

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

Part 22.1: Standard to Enhance Harmful Interference Protection for Low-Power Licensed Devices Operating in TV Broadcast Bands

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

IEEE Std 802.22.1™-2010

1 November 2010

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

**Part 22.1: Standard to Enhance
Harmful Interference Protection for
Low-Power Licensed Devices
Operating in TV Broadcast Bands**

Sponsor

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

Approved 30 September 2010

IEEE-SA Standards Board

Approved 31 August 2011

American National Standards Institute

Abstract: This standard defines the protocol and data formats for communication devices forming a beaconing network that are used to protect low-power, licensed devices operating in television broadcast bands from harmful interference generated by license-exempt devices, such as Wireless Regional Area Networks (WRAN), intended to operate in the same bands. The devices being protected are devices licensed as secondary under Title 47, Part 74, Subpart H in the USA and equivalent devices in other regulatory domains.

Keywords: ad hoc network, beacons, TV white space, Wireless Regional Area Networks, WRAN

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

Copyright © 2010 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 1 November 2010. Printed in the United States of America.

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

PDF: ISBN 978-0-7381-6497-7 STD97037
Print: ISBN 978-0-7381-6498-4 STDPD97037

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.

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

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

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

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

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

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the 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, explanation, or interpretation of the IEEE. Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required.

Comments and recommendations on standards, and requests for interpretations should be addressed to:

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

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

Introduction

This introduction is not part of IEEE Std 802.22.1-2010, IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 22.1: Standard to Enhance Protection for Low-Power, Licensed Devices Operating in Television Broadcast Bands.

This standard defines the protocol and data formats for communication devices offering enhanced protection for low-power, licensed devices, such as those used in the production and transmission of broadcast programs (i.e., devices licensed as secondary under Title 47, Part 74, Subpart H in the USA and equivalent devices in other regulatory domains), operating in television broadcast bands. Protection is provided through the use of a beacon, which contains information relevant to the licensed device, including its physical location and estimated duration of TV channel occupancy. The standard uses the ALOHA medium access mechanism, and all transmissions are broadcast.

The physical layer uses direct sequence spread spectrum (DSSS) with differential quadrature phase-shift keying (DQPSK). A synchronization word and countdown mechanism (i.e., time until the next beacon transmission) is transmitted continuously on the I channel, while beacons and inter-device communications are transmitted on the Q channel. Frequency, modulation rate, and transmit power vary from region to region and shall adhere to local regulations.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard 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

This document is copyrighted by the IEEE. It is made available 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 this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards 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. 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 Standards Association website at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA website at <http://standards.ieee.org>.

Errata

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

Downloads

Portions of this standard can be downloaded from the Internet. Materials include PICS tables, data tables, and code. URLs are listed in the text in the appropriate sections.

Interpretations

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

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE 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 submitted to the IEEE-SA for approval, the IEEE P802.22 Working Group had the following voting members:

Apurva N. Mody, *Chair*
Gerald Chouinard, *Vice Chair*

Greg Buchwald, *P802.22.1 Chair*
Monique Bourgeois Brown, *P802.22.1 Editor-in-Chief*

Chee Wei Ang	Baowei Ji	Edgar Reihl
Kwok Shum Au	Jerome J. Kalke	Jon Rosdahl
John Benko	Ramon Khalona	William Rose
Winston Caldwell	Chang-Joo Kim	Shigenobu Sasaki
Ed Callaway	Kihong Kim	Cheng Shan
Dave Cavalcanti	Gwangzeen Ko	Steve Shellhammer
Soo-Young Chang	Stephen Kuffner	Kirk Skeba
Chris Clanton	Jeong Suk Lee	Eli Sofer
Johnny Dixon	Zhongding Lei	Myung Sun Song
Charles Einolf	Kyutae Lim	Srikathyayani Srikanteswara
Wen Gao	Jiezhen Lin	Carl R. Stevenson
Ingo Gaspard	David Mazzaresse	Victor Tawil
Monisha Ghosh	Peter Murray	James Tomcik
Joanna Guenin	Paul Nikolic	Jungsun Um
Tom Gurley	Moh Nouroozian	George Vlantis
Anh Tuan Hoang	Juha Pihlaja	Kelly Williams
Wendong Hu	Jeff Poston	Yu-chun Wu
Sung Hyun Hwang	Ranga Reddy	Changlong Xu
Tae-In Hyon	Ivan Reede	Yonghong Zeng
		Jianwei Zhang

Major contributions were received from the following individuals:

Greg Buchwald	Mingwei Jie	K. Sivanesan
Ed Callaway	Jerome J. Kalke	Yang Tang
Soo-Young Chang	Mark Kenkel	Victor Tawil
Gerald Chouinard	Stephen Kuffner	Ke Wang
Chris Clanton	Linjun Lv	Kexue Wang
Charles Einolf	David Mazzaresse	Yu-chun Wu
Paul Gorday	Tom Messerges	Zhou Wu
Garret Heath	Zhixue Shi	Jianwei Zhang
Baowei Ji	Dave Silk	Xuesheng Zhu

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

Thomas Alexander	Randall Groves	Apurva N. Mody
Butch Anton	Joanna Guenin	Ronald Murias
Reza Arefi	Thomas Gurley	Peter Murray
Kwok Shum Au	Hiroshi Harada	Michael S. Newman
Alexander Awuviri	William Hayes	Charles Ngethe
Taehan Bae	Robert F. Heile	Paul Nikolich
Youngkyo Baek	Oliver Hoffmann	John Notor
Stephen Berger	Seock Deock Hong	Satoshi Obara
Gregory Best	Victor Hou	Jisung Oh
Harry Bims	David Hunter	Okundu Omeni
Gennaro Boggia	Chan-Soo Hwang	Chris Osterloh
Achim Brandt	Tae-In Hyon	Satoshi Oyama
Nancy Bravin	Tetsushi Ikegami	Jeongho Park
Monique Bourgeois Brown	Atsushi Ito	Jungshin Park
Timothy Brown	Raj Jain	William Pechey
William Byrd	Jaehyuk Jang	Venkatesha Prasad
Sean Cai	Hongkyu Jeong	Michael Probasco
Peter J. Calderon	Suryong Jeong	Henry Ptasinski
Edgar Callaway	Baowei Ji	Ivan Reede
James Carlo	Bobby Jose	Benjamin Rolfe
Juan Carreon	Woochul Jung	William Rose
Youngbin Chang	Tal Kaitz	Jaeyoung Ryu
Clint Chaplin	Hyunjeong Kang	Randall Safier
Yung-Mu Chen	Noh-Gyoung Kang	John Santhoff
Kichun Cho	Efthymios Karabetsos	Shigenobu Sasaki
Hokyu Choi	Piotr Karocki	Bartien Sayogo
Seung-Hoon Choi	Shuzo Kato	Cheng Shan
Gerald Chouinard	Stuart J. Kerry	Stephen Shellhammer
Keith Chow	Eunkyung Kim	Jaejeong Shim
jinyong chung	Gil Kim	Changyong Shin
Jules Cohen	Sangbum Kim	Wonjae Shin
Charles Cook	Yongbum Kim	Gil Shultz
Todor Cooklev	Youngdoo Kim	Jaeseung Son
Jose Costa	Youngsoo Kim	Jung Je Son
Manoj Das	Patrick Kinney	Kapil Sood
Russell Dietz	Dongkeon Kong	Amjad Soomro
Thomas Dineen	Bruce Kraemer	Kenneth Stanwood
Mi-Sun Do	Joseph Kwak	Thomas Starai
Carlo Donati	Edwin Kwon	Adrian Stephens
Paul Eastman	Jeremy Landt	Carl Stevenson
Peter Ecclesine	Insun Lee	Rene Struik
Richard Eckard	Jae Min Lee	Walter Struppler
Charles Einolf	Jeongho Lee	Jun Ichi Takada
Marc Emmelmann	Mi Hyun Lee	Masahiro Takagi
Bernard Eydt	Myung Lee	Michael Johas Teener
Shulan Feng	Seong-hee Lee	David Tepen
Michael Fischer	Sungjin Lee	Adam Toner
C. Fitzgerald	Tae Hoon Lee	Wen Tong
David Fort	Joseph Levy	Masahiro Umehira
Andre Fournier	Jan-Ray Liao	Dmitri Varsanofiev
Robert Frazier	Arthur Light	Prabodh Varshney
Avraham Freedman	Chiwoo Lim	George Vlantis
Devon Gayle	Hyoung-Kyu Lim	Stanley Wang
Theodore Georgantas	Daniel Lubar	Robert Weller
James Gilb	William Lumpkins	Harry Worstell
Jaganathan Gnanavelu	Mark Maloney	Xuyong Wu
Mariana Goldhamer	David Mazzaresse	Oren Yuen
	Steven Methley	Juan Zuniga

When the IEEE-SA Standards Board approved this standard on 30 September 2010, it had the following membership:

Robert M. Grow, *Chair*
Richard H. Hulett, *Vice Chair*
Steve M. Mills, *Past Chair*
Judith Gorman, *Secretary*

Karen Bartleson
Victor Berman
Ted Burse
Clint Chaplin
Andy Drozd
Alexander Gelman
Jim Hughes

Young Kyun Kim
Joseph L. Koepfinger*
John Kulick
David J. Law
Hung Ling
Oleg Logvinov
Ted Olsen

Ronald C. Petersen
Thomas Prevost
Jon Walter Rosdahl
Sam Sciacca
Mike Seavey
Curtis Siller
Don Wright

*Member Emeritus

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

Satish Aggarwal, NRC Representative
Richard DeBlasio, DOE Representative
Michael Janezic, NIST Representative

Catherine Berger
IEEE Project Editor

Michael Kipness
IEEE Standards Program Manager, Technical Program Development

Contents

1.Overview	1
1.1 General.....	1
1.2 Scope.....	2
1.3 Purpose.....	2
2.Normative references	3
3.Definitions	5
4.Acronyms and abbreviations	7
5.Functional overview	9
5.1 Introduction.....	9
5.2 Architecture	9
5.3 Superframe structure.....	9
5.3.1 Synchronization burst structure	11
5.3.2 Beacon frame structure	12
5.4 Data transfer model.....	12
5.5 Security	14
5.5.1 Public-key approach	15
5.5.2 Security considerations	15
5.5.3 Beacons device life cycle	16
6.PHY specification.....	17
6.1 General requirements and definitions	17
6.1.1 TV channel/licensed auxiliary service (LAS) channel information	17
6.1.2 Modulation rates and beacon offset location for ATSC DTV regions	17
6.1.3 RF power measurement information	18
6.1.4 Receiver sensitivity definitions.....	18
6.2 PHY service specifications	18
6.2.1 PHY data service	19
6.2.2 PHY management service.....	20
6.2.3 PHY enumerations description	27
6.3 Synchronization burst	27
6.4 PPDU format.....	28
6.5 Inter-device communication interval (ICI).....	28
6.5.1 Receive (Rx) period	29
6.5.2 Acknowledgement/no acknowledgement period (ANP)	31
6.6 PHY constants and PIB attributes.....	32
6.6.1 PHY constants.....	32
6.6.2 PHY PIB attributes	32
6.7 PHY specifications	33
6.7.1 Modulation and spreading	33
6.7.2 Forward error correction (FEC).....	35
6.8 Radio specifications	37
6.8.1 Transmit center frequency tolerance.....	37
6.8.2 Transmit power	37
6.8.3 Transmit PSD mask	37
6.8.4 Modulation accuracy.....	38
6.8.5 Spurious harmonically-related emission suppression.....	39

