost throughput due to

missed beacons, DEVs are allowed to request a special type of CTA called a pseudo-static CTA, as described in 7.4.3.1. If the DEV is allocated a pseudo-static CTA, it is allowed to use the CTA for up to *mMaxLostBeacons* missed beacons. The PNC is allowed to move the locations of these CTAs, but needs to maintain the time for the old allocation for *mMaxLostBeacons* superframes to avoid collisions, as described in 7.4.3.1.

Asynchronous allocation is slightly different. Rather than requesting recurring channel time, an asynchronous channel time request, as described in 7.5.2.1, is a request for a total amount of time to be used to transfer its data. The PNC is then able to schedule time for this request when available based on the channel time requirements. Unlike an isochronous allocation, only the source DEV or PNC are allowed to terminate an asynchronous allocation, as described in 7.5.2.2.

4.3.8 Data communications between DEVs

In order to handle large data frames from layers above the MAC sublayer, this standard supports the fragmentation and defragmentation of these data frames, as described in 7.7. The ability to fragment data frames is also useful to reduce the frame error rate (FER) of a marginal link by decreasing the frame size. The fragments are numbered with a sequence number for the upper layer frame as well as a sequence number for the fragment itself. The total number of fragments of that data frame is also sent to enable the receiving DEV to allocate the correct amount of internal memory to hold the incoming frame.

If the source DEV wishes to verify the delivery of a frame, then one of the acknowledgment (ACK) policies is used, as described in 7.9. This standard provides for three types of ACKs to enable different applications. The no-ACK policy, as described in 7.9.1, is appropriate for frames that do not require guaranteed delivery, where the retransmitted frame would arrive too late or where an upper layer protocol is handling the ACK and retransmission protocol. The immediate-ACK (Imm-ACK) policy, as described in 7.9.2, provides an ACK process in which each frame is individually ACKed following the reception of the frame. The delayed-ACK (Dly-ACK) policy, as described in 7.9.3, lets the source send multiple frames without the intervening ACKs. Instead, the ACKs of the individual frames are grouped into a single response frame that is sent when requested by the source DEV. The Dly-ACK process decreases the overhead in the Imm-ACK process while allowing the source DEV to verify the delivery of frames to the destination.

If the source DEV does not receive the requested ACK, then it has the option of retransmitting the frame, as described in 7.9.6, or dropping the frame. The decision to retransmit or drop the frame depends on the type of data or command that is being sent, the number of times that the source DEV has attempted sending the frame, the length of time it has spent attempting to send the frame, or other implementation-dependent factors.

4.3.9 Information discovery in the piconet

Since IEEE 802.15.3 piconets are ad hoc in nature, it is important for the DEVs in the piconet to be able to find out information about the services and capabilities of the other DEVs in the piconet at any instant in time. This standard supports four methods for discovering information about other DEVs in the piconet: the PNC Information Request command, as described in 6.5.4.1; the Probe Request command, as described in 6.5.4.5; the Announce command, as described in 6.5.5.2; and the Piconet Services command, as described in 6.5.5.1. In addition, the PNC is able to ask a DEV in the piconet to evaluate the channel conditions in either the current channel or in an alternate channel with the Remote Scan Request command, as described in 6.5.7.3. Any DEV in the piconet is able to ask another DEV about the status of the current channel with the Channel Status Request command, as described in 6.5.7.1.

The PNC Information Request command, as described in 7.10.1, is used to obtain information from the PNC about either a specific DEV in the piconet or all of the DEVs in the piconet. The PNC responds to the request with the PNC Information command, as described in 6.5.4.2, which contains information about the DEV (or DEVs) that was requested by the originator of the command.

A DEV uses the Probe Request command, 7.10.2, to find out more detailed information about other DEVs in the piconet. This command allows the originating DEV to retrieve some IEs, as defined in 7.10.2, from a target DEV in the piconet.

One of the goals of connecting DEVs in a piconet is to enable them to share services. However, to do this a DEV needs to be able to discover the services that are available in the piconet as well as to advertise its services to other DEVs in the piconet. This standard enables this with the Piconet Services IE, as described in 6.4.16, which optionally is exchanged in the association process, as described in 7.3.1.

The PNC is responsible for determining the channel in which the piconet will operate. Because the DEVs in the piconet are typically at different geographic locations, they provide additional information about interference or other piconets in the area. The Remote Scan Request command, as described in 7.10.5, is used by the PNC to request information about the channel from other DEVs. In response to the PNC's request, the DEV either scans the channels as requested or rejects the request from the PNC if it is not going to perform the scan.

