

IEEE Standard for High Data Rate Wireless Multi-Media Networks

Amendment 1: High-Rate Close Proximity Point-to-Point Communications

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

IEEE Std 802.15.3e™-2017
(Amendment to
IEEE Std 802.15.3™-2016)

IEEE Standard for High Data Rate Wireless Multi-Media Networks

Amendment 1: High-Rate Close Proximity Point-to-Point Communications

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 14 February 2017
IEEE-SA Standards Board

Abstract: An alternative physical layer (PHY) and a modified medium access control (MAC) layer is defined in this amendment.

Two PHY modes have been defined that enable data rates up to 100 Gb/s using the 60 GHz band. MIMO and aggregation methods have been defined to increase the maximum achievable communication speeds. Stack acknowledgment has been defined to improve the medium access control (MAC) efficiency when used in a point-to-point (P2P) topology between two devices.

Keywords: 60 GHz, close proximity, fast setup, IEEE 802.15.3™, IEEE 802.15.3e™, millimeter wave, point-to-point, P2P, wireless

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

Copyright © 2017 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 7 June 2017. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

Print: ISBN 978-1-5044-4007-3 STD22571
PDF: ISBN 978-1-5044-4008-0 STDPD22571

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 Notices and Disclaimers Concerning IEEE Standards Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

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. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups 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 Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users 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.

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:

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*

Andrew Estrada, *Task Group 15.3e Chair*
Thomas Kürner, *Task Group 15.3e Vice-Chair*
Ken Hiraga, *Task Group 15.3e Secretary*
Ko Togashi, *Task Group 15.3e Technical Editor*

Mounir Archir
Keiji Akiyama
Arthur Astrin
Philip Beecher
Frederik Beer
Chandrashekhara P. S. Bhat
Kiran Bynam
Edgar Callaway
Chris Calvert
Radhakrishna Canchi
Kapseok Chang
Soo-Young Chang
Clint Chaplin
Stephen Chasko
Paul Chilton
Sangsung Choi
Hendricus De Ruijter
Guido Dolmans
Igor Dotlic
Stefan Drude
Dietmar Eggert
Shahriar Emami
David Evans
George Flammer
Kiyoshi Fukui
Matthew Gillmore
Tim Godfrey
Elad Gottlieb
Jussi Haapola

Rainer Hach
Shinsuke Hara
Timothy Harrington
James Hartman
Marco Hernandez
Iwao Hosako
Yeong Min Jang
Seong-Soon Joo
Akifumi Kasamatsu
Shuzo Kato
Toyoyuki Kato
Jeritt Kent
Jaehwan Kim
Youngsoo Kim
Shoichi Kitazawa
Tero Kivinen
Ryuji Kohno
Fumihide Kojima
Byung-Jae Kwak
Jae Lee
Myung Lee
Sangjae Lee
Huan-Bang Li
Liang Li
Qing Li
Michael Lynch
Itaru Maekawa
Hiroyuki Matsumura
Michael McLaughlin

Michael McInnis
Kenichi Mori
Robert Moskowitz
Jinesh Nair
Chiu Ngo
Paul Nikolich
John Notor
Hiroyo Ogawa
Taejoon Park
Glenn Parsons
Albert Petrick
Ivan Reede
Richard Roberts
Ruben Salazar Cardozo
Noriyuki Sato
Norihiko Sekine
Kunal Shah
Stephen Shellhammer
Shusaku Shimada
Gary Stuebing
Don Sturek
Mineo Takai
Billy Verso
Gabriel Villardi
Brian Weis
Makoto Yaita
Peter Yee
Yu Zeng
Chunhui Zhu

Major contributions were received from the following individuals:

Keiji Akiyama
Hideki Iwami
Jun Kobayashi
Keitarou Kondou

Jae Seung Lee
Moon-Sik Lee
Itaru Maekawa
Hiroshi Nakano

Makoto Noda
Ichiro Seto
Masashi Shimizu
Kiyoshi Toshimitsu

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

Tomoko Adachi
Iwan Adhicandra
Thomas Alexander
Richard Alfvén
Nobumitsu Amachi
Carol Ansley
Butch Anton
Yusuke Asai
Harry Bims
Nancy Bravin
Vern Brethour
William Byrd
Radhakrishna Canchi
William Carney
Juan Carreon
Yesenia Cevallos
Keith Chow
Charles Cook
Richard Doyle
Sourav Dutta
Richard Edgar
Andrew Estrada
David Evans
Avraham Freedman
Yukihiro Fujimoto
Devon Gayle
James P. K. Gilb
Randall Groves
Michael Gundlach

Robert F. Heile
Marco Hernandez
Ken Hiraga
Werner Hoelzl
Noriyuki Ikeuchi
Yasuhiko Inoue
Sergiu Iordanescu
Atsushi Ito
Raj Jain
Michael Johas Teener
Adri Jovin
Piotr Karocki
Jeritt Kent
Stuart Kerry
Yongbum Kim
Tero Kivinen
Jun Kobayashi
Keitarou Kondou
Yasushi Kudoh
Thomas Kuerner
Thomas Kurihara
Hyeong Ho Lee
Jae Seung Lee
Moon-Sik Lee
Arthur H Light
Michael Lynch
Elvis Maculuba
Itaru Maekawa
Michael McInnis

Michael Montemurro
Hiroshi Nakano
Michael Newman
Charles Ngethe
Paul Nikolich
John Notor
Yoshihiro Ohba
Satoshi Oyama
Arumugam Paventhan
Clinton C Powell
Venkatesha Prasad
Verotiana Rabarijaona
Maximilian Riegel
Robert Robinson
Benjamin Rolfe
Kazuyuki Sakoda
Naotaka Sato
Thomas Starai
Rene Struik
Walter Struppler
Mark Sturza
Bo Sun
Chen Sun
Masayuki Tsujita
Mark-Rene Uchida
Lorenzo Vangelista
Prabodh Varshney
George Vlantis
Hung-Yu Wei
Oren Yuen

When the IEEE-SA Standards Board approved this standard on 14 February 2017, it had the following membership:

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

Chuck Adams
Masayuki Ariyoshi
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Gary Hoffman

Michael Janezic
Thomas Koshy
Joseph L. Koepfinger*
Kevin Lu
Daleep Mohla
Damir Novosel
Ronald C. Petersen
Annette D. Reilly

Robby Robson
Dorothy Stanley
Adrian Stephens
Mehmet Ulema
Phil Wennblom
Howard Wolfman
Yu Yuan

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802.15.3e-2017, IEEE Standard for High Data Rate Wireless Multi-Media Networks—Amendment 1: High-Rate Close Proximity Point-to-Point Communications.

IEEE Std 802.15.3e is an amendment to IEEE Std 802.15.3-2016 that defines an alternative physical layer operating in the millimeter wave band along with the necessary MAC changes to support this PHY. Some of the key features and additions are as follows:

- Operation in the 60 GHz band
- New data rates, with the highest reaching 100 Gb/s
- Limiting communication range to 10 centimeters or less
- Use of a pairnet structure and Stack ACK mechanism to simplify and optimize the MAC
- Selectable PHY modes (single carrier and OOK) to achieve either high-speed operation or system simplicity

Interest in developing a close proximity version of a 60 GHz band PHY and associated MAC changes began in 2014. Activity was initially conducted as part of Task Group 3d, formed in May 2014, which covered switched, point-to-point connections operating in the frequencies from 60 GHz up to the lower THz bands. The Application Requirements Document (ARD), Technical Requirements Documents (TRD), channel models, and regulatory issues for close proximity scenarios were reviewed in July 2014. Discussions began to separate the close proximity efforts at 60 GHz from the other activities at the lower THz band in September 2014 and a decision was made in November 2014 to split the Task Group 3d into two, one optimized for ranges under 10 centimeters (3e) and another covering several meters or more (3d). The first meeting of 3e as a task group was held in March 2015 in Berlin, Germany, where the Project Authorization Request (PAR) and Criteria for Standards Development (CSD) were approved. At the May 2015 meeting, the ARD and TRD were combined as a single Technical Guidance Document (TGD) and proposals were reviewed in the July and September 2015 sessions, including the selection of two PHY modes. The group entered working group letter ballot in January 2016. After two working group recirculation ballots, sponsor ballot started in July 2016. A total of three sponsor recirculation ballots were held, leading to approval of IEEE Std 802.15.3e-2017 by the IEEE-SA Standards Board on 14 February 2017.

Contents

2.	Normative references	16
3.	Definitions, acronyms, and abbreviations.....	17
3.1	Definitions	17
3.2	Acronyms and abbreviations	17
4.	General description	17
4.1	What is a piconet?.....	17
4.1a	Pairnet	18
4.2	Components of an IEEE 802.15.3 piconet.....	18
4.2.1	Pairnet components.....	18
4.3	Overview of medium access control (MAC) functionality	18
4.3.1	Coordination	18
4.3.1.1	Starting a piconet or a pairnet	18
4.3.2	Ending a piconet or a pairnet	19
4.3.4	Association and disassociation	19
4.3.5	Security overview	19
4.3.6	The IEEE 802.15.3 superframe.....	19
4.3.7	Channel time management.....	20
4.3.7.1	Channel time management for piconets.....	21
4.3.7.2	Channel time management for pairnets	21
4.3.10	Dynamic channel selection	21
4.3.14	Frame aggregation	21
4.3.16	Channel probing.....	21
4.5	Characteristics of the mmWave PHY	21
4.5a	Characteristics of HRCP PHY	21
4.5a.1	HRCP PHY characteristics	21
4.5a.2	Pairnet using HRCP PHY	22
5.	Layer management.....	22
5.3	MLME SAP interface	22
5.3.2	Scanning for piconets and pairnets	23
5.3.2.1	MLME-SCAN.request	23
5.3.2.2	MLME-SCAN.confirm	24
5.3.2.3	MLME-SCAN.indication	25
5.3.3	Starting a piconet or pairnet.....	25
5.3.3.1	MLME-START.request.....	27
5.3.4	Stopping a piconet or pairnet	27
5.3.4.1	MLME-STOP.request.....	28
5.3.4.2	MLME-STOP.confirm.....	28
5.3.5	Associating with a piconet or pairnet	29
5.3.5.1	MLME-ASSOCIATE.request.....	30
5.3.5.2	MLME-ASSOCIATE.confirm	30
5.3.5.3	MLME-ASSOCIATE.indication	30
5.3.5.4	MLME-ASSOCIATE.response	31
5.3.6	Disassociation from a piconet or pairnet	31
5.3.6.1	MLME-DISASSOCIATE.request	31
5.3.6.3	MLME-DISASSOCIATE.indication.....	32