6.8.6	Receiver sensitivity.....	39
6.8.7	Adjacent LAS channel rejection.....	39
6.8.8	Receiver maximum input level of compliant beacon signal (blocking).....	40
6.8.9	Link quality indicator (LQI).....	40
7.	MAC sublayer specification.....	43
7.1	MAC sublayer service specification.....	43
7.1.1	MAC management service.....	43
7.1.2	Enumeration description.....	51
7.2	MAC beacon frame.....	52
7.2.1	MSF 1.....	52
7.2.2	MSF 2.....	58
7.2.3	MSF 3.....	61
7.3	MAC constants and MIB attributes.....	62
7.3.1	MAC constants.....	62
7.3.2	MIB attributes.....	62
7.4	MAC functional description.....	65
7.4.1	Transmission protocol.....	65
7.4.2	Retry procedure for an SPD.....	65
7.4.3	Frame reception and rejection.....	66
7.4.4	Device initialization procedure.....	67
7.4.5	Inter-device communications.....	68
7.4.6	Beaconing.....	71
7.4.7	Ceasing transmissions.....	75
7.4.8	Setting the internal operating states of the transceiver.....	77
7.5	Security suite specifications.....	79
7.5.1	Notation and representation.....	79
7.5.2	Representation of time.....	79
7.5.3	Elliptic-curve building blocks.....	80
7.5.4	Signature scheme.....	81
7.5.5	Certificate scheme.....	83
7.6	Message sequence charts (MSC) illustrating MAC-PHY interaction.....	85
Annex A	(informative) Example block decoding method.....	93
A.1	Introduction.....	93
A.2	Method details.....	93
A.3	Example.....	94
Annex B	(informative) Recommended deployment in the United States.....	97
B.1	Introduction.....	97
B.2	Physical positioning of the beacon relative to other Part 74 wireless systems.....	97
B.3	Additional beacon antenna deployment considerations.....	101
B.4	Recommended wireless system frequencies of operation.....	102
Annex C	(informative) Receiver sensitivity and adjacent channel protection justification.....	103
C.1	Introduction.....	103
C.2	Analysis.....	104
C.2.1	Link 1 Rx signal.....	104
C.2.2	Microphone interfering signal.....	105

Annex D (informative) Next higher layer (NHL) operation.....	107
D.1 Introduction.....	107
D.2 Next higher layer (NHL).....	107
D.3 Beaconing device types	108
D.4 Generic PD behavior.....	108
D.4.1 Searching for existing PDs	108
D.4.2 Deciding to become a PPD or an SPD after an initial search	109
D.4.3 Beacon frame construction and transmission	110
D.4.4 Beacon transmission failure-related enumeration values	111
D.5 PPD behaviors.....	112
D.5.1 Insertion of Rx period and ANP	112
D.5.2 Data aggregation	112
D.5.3 NPD selection	114
D.5.4 SPD lost indication	115
D.5.5 NPD lost indication.....	115
D.5.6 Planned termination of PPD transmission	115
D.5.7 Behavior following termination of SPD transmissions without warning	115
D.5.8 Behavior following planned termination of SPD transmissions.....	116
D.5.9 Behavior following termination of NPD transmissions without warning	116
D.5.10 Behavior following planned termination of NPD transmissions	116
D.5.11 PPD-specific MIB attributes	116
D.6 SPD behaviors.....	116
D.6.1 PPD beacon reception	117
D.6.2 Inter-device communication	117
D.6.3 Inter-device communication—retry failure handling	117
D.6.4 Inter-device communication—selection of the same RTS codeword	118
D.6.5 PPD protection of an SPD	118
D.6.6 Transmission of more than one beacon frame	119
D.6.7 Behavior on SPD receiving a PPD lost indication.....	119
D.6.8 Behavior on SPD receiving an NPD lost indication	119
D.6.9 Behavior if both PPD and NPD are lost	120
D.6.10 Behavior when selected as the NPD	121
D.6.11 Planned termination of SPD transmission	121
D.6.12 Behavior following termination of PPD transmissions without warning	121
D.6.13 Behavior following planned termination of PPD transmissions.....	122
D.6.14 Behavior following termination of NPD transmissions without warning	122
D.6.15 Behavior following planned termination of NPD transmissions	122
D.6.16 SPD-specific MIB attributes	122
D.7 NPD behaviors	122
D.7.1 Behavior on reception of the PPD NPD Indication subfield	123
D.7.2 Behavior on NPD receiving a PPD lost indication	123
D.7.3 Planned termination of NPD transmissions	123
D.7.4 Behavior following termination of PPD transmissions without warning	123
D.7.5 Behavior following planned termination of PPD transmissions.....	124
D.7.6 NPD-specific MIB attributes	124

Annex E (informative) Acquisition of time and location information	125
E.1 Introduction.....	125
E.2 Time	125
E.3 Location information	126
Annex F (informative) Concept of service primitives	129
Annex G (informative) Bibliography	131

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

Part 22.1: Standard to Enhance Harmful Interference Protection for Low-Power Licensed Devices Operating in the TV Broadcast Bands

IMPORTANT NOTICE: *This standard is not intended to ensure safety, security, health, or environmental protection in all circumstances. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.*

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

1. Overview

1.1 General

National regulators are advancing regulations that allow license-exempt devices to operate on a non-interfering basis within the portions of the TV spectrum that are not used for broadcasts or required to remain unused in order to protect broadcast stations from interference. The Federal Communications Commission (FCC) in the United States of America has proposed to allow license-exempt devices to operate on a non-interfering basis within the portions of the TV spectrum that are not used for broadcasts or required to remain unused in order to protect broadcast stations from interference. It is expected that other regulatory bodies will take similar actions. Although the TV channels in these portions are not used for TV broadcasts, low-power, licensed devices, such as wireless microphones operated by broadcasters, do use these channels, and are entitled to protection by regulation to avoid disrupting incumbent services.

Furthermore, national regulators in many regions of the world are advancing regulations that allow license-exempt devices to operate on a non-interfering basis within the portions of the TV spectrum that are not used for broadcasts or required to remain unused in order to protect broadcast stations from interference.

This standard describes the air interface of devices that serve as warning beacons to protect the operation of incumbent licensed low-power devices. The beacons should be installed by the operator of the licensed device at a location appropriate to afford protection to the protected service. The beacons transmit identifiable sync bursts as well as, optionally, information about locations and operational parameters of the protected devices. The unlicensed system should include an appropriate receiver to receive and decode the information and should have an operation policy that would avoid inflicting any interference to the protected device.

1.2 Scope

This standard specifies methods to provide enhanced protection to protected devices such as those used in the production and transmission of broadcast programs [e.g., devices licensed as secondary under Title 47 of the Code of Federal Regulations (CFR) in the USA and equivalent devices in other regulatory domains] from harmful interference caused by license-exempt devices (e.g., IEEE P802.22TM^{1, 2}) that also are intended to operate in the TV Broadcast Bands.

1.3 Purpose

This standard provides a standard and efficient method for license-exempt devices to provide enhanced protection to low-powered licensed devices that are entitled to protection from harmful interference, and that share the same spectrum. This standard may be applicable in global regulatory environments.

¹Information on references can be found in Clause 2.

²This IEEE standards project was not approved by the IEEE-SA Standards Board at the time this publication went to press. For information about obtaining a draft, contact the IEEE.

2. Normative references

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

ANSI X9.63-2001, Public Key Cryptography for the Financial Services Industry—Key Agreement and Key Transport Using Elliptic Curve Cryptography, American Bankers Association, November 20, 2001.³

IEEE P802.22/Draft 5.0, Draft Standard for Local and metropolitan area networks, Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Policies and procedures for operation in the TV Bands, October 2010.⁴

IEEE Std 1363TM-2000, IEEE Standard Specifications for Public-Key Cryptography.^{5, 6}

IEEE Std 1363aTM-2004, IEEE Standard Specifications For Public Key Cryptography—Amendment 1: Additional Techniques.

NIST Special Publication 800-57, “Recommendation for Key Management—Part 1: General.”⁷

Standards for Efficient Cryptography, SEC 4: Elliptic Curve Cryptography, Version 1.1r1, Certicom Research, June 9, 2006.⁸

U.S. Code of Federal Regulations, Title 47, Part 74, Subpart H.⁹

³ANSI publications are available from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (<http://www.ansi.org/>).

⁴Numbers preceded by P are IEEE authorized standards projects that were not approved by the IEEE-SA Standards Board at the time this publication went to press. For information about obtaining drafts, contact the IEEE.

⁵IEEE Publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (<http://standards.ieee.org>).

⁶The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

⁷National Institute of Standards and Technology publications are available from <http://csrc.nist.gov/>.

⁸Standards for Efficient Cryptography publications are available from <http://www.secg.org/>.

⁹U.S. Regulatory Guides are available from the Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082, USA (<http://www.access.gpo.gov/>).

3. Definitions

For the purposes of this document, the following terms and definitions apply. *The IEEE Standards Dictionary: Glossary of Terms & Definitions* should be referenced for terms not defined in this clause.¹⁰

3.1 beacon certificate: A certificate used by a beaconing device to convey its public key in a verifiable way to other entities.

3.2 beacon channel: The logical channel on which the PHY protocol data unit (PPDU) is sent. The PPDU comprises the 120-octet length beacon frame followed by 4 octets of all zeros.

3.3 beaconing device: A device that complies with IEEE Std 802.22.1.

3.4 beaconing network: A collection of devices consisting of a single primary protecting device (PPD) and the secondary protecting devices (SPDs) the PPD protects.

3.5 beacon private key: A key used by the beaconing device to create a digital signature of the beacon frame.

3.6 beacon public key: A key used by a receiving device to verify the authenticity of a digital signature that was created using the corresponding private key.