Any DEV in the piconet is able to request information about the quality of the link between itself and another DEV with the Channel Status Request command, as described in 6.5.7.1. This command is used for two purposes. The first is to allow the DEVs to change transmit power, the data rate, or the requested channel time based on the quality of the data connection between the DEVs. The other use is for the PNC to determine if the DEVs in the piconet are having trouble with the channel. This information along with PNC's scanning of the channel and optional remote scan requests assists the PNC in determining if it needs to change the channel that the piconet is currently using.

4.3.10 Dynamic channel selection

The piconet operates in a dynamic environment and under unlicensed operation rules. Thus, it is subject to interference from licensed users, other IEEE 802.15.3 piconets as well as other unlicensed wireless entities in its channels. To enable the piconet to continue operation in this type of environment, the PNC has the capability to dynamically change the channel that the piconet is using without requiring either user intervention or the disruption of services in the piconet. To evaluate the status of the current channel as well as other channels, the PNC is able to use many methods including the following:

- Gathering information about the current channel from other DEVs in the piconet using the Channel Status Request command, as described in 7.10.4.
- Performing a passive scan of the channels, as described in 7.12.1.
- Requesting other DEVs to perform a channel scan using the Remote Scan Request command, as described in 7.10.5.

If the PNC determines that the current channel is unsuitable, it uses the dynamic channel selection procedure, as described in 7.12.1, to move the piconet to the new channel. The configuration of the piconet and the CTAs do not change with a channel change so that the services provided by the piconet are not interrupted by the change.

4.3.11 Power management

This standard provides techniques to allow DEVs to reduce power usage by enabling the DEVs to turn off for one or more superframes. These techniques are as follows:

- Device synchronized power save (DPS) mode
- Piconet synchronized power save (PSPS) mode
- Asynchronous power save (APS) mode

DSPS and PSPS are collectively known as synchronized power save (SPS) modes. In the piconet, DEVs operate in one of four power management (PM) modes; ACTIVE mode, DSPS mode, PSPS mode, or APS mode.

PSPS mode, as described in 7.14.1, allows DEVs to sleep at intervals defined by the PNC. The DEV sends a request to the PNC when it wants to enter the PSPS mode. The PNC informs the piconet by setting the DEV's bit in its power save (PS) Status IE in the beacon. The PNC then selects beacons that will be the system wake beacons and indicates the next one in the PS Status IE for the PSPS set. All DEVs in PSPS mode are required to listen to the system wake beacons.

DSPS mode, as described in 7.14.2, is designed to enable groups of DEVs to sleep for multiple superframes but still be able to wake up during the same superframe. DEVs synchronize their sleep patterns by joining a DSPS set that specifies the interval between wake periods for the DEVs and the next time the DEVs will be awake. Besides allowing the DEVs to wake up and exchange traffic at the same time, the use of DSPS sets makes it easy for other DEVs in the piconet to determine exactly when a DSPS DEV will be available to receive traffic.

APS mode, as described in 7.14.3, allows a DEV to conserve power for extended periods until the DEV chooses to listen for a beacon. The only responsibility of a DEV in APS mode is to communicate with the PNC before the end of its ATP in order to preserve its membership in the piconet.

The PNC allocates asynchronous CTAs to a destination DEV that is in either PSPS mode or DSPS mode in the wake superframes for that DEV.

Regardless of the DEV's power management mode, every DEV in the piconet is allowed to power down during parts of the superframe when the DEV is not scheduled to transmit or receive data.

4.3.12 Controlling transmit power in the piconet

The ability to control transmit power in the piconet enables DEVs to minimize interference with other wireless networks that share the same channel as well as to decrease the power usage in some PHY implementations. Two methods are provided by this standard for controlling transmitter power. The first method allows the PNC to set a maximum transmit power for the CAP, beacon, and MCTAs, excluding association MCTAs, as described in 7.12.2.1. Since the link between the PNC and the DEV defines the size of the piconet, controlling the power during these times allows the PNC to reduce transmit power without adversely affecting operation of the piconet.

The second method allows DEVs using a CTA to request either an increase or a decrease in the transmit power of the remote DEV, as described in 7.12.2.2. Thus if two DEVs have a "good" link in a CTA, they are able to reduce their transmitter power to decrease the power usage in some PHY implementations, and to reduce interference to other networks.