5.3.7	Security management.....	32
5.3.7.4	MLME-SECURITY-MESSAGE.request.....	34
5.3.7.6	MLME-SECURITY-MESSAGE.indication.....	34
5.3.8	PNC handover.....	34
5.3.9	Requesting DEV information from the PNC.....	34
5.3.10	Security information retrieval.....	34
5.3.10.1	MLME-SECURITY-INFO.request.....	35
5.3.10.2	MLME-SECURITY-INFO.confirm.....	35
5.3.10.3	MLME-SECURITY-INFO.indication.....	35
5.3.13	Stream management.....	35
5.3.15	Power management.....	36
5.3.16	Multicast operations.....	36
5.3.17	Timing synchronization.....	36
5.3.18	Transmit switched diversity (TSD).....	36
5.4	MAC management.....	36
5.4.1	MAC PIB PNC and PRC group.....	36
5.4.2	MAC PIB characteristic group.....	37
5.5	MAC SAP.....	38
5.5.7	MAC-HRCP-DATA.request.....	39
5.5.8	MAC-HRCP-DATA.confirm.....	40
5.5.9	MAC-HRCP-DATA.indication.....	40
5.5.10	MAC-HRCP-MUL-DATA.request.....	40
5.5.11	MAC-HRCP-MUL-DATA.confirm.....	41
5.5.12	MAC-HRCP-MUL-DATA.indication.....	41
6 .	MAC frame formats.....	41
6.2	General frame format.....	41
6.2.1	Frame Control field.....	43
6.2.1.1	Protocol Version field.....	43
6.2.1.2	Frame Type field.....	43
6.2.1.4	ACK Policy field, Imp-ACK Request field, and Blk-ACK field for piconet.....	44
6.2.1.4a	ACK Policy field for pairnet.....	44
6.2.1.9	Logical Channel.....	45
6.2.2a	PairnetID.....	45
6.2.3	SrcID and DestID fields for piconet.....	45
6.2.3a	SrcID and DestID fields for pairnet.....	45
6.2.5	Stream Index field.....	45
6.2.6	MAC header validation.....	45
6.2.7	MAC Frame Body field.....	46
6.2.7.1	Frame Payload field.....	46
6.2.7.2	Secure session ID (SECID) field.....	46
6.2.7.3	Secure Frame Counter (SFC) field.....	46
6.2.7.4	Secure Payload field.....	46
6.2.7.5	Integrity Code field.....	47
6.2.7.7	MAC frame body for pairnet.....	47
6.2.7.8	Security header for pairnet.....	47
6.2.7.9	Secure MAC frame body for pairnet.....	47
6.2.10	TX and ACK Information field for pairnets.....	47
6.3	Format of individual frame types.....	48
6.3.1	Beacon frame.....	48
6.3.1.1	Non-secure Beacon frame for piconet.....	48
6.3.1.1a	Non-secure Beacon frame for pairnet.....	48

6.3.1.2	Secure Beacon frame for piconet.....	50
6.3.1.2a	Secure Beacon frame for pairnet	50
6.3.3	Command frame for piconet.....	51
6.3.3.2	Secure Command frame.....	51
6.3.3a	Command frame for pairnet.....	51
6.3.3a.1	Non-secure Command frame.....	51
6.3.3a.2	Secure command frame	52
6.3.4	Data frame for piconet.....	53
6.3.4a	Data frame for pairnet.....	53
6.3.4a.1	Non-Secure Pairnet Aggregated Data frame	53
6.3.4a.2	Secure Pairnet Aggregated Data frame.....	55
6.3.5a	Multi-protocol Data frame for pairnet	56
6.3.5a.1	Non-Secure Pairnet Aggregated Multi-protocol Data frame.....	56
6.3.5a.2	Secure Pairnet Aggregated Multi-protocol Data frame	57
6.4	Information elements (IEs)	58
6.4.1a	PRC Capability IE	61
6.4.1b	PRDEV Capability IE.....	65
6.4.1c	Pairnet Operation Parameters IE.....	66
6.4.37	MIMO Information IE	69
6.4.38	Higher Layer Protocol Information IE.....	70
6.5	MAC commands	70
6.5.1	Association and disassociation commands	73
6.5.1.1	Association Request command.....	73
6.5.1.2	Association Response command	73
6.5.1.3	Disassociation Request command	74
6.5.2	Security commands.....	75
6.5.2.3	Distribute Key Request command	75
6.5.4.4	Security Information command	75
6.5.4.5	Probe Request command	75
6.5.4.6	Probe Response command	76
6.5.9	Special commands	76
6.5.9.1	Security Message command	76
6.5.9.5	Array Training command.....	77
6.5.9.6	Array Training Feedback	77
7.	MAC functional description	79
7.2a	Starting a pairnet.....	79
7.3a	Association and disassociation with a pairnet	79
7.3a.1	Association.....	79
7.3a.2	Disassociation	81
7.3a.3	Higher layer protocol setup during association procedure for a pairnet.....	82
7.4	Channel access.....	82
7.4.1	Interframe Space (IFS).....	82
7.4.4	PAP after association	83
7.6	Synchronization for piconet.....	84
7.6a	Synchronization for pairnet	84
7.6a.1	Time accuracy.....	84
7.6a.2	Beacon generation.....	84
7.6a.3	Beacon Information announcement	85
7.8	Aggregation	85
7.8.3	Pairnet aggregation	85
7.9	Acknowledgment and retransmission.....	87
7.9.2a	Stk-ACK	88

7.9.2a.1	Ping-pong transmission and Stk-ACK (Synchronous Phase).....	88
7.9.2a.2	Recovery Process (Asynchronous Phase).....	89
7.13	Multi-rate support	89
7.14	Power management for piconets	90
7.14a	Power management for pairnet	90
7.16	MAC sublayer parameters	91
8.	Security	92
8.1	Security mechanisms	92
8.1.2	Key transport.....	92
8.1.4	Data integrity	92
8.1.5	Beacon integrity protection.....	93
8.1.6	Command integrity protection	93
8.1.7	Freshness protection	93
8.2	Security modes.....	94
8.2.2	Security mode 1	94
8.3	Security support	94
8.3.1	PNC handover.....	94
8.3.2	Changes in the piconet group data key or pairnet group data key	94
8.3.3	Joining a secure piconet or secure pairnet	95
8.3.4	Membership update.....	95
8.3.5	Secure frame generation	96
8.3.6	Updating CurrentTimeToken.....	97
8.3.7	Secure frame reception	97
8.3.8	Selecting the SECID for a new key	98
8.3.9	Key selection.....	98
8.4	Protocol details	100
8.4.1	Security information request and distribution	100
8.4.2	Key distribution protocol	101
8.4.3	Key request protocol.....	101
9.	Security specifications	101
9a.	Security specifications for pairnets	101
9a.1	Modes for security	102
9a.2	Symmetric cryptography building blocks.....	102
9a.2.1	Notational conventions	102
9a.2.2	Galois/Counter Mode (GCM) combined encryption and data authentication.....	102
9a.2.3	GCM parameters.....	102
9a.2.4	Nonce value	102
9a.2.5	AES encryption.....	103
9a.3	Symmetric cryptography implementation	103
9a.3.1	Symmetric cryptography data formats.....	103
9a.3.2	Symmetric cryptographic operations	104
9a.4	GCM mode	106
9a.4.1	Inputs for authenticated encryption	106
9a.4.2	Authenticated encryption.....	106
9a.4.3	Outputs from authenticated encryption.....	109
9a.4.4	Inputs for authenticated decryption	109
9a.4.5	Authenticated decryption.....	109
9a.4.6	Restrictions	110
9a.4.7	List of symbols.....	110

11a.	PHY specification for HRCP	110
11a.1	General requirements	110
11a.1.1	Regulatory Information.....	111
11a.1.2	RF power measurements.....	111
11a.1.3	Unwanted emissions	111
11a.1.4	RF channelization	111
11a.1.5	Transmit PSD mask	112
11a.1.6	Error vector magnitude calculation.....	114
11a.1.7	HRCP-PHY management	114
11a.1.7.1	Supported MCSs.....	114
11a.1.7.2	HRCP-PHY PIB	114
11a.2	HRCP-SC PHY	114
11a.2.1	Channelization of HRCP-SC PHY	116
11a.2.2	Modulation and coding	116
11a.2.2.1	MCS dependent parameters.....	116
11a.2.2.2	Header rate-dependent parameters.....	117
11a.2.2.3	Timing-related parameters	117
11a.2.2.4	Frame-related parameters	118
11a.2.2.5	Modulation.....	119
11a.2.2.6	Forward Error Correction	120
11a.2.2.7	Stuff bits.....	122
11a.2.2.8	Code spreading	123
11a.2.2.9	Scrambling	123
11a.2.3	HRCP-SC PHY frame format.....	123
11a.2.3.1	PHY preamble.....	124
11a.2.3.1.1	Frame synchronization (SYNC).....	124
11a.2.3.1.2	SFD	124
11a.2.3.1.3	CES	125
11a.2.3.2	Frame header.....	125
11a.2.3.2.1	HRCP-SC PHY header	127
11a.2.3.2.2	Header HCS	128
11a.2.3.2.3	Header FEC.....	128
11a.2.3.3	HRCP-SC PHY Payload field.....	129
11a.2.3.3.1	HRCP-SC PHY Payload scrambling	129
11a.2.3.3.2	Modulation	129
11a.2.3.3.3	FEC	129
11a.2.3.4	Pilot word and PPRE	130
11a.2.3.4.1	Block and pilot word.....	130
11a.2.3.4.2	PPRE	130
11a.2.4	Transmitter specifications.....	130
11a.2.4.1	EVM requirement	130
11a.2.4.2	Transmit center frequency tolerance.....	131
11a.2.4.3	Symbol rate	131
11a.2.4.4	Transmit power-on and power-down ramp	131
11a.2.5	Receiver specifications	131
11a.2.5.1	Error rate criterion	131
11a.2.5.2	Receiver sensitivity	131
11a.2.5.3	Receiver maximum input level.....	132
11a.2.6	PHY layer timing	132
11a.2.6.1	Interframe space.....	132
11a.2.6.2	Receive-to-transmit turnaround time	133
11a.2.6.3	Transmit-to-receive turnaround-time.....	133
11a.2.6.4	Time between transmission	133

11a.2.6.5	Channel switch.....	133
11a.2.7	PHY management for HRCP-SC PHY.....	133
11a.2.7.1	Maximum frame size	133
11a.2.7.2	Maximum transfer unit size	133
11a.2.7.3	Minimum fragment size.....	133
11a.2.8	MIMO, channel bonding, and channel aggregation	133
11a.2.8.1	Introduction to MIMO in SC-PHY	133
11a.2.8.2	Channel aggregation and channel bonding.....	134
11a.2.8.3	Link setup procedure for MIMO mode.....	134
11a.2.8.4	Selecting antenna element	137
11a.2.8.5	MIMO PHY Preamble	137
11a.2.8.5.1	SYNC	138
11a.2.8.5.2	SFD	138
11a.2.8.5.3	CES for frequency domain channel estimation.....	138
11a.2.8.5.4	CES for time domain channel estimation	138
11a.2.8.6	Data processing for M-streams transmission in MIMO mode or channel aggregation	139
11a.2.8.7	HRCP-SC-MIMO PHY Header.....	139
11a.2.8.8	HRCP-SC PHY MIMO Payload field	139
11a.2.8.9	Scrambler	140
11a.2.8.10	Transmitter specifications	140
11a.2.8.11	Receiver specifications	140
11a.2.8.11.1	Error rate criterion.....	140
11a.2.8.11.2	Receiver sensitivity	140
11a.3	HRCP-OOK PHY	141
11a.3.1	Channel bonding	141
11a.3.1.1	Channelization for HRCP-OOK PHY	141
11a.3.1.2	Transmit PSD mask for HRCP-OOK	142
11a.3.2	Modulation and coding	142
11a.3.2.1	MCS dependent parameters	142
11a.3.2.2	Header rate-dependent parameters.....	143
11a.3.2.3	Timing-related parameters	143
11a.3.2.4	Frame-related parameters	144
11a.3.2.5	Modulation.....	145
11a.3.2.5.1	OOK	145
11a.3.2.5.2	Description of signals.....	146
11a.3.2.6	Forward Error Correction	146
11a.3.2.6.1	Reed-Solomon block codes in GF(28).....	146
11a.3.2.7	Code spreading	148
11a.3.2.7.1	PRBS generation with LFSR	148
11a.3.2.8	Scrambling	149
11a.3.3	HRCP-OOK PHY frame format	150
11a.3.3.1	PHY Preamble	150
11a.3.3.1.1	SYNC	151
11a.3.3.1.2	SFD	151
11a.3.3.1.3	CES	152
11a.3.3.1.4	Preamble Repetition.....	152
11a.3.3.2	Frame Header.....	153
11a.3.3.2.1	HRCP-OOK PHY header.....	154
11a.3.3.2.2	Base header HCS	155
11a.3.3.2.3	Base header FEC	155
11a.3.3.3	HRCP-OOK PHY Payload field.....	155
11a.3.3.3.1	HRCP-OOK PHY Payload scrambling.....	156
11a.3.3.3.2	Modulation	156