3.7 certificate authority: An entity responsible for provisioning asymmetric authentication data (public keys, digital certificates, etc.) to beaconing devices.

3.8 FCC Part 74 device: Low-power auxiliary stations as defined in the U.S. Code of Federal Regulations, Title 47, Part 74, Subpart H.

3.9 inter-device communication interval (ICD): A length of time, equal to one slot, consisting of a receive period (Rx period) and an acknowledgement/no acknowledgement period (ANP).

3.10 licensed auxiliary service (LAS) channel: A 200 kHz-wide portion of a TV channel. The lowest frequency LAS channel is centered 100 kHz above the lower edge of the TV channel, and the highest frequency LAS channel is centered 100 kHz below the upper edge of the TV channel. The number of LAS channels within a given TV channel depends on the width of the TV channel.

3.11 license-exempt device: A device that is tested and authorized by a regulatory body and is allowed to operate according to certain technical specifications without acquiring a license.

3.12 next-in-line protecting device (NPD): An secondary protecting device (SPD) that will become a primary protecting device (PPD) in the event that the already-existing PPD stops transmitting periodic beacon frames.

3.13 primary protecting device (PPD): A device that uses periodic beacons to protect its corresponding licensed device. Its protection may be extended to other licensed devices in the area [i.e., secondary protecting devices (SPDs)].

3.14 protected device: A low-power, licensed device that is being protected by a beaconing device.

3.15 protecting device (PD): A beaconing device that is protecting a low-power, licensed device. The PD may be either the primary protecting device (PPD) or a secondary protecting device (SPD).

¹⁰The *IEEE Standards Dictionary: Glossary of Terms & Definitions* is available at <http://shop.ieee.org/>.

3.16 secondary protecting device (SPD): A device that shares the responsibility of protecting its corresponding licensed device with the primary protecting device (PPD). An SPD occasionally sends beacons for the sole purpose of communicating with the PPD.

3.17 slot: An interval of time equal to 32 symbol times, or the duration of one sync burst.

3.18 synchronization channel: The logical channel consisting of a succession of 32-bit long synchronization bursts.

3.19 television (TV) channel: A contiguous segment of spectrum within the television broadcast bands, which may be 6, 7, or 8 MHz wide, depending on relevant regulations.

3.20 wireless microphone: A wireless microphone licensed for operation in the TV broadcast bands (e.g., an FCC Title 47, Part 74, Subpart H device in the United States).

3.21 wireless regional area network (WRAN) device: A device that is compliant with IEEE P802.22 or, once published, the latest published version of the standard.

4. Acronyms and abbreviations

ACK	acknowledgement
AGL	above ground level
ANP	acknowledgement/no acknowledgement period
ARIB	Association of Radio Industries and Businesses
ATSC	Advanced Television Systems Committee
CRC	cyclic redundancy check
DSSS	direct sequence spread spectrum
DQPSK	differential quadrature phase-shift keying
DTV	digital television
ECC	elliptic-curve cryptography
ECSSR-PV	elliptic-curve signature scheme with recovery, Pintsov-Vanstone version
ECSP-NR2/PV	elliptic curve pre-signature primitive, Nyberg-Rueppel and Pintsov-Vanstone version
ECSP-PV	elliptic curve signature primitive, Pintsov-Vanstone version
ECSSR-PV	elliptic-curve signature scheme with recovery, Pintsov-Vanstone version
ECVP-PV	elliptic curve verification primitive, Pintsov-Vanstone version
ED	energy detection
EIRP	effective isotropic radiated power
EMSR2	encoding method for signatures giving message recovery
ETSI	European Telecommunications Standards Institute
EVM	error vector magnitude
FCC	Federal Communications Commission
HDTV	high definition television
I2OSP	integer to octet string conversion primitive
ICI	inter-device communication interval
KDF2	key derivation function 2
LAS channel	licensed auxiliary service channel
LQI	link quality indicator
LSB	least significant bit
MAC	medium access control sublayer
MFR	MAC footer
MHR	MAC header
MIB	MAC information base
MIC	message integrity code
MLME	MAC sublayer management entity
MLME-SAP	MAC sublayer management entity service access point
MPDU	MAC protocol data unit
MSB	most significant bit
MSF	MAC subframe
MSI	manufacturer-specific information
NACK	no acknowledgement
NED	National Elevation Dataset
NHL	next higher layer
NPD	next-in-line protecting device
NST	next SPD superframe to transmit

NTSC	National Television System Committee
OSI	open systems interconnection
PD	protecting device
PD-SAP	PHY data service access point
PER	packet error rate
PHR	PHY header
PHY	physical layer
PIB	PHY information base
PLME	PHY layer management entity
PLME-SAP	PHY layer management entity service access point
PN	pseudo-random noise
PPD	primary protecting device
PPDU	PHY protocol data unit
PSDU	PHY service data unit
RATSC	symbol rate defined by the Advanced Television Systems Committee
RTS	request to send
Rx period	receive period
SAP	service access point
SHR	synchronization header
SPD	secondary protecting device
SRTM	Shuttle Radar Topography Mission
USGS	United States Geological Survey
UTC	universal coordinated time

5. Functional overview

5.1 Introduction

This standard defines the protocol and data formats for communication devices that form a beaconing network that offers an enhanced protection method to help prevent interference with low-power, licensed devices operating in television broadcast bands.

A brief introduction to the beaconing device architecture is given in 5.2, which is followed by a brief overview of the general functions of a beaconing network in 5.3 through 5.5. The general functions include information on the superframe structure, the data transfer model, and security.

Upon initialization, a protecting device (PD) is neither a primary protecting device (PPD) nor a secondary protecting device (SPD). Each PD monitors its TV channel for a random number of superframes to determine the presence or absence of a PPD. If no PPD is heard, the PD should act as a PPD and begin beaconing; if one or more PPDs are heard, under control of an upper layer, the PD may determine either to act as a PPD and initiate its own beacon, or as an SPD and attempt to contact a PPD. The device may take into consideration factors such as location and keep-out zone radius when making this decision. See 7.4.4 for more details on the device initialization procedure.

When a PPD is in operation, it should choose an SPD as the next-in-line protecting device (NPD). In the event that the PPD stops beaconing, the NPD shall promote itself from SPD to PPD. The remaining SPDs will eventually contact the new PPD, and the new PPD should choose an SPD to become the new NPD.

5.2 Architecture

The beaconing device architecture, shown in Figure 1, is a multilayer structure based on the open systems interconnection (OSI) seven-layer model. Each layer is responsible for one part of the protocol and offers services to the layers above it.

An IEEE 802.22.1 device comprises the physical layer (PHY), which contains the radio frequency (RF) transceiver along with its low-level control mechanism, and the medium access control sublayer (MAC), which provides access to the physical channel for the purpose of transferring information. The PHY and MAC are fully described in Clause 6 and Clause 7, respectively.

The upper layers provide services such as selecting an operating channel, deciding on an operating mode (i.e., PPD or SPD), starting and stopping beacon frame transmissions, processing incoming beacon frame information, aggregating data, and handling security errors. The definition of the upper layers is outside the scope of this standard. However, the intended behavior of the layer just above the MAC sublayer, which is known here as the next higher layer (NHL), is specified in Annex D.

The interfaces between the layers are called service access points (SAPs). Each SAP provides a means of passing information between two adjacent layers. More information on each particular SAP can be found in the text describing its associated layer (see 6.2 for information on PD-SAP, PLME-SAP, and RF-SAP; see 7.1 for information on MLME-SAP).

5.3 Superframe structure

The superframe structure repeats without interruption on a given TV channel occupied by an incumbent licensed wireless microphone or other licensed low-power devices. The superframe format is shown in Figure 2.

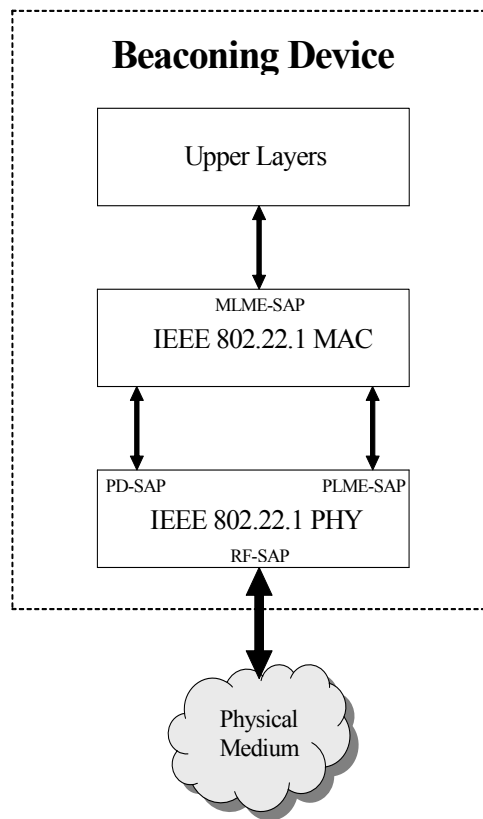


Figure 1—Beaconing device architecture

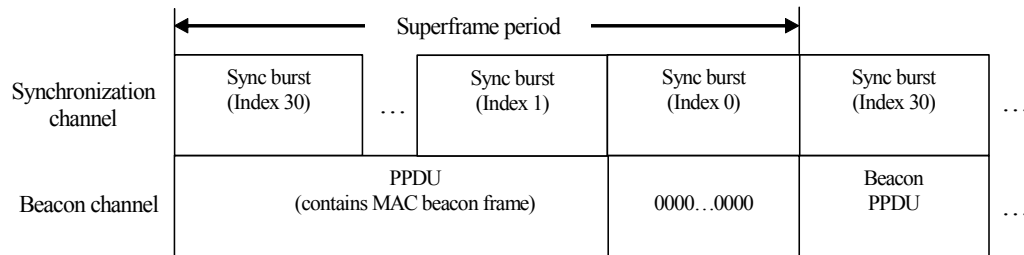
A large portion of the superframe structure is divided over two logical channels, which are transmitted in parallel. The synchronization logical channel consists of a succession of synchronization bursts (6.3), and the beacon logical channel consists of the PHY protocol data unit (PPDU), which contains the MAC beacon frame (7.2).

The superframe structure consists of a succession of 31 slots. Each slot is comprised of 32 DQPSK symbols, where one symbol has a duration of 1/9609.1 s. Each slot contains one synchronization burst, as well as a fixed number of PPDU bits. An inter-device communication interval (ICI) (6.5) may also be included. This format repeats on the TV channel without interruption as long as at least one PD is in operation. Note that the synchronization bursts and PPDU may be sent by either a PPD or an SPD.