4.3.13 Superframe structure using quasi-omni mode

A mmWave piconet operates in either omni mode or quasi-omni mode. The superframe structure for omni mode is illustrated in Figure 4-2. The superframe structure for quasi-omni mode is illustrated in Figure 4-3. In quasi-omni mode, the same Beacon frame is transmitted in different quasi-omni directions in a round-robin way in order to allow mmWave DEVs located in different directional coverage to join the piconet, as described in 7.6.5.

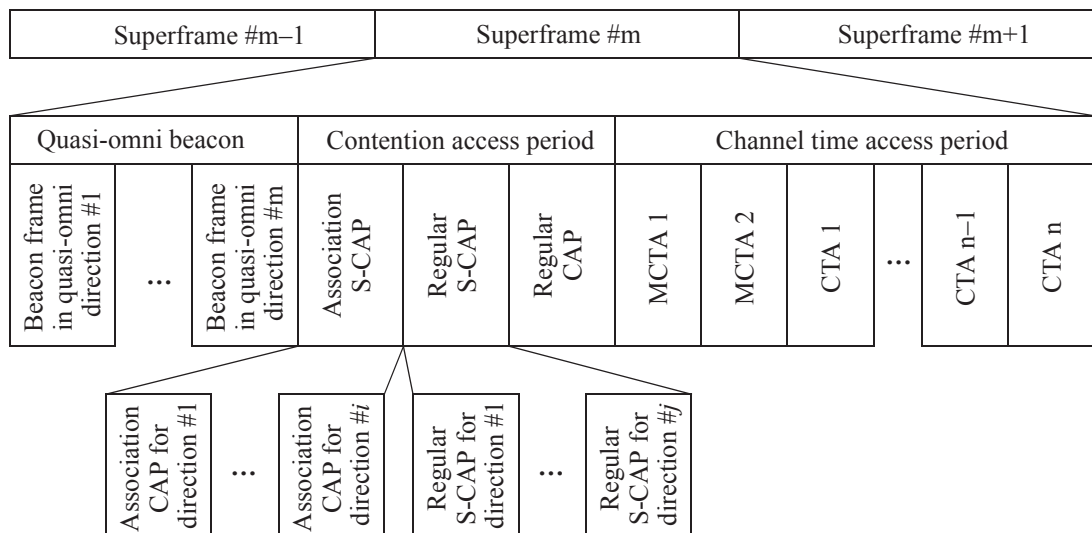


Figure 4-3—Piconet superframe structure in quasi-omni mode

4.3.14 Frame aggregation

Frame aggregation, as described in 7.8, is supported for the purpose of high throughput. Two aggregation methods are provided for mmWave DEVs, one is suitable for normal data and A/V streaming and the other is optimized for low-latency communications.

4.3.15 Beam forming

The beam forming procedure allows a mmWave DEV that is capable of beam forming to increase the antenna gain for supporting high data rate transmission. The beam forming procedures are described in Clause 12.

4.3.16 Channel probing

Channel probing, as described in 7.10.7, is an optional capability that is used by a DEV to determine the best modulation and coding scheme (MCS) to use with the target DEV under current channel condition.

4.3.17 Unequal error protection (UEP)

For flexible error protection that accounts for data that has more emphasis on the MSBs than the LSBs, e.g., video, UEP is provided as an option only for mmWave DEVs. Three types of UEP are defined, as described in 7.17, for use with the three mmWave PHYs.

4.4 Characteristics of the 2.4 GHz PHY

4.4.1 General characteristics

The 2.4 GHz PHY, Clause 10, uses the 2.4 GHz to 2.4835 GHz band that is available for unlicensed use in much of the world, as described in 10.1. Two channel plans are defined, one with 4 channels for high-density applications and one with 3 channels to enable better coexistence with IEEE Std 802.11b™-1999 [B3]⁷

⁷The numbers in brackets correspond to those of the bibliography in Annex A.

networks, as described in 10.2.3. The PHY also supports 5 data rates, ranging from 11 Mb/s to 55 Mb/s, utilizing, quadrature phase-shift keying (QPSK), differential quadrature phase shift keying (DQPSK), 16-quadrature amplitude modulation (16-QAM), 32-QAM and 64-QAM. The base rate of 22 Mb/s is uncoded, while the 11 Mb/s, 33 Mb/s, 44Mb/s, and 55 Mb/s use trellis coded modulation, 10.3.