11a.3.3.3FEC	156
11a.3.3.3.4Code spreading.....	156
11a.3.3.3.5Blocks and Pilot symbol	156
11a.3.4Transmitter specifications.....	156
11a.3.4.1 Error Vector Magnitude.....	156
11a.3.4.2 Transmit center frequency tolerance.....	157
11a.3.4.3 Symbol rate	157
11a.3.5Receiver specifications	157
11a.3.5.1 Error rate criterion	157
11a.3.5.2 Receiver sensitivity.....	157
11a.3.5.3 Receiver maximum input level.....	158
11a.3.6PHY layer timing.....	158
11a.3.6.1 IFS.....	158
11a.3.6.2 Receive-to-transmit turnaround time.....	158
11a.3.6.3 Transmit-to-receive turnaround time.....	158
11a.3.6.4 Time between transmission	159
11a.3.6.5 Channel switch.....	159
11a.3.7PHY management for HRCP-OOK PHY	159
11a.3.7.1 Mximum frame size.....	159
11a.3.7.2 Maximum transfer unit size.....	159
11a.3.7.3 Minimum fragment size.....	159
Annex C (informative) Security consideration.....	160
Annex E (informative) Protocol implementation conformance statement (PICS) proforma	164

IEEE Standard for High Data Rate Wireless Multi-Media Networks

Amendment 1: High-Rate Close Proximity Point-to-Point Communications

(This amendment is based on IEEE Std 802.15.3™-2016)

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

The editing instructions are shown in ***bold italic***. Four editing instructions are used: change, delete, insert, and replace. ***Change*** is used to make corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using ~~strike through~~ (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editing instructions, change markings, and this NOTE will not be carried over into future editions because the changes will be incorporated into the base standard.¹

2. Normative references

Insert the following new reference in alphabetical order:

NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Morris Dworkin, November 2007.²

¹Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

²NIST publications are available from the National Institute of Standards and Technology (<http://csrc.nist.gov/>).

3. Definitions, acronyms, and abbreviations

3.1 Definitions

Insert the following definitions in alphabetical order:

pairnet setup phase: Phase during which the pairnet beacon is active but pairnet devices are not yet associated.

pairnet associated phase: Phase during which the pairnet devices are associated.

stack acknowledgment (Stk-ACK): An acknowledgment method where the device receiving data returns the frame number to jump back to and starts retransmission when the received frame(s) are corrupted.

3.2 Acronyms and abbreviations

Change the following acronym as indicated:

PNID piconet or pairnet identifier

Insert the following acronyms in alphabetical order:

GCM	Galois/counter mode
HRCP	high rate close proximity
IP	internet protocol
LLPS	low-latency power save
MIMO	multiple-input, multiple-output
OBEX ³	object exchange
PAP	pairnet associated phase
PPRE	pilot preamble
PRC	pairnet coordinator
PRCID	pairnet coordinator identifier
PRDEV	pairnet DEV
PSP	pairnet setup phase
SISO	single-input, single-output
Stk-ACK	stack acknowledgment

4. General description

4.1 What is a piconet?

After 4.1, insert the following new subclause as 4.1a:

³The OBEX word mark and logo are trademarks owned by Infrared Data Association (IrDA®).

4.1a Pairnet

A pairnet consists of at most two DEVs, as shown in Figure 4-0a. Typical communication distance is 10 cm or less for a PRDEV. A PRDEV always connects as a pairnet.

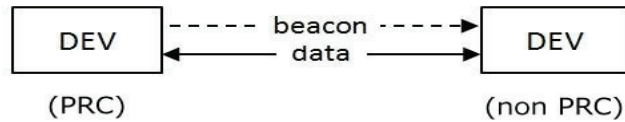


Figure 4-0a—IEEE 802.15.3 pairnet elements

4.2 Components of an IEEE 802.15.3 piconet

Insert the following new paragraph after the third paragraph of 4.2:

For HRCP PHYs, the IEEE 802.15.3 piconet is not used.

After 4.2, insert the following new subclause as 4.2.1:

4.2.1 Pairnet components

An IEEE 802.15.3 pairnet consists of at most two DEVs as components. A Beacon frame is transmitted from a DEV to allow another DEV to connect. The DEV sending the Beacon frame is the pairnet coordinator (PRC). Once a pairnet connection is established, the Beacon frame transmissions are turned off.

4.3 Overview of medium access control (MAC) functionality

4.3.1 Coordination

Insert the following new paragraph after the first paragraph of 4.3.1:

PRDEVs are not capable of participating in a piconet. PRDEVs are used in a pairnet.

Change the title of 4.3.1.1, and insert the following new paragraph at the end of 4.3.1.1:

4.3.1.1 Starting a piconet or a pairnet

A DEV that is capable of acting as the PRC starts the pairnet by initializing the Sequence Number field and Last Received Sequence Number field and then sending the Beacon frame in the default channel. The default channel is defined in 11a.1.4. The PRC need not scan the channels beforehand for availability.

Change the title of 4.3.2, and insert the following new paragraph at the end of 4.3.2:

4.3.2 Ending a piconet or a pairnet

In the case of a pairnet, if the PRC or PRDEV determines that the connected peer is gone, the pairnet is terminated. The PRC or PRDEV terminates a pairnet by sending a Disassociation Request command. The PRC can then restart sending Beacon frames in order to prepare for creating a new pairnet, as described in 8.2.7.

4.3.4 Association and disassociation

Insert the following new paragraph after the second paragraph of 4.3.4:

For a pairnet, a DEV connects to a PRC by sending an Association Request Command during one of the available Access Slots after a Beacon frame is received as specified in 7.3a.1. The peer-to-peer data transfer begins after completion of the association process.

Insert the following new paragraph after the third paragraph of 4.3.4:

Disassociation for pairnet takes place as specified in 7.3a.2.

4.3.5 Security overview

Change the text in 4.3.5 as indicated:

Security for the piconet or pairnet 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. A PRC is allowed to use a list of DEV addresses to admit or deny entry to the pairnet.
- b) Mode 1—Secure membership and payload protection: DEVs establish secure membership with the PNC in a piconet, or with the PRC in a pairnet, before they have access to the piconet's or pairnet'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 or pairnet are required to establish secure membership with the PNC or PRC, respectively. 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, PRC, or DEV that generates and distributes the key is called the key originator.

The payload protection protocol, as described in 9.2.2 for piconets and 9a.2.2 for pairnets, 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. For piconets, 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). For pairnets, Galois/counter mode (GCM) of the AES-128 is used.

4.3.6 The IEEE 802.15.3 superframe

Insert the following new text and Figure 4-2a at the end of 4.3.6:

The superframe structure for pairnets is shown in Figure 4-2a. Carrier sensing is not required during the pairnet setup period (PSP) and pairnet associated period (PAP). Access method during PSP is different from that during PAP.

a) Pairnet setup period (PSP)

A PRC sends a Beacon frame periodically to initiate a P2P connection. A Beacon frame includes information on the number and duration of the access slots which any target DEV can use by responding with an Association Request. The number of access slots is defined in $pNAccessSlot$ and the duration of each slot is defined in $pDAccessSlot$. These values are specified in the Pairnet Synchronization Parameters field set in the Beacon frames, as shown in Figure 6-50b. A target DEV selects one of the access slots to send an Association Request command and sends it at the beginning of the selected access slot.

During the PSP, all frames are transmitted using an MCS from the mandatory MCS set. The superframe duration during the PSP equals the interval between the transmission of Beacon frames with the same PHY mode and is indicated by the Pairnet Synchronization Parameters field in the Beacon frame.

b) Pairnet associated period (PAP)

All frames are sent using SIFS or RIFS. The superframe in PAP starts from the transmission start time of the Association Response command that replaces the Beacon frame. The superframe has no scheduled end time and is terminated by a Disassociation Request command or an ATP expiration.

NOTE—It is recommended that, for the case of single-carrier PHY, $pNAccessSlot$ should be set to 4 in order to optimize the setup time and reduce the probability of collisions between DEVs during the association process.

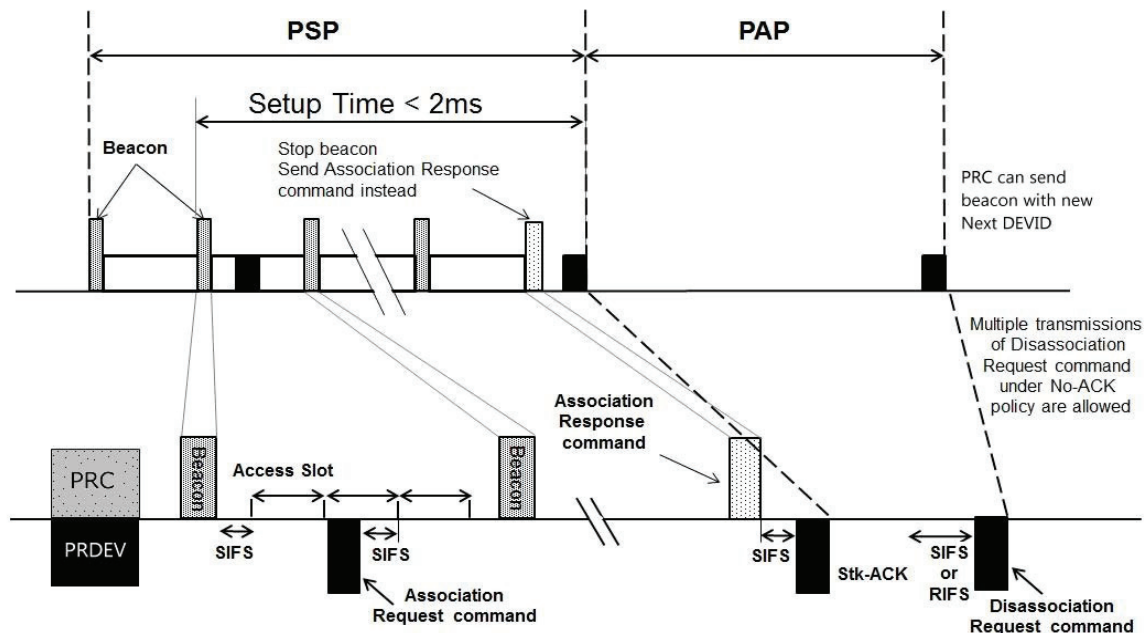


Figure 4-2a—One pairnet session

4.3.7 Channel time management

After 4.3.7, insert the following new subclause title as 4.3.7.1 and move all of 4.3.7 to 4.3.7.1:

4.3.7.1 Channel time management for piconets

After 4.3.7.1, insert the following new subclause as 4.3.7.2:

4.3.7.2 Channel time management for pairnets

There is one method for transmitting data between DEVs that form a pairnet. Data exchanges are achieved during a PAP, which is described in 7.4.4.