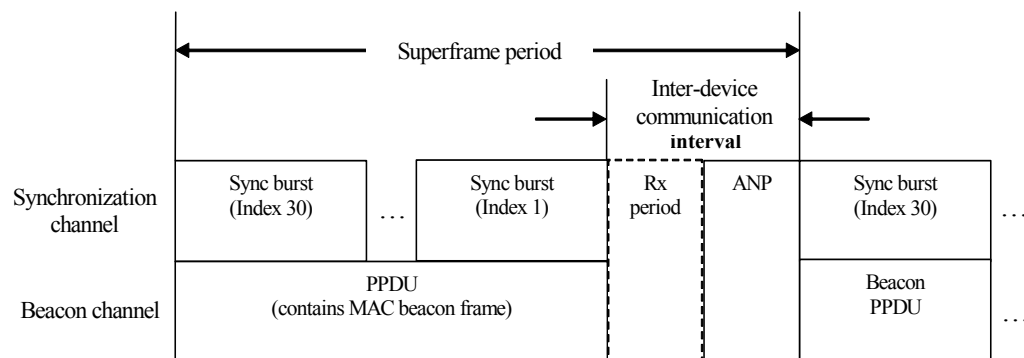
The synchronization bursts, which consists of a synchronization word followed by a decrementing index value, enable a receiver asynchronously sampling the radio channel to quickly determine when the next beacon will be sent. Parity bits follow the index value and provide error detection and correction on the index value.

The PPDU consists largely of the MAC beacon frame. The MAC beacon frame contains information relevant to the device or devices protected by the PD, including the physical location of the beaconing device and the estimated duration of TV channel occupancy.

Following thirty synchronization bursts and the PPDU, there may be an ICI, which includes a receive (Rx) period, during which the PPD pauses to monitor the TV channel for a request to send (RTS) burst transmitted by an SPD or an NPD codeword transmitted by the NPD, and an acknowledgement/no acknowledgement period (ANP), during which the PPD indicates whether it will transmit its own beacon frame during the next superframe or allow an SPD to transmit instead. During the initial transmission period, which lasts for *aInitializationPeriod* superframes (6.6.1), no ICI shall be included in the superframe structure.



(a) Initial transmission period



(b) Following the initial transmission period

Figure 2—Superframe logical format

If the PPD is in its initial transmission period and, therefore, the ICI is not included, the final index value in the series of synchronization bursts shall be zero and the next superframe shall start immediately after the end of this final synchronization burst [as illustrated in Figure 2 (a)]. While this synchronization burst with index zero is being transmitted on the synchronization channel, the beacon channel shall transmit all zeros. Because an SPD that has just joined the beaconing network shall not attempt to communicate on the channel for 100 superframes, no SPD will interfere with the PPD during its initial transmission period. Once the PPD has concluded its initial transmission period and, therefore, the ICI is included, the final index value in the series of synchronization bursts shall be one and the next superframe shall start after the ICI [as illustrated in Figure 2 (b)].

5.3.1 Synchronization burst structure

Figure 3 shows the structure of the synchronization burst sequence, which originates from within the PHY layer of a PD. Each synchronization burst contains a 15-bit synchronization word, an 8-bit parity field for detecting and correcting errors on the subsequent index value, a 7-bit index value that decrements with each

burst transmission, and a 2-bit reserved field. The synchronization burst sequence enables fast detection of the PPD or SPD that transmitted the sequence, while the decrementing index value identifies the start time of the next superframe transmission in multiples of slots. Each synchronization burst occupies one 32-bit-long synchronization channel slot of duration $32\text{ bits}/9609.1\text{ Hz} = 3.3301\text{ ms}$.

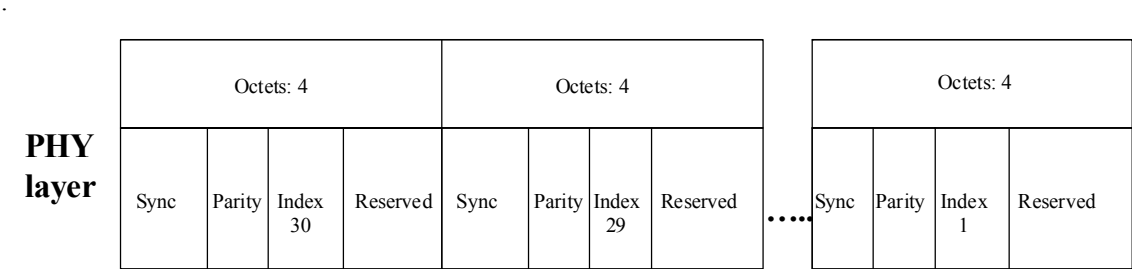


Figure 3—Schematic view of synchronization burst sequence

5.3.2 Beacon frame structure

Figure 4 shows the structure of the beacon frame, which originates from within the MAC sublayer of either the PPD or an SPD. The beacon frame contains three MAC subframes (MSF). Each MSF is composed of a MAC header (MHR) and a MAC footer (MFR). The MHR in MSF 1 contains the three MAC parameter fields, the Source Address field, and the Location field. The MHR in MSF 2 contains the Map and Signature fields, while the MHR in MSF 3 contains the Certificate field; the Signature and Certificate fields are part of the public-key cryptography security solution (5.5.1). The MFR 1, MFR 2, and MFR 3 each contain a 2-octet cyclic redundancy check (CRC). The three MSFs together form the MAC protocol data unit (MPDU), which has the same contents as the unencoded PHY service data unit (PSDU).

The MAC beacon frame is passed to the PHY as the unencoded PSDU (or unencoded PHY payload). The MSF 1 in the PHY payload is protected by a half-rate convolutional code (6.7.2.2), and the addition of this code increases the payload length by 17 octets.

Because the length of a synchronization burst is 4 octets, zero padding is added following MSF 3 to ensure that the PPDU length is a multiple of four. Therefore, the overall length of the PPDU is 120 octets. The PHY payload and zero padding together form the PPDU (i.e., the PHY packet).

5.4 Data transfer model

All transmissions are broadcast. Transmitted data may be received and processed by any device in the area, including WRAN devices and other devices compliant with IEEE Std 802.22.1.

Two types of data transfer transactions exist for a device compliant with IEEE Std 802.22.1. The first type is the data transfer from the PPD to an SPD, in which the PPD transmits the data. The second type is the data transfer from an SPD to the PPD, in which the SPD transmits the data.

When the PPD wants to send data to an SPD, it does so by placing the information in its beacon PSDU. The SPD, which may be one of many in range of the PPD, monitors the beacon PSDU of the PPD, and decodes its address and recovers the message. No acknowledgement of data reception is provided at the MAC level. See Figure 5.

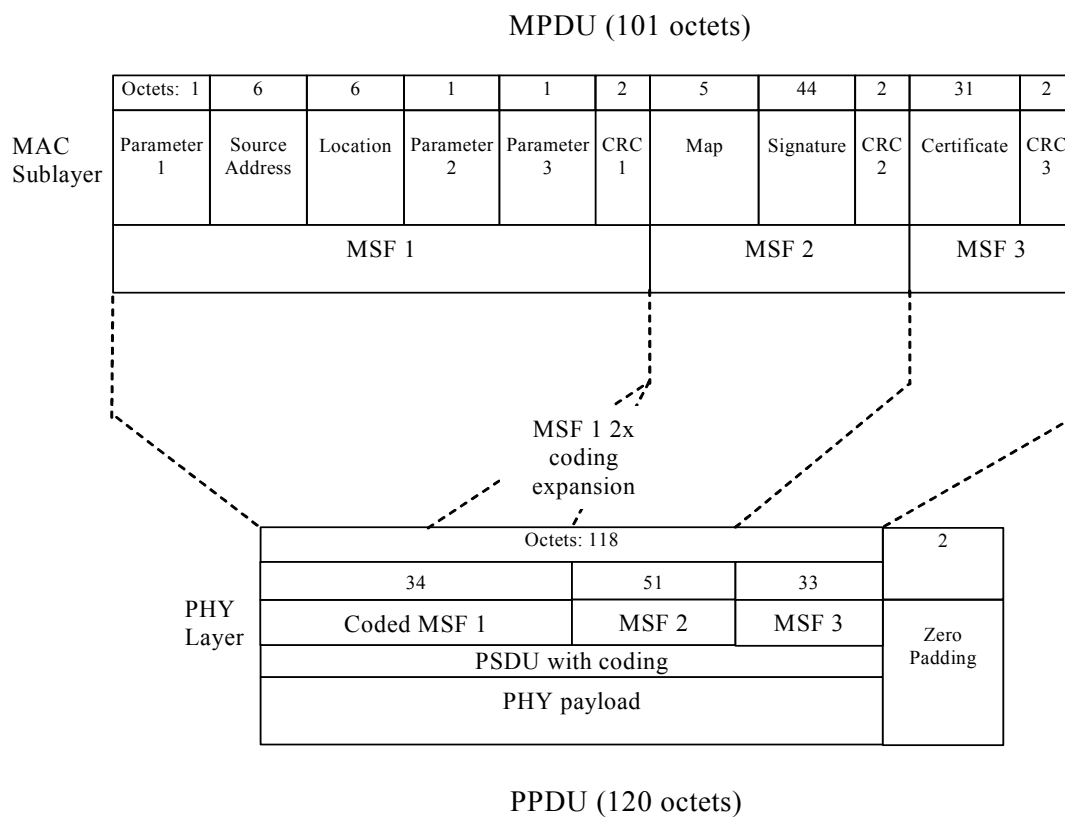


Figure 4—Schematic view of the beacon frame and the PHY packet (PPDU)

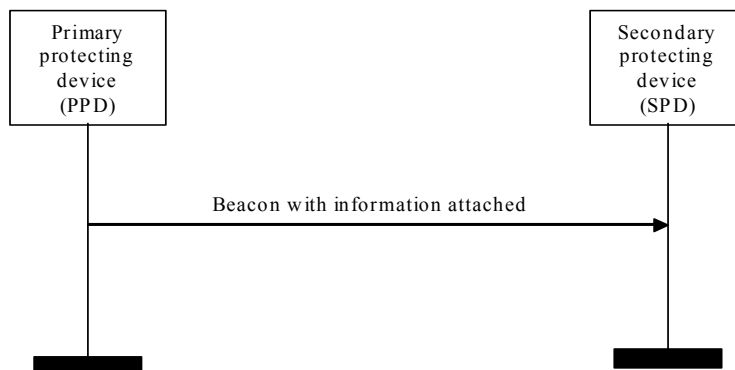


Figure 5—Communication from primary to secondary protecting devices

When an SPD wants to send data to the PPD, it first sends an RTS burst to the PPD during the Rx period of the PPD's superframe. When the PPD receives the RTS burst, it may send the corresponding acknowledgement (ACK) during the ANP (6.5.2). Assuming the PPD does send the corresponding ACK, the PPD then yields the following superframe to the SPD, which then transmits its own superframe, containing its data and the synchronization channel, during this time. Following the transmission by the SPD, the PPD monitors the radio channel during the Rx period in order to check for the appearance of an NPD codeword. The PPD then sends a no acknowledgement (NACK) during the subsequent ANP, since it is required to transmit at least every other beacon frame. Following that, the PPD resumes its normal transmission of the beacon frames. See Figure 6.