For efficiency, the PHY calculates the header check sequence over both the MAC and PHY headers and appends this to the MAC header. The header for all frames is sent at the base rate, 22 Mb/s, to allow all DEVs in the piconet to detect traffic. In the 11 Mb/s mode, the entire MAC and PHY header is repeated at the lower modulation rate to increase the probability of receiving the entire header correctly.

The PHY uses a constant-amplitude, zero-autocorrelation (CAZAC) sequence for the preamble, as described in 10.4.2. This sequence has good properties for obtaining synchronization, timing information, and frequency offset.

The on-air bandwidth is limited to 15 MHz in order to allow more channels as well as to decrease the interference to other systems and to decrease the susceptibility to interference from other systems. The transmitter power is constrained by the limitations of the appropriate regulatory bodies.

The receiver of a compliant system reports both the signal level and, if the higher order modulations are used, an indication of the signal quality. This allows a DEV to determine if errors in the channel are due to poor signal quality or due to interference from other systems.

4.4.2 Coexistence and interoperability

While this standard does not require interoperability with other standards, there were choices made with the 2.4 GHz PHY specification that make it easier to design dual-mode radios. The commonalities that allow interoperable radios are discussed in D.1.

Because the 2.4 GHz PHY operates as an unlicensed system, it needs to share the medium with both licensed and unlicensed users in the band. The IEEE 802.15.3 MAC and the 2.4 GHz PHY offer a variety of techniques to enhance the coexistence with other users in the band. The methods provided by this standard include the following:

- Passive scanning
- Dynamic channel selection
- The ability to request channel quality information
- Link quality and RSSI
- A channel plan that minimizes channel overlap
- Lower transmit power
- Transmit power control
- Neighbor piconet capability

The use of these methods to improve coexistence is described in D.2.

4.5 Characteristics of the mmWave PHY

4.5.1 mmWave PHY characteristics

The mmWave PHY, as described in Clause 11, is defined for the frequency band of 57.0–66.0 GHz, as allocated by the regulatory agencies in Europe, Japan, Canada, and the United States as well as any other areas where the regulatory bodies have allocated this band. While four channels are defined for the PHY, regulatory requirements allow fewer in some regions.

A total of three PHYs are defined for the mmWave PHY. They are as follows:

- a) Single Carrier mode in mmWave PHY (SC PHY), as described in 11.2.
- b) High Speed Interface mode in mmWave PHY (HSI PHY), as described in 11.3.
- c) Audio/Visual mode in mmWave PHY (AV PHY), as described in 11.4.

For DEVs that implement the mmWave PHY, at least one of the three PHYs is required. In addition, to promote coexistence and interoperability, a common mode signaling (CMS) is defined based on a low data rate SC PHY mode, as described in 11.1.12.

The SC PHY supports data rates up to 5 Gb/s. The SC PHY supports a wide range of modulations, $\pi/2$ BPSK, $\pi/2$ QPSK, $\pi/2$ 8-phase shift keying (8-PSK), $\pi/2$ 16-QAM, on-off keying (OOK), and dual alternate mark inversion (DAMI). The coding schemes included are Reed-Solomon (RS) coding with low-complexity implementation and low-density parity check (LDPC) coding with high error-correcting capability. Code spreading using either linear feedback shift register (LFSR) code or Golay sequence is also applied to increase robustness of the system.

The HSI PHY, as described in 11.3, is designed for non-line-of-sight (NLOS) operation and uses OFDM with an FEC based on LDPC.

The AV PHY, as described in 11.4, is designed for NLOS operation and the transport of uncompressed, high definition video and audio. It uses OFDM modulation with convolutional inner code and a Reed Solomon(RS) outer code. The AV mode supports omni-directional coverage via the low-rate PHY (LRP) for the purpose of setting up high-throughput connections using the high-rate PHY (HRP).

Different PHYs are a result of demands of different market segments, which were based on the development of the usage models for this standard. For example one usage model is for kiosk applications. This usage model requires 1.5 Gb/s at a 1 m range. The SC-PHY can provide such a data rate at that short range with less complexity thus lower cost than an OFDM PHY. Another usage model required the streaming of uncompressed video. Due to the nature of uncompressed video signals a special PHY, the AV PHY, was selected to provide high throughput. A third usage model involves an ad hoc system to connect computers and devices around a conference table. In this usage model, all of the devices in the wireless personal area network (WPAN) will have bidirectional, NLOS high-speed, low-latency communication, which is provided for by the HSI PHY. Mandatory data rates of all those PHYs are selected according to specific usage models. In addition, higher data rates are provided to give options to the implementers so that they can best address the different market segments.