4.3.10 Dynamic channel selection

Add the following new sentence to the end of 4.3.10:

This operation is not applicable for pairnets.

4.3.14 Frame aggregation

Change the first paragraph in 4.3.14 as follows:

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. Both use the block acknowledgment (Blk-ACK) mechanism. A third aggregation method is provided for PRDEVs, which is suitable for low-latency, high-efficiency communications and uses the stack acknowledgment (Stk-ACK) feedback mechanism.

4.3.16 Channel probing

Insert the following new paragraph at the end of 4.3.16:

This operation is not applicable to pairnets.

4.5 Characteristics of the mmWave PHY

After 4.5, insert the following new subclauses as 4.5a, 4.5a.1, and 4.5a.2:

4.5a Characteristics of HRCP PHY

4.5a.1 HRCP PHY characteristics

The HRCP PHY, as described in Clause 11a, is designed for a high data-rate application. The frequency band is 57.0–66.0 GHz, the same as that for the mmWave PHY.

Two PHYs are defined for the HRCP PHY. They are as follows:

- a) Single Carrier mode in HRCP (HRCP-SC) PHY, as described in 11a.2
- b) OOK mode in HRCP (HRCP-OOK) PHY, as described in 11a.3

For DEVs that implement the HRCP PHY, at least one of the PHYs is required. The HRCP PHY supports channel bonding using up to four channels for high throughput.

The HRCP-SC PHY is designed for extremely high PHY-SAP payload bit-rate up to 13 Gb/s with a single channel and up to 157 Gb/s with a multiple input, multiple output (MIMO) channel. The SC PHY supports a wide range of modulations, $\pi/2$ BPSK, $\pi/2$ QPSK, 16-QAM, 64-QAM, and 256 QAM. The FEC scheme defines user rate-compatible low-density parity-check (LDPC) codes with rates of 14/15 and 11/15. Channel aggregation is supported in HRCP-SC PHY.

The HRCP-OOK PHY is designed for cost effective DEVs that require low power, low complexity and simple design. The HRCP-OOK PHY supports a single modulation scheme, OOK, and a single FEC scheme, RS. Channel aggregation and MIMO are not used in HRCP-OOK PHY.

4.5a.2 Pairnet using HRCP PHY

When a PRC-capable DEV starts a pairnet, the type of pairnet it starts depends on the PHY modes that are supported. For example, if the PRC-capable DEV supports only the HRCP-SC mode, it would start an HRCP-SC pairnet in which the Beacon frame is sent with the HRCP-SC mode. DEVs that support only the HRCP-SC mode are able to find and connect to the pairnet in HRCP-SC mode.

The same process is used for a PRC-capable DEV that supports only HRCP-OOK mode. If a PRC-capable DEV supports more than one HRCP PHY mode, then it is able to select the type of pairnet it starts. It allows connection from each type of DEV by transmitting both the HRCP-SC mode Beacon frame and the HRCP-OOK mode Beacon frame. Figure 4-3a is an example of transmitting dual mode Beacon frames. The number and duration of the access slots and the superframe duration for each PHY mode are indicated by the Beacon frame with the corresponding PHY mode.

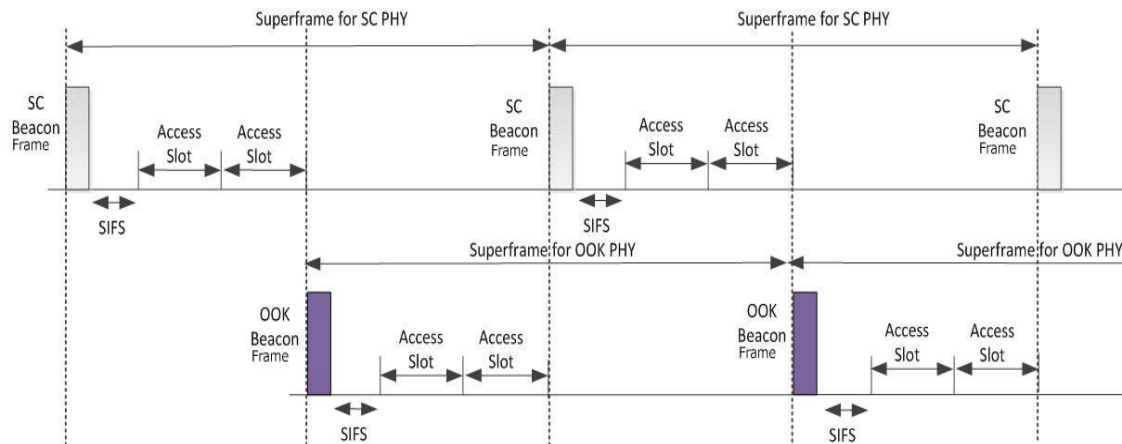


Figure 4-3a—Example of transmitting dual mode beacons

5. Layer management

5.3 MLME SAP interface

Change Table 5-3 and insert the following note (the entire table is not shown) as indicated:

Table 5-3—Summary of MLME primitives

Name	Request	Confirm	Indication	Response
MLME-ASSOCIATE	5.3.5.1	5.3.5.2	5.3.5.3	<u>5.3.5.4</u>
NOTE 1—MLME-ASSOCIATE.Response primitive is valid only for pairnets.				

Insert the following new paragraph at the end of 5.3:

For piconets and pairnets, the MLME interface models a single piconet or pairnet environment; while support for multiple pairnets for PRDEVs is not allowed, support for multiple piconets for non-PRDEVs is implementation-dependent.

Change the title and first paragraph of 5.3.2 as follows:

5.3.2 Scanning for piconets and pairnets

These primitives support the process of determining the presence or absence of piconets or pairnets, as described in 7.2.1. The parameters used for these primitives are defined in Table 5-5.

Change Table 5-5 (the entire table is not shown) as indicated:

Table 5-5—MLME-SCAN primitive parameters

Name	Type	Valid range	Description
ScanForBsid	Boolean	TRUE, FALSE	Indicates if the scan process should search for a specific BSID, as described in 7.2.1. <u>Not applicable for pairnets.</u>
<u>ScanMode</u>	<u>Enumeration</u>	<u>IMMEDIATE,</u> <u>TIMEOUT</u>	<u>Indicates the scan mode for pairnets.</u>
<u>NumberOfPairnets</u>	<u>Integer</u>	<u>0–255</u>	<u>The number of pairnets found during the scanning process.</u>
<u>PairnetDescriptionSet</u>	<u>Set of pairnet descriptions, as defined in Table 5-6a</u>	<u>A set containing zero or more instances of a PairnetDescription</u>	<u>The PairnetDescriptionSet is returned to indicate the results of the scan request.</u>

Add the following new paragraph and Table 5-6a at the end of 5.3.2:

In Table 5-5, a PairnetDescriptionSet is a set of PairnetDescriptions. Each PairnetDescription consists of the elements shown in Table 5-6a.

5.3.2.1 MLME-SCAN.request

Change the first two paragraphs of 5.3.2.1 as follows:

Table 5-6a—Elements of PairnetDescription

Name	Type	Valid range	Description
Bsid	Octet string	As defined in 6.4.2	The text string identifier of a discovered pairnet.
Pnid	Integer	0–65535	The PNID of a discovered pairnet.
PrcAddress	MAC address	Any valid individual MAC address	The MAC address of the PRC of the pairnet that was found.
SECmode	Enumeration	MODE_0, MODE_1	The security mode of the pairnet that was found, as described in 6.3.1.
SignalQuality	Integer	0–15	Indicates the quality of the received frame or beacon for this pairnet. The value is implementation dependent, with 0 indicating the lowest quality and 15 the highest quality.
PrcCapability	PRC Capability, as defined in 6.4.11a	As defined in 6.4.11a	Capability of the PRC in the Beacon frame.
HigherLayerProtocolInformation	As defined in the Higher Layer Protocol Information IE	As defined in 6.4.38	Included 3 octets Unique ID and Higher Layer Protocol Information in variable length.
PhyMode	Enumeration	HRCP_SC_PHY, HRCP_OOK_PHY, HRCP_BOTH_PHY	The PHY mode that is being used in the pairnet that was found.

This primitive is used to initiate the passive scan procedure to search for either a specific piconet or pairnet if ScanForBsid is TRUE and as indicated by Bsid, or any piconet or pairnet if ScanForBsid is FALSE. The semantics of this primitive are as follows:

```
MLME-SCAN.request
(
  ScanForBsid,
  Bsid,
  ScanForPnid,
  Pnid,
  ScanForPncAddress,
  PncAddress,
  ScanMode,
  Timeout
)
```

5.3.2.2 MLME-SCAN.confirm

Change the first paragraph of 5.3.2.2 as follows:

This primitive is used to report the result of the request to initiate the passive scan procedure to search for either a specific piconet or pairnet if ScanForBsid is TRUE and as indicated by Bsid, or any piconet or pairnet if ScanForBsid is FALSE. The semantics of this primitive are as follows:

Insert the following new parameter at the end of the list in 5.3.2.2 (before the closing parenthesis):

```
MLME-SCAN.confirm      (  
    NumberOfPiconets,  
    PiconetDescriptionSet,  
    NumberOfChannels,  
    ChannelRatingList,  
    ResultCode,  
    ReasonCode,  
    NumberOfPairnets,  
    PairnetDescriptionSet  
)
```

Change the second paragraph of 5.3.2.2 as follows:

The primitive parameters are defined in Table 5-5. All of the piconets found during the scan will be reported in separate elements of the PiconetDescriptionSet, even if more than one piconet is found on a given channel. For a PRDEV, only pairnets will be reported.

5.3.2.3 MLME-SCAN.indication

Insert the following new parameter at the end of the list in 5.3.2.3 (before the closing parenthesis):

```
MLME-SCAN.indication    (  
    NumberOfPiconets,  
    PiconetDescriptionSet,  
    NumberOfChannels,  
    ChannelRatingList,  
    NumberOfPairnets,  
    PairnetDescriptionSet  
)
```

Change the second paragraph as indicated:

The primitive parameters are defined in Table 5-5. For a PRDEV, only pairnets will be reported immediately if the ScanMode parameter is set to IMMEDIATE. If the ScanMode parameter is set to TIMEOUT, the result will be reported after the SCAN Timeout timer expires.

5.3.3 Starting a piconet or pairnet

Change the first paragraph of 5.3.3 as follows:

These primitives support the process of creating a new piconet or pairnet with the DEV acting as PNC or PRC, as described in 7.2.2. The parameters used for these primitives are defined in Table 5-8.