Although it is possible for more than one SPD to select and transmit the same RTS codeword during a given receive period and, therefore, possibly cause a collision, the probability is reduced, since there are multiple RTS codewords from which each SPD may choose. However, if this does happen and each SPD receives the ACK corresponding to this RTS codeword, each SPD shall execute the retry procedure (7.4.2). The retry procedure shall also be executed when an SPD sends an RTS codeword but either receives a NACK or an ACK that does not match the transmitted RTS codeword. If the SPD still does not receive the corresponding ACK following the conclusion of the retry procedure, the SPD shall not send a beacon frame.

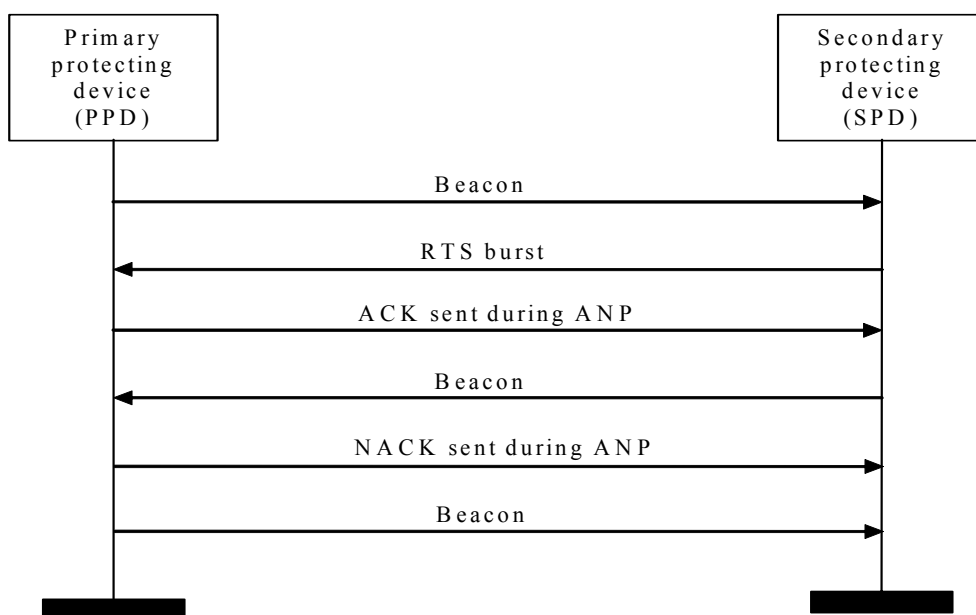


Figure 6—Communication from secondary to primary protecting devices

5.5 Security

It is important that the authenticity of a beacon frame can be determined by a device receiving the beacon frame. If authenticity cannot be determined, security issues could arise. For example, a rogue device may send out an illegitimate beacon to cause another device to leave a particular TV channel (a denial-of-service attack).

A device that operates in the radio frequency (RF) spectrum managed via beacons should, on a regular basis, listen for the potential presence of beacon frames. The security scheme chosen for this standard is based on asymmetric cryptography (i.e., public-key cryptography). Although this choice leads to a larger beacon frame over a symmetric-key approach, the effect of this larger frame size on system performance can be

minimized. The receiving device can trade off network downtime to intercept a beacon, but each MSF must be received sequentially and contiguously. For example MSF1 can be copied alone, or MSF1 plus MSF2, or MSF1 plus MSF2 plus MSF3, but each preceding MSF element must be copied in order to copy the following MSF element. Also, the burden of a larger beacon frame can be offset by a significant simplification in the area of key management. For example, because the beacon frame is comprised of three successive subframes, the receiving device can trade off network downtime and the level of trust to intercept a beacon, recognizing that by copying only MSF1 or MSF1 plus MSF2, the operator is accepting the risk that the beacon that may turn out to be illegitimate. Rather than relying on complex on-line verification (e.g., where symmetric keys needed for verification are kept within the infrastructure) or relying on complex key distribution schemes via tamper-resistant hardware, the asymmetric key approach requires minimal key management for receiving devices. Furthermore, since asymmetric cryptography leads to beacon frames that can be authenticated off-line, it is well-suited for securing inter-beacon communications, where the beaconing devices do not have a backend connection to the infrastructure.

5.5.1 Public-key approach

In this standard, each beaconing device, identified via its MAC address, shall be associated with a public key and corresponding private key. The beaconing device shall use its private key to generate a signature. Any receiving device can use the public key corresponding to a beaconing device's private key to verify a signature. However, a receiving device cannot create a valid signature simply through knowledge of the public key.

In one approach, a trusted authority would assign each beaconing device a unique private/public key pair and give each beaconing device a certificate for the public key. A receiving device would need the appropriate public key to verify a particular beaconing device's signatures. The appropriate public key can be obtained either via a database of MAC address/public key pairs or via a beacon's public-key certificate that a beaconing device shall send over-the-air as part of the beacon frame. When sent over-the-air, the public key is encapsulated into a certificate that is signed by an authority trusted by the receiving device. The authenticity of the received public key can be verified through the help of this certificate.

Figure 4 shows that MSF 2 shall contain the beaconing device's digital signature. This digital signature enables a receiving device to verify the authenticity and timeliness of the contents of the MHR in MSF 1 and the Map field in MSF 2. The signature shall be generated using the beaconing device's private key and can be verified using the receiving device's public key, as specified in 7.5.4. Figure 4 also shows that MSF 3 shall contain a public-key certificate. This certificate enables a receiving device to verifiably acquire the purported public key of the beaconing device. The certificate scheme used in this approach is specified in 7.5.5.

5.5.2 Security considerations

There are a variety of threats that need to be mitigated in a beaconing system. For example, a legitimate beacon could be replayed in an attempt to trick a receiving device into leaving a TV channel. To mitigate a replay attack, the signature is generated not only over the MHR in MSF 1, but also over time and date information. Relay attacks, where a device relays a valid beacon from one geographic location to another may also be possible. A relay attack is mitigated because the MHR contains location information, which is checked during the signature verification. A cryptanalysis attack may also be possible if weak encryption is used. Table 4 in NIST Special Publication 800-57¹¹ has recommended key lengths of cryptosystems for various time frames. It is desirable for this standard to be secure through the year 2030 time frame, so according to NIST, the security level should be at a minimum of 112 bits of strength. NIST also recommends that the cryptoperiod for a private signature key should be limited to 1–3 years (see Table 1 in

¹¹For information on references, see Clause 2.

NIST Special Publication 800-57). As cryptanalysis technology progresses, updates to these recommendations may be needed.

5.5.3 Beaconsing device life cycle

At time of manufacture, the beaconsing device shall be assigned a unique MAC address that will be embedded into its hardware. This MAC address shall resist tampering, i.e., manipulation and change, by any means (e.g., physical, electrical and software). The beaconsing device alone will not be able to generate beacon frames with legitimate signatures, so the end user will need to get a license to operate it. The end user will need to go to a licensing authority (e.g., an industry consortium or an appropriate regulatory body) and obtain a license for that particular beaconsing device (identified via its MAC address) that may be valid for a number of years. This licensing authority would be responsible for provisioning a private key and a public-key certificate to the beaconsing device. It is important that the private key remain a secret, so a good approach would be to provision this private key embedded in a tamper-resistant device such as a secure smart card. The end user would get this smart card, insert it into the beaconsing device, and the smart card would be used to create the beacon frame signatures. If a smart card for a beaconsing device was ever lost, stolen, or decommissioned, the end user could report this to the licensing authority so that a blacklist of devices could be maintained and periodically queried by receiving devices. The certificate would contain an expiration date so that end users would periodically need to renew their licenses to get new certificates (e.g., to enforce NIST's recommended cryptoperiod recommendation). Also, the certificate should be cryptographically bound to a specific beaconsing device's MAC address so that, if the security of a smart card is compromised, this smart card cannot be replicated and easily used with other beaconsing devices.

6. PHY specification

The PHY is responsible for the following tasks:

- Activation and deactivation of the radio transceiver
- Link quality indicator (LQI) for received packets
- TV channel frequency selection
- Data transmission and reception
- Synchronization of PDs
- Generating codewords during the inter-device communication interval (ICI)

Constants and attributes that are specified and maintained by the PHY are written in the text of this clause in italics. Constants have a general prefix of “a”, e.g., *aRegion*, and are listed in Table 18. Attributes have a general prefix of “phy”, e.g., *phyCurrentChannel*, and are listed in Table 19.

6.1 General requirements and definitions

This subclause describes the TV channel/licensed auxiliary service (LAS) channel information, modulation rates and beacon offset location, RF power measurement information, and receiver sensitivity definitions.

6.1.1 TV channel/licensed auxiliary service (LAS) channel information

The region of operation determines the width of the protected TV channels. Protected TV channels may be 6 MHz wide, 7 MHz wide, or 8 MHz wide. Each TV channel is divided into 200 kHz-wide LAS channels, with the lowest frequency LAS channel being centered 100 kHz above the lower edge of the TV channel and the highest frequency LAS channel being centered 100 kHz below the upper edge of the TV channel. A 6 MHz-wide TV channel has 30 LAS channels, while a 7 MHz-wide and an 8 MHz-wide TV channel have 35 and 40 LAS channels, respectively.

Equation (1) gives the location of the center frequency of LAS channel M .

$$\text{LAS channel } M \text{ center frequency} = f_{TV_N} - BW_{TV}/2 + (2M - 1) \times 100 \text{ kHz} \quad (1)$$

where

f_{TV_N} is the center frequency of TV channel N

BW_{TV} is the bandwidth of the TV channel

6.1.2 Modulation rates and beacon offset location for ATSC DTV regions

A beaconing device shall operate using the parameters in Table 1.

Table 1—Modulation rates and beacon offset location for ATSC DTV regions

Offset from lower TV channel edge (kHz)	Chip rate (kchips/s)	Symbol rate (kBaud)
309.4	76.873	9.6091

The beacon offset location was chosen due to its proximity to the DTV pilot frequency; the exact frequency of the DTV pilot frequency is 309.4406 kHz. An explanation of the origin of the chip and symbol rate are given in 6.7.1.6.