4.5.2 Piconets using mmWave PHY modes

When a mmWave PHY PNC-capable DEV starts a piconet, the type of piconet it starts depends on the PHY modes that are supported. For example, if the PNC-capable DEV supports only the AV PHY mode, it would start an AV piconet in which the beacon is sent with the AV PHY mode and the contention periods (CPs) would use the AV PHY mode. The AV PNC would also send the Sync frame to improve coexistence with other piconets. DEVs that support only the AV PHY mode are able to find and join the piconet using the AV PHY mode.

The same process is used for a mmWave PHY PNC-capable DEV that supports only HSI PHY mode or SC PHY mode, with the exception that an SC PHY mode PNC does not need to send a Sync frame since its beacon is sent in CMS mode already.

If a PNC-capable DEV supports more than one mmWave PHY mode, then it is able to select the type of piconet it starts, potentially starting more than one piconet, each with a different PHY mode, with the additional piconets as dependent piconets. Alternatively, the multi-mode PNC is able to have a single piconet in which DEVs use any MCS in a CTA that is supported by both of the DEVs.

The complete rules are described in 11.1.

4.6 Conventions

Unless otherwise specified, the term increment or incremented means to increase a value by one.

The editorial conventions in this standard are as follows:

- Frame names (e.g., Beacon frame, MAC Command frame) are capitalized and include the word *frame*.
- Command names (e.g., Association Request command) are capitalized and include the word *command*.
- Field names are capitalized and include the word *field*, which is not capitalized, e.g., Destination PAN Identifier field. The only exception is in a figure that shows the field, in which the word “field” is not included.
- IE names are capitalized and include the acronym IE (e.g., Capability IE).
- MAC and PHY PIB entries are preceded by a lower case prefix, *mac* or *phy*, respectively, and are capitalized at word boundaries, e.g., “*macDevServicesBroadcast*” and “*phyCurrentChannel*”.
- Constants begin with a lower case, italicized “*m*” for MAC related constants and a lower case italicized “*p*” for PHY related constants. Both use the same capitalization and use rules as PIB attributes.
- Service primitives names (e.g., MLME or MCPS) are ALL CAPS, but the .request, .indication, .response, and .confirm in the primitive names are always lower case.
- Primitive parameters are capitalized at word boundaries, e.g., NumberOfPiconets.
- In a PIB attribute, constant or service primitive, acronyms are not capitalized after the first letter, e.g., “*pMinTpcLevel*”, “*macDevServicesBroadcast*”, or “ScanForBsid”.

4.7 Concept of primitives

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 4-4, showing the service hierarchy and the relationship of the two correspondent users and their associated layer (or sublayer) peer protocol entities.

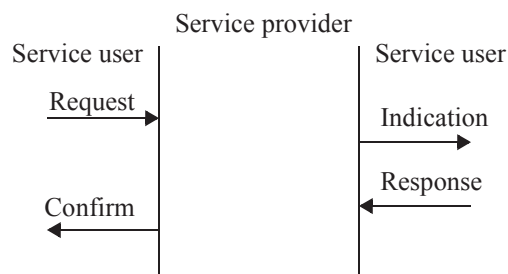


Figure 4-4—Service primitives

The services are specified by describing the information flow between the user and the 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 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 primitive can be one of the following four generic types:

- *Request*: The request primitive is used to request that a service is initiated.
- *Indication*: The indication primitive is used to indicate to the user an internal event.
- *Response*: The response primitive is used to complete a procedure previously invoked by an indication primitive.
- *Confirm*: The confirm primitive is used to convey the results of one or more associated previous service requests.

5. Layer management

5.1 Overview of management model

Both MAC and PHY layers conceptually include management entities, called the MAC sublayer management entity and PHY layer management entity (MLME and PLME, respectively). These entities provide the layer management service interfaces for the layer management functions. Figure 5-1 depicts the relationship among the management entities. The protocol adaptation layer (PAL) includes both the FCSL and DME. The reference model depicts the interactions of a single PAL in a single piconet; support for multiple piconets and/or PALs is implementation dependent.