Change Table 5-8 (the entire table is not shown) as indicated:

Table 5-8—MLME-START primitive parameters

Name	Type	Valid range	Description
Bsid	Octet string	As defined in 6.4.2	The BSID of the new piconet <u>or pairnet</u> .
SecMode	Enumeration	MODE_0, MODE_1	The security mode of the piconet <u>or pairnet</u> , as described in 6.3.1.
DevId	Integer	Any valid DEVID, as defined in 6.2.3	The assigned DEVID for the DEV that is acting as the PNC, as described in 7.2.2. <u>This parameter is not valid for PRDEVS.</u>
MinDepSuperframePercent	Integer	1–100	The minimum percent of the superframe requested as a CTA for the dependent piconet, as described in 7.2.7 and 7.2.8. <u>This parameter is not valid for PRDEVS.</u>
DesiredDepSuperframePercent	Integer	1–100	The desired percent of the superframe requested as a CTA for the dependent piconet, as described in 7.2.7 and 7.2.8. <u>This parameter is not valid for PRDEVS.</u>
AllocatedSuperframePercent	Integer	0–100	The percent of the superframe allocated to the new dependent piconet. If the channel time request was rejected, the value shall be set to zero. This parameter is ignored if the DEV is starting an independent piconet. <u>This parameter is not valid for PRDEVS.</u>
ResultCode	Enumeration	SUCCESS, FAILURE	Indicates the result of the MLME request.
ReasonCode	Enumeration	NOT_PNC_CAPABLE, NO_CHANNELS_AVAILABLE, ALREADY_PNC, OTHER	Indicates the reason for a ResultCode of FAILURE.
PhyMode	Enumeration	2.4_GHZ, SC_MMWAVE, HSI_MMWAVE, AV_MMWAVE, <u>HRCP SC PHY</u> , <u>HRCP OOK PHY</u> , <u>HRCP_BOTH_PHY</u>	The PHY that will be used for the Beacon frames and the CP(s) in the piconet <u>or pairnet</u> that will be started.
<u>PrcCapabilityIe</u>	<u>PRC Capability, as defined in 6.4.11a</u>	<u>As defined in 6.4.11a</u>	<u>Capability of the PRC in the Beacon frame.</u>
<u>HigherLayerProtocol Information</u>	<u>As defined in the Higher Layer Protocol Information IE</u>	<u>As defined in 6.4.38</u>	<u>Includes 3 octets Unique ID and HigherLayerProtocol Information in variable length</u>

5.3.3.1 MLME-START.request

Change the first paragraph of 5.3.3.1 as follows:

This primitive is used to start a piconet or pairnet. If the DEV is not a member of the piconet or pairnet, this primitive causes the DEV to start an independent piconet or pairnet. If the DEV is a member of the piconet, this primitive causes the DEV to start a child piconet. If the DEV is associated as a neighbor member of a piconet, this primitive causes the DEV to start a neighbor piconet. The semantics of this primitive are as follows:

Insert the following new parameter at the end of the list in 5.3.3.1 (before the closing parenthesis):

```
MLME-START.request      (  
                          Bsid,  
                          SecMode,  
                          MinDepSuperframePercent,  
                          DesiredDepSuperframePercent,  
                          PhyMode,  
                          PrcCapabilityIe,  
                          HigherLayerProtocolInformation  
                          )
```

Change the title and first paragraph of 5.3.4 as follows:

5.3.4 Stopping a piconet or pairnet

These primitives support the process of stopping operations as a PNC or PRC. The process may result in the shutdown of piconet or pairnet operations, as described in 7.2.9, or the handover of PNC operations to another DEV in the piconet, as described in 7.2.3 and 7.2.6. The parameters used for these primitives are defined in Table 5-9.

Change Table 5-9 (the entire table is not shown) as indicated:

Table 5-9—MLME-STOP primitive parameters

Name	Type	Valid range	Description
RequestType	Enumeration	SHUTDOWN, HANDOVER	If SHUTDOWN, the current piconet operations will be stopped. If HAN-DOVER, an attempt to handover PNC operations will be made. <u>Only SHUT-DOWN is valid for PRDEV.</u>
AllowedHandoverTime	Duration	0–65535	If RequestType is HANDOVER, the time in milliseconds in which a handover attempt must be completed. <u>This parameter is not valid for PRDEV.</u>
NumHandoverTargetDev	Integer	0– <i>mMaxNumValid-DEVS</i>	The number of DEVs in the Handover-TargetList. <u>This parameter is not valid for PRDEVs.</u>
HandoverTargetList	List of DEVIDs	0 to maximum number of DEVIDs, as defined in 6.2.3	If RequestType is HANDOVER, specifies a list of Target DEVIDs for a handover attempt. <u>This parameter is not valid for PRDEV.</u>
ResultCode	Enumeration	SUCCESS, FAILURE	Indicates the result of the MLME request.
ReasonCode	Enumeration	NOT_A_PNC, HANDOVER - FAILED, ~~HIGH- ER_LAYER_DENI- ED, HIGHER LAY- ER REQUESTED,~~ OTHER	Indicates the reason for a ResultCode. <u>NOT_A_PNC and HANDOVER - FAILED are not valid responses for PRDEVs.</u>

5.3.4.1 MLME-STOP.request

Change the first paragraph of 5.3.4.1 as follows:

This primitive initiates the piconet or pairnet shutdown procedure or the piconet handover procedure. The semantics of this primitive are as follows:

5.3.4.2 MLME-STOP.confirm

Change the first paragraph of 5.3.4.2 as follows:

This primitive reports the results of the request to stop operations as a PNC or PRC. The semantics of this primitive are as follows:

Change the title and first paragraph of 5.3.5 as follows:

5.3.5 Associating with a piconet or pairnet

The following primitives support the process of a DEV associating with a PNC or PRC, as defined in 7.3.1. The parameters used for these primitives are defined in Table 5-10.

Change Table 5-10 as indicated. Only those rows being changed or inserted are shown:

Table 5-10—MLME-ASSOCIATE primitive parameters

Name	Type	Valid range	Description
Bsid	Octet string	As defined in 6.4.2	The BSID of the target PNC <u>or</u> PRC for the association.
Pnid	Integer	0–65535	The PNID of the target PNC <u>or</u> PRC for the association, as defined in 6.2.2.
PncAddress	MAC address	Any valid individual MAC address	The MAC address of the target PNC <u>or</u> PRC for the association.
PiconetServicesInquiry	Boolean	TRUE, FALSE	Requests that the PNC <u>or</u> PRC send the services information about the piconet or pairnet, as described in 7.3.2.
NeighborPiconetRequest	Boolean	TRUE, FALSE	Indicates that the DEV will join as a neighbor PNC rather than as a member of the piconet. <u>Not valid for PRDEV.</u>
<u>PrdevCapabilityIe</u>	<u>PRDEV Capability as defined in 6.4.11b</u>	<u>As defined in 6.4.11b</u>	<u>Capability of the PRDEV in the Association Request command.</u>
<u>PairnetOperationParametersIe</u>	<u>As defined in 6.4.11c</u>	<u>As defined in 6.4.11c</u>	<u>Capability of the PRDEV in the Association Response command.</u>
ReasonCode	Enumeration	REQUEST_TIMEOUT, PNC_NOT_FOUND, PNC_DENIED, PNCBUSY, ALREADY_ASSOCIATED, NEIGHBOR_REFUSED, <u>HIGHER_LAYER_DENIED</u> , OTHER	Indicates the reason for a ResultCode of FAILURE. For PRDEVs, <u>NEIGHBOR_REFUSED is not applicable.</u>
<u>HigherLayerProtocolInformation</u>	<u>As defined in the Higher Layer Protocol Information IE</u>	<u>As defined in 6.4.38</u>	<u>Includes 3 octets, Unique ID and Higher Layer Protocol Information in variable length.</u>

Change the first and second paragraphs of 5.3.5.1 as follows:

5.3.5.1 MLME-ASSOCIATE.request

This primitive initiates the association procedure. The semantics of this primitive are as follows:

```
MLME-ASSOCIATE.request    (  
    Bsid,  
    Pnid,  
    PncAddress,  
    ChannelIndex,  
    NeighborPiconetRequest,  
    PiconetServicesInquiry,  
    PrdevCapabilityIe,  
    Timeout,  
    HigherLayerProtocolInformation  
)
```

The primitive parameters are defined in Table 5-10.

Change the first and second paragraphs of 5.3.5.2 as follows:

5.3.5.2 MLME-ASSOCIATE.confirm

This primitive reports the result of the association procedure. The semantics of this primitive are as follows:

```
MLME-ASSOCIATE.confirm    (  
    DevId,  
    VendorSpecificIe,  
    PairnetOperationParametersIe,  
    HigherLayerProtocolInformation,  
    ResultCode,  
    ReasonCode  
)
```

5.3.5.3 MLME-ASSOCIATE.indication

Change the first paragraph of 5.3.5.3 as follows:

This primitive is used to indicate that a new non-PRDEV has associated with the same piconet as this DEV_x or a new PRDEV has associated with this PRDEV. The semantics of this primitive are as follows:

```
MLME-ASSOCIATE.indication (  
    DevId,  
    DevAddress,  
    PairnetOperationParametersIe,  
    HigherLayerProtocolInformation,  
)
```

After 5.3.5.3, insert the following new subclause as 5.3.5.4:

5.3.5.4 MLME-ASSOCIATE.response

This primitive is used to indicate the DEVID that the PRC has selected to associate with. The semantics of this primitive are as follows:

```
MLME-ASSOCIATE.response    (
                             DevId,
                             PncAddress,
                             HigherLayerProtocolInformation,
                             ResultCode,
                             ReasonCode
                             )
```

The primitive parameters are defined in Table 5-10.

Change the title and first paragraph of 5.3.6 as follows:

5.3.6 Disassociation from a piconet or pairnet

The following primitives are used when a DEV disassociates from a PNC or PRC and when the PNC or PRC disassociates a DEV from the piconet or pairnet, as described in 7.3.4. For the pairnet, disassociation by either the DEV or the PRC invokes termination of the pairnet. The parameters used for these primitives are defined in Table 5-11.

Change Table 5-11 (the entire table is not shown) as indicated:

Table 5-11—MLME-DISASSOCIATE primitive parameters

Name	Type	Valid range	Description
ReasonCode	Enumeration	REQUEST_TIMEOUT, NOT_ASSOCIATED, CURRENTLY_PNC, DEV_ATP_EXPIRED, PNC_ATP_EXPIRED, DEV_DISASSOCIATED, OTHER_PNC_ACTION, <u>HIGHER_LAYER_INITIATED.</u> UNKNOWN	Indicates the reason for the disassociation of a DEV from a piconet <u>or pairnet</u> .

5.3.6.1 MLME-DISASSOCIATE.request

Change the first and second paragraphs of 5.3.6.1 as follows:

This primitive initiates the procedure for a DEV to disassociate from a piconet or pairnet. The semantics of this primitive are as follows:

```
MLME-DISASSOCIATE.request (
    DevId,
    DEVAddress,
    Timeout,
    ReasonCode,
)
```

The primitive parameters are~~is~~ defined in Table 5-11.

5.3.6.3 MLME-DISASSOCIATE.indication

Change the first paragraph of 5.3.6.3 as follows:

This primitive is used to indicate that either this DEV or another DEV has been disassociated from the piconet or pairnet. The semantics of this primitive are as follows:

5.3.7 Security management

Change Table 5-12 and Table 5-13 as follows:

Table 5-12—MLME-MEMBERSHIP-UPDATE and MLME-SECURITY-ERROR primitive parameters

Name	Type	Valid range	Description
SECID	2 octets	As defined in 6.2.7.2	The identifier for the key.
OrigId	Integer	Any valid DEVID, as defined in 6.2.3 <u>for piconet and as defined in 6.2.3a for pairnet</u> , except for the BestID, the McstID or the UnassocID	Either the PNCID <u>or</u> PRCID, if this key is for the DEV's PNC <u>or</u> PRC personality, or the DEV's DEVID.
TrgtId	Integer	Any valid DEVID, as defined in 6.2.3 <u>for piconet and as defined in 6.2.3a for pairnet</u> , except for the BestID, the McstID or the UnassocID	The DEVID of the target DEV for this relationship.
MembershipStatus	Enumeration	MEMBER, NON-MEMBER	Indicates the membership status for the provided SECID. If NON-MEMBER, KeyInfo is zero length.
KeyOriginator	Boolean	TRUE, FALSE	Indicates if the DEV is the key originator for this relationship. This is always true when the OrigId is the PNCID <u>or</u> PRCID.
KeyInfo	Octet string	Any valid symmetric key for the symmetric key security operations, as defined in 9.3 <u>for piconet and as defined in 9a.3 for pairnet</u>	The key used for protecting frames between this DEV and the TrgtId DEV.