Figure 7 illustrates the position of the beacon offset frequency with respect to the LAS channel boundaries.

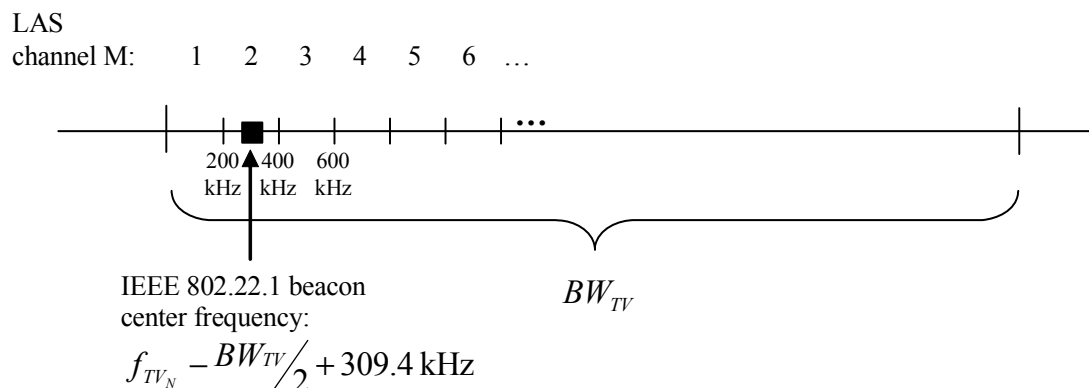


Figure 7—The position of the beacon offset frequency with respect to LAS channel boundaries

6.1.3 RF power measurement information

Unless otherwise stated, all RF power measurements, either transmit or receive, shall be made at the appropriate transceiver-to-antenna connector. The measurements shall be made with the transceiver terminated with the characteristic impedance of the antenna. For devices without an antenna connector, the measurements shall be interpreted as effective isotropic radiated power (EIRP) (i.e., employing a 0 dBi gain antenna), and any radiated measurements shall be corrected to compensate for the antenna gain in the implementation (ANSI C63.17-1998 [B1]).

6.1.4 Receiver sensitivity definitions

The definitions related to the receiver sensitivity and referred to in later subclauses are given in Table 2.

6.2 PHY service specifications

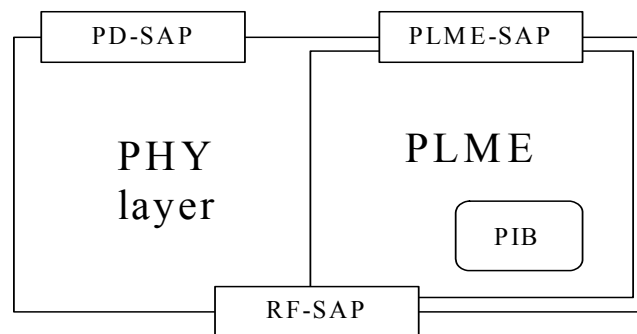
The PHY provides an interface between the MAC sublayer and the physical radio channel. The PHY conceptually includes a management entity called the PHY Layer Management Entity (PLME). The PLME provides a means of passing information between the MAC sublayer and the PHY layer (but not across the air interface). The PLME is also responsible for maintaining a database of variables pertaining to the PHY, which is called the PHY Information Base (PIB).

Figure 8 depicts the components and interfaces of the PHY.

The PHY provides two services, accessed through two service access points (SAPs): the PHY data service, accessed through the PHY data SAP (PD-SAP), and the PHY management service, accessed through the PLME-SAP. The RF-SAP provides a means to pass information across the air interface between the PHY of the present device and that of another device.

Table 2—Receiver sensitivity definitions

Term	Definition of term	Conditions
Packet	One synchronization word, one index value, one MAC subframe of the beacon channel, or one RTS/ANP burst.	– Synchronization word packet = 15 bits – Index value packet = 15 bits – MSF1 beacon packet = 17 uncoded octets (coded: 34 octets using 1:2 encoding) – MSF2 beacon packet = 51 octets – MSF3 beacon packet = 33 octets – RTS/ANP burst packet = 2 octets
Packet error rate (PER)	Average fraction of transmitted packets that are not correctly received.	Averaged over 10 000 superframes in a Gaussian channel with structured MAC synchronization channel data and random MAC beacon channel data.
Sensitivity	Threshold input signal power that yields a specified PER.	– PER = 1%. – Power measured at antenna terminals. – Sensitivities of different packet types will differ due to packet sizes and coding strength (6.8.6).

**Figure 8—PHY reference model**

6.2.1 PHY data service

The PD-SAP is an interface that provides a means of passing MPDUs between the MAC sublayer and the PHY layer. In the case of this standard, the MPDU always contains a beacon frame. Table 3 lists the primitives¹² supported by the PD-SAP. These primitives are discussed in 6.2.1.1 through 6.2.1.3.

Table 3—PD-SAP primitives

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

¹²See Annex F for an overview of the concept of service primitives.

6.2.1.1 PD-DATA.request

The PD-DATA.request primitive is generated by a MAC sublayer entity and issued to its PHY entity to request the transfer of an MPDU (i.e., PSDU). Table 4 specifies the parameters for the PD-DATA.request primitive.

Table 4—PD-DATA.request parameters

Name	Type	Valid range	Description
psdu	Set of octets	—	The set of octets forming the PSDU to be transmitted by the PHY entity.

On receipt of the PD-DATA.request primitive by the PHY entity, the PHY will attempt to transmit the supplied PSDU. Provided the transmitter is enabled, the PHY will construct and transmit a PPDU containing the supplied PSDU. When the PHY entity has completed the transmission, it will issue the PD-DATA.confirm primitive with a status of SUCCESS.

6.2.1.2 PD-DATA.confirm

The PD-DATA.confirm primitive is generated by the PHY entity and issued to its MAC sublayer entity in response to a PD-DATA.request primitive, in order to confirm the end of the transmission attempt of an MPDU (i.e., PSDU) from a local PHY layer entity to a peer PHY layer entity. This primitive has no parameters.

6.2.1.3 PD-DATA.indication

The PD-DATA.indication primitive is generated by the PHY entity and issued to its MAC sublayer entity to transfer a received MPDU (i.e., PSDU). Table 5 specifies the parameters for the PD-DATA.indication primitive.

Table 5—PD-DATA.indication parameters

Name	Type	Valid range	Description
psdu	Set of octets	—	The set of octets forming the PSDU received by the PHY entity.
ppduLinkQuality	Integer	0x00–0xff	The LQI value measured during reception of the PPDU (6.8.9).

6.2.2 PHY management service

The PLME-SAP is an interface that provides a means of passing information between the MAC sublayer and the PHY layer via the MAC sublayer management entity (MLME) and the PLME. Table 6 lists the primitives supported by the PLME-SAP. These primitives are discussed in the clauses referenced in the table.

Table 6—PLME-SAP primitives

PLME-SAP primitive	Request	Indication	Confirm
PLME-ANP-DECISION	6.2.2.1	—	6.2.2.2
PLME-ANP-RESPONSE	—	6.2.2.3	—
PLME-GET	6.2.2.4	—	6.2.2.5
PLME-INITIALIZE	6.2.2.6	—	6.2.2.7
PLME-INITIATE-RTS-BURST	6.2.2.8	—	6.2.2.9
PLME-NPD-ACTIVE	—	6.2.2.10	—
PLME-NPD-HEARTBEAT	6.2.2.11	—	6.2.2.12
PLME-SET	6.2.2.13	—	6.2.2.14
PLME-SET-TRX-STATE	6.2.2.15	—	6.2.2.16

6.2.2.1 PLME-ANP-DECISION.request

The PLME-ANP-DECISION.request primitive is generated by the MLME of the PPD and issued to its PLME to request that the PHY entity send a particular response during the ANP. Table 7 specifies the parameter for the PLME-ANP-DECISION.request primitive.

Table 7—PLME-ANP-DECISION.request parameter

Name	Type	Valid range	Description
ANPResponse	Enumeration	ACK, NACK, GO_ON	The response that the MAC sublayer requests to be sent during the ANP.

On receipt of the PLME-ANP-DECISION.request primitive, the PLME will consider both the ANPResponse parameter received in PLME-ANP-DECISION.request primitive and what was received over the air during the Rx period before making a final decision on which response to send (6.5.2).

6.2.2.2 PLME-ANP-DECISION.confirm

The PLME-ANP-DECISION.confirm primitive is generated by the PLME of the PPD and issued to its MLME in response to a PLME-ANP-DECISION.request primitive. This primitive contains the response transmitted by the PHY layer during the ANP. Table 8 specifies the parameter for the PLME-ANP-DECISION.confirm primitive.

On receipt of the PLME-ANP-DECISION.confirm primitive, the MLME of the PPD is notified of the response transmitted by the PHY layer during the ANP. An ANPResponse parameter equal to either ACK or GO_ON indicates that the PPD will allow an SPD to transmit its beacon frame during the upcoming superframe. An ANPResponse parameter equal to NACK indicates that the PPD will transmit its own beacon frame during the upcoming superframe.

Table 8—PLME-ANP-DECISION.confirm parameter

Name	Type	Valid range	Description
ANPResponse	Enumeration	ACK, NACK, GO_ON	The response transmitted by the PHY layer during the ANP.

6.2.2.3 PLME-ANP-RESPONSE.indication

The PLME-ANP-RESPONSE.indication primitive is generated by the PLME of an SPD and issued to its MLME as a notification of the response received from the PPD during the ANP. This primitive is only issued if the SPD did not send an RTS burst in the Rx period immediately preceding the ANP; see 7.4.5.2 for details on the usage of this primitive. Note that when an SPD does send an RTS burst, it will receive the response via the PLME-INITIATE-RTS-BURST.response primitive (6.2.2.9).

Table 9 specifies the parameter for the PLME-ANP-RESPONSE.indication primitive.

Table 9—PLME-ANP-RESPONSE.indication parameter

Name	Type	Valid range	Description
ANPResponse	Enumeration	ACK, NACK, GO_ON	The response received during the ANP.

6.2.2.4 PLME-GET.request

The PLME-GET.request primitive is generated by the MLME and issued to its PLME to obtain information from the PIB about one or more PIB attributes. Table 10 specifies the parameters for the PLME-GET.request primitive.

Table 10—PLME-GET.request parameters

Name	Type	Valid range	Description
PIBAttribute1	Integer	See Table 19	The identifier of the PIB attribute being requested.
PIBAttribute2	Integer	See Table 19	The identifier of the PIB attribute being requested.
...			
PIBAttributeN	Integer	See Table 19	The identifier of the PIB attribute being requested.