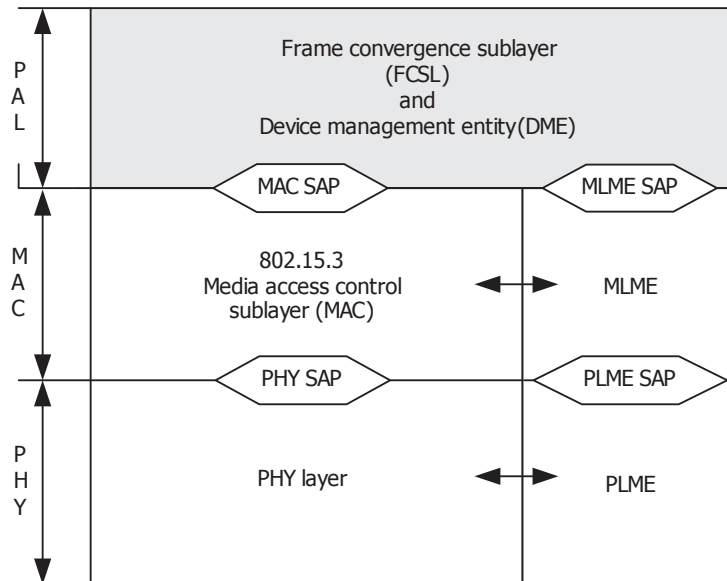


Figure 5-1—The reference model used in this standard

The various entities within this model interact in various ways. Certain of these interactions are defined explicitly within this standard, via a service access point (SAP) across which defined primitives are exchanged. Other interactions are not defined explicitly within this standard, such as the interface between the MAC and the MLME or the interface between the PHY and the PLME. The specific manner in which these MAC and PHY interfaces are integrated into the overall MAC and PHY layers are not specified within this standard.

The various SAPs within this model are the following:

- a) PAL SAP (not shown)
- b) MAC SAP
- c) MLME SAP

The PHY SAP and PLME SAP are not defined in this standard as they are rarely, if ever, exposed in a typical implementation. The PHY management objects and attributes are accessed through the MLME SAP with the generic management primitives defined in 5.2.

The MAC SAP is described further in Annex B.

If the SAP interfaces are not exposed in an IEEE 802.15.3 DEV, then these interfaces do not have to be implemented as described here. If the interfaces are exposed, then they should support the primitives described in this clause.

5.2 Generic management primitives

The management information specific to each layer is represented as a personal area network (PAN) information base (PIB) for that layer. In a LAN/MAN the corresponding information is in the management information base (MIB) and is often associated with a management protocol such as simple network management protocol (SNMP) (see IETF RFC 1157:1990 [B10]). However, piconets are not intended to be managed across a network but rather use the management information to ascertain the characteristics of the layer or sublayer.

The MLME and PLME are viewed as “containing” the PIB for that layer or sublayer. The generic model of PIB-related management primitives exchanged across the management SAPs is to allow the SAP user entity to either “GET” the value of a PIB attribute, or to “SET” the value of a PIB attribute. The invocation of a SET.request primitive may require the layer entity to perform certain defined actions. An attempt to “GET” a PIB attribute identified as a “write only” attribute is not a valid operation. An attempt to “SET” a PIB attribute identified as a “read only” attribute is not a valid operation.

The GET and SET primitives are represented as requests with associated confirm primitives. The DME uses the services provided by the MLME through the MLME SAP to access the management objects in either the MAC PIB or PHY PIB. The primitives are summarized in Table 5-1.

Table 5-1—Summary of generic management primitives

Name	Request	Confirm
MLME-GET	5.2.1	5.2.2
MLME-SET	5.2.3	5.2.4

The parameters used for these primitives are defined in Table 5-2.

Table 5-2—MLME generic management primitive parameters

Name	Type	Valid range	Description
PIBattribute	Octet string	Any PIB attribute, as defined in 5.4 or 10.7	The name of the PIB attribute
PIBvalue	Variable	As defined in 5.4 or 10.7	The PIB value
ResultCode	Enumeration	SUCCESS, FAILURE	Indicates the result of the MLME request
ReasonCode	Enumeration	INVALID_PIB_ATTRIBUTE_NAME, INVALID_PIB_ATTRIBUTE_VALUE, READ_ONLY_PIB_ATTRIBUTE, WRITE_ONLY_PIB_ATTRIBUTE	Indicates the reason for a ResultCode of FAILURE

Other SAP-specific primitives are identified in 5.3.