Table 5-12—MLME-MEMBERSHIP-UPDATE and MLME-SECURITY-ERROR primitive parameters (continued)

Name	Type	Valid range	Description
SrcID	Integer	Any valid DEVID, as defined in 6.2.3 for <u>piconet</u> and as defined in 6.2.3a for <u>pairnet</u> , except for the BestID, the McstID or the UnassocID	The DEVID of the DEV that is the source of a security error.
Timeout	Integer	0–65535	The time in milliseconds allowed for the primitive to complete.
ResultCode	Enumeration	SUCCESS, FAILURE	Indicates the result of the MLME request.
ReasonCode	Enumeration	NOT_ASSOCIATED, TARGET_UNAVAILABLE, UNAVAILABLE_KEY, FAILED_SECURITY_CHECK, BAD_TIME_TOKEN, INVALID_SEC_VALUE, <u>BAD_SFC</u> , OTHER	The reason for a security error.

Table 5-13—MLME-SECURITY-MESSAGE primitive parameters

Name	Type	Valid range	Description
TrgtId	Integer	Any valid DEVID, as defined in 6.2.3 for <u>piconet</u> and as defined in 6.2.3a for <u>pairnet</u>	Specifies the DEVID of the target of the MLME request.
OrigId	Integer	Any valid DEVID, as defined in 6.2.3 for <u>piconet</u> and as defined in 6.2.3a for <u>pairnet</u>	Specifies the DEVID of the originator of the MLME request.
UniqueId	Octet string	Any valid OUI or CID, as defined in 6.4.7	A unique identifier for the entity that defines the format of the security information, as described in 6.4.7.
SecurityInformation	Octet string	Any valid octet string	Security information that will be passed from one DEV to another peer DEV in the <u>piconet</u> or <u>pairnet</u> .
Timeout	Integer	0–65535	The time in milliseconds allowed for the primitive to complete.
ResultCode	Enumeration	SUCCESS, FAILURE	Indicates the result of the MLME request.
ReasonCode	Enumeration	REQUEST_TIMEOUT, NOT_ASSOCIATED, TARGET_UNAVAILABLE, OTHER	The reason for a security error.

5.3.7.4 MLME-SECURITY-MESSAGE.request

Change the first paragraph of 5.3.7.4 as follows:

This primitive initiates the sending of a Security Message command, as described in 6.5.9.1, to the target DEV in the piconet or pairnet. The semantics of this primitive are as follows:

5.3.7.6 MLME-SECURITY-MESSAGE.indication

Change the first paragraph of 5.3.7.6 as follows:

This primitive reports the reception of a Security Message command, as described in 6.5.9.1, from a DEV in the piconet or pairnet. The semantics of this primitive are as follows:

5.3.8 PNC handover

Insert the following new paragraph before the first paragraph of 5.3.8:

This function is not applicable for pairnets.

5.3.9 Requesting DEV information from the PNC

Insert the following new paragraph before the first paragraph of 5.3.9:

This function is not applicable for pairnets.

5.3.10 Security information retrieval

Change the first paragraph of 5.3.10 and Table 5-16 as follows:

These primitives are used to request security information about other DEVs in the piconet or pairnet, as described in 8.4.1. The parameters used for the MLME-SECURITY-INFO primitives are defined in Table 5-16.

Table 5-16—MLME-SECURITY-INFO primitive parameters

Name	Type	Valid range	Description
QueriedDevId	Integer	Any valid DEVID, as defined in 6.2.3 <u>for piconet and as defined in 6.2.3a for pairnet</u> , except for the McastID or the UnassocID	The DEVID of the DEV for which information is being requested. If it is set to the BestID, then the information is being requested for all DEVs.
TrgtId	Integer	Any valid DEVID, as defined in 6.2.3 <u>for piconet and as defined in 6.2.3a for pairnet</u>	The DEVID of the DEV for which the security information request is intended.
OrigId	Integer	Any valid DEVID, as defined in 6.2.3 <u>for piconet and as defined in 6.2.3a for pairnet</u>	Specifies the DEVID of the DEV that initiated the MLME request.

Table 5-16—MLME-SECURITY-INFO primitive parameters (continued)

Name	Type	Valid range	Description
NumSecurityRecords	Integer	0–65535	Number of entries in the SecurityRecordSet.
SecurityRecordSet	A set of Security Record fields, as defined in 6.5.4.4	A set containing 0 or more instances of variable-length Security Record field. The maximum number of instances depends on the size of the records, <i>pMaxFrameBodySize</i> and the length of the secure command security fields, as defined in 6.3.3.2 for piconet and as defined in 6.3.3a for pairnet.	The SecurityRecordSet is returned to indicate the results of a Security Information Request command.
Timeout	Integer	0–65535	The time in milliseconds allowed for the primitive to complete.
ResultCode	Enumeration	SUCCESS, FAILURE	Indicates the result of the MLME request.
ReasonCode	Enumeration	REQUEST_TIMEOUT, NOT_ASSOCIATED, TARGET_NOT_ASSOCIATED, OTHER	Indicates the reason for a ResultCode of FAILURE.

5.3.10.1 MLME-SECURITY-INFO.request

Change the first paragraph of 5.3.10.1 and Table 5-16 as follows:

This primitive initiates a request to a DEV for security information regarding either a single DEV or all of the DEVs in the piconet or pairnet. The semantics of the primitive are as follows:

5.3.10.2 MLME-SECURITY-INFO.confirm

Change the first paragraph of 5.3.10.2 as follows:

This primitive reports the result of the request to a DEV for security information regarding either a single DEV or all of the DEVs in the piconet or pairnet. The semantics of the primitive are as follows:

5.3.10.3 MLME-SECURITY-INFO.indication

Change the first paragraph of 5.3.10.3 as follows:

This primitive indicates the reception of a request by a DEV for security information it manages regarding either a specific DEV or all of the DEVs in the piconet or pairnet. The semantics of the primitive are as follows:

5.3.13 Stream management

Insert the following new paragraph before the first paragraph of 5.3.13:

This function is not applicable for pairnets.

5.3.15 Power management

Change the first sentence of 5.3.15 as follows:

This mechanism supports the process of establishment and maintenance of power management (PM) modes of a DEV, as described in 7.14, and is applicable for piconets only.

5.3.16 Multicast operations

Change the first sentence of 5.3.16 as follows:

These primitives support multicast operations and thus are not applicable for pairnets that do not use multicast.

5.3.17 Timing synchronization

Insert the following new paragraph after the first paragraph of 5.3.17:

This function is not applicable for pairnets.

5.3.18 Transmit switched diversity (TSD)

Insert the following new paragraph before the first paragraph of 5.3.18:

This subclause only applies to mmWave DEVs.

5.4 MAC management

Change the title of 5.4.1 as follows:

5.4.1 MAC PIB PNC and PRC group

Insert the following new paragraph and Table 5-28a after Table 5-28:

The MAC PIB PRC group, given in Table 5-28a, describes the DEV's PRC capabilities as well as the characteristics of the current pairnet.

Table 5-28a—MAC PIB PRC group parameters

Managed Object	Octets	Definition	Access
<i>macSuperframeDuration</i>	2	Duration of the superframe.	Read Only
<i>macNumAssocSlots</i>	1	Number of association slot.	Read Only
<i>macDurAssocSlots</i>	1	Duration of an association slot.	Read Only

Table 5-28a—MAC PIB PRC group parameters (continued)

Managed Object	Octets	Definition	Access
<i>macPrcCapable</i>	1 bit	1 if the DEV has the capability to become the PRC, 0 otherwise.	Read Only
<i>macPrcDesMode</i>	1 bit	1 if it is desired that the DEV be the PRC, 0 otherwise. Provided only for PRC.	Read/Write
<i>macSec</i>	1 bit	1 if the DEV is capable of operating a secure pairnet as the PRC, 0 otherwise.	Read Only
<i>macAllowedChannelSet</i>	Variable	A set of channel indices, one for each channel that the MAC is allowed to use for scanning and starting pairnet.	Read/Write
<i>macAssocVendorSpecificle</i>	Variable	A Vendor Defined IE, as defined in 6.4.3, that is sent in the Association Response command, as described in 6.5.1.2, when the PRDEV is acting as the PRC.	Read/Write
<i>macAssocHigherLayerIe</i>	Variable	A Higher layer protocol information IE, as defined in 6.4.38, that is sent in the Beacon frame and association related commands, as described in 7.3a.3, when the PRDEV is acting as the PRC. Provided only for PRC.	Read/Write
<i>macDesiredAtp</i>	2	The ATP value to send in an Association Request command.	Read/Write
<i>macNextDevId</i>	1	The Next DEVID value to send in a Beacon frame.	Read/Write

5.4.2 MAC PIB characteristic group

Insert the following new paragraph and Table 5-29a after Table 5-29:

The MAC PIB PRDEV characteristics group, given in Table 5-29a, contains information about the capabilities and characteristics of the PRDEV.

Table 5-29a—MAC PIB PRDEV characteristic group parameters

Managed Object	Octets	Definition	Access
<i>macDevAddress</i>	6	The MAC address of the PRDEV.	Read Only
<i>macDevId</i>	1	The ID of the PRDEV.	Read Only
<i>macPowerManagementMode</i>	1	The current power management mode of the PRDEV. 0x00 = ACTIVE From 0x01 to 04, ignored 0x05 = LLPS	Read Only

Table 5-29a—MAC PIB PRDEV characteristic group parameters (continued)

Managed Object	Octets	Definition	Access
<i>macLlpsSupported</i>	1	0x00 = PRDEV does not support LLPS mode. 0x01 = PRDEV supports LLPS mode.	Read Only
<i>macPowerSource</i>	1	0x00 = Battery power. 0x01 = Mains power.	Read/Write
<i>macSecurityOptionImplemented</i>	1	0x00 = Mode 0. 0x01 = Mode 1.	Read Only
<i>macAggregationCapable</i>	1	0x00 = PRDEV does not support aggregation. 0x01 = PRDEV supports aggregation.	Read Only

5.5 MAC SAP

Change Table 5-30 as follows:

Table 5-30—Summary of MAC SAP primitives

Name	Request	Confirm	Indication	Response
MAC-ASYNC-DATA	5.5.1	5.5.2	5.5.3	—
MAC-ISOCH-DATA	5.5.4	5.5.5	5.5.6	—
<u>MAC-HRCP-DATA</u>	<u>5.5.7</u>	<u>5.5.8</u>	<u>5.5.9</u>	—
<u>MAC-HRCP-MUL-DATA</u>	<u>5.5.10</u>	<u>5.5.11</u>	<u>5.5.12</u>	—

Change the title and insert the following rows at the end of Table 5-31:

Table 5-31—MAC-ISOCH-DATA, and MAC-ASYNC-DATA, MAC-HRCP-DATA, and MAC-HRCP-MUL-DATA primitive parameters

Name	Type	Valid range	Description
<u>LogicalChannel</u>	<u>Enumeration</u>	<u>CH0, CH1</u>	<u>LogicalChannel value is available for use by the Higher Layer Protocol user and is therefore out of scope of this specification. This parameter is valid only for MAC-HRCP-DATA primitives.</u>
MCSIdentifier	Enumeration	Any valid MCS identifier, as defined in Table 11a-6	MCS used in the transmitted PHY frame. Only applicable for HRCP SC PHY.
ChIdentifier	Enumeration	Any valid combinations of channel, as defined in Figure 11a-1	The frequency channel used in the transmitted PHY frame. Only applicable for HRCP SC PHY.