On receipt of the PLME-GET.request primitive, the PLME attempts to retrieve the requested PIB attribute or attributes from its database. Each successfully retrieved PIB attribute will have a corresponding status of SUCCESS in the PLME-GET.confirm primitive. Any PIB attribute value(s) that could not be retrieved will have a corresponding status indicating the appropriate error status (6.2.2.5).

6.2.2.5 PLME-GET.confirm

The PLME-GET.confirm primitive is generated by the PLME and issued to its MLME in response to a PLME-GET.request primitive, and it reports the results of an information request from the PIB. Table 11 specifies the parameters for the PLME-GET.confirm primitive.

Table 11—PLME-GET.confirm parameters

Name	Type	Valid range	Description
Status1	Enumeration	SUCCESS or ATTRIBUTE_NOT_FOUND	The result of the request for PIB attribute information.
PIBAttribute1	Integer	See Table 19	The identifier of the PIB attribute that was requested.
PIBAttributeValue1	Various	Attribute specific	The value of the indicated PIB attribute that was requested. This parameter has zero length when the Status parameter is set to ATTRIBUTE_NOT_FOUND.
Status2	Enumeration	SUCCESS or ATTRIBUTE_NOT_FOUND	The result of the request for PIB attribute information.
PIBAttribute2	Integer	See Table 19	The identifier of the PIB attribute that was requested.
PIBAttributeValue2	Various	Attribute specific	The value of the indicated PIB attribute that was requested. This parameter has zero length when the Status parameter is set to ATTRIBUTE_NOT_FOUND.
...			
StatusN	Enumeration	SUCCESS or ATTRIBUTE_NOT_FOUND	The result of the request for PIB attribute information.
PIBAttributeN	Integer	See Table 19	The identifier of the PIB attribute that was requested.
PIBAttributeValueN	Various	Attribute specific	The value of the indicated PIB attribute that was requested. This parameter has zero length when the Status parameter is set to ATTRIBUTE_NOT_FOUND.

On receipt of the PLME-GET.confirm primitive, the MLME is notified of the results of its request to read one or more PIB attributes. If the request to read a PIB attribute was successful, the corresponding Status parameter is set to SUCCESS. If the identifier of a PIB attribute was not found in the database, the corresponding Status parameter is set to ATTRIBUTE_NOT_FOUND.

6.2.2.6 PLME-INITIALIZE.request

The PLME-INITIALIZE.request primitive is generated by the MLME of the PPD and issued to its PLME upon receipt of the MLME-START-BEACON.request primitive with the Initialize parameter set to TRUE to request that the PD enter the initial transmission period. If the PD is a PPD, the PHY entity will start to transmit a continuous series of superframes, which shall not include inter-device communication intervals, for a period of *aInitializationPeriod* superframes. If the PD is an SPD, the PHY entity will wait for a period of *aInitializationPeriod* superframes before attempting to send an RTS burst. This primitive has no parameters.

6.2.2.7 PLME-INITIALIZE.confirm

The PLME-INITIALIZE.confirm primitive is generated by the PLME of the PPD and issued to its MLME in response to a PLME-INITIALIZE.request primitive once the initial transmission period is over. This primitive has no parameters.

6.2.2.8 PLME-INITIATE-RTS-BURST.request

The PLME-INITIATE-RTS-BURST.request primitive is generated by the MLME of an SPD and issued to its PLME to request that the PHY entity generate an RTS burst packet. The PLME-INITIATE-RTS-BURST.request primitive has no parameters.

Once the burst packet is transmitted and the ANP concludes, the PLME will issue the PLME-INITIATE-RTS-BURST.confirm primitive with the appropriate status (6.2.2.9).

6.2.2.9 PLME-INITIATE-RTS-BURST.confirm

The PLME-INITIATE-RTS-BURST.confirm primitive is generated by the PLME of an SPD and issued to its MLME in response to a PLME-INITIATE-RTS-BURST.request primitive. This primitive confirms that an RTS burst packet was sent by the PHY entity and indicates whether the SPD has permission to send a beacon frame. Table 12 specifies the parameters for the PLME-INITIATE-RTS-BURST.confirm primitive.

Table 12—PLME-INITIATE-RTS-BURST.confirm parameters

Name	Type	Valid range	Description
Status	Enumeration	ACK, INCORRECT_ACK, or NACK	The result of the request to send a beacon frame.

On receipt of the PLME-INITIATE-RTS-BURST.confirm primitive, the MLME is notified whether its request to send a beacon frame was accepted or rejected. The Status parameter shall be set equal to ACK if the request was accepted. If the request was rejected due to the receipt of an acknowledgement codeword that does not match the transmitted RTS codeword (e.g., a competing SPD transmitted a different RTS codeword during the same Rx period), the Status parameter shall be set equal to INCORRECT_ACK. If the request was rejected due to the receipt of a NACK, the Status parameter shall be set equal to NACK.

6.2.2.10 PLME-NPD-ACTIVE.indication

The PLME-NPD-ACTIVE.indication primitive is generated by the PLME of a PD and issued to its MLME as a notification that an NPD codeword has been detected. This primitive has no parameters.

6.2.2.11 PLME-NPD-HEARTBEAT.request

The PLME-NPD-HEARTBEAT.request primitive is generated by the MLME of the SPD that was selected as the NPD and issued to its PLME to request that the PHY entity send the NPD codeword during the upcoming receive period. The PLME-NPD-HEARTBEAT.request primitive has no parameters.

Once the NPD codeword is transmitted, the PLME will issue the PLME-NPD-HEARTBEAT.confirm primitive.

6.2.2.12 PLME-NPD-HEARTBEAT.confirm

The PLME-NPD-HEARTBEAT.confirm primitive is generated by the PLME of the SPD that was selected as the NPD and issued to its MLME in response to a PLME-NPD-HEARTBEAT.request primitive. This primitive confirms that the NPD codeword was sent by the PHY entity. This primitive has no parameters.

On receipt of the PLME-NPD-HEARTBEAT.confirm primitive, the MLME is notified that its request to send the NPD codeword was granted.

6.2.2.13 PLME-SET.request

The PLME-SET.request primitive is generated by the MLME and issued to its PLME to attempt to set the indicated PIB attribute(s) to the given value(s). This primitive may have several pairs of parameters, with each pair specifying a PIB attribute and its corresponding value. Table 13 specifies the parameters for the PLME-SET.request primitive.

Table 13—PLME-SET.request parameters

Name	Type	Valid range	Description
PIBAttribute1	Enumeration	See Table 19	The identifier of the PIB attribute to set.
PIBAttributeValue1	Various	Attribute specific	The value of the indicated PIB attribute to set.
PIBAttribute2	Enumeration	See Table 19	The identifier of the PIB attribute to set.
PIBAttributeValue2	Various	Attribute specific	The value of the indicated PIB attribute to set.
...			
PIBAttributeN	Enumeration	See Table 19	The identifier of the PIB attribute to set.
PIBAttributeValueN	Various	Attribute specific	The value of the indicated PIB attribute to set.

On receipt of the PLME-SET.request primitive, the PLME attempts to write the given value or values to the indicated PIB attributes in its database. Each successfully written PIB attribute will have a corresponding status of SUCCESS in the PLME-SET.confirm primitive. Any PIB attribute value(s) that could not be written will have a corresponding status indicating the appropriate error status (6.2.2.14).

6.2.2.14 PLME-SET.confirm

The PLME-SET.confirm primitive is generated by the PLME and issued to its MLME in response to a PLME-SET.request primitive, and it reports the results of the attempt to write one or more values to their corresponding PIB attributes. Table 14 specifies the parameters for the PLME-SET.confirm primitive.

Table 14—PLME-SET.confirm parameters

Name	Type	Valid range	Description
Status1	Enumeration	SUCCESS, ATTRIBUTE_NOT_FOUND, or INVALID_PARAMETER	The status of the attempt to set the requested PIB attribute.
PIBAttribute1	Enumeration	See Table 19	The identifier of the PIB attribute being confirmed.
Status2	Enumeration	SUCCESS, ATTRIBUTE_NOT_FOUND, or INVALID_PARAMETER	The status of the attempt to set the requested PIB attribute.
PIBAttribute2	Enumeration	See Table 19	The identifier of the PIB attribute being confirmed.
...			
StatusN	Enumeration	SUCCESS, ATTRIBUTE_NOT_FOUND, or INVALID_PARAMETER	The status of the attempt to set the requested PIB attribute.
PIBAttributeN	Enumeration	See Table 19	The identifier of the PIB attribute being confirmed.

On receipt of the PLME-SET.confirm primitive, the MLME is notified of the result of its request to set the value of one or more PIB attributes. If a requested value was successfully written to the indicated PIB attribute, the Status parameter is set to SUCCESS.

If a PIBAttribute parameter specifies an attribute that was not found in the database, the corresponding Status parameter is set to ATTRIBUTE_NOT_FOUND. If a PIBAttributeValue parameter specifies a value that is out of the valid range for the given attribute, the corresponding Status parameter is set to INVALID_PARAMETER.

6.2.2.15 PLME-SET-TRX-STATE.request

The PLME-SET-TRX-STATE.request primitive is generated by the MLME and issued to its PLME to request that the PHY entity change the internal operating state of the transceiver during a superframe period or periods. Table 15 specifies the parameters for the PLME-SET-TRX-STATE.request primitive.

The transceiver has the following three main states:

- Transceiver disabled (TRX_OFF)
- Transmitter enabled (TX_ON)
- Receiver enabled (RX_ON)

On receipt of the PLME-SET-TRX-STATE.request primitive, the PLME will cause the PHY to change the operating state of the transceiver, according to the parameters of this primitive, during the appropriate periods of the following superframe(s). Once the state change is accepted, the PLME will issue the PLME-SET-TRX-STATE.confirm primitive.

For the special case of device initialization (7.4.4), the concept of a superframe period does not yet exist. In order to start the search portion of the device initialization procedure (i.e., following the receipt of the MLME-SEARCH.request primitive by the MLME), a PLME-SET-TRX-STATE.request primitive will be issued with the parameters set in the following way: TRX_State1 = RX_ON, TRX_State2 = RX_ON,

Table 15—PLME-SET-TRX-STATE.request parameters

Name	Type	Valid range	Description
TRX_State1	Enumeration	RX_ON, TX_ON, or TRX_OFF	The new state in which to configure the transceiver during the beaconing portion of the superframe.
TRX_State2	Enumeration	RX_ON, TX_ON, or TRX_OFF	The new state in which to configure the transceiver during the Rx period.
TRX_State3	Enumeration	RX_ON, TX_ON, or TRX_OFF	The new state in which to configure the transceiver during the ANP.
Periodic	Boolean	TRUE or FALSE	If this parameter is TRUE, the operating states of the transceiver will be valid for each superframe that follows, unless a new PLME-SET-TRX-STATE.request primitive is received from the MLME. Otherwise, the operating states will only apply to the upcoming superframe.