5.2.1 MLME-GET.request

This primitive requests information about a given MAC or PHY PIB attribute. The semantics of this primitive are as follows:

```
MLME-GET.request      (  
                        PIBattribute  
                        )
```

The primitive parameter is defined in Table 5-2.

5.2.2 MLME-GET.confirm

This primitive reports the results of an information request about either the MAC or PHY PIB. The semantics of this primitive are as follows:

```
MLME-GET.confirm      (  
                        PIBattribute,  
                        PIBvalue,  
                        ResultCode,  
                        ReasonCode  
                        )
```

The primitive parameters are defined in Table 5-2.

5.2.3 MLME-SET.request

This primitive attempts to set the indicated MAC or PHY PIB attribute to the given value. The semantics of this primitive are as follows:

```
MLME-SET.request      (  
                        PIBattribute,  
                        PIBvalue  
                        )
```

The primitive parameters are defined in Table 5-2.

5.2.4 MLME-SET.confirm

This primitive reports the results of an attempt to set the value of an attribute in either the MAC or PHY PIB. The semantics of this primitive are as follows:

```
MLME-SET.confirm      (  
                        PIBattribute,  
                        ResultCode,  
                        ReasonCode  
                        )
```

The primitive parameters are defined in Table 5-2.

5.3 MLME SAP interface

The services provided by the MLME to the DME are specified in this subclause. These services are described in an abstract way and do not imply any particular implementation. MLME SAP primitives are of the general form ACTION.request followed by ACTION.confirm. An ACTION.indication provides information to the DME that originated either in the local MAC or from another DEV. The DME optionally responds to the indication by issuing an ACTION.response. The DME uses the services provided by the MLME through the MLME SAP. The MLME interface models a single piconet environment; support for multiple piconets is implementation dependent. The primitives are summarized in Table 5-3.

Table 5-3—Summary of MLME primitives

Name	Request	Confirm	Indication	Response
MLME-RESET	5.3.1.1	5.3.1.2	—	—
MLME-SCAN	5.3.2.1	5.3.2.2	5.3.2.3	—
MLME-START	5.3.3.1	5.3.3.2	—	—
MLME-STOP	5.3.4.1	5.3.4.2	—	—
MLME-ASSOCIATE	5.3.5.1	5.3.5.2	5.3.5.3	—
MLME-DISASSOCIATE	5.3.6.1	5.3.6.2	5.3.6.3	—
MLME-MEMBERSHIP-UPDATE	5.3.7.1	5.3.7.2	—	—
MLME-SECURITY-ERROR	—	—	5.3.7.3	—
MLME-SECURITY-MESSAGE	5.3.7.4	5.3.7.5	5.3.7.6	—
MLME-PNC-HANDOVER	—	—	5.3.8.1	5.3.8.2
MLME-NEW-PNC	—	—	5.3.8.3	—
MLME-DEV-INFO	5.3.9.1	5.3.9.2	5.3.9.3	—
MLME-SECURITY-INFO	5.3.10.1	5.3.10.2	5.3.10.3	5.3.10.4
MLME-APPLICATION-SPECIFIC	5.3.11.1	5.3.11.2	5.3.11.3	—
MLME-ANNOUNCE-SERVICE	5.3.12.1	5.3.12.2	—	—
MLME-PICONET-SERVICES	5.3.12.3	5.3.12.4	5.3.12.5	—
MLME-CREATE-STREAM	5.3.13.1	5.3.13.2	5.3.13.3	—
MLME-MODIFY-STREAM	5.3.13.4	5.3.13.5	—	—
MLME-TERMINATE-STREAM	5.3.13.6	5.3.13.7	5.3.13.8	—
MLME-BSID-CHANGE	5.3.14.1	5.3.14.2	—	—
MLME-PICONET-PARM-CHANGE	—	—	5.3.14.3	—
MLME-PS-SET-INFORMATION	5.3.15.1	5.3.15.2	—	—
MLME-SPS-CONFIGURE	5.3.15.3	5.3.15.4	—	—
MLME-PM-MODE-CHANGE	5.3.15.5	5.3.15.6	5.3.15.7	—
MLME-MONITOR-PM-MODE	5.3.15.8	5.3.15.9	5.3.15.10	—
MLME-MULTICAST-CONFIGURATION	5.3.16.1	5.3.16.2	—	—