Table 5-31—MAC-ISOCH-DATA, and MAC-ASYNC-DATA, MAC-HRCP-DATA, and MAC-HRCP-MUL-DATA primitive parameters (continued)

Name	Type	Valid range	Description
<u>DataID</u>	<u>Enumeration</u>	<u>ETHERTYPE_PROT</u> <u>OCOL_DISCRIMINA</u> <u>TION_OUI_CID_</u> <u>ETHERTYPE</u>	<u>The DataID specifies Data header type</u>
<u>DestinationAddress</u>	<u>MAC Address</u>	<u>Any valid individual</u> <u>MAC address</u>	<u>The destination address representing the</u> <u>address of data destination when the</u> <u>DataID is</u> <u>“ETHERTYPE_PROTOCOL_DISCRI</u> <u>MINATION”</u>
<u>SourceAddress</u>	<u>MAC Address</u>	<u>Any valid individual</u> <u>MAC address</u>	<u>The source address representing the</u> <u>address of data origin when the DataID</u> <u>is</u> <u>“ETHERTYPE_PROTOCOL_DISCRI</u> <u>MINATION”</u>
<u>Ethertype</u>	<u>Octet string</u>	<u>Ethertype defined in</u> <u>IEEE Std 802-2014</u>	<u>The Ethertype specified when DataID is</u> <u>“ETHERTYPE_PROTOCOL_DISCRI</u> <u>MINATION” or “ETHERTYPE”</u>
<u>OUI_CID</u>	<u>Octet string</u>		<u>The OUI or CID strings specified when</u> <u>DataID is “OUI_CID”</u>
<u>LogicalChannel</u>	<u>Enumeration</u>	<u>CH0, CH1</u>	<u>LogicalChannel value is available for</u> <u>use by the Higher Layer Protocol user</u> <u>and is therefore out of scope of this</u> <u>specification. This parameter is valid</u> <u>only for MAC-HRCP-DATA primitives.</u>

After 5.5.6, insert the following new subclauses as 5.5.7–5.5.12:

5.5.7 MAC-HRCP-DATA.request

This primitive is used to initiate the transfer of an MSDU from one MAC entity to another MAC entity or entities using HRCP PHY. The semantics of this primitive are as follows:

```
MAC-HRCP-DATA.request (
    RequestID,
    LogicalChannel,
    ACKRequested,
    ConfirmRequested,
    Length,
    Data
)
```

The primitive parameters are defined in Table 5-31.

5.5.8 MAC-HRCP-DATA.confirm

This primitive is used to report the result of a request to transfer an MSDU from one MAC entity to another MAC entity or entities using HRCP PHY. This primitive is only generated if the ConfirmRequested parameter in the MAC-HRCP-DATA.request with the same RequestID value is ALWAYS or is ON_ERROR and the ResultCode is FAILURE. MCSIdentifier and ChIdentifier parameters are used to indicate the current MCS identifier and frequency channel used in the transmitted frame to the upper layer. These two parameters are only applicable for HRCP SC PHY. The semantics of this primitive are as follows as follows:

```
MAC-HRCP-DATA.confirm      (  
    RequestID,  
    TransmitDelay,  
    MCSIdentifier,  
    ChIdentifier,  
    ResultCode,  
    ReasonCode  
)
```

The primitive parameters are defined in Table 5-31.

5.5.9 MAC-HRCP-DATA.indication

This primitive is used to indicate the reception of an MSDU. The semantics of this primitive are as follows:

```
MAC-HRCP-DATA.indication   (  
    Length,  
    Data  
)
```

The primitive parameters are defined in Table 5-31.

5.5.10 MAC-HRCP-MUL-DATA.request

This primitive is used to initiate the transfer of a Multi-protocol MSDU from one MAC entity to another MAC entity or entities using HRCP PHY. The semantics of this primitive are as follows:

```
MAC-HRCP-MUL-DATA.request  (  
    RequestID,  
    StreamIndex,  
    LogicalChannel,  
    ACKRequested,  
    ConfirmRequested,  
    Length,  
    DataID,  
    DestinationAddress,  
    SourceAddress,  
    Ethertype,  
    OUI_CID,  
    Data  
)
```

The primitive parameters are defined in Table 5-31.

5.5.11 MAC-HRCP-MUL-DATA.confirm

This primitive is used to report the result of a request to transfer a Multi-protocol MSDU from one MAC entity to another MAC entity or entities. This primitive is only generated if the ConfirmRequested parameter in the MAC-HRCP-MUL-DATA.request primitive with the same RequestID value is ALWAYS or is ON_ERROR and the ResultCode is FAILURE. The semantics of this primitive are as follows:

```
MAC-HRCP-MUL-DATA.confirm (
    RequestID,
    TransmitDelay,
    ResultCode,
    ReasonCode,
    MCSIdentifier,
    ChIdentifier
)
```

The primitive parameters are defined in Table 5-31.

5.5.12 MAC-HRCP-MUL-DATA.indication

This primitive is used to indicate the reception of a Multi-protocol MSDU. The semantics of this primitive are as follows:

```
MAC-HRCP-MUL-DATA.indication (
    Length,
    DataID,
    DestinationAddress,
    SourceAddress,
    Ethertype,
    OUI_CID,
    LogicalChannel,
    Data
)
```

The primitive parameters are defined in Table 5-31.

6 . MAC frame formats

6.2 General frame format

Change the first paragraph and dashed list in 6.2 as follows:

The MAC frame format, illustrated in Figure 6-3 for piconet DEVs and in Figure 6-3a for PRDEVs, comprises a set of fields that occur in a fixed order in all frames. The figures in this subclause are a representation of the MAC Header field and MAC Frame Body field. The HCS is not shown since this is calculated and verified by the PHY. The MAC frame shall be formatted as illustrated in Figure 6-3 for piconet DEVs and in Figure 6-3a for PRDEVs. For piconet DEVs, the maximum size of the MAC Frame Body field, *pMaxFrameBodySize*, is a PHY-dependent parameter that includes the frame payload and FCS fields, but not the PHY preamble, PHY header, MAC header, MAC subheader, or MAC header validation. For PRDEVs, the maximum size of the MAC Frame Body field, *pMaxFrameBodySize*, is a PHY-dependent parameter that includes the frame payload(s), MAC subheader(s) and padding octets in the aggregated

frames, and FCS field(s) but not the PHY preamble, PHY header, MAC header, or MAC header validation. The parameter *pMaxFrameBodySize* is defined in the following subclauses:

- 10.2.8.1 for the 2.4 GHz PHY
- 11.2.7.1 for the SC PHY mode
- 11.3.6.3 for the HSI PHY mode
- 11.4.1.3.1 for the AV PHY mode
- 11a.2.7.1 for the HRCP-SC PHY mode
- 11a.3.7.1 for the HRCP-OOK PHY mode

Change the title of Figure 6-3 as follows:

Figure 6-3—MAC Header field and MAC Frame Body field formats for piconet

Insert Figure 6-3a as follows:

Octets:2	2	1	1	3	1	variable
Frame Control	Pairnet ID	DestID	SrcID	TX and ACK Information	Stream Index	Frame Payload
MAC header						MAC Frame Body

Figure 6-3a—MAC Header field and MAC Frame Body field format for pairnet

Change the title of Figure 6-4 as follows:

Figure 6-4—Non-secure MAC Frame Body field format for piconet

After Figure 6-4, insert the following new paragraph and Figure 6-4a:

The non-secure MAC frame body for PRDEVs shall be formatted as illustrated in Figure 6-4a when the SEC bit is set to zero in the Frame Control field.

Octets: variable
Frame Payload
MAC Frame Body

Figure 6-4a—Non-secure MAC Frame Body field format for pairnet

Change the title of Figure 6-5 as follows:

Figure 6-5—Secure MAC Frame Body field format for piconet

After Figure 6-5, insert the following new paragraph and Figure 6-5a:

The secure MAC frame body for PRDEVs shall be formatted as illustrated in Figure 6-5a when the SEC bit is set to one in the Frame Control field.

Octets: 8	variable
Security Header	Frame Payload
Secure MAC Frame Body	

Figure 6-5a—Secure MAC Frame Body field format for pairnet

6.2.1 Frame Control field

Change the title of Figure 6-6 as follows:

Figure 6-6—Frame control field format for piconet

After Figure 6-6, insert the following new paragraph and Figure 6-6a:

The Frame Control field for a pairnet shall be formatted as illustrated in Figure 6-6a.

Bits: b0–b2	b3–b5	b6	b7–b8	b9	b10–b15
Protocol Version	Frame Type	SEC	ACK Policy	Logical Channel	Reserved

Figure 6-6a—Frame control field format for pairnet

6.2.1.1 Protocol Version field

Change the first paragraph of 6.2.1.1 as follows:

The Protocol Version field is invariant in size and placement across all revisions of IEEE Std 802.15.3. For this revision of the standard the value of the protocol version is 0b000 for piconet and 0b001 for pairnet. All other values are reserved. The revision level will be incremented only when a fundamental incompatibility exists between a new revision and the prior revision of the standard. A DEV that receives a frame with a higher revision level than it supports may discard the frame without indication to the sending DEV.

6.2.1.2 Frame Type field

Change the title of Table 6-1 as follows:

Table 6-1—Valid frame type values for piconet

After Table 6-1, add the following new text and Table 6-1a:

Table 6-1a lists the valid frame type values and their description for pairnet.

Stk-ACK frames with no data which are sent in response to data frames are treated as data frames and those sent in response to command frames are treated as command frames.

Change the title of 6.2.1.4 as follows:

Table 6-1a—Valid frame type values for pairnet

Type value b5 b4 b3	Frame type description	Subclause
0b000	Beacon frame	6.3.1
0b001	Reserved	—
0b010	Reserved	—
0b011	Command frame	6.3.3a
0b100	Data frame	6.3.4a
0b101	Multi-protocol Data frame	6.3.5a
0b110–0b111	Reserved	—

6.2.1.4 ACK Policy field, Imp-ACK Request field, and Blk-ACK field for piconet

Change the title of Table 6-2 as follows:

Table 6-2—Valid ACK policy field type values for piconet

After 6.2.1.4, insert new subclause 6.2.1.4a as follows:

6.2.1.4a ACK Policy field for pairnet

The ACK Policy field is used to indicate the type of acknowledgment procedure that the addressed recipient is required to perform. The allowed values of the ACK Policy field are defined in 7.9.