TRX_State3 = RX_ON, and Periodic = TRUE. The receiver will remain on until the search portion is over and a new PLME-SET-TRX-STATE.request primitive is issued.

If, upon conclusion of the search portion, the PD promotes itself to PPD, a new PLME-SET-TRX-STATE.request primitive will be issued in order to start the initial transmission period with the parameters set in the following way: TRX_State1 = TX_ON, TRX_State2 = TX_ON, TRX_State3 = TX_ON, and Periodic = TRUE. The transmitter will remain on until the device initialization procedure is over and a new PLME-SET-TRX-STATE.request primitive is issued with the parameters set in the following way: TRX_State1 = TX_ON, TRX_State2 = RX_ON, TRX_State3 = TX_ON, and Periodic = TRUE.

6.2.2.16 PLME-SET-TRX-STATE.confirm

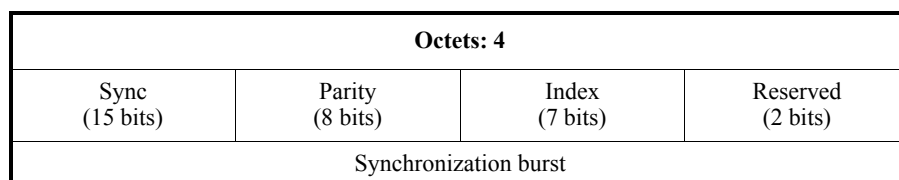
The PLME-SET-TRX-STATE.confirm primitive is generated by the PLME and issued to its MLME upon receipt of a PLME-SET_TRX_STATE.request primitive. This primitive has no parameters.

6.2.3 PHY enumerations description

The enumeration values used by the PHY data and management primitives are given in Table 37.

6.3 Synchronization burst

A synchronization burst is composed of four fields: the Sync field, the Parity field, the Index field, and the Reserved field. The format of the synchronization burst is shown in Figure 9.

**Figure 9—Format of the synchronization burst**

The Sync field is used by a receiver to detect the presence of the synchronization burst and to synchronize to the slot timing. The Sync field shall have the value shown in Table 16.

Table 16—Format of the Sync field

Bits	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Name	s ₀	s ₁	s ₂	s ₃	s ₄	s ₅	s ₆	s ₇	s ₈	s ₉	s ₁₀	s ₁₁	s ₁₂	s ₁₃	s ₁₄
Value	1	1	1	1	0	1	0	1	1	0	0	1	0	0	0

The Index field is used to obtain frame synchronization with an incoming beacon. It contains a numerical value equal to the number of slots remaining (not including the present slot) before the start of the next superframe. The Index field shall be decremented by one each time the data contained within a slot is transmitted until the index reaches either zero or one, depending on whether the PPDU will be followed by a Rx period (6.5.1) and a corresponding acknowledgement/no acknowledgement period (ANP) burst (6.5.2).

If the PPDU will not be followed by a Rx period and a corresponding ANP, the final index shall be zero, and the next superframe shall start immediately thereafter. If the PPDU is to be followed by a Rx period and an ANP, the final index shall be one, and the next superframe shall start immediately after the Rx period and corresponding ANP.

To improve the receive performance of the Index field, a (15, 7) linear block code shall be applied. The Parity field shall be used for both error-correction and error-detection of the index (6.7.2).

The two bits in the Reserved field shall be set to zero.

6.4 PPDU format

Each PPDU packet consists of a constant length payload of length 120 octets, which carries the MAC sublayer beacon frame. The beacon frame is divided into three MAC subframes (MSF), as shown in Figure 4 of Clause 5, and is passed to the PHY layer for inclusion in the PHY payload.

A half-rate convolutional code with puncturing shall be applied by the PHY layer to the first MAC subframe (MSF 1), which includes the three MAC parameter fields, the Source Address field, the Location field, and a 2-octet CRC. The addition of this convolutional code with puncturing increases the PHY payload length by 17 octets, bringing the total length to 118 octets. Then, because the length of a synchronization burst is 4 octets, zero padding shall be added to the end of the PPDU (i.e., following MSF 3) to ensure that its length is a multiple of four. Therefore, the overall length of the PPDU is 120 octets.

For the PPDU packet structure, the multiple octet field shall be transmitted or received least significant octet first and each octet shall be transmitted or received least significant bit (LSB) first.

6.5 Inter-device communication interval (ICI)

The ICI is only excluded from the superframe if the PPD is executing the device initialization procedure (7.4.4). This period consists of the Rx period and the ANP. It is 32 symbols in duration, corresponding to the slot in the superframe immediately following the 30 synchronization bursts and the PPDU. The order of symbols within the ICI is as follows:

- a) 3 symbols of turnaround time
- b) An 11 symbol Rx period composed of
 - 2 symbols of AGC training (since the RTS will be coming from an unfamiliar transmitter)
 - A phase reference symbol for the RTS burst
 - The 8 symbol RTS burst
- c) 4 symbols of turnaround time

- d) A 9 symbol ANP burst composed of
 - A phase reference symbol for the ANP burst
 - The 8 ANP symbols
- e) 4 symbols of turnaround time
- f) A phase reference symbol for the start of the next superframe

The 3 symbol turn-around time is composed of 1 symbol (8 chips) of PPD superframe ramp-down, 1 symbol of propagation delay, and 1 symbol of RTS ramp-up. The first 4 symbol turn-around time has 1 symbol of RTS ramp-down, 2 symbols for propagation delay and processing, and 1 symbol of ANP ramp-up. The second 4 symbol turn-around time has 1 symbol of ANP ramp-down, 2 symbols of propagation delay and processing, and 1 symbol of ramp-up for the next superframe. Figure 10 illustrates an ICI during which an RTS burst is sent by an SPD and an ANP burst is sent by the PPD.

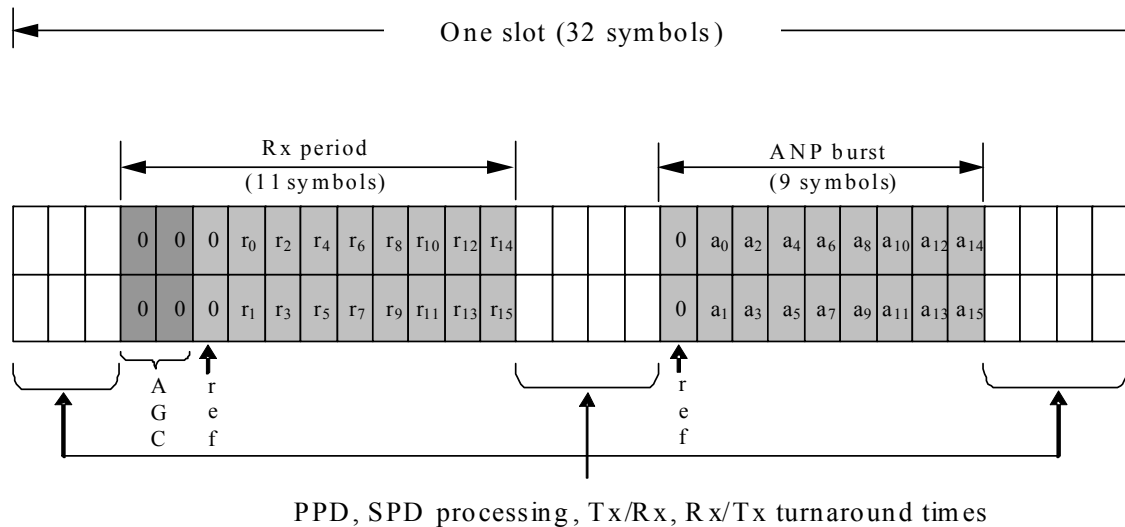


Figure 10—ICI structure

6.5.1 Receive (Rx) period

The Rx period is a length of time equal to 11 symbols that has two purposes. The first is for the PPD to listen for an RTS burst transmission from an SPD. The second is for the PPD to listen for an NPD codeword transmission from the NPD in order to learn whether the NPD is still active.

For convenience, the Rx period structure is presented so that the leftmost field as written in this standard shall be transmitted or received first. All multiple octet fields shall be transmitted or received least significant octet first and each octet shall be transmitted or received LSB first.

The RTS burst is used by an SPD to reserve the next superframe to transmit its beacon frame to the PPD. Each RTS burst consists of an RTS codeword field, and the list of available RTS codewords is given in Table 17, with the exception of the codewords with indices 1 and 32. Note that these two codewords shall not be available as RTS codewords but shall instead be reserved for special purposes that will be explained in the following paragraphs. An SPD shall randomly select an RTS codeword from the list to send in the Rx period; this process shall be repeated prior to each transmission (including retransmissions).

When more than one SPD simultaneously transmits an RTS codeword during the Rx period, the PPD may be able to detect one or more SPDs by their RTS codewords, since each SPD may select a different RTS codeword (6.5.2). In the unlikely event that more than one SPD simultaneously transmits the same RTS

Table 17—List of available codewords

Index	Codeword															
	r_0/a_0	r_1/a_1	r_2/a_2	r_3/a_3	r_4/a_4	r_5/a_5	r_6/a_6	r_7/a_7	r_8/a_8	r_9/a_9	r_{10}/a_{10}	r_{11}/a_{11}	r_{12}/a_{12}	r_{13}/a_{13}	r_{14}/a_{14}	r_{15}/a_{15}
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
4	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0
5	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
6	0	0	1	1	0	0	1	1	1	1	0	0	1	1	0	0
7	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0
8	0	0	1	1	1	1	0	0	1	1	0	0	0	0	1	1
9	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
10	0	1	0	1	0	1	0	1	1	0	1	0	1	0	1	0
11	0	1	0	1	1	0	1	0	0	1	0	1	1	0	1	0
12	0	1	0	1	1	0	1	0	1	0	1	0	0	1	0	1
13	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
14	0	1	1	0	0	1	1	0	1	0	0	1	1	0	0	1
15	0	1	1	0	1	0	0	1	0	1	1	0	1	0	0	1
16	0	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0
17	1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1
18	1	0	0	1	0	1	1	0	1	0	0	1	0	1	1	0
19	1	0	0	1	1	0	0	1	0	1	1	0	0	1	1	0
20	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1
21	1	0	1	0	0	1	0	1	0	1	0	1	1	0	1	0
22	1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1
23	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0	1
24	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
25	1	1	0	0	0	0	1	1	0	0	1	1	1	1	0	0
26	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1
27	1	1	0	0	1	1	0	0	0	0	1	1	0	0	1	1
28	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
29	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1
30	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
31	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
32	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1