Table 6-2a—Valid ACK policy field type values for pairnet

ACK policy field b8 b7	ACK policy type	Description
0b00	No ACK	The recipient(s) does not acknowledge the transmission, and the sender treats the transmission as successful without regard for the result, as described 7.9.1.
0b01	Reserved	—
0b10	Stk-ACK	The addressed recipient uses a Stk-ACK procedure for subframe exchange described 7.9.2a.
0b11	Reserved	—

After 6.2.1.8, insert new subclause 6.2.1.9 as follows:

6.2.1.9 Logical Channel

Logical Channel is available for use by the Higher Layer Protocol User and therefore out of scope from this specification. The value of this field is set to zero for CH0 of Logical Channel, and is set to one for CH1. All MSDUs in the MAC frame shall be sent in same Logical Channel.

After 6.2.2, insert new subclause 6.2.2a as follows:

6.2.2a PairnetID

The PairnetID field contains the unique identifier for the pairnet. The PairnetID normally remains constant during the current instantiation of the pairnet and may be persistent for multiple sequential instantiations of the pairnet by the same PRC. The PairnetID shall be set to the current PNID for the pairnet and is used to identify frames from DEVs in the pairnet.

Change the title of subclause 6.2.3 as follows:

6.2.3 SrcID and DestID fields for piconet

After 6.2.3, insert the following new subclause as 6.2.3a:

6.2.3a SrcID and DestID fields for pairnet

There are two DEVID fields in the MAC frame format. These fields are used to indicate the source DEVID (SrcID) and destination DEVID (DestID). A DEVID for a DEV is preassigned by the PRC in the Beacon frame before the association of the DEV. The DEVID is unique to an associated DEV within a pairnet. The following DEVIDs are reserved:

- The DEVID value of 0x00 shall be reserved for the PRC
- The DEVID values of 0xED through 0xFE shall be reserved
- The DEVID value of 0xFF shall be reserved for broadcast frames (BcstID)

The maximum number of valid DEVs, *mMaxNumValidDEVs*, is the maximum number of DEVIDs that the PRC is able to allocate in a pairnet. This includes all of the regular DEVIDs and the PRCID but not the remaining reserved IDs.

6.2.5 Stream Index field

Insert text immediately after the last paragraph in 6.2.5 as follows:

For pairnet, the Stream Index field assigned values are as follows:

- 0x00 is assigned for data
- 0x01 to 0xFF is reserved

6.2.6 MAC header validation

Change the dashed list after the first paragraph as follows:

- 10.2.9 for the 2.4 GHz PHY

- 11.2.3.2.2 for the SC PHY mode
- 11.3.3.4 for the HSI PHY mode
- 11.4.1.4 for the AV PHY mode
- 11a.2.3.2.2 for HRCP-SC PHY mode
- 11a.3.3.2.2 for HRCP-OOK PHY mode

6.2.7 MAC Frame Body field

Change the first paragraph in 6.2.7.1 as follows:

6.2.7.1 Frame Payload field

The Frame Payload field is a variable-length field that carries the information that is to be transferred to a DEV or group of DEVs in the piconet or to a DEV in the pairnet. In the case of a secure frame, it also includes the required security information and the secure payload, as illustrated in Figure 6-5 for piconet and as described in 6.2.7.9 for pairnet.

Change the second paragraph in 6.2.7.2 as follows:

6.2.7.2 Secure session ID (SECID) field

The Key Originator field for all keys except the piconet group data key or the pairnet group data key shall be set to the DEVID of the key originator in the relationship. The Key Originator field for the piconet group data key or the pairnet group data key shall be set to the BestID.

Change the first paragraph of 6.2.7.3 as follows:

6.2.7.3 Secure Frame Counter (SFC) field

The Secure Frame Counter (SFC) field contains a counter that is used to ensure the uniqueness of the nonce in a secure frame. ~~A~~For piconets, a DEV shall not reuse a frame counter with the same time token, as described in 6.3.1.1, and key, as described in 8.3.5. For pairnets, a DEV shall not reuse a frame counter with the same key, as described in 8.3.5. ~~¶~~For piconets, the DEV shall initialize the SFC to zero for the first frame sent and increment it for each successive secure frame sent. For pairnets, the DEV shall initialize the SFC value to zero for the first frame or subframe sent and increment it for each successive secure frame sent or each successive subframe sent in the aggregated frame. Only the SFC value of the first subframe is explicitly included in the transmitted aggregated frame. ~~¶~~For piconets, when the time token, as described in 6.3.1, is updated, the DEV shall reset the SFC to zero. For pairnets, the SFC value shall be increased even when the time token is updated. In the case where the DEV receives a new key, the DEV shall set the SFC to zero.

6.2.7.4 Secure Payload field

Change the first paragraph in 6.2.7.4 as follows:

The Secure Payload field is a variable-length field that contains the information, protected by the symmetric key security operations, as defined in 9.3 for piconet and as defined in 9a. for pairnet, that is to be transferred to a DEV or group of DEVs in the piconet or to a DEV in the pairnet. As illustrated in Figure 6-5 for piconet and as described in 6.2.7.9 for pairnet, the Secure Payload field is a part of the Frame Payload field and does not include the SECID, SFC, or Integrity Code fields.

6.2.7.5 Integrity Code field

Change the first paragraph of 6.2.7.5 as follows:

The Integrity Code field contains an encrypted integrity code that is used to cryptographically protect the integrity of the MAC header and Frame Payload. The integrity code is computed as specified in 9.3 for piconets, and is computed as specified in 9a.3 for pairnets.

After 6.2.7.6, insert the following new subclauses as 6.2.7.7, 6.2.7.8, and 6.2.7.9:

6.2.7.7 MAC frame body for pairnet

The MAC frame body for pairnet is described in 6.3.1.1a, 6.3.3a.1, 6.3.4a.1 and 6.3.5a.2.

6.2.7.8 Security header for pairnet

The Security header for pairnet shall be formatted as illustrated in Figure 6-8a.

Octets: 2	6
SECID	SFC

Figure 6-8a—Security header

The SECID field is used to identify the key set that is used to encrypt and/or authenticate the data in the frame, as defined in 6.2.7.9.

The SFC field contains a counter that is used to ensure the uniqueness of the nonce of a secure frame, as defined in 6.2.7.3.

6.2.7.9 Secure MAC frame body for pairnet

The Secure MAC frame body for pairnet is described in 6.3.1.2a, 6.3.3a.2, 6.3.4a.2 and 6.3.5a.2.

After 6.2.9.5, insert the new subclause 6.2.10:

6.2.10 TX and ACK Information field for pairnets

The TX and ACK Information field shall be formatted as illustrated in Figure 6-46a.

Bits: b0–b8	b9	b10–b19	b20	b21	b22	b23
Number of Subframes	Last Received Frame Type	Last Received Sequence Number	Buffer Full	Buffer Empty	DEV Sleep	Reserved

Figure 6-46a—TX and ACK Information field format for pairnets

The Number of Subframes field indicates the number of subframes included in the current frame. Up to 256 subframes can be aggregated into a single frame. The valid range of this field is [0–256] and other values outside this range are reserved.

The Last Received Frame Type field indicates the type of frame that was sent with the sequence number indicated by the Last Received Sequence Number field. A value of one indicates a data frame, and a value of zero indicates a command frame.

The Last Received Sequence Number field indicates the most recent contiguous sequence number of subframes that was successfully received by the DEV. The details are illustrated in 7.9.2a. The initial value of the Last Received Sequence Number field for both command and data frames is 0x3FF.

The Buffer Full field indicates that the reception buffer of the sender is full. A value of one indicates that the buffer is full and a value of zero indicates that the buffer is not full.

The Buffer empty field shall be set to one when the reception buffer becomes empty at any point in time between the previous ACK replying frame and the current ACK transmission. Otherwise this field shall be set to zero.

The DEV Sleep field indicates if the sender will transition to sleep state. A value of one indicates the sender is going to sleep and shall be set to zero otherwise.

6.3 Format of individual frame types

6.3.1 Beacon frame

Change the title of subclause 6.3.1.1 as follows:

6.3.1.1 Non-secure Beacon frame for piconet

After 6.3.1.1, insert the following new subclause as 6.3.1.1a:

6.3.1.1a Non-secure Beacon frame for pairnet

The Beacon frame shall be formatted as illustrated in Figure 6-50a.

Octets:15	variable	...	variable	4
Pairnet Synchronization Parameters	Information element-1		Information element-n	FCS

Figure 6-50a—Non-secure Beacon frame Frame Payload field format for pairnets

The individual information elements (IEs) in the Beacon frame body are listed in Table 6-13a. These IEs are defined in 6.4. The IEs in the Beacon frame's payload may appear in any order. A Beacon frame sent by a PRC shall contain a PRC Capability IE.

The Pairnet Synchronization Parameters field shall be formatted as illustrated in Figure 6-50b.

Octets:1	1	2	2	1	1	1	6
Number of Association Slots	Duration of an Association Slot	Superframe Duration	Recommended ATP	Next DEVID	Pairnet Mode	Expected RSSI	PRC address

Figure 6-50b—Pairnet Synchronization Parameters field format

Number of Association Slots field indicates the number of slots available for the DEVs to send Association Request commands. This value is the same as *pNAccessSlot*.

Duration of an Association Slot field indicates the time length of a slot. This value is the same as *pDAccessSlot*.

The Superframe Duration field contains the duration of the current superframe in the PSP. The resolution of this field is 1 μ s and has a range of [0–65535] μ s. However, the valid range of this field lies between *mMinSuperframeDuration* and *mMaxSuperframeDuration*. Note that the superframe duration may be longer than *pNAccessSlot***pDAccessSlot* when dual Beacon frames are transmitted.

The Recommended ATP field indicates ATP length value that is recommended by PRC. The resolution of this field is 1 ms and therefore has a range of [0–65535] ms.

NOTE 1—It is recommended that a PRDEV should use short ATP length value less than or equal to 500 ms.

The Next DEVID field indicates the DEVID for the subsequent DEV. The DEV that wishes to associate with the PRC shall set this value as its own DEVID. The value of the Next DEVID field shall be different from the current DEVID and selected randomly.

The Expected RSSI field indicates the RSSI value of received signal at the antenna input of DEV located at specific distance from the PRC. EIRP and path loss between the PRC and the PRDEV can be used to determine the Expected RSSI value at the PRC. The DEV shall only send an Association Request command to the PRC when the actual measured RSSI level of the received Beacon frame exceeds this value. The resolution of this field is 1 dB and has a range of [+30 to –226] dBm.

NOTE 2—Expected RSSI can be calculated at the PRC as follows: Expected RSSI = EIRP – Path Loss [this value is equal to: TX Power at RF of the PRC + (antenna gain – cable loss at the PRC) – Path Loss].

When the DEV measures the RSSI level of the received Beacon frame, antenna gain and cable loss at the DEV should be considered in the decision on sending an Association Request. That is, the DEV transmits an Association Request when the following condition holds: Measured RSSI at the DEV $\geq$ Expected RSSI value indicated in the Beacon frame + (antenna gain – cable loss at the DEV).

The Pairnet Mode field defines certain characteristics about the pairnet and the superframe. The encoding of this octet shall be formatted as illustrated in Figure 6-50c.

Bits: b0–b3	b4	b5–b7
Reserved	SEC Mode	Reserved

Figure 6-50c—Pairnet Mode field

The SEC Mode field indicates the current security settings in the pairnet as defined in 8.2. The field is encoded as illustrated in Table 6-5.

The PRC Address field contains the DEV address of the PRC, as described in 6.